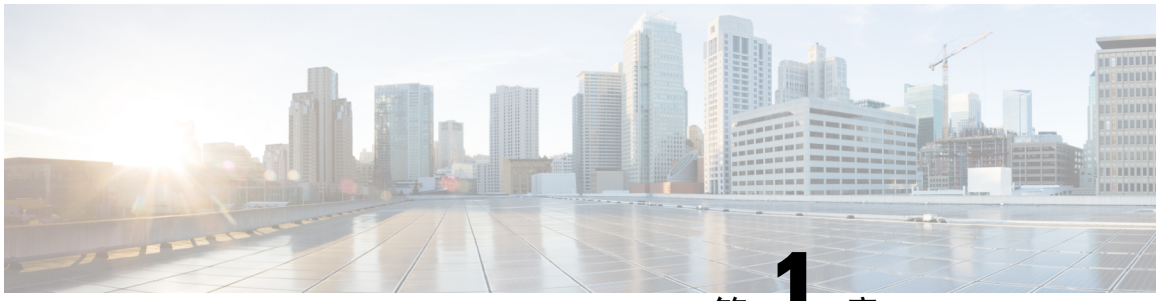
适用于思科邮件安全设备的 AsyncOS 11.0 用户指南

首次发布日期: 2017 年 5 月 31 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录



第 1 章

思科邮件安全设备使用入门

本章包含以下部分：

Async OS 11.0 中的新增功能

表 *1:* 此版本中的新增功能

特性	说明
FIPS 认证	思科邮件安全设备将会经过FIPS认证，并已集成以下FIPS 140-2认可的加密模块：思科通用加密模块（FIPS 140-2 认证编号 1643）。 请参阅FIPS 管理， 第 671 页。
新的防数据丢失 (DLP) 解决方案	RSA 已宣布 RSA 防数据丢失套件的寿命终止 (EOL)。有关详细信息，请参阅 https://community.rsa.com/docs/DOC-59316。 思科现在提供了一种替代DLP解决方案，它允许将RSA DLP中创建的所有现有 DLP 策略无缝迁移到新的 DLP 引擎。升级后，您可以在 Web 界面中的“邮件策略”>“DLP 策略管理器”页面中查看或修改迁移的 DLP 策略。有关详细信息，请参阅用户指南中的“防数据丢失”一章。 **注释** AsyncOS 11.0 和更高版本不支持 RSA 企业管理器集成。如果在 RSA 企业管理器中创建了 DLP 策略，则升级后必须在设备中重新创建这些策略。

特性	说明
支持双因素身份验证	思科邮件安全设备现在支持双因素身份验证，以确保您在登录设备时可以进行安全访问。 您可以通过符合标准 RFC 的任何标准 RADIUS 服务器为您的设备配置双因素身份验证。 可以通过以下方式之一启用双因素身份验证： • Web 界面中的“系统管理”>“用户”页面。请参阅分配管理任务，第 723 页。 • CLI 中的 `userconfig > twofactorauth`。请参阅《适用于思科邮件安全设备的 *AsyncOS CLI* 参考指南》。 如果您在设备上启用了双因素身份验证，则可以使用预共享密钥将其加入集群计算机。使用 CLI 中的 `clusterconfig prepjoin` 命令配置此设置。 请参阅使用集群进行集中管理，第 907 页。

特性	说明
处理来自不同地理位置的传入邮件连接和传入邮件	思科邮件安全设备现在可以处理来自特定地理位置的传入邮件连接和传入邮件，并对这些邮件执行适当的操作，例如： • 防止来自特定地理区域的邮件威胁。 • 允许或禁止来自特定地理区域的邮件。 可通过以下方式使用此功能： • **SMTP 连接级别**。现在，您可以使用下列方式之一将发件人组配置为处理来自特定地理位置的传入邮件连接： • Web 界面中的“邮件策略”>“HAT 概述”>“添加发件人组”>“提交并添加发件人”>**地理位置**选项。 • CLI 中的 `listenerconfig > hostaccess > country` 命令。 有关详细信息，请参阅“使用主机访问表定义允许连接的主机，第 81 页”或适用于思科邮件安全设备的 *AsyncOS CLI* 参考指南》。 您可以使用**地理分布**报告基于发件人的来源国家/地区查看来自特定地理位置的传入邮件连接的详细信息。有关更多信息，请参阅“使用邮件安全监控，第 637 页”。 • **内容或邮件过滤级别**：您现在可以创建内容或邮件过滤器来处理来自特定地理位置的传入邮件，并对这些邮件执行适当的操作。内容和邮件过滤器包括以下新选项： • 新的内容过滤器条件 - **地理位置** • 新的邮件过滤器规则 - `geolocation-rule()`。 有关详细信息，请参阅内容过滤器，第235页或使用邮件过滤器实施邮件策略，第 117 页。 可以使用“内容过滤器”和“邮件过滤器”报告查看由内容或邮件过滤器检测到的来自特定地理位置的传入邮件详细信息。请参阅使用邮件安全监控，第 637 页。 可以使用邮件跟踪来搜索内容或邮件过滤器检测到的来自特定地理位置的传入邮件。为邮件跟踪的“高级”部分中的“邮件事件”选项使用**地理位置**过滤器。 国家/地理的地理位置列表可进行云更新。

特性	说明
使用 AMP 引擎扫描传出邮件	现在，您可以将设备配置为使用 AMP 引擎扫描传出邮件。 可以使用此功能执行以下操作： • 防止用户通过组织的网络发送恶意邮件，否则可能造成 IP 或域的信誉较低。 • 跟踪发送包含恶意附件的出站邮件的用户，并对其执行适当的操作。 您可以通过以下方式之一将设备的传出邮件策略配置为允许由 AMP 引擎扫描邮件： • Web 界面中的“邮件策略”>“传出邮件策略”页面。请参阅文件信誉过滤和文件分析：，第 353 页。 • CLI 中的 `policyconfig` 命令。 以下报告已得到增强，以显示 AMP 引擎扫描的传出邮件的详细信息： • 高级恶意软件防护 • AMP 文件分析 • AMP 判定更新 • “概述”页面 • 外发目标 • 外发邮件发件人 • 内部用户 请参阅 使用邮件安全监控，第 637 页 您可以在“邮件跟踪”>“邮件事件”>“高级恶意软件保护”选项中的“邮件流方向”过滤器搜索 AMP 引擎扫描的传入和传出邮件。

特性	说明
手动回滚到服务引擎的上一个版本	现在，您可以在以下情况下手动回滚到当前引擎的上一个版本： • 引擎更新有缺陷。 • 引擎无法正常工作。 目前，您可以对以下引擎执行引擎回滚： • McAfee • Sophos • Graymail 只能在计算机级别而不能在集群级别执行引擎回滚。 可以使用 Web 界面中的“安全服务”>“服务概述”页面执行以下操作： • 回滚到服务引擎的上一个版本。 • 将服务引擎手动更新到所需的版本。 有关详细信息，请参阅 系统管理，第 749 页
启用或禁用自动更新	现在，您可以在以下服务引擎的“全局设置”页面中启用或禁用自动更新： • McAfee • Sophos • Graymail 您现在可以在面向特定服务引擎禁用自动更新时收到定期警报。可以通过以下方式之一更改现有警报级别： • Web 界面中的“安全服务”>“服务更新”>“禁用的自动引擎更新的警报间隔”选项。请参阅系统管理，第 749 页。 • CLI 中的 `updateconfig` 命令。
对邮件策略中的高级恶意软件保护检测到的附件执行其他操作	如果附件在传入或传出邮件策略的“高级恶意软件保护”部分中被视为“恶意”、“不可扫描”或“已送交进行文件分析”，可以执行以下附加操作： • 修改邮件收件人。 • 将邮件发送到备用目标主机。 有关详细信息，请参阅文件信誉过滤和文件分析：，第 353 页。

特性	说明
改进的 AMP 引擎日志	有关以下方案的信息现在记录在 AMP 引擎日志中： • 未上传到文件分析服务器的文件。 • 因设备超出了文件分析服务器的每日文件上传限制而跳过进行文件分析的文件。 • 标记为不可扫描的文件。
支持进行内容扫描的存档文件格式	设备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

特性	说明
宏检测增强功能	现在，可以检测以下文件中的宏： • Adobe Acrobat 便携式文档格式 (PDF) 文件中的 Javascript 宏。 • Microsoft Office 文件（开放式 XML）和 OLE 文件中的 Visual Basic for Application (VBA) 宏。 有关详细信息，请参阅内容过滤器，第 235 页或使用邮件过滤器实施邮件策略，第 117 页。
对 Web 界面登录进行 CRL 检查	您可以使用以下方式之一配置对 Web 界面登录的 CRL 检查： • Web 界面中的“网络”>“CRL 源”>“编辑设置”>“对 Web UI 的 CRL 检查”选项。 请参阅 使用客户端证书对 SMTP 会话进行身份验证，第 629 页 • CLI 中的 `certconfig > crl` 命令。 如果启用此选项并且吊销了证书： • 您将收到一个警报，指示证书已被吊销。 • 您将无法访问设备的 Web 界面。但是，您仍然可以使用 CLI 登录设备。 您必须通过 CLI 导入和配置有效证书，才能访问设备的 Web 界面。请参阅《用于思科邮件安全设备的 *AsyncOS CLI* 参考指南》。
为文件信誉处置值配置缓存有效期。	可以通过以下方式之一配置文件信誉处置值的缓存有效期： • Web 界面中的“安全服务”>“文件信誉和分析”>“缓存设置”页面。 • CLI 中的 `ampconfig > cachesettings > modifytimeout` 命令。 请参阅文件信誉过滤和文件分析：，第 353 页。

特性	说明
在欧洲地区为文件信誉和文件分析服务增加的新数据中心	思科在欧洲地区为文件信誉和文件分析服务增加了新数据中心： • EUROPE *(cloud-sa.eu.amp.cisco.com)*，适用于文件信誉服务器 • EUROPE *(https://panacea.threatgrid.eu)*，适用于文件分析服务器 您可以将邮件安全设备配置为使用新的文件信誉和文件分析服务。有关详细信息，请参阅文件信誉过滤和文件分析：，第 353 页。

哪里可以获得详细信息

思科提供以下资源用于了解有关设备的更多信息：

文档

可通过点击右上角的“帮助和支持”(Help and Support)，直接从设备 GUI 访问联机帮助版本的用户指南。

思科内容安全设备的文档集包括以下文档和手册：

- 版本说明
- 思科邮件安全设备模型快速入门指南
- 所用型号或系列的硬件安装或硬件安装与维护指南
- 思科内容安全虚拟设备安装指南
- 适用于思科邮件安全设备的 *AsyncOS* 用户指南（本手册）
- 适用于思科邮件安全设备的 *AsyncOS CLI* 参考指南
- 适用于思科邮件安全设备的 AsyncOS API - 使用入门指南

所有思科内容安全产品的文档均可从以下位置获取：

思科内容安全产品的文档	位置
硬件和虚拟设备	请参阅此表中适用的产品。
思科邮件安全	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd- products-support-series-home.html
思科网络安全	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products- support-series-home.html
思科内容安全管理	http://www.cisco.com/c/en/us/support/security/content-security-management- appliance/tsd-products-support-series-home.html

思科内容安全产品的文档	位置
适用于思科内容安全设备的 CLI 参考指南	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
思科 IronPort 加密	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html

培训

有关培训的详细信息可从以下网址获得：

- http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html
- http://www.cisco.com/c/en/us/training-events/training-certifications/overview.html

思科通知服务

注册可接收与您的思科内容安全设备相关的通知，例如安全建议、现场通知、停止销售或停止支持声明，以及有关软件更新和已知问题的信息。

可以指定通知频率和接收的信息类型等选项。有关使用的每种产品的通知，应单独注册。

要进行注册，请访问 http://www.cisco.com/cisco/support/notifications.html

需要有 Cisco.com 帐户。如果没有，请参阅注册思科帐户，第 10 页。

知识库

步骤 1 转到主产品页面 (http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html)

步骤 2 查找名称中包含 **TechNotes** 的链接。

思科支持社区

思科支持社区是一个面向思科客户、合作伙伴和员工的在线论坛。它提供了一个讨论常规电邮和web安全问题以及有关具体思科产品的技术信息的场合。您可以向论坛发布主题咨询问题，并与其他思科用户分享信息。

请通过以下 URL 访问客户支持门户上的思科支持社区：

- 针对邮件安全和相关管理：

  https://supportforums.cisco.com/community/5756/email-security

- 针对网络安全和相关管理：

https://supportforums.cisco.com/community/5786/web-security

思科客户支持

思科 TAC：http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

旧版 IronPort 的支持站点：http://www.cisco.com/c/en/us/services/acquisitions/ironport.html

对于普通问题，您还可以联系设备客户支持人员。有关说明，请参阅用户指南或在线帮助。

第三方贡献者

有关与您的版本对应的开源代码授权信息，请访问以下页面：
http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-release-notes-list.html。

Cisco AsyncOS 的某些软件根据 FreeBSD, Inc.、Stichting Mathematisch Centrum、Corporation for National Research Initiatives, Inc. 及其他第三方贡献者的软件许可协议条款、通知和条件分发，所有此类条款和条件均包含在思科许可协议当中。

这些协议的全文可通过以下网站查看：

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html。

经 Tobi Oetiker 明确书面同意，Cisco AsyncOS 的部分软件基于 RRDtool。

本文档中部分相关内容的复制已取得 Dell Computer Corporation 的许可。本文档中部分相关内容的复制已取得 McAfee, Inc. 的许可。本文档中部分相关内容的复制已取得 Sophos Plc 的许可。

思科欢迎您发表意见

思科技术出版物团队乐于提高产品文档的质量。我们时刻欢迎您的评论和建议。您可以将评论发送至以下电邮地址：

contentsecuritydocs@cisco.com

请在邮件主题中提供产品名称、版本号和文档发布日期。

注册思科帐户

要访问 Cisco.com 上的许多资源，都需要有思科帐户。

如果您没有 Cisco.com 用户 ID，可以点击以下链接进行注册：
https://tools.cisco.com/RPF/register/register.do%20

相关主题

- 思科通知服务，第 9 页
- 知识库，第 9 页

思科邮件安全设备概述

AsyncOS™ 操作系统包括以下功能：

- 网关处的**反垃圾邮件**，通过 SenderBase 信誉过滤器和思科反垃圾邮件集成的独特多层方法。
- 网关处的**防病毒**，使用 Sophos 和 McAfee 防病毒扫描引擎。
- **病毒爆发过滤器™**，思科针对新病毒、诈骗和网络钓鱼爆发提供的独特预防保护，可以隔离危险邮件，直到应用新的更新，从而缩短新邮件威胁的漏洞窗口。
- **策略、病毒和爆发隔离区**提供一个安全的位置来存储可疑邮件供管理员评估。
- 内部或外部的**垃圾邮件隔离区**，使终端用户可以访问隔离的垃圾邮件和疑似垃圾邮件。
- **邮件身份验证**。Cisco AsyncOS 支持各种不同形式的邮件身份验证，包括传入邮件的发件人策略框架 (SPF)、发件人 ID 框架 (SIDF) 和 DomainKeys 确定的邮件 (DKIM) 验证，以及传出邮件的 DomainKeys 和 DKIM 签名。
- 思科**邮件加密**。可以加密传出邮件以满足 HIPAA、GLBA 或类似的管理需求。为此，需要在邮件安全设备上配置加密策略并使用本地密钥服务器或托管密钥服务来加密邮件。
- **邮件安全管理器**，一个综合控制面板，用于管理设备中的所有邮件安全服务和应用。邮件安全管理器可以基于用户组实施邮件安全，以便通过不同的入站和出站策略管理思科信誉过滤器、病毒爆发过滤器、反垃圾邮件、防病毒和邮件内容策略。
- **机上邮件跟踪**。AsyncOS for Email 包含机上邮件跟踪功能，可帮助轻松获取邮件安全设备所处理邮件的状态。
- 针对入站和出站邮件的**邮件流监控**，用于全面了解企业的所有邮件流量。
- 基于发件人的 IP 地址、IP 地址范围或域，针对入站发件人的**访问控制**。
- 广泛的**邮件和内容过滤**技术，用于实施公司策略并在特定邮件进入或离开公司基础设施时执行相应操作。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。过滤器操作允许删除、退回、存档、密件复制或更改邮件，或者生成通知。
- **通过传输层安全使用安全 SMTP 进行邮件加密**可确保加密在公司基础设施与其他可信主机之间传输的邮件。
- **Virtual Gateway™** 技术允许邮件安全设备在单个服务器中用作多个邮件网关，以便划分不同来源或活动中的邮件以通过单独的 IP 地址发送。这样可以确保影响一个 IP 地址的可传送性问题不会影响其他 IP 地址。
- **防止恶意附件和链接**（在邮件中），由多个服务提供。
- 使用**防数据丢失**控制和监控从组织传出的信息。

AsyncOS 支持符合 RFC 2821 标准的简单邮件传输协议 (SMTP)，以接受并传输邮件。

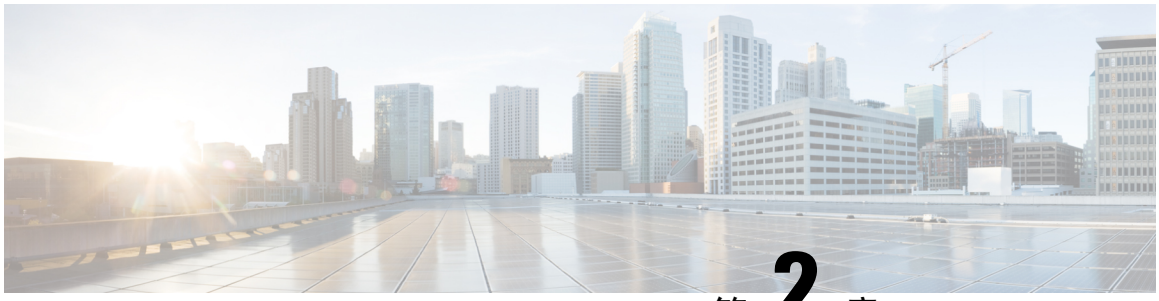
大多数报告、监控和配置命令都可通过基于 Web 的 GUI 和 HTTP 或 HTTPS 使用。此外，还为系统提供了从 Secure Shell (SSH) 或直接串行连接访问的交互式命令行界面 (CLI)。

您还可以设置安全管理设备，来统一管理多个邮件安全设备的报告、跟踪和隔离管理。

支持的语言

AsyncOS 可使用以下任何语言显示其 GUI 和 CLI：

- 英语
- 法语
- 西班牙语
- 德语
- 意大利语
- 韩语
- 日语
- 葡萄牙语（巴西）
- 中文（繁体和简体）
- 俄语



第 2 章

访问设备

本章包含以下部分：

基于 Web 的图形用户界面 (GUI)

可以使用基于 Web 的图形用户界面 (GUI) 和命令行界面 (CLI) 管理设备。GUI 包含配置和监控系统所需的多数功能。但是，并非所有 CLI 命令在 GUI 中都提供；某些功能只能通过 CLI 提供。

浏览器要求

要访问基于 Web 的 UI，您的浏览器必须支持和能够接受 JavaScript 和 Cookie，而且还必须能够显示包含级联样式表 (CSS) 的 HTML 页面。

浏览器	操作系统
Internet Explorer 11.0	Microsoft Windows 7
Safari 7.0 及更高版本	Mac OS X
Firefox 39.0 及更高版本	Microsoft Windows 7，Mac OS X
Chrome 44.0 及更高版本	Microsoft Windows 7，Mac OS X

请勿同时使用多个浏览器窗口或选项卡对设备进行更改。也不要使用并行 GUI 和 CLI 会话。否则将会导致意外行为，且不受支持。

要使用 Web 界面，可能需要配置浏览器的弹出阻止设置，因为界面中的某些按钮或链接会导致其他窗口打开。

访问 GUI

要在全新的系统中访问 GUI，请访问以下 URL：

http://192.168.42.42/

显示登录页面时，使用默认的用户名和密码登录系统。

出厂默认用户名和密码

- 用户名：**admin**
- 密码：**ironport**

在全新的（不是从以前的 AsyncOS 版本升级而来）系统上，您将自动重定向到系统设置向导。

在初始系统设置期间，需要为接口选择 IP 地址以及是否为这些接口运行 HTTP 和 HTTPS 服务。为接口启用 HTTP 和/或 HTTPS 服务后，可以使用任意支持的浏览器查看 GUI，只需在浏览器的位置区域（即“地址栏”）输入 IP 接口的 IP 地址或主机名作为 URL 即可。

例如：

`http://192.168.1.1` 或

`https://192.168.1.1` 或

`http://mail3.example.com` 或

`https://mail3.example.com`

注释 如果已为某个接口启用了 HTTPS（而且 HTTP 请求未被重定向到安全服务），请记住使用“`https://`”前缀访问 GUI。

相关主题

- 添加用户，第 726 页

集中管理

如果您创建了一个集群，则可以在集群中浏览计算机，也可以从 GUI 内在集群、组和计算机之间创建、删除、复制和移动设置（即执行 `clustermode` 和 `clusterset` 命令的等价命令）。

有关详细信息，请参阅通过 GUI 管理集群，第 921 页。

更改配置设置

配置更改

您可以在邮件操作正常进行的同时，对配置进行更改。

提交或放弃更改

您必须明确保存多数配置更改。

更改等待确认时，“确认更改”(Commit Changes) 按钮变为橙色。

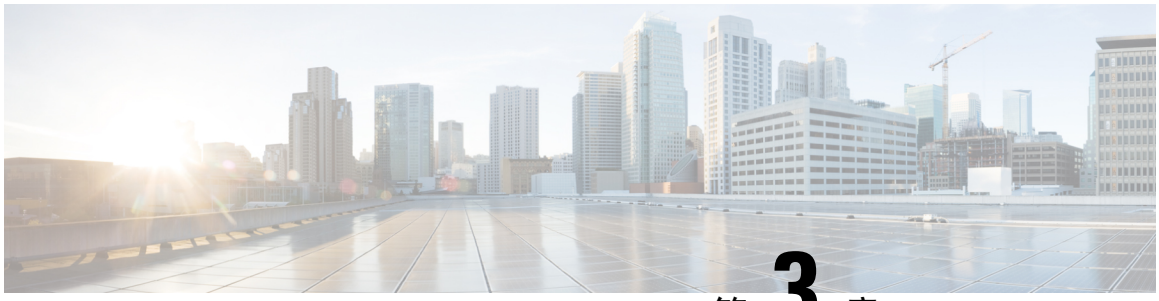
要清除或确认这些更改，请点击**确认更改 (Commit Changes)**。

命令行界面 (CLI)

命令行界面可通过（已配置为启用这些服务的）IP 接口上的 SSH 访问或串行端口上的终端仿真软件访问。默认情况下，SSH 在管理端口上配置。使用 `interfaceconfig` 命令禁用这些服务。

有关CLI命令和约定的详细信息，请参阅《适用于思科邮件安全设备的AsyncOS的CLI参考指南》。

注释 访问 CLI 的出厂默认用户名和密码与网络界面相同。请参阅出厂默认用户名和密码，第 14 页。



第 3 章

设置和安装

本章包含以下部分：

安装规划

查看影响规划决策的信息

- 如果您要配置虚拟邮件安全设备，请先参阅思科内容安全虚拟设备安装指南，然后再继续阅读本章。
- 如果您要配置 M 系列思科内容安全管理设备，请参阅在思科内容（M 系列）安全管理设备上集中管理服务，第 969 页。
- 我们建议在安装之前先查看了解邮件通道，第 51 页，因为某些特性和功能可能会影响您的基础设施中设备的放置。

计划将邮件安全设备放置在网络外围

您的邮件安全设备旨在用作SMTP网关，也称为邮件交换(MX)。为获得最佳效果，某些功能要求设备是具有可直接访问互联网的 IP 地址的第一台机器（即它是外部 IP 地址）才能发送和接收邮件。

根据收件人的信誉过滤，反垃圾邮件、防病毒和爆发过滤器功能（请参阅 SenderBase网络参与，第 833 页、IronPort 反垃圾邮件过滤，第 271 页、Sophos 防病毒过滤，第 254 页和病毒爆发过滤器，第 307 页）旨在处理互联网和内部网络邮件的直接流量。您可以配置设备，对传入及传出企业的所有邮件流量进行策略实施（有关定义允许连接哪些主机的概述，第 81 页）。

确保邮件安全设备可通过公共互联网访问，且是您的邮件基础设施中的“第一跳”。如果允许另一个 MTA 位于网络周界并处理所有外部连接，则邮件安全设备将无法确定发件人的 IP 地址。需要发

件人的 IP 地址才能识别和区分邮件流监控中的发件人，以查询 SenderBase 信誉服务获得发件人的 SenderBase 信誉得分 (SBRS)，以及提高反垃圾邮件和爆发过滤器功能的效果。

注释 如果无法将设备配置为从互联网接收邮件的第一台机器，仍可以使用设备上提供的一些安全服务。有关详细信息，请参阅通过传入中继确定部署中的发件人 IP 地址，第 286 页。

当您将邮件安全设备用作 SMTP 网关时：

- 通过邮件流监控功能（请参阅使用邮件安全监控，第 637 页），可以全面了解贵企业中来自内部和外部发件人的所有邮件流量。
- LDAP 路由、别名和伪装查询（请参阅LDAP 查询，第 585 页）可以整合您的目基础设施并提供更简单的更新。
- 别名表（请参阅创建别名表，第 528 页）、基于域的路由（域映射功能，第 544 页）和伪装（配置伪装，第 535 页）等熟悉的工具可以让您更轻松地从开源 MTA 进行过渡。

在 DNS 中注册邮件安全设备

恶意邮件发件人会主动搜索公共 DNS 记录寻找新的受害者。为了充分利用反垃圾邮件、爆发过滤器、McAfee 防病毒和 Sophos 防病毒功能，请确保在 DNS 中注册邮件安全设备。

要在 DNS 中注册设备，请创建一条 A 记录，将设备的主机名映射到其 IP 地址，再创建一条 MX 记录，将您的公共域映射到设备的主机名。您必须为 MX 记录指定优先级，才能将邮件安全设备公布为域的主 MTA 或备用 MTA。

在下面的示例中，邮件安全设备 (ironport.example.com) 是域 example.com 的备用 MTA，因为其 MX 记录具有更高的优先级值 (20)。换句话说，该数值越大，MTA 的优先级越低。

```
$ host -t mx example.com
example.com mail is handled (pri=10) by mail.example.com
example.com mail is handled (pri=20) by ironport.example.com
```

通过在 DNS 中注册邮件安全设备，无论如何设置 MX 记录的优先级，都将吸引垃圾邮件攻击。但是，病毒攻击很少会瞄准备用 MTA。在这种情况下，如果您最终分地挖掘出防病毒引擎的潜能，请将邮件安全设备的 MX 记录优先级值设置为等于或高于其他 MTA 值。

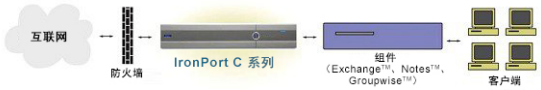
安装情景

您可以采用多种方式在现有网络基础设施中安装邮件安全设备。

以下情景代表了大多数客户的网络配置。如果您的网络配置有很大的差异，并且您需要获得有关安装规划方面的帮助，请联系思科客户支持（请参阅思科客户支持，第 10 页）。

配置概述

下图显示邮件安全设备在企业网络环境中的典型安装。



在某些情况下，邮件安全设备位于网络“DMZ”内，此时邮件安全设备和组件服务器之间会有一道额外的防火墙。

下面介绍以下网络方案：

- 防火墙背后：两个侦听程序配置（图 - 防火墙背后情景/2 个侦听程序配置）

选择与您的基础设施最匹配的配置。然后继续下一部分为系统设置做好准备，第 23 页。

传入

- 您指定的本地域接受传入邮件。
- 所有其他域都将被拒绝。
- 外部系统直接连接到邮件安全设备以在本地域中传输邮件，邮件安全设备通过 SMTP 路由将邮件中继到适当的组件服务器（例如，Exchange™、Groupwise™、Domino™）。（请参阅路由本地域的邮件，第 523 页。）

传出

- 内部用户发送的传出邮件通过组件服务器路由到邮件安全设备。
- 邮件安全设备根据私人侦听程序的主机访问表中的设置接受传出邮件。（有关详细信息，请参阅 使用侦听程序，第 62 页。）

以太网接口

在这些配置中，只需要邮件安全设备上的一个可用以太网接口。但是，您可以配置两个以太网接口，并将您的内部网络与外部互联网连接分开。

有关将多个 IP 地址分配到可用接口的详细信息，请参阅使用虚拟网关™ 技术为所有托管的域配置邮件网关，第 570 页和分配网络和 IP 地址，第 985 页。

硬件端口

硬件设备上端口的数量和类型取决于型号：

端口	Type	C170	C370	C670	X1070	C380	C680	C190	C390	C690
管理	以太网	0	1	1	1	1	1	0	1	1
数据	以太网	2*	3	3	3	3	3	2*	5	5
控制台	序列	9 针	9 针	9 针	9 针	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45

端口	Type	C170	C370	C670	X1070	C380	C680	C190	C390	C690
远程电源管理 (RPC)	以太网	N	N	N	N	支持	支持	支持	支持	支持

*对于没有专用管理端口的设备，请使用 Data1 端口进行管理。

有关端口的详细信息，请参阅您的设备型号对应的硬件安装指南。

高级配置

除了图 - 防火墙后情景/2 个侦听程序配置和图 - 1 个侦听程序配置中显示的配置之外，还可以配置:

- 使用集中管理功能的多个邮件安全设备。请参阅 使用集群进行集中管理，第 907 页
- 网络接口卡级别的冗余，方法是使用 NIC 配对功能“组合”邮件安全设备上的两个以太网接口。请参阅 高级网络配置，第 841 页

防火墙设置（NAT，端口）

SMTP 和 DNS 服务必须具有互联网访问权限。其他服务可能也需要打开的防火墙端口。有关详细信息，请参阅防火墙资讯，第 1005 页。

将邮件安全设备通过物理方式连接到网络

配置场景

邮件安全设备的典型配置场景如下：

- **接口** - 大多数网络环境只需要邮件安全设备上三个可用以太网接口中的一个。但是，您可以配置两个以太网接口，并将您的内部网络与外部互联网连接分开。
- **公共侦听程序（传入邮件）** - 公共侦听程序接收来自许多外部主机的连接并将邮件定向到数量有限的内部组件服务器。
  - 根据主机访问表 (HAT) 中的设置接受来自外部邮件主机的连接。默认情况下，HAT 配置为接受来自所有外部邮件主机的连接。
  - 仅当为收件人访问表 (RAT) 中指定的本地域寻址时接受传入邮件。所有其他域都将被拒绝。
  - 将邮件中继到适当的内部组件服务器，如 SMTP 路由所定义。
- **私人侦听程序（传出邮件）** - 私人侦听程序接收来自数量受限的内部组件服务器的连接，并将邮件定向到许多外部邮件主机。
  - 内部组件服务器配置为将传出邮件路由到思科 C 或 X 系列设备。
  - 邮件安全设备根据 HAT 中的设置接受来自内部组件服务器的连接。默认情况下，HAT 配置为中继来自所有内部邮件主机的连接。

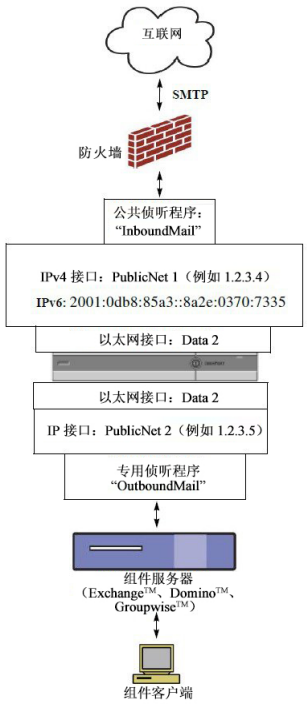
将传入和传出邮件分离

您可以通过单独的侦听程序以及在单独的 IP 地址上分离传入和传出邮件流量。您可以使用互联网协议第 4 版 (IPv4) 和第 6 版 (IPv6) 地址。但是，设备上的系统设置向导支持下列初始配置：

- 在独立的物理接口上配置的 2 个逻辑 IPv4 和 2 个 IPv6 地址上的 2 个独立侦听程序
  - 分离传入和传出流量
  - 您可以将 IPv4 和 IPv6 地址分配到每个侦听程序
- 在一个物理接口配置的 1 个逻辑 IPv4 地址上的 1 个侦听程序
  - 合并传入和传出流量
  - 您可以将 IPv4 和 IPv6 地址都分配到侦听程序

下面包括了一个和两个侦听程序配置的配置工作表（请参阅收集设置信息，第 26 页）。大多数配置情景都通过以下三个图之一表示。

图 *1:* 防火墙保护的场景*/2* 个侦听程序配置



注：

- 2 个侦听程序
- 2 个 IPv4 地址
- 2 个 IPv6 地址
- 1 个或 2 个以太网接口（仅显示了 1 个接口）

- 配置的 SMTP 路由

入站侦听程序：“InboundMail”（公共）

- IPv4 地址：1.2.3.4
- IPv6 地址：2001:0db8:85a3::8a2e:0370:7334
- Data2 接口上的侦听程序侦听端口 25
- HAT（全部接受）
- RAT（接受本地域的邮件；全部拒绝）

出站侦听程序：“OutboundMail”（专用）

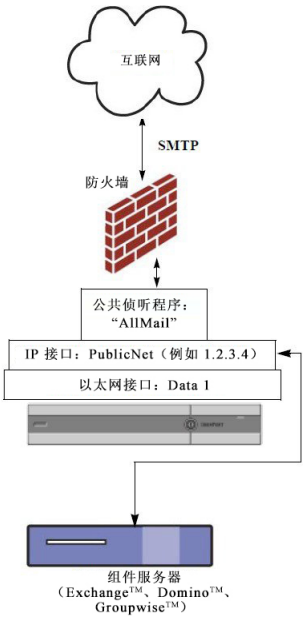
- IP 地址：1.2.3.5
- IPv6 地址：2001:0db8:85a3::8a2e:0370:7335
- Data2 接口上的侦听程序侦听端口 25
- HAT（中继本地域；全部拒绝）

DNS 可配置为使用互联网根服务器或内部 DNS 服务器

SMTP 将邮件直接路由到适当的组件服务器

为适当的服务打开的防火墙端口，用于在与邮件安全设备之间传输数据

图 *2:* 一个侦听程序配置



注意：

- 1 个侦听程序
- 1 个 IP 地址
- 1 个以太网接口
- 配置的 SMTP 路由

入站侦听程序：“InboundMail”（公共）

- IP 地址：1.2.3.4
- Data2 接口上的侦听程序侦听端口 25
- HAT（接受 ALL）包括 RELAYLIST 中组件服务器的条目
- RAT（接受本地域的邮件；全部拒绝）

DNS 可配置为使用互联网根服务器或内部 DNS 服务器

SMTP 将邮件直接路由到适当的组件服务器

为适当的服务打开的防火墙端口，用于在与设备之间传输数据

为系统设置做好准备

过程

	命令或操作	目的
步骤 1	确定如何连接到设备。	请参阅 确定连接设备的方式，第 24 页
步骤 2	确定网络和 IP 地址分配。 • 如果您已将设备连接到网络，请确保邮件安全设备的默认 IP 地址与网络中的其他 IP 地址不冲突。	请参阅 确定连接设备的方式，第 24 页 和 确定网络和 IP 地址分配，第 24 页
步骤 3	收集系统设置的相关信息。	请参阅收集设置信息，第 26 页。
步骤 4	查看设备的最新产品版本说明。	有关版本说明，请访问文档，第 8 页中的链接。
步骤 5	打开设备包装，在机架中对设备进行物理安装，然后将其打开。	请参阅设备的《快速入门指南》。如需该指南，请访问文档，第 8 页中的链接。
步骤 6	如果使用命令行界面 (CLI) 运行安装向导，请访问 CLI。	请参阅运行命令行界面 (CLI) 系统设置向导，第 38 页）
步骤 7	如果使用 Web 界面运行安装向导，请执行以下操作：	1. （仅限虚拟设备）使用 `interfaceconfig` 命令访问命令行界面并启用 HTTP 和/或 HTTPS。 2. 启动 Web 浏览器并输入设备的 IP 地址。

	命令或操作	目的
步骤 8	如果设置的是虚拟邮件安全设备，请加载虚拟设备许可证。	使用 `loadlicense` 命令。有关详细信息，请参阅思科内容安全虚拟设备安装指南，该指南在文档，第 8 页中的链接中提供。
步骤 9	配置系统的基本设置。	请参阅 使用系统设置向导，第 29 页

确定连接设备的方式

要在您的环境中成功设置邮件安全设备，您必须从网络管理员那里收集有关您想如何将邮件安全设备连接到网络的重要网络信息。

连接到设备

在初始设置过程中，您可以通过以下两种方式之一连接到设备：

表 *2:* 连接设备的选项

以太网	PC 和网络之间以及网络和管理端口之间的以太网连接。出厂时分配给 Management 端口的 IPv4 地址是 192.168.42.42。这是使用网络配置时最容易的连接方式。
序列	PC 与串行控制台端口之间的串行通信连接。如果您无法使用以太网连接方法，而且暂时无法对管理端口应用其他网络设置，您可以直接在计算机与设备之间建立串行端口到串行端口的连接。有关引出线信息，请参阅通过串行连接访问邮件安全设备，第 983 页。串行端口的通信设置具体如下： **每秒位数**：9600 **数据位**：8 **奇偶校验**：无 **停止位**：1 **流量控制**：硬件

注释 请记住，初始连接方法不是最终的。此过程仅适用于初始配置。您只能稍后更改网络设置，以允许不同的连接方式。（有关详细信息，请参阅FTP、SSH 和 SCP 访问，第 979 页。）您还可以使用不同的管理权限创建多个用户帐户来访问设备。（有关详细信息，请参阅 添加用户，第 726 页。）

确定网络和 IP 地址分配

您可以使用 IPv4 和 IPv6 地址。

管理和数据端口的默认 IP 地址

在管理端口（C170 和 C190 设备上的 Data 1 端口）上预配置的 IP 地址是 192.168.42.42。

选择接收和传送邮件的网络连接

大多数用户会从设备连接到两个网络，充分利用邮件安全设备的两个数据以太网端口：

- 专用网络接受邮件并将其传送到内部系统。
- 公共网络接受邮件并将其传送到互联网。

其他用户可能希望仅使用一个数据端口来提供两种功能。尽管管理以太网端口可支持任何功能，但它预配置为访问图形用户界面和命令行界面。

将逻辑 IP 地址绑定到物理以太网端口

您可以通过单独的侦听程序以及在单独的 IP 地址上分离传入和传出邮件流量。您可以使用互联网协议第 4 版 (IPv4) 和第 6 版 (IPv6) 地址。但是，设备上的系统设置向导支持下列初始配置：

- 在独立的物理接口上配置的 2 个逻辑 IPv4 和 2 个 IPv6 地址上的 2 个独立侦听程序
  - 分离传入和传出流量
  - 您可以将 IPv4 和 IPv6 地址分配到每个侦听程序
- 在一个物理接口配置的 1 个逻辑 IPv4 地址上的 1 个侦听程序
  - 合并传入和传出流量
  - 您可以将 IPv4 和 IPv6 地址都分配到侦听程序

邮件安全设备可以在单个侦听程序上同时支持 IPv4 和 IPv6 地址。侦听程序将接受两种地址的邮件。侦听程序的所有设置均适用于 IPv4 和 IPv6 地址。

选择连接的网络设置

您将需要有关您选择使用的每个以太网端口的以下网络信息：

- IP 地址（IPv4 或/或 IPv6）
- CIDR 格式的 IPv4 地址的网络掩码
- CIDR 格式的 IPv6 地址的前缀

此外，还需要有关整个网络的以下信息：

- 网络上默认路由器（网关）的 IP 地址
- DNS 服务器的 IP 地址和主机名（如果要使用互联网根服务器，则无需此信息）
- NTP 服务器的主机名或 IP 地址（如果要使用思科的时间服务器，则无需此信息）

有关详细信息，请参阅分配网络和 IP 地址 ， 第 985 页。

注释 如果您是在网络上的互联网与邮件安全设备之间运行防火墙，则可能需要打开特定端口以使设备正常运行。有关详细信息，请参阅防火墙资讯 ， 第 1005 页。

收集设置信息

既然您已了解在系统设置向导中进行必要选择时的需求和策略，请在阅读本节时使用下表收集有关系统设置的信息。

有关网络和 IP 地址的详细信息，请参阅分配网络和 IP 地址，第 985 页。如果配置的是思科内容安全管理设备，请参阅在思科内容（M 系列）安全管理设备上集中管理服务，第 969 页。

表 *3:* 系统设置工作表：用于分离邮件流量的 *2* 个侦听程序

系统设置		
默认系统主机名：		
通过邮件将系统警告发送至：		
将计划报告发送到:		
时区信息:		
时钟同步服务器:		
管理员密码：		
SenderBase 网络参与：	启用/禁用	
自动支持：	启用/禁用	
网络集成		
网关：		
DNS（互联网或指定自有 DNS）:		
接口		
Data 1 端口		
IPv4 地址/网络掩码：		
IPv6 地址/前缀：		
完全限定的主机名:		
接受传入邮件:	**域**	**目标**
中继传出邮件:	**System**	
Data 2 端口		
IPv4 地址/网络掩码：		

系统设置		
IPv6 地址/前缀：		
完全限定的主机名:		
接受传入邮件:	**域**	**目标**
中继传出邮件:	**System**	
管理端口		
IP 地址：		
网络掩码：		
IPv6 Address:		
前缀：		
完全限定的主机名:		
接受传入邮件:	**域**	**目标**
中继传出邮件:	**System**	
邮件安全		
SenderBase 声誉过滤:	启用/禁用	
反垃圾邮件扫描引擎	无/IronPort	
McAfee 防病毒扫描引擎	启用/禁用	
Sophos 防病毒扫描引擎	启用/禁用	
病毒爆发过滤器	启用/禁用	

表 *4:* 系统设置工作表：用于所有邮件流量的 *1* 个侦听程序

系统设置		
默认系统主机名：		
通过邮件将系统警告发送至：		
将计划报告发送到:		
时区：		
时钟同步服务器:		

系统设置		
管理员密码：		
SenderBase 网络参与：	启用/禁用	
自动支持：	启用/禁用	
网络集成		
网关：		
DNS（互联网或指定自有 DNS）：		
接口		
Data 2 端口		
IPv4 地址/网络掩码：		
IPv6 地址/前缀：		
完全限定的主机名:		
接受传入邮件:	**域**	**目标**
中继传出邮件:	**System**	
Data 1 端口		
IPv4 地址/网络掩码：		
IPv6 地址/前缀：		
完全限定的主机名:		
邮件安全		
SenderBase 声誉过滤:	启用/禁用	
反垃圾邮件扫描引擎	无/IronPort	
McAfee 防病毒扫描引擎	启用/禁用	
Sophos 防病毒扫描引擎	启用/禁用	
病毒爆发过滤器	启用/禁用	

使用系统设置向导

您必须使用系统设置向导进行初始设置才能确保配置完整。之后，您可以配置系统设置向导中未提供的自定义选项。

您可以使用浏览器或命令行界面 (CLI) 运行系统设置向导。有关详细信息，请参阅访问基于 Web 的图形用户界面 (GUI)，第 29 页或运行命令行界面 (CLI) 系统设置向导，第 38 页

开始之前，请完成为系统设置做好准备，第 23 页中的先决条件。

注意 如果要设置虚拟邮件安全设备，您必须在运行系统设置向导之前使用 loadlicense 命令加载您的虚拟设备许可证。有关详细信息，请参阅思科内容安全设备安装指南。

注意 系统设置向导将完全重新配置您的系统。第一次安装设备时，或者您要完全覆盖现有配置时，您只能使用系统设置向导。

注意 邮件安全设备在所有硬件的管理端口上配置默认 IP 地址 192.168.42.42，C170 和 C190 设备除外，其使用 Data 1 端口。在将设备连接到网络之前，请确保其他设备的 IP 地址与此出厂默认设置都不冲突。如果配置的是思科内容安全管理设备，请参阅在思科内容（M 系列）安全管理设备上集中管理服务，第 969 页。

如果要将多个出厂配置的内容安全设备连接到网络，请一次添加一个，然后对应重新配置每个设备的默认 IP 地址。

访问基于 Web 的图形用户界面 (GUI)

要访问基于 Web 的图形用户界面 (GUI)，请打开浏览器并将其指向 192.168.42.42。

出厂默认用户名和密码

- 用户名：**admin**
- 密码：**ironport**

例如：

```
login: admin
passphrase: ironport
```

注释 如果会话超时，系统会要求您重新输入用户名和密码。如果在运行系统设置向导时会话超时，您将必须重新启动。

使用基于 Web 的系统设置向导定义基本配置

步骤 1 启动系统设置向导

- 按照访问基于 Web 的图形用户界面 (GUI)，第 29 页中的说明登录到图形用户界面。
- 开始使用全新（并非从旧版 AsyncOS 升级）系统时，会将您的浏览器会自动重新定向到系统设置向导。
- 否则，在“系统管理”(System Administration) 选项卡中，点击左侧链接列表中的“系统设置向导”(System Setup Wizard)。

步骤 2 开始。请参阅第 1 步：开始，第 31 页。

- 阅读并接受许可协议

步骤 3 系统。请参阅第 2 步：系统，第 31 页。

- 设置设备的主机名
- 配置警告设置、报告交付设置和自动支持
- 设置系统时间设置和 NTP 服务器
- 重新设置管理员密码
- 启用 SenderBase 网络参与

步骤 4 网络。请参阅第 3 步：网络，第 32 页。

- 定义默认路由器和 DNS 设置
- 启用和配置网络接口，包括：配置传入邮件（入站侦听程序）、定义SMTP路由（可选）、配置传出邮件（出站侦听程序）和定义允许通过设备中继邮件的系统（可选）

步骤 5 安全性请参阅第 4 步：安全，第 35 页。

- 启用 SenderBase 信誉过滤
- 启用反垃圾邮件服务
- 启用垃圾邮件隔离区
- 启用防病毒服务
- 启用高级恶意软件保护（文件信誉和分析服务）
- 启用爆发过滤器服务

步骤 6 审查。请参阅第 5 步：审查，第 36 页。

- 审查您的设置和安装配置
- 在该过程结束时，系统会提示

步骤 7 提交您做出的更改。

在您提交后更改才会生效。

第 1 步：开始

首先阅读许可协议。阅读并接受许可协议后，请选中指示您同意的框，然后点击**开始设置** (Begin Setup) 执行。

您还可以在以下位置查看协议的文本：https://support.ironport.com/license/eula.html

第 2 步：系统

设置主机名

定义邮件安全设备的安全限定主机名。此名称应由网络管理员分配。

配置系统警报

如果存在需要用户干预的系统错误，则 Cisco AsyncOS 会通过邮件发送警报消息。输入接收这些警报的邮件地址。

您必须至少添加一个接收系统警报的邮件地址。输入一个邮件地址或用逗号分隔多个地址。邮件收件人最初会收到所有级别的所有类型的警报，但不会收到目录收割攻击预防警报。您可以稍后进一步细化警报配置。有关详细信息，请参阅告警信息，第 777 页。

配置报告交付

输入接收默认计划报告的地址。如果您将此值留空，仍会运行计划报告。计划报告将在设备上存档而非通过设备交付。

设置时间

设置邮件安全设备的时区，以使邮件信头和日志文件的时间戳保持正确。使用下拉菜单找到您所在的时区或通过 GMT 偏移定义时区（有关详细信息，请参阅选择 GMT 偏移，第 801 页）。

您可以之后手动设置系统时钟时间，也可以使用网络时间协议 (NTP) 来与网络或互联网中的其他服务器同步。默认情况下，已配置用于同步设备时间的思科系统时间服务器 (**time.ironport.com**) 的一个条目。

设置密码

设置管理员帐户的密码。这是必需的步骤。在更改 Cisco AsyncOS 管理员帐户的密码时，新密码的长度必须为六个或以上字符。请务必将密码保存在安全的位置。

参与 SenderBase 网络

SenderBase 是一项邮件信誉服务，旨在帮助邮件管理员调查发件人，识别合法的邮件来源并阻止垃圾邮件。

如果您同意参与 SenderBase 网络，思科将收集有关贵组织的邮件流量的汇总统计数据。这仅包括有关邮件属性的摘要数据和邮件安全设备如何处理不同类型邮件的信息。例如，思科不会收集邮件正文或邮件主题。可识别的个人信息或识别组织的相关信息将保密。要了解有关 SenderBase 更多信息（包括收集的数据的示例），请按照**点击此处了解有关要共享数据的更多信息…**链接中的说明操作（请参阅常见问题解答，第 834 页）。

要参与 SenderBase 网络，请选中此复选框旁边的“允许收集邮件中的 IronPort 匿名统计信息，并将其报告到 SenderBase 报告，以识别和阻止基于邮件的威胁”(Allow IronPort to gather anonymous statistics on email and report them to SenderBase in order to identify and stop email-based threats)，然后点击**接受 (Accept)**。

有关详细信息，请参阅SenderBase网络参与，第 833 页。

启用自动支持

自动支持功能（默认已启用）使思科客户支持团队能够及时了解设备的问题，以便可以更好地为您提供支持。（有关详细信息，请参阅 自动支持，第 777 页。）

点击 **Next** 继续操作。

第 3 步：网络

步骤 3，定义默认路由器（网关）并配置 DNS 设置，然后通过配置 Data 1、Data 2 和管理接口设置设备来接收和或回复邮件。

配置 DNS 和默认网关

输入网络中默认路由器（网关）的 IP 地址。您可以使用 IPv4 地址、IPv6 地址或以上两者。

接下来，配置 DNS（域名服务）设置。Cisco AsyncOS 包含可以直接查询互联网根服务器的高性能内部 DNS 解析程序/缓存，或者系统可以使用您指定的 DNS 服务器。如果选择使用自己的服务器，将需要提供每个 DNS 服务器的 IP 地址和主机名。您可以通过系统设置向导最多输入四个 DNS 服务器。请注意，您输入的 DNS 服务器的初始优先级为 0。有关详细信息，请参阅配置域名系统 (DNS) 设置，第 796 页。

注释 设备需要访问正在工作的 DNS 服务器才能对传入连接执行 DNS 查询。如果您在设置设备时无法指定设备可访问的正在工作的DNS服务器，解决方法是选择“使用互联网根DNS服务器”(Use Internet Root DNS Servers)，或临时指定管理接口的 IP 地址，以便完成系统设置向导。

配置网络接口

您的邮件安全设备具有与计算机的物理以太网端口关联的网络接口。

要使用某个接口，请选中“启用”(Enable) 复选框，然后指定 IP 地址、网络掩码和完全限定的主机名。您输入的 IP 地址应当是您的 DNS 记录反映的入站邮件的 IP 地址。此地址通常具有与 DNS 中的记录关联的 MX记录。您可以使用 IPv4 地址、IPv6 地址或以上两者。如果使用以上两者，接口将接受两种类型的连接。

每个接口都可配置为接受邮件（传入）、中继邮件（传出）或设备管理。在设置过程中，每个接口只能限制为配置一种功能。在大多数设备上，通常一个接口用于传入邮件，一个接口用于传出邮件，一个接口用于设备管理。在 C170 和 C190 设备上，通常一个接口用于传入和传出邮件，另一个接口用于管理。

您必须将一个接口配置为接收邮件。

向设备上的其中一个物理以太网接口分配和配置逻辑 IP 地址。如果决定同时使用 Data 1 以太网端口和 Data 2 以太网端口，则两个连接都需要此信息。

对于 C370、C670、X1070、C380、C680、C390 和 C690 设备：思科建议使用其中一个物理以太网端口直接连接到互联网，以通过公共侦听程序接收入站邮件；建议使用另一个物理以太网端口直接连接到您的内部网络，以通过专用侦听程序中继出站邮件。

对于 C170 和 C190 设备：通常，系统设置向导仅配置一个物理以太网端口和一个侦听程序，同时用于接收入站邮件和中继出站邮件。

请参阅将逻辑 IP 地址绑定到物理以太网端口，第 25 页。

需要提供以下信息：

- 由网络管理员分配的 **IP 地址**。这可以是 IPv4 地址、IPv6 地址或以上两者。
- 对于 IPv4 地址：接口的**网络掩码**。AsyncOS 仅接受 CIDR 格式的网络掩码。例如，`255.255.255.0` 子网的网络掩码为 `/24`。

  对于 IPv6 地址：CIDR 格式的**前缀**。例如 64 位前缀为 `/64`。
- （可选）IP 地址的完全限定主机名。

注释 不能在单独的物理以太网接口上配置同一子网内的 IP 地址。有关网络和 IP 地址配置的详细信息，请参阅分配网络和 IP 地址，第 985 页。

接受邮件

在配置接口接收邮件时，需要定义：

- 为其接受邮件的域
- 每个域的目标（SMTP 路由），这是可选选项

选中“接受传入邮件”(Accept Incoming Mail) 复选框以将接口配置为接受邮件。输入为其接受邮件的域名。

输入目的地。这是要为指定的域路由邮件所在计算机的 SMTP 路由或名称。

这是第一个 SMTP 路由条目。SMTP 路由表可让您为输入到特定邮件交换 (MX) 主机的每个域（也称为收件人访问表 [RAT] 条目）重定向所有邮件。在典型安装中，SMTP 路由表定义特定组件（例如，Microsoft Exchange）服务器或基础设施的邮件传送中的“下一跳”。

例如，您可以定义一个路由，指定为域 `example.com` 和所有其子域 `.example.com` 接受的邮件路由到组件服务器 `exchange.example.com`。

您可以输入多个域和目标。点击**添加行 (Add Row)** 添加另一个域。点击垃圾箱图标可删除行。

注释 在此步骤中配置 SMTP 是可选操作。如果未定义任何 SMTP 路由，系统将使用 DNS 查询并确定侦听程序收到的传入邮件的传输主机。（请参阅路由本地域的邮件，第 523 页。）

您必须至少添加一个域到收件人访问表。例如，输入域 example.com。要确保发往 example.net 任何子域的邮件在收件人访问表中匹配，请输入 .example.net 以及域名。有关详细信息，请参阅定义收件人地址，第 113 页。

中继邮件（可选）

在配置邮件中继接口时，要定义系统，允许通过设备中继邮件。

这些是侦听程序的主机访问表的 RELAYLIST 中的条目。有关详细信息，请参阅发件人组语法，第 83 页。

选中“中继传出邮件”(Relay Outgoing Mail) 复选框以将接口配置为中继邮件。输入可以通过设备中继邮件的主机。

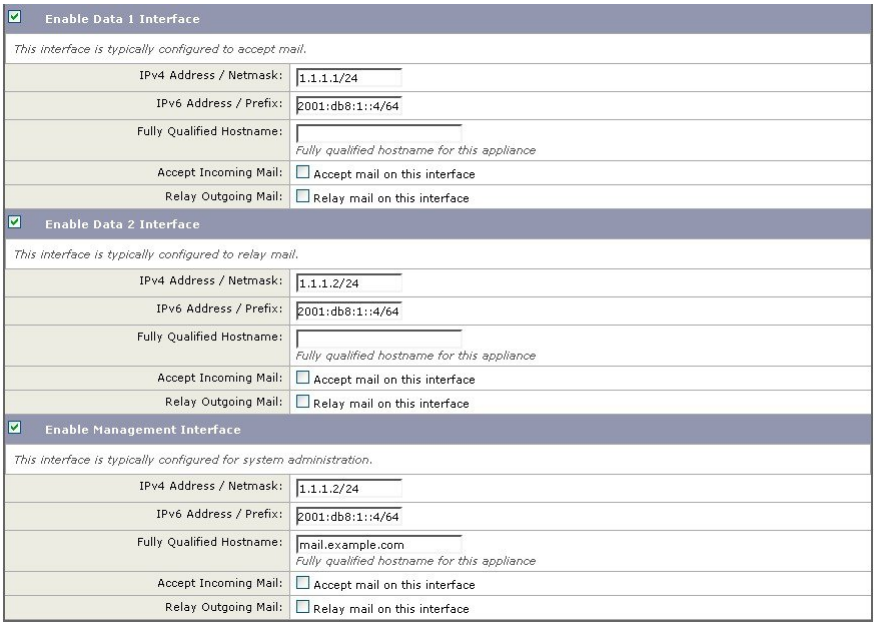
当您配置中继出站邮件的接口时，只要没有公共侦听程序配置为使用该接口，系统设置向导就会打开该接口的 SSH。

在下面的示例中，创建两个具有 IPv4 地址的接口：

- 管理接口依然配置为 192.168.42.42。
- 在 Data 1 以太网接口上启用 192.168.1.1。它配置为接受以 .example.com 结尾的域的邮件，SMTP 路由为 exchange.example.com 定义。
- 在 Data 2 以太网接口上启用 192.168.2.1。它配置为从 exchange.example.com 中继邮件。

C370、C670、X1070、C380、C680、C390 和 C690 安装

图 *3:* 网络接口：除了管理接口（已分流的流量）之外的 *2* 个接口

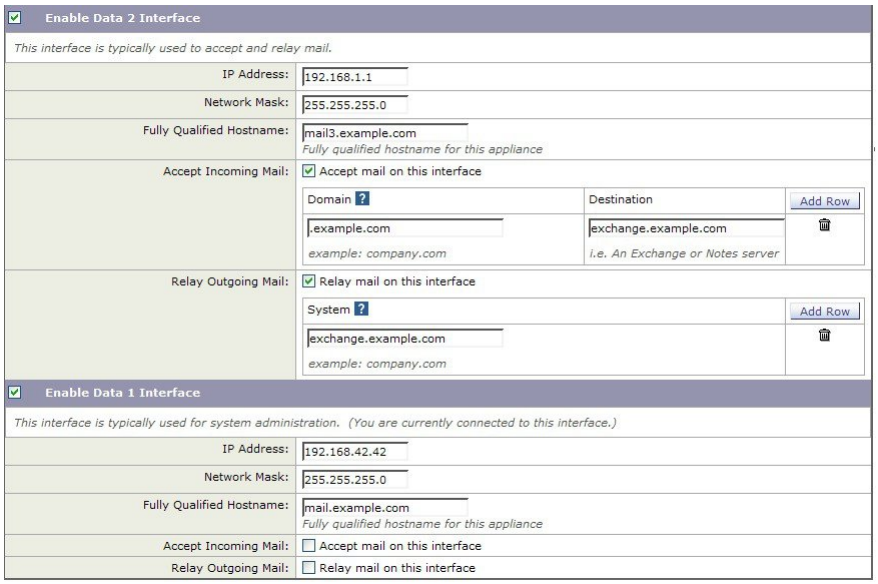


C170 和 C190 安装

对于 C170 和 C190 设备，Data 1 接口通常配置为用于传入邮件和传出邮件，而 Data 2 接口用于设备管理。

当配置单一 IP 地址用于所有邮件流量（未分流的流量）时，系统设置向导的第 3 步如下所示：

图 *4:* 网络接口：用于传入和传出（未分流）流量的 *1* 个 *IP* 地址



点击 **Next** 继续操作。

第 4 步：安全

步骤 4，配置反垃圾邮件和防病毒设置。反垃圾邮件选项包括 SenderBase 信誉过滤和选择反垃圾邮件扫描引擎。对于防病毒，您可以启用病毒爆发过滤器和 Sophos 或 McAfee 防病毒扫描。

启用 SenderBase 信誉过滤

SenderBase 信誉服务可以用作独立的反垃圾邮件解决方案，但是，它主要用于提高基于内容的反垃圾邮件系统（例如反垃圾邮件）的效率。

SenderBase 信誉服务 （http://www.senderbase.org) 提供了一种准确而灵活的方法，供用户根据远程主机的连接 IP 地址拒绝或限制可疑垃圾邮件。SenderBase 信誉服务根据从指定源发送的邮件是垃圾邮件的概率返回一个分数。SenderBase 信誉服务的独特之处在于它提供邮件量的全局视图且数据组织方式易于识别和分组邮件的相关源。思科强烈建议您启用 SenderBase 信誉过滤。

启用后，SenderBase 信誉过滤会应用到传入（接受）侦听程序。

启用反垃圾邮件扫描

您的设备可能随附反垃圾邮件软件的30天试用版密钥。在系统设置向导的这一部分，您可以选择在设备上全局启用反垃圾邮件。您还可以选择不启用该服务。

如果您选择启用反垃圾邮件服务，则可以将 AsyncOS 配置为将垃圾邮件和可疑垃圾邮件发送到本地垃圾邮件隔离区。垃圾邮件隔离区用作设备的最终用户隔离区。在配置最终用户访问权限之前，只有管理员可以访问隔离区。

请参阅反垃圾邮件，第269页，了解设备上提供的所有反垃圾邮件配置选项。请参阅集中化的策略、病毒和病毒爆发隔离区，第 685 页。

启用防病毒扫描

您的设备可能随附 Sophos 防病毒或 McAfee 防病毒扫描引擎的 30 天试用版密钥。在系统设置向导的这一部分，您可以选择在设备上全局启用防病毒扫描引擎。

如果选择启用防病毒扫描引擎，则会为默认传入邮件和默认传出邮件策略都启用该引擎。设备会扫描邮件以查看是否存在病毒，但不修复受感染的附件。设备会丢弃受感染的邮件。

请参阅防病毒，第 253 页，了解设备上提供的所有防病毒配置选项。

启用高级恶意软件防护（文件信誉和分析服务）

高级恶意软件防护可获取有关基于云的服务所附加文件的相关信誉信息。

有关详细信息，请参阅 文件信誉过滤和文件分析：，第 353 页

启用病毒爆发过滤器

您的设备可能随附病毒爆发过滤器的30天试用版密钥。病毒爆发过滤器会在传统的防病毒安全服务更新为新的病毒签名文件之前隔离可疑邮件，提供防新病毒爆发的“第一道防线”。

有关详细信息，请参阅病毒爆发过滤器，第 307 页。

点击 **Next** 继续操作。

第 5 步：审查

配置信息的摘要已显示。您可以点击**旧版 (Previous)** 按钮或点击每部分右上角的**编辑 (Edit)** 链接编辑系统设置、网络集成和邮件安全信息。当您返回某步进行更改时，您必须继续完成所有剩余步骤，一直到此审查页面。您之前输入的所有设置都会保留。

您对显示的信息满意后，请点击**安装此配置 (Install This Configuration)**。

系统会显示确认对话框。点击**安装 (Install)** 安装新配置。

您的设备现已就绪，可以发送邮件。

注释 如果您更改了用于连接到设备的接口（C370、C670、X1070、C380、C680、C390 和 C690 设备上的管理接口或 C170 和 C190 设备上的 Data 1 接口）的默认 IP 地址，则点击**安装**将导致与当前 URL (http://192.168.42.42) 的连接丢失。但是，您的浏览器将重新定向到新的 IP 地址。

系统设置完成后，系统会发送多条警报消息。有关详细信息，请参阅即时警报，第 50 页。

设置与 Active Directory 的连接

如果系统设置向导在邮件安全设备上正确安装了该配置，则会显示 Active Directory 向导。如果要在您的网络中运行 Active Directory 服务器，请使用 Active Directory 向导为 Active Directory 服务器配

置 LDAP 服务器配置文件，并分配侦听程序进行收件人验证。如果没有使用 Active Directory 或者希望稍后再进行配置，请点击“跳过此步骤”。您可以在**系统管理 (System Administration) > Active Directory 向导 (Active Directory Wizard)** 页面上运行 Active Directory 向导。您还可以在**系统管理 (System Administration) > LDAP** 页面上配置 Active Directory 和其他 LDAP 配置文件。

Active Directory 向导会检索创建 LDAP 服务器配置文件所需的系统信息，例如身份验证方法、端口、基本 DN 以及是否支持 SSL。Active Directory 向导还创建 LDAP 服务器配置文件的 LDAP 接受和分组查询。

Active Directory 向导创建 LDAP 服务器配置文件后，请使用**系统管理 > LDAP** 页面查看新的配置文件并进行其他更改。

步骤 1 在“Active Directory 向导”(Active Directory Wizard) 页面上，点击**运行 Active Directory 向导 (Run Active Directory Wizard)**。

步骤 2 输入 Active Directory 服务器的主机名。

步骤 3 输入身份验证请求的用户名和密码。

步骤 4 点击 **Next** 继续操作。

Active Directory 向导会测试与 Active Directory 服务器的连接。如果成功，则会显示“测试目录设置”(Test Directory Settings) 页面。

步骤 5 输入您知道存在于 Active Directory 中的邮件地址并点击**测试 (Test)**，来测试目录设置。结果会显示在“连接状态”(Connection Status) 字段中。

步骤 6 点击 **Done**。

继续执行后续步骤

在您已成功将设备配置为与 Active Directory 向导配合使用或跳过该流程后，系统会显示“系统设置后续步骤”(System Setup Next Steps) 页面。

点击“系统设置后续步骤”(System Setup Next Steps) 页面上的链接，继续配置您的设备。

访问命令行界面 (CLI)

对 CLI 的访问因您在连接到设备，第 24 页中选择的管理连接方式而异。出厂默认用户名和口令在后面列出。最初，只有管理员用户帐户可以访问 CLI。首次通过管理员帐户进入命令行界面后，您可以添加具有不同权限的其他用户。（有关添加用户的信息，请参阅添加用户，第 726 页。）“系统设置向导”会要求您更改管理员帐户的口令。还可以随时使用 `passphrase` 命令直接重置管理员帐户的口令。

通过以太网连接：使用出厂默认 IP 地址 192.168.42.42 启动 SSH 会话。SSH 配置为使用端口 22。在下面输入您的用户名和口令。

通过串行连接端口连接：使用串行电缆所连接的 PC 通信端口启动终端会话。使用连接到设备，第 24 页中概述的串行端口设置。在下面输入您的用户名和口令。

通过输入用户名和口令登录设备。

出厂默认用户名和密码

- 用户名：**admin**
- 密码：**ironport**

例如：

```
login: admin
passphrase: ironport
```

注释 如果会话超时，系统会要求您重新输入用户名和密码。如果在运行系统设置向导时会话超时，您将必须重新启动。

运行命令行界面 (CLI) 系统设置向导

CLI 版系统设置向导与 GUI 版中的步骤基本一致，只有少数例外情况：

- CLI 版包括启用 Web 界面的提示。
- CLI 版允许您编辑自己创建的每个侦听程序的默认邮件流策略。
- CLI 版包含配置全局防病毒和爆发过滤器安全设置的提示。
- 在系统设置完成后，CLI 版不提示您创建 LDAP 配置文件。使用 `ldapconfig` 命令创建 LDAP 配置文件。

要运行系统设置向导，请在命令提示符下键入 `systemsetup`。

```
IronPort> systemsetup
```

系统设置向导会警告您将重新配置您的系统。如果这是您第一次安装设备，或者如果您要完全覆盖现有配置，请回答“是”来解决此问题。

```
WARNING: The system setup wizard will completely delete any existing

'listeners' and all associated settings including the 'Host Access Table' -
mail operations may be interrupted.


Are you sure you wish to continue? [Y]> Y
```

注释 剩余的系统设置步骤在下面介绍。将仅为使用基于 Web 的系统设置向导定义基本配置，第 30 页中上述 GUI 系统设置向导偏离的部分包括“CLI 系统设置向导”(CLI System Setup Wizard) 对话框的示例。

更改管理员密码

首先，更改 AsyncOS 管理员帐户的密码。您必须输入旧密码才能继续。新密码必须至少为 6 个或以上字符。请务必将密码保存在安全的位置。密码更改在系统设置完成后生效。

接受许可协议

阅读并接受显示的软件许可协议。

设置主机名

接下来，为邮件安全设备定义完全限定主机名。此名称应由网络管理员分配。

分配并配置逻辑 IP 接口

下一步是分配并配置物理以太网管理接口（C370、C670、X1070、C380、C680、C390 和 C690 设备）或 Data 1 接口（C170 和 C190 设备）上的逻辑 IP 接口，然后提示您配置设备上提供的任何其他物理以太网接口的逻辑 IP 接口。

每个以太网接口都分配有多个 IP 接口。IP 接口是将 IP 地址和主机名与物理以太网接口关联的逻辑结构。如果您决定使用 Data 1 和 Data 2 以太网端口，您需要两个连接的 IP 地址和主机名。

对于 C370、C670、X1070、C380、C680、C390 和 C690 设备：思科建议使用其中一个物理以太网端口直接连接到互联网，以通过公共侦听程序接收入站邮件；建议使用另一个物理以太网端口直接连接到您的内部网络，以通过私人侦听程序中继出站邮件。

对于 C170 和 C190 设备：默认情况下，`systemsetup` 命令将通过一个侦听程序仅配置一个物理以太网端口，既可以接收入站邮件，也可以中继出站邮件。

注释 当您配置中继出站邮件的接口时，只要没有公共侦听程序配置为使用该接口，系统就会打开该接口的 SSH。

需要提供以下信息：

- 您创建的之后引用 IP 接口的**名称**（昵称）。例如，如果您将一个以太网端口用于专用网络，另一个用于公共网络，您可能想要将它们分别命名为 PrivateNet 和 PublicNet。

  注释 为接口定义的名称区分大小写。AsyncOS 不允许创建两个相同的接口名称。例如，名称 **`Privatenet`** 和 **`PrivateNet`** 被视为两个不同（唯一）的名称。

- 由网络管理员分配的 **IP 地址**。这可以是 IPv4 或 IPv6 地址，您可以为单一 IP 接口分配两种类型的 IP 地址。
- 接口的**网络掩码**。网络掩码必须采用 CIDR 格式。例如，使用 `/24` 作为 `255.255.255.0` 子网的网络掩码。

注释 无法在单独的物理以太网接口上配置相同子网内的 IP 地址。有关网络和 IP 地址配置的详细信息，请参阅分配网络和 IP 地址，第 985 页。

对于 C170 和 C190 设备，首先配置 Data 2 接口。

指定默认网关

在 `systemsetup` 命令的下一部分中，键入网络上默认路由器（网关）的 IP 地址。

启用 Web 界面

在 `systemsetup` 命令的下一部分中，启用设备的 Web 界面（对于管理以太网接口）。您还可以选择通过安全的 HTTP (https) 运行 Web 界面。如果选择使用 HTTPS，则系统将使用演示证书，直至您上传自己的证书为止。

配置 DNS 设置

接下来，配置 DNS（域名服务）设置。Cisco AsyncOS 具有可直接查询互联网根服务器的高性能内部 DNS 解析程序/缓存，系统还可以使用您自己的 DNS 服务器。如果选择使用自己的服务器，则需要提供每个 DNS 服务器的 IP 地址和主机名。您可以输入所需数量的 DNS 服务器（每个服务器将具有优先级 0）。默认情况下，`systemsetup` 会提示您输入您自己的 DNS 服务器的地址。

创建侦听程序

“侦听程序”管理将在特定 IP 接口上配置的入站邮件处理服务。侦听程序仅应用于进入邮件安全设备的邮件 - 来自内部系统或互联网。Cisco AsyncOS 使用侦听程序指定邮件为获得接受和转发到收件人主机所必须满足的条件。您可以将侦听程序视为针对以上指定的 IP 地址运行的邮件侦听程序（甚至“SMTP 后台守护程序”）。

对于 C370、C670、X1070、C380、C680、C390 和 C690 设备：默认情况下，`systemsetup` 命令配置两个侦听程序 - 一个公共侦听程序，一个专用侦听程序。（有关可用侦听程序类型的详细信息，请参阅配置网关以接收邮件，第 61 页。）

对于 C170 和 C190 设备：默认情况下，`systemsetup` 命令配置一个公共侦听程序，既接收来自互联网的邮件，也中继来自内部网络的邮件。请参阅C170 和 C190 设备的侦听程序示例，第 45 页。

定义侦听程序时，需要指定以下属性：

- 您创建的之后引用侦听程序的**名称**（昵称）。例如，接收来自内部系统的邮件传送到互联网的侦听程序可能称为 OutboundMail。
- 用于接收邮件的其中一个 IP 接口（您之前使用 `systemsetup` 命令创建的接口）。
- 要将邮件路由到的计算机的名称（仅公共侦听程序）。（这是第一个 `smtproutes` 条目。请参阅路由本地域的邮件，第 523 页。）
- 根据 SenderBase 信誉得分确定是否为公共侦听程序启用过滤功能。如果启用，系统还会提示您在“保守”(Conservative)、“中等”(Moderate) 或“主动”(Aggressive) 设置之间做出选择。
- 每台主机的速率限制：每小时想要从远程主机接收的收件人最大数（仅公共侦听程序）。

- 要接收邮件的收件人域或特定地址（公共侦听程序），或允许通过设备中继邮件的系统（私人侦听程序）。（这些是侦听程序的第一个收件人访问表和主机访问表条目。如需更多信息，请参阅发件人组语法，第 83 页和添加为其接受邮件的域和用户，第 113 页。）

公共侦听程序

注释 创建公共和专用侦听程序的以下示例仅适用于 C370、C670、X1070、C380、C680、C390 和 C690 设备。对于 C170 和 C190 设备，请跳到下一部分C170 和 C190 设备的侦听程序示例，第 45 页。

在 `systemsetup` 命令的此示例部分中，名为 InboundMail 的公共侦听程序配置为在 PublicNet IP 接口上运行。然后，该侦听程序配置为接受 `example.com` 域的所有邮件。配置到邮件交换 `exchange.example.com` 的初始 SMTP 路由。已启用速率限制，并为公共侦听程序指定了单个主机每小时 4500 个收件人的最大值。

注释 您为希望从远程主机每小时接收的最大邮件数输入的值是完全随机值，通常相对于您要为其管理邮件的企业规模。例如，在 1 小时内发送 200 封邮件的发件人可能被视为“垃圾邮件发送者”（来路不明的批量邮件的发件人），但是，如果您将邮件安全设备配置为处理一家 10,000 人的公司的所有邮件，从远程主机每小时接收 200 封邮件可能是一个合理值。相反，在一家 50 人的公司中，在一小时内发送 200 封邮件的发件人可能是明显的垃圾邮件发送者。当您对企业的公共侦听程序（限制）入站邮件启用速率限制时，必须选择适当的值。有关默认主机访问策略的详细信息，请参阅发件人组语法，第 83 页。

之后，系统接受侦听程序的默认主机访问策略。

```
You are now going to configure how the appliance accepts mail by

creating a "Listener".

Please create a name for this listener (Ex: "InboundMail"):

[]> InboundMail


Please choose an IP interface for this Listener.

1. Management (192.168.42.42/24: mail3.example.com)

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 3
```

```
Enter the domains or specific addresses you want to accept mail for.


Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

Usernames such as "postmaster@" are allowed.

Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.

Separate multiple addresses with commas.

[]> example.com


Would you like to configure SMTP routes for example.com?  [Y]> y


Enter the destination mail server which you want mail for example.com to be delivered.
Separate multiple entries with commas.

[]> exchange.example.com


Do you want to enable rate limiting for this listener? (Rate limiting defines the maximum
number
of recipients per hour you are willing to receive from a remote domain.) [Y]> y


Enter the maximum number of recipients per hour to accept from a remote domain.

[]> 4500


Default Policy Parameters

==========================

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 1,000

Maximum Number Of Messages Per Connection: 1,000

Maximum Number Of Recipients Per Message: 1,000
```

```
Maximum Number Of Recipients Per Hour: 4,500

Maximum Recipients Per Hour SMTP Response:

    452 Too many recipients received this hour

Use SenderBase for Flow Control:  Yes

Virus Detection Enabled:  Yes

Allow TLS Connections: No

Would you like to change the default host access policy?  [N]> n


Listener InboundMail created.

Defaults have been set for a Public listener.

Use the listenerconfig->EDIT command to customize the listener.

*****
```

专用侦听程序

在 systemsetup 命令的此示例部分中，名为 OutboundMail 的专用侦听程序配置为在 PrivateNet IP 接口上运行。然后，配置为中继 `example.com` 域内所有主机的所有邮件。（请注意，条目开始处的句点：`.example.com`）

然后接受速率限制（未启用）的默认值和此侦听程序的默认主机访问策略。

请注意，私人侦听程序的默认值不同于之前的公共侦听程序。有关详细信息，请参阅使用侦听程序，第 62 页。

```
Do you want to configure the appliance to relay mail for internal hosts?  [Y]> y


Please create a name for this listener (Ex: "OutboundMail"):

[]> OutboundMail


Please choose an IP interface for this Listener.

1. Management (192.168.42.42/24: mail3.example.com)

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)
```

```
[1]> 2


Please specify the systems allowed to relay email through the appliance.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addressed are allowed.

Separate multiple entries with commas.

[]> .example.com


Do you want to enable rate limiting for this listener?
(Rate limiting defines the maximum number of recipients per hour you are willing
to receive from a remote domain.)  [N]> n


Default Policy Parameters

==========================

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 600

Maximum Number Of Messages Per Connection: 10,000

Maximum Number Of Recipients Per Message: 100,000

Maximum Number Of Recipients Per Hour: Disabled

Use SenderBase for Flow Control:  No

Virus Detection Enabled:  Yes

Allow TLS Connections: No

Would you like to change the default host access policy?  [N]> n


Listener OutboundMAil created.

Defaults have been set for a Private listener.
```

```
Use the listenerconfig->EDIT command to customize the listener.

*****
```

C170 和 C190 设备的侦听程序示例

注释 创建侦听程序的以下示例仅适用于 C170 和 C190 设备。

在 systemsetup 命令的此示例部分中，名为 MailInterface 的侦听程序配置为在 MailNet IP 接口上运行。然后，该侦听程序配置为接受 `example.com` 域的所有邮件。配置到邮件交换 `exchange.example.com` 的初始 SMTP 路由。然后，同一侦听程序会配置为中继 `example.com` 域内所有主机的所有邮件。（请注意，条目开始处的句点：`.example.com`）

已启用速率限制，并为公共侦听程序指定了单个主机每小时 450 个收件人的最大值。

注释 您为希望从远程主机每小时接收的最大邮件数输入的值是完全随机值，通常相对于您要为其管理邮件的企业规模。例如，在 1 小时内发送 200 封邮件的发件人可能被视为“垃圾邮件发送者”（来路不明的批量邮件的发件人），但是，如果您要配置该设备来处理一家 10,000 人的公司的所有邮件，从远程主机每小时接收 200 封邮件可能是一个合理值。相反，在一家 50 人的公司中，在一小时内发送 200 封邮件的发件人可能是明显的垃圾邮件发送者。当您对企业的公共侦听程序（限制）入站邮件启用速率限制时，必须选择适当的值。有关默认主机访问策略的详细信息，请参阅发件人组语法，第 83 页。

之后，系统接受侦听程序的默认主机访问策略。

```
You are now going to configure how the appliance accepts mail by creating a "Listener".

Please create a name for this listener (Ex: "MailInterface"):

[]> MailInterface


Please choose an IP interface for this Listener.

1. MailNet (10.1.1.1/24: mail3.example.com)

2. Management (192.168.42.42/24: mail3.example.com)

[1]> 1


Enter the domain names or specific email addresses you want to accept mail for.
```

```
Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

Usernames such as "postmaster@" are allowed.

Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.

Separate multiple addresses with commas.

[]> example.com


Would you like to configure SMTP routes for example.com?  [Y]> y


Enter the destination mail server where you want mail for example.com to be delivered.
Separate multiple entries with commas.

[]> exchange.example.com


Please specify the systems allowed to relay email through the appliance.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addresses are allowed.

Separate multiple entries with commas.

[]> .example.com


Do you want to enable rate limiting for this listener?
(Rate limiting defines the maximum number of recipients per hour you are willing
to receive from a remote domain.)  [Y]> y


Enter the maximum number of recipients per hour to accept from a remote domain.

[]> 450


Default Policy Parameters
```

```
============================

Maximum Message Size: 10M

Maximum Number Of Connections From A Single IP: 50

Maximum Number Of Messages Per Connection: 100

Maximum Number Of Recipients Per Message: 100

Maximum Number Of Recipients Per Hour: 450

Maximum Recipients Per Hour SMTP Response:

    452 Too many recipients received this hour

Use SenderBase for Flow Control:  Yes

Spam Detection Enabled:  Yes

Virus Detection Enabled:  Yes

Allow TLS Connections: No

Would you like to change the default host access policy?  [N]>


Listener MailInterface created.

Defaults have been set for a Public listener.

Use the listenerconfig->EDIT command to customize the listener.

*****
```

注释 由于 `systemsetup` 命令仅配置一个侦听程序，用于处理 C170 和 C190 设备的入站和出站邮件，所有传出邮件将采用邮件流监控功能计算（通常用于入站邮件）。请参阅 使用邮件安全监控，第 637 页

启用反垃圾邮件

您的设备随附反垃圾邮件软件的30天试用版密钥。在 **systemsetup** 命令的此部分中，您可以选择接受许可协议，并且在设备上全局启用反垃圾邮件功能。

然后，将会在传入邮件策略上启用反垃圾邮件扫描。

注释 如果未接受许可协议，则不会在设备上启用反垃圾邮件功能。

请参阅反垃圾邮件，第 269 页，了解设备上提供的所有反垃圾邮件配置选项。

选择默认反垃圾邮件扫描引擎

如果您启用了多个反垃圾邮件扫描引擎，系统会提示您选择启用哪个引擎以对默认传入邮件策略使用。

启用垃圾邮件隔离区

如果您选择启用反垃圾邮件服务，则可以启用传入邮件策略，以将垃圾邮件和可疑垃圾邮件发送到本地垃圾邮件隔离区。启用垃圾邮件隔离区还会在设备上启用终端用户隔离区。在配置终端用户访问权限之前，只有管理员可以访问终端用户隔离区。

请参阅设置本地垃圾邮件隔离区，第 702 页。

启用防病毒扫描

您的设备随附病毒扫描引擎的 30 天试用版密钥。在 `systemsetup` 命令这一部分，您可以选择在设备上全局接受一个或多个许可协议并启用防病毒扫描功能。您必须接受想要在设备上启用的每个防病毒扫描引擎的许可协议。

接受协议后，将会在传入邮件策略上启用所选择的防病毒扫描引擎。邮件安全设备会扫描传入邮件以查看是否存在病毒，但不修复受感染的附件。设备会丢弃受感染的邮件。

请参阅防病毒，第 253 页，了解设备上提供的防病毒配置选项。

启用病毒爆发过滤器和 SenderBase 邮件流量监控网络

下一步，提示您启用 SenderBase 参与和病毒爆发过滤器。您的设备随附病毒爆发过滤器的 30 天试用版密钥。

病毒爆发过滤器

爆发过滤器会在传统的防病毒安全服务更新为新的病毒签名文件之前隔离可疑邮件，提供防新病毒爆发的“第一道防线”。如果启用，将对默认传入邮件策略启用爆发过滤器。

如果您选择启用爆发过滤器，请输入阈值以及您是否想接收爆发过滤器警报。有关爆发过滤器和阈值的更多信息，请参阅病毒爆发过滤器，第 307 页。

SenderBase 参与

SenderBase 是一项邮件信誉服务，旨在帮助邮件管理员调查发件人，识别合法的邮件来源并阻止垃圾邮件。

如果您同意参与 SenderBase 邮件流量监控网络，思科将收集有关贵组织的邮件流量的汇总统计数据。这包括有关邮件属性的摘要数据和邮件安全设备如何处理不同类型邮件的信息。

有关详细信息，请参阅思科邮件安全设备中的“*SenderBase* 网络参与”一章。

配置警报设置和自动支持

如果存在需要用户干预的系统错误，则 Cisco AsyncOS 会通过邮件向用户发送警报消息。至少添加一个接收系统警报的邮件地址。多个地址之间用逗号分隔。您输入的邮件地址最初会收到所有级别的所有类型的警报，但不会收到目录搜集攻击预防警报。之后您可以使用 CLI 中的 `alertconfig` 命令和 GUI 中的**系统管理 > 警报**页面进一步细化警报配置。有关详细信息，请参阅《思科邮件安全设备指南》的分发管理任务一章的警报一节。

自动支持功能使思科客户支持团队能够及时了解设备的问题，以便思科可以为您提供行业领先的支持。回答“是”(Yes) 可发送思科支持警告和每周状态更新。（有关详细信息，请参阅《思科邮件安全设备指南》的分发管理任务一章的自动支持一节。）

配置计划报告

输入发送默认计划报告的地址。您可以将此值留空，报告会在设备上归档而不是通过邮件发送。

配置时间设置

通过 Cisco AsyncOS，您可以使用网络时间协议 (NTP) 将时间与网络上的其他服务器或互联网同步，或者手动设置系统时钟。您还必须在设备上设置时区，以便邮件信头和日志文件中的时间戳正确。您还可以使用思科系统时间服务器来同步设备上的时间。

选择洲、国家/地区和时区以及是否使用 NTP（包括要使用的 NTP 服务器的名称）。

确认更改

最后，系统设置向导将提示您确认整个过程中所做的配置更改。如果要确认更改，请回答“是”(Yes)。

在成功完成系统设置向导后，将显示下列消息和命令提示：

```
Congratulations! System setup is complete. For advanced configuration, please refer to the
 User Guide.

mail3.example.com>
```

设备现已就绪，可以发送邮件。

测试配置

要测试思科 AsyncOS 配置，您可以使用 mailconfig 命令立即发送包含您刚通过 `systemsetup` 命令创建的系统配置数据的测试邮件：

```
mail3.example.com> mailconfig


Please enter the email address to which you want to send

the configuration file. Separate multiple addresses with commas.
```

```
[]> user@example.com


The configuration file has been sent to user@example.com.

mail3.example.com>
```

将配置发送到您有权访问的邮箱，以确认系统能够在您的网络中发送邮件。

即时警报

邮件安全设备使用功能没要启用功能。第一次使用 `systemsetup` 命令创建侦听程序、启用反垃圾邮件、启用 Sophos 或 McAfee 防病毒或启用爆发过滤器时，系统会生成警报并发送至您在第 2 步：系统，第 31 页中指定的地址。

警报会定期通知您密钥的剩余时间。例如：

```
Your "Receiving" key will expire in under 30 day(s).
Please contact IronPort Customer Support.

Your "Sophos" key will expire in under 30 day(s).
Please contact IronPort Customer Support.

Your "Outbreak Filters" key will expire in under 30 day(s).
Please contact IronPort Customer Support.
```

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` 命令来查看密钥的剩余时间。（有关详细信息，请参阅功能密钥，第 752 页。）

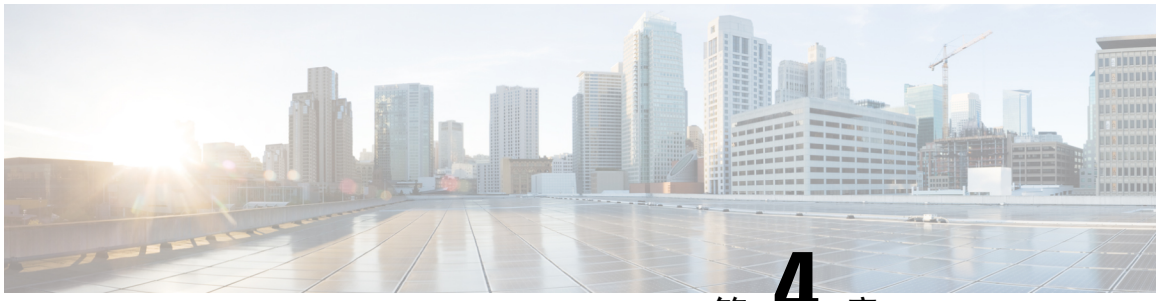
将系统配置为企业网关

要将系统配置为企业网关（接受来自互联网的邮件），请先完成本章，然后参阅配置网关以接收邮件，第 61 页了解更多信息。

验证您的配置和后续步骤

系统设置完成后，您的邮件安全设备应该可以发送和接收邮件。如果您已启用防病毒、反垃圾邮件和爆发过滤器安全功能，系统还将扫描传入和传出邮件，以查找是否存在垃圾邮件和病毒。

下一步是了解如何自定义您的设备的配置。了解邮件通道，第 51 页详细概述如何通过系统路由邮件。每项功能会按顺序处理（从上到下），会在本指南的剩余章节中介绍。



第 4 章

了解邮件通道

本章包含以下部分：

邮件管道概述

邮件管道是设备处理的邮件流。它有三个阶段：

- 回执 - 当设备连接到一台远程主机以接收传入邮件时，会遵守配置的限制和其他回执策略。例如，验证主机是否可以发送您的用户邮件，实施传入连接和邮件限制，以及验证邮件的收件人。
- 工作队列 - 设备处理传入和外发邮件，并执行一些任务，例如过滤、安全列表/阻止列表扫描、反垃圾邮件和防病毒扫描、爆发过滤器和隔离。
- 传送 - 当设备建立连接以发送外发邮件时，会遵守配置的传送限制和策略。例如，实施出站连接限制和根据说明处理无法传送的邮件。

邮件管道流

下列各图概述了系统处理邮件的过程，从接收到路由再到传送都包括在内。每项功能都按顺序（从上到下）处理。可以使用 trace 命令可以测试此管道中功能的大多数配置。

图 *5:* 邮件管道 - 接收邮件连接

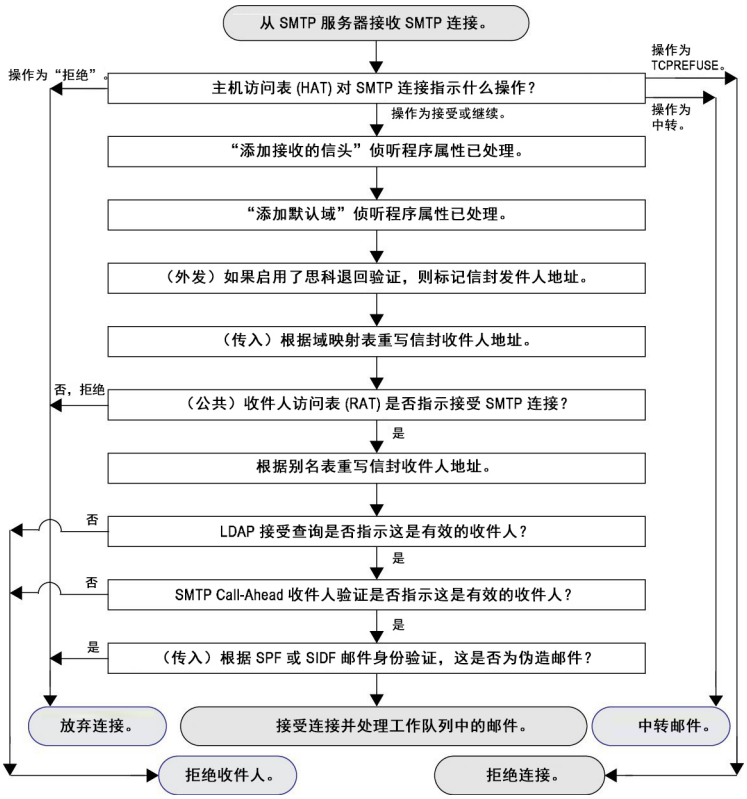


图 *6:* 邮件管道 - 工作队列

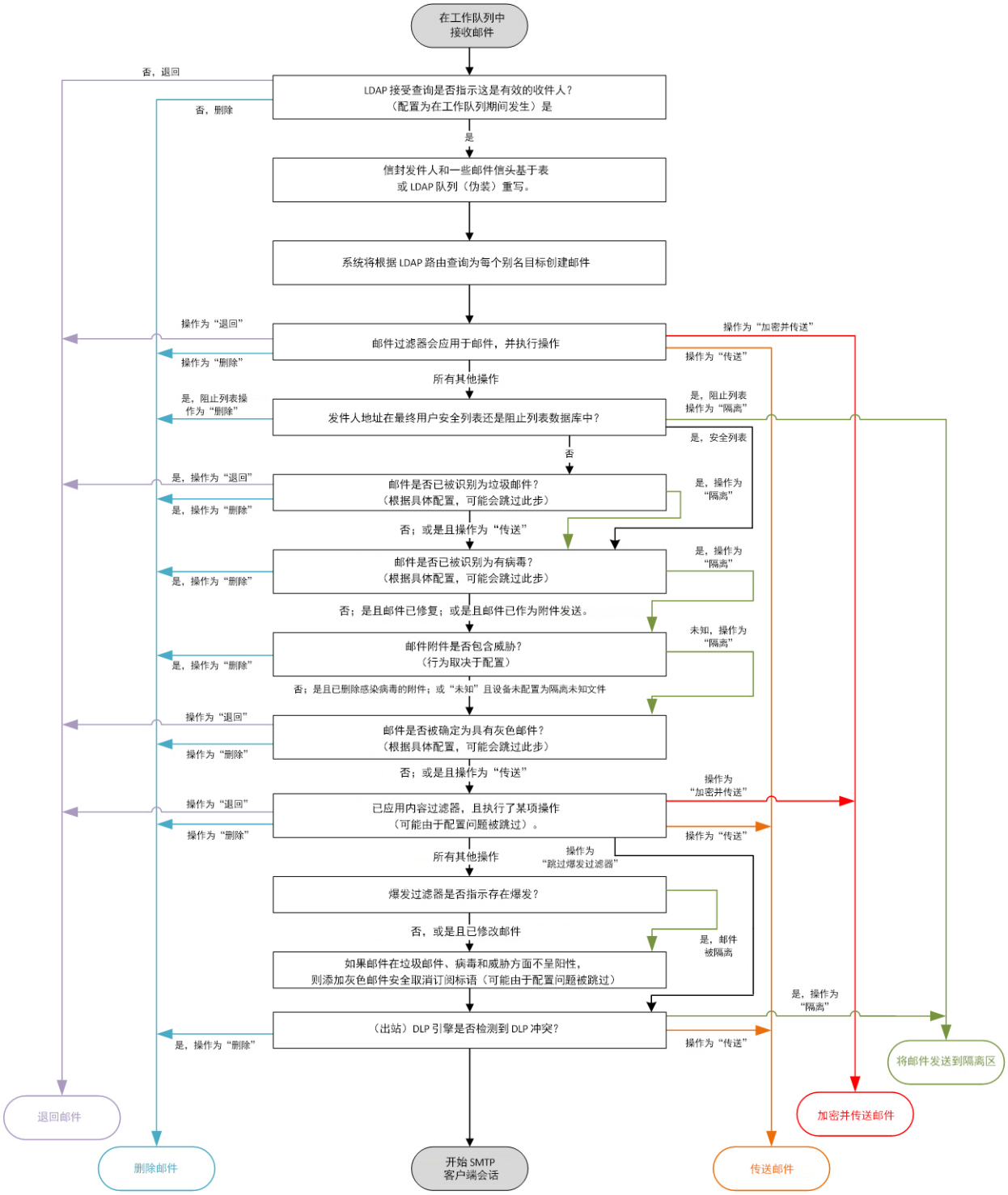
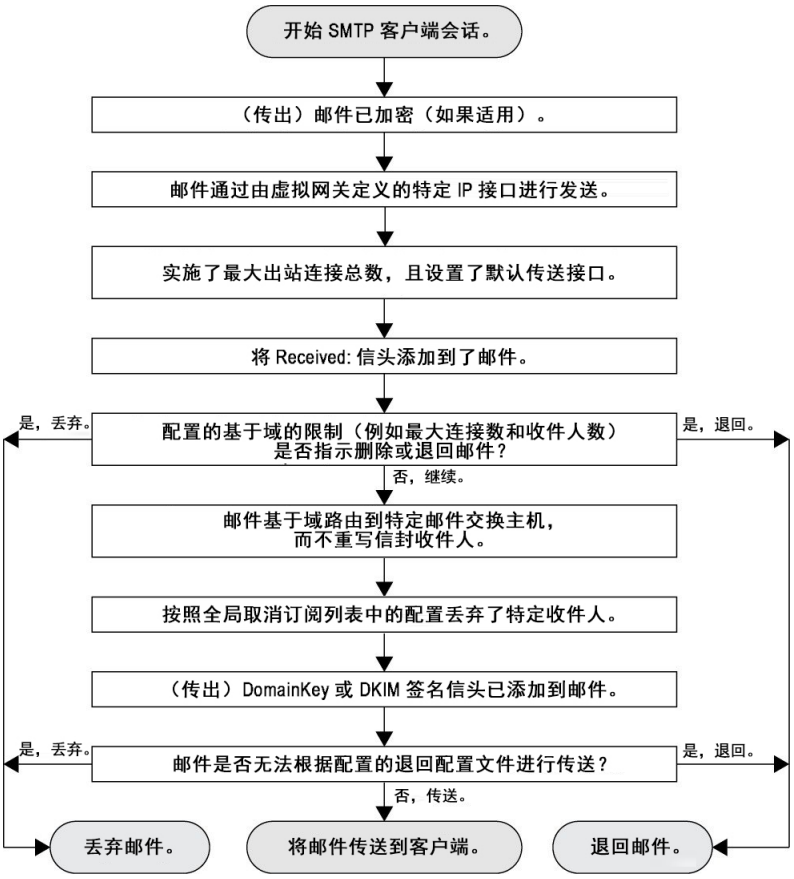

在工作队列中
接收邮件
LDAP 接受查询是否指示这是有效的收件人？
（配置为在工作队列期间发生）是
否，退回
否，删除
是
信封发件人和一些邮件信头基于表
或 LDAP 队列（伪装）重写。
系统将根据 LDAP 路由查询为每个别名目标创建邮件
邮件过滤器会应用于邮件，并执行操作
操作为“退回”
操作为“删除”
操作为“加密并传送”
操作为“传送”
所有其他操作
发件人地址在最终用户安全列表还是阻止列表数据库中？
是，阻止列表操
作为“删除”
是，阻止列表
操作为“隔离”
是，安全列表
否
邮件是否已被识别为垃圾邮件？
（根据具体配置，可能会跳过此步）
是，操作为“退回”
是，操作为“删除”
是，操作为
“隔离”
否；或是且操作为“传送”
邮件是否已被识别为有病毒？
（根据具体配置，可能会跳过此步）
是，操作为“删除”
是，操作为
“隔离”
否；是且邮件已修复；或是且邮件已作为附件发送。
邮件附件是否包含威胁？
（行为取决于配置）
是，操作为“删除”
未知，操作为
“隔离”
否；是且已删除感染病毒的附件；或“未知”且设备未配置为隔离未知文件
邮件是否被确定为具有灰色邮件？
（根据具体配置，可能会跳过此步）
操作为“退回”
操作为“删除”
否；或是且操作为“传送”
已应用内容过滤器，且执行了某项操作
（可能由于配置问题被跳过）。
操作为“退回”
操作为“删除”
操作为
“加密并传送”
操作为“传送”
所有其他操作
操作为
“跳过爆发过滤器”
爆发过滤器是否指示存在爆发？
否，或是且已修改邮件
是，邮件
被隔离
如果邮件在垃圾邮件、病毒和威胁方面不呈阳性，
则添加灰色邮件安全取消订阅标语（可能由于配置问题被跳过）
（出站）DLP 引擎是否检测到 DLP 冲突？
是，操作为“删除”
是，操作为
“隔离”
操作为“传送”
将邮件发送到隔离区
加密并传送邮件
退回邮件
删除邮件
开始 SMTP
客户端会话
传送邮件

图 *7:* 邮件管道 - 传送邮件



传入/接收

邮件管道的接收阶段涉及从发件人的主机发起连接。可以设置每个邮件的域，对收件人进行检查，然后将邮件转交到工作队列。

主机访问表 (HAT)、发件人组和邮件流策略

通过 HAT 可以指定允许连接到侦听程序的主机（允许哪些主机发送邮件）。

发件人组用于将一个或多个发件人关联到组中，以便根据组应用邮件过滤器和其他邮件流量策略。邮件流量策略是表示一组 HAT 参数（访问规则，后跟速率限制参数以及自定义 SMTP 代码和响应）的方式。

发件人组和邮件流量策略都在侦听程序的 HAT 中定义。

发件人组的主机 DNS 验证设置允许在 SMTP 会话之前对未验证的发件人进行分类，并将不同类型的未验证发件人包含在各种发件人组中。

尽管连接主机需要在发件人组中进行主机 DNS 验证（在 SMTP 会话之前），但信封发件人的域部分是在邮件流量策略中进行验证的 DNS，并且验证在 SMTP 会话期间执行。具有格式不正确的信封发件人的邮件可被忽略。可以向发件人验证例外表（接受从其发送的邮件或拒绝其邮件的域和邮件地址的列表）添加条目，不管信封发件人 DNS 验证设置如何都是如此。

发件人信誉过滤允许您对邮件发件人进行分类，根据由 Cisco SenderBase 信誉服务确定的发件人信誉度，限制对您的邮件基础设施的访问。

有关详细信息，请参阅了解预定义发件人组和邮件流策略，第 90 页。

Received: 信头

使用 **listenerconfig** 命令，可以将侦听程序配置为默认情况下不包括侦听程序接收的所有邮件中的“已接收:”(Received:) 信头。

有关详细信息，请参阅使用侦听程序，第 62 页。

默认域

可以将侦听程序配置为将默认域自动附加到不包含完全限定域名的发件人地址；这些地址也称为没有域的地址（例如“joe”与“joe@example.com”）。

有关详细信息，请参阅使用侦听程序，第 62 页。

退回验证

外发邮件通过特殊键标记，因此如果邮件被作为退回邮件发回，则系统可以识别可标记并传送邮件。

有关详细信息，请参阅退回验证，第 558 页。

域名Map

对于配置的每个侦听程序，可以构建一个域映射表，以便为匹配域映射表中某个域的邮件中的每个收件人重写信封收件人。例如，joe@old.com -> joe@new.com

有关详细信息，请参阅域映射功能，第 544 页。

收件人访问表 (RAT)

仅对于入站邮件，RAT 才允许指定设备将接受其邮件的所有本地域的列表。

有关详细信息，请参阅基于收件人地址接受或拒绝连接概述，第 111 页。

别名表

别名表提供一种机制，将邮件重定向至一个或多个收件人。别名存储在映射表中。当邮件的信封收件人（也称为信封至或 RCPT TO）与别名表中定义的别名匹配时，该邮件的信封收件人地址会被覆盖。

有关别名表的详细信息，请参阅创建别名表，第 528 页。

LDAP 收件人接受

可以使用现有 LDAP 基础设施来定义如何在 SMTP 会话期间或工作队列中处理传入邮件的收件人邮件地址（在公共侦听程序中）。有关详细信息，请参阅使用侦听程序，第 62 页。这使设备通过单一方式便可抵御目录搜集攻击 (DHAP)：系统接受邮件并在 SMTP 会话或工作队列中执行 SMTP 会话验证。如果在 LDAP 目录中找不到收件人，可以配置系统以执行延迟退回或彻底删除邮件。

有关详细信息，请参阅处理 LDAP 查询，第 594 页。

SMTP Call-Ahead 收件人验证

当配置邮件安全设备进行 SMTP Call-Ahead 收件人验证时，邮件安全设备会暂停与发送 MTA 的 SMTP 会话，同时对 SMTP 服务器进行“Call-Ahead”以验证收件人。当设备查询 SMTP 服务器时，它会将 SMTP 服务器的响应返回到邮件安全设备。邮件安全设备将恢复 SMTP 会话并向发送 MTA 发送响应，以便基于 SMTP 服务器响应（以及在 SMTP Call-Ahead 配置文件中配置的设置）继续会话或删除连接。

有关详细信息，请参阅 使用 SMTP 服务器验证收件人，第 501 页

工作队列/路由

工作队列是在将收到的邮件移至传送阶段之前对其进行处理的地方。处理包括伪装、路由、过滤、安全列表/阻止列表扫描、反垃圾邮件和防病毒扫描、文件信誉扫描和分析、爆发过滤器和隔离。

注释 防数据丢失 (DLP) 扫描仅适用于外发邮件。有关在工作队列中的什么位置进行 DLP 邮件扫描的信息，请参阅邮件拆分，第 227 页。

邮件管道和安全服务

请注意，通常对安全服务（反垃圾邮件扫描、防病毒扫描和爆发过滤器）的更改不会影响已在工作队列中的邮件示例：

如果由于任何原因，邮件在首次进入管道后绕过防病毒扫描，则说明：

- 没有为设备全局启用防病毒扫描，
- HAT 策略是跳过防病毒扫描，

- 存在某个邮件过滤器导致邮件绕过防病毒扫描，

该邮件在从隔离区放行后不会进行防病毒扫描，无论是否重新启用了防病毒扫描都是如此。但是，由于邮件策略而绕过防病毒扫描的邮件可在从隔离区放行后进行防病毒扫描，因为当邮件在隔离区中时，邮件策略的设置可能已更改。例如，如果邮件由于邮件策略而绕过防病毒扫描并且被隔离，而且在从隔离区释放之前，邮件策略已更新为包括防病毒扫描，则该邮件从隔离区释放后将进行防病毒扫描。

同样，假设您无意中全局（或在HAT中）禁用了反垃圾邮件扫描，并且您在邮件处于工作队列期间注意到了该情况。则此时启用反垃圾邮件不会导致工作队列中的邮件进行反垃圾邮件扫描。

LDAP 收件人接受

可以使用现有 LDAP 基础设施来定义如何在 SMTP 会话期间或工作队列中处理传入邮件的收件人邮件地址（在公共侦听程序中）。有关详细信息，请参阅使用侦听程序，第 62 页。这使设备通过单一方式便可抵御目录搜集攻击 (DHAP)：系统接受邮件并在 SMTP 会话或工作队列中执行 SMTP 会话验证。如果在 LDAP 目录中找不到收件人，可以配置系统以执行延迟退回或彻底删除邮件。

有关详细信息，请参阅处理 LDAP 查询，第 594 页。

伪装或 LDAP 伪装

伪装是根据构建的表重写专用或公共侦听程序处理的邮件中的信封发件人（也称为发件人或 MAIL FROM）以及“收件人:”、“发件人:”和/或“抄送:”信头的一项功能。可以通过以下两种方式之一为创建的每个侦听程序指定不同的伪装参数：静态映射表或 LDAP 查询。

有关通过静态映射表进行伪装的详细信息，请参阅配置伪装，第 535 页。

有关通过 LDAP 查询进行伪装的详细信息，请参阅处理 LDAP 查询，第 594 页。

LDAP 路由

可以将设备配置为根据网络中 LDAP 目录中的可用信息，将邮件路由至相应地址和/或邮件主机。

有关详细信息，请参阅处理 LDAP 查询，第 594 页。

邮件过滤器

通过邮件过滤器可以创建特殊规则来说明如何处理接收的邮件和附件。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。过滤器操作允许删除、退回、存档、隔离、密件复制或更改邮件。

有关详细信息，请参阅使用邮件过滤器实施邮件策略，第 117 页。

在此阶段之后且在由邮件安全管理器处理之前，多收件人邮件将会“拆分”。拆分邮件是指创建具有单个收件人的邮件拆分副本，以便通过邮件安全管理器进行处理。

邮件安全管理器（按收件人扫描）

安全列表/阻止列表扫描

最终用户安全列表和阻止列表由最终用户创建，并且存储在进行反垃圾邮件扫描之前选择的数据库中。每个最终用户都可以识别将其邮件始终视为垃圾邮件或从不视为垃圾邮件的域、子域或邮件地址。如果发件人地址在最终用户安全列表中，则会跳过反垃圾邮件扫描；如果发件人地址在阻止列表中列出，则会根据管理员设置隔离或删除其邮件。有关配置配置安全列表和阻止列表的详细信息，请参阅垃圾邮件隔离区，第 701 页。

反垃圾邮件

反垃圾邮件扫描提供完整的、互联网范围的、服务器端反垃圾邮件保护。它可主动识别并抵御垃圾邮件攻击，避免这些攻击侵扰您的用户以及破坏您的网络，从而使您可以及早删除不需要的邮件，避免它们进入用户的收件箱，同时又不侵犯用户的隐私。

反垃圾邮件扫描可以配置为向垃圾邮件隔离区（机上或机下）传送邮件。从垃圾邮件隔离区释放的邮件会直接转到目标队列，跳过邮件管道中的任何其他工作队列处理。

有关详细信息，请参阅反垃圾邮件，第 269 页。

防病毒

设备提供集成的病毒扫描引擎。可以将设备配置为根据“邮件策略”扫描邮件和附件中的病毒。可以将设备配置为在发现病毒时执行诸如以下操作：

- 尝试修复附件
- 删除附件
- 修改主题信头
- 添加额外的 X 信头
- 将邮件发送到其他地址或邮件主机
- 存档邮件
- 删除邮件

对从隔离区释放的邮件（请参阅隔离区，第 59 页）执行病毒扫描。有关防病毒扫描的详细信息，请参阅防病毒，第 253 页。

灰色邮件检测和安全取消订阅

可以将设备配置为检测灰色邮件，并代表最终用户执行安全取消订阅。可用的操作类似于防病毒扫描。

有关详细信息，请参阅 管理灰色邮件，第 297 页

文件信誉扫描和文件分析

可以将设备配置为扫描邮件附件中的新兴威胁和针对性威胁。可用的操作类似于防病毒扫描。

有关详细信息，请参阅 文件信誉过滤和文件分析：，第 353 页

内容过滤器

可以创建将按照收件人或发件人应用到邮件的内容过滤器。内容过滤器与邮件过滤器类似，不同之处在于，它们在邮件管道的后面部分应用 - 在已针对每个匹配的邮件安全管理器策略将邮件“拆分”为许多单独的邮件之后。内容过滤器的功能在对邮件进行了邮件过滤器处理以及反垃圾邮件和防病毒扫描后应用。

有关内容过滤器的详细信息，请参阅内容过滤器，第 235 页。

病毒爆发过滤器

思科的病毒爆发过滤器功能提供可主动执行操作的特殊过滤器，从而为抵御新的病毒爆设置了第一道防线。根据思科发布的病毒爆发规则，具有特定文件类型附件的邮件将发送到名为“病毒爆发”(Outbreak) 的隔离区。

“病毒爆发”(Outbreak) 隔离区中的邮件在处理方式上类似于隔离区中的任何其他邮件。有关隔离区和工作队列的详细信息，请参阅隔离区，第 59 页。

有关详细信息，请参阅病毒爆发过滤器，第 307 页。

隔离区

可以过滤传入或外发邮件，并将邮件放入隔离区。隔离区是用于保留和处理邮件的特殊队列或存储库。隔离区中的邮件可以根据隔离区的具体配置进行传送或删除。

以下工作队列功能可将邮件发送到隔离区：

- 垃圾邮件过滤器
- 邮件过滤器
- 防病毒
- 病毒爆发过滤器
- 内容过滤器
- 文件分析（高级恶意软件防护）

从隔离区传送的邮件会重新进行威胁扫描。

交付

邮件管道的传送阶段的侧重于邮件处理的最后阶段，包括限制连接、退回和收件人。

虚拟网关

虚拟网关技术使用户可以将设备分隔成多个虚拟网关地址，以用于发送和接收邮件。每个虚拟网关地址都具有不同的 IP 地址、主机名和域以及邮件传送队列。

有关详细信息，请参阅使用虚拟网关™ 技术为所有托管的域配置邮件网关，第 570 页。

传送限制

使用 `deliveryconfig` 命令根据传送时要使用到IP接口设置传送限制，并设置设备为进行出站邮件传送可建立的最大并发连接数。

有关详细信息，请参阅设置邮件传送参数，第 568 页。

基于域的限制

对于每个域，可以分配最大连接数和最大收件人数，使系统在指定时间段内不超过这些数量。该“好邻居”表通过“邮件策略”(Mail Policies) > “目标控制”(Destination Controls) 页面（或 `destconfig` 命令）定义。

有关详细信息，请参阅使用目标控制来控制邮件传送，第 557 页。

基于域的路由

使用“网络”(Network) > “SMTP 路由”(SMTP Routes) 页面（或 `smtproutes` 命令）将发往特定域的所有邮件重定向至特定邮件交换 (MX) 主机，无需重写信封收件人。

有关详细信息，请参阅路由本地域的邮件，第 523 页。

全局取消订阅

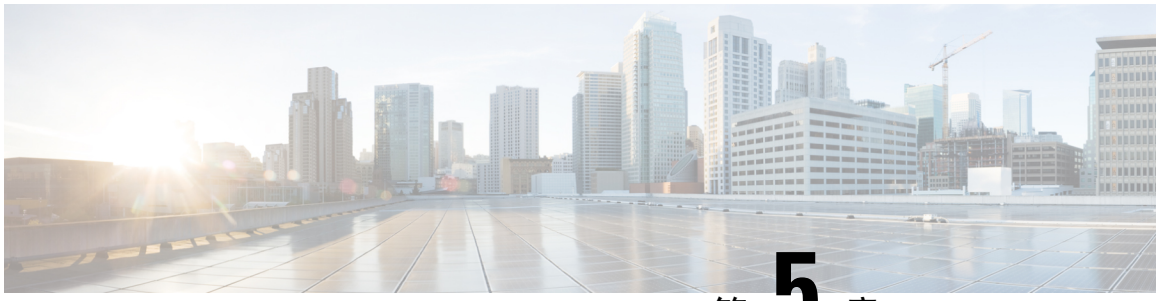
使用“全局取消订阅”(Global Unsubscribe) 可确保特定收件人、收件人域或 IP 地址永远不会接收到来自设备的邮件。如果已启用“全局取消订阅”(Global Unsubscribe)，则系统将根据“全局取消订阅”用户、域、邮件地址和 IP 地址的列表来检查所有收件人地址。不发送匹配的邮件。

有关详细信息，请参阅使用全局取消订用，第 578 页。

退回限制

使用“网络”(Network) > “退回配置文件”(Bounce Profiles) 页面（或 `bounceconfig` 命令）配置 AsyncOS 如何处理所创建的每个侦听程序的硬和软会话退回。创建退回配置文件，然后使用“网络”(Network) > “侦听程序”(Listeners) 页面（或 `listenerconfig` 命令）将配置文件应用到每个侦听程序。还可以使用邮件过滤器，将退回配置文件分配给特定邮件。

有关退回配置文件的详细信息，请参阅定向退回的邮件，第 550 页。



第 5 章

配置网关以接收邮件

本章包含以下部分：

配置网关以接收邮件的概述

该设备用作组织的邮件网关，提供邮件连接、接受邮件，以及将它们中继到相应的系统的功能。该设备可用于从互联网到网络内的收件人主机之间以及从网络内的系统到互联网之间的邮件连接服务。通常，邮件连接请求使用简单邮件传输协议 (SMTP)。默认情况下，该设备用于 SMTP 连接服务，并用作网络的 SMTP 网关（也称为邮件交换器，即“MX”）。

该设备使用侦听程序为传入 SMTP 连接请求服务，侦听程序描述将在特定 IP 接口上配置的邮件处理服务。侦听程序适用于从互联网或从您尝试连接到互联网的网络内的系统进入设备的邮件。可以使用侦听程序指定邮件和连接必须满足的条件，以便能够接受邮件，以及将邮件中继到收件人主机。可将侦听程序视为运行于每个指定 IP 地址的特定端口上的“SMTP 后台守护程序”。此外，侦听程序还定义设备如何与尝试向设备发送邮件的系统通信。

可以创建以下类型的侦听程序：

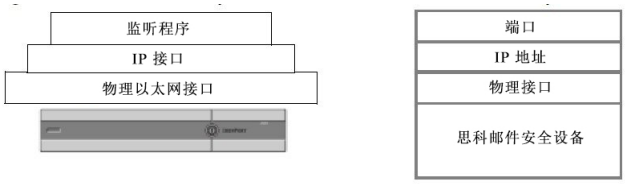
- **公共云**，侦听并接受来自互联网的邮件。公共侦听程序接收来自许多主机的连接，并将邮件定向到有限数量的收件人。
- **私有云**，侦听并接受来自网络内的系统（通常来自内部组件和邮件服务器 (POP/IMAP)）、计划发送给互联网中网络外部的收件人的邮件。专用侦听程序接收来自有限（已知）数量的主机的连接，并将邮件定向到很多收件人。

在创建侦听程序时，还必须指定以下信息：

- **侦听程序属性**。定义适用于所有侦听程序的全局属性，以及特定于每个侦听程序的属性。例如，您可以指定要用于侦听程序的IP接口和端口，以及它是公共还是专用侦听程序。有关如何进行此操作的详细信息，请参阅使用侦听程序，第 62 页。
- **允许哪些主机连接到侦听程序**。定义一组规则，用于控制来自远程主机的传入连接。例如，可以定义远程主机，以及它们是否可以连接到侦听程序。有关如何进行此操作的详细信息，请参阅使用主机访问表定义允许连接的主机，第 81 页。
- **（仅适用于公共侦听程序）侦听程序为其接受邮件的本地域**。定义公共侦听程序接受哪些收件人。例如，如果组织现在使用域 `currentcompany.com`，而其先前使用 `oldcompany.com`，则您可以接受 currentcompany.com 和 `oldcompany.com` 的邮件。有关如何进行此操作的详细信息，请参阅基于域名或收件人地址接受或拒绝连接，第 111 页。

在侦听程序中配置的设置（包括其“主机访问表”(Host Access Table) 和“收件人访问表”(Recipient Access Table)），将会影响在 SMTP 会话期间侦听程序与 SMTP 服务器的通信方式。这使设备能在连接关闭之前拦截垃圾邮件主机。

图 *8:* 侦听程序、*IP* 接口和物理以太网接口之间的关系



使用侦听程序

可在 GUI 中的“网络”>“侦听程序”页面上或使用 CLI 中的 listenerconfig 命令来配置侦听程序。

可以定义适用于所有侦听程序的全局设置。有关详细信息，请参阅配置侦听程序的全局设置，第 64 页。

在使用和配置设备上的侦听程序时，需要考虑以下规则和指南：

- 可为配置的每个 IP 接口定义多个侦听程序，但每个侦听程序都必须使用一个不同的端口。
- 默认情况下，侦听程序使用 SMTP 作为邮件协议提供邮件连接服务。但也可以将设备配置为使用快速邮件队列协议 (QMQP) 提供邮件连接服务。可以使用 `listenerconfig` CLI 命令进行此操作。
- 侦听程序支持互联网协议第 4 版 (IPv4) 和第 6 版 (IPv6) 地址。可在单个侦听程序上使用任一版本的协议，也可同时使用两个版本。侦听程序使用与连接主机相同版本的协议传输邮件。例如，如果同时针对 IPv4 和 IPv6 配置了侦听程序，并将其连接到使用 IPv6 的主机，则该侦听程序将使用 IPv6。但是，如果将侦听程序配置只使用 IPv6 地址，它将无法连接到只使用 IPv4 地址的主机。
- 在运行“系统设置向导”(System Setup Wizard) 后，将在设备上配置至少一个侦听程序（使用默认值）。但是，当您手动创建侦听程序时，AsyncOS 不会使用这些默认 SBRS 值。

- **C170 和 C190 设备**：默认情况下，“系统设置向导”引导您配置一个公共侦听程序，即可用于接收来自互联网的邮件，也可用于中继来自内部网络的邮件。也就是说，一个侦听程序可以执行两种功能。
- 为了帮助测试设备和排除设备故障，可以创建“黑洞”类型的侦听程序，而不是公共或专用侦听程序。在创建黑洞侦听程序时，可以选择是否在删除邮件之前将邮件写入磁盘。（有关详细信息，请参阅“测试和故障排除”。）在删除邮件之前将邮件写入磁盘，可以帮助测量接收速率和队列的速度。不将邮件写入磁盘的侦听程序，可以帮助测量从邮件生成系统接收邮件的纯接收速率。此侦听程序类型只能通过 CLI 中的 `listenerconfig` 命令使用。

图 - 具有两个以上以太网接口的设备模型上的公共和专用侦听程序展示了“系统设置向导”在具有两个以上以太网接口的设备模型上创建的典型邮件网关配置。创建了两个侦听程序：一个公共侦听程序，在一个接口上提供入站连接服务；一个专用侦听程序，在第二个 IP 接口上提供出站连接服务。

图 - 仅具有两个以太网接口的设备模型上的公共侦听程序展示了“系统设置向导”在仅具有两个以太网接口的设备模型上创建的典型邮件网关配置。在一个 IP 接口上创建了一个公共侦听程序，同时提供入站和出站连接服务。

图 *9:* 多种型号具有两个以上以太网接口的设备上的公共和专用侦听程序

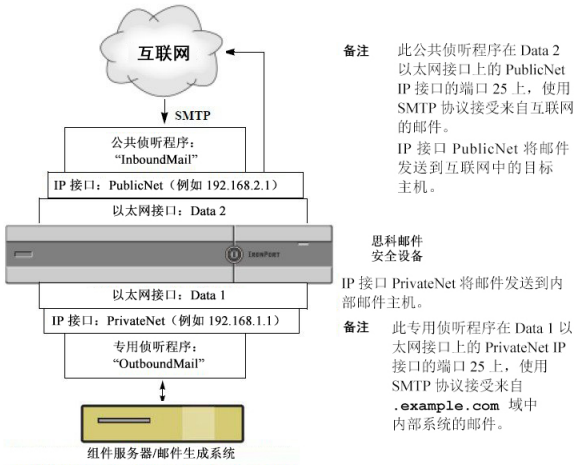
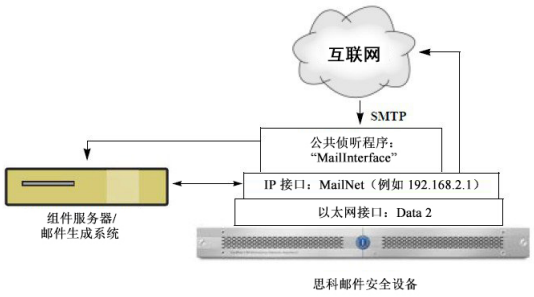


图 *10:* 多种型号仅有两个以太网接口的设备上的公共侦听程序



注释 此公共侦听程序在 Data 2 以太网接口上的 PublicNet IP 接口的端口 25 上，使用 SMTP 协议接受来自互联网的邮件，并中继来自 .example.com 域中内部系统的邮件。IP 接口 MailNet 将邮件发送到互联网中的目标主机，以及内部邮件主机。

配置侦听程序的全局设置

侦听程序的全局设置会影响在设备上配置的所有侦听程序。如果侦听程序使用同时具有互联网协议第 4 版 (IPv4) 和第 6 版 (IPv6) 地址的接口，则侦听程序设置将同时适用于 IPv4 和 IPv6 流量。

步骤 1 依次选择**网络 > 侦听程序**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 更改下表中定义的设置。

表 5: 侦听程序全局设置

全局设置	说明
最大并发连接数	为侦听程序设置最大并发连接数量。C3x0 和 C6x0 模型的默认值为 300，C1x0 模型的默认值为 50。如果侦听程序同时接受 IPv4 和 IPv6 连接，则连接数量将分为两个部分。例如，如果最大并发连接数量为 300，则 IPv4 和 IPv6 连接的总和不能超过 300。
最大并发 TLS 连接数	设置所有侦听程序组合在一起的最大并发 TLS 连接数量。默认值为 100。如果侦听程序同时接受 IPv4 和 IPv6 TLS 连接，则连接数量将分为两个部分。例如，如果最大并发连接数量为 100，则 IPv4 和 IPv6 TLS 连接的总和不能超过 100。
注入计数器重新设置时间	允许您在重置注入控制计数器时进行调整。对于为大量不同的 IP 地址保留计数器的非常繁忙的系统，将计数器配置为更频繁地重置（例如，每 15 分钟而不是每 60 分钟）可以确保数据不会增长到一个无法管理的规模并影响系统性能。 目前的默认值为 1 小时。可以指定的期限最短为1分钟（60 秒），最长为 4 小时（14,400 秒）。 请参阅注入控制周期性，第 102 页。
不成功入站连接的超时周期 (Timeout Period for Unsuccessful Inbound Connections)	设置 AsyncOS 在关闭不成功入站连接之前将允许其保持不变的时间长度。 不成功的连接可能是这样一种 SMTP 会话：不断发出 SMTP 或 ESMTP 命令，但未发生成功的邮件注入。当达到指定的超时时间后，该行为将发送错误消息并断开连接： “421 等待成功的邮件注入超时，正在断开连接。”(421 Timed out waiting for successful message injection, disconnecting.) 在连接成功注入邮件之前，都会被视为不成功。 仅可用于公共侦听程序上的 SMTP 连接。默认值为 5 分钟。

全局设置	说明
所有入站连接的总时间限制 (Total Time Limit for All Inbound Connections)	设置 AsyncOS 在关闭入站连接以前允许其保持完整的时间长度。 此设置旨在通过实施最大允许连接时间来保留系统资源。一旦达到此最大连接时间的大约 80%，将发出以下消息： “421 已超过允许的连接时间，正在断开。”(421 Exceeded allowable connection time, disconnecting.) 当连接超过最大连接时间的 80% 时，设备将尝试断开连接，以防止在邮件中间断开连接。如果入站连接打开的时间长度足以达到最大连接时间的 80%，则该入站连接可能会发生问题。在指定时间限制时，请牢记此阈值。 仅可用于公共侦听程序上的 SMTP 连接。默认值为 15 分钟。
主题的最大大小 (Maximum size of subject)	主题大小处于指定限制范围内的邮件将被接受，任何其他邮件将被拒绝。如果将此值设置为 0，则不应用任何限制。
HAT 延迟拒绝 (HAT delayed rejections)	配置是否在邮件收件人级别执行 HAT 拒绝。默认情况下，HAT 拒绝的连接将关闭，并且在 SMTP 会话开始处显示标语消息。 当邮件因 HAT“拒绝”(Reject) 设置而被拒绝时，AsyncOS 可在邮件收件人级别 (RCPT TO)（而不是在 SMTP 会话开始时）执行拒绝。通过此方式拒绝邮件会延迟邮件拒绝并退回邮件，以便 AsyncOS 保留更多有关已拒绝邮件的详细信息。例如，可以通过被阻止的邮件的地址和每个收件人地址查看邮件。延迟 HAT 拒绝还可以降低发送 MTA 将执行多次重试的可能性。 在启用 HAT 延迟拒绝后，将发生以下行为： MAIL FROM 命令将被接受，但不会创建邮件对象。 所有 RCPT TO 命令都将被拒绝，并显示一段文本，阐明发送邮件的权限已被拒绝。 如果发送 MTA 通过 SMTP AUTH 进行身份验证，则它们将被授予“中继”(RELAY) 策略，并且允许它们正常传送邮件。 只能通 CLI `listenerconfig --> setup command` 命令进行配置。

步骤 4 提交并确认更改。

包含多种编码的邮件设置

您可以在修改以下参数的邮件编码时定义设备的行为：

- 报头
- 未标记的非 ASCII 信头
- 不匹配的页脚或页眉编码

要配置此行为，请使用 CLI 中的 localeconfig 命令。

注释 不能使用 Web 界面配置此行为。

有关示例 CLI 脚本，请参阅免责声明设置标记和多个编码，第 493 页。

通过使用 Web 界面创建侦听程序侦听连接请求

步骤 1 依次选择网络 > 侦听程序。

步骤 2 点击**添加侦听程序 (Add Listener)**。

步骤 3 配置下表中定义的设置。

表 6: 侦听程序设置

Name	为侦听程序提供的唯一昵称，供将来参考。为侦听程序定义的名称区分大小写。AsyncOS 不允许创建两个相同的侦听程序名称。
侦听程序类型 (Type of Listener)	从以下侦听程序类型中选择一个： • **公共云**，公共侦听程序包含接收来自互联网的邮件的默认特征。 • **私有云**，专用侦听程序供专用（内部）网络使用。
接口	选择要在其上创建侦听程序的已配置设备 IP 接口和 TCP 端口。根据接口使用的 IP 地址的版本，侦听程序可以接受来自 IPv4 地址、IPv6 地址或两个版本的连接。默认情况下，SMTP 使用端口 25，QMQP 使用端口 628。
退回配置文件	选择退回配置文件（列表中提供了通过 CLI 中的 `bounceconfig` 命令创建的退回配置文件，请参阅创建新的退回配置文件，第 556 页）。
免责声明在上 (Disclaimer Above)	选择一个免责声明，以附加在邮件上方或下方（列表中提供了通过“邮件策略”(Mail Policies) >“文本资源”(Text Resources) 页面或 CLI 中的 `textconfig` 命令创建的免责声明，请参阅“文本资源”一章）。
免责声明在下 (Disclaimer Below)	选择要在邮件上方或下方附加的免责声明（通过“邮件策略”[Mail Policies]>“文本资源”[Text Resources] 页面或 CLI 中的 `textconfig` 命令创建的免责声明可在列表中获取，请参阅“文本资源”一章）。
SMTP 身份验证配置文件	指定 SMTP 身份验证配置文件。
证书	为指向侦听程序的 TLS 连接指定一个证书（列表中提供了通过“网络”(Network) >“证书”(Certificates) 页面或 CLI 中的 `certconfig` 命令添加的证书，请参阅加密与其他 MTA 的通信概述，第 509 页）。

步骤 4 （可选）根据下表中的定义，配置用于控制 SMTP“`MAIL FROM`”和“`RCPT TO`”命令中解析的设置。

设置	说明
地址解析器类型 (Address Parser Type)	使用以下解析器类型之一选择设备遵守 RFC2821 标准的严格程度： **严格模式：** • 严格模式将尽量遵从 RFC 2821。在严格模式下，地址解析器将遵从 RFC 2821 规则，但有以下例外情况/增强功能： • 在冒号后允许使用空格，如在“MAIL FROM: <joe@example.com>”一样。 • 在域名中允许使用下划线。 • “MAIL FROM”和“RCPT TO”命令不区分大小写。 • 不会特殊处理句点（例如，RFC 2821 不允许“J.D.”这类用户名）。 可以启用下面的一些附加选项，这些选项在技术上违反 RFC 2821。 **宽松模式：** 宽松解析器基本上执行源自先前版本 AsyncOS 的现有行为。它将尽力“查找”邮件地址，并且： • 忽略注释。它支持嵌套注释（在括号中找到的任何内容），并会忽略它们。 • 在“RCPT TO”和“MAIL FROM”命令中提供的邮件地址周围不需要使用尖括号。 • 允许多个嵌套尖括号（它将搜索处于最深嵌套级别的邮件地址）。
允许 8 位用户名 (Allow 8-bit User Names)	如果启用该选项，则允许在地址的用户名部分使用 8 位字符，无需转义。
允许 8 位域名 (Allow 8-bit Domain Names)	如果启用该选项，则允许在地址的域部分使用 8 位字符。

设置	说明
允许部分域 (Allow Partial Domains)	如果启用该选项，将允许部分域。部分域可以根本不是域，也可以是不带句点的域。 以下地址是部分域的示例： • foo • foo@ • foo@bar 为使“默认域”(Default Domain) 功能正常工作，必须启用此选项。 **添加默认域**：用于不具有完全限定域名的邮件地址的默认域。除非在“SMTP 地址解析”选项中启用了“允许部分域”，否则将禁用此选项。这将通过将“默认发件人域”添加到不含完全限定域名的发件人和收件人地址，影响侦听程序如何修改它所中继的邮件。（换句话说，可以自定义侦听程序如何处理“裸”地址。） 如果您有某种传统系统，在发送邮件时不会将贵公司的域添加（附加）到发件人地址，则会使用此选项添加默认发件人域。例如，传统系统可以自动创建邮件，仅输入字符串“`joe`”作为邮件的发件人。更改默认发件人域会将“`@yourdomain.com`”附加到“joe”，以创建完全限定的发件人名称 `joe@yourdomain.com`。
源路由 (Source Routing)	确定是否在“MAIL FROM”和“RCPT TO”地址中检测源路由的行为。源路由是一种特殊格式的邮件地址，使用多个“@”字符来指定路由（例如：@one.dom@two.dom:joe@three.dom）。如果设置为“拒绝”(reject)，地址将被拒绝。如果设置为“拆分”(strip)，将删除地址的源路由部分，并将正常注入邮件。
未知的地址文字 (Unknown Address Literals)	确定收到系统无法处理的地址文字时的行为。目前，这是指除 IPv4 以外的所有文字。因此，举例来说，对于 IPv6 地址文字，您可以在协议级别拒绝该地址，也可以接受并立即硬退回该地址。 包含文字的收件人地址将导致立即硬退回。发件人地址可以完成传送。如果无法传送邮件，则该硬退回将被硬退回（双重硬退回）。 在拒绝的情况下，无论是发件人地址还是收件人地址，都将在协议级别立即被拒绝。
在用户名中拒绝使用这些字符 (Reject These Characters in User Names)	包括此处输入的字符（例如 % 或 !）的用户名将被拒绝。

步骤 5 （可选）根据下表中的定义，配置用于自定义侦听程序行为的高级设置。

设置	说明
最大并发连接数	允许的最大连接数量。
TCP 侦听队列大小 (TCP Listen Queue Size)	AsyncOS 将在 SMTP 服务器接受连接之前管理的连接积压。

设置	说明
CR 和 LF 处理 (CR and LF Handling)	选择如何处理包含裸 CR（回车）符和 LF（换行）符的邮件。 • **正常 (Clean)**。允许该邮件，但将裸 CR 符和 LF 符转换为 CRLF 符。 • **拒绝 (Reject)**。拒绝该邮件。 • **允许 (Allow)**。允许消息。
添加Received信头	为所有已收到的邮件添加已接收信头。侦听程序还可通过在每个邮件上添加“Received:”信头，修改其中继的邮件。如果您不想包括“已收到：”(Received:) 信头，可以使用此选项禁用该功能。 **注释** “已收到：”(Received:) 信头不会添加到工作队列处理中的邮件，而是会在邮件进入队列等待传送时添加。 通过禁用已接收信头这种方式，可以确保不会因在任何离开您的基础设施的邮件上显示内部服务器的 IP 地址或主机名，而暴露网络的拓扑。在禁用已接收信头时，请小心。
使用SenderBase IP Profiling	选择是否启用“SenderBase IP 剖析”(SenderBase IP Profiling)，并配置以下设置： • **查询的超时时间 (Timeout for Queries)**。定义设备缓存通过 SenderBase 信誉服务查询的信息的时间长度。 • **每个连接的 SenderBase 超时时间 (SenderBase Timeout per Connection)**。定义设备缓存每个连接的 SenderBase 信息的时间长度。

步骤 6 （可选）根据下表中的定义，配置用于控制与此侦听程序相关联的 LDAP 查询的设置。

使用这些设置在侦听程序上启用 LDAP 查询。在使用此选项之前，必须首先创建 LDAP 查询。每种类型的查询都有单独的子部分需要配置。点击查询的类型可以展开子部分。

有关创建 LDAP 查询的详细信息，请参阅LDAP 查询，第 585 页。

查询类型	说明
接受查询 (Accept Queries)	对于接受查询，请从列表中选择要使用的查询。可以指定是在工作队列处理期间还是在 SMTP 会话期间发生 LDAP 接受。 对于发生于工作队列处理期间的 LDAP 接受，请为不匹配收件人指定行为：退回或丢弃。 对于发生于 SMTP 会话期间的 LDAP 接受，请指定如果无法访问 LDAP 服务器应该如何处理邮件。可以选择通过一段代码和自定义响应允许邮件或丢弃连接。最后，选择如果在 SMTP 会话期间达到“帐户搜集攻击预防”(Directory Harvest Attack Prevention, DHAP) 阈值，是否丢弃连接。 在 SMTP 会话中执行收件人验证可能会减少多个 LDAP 查询之间的延迟。因此，您可能会注意到，在启用会话 LDAP 接受后，目录服务器上的负载将增加。 有关详细信息，请参阅LDAP 查询概述，第 585 页。

查询类型	说明
路由查询 (Routing Queries)	对于路由查询，请从列表中选择查询。有关详细信息，请参阅LDAP 查询概述，第 585 页。
伪装查询 (Masquerade Queries)	对于伪装查询，请从列表中选择一项查询，然后选择要伪装哪个地址，如“发件人”(From) 或“抄送”(CC) 信头地址。 有关详细信息，请参阅LDAP 查询概述，第 585 页。
组查询 (Group Queries)	对于组查询，请从列表中选择查询。有关详细信息，请参阅LDAP 查询概述，第 585 页。

步骤 7 提交并确认更改。

部分域、默认域和格式不正确的 MAIL FROM

如果您在“SMTP 地址解析”(SMTP Address Parsing) 选项中为侦听程序启用了信封发件人验证或禁用了允许部分域，则将不再使用该侦听程序的默认域设置.

这些功能互相排斥。

通过使用 CLI 创建侦听程序来侦听连接请求

下表列出了与创建和编辑侦听程序有关的任务中使用的一些 listenerconfig 子命令。

表 7: 创建侦听程序的任务

创建侦听程序的任务	命令和子命令
创建新侦听程序	`listenerconfig -> new`
编辑侦听程序的全局设置	`listenerconfig -> setup`
为侦听程序指定退回配置文件	`bounceconfig, listenerconfig-> edit -> bounceconfig`
将免责声明与侦听程序关联起来	`textconfig, listenerconfig -> edit -> setup -> footer`
配置 SMTP 身份验证	`smtpauthconfig, listenerconfig -> smtpauth`
配置 SMTP 地址解析	`textconfig, listenerconfig -> edit -> setup -> address`
配置侦听程序的默认域	`listenerconfig -> edit -> setup -> defaultdomain`

创建侦听程序的任务	命令和子命令
为邮件添加已接收信头	`listenerconfig -> edit -> setup -> received`
将裸 CR 符和 LF 符更改为 CRLF	`listenerconfig -> edit -> setup -> cleansmtp`
修改主机访问表	`listenerconfig -> edit -> hostaccess`
为本地域或特定用户 (RAT) 接受邮件（仅适用于公共侦听程序）	`listenerconfig -> edit -> rcptaccess`
加密侦听程序上的对话 (TLS)	`certconfig, listenerconfig -> edit`
选择证书 (TLS)	`listenerconfig -> edit -> certificate`

有关 listenerconfig 命令的详细信息，请参阅适用于思科邮件安全设备的 AsyncOS 的 CLI 参考指南。

有关邮件路由和传输配置的信息，请参阅配置路由和传送功能，第 523 页。

高级 HAT 参数

下表定义了高级 HAT 参数的语法。请注意，对于以下数值，可以添加后缀 **k** 代表千字节，或后缀 **M** 代表兆字节。没有字母的值将被视为字节数。标有星号的参数支持下表中所示的变量语法。

表 *8:* 高级 *HAT* 参数语法

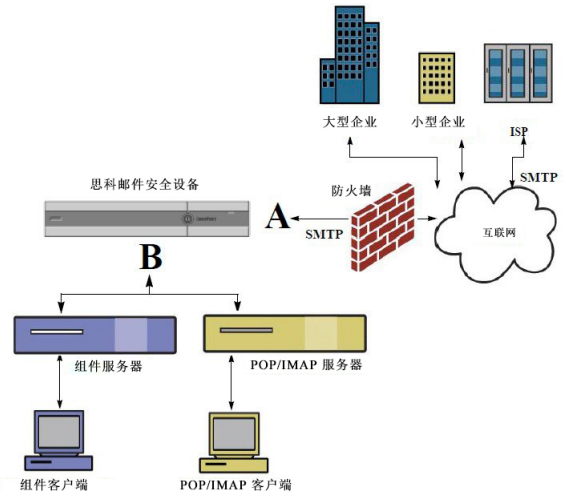
参数	语法	值	示例值
每个连接的最大邮件数 (Maximum messages per connection)	`max_msgs_per_session`	编号	`1000`
每封邮件的最大收件人数	`max_rcpts_per_msg`	编号	`10000` `1k`
最大邮件大小	`max_message_size`	编号	`1048576` `20M`
此侦听程序允许的最大并发连接数量 (Maximum Concurrent Connections) (Maximum concurrent connections allowed to this listener)	`max_concurrency`	编号	`1000`
SMTP 横幅代码 (SMTP Banner Code)	`smtp_banner_code`	编号	`220`

参数	语法	值	示例值
SMTP 横幅文本 (SMTP Banner Text) (*)	`smtp_banner_text`	字符串	`Accepted`
SMTP 拒绝横幅代码 (SMTP Reject Banner Code)	`smtp_banner_code`	编号	`550`
SMTP 拒绝横幅文本 (SMTP Reject Banner Text) (*)	`smtp_banner_text`	字符串	`Rejected`
忽略 SMTP 横幅主机名 (Override SMTP Banner Hostname)	`use_override_hostname`	on | off | default	`default`
	`override_hostname`	字符串	`newhostname`
使用 TLS	`tls`	on | off | required	`on`
使用反垃圾邮件扫描 (Use anti-spam scanning)	`spam_check`	on | off	`off`
使用病毒扫描 (Use virus scanning)	`virus_check`	on | off	`off`
每小时最大收件人数 (Maximum Recipients per Hour)	`max_rcpts_per_hour`	编号	`5k`
每小时允许的最大收件人数量错误代码 (Maximum Recipients per Hour Error Code)	`max_rcpts_per_hour_code`	编号	`452`
每小时允许的最大收件人数量文本 (Maximum Recipients per Hour Text) (*)	`max_rcpts_per_hour_text`	字符串	`Too manyrecipients`
使用 SenderBase (Use SenderBase)	`use_sb`	on | off	`on`
定义 SenderBase 信誉得分 (Define SenderBase Reputation Score)	`sbrs[`*`value1`*`:`*`value2`*`]`	-10.0- 10.0	`sbrs[-10:-7.5]`
目录搜集攻击预防: 每小时的最大无效收件人数 (Directory Harvest Attack Prevention: Maximum Invalid Recipients Per Hour)	`dhap_limit`	编号	`150`

企业网关配置

在此配置中，企业网关配置接受来自互联网的邮件，并将邮件中继到组件服务器、POP/IMAP 服务器，或其他 MTA。同时，企业网关接受来自组件服务器和其他邮件服务器的 SMTP 邮件，以便中继到互联网上的收件人。

图 *11:* 企业网关的公共和专用侦听程序

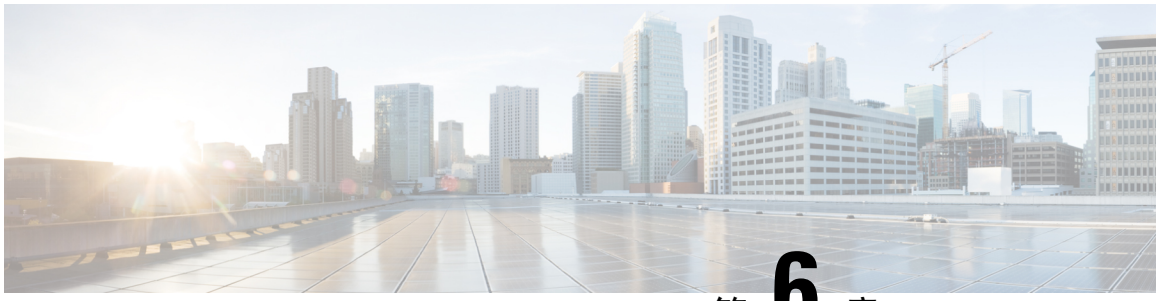


在此配置中，需要至少两个侦听程序：

- 专门配置一个侦听程序，用于接受来自互联网的邮件
- 专门配置一个侦听程序，用于接受来自内部组件和邮件服务器 (POP/IMAP) 的邮件

通过为不同的公共和专用网络创建不同的公共和专用侦听程序，可在邮件中区分安全、策略实施、报告和管理。例如，默认情况下，在公共侦听程序上接收的邮件将由您配置的反垃圾邮件引擎和防病毒扫描引擎扫描，而在专用侦听程序上接收的邮件则不会受到扫描。

图 - 企业网关的公共和专用侦听器显示在本企业网关配置中配置了一个公共侦听器 (A) 和一个专用侦听器 (B)。



第 6 章

发件人信誉过滤

本章包含以下部分：

发件人信誉过滤概述

发件人信誉过滤是垃圾邮件的第一道防线，允许您基于 Cisco SenderBase™ 信誉服务确定的发件人信誉来控制通过邮件网关的邮件。

设备可以接受来自已知或高信誉发件人（例如客户和合作伙伴）的邮件，并直接将它们传送给终端用户，不进行任何内容扫描。来自未知或低信誉发件人的邮件可能需要接受内容扫描，例如反垃圾邮件和防病毒扫描，也可以限制您愿意从每个发件人那里接受的邮件数。对于信誉最差的邮件发件人，可以根据首选项设置拒绝其连接或退回邮件。

注释 文件信誉过滤是一项独立服务。有关信息，请参阅 文件信誉过滤和文件分析： ，第 353 页

SenderBase 信誉服务

思科 SenderBase 信誉服务使用 SenderBase 成员网络中的全球数据，基于抱怨次数、邮件数量统计数据及公共黑名单和开放式代理列表中的数据，向邮件发件人分配一个 SenderBase 信誉得分。SenderBase 信誉得分有助于区分合法发件人与垃圾邮件来源。您可以决定阻止信誉得分低的发件人的邮件数量阈值。

SenderBase 安全网络网站 (www.senderbase.org) 提供最新邮件和网络威胁的全局概述，按国家/地区显示当前的邮件流量，并允许您根据 IP 地址、URL 或域查询信誉得分。

SenderBase 信誉得分 (SBRS)

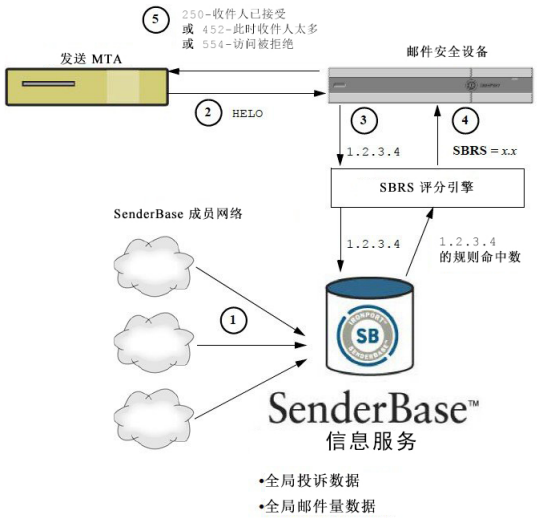
SenderBase 信誉得分 (SBRS) 是基于 SenderBase 信誉服务中的信息分配给 IP 地址的数值。SenderBase 信誉服务整合 25 个公共黑名单和开放式代理列表中的数据，并将此数据与 SenderBase 中的全球数据合并，进而分配一个介于 -10.0 到 +10.0 之间的分数，如下所示：

得分	含义
-10.0	很可能是垃圾邮件的来源
0	中立；或信息不足，无法提供相关建议
+10.0	很可能是可信发件人

得分越低（负值越大），越有可能是垃圾邮件。得分为 -10.0，表示此邮件“一定”是垃圾邮件；而得分为 10.0，表示邮件“一定”是合法的。

使用 SBRS，可以将设备配置为基于发件人的可信度对发件人应用邮件流策略。（还可以创建邮件过滤器来指定 SenderBase 信誉得分的“阈值”，进一步对系统处理的邮件执行操作。有关详细信息，请参阅SenderBase 信誉规则，第 145 页和绕过反垃圾邮件系统操作，第 184 页。）

图 *12: SenderBas* 信誉服务



1. SenderBase 成员实时发送全球数据
2. 发送 MTA 将打开与设备的连接
3. 设备检查连接 IP 地址的全球数据
4. SenderBase 信誉服务计算此邮件是垃圾邮件的概率，并分配 SenderBase 信誉得分
5. 思科根据 SenderBase 信誉得分返回响应

SenderBase 信誉过滤器的工作原理

发件人信誉过滤器技术旨在从设备中可用的剩余安全服务处理中，转轨尽可能多的邮件。（请参阅了解邮件通道，第 51 页。）

启用发件人信誉过滤时，将简单拒绝已知恶意发件人的邮件。来自全球2000家公司的已知正常邮件会自动路由到垃圾邮件过滤器，降低误报的可能性。未知或“灰色”邮件将路由到反垃圾邮件扫描引擎。使用此方法，发件人信誉过滤器可使内容过滤器的负载降低多达 50%。

图 *13:* 发件人信誉过滤示例

不同发件人信誉过滤方法的建议设置

根据企业目标，可以实施保守、中等或主动方法。

方案	特征	白名单	黑名单	可疑列表	未知列表
		发件人基本信誉得分范围：			
保守	接近零误报，较好性能	7 到 10	-10 到 -4	-4 到 -2	-2 到 7
中等 （系统设定值）	很少误报，高性能	不使用发件人基本信誉得分。	-10 到 -3	-3 到 -1	-1 到 +10
积极	有些误报，最高性能 此选项将从反垃圾邮件处理中转轨大多数邮件。	4 到 10	-10 到 -2	-2 到 -1	-1 到 4
所有方法		**邮件流策略：**			
		受信任	已阻止	限制的	已接受

编辑侦听程序的发件人信誉过滤得分阈值

如果要更改默认 SenderBase 信誉服务 (SBRS) 得分阈值或添加信誉过滤的发件人组，请使用此过程。

注释 介绍有关 SBRS 得分阈值的其他设置及邮件流策略设置。 使用主机访问表定义允许连接的主机，第 81 页

准备工作

- 如果您的设备设置为从本地 MX/MTA 接收邮件，请标识出可能会屏蔽发件人 IP 地址的上游主机。有关详细信息，请参阅通过传入中继确定部署中的发件人 IP 地址，第 286 页。
- 了解发件人基本信誉得分。请参阅按 SenderBase 信誉得分定义发件人组，第 86 页。
- 选择适合您的组织的过滤方法，并注意针对该方法的建议设置。请参阅不同发件人信誉过滤方法的建议设置，第 77 页。

步骤 1 依次选择**邮件策略 (Mail Policies)** > **HAT 概述 (HAT Overview)**。

步骤 2 从**发件人组(监听程序) (Sender Groups (Listener))** 菜单中选择公共监听程序。

步骤 3 点击某个发件人组的链接。

例如，点击“SUSPECTLIST”链接。

步骤 4 点击**编辑设置 (Edit Settings)**。

步骤 5 针对此发件人组，输入 SenderBase 信誉得分范围。

例如，对于“WHITELIST”，输入范围 7.0 到 10。

步骤 6 点击 **Submit**。

步骤 7 根据需要，针对此监听程序的每个发件人组重复上述操作。

步骤 8 确认更改。

使用 SBRS 测试发件人信誉过滤

除非定期接收大部分垃圾邮件或已设置“虚拟”帐户来专门接收组织的垃圾邮件，否则可能很难立即测试实施的 SBRS 策略。但是，如果您将使用 SenderBase 信誉得分的信誉过滤条目添加到了下表中所示的监听程序 HAT 中，会看到有小比例的传入邮件为“未分类”。

使用任意 SBRS 的 `trace` 命令测试策略。请参阅使用测试邮件调试邮件流：追踪，第 935 页。在 CLI 和 GUI 中都可使用 `trace` 命令。

表 *9:* 实施 *SBRS* 的建议邮件流量策略

策略名称	主要行为（访问规则）	参数	值
$BLOCKED	REJECT	None	

策略名称	主要行为（访问规则）	参数	值
$THROTTLED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: 启用Anti-Spam扫描: 使用TLS: Maximum recipients / hour: 使用SenderBase:	10 20 1 MB 10 开启 关闭 **20**（建议） 开启
$ACCEPTED （公共监听程序）	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: 启用Anti-Spam扫描: 使用TLS: 使用SenderBase:	1,000 1,000 100 MB 1,000 开启 关闭 开启
$TRUSTED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: 启用Anti-Spam扫描: 使用TLS: Maximum recipients / hour: 使用SenderBase:	1,000 1,000 100 MB 1,000 关闭 关闭 -1 （已禁用） 关闭

注释 在 $THROTTLED 策略中，每小时来自远程主机的最大收件人数默认设置为每小时 20 位收件人。请注意，此设置控制最大可用限制。如果此参数过于严格，可以提高每小时接收的收件人数。有关默认主机访问策略的详细信息，请参阅了解预定义发件人组和邮件流策略，第 90 页。

监控 SenderBase 信誉服务的状态

SenderBase 信誉得分服务将 SRBS 得分发送到设备。SenderBase 网络服务器向设备发送对您发送邮件的 IP 地址、域和组织的相关信息。AsyncOS 将这些数据用于其报告和邮件监控功能。

要查看这些服务的连接状态，请依次选择**安全服务 (Security Services) > SenderBase**。

“安全服务”(Security Services) 菜单的“SenderBase”页面显示从设备到 SenderBase 网络状态服务器和 SenderBase 信誉得分服务的连接状态和最近查询时间戳。

在 CLI 中执行 `sbstatus` 命令可显示相同的信息。

在邮件主题中输入低 SBRS 分数

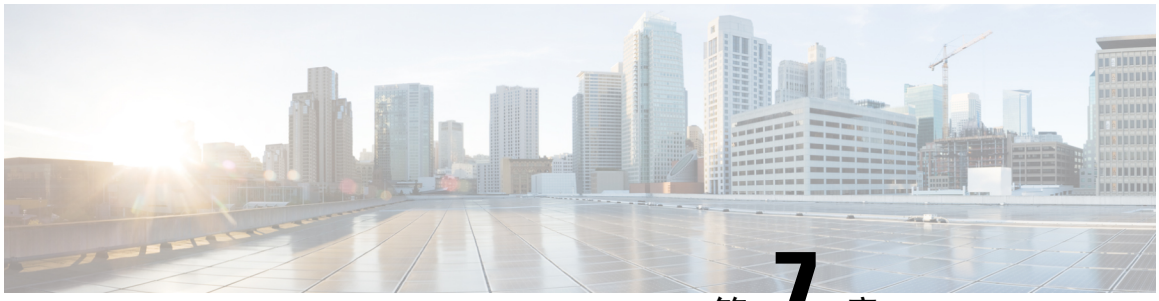
虽然思科建议执行限制，不过使用 SenderBase 信誉服务的另一种方法是修改可疑垃圾邮件的主题行。为此，请使用下表中所示的邮件过滤器。此过滤器使用 reputation 过滤器规则及 strip-header 和 insert-header 过滤器操作，将 SenderBase 信誉分数低于 -2.0 的邮件主题行替换为包括实际 SenderBase 信誉分数的主题行，表示形式为：**{Spam** *SBRS***}**。在本例中，会将 *listener_name* 替换为您的公共监听程序。（包括其自有行中的句号，以便可以直接剪切此文本并粘贴到 filters 命令的命令行界面。）

表：使用 SBRS 修改主题信头的邮件过滤器：示例 1

```
sbrs_filter:

if ((recv-inj == "listener_name
" AND subject != "\\{Spam -?[0-9.]+\\}"))

{

       insert-header("X-SBRS", "$REPUTATION");

       if (reputation <= -2.0)

{

       strip-header("Subject");

       insert-header("Subject", "$Subject \\{Spam $REPUTATION\\}");

      }

 }

.
```

相关主题

- 使用邮件过滤器实施邮件策略 ， 第 117 页



第 7 章

使用主机访问表定义允许连接的主机

本章包含以下部分：

有关定义允许连接哪些主机的概述

对于每个配置的侦听程序，必须定义一个规则集来控制来自远程主机的传入连接。例如，可以定义远程主机，以及它们是否可以连接到侦听程序。通过 AsyncOS 可以使用主机访问表 (HAT) 定义允许将哪些主机连接到侦听程序。

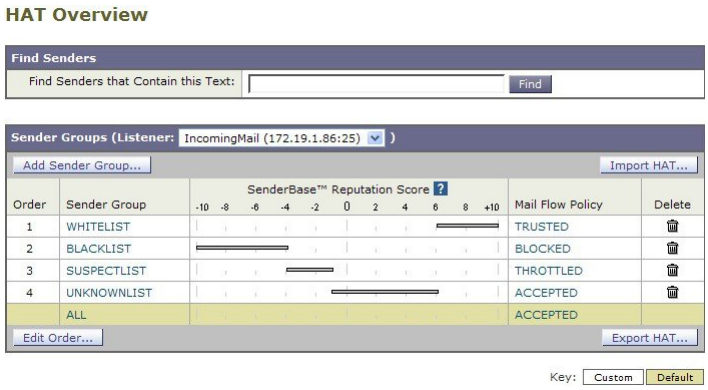
HAT 维护一组规则，通过这些规则可控制侦听程序来自远程主机的传入连接。每个配置的侦听程序都有自己的 HAT。为公共和专用侦听程序配置 HAT。

要控制来自远程主机的传入连接，可定义以下信息：

- **远程主机**。定义远程主机尝试连接到侦听程序的方式。将远程主机定义分组为发件人组。例如，可以按 IP 地址和部分主机名在发件人组中定义多个远程主机。还可以通过远程主机的 SenderBase 信誉得分来定义远程主机。有关详细信息，请参阅将远程主机定义在发件人组中， 第 82 页。
- **访问规则**。可以定义是否允许发件人组中定义的远程主机连接到侦听程序，以及在什么情况下进行连接。使用邮件流策略定义访问规则。例如，可以定义允许特定发件人组连接到侦听程序，但是每个连接只允许最大邮件数。有关详细信息，请参阅 使用邮件流策略定义邮件发件人的访问规则， 第 87 页

在“邮件策略”(Mail Policies) >“HAT 概述”(HAT Overview) 页面上定义允许哪些主机连接到侦听程序。下图显示了 HAT 概述，其中包括在默认情况下为公共侦听程序定义了发件人组和邮件流策略。

图 *14:* 邮件策略 > *HAT* 概述页 - 公共侦听程序



当侦听程序收到 TCP 连接时，会将源 IP 地址与配置的发件人组进行比较。它会按照在“HAT 概述”(HAT Overview) 页面上列出的顺序评估发件人组。当找到匹配项时，它会将配置的邮件流策略应用到连接。如果已在发件人组中配置了多个条件，则只要匹配其任何条件，就会匹配该发件人组。

当创建侦听程序时，AsyncOS 会为侦听程序创建预定义的发件人组和邮件流策略。可以编辑预定义的发件人组和邮件流策略，并创建新的发件人组和邮件流策略。有关详细信息，请参阅了解预定义发件人组和邮件流策略，第 90 页。

可以将主机访问表中存储的所有信息导出到文件，而且可以将文件中存储的主机访问表信息导入到侦听程序的设备，从而覆盖所有配置的主机访问表信息。有关详细信息，请参阅使用主机访问表配置，第 99 页。

默认 HAT 条目

默认情况下，会定义 HAT 以根据侦听程序类型采取不同的操作：

- **公共侦听程序**。HAT 设置为接受来自所有主机的邮件。
- **专用侦听程序**。HAT 设置为转发来自您指定主机的邮件，并拒绝所有其他主机。

在“HAT 概述”(HAT Overview) 中，默认条目名为“ALL”。可以编辑默认条目，方法是：在“邮件策略”(Mail Policies) >“HAT 概述”(HAT Overview) 页面上，点击 ALL 发件人组的邮件流策略。

注释 通过拒绝除指定主机之外的所有主机，`listenerconfig` 和 `systemsetup` 命令可防止意外将系统配置为“开放中继”。开放中继（有时称为“不安全中继”或“第三方”中继）是允许邮件的第三方中继的 SMTP 邮件服务器。通过处理既非发送给本地用户也不是来自本地用户的邮件，开放中继使肆无忌惮的发件人可以通过网关路由大量垃圾邮件。

将远程主机定义在发件人组中

可以定义远程主机尝试连接到侦听程序的方式。将远程主机定义分组为发件人组。发件人组是一个远程主机列表，是为了以相同方式处理这些发件人所发送的邮件而定义。

发件人组是根据以下方式识别的发件人的列表：

- IP 地址（IPv4 或 IPv6）
- IP 范围
- 特定主机或域名
- SenderBase 信誉服务“组织”分类
- SenderBase 信誉得分 (SBRS) 范围（或缺少得分）
- DNS 列表查询响应

有关发件人组中可接受地址列表的详细信息，请参阅发件人组语法，第 83 页。

当 SMTP 服务器尝试与设备建立 SMTP 连接时，侦听程序会按顺序评估发件人组，并且在符合发件人组中的任何条件（例如 SenderBase 信誉得分、域或 IP 地址）时将连接分配给发件人组。

注释 系统通过执行双重 DNS 查找来获得和验证远程主机 IP 地址的有效性。其中包括对连接主机的 IP 地址的反向 DNS (PTR) 查找，之后是对 PTR 查找结果的正向 DNS (A) 查找。然后，系统将检查 A 查找结果是否与 PTR 查找结果匹配。如果结果不匹配或 A 记录不存在，则系统将仅使用 IP 地址来匹配 HAT 中的条目。

在“邮件策略”(Mail Policies) > “HAT 概述”(HAT Overview) 页面上定义发件人组。

发件人组语法

表 *10:* 在 *HAT* 中定义远程主机：发件人组语法

语法	含义
`n:n:n:n:n:n:n:n`	IPv6 地址；不需要包括前导零。
`n:n:n:n:n:n:n:n-n:n:n:n:n:n:n:n` `n:n:n-n:n:n:n:n:n`	IPv6 地址的范围；不需要包括前导零。
`n.n.n.n`	完全（完整）IPv4 地址

`n.n.n.`
`n.n.n.`
`n.n.`
`n.n.`
`n.`
	部分 IPv4 地址

语法	含义
n.n.n.n-n. n.n.n.n-n. n.n.n-n. n.n-n. n.n-n n-n. n-n	IPv4 地址范围
yourhost.example.com	完全限定域名
.partialhost	partialhost 域中的所有内容
n/c n.n/c n.n.n/c n.n.n.n/c	IPv4 CIDR 地址块
n:n:n:n:n:n:n:n/c	IPv6 CIDR 地址块；不需要包括前导零
SBRS[n:n]SBRS[none]	SenderBase 信誉得分。有关详细信息，请参阅按 SenderBase 信誉得分定义发件人组，第 86 页。
SBO:n	SenderBase 网络所有者标识号。有关详细信息，请参阅按 SenderBase 信誉得分定义发件人组，第 86 页。
dnslist[dnsserver.domain]	DNS 列表查询。有关详细信息，请参阅通过查询 DNS 列表定义的发件人组，第 87 页。
所有	匹配 ALL 地址的特殊关键字。它仅适用于 ALL 发件人组，并且始终会包括在内（但不会列出）。

网络所有者、域和 IP 地址定义的发件人组

由于 SMTP 协议没有用于验证邮件发件人的内置方法，因此主动的批量邮件的发件人已成功利用一些手段来隐藏其身份。例如，在邮件中伪造信封发件人地址，使用伪造的 HELO 地址，或者只是循环利用不同的域名。这使得许多邮件管理员不断询问自己一个根本性的问题：“是谁在向我发送所有这些邮件？”为了回答此问题，SenderBase 信誉服务开发了一个独特的层次结构，用于根据连接主机的 IP 地址聚合基于身份的信息 - IP 地址是发件人基本上无法在邮件中伪造的一种消息。

IP 地址定义为发送邮件主机的 IP 地址。邮件安全设备支持互联网协议版本 4 (IPv4) 和版本 6 (IPv6) 地址。

域定义为使用具有指定的二级域名（例如，yahoo.com）的主机名的实体，具体根据对 IP 地址的反向 (PTR) 查询确定。

网络所有者定义为控制一个 IP 地址块的实体（通常是公司），具体根据 ARIN（美国互联网编号注册机构）和其他来源的全球注册机构的 IP 地址空间分配情况确定。

组织定义为严格控制网络所有者 IP 地址块中特定一组邮件网关的实体，具体由 SenderBase 确定。组织可以与网络所有者相同，可以是该网络所有者中的一个部门，也可以是该网络所有者的客户。

根据 HAT 设置策略

下表列出了网络所有者和组织的一些示例。

表 *11:* 网络所有者和组织示例

示例类型	网络所有者	**Organization**
网络服务运营商	Level 3 Communications	Macromedia Inc. AllOutDeals.com GreatOffers.com
邮件服务运营商	GE	GE Appliances GE Capital GE Mortgage
商业发件人	The Motley Fool	The Motley Fool

由于网络所有者在规模上可能相当大，因此邮件流策略所基于的合适实体为组织。SenderBase 信誉服务对于细化到组织级别的邮件源具有独特的了解，而设备正是利用这种了解来基于组织自动应用策略。在上面的示例中，如果用户指定了“3 级通信”(Level 3 Communications) 作为主机访问表 (HAT) 中的发件人组，则 SenderBase 将基于该网络所有者控制的各个组织实施策略。

例如，在上表中，如果用户为级别 3 输入每小时 10 个收件人的限制，则设备对于 Macromedia Inc.、Alloutdeals.com 和 Greatoffers.com 每小时最多允许 10 个收件人（对于级别 3 网络所有者，每小时总共 30 个收件人）。此方法的优点在于，如果其中一个组织开始发送垃圾邮件，则级别 3 控制的其他组织不会受到影响。将此与“The Motley Fool”网络所有者示例进行比较。如果用户将速率限制设置为每小时 10 个收件人，则 The Motley Fool 网络所有者每小时接收限于 10 个收件人发送的邮件。

邮件流监控功能是定义发件人并提供监控工具来创建有关发件人的邮件流策略决策的一种方式。要创建有关指定发件人的邮件流策略决策，需要回答以下问题：

- **该发件人控制哪些 IP 地址**？

  邮件流监控功能用于控制入站邮件处理的第一条信息便可回答该问题。答案通过查询SenderBase 信誉服务获得。SenderBase 信誉服务提供有关发件人相对规模（SenderBase 网络所有者或 SenderBase 组织）的信息。回答该问题时假设以下情况：

  - 更大的组织通常会控制更多 IP 地址，并且发送更多合法邮件。

- **根据其规模，应如何为此发件人分配总连接数**？

  - 更大的组织通常会控制更多 IP 地址，并且发送更多合法邮件。因此，应为其分配更多与设备的连接。

- 大量邮件的源通常是ISP、NSP、管理外包邮件传送的公司或主动批量邮件的源。ISP、NSP和管理外包邮件传送的公司都属于控制许多 IP 地址并且应获得更多与设备的连接的组织。主动批量邮件的发件人通常不会控制许多 IP 地址，而是通过少数 IP 地址发送大量邮件。应为其分配更少的与设备的连接。

邮件流监控功能使用其在 SenderBase 网络所有者与 SenderBase 组织之间的差异，来确定如何根据 SenderBase 中的逻辑来分配每个发件人的连接数。有关使用邮件流监控功能的详细信息，请参阅“使用邮件安全监控”一章。

按 SenderBase 信誉得分定义发件人组

设备可以查询 SenderBase 信誉服务来确定发件人的信誉得分 (SBRS)。SBRS 是根据 SenderBase 信誉服务提供的信息分配给 IP 地址、域或组织的数字值。得分范围介于 -10.0 到 +10.0 之间，如下表中所述。

表 *12: SenderBase* 信誉得分的定义

得分	含义
-10.0	很可能是垃圾邮件的来源
0	中立；或信息不足，无法提供相关建议
+10.0	很可能是可信发件人
none	没有适用于此发件人的数据（通常是垃圾邮件的来源）

使用 SBRS，可以将设备配置为基于发件人的可信度对发件人应用邮件流策略。例如，得分少于 -7.5 的所有发件人都将被拒绝。这可以通过 GUI 非常轻松地完成；请参阅创建发件人组用于邮件处理，第 92 页。但是，如果在文本文件中修改导出的 HAT，请参阅下表中介绍的用于包括 SenderBase 信誉得分的语法。

表 *13: SenderBase* 信誉得分的语法

`SBRS[ n n`	SenderBase 信誉得分。发件人是通过查询 SenderBase 信誉服务确定的，而得分在范围之间定义。
SBRS[none]	不指定 SBRS（非常新的域可能没有 SenderBase 信誉得分）。

注释 通过 GUI 添加到 HAT 的网络所有者使用语法 `SBO:n`，其中 *n* 是网络所有者在 SenderBase 信誉服务中的唯一标识号。

使用“网络”>“侦听程序”页面或 CLI 中的 `listenerconfig -> setup` 命令来查询 SenderBase 信誉服务。还可以定义在查询 SenderBase 信誉服务时设备应等待的超时值。然后，可以使用 GUI 中邮件策略页面的值或 CLI 中的 `listenerconfig -> edit -> hostaccess` 命令配置不同的策略来查询 SenderBase 信誉服务。

注释 还可以创建邮件过滤器来指定 SenderBase 信誉得分的“阈值”以进一步对系统处理的邮件执行操作。有关详细信息，请参阅反垃圾邮件和防病毒章节中的“SenderBase 信誉规则”、“绕过反垃圾邮件系统操作”和“绕过防病毒系统操作”。

通过查询 DNS 列表定义的发件人组

还可以在侦听程序的 HAT 中将发件人组定义为使查询与特定 DNS 列表服务器匹配。在连接远程客户端时将通过DNS执行该查询。查询远程列表的功能当前还以邮件过滤器规则（请参阅“使用邮件过滤器实施邮件策略”一章中的“DNS 列表规则”）的形式存在，但是，仅在完全接收邮件内容后存在。

通过该机制可以在查询DNS列表的组中配置发件人，以便相应地调整邮件流策略。例如，可以拒绝连接或限制连接域的行为。

注释 一些 DNS 列表使用变量响应（例如，“127.0.0.1”、“127.0.0.2”与“127.0.0.3”）来指示有关查询所依据的 IP 地址的各种情况。如果使用邮件过滤器 DNS 列表规则（请参阅“使用邮件过滤器实施邮件策略”一章中的“DNS 列表规则”），可以将查询的结果与不同的值进行比较。但是，为了简便起见，在 HAT 中指定要查询的 DNS 列表服务器仅支持布尔操作（即是否在列表中显示 IP 地址）

注释 在 CLI 中，请确保在查询中包含括号。在 GUI 中指定 DNS 列表查询时，不需要使用括号。在 CLI 中使用 dnslistconfig 命令测试查询，为 DNL 查询配置常规设置或刷新当前的 DNS 列表缓存。

请注意，此机制可用于识别“正常”连接以及“不良”连接。例如，对 query.bondedsender.org 的查询将匹配通过思科系统公司的Bonded Sender™计划发布了财务绑定的连接主机，以确保其邮件活动的完整性。可以修改默认的 WHITELIST 发件人组以查询 Bonded Sender 计划的 DNS 服务器（列出自愿发布绑定的合法邮件发件人），并相应地调整邮件流策略。

使用邮件流策略定义邮件发件人的访问规则

通过邮件流策略可以控制或限制 SMTP 会话期间从发件人到侦听程序的邮件流。通过在邮件流策略中定义以下类型的参数来控制 SMTP 会话：

- 连接参数，例如每个连接的最大邮件数。
- 速率限制参数，例如每小时的最大收件人数。
- 修改在 SMTP 会话期间传输的自定义 SMTP 代码和响应。
- 启用垃圾邮件检测。
- 启用病毒防护。
- 加密，例如使用 TLS 加密 SMTP 连接。

- 身份验证参数，例如使用 DKIM 验证传入邮件。

最后，邮件流策略会从远程主机对连接执行以下操作之一：

- **ACCEPT**。接受连接，并且邮件接受随后由侦听程序设置进一步限制，包括收件人访问表（仅适用于公共侦听程序）。
- **REJECT**。最初接受连接，但是尝试连接的客户端会获得 4XX 或 5XX SMTP 状态代码。系统不会接受邮件。

注释 还可以配置 AsyncOS 以在邮件收件人级别 (RCPT TO) 而不是在 SMTP 会话开始时执行此拒绝。通过此方式拒绝邮件会延迟邮件拒绝并退回邮件，以便 AsyncOS 保留更多有关已拒绝邮件的详细信息。此设置通过 CLI 的 `listenerconfig > setup` 命令配置。有关详细信息，请参阅通过使用 CLI 创建侦听程序来侦听连接请求，第 70 页。

- **TCPREFUSE**。在 TCP 级别拒绝连接。
- **RELAY**。接受连接。允许任何收件人进行接收，并且不受收件人访问表的限制。
- **CONTINUE**。忽略 HAT 中的映射，并且继续进行 HAT 处理。如果传入连接与稍后某个非 CONTINUE 条目搭配，则改为使用该条目。CONTINUE 规则用于促进在 GUI 中对 HAT 的编辑。有关详细信息，请参阅创建发件人组用于邮件处理，第 92 页。

HAT 变量语法

下表定义了一组变量，这些变量还可以与为邮件流策略定义的自定义SMTP速率限制横幅结合使用。变量名称不区分大小写。（例如 $group 与 $Group 是一样的。）

表 *14: HAT* 变量语法

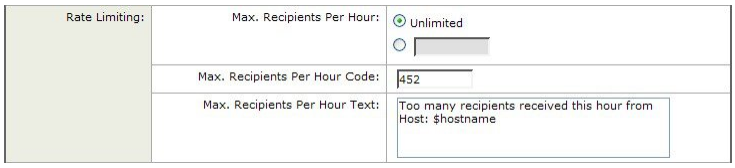
变量	定义
$Group	替换为在 HAT 中匹配的发件人组的名称。如果发件人组没有名称，则会显示“无”(None)。
$Hostname	仅在经过设备验证后，才可替换为远程主机名。如果 IP 地址的反向 DNS 查询成功，但不返回主机名，则显示“无”。如果反向 DNS 查询失败（例如，如果无法连接 DNS 服务器，或未配置 DNS 服务器），则显示“未知”(Unknown)。
$OrgID	替换为 SenderBase 组织 ID（整数值）。 如果设备无法获取 SenderBase 组织ID，或者如果 SenderBase 信誉服务没有返回值，则显示“无”(None)。
$RemoteIP	替换为远程客户端的 IP 地址。
$HATEntry	替换为远程客户端匹配的 HAT 中的条目。

使用 HAT 变量

注释 这些变量可与“配置网关以接收邮件”一章中介绍的 smtp_banner_text 和 max_rcpts_per_hour_text 高级 HAT 参数配合使用。

使用这些变量，可以在 GUI 中为 $TRUSTED 策略的已接受连接编辑自定义 SMTP 横幅响应文本。

图 *15:* 使用 *HAT* 变量



或者类似地，在 CLI 中：

```
Would you like to specify a custom SMTP response?  [Y]> y


Enter the SMTP code to use in the response. 220 is the standard code.

[220]> 200


Enter your custom SMTP response.  Press Enter on a blank line to finish.

You've connected from the hostname: $Hostname, IP address of: $RemoteIP, matched the group:
 $Group,
$HATEntry and the SenderBase Organization: $OrgID.
```

测试 HAT 变量

要测试这些变量，请将一个已知可信的计算机的 IP 地址添加身上侦听程序的 $WHITELIST 发件人组。然后，从该计算机通过 Telnet 进行连接。可以在 SMTP 响应中看到变量替换。例如：

```
# telnet
IP_address_of_Email_Security_Appliance port

220 hostname
 ESMTP

200 You've connected from the hostname: hostname
, IP address of: IP-address_of_connecting_machine
, matched the group: WHITELIST, 10.1.1.1 the SenderBase Organization: OrgID
.
```

了解预定义发件人组和邮件流策略

下表列出了在创建公共侦听程序时配置的预定义发件人组和邮件流策略。

表 *15:* 公共侦听程序的预定义发件人组和邮件流策略

预定义发件人组	说明	默认配置的邮件流策略
WHITELIST	将您信任的发件人添加到白名单发件人组。配置 $TRUSTED 邮件流策略，以便来自信任的发件人的邮件没有启用任何速率限制，并且来自这些发件人的内容不会被反垃圾邮件或防病毒软件进行扫描。	$TRUSTED
BLACKLIST	Blacklist 发件人组中的发件人被拒绝（通过在 $BLOCKED 邮件流策略中设置的参数）。将发件人添加到此组会通过在 SMTP HELO 命令中返回 5XX SMTP 响应来拒绝从这些主机进行的连接。	$BLOCKED
SUSPECTLIST	Suspectlist 发件人组中包含可限制或降低传入邮件速率的邮件流策略。如果发件人可疑，可以将其添加到 Suspectlist 发件人组，其中的邮件流策略指明： • 速率限制会限制每个会话的最大邮件数量、每封邮件的最大收件人数量、最大邮件大小和愿意从远程主机接受的最大并发连接数量。 • 来自远程主机的每小时最大收件人数设置为每小时 20 个收件人。请注意，此设置为可用的最大限制。如果此参数过于严格，可以提高每小时接收的收件人数。 • 邮件内容将由反垃圾邮件扫描引擎和防病毒扫描引擎进行扫描（如果已为系统启用这些功能）。 • 系统将查询 SenderBase 信誉服务以获取有关发件人的详细信息。	$THROTTLED

预定义发件人组	说明	默认配置的邮件流策略
UNKNOWNLIST	如果不确定要用于指定发件人的邮件流策略，则Unknownlist发件人组可能非常有用。此组的邮件流策略指明邮件已由此组中的发件人接受，但是反垃圾邮件软件（如果已为系统启用）、防病毒扫描引擎和SenderBase信誉服务都应当用于获取有关发件人和邮件内容的详细信息。此外，还启用了此组中的发件人速率限制，并且采用默认值。有关病毒扫描引擎的详细信息，请参阅病毒扫描，第 255 页。有关SenderBase信誉服务方面的详细信息，请参阅SenderBase信誉服务，第 75 页。	$ACCEPTED
所有	适用于其他所有发件人的默认发件人组。有关详细信息，请参阅默认 HAT 条目，第 82 页。	$ACCEPTED

下表列出了在创建专用侦听程序时配置的预定义发件人组和邮件流策略。

表 *16:* 专用侦听程序的预定义发件人组和邮件流策略

预定义发件人组	说明	默认配置的邮件流策略
RELAYLIST	将您知道应当允许转发的发件人添加到Relaylist发件人组。配置$RELAYED邮件流策略，以便来自允许转发的发件人的邮件没有任何速率限制，并且来自这些发件人的内容不会被反垃圾邮件或防病毒软件进行扫描。 **注释** RELAYLIST发件人组包括在运行“系统设置向导”(System Setup Wizard)时允许转发邮件的系统。	$RELAYED
所有	适用于其他所有发件人的默认发件人组。有关详细信息，请参阅默认 HAT 条目，第 82 页。	$BLOCKED

注释 在仅有两个以太网端口的设备型号上运行“系统设置向导”(System Setup Wizard)时，系统会提示您仅创建一个侦听程序。它会创建一个公共侦听程序，其中包含一个还可用于为内部系统转发邮件的$RELAYED邮件流策略。对于具有两个以上以太网端口的设备型号，RELAYLIST发件人组和$RELAYED邮件流策略只会显示在专用侦听程序中。

以相同方式处理来自一个发件人组的邮件

使用“邮件策略”(Mail Policies)>“HAT 概述”(HAT Overview) 和“邮件流策略”(Mail Flow Policy) 页面配置侦听程序处理来自发件人的邮件的方式。通过创建、编辑和删除发件人组和邮件流策略可实现此目的。

创建发件人组用于邮件处理

步骤 1 导航到**邮件策略 (Mail Policies) > HAT 概述 (HAT Overview)** 页面。

步骤 2 在“侦听程序”(Listeners) 字段中选择要编辑的侦听程序。

步骤 3 点击**添加发件人组 (Add Sender Group)**。

步骤 4 键入发件人组的名称。

步骤 5 选择将其放置在发件人组列表中的顺序。

步骤 6 （可选）输入注释，例如有关此发件人组或其设置的信息。

步骤 7 选择将此发件人组应用到的邮件流策略。

注释 如果不知道要应用到此组的邮件流策略（或如果邮件流策略不存在），则使用默认的“CONTINUE（无策略）”邮件流策略。

步骤 8 （可选）选择一个 DNS 列表。

步骤 9 （可选）包括 SBRS 没有其相关信息的发件人。这以“无”(None) 指示，并且通常表示可疑。

步骤 10 （可选）输入一个 DNS 列表。

步骤 11 （可选）配置主机 DNS 验证设置。

有关详细信息，请参阅对未经验证的发件人实施更严格的限制设置，第 106 页。

步骤 12 点击**提交**以创建发件人组。

步骤 13 点击新创建的发件人组。

步骤 14 点击**添加发件人**将发件人添加到发件人组中。

- **添加发件人 IP 地址**。选择 **IP 地址**，添加 IPv4 地址、IPv6 地址或主机名，然后提交更改。

  发件人可以包括一系列 IP 地址和部分主机名。

- **添加发件人的来源国家/地区**。选择**地理位置**，选择国家/地区，然后提交更改。

步骤 15 提交并确认更改。

将发件人添加到现有发件人组

步骤 1 从域、IP 或网络所有者配置文件页面中，点击“添加到发件人组”(Add to Sender Group) 链接。

步骤 2 从为每个侦听程序定义的列表中选择发件人组。

步骤 3 提交并确认更改。

注释 将域添加到发件人组时，GUI 中会列出两个实际域。例如，但是如果在“添加到发件人组”页面上添加域 `example.net`，则会添加 `example.net` 和 `.example.net`。第二个条目可确保 `example.net` 子域中的任何主机都将添加到发件人组。有关详细信息，请参阅发件人组语法，第 83 页。

如果要添加到发件人组的一个或多个发件人是已存在于该发件人组中的发件人的重复项，则不会添加重复的发件人，并且您将看到确认邮件。

步骤 4 点击**保存 (Save)** 添加发件人并返回到“传入邮件概述”(Incoming Mail Overview) 页面。

重新排列对传入连接所执行规则的顺序

如果将一个发件人组添加到侦听程序，则可能需要编辑该发件人组的顺序。

每个尝试连接侦听程序的主机都会从上到下读取 HAT。如果某个规则与连接主机匹配，则系统会立即对该连接执行操作。

步骤 1 导航到**邮件策略 (Mail Policies) > HAT 概述 (HAT Overview)** 页面。

步骤 2 在“侦听程序”(Listeners) 字段中选择要编辑的侦听程序。

步骤 3 点击**编辑顺序 (Edit Order)**。

步骤 4 键入发件人组的现有行在 HAT 中的新顺序。

思科建议保持默认顺序：RELAYLIST（仅限特定硬件型号），其次是 WHITELIST、BLACKLIST、SUSPECTLIST 和 UNKNOWNLIST。

步骤 5 提交并确认更改。

搜索发件人

可以通过在“HAT 概述”页面顶部的“查询发件人”字段中输入文本来查询发件人。输入要用于搜索的文本，然后点击“查询”(Find)。

使用邮件流策略定义传入邮件规则

在创建邮件流策略之前请考虑以下规则和指导原则：

- “使用默认值”(Use Default) 单选按钮处于选中状态时，策略的默认值将“灰显”。要覆盖默认值，请通过选择“打开”(On) 单选按钮并对当前可访问的值进行更改以启用该功能或设置。要定义默认值，请参阅定义邮件流策略的默认值，第 99 页。
- 有些参数取决于特定的预配置。（例如，目录搜集攻击预防设置要求已配置LDAP接受查询。）

步骤 1 依次导航到**邮件策略 (Mail Policies) > 邮件流策略 (Mail Flow Policies)** 页面。

步骤 2 点击**添加策略**。

步骤 3 输入下表中描述的信息。

表 *17:* 邮件流策略参数

参数	说明
连接	
最大邮件大小	该侦听程序将接受的最大邮件的大小。最小的最大邮件大小为 1 KB。
来自单个 IP 的最大并发连接数	允许从一个 IP 地址连接到此侦听程序的最大并发连接数。
每个连接的最大邮件数	每个连接可以通过此侦听程序从远程主机发送的最大邮件数。
每封邮件的最大收件人数	将从此主机接受的每封邮件的最大收件人数。
SMTP 标语	
自定义 SMTP 标语代码	当与此侦听程序建立连接时，返回的 SMTP 代码。
自定义 SMTP 标语文本	当与此侦听程序建立连接时，返回的 SMTP 标语文本。 **注释** 可以在此字段中输入一些变量。有关详细信息，请参阅HAT 变量语法，第 88 页。
自定义 SMTP 拒绝标语代码	当此侦听程序拒绝连接时，返回的 SMTP 代码。
自定义 SMTP 拒绝标语文本	当此侦听程序拒绝连接时，返回的 SMTP 横幅文本。
覆盖 SMTP 横幅主机名	默认情况下，当为远程主机显示 SMTP 横幅时，设备将包括与侦听程序的接口关联的主机名（例如，220- *hostname* ESMTP）。可以选择通过在此处输入其他主机名来覆盖此标语。此外，可以将主机名字段留空以选择不在标语中显示主机名。
主机的速率限制	

参数	说明
每小时最大收件人数	此侦听程序每小时将从远程主机接收的最大收件人数。系统会全局跟踪每个发件人 IP 地址的收件人数。每个侦听程序会跟踪自己的速率限制阈值；但是，由于所有侦听程序都根据单个计数器进行验证，因此当同一 IP 地址（发件人）连接到多个侦听程序时，更有可能超过速率限制。 **注释** 可以在此字段中输入一些变量。有关详细信息，请参阅HAT 变量语法，第 88 页。
每小时最大收件人数的代码	当主机超过为此侦听程序定义的每小时最大收件人数时，返回的 SMTP 代码。
超过每小时最大收件人数的文本	当主机超过为此侦听程序定义的每小时最大收件人数时，返回的 SMTP 横幅文本。
发件人的速率限制	
每个时间间隔的最大收件人数	在指定的时段内，此侦听程序根据邮件发件人地址从唯一信封发件人收到的最大收件人数。系统不会全局跟踪收件人数。每个侦听程序会跟踪自己的速率限制阈值；但是，由于所有侦听程序都根据单个计数器进行验证，因此当多个侦听程序收到来自同一邮件发件人地址的邮件时，更有可能超过速率限制。 选择是使用默认最大收件人，接受无限的收件人，还是指定另一个最大收件人数。 使用“默认邮件流策略”(Default Mail Flow Policy) 设置指定最大收件人数，以及默认情况下由其他邮件流策略使用的时间间隔。时间间隔仅可以使用“默认邮件流策略”(Default Mail Flow Policy) 指定。
超过发件人速率限制的错误代码	当信封超过为此侦听程序定义的时间间隔的最大收件人数时，返回的 SMTP 代码。
超过发件人速率限制的错误文本	当信封发件人超过为此侦听程序定义的时间间隔的最大收件人数时，返回的 SMTP 标语文本。
例外	如果希望从定义的速率限制中免除某些信封发件人，请选择包含信封发件人的地址列表。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，第 100 页。
流量控制	
使用 SenderBase 控制流量	为此侦听程序启用对 SenderBase 信誉服务的“查询”。
按 IP 地址的相似性分组：（有效位 0-32）	用于根据 IP 地址跟踪传入邮件并限制其速率，同时在大型 CIDR 块中管理侦听程序的主机访问表 (HAT) 中的条目。定义一个重要位数范围（从 0 到 32）以根据其对相似 IP 地址进行分组来限制速率，同时仍为该范围内的每个 IP 地址维护各个计数器。要求禁用“使用 SenderBase”(Use SenderBase)。有关 HAT 重要位数的详细信息，请参阅配置路由和传送功能，第 523 页。
目录搜集攻击预防 (DHAP)	

参数	说明
目录搜集攻击预防：每小时的最大无效收件人数	此侦听程序每小时将从远程主机接收的最大无效收件人数。此阈值表示 RAT 拒绝和 SMTP Call-Ahead 服务器拒绝总数与在 SMTP 会话中删除或在工作队列中退回的无效 LDAP 收件人邮件的总数相结合的结果（在关联侦听程序中的 LDAP 接受设置中定义）。有关为 LDAP 接受查询配置 DHAP 的详细信息，请参阅处理 LDAP 查询，第 594 页。
目录搜集攻击预防：如果在 SMTP 会话中达到 DHAP 阈值，则放弃连接。	如果达到无效收件人阈值，则设备会放弃与主机的连接。
每小时的最大无效收件人数量代码:	指定在放弃连接时使用的代码。默认代码为 550。
每小时的最大无效收件人数量文本:	指定用于放弃的连接的文本。默认文本为“无效收件人过多”(Too many invalid recipients)。
如果在 SMTP 会话中达到 DHAP 阈值，则放弃连接	启用该项可在 SMTP 会话中达到 DHAP 阈值时放弃连接。
每小时的最大无效收件人数量代码	指定由于 SMTP 会话中的 DHAP 而放弃连接时要使用的代码。默认代码为 550。
每小时的最大无效收件人数量文本:	指定由于 SMTP 会话中的 DHAP 而放弃连接时要使用的文本。
垃圾邮件扫描	
反垃圾邮件扫描	在此侦听程序中启用反垃圾邮件扫描。
病毒检测	
防病毒扫描	在此侦听程序中启用防病毒扫描。
加密和身份验证	

参数	说明
TLS	在此侦听程序的 SMTP 会话中拒绝、首选或要求传输层安全 (TLS)。 如果选择“首选”(Preferred)，可以通过选择地址列表来指定相关域和邮件地址，从而要求来自特定域或具有特定邮件地址的信封发件人必须使用 TLS。当与该列表中的域或地址匹配的信封发件人尝试通过不使用 TLS 的连接发送邮件时，设备会拒绝连接，并且发件人必须使用 TLS 重试。 如果客户端证书有效，“验证客户端证书”(Verify Client Certificate) 选项会指导邮件安全设备与用户邮件应用程序建立 TLS 连接。如果您为“首选 TLS”(TLS Preferred) 设置选择此选项，当用户没有证书时，设备仍允许非 TLS 连接；但在用户具有的证书无效时，将拒绝连接。对于“需要 TLS”(TLS Required) 设置，选择此选项将要求用户具备有效证书，设备才能允许连接。 有关创建地址列表的信息，请参阅为传入连接规则使用发件人地址列表，第 100 页。 有关将客户端证书用于 TLS 连接的信息，请参阅从设备建立 TLS 连接，第 632 页。
SMTP 身份验证	从远程主机连接到侦听程序时允许、禁止或需要 SMTP 身份验证。在“LDAP 查询”一章中详细介绍了 SMTP 身份验证。
如果 TLS 和 SMTP 身份验证同时启用:	需要 TLS 以提供 SMTP 身份验证
域密钥/DKIM 签名	对此侦听程序启用域密钥或 DKIM 签名（仅限 ACCEPT 和 RELAY）。
DKIM 验证	启用 DKIM 验证。
S/MIME 解密和验证	
S/MIME 解密/验证	• 启用 S/MIME 解密或验证。 • 选择在 S/MIME 验证后是保留还是删除邮件中的数字签名。对于三重封装的邮件，仅保留或删除内部签名。
S/MIME 公钥搜集	
S/MIME 公钥搜集	启用 S/MIME 公钥搜集。
在验证失败时搜集证书	如果传入签名邮件的验证失败，则选择是否搜集公钥。
存储更新的证书	选择是否搜集更新的公钥。
SPF/SIDF 验证	
启用 SPF/SIDF 验证	对此侦听程序启用 SPF/SIDF 签名。有关详细信息，请参阅电邮验证，第 445 页。
一致性级别	设置 SPF/SIDF 一致性级别。可以选择 SPF、SIDF 或 SIDF 兼容。有关详细信息，请参阅电邮验证，第 445 页。

参数	说明
如果使用了“Resent-Sender:”或“Resent-From:”，则降级 PRA 验证结果:	如果选择 SIDF 兼容一致性级别，请配置当邮件中存在“Resent-Sender:”或“Resent-From:”信头时，是否要将 PRA 身份验证的通过结果降级为“无”(None)。为了安全起见，可以选择此选项。
HELO 测试	配置是否要对 HELO 身份执行测试（将此选项用于 SPF 和 SIDF 兼容一致性级别）。
DMARC 验证	
启用 DMARC 验证	对此侦听程序启用 DMARC 验证。有关详细信息，请参阅DMARC 验证，第 471 页。
使用 DMARC 验证配置文件	选择要对此侦听程序使用的 DMARC 验证配置文件。
DMARC 反馈报告	启用发送 DMARC 汇聚反馈报告的功能。 有关 DMARC 汇聚反馈报告的详细信息，请参阅DMARC 汇聚报告，第 477 页。 **注释** DMARC规范要求反馈报告邮件符合DMARC标准。请确保这些邮件经过DKIM签名，或必须发布适当的 SPF 记录。
无标记的退回	
将无标记的退回视为有效	仅当启用了退回验证标记功能（在“配置路由和传输功能”一章中进行了介绍）时应用。默认情况下，设备将无标记的退回使用无效并拒绝退回或添加自定义信头，具体取决于“退回验证”(Bounce Verification) 设置。如果选择将无标记的退回视为有效，则设备会接受退回邮件。
信封发件人 DNS 验证	
	请参阅验证发件人，第 102 页。
例外表	
使用例外表	使用发件人验证域例外表。只能有一个例外表，但是可以按邮件流策略来启用它。有关详细信息，请参阅发件人验证例外表，第 105 页。

注释 如果在 HAT 中全局启用了反垃圾邮件扫描或防病毒扫描，则设备接受邮件时会将它们标记为进行反垃圾邮件扫描或防病毒扫描。如果在接受邮件后禁用反垃圾邮件扫描或防病毒扫描，则邮件离开工作队列时仍会进行扫描。

步骤 4 提交并确认更改。

定义邮件流策略的默认值

步骤 1 依次点击**邮件策略 (Mail Policies) > 邮件流策略 (Mail Flow Policies)**。

步骤 2 在“侦听程序”(Listeners) 字段中选择要编辑的侦听程序。

步骤 3 点击配置的邮件流策略下方的**默认策略参数 (Default Policy Parameters)** 链接。

步骤 4 定义此侦听程序使用的所有邮件流策略的默认值。

有关属性的详细信息，请参阅使用邮件流策略定义传入邮件规则，第 93 页。

步骤 5 提交并确认更改。

使用主机访问表配置

可以将主机访问表中存储的所有信息导出到文件，而且可以将文件中存储的主机访问表信息导入到侦听程序，从而覆盖所有现有主机访问表信息。

将主机访问表配置导出到外部文件

步骤 1 导航到“邮件策略”(Mail Policies) >“HAT 概述”(HAT Overview) 页面。

步骤 2 在“侦听程序”(Listener) 菜单中选择要编辑的侦听程序。

步骤 3 点击**导出 HAT (Export HAT)**。

步骤 4 为导出的 HAT 输入文件名。这是在设备的配置目录中创建的文件的名称。

步骤 5 提交并确认更改。

从外部文件导入主机访问表配置

当导入 HAT 时，将从当前 HAT 中删除所有现有 HAT 条目。

步骤 1 导航到“邮件策略”(Mail Policies) >“HAT 概述”(HAT Overview) 页面。

步骤 2 在“侦听程序”(Listener) 菜单中选择要编辑的侦听程序。

步骤 3 点击**导入 HAT (Import HAT)**。

步骤 4 从列表中选择文件。

注释 要导入的文件必须在设备的配置目录中。

步骤 5 点击 **Submit**。系统将显示一条警告消息，要求确认要删除现有的所有 HAT 条目。

步骤 6 点击 **Import**。

步骤 7 确认您的更改。

可以在文件中放置“注释”。以“#”字符开头的行被视为注释，AsyncOS 会忽略注释。例如：

```
# File exported by the GUI at 20060530T215438
$BLOCKED
    REJECT {}
[ ... ]
```

为传入连接规则使用发件人地址列表

通过邮件流策略可以将一个地址列表用于针对一组信封发件人的特定设置，例如速率限制例外和必需 TLS 连接。地址列表可以包含邮件地址、域、部分域和 IP 地址。可以使用 GUI 中的**邮件策略 (Mail Policies) > 地址列表 (Address Lists)** 页面或 CLI 中的 `addresslistconfig` 命令创建地址列表。“地址列表”(Address Lists) 页面会显示设备中的所有地址列表，以及使用地址列表的任何邮件流策略。

步骤 1 依次选择**邮件策略 (Mail Policies) > 地址列表 (Address Lists)**。

步骤 2 点击**添加地址列表 (Add Address List)**。

步骤 3 输入地址列表的名称。

步骤 4 输入地址列表的说明。

步骤 5 （可选）要强制在地址列表中使用完整邮件地址，请选择**仅允许完整的邮件地址 (Allow only full Email Addresses)**。

步骤 6 输入要包括的地址。您可以使用以下格式：

- 完整的邮件地址：`user@example.com`
- 不完整邮件地址：`user@`

  注释 如果选择了**仅允许完整的邮件地址 (Allow only full Email Addresses)**，则不能使用不完整邮件地址。

- 其邮件地址中的 IP 地址：`@[1.2.3.4]`
- 域中的所有用户：`@example.com`
- 不完整域中的所有用户：`@.example.com`

请注意，域和 IP 地址必须以字符 `@` 开头。

以逗号分隔多个邮件地址。如果使用新行分隔地址，AsyncOS 会自动将条目转换为逗号分隔列表。

步骤 7 提交并确认更改。

SenderBase 设置和邮件流策略

为了分类与设备的连接并应用邮件流策略（可能包含或不包含速率限制），侦听程序会使用以下方法：

分类 (Classification) -> 发件人组 (Sender Group) -> 邮件流策略 (Mail Flow Policy) -> 速率限制 (Rate Limiting)

有关详细信息，请参阅网络所有者、域和 IP 地址定义的发件人组 ，第 84 页。

“分类”阶段使用发送主机的 IP 地址将入站 SMTP 会话（在公共侦听程序中接收）分类在发件人组中。与该发件人组关联的邮件流策略可能已启用速率限制的参数。（速率限制会限制每个会话的最大邮件数量、每封邮件的最大收件人数量、最大邮件大小和/或愿意从远程主机接受的最大并发连接数量。）

通常在此流程中，将根据相应的指定发件人组中的每个发件人来计数收件人。如果在同一时间收到来自多个发件人的邮件，则会将所有发件人的总收件人数与限制进行比较。

此计数方法存在一些例外情况：

- 如果分类由网络所有者执行，则 SenderBase 信誉服务会自动将大型地址块分为更小的块。

对收件人和收件人速率限制的计数针对这些较小的块（通常相当于 1/24 的 CIDR 块，但不总是如此）单独进行。

- 如果使用了 HAT 重要位数功能。在这种情况下，通过应用与策略关联的重要位数参数将大型地址块分为较小的块。

请注意，此参数与**邮件流策略 (Mail Flow Policy) -> 速率限制 (Rate Limiting)** 阶段相关。这不同于“网络/位数”CIDR 记法（可用于分类发件人组中的 IP 地址）中的“位数”字段。

默认情况下，SenderBase 信誉服务和 IP 配置支持对于公共侦听程序已启用，而对于专用侦听程序则已禁用。

SenderBase 查询的超时

当配置侦听程序时，可以确定设备将从 SenderBase 信誉服务查询的信息缓存多长时间。然后，在配置邮件流策略时，可以启用 SenderBase 以允许它控制进入侦听程序的邮件流。

在配置邮件流策略时，在 GUI 中使用“使用 SenderBase 控制流量”设置，或者在 CLI 中使用 `listenerconfig > hostaccess > edit` 命令，从而在邮件流策略中启用 SenderBase。

HAT 有效位功能

从 AsyncOS 3.8.3 版开始，可以根据 IP 地址跟踪传入邮件并限制其速率，同时在大型 CIDR 块中管理侦听程序的主机访问表 (HAT) 中的发件人组条目。例如，如果传入连接根据主机“10.1.1.0/24”匹配，则仍可为该范围内的各个地址生成计数器，而不是将所有流量汇聚到一个大型计数器中。

注释 为了使重要位数 HAT 策略选项生效，不能在 HAT 的流量控制选项中启用“用户 SenderBase”（或对于 CLI，在 `listenerconfig -> setup` 命令中对于启用 SenderBase 信息服务的以下问题回答 **no**：“Would you like to enable SenderBase Reputation Filters and IP Profiling support?”）。这就是说，HAT 重要位数功能与启用 SenderBase IP 配置支持是互相排斥的。

在许多情况下，可以使用此功能来广泛定义发件人组（即，大型 IP 地址组，例如“10.1.1.0/24”或“10.1.0.0/16”），同时将邮件流策略限制有限地应用于较小的 IP 地址组。

HAT 重要位数功能对应于系统中的以下组件：

HAT 配置

HAT 配置有两个部分：发件人组和邮件流策略。发件人组配置定义发件人的 IP 地址如何“分类”（放置在发件人组中）。邮件流策略配置定义如何控制来自该 IP 地址的 SMTP 会话。在使用此功能时，IP 地址可以“分类在 CIDR 块”（例如 10.1.1.0/24）发件人组中，同时作为单独的主机 (/32) 进行控制。可以通过“signficant_bits”策略配置设置实现此目的。

有效位元 HAT 策略选项

HAT 语法适用于 signficant_bits 配置选项。该功能显示在 GUI 的“邮件策略”>“邮件流策略”页面中。

将 SenderBase 用于流量控制选项设置为“关闭”(OFF) 或目录搜集攻击预防已启用时，“重要位数”值将应用于连接发件人的 IP 地址，并且产生的 CIDR 记法用作令牌以匹配在 HAT 中定义的发件人组。在构造字符串时，CIDR 块涵盖的任何最右侧的位数都“清零”。因此，从 IP 地址 1.2.3.4 建立连接并且根据 significant_bits 选项设置为 24 的策略进行匹配时，生成的 CIDR 块将为 1.2.3.0/24。因此通过使用此功能，HAT 发件人组条目（例如，10.1.1.0/24）可以具有与分配给该组的策略中的重要位数条目（在本示例中为 32）不同的网络重要位数 (24)。

有关 `listenerconfig` 命令的详细信息，请参阅《适用于思科邮件安全设备的 AsyncOS CLI 参考指南》。

注入控制周期性

存在全局配置选项，可用来调整何时重置注入控制计数器。对于为大量不同的 IP 地址保留计数器的非常繁忙的系统，将计数器配置为更频繁地重置（例如，每 15 分钟而不是每 60 分钟）可以确保数据不会增长到一个无法管理的规模并影响系统性能。

当前的默认值为 3600 秒（1 小时）。可以指定其他周期，从短至 1 分钟（60 秒）到长至 4 小时（14,400 秒）均可。

通过 GUI 使用全局设置调整此周期（有关详细信息，请参阅配置侦听程序的全局设置，第 64 页）。

还可以在 CLI 中使用 `listenerconfig -> setup` 命令设置调整此周期。有关 `listenerconfig` 命令的详细信息，请参阅《适用于思科邮件安全设备的 AsyncOS 的 CLI 参考指南》。

验证发件人

通常，垃圾邮件和不需要的邮件来自其域或 IP 地址无法由 DNS 解析的发件人。DNS 验证意味着可以获取有关发件人的可靠信息并相应地处理邮件。SMTP 会话前的发件人验证（根据发件人 IP 地址的 DNS 查询的连接过滤）还可帮助减少通过设备上邮件管道处理的垃圾邮件量。

来自未经验证发件人的邮件不会被自动丢弃。相反， AsyncOS 提供发件人验证设置，以便确定设备如何处理来自未经验证的发件人的邮件：例如，可将设备配置为在 SMTP 会话之前自动阻止来自未经验证的发件人的邮件，或限制未经验证的发件人。

发件人验证功能包含以下组件：

- **连接主机的验证**。这在 SMTP 会话之前发生。有关详细信息，请参阅发件人验证：主机 ，第 103 页。
- **信封发件人的域部分的验证**。这在 SMTP 会话期间发生。有关详细信息，请参阅发件人验证：信封发件人 ，第 103 页。

发件人验证：主机

发件人可能因多种原因而未经验证。例如，DNS 服务器可能“已关闭”或不响应，或者域不存在。发件人组的主机 DNS 验证设置允许在 SMTP 会话之前对未验证的发件人进行分类，并将不同类型的未验证发件人包含在各种发件人组中。

设备尝试通过传入邮件的 DNS 验证连接主机的发送域。此验证在 SMTP 会话之前执行。系统通过执行双重 *DNS* 查找，获取和验证远程主机 IP 地址（即域）的有效性。双重 DNS 查找定义为：对连接主机的 IP 地址的反向 DNS (PTR) 查找，之后是对 PTR 查找结果的正向 DNS (A) 查找。然后，设备将检查 A 查找结果是否与 PTR 查找结果匹配。如果 PTR 或 A 查找失败，或者结果不匹配，则系统仅使用 IP 地址来匹配 HAT 中的条目，并且发件人被视为未经验证。

未经验证的发件人分为以下类别：

- 连接主机 PTR 记录在 DNS 中不存在。
- 连接主机PTR记录检查由于临时DNS故障而失败。
- 连接主机反向 DNS 查询 (PTR) 不匹配正向 DNS 查询 (A)。

使用发件人组“连接主机 DNS 验证”设置，可以为未经验证的发件人指定行为（请参阅使用 SUSPECTLIST 发件人组限制来自未经验证的发件人的邮件 ，第 106 页）。

可以在任何发件人组的发件人组设置中启用主机DNS验证；但是，请记住向发件人组添加主机DNS验证设置意味着在该组中包括未经验证的发件人。这意味着将包括垃圾邮件和其他不需要的邮件。因此，仅应在用于拒绝或限制发件人的发件人组中启用这些设置。例如，在 WHITELIST 发件人组中启用主机 DNS 验证意味着来自未经验证的发件人的邮件将获得与来自 WHITELIST 中可信发件人的邮件相同的处理（包括绕开反垃圾邮件/防病毒检查、速率限制等，具体取决于邮件流策略的配置）。

发件人验证：信封发件人

通过信封发件人验证，信封发件人的域部分会经过DNS验证。（信封发件人域是否可解析？在信封发件人域的 DNS 中是否有 A 或 MX 记录？）如果尝试在 DNS 中查找域时遇到临时错误条件，例如超时或DNS服务器故障，则无法解析域。另一方面，如果尝试查询域时返回明确的“域不存在”状态，则域不存在。此验证在 SMTP 会话期间发生，而主机 DNS 验证在会话开始之前发生 - 它适用于连接 SMTP 服务器的 IP 地址。

更加详细：AsyncOS 对发件人地址的域执行 MX 记录查询。然后，AsyncOS 根据 MX 记录查询的结果执行 A 记录查询。如果 DNS 服务器返回“NXDOMAIN”（此域没有记录），AsyncOS 会将该域视为不存在。这将属于“其域不存在的信封发件人”类别。NXDOMAIN 可能意味着根名称服务器没有为此域提供任何授权名称服务器。

但是，如果DNS服务器返回“SERVFAIL”，则其归类为“其域无法解析的信封发件人”。SERVFAIL 意味着域存在，但 DNS 在查询记录方面存在临时问题。

垃圾邮件发送者或邮件的其他非法发件人的常用技术是伪造MAIL FROM信息（在信封发件人中），以便来自接受的未经验证的发件人的邮件将得到处理。这可能会导致问题，因为发送至MAIL FROM地址的退回邮件无法发送。使用信封发件人验证，可将设备配置为拒绝MAIL FROM格式不正确（但不为空）的邮件。

对于每个邮件流策略，可以：

- 启用信封发件人 DNS 验证。
- 为格式不正确的信封发件人提供自定义SMTP代码和响应。如果启用了信封发件人DNS验证，则格式不正确的信封发件人会被阻止。
- 为无法解析的信封发件人域提供自定义响应。
- 为 DNS 中不存在的信封发件人域提供自定义响应。

可以使用发件人验证例外表存储将自动允许或拒绝其邮件的域或地址的列表（请参阅发件人验证例外表，第 105 页）。可以独立于信封发件人验证启用发件人验证例外表。因此，例如，在不启用信封发件人验证的情况下仍可拒绝在例外表中指定的特殊地址或域。还可以始终允许来自内部域或测试域的邮件，即使这些域不会进行验证也是如此。

虽然大部分垃圾邮件来自无法验证的发件人，但是您可能因某些原因希望接受来自未经验证的发件人的邮件。例如，并非所有合法的邮件都可以通过 DNS 查找进行验证 - 临时 DNS 服务器问题可能会阻止对发件人进行验证。

当尝试接收来自未经验证的发件人的邮件时，在 SMTP 会话期间将使用发件人验证例外表和邮件流策略信封发件人 DNS 验证设置对信封发件人分类。例如，可以接受和限制来自由于在 DNS 中不存在而未验证的发送域的邮件。接受该邮件后，将使用可自定义的SMTP代码和响应拒绝MAIL FROM格式不正确的邮件。这在 SMTP 会话期间发生。

可以通过 GUI 或 CLI (`listenerconfig -> edit -> hostaccess -> < policy >`) 在邮件流策略设置中为任何邮件流策略启用信封发件人 DNS 验证（包括域例外表）。

部分域、默认域和格式不正确的 MAIL FROM

如果启用信封发件人验证或在侦听程序的 SMTP 地址解析选项中禁止允许部分域（请参阅“配置网关以接收邮件”一章中的 SMTP 地址解析选项部分），则该侦听程序的默认域设置将不再使用。

这些功能互相排斥。

自定义 SMTP 代码和响应

可以为信封发件人格式不正确的邮件、在 DNS 中不存在的信封发件人以及无法通过 DNS 查询解析（DNS 服务器可能已关闭等）的信封发件人指定 SMTP 代码和响应邮件。

在SMTP响应中可以包含一个变量 `$EnvelopeSender`，在发送自定义响应时，该变量扩展为信封发件人的值。

尽管通常“域不存在”结果是永久的，它也可能是一种临时情况。要处理此类情况，“保守的”用户可能希望将错误代码从默认值 5XX 更改为 4XX 代码。

发件人验证例外表

发件人验证例外表是在 SMTP 会话期间将自动被允许或拒绝的域或邮件地址的列表。还可以为拒绝的域指定可选的 SMTP 代码和拒绝响应。每台设备只能有一个发件人验证例外表，并且它会根据邮件流策略启用。

发件人验证例外表可以用于列出要拒绝其邮件的明显伪造但是格式正确的域或邮件地址。例如，格式正确的MAIL FROM `pres@whitehouse.gov` 可以在发件人验证例外表中列出，并且自动被拒绝。还可以列出要自动允许的域，如内部域或测试域。这类似于在收件人访问表 (RAT) 中进行的信封收件人（SMTP RCPT TO 命令）处理。

发件人验证例外表在 GUI 中通过“邮件策略”>“例外表”页面（或在 CLI 中通过 `exceptionconfig` 命令）定义，然后通过GUI（请参阅定义邮件以使用 ACCEPTED 邮件流策略发送到未经验证的发件人，第 107 页）或 CLI（请参阅《适用于思科邮件安全设备的 *AsyncOS CLI* 参考指南》）以逐个策略为基础启用。

发件人验证例外表中的条目具有以下语法：

有关修改例外表的详细信息，请参阅根据发件人的邮件地址从发件人验证规则中排除未经验证的发件人，第 107 页。

实施发件人验证 - 设置示例

本节提供保守实施主机和信封发件人验证的典型示例。

对于此示例，当实施主机发件人验证时，来自反向DNS查询与其不匹配的连接主机的邮件将通过现有 SUSPECTLIST 发件人组和 THROTTLED 邮件流策略进行限制。

将创建新的发件人组 (UNVERIFIED) 和新的邮件流策略 (THROTTLEMORE)。来自未验证的连接主机的邮件将在 SMTP 会话之前被限制（使用 UNVERIFIED 发件人组和更严格的 THROTTLEMORE 邮件流策略）。

为 ACCEPTED 邮件流策略启用了信封发件人验证。

下表显示为实施发件人验证而建议的设置：

表 *18:* 发件人验证：建议的设置

发件人组	策略	包含
未验证 SUSPECTLIST	THROTTLEMORE THROTTLED	在 SMTP 会话之前： 连接主机 PTR 记录在 DNS 中不存在。 连接主机反向 DNS 查询 (PTR) 不匹配正向 DNS 查询 (A)。

发件人组	策略	包含
	ACCEPTED	SMTP 会话期间的信封发件人验证： - 格式不正确的 MAIL FROM： - 信封发件人在 DNS 中不存在。 - 信封发件人 DNS 无法解析。

使用 SUSPECTLIST 发件人组限制来自未经验证的发件人的邮件

步骤 1 依次选择**邮件策略 (Mail Policies) > HAT 概述 (HAT Overview)**。

步骤 2 点击发件人组列表中的 **SUSPECTLIST**。

步骤 3 点击**编辑设置 (Edit Settings)**。

步骤 4 从列表中选择 THROTTLED 策略。

步骤 5 选中“连接主机 DNS 验证”(Connecting Host DNS Verification) 下的“连接主机反向 DNS 查询 (PTR) 不匹配正向 DNS 查询 (A)”(Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A)) 复选框。

步骤 6 提交并确认更改。

现在，其反向 DNS 查询失败的发件人将匹配 SUSPECTLIST 发件人组，并将收到来自 THROTTLED 邮件流策略的默认操作。

对未经验证的发件人实施更严格的限制设置

步骤 1 创建新的邮件流策略（对于本例，其名为 THROTTLEMORE ）并为其配置更为严格的限制设置。

a) 在“邮件流策略”(Mail Flow Policies) 页面上，点击**添加策略 (Add Policy)**
b) 输入邮件流策略的名称，然后选择“接受”(Accept) 作为“连接行为”(Connection Behavior)。
c) 配置策略以限制邮件。
d) 提交并确认更改。

步骤 2 创建一个新的发件人组（对于本例，其名为 UNVERIFIED）并将其配置为使用 THROTTLEMORE 策略：

a) 在“HAT 概述”(HAT Overview) 页面上，点击**添加发件人组 (Add Sender Group)**
b) 从列表中选择 THROTTLEMORE 策略。
c) 选中“连接主机 DNS 验证”(Connecting Host DNS Verification) 下的“连接主机 PTR 记录在 DNS 中不存在”(Connecting host PTR record does not exist in DNS) 复选框。
d) 提交并确认更改。

定义邮件以使用 ACCEPTED 邮件流策略发送到未经验证的发件人

步骤 1 依次选择**邮件策略 (Mail Policies) > 邮件流策略 (Mail Flow Policies)**。

步骤 2 在“邮件流策略”(Mail Flow Policies) 页面上，点击 ACCEPTED 邮件流策略。

步骤 3 向下滚动到**发件人验证 (Sender Verification)** 部分。

步骤 4 在**信封发件人 DNS 验证 (Envelope Sender DNS Verification)** 部分，执行以下操作：

- 选择**启用 (On)** 为此邮件流策略启用信封发件人 DNS 验证。
- 还可以定义自定义 SMTP 代码和响应。

步骤 5 在**使用域例外表 (Use Domain Exception Table)** 部分，选择**开 (On)** 来启用域例外表。

步骤 6 提交并确认更改。

根据发件人的邮件地址从发件人验证规则中排除未经验证的发件人

步骤 1 依次选择**邮件策略 (Mail Policies) >“例外表”(Exception Table)**。

注释 例外表将全局应用到启用了“使用例外表”(Use Exception Table) 的所有邮件流策略。

步骤 2 在“邮件策略”(Mail Policies) >“例外表”(Exception Table) 页面上，点击**添加域例外 (Add Domain Exception)**。

步骤 3 输入邮件地址。可以输入特定地址 (pres@whitehouse.gov)、名称 (user@)、域（@example.com 或 @.example.com）或具有用括号括起来的 IP 地址的地址 (user@[192.168.23.1])。

步骤 4 指定是允许还是拒绝来自该地址的邮件。如果拒绝邮件，还可以指定 SMTP 代码和自定义响应。

步骤 5 提交并确认更改。

在发件人验证例外表中搜索地址

步骤 1 在“例外表”(Exception Table) 页面的“查询发件人验证例外”(Find Domain Exception) 部分中输入邮件地址。

步骤 2 点击 **Find**（**查找**）。

如果该地址与表中的任何条目匹配，则会显示第一个匹配的条目。

为来自未经验证的发件人的邮件测试设置

您已经配置了发件人验证设置，可以验证设备的行为了。

请注意，测试 DNS 相关的设置不属于本文档的讨论范围。

发送 MAIL FROM 发件人地址格式不正确的测试邮件

尽管为 THROTTLED 策略测试各种 DNS 相关的设置会非常困难，但可以测试格式不正确的 MAIL FROM 设置。

步骤 1 打开与设备的 Telnet 会话。

步骤 2 使用 SMTP 命令发送具有格式不正确的 MAIL FROM（类似于没有域的“管理员”）的测试邮件。

注释 如果将设备配置为使用默认域或在发送或接收邮件时明确允许部分域，或者如果启用了地址解析（请参阅“配置网关以接收邮件”一章），则可能无法创建、发送和接收缺少域或域格式不正确的邮件。

步骤 3 验证邮件是否被拒绝。

```
# telnet IP_address_of_Email_Security_Appliance port
220 hostname ESMTP
helo example.com
250 hostname
mail from: admin
553 #5.5.4 Domain required for sender address
```

请注意，SMTP 代码和响应是您为 THROTTLED 邮件流策略的信封发件人验证设置配置的代码和响应。

从发件人验证规则中排除的地址发送邮件

要确认来自发件人验证例外表中列出的邮件地址的邮件不受信封发件人验证的约束，请执行以下操作：

步骤 1 将以下地址添加到具有“允许”行为的例外表：admin@zzzaaazzz.com

步骤 2 确认您的更改。

步骤 3 打开与设备的 Telnet 会话。

步骤 4 使用 SMTP 命令从您在发件人验证例外表中输入的邮件地址 (admin@zzzaaazzz.com) 发送测试邮件。

步骤 5 验证邮件是否已被接受。

```
# telnet IP_address_of_Email_Security_Appliance port
220 hostname ESMTP
helo example.com
250 hostname
mail from: admin@zzzaaazzz.com
250 sender <admin@zzzaaazzz.com> ok
```

如果从发件人验证例外表中移除该邮件地址，则来自该发件人的邮件将被拒绝，因为信封发件人的域部分未经过 DNS 验证。

发件人验证和日志记录

以下日志条目提供发件人验证判定结果的示例。

信封发件人验证

不合法的信封发件人地址:

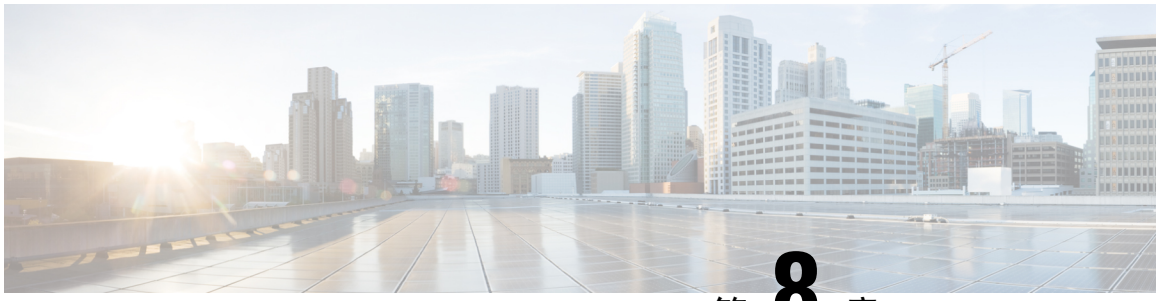
```
Thu Aug 10 10:14:10 2006 Info: ICID 3248 Address: <user> sender rejected, envelope sender
 domain missing
```

域不存在 (NXDOMAIN):

```
Wed Aug  9 15:39:47 2006 Info: ICID 1424 Address: <user@domain.com> sender rejected, envelope
 sender domain does not exist
```

域无法解析 (SERVFAIL):

```
Wed Aug  9 15:44:27 2006 Info: ICID 1425 Address: <user@domain.com> sender rejected, envelope
 sender domain could not be resolved
```



第 8 章

基于域名或收件人地址接受或拒绝连接

本章包含以下部分：

基于收件人地址接受或拒绝连接概述

AsyncOS 使用每个公共侦听程序的收件人访问表 (RAT) 管理针对收件人地址的接受和拒绝操作。收件人地址包括：

- 域
- 邮件地址
- 邮件地址组

管理员可根据系统设置向导在设备上配置至少一个公共侦听程序（使用默认值）。在设置过程中配置公共侦听程序需要指定接受邮件的默认本地域或特定地址。这些本地域或特定地址是此公共侦听程序 RAT 中排在前面的条目。

默认条目“所有其他收件人”将拒绝来自所有收件人的邮件，在任何公共侦听程序中均如此。管理员定义设备接受哪些本地域的邮件。或者，您也可以定义设备接受或拒绝哪些特定用户的邮件。AsyncOS 支持用户使用收件人访问表 (RAT) 定义可接受的本地域和特定用户。

您可能需要配置侦听程序来接受多个域的邮件。例如，如果您的组织使用域 `currentcompanyname.com`，而组织过去曾使用 `oldcompanyname.com`，那么您可以接受来自 `currentcompanyname.com` 和 `oldcompanyname.com` 这两个域的邮件。在这种情况下，请在公共侦听程序的 RAT 中添加这两个本地域。

（注意，域映射功能可将一个域的邮件映射至另一个域。请参阅“配置路由和传送功能”章节的“域映射功能”部分。）

收件人访问表 (RAT) 概述

收件人访问表定义公共侦听程序接受的收件人。此列表至少将指定地址以及接受还是拒绝此地址。

“收件人访问表”(RAT) 页面列出了 RAT 中的条目，其中包括条目顺序、默认操作，以及条目是否配置为绕过 LDAP 接受查询。

使用 GUI 访问 RAT

GUI

依次导航到**邮件策略 (Mail Policies)** > **收件人访问表 (Recipient Access Table, RAT)**。

使用 CLI 访问 RAT

CLI

使用 `listenerconfig` 命令和 `edit > rcptaccess > new` 子命令。

编辑默认 RAT 条目

准备工作

- 设置一个公共侦听程序。
- 编辑时务必谨慎，确保不会在互联网上创建开放中继。开放中继（有时称为“不安全中继”或“第三方”中继）是允许邮件的第三方中继的 SMTP 邮件服务器。开放中继可处理并非本地用户接收/发出的邮件，肆无忌惮的发件人因此能够通过您的网关发送大量垃圾邮件。默认情况下，RAT 将拒绝所有收件人，防止创建开放中继。
- 注意，您不能删除 RAT 中的默认条目。

步骤 1 导航到**邮件策略 > 收件人访问表 (RAT)**。

步骤 2 点击**所有其他收件人 (All Other Recipients)**。

域和用户

使用 RAT 修改接受邮件的域

使用“邮件策略”>“收件人访问表”(RAT)页面配置设备可为其接受邮件的本地域和特定用户。在此页面，您可以执行下列任务：

- 添加、删除以及修改 RAT 中的条目。
- 更改条目的顺序。
- 将 RAT 条目导出到文本文件。
- 从文本文件导入 RAT 条目。从文本文件导入条目将覆盖现有条目。

添加为其接受邮件的域和用户

步骤 1 导航到**邮件策略 > 收件人访问表 (RAT)** 页。

步骤 2 在“侦听程序概述”(Overview for Listener) 字段，选择要编辑的侦听程序。

步骤 3 点击**添加收件人 (Add Recipient)**。

步骤 4 选择条目的顺序。

步骤 5 输入收件人地址。

步骤 6 选择接受或拒绝收件人。

步骤 7 （可选）选择对收件人绕过 LDAP 接受查询。

步骤 8 （可选）对此条目使用自定义 SMTP 响应。

a) 对“自定义 SMTP 响应”(Custom SMTP Response) 选择“是”(Yes)。

b) 输入 SMTP 响应代码和文本。将 SMTP 响应添加到收件人 RCPT TO 命令。

步骤 9 （可选）对“绕过接收控制”(Bypass Receiving Control) 选择“是”(Yes) 以绕过控制。

步骤 10 提交并确认更改。

定义收件人地址

RAT 允许定义一个收件人或一组收件人。可以使用完整邮件地址、域、子域、用户名或 IP 地址定义收件人：

[IPv4 地址]	主机的特定互联网协议第 4 版 (IPv4) 地址。注意，IP 地址必须括在“[]”字符中。
[IPv6 地址]	主机的特定互联网协议第 6 版 (IPv4) 地址。注意，IP 地址必须括在“[]”字符中。
`division.example.com`	完全限定域名。
`.partialhost`	“partialhost”域中的所有对象。
`user@domain`	完整邮件地址。
`user@`	使用指定用户名的所有对象。

user@[*IP_address*]	位于特定 IPv4 或 IPv6 地址的用户名。注意，IP 地址必须括在“[]”字符中。 注意，“user@*IP_address*”（不含括号字符）为无效地址。收到创建有效地址的消息后，系统会附加括号，这可能会影响收件人在RAT中的匹配。

注释 在 GUI 的系统设置向导步骤 4 中，当您在收件人访问表中添加域时（请参阅第 3 步：网络，第 32 页），可能需要考虑再添加一个指定子域的条目。例如，如果您输入域 example.net，可能还需要输入 .example.net。第二个条目可确保发往任何 example.net 子域的邮件在收件人访问表中存在匹配项。注意，在 RAT 中仅指定 .example.com 可接受发送至 .example.com 所有子域的邮件，但不会接受发送至没有子域的完整邮件地址收件人（例如 joe@example.com ）的邮件。

对特定收件人绕过 LDAP 接受查询

如果您配置 LDAP 接受查询，您可能希望对某些收件人绕过接受查询。如果您接收某些人员（例如 customercare@example.com）的邮件，但不希望这些邮件在LDAP查询过程中被延迟或排队，此功能可能会非常有用。

如果您将收件人地址配置为在 LDAP 接受查询之前在工作队列重写（例如，使用别名或域映射），此重写地址不会绕过 LDAP 接受查询。例如，使用别名表将 customercare@example.com 映射至 bob@example.com 和 sue@example.com。如果对 customercare@example.com 配置绕过 LDAP 接受，执行使用别名后，LDAP 接受查询仍对 bob@example.com 和 sue@example.com 有效。

要通过 GUI 配置绕过 LDAP 接受，请在添加或编辑 RAT 条目时，选择**对此收件人绕过 LDAP 接受查询 (Bypass LDAP Accept Queries for this Recipient)**。

要通过 CLI 配置绕过 LDAP 接受查询，请在使用 listenerconfig -> edit -> rcptaccess 命令输入收件人时对以下问题回答 yes：

```
Would you like to bypass LDAP ACCEPT for this entry? [Y]> y
```

注意，配置 RAT 条目绕过 LDAP 接受查询时，RAT 条目的顺序会影响收件人地址的匹配。RAT 会将收件人地址与第一条满足条件的 RAT 条目匹配。例如，您有 RAT 条目 postmaster@ironport.com 和 ironport.com。您配置 postmaster@ironport.com 的条目绕过 LDAP 接受查询，将 ironport.com 的条目配置为 ACCEPT。当您收到发送至 postmaster@ironport.com 的邮件时，只有当 postmaster@ironport.com 的条目在 ironport.com 条目前面时才会发生绕过 LDAP 接受查询。如果 ironport.com 的条目在 postmaster@ironport.com 条目前面，RAT 会将收件人地址与此条目匹配，并应用 ACCEPT 操作。

绕过针对特殊收件人的限制

对于收件人条目，您可以指定收件人绕过侦听程序上启用的限制控制机制。

如果您不想限制某些收件人的邮件，可以使用此功能。例如，很多用户希望收到侦听程序上发送至地址“postmaster@domain”的邮件，即使基于邮件流策略中定义的接收控制已限制此发送域。指定此收件人绕过侦听程序RAT中的接收控制，可让侦听程序不受限制地接收“postmaster@domain”收

件人的邮件，同时对同一域中的其他收件人应用邮件流策略。如果发送域受限制，系统维护的每小时收件人计数器将不对此收件人计数。

要通过 GUI 指定某些收件人绕过接收控制，请在添加或编辑 RAT 条目时对“绕过接收控制”设置选择“是”：

要通过 CLI 指定某些收件人绕过接收控制，请在使用 `listenerconfig > edit > rcptaccess` 命令输入收件人时对以下问题回答 yes：

```
Would you like to bypass receiving control for this entry?  [N]> y
```

重新排列收件人访问表中域和用户的顺序

步骤 1 导航到**邮件策略 > 收件人访问表 (RAT)** 页。

步骤 2 在**侦听程序概述**字段中，选择要编辑的侦听程序。

步骤 3 点击**编辑顺序 (Edit Order)**。

步骤 4 通过调整**顺序**列的值来更改顺序。

步骤 5 提交并确认更改。

将收件人访问表导出至外部文件

步骤 1 依次导航到**邮件策略 > 收件人访问表 (RAT)** 页。

步骤 2 在**侦听程序概述**字段，选择要编辑的侦听程序。

步骤 3 点击**导出 RAT (Export RAT)**。

步骤 4 输入导出条目的文件名。

这是在设备的配置目录中创建的文件的名称。

步骤 5 提交并确认更改。

从外部文件导入收件人访问表

从文本文件导入收件人访问表条目时，所有现有条目将从收件人访问表中删除。

步骤 1 导航到**邮件策略 > 收件人访问表 (RAT)** 页面。

步骤 2 在**侦听程序的概述**字段中选择要编辑的侦听程序。

步骤 3 点击**导入 RAT (Import RAT)**。

步骤 4 从列表中选择文件。

AsyncOS 将列出设备配置目录中的所有文本文件。

步骤 5 点击 **Submit**。

设备将显示警告消息，询问您是否确认要删除现有的所有收件人访问表条目。

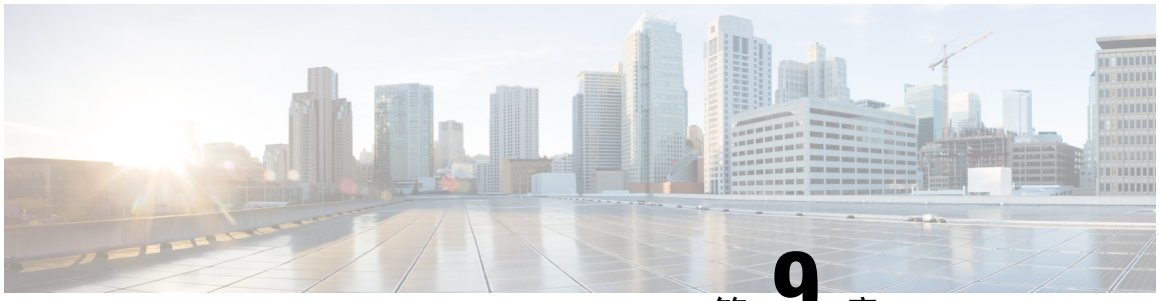
步骤 6 点击 **Import**。

步骤 7 确认您的更改。

可以在文件中放置“注释”。以“#”字符开头的行被视为注释，AsyncOS 会忽略注释。例如：

示例：

```
# File exported by the GUI at 20060530T220526
.example.com  ACCEPT
ALL  REJECT
```



第 9 章

使用邮件过滤器实施邮件策略

思科设备采用一系列内容扫描和邮件过滤技术，可帮助您实施公司策略，并对进出公司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

通过邮件过滤器，您可以创建描述在思科设备收到邮件时如何对其进行处理的特殊规则。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，第 118 页。
- **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，第 119 页。
- **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，第 118 页。

- **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、删除或退回邮件）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，第 118 页。
- **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。图像分析器创建测量颜色、正文大小和曲度的算法，确定图像是否包含不适当的内容。有关详细信息，请参阅附件扫描，第 190 页。
- **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，第 199 页。
- **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，第 213 页。

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。

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选定的邮件执行操作。

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，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。

注释 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。

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

`{`
`  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，第 120 页。
- **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，第 120 页。
- **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，第 121 页。
- **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。可通过此配置，“权衡”针对不同条件的响应。有关详细信息，请参阅内容扫描中的匹配阈值，第 121 页。
- **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，第 124 页。

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。

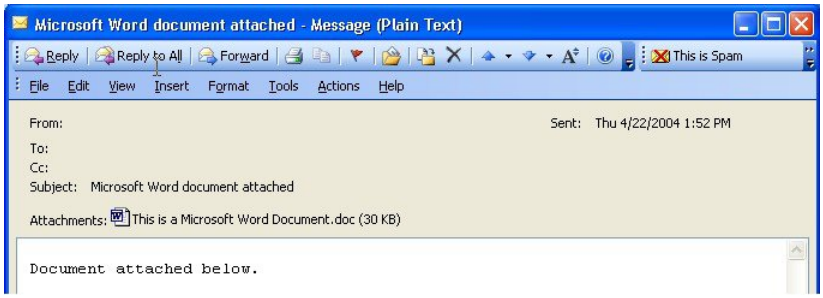
邮件正文与邮件附件

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，思科设备将按照很多 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，下图显示 Microsoft Outlook MUA 中的一封邮件，其中语句“`Document attached below.`”显示为纯文本邮件正文，“`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。

图 *16:* 含“附件”的邮件



由于思科设备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”，思科设备会将整封邮件视为正文。如果内容类型是其他类型，思科设备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。

注释 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。

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)){
```

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。然后比较这些分数的结果，并从结果中选择最高分。接下来，将此结果与每个附件的分数相加得出最终分数。假设该邮件有以下数量的匹配项：

```
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分数。例如，假设您创建了包含以下内容和权重的内容词典：

表 *19:* 示例内容词典

术语/智能标识符	重量
美国银联转帐号码	3
帐户	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“账号”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，因此改变测试项的顺序不会产生任何影响。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。

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。

表 *20:* 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，第 136 页。
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，第 138 页。
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，第 137 页。
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，第 137 页。
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，第 138 页。
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，第 136 页。 **注释** `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，第 137 页。 **注释** `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，第 139 页。
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，第 140 页
接收侦听器	`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，第 139 页。

规则	语法	说明
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，第 140 页。
标头	`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，第 140 页。
随机数	`random(<integer>)`	随机数是否在某一范围内？请参阅随机规则，第 141 页。
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，第 142 页。
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，第 142 页。
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，第 148 页。
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，第 149 页。
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，第 149 页
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，第 150 页。
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，第 192 页。
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，第 150 页。
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，第 142 页。
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，第 142 页。

规则	语法	说明
加密检测	`encrypted`	邮件是否加密？请参阅加密检测规则，第 143 页。
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，第 144 页。
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，第 144 页。
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，第 145 页。
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，则设备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，第 196 页。
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，第 198 页。
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，第 199 页。

规则	语法	说明
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，第 196 页。
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。
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，第 196 页。
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，第 196 页。
公共黑名单	`dnslist(<query server>)`	发件人的 IP 地址是否出现在公共黑名单服务器上(RBL)？请参阅DNS 列表规则，第 145 页。
SenderBase 信誉	`reputation`	什么是发件人的 SenderBase 信誉得分？请参阅SenderBase 信誉规则，第 145 页。
无 SenderBase 信誉	`no-reputation`	用于测试SenderBase信誉得分是否为“None”。请参阅SenderBase 信誉规则，第 145 页。
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，第 146 页。
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，第 146 页。
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，第 146 页。

规则	语法	说明
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，第 146 页。
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，第 146 页。
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，第 146 页。
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，第 146 页。
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，第 150 页。
真	`true`	匹配所有邮件。请参阅True 规则，第 135 页。
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，第 135 页。
已签名	`signed`	邮件是否已签名？请参阅已签名规则，第 152 页。
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，第 152 页。
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，第 155 页。
URL Reputation	`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，第 156 页。
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，第 157 页。
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，第 157 页。

规则	语法	说明
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，第 157 页。
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了宏的附件？ 请参阅 宏检测规则，第 158 页
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:”标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，第 159 页。
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，第 160 页。
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，第 160 页。
地理定位	`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？ **注释** 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，第 160 页

系统会按顺序对进入思科设备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，第 118 页。）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：

表 *21:* 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。特别是，句点和星号 (.*) 的顺序匹配任何字符序列（不包含新行）。 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。将该符号放在区分大小写的正则表达式的开头会导致完全不区分大小写的匹配。 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。
Or (|)	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。

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，第 199 页和配置扫描行为，第 220 页。

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。

注释 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，第 136 页中的第二个示例

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)$") {
```

正则表达式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) 转账号码

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：

表 *22*: 邮件过滤器中的智能标识符

关键词	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。

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。

注释 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。

注释 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”);}
```

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。

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）。有关更多信息，请参阅邮件信头规则和求值，第 120 页。

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();

}
```

注释 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，以下过滤器会删除发送地址包含字符串“scarface”的所有邮件。

注释 rcpt-to 规则的正则表达式不区分大小写。

```
scarfaceFilter:

if (rcpt-to == 'scarface')

{
```

```
drop();

}
```

注释 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();

}
```

注释 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。

注释 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

示例	对比类型
`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：思科设备无法接收超过 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`、SBRS、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();

}
```

注释 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，第 120 页。

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：

```
large_list_filter:


if (rcpt-count > 100) {

alt-src-host('mass_mailing_interface');

}
```

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，第 220 页。

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，第 121 页。

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。

注释 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，第 220 页。

下列过滤器检查所有通过侦听程序发送的电子邮件，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”页面或 `scanconfig` 命令中的形式（如配置扫描行为，第 220 页所述），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，第 220 页所述的所有选项。

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，第 190 页。

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，思科设备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，第 220 页）。
    - 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，第 145 页。

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，第 190 页。

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();
```

```
}
```

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：

```
whitelist_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。

```
blacklist:

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

drop();

}
```

SenderBase 信誉规则

`reputation` 规则根据另一个值检查 SenderBase 信誉得分。支持所有比较运算符，例如，>、==、<= 等。如果邮件根本没有 SenderBase 信誉得分（由于从未检查过该得分，或由于系统收不到 SenderBase

Reputation Service 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 SBRS 得分是否为“无”(None)。以下示例将邮件的“Subject:”行调整为，在 SenderBase Reputation Service 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，第 184 页

SenderBase 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 Policy 隔离区，前提是邮件正文中包含“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 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，第 468 页。

注释 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");
}
```

注释 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");
}
```

有关更多信息，请参阅S/MIME 安全服务，第 413 页。

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，第 413 页

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，第 462 页。

SMTP 身份验证用户匹配规则

如果思科设备使用 SMTP 身份验证发送邮件，`smtp-auth-id-matches` (<目标> *[, <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
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，设备将隔离邮件。

```
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。

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']
```

示例 1

```
},
{
'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 ，第 784 页。

注释 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。

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白名单：

```
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，请参阅按 URL 信誉或 URL 类别过滤：条件和规则，第 333 页 防御恶意或不需要的 URL，第 327 页

在这些规则中：

- `Msg_filter_name` 为邮件过滤器的名称。
- `whitelist` 为已定义 URL 列表的名称（通过 urllistconfig 命令定义）。可以选择是否指定白名单。

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>:
{<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。

-

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>:
{<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，第 327 页中的按 URL 信誉或 URL 类别过滤：条件和规则，第 333 页。

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_white_list>’ ,'<include_attachments>')

<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，第 340 页。
- `url_white_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恶意 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。

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无法扫描且识别为已损坏的附件。

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。

注释 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

思科邮件安全设备使用内置语言检测引擎来检测邮件中所采用的语言。设备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，并将其传递回设备。设备将概率最高的语言视为邮件的语言。在下列某种情况下，设备将邮件的语言视为“待定”：

- 如果思科邮件安全设备不支持检测到的语言
- 如果设备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。

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，设备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”，则设备会将相似性得分 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”，则设备会将相似性得分 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，第 478 页。

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。

注释 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）。

邮件过滤器示例

```
<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");}
```

邮件过滤器操作

邮件过滤器的目的是对选定的邮件执行操作。

操作分为两类：

- 最终操作，例如，传送、删除以及退回，结束邮件处理，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。

注释 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。

“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：

表 *23:* 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，第 180 页。
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，第 179 页。
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，第 179 页。
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，第 174 页。

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，第 174 页。
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，第 176 页。
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，第176页。
存档	存档	将邮件归档为 mbox 格式的文件。请参阅存档操作，第 180 页。
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，第 178 页。
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，第 178 页。
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，第 181 页。
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，第 181 页。
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，第 182 页。
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，第 182 页。
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，第 183 页.
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，第 184 页。

操作	语法	说明
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，第 184 页。
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，第 184 页。
	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，第 184 页。
	skip-bulkcheck	绕过针对批量邮件的操作。请参阅绕过灰色邮件操作，第 184 页。
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，第 185 页。
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，第 185 页。
跳过爆发过滤器扫描	`skip-vofcheck`	确保邮件不通过爆发过滤器扫描处理。请参阅绕过防病毒系统操作，第 185 页。
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。如果归档文件附件(zip、tar) 包含匹配的文件，也将删除这些附件。请参阅附件扫描邮件过滤器示例，第 196 页。
按类型删除附件	`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。如果归档文件附件(zip、tar) 包含匹配的文件，也将删除这些附件。请参阅附件扫描邮件过滤器示例，第 196 页。
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。如果归档文件附件(zip、tar) 包含匹配的文件，也将删除这些附件。有关详细信息，请参阅附件扫描邮件过滤器示例，第 196 页。

操作	语法	说明
按 MIME 类型删除附件	`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，因此也不会检查归档的内容。请参阅附件扫描邮件过滤器示例，第 196 页。
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，对于归档或压缩文件，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，第 196 页。
按内容删除附件	`drop-attachments-where-contains`	删除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，则存档文件将被删除。请参阅附件扫描邮件过滤器示例，第 196 页。 可选注释用来修改用于替换已删除附件的文本。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。 **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。 **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 Portable Document Format` • `Microsoft Office Files` • `OLE File types` • **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，第 158 页
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，第 196 页。
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”。
发送时加密	`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，第 174 页。
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，第 174 页。
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，第 186 页和“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。请参阅添加日志条目操作，第 186 页。
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，第 187 页。
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，第 189 页。
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，第 190 页。

操作	语法	说明
无操作	`no-op`	未执行任何操作。请参阅无操作，第 190 页。
*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，第 172 页。
*删除邮件	`drop`	删除并删除邮件。请参阅删除操作，第 173 页。
*退回邮件	`bounce`	将邮件发回给发件人。请参阅退回操作，第 173 页。
*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，第 173 页。
* 最终操作		

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，邮件安全设备便会删除该邮件，即使其他附件不是 `.exe` 文件。

表 *24:* 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 **注释** 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。
缩写格式	• 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”

附件组名称	扫描的文件类型
文本	• txt • html • xml
映像	• bmp • cur • gif • ico • jpeg • pcx • png • psd • psp • tga • tiff
Media	• 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。 思科设备支持以下操作变量：

表 *25:* 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，第 153 页。
日期	`$Date`	使用 MM/DD/YYYY 格式返回当前日期。
已删除的文件名	`$dropped_filename`	仅返回最近丢弃的文件名。
已删除的文件名	`$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 $filetypes）。
信封发件人	`$EnvelopeFrom`	返回邮件的信封发件人 (Envelope From, <MAIL FROM>)。
信封收件人	`$EnvelopeRecipients`	返回邮件的所有信封收件人 (Envelope To, <RCPT TO>)。
文件名	`$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“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<”。

变量	语法	说明
标头	`$Header['string']`	如果原始邮件中包含匹配的信头，返回引用信头的值。请注意，也可以使用双引号。
主机名	`$Hostname`	返回思科设备的主机名。
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 $Header 检索该值）混淆。
接收侦听器	`$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`	返回向思科设备发送邮件的系统的 IP 地址。
远程主机地址	`$remotehost`	返回向思科设备发送邮件的系统的主机名。
SenderBase 信誉得分	`$Reputation`	返回发件人的 SenderBase 信誉得分。如果没有信誉得分，会替换为“无”。
主题	`$Subject`	返回邮件的主题。
时间	`$Time`	返回本地时区的当前时间。
时间戳	`$Timestamp`	返回邮件消息“Received:”行中本地时区的当前时间和日期。

非 ASCII 字符集和邮件过滤器操作变量

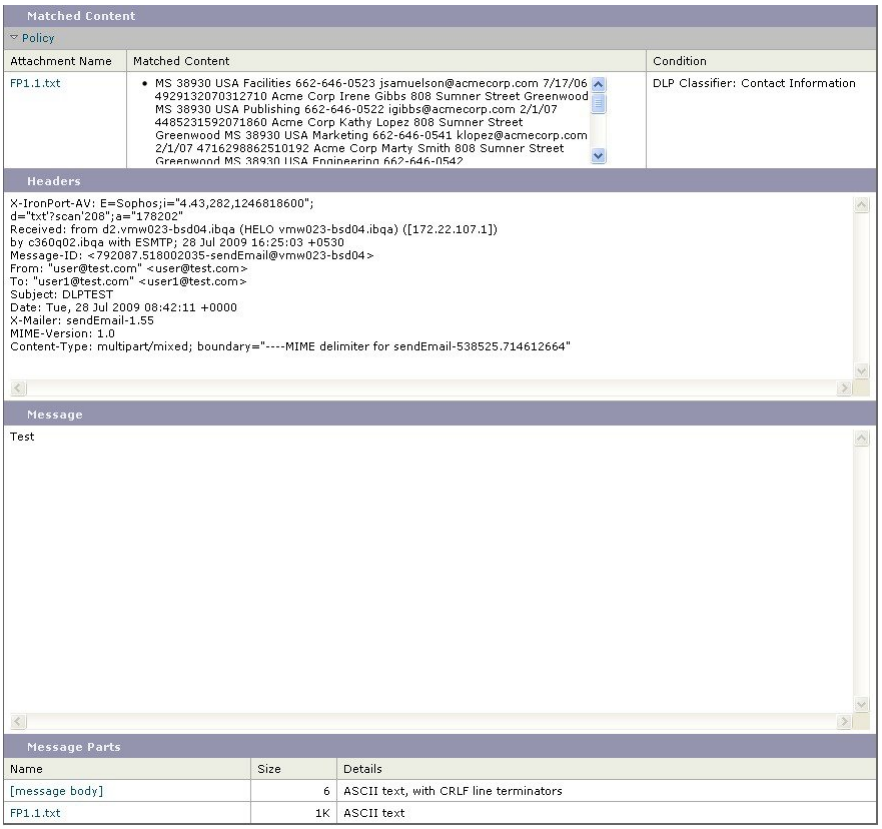
系统支持包含 ISO-2022 样式字符编码（信头值的编码方式）的操作变量扩展，并支持通知中的国际文本。它们将结合生成可作为 UTF-8 可打印引用消息发送的通知。

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。

查看触发了邮件或内容过滤器规则的本地隔离区的邮件时，GUI 可能显示实际上未触发过滤器操作的内容（及已触发过滤器操作的内容）。应将 GUI 显示作为查找内容匹配的指南，但它不一定反映确切的内容匹配。发生这种情况，是因为 GUI 比过滤器使用的内容匹配逻辑更宽松。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。

图 *17:* 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。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，如果设备执行此类扫描。`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();

}
```

删除操作

drop 操作会删除邮件，不进行任何传送。邮件不会退回给发件人、不会发送至原定收件人，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');
}
```

注释 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。
- 与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，第 169 页）：

```
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，第 169 页）。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，第 196 页。

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');
}
```

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，第 169 页）。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');

}
```

⚠

注意 `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');
```

```
}
```

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。另一个包含所有附件的原始邮件 副本将被隔离（发送到 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。

注释 `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，第 523 页。）

注释 `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，此操作可以在一个思科邮件安全设备上创建多个虚拟网关地址。有关详细信息，请参阅使用虚拟网关™ 技术为所有托管的域配置邮件网关，第 570 页。

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` 操作可在设备上将原始邮件（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。

注释 `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，第 199 页。

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“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，第 120 页。

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。

注释 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 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“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，第 120 页。

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，第 121 页。

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");

}
```

注释 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，第 121 页。

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，第 550 页。）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 SenderBase 信誉得分的邮件绕过基于内容的反垃圾邮件过滤功能：

```
whitelist_on_reputation:

if (reputation > 7.5)

{

skip-spamcheck();

}
```

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爆发过滤器扫描。如果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“数据丢失防护”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();
}
```

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，请参阅修改邮件中的 URL：在过滤器中使用 URL 信誉和 URL 类别操作，第 334 页 防御恶意或不需要的 URL，第 327 页

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。
- `whitelist` 为已定义 URL 列表的名称（通过 `urllistconfig` 命令定义）。可以选择是否指定白名单。
- 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。

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>' , '< whitelist>', <
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>', '<whitelist>', <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>, '<whitelist>', <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 ('<whitelist>', <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>, '<whitelist>', <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 ('<whitelist>', <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，请参阅修改邮件中的 URL：在过滤器中使用 URL 信誉和 URL 类别操作，第 334 页 防御恶意或不需要的 URL，第 327 页

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，第 340 页。
- url_white_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

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_white_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_white_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_white_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、隔离或删除等其他操作，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

邮件安全设备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。

设备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

注释 您可以在 Web 界面中使用**安全服务** > **扫描行为**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，第 220 页。

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，第 196 页）。

表 *26:* 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。如果归档文件附件 (zip、tar) 包含匹配的文件，也将删除这些附件。请参阅附件扫描邮件过滤器示例，第 196 页。
按类型删除附件	`drop-attachments-by-type (<MIME type >[, <optional comment >])`	删除邮件中 MIME 类型的所有附件（按给定 MIME 类型或文件扩展名判断）。如果归档文件附件 (zip、tar) 包含匹配的文件，也将删除这些附件。

操作	语法	说明
按文件类型删除附件	drop-attachments-by-filetype (<*fingerprint name* >[, <*optional comment* >])	删除邮件中匹配给定文件“指纹”的所有附件。如果归档文件附件 (zip、tar) 包含匹配的文件，也将删除这些附件。
按 MIME 类型删除附件	drop-attachments-by-mimetype (<*MIME type* >[, <*optional comment* >])	删除邮件中给定 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，因此也不会检查归档的内容。
按大小删除附件	drop-attachments-by-size (<*number* >[, <*optional comment* >])	删除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。
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，则存档文件将被删除。
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，第 196 页。

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。您可以使用图像分析引擎搜索邮件中的不当内容。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。

配置设备进行图像分析后，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。图像分析器使用测量颜色、正文大小和曲度的算法，确定图形是否包含不适当的内容。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：

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**。

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

下一步做什么

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。

微调图像分析设置

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

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分数。无法扫描的注释可表明是否有任何图像无法扫描。

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删除了附件：

```
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。

注释 思科建议您不要删除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");

}

}
```

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。

根据图像分析判定删除附件：

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：

- 可疑的
- 不适当
- 可疑或不适当
- 不可扫描
- 清洁

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：

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：

- 可疑的
- 不适当
- 可疑或不适当
- 不可扫描
- 清洁

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”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');

}
```

有关更多信息，请参阅通知和通知并抄送操作，第 174 页。

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

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。

注释 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，邮件将被删除。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，邮件安全设备便会删除该邮件，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”词典中的词语将删除附件。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 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 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。

表 *27:* 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，过滤器会插入到序列中的指定位置。有关详细信息，请参阅创建新的邮件过滤器，第 200 页。
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，第 201 页。
move	重新排列现有的过滤器。有关详细信息，请参阅创建新的邮件过滤器，第 200 页。
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，第 200 页。
import	将当前的过滤器集合替换为文件中存储的新集合（设备的 /configuration 目录）。有关详细信息，请参阅创建新的邮件过滤器，第 200 页。
export	将当前的过滤器集合导出至文件（设备的 /configuration 目录）。有关详细信息，请参阅导出邮件过滤器，第 204 页。
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，第 205 页。

语法	说明
`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，第 205 页。
`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，第 205 页。

注释 必须发出 commit 命令，过滤器才能生效。

参数的三种类型如下：

表 *28*: 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	过滤器的描述性名称。
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。

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。
- 过滤器的操作引用不存在的系统资源（如接口）。

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。

注释 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.

[]>
```

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。

注释 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:。

导入邮件过滤器

`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，第 979 页。考虑导出当前过滤器列表（请参阅导出邮件过滤器，第 204 页），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。
- 过滤器的操作引用不存在的系统资源（如接口）。

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（位于设备 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，第 979 页。

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（参阅导入邮件过滤器，第 204 页）设备。

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。

过滤器日志订阅具有以下默认值，可使用 logconfig 子命令进行修改：

- 检索方法 - FTP 轮询
- 文件大小 - 10 MB
- 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: Only try encoding from message body
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]>
Footers or headings are added in-line with the message body whenever
possible. However, if the footer or heading 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 footer or
heading. If that fails, and if the message body's encoding is USASCII,
the system can try to edit the message body to use the footer's
or heading's encoding. Should the system try to impose the footer's
or headings's encoding on the message body? [N]> y
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
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，设备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。

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` 规则删除超过 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`。

之后使用 `filter -> list` 子命令列出过滤器，确定过滤器是否为活动和有效状态，然后使用 `move` 子命令交换第一个过滤器和最后一个过滤器的位置。最后，提交更改，以使过滤器生效。

```
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。

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();

}
```

思科设备不易 受到通常用于利用传统 Sendmail/Qmail 系统漏洞发起的这些第三方中继黑客攻击。由于其中许多符号（例如%）可以是完全合法的邮件地址的一部分，因此思科设备 会将这些地址接受

作为有效地址，针对所配置的收件人列表 对其进行验证，并将其传递到下一个内部服务器。思科设备不会向 全球转发这些邮件。

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。

注释 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，第 66 页。

策略实施过滤器

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，第 146 页）：

```
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 ();
}
```

SRBS 过滤器

SenderBase 信誉过滤器：

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

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

更改 SRBS 过滤器

更改某些域的 SBRS（SenderBase 信誉得分）阈值：

```
mod_sbrs:
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 SenderBase 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_SBRS:

if (true) {
```

```
insert-header('X-SBRS', '$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至接口“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");
}
```

注释 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。

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，这意味着它们影响所有扫描行为。

注释 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。

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。

  注释 要执行此步骤，配置文件必须位于设备的配置目录中。请参阅管理配置文件，第 754 页。

- 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) 编辑所需字段：

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。

字段	说明
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）。

c) 点击 **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。

注释 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。

第 10 章

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
- 机密企业数据
- 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，第 253 页 • 文件信誉过滤和文件分析：，第 353 页（仅限传入邮件） • 反垃圾邮件，第 269 页 • 灰色邮件检测和安全取消订用。请参阅管理灰色邮件，第 297 页。 • 病毒爆发过滤器，第 307 页 • 数据防泄漏，第 373 页（仅限传出邮件） • 内容过滤器，第 235 页
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，第 235 页
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，第 604 页。
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229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 228 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，第 250 页 • 防病毒: 配置面向用户的病毒扫描操作，第 259 页 • 文件声誉过滤和文件分析: 文件信誉过滤和文件分析：，第 353 页 • 反垃圾邮件: 定义反垃圾邮件策略，第 275 页 • 灰色邮件检测和安全取消订用：配置灰色邮件检测和安全取消订用的传入邮件策略，第 301 页 • Outbreak Filters: 病毒爆发过滤器功能和病毒爆发隔离区，第 323 页 • 数据丢失保护：使用外发邮件策略向发件人和收件人指定 DLP 策略，第 390 页。

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。高级恶意软件保护（文件信誉扫描和文件分析）只能用于传入邮件策略。

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。

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 *29:* 策略匹配示例

订单	策略名称	用户	
		发送方	接收方
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	ANY	ANY

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 227 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、高级恶意软件保护（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。

工作队列	**邮件过滤器** **(filters)**	邮件安全管理器扫描（每个收件人）	↓ **所有收件人的邮件**
	反垃圾邮件 （**antispamconfig**、**antispamupdate**）		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。
	防病毒 （**antivirusconfig**、**antivirusupdate**）		
	文件信誉和分析（高级恶意软件防护） **(ampconfig)**		
	灰色邮件管理		
	内容过滤器 **(policyconfig -> filters)**		
	病毒爆发过滤器 （**outbreakconfig**、**outbreakflush**、**outbreakstatus**、**outbreakupdate**）		
	数据防泄漏 **(policyconfig)**		

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。

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。

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 224 页。

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 点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。可以点击“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 点击 **Submit**。

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224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 225 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。

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 点击**添加策略**。

步骤 3 输入邮件策略的名称。

步骤 4 （可选）点击“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 230 页。

步骤 6 点击 **Submit**。

步骤 7 点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。

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。

步骤 1 在**用户 (Users)** 部分下，点击**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 231 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 231 页。

步骤 4 点击 **Submit**。

步骤 5 查看在**用户 (Users)** 部分所选的条件。

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。

发送方			接收人			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

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 并点击“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。

点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。

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。下表概述了几个示例策略。“主动”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 *30:* 主动和保守邮件安全管理器设置

	主动设置	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 无法扫描的邮件：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 无法扫描的邮件：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

第 11 章

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，第 227 页），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。邮件安全设备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，确定设备何时使用内容过滤器扫描邮件（可选）
- 操作，即设备对邮件所采取的操作（必需）
- 操作变量，即修改邮件时设备可向其添加的操作变量（可选）

如何使用内容过滤器扫描邮件内容

过程

	命令或操作	目的
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 白名单
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，第 236 页 （可选） • 内容过滤器操作，第 242 页 • 操作变量，第 246 页 （可选） 创建内容过滤器，第 248 页
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，第 223 页

内容过滤器条件

条件为“触发”条件，可确定邮件安全设备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。

表 *31:* 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。

情况	说明
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？ **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，第 481 页。 **注释** 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，第 481 页。 **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。
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，第 481 页。 **注释** 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，第 481 页。 **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，第 333 页 和 关于 URL 类别，第 340 页。
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。

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，第 481 页。 **注释** 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，第 481 页。 **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。
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，第 481 页。 **注释** 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，第 481 页。 **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，则设备不会尝试根据其扩展名来“猜测”文件的类型。） **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。 **附件已损坏**。此邮件是否具有已损坏的附件？ **注释** 损坏的附件是扫描引擎无法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无法扫描的附件） **包含未受密码保护或加密的附件**。

情况	说明
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，第 481 页。 **注释** 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，第 481 页。
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，第 481 页 **注释** 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，第 481 页。 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，第 278 页。
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，第 481 页。 **注释** 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，第 481 页。

情况	说明
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，第 481 页。 **注释** 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，第 481 页。 “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？
接收侦听器	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。
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，第 83 页中描述的允许的主机记法指定，但 SBO、SBRS、dnslist 记法和特殊关键字 ALL 除外。
声誉得分	什么是发件人的 SenderBase 信誉得分？信誉得分规则根据另一个值来检查 SenderBase 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？

情况	说明
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：”信头是否与内容词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，设备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”，设备将为该用户分配 82 的相似性得分。 • 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”，设备将为该用户分配 100 的相似性得分。 相似性得分越高，邮件是伪造邮件的可能性就越大。如果相似性得分大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，第 478 页。
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 验证的更多信息，请参阅“邮件身份验证”一章。 **注释** 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，第 413 页
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，第 413 页
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？** 思科邮件安全设备使用内置语言检测引擎来检测邮件中所采用的语言。设备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，并将其传递回设备。设备将概率最高的语言视为邮件的语言。在下列某种情况下，设备将邮件的语言视为“待定”： • 如果思科邮件安全设备不支持检测到的语言 • 如果设备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。

情况	说明
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。 **注释** 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。 **注释** 在使用地理定位内容过滤器之前，请启用设备上的反垃圾邮件引擎。

内容过滤器操作

该操作是邮件安全设备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、将其隔离或删除。对邮件执行的“最终操作”为发送或删除，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、传送和删除都是最终操作。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，第 246 页。

表 *32:* 内容过滤器操作

操作	描述
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。

操作	描述
发送时加密	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，第 406 页。 **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**。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，则存档文件将被删除。 **包含智能标识符**。丢弃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删除附件的文本。附件页脚会直接附加到邮件。
按文件信息删除附件	**文件名**。删除邮件中其文件名与指定的正则表达式匹配的所有附件。如果归档文件附件 (zip、tar) 包含匹配的文件，也将删除这些附件。 **文件大小**。删除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**。删除邮件中匹配给定文件“指纹”的所有附件。如果归档文件附件 (zip、tar) 包含匹配的文件，也将删除这些附件。 **MIME 类型**。丢弃邮件中给定 MIME 类型的所有附件。 **图像分析判定**。丢弃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。 **替换邮件**。可选注释用来修改用于替换已删除附件的文本。附件页脚会直接附加到邮件。

操作	描述
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。 **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。 **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**字段中输入的自定义邮件将替换系统生成的邮件。
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，第 334 页 和 创建 URL 过滤的白名单，第 331 页。 使用“没有分数”来指定无法确定其声誉的 URL 的操作。 **注释** 设备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，第 334 页 和 关于 URL 类别，第 340 页。 **注释** 设备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（信头）添加免责声明。 **下方**。在邮件下方（页脚）添加免责声明。 **注**：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，第 491 页。
忽略病毒爆发过滤器扫描	绕过对此邮件进行的病毒爆发过滤器扫描。
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。

操作	描述
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。
投递到指定的目标主机	**邮件主机**。将邮件的目标邮件主机更改为指定的邮件主机。 **注释** 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。
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，第 478 页。
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，第 376 页。
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	描述
传送时进行 S/MIME 签名/加密	在发送期间，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，第 421 页。
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，第 406 页。 **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）(S/MIME Sign/Encrypt [Final Action])	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，第 421 页。
退回(最终操作)	将邮件发回给发件人。
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。
放弃(最终操作)	删除并丢弃邮件。

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。 设备支持以下操作变量：

表 *33*: 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	`$Date`	替换为当前日期，采用 MM/DD/YYYY 格式。
已删除的文件名	`$dropped_filename`	仅返回最近丢弃的文件名。

变量	语法	说明
已删除的文件名	`$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 `$envelopesender`	替换为邮件的信封发件人（信封来源，<MAIL FROM>）。
信封收件人	`$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。
标头	`$Header['`*`string`*`']`	如果原始邮件包含匹配的信头，则替换为被引用信头的值。请注意，也可以使用双引号。
Hostname	`$Hostname`	替换为邮件安全设备的主机名。
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 $Header 检索该值）混淆。
接收侦听器	`$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`	替换为将邮件发送到邮件安全设备的系统的 IP 地址。
远程主机地址	`$remotehost`	替换为将邮件发送到设备的系统的主机名。
SenderBase 信誉得分	`$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”。
Subject	`$Subject`	替换为邮件的主题。
Time	`$Time`	替换为本地时区中的当前时间。
Timestamp	`$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

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。

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 **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”。

b) 选择条件类型。

c) 定义条件的规则。
d) 点击 **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。

注释 如果不添加条件，则设备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 为设备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”。
b) 选择操作类型。
c) 定义操作。
d) 点击 **OK**。
e) 对希望设备执行的任何其他操作重复先前的步骤。
f) 对于多个操作，按照希望设备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。

下一步做什么

- 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

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，第 235 页中创建）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，第 229 页。

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，并且可以由任何委派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“常规管理任务”一章。
- 管理员和操作员可以查看和编辑设备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*”

- 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，它们会立即影响设备对所有邮件的处理。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。（请参阅集中化的策略、病毒和病毒爆发隔离区，第 685 页）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释放邮件（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。
- 如果在设备中配置了 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，情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：
  - **描述 (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。

第 12 章

防病毒

本章包含以下部分：

防病毒扫描概述

思科设备包括来自第三方公司 Sophos 和 McAfee 的集成病毒扫描引擎。您可以获取思科设备的许可密钥，以便使用其中一种或这两种病毒扫描引擎来扫描邮件中的病毒，然后将设备配置为使用任一种防病毒扫描引擎扫描病毒。

McAfee 和 Sophos 引擎包含执行以下操作所需的程序逻辑：在特定位置扫描文件、处理和模式匹配病毒定义与在您的文件中找到的数据、在模拟环境下解密和运行病毒代码、应用启发式技术以识别新病毒，以及从合法文件中删除受感染代码。

您可以将设备配置为扫描邮件病毒（根据匹配的传入或外发邮件策略），如果发现病毒，则对该邮件执行不同的操作（包括“修复”病毒邮件、修改主题信头、添加额外的 X-Header、将邮件发送到备用地址或邮件主机、存档邮件或删除邮件）。

如果启用，则在设备的“工作队列”中进行反垃圾邮件扫描后，立即执行病毒扫描。（请参阅邮件管道和安全服务， 第 56 页。）

默认情况下，默认传入和外发邮件策略启用病毒扫描。

试用版密钥

思科设备为每个可用的防病毒扫描引擎附送30天的试用版密钥。通过以下方式可启用试用版密钥：访问“系统设置向导”(System Setup Wizard) 或“安全服务”(Security Services) > “Sophos/McAfee 防病毒”(Sophos/McAfee Anti-Virus) 页面中的许可协议，或者运行 `antivirusconfig` 或 `systemsetup` 命令（在 CLI 中）。一旦接受许可协议，默认情况下将为默认传入和外发邮件策略启用防病毒扫描

引擎。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，第 752 页。）

使用多个防病毒扫描引擎扫描邮件

AsyncOS 支持使用多个防病毒扫描引擎扫描邮件 - 多层防病毒扫描。您可以将思科设备配置为：基于每个邮件策略使用一个或两个许可的防病毒扫描引擎。例如，可以为高管创建一个邮件策略，并将该策略配置为同时使用 Sophos 和 McAfee 引擎扫描邮件。

使用多个扫描引擎扫描邮件可结合 Sophos 和 McAfee 防病毒扫描引擎的优势，提供“深度防御”。每个引擎都具有领先的防病毒捕获率，但由于每种引擎依赖不同的技术基础（在McAfee 防病毒过滤，第 256 页和Sophos 防病毒过滤，第 254 页中已讨论）来检测病毒，所以多次扫描方法更为有效。使用多个扫描引擎可能造成系统吞吐量下降，有关详细信息，请与您的思科支持代表联系。

无法配置病毒扫描的顺序。启用多层防病毒扫描时，McAfee 引擎首先扫描病毒，其次 Sophos 引擎再扫描病毒。如果 McAfee 引擎确定某封邮件无病毒，Sophos 引擎再扫描邮件，可添加第二层保护。如果 McAfee 引擎确定某封邮件包含病毒，思科设备将跳过 Sophos 扫描，并根据您配置的设置对病毒邮件执行操作。

Sophos 防病毒过滤

思科设备包括来自 Sophos, Plc. 的集成病毒扫描技术。Sophos 防病毒技术可以跨平台提供防病毒保护、检测和杀毒。

Sophos 防病毒技术提供病毒检测引擎，可扫描文件中的病毒、特洛伊木马和蠕虫。这些程序统称为恶意软件，即“带有恶意的软件”。各种恶意软件之间的相似之处在于，不仅允许防病毒扫描程序检测和删除病毒，还允许检测和删除所有类型的恶意软件。

病毒检测引擎

Sophos 病毒检测引擎的核心是 Sophos 防病毒技术。它使用类似于 Microsoft COM（组件对象模型）的专有架构，其中包括许多带有已明确定义接口的对象。该引擎使用的模块化文件系统基于独立、完备的动态库，每个库处理不同的“存储类”，例如文件类型。这种方法允许在通用数据源中应用病毒扫描操作，不考虑类型。

专业的数据加载和搜索技术，支持该引擎实现快速扫描。其中包含：

- 用于检测多态病毒的完整代码仿真程序
- 用于扫描存档文件内部的在线解压程序
- 用于检测和查杀宏病毒的 OLE2 引擎

思科设备通过 SAV 接口与病毒引擎集成。

病毒扫描

宽泛来讲，引擎的扫描功能由强强联合的两个重要组件来管理：知道查找位置的分类器和知道查找内容的病毒数据库。引擎按类型对文件分类，而不依赖扩展名。

病毒引擎查找系统收到的邮件正文和附件中的病毒；附件的文件类型有助于确定其扫描。例如，如果邮件的附件是可执行文件，引擎将检查信头，从中得知可执行文件代码的开始位置及其外观。如果该文件是 Word 文档，引擎将在宏数据流中查找。如果是 MIME 文件（用于邮件传输的格式），引擎将在存储附件的位置查找。

检测方法

检测病毒的方式取决于病毒类型。在扫描过程中，引擎将分析每个文件，识别类型，然后应用相关的技术。所有方法的基本原理都是查找特定类型的指令或指令的特定顺序。

模式匹配

在模式匹配技术中，引擎知道特定的代码序列，并查找将代码识别为病毒的完全匹配。更常见的是，引擎查找与已知病毒代码序列类似的代码序列，但不一定完全相同。在创建扫描过程中比较文件的说明时，Sophos 病毒研究人员努力确保以尽可能通用的方式识别代码，以便（使用启发式技术，如下所述）引擎不仅可发现原始病毒，还能发现其后续衍生物。

启发式方法

病毒引擎可结合基本模式匹配技术与启发式技术（使用通用规则而不是特定规则），由此检测相同系列的多种病毒，即使Sophos研究人员可能仅分析了该系列的一种病毒亦不例外。利用此项技术，只需创建一个描述，即可捕获一种病毒的多个变体。Sophos 可使用其他方法改动其启发式技术，将误报的可能性降到最低。

仿真

仿真是病毒引擎应用于多态病毒的一种技术。多态病毒是加密病毒，可自我修改以便隐藏自己。病毒代码没有明显固定的样式，并且该病毒每次传播时都以不同的方式对自己加密。运行时，可以自行解密。DOS 和 Windows 可执行文件中使用病毒检测引擎中的仿真程序，而多态宏病毒可通过以 Sophos 的病毒描述语言编写的检测代码发现。

此解密输出即真正的病毒代码，在仿真程序中运行它们后，Sophos 病毒检测引擎即可检测到这种输出。

发送到引擎进行扫描的可执行文件在仿真程序中运行，仿真程序可在病毒体写入内存时跟踪其解密。通常，病毒入口点位于文件前端，是要运行的首批内容。大多数情况下，只需解密少量病毒体，即可识别病毒。大多数正常可执行文件在执行几个指令后就会停止模拟，从而降低开销。

由于仿真程序在限定区域内运行，所以如果代码被证实为病毒，不会感染设备。

病毒描述

Sophos 每个月会与其他可信防病毒公司交换病毒。此外，客户每个月会直接向 Sophos 发送数千个可疑文件，其中大约 30% 被证实是病毒。每个样本都会在高度安全的病毒实验室进行严格分析，以确定其是否为病毒。对于每个新发现的病毒或病毒组，Sophos 将创建描述。

Sophos 警报

思科建议启用 Sophos 防病毒扫描的客户在 Sophos 站点 (http://www.sophos.com/virusinfo/notifications/) 上订用 Sophos 警报。从 Sophos 直接订用接收警报，可确保您了解最新的病毒爆发及其可用的解决方案。

发现病毒时

检测到病毒时，Sophos 防病毒可以修复（查杀）文件。Sophos 防病毒通常可以修复发现病毒的任何文件，在此之后即可毫无风险地使用该文件。具体采取的操作取决于病毒。

提到查杀病毒可能有所限制，因为并不总是能将文件恢复为原始状态。有些病毒会覆盖部分无法恢复的可执行程序。在这种情况下，需要定义如何处理附件可能无法修复的邮件。使用邮件安全功能可基于每个收件人配置这些设置：**邮件策略 > 传入或外发邮件策略**页 (GUI) 或 `policyconfig -> antivirus` 命令 (CLI)。有关配置这些设置的详细信息，请参阅配置面向用户的病毒扫描操作，第 259 页。

McAfee 防病毒过滤

McAfee® 扫描引擎可以：

- 通过匹配病毒签名与文件中数据的模式扫描文件。
- 在模拟环境下解密和运行病毒代码。
- 应用启发式技术以识别新的病毒。
- 从文件中删除受感染的代码。

病毒签名模式匹配

McAfee 使用防病毒定义 (DAT) 文件及扫描引擎检测特定病毒、病毒类型或其他可能不需要的软件。同时，它们还可以从文件中的已知位置开始搜索病毒签名，进而检测简单的病毒。通常，它们只需搜索文件的一小部分便可确定该文件是否未受到病毒侵害。

加密的多态病毒检测

复杂病毒通常使用两种技巧来规避签名扫描检测：

- **加密**。对病毒内的数据加密，使防病毒扫描程序看不到邮件或病毒的计算机代码。当激活病毒时，它会将自身转变为运行版本，然后执行。

- **多态**。此过程与加密类似，但病毒会自我复制，改变其外观。

为了应对此类病毒，引擎将使用仿真技术。如果引擎怀疑某个文件包含此类病毒，将创建一个人为环境，在此环境下病毒可以毫无危害地运行，直到其自我解码并显示出真正的形式。然后，引擎通常可通过扫描病毒签名识别该病毒。

启发式分析

仅使用病毒签名时，由于签名尚不可知，引擎无法检测新的病毒。因此，引擎可以使用其他技术 - 启发式分析。

携带病毒的计划、文档或邮件通常具有不同的特性。它们可能会尝试对文件进行自发修改、调用邮件客户端，或者通过其他方式进行自我复制。引擎可分析程序代码，以检测这些类型的计算机说明。此外，引擎还可搜索类似无病毒的合法行为（例如在执行操作前提示用户），由此避免引发错误警报。

通过这些技术，引擎可以检测到许多新的病毒。

发现病毒时

检测到病毒时，Sophos 防病毒可以修复（查杀）文件。Sophos 防病毒通常可以修复发现病毒的任何文件，在此之后即可毫无风险地使用该文件。具体采取的操作取决于病毒。

提到查杀病毒可能有所限制，因为并不总是能将文件恢复为原始状态。有些病毒会覆盖部分无法恢复的可执行程序。在这种情况下，需要定义如何处理附件可能无法修复的邮件。使用邮件安全功能可基于每个收件人配置这些设置：**邮件策略 > 传入或外发邮件策略**页 (GUI) 或 `policyconfig -> antivirus` 命令 (CLI)。有关配置这些设置的详细信息，请参阅配置面向用户的病毒扫描操作，第 259 页。

如何配置设备以扫描病毒

如何扫描邮件中的病毒

	请	更多信息
第 1 步	在邮件安全设备上启用防病毒扫描。	启用病毒扫描和配置全局设置，第 258 页
第 2 步	定义您想要扫描其邮件病毒的用户组。	为发件人和收件人组创建邮件策略，第 229 页
第 3 步	（可选）配置您希望病毒隔离区如何处理邮件。	配置策略、病毒和爆发隔离区，第 688 页
第 4 步	确定您希望设备如何处理带病毒的邮件。	配置面向用户的病毒扫描操作，第 259 页

	请	更多信息
第 5 步	为您定义的用户组配置防病毒扫描规则。	为不同发件人和收件人组配置防病毒策略，第 263 页
第 6 步	（可选）发送邮件以测试配置。	向设备发送邮件以测试防病毒扫描，第 266 页

启用病毒扫描和配置全局设置

在运行“系统设置向导”(System Setup Wizard)时，您可能已启用防病毒扫描引擎。无论如何，请按照以下过程配置设置。

注释 根据您的功能密钥，可以启用 Sophos、McAfee 或两者。

步骤 1 导航到**安全服务 > McAfee** 页面。

或

导航到**安全服务 > Sophos** 页面。

步骤 2 点击**启用 (Enable)**。

注释 点击**启用 (Enable)** 全局对设备启用该功能。但是，稍后必须在邮件策略中启用每个收件人的设置。

步骤 3 阅读许可协议后，滚动到页面底部并点击**接受 (Accept)** 以接受该协议。

步骤 4 点击**编辑全局设置 (Edit Global Settings)**。

步骤 5 选择最大病毒扫描超时值。

配置系统停止执行邮件防病毒扫描的超时值。默认值为 60 秒。

步骤 6 （可选）点击**启用自动更新**以启用引擎自动更新。

设备从更新服务器获取特定引擎所需的更新。

步骤 7 提交并确认更改。

下一步做什么

基于每个收件人配置防病毒设置。请参阅配置面向用户的病毒扫描操作，第 259 页。

配置面向用户的病毒扫描操作

思科设备中集成的病毒扫描引擎可根据您使用邮件安全管理器功能配置的策略（配置选项），处理传入和外发邮件中的病毒。使用邮件安全功能基于每个收件人启用防病毒操作：“邮件策略”(Mail Policies) >“传入或外发邮件策略”(Incoming or Outgoing Mail Policies) 页面 (GUI) 或 `policyconfig > antivirus` 命令 (CLI)。

邮件扫描设置

- 仅扫描病毒：

  扫描系统处理的邮件是否存在病毒。不尝试修复受感染的附件。可以选择是丢弃附件并传送包含病毒的邮件的邮件正文，还是无法修复。

- 扫描并修复病毒：

  扫描系统处理的邮件是否存在病毒。如果在附件中发现病毒，系统将尝试“修复”附件。

- 丢弃附件

  您可以选择丢弃受感染的附件。

  当防病毒扫描引擎扫描邮件受感染的附件并丢弃附件后，原附件将替换为名为“已删除附件”的新附件。附件为纯文本类型，并包含以下信息：

```
This attachment contained a virus and was stripped.
 Filename: filename
Content-Type: application/filetype
```

如果用户的邮件由于感染不安全附件而出现任何形式的修改，用户总会获得通知。您也可以配置辅助通知操作（请参阅发送通知，第 262 页）。如果选择丢弃受感染的附件，在通知用户邮件修改时，则不需要通知操作。

- X-IronPort-AV 信头

  在设备上，防病毒扫描引擎处理的所有邮件都会向邮件中添加信头 X-IronPort-AV:。在调试防病毒配置的问题时（特别是被视为“不可扫描”的邮件），此信头可为您提供更多信息。对于是否在扫描订单邮件中包括 X-IronPort-AV 信头，可以切换。建议包含此信头。

邮件处理设置

可配置病毒扫描引擎来处理侦听程序收到的四种不同类别的邮件，并为每类邮件配置单独的操作。图 - 处理病毒扫描邮件的选项总结了启用病毒扫描引擎时系统执行的操作。

对于以下每种邮件类型，可以选择要执行的操作。下面介绍了相关操作说明（请参阅配置邮件处理操作的设置，第 260 页）。例如，可以为感染病毒的邮件配置防病毒设置，这样将丢弃受感染的附件、修改邮件主题，并向邮件收件人发送自定义警报。

已修复邮件处理

如果邮件经过全面扫描且所有病毒均已修复或删除，则认为这些邮件已修复。这些邮件将按原样传送。

已加密邮件处理

如果引擎因邮件中的加密或保护字段而无法完成扫描，则认为这些邮件已加密。标记为已加密的邮件也可以修复。

请注意加密检测邮件过滤器规则（请参阅加密检测规则，第 143 页）和面向“已加密”邮件的病毒扫描操作之间的差异。对于使用 PGP 或 S/MIME 加密的任何邮件，加密的邮件过滤器规则评估为“true”。已加密规则只能检测 PGP 和 S/MIME 加密的数据。无法检测受密码保护的压缩文件或包括加密内容的 Microsoft Word 和 Excel 文档。病毒扫描引擎将受密码保护的任何邮件或附件都视为“已加密”。

注释 如果要从 AsyncOS 3.8 或更早版本升级，并已配置 Sophos 防病毒扫描，则在升级后必须配置“加密邮件的处理”部分。

不可扫描邮件的处理

如果已达到扫描超时值或引擎因内部错误而变得不可用，则认为这些邮件不可扫描。被标记为不可扫描的邮件也可以修复。

感染病毒的邮件的处理

系统可能无法丢弃附件或彻底修复邮件。在这些情况下，可以配置系统如何处理仍可能包含病毒的邮件。

加密邮件、不可扫描的邮件和病毒邮件的配置选项相同。

配置邮件处理操作的设置

要应用的操作

选择针每种类型（已加密、不可扫描或具有病毒特征）的邮件要采取的总体操作：丢弃邮件、将邮件作为新邮件的附件传送、原样传送邮件或将邮件发送到防病毒隔离区（隔离区和防病毒扫描，第 261 页）。

将设备配置为作为新邮件的附件传送受感染的邮件，这样允许收件人选择如何处理原始受感染的附件。

如果选择传送邮件或作为新邮件的附件传送该邮件，还可以进行以下操作：

- 修改邮件主题
- 存档原始邮件
- 发送常规通知 在 GUI 的“高级”部分，可执行以下操作：
- 为邮件添加自定义信头
- 修改邮件收件人

- 将邮件发送到备用目标主机
- 发送自定义警报通知

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。有关使用这些选项定义各种扫描策略的详细信息，请参阅以下部分和防病毒配置注意事项，第 264 页。

已修复邮件只有两个高级选项：添加自定义信头和发送自定义警报通知。所有其他邮件类型都能访问全部高级选项。

隔离区和防病毒扫描

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。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。

存档原始邮件

您可以将系统判定为包含（或可能包含）病毒的邮件存档到“avarchive”目录。日志文件为 mbox 格式。您必须配置“防病毒存档”日志订用，才能存档包含病毒的邮件或无法全面扫描的邮件。有关详细信息，请参阅 日志记录，第 855 页

注释 在 GUI 中，可能需要点击“高级”(Advanced) 链接，才能显示“存档原始邮件”(Archive original message) 设置。

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更改已识别邮件的文本，从而帮助用户轻松识别邮件及对识别的邮件排序。

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，如果要后加，可在添加文本 `[WARNING: VIRUS REMOVED]` 后加上几个空格。

默认文本为：

适用于修改防病毒主题行的默认主题行文本

裁定	添加到主题的默认文本
已加密	`[WARNING: MESSAGE ENCRYPTED]`

裁定	添加到主题的默认文本
受感染	[WARNING: VIRUS DETECTED]
已修复	[WARNING: VIRUS REMOVED]
不可扫描	[WARNING: A/V UNSCANNABLE]

如果任何邮件包含多个状态，将会生成一封多部分通知邮件，用来通知用户设备对邮件所执行的操作（例如，通知用户已修复邮件中的病毒，但邮件的另一部分已加密）。

发送通知

当系统判定邮件包含病毒时，可以向发件人、收件人和/或其他用户发送默认通知。在指定要通知的其他用户时，请用逗号分隔多个地址（在 CLI 和 GUI 中）。默认通知邮件如下所示：

防病毒通知的默认通知

裁定	Notification
已修复	在邮件中检测到以下病毒：<病毒名称> 执行操作：已丢弃感染的附件（或已修复感染的附件）。
已加密	由于加密，防病毒引擎无法全面扫描以下邮件。
不可扫描	防病毒引擎无法全面扫描以下邮件。
感染病毒	在邮件中检测到以下不可修复的病毒：<病毒名称>。

在邮件中添加自定义信头

可以定义额外的自定义信头，从而添加到防病毒扫描引擎扫描的所有邮件。点击**是 (Yes)**，并定义信头名称和文本。

此外，还可以创建使用 `skip-viruscheck` 操作的过滤器，以便某些邮件绕开病毒扫描。请参阅绕过防病毒系统操作，第 185 页。

修改邮件收件人

您可以修改邮件收件人，使邮件传送至其他地址。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

对于已加密、不可扫描或感染病毒的邮件，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，可以将可疑邮件路由到管理员邮箱或专门的邮件服务器，以便进行后续检查。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。

发送自定义警报通知

您可以向发件人、收件人和/或其他用户（邮件地址）发送自定义通知。为此，首先必须创建自定义通知，然后再配置设置。有关详细信息，请参阅了解文本资源，第 487 页。

图 *18:* 处理扫描病毒邮件的操作

注释 默认情况下，WHITELIST 发件人组引用的公共侦听程序所用的 $TRUSTED 邮件流策略中启用防病毒扫描。请参阅使用邮件流策略定义邮件发件人的访问规则，第 87 页。

为不同发件人和收件人组配置防病毒策略

为邮件策略编辑每个用户的防病毒设置的过程，与为传入或外发邮件编辑的过程基本相同。

各个策略（非默认策略）有一个使用“使用默认”(Use Default) 设置的额外字段。选择此设置可继承默认邮件策略的设置。

使用传入或外发邮件策略可基于每个收件人启用防病毒操作。可以在 GUI 中配置邮件策略，也可以在 CLI 中使用 policyconfig > antivirus 命令配置。在全局启用防病毒设置后，需要单独为创建的每个邮件策略配置这些操作。可以为不同的邮件策略配置不同的操作。

步骤 1 依次导航到“邮件策略”(Mail Policies) >“传入邮件策略”(Incoming Mail Policies) 或“邮件策略”(Mail Policies) >“外发邮件策略”(Outgoing Mail Policies) 页面。

步骤 2 对于要配置的策略，点击防病毒安全服务的链接。

注释 点击默认策略行中的链接，以编辑默认策略的设置。

步骤 3 点击**是 (Yes)** 或**使用默认 (Use Default)**，对该策略启用防病毒扫描。

页面中的第一个设置定义是否对该策略启用此服务。可以点击**禁用 (Disable)** 完全禁用该服务。

对于默认策略之外的邮件策略，选择“是”(Yes) 可启用已修复、已加密、不可扫描和感染病毒的邮件中的字段。

步骤 4 选择防病毒扫描引擎。可以选择 McAfee 或 Sophos 引擎。

步骤 5 配置邮件扫描设置。

有关详细信息，请参阅邮件扫描设置，第 259 页。

步骤 6 配置已修复、已加密、不可扫描和感染病毒的邮件的设置。

请参阅邮件处理设置，第 259 页 和 配置邮件处理操作的设置，第 260 页。

步骤 7 点击 **Submit**。

步骤 8 确认您的更改。

防病毒配置注意事项

丢弃附件标记会对防病毒扫描的工作方式产生很大的影响。当系统配置为“发现病毒且病毒无法修复时，丢弃受感染的附件”(Drop infected attachments if a virus is found and it could not be repaired) 时，将从邮件中清除任何病毒或不可扫描的 MIME 部分。然后，防病毒扫描的输出几乎都是正常邮件。GUI 面板中所示的为不可扫描邮件定义的操作几乎不会执行。

在“仅扫描病毒”环境中，这些操作将通过丢弃邮件不安全的部分来“清理”邮件。只有 RFC822 信头本身遭受攻击或遇到一些其他问题，才会执行不可扫描的操作。但是，如果为“仅扫描病毒”配置了防病毒扫描，但未选择“发现病毒且病毒无法修复时，丢弃受感染的附件”，则很可能执行不可扫描操作。

下表列出了一些常用的防病毒配置选项

常用的防病毒配置选项

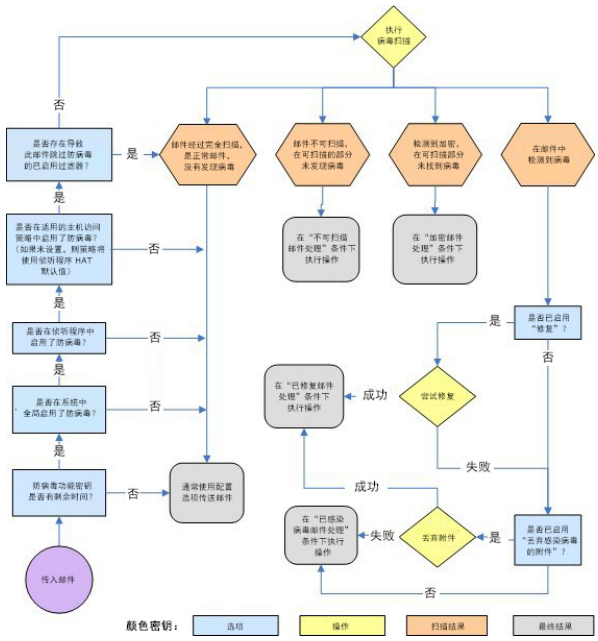
情况	防病毒配置
普遍病毒爆发 从系统中丢弃任何病毒邮件，而不进行任何其他处理。	**丢弃附件**：否 **扫描**：仅扫描 **清除病毒后的邮件**：传送 **不可扫描的邮件**：丢弃邮件 加密邮件：发送给管理员或隔离区以供审核。 病毒邮件：丢弃邮件

情况	防病毒配置
宽松策略 发送尽可能多的文档。	**丢弃附件**：是 **扫描**：扫描并修复 **清除病毒后的邮件**：[清除病毒] 并传送 **不可扫描的邮件**：作为附件转发 加密邮件：标记并转发 病毒邮件：隔离或标记并转发。
较保守型策略	**丢弃附件**：是 **扫描**：扫描并修复 **清除病毒后的邮件**：[清除病毒] 并传送 （对于更谨慎的策略，存档清除病毒后的邮件、。） **不可扫描的邮件**：发送通知、隔离或丢弃并存档。 加密邮件：标记并转发或视为不可扫描 病毒邮件：存档并丢弃
保守待审核 将可能包含病毒的邮件发送到隔离区邮箱，以便管理员能够审核内容。	**丢弃附件**：否 **扫描**：仅扫描 **清除病毒后的邮件**：传送（通常不会执行此操作） **不可扫描的邮件**：作为附件转发、alt-src-host 或 alt-rcpt-to 操作。 加密邮件：视为不可扫描 病毒邮件：转发到隔离区或管理员。

防病毒操作的流程图

下图说明防病毒操作和选项对设备处理的邮件有何影响。

图 *19:* 防病毒操作的流程图



注释 如果已配置多层防病毒扫描，则思科设备将首先使用 McAfee 引擎执行病毒扫描，其次是 Sophos 引擎。它将使用两个引擎扫描邮件，除非 McAfee 引擎检测到病毒。如果 McAfee 引擎检测到病毒，思科设备将执行为邮件策略定义的防病毒操作（修复、隔离等）。

向设备发送邮件以测试防病毒扫描

步骤 1 针对邮件策略启用病毒扫描。

使用**安全服务 > Sophos/McAfee 防病毒**页面或 `antivirusconfig` 命令设置全局设置，然后使用“邮件安全管理器”页面 (GUI) 或 `policyconfig` 的 `antivirus` 子命令配置适用于特定邮件策略的设置。

步骤 2 打开标准的文本编辑器，然后键入下列字符串，让它们单独为一行，不含空格或换行符：

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

注释 以上所示的行在文本编辑器窗口中应显示为一行，所以请确保文本编辑器窗口最大化，并删除任何换行符。此外，请务必在文本消息开头的“X5O...”中键入字母 O，而不是数字 0。

如果您正在计算机上阅读本手册，可以直接从 PDF 文件或 HTML 文件中将该行复制粘贴到文本编辑器。如果复制此行，请务必删除多余的回车或空格。

步骤 3 使用名称 **`EICAR.COM`** 保存该文件。

文件大小为 68 或 70 个字节。

注释　此文件不是病毒 - 它不会传播或感染其他文件或者损害您的计算机。但是，在完成扫描程序测试后应删除该文件，以免警报影响其他用户。

步骤 4 将文件 EICAR.COM 附加到邮件中，并将其发送到与您在步骤 1 配置的邮件策略匹配的侦听程序。

确保在该监听程序上接受您在测试邮件中指定的收件人。（有关详细信息，请参阅添加为其接受邮件的域和用户，第 113 页。）

请注意，如果在思科之外的网关（例如 Microsoft Exchange 服务器）上安装了针对外发邮件的病毒扫描软件，可能难以通过邮件发送文件。

注释　测试文件始终扫描为不可修复。

步骤 5 评估您在监听程序上为病毒扫描配置的操作，并确保它们已启用并按预期运行。

通过执行以下操作之一，可非常轻松地完成这些设置：

1. 将病毒扫描设置配置为“扫描并修复”(Scan and Repair) 模式或“仅扫描”(Scan only) 模式，不丢弃附件。
   - 发送邮件，使用 Eicar 测试文件作为附件。确认执行的操作是否与您对“感染病毒的邮件的处理”(Virus Infected Message Handling) 的配置（感染病毒的邮件的处理，第 260 页中的设置）匹配。
2. 将病毒扫描设置配置为“扫描并修复”(Scan and Repair) 模式或“仅扫描”(Scan only) 模式，丢弃附件。
   - 发送邮件，使用 Eicar 测试文件作为附件。
   - 确认执行的操作是否与您对“已修复邮件的处理”(Repaired Message Handling) 的配置（已修复邮件处理，第 260 页中的设置）匹配。

有关获取测试防病毒扫描用的病毒文件的详细信息，请参阅：http://www.eicar.org/anti_virus_test_file.htm

此页面提供4个文件以供下载。请注意，如果您已安装客户端病毒扫描软件，下载和提取这些文件可能比较困难。

更新病毒定义

关于通过 HTTP 检索防病毒更新

Sophos 和 McAfee 经常根据新确定的病毒更新其病毒定义。必须将这些更新传递到您的设备。

默认情况下，思科设备配置为每 5 分钟检查一次更新。对于 Sophos 和 McAfee 防病毒引擎，服务器通过动态网站进行更新。

只要将更新有效下载到设备中，系统在更新时就不会超时。如果更新下载由于时间太长而暂停，则下载超时。

系统等待更新完成的最长时间（超过该时间将超时）是一个动态值，定义为比防病毒更新间隔少 1 分钟（在“安全服务”(Security Services) > “服务更新”(Service Updates) 中定义）。对于下载可能超过 10 分钟才能完成的大型更新时连接较慢的设备，此配置值比较有利。

配置更新服务器设置

通过“安全服务”(Security Services) >“服务更新”(Service Updates) 页面，可配置病毒更新设置。例如，您可以配置系统接收防病毒更新的方式和检查更新的频率。有关这些其他设置的详细信息，请参阅服务更新，第 761 页。

监控和手动检查防病毒更新

您可以使用“**安全服务**”>“**Sophos**”或“**McAfee**”页面或`antivirusstatus` CLI 命令验证设备是否已安装最新防病毒引擎和身份文件，并确认最后执行更新的时间。

也可以手动执行更新请参阅 手动更新防病毒引擎，第 268 页

手动更新防病毒引擎

步骤 1 导航到“安全服务”(Security Services) >“Sophos 或 McAfee 防病毒”(Sophos or McAfee Anti-Virus) 页面。

步骤 2 点击“当前 McAfee/Sophos 防病毒文件”(Current McAfee/Sophos Anti-Virus Files) 表中的**立即更新 (Update Now)**。

设备将检查并下载最新更新。

下一步做什么

此外，也可以在命令行界面中使用 antivirusstatus 和 antivirusupdate 命令配置此操作

验证设备上的防病毒文件是否已更新

您可以查看更新程序日志，验证是否已成功下载、提取或更新防病毒文件。使用 tail 命令可显示更新程序日志订用的最后条目，确保已获取病毒更新。

第 13 章

反垃圾邮件

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，您可能希望删除已确认的垃圾邮件，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。

注释 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，第 56 页。

反垃圾邮件解决方案

您的思科设备提供以下反垃圾邮件解决方案：

- IronPort 反垃圾邮件过滤，第 271 页.
- 思科智能多重扫描过滤，第 273 页.

可以在思科设备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。

将设备配置为扫描邮件以检测垃圾邮件的方法

过程

	命令或操作	目的
步骤 1	在邮件安全设备上启用反垃圾邮件扫描。	注释 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 Cisco IronPort 反垃圾邮件和智能多扫描的功能密钥，则可以在设备上启用这两个解决方案。 • IronPort 反垃圾邮件过滤，第 271 页 • 思科智能多重扫描过滤，第 273 页
步骤 2	配置是在本地邮件安全设备上隔离垃圾邮件，还是使用安全管理设备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，第 702 页 • 使用外部垃圾邮件隔离区，第 970 页
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，第 229 页
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，第 275 页
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，第 184 页
步骤 6	（推荐）为每个入站邮件流量策略启用 SenderBase 信誉服务评分，即使不根据 SenderBase 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，第 93 页。

	命令或操作	目的
步骤 7	如果邮件安全设备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，第 286 页
步骤 8	避免设备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设备生成的邮件，第 281 页
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，第 328 页
步骤 10	测试配置。	测试反垃圾邮件，第 294 页
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，第 761 页 • 通过代理服务器进行更新，第 765 页 • 配置服务器设置以下载升级和更新，第 765 页

IronPort 反垃圾邮件过滤

试用版密钥

思科设备附带了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，第 31 页），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，第 752 页。）

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。

国际地区的垃圾邮件扫描

思科反垃圾邮件在全球都有效，并且使用区域特定的内容感知威胁检测技术。还可以使用地区规则配置文件，为特定地区优化反垃圾邮件扫描。

- 如果从美国以外的特定地区收到大量垃圾邮件，则可能需要使用地区规则配置文件来帮助阻止来自该地区的垃圾邮件。

  例如，中国大陆和中国台湾地区会收到繁体中文或简体中文占较高百分比的垃圾邮件。中文地区规则针对此类垃圾邮件进行了优化。如果您主要接收中国大陆、中国台湾地区和中国香港特别行政区的邮件，则思科强烈建议使用反垃圾邮件引擎附带的中文地区规则配置文件。

- 如果垃圾邮件主要来自美国或没有特定地区，请不要启用地区规则，因为这样做可能降低对其他类型的垃圾邮件的捕获率。这是因为，地区规则配置文件针对特定地区优化反垃圾邮件引擎。

在配置 IronPort 反垃圾邮件扫描时，可以启用地区规则配置文件。

配置 IronPort 反垃圾邮件扫描

注释 在系统设置期间启用了 IronPort 反垃圾邮件时，它会用于默认传入邮件策略，并且对全局设置使用默认值。

准备工作

- 确定是否使用区域扫描。请参阅国际地区的垃圾邮件扫描，第 272 页。

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) 点击**启用 (Enable)**。

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

步骤 3 点击**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，将以全局方式为设备启用该功能。

步骤 5 要优化设备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	1. 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3MB。更大的值可能导致性能降低。 2. 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10MB。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。 **注释** 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	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。
地区扫描 (Regional Scanning)	启用或禁用区域扫描，并选择一个地区（如果适用）。 仅当从指定地区接收大量邮件时，才可启用该功能。由于此功能可针对特定地区优化反垃圾邮件引擎，因此会降低对其他类型垃圾邮件的捕获率。

步骤 6 提交并确认更改。

思科智能多重扫描过滤

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设备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。

配置思科智能多重扫描

注释 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。

准备工作

激活此功能的功能密钥。请参阅功能密钥，第 752 页。仅当您执行了此操作后，才会看到 IronPort 智能多重扫描选项。

步骤 1 依次选择**安全服务 (Security Services) > IronPort 智能多扫描 (IronPort Intelligent Multi-Scan)**。

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) 点击**启用 (Enable)**。

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

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

步骤 4 选中**启用 IronPort 智能多扫描 (Enable IronPort Intelligent Multi-Scan)** 对应的复选框。

选中此复选框，将以全局方式为设备启用该功能。但是，仍然必须在邮件策略中启用按收件人的设置。

步骤 5 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。
- 绝不扫描 1M 或更大的邮件。

步骤 6 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。

大多数用户不需要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设备的吞吐量。

步骤 7 提交并确认更改。

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。

可以为默认传入和外发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

- 完成将设备配置为扫描邮件以检测垃圾邮件的方法，第 270 页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，第 277 页
  - 配置示例：针对肯定是垃圾邮件与疑似垃圾邮件的操作，第 278 页
  - 来自合法源的不需要的营销邮件，第 278 页
  - 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，第 279 页
  - 在反垃圾邮件扫描期间添加的信头，第 281 页
- 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，第 855 页。
- 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，第 179 页。

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) > 外发邮件策略 (Outgoing Mail Policies)** 页面。

步骤 3 点击邮件策略的**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 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	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： • 投递 • 丢弃 • 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，第 179 页。
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。 **注释** 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	可以将自定义信头添加到识别的邮件。 点击**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，第 278 页。
（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。 点击**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。

选项	说明
垃圾邮件阈值	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。

下一步做什么

如果为外发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，第 87 页。

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分数。然后，将分数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（更严格的配置）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，您可能希望删除“已确认的”垃圾邮件，但隔离“疑似”垃圾邮件。

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 （严格）	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
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

严格策略的示例仅标记疑似垃圾邮件，同时删除确认的垃圾邮件。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，第 232 页。

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。请参阅管理灰色邮件，第 297 页。

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，以便在收件人点击邮件中的链接时，将通过思科网络安全代理服务（该服务会评估点击时的网站安全性，并阻止访问已知的恶意网站）路由请求。

准备工作

启用 URL 过滤功能及其必备条件。请参阅设置 URL 过滤，第 328 页。

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 > 传入邮件策略**。
b) 点击**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) 点击**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) 点击 **Add Filter**。
c) 将过滤器命名为 url_redirect。
d) 点击**添加条件 (Add Condition)**。
e) 点击**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) 点击 **OK**。
i) 点击**添加操作 (Add Action)**。
j) 点击 **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) 点击 **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 > 传入邮件策略**。
b) 点击**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。

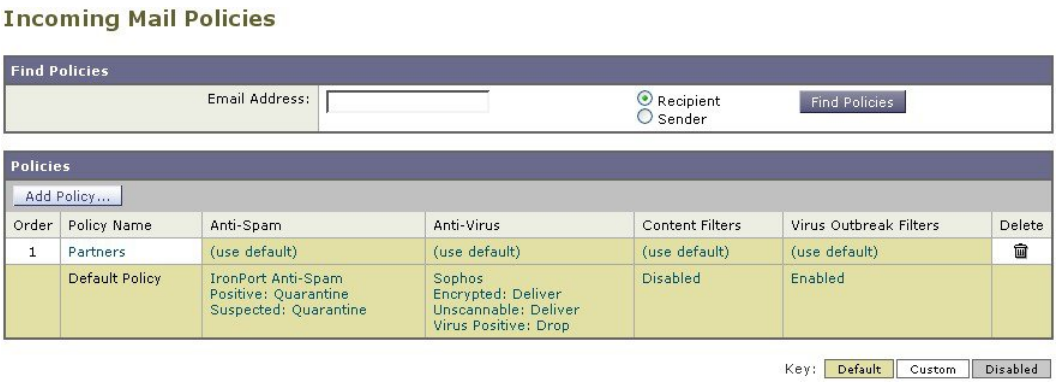
在不同的邮件策略中启用不同的反垃圾邮件扫描引擎：配置示例

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。

图 *20:* 邮件策略 - 按收件人的反垃圾邮件引擎

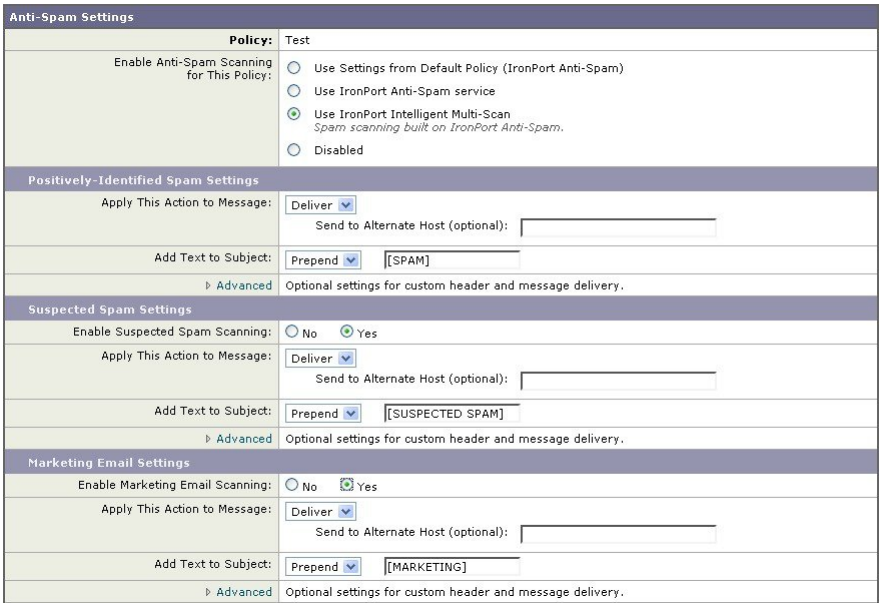


要将“合作伙伴”(Partners) 策略更改为使用思科智能多重扫描，并扫描不需要的营销邮件，请点击“反垃圾邮件”(Anti-Spam) 列中与“合作伙伴”(Partners) 行（“use default”）对应的条目。

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。

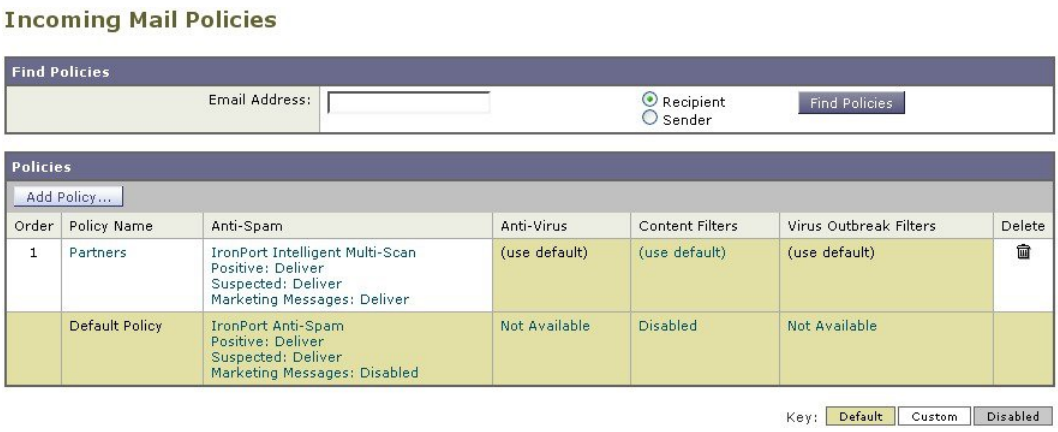
下图显示了在某个策略中启用的思科智能多重扫描和不需要的营销邮件检测。

图 *21:* 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：

图 *22:* 邮件策略 - 在策略中启用智能多扫描



避免垃圾邮件过滤器过滤设备生成的邮件

由于思科 IronPort 设备自动发送的邮件（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，第 229 页和绕过反垃圾邮件系统操作，第 184 页。

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，第 275 页。

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

如何向思科报告分类错误的邮件

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。

步骤 1 为组织中的所有设备设置通用注册 ID。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。

1. 使用 Web 界面登录到您的设备。
2. 转到**系统管理** > **邮件提交和跟踪门户注册**。
3. 如果您的设备是集群的一部分，请将该模式设置为集群级别。
4. 点击**设置注册 ID**。
5. 在**注册 ID** 字段中输入值。您输入的值必须至少包含 16 个字符，但是最多不能超过 48 个字符，且只能包含字母数字字符、连字符 (-) 和下划线 (_)。
6. 提交并确认更改。
7. 如果您的设备不是集群的一部分，则必须对组织中的所有设备重复第 1 步到第 6 步。

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

步骤 2 可以通过以下任一方式在思科邮件提交和跟踪门户上注册为管理员：思科邮件提交和跟踪门户是一个基于 Web 的工具，允许邮件管理员将分类错误的邮件报告给思科并跟踪它们。

注释 思科邮件提交和跟踪门户是一个基于 Web 的工具，允许邮件管理员将分类错误的邮件报告给思科并跟踪它们。

- 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. 使用思科凭据登录到思科 SecurityHub (https://securityhub.cisco.com/)。
  2. 点击**邮件提交和跟踪**。
  3. 在邮件提交和跟踪门户网站上，选择**注册新的注册 ID**，输入您在**第 1 步**中创建的注册 ID，然后点击**注册**。确保您在此处输入的注册 ID 与您在设备上配置邮件提交和跟踪门户设置时输入的注册 ID 相同。

- 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. 使用思科凭据登录到思科 SecurityHub (https://securityhub.cisco.com/)。
  2. 点击**邮件提交和跟踪**。
  3. 在邮件提交和跟踪门户网站上，选择**注册为管理员**，输入已在门户中注册的管理员的邮件地址，然后点击**注册**。

点击“注册”后，将向已在门户上注册的管理员发送邮件通知。管理员需要登录到门户，然后点击配置面板中的**管理注册请求**以允许或拒绝注册请求。

步骤 3 将您的域注册到思科邮件提交和跟踪门户。

1. 转到思科邮件提交和跟踪门户。
2. 点击**配置** > **域**。
3. 点击**添加新域**。
4. 输入组织的域，然后点击**添加**。

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。

添加域的请求将发送到`postmaster@domain.com`，其中 domain.com 是您在此步骤中输入的域。来自此域的管理员必须审核并批准您的请求。

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（在所有设备上），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"); }
```

如何向思科报告分类不正确的邮件

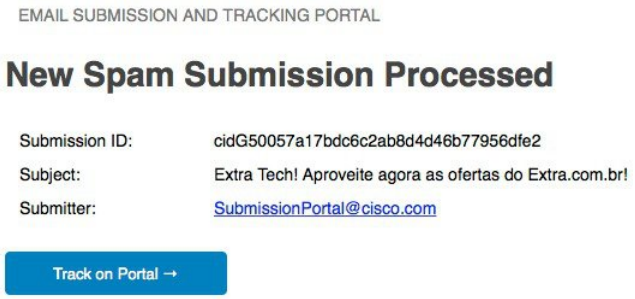
有关详细信息，请参阅https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200648-ESA-FAQ-How-to-work-with-Cisco-Email-Su.html。

步骤 1 执行如何向思科报告分类错误的邮件，第 282 页的**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，第 284 页
- 使用思科邮件提交和跟踪门户，第 284 页
- 将分类错误的邮件作为附件进行转发，第 285 页

向思科报告分类不正确的邮件后，您会在两个小时内收到邮件通知。下面是一个邮件通知示例：



如果在两个小时内未收到邮件通知，您的提交可能已失败。有关故障排除说明，请点击门户上的**帮助** > **故障排除说明**。

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（邮件管理员和终端用户）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。

使用思科邮件提交和跟踪门户

思科邮件提交和跟踪门户网站是一个基于 Web 的工具，允许邮件管理员向思科报告分类不正确的邮件。管理员还可以使用该门户跟踪其组织提交的内容。

注释 当前，只能使用该门户报告分类不正确的垃圾邮件。

步骤 1 使用您的思科凭证登录到思科 SecurityHub (https://securityhub.cisco.com/)。

步骤 2 点击**邮件提交和跟踪**。

步骤 3 在邮件提交和跟踪门户的**提交**选项卡下，点击**新建提交**。

步骤 4 选择分类不正确的邮件。这些邮件必须采用 EML 格式，并且邮件的总体大小不得超过 15 MB。

步骤 5 点击**创建**。

下一步做什么

更多信息

有关思科邮件提交和跟踪门户的详细信息，请参阅以下文档：

方法	请参阅
使用邮件提交和跟踪门户向思科报告分类错误的邮件	https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117822-qanda-esa-00.html
使用思科邮件提交和跟踪门户	https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200648-ESA-FAQ-How-to-work-with-Cisco-Email-Su.html
思科邮件提交和跟踪门户故障排除	https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200653-ESA-FAQ-Troubleshooting-Email-Submissio.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 附件转发到以下地址：

- 错过的垃圾邮件 - spam@access.ironport.com
- 标记为垃圾邮件但却不是垃圾邮件的邮件 - ham@access.ironport.com
- 错过的营销邮件 - ads@access.ironport.com
- 标记为营销邮件但却不是营销邮件的邮件 - not_ads@access.ironport.com
- 错过的网络钓鱼邮件 - phish@access.ironport.com

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，可以在思科邮件提交和跟踪门户网站上查看和跟踪邮件提交。

步骤 1 使用思科凭证登录思科 SecurityHub (https://securityhub.cisco.com/)。

步骤 2 点击**邮件提交和跟踪**。

步骤 3 在邮件提交和跟踪门户网站上，点击**提交**。

步骤 4 使用过滤器（“持续时间”、“提交 ID”、“主题”、“提交者”和“状态”）来查找您的提交。

下一步做什么

有关详细信息，请参阅https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200648-ESA-FAQ-How-to-work-with-Cisco-Email-Su.html.。

通过传入中继确定部署中的发件人 IP 地址

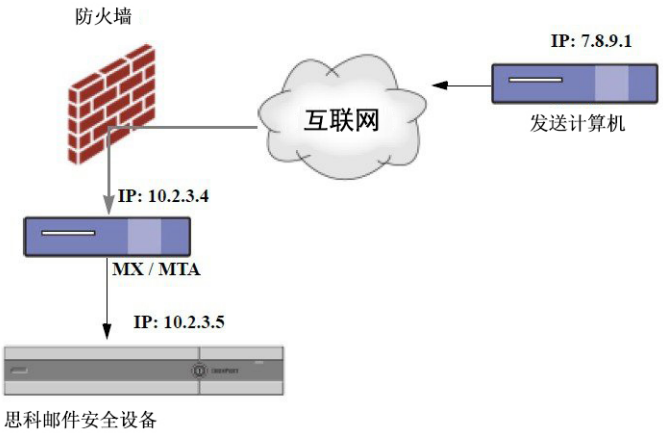
如果一个或多个邮件交换/传输代理（MX 或 MTA）、过滤服务器等位于网络边缘，且在思科设备与发送传入邮件的外部计算机之间，则设备无法确定发送计算机的 IP 地址。相反，邮件看似来自本地 MX/MTA。但是，IronPort 反垃圾邮件和思科智能多扫描（使用 SenderBase 信誉服务）取决于外部发件人的准确 IP 地址。

解决方案是将设备配置为使用传入中继。指定连接到思科设备的所有内部 MX/MTA 的名称和 IP 地址，以及用于存储来源 IP 地址的信头。

具有传入中继的环境示例

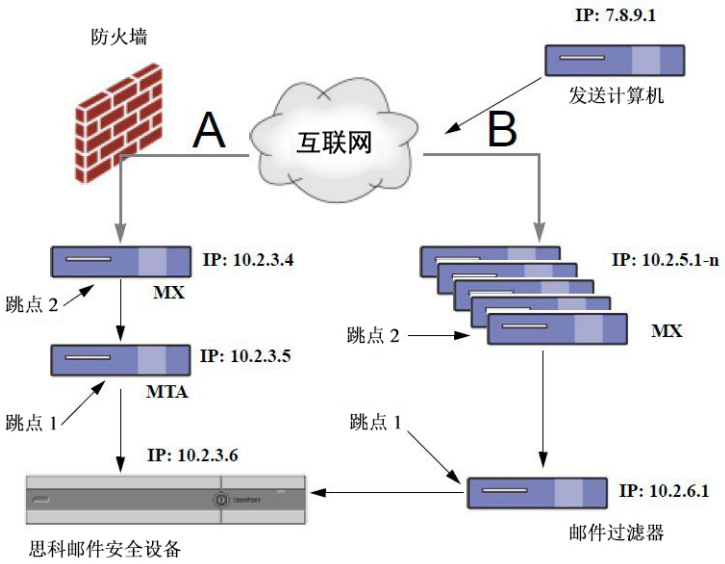
下图显示了一个非常基本的传入中继示例。从 IP 地址 7.8.9.1 发来的邮件看似是从 IP 地址 10.2.3.4 发来，因为本地 MX/MTA 正在向思科设备中继邮件。

图 *23*: 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思科设备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思科设备之前通过 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，然后在传送到思科设备之前发送到任意一个 MX。

图 *24:* 通过 *MX/MTA* 中继的邮件 - 高级



配置设备以使用传入中继

启用传入中继功能

注释 仅当本地 MX/MTA 将邮件中继到思科设备时，才能启用传入中继功能。

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

步骤 2 点击**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安全设备的每台计算机，以及
- 将标记原始外部发件人的 IP 地址的信头。

准备工作

有关完成这些必备条件所需的信息，请参阅中继邮件的邮件信头，第 289 页。

- 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。

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

步骤 2 点击**添加中继 (Add Relay)**。

步骤 3 输入中继的名称。

步骤 4 输入连接到邮件安全设备的 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。

下一步做什么

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，第 292 页。
- 为便于跟踪和故障排除，请配置设备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，第 293 页。

中继邮件的邮件信头

将设备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

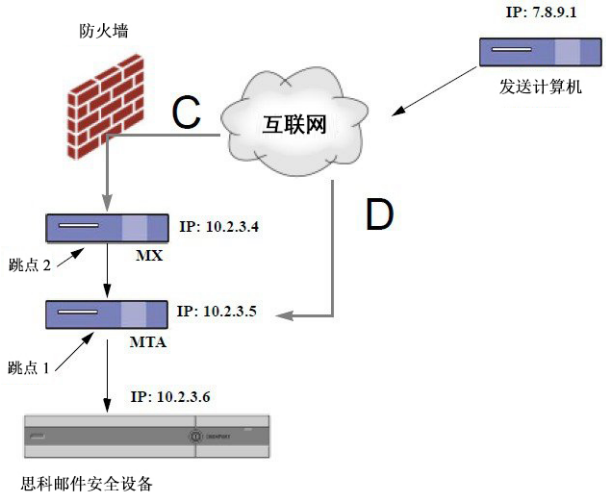
建议的识别原始发件人的方法是使用自定义信头。连接到原始发件人的计算机需要添加此自定义信头。信头的值应是外部发送计算机的 IP 地址。例如：

```
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。

图 *25: MX/MTA* 中继的邮件 - 可变跳数



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“已接收:”(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）到达连接到思科设备的计算机，则必须使用自定义信头（请参阅自定义信头，第 289 页）。

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（由思科设备接收不计为一跳。有关更多信息，请参阅配置日志以指定要

使用的信头，第 293 页）。AsyncOS 会在与指定的跳数对应的 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，则会解析从思科设备向后数第二个 Received: 信头。如果没有找到解析字符和有效的 IP 地址，思科设备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思科设备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（被思科设备忽略），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。

表 *34:* 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：

- 思科设备会忽略这些信头。
- 思科设备收到邮件（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。
- 思科设备会忽略这些 Microsoft Exchange 信头。

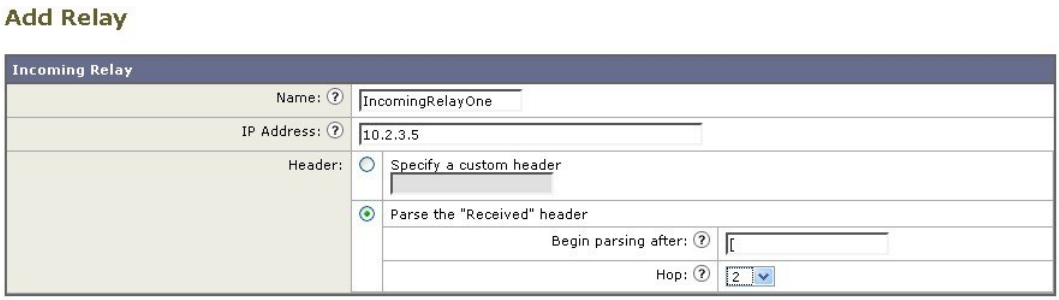
下表显示了同一邮件的信头，没有外来信头

表 *35:* 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）：

图 *26:* 配置的具有已接收信头的传入中继



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 SenderBase 信誉得分提供各种 SenderBase 信誉服务相关的过滤器规则（reputation、no-reputation）。

传入中继、HAT、SBRS 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 SenderBase 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，设备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）进入邮件安全设备。设备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至发件人组。

传入中继和跟踪

跟踪会在跟踪结果中显示传入中继的 SenderBase 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。
- SenderBase 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 SenderBase 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 SenderBase 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 SenderBase 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 SBRS 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, **SBRS 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

思科设备只检查在收到邮件时存在的信头。因此，在本地添加的（例如 Microsoft Exchange 信头等）或思科设备接收邮件时添加的附加信头不会进行处理。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，第 898 页。

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。

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 依次选择**安全服务 (Security Services) > IronPort 智能多扫描 (IronPort Intelligent Multi-Scan)**。

步骤 3 查看**规则更新 (Rule Updates)** 部分和：

目标	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)。

目标	更多信息
查看更新是否可用	-
如果更新可用，则更新规则	点击 **Update Now**。

测试反垃圾邮件

目标	请	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，第 275 页）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。请参阅向设备发送邮件以测试思科反垃圾邮件，第 294 页。 • 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，第 935 页。
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，第 295 页。

向设备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，第 295 页中的示例。

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 检查测试帐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？
- 邮件是否已被删除？

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 SBRS、黑名单、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。

第 14 章

管理灰色邮件

本章包含以下部分：

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。

邮件安全设备中的灰色邮件管理解决方案

邮件安全设备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点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，第 298 页），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**

灰色邮件分类

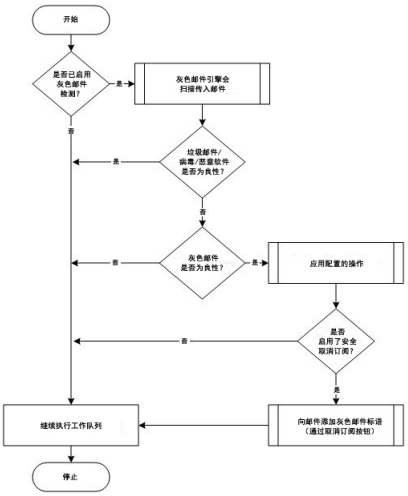
灰色邮件引擎将每封灰色邮件分类为以下类别之一：

- **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：

图 *27:* 灰色邮件管理解决方案工作流程



工作流程

步骤 1 邮件安全设备接收传入邮件。

步骤 2 邮件安全设备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 邮件安全设备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 邮件安全设备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 邮件安全设备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 邮件安全设备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。

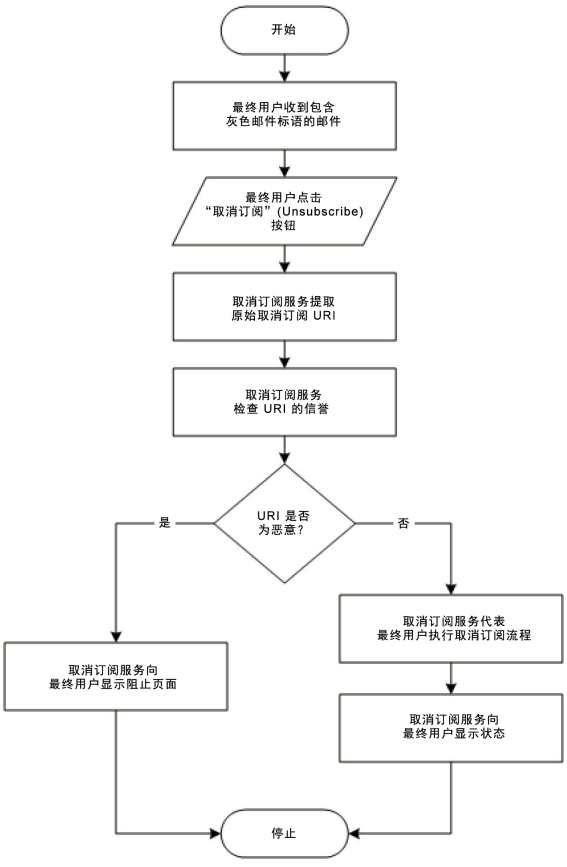
步骤 7 邮件安全设备会将具有取消订用按钮的横幅添加到邮件。此外，邮件安全设备会重写邮件正文中的现有取消订用链接。

步骤 8 邮件安全设备通过其邮件工作队列的后续阶段处理邮件。

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。

图 *28:* 安全取消订用工作流程



工作流程

步骤 1 最终用户收到包含灰色邮件标语的邮件。

步骤 2 最终用户点击“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 的声誉，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。可以启用 IronPort 反垃圾邮件，也可以启用智能多扫描功能。请参阅 反垃圾邮件，第 269 页
- 对于安全取消订用，
  - 添加安全取消订用功能键。
  - 终端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

准备工作

满足灰色邮件检测和安全取消订用的要求，第 300 页。

步骤 1 依次点击**安全服务 (Security Services)** > **检测和安全取消订用 (Detection and Safe Unsubscribe)**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

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

步骤 4 （可选）要优化设备的吞吐量同时仍可扫描由灰色邮件发件人发送的不断增加的邮件，请配置邮件扫描的阈值：

- 希望设备扫描的最大邮件大小。
- 扫描邮件时等待超时的秒数。

步骤 5 （可选）点击**启用自动更新**以启用引擎自动更新。

设备从更新服务器获取特定引擎所需的更新。

步骤 6 选中**启用安全取消订用 (Enable Safe Unsubscribe)**。

步骤 7 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 graymailconfig 命令。有关详细信息，请参阅《适用于思科邮件安全设备的 *AsyncOS* 的 *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，第 301 页

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

步骤 2 点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
- 启用安全取消订用的
- 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。

  注释 设备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

注释　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

注释　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

注释　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，邮件安全设备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。

下一步做什么

注释　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《适用于思科邮件安全设备的 *AsyncOS* 的 *CLI* 参考指南》。

在灰色邮件扫描过程中添加的 X-IronPort-PHdr 信头

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

- 在设备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，则在设备上全局启用了灰色邮件引擎时，仍会将 X-IronPort-PHdr 信头添加到所有邮件。

X-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 X-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)	每个灰色邮件类别（营销、社交和批量）下的传入灰色邮件数量以及灰色邮件总数。	“概述”页面，第 641 页
“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，第 644 页
“传入邮件”(Incoming Mail) 页面 > “传入邮件详细信息”(Incoming Mail Details)	对于所有 IP 地址、域名称或网络所有者，每个灰色邮件类别（营销、社交和批量）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）	对于指定 IP 地址、域名称或网络所有者，每个灰色邮件类别（营销、社交和批量）下的传入灰色邮件数量以及灰色邮件总数。	

报告	包含以下灰色邮件数据	更多信息
“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，第 651 页
“内部用户”(Internal Users) 页面 > “用户邮件流详细信息”(User Mail Flow Details)	对于所有用户，每个灰色邮件类别（营销、社交和批量）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）	对于指定用户，每个灰色邮件类别（营销、社交和批量）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，转至**安全服务 (Security Service)** > **灰色邮件检测和安全取消订用 (Graymail Detection and Safe Unsubscribing)** 页面，然后点击**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**灰色邮件检测和安全取消订用**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

当最终用户点击取消订用链接时，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，第 299 页）。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，第 332 页。

终端用户安全列表

如果贵组织中的终端用户为他们自己的邮件帐户配置了安全列表，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，第 705 页。

查看日志

灰色邮件检测和安全取消订阅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阅添加标语的信息。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阅进行故障排除

无法执行安全取消订用

问题

点击“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帐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。

第 15 章

病毒爆发过滤器

本章包含以下部分：

病毒爆发过滤器概述

病毒爆发过滤器既能保护您的网络免受大规模病毒爆发，又能在出现小规模非病毒攻击时防御它们，例如网络钓鱼、诈骗和恶意软件传播。大多数防恶意软件安全软件在收集数据及发布软件更新之前无法检测新爆发，而思科与之不同，我们可在爆发传播时收集相关数据并实时向您的邮件安全设备发送更新信息，从而阻止这些邮件到达用户。

思科使用全局流量模式开发规则，由此确定传入邮件安全还是爆发的一部分。可能属于爆发的邮件将被隔离，直到根据思科更新的爆发信息或 Sophos 和 McAfee 发布的新防病毒定义，确定它们安全为止。

小规模、非病毒攻击的邮件采用外观合法的设计、收件人的信息和指向网络钓鱼及恶意软件网站的自定义 URL，这些自定义 URL 仅短期有效，且网络安全服务无法识别。爆发过滤器可分析邮件内容，并搜索 URL 链接以检测此类非病毒攻击。爆发过滤器可以重写 URL，通过网络安全代理将流量重定向到可能有害的网站，由此警告用户其尝试访问的网站可能是恶意的，或者完全阻止该网站。

病毒爆发过滤器工作原理

延迟、重定向和修改邮件

爆发过滤器功能使用三种方法保护您的用户免受爆发：

- **延迟**。爆发过滤器隔离可能属于病毒爆发或非病毒攻击的邮件。隔离后，设备将会收到更新的爆发信息并重新扫描邮件以确认它是否属于攻击。
- **重定向**。爆发过滤器重写非病毒攻击邮件中的 URL，以便在收件人尝试访问任何链接的网站时，通过思科网络安全代理重定向他们。如果网站仍在运行，代理将显示启动画面，警告用户该网站可能包含恶意软件；如果网站已经下线，将显示错误消息。有关重定向 URL 的详细信息，请参阅重定向 URL，第 310 页。
- **修改**。除了重写非病毒威胁邮件中的URL之外，爆发过滤器还可以修改邮件主题和在邮件正文上方添加免责声明，以警告用户注意邮件内容。有关详细信息，请参阅修改邮件，第 311 页。

威胁类别

爆发过滤器功能可防御两类基于邮件的爆发：病毒爆发，即邮件附件中包含前所未见的病毒；以及非病毒威胁，其中包括网络钓鱼尝试、诈骗和恶意软件传播，通过链接传播到外部网站。

默认情况下，爆发过滤器在爆发期间会扫描传入和外发邮件中的潜在病毒。如果在设备上已启用反垃圾邮件扫描，则除了病毒爆发之外，还可对非病毒威胁启用扫描。

注释 要让爆发过滤器扫描非病毒威胁，设备需要一个功能密钥以用于反垃圾邮件或智能多次扫描。

病毒爆发

在对抗病毒爆发时，爆发过滤器功能可为您提供领先优势。如果邮件附件包含前所未见的病毒，或现有病毒的变体通过专用网络和互联网快速传播，则会发生爆发。由于这些新病毒或变体进入互联网，所以从病毒发布到防病毒供应商发布更新的病毒定义，这段时间窗口最为关键。预先通知 - 即使只有几个小时，对于遏制恶意软件或病毒的传播也至关重要。在该漏洞时段，新发现的病毒可能全局传播，导致邮件基础设施中断服务。

网络钓鱼、恶意软件传播和其他非病毒威胁

包含非病毒威胁的邮件，其设计看起来与合法来源的邮件很像，而且通常是发送给少量收件人。为了看起来可靠，这些邮件可能具有以下一个或多个特征：

- 收件人的联系信息。
- 旨在模仿合法来源（例如社交网络和在线零售商）邮件的 HTML 内容。
- URL 指向使用新 IP 地址且仅短期上线的网站，也就是说，邮件和网络安全服务没有关于该网站的充足信息来确定其是否属于恶意网站。
- URL 指向 URL 缩短服务。

所有这些特性，使得这些邮件更加难以被作为垃圾邮件检测到。爆发过滤器功能提供对这些非病毒威胁的多层防御，以防用户下载恶意软件或向可疑新网站提供个人信息。

如果 CASE 发现邮件中存在 URL，则将该邮件与现有爆发规则比较，以确定该邮件是否属于小规模非病毒爆发，然后分配威胁级别。根据威胁级别，邮件安全设备将延迟传送给收件人，直到收集到更多威胁数据；如果收件人尝试访问网站，设备将重写邮件中的 URL，以便将收件人重定向到思科网络安全代理。代理将显示启动页面，警告用户该网站可能包含恶意软件。

思科安全智能运营中心

思科安全智能运营中心 (SIO) 是一种安全生态系统，它将全球威胁信息、基于信誉的服务和复杂分析连接到思科安全设备，从而提供更强大的保护，并缩短响应时间。

SIO 由三个组件组成：

- SenderBase、全球最大的威胁监控网络和漏洞数据库。
- 威胁操作中心 (TOC)一支安全分析师和自动化系统全球团队，提取由 SenderBase 收集的切实可行的情报。
- 动态更新。发生爆发时，自动将实时更新传送到设备。

SIO 会比较全球 SenderBase 网络提供的实时数据与常规流量模式，以识别被证实为爆发征兆的异常。TOC 将审查数据并发布潜在爆发的威胁级别可能的爆发。思科邮件安全设备下载更新的威胁级别和爆发规则，并使用它们来扫描传入和外发邮件，以及爆发隔离区中已有的邮件。

有关当前病毒爆发的信息，请参阅以下 SenderBase 网站：

http://www.senderbase.org/

SIO 网站提供当前的非病毒威胁列表，包括垃圾邮件、网络钓鱼和恶意软件传播尝试：

http://tools.cisco.com/security/center/home.x

上下文自适应扫描引擎

病毒爆发过滤器由思科独特的情景自适应扫描引擎 (CASE) 提供支持。CASE 根据对邮件威胁的实时分析，定期利用自动调整的 100,000 多个自适应邮件属性。

对于病毒爆发，CASE 可分析邮件内容、上下文和结构，以便准确确定可能的自适应规则触发器。CASE 可以结合自适应规则与 SIO 发布的实时爆发规则，共同评估每封邮件并分配唯一的威胁级别。

要检测非病毒威胁，CASE 可扫描邮件中的 URL，如果发现一个或多个 URL，可使用 SIO 的爆发规则评估邮件的威胁级别。

根据邮件的威胁级别，CASE 将给出隔离邮件的时间建议，以防爆发。此外，CASE 还可决定重新扫描间隔，这样即可根据来自 SIO 的更新爆发规则重新评估邮件。威胁级别越高，越经常重新扫描隔离的邮件。

从隔离区释放邮件后，CASE 也会对它们重新扫描。如果 CASE 在重新扫描后确定某封邮件是垃圾邮件或包含病毒，可以重新将其隔离。

有关 CASE 的详细信息，请参阅思科反垃圾邮件：概述 ，第 271 页。

延迟邮件

从发生爆发或邮件攻击到软件供应商发布更新的规则，这段期间是您的网络和用户最容易受到攻击的时段。在此段时间内，现代病毒可以全局传播，恶意网站可以传送恶意软件或收集用户的敏感信息。爆发过滤器通过在限定时段内隔离可疑邮件，可保护您的用户和网络，并为思科和其他供应商提供时间调查新的爆发。

发生病毒爆发时，带附件的可疑邮件将被隔离，直到更新的爆发规则和新的防病毒签名证明邮件附件正常或属于病毒。

小规模、非病毒威胁包含的指向恶意网站的URL可能是短期上线，以便规避网络安全服务检测；或者通过URL缩短服务在中间放置可靠的网站，由此规避网络安全。通过隔离包含符合威胁级别阈值的 URL 的邮件，CASE 不仅有机会基于来自 SIO 的更新爆发规则重新评估邮件内容，而且这些邮件可以在隔离区保留足够长的时间，直到链接的网站下线或被网络安全解决方案阻止。

有关爆发过滤器如何隔离可疑邮件的详细信息，请参阅动态隔离，第 314 页。

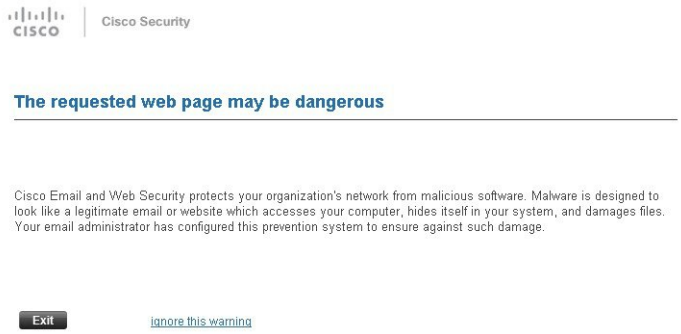
重定向 URL

当 CASE 在爆发过滤器阶段扫描邮件时，除了其他可疑内容以外，它还会搜索邮件正文中的 URL。CASE 使用发布的爆发规则来评估邮件是否属于威胁，然后为该邮件评定适当的威胁级别。根据威胁级别，爆发过滤器将通过以下方式来保护收件人：重写所有 URL（指向绕行域的 URL 除外），将收件人重定向到思科网络安全代理，并延迟邮件传送，以便TOC详细了解出现在更大爆发中的网站。有关绕行受信任的域的 URL 的详细信息，请参阅URL 重写和绕行域，第 322 页。

在邮件安全设备释放并传送邮件后，系统将通过思科网络安全代理重定向收件人访问网站的任何尝试。这是由思科托管的外部代理，如果网站仍在运行，它将显示启动画面，警告用户该网站可能具有危险。如果该网站已下线，启动画面将显示错误消息。

如果收件人决定点击邮件的URL，思科网络安全代理将在用户的Web浏览器中显示启动画面，警告该用户注意邮件的内容。下图显示启动画面警告的示例。收件人可以点击**忽略此警告 (Ignore this warning)** 继续访问网站，也可以点击**退出 (Exit)** 离开并安全关闭浏览器窗口。

图 *29*: 思科安全启动画面警告 *(proxy_splash_screen)*



要访问思科网络安全代理，只能通过重写邮件中 URL。通过在 Web 浏览器中键入 URL，无法访问该代理。

注释 您可以自定义此启动画面的外观，并显示您所在组织的品牌，例如公司徽标、联系信息等。请参阅自定义最终用户访问恶意站点时看到的通知，第 332 页。

提示 要将可疑垃圾邮件中的所有 URL 重定向到思科 Web 安全代理服务，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，第 278 页。

修改邮件

爆发过滤器功能可以修改非病毒威胁邮件的邮件正文，不仅是重写 URL，还可提示用户该邮件是可疑威胁。爆发过滤器功能可以修改主题信头，也可以在邮件正文上方添加关于邮件内容的免责声明。有关详细信息，请参阅邮件修改，第 321 页。

通过“邮件策略”(Mail Policies) >“文本资源”(Text Resources) 页面的免责声明模板，可创建威胁免责声明。有关详细信息，请参阅文本资源管理概述，第 488 页。

规则的类型：自适应和病毒爆发

爆发过滤器使用两类规则来检测潜在爆发：自适应和爆发。爆发过滤器功能使用这两个规则集提供效果最高、标准最集中的威胁检测，以确保过滤器可聚焦于特定爆发。爆发过滤器规则和操作对于管理员可见，而不是隐藏在幕后，由此可即时访问隔离的邮件及其被隔离的原因。

爆发规则

爆发规则由威胁操作中心 (TOC) 生成，威胁操作中心是思科安全情报运营中心的一部分，注重邮件整体，而不是附件文件类型。爆发规则使用 SenderBase 数据（实时和历史流量数据）及邮件参数的任意组合（例如附件文件类型、文件名称关键字或防病毒引擎更新）实时识别和防御爆发。系统会为爆发规则指定一个唯一 ID，用来在 GUI 的各个位置引用规则（例如爆发隔离区）。

然后，比较来自全球 SenderBase 网络的实时数据与此基准，以识别证实为爆发征兆的异常。TOC 可审查数据并发布威胁指标或威胁级别。威胁级别是一个介于 0（无威胁）和 5（非常危险）之间的数值（非常危险），衡量邮件是威胁的可能性（因为思科客户尚未针对其广泛部署任何其他网关防御）（有关详细信息，请参阅威胁级别，第 312 页）。威胁级别由 TOC 作为爆发规则发布。

爆发规则中可以合并的一些示例特征包括：

- 文件类型、文件类型和大小、文件类型和文件名关键字等
- 文件名关键字和文件大小
- 文件名关键字
- 邮件 URL
- 文件名和 Sophos IDE

适应规则

自适应规则是 CASE 内的一组规则，可精确比较邮件属性与已知病毒爆发邮件的属性。这些规则是在学习大量病毒资料库内的已知威胁邮件和已知正常邮件后创建的。自适应规则通常随着资料库评估而更新。它们与现有的爆发规则相互补充，确保始终检测爆发邮件。虽然爆发规则在可能出现爆发时才生效，但自适应规则（一旦启用）“始终有效”，在本地捕获爆发邮件，然后在全局基础上

形成完整的异常。此外，自适应规则可持续响应邮件流量和结构中的细微变化，面向客户提供更新的保护。

病毒爆发

基本上，病毒爆发过滤器规则就是威胁级别（例如威胁级别4），与一组邮件和附件的特征相关联，例如文件大小、文件类型、文件名、邮件内容等。例如，假设思科 SIO 发现携带 .exe 附件的可疑邮件数量越来越多，附件大小为 143 KB，且文件名中包括特定关键字（例如“hello”）。于是，系统发布了爆发规则，提高与此条件匹配的邮件的威胁级别。默认情况下，您的设备每隔 5 分钟就检查一次新发布的爆发和自适应规则，并进行下载（请参阅更新爆发过滤器规则，第 319 页）。自适应规则更新的频率比爆发规则小。在设备上，设置隔离可疑邮件的阈值。如果某封邮件的威胁级别等于或超过隔离阈值，则将该邮件发送到爆发隔离区。此外，还可以设置修改非病毒威胁邮件的阈值，重写可疑邮件中发现的任何 URL 或在邮件正文顶部添加通知。

威胁级别

下表 为其中每个级别提供一系列基本指导原则或定义。

Level	风险	含义
0	无	没有任何邮件威胁风险。
1	低	邮件是威胁的风险较低。
2	低/中	邮件是威胁的风险为低到中等。这是“可疑”威胁。
3	中等	邮件属于确认的爆发，或其内容构成威胁的风险为中等到巨大。
4	高	邮件已确认属于大规模爆发，或其内容非常危险。
5	极高	邮件内容已确认属于极大规模、大规模和极其危险的爆发。

有关威胁级别和爆发规则的详细信息，请参阅病毒爆发过滤器规则，第 318 页。

设置隔离区威胁级别阈值的指导原则

通过隔离区威胁级别阈值，管理员可以加大或减小隔离可疑邮件的积极性。设置越低（1或2）表示积极性越高，将隔离更多邮件；相反，分数越高（4或5），积极性越低，且只能隔离极大可能是恶意的邮件。

同一阈值既适用于病毒爆发，也适用于非病毒威胁，但可以为病毒攻击和其他威胁指定不同的隔离区保留时间。有关详细信息，请参阅动态隔离，第 314 页。

思科建议使用默认值 3。

容器：“特定”和“始终”规则

容器文件是包含其他文件的压缩 (.zip) 存档文件。TOC 可以发布处理存档文件中特定文件的规则。

例如，如果 TOC 确定某个病毒爆发包含带 .exe 文件的 .zip 文件，则会发布特定爆发规则，由此设置 .zip 文件内 .exe 文件的威胁级别 (.zip(exe))，但不会为 .zip 文件内包含的任何其他文件类型（例如 .txt 文件）设置威胁级别。第二规则 (.zip(*)) 涵盖该容器文件类型中的所有其他文件类型。容器总是使用“始终”(Always) 规则来计算邮件的威胁级别，而不考虑容器内的文件类型。如果已知所有这类容器类型都具有危险，SIO 则会发布一项始终规则。

表 *36:* 回退规则和威胁级别得分

爆发规则	爆发等级	说明
.zip(exe)	4	此规则集为 .zip 文件中的 .exe 文件设置威胁级别 4。
.zip(doc)	0	此规则集为 .zip 文件中的 .doc 文件设置威胁级别 0。
zip(*)	2	此规则集为所有 .zip 文件设置威胁级别 2，不考虑其中包含的文件类型。

病毒爆发过滤器功能的工作原理

设备在处理邮件时，邮件将通过一系列步骤，即“邮件管道”（有关邮件管道的详细信息，请参阅了解邮件通道，第 51 页）。如果为该邮件策略启用了反垃圾邮件和防病毒扫描引擎，则在邮件通过邮件管道继续处理时，将运行这些引擎。换句话说，病毒爆发过滤器功能不会扫描已知垃圾邮件或包含已识别病毒的邮件，因为系统已根据您的反垃圾邮件和防病毒设置，将这些邮件从邮件流中删除 - 删除、隔离等。因此，抵达病毒爆发过滤器功能的邮件已被标记为无垃圾邮件和病毒。请注意，根据更新的垃圾邮件规则和病毒定义，从隔离区放行及由 CASE 重新扫描被病毒爆发过滤器隔离的邮件时，可能会再次将其标记为垃圾邮件或包含病毒。

注释 因过滤器或引擎被禁用而跳过反垃圾邮件和防病毒扫描的邮件，仍要接受爆发过滤器扫描。

邮件得分

如果新的病毒攻击或非病毒威胁释放而肆虐，任何防病毒或反垃圾邮件软件都还无法识别该威胁，这正是爆发过滤器功能发挥重大价值的所在。CASE将使用发布的爆发和自适应规则扫描传入邮件，并对其评分（请参阅规则的类型：自适应和病毒爆发，第 311 页）。邮件得分与其威胁级别相对应。CASE 根据邮件匹配的规则（如有）分配相应的威胁级别。如果没有关联的威胁级别（邮件与任何规则都不匹配），则为邮件分配威胁级别 0。

一旦完成该计算，邮件安全设备将检查该邮件的威胁级别是否符合或超过隔离或邮件修改阈值，并隔离邮件或重写其 URL。如果威胁级别低于阈值，将继续传送该邮件以便在管道中进一步进行处理。

此外，CASE会对照最新规则重新评估当前隔离的邮件，以确定邮件的最新威胁级别。这样可确保，只在隔离区内保留威胁级别与爆发邮件一致的邮件，而不再构成威胁的邮件经过自动重新评估后将离开隔离区。

如果一封爆发邮件有多个得分 - 一个得分来自自适应规则（或为多个自适应规则适用时的最高得分），另一个得分来自爆发规则（或为多个爆发规则适用时的最高得分），则使用智能算法来确定最终威胁级别。

可以使用病毒爆发过滤器功能，而不在设备上启用防病毒扫描。两种安全服务的宗旨是相辅相成，但也可以独立工作。也就是说，如果没有在设备上启用防病毒扫描，您则需要监控防病毒供应商的更新，并手动放行或重新评估爆发隔离区的部分邮件。使用病毒爆发过滤器而未启用防病毒扫描时，请牢记以下事项：

- 应该禁用自适应规则
- 将根据爆发规则来隔离邮件
- 如果威胁级别降低或时间过期，邮件将被放行

下游防病毒供应商（桌面/组件）可能会捕获放行的邮件。

注释 要通过病毒爆发过滤器功能扫描非病毒威胁，需要在设备上全局启用反垃圾邮件扫描。

动态隔离

爆发过滤器功能的爆发隔离区是用来临时存储邮件的区域，直到邮件被确认为威胁或可安全传送给用户为止。（有关详细信息，请参阅病毒爆发生命周期和规则发布，第 315 页。）可通过多种方式释放爆发隔离区中隔离的邮件。下载新规则后，系统将根据 CASE 计算的推荐重新扫描间隔，重新扫描爆发隔离区中的邮件。如果某封邮件修订的威胁级低于隔离区保留阈值，则会自动放行该邮件（不考虑爆发隔离区的设置），由此尽可能地减少其在隔离区中耗费的时间。如果在重新评估邮件时有新规则发布，则会重新启动重新扫描。

请注意，当新的防病毒签名可用时，不会从病毒爆发隔离区自动放行作为病毒攻击隔离的邮件。新规则可能会引用新的防病毒签名，也可能不会引用；但邮件不会由于防病毒引擎更新而被放行，除非爆发规则将该邮件的威胁级别改为低于威胁级别阈值的得分。

此外，在 CASE 建议的保留期限过后，也会从爆发隔离区释放邮件。CASE 根据邮件的威胁级别计算保留期限。您可以为病毒爆发和非病毒威胁定义独立的最长保留时间。如果 CASE 建议的保留时间超过该威胁类型的最长保留时间，邮件安全设备将在最长保留时间过后释放邮件。病毒邮件的默认最长隔离期限为 1 天。非病毒威胁的默认隔离期限为 4 小时。您可以手动从隔离区释放邮件。

另外，如果隔离区已满且有更多邮件插入（这种情况称为“溢出”），邮件安全设备也会放行邮件。只有爆发隔离区的容量达到 100%，并有新邮件添加到隔离区时，才会发生溢出。此时，将按以下优先顺序放行邮件：

- 自适应规则隔离的邮件（计划尽快放行的邮件优先）
- 爆发规则隔离的邮件（计划尽快释放的邮件优先）

一旦爆发隔离区的容量低于 100%，则停止溢出释放。有关如何处理隔离区溢出的详细信息，请参阅邮件在隔离区中的保留时间，第 687 页和自动处理的隔离邮件的默认操作，第 688 页。

如果为邮件策略启用了防病毒和反垃圾邮件引擎，则这些引擎将对从爆发隔离区释放的邮件重新扫描。如果邮件现在被标记为已知病毒或垃圾邮件，则会按照邮件策略设置进行处理（包括可能再次

被病毒隔离区或垃圾邮件隔离区隔离）。有关详细信息，请参阅病毒爆发过滤器功能和病毒爆发隔离区，第 323 页。

因此，需要注意的是，在邮件的生命期限内，它实际上可能被隔离两次 - 一次是由于爆发过滤器功能，一次是从爆发隔离区释放时。如果两次扫描（在爆发过滤器之前和从爆发隔离区释放时）的判定相符，则不会再次隔离邮件。另请注意，爆发过滤器功能不会对邮件采取任何最终操作。爆发过滤器功能将隔离邮件（以便进一步处理），或将邮件移至管道中的下一个步骤。

病毒爆发生命周期和规则发布

在病毒爆发生命周期的早期阶段，系统使用更广泛的规则来隔离邮件。随着越来越多的信息变得可用，发布的规则越来越突出重点，从而缩小了对隔离内容的定义。发布新规则后，不再被视为潜在病毒邮件的邮件将从隔离区中放行（发布新规则时，会重新扫描爆发隔离区中的邮件）。

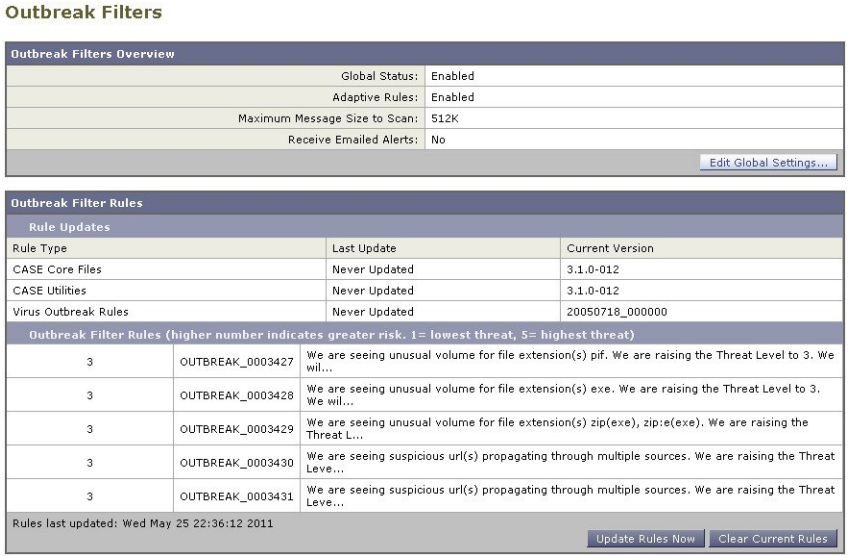
表 *37:* 病毒爆发生命周期的规则示例

时间	规则类型	规则描述	操作
T=0	自适应规则（基于过去的爆发）	根据 100K 以上的邮件属性合并的规则集，用于分析邮件内容、上下文和结构	如果邮件与自适应规则匹配，则自动隔离邮件。
T=5 min	爆发规则	隔离包含 .zip (exe) 文件的邮件	隔离属于包含 .exe 的 .zip 的所有附件
T=10 min	爆发规则	隔离包含的 .zip (exe) 文件超过 50 KB 的邮件	如果任何邮件包含的 .zip (exe) 文件小于 50 KB，将从隔离区放行
T=20 min	爆发规则	隔离 .zip (exe) 文件介于 50 到 55 KB 之间且文件名中包含“Price”的邮件	不符合此条件的任何邮件将从隔离区放行。
T=12 hours	爆发规则	对照新签名扫描	对照最新的防病毒签名扫描所有剩余的邮件

管理病毒爆发过滤器

登录到图形用户界面 (GUI)，选择菜单中的“安全服务”(Security Services)，然后点击“爆发过滤器”(Outbreak Filters)。

图 *30*: 病毒爆发过滤器主页



“爆发过滤器”(Outbreak Filters) 页面显示两部分：爆发过滤器概况和当前爆发过滤器规则的列表（如有）。

在上图中，已启用病毒爆发过滤器、自适应扫描，并且最大邮件大小设置为 512k。要更改这些设置，请点击**编辑全局设置 (Edit Global Settings)** 有关编辑全局设置的详细信息，请参阅配置病毒爆发过滤器全局设置，第 316 页。

“爆发过滤器规则”(Outbreak Filter Rules) 部分列出各种组件（规则引擎以及规则本身）最新更新的时间、日期和版本，以及当前的爆发过滤器规则及威胁级别列表。

有关爆发规则的详细信息，请参阅病毒爆发过滤器规则，第 318 页。

配置病毒爆发过滤器全局设置

步骤 1 依次点击**安全服务 (Security Services)** > **爆发过滤器 (Outbreak Filters)**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 根据您的要求，执行以下操作：

- 全局启用爆发过滤器
- 启用自适应规则扫描
- 设置要扫描的文件的最大大小（请注意要以字节为单位输入大小）
- 启用爆发过滤器警报
- 启用网络交互跟踪请参阅Web 互动跟踪，第 330 页。

步骤 4 提交并确认更改。

下一步做什么

此功能还可通过 outbreakconfig CLI 命令（请参阅《适用于思科邮件安全设备的 AsyncOS CLI 参考指南》。做出更改后，请提交并确认更改。

注释 无法使用 Web 界面启用 URL 的日志记录。有关使用 CLI 启用 URL 日志记录的说明，请参阅启用 URL 日志记录和 URL 邮件跟踪详细信息，第 317 页。

启用病毒爆发过滤器功能

要全局启用病毒爆发过滤器功能，请选中“爆发过滤器全局设置”(Outbreak Filters Global Settings) 页面“启用爆发过滤器”(Enable Outbreak Filters) 旁边的复选框，然后点击**提交 (Submit)**。您必须首先同意病毒爆发过滤器许可协议。

一旦全局启用，则可以针对每个传入和外发邮件策略（包括默认策略）单独启用或禁用病毒爆发过滤器功能。有关更多信息，请参阅爆发过滤器功能和邮件策略，第 319 页。

病毒爆发过滤器功能使用情景自适应扫描引擎 (CASE) 检测病毒威胁，不考虑是否启用反垃圾邮件扫描，但要扫描非病毒威胁，则确实要在设备上全局启用反垃圾邮件或智能多次扫描。

注释 如果您尚未在系统设置期间同意许可（请参阅第 4 步：安全，第 35 页），则必须在“安全服务”(Security Services) > “爆发过滤器”(Outbreak Filters) 页面上点击**启用 (Enable)**，然后阅读并同意许可。

启用自适应规则

自适应扫描支持在病毒爆发过滤器中使用自适应规则。如果与邮件内容相关的病毒签名或垃圾邮件条件不可用，则使用一组因素或特征（文件大小等）来确定邮件属于爆发的可能性。要启用自适应扫描，请选中“爆发过滤器全局设置”(Outbreak Filters Global Settings) 页面“启用自适应规则”(Enable Adaptive Rules) 旁边的复选框，然后点击**提交 (Submit)**。

启用病毒爆发过滤器的警报

选中标记为“邮件警报”的框，以启用病毒爆发过滤器功能警报。启用病毒爆发过滤器启用邮件警告，只是让警报引擎发送有关病毒爆发过滤器的警报。通过“系统管理”(System Administration) 选项卡的“警报”(Alerts) 页面，指定发送的以及配置的邮件地址。有关配置爆发过滤器警报的详细信息，请参阅警报、SNMP 陷阱和病毒爆发过滤器，第 325 页。

启用 URL 日志记录和 URL 邮件跟踪详细信息

默认情况下，将禁止记录与URL相关的日志，并禁止在邮件跟踪详细信息中显示此信息。其中包括以下事件的日志：

- 邮件中与 URL 类别过滤器匹配的任何 URL 的类别
- 邮件中与 URL 信誉过滤器匹配的任何 URL 的信誉得分

- 爆发过滤器将重写邮件中的任何 URL

要启用这些事件的日志记录，请在命令行界面 (CLI) 中使用 outbreakconfig 命令。

示例：使用 outbreakconfig 命令启用 URL 的日志记录

以下示例展示如何使用 outbreakconfig 命令启用 URL 的日志记录

```
mail.example.com> outbreakconfig

Outbreak Filters: Enabled

Choose the operation you want to perform:

- SETUP - Change Outbreak Filters settings.

[]> setup

Outbreak Filters: Enabled

Would you like to use Outbreak Filters? [Y]>

Outbreak Filters enabled.

Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or back
down below), meaning that new messages of

certain types could be quarantined or will no longer be quarantined, respectively.

Would you like to receive Outbreak Filter alerts? [N]>

What is the largest size message Outbreak Filters should scan?

[524288]>

Do you want to use adaptive rules to compute the threat level of messages? [Y]>

Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> Y

Logging of URLs has been enabled.

The Outbreak Filters feature is now globally enabled on the system.  You must use the
'policyconfig' command in the CLI or the Email

Security Manager in the GUI to enable Outbreak Filters for the desired Incoming and Outgoing
 Mail Policies.

Choose the operation you want to perform:

- SETUP - Change Outbreak Filters settings.

[]>
```

病毒爆发过滤器规则

爆发规则由思科安全情报运营中心发布，设备每隔 5 分钟将检查一次新爆发规则，并进行下载。此更新间隔可以更改。有关详情，请参见配置服务器设置以下载升级和更新，第 765 页。

管理爆发过滤器规则

由于系统自动下载爆发过滤器规则，所以实际上并不需要用户进行任何管理。

但是，如果您的设备一段时间后由于某种原因无法访问思科的更新服务器获取新规则，可能是本地缓存的得分失效，例如某个已知病毒附件类型在防病毒软件中已更新和/或不再构成威胁时。这时，您可能希望不再隔离具有这些特征的邮件。

可以点击**立即更新规则 (Update Rules Now)**，从思科更新服务器手动下载更新的爆发规则。

注释 **立即更新规则 (Update Rules Now)** 按钮不会“刷新”设备上所有现有的爆发规则，只是替换更新的爆发规则。如果思科的更新服务器上没有可用的更新，点击此按钮时，设备则不会下载任何爆发规则。

更新爆发过滤器规则

默认情况下，设备每隔 5 分钟尝试下载一次新爆发过滤器规则。通过“安全服务”(Security Services) >“服务更新”(Service Updates) 页面，可更改此间隔。有关详细信息，请参阅服务更新，第 761 页。

爆发过滤器功能和邮件策略

爆发过滤器功能包含可根据邮件策略进行的设置。在设备上，可针对每个邮件策略启用或禁用爆发过滤器功能。根据邮件策略，可对特定文件扩展名和域免于执行爆发过滤器功能处理。此功能还可以通过 policyconfig CLI 命令（请参阅《适用于思科邮件安全设备的 AsyncOS 的 CLI 参考指南》）获取。

注释 要通过爆发过滤器功能扫描非病毒威胁，需要在设备上全局启用反垃圾邮件或智能多次扫描。

要修改特定邮件策略的爆发过滤器功能设置，请点击要更改策略“爆发过滤器”(Outbreak Filters) 列中的链接。

要启用和自定义特定邮件策略的爆发过滤器功能，请选择**启用爆发过滤器 (自定义设置) (Enable Outbreak Filtering (Customize Settings))**。

可以为邮件策略配置以下爆发过滤器设置：

- 隔离区威胁级别
- 隔离区最长保留时间
- 立即传送非病毒威胁邮件，而不将其添加到隔离区
- 绕行的文件扩展名类型
- 邮件修改阈值
- 使用自定义文本和爆发过滤器变量修改主题信头，例如 $threat_verdict、$threat_category、$threat_type、$threat_description 和 $threat_level。
- 包括以下邮件信头：

- X-IronPort-Outbreak-Status
- X-IronPort-Outbreak-Description

- 将邮件发送到备用目标，例如邮件安全设备或交换服务器。
- URL 重写
- 威胁免责声明

选择**启用爆发过滤 (继承默认邮件策略设置) (Enable Outbreak Filtering (Inherit Default mail policy settings))**,可使用为默认邮件策略定义的爆发过滤器设置。如果默认邮件策略已启用爆发过滤器功能，则所有其他邮件策略将使用相同的爆发过滤器设置，除非已进行自定义。

进行更改后，请确认您的更改。

设置隔离区级别阈值

从列表中选择适用于爆发威胁的隔离区威胁级别阈值。数字越小,表示隔离的邮件越多；而数字越大，隔离的邮件越少。思科建议使用默认值 3。

有关详细信息，请参阅设置隔离区威胁级别阈值的指导原则 ，第 312 页。

隔离区最长保留时间

指定邮件留在爆发隔离区的最长时间。对于可能包含病毒附件的邮件和可能包含网络钓鱼或恶意软件链接等其他威胁的邮件，可以指定不同的保留时间。对于非病毒威胁，选中**传送邮件而不将其添加到隔离区 (Deliver messages without adding them to quarantine)** 复选框可立即传送邮件，而不将其添加到隔离区。

注释 除非已为策略启用“邮件修改”(Message Modification)，否则无法隔离非病毒威胁。

CASE 建议在向邮件分配威胁级别时设置隔离区保留期限。在 CASE 建议的时间内，邮件安全设备将保持隔离邮件，除非建议的时间超出隔离区适用于其威胁类型的最长保留时间。

绕过文件扩展名类型

您可以修改策略以绕行特定文件类型。CASE 计算邮件的威胁级别时，不含绕行的文件扩展名；但附件仍由其余邮件安全管道处理。

要绕行某个文件扩展名，请点击“绕行附件扫描”(Bypass Attachment Scanning)，选择或键入文件扩展名，然后点击**添加扩展名 (Add Extension)**。AsyncOS 在“绕行的文件扩展名”(File Extensions to Bypass) 列表中显示扩展名类型。

要从绕行的扩展名列表中删除某个扩展名，请在“绕行的文件扩展名”(File Extensions to Bypass) 列表中点击该文件扩展名旁边的垃圾桶图标。

绕过文件扩展名：容器文件类型

绕行文件扩展名时，如果扩展名在绕行的扩展名列表中，将绕行容器文件中的相关文件（例如 .zip 文件中的 .doc 文件）。例如，如果将 .doc 添加到绕行的扩展名列表中，则绕过所有 .doc 文件，即便它们在容器文件内亦不例外。

邮件修改

如果希望设备扫描网络钓鱼尝试或恶意软件网站链接等非病毒威胁，请启用“邮件修改”(Message Modification)。

根据邮件的威胁级别，AsyncOS 可以修改邮件以重写所有 URL，从而通过思科网络安全代理重定向收件人（如果他们尝试打开邮件中的网站）。另外，设备也可以在邮件中添加免责声明，以提示用户邮件内容可疑或是恶意的。

要隔离非病毒威胁邮件，需要启用邮件修改。

邮件修改威胁等级

从列表中选择一个邮件修改威胁级别阈值。此设置决定是否根据 CASE 返回的威胁级别修改邮件。数字越小，表示要修改的邮件越多；而数字越大，表示要修改的邮件越少。思科建议使用默认值3。

邮件主题

对于包含已修改链接的非病毒威胁邮件，可以改动其主题信头文本，以便通知用户为了提供保护已对邮件进行修改。在主题信头前面或后面加上自定义文本、病毒爆发过滤器变量，例如：`$threat_verdict`、`$threat_category`、`$threat_type`、`$threat_description` 和 `$threat_level`，或者两者的组合。要插入变量，请点击**插入变量 (Insert Variables)** 并从变量列表中选择。

“邮件主题”(Message Subject) 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，如果要前加，可在添加文本 `[MODIFIED FOR PROTECTION]` 后加上几个空格。

注释 “邮件主题”(Message Subject) 字段仅接受 US-ASCII 字符。

病毒爆发过滤器邮件信头

可以向邮件中添加以下附加信头：

标头	格式	示例	选项
X-IronPort-Outbreak-Status	`X-IronPort-Outbreak-Status: $threat_verdict, level $threat_level, $threat_category - $threat_type`	`X-IronPort-Outbreak-Status: Yes, level 4, Phish - Password`	• 对所有邮件启用 (Enable for all messages) • 仅为非病毒爆发启用 (Enable only for non-viral outbreak) • 禁用

标头	格式	示例	选项
X-IronPort-Outbreak-Description	`X-IronPort-Outbreak-Description: $threat_description`	`X-IronPort-Outbreak-Description: It may trick victims into submitting their username and password on a fake website.`	• 启用 • 禁用

注释 如果要根据这些信头过滤邮件，则必须将爆发过滤器处理的邮件发回到邮件安全设备（通过配置备用目标邮件主机），然后使用与这些信头匹配的内容过滤器扫描它们。

备用目标邮件主机

如果要对爆发过滤器处理的邮件执行基于内容过滤器的扫描，则必须将爆发过滤器配置为：将处理的邮件发回到邮件安全设备。这是因为，在处理管道中先进行内容过滤器扫描，然后才执行爆发过滤器扫描。

在**备用目标邮件主机 (Alternate Destination Mail Host)** 字段中，输入要发送处理的邮件（以供进一步扫描）的设备的 IP 地址（IPv4 或 IPv6）或 FQDN。

URL 重写和绕行域

如果邮件的威胁级别超过邮件修改阈值，则爆发过滤器功能将重写邮件中的所有 URL，以便在用户点击其中任意URL时将他们重定向到思科网络安全代理的启动页面。（有关详细信息，请参阅重定向 URL，第 310 页。）如果邮件的威胁级别超过隔离阈值，设备还会隔离该邮件。如果正在发生小规模、非病毒爆发，隔离邮件会让TOC有时间分析可能是爆发的邮件中链接的任何可疑网站，并确定网站是否是恶意的。CASE 使用 SIO 发布的更新爆发规则重新扫描邮件，以确定它是否属于爆发。在保留期限到期后，设备将从隔离区释放邮件。

AsyncOS 重写邮件中的所有 URL，指向绕行域的 URL 除外。

要重写 URL，可使用以下选项：

- **对未签名的邮件启用 (Enable only for unsigned messages)**。此选项允许 AsyncOS 重写未签名邮件中符合或超出邮件修改阈值的 URL，但不含签名的邮件。思科建议对于 URL 重写使用此设置。

注释 如果在网络中由邮件安全设备之外的服务器或设备负责验证 DomainKeys/DKIM 签名，则邮件安全设备可以重写DomainKeys/DKIM 签名的邮件中的 URL，并废弃邮件的签名。

设备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。

- **对所有邮件启用 (Enable for all messages)**。此选项允许 AsyncOS 重写所有邮件中符合或超出邮件修改阈值的 URL，包括签名的邮件。如果 AsyncOS 修改签名的消息，签名将失效。
- **禁用 (Disable)**。此选项将禁用爆发过滤器的 URL 重写。

可以修改策略以排除修改特定域的 URL。要绕过域，请在“绕过域扫描”(Bypass Domain Scanning) 字段中输入 IPv4 地址、IPv6 地址、CIDR 范围、主机名，部分主机名或域。使用逗号分隔多个条目。

绕过域扫描功能与URL过滤使用的全局白名单类似，但与之无关。有关该白名单的详细信息，请参阅创建 URL 过滤的白名单，第 331 页。

威胁免责声明

邮件安全设备可以在可疑邮件标题上方附加免责声明消息，以警告用户注意其内容。根据邮件类型，此免责声明可以是 HTML 或纯文本形式。

从“威胁免责声明”(Threat Disclaimer) 列表中选择要使用的免责声明文本；或点击“邮件策略”(Mail Policies) > “文本资源”(Text Resources) 链接，使用免责声明模板创建新免责声明。免责声明模板包括用于爆发威胁信息的变量。点击“预览免责声明”(Preview Disclaimer)，可以查看威胁免责声明预览。对于自定义免责声明消息，可以使用变量显示邮件中的威胁级别、威胁类型和威胁说明。有关创建免责声明消息的信息，请参阅文本资源管理概述，第 488 页。

病毒爆发过滤器功能和病毒爆发隔离区

爆发过滤器功能隔离的邮件将发送到爆发隔离区。此隔离区的功能与任何其他隔离区类似（有关使用隔离区的详细信息，请参阅集中化的策略、病毒和病毒爆发隔离区，第 685 页），但此隔离区具有“摘要”(summary) 视图，该视图对于根据在隔离区中放置邮件所用的规则，从隔离区删除或释放所有邮件非常有用（对于爆发规则，显示爆发 ID；对于自适应规则，显示通用术语）。有关摘要视图的详细信息，请参阅病毒爆发隔离区和“按规则摘要管理”视图，第 324 页。

监控病毒爆发隔离区

虽然执行任何监控时正确配置的隔离区需求很少，但最好留意爆发隔离区，特别是在病毒爆发期间或之后，这段时间合法邮件可能被延迟。

如果某个合法邮件被隔离，则根据爆发隔离区的设置，会出现下列情况之一：

- 如果隔离区的“默认操作”(Default Action) 设置为“放行”(Release)，当保留期限到期或隔离区溢出时将放行该邮件。您可以配置爆发隔离区，以便在邮件因溢出而被放行之前，对其执行以下操作：拆离附件、修改主题和添加X-Header。有关这些操作的详细信息，请参阅自动处理的隔离邮件的默认操作，第 688 页。
- 如果隔离区的“默认操作”(Default Action) 设置为“删除”(Delete)，当保留期限到期或隔离区溢出时将删除该邮件。
- 如果隔离区已满，再添加更多邮件，将会发生溢出。在这种情况下，将首先放行距到期日期最近的邮件（不一定是时间最长的邮件），直到为新邮件留出充足的空间。您可以配置爆发隔离区，以便在邮件因溢出而被放行之前，对其执行以下操作：拆离附件、修改主题、添加X-Header。

由于只要发布新规则就会重新扫描隔离的邮件，所以爆发隔离区中的邮件很可能在到期时间之前就被放行。

但是，如果“默认操作”(Default Action) 设置为“删除”(Delete)，监控爆发隔离区仍然非常重要。思科建议大多数用户不要将默认操作设置为“删除”(Delete)。有关从爆发隔离区放行邮件或更改爆发隔离区默认操作的详细信息，请参阅自动处理的隔离邮件的默认操作，第 688 页。

相反，如果您的爆发隔离区中包含邮件，假如在等待新规则更新时希望延长它们在隔离区中的保留期限，可以延迟这些邮件的到期时间。切记，延长邮件的保留时间可能导致隔离区变大。

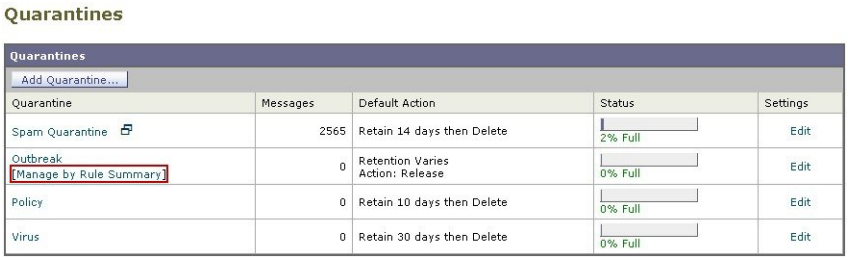
注释 如果已全局禁用防病毒扫描（并非通过邮件策略），而爆发隔离区中包含邮件，则在该邮件离开隔离区时不会对其执行防病毒扫描，即使在该邮件离开隔离区之前重新启用防病毒扫描亦不例外。

注释 可以使用病毒爆发过滤器功能，而不在设备上启用防病毒扫描。但是，如果设备上未启用反垃圾邮件扫描，病毒爆发过滤器则无法扫描非病毒威胁。

病毒爆发隔离区和“按规则摘要管理”视图

在 GUI 中，点击“监控”(Monitor) 菜单中列出的隔离区名称，可查看爆发隔离区的内容。爆发隔离区也有一个额外视图，即爆发隔离区的“按规则摘要管理”(Manage by Rule Summary) 链接。

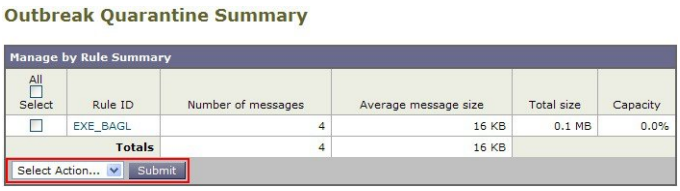
图 *31:* 爆发隔离区的“按规则摘要管理”*(Manage by Rule Summary)* 视图



使用摘要视图可根据规则 **ID** 对爆发隔离区中的邮件执行邮件操作。

点击“按规则摘要管理”(Manage by Rule Summary) 链接，可按规则 ID 分组查看爆发隔离区的内容列表：

图 *32:* 爆发隔离区的“按规则摘要管理”*(Manage by Rule Summary)* 视图



在此视图中，可以选择释放、删除或延迟与特定爆发或自适应规则相关的所有邮件的退出，而不必逐个选择邮件。此外，也可以在列表中搜索或对其排序。

通过 quarantineconfig -> outbreakmanage CLI 命令也可以使用此功能。有关详细信息，请参阅适用于思科邮件安全设备的 AsyncOS 的 CLI 参考指南。

监控病毒爆发过滤器

该设备包括多种监控爆发过滤器功能的性能和活动的工具。

病毒爆发过滤器报告

通过爆发过滤器报告，可查看设备中爆发过滤器的当前状态和配置，以及有关最近爆发和由于爆发过滤器而被隔离的邮件的信息。在“监控”(Monitor) >“爆发过滤器”(Outbreak Filters) 页面上可查看此信息。有关详细信息，请参阅“邮件安全监控”一章。

爆发过滤器概述和规则列表

概述和规则列表提供有关爆发过滤器功能当前状态的有用信息。通过“安全服务”(Security Services) >“爆发过滤器”(Outbreak Filters) 页面可查看此信息。

病毒爆发隔离区

使用爆发隔离区可监控被爆发过滤器威胁级别阈值标记的邮件数量。另外，还可查看按规则隔离的邮件列表。有关信息，请参阅病毒爆发隔离区和“按规则摘要管理”视图，第 324 页和集中化的策略、病毒和病毒爆发隔离区，第 685 页

警报、SNMP 陷阱和病毒爆发过滤器

病毒爆发过滤器功能支持两种不同类型的通知：普通 AsyncOS 警报和 SNMP 陷阱。

当规则更新失败时，将生成 SNMP 陷阱。有关 AsyncOS 中 SNMP 陷阱的详细信息，请参阅“通过 CLI 管理和监控”一章。

AsyncOS 有两种类型的病毒爆发过滤器功能警报：大小和规则

每当爆发隔离区的大小超过最大大小的 5%、50%、75% 和 95% 时，将生成 AsyncOS 警报。针对 95% 阈值生成的警报的严重性为“严重”(CRITICAL)，而其余警报阈值的严重性为“警告”(WARNING)。随着隔离区范围加大而超过阈值时，将生成警报。随着隔离区范围减小而越过阈值时，不会生成警报。有关警报的详细信息，请参阅告警信息，第 777 页。

当发布规则、更改阈值时，或更新规则或 CASE 引擎出现问题时，AsyncOS 也会生成警报。

病毒爆发过滤器功能故障排除

本节提供适用于爆发过滤器功能的一些基本故障排除提示。

向思科报告分类错误的邮件

使用爆发隔离区“管理隔离区”(Manage Quarantine) 页面上的复选框，通知思科分类错误。

多个附件和绕过的文件类型

只有邮件的唯一附件是绕过的文件类型时，才会排除绕过的文件类型；如果有多个附件，只有其他附件当前没有设定规则时，才会排除绕过的文件类型。否则，将对邮件进行扫描。

邮件和内容过滤器及邮件管道

首先对邮件应用邮件和内容过滤器，然后才执行爆发过滤器扫描。这些过滤器可能导致邮件跳过或绕过爆发过滤器扫描。

第 16 章

防御恶意或不需要的 URL

本章包含以下部分：

关于 URL 的保护和控制

在工作队列的反垃圾邮件、爆发、内容和邮件过滤过程中，已纳入对恶意或不需要链接的控制和防御。这些控制：

- URL 过滤合并到病毒爆发过滤中。即使您所在的组织已拥有思科 Web 安全设备或对网络威胁的类似防御，这种增强保护仍然非常有用，因为它可在入口点阻止威胁。

  根据邮件中 URL 的网络信誉得分 (WBRS)，还可以使用内容或邮件过滤器采取措施。例如，可以重写信誉不确定或未知的 URL，将它们重定向至思科 Web 安全代理进行点击时间安全评估。

- 更好地识别垃圾邮件

  该设备利用邮件中链接的信誉和类别以及其他垃圾邮件识别算法，帮助识别垃圾邮件。例如，如果邮件中的链接属于营销网站，则该邮件很可能是营销邮件。

- 支持执行公司可接受的使用策略

  URL 类别（例如，成人内容或非法活动）可以与内容和邮件过滤器搭配使用，共同来执行公司可接受的使用策略。

- 允许识别组织中最常点击邮件中经过重写保护的 URL 的用户，以及最常被点击的链接。

评估的 URL

评估传入和外发邮件中的 URL（不包括附件）。评估 URL 的任何有效字符串，包括含以下内容的字符串：

- http、https 或 www
- 域或 IP 地址
- 前缀冒号 (:) 的端口号
- 大写或小写字母

在评估URL以确定邮件是否为垃圾邮件时，如果需要进行负载管理，系统会优先检查传入邮件，然后是外发邮件。

设置 URL 过滤

URL 过滤要求

除了启用 URL 过滤之外，还必须根据所需功能启用其他特性。

要增强防御垃圾邮件，请执行以下操作：

- 必须对每个适用的邮件策略，全局启用反垃圾邮件扫描。可以启用 IronPort 反垃圾邮件，也可以启用智能多重扫描功能。请参阅反垃圾邮件章节。

  要增强防御恶意软件，请执行以下操作：

- 必须对每个适用的邮件策略，全局启用病毒爆发过滤器功能。请参阅“病毒爆发过滤器”一章。

  要基于URL信誉采取操作或使用邮件和内容过滤器执行可接受的使用策略，请执行以下操作：

- 必须全局启用病毒爆发过滤器功能。请参阅“病毒爆发过滤器”一章。

启用 URL 过滤

可以在 Web 界面中使用**安全服务 (Security Services) > URL 过滤 (URL Filtering)** 页面启用 URL 过滤，也可以在 CLI 中使用 **`websecurityconfig`** 命令启用。

准备工作

- 确保满足要使用的各项 URL 过滤功能的要求。请参阅URL 过滤要求，第 328 页。
- （可选）创建一个希望所有 URL 过滤功能都忽略的 URL 列表。请参阅创建 URL 过滤的白名单，第 331 页。

步骤 1 依次选择**安全服务 (Security Services) > URL 过滤 (URL Filtering)**。

步骤 2 点击**启用 (Enable)**。

步骤 3 选中**启用 URL 类别和信誉过滤器 (Enable URL Category and Reputation Filters)** 复选框。

步骤 4 （可选）在评估邮件是否为垃圾邮件和恶意软件时，如果已创建了免于执行 URL 过滤及所有内容和邮件过滤的 URL 列表，请选择该列表。

通常，此设置不会导致邮件绕过反垃圾邮件或爆发过滤器处理。

步骤 5 （可选）启用网络交互跟踪。请参阅Web 互动跟踪，第 330 页。

步骤 6 提交并确认更改。

如果符合相应的必备条件，并且已配置病毒爆发过滤器和反垃圾邮件保护，则无需要进行其他配置，即可执行增强的垃圾邮件和恶意 URL 自动检测。

下一步做什么

- 要基于邮件中的 URL 信誉采取操作，请参阅根据邮件中 URL 的信誉或类别采取操作，第 333 页。
- 要使用内容和邮件过滤器中的URL类别（例如，执行可接受的使用策略），请参阅根据邮件中 URL 的信誉或类别采取操作，第 333 页。
- 要将可疑垃圾邮件中的所有 URL 重定向到思科 Web 安全代理服务，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，第 278 页。
- （可选）要自定义最终用户通知页面的外观，请参阅自定义最终用户访问恶意站点时看到的通知，第 332 页。
- 确保您收到与此功能相关的问题警报。请参阅将来的URL类别集变更，第351页、AsyncOS 版本的版本说明和添加警报收件人，第 778 页。

关于与思科网络安全服务的连接

URL 信誉和类别由基于云的思科网络安全服务提供。

邮件安全设备使用防火墙资讯，第1005页中指定用于URL过滤服务的端口，直接或通过网络代理连接到思科网络安全服务。使用双方证书身份验证，通过HTTPS进行通信。证书是自动更新的（请参阅服务更新，第761页。）有关所需证书的其他信息，请参阅版本说明（可从适用于URL过滤功能的证书，第 330 页指定的位置获取）。

如果已在**安全服务 > 服务更新**页面配置 HTTP 或 HTTPS 代理，邮件安全设备将使用它与思科网络安全服务通信。有关使用代理服务器的详细信息，请参阅配置服务器设置以下载升级和更新，第 765 页。

在 FIPS 模式下，与思科网络安全服务的通信使用 FIPS 密码。

注释 不随同配置文件保存证书。

适用于 URL 过滤功能的证书

AsyncOS 旨在自动部署和更新与用于URL过滤功能的云服务通信所需的证书。但是，如果系统因任何原因无法更新这些证书，您将会收到需要您采取行动的风险通告。

确保设备配置为向您发送这些风险通告（“系统”类型、“警告”严重性）。有关说明，请参阅告警信息，第 777 页。

如果收到关于证书无效的风险通告，请联系思科 TAC，其中可提供所需的替换证书。有关使用替换证书的说明，请参阅手动配置与思科 Web 安全服务通信的证书，第 339 页。

Web 互动跟踪

网络交互跟踪功能提供有关点击重写的URL的最终用户的信息，以及每位用户点击的相关操作（允许、组织或未知）。启用此功能后，您可以使用 Web 互动跟踪报告查看很多信息，例如点击数最高的恶意 URL，点击恶意 URL 次数最多的用户，等等。有关网络交互跟踪报告的详细信息，请参阅“网络交互跟踪”页面，第 657 页。

网络交互跟踪数据由基于云的思科汇聚器服务器 (Cisco Aggregator Server) 提供。

配置网络交互跟踪

根据您的需求，可以在其中一个全局设置页面中启用网络交互跟踪：

- **爆发过滤器**。跟踪点击了爆发过滤器重写的URL的最终用户。请参阅配置病毒爆发过滤器全局设置，第 316 页。
- **URL 过滤**。跟踪点击了策略（使用内容和邮件过滤器）重写的 URL 的最终用户。请参阅启用 URL 过滤，第 328 页。

关于与思科聚合器服务器的连接

邮件安全设备每隔30分钟（不可配置），使用防火墙资讯，第1005页中指定用于URL过滤的端口，直接或通过网络代理连接到思科聚合器服务器。使用双方证书身份验证，通过HTTPS进行通信。证书自动更新（请参阅服务更新，第 761 页。）

如果已在**安全服务 (Security Services)** > **服务更新 (Service Updates)** 页面上配置 HTTP 或 HTTPS 代理，则邮件安全设备将使用它来与思科聚合器服务器通信。有关使用代理服务器的详细信息，请参阅配置服务器设置以下载升级和更新，第 765 页。

在 FIPS 模式下，与思科聚合器服务器的通信使用 FIPS 密码。

注释 不随同配置文件保存证书。

集群配置中的 URL 过滤

- 您可以在计算机、组或集群级别启用 URL 过滤。

- 如果在计算机级别启用 URL 过滤，则可以在计算机、组或集群级别配置 URL 白名单和网络交互跟踪。
- 如果在组级别启用 URL 过滤，则必须在组或集群级别配置 URL 白名单和网络交互跟踪。
- 如果在集群级别启用 URL 过滤，则必须在集群级别配置 URL 白名单和网络交互跟踪。
- 适用用于邮件过滤器和内容过滤器的集群的标准规则。

创建 URL 过滤的白名单

如果在配置 URL 过滤功能时指定了全局白名单，则不评估白名单中 URL 的信誉或类别，不执行反垃圾邮件、爆发过滤或内容和邮件过滤。但是，反垃圾邮件扫描和病毒爆发过滤器将正常评估包含这些 URL 的邮件。此外，还可以在每个 URL 过滤条件（规则）和内容与邮件过滤器操作中指定 URL 白名单，以补充全局 URL 白名单。

通常，要将URL加入绕过爆发过滤的白名单，可使用在“邮件策略：病毒爆发过滤器”(Mail Policies: Outbreak Filters) 页面配置的“绕过域扫描”(Bypass Domain Scanning) 选项。URL 过滤的 URL 白名单与之类似，但与“绕过域扫描”(Bypass Domain Scanning) 无关。有关该功能的详细信息，请参阅URL 重写和绕行域，第 322 页。

此部分介绍的 URL 过滤白名单与基于 SBRS 得分的发件人信誉过滤所用的白名单之间没有关系。

准备工作

请考虑导入 URL 列表，而不是在 Web 界面中创建 URL 列表。请参阅导入 URL 列表，第 332 页。

步骤 1 依次选择**邮件策略 (Mail Policies) > URL 列表 (URL Lists)**。

步骤 2 选择**添加 URL 列表 (Add URL List)**，或点击一个列表进行编辑。

确保希望全局加入白名单的所有 URL 都在一个列表中。只能为 URL 过滤选择一个全局白名单。

步骤 3 创建并提交该 URL 列表。

要查看支持的 URL 格式的列表，请向 **URL** 框中输入分号 (;)，并点击**提交 (Submit)**。然后，点击显示的**更多... (more...)** 链接。

每个 URL、域或 IP 地址可以单独为一行，或使用逗号相互隔开。

步骤 4 确认您的更改。

下一步做什么

- 要将 URL 列表指定为全局白名单，请参阅启用 URL 过滤，第 328 页。
- 要将 URL 指定为内容或邮件过滤器中特定条件（规则）或操作的白名单，请参阅根据邮件中 URL 的信誉或类别采取操作，第 333 页和内容过滤器操作，第 242 页。对于邮件过滤器，另请参阅URL 类别操作，第 189 页和URL 类别规则，第 157 页。

导入 URL 列表

您可以导入 URL 列表，用作 URL 过滤的白名单。

步骤 1 创建要导入的文本文件：

- 第一行必须是 URL 列表的名称。
- 每个 URL 必须单独为一行。

步骤 2 将文件上传到设备的 `/configuration` 目录。

步骤 3 在命令行界面使用 `urllistconfig > new` 命令。

自定义最终用户访问恶意站点时看到的通知

如果最终用户点击了爆发过滤或策略（使用内容或邮件过滤器）所识别的恶意 URL，思科 Web 安全代理将在最终用户的 Web 浏览器中显示通知。此通知将指出：该站点是恶意的，对该站点的访问已被阻止。

当最终用户点击使用爆发过滤重写的 URL 时，通知页面将显示 10 秒，然后会重定向到思科 Web 安全代理进行点击时评估。

您可以自定义此通知页面的外观，并显示您所在组织的品牌，例如公司徽标、联系信息等。

注释 如果您未自定义通知页面，则最终用户将看到思科品牌的通知页面。

准备工作

- 启用 URL 过滤。请参阅启用 URL 过滤，第 328 页。

步骤 1 依次选择**安全服务 (Security Services)** > **阻止页面自定义 (Block Page Customization)**。

步骤 2 点击**启用 (Enable)**。

步骤 3 选中**启用阻止页面自定义 (Enable Block Page customization)** 复选框，并输入以下详细信息：

- 组织徽标的 URL。建议将徽标图像托管在可公开访问的服务器。
- 组织名称
- 组织的联系信息

步骤 4 选择通知的语言。可以选择 Web 界面支持的任何一种语言。

注释 最终用户的浏览器默认语言优先于您在此所选的语言。此外，如果 AsyncOS 不支持最终用户的浏览器默认语言，则以您在此所选的语言显示通知。

步骤 5 （可选）点击**预览阻止页面自定义 (Preview Block Page Customization)** 链接可预览通知页面。

步骤 6 提交并确认更改。

后续步骤

通过以下任一方式设置 URL 重写：

- 使用爆发过滤器。请参阅重定向 URL，第 310 页。
- 使用内容或邮件过滤器。请参阅根据邮件中 URL 的信誉或类别采取操作，第 333 页。

根据邮件中 URL 的信誉或类别采取操作

由于爆发过滤器在评估邮件是否为恶意软件时要考虑许多因素，而且单独URL信誉可能不会触发主动邮件处理，所以您可能希望基于 URL 信誉创建过滤器。

例如，您可以使用 URL 信誉过滤器：

- 重写信誉不确定或未知的 URL，将它们重定向到思科云网络安全代理服务以进行点击时评估。
- 丢弃包含的 URL 的信誉得分属于恶意范围的邮件。

您可以使用 URL 类别过滤器：

- 过滤 URL 的类别，以执行组织可接受的 Web 使用策略，例如阻止用户在办公室访问成人或赌博站点。

使用 URL 相关条件（规则）和操作

目标	示例	请
整体上针对邮件采取操作。	丢弃或隔离邮件。	创建 URL 信誉或 URL 类别条件或规则，然后将其与 URL 信誉或 URL 类别操作以外的任何操作配对。 例外：请勿将 URL 信誉条件或规则与退回操作配对。
	用文本说明替换邮件中的 URL，或将 URL 设为不可点击状态。	仅创建 URL 信誉或 URL 类别操作；请勿使用单独的 URL 过滤条件。

一如既往，必须在邮件策略中指定内容过滤器，才能使用它。

按 URL 信誉或 URL 类别过滤：条件和规则

例如，如果要对包含“成人”(Adult) 类别 URL 的所有邮件应用**丢弃**（**最终操作**）操作，请添加一个 **URL 类别 (URL Category)** 的条件，并选择**成人 (Adult)** 类别。

如果未指定类别，将对所有邮件应用您所选的操作。

正常、不确定和恶意 URL 的 URL 信誉得分范围是预定义的，不可编辑。但是，您可以改为指定自定义范围。指定的终端包含在所指定的范围内。例如，如果创建了一个从 -8 到 -10 的自定义范围，则 -8 和 -10 包含在该范围内。对于信誉得分无法确定的 URL，请使用“无分数”。

注释 不确定的 URL 信誉表示这些 URL 目前是安全的，但将来可能会变为恶意的，因为它们容易受到攻击。对于此类URL，管理员可创建非阻止策略，例如将它们重定向到思科Web安全代理以进行点击时评估。

不评估特定 URL 白名单或全局 URL 白名单中包含的 URL。

如果邮件中的任何 URL 与条件中指定的信誉得分或任何类别匹配，则执行与此条件配对的操作。

如果您要修改邮件中的 URL，或修改其行为，则仅配置 URL 信誉或 URL 类别操作即可。对此，您不需要单独的 URL 信誉或 URL 类别条件或规则。

注释 请勿将 URL 信誉条件与退回操作配对。

提示 要检查特定 URL 的类别，请访问报告未分类和误分类的 URL，第 350 页中的链接。

修改邮件中的 URL：在过滤器中使用 URL 信誉和 URL 类别操作

根据 URL 的信誉或类别，使用 URL 信誉或 URL 类别操作修改邮件中的 URL 或其行为。

URL 信誉和 URL 类别操作不需要单独的条件。相反，系统会根据您在 URL 信誉或 URL 类别操作中选择的信誉或类别应用所选的操作。

仅对符合操作中指定条件的 URL 应用该操作。不会修改邮件中的其他 URL。

如果未指定类别，将对所有邮件应用您所选的操作。

正常、不确定和恶意 URL 的 URL 信誉得分范围是预定义的，不可编辑。但是，您可以改为指定自定义范围。指定的终端包含在所指定的范围内。例如，如果创建了一个从 -8 到 -10 的自定义范围，则 -8 和 -10 包含在该范围内。对于信誉得分无法确定的 URL，请使用“无分数”。

注释 不确定的 URL 信誉表示这些 URL 目前是安全的，但将来可能会变为恶意的，因为它们容易受到攻击。对于此类URL，管理员可创建非阻止策略，例如将它们重定向到思科Web安全代理以进行点击时评估。

- 去除 URL，使其不可点击。邮件收件人仍然可以查看和复制 URL。
- 重定向 URL，这样当邮件收件人点击链接，事务将路由到云中的思科网络安全代理；如果站点是恶意的，则阻止访问。

示例：您可能希望将**未分类**类别中的所有URL都定向到思科云网络安全代理服务，因为网络钓鱼攻击中所用的恶意站点存在的时间通常不足以进行分类。

另请参阅重定向 URL：终端用户会有哪些体验？ ，第 335 页。

要将 URL 重新定向到不同的代理，请参阅以下项目中的示例。

注释 在此版本中，Cisco Cloud Web Security 代理服务没有可配置的选项。例如，没有威胁分数阈值供调整或基于威胁分数指定操作。

- 使用任何文本替换 URL。

  要在邮件显示的文本中包括原始 URL，请使用 $URL 变量。

  示例：

  - 使用以下注释替换**非法下载 (Illegal Downloads)** 类别的所有 URL：

    ```
    Message from your system administrator: A link to an illegal downloads web site has
    been removed from this message.
    ```

  - 包含原始 URL 及警告：

    ```
    警告! The following URL may contain malware: $URL
    ```

    这样将变成：WARNING: The following URL may contain malware: http://example.com。

  - 重定向到自定义代理或网络安全服务：

    ```
    http://custom_proxy/$URL
    ```

    这样将变成：http://custom_proxy/http://example.com

不评估包含在所选 URL 白名单或全局 URL 白名单中的 URL 的信誉和类别。

如果要去除或替换 URL，可以选择忽略已签名邮件中的 URL。

不建议将 URL 信誉或 URL 类别操作与 URL 信誉或 URL 类别条件（或规则）配对。如果配对的条件（规则）和操作包括其他类别，则不会产生匹配。

提示 要检查特定 URL 的类别，请访问报告未分类和误分类的 URL ，第 350 页中的链接。

重定向 URL：终端用户会有哪些体验？

根据 Cisco Cloud Web Security 代理服务的评估：

- 如果站点是良性的，用户将定向到目标网站，并且不知道链接已被重定向。
- 如果站点是恶意的，用户将看到通知，表示该站点是恶意的，对该站点的访问已被阻止。

您可以自定义终端用户通知页面的外观，并显示您所在组织的品牌，例如公司徽标、联系信息等。请参阅自定义最终用户访问恶意站点时看到的通知，第 332 页。

- 如果与思科云网络安全代理服务的通信超时，系统将允许用户访问目标网站。
- 如果出现任何其他错误，用户将看到通知。

监控 URL 过滤结果

要查看有关检测到的恶意和不确定 URL 的数据，请选择**监控 (Monitor)** > **URL 过滤 (URL Filtering)**。有关此页面中数据的重要信息，请参阅“URL 过滤”页面，第 656 页。

在邮件跟踪中显示 URL 详细信息

要显示爆发过滤器和相关内容过滤器所捕获 URL 的邮件跟踪的详细信息，请执行以下操作：

- 必须启用邮件跟踪。
- 基于 URL 信誉或 URL 类别的爆发过滤器和/或内容过滤器器必须是可操作的。
- 对于爆发过滤器，必须启用 URL 重写。请参阅URL 重写和绕行域，第 322 页。
- 必须启用 URL 日志记录。请参阅启用 URL 日志记录和 URL 邮件跟踪详细信息，第 317 页。

有关所显示数据的详细信息，请参阅邮件跟踪详细信息，第 681 页。

若要管理对这些潜在敏感的详细信息的管理用户访问，请参阅控制对“邮件跟踪”中敏感信息的访问权限，第 727 页。

URL 过滤故障排除

查看日志

URL 过滤信息将发布到以下日志：

- 邮件日志 (mail_logs)。有关 URL 扫描结果（根据 URL 对邮件采取的操作）的信息将发布到此日志。
- URL 过滤日志 (web_client)。尝试查找 URL 时，有关错误、超时、网络问题等的信息将发布到此日志。

大多数信息处于信息或调试级别。

日志中不包括有关用户点击邮件中重定向的链接时所发生状况的信息。

日志中的“SDS”是指 URL 信誉服务。

警报：SDS：获取注册证书时出错

问题

关于获取注册客户端证书时出现的错误，您将会收到参考级别的风险通告。

解决方案

要连接到以下基于云的服务，需要使用此证书：思科 Web 安全服务（获取 URL 信誉和类别）和思科汇聚器服务器（获取网络交互跟踪数据）。请尝试以下操作：

1. 检查网络连接问题，例如代理设置不正确或防火墙问题。
2. 确认您的 URL 过滤功能密钥是否有效且处于活动状态。
3. 如果问题仍然存在，请联系思科 TAC。

警报：SDS：证书无效

问题

您将收到有关无效 SDS 证书的严重风险通告。

解决方案

要连接到云中的思科 Web 安全服务以获取 URL 信誉和类别，需要使用此证书。

要获取和手动安装证书，请参阅手动配置与思科 Web 安全服务通信的证书，第 339 页。

无法连接到思科 Web 安全服务

问题

安全服务 (Security Services) > URL 过滤 (URL Filtering) 页面将持续指示连接到思科 Web 安全服务的问题。

解决方案

- 如果已启用 URL 过滤，但尚未确认更改，请确认更改。
- 检查最近有关连接思科网络安全服务的警报。请参阅查看最近的警报，第 780 页。如果适用，请参阅警报：SDS：获取注册证书时出错，第 336 页和警报：SDS：证书无效，第 337 页。
- 如果要通过**安全服务 > 服务更新**指定的代理连接，请确认已配置代理并且代理工作正常。
- 检查可能会阻止连接的其他网络问题。
- 如果在 URL 过滤日志中看到有关请求连接 SDS 客户端超时的错误，请在命令行界面使用 websecuritydiagnostics 命令和 **websecurityadvancedconfig** 命令调查并进行更改：
  - 如果诊断表示：响应时间或 DNS 查找时间大于或等于所配置的 URL 查找超时，请相应地增加 URL 查找超时值。
  - 如果诊断表示：缓存大小已达到或接近高级配置设置中指定的容量，请增加缓存大小。
- 检查 URL 过滤日志中与 URL 扫描仪、思科 Web 安全服务或 SDS 通信时的非超时错误。日志中的“SDS”表示思科 Web 安全服务。如果看到这种日志消息，请联系 TAC。

警报：无法连接到思科汇聚器服务器

问题

您将会收到以下警告风险通告：无法连接到思科汇聚器服务器。

解决方案

执行以下操作：

1. 通过从设备 ping 服务器的主机名，检查设备和思科汇聚器服务器之间的连接。在 CLI 中使用 aggregatorconfig 命令，查看思科汇聚器服务器的主机名。
2. 如果要通过“安全服务”(Security Services) > “服务更新”(Service Updates) 指定的代理连接，请确认已配置代理并且代理工作正常。
3. 检查可能会阻止连接的其他网络问题。
4. 检查 DNS 服务是否正在运行。
5. 如果问题仍然存在，请联系思科 TAC。

警报：无法从思科汇聚器服务器检索网络交互跟踪信息

问题

您将会收到以下警告风险通告：无法从思科汇聚器服务器检索网络交互跟踪信息。

解决方案

执行以下操作：

1. 如果要通过**安全服务 > 服务更新**指定的代理连接，请确认已配置代理并且代理工作正常。
2. 检查可能会阻止连接的其他网络问题。
3. 检查 DNS 服务是否正在运行。
4. 如果问题仍然存在，请联系思科 TAC。

使用 websecurityadvancedconfig 命令

除本文档明确描述的更改之外，未经 TAC 指导，请勿使用 websecurityadvancedconfig 命令进行任何其他更改。

邮件跟踪搜索未找到指定类别的邮件

问题

按某个类别搜索时，未找到包含该特定类别的 URL 的邮件。

解决方案

请参阅搜索结果中缺少预期邮件，第 684 页。

反垃圾邮件或病毒爆发过滤器不会捕获恶意 URL 和营销邮件

问题

反垃圾邮件或爆发过滤器不会捕获恶意 URL 和包含营销链接的邮件。

解决方案

- 出现这种情况，可能是因为网站信誉和类别仅是反垃圾邮件和病毒爆发过滤器用于确定其判定的众多条件中的两个。您可以通过降低重写URL、用文本替换URL、隔离或丢弃邮件等操作所需的阈值，提高这些过滤器的敏感度。有关详细信息，请参阅爆发过滤器功能和邮件策略，第 319 页和定义反垃圾邮件策略，第 275 页。或者，根据 URL 信誉得分创建内容或邮件过滤器。
- 如果邮件安全设备无法连接到思科网络安全服务，也可能会出现这种情况。请参阅无法连接到思科 Web 安全服务，第 337 页。

过滤类别中的 URL 未得到正确处理

问题

未应用内容或邮件过滤器中根据 URL 类别定义的操作。

解决方案

- 使用跟踪功能（“故障排除”一章中介绍）跟进邮件处理路径。
- 如果邮件安全设备无法连接到思科网络安全服务，可能会出现这种情况。请参阅无法连接到思科 Web 安全服务，第 337 页。
- 如果没有任何连接问题，URL仍可能不会分类或分类错误。请参阅报告未分类和误分类的URL，第 350 页。您可以使用此站点确定 URL 的类别。

终端用户通过重写的 URL 访问恶意站点

问题

恶意 URL 将被重定向到思科 Web 安全代理，但终端用户仍无法访问站点。

解决方案

如果满足以下条件，就可能出现这种情况：

- 该站点未被识别为恶意站点。
- 连接思科网络安全代理超时，这种情况应该很少见。确保网络问题不会妨碍连接。

手动配置与思科 Web 安全服务通信的证书

如果设备无法自动获取与思科 Web 安全服务通信的证书，请使用此过程。

步骤 1 获取所需的证书。

步骤 2 使用**网络 > 证书**上传证书，或在命令行界面中使用 certconfig 命令。

步骤 3 在命令行界面，输入 **websecurityconfig** 命令。

步骤 4 按照提示设置思科 Web 安全服务身份验证的客户端证书。

步骤 5 完成证书安装过程后，输入 **webcacheflush** 命令。

关于 URL 类别

URL 类别说明

这些 URL 类别与 AsyncOS for Web Security 设备最新版本中所用的类别相同。

URL 类别	缩写	代码	说明	示例 URL
成人	adlt	1006	主要面向成年人，但不一定包含色情内容。内容可能涉及成人俱乐部（脱衣舞俱乐部、换妻俱乐部、三陪服务、脱衣舞表演等）；有关性的一般信息（非色情性质）；生殖器穿刺；成人用品或成人贺卡；不涉及性暗示的有关健康或疾病的内容。	www.adultentertainmentexpo.com www.adultnetline.com
广告	adv	1027	通常会伴随网页显示横幅广告和弹窗广告的网站；其他提供通告内容的广告网站。与广告服务和销售相关的网站属于“商业和工业网站”类别。	www.adforce.com www.doubleclick.com
酒类网站	alc	1077	涉及以下内容的网站：以酒类为主题的快乐活动；啤酒和葡萄酒酿造、鸡尾酒调制方法；酒商、酒庄、葡萄园、酿酒厂、酒类经销商。酒瘾分类为“健康和营养”。酒吧和餐厅分类为“餐饮”。	www.samueladams.com www.whisky.com
艺术	作画	1002	涉及以下内容的网站：画廊和画展；艺术家和艺术；摄影；文献和著作；表演艺术和剧场；音乐；芭蕾；博物馆；设计；建筑。与电影院和电视相关的网站属于“娱乐网站”类别。	www.moma.org www.nga.gov
占星网站	astr	1074	涉及以下内容的网站：占星术；星座占卜；算命；数字占卜；通灵；塔罗牌占卜。	www.astro.com www.astrology.com

URL 类别	缩写	代码	说明	示例 URL
拍卖	auct	1088	涉及以下内容的网站：网络和线下竞拍、拍卖行和分类广告。	www.craigslist.com www.ebay.com
商业和工业	busi	1019	涉及以下内容的网站：市场营销、商务、公司、业务实践、员工、人力资源、交通运输、薪酬、安全和风险投资；办公用品；工业设备（工艺设备）、机器和机械系统；加热设备、冷却设备；材料搬运设备；包装设备；制造业相关的固体物质运输、金属加工、建筑和建造；乘客运输；商业活动；工业设计；建设施工、建筑材料；运输和货运（货运服务、卡车运输、货运代理、卡车运输公司、货运和运输代理、快递服务、空车配运、运输跟踪、铁路运输、海运、货运专线服务、搬运和储存）。	www.freightcenter.com www.staples.com
聊天和即时消息	chat	1040	提供基于 Web 的即时消息和聊天室服务的网站。	www.icq.com www.meebo.com
抄袭和剽窃网站	plag	1051	助长抄袭，并出于剽窃目的销售书面著作（例如学期论文）的网站。	www.bestessays.com www.superiorpapers.com
虐童网站	cprn	1064	涉及全球违法儿童性侵内容的网站。	—
计算机安全	csec	1065	为公司和家庭用户提供安全产品和服务的网站。	www.computersecurity.com www.symantec.com
计算机和互联网	comp	1003	有关计算机和软件的信息，例如硬件、软件、软件支持；软件工程师、编程和网络信息；网站设计；常用 Web 和互联网；计算机科学；计算机图形和剪贴画。“免费软件和共享软件网站”单独分为一类。	www.xml.com www.w3.org
约会	日期	1055	提供约会、网上交友、婚介服务的网站。	www.eharmony.com www.match.com

URL 类别	缩写	代码	说明	示例 URL
数字明信片网站	card	1082	支持发送数字明信片和电子贺卡的网站。	www.all-yours.net www.delivr.net
餐饮网站	食品	1061	涉及以下内容的网站：餐饮设施；餐厅、酒吧、酒馆和休闲吧；酒店指南和评价。	www.hideawaybrewpub.com www.restaurantrow.com
动态 IP 和住宅 IP	dyn	1091	通常表明用户尝试访问其家庭网络的宽带连接 IP 地址（例如远程访问家用计算机）。	http://109.60.192.55 http://dynalink.co.jp http://ipadsl.net
教育	edu	1001	与教育相关的网站，内容可能涉及学校、学院、大学、教材和教学资源；技术和职业培训；在线培训；教育难题和教育政策；助学金；学校基金；标准和测试。	www.education.com www.greatschools.org
娱乐	ent	1093	涉及以下内容的网站：电影情节或讨论；音乐和乐队；电视；名人和粉丝网站；娱乐新闻；明星八卦；娱乐场所。独立于“艺术网站”类别。	www.eonline.com www.ew.com
Extreme	extr	1075	涉及以下内容的网站：具有性暴力或性犯罪性质的材料；暴力和暴力行为；品味低下的材料（通常是血腥暴力的图片，例如尸体解剖照片）；犯罪现场、犯罪和事故受害者的照片；极度淫秽的材料；冲击性网站。	www.car-accidents.com www.crime-scene-photos.com
时尚网站	fash	1076	涉及以下内容的网站：服装和时尚；发廊；化妆品；饰物；珠宝；香水；与人体改造相关的图片和文字；纹身和穿刺；模特经纪公司。与护肤产品相关的网站属于“健康和营养网站”类别。	www.fashion.net www.findabeautysalon.com
文件传输服务	fts	1071	以提供下载服务和托管文件共享服务为主要目的的文件传输服务网站。	www.rapidshare.com www.yousendit.com

URL 类别	缩写	代码	说明	示例 URL
过滤逃避网站	filt	1025	推动并帮助实现无法检测的网络使用和匿名网络使用（包括 cgi、php 和 glype 匿名代理服务）的网站。	www.bypassschoolfilter.com www.filterbypass.com
金融业	fnnc	1015	在性质上以金融为主的网站，内容可能涉及会计实务和会计人员、税务、税收、银行、保险、投资、国家经济、个人理财（包括所有类型的保险）、信用卡、退休规划和房地产规划、贷款、抵押等。与股票和股份相关的网站属于“在线交易网站”类别。	finance.yahoo.com www.bankofamerica.com
免费软件和共享软件网站	free	1068	提供免费软件和共享软件下载服务的网站。	www.freewarehome.com www.shareware.com
赌博	gamb	1049	涉及以下内容的网站：赌场和网上赌博；庄家和赔率；赌博建议；具有赌博性质的竞速比赛；体育博彩；体育赌博；股票和股份点差交易服务。处理赌瘾的的网站属于“健康和营养网站”类别。国有彩票属于“彩票”类别。	www.888.com www.gambling.com
游戏	游戏	1007	涉及以下内容的网站：各种卡片游戏、桌上游戏、文字游戏和视频游戏；对战游戏；体育游戏；可下载的游戏；游戏评论；作弊码；计算机游戏和互联网游戏（例如角色扮演游戏）。	www.games.com www.shockwave.com

URL 类别	缩写	代码	说明	示例 URL
政府和法律	gov	1011	涉及以下内容的网站：政府网站；对外关系；与政府和选举相关的新闻和信息；与法律领域相关的信息（例如律师、律师事务所、法律著作、法律参考资料、法院、备审案件目录和法律协会）；立法及判决；民权问题；移民；专利和版权；与执法和执法系统相关的信息；犯罪报告、执法和犯罪统计；军事（例如军队、军事基地、军事组织）；反恐怖主义。	www.usa.gov www.law.com
黑客攻击	hack	1050	讨论如何绕过网站、软件和计算机安全保护的网站。	www.hackthissite.org www.gohacking.com
仇恨言论网站	hate	1016	煽动以下内容的网站：基于社会团体、肤色、宗教信仰、性取向、残疾、阶级、种族、民族、年龄、性别和性身份的仇恨、蔑视和歧视；种族主义；性别歧视；种族神学；厌世音乐；新纳粹组织；种族优越主义；否认大屠杀。	www.kkk.com www.nazi.org
健康和营养网站	hlth	1009	涉及以下内容的网站：卫生保健；疾病和残疾；医疗；医院；医生；医用药物；心理健康；精神病学；药物学；锻炼和健身；身体残疾；维生素和营养品；与性相关的健康知识（疾病和医疗）；与吸烟、饮酒、吸毒和赌博相关的健康知识（疾病和医疗）；与食物相关的一般知识；食物和饮料；烹饪和菜谱；食物与营养、健康、节食；烹饪方法（包括菜谱和烹饪网站）；替代疗法。	www.health.com www.webmd.com
幽默网站	lol	1079	与笑话、涂鸦、漫画和其他幽默内容相关的网站。与可能具有冒犯性的成人幽默相关的网站属于“成人网站”类别。	www.humor.com www.jokes.com

URL 类别	缩写	代码	说明	示例 URL
非法活动网站	ilac	1022	煽动犯罪的网站，内容可能涉及：盗窃、欺诈、非法接入电话网络；计算机病毒；恐怖主义、炸弹和无政府主义。也包括描述谋杀和自杀以及介绍谋杀和自杀方法的网站。	www.ekran.no www.thedisease.net
非法下载	ildl	1084	提供以下下载内容的网站：软件或其他材料、序列号、密钥生成器，以及违反版权协议绕过软件保护的工具。与 Torrent 下载相关的网站属于“点对点文件传输网站”类别。	www.keygenguru.com www.zcrack.com
违禁药物	drug	1047	此类网站提供有关娱乐性毒品、吸毒工具，以及毒品购买和制造的信息。	www.cocaine.org www.hightimes.com
基础设施和内容交付网络	infr	1018	内容交付基础设施和涉及动态生成内容的网站；由于安全原因而无法更具体分类的网站，或者难以分类的网站。	www.akamai.net www.webstat.net
互联网电话服务	voip	1067	提供基于互联网的电话服务的网站。	www.evaphone.com www.skype.com
求职	作业	1004	涉及以下内容的网站：职业建议；编写简历和应对面试的技巧；就业服务；职位数据库；固定职业和临时职业介绍所；招聘网站。	www.careerbuilder.com www.monster.com
女用内衣和泳装	ling	1031	贴身衣服和泳装，特别是做模特时。	www.swimsuits.com www.victoriassecret.com
彩票网站	lotr	1034	与奖券、竞赛和国家赞助的彩票相关的网站。	www.calottery.com www.flalottery.com
手机	cell	1070	短消息服务 (SMS)、铃声和手机下载。移动运营商网站属于“商业和工业网站”类别。	www.cbfsms.com www.zedge.net

URL 类别	缩写	代码	说明	示例 URL
自然网站	natr	1013	涉及以下内容的网站：自然资源；生态学和环境保护；森林；原野；植物；花；森林保护；森林、原野和林业实践；森林管理（重新造林、森林保护、保持、砍伐、森林健康状况、抚育间伐和计划烧除）；农业实践（农学、园艺、园林、景观、绿化、除草、灌溉、修剪和收割）；污染问题（空气质量、危险废弃物、污染防治、回收利用、废弃物管理、水质和环境清理行业）；动物、宠物、家畜和动物学；生物学；植物学。	www.enature.com www.nature.org
新闻	新闻	1058	涉及以下内容的网站：新闻；头条新闻；报纸；电视台；杂志；天气；滑雪条件。	www.cnn.com news.bbc.co.uk
非政府组织网站	ngo	1087	非政府组织（如俱乐部、游说团、社区、非营利组织和工会）的网站。	www.panda.org www.unions.org
非色情裸体网站	nsn	1060	涉及以下内容的网站：裸体主义和裸体行为；自然崇拜；裸体主义者联盟；裸体艺术。	www.artenuda.com www.naturistsociety.com
在线社区	comm	1024	涉及以下内容的网站：有亲密关系的群体；有特殊爱好的群体；网络新闻组；网络论坛。不包括“专业网络”类别和“社交网络”类别的网站。	www.igda.org www.ieee.org
在线存储和备份	osb	1066	出于备份、共享和托管目的提供离线和对等存储的网站。	www.adrive.com www.dropbox.com

URL 类别	缩写	代码	说明	示例 URL
在线交易网站	trad	1028	涉及以下内容的网站：网上证券交易；与股市、股票、债券、共同资金、经纪人、股票分析和股评、股市行情、股票走势、IPO 和股票分割相关的信息。也包括支持用户在线交易股票的网站。股票和股份点差交易服务属于“赌博”类别。其他金融服务属于“财务”类别。	www.tdameritrade.com www.scottrade.com
企业邮件	pem	1085	用于访问企业电子邮件的网站（通常通过 Outlook Web Access 访问）。	—
寄放域	park	1092	通过使用广告网络付费列表的域，对流量进行收费的网站；或者由希望出售域名以谋取利润的“投机者”拥有的网站。此类网站也包括含有付费广告链接的虚假搜索网站。	www.domainzaar.com www.parked.com
点对点文件传输网站	p2p	1056	对等文件请求网站。此类网站不会对文件传输进行跟踪。	www.bittorrent.com www.limewire.com
个人网站	pers	1081	与个人相关或由个人运营的网站；个人主页服务器；含有个人内容的网站；没有特定主题的个人博客。	www.karymullis.com www.stallman.org
照片搜索和图片网站	img	1090	为存储和搜索图片、照片和剪贴画提供便利的网站。	www.flickr.com www.photobucket.com
政治	pol	1083	涉及以下内容的网站：政治家；政党；与政治、选举，民主和投票相关的新闻和信息。	www.politics.com www.thisnation.com
色情	porn	1054	含有露骨的色情文字或内容的网站。内容可能涉及露骨的动画和卡通；一般的露骨内容；其他色情材料；毫无隐晦的聊天室；情爱模拟器；脱衣扑克游戏；成人电影；猥亵的艺术；基于 Web 的露骨电子邮件。	www.redtube.com www.youporn.com

URL 类别	缩写	代码	说明	示例 URL
职业社交网络	pnet	1089	以事业或职业发展为目的的社交网络。另请参阅“社交网络”。	www.linkedin.com www.europeanpwn.net
房地产	rest	1045	为帮助搜索以下内容提供信息的网站：房地产；办公室和商业场所；房地产列表（如出租房屋、公寓和住宅）；住宅建筑。	www.realtor.com www.zillow.com
参考	ref	1017	涉及以下内容的网站：城市和州指南；地图、时间；参考源；词典；资料库。	www.wikipedia.org www.yellowpages.com
宗教	版本	1086	涉及宗教内容和宗教信息的网站；宗教社区。	www.religionfacts.com www.religioustolerance.org
SaaS 和 B2B	saas	1080	提供在线业务服务以及支持在线会议的网络门户。	www.netsuite.com www.salesforce.com
儿童网站	kids	1057	专门面向少年儿童（尤其是经过批准）的网站。	kids.discovery.com www.nickjr.com
委员会	sci	1012	与科学技术相关的网站，内容可能涉及航空航天、电子、工程、数学和其他类似学科；太空探索；气象学；地理；环境；能源（化石能源、核能、可再生能源）；通信（电话、电信）。	www.physorg.com www.science.gov
搜索引擎和门户	srch	1020	搜索引擎以及其他访问互联网信息的入口点。	www.bing.com www.google.com
性教育	sxed	1052	如实介绍性、性健康、避孕和怀孕知识的网站。	www.avert.org www.scarleteen.com
购物	shop	1005	涉及以下内容的网站：以物换物；网络购物；优惠券和赠品；常规办公用品；在线目录；在线商城。	www.amazon.com www.shopping.com
社交网络	snet	1069	社交网络。另请参阅“专业网络”。	www.facebook.com www.twitter.com

URL 类别	缩写	代码	说明	示例 URL
社会科学网站	socs	1014	涉及以下内容的网站：与社会相关的科学和历史；考古学；人类学；文化研究；历史；语言学；地理学；哲学；心理学；女性研究。	www.archaeology.org www.anthropology.net
社会文化网站	scty	1010	涉及以下内容的网站：家族和关系；种族；社会组织；家谱；敬老；儿童看护。	www.childcare.gov www.familysearch.org
软件更新	swup	1053	托管软件包更新的网站。	www.softwarepatch.com www.versiontracker.com
体育和娱乐网站	sprt	1008	涉及以下内容的网站：各种体育运动（职业和业余）；娱乐活动；钓鱼；梦幻竞技；公园；游乐园；水上公园；主题公园；动物园和水族馆；SPA。	www.espn.com www.recreation.gov
流式音频网站	aud	1073	提供实时流式音频内容（包括互联网电台和音频源）的网站。	www.live-radio.net www.shoutcast.com
流视频	vid	1072	提供实时流式视频（包括互联网电视、网播和共享视频）的网站。	www.hulu.com www.youtube.com
烟草网站	tob	1078	烟草宣传网站；烟草制造商网站；有关烟斗和吸烟产品（不是用于非法吸毒目的）的网站。与烟瘾相关的网站属于“健康和营养网站”类别。	www.bat.com www.tobacco.org
交通运输业	trns	1044	涉及以下内容的网站：个人交通；有关汽车和摩托车的信息；全新和二手汽车与摩托车的商店；汽车俱乐部；船只、飞机、房车 (RV) 和其他类似物品。注意：汽车和摩托车比赛属于“体育和娱乐网站”类别。	www.cars.com www.motorcycles.com

URL 类别	缩写	代码	说明	示例 URL
差旅费	trvl	1046	涉及以下内容的网站：商务和个人旅行；旅游信息；旅游资源；旅行社；度假套装；游轮航线；住宿和宿泊；旅行交通；航班预订；机票；租车；度假屋。	www.expedia.com www.lonelyplanet.com
未分类	-	-	未包含在思科数据库中的网站将被分类为“未分类网站”，以便于报告。此类网站可能包括输入错误的 URL。	—
武器	weap	1036	此类网站提供有关常规武器购买或使用的信息，例如枪支贩卖商、枪支拍卖、枪支分类广告、枪支配件、枪展和枪支培训；有关枪的一般信息。此类网站也可能包括其他武器和图片搜索网站。政府军事网站属于“政府和法律网站”类别。	www.coldsteel.com www.gunbroker.com
Web 托管	whst	1037	提供网站托管和带宽服务的网站。	www.bluehost.com www.godaddy.com
网页转换网站	tran	1063	在不同语言之间翻译网页的网站。	babelfish.yahoo.com translate.google.com
基于网络的邮件	mail	1038	提供基于 Web 的公共电子邮件服务的网站。为个人访问其公司或组织的电子邮件服务提供支持的网站属于“组织电子邮件网站”类别。	mail.yahoo.com www.hotmail.com

确定 URL 的类别

要查找特定 URL 的类别，请访问报告未分类和误分类的 URL ， 第 350 页中显示的站点。

报告未分类和误分类的 URL

要报告归类错误的 URL 及未归类而应归类的 URL，请访问：

https://securityhub.cisco.com/web/submit_urls

要检查已提交的URL 的状态，请点击此页面上的**有关已提交 URL 的状态 (Status on Submitted URLs)** 选项卡。

将来的 URL 类别集变更

难得，URL 类别集会随着新兴趋势和技术的发展而变化。例如，可能会添加、删除、重命名某个类别，也可能会将其与其他类别合并或拆分为两个类别。这些变化可能会影响现有过滤器的结果，因此如果发生变化，设备将发送风险通告（“系统”类型，“警告”严重性）。如果您收到此类风险通告，可以评估和更新处理更新类别的内容和邮件过滤器。现有过滤器不会自动更改。要确保收到这些警报，请参阅添加警报收件人，第 778 页。

以下更改不需要更改类别集，并且不会生成风险通告：

- 例行归类新分类的站点。
- 将分类错误的站点重新归类。

第 17 章

文件信誉过滤和文件分析：

本章包含以下部分：

文件信誉过滤和文件分析概述

高级恶意软件防护通过如下方式防范邮件附件中的零日威胁和基于文件的针对性威胁：

- 获取已知文件的信誉。
- 分析尚不为信誉服务所知的某些文件行为。
- 在获得新信息时持续评估新出现的威胁，并在确定为威胁的文件进入您的网络后通知您。

此功能可用于传入邮件和传出邮件。

文件信誉服务在云中。文件分析服务提供适用于公共云或私有云（本地）的选项。

- 私有云文件信誉服务由思科 AMP 虚拟私有云设备提供，在“proxy”或“air-gap”（本地）模式下运行。请参阅配置本地文件信誉服务器，第 357 页。
- 私有云文件分析服务由本地思科 AMP Threat Grid 设备提供。请参阅配置本地文件分析服务器，第 357 页。

文件威胁判定更新

威胁判定可以随着新信息的出现而更改。文件最初可能会被评定为未知或正常，然后，因此，文件可能会被发送至收件人。如果获得新信息时威胁判定更改，您会收到警报，且文件及其新判定将出现在 AMP 判定更新报告中。可以调查进入点，作为补救任何威胁影响的起点。

判定还可能从恶意更改为干净。

当设备处理同一文件的后续实例时，系统将立即应用已更新的判定。

有关判定更新的定时信息包括在文件信誉和分析服务所支持的文件，第 355 页中引用的文件条件文档中。

文件处理概述

除非已对邮件采取最终操作，否则无论来自先前扫描引擎的判定如何，在防病毒扫描后都将立即评估文件信誉和发送文件进行分析。

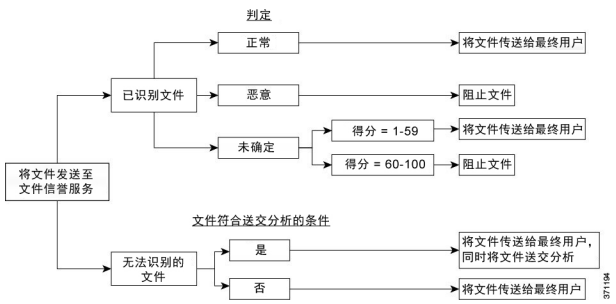
注释 默认情况下，如果邮件的 MIME 信头格式不正确，文件信誉服务将返回“不可扫描”的判定。设备还将尝试从该邮件中提取附件。如果设备无法提取附件，判定将保留为“不可扫描”。如果设备能够提取附件，则评估附件的文件信誉。如果附件是恶意的，判定将从“不可扫描”更改为“恶意”。

设备和文件信誉服务之间的通信已加密并已防止篡改。

评估文件的信誉后：

- 如果邮件不包含任何附件，则文件信誉服务将返回“已跳过”的判定。
- 如果文件为文件信誉服务所熟知且被确定为正常， 邮件继续通过工作队列。
- 对于邮件中的任何附件，，如果文件信誉服务返回恶意判定，则设备应用您在适用邮件策略中。
- 如果文件为信誉服务所知但信息不足以作出最后判定，则信誉服务基于文件特征（例如威胁指纹和行为分析）返回信誉得分。如果此分数达到或超过所配置的信誉阈值，则设备将应用您在邮件策略中为包含恶意软件的文件所配置的操作。
- 如果信誉服务没有文件相关信息，且文件不符合分析标准（请参阅文件信誉和分析服务所支持的文件，第 355 页），则将文件视为正常并且邮件继续通过工作队列。
- 如果启用了文件分析服务，信誉服务没有关于文件的信息，并且文件满足可以分析的文件的标准（请参阅文件信誉和分析服务所支持的文件，第 355 页），则可以隔离邮件（请参阅隔离附件送交分析的邮件，第 364 页）并将文件送交分析。如果在发送附件以供分析时尚未将设备配置为隔离邮件或者不发送文件以供分析，则系统会向该用户释放邮件。
- 对于具备本地文件分析的部署，信誉评估和文件分析同时进行。如果信誉服务返回判定结果，则使用该判定结果，这是因为信誉服务包含的信息具有更为广泛的来源。如果文件对于信誉服务来说是未知的，则会使用文件分析判定。
- 如果因为与服务器的连接超时而导致文件信誉判定信息不可用，则将该文件视为“不可扫描”，并应用配置的操作。

图 *33*: 面向公共云文件分析部署的高级恶意软件防护工作流程



如果将文件送交分析：

- 如果将文件发送到云进行分析：文件将通过 HTTPS 发送。
- 分析通常需要数分钟，但可能更长。
- 在文件分析后标记为恶意的文件可能不会被信誉服务识别为恶意文件。文件信誉由一段时间内的多种因素确定，而不一定由单一的文件分析判定来确定。
- 使用本地 Cisco AMP Threat Grid 设备分析文件的结果将缓存在本地。

有关判定更新的信息，请参阅文件威胁判定更新，第 353 页。

文件信誉和分析服务所支持的文件

信誉服务会评估大多数文件类型。文件类型识别由文件内容确定，并且不取决于文件扩展名。

可以分析某些信誉未知的文件来查找威胁特征。配置文件分析功能时，选择分析的文件类型。可以动态添加新类型；当可上传的文件类型列表变化时，则会收到警报，并可以选择添加的文件类型进行上传。

有关信誉及分析服务支持哪些文件的详细信息只向注册思科客户提供。有关评估和分析文件的信息，请参阅以下位置的思科内容安全产品高级恶意软件保护服务的文件条件：http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html。评估文件信誉和文件送交分析的标准可能随时变更。

要访问此文档，您必须拥有一个含有支持合同的思科客户帐户。要注册帐户，请访问 https://tools.cisco.com/RPF/register/register.do。

您应将策略配置为阻止传送并非由高级恶意软件保护处理的文件。

注释 已从源上传以进行分析的文件（传入邮件或传出邮件中的文件）不会再次上传。要查看此类文件的分析结果，请在“文件分析”(File Analysis) 报告页面中搜索 SHA-256。

存档或压缩文件处理

如果文件已压缩或存档，

- 则系统会评估压缩或存档文件的信誉。
- 将压缩或存档文件解压缩，并评估所有提取文件的信誉。

有关检查哪些存档和压缩文件的信息（包括文件格式），请参阅文件信誉和分析服务所支持的文件，第 355 页链接的信息。

在此情景中，

- 如果提取的其中一个文件是恶意的，则文件信誉服务会针对压缩或存档文件返回“恶意”判定。
- 如果压缩或存档文件是恶意的，并且所有已提取文件都是干净的，则文件信誉服务会针对压缩或存档文件返回“恶意”判定。
- 如果判定任何提取的文件为未知文件，则可以选择将提取的文件送交分析（如果已配置该功能且文件分析支持该文件类型）。

- 如果在对压缩或存档文件解压缩时文件提取失败，则文件信誉服务会针对压缩或存档文件返回“不可扫描”判定。请记住，在此情景中，如果提取的其中一个文件是恶意的，则文件信誉服务会针对压缩或存档文件返回“恶意”判定（“恶意”判定优先于“不可扫描”判定）。

注释 系统不会评估具有安全 MIME 类型（例如文本/纯文本）的已提取文件的信誉。

发送到云端的信息的隐私性

- 只有唯一标识文件的 SHA 才会发送到云端的信誉服务。不会发送文件本身。
- 如果使用云端的文件分析服务，并且文件符合分析条件，则该文件本身将发送到云端。
- 有关每个发送到云端进行分析并且判定为“恶意”的文件的信息将添加到信誉数据库中。此信息与其他数据共同用于确定信誉分数。

  有关现场 Cisco AMP Threat Grid 设备所分析文件的信息不会与信誉服务共享。

- 如果已将设备配置为允许将数据发送到 SenderBase 信誉服务，则会发送有关某些文件的信息。有关详细信息，请参阅思科邮件安全设备指南“SenderBase 网络参与”一章中关于 AMP 云的信息。

FIPS 合规性

文件信誉扫描和文件分析符合 FIPS 标准。

配置文件信誉和分析功能

与文件信誉和分析服务通信的要求

- 所有使用这些服务的邮件安全设备都必须能通过互联网直接与其连接（不包括配置为使用现场思科 AMP Threat Grid 设备的文件分析服务）。
- 默认情况下，与文件信誉和分析服务的通信。
- 默认情况下，通过与默认网关相关联的接口来路由与文件信誉分析服务和基于云的分析服务的通信。要通过其他接口路由此流量，请在“安全服务”(Security Services) >“文件信誉和分析”(File Reputation and Analysis) 页面的“高级”(Advanced) 部分中为每个地址创建静态路由。
- 必须打开以下防火墙端口：

防火墙端口	说明	协议	输入/输出	Hostname	设备接口
32137（默认）或 443	访问云服务获取文件信誉。	TCP	输出	如在“安全服务”>“防恶意软件和信誉”，“高级”部分的云服务器池参数中所配置的一样。	管理，除非将静态路由配置为通过数据端口路由该流量。
443	访问云服务以进行文件分析。	TCP	输出	如在“安全服务”>“防恶意软件和信誉”，“高级”部分中所配置的一样。	

配置本地文件信誉服务器

如果您将思科 AMP 虚拟私有云设备用作私有云文件分析服务器：

- 您可以从以下位置获得思科高级恶意软件保护虚拟私有云设备文档，包括安装和配置 FireAMP 私有云指南：
  http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/tsd-products-support-series-home.html

  使用此文档执行本主题中介绍的任务。

  其他文件可从 AMP 虚拟私有云设备的“帮助”链接获取。
- 在“代理”或“空隙”（本地部署）模式中设置和配置思科 AMP 虚拟私有云设备。
- 确保思科 AMP 虚拟私有云设备软件版本为 2.2，该版本可与思科邮件安全设备集成。
- 在该设备上下载 AMP 虚拟私有云证书和密钥，以便上传到此邮件安全设备
- 当邮件安全设备信任的根颁发机构未对隧道代理服务器证书签名时，请使用**根证书**选项跳过标准验证。

注释 设置本地文件信誉服务器之后，您将从此邮件安全设备配置与该服务器的连接；请参阅步骤 6 启用和配置文件信誉和分析服务，第 358 页

配置本地文件分析服务器

如果您将 Cisco AMP Threat Grid 设备用作私有云文件分析服务器：

- 获取《思科 AMP Threat Grid 设备设置和配置指南》以及《思科 AMP Threat Grid 设备管理指南》。思科 AMP Threat Grid 设备文档可从
  http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides%20-list.html
  获取。

  使用此文档可执行本主题中描述的任务。

  使用 AMP Threat Grid 设备中的“帮助”(Help) 链接可获取其他文档。

在《管理指南》中，请搜索有关下列所有各项的信息：与其他思科设备、CSA、思科沙盒API、ESA 以及邮件安全设备、的集成。

- 设置和配置思科 AMP Threat Grid 设备。
- 如果需要，请将思科 AMP Threat Grid 设备软件更新为版本 1.2.1，该版本支持与思科邮件安全设备的集成。

  有关确定版本号和执行更新的说明，请参阅 AMP Thread Grid 文件。

- 确保您的设备能够通过您的网络彼此通信。思科邮件安全设备必须能够连接到 AMP Threat Grid 设备的正常接口。
- 如果您要部署自签名证书：从思科 AMP Threat Grid 设备生成要在您的邮件安全设备上使用的自签名 SSL 证书。请参阅 AMP Threat Grid 设备管理员指南中有关下载 SSL 证书和密钥的说明。请务必生成一个将 AMP Threat Grid 设备主机名作为 CN 的证书。来自 AMP Threat Grid 设备的默认证书不起作用。
- 当您提交用于文件分析的配置时，系统将自动向 Threat Grid 设备注册您的邮件安全设备，如启用和配置文件信誉和分析服务，第358页中所述。但是，您必须按照同一程序中所述激活注册。

启用和配置文件信誉和分析服务

开始之前

- 获取文件信誉服务和文件分析服务的功能密钥，并将其传输到此设备。
- 符合与文件信誉和分析服务通信的要求，第 356 页。
- 验证与配置升级和服务更新设置中“更新”页面上。
- 如果您将思科 AMP Threat Grid 设备用作私有云文件信誉服务器，请参阅配置本地文件信誉服务器，第 357 页。
- 如果您将 Cisco AMP Threat Grid 设备用作私有云文件分析服务器，请参阅配置本地文件分析服务器，第 357 页。

步骤 1 选择**安全服务 > 文件信誉和分析**。

步骤 2 点击**编辑全局设置**。

步骤 3 点击**启用文件信誉过滤**和（可选）**启用文件分析**。

- 如果选中**启用文件信誉过滤**，则必须配置**文件信誉服务器**部分（在**步骤 6** 中），方式如下：选择外部公共信誉云服务器的 URL，或提供私有信誉云服务器连接信息。
- 同样，如果选中**启用文件分析**，则必须配置**文件分析服务器 URL** 部分（在**步骤 7** 中），方式如下：提供外部云服务器的 URL，或提供私有分析云连接信息。

步骤 4 接受许可协议（如果存在）。

步骤 5 展开**文件信誉的高级设置**面板，并根据需要调整下列选项：

选项	说明
云域 (Cloud Domain)	用于文件信誉查询的域的名称。
文件信誉服务器	选择公共信誉云服务器的主机名，或私有信誉云。 如果选择私有信誉云，请提供以下内容： • **服务器** - 思科 AMP 虚拟私有云设备的主机名或 IP 地址。 • **公钥** - 为此设备与您的私有云设备之间的加密通信提供有效的公钥。此公钥必须与私有云服务器使用的密钥相同：找到此设备上的密钥文件，然后点击**上传文件**。 **注释** 您必须已将此密钥文件从服务器下载到此设备。
文件信誉的 SSL 通信 (SSL Communication for File Reputation)	选中**使用 SSL (端口 443）(Use SSL [Port 443])** 以在端口 443 而不是默认端口 32137 上进行通信。有关启用对服务器的 SSH 访问的信息，请参阅《思科 AMP 虚拟私有云设备用户指南》。 **注释** 通过端口 32137 的 SSL 通信可能需要您在防火墙中打开该端口。 通过此选项，您还可配置上游代理来与文件信誉服务进行通信。如果选中此选项，请提供相应的**服务器**、**用户名**和**密码**信息。 选中**使用 SSL (端口 443)** 时，如果隧道代理服务器的证书未由受信任的根颁发机构签名，还可以选中**放宽证书验证**以跳过标准证书验证。例如，如果在受信任的内部隧道代理服务器上使用自签名证书，则选择此选项。 **注释** 如果在“文件信誉的高级设置”的“文件信誉的 SSL 通信”部分选中**使用 SSL (端口 443)**，则必须使用 CLI 命令 certconfig > CERTAUTHORITY > CUSTOM 或 Web 界面中的“网络”>“证书”（自定义证书颁发机构）将内部部署信誉服务器 CA 证书上的 AMP 添加到此设备上的证书存储库。从服务器获得此证书（“配置”>“SSL”>“云服务器”>“下载”）。
Heartbeat Interval	以分钟为单位的 ping 追溯事件频率。
信誉阈值 (Reputation Threshold)	可接受的文件信誉分数的上限。高于此阈值的分数表示文件被感染。 • **使用来自云服务的值 (60)** • **输入自定义值** - 默认值为 60。
查询超时 (Query Timeout)	信誉查询超时前经过的秒数。
处理超时 (Processing Timeout)	文件处理超时前经过的秒数。
文件信誉客户端 ID	文件信誉服务器上此设备的客户端 ID（只读）。

注释 在无思科支持指导的情况下，请勿更改本部分中的任何其他设置。

步骤 6 如果要使用云服务进行文件分析，请展开“文件分析的高级设置”面板并根据需要调整以下选项：

选项	说明
文件分析服务器 URL (File Analysis Server URL)	选择外部云服务器的名称 (URL) 或**私有分析云**。 如果指定外部云服务器，请选择与您的设备物理距离最近的服务器。系统将使用标准更新流程定期将新的可用服务器添加到该列表中。 选择私有分析云以使用内部部署的思科 AMP Threat Grid 设备进行文件分析，并提供以下内容： • **服务器** - 内部部署的私有分析云服务器的 URL。 • **证书颁发机构** - 选择**使用思科默认的证书颁发机构**或**使用上传的证书颁发机构**。 如果选择**使用上传的证书颁发机构**，请点击**浏览**，为此设备与私有云设备之间的加密通信上传有效的证书文件。此证书必须与私有云服务器使用的证书相同。
文件分析客户端 ID	文件分析服务器上此设备的客户端 ID（只读）。

步骤 7 （可选）如果要为文件信誉处置值配置缓存到期期限，请展开“缓存设置”面板。

步骤 8 提交并确认更改。

步骤 9 如果您使用现场 Cisco AMP Threat Grid 设备，请在 AMP Threat Grid 设备上激活此设备的帐户。

激活“用户”帐户的完整说明在 AMP Threat Grid 文档中提供。

a) 请记下页面部分底部显示的文件分析客户端 ID。此 ID 标识您将要激活的“用户”。
b) 登录 AMP Threat Grid 设备。
c) 选择**欢迎...> 管理用户**，并浏览到“用户详细信息”。
d) 根据邮件安全设备的文件分析客户端 ID 找到“用户”帐户。
e) 为设备激活该“user”帐户。

重要提示！文件分析设置中所需的更改

如果计划使用新的公共云文件分析服务，请务必阅读以下说明以保持数据中心隔离：

- 新文件分析服务器中不保留现有的设备分组信息。您必须在新文件分析服务器上对设备重新分组。
- 隔离到文件分析隔离区的邮件将会被保留到保留期。隔离区保留期过后，邮件将从文件分析隔离区中删除，并由 AMP 引擎重新扫描。然后，将该文件上传到新的文件分析服务器以进行分析，但不会再次将该邮件发送到文件分析隔离区。

有关详细信息，请参阅 http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html 中的思科 AMP Thread Grid 文档。

（仅公共云文件分析服务）配置设备组

对于发自组织内任意设备的待分析文件，为了允许组织内的所有内容安全设备可以在云中查看这些文件的文件分析结果详细信息，您需要将所有设备加入到同一设备组。

注释 可以在计算机级别配置设备组。无法在集群级别配置设备组。

步骤 1 选择**安全服务 > 文件信誉和分析**。

步骤 2 在“用于文件分析云报告的设备分组”部分中，输入文件分析组 ID。

- 如果这是要添加到组中的第一个设备，请为该组提供有用的标识符。
- 此 ID 区分大小写，并且不能包含空格。
- 提供的 ID 在将要共享有关上传以供分析的文件的数据的所有设备上必须相同。但在后续组设备上，不会验证该 ID。
- 如果未正确输入组 ID 或出于任何其它原因需要对其进行更改，则必须向思科 TAC 提交请求。
- 此更改会立即生效；它不需要“确认”(Commit)。
- 该组中的所有设备都必须配置为在云中使用相同的文件分析服务器。
- 一个设备只能属于一个组。
- 您可以随时将设备添加到组，但是只能添加一次。

步骤 3 点击**立即分组**。

哪些设备在分析组中？

步骤 1 选择**安全服务 > 文件信誉和分析**。

步骤 2 在“用于文件分析云报告的设备分组”部分中，点击**查看设备**。

步骤 3 要查看特定设备的**文件分析客户端 ID**，请查看以下位置：

设备	文件分析客户端 ID 的位置
邮件安全设备	**安全服务 > 文件信誉和分析**页面上的“文件分析的高级设置”部分。
网络安全设备	**安全服务 > 防恶意软件和信誉**页面上的“文件分析高级设置”部分。

设备	文件分析客户端 ID 的位置
安全管理设备	在**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)** 页面的底部。

配置用于文件信誉扫描和文件分析的邮件策略

步骤 1 依次选择**邮件策略 > 传入邮件策略**或**邮件策略 > 传出邮件策略**（如果适用）。

步骤 2 点击邮件策略的**高级恶意软件防护 (Advanced Malware Protection)** 列中的链接进行修改。

步骤 3 选择选项。

- 如果您没有现场 Cisco AMP Threat Grid 设备，并且不希望将文件发送至云（例如出于机密性原因），请取消选中**启用文件分析 (Enable File Analysis)**。
- 如果附件被视为“无法扫描”，则选择设备必须执行的操作。当设备因以下原因无法扫描文件时，附件被视为“无法扫描”：
  - **邮件错误**：
    - 受密码保护的存档或压缩文件
    - 存在 RFC 违规的邮件。
    - 包含 200 个以上子文件的邮件
    - 包含五个以上嵌套级别的子文件的邮件
    - 提取失败的邮件
  - **速率限制** - 文件分析服务器未扫描文件，因为设备已达到文件上传限制。
  - **AMP 服务不可用**：
    - 文件信誉服务不可用。
    - 文件分析服务不可用。
    - 文件信誉查询超时
    - 文件上传查询超时
- 您可以对 AMP 引擎未扫描的邮件配置下列任一邮件处理操作：
  - 删除邮件
  - 原样传送邮件
  - 将邮件发送到策略隔离区

- 如果选择传递邮件，请选择以下附加操作：
  - 是否将原始邮件存档。存档邮件以 mbox 格式日志文件存储在设备上的 amparchive 目录中。需要预配置的 AMP 存档 (amparchive) 日志订用。
  - 是否通过修改邮件主题来警告终端用户，例如，[警告：附件可能包含恶意软件]。
  - 是否添加自定义报头，以向管理员提供精细控制。
  - 是否修改邮件收件人，使邮件传送至其他地址。点击“是”，并输入新的收件人地址。
  - 是否将无法扫描的邮件发送到备用目标主机。点击“是”，并输入备用 IP 地址或主机名。
- 如果选择将邮件发送到策略隔离区，请选择以下附加操作：
  - 是否从下拉列表中选择策略隔离区。当标记为隔离时，邮件到达邮件管道的末尾时，将放置在隔离区中，并由邮件管道中的所有其他引擎进行扫描。
  - 是否将原始邮件存档。存档邮件以 mbox 格式日志文件存储在设备上的 amparchive 目录中。需要预配置的 AMP 存档 (`amparchive`) 日志订用。
  - 是否通过修改邮件主题来警告终端用户，例如，[警告：附件可能包含恶意软件]。
  - 是否添加自定义信头来向管理员提供精细控制。
- 选择附件被视为“恶意”时 AsyncOS 必须执行的操作。以下选项
  - 传送还是丢弃邮件。
  - 是否将原始邮件存档。存档邮件以 mbox 格式日志文件存储在设备上的 amparchive 目录中。需要预配置的 AMP 存档 (amparchive) 日志订用。
  - 是否在删除恶意软件附件后传送邮件。
  - 是否通过修改邮件主题来警告终端用户，例如，[警告：在附件中检测到恶意软件]。
  - 是否添加自定义报头，以向管理员提供精细控制。
  - 是否修改邮件收件人，使邮件传送至其他地址。点击**是 (Yes)**，并输入新的收件人地址。
  - 是否将恶意邮件发送到备用目标主机。点击**是**，并输入备用 IP 地址或主机名。
- 选择附件被发送进行文件分析时 AsyncOS 必须执行的操作。以下选项
  - 传送还是隔离邮件。
  - 是否将原始邮件存档。存档邮件以 mbox 格式日志文件存储在设备上的 amparchive 目录中。需要预配置的 AMP 存档 (amparchive) 日志订用。
  - 是否通过修改邮件主题来警告终端用户，例如，“[警告：附件可能包含恶意软件]”。
  - 是否添加自定义报头，以向管理员提供精细控制。
  - 是否修改邮件收件人，使邮件传送至其他地址。点击**是 (Yes)**，并输入新的收件人地址。

- 是否将发送进行文件分析的邮件发送到备用目标主机。点击**是**，并输入备用 IP 地址或主机名。

- （仅用于传入邮件策略）配置当威胁判决更改为恶意时，对发送给终端用户的邮件将执行的补救操作。选择“启用邮箱自动补救”并选择下列操作之一：
  - 转发到某个邮件地址。选择此选项可将包含恶意附件的邮件转发给指定用户，例如邮件管理员。
  - 删除邮件。选择此选项可从终端用户的邮箱中永久删除包含恶意附件的邮件。
  - 转发到邮件地址并删除该邮件。选择此选项可将包含恶意附件的邮件转发给指定用户（例如邮件管理员），并从终端用户的邮箱中永久删除该邮件。

    注释 由于Office 365服务不支持删除这些文件夹中的邮件，因此无法删除来自某些文件夹（例如，已删除邮件）的邮件。

  重要事项 在配置“邮箱自动补救”设置之前，请查看 自动修补 Office 365 邮箱中的邮件，第 435 页

步骤 4 提交并确认更改。

隔离附件送交分析的邮件

您可以将设备配置为隔离已发送进行分析的文件，而不是立即将其放行到工作队列。隔离的邮件及其附件在从隔离区中放行时会进行重新扫描以查找威胁。如果在文件分析结果可供信誉扫描程序使用后放行邮件，则在重新扫描过程中将捕获识别的任何威胁。

步骤 1 依次选择**邮件策略 > 传入邮件策略** 或**邮件策略 > 传出邮件策略**（如果适用）。

步骤 2 点击邮件策略的**高级恶意软件保护**列中的链接进行修改。

步骤 3 在“文件分析待定的邮件”(Messsages with File Analysis Pending) 部分下面，从“应用于邮件的操作”(Action Applied to Message) 下拉列表中选择**隔离 (Quarantine)**。

隔离的邮件存储在文件分析隔离区中。请参阅使用文件分析隔离，第 365 页。

步骤 4 （可选）在“文件分析待处理的邮件”(Messages with File Analysis Pending) 部分下，选择以下操作：

- 是否将原始邮件存档。存档消息作为 mbox 格式日志文件存储在设备上的 amparchive 目录中。需要预配置的 AMP 存档 (amparchive) 日志订用。
- 是否通过修改邮件主题来警告终端用户，例如，“[警告：附件可能包含恶意软件]”。
- 是否添加自定义报头，以向管理员提供精细控制。

注释　仅当从隔离区释放邮件而非将该邮件发送到隔离区时，步骤 4 中提到的上述操作才会适用：

- 存档原始邮件。
- 修改邮件主题。
- 添加自定义信头。

步骤 5 提交并确认更改。

下一步做什么

相关主题

使用文件分析隔离，第 365 页

使用文件分析隔离

编辑文件分析隔离区设置

步骤 1 选择**监控** > **策略、病毒和爆发隔离区**。

步骤 2 点击**文件分析(File Analysis)** 隔离区链接。

步骤 3 指定保留期。

不建议更改为有别于默认值（1 小时）的值。

步骤 4 请指定保留期经过后 AsyncOS 必须采取的默认操作。

步骤 5 如果您不希望在指定的保留期结束之前处理此隔离区中的邮件，即使隔离区磁盘空间已满也如此，请取消选择**通过在空间溢出后对邮件应用默认操作来释放空间 (Free up space by applying default action on messages upon space overflow)**。

步骤 6 如果选择**释放** (Release) 作为默认操作，则可以根据情况指定要应用于在保留期之前释放的邮件的其他操作：

选项	信息
修改主题 (Modify Subject)	键入要添加的文本并选择要将其添加到原始邮件主题的开头还是结尾。 例如，您可能希望警告收件人，该邮件可能包含恶意软件附件。 注释　要正常显示使用非 ASCII 字符的主题，必须根据 RFC 2047 进行表示。

选项	信息
添加 X-Header (Add X-Header)	X 报头可提供对邮件采取的操作的记录。这可能会非常有用，例如在处理有关传送特定邮件的原因的查询时。 输入名称和值。 示例： 名称 = Inappropriate-release-early 值 = True
删除附件 (Strip Attachments)	删除附件可防御邮件中包含的恶意软件附件。

步骤 7 指定可以访问此隔离区的用户：

用户	信息
本地用户	本地用户列表仅包含具有可以访问隔离区的角色的用户。 该列表不包括具有管理员权限的用户，因为所有管理员都对隔离区具有完全访问权限。
以外部方式进行身份验证的用户 (Externally Authenticated Users)	您必须已配置外部身份验证。
自定义用户角色	仅当您已创建至少一个具有隔离区访问权限的自定义用户角色时，才会看到此选项。

步骤 8 提交并确认更改。

手动处理文件分析隔离区中的邮件

步骤 1 选择**监控** > **策略、病毒和爆发隔离区**。

步骤 2 在文件分析隔离区的对应行中，点击表的“邮件” (Messages) 列中的蓝色数字。

步骤 3 根据要求，对邮件执行以下操作：

- 删除
- 发布
- 延迟从隔离区计划退出
- 将邮件副本发送到您指定的邮件地址

集中文件分析隔离区

有关集中文件分析隔离的信息, 请参阅 Cisco 电子邮件安全装置指南 中的 "集中策略、病毒和爆发隔离" 一章。

文件信誉和分析 X 报头

您可以使用 X-Header 来标记带有操作的邮件和邮件处理步骤的结果在邮件策略中使用 X-Header 标记邮件，然后使用内容过滤器选择这些邮件的处理选项和最终操作。

值区分大小写。

标头名称	可能的值（区分大小写）	说明
X-Amp-Result	清洁 恶意 不可扫描	判定适用于文件信誉服务所处理的消息。
X-Amp-Original-Verdict	文件未知 判定未知	基于信誉阈值的调整前的判定。仅当原始判定是其中一个可能的值时，此信头才存在。
X-Amp-File-Uploaded	true false	如果将附加至消息的任何文件送交分析，则该报头为“真”(true)。

向最终用户发送有关已丢弃邮件或附件的通知

要在根据文件信誉扫描丢弃可疑附件或其父邮件后向最终用户发送通知，请使用 X 报头或自定义报头和内容过滤器。

高级恶意软件防护和集群

如果您使用集中管理，则可以在集群、组和计算机级别启用高级恶意软件防护和邮件策略。

必须在计算机级别添加功能密钥。

不应在群集级别配置设备组。

确保接收有关高级恶意软件防护问题的警报

确保设备配置为向您发送与高级恶意软包含相关的警报。

当出现以下情况时，您将收到警报：

警报说明	类型	严重性
您正在建立与现场（私有云）思科 AMP Threat Grid 设备的连接，并且需要激活帐户，如中所述。启用和配置文件信誉和分析服务，第358页	防恶意软件	警告
功能密钥过期	（作为所有功能的标准）	
不可访问文件信誉或文件分析服务。	防病毒和 AMP	警告
与云服务建立通信。	防病毒和 AMP	信息
信誉和分析引擎由监视程序服务重新启动	防病毒和 AMP	信息
文件信誉判定更改。	防病毒和 AMP	信息
可以发送进行分析的文件类型已更改。您可能需要启用上传新文件类型。	防病毒和 AMP	信息
暂时无法分析某些文件类型。	防病毒和 AMP	警告
临时性中断后恢复分析所有受支持文件类型。	防病毒和 AMP	信息

配置高级恶意软件防护功能的集中报告

如果您将在安全管理设备上集中报告，请参阅管理设备的联机帮助或用户指南的邮件报告章节中“高级恶意软件防护”部分中的重要配置要求。

文件信誉和文件分析报告与跟踪

通过 SHA-256 散列标识文件

由于文件名很容易更改，因此设备会使用安全散列算法 (SHA-256) 为每个文件生成标识符。如果设备处理具有不同名称的同一文件，所有实例被识别为相同的 SHA-256。如果多个设备处理相同的文件，则该文件的所有实例都具有相同的 SHA-256 标识符。

在大多数报告中，文件按其 SHA-256 值列出（以缩写格式

文件信誉和文件分析报告页面

报告	说明
高级恶意软件防护	显示由文件信誉服务识别的基于文件的威胁。 对于那些具有已更改判定的文件，请参阅 AMP 判定更新报告。这些判定不会反映在“高级恶意软件保护”(Advanced Malware Protection) 报告中。 **注释** 如果从压缩或存档文件中提取的某个文件是恶意文件，则高级恶意软件防护报告中仅包含压缩或存档文件的 SHA 值。 要查看面向终端的 AMP 控制台中已列入黑名单的文件 SHA 的文件轨迹详细信息，请执行以下步骤： **1.** 选择**报告** > **文件分析**。 **2.** 点击要查看其轨迹详细信息的文件 SHA 链接。 **3.** 点击**更多详细信息**部分中的 AMP 控制台链接。 您可以在报告的“AMP 处理的传入文件”部分查看**低风险**判定详细信息。
高级恶意软件保护文件分析	显示送交分析的每个文件的时间和判定（或临时判定）。 在思科 AMP Threat Grid 设备上已列入白名单的文件显示为“正常”。有关白名单的信息，请参阅 AMP Threat Grid 联机帮助。 要查看超过 1000 个文件分析结果，请将数据导出为 .csv 文件。 深入查看详细分析结果，包括每个文件的威胁特征和得分。 您还可以直接在执行分析的 AMP Threat Grid 设备或云服务器上查看有关 SHA 的其他详细信息，方法是搜索 SHA 或点击文件分析详细信息页面底部的思科 AMP Threat Grid 链接。 **注释** 如果从某个压缩文件或存档文件中提取的文件送交文件分析，则只有这些已提取文件的 SHA 值包括在“文件分析”(File Analysis) 报告中。
高级恶意软件保护裁决更新	列出由该设备处理且在后判定已更改的文件。有关这种情况的信息，请参阅文件威胁判定更新，第 353 页。 要查看超过 1000 个判定更新，请将数据导出为 .csv 文件。 如果单个 SHA-256 的判定多次发生变化，则此报告仅显示最新判定，而不显示判定历史记录。 点击 SHA-256 链接会显示 要查看在最大可用时间范围内（不管选定的报告时间范围如何）特定 SHA-256 的所有受影响邮件，请点击 SHA-256 链接

查看其他报告中的文件信誉过滤数据

在相关的情况下，其他报告中会提供文件信誉和分析的数据。默认情况下，“被高级恶意软件防护阻止检测”列在适用报告中可能被隐藏。要显示其他列，请点击表格下方的“列“(Columns)链接。

关于邮件跟踪和高级恶意软件保护功能

在“邮件跟踪”中搜索文件威胁信息时，请注意以下几点：

- 要搜索文件信誉服务找到的恶意文件，请在**积极的高级恶意软件保护**。
- “邮件跟踪”仅包括处理事务邮件时返回的文件信誉处理和原始文件信誉判定的相关信息。例如，如果最初发现文件是干净的，然后判定更新发现文件是恶意的，则在跟踪结果中仅显示干净判定。

  在“邮件跟踪”(Message Tracking)详细信息的“处理详细信息”(Processing Details)部分显示：

  - 邮件中每个附件的 SHA-256；
  - 邮件的整体最终高级恶意软件保护判定，以及
  - 发现包含恶意软件的任何附件。

- 判定更新仅在AMP判定更新报告中可用。“邮件跟踪”中的原始邮件详细信息不会随着判定变化而更新。要查看涉及特定文件邮件（具有特定附件）的事务，请点击判定更新报告中的SHA-256。
- 有关文件分析的信息（包括分析结果以及是否发送文件进行分析）仅在文件分析报告中可用。

  有关所分析的文件的其他信息，可从云端或现场文件分析服务器获取。要查看文件的任何可用文件分析信息，请依次选择**报告监控 > 文件分析**，然后输入 SHA-256 搜索文件或。如果文件分析服务已从任意来源分析了该文件，您可以查看该详细信息。系统仅会为已分析的文件的结果。

  如果设备处理了送交分析的某个文件的后续实例，这些实例将显示在“邮件跟踪”搜索结果中。

在文件威胁判定更改时采取操作

步骤 1 查看“AMP 判定更新”(AMP Verdict Updates)报告。

步骤 2 点击相关的 SHA-256 链接查看所有事务的 Web 消息跟踪数据，这些事务涉及包含终端用户的文件。

步骤 3 使用跟踪数据标识可能已危及用户、违规中所涉及的文件名等信息以及文件发件人。

步骤 4 检查“文件分析”(File Analysis)报告查看是否将该 SHA-256 送交分析，以更详细地了解文件威胁行为。

故障排除文件信誉和分析

日志文件

在日志中：

- AMP 和 amp 是指文件信誉服务或引擎。
- Retrospective 是指判定更新。
- VRT 和 sandboxing 是指文件分析服务。

将有关高级恶意软件保护（包括文件分析）的信息记录在 AMP 引擎日志中。

文件信誉过滤和分析事件记录在 AMP 引擎日志和邮件日志中。

在日志消息“文件信誉查询收到的响应”中，“上传操作”的可能值为：

- 0：文件不为信誉服务所知；不送交分析。
- 1：发送
- 2：文件不为信誉服务所知；不送交分析。

对于邮件日志中的“Disposition”：

- 1: 未检测到恶意软件，或假定为正常（视为正常）
- 2：正常
- 3：恶意软件

Spyname 是威胁名称。

使用跟踪

跟踪不可用于文件信誉过滤和分析功能。请改为从组织外的帐户发送测试消息。

有关无法连接至文件信誉或文件分析服务器的若干警报

问题

您收到有关无法连接到云中的文件信誉或分析服务的若干警报。（单个警报可能仅表示瞬态问题。）

解决方案

- 确保符合与文件信誉和分析服务通信的要求，第 356 页中的要求。
- 检查可能阻止设备与云服务进行通信的网络问题。
- 增加查询超时值：

  选择**安全服务 > 文件信誉和分析**。“查询超时”值出现在“高级”设置区域中。

API 密钥错误（本地文件分析）

问题

您在尝试查看“文件分析”报告详细信息时收到API密钥警告，或者 邮件安全设备无法连接到AMP Threat Grid 服务器以上传要分析的文件。

解决方案

如果更改 AMP Threat Grid 服务器的主机名并且使用来自 AMP Threat Grid 服务器的自签名证书，则会出现该错误。此外，在其他情况下也有可能出现。解决问题：

- 从拥有新主机名的 AMP Threat Grid 设备生成新证书。
- 将新证书上传到邮件安全设备。
- 在 AMP Threat Grid 设备上重置 API 密钥。有关说明，请参阅 AMP Threat Grid 设备的在线帮助。

未按预期上传文件

问题

未按预期评估或分析文件。无警报或明显错误。

解决方案

请考虑以下方面：

- 该文件可能已由另一设备送交分析，因此已存在于文件分析服务器上，或存在于正在处理该文件的设备的缓存中。

有关可送交分析的文件类型警报

问题

您会收到有关可送交文件分析的文件类型严重性信息警报。

解决方案

受支持文件类型更改或检查设备以查看受支持的文件类型时，发送该警报。这可能会出现于：

- 您或其他管理员更改选作分析的文件类型时。
- 基于云服务可用性受支持文件类型暂时改变。在这种情况下，将尽快恢复设备上选定的文件类型支持。两个过程均是动态的，您无需进行任何操作。
- 设备重新启动，例如作为 AsyncOS 升级的一部分。

第 18 章

数据防泄漏

本章包含以下部分：

防数据丢失概述

防数据丢失 (DLP) 功能可以防止用户恶意或无意中通过邮件将您网络中的敏感数据发送出去，从而保护您的组织的专有信息和知识产权，同时强制遵守政府法规。您可通过创建 DLP 策略来定义不允许员工通过邮件发送的数据类型，这些策略用于扫描外发邮件，确定其中是否包含任何可能违反法律或公司政策的数据。

DLP 扫描过程概述

	操作	更多信息
1.	在您的组织中，某位用户给组织外部的收件人发送了一封邮件。	邮件安全设备是一个“网关”设备，用于处理进入或离开您的网络的邮件。 发送给您的网络内其他用户的邮件不会受到扫描。

	操作	更多信息
2.	邮件安全设备将在邮件到达 DLP 扫描阶段之前，在其邮件“工作队列”的各个阶段对邮件进行处理。	例如，DLP扫描前的过程可确保邮件不包含垃圾邮件或恶意软件。 要了解在工作队列的什么位置进行 DLP 处理，请参阅邮件管道流，第 51 页中的工作队列流程图。
3.	此设备将扫描邮件正文、信头和附件，确定其中是否包含 DLP 策略中标识的敏感内容。	请参阅防数据丢失的工作原理，第 374 页。
4.	如果发现敏感内容，该设备将采取措施保护数据，如隔离邮件、丢弃邮件，或在传送时施加限制。 否则，该邮件将在设备的工作队列中继续传送，如果未发现任何问题，邮件安全设备便会将其传送给收件人。	要采取的操作由您定义。请参阅邮件操作，第 390 页。

防数据丢失的工作原理

当您的组织中的某人向组织外的收件人发送邮件时，此设备将根据您定义的规则，确定要应用于该邮件的发件人或收件人的外发邮件策略。此设备将使用该外发邮件策略中指定的DLP策略来评估邮件内容。

具体而言，该设备将扫描邮件内容（包括标题和附件），查找其中是否包含与您在适用的DLP策略中确定为敏感内容的词汇、短语、预定义模式（如社会保障号）或正则表达式相匹配的文本。

该设备还将评估禁止内容的上下文，以尽量减少误报匹配。例如，某个数字与信用卡号模式相匹配，如果还随该数字一起提供了到期日期、信用卡公司名称（Visa、AMEX等）或者某人的姓名和地址，则只能认定该数字违规。

如果邮件内容与多个DLP策略相匹配，则根据您指定的顺序，列表中第一个匹配的DLP策略适用。如果某项传出邮件策略包含多项 DLP 策略，这些 DLP 策略使用相同条件来确定内容否违规，则所有这些策略都将使用单个内容扫描所产生的结果。

当邮件中出现可能敏感的内容时，该设备将为可能违规的内容分配一个介于 0 - 100 之间的风险因素得分。此得分表示邮件包含 DLP 违规的可能性。

随后，该设备将分配您为该风险因素得分定义的严重性级别（如“关键”(Critical)或“低”(Low)），并执行您在适用的 DLP 策略中为该严重性级别指定的邮件操作。

防数据丢失的系统需求

除使用 D-模式许可证的设备以外，所有受支持的 C 系列和 X 系列设备都支持防数据丢失。

防数据丢失的设置方式

请按顺序执行下列步骤：

过程

	命令或操作	目的
步骤 1	启用 DLP 功能。	启用防数据丢失 (DLP)，第 375 页
步骤 2	定义对于在其中发现或怀疑其中存在违规的邮件可以采取的可能操作。例如，您可隔离此类邮件。	邮件操作，第 390 页
步骤 3	创建 DLP 策略，这些策略将： • 标识不得从您的组织通过邮件发送的内容，并且 • 指定对于每一项违规将采取的操作。	选择一种方法： • 使用向导来设置 DLP 防护，第 377 页 • 使用预定义模板创建 DLP 策略，第 378 页 • 创建自定义 DLP 策略（高级），第 379 页
步骤 4	设置 DLP 策略的顺序，以确定当内容可能与多个 DLP 策略匹配时，使用哪个 DLP 策略来评估邮件是否发生 DLP 违规。	排列邮件 DLP 策略用于违规匹配的顺序，第 389 页
步骤 5	对于要扫描其邮件是否发生 DLP 违规的每一组发件人和收件人，确保您已创建相应的外发邮件策略。	请参阅 邮件策略，第 223 页 要在各个 DLP 策略中进一步优化允许的及限制的邮件发件人和收件人，请参阅根据 DLP 策略过滤邮件，第 387 页。
步骤 6	通过将 DLP 策略分配给外发邮件策略，指定哪些 DLP 策略应用于哪些发件人和收件人。	将 DLP 策略与传出邮件策略关联，第 389 页
步骤 7	配置敏感 DLP 信息的存储设置及访问设置。	• 在邮件跟踪中显示敏感 DLP 数据，第 395 页 • 控制对“邮件跟踪”中敏感信息的访问权限，第 727 页

启用防数据丢失 (DLP)

步骤 1 选择**安全服务 > 防数据丢失**。

步骤 2 点击**启用 (Enable)**。

步骤 3 滚动到许可协议页面底部，并点击**接受 (Accept)** 以接受该协议。

注释 如果您不接受许可协议，则不会在设备上启用 DLP。

步骤 4 在**防数据丢失全局设置**下，选择**启用防数据丢失**。

步骤 5 （建议）目前，请取消选择此页面上的其他选项。

您稍后可根据本章中其他部分提供的说明来更改这些设置。

步骤 6 提交并确认更改。

下一步做什么

请参阅防数据丢失的设置方式，第 375 页。

防数据丢失策略

DLP 策略说明

DLP 策略包含以下内容：

- 一组条件，用于确定外发邮件是否包含敏感数据，以及
- 当邮件包含敏感数据时要采取的操作。

您可指定如何根据以下条件来评估邮件内容：

- 不允许的特定内容或信息模式。根据策略，您可能需要创建正则表达式以搜索标识号。请参阅关于使用内容匹配分类器来定义不允许的内容，第 380 页。
- 特定发件人和收件人的列表，用于过滤邮件。请参阅根据 DLP 策略过滤邮件，第 387 页。
- 附件文件类型的列表，用于过滤邮件。请参阅根据 DLP 策略过滤邮件，第 387 页。
- 允许根据违规的严重性来采取不同操作的设置。请参阅关于评估违规严重性，第 388 页。

您在外发邮件策略中启用 DLP 策略时，应确定应用每个策略的邮件发件人及收件人。

预定义的 DLP 策略模板

为了简化 DLP 策略的创建，设备包括大量预定义策略模板。

模板类别包括：

- **合规性**。这些模板用于识别包含个人身份信息、信用信息或者其他受保护或非公共信息的邮件及附件。
- **使用规定**。这些模板用于识别发送给竞争对手或受限收件人的包含组织敏感信息的邮件。
- **隐私保护**。这些模板用于识别包含财务帐户识别号、报税记录或身份证号码的邮件及附件。
- **知识产权保护**。这些模板用于识别可能包含组织想要保护的知识产权的常用发布和设计文档文件类型。
- **公司机密**。这些模板用于识别包含公司会计信息及即将进行的合并和收购的相关信息的文档及邮件。

- **自定义策略**。这个“模板”允许您使用预定的内容匹配分类器或者组织所指定的违规识别条件，从头创建您自己的策略。这是一个高级选项，只应该在预定义策略模板无法满足网络环境的独特要求的极少数情况下使用。

这其中的一些模板需要自定义。

使用向导来设置 DLP 防护

DLP 评估向导可帮助您配置常用的 DLP 策略，并在设备的默认外发邮件策略中启用这些策略。

注释 默认情况下，使用 DLP 评估向导添加的 DLP 策略将传送所有邮件，而不考虑所检测到的 DLP 违规的严重性。您需要对使用此向导创建的策略进行编辑。

准备工作

- 从设备中删除所有的现有 DLP 策略。仅当设备上不存在现有的 DLP 策略时，才能使用 DLP 评估向导。
- 如果您需要检测包含除信用卡号、美国社会保险号和美国驾驶执照号码以外的学生标识号或帐号的邮件，请创建识别这些号码的正则表达式。有关详细信息，请参阅用于识别标识号的正则表达式，第 383 页。

步骤 1 选择**安全服务 > 防数据丢失**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选中**使用 DLP 评估向导启用并配置 DLP (Enable and configure DLP using the DLP Assessment Wizard)** 复选框。

步骤 4 点击 **Submit**。

步骤 5 完成向导。

记住以下几点：

- 任何在美国加利福尼亚州开展业务并且拥有或许可使用加利福尼亚州居民的计算机化个人身份信息 (PII) 数据的企业，无论其实体位置在哪，均需遵守**美国国家法规（加利福尼亚州 SB-1386 号法案）**。此法律是该向导中的策略选择之一。
- 如果您不输入用于接收自动生成的计划内 DLP 事件摘要报告的邮件地址，则不会生成该报告。
- 在审核已配置的设置时，如果您返回到某个步骤进行更改，则必须继续完成余下的步骤，直至再次到达审核页面为止。系统将记住您先前输入的所有设置。
- 完成此向导时，将显示“外发邮件策略”(Outgoing Mail Policies) 页面，并且已在默认外发邮件策略中启用您的 DLP 策略。您的 DLP 策略配置摘要将显示在该页面顶部。

步骤 6 确认您的更改。

下一步做什么

- （可选）要编辑这些 DLP 策略、创建其他策略、更改对邮件执行的总体操作，或更改严重性级别设置，请依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。有关信息，请参阅使用预定义模板创建 DLP 策略，第 378 页、创建自定义 DLP 策略（高级），第 379 页和调整严重性刻度，第 388 页。
- （可选）要为其他外发邮件策略启用现有的 DLP 策略，请参阅使用外发邮件策略向发件人和收件人指定 DLP 策略，第 390 页。

使用预定义模板创建 DLP 策略

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。

步骤 2 点击**添加 DLP 策略 (Add DLP Policy)**。

步骤 3 点击类别名称，以显示可用的 DLP 策略模板的列表。

注释 要查看每个模板的说明，请点击**显示策略说明 (Display Policy Descriptions)**。

步骤 4 对于您想要使用的 DLP 策略模板，点击**添加**。

步骤 5 （可选）更改该模板的预定义名称和说明。

步骤 6 如果策略要求或建议自定义一个或多个内容匹配分类器，请输入一个正则表达式以定义您的组织的标识编号系统模式，并输入一系列与标识号相关的字词或短语，这些字词或短语将它们标识为标识号或者通常与其相关联。

有关信息，请参阅：

关于使用内容匹配分类器来定义不允许的内容，第 380 页和 用于识别标识号的正则表达式，第 383 页。

注释 无法为基于预定义模板的策略添加或删除内容匹配分类器。

步骤 7 （可选）只能将 DLP 策略应用于具有特定收件人、发件人、附件类型或先前添加的邮件标记的邮件。

有关详细信息，请参阅根据 DLP 策略过滤邮件，第 387 页。

您可使用换行符或逗号来分隔多个条目。

步骤 8 在“严重性设置”(Severity Settings) 部分：

- 选择针对每个违规严重性级别要采取的操作。有关详细信息，请参阅关于评估违规严重性，第 388 页。
- （可选）点击**编辑刻度 (Edit Scale)**，以调整该策略的违规严重性刻度。有关详细信息，请参阅调整严重性刻度，第 388 页。

步骤 9 提交并确认更改。

创建自定义 DLP 策略（高级）

注释 创建自定义策略非常复杂；仅当预定义 DLP 策略模板无法满足您的组织需求时，才应创建自定义策略。

您可使用自定义策略模板从头开始创建自定义 DLP 策略，然后向该策略添加预定义内容匹配分类器或自定义分类器。

如果内容与一个或所有分类器匹配，则自定义策略可以根据策略的定义方式返回 DLP 违规。

准备工作

建议：定义可识别内容违规的条件。请参阅为自定义 DLP 策略创建内容匹配分类器，第 382 页。您也可以在此过程中定义这些条件。

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。

步骤 2 点击**添加 DLP 策略 (Add DLP Policy)**。

步骤 3 点击**自定义策略**。

步骤 4 对于自定义策略模板，点击**添加 (Add)**。

步骤 5 输入该策略的名称和说明。

步骤 6 标识构成 DLP 违规的内容和上下文：

a) 选择内容匹配分类器。

b) 点击 **Add**。

- 如果您已选择**创建分类器**，请参阅为自定义 DLP 策略创建内容匹配分类器，第 382 页。
- 否则，选择的分类器将添加到表中。

c) （可选）将其他分类器添加到策略。

例如，您可以通过添加另一个分类器并选择“否”(NOT)，消除已知可能发生的误报匹配。

d) 如果您已添加多个分类器：请在表格标题中选择一个选项，以指定是匹配**任何**分类器即可使实例计作违规，还是必须匹配**全部**分类器才会计作违规。

步骤 7 （可选）将该 DLP 策略仅应用于具有特定收件人、发件人、附件类型或先前添加的邮件标记的邮件。

有关详细信息，请参阅根据 DLP 策略过滤邮件，第 387 页。

您可使用换行符或逗号来分隔多个条目。

步骤 8 在“严重性设置”(Severity Settings) 部分：

- 选择要为每个违规严重性级别采取的操作。有关详细信息，请参阅关于评估违规严重性，第 388 页。
- （可选）点击**编辑刻度 (Edit Scale)**，以调整该策略的违规严重性刻度。有关详细信息，请参阅调整严重性刻度，第 388 页

步骤 9 提交并确认更改。

关于使用内容匹配分类器来定义不允许的内容

内容匹配分类器定义不能通过邮件发送的内容，还可（可选）定义内容必须处于何种上下文才会被视为防数据丢失违规。

假设您希望防止通过邮件将患者标识号从您的组织中发送出去。

要让设备识别这些号码，您必须使用一个或多个正则表达式指定您的组织所使用的记录编号系统的模式。您还可以添加一系列可能作为支持信息伴随记录号一起出现的字词和短语。如果分类器在某一传出邮件中检测到相应的号码模式，它将搜索支持信息，以验证该模式是标识号而不是随机数字符串。包括上下文匹配信息可以减少误报匹配。

对于此示例，您可以创建一项使用 HIPAA 和 HITECH 模板的 DLP 策略。此模板包含“患者标识号”内容匹配分类器，您可自定义该分类器，以检测患者标识号。要检测 123-CL456789 模式的号码，请为分类器输入正则表达式 [0-9]{3}\-[A-Z]{2}[0-9]{6}。输入“患者 ID”，作为相关短语。完成创建该策略，并在外发邮件策略中将其启用。提交并确认更改。现在，如果该策略在外发邮件中检测到此数字模式旁边出现短语“患者 ID”，则 DLP 策略会返回 DLP 违规。

关于在 DLP 策略中使用内容匹配分类器

许多预定义的 DLP 策略模板包含来自 RSA 的内容匹配分类器。其中的一些分类器要求进行自定义，才能识别您组织中的数据所使用的模式。

如果创建自定义 DLP 策略，可以选择自定义分类器，或者创建自己的分类器。

内容匹配分类器示例

以下示例显示分类器如何匹配邮件内容：

信用卡号

多个 DLP 策略模板包含“信用卡号”分类器。信用卡号本身受各种约束制约，例如数字和标点的模式、发卡行专用前缀以及最终校验位。分类器需要额外的支持信息才能做出匹配决策，例如，到期日期、发卡行名称。这将减少误报的数量。

示例：

- `378734493671000`（因为没有支持信息，所以不匹配）
- `378734493671000 VISA`（匹配）
- `378734493671000 exp: 12/2019`（匹配）

美国社会保险号

“美国社会保险号”分类器需要格式正确的号码以及支持数据（例如出生日期、姓名或字符串 SSN）。

示例：

- `321-02-3456`（因为没有支持信息，所以不匹配）

- SN: 281234123458（匹配）

ABA 路由编号

“美国银联转帐号”分类器与“信用卡号”分类器类似。

示例：

- 119999992（因为没有支持信息，所以不匹配）
- ABA No.800000080（匹配）

驾驶执照编号（美国）

许多策略使用“美国驾驶执照”分类器。默认情况下，此分类器将搜索在美国颁发的驾驶执照。美国政府特定的策略（如加利福尼亚 AB-1298 和蒙大拿 HB-732）仅搜索其各自的州的美国驾照。

各个州分类器根据相应州的模式进行匹配，并需要相应的州名或缩写以及额外的支持数据。

示例：

- CA DL: C3452362（因为具有正确的号码模式以及支持数据，所以匹配）
- California DL: C3452362（匹配）
- DL: C3452362（因为没有足够的支持数据，所以不匹配）
- California C3452362（因为没有足够的支持数据，所以不匹配）
- OR DL: C3452362（匹配）
- OR DL: 3452362（因为是俄勒冈州的正确模式，所以匹配）
- WV DL: D654321（因为是西弗吉尼亚州的正确模式，所以匹配）
- WV DL: G6543（匹配）

国家运营商 ID（美国）

“美国国内供应商标识”分类器用于扫描“美国国内供应商标识”(NPI) 号码，后者是带有校验位的 10 位数号码。

示例：

- NPI No. 1245319599（与 NPI 匹配）
- NPI No. 1235678996（与 NPI 匹配）
- 3459872347（因为没有支持信息，所以不匹配）
- NPI: 3459872342（因为校验位不正确，所以不匹配）

学术记录（英文）

预定义的FERPA（《家庭教育权和隐私权法案》）DLP 策略模板使用“学生记录”分类器。将其与自定义“学生标识号”分类器组合可检测特定的学生 ID 模式，以提高准确度。

示例：

- Fall Semester Course Numbers: CHEM101, ECON102, MATH103（匹配）

财务声明（英文）

预定义的“沙宾法案”(SOX) 策略模板使用“公司财务”分类器来搜索非公共公司财务信息。

示例：

```
Gross Profits, Current Assets, and Cash Flow Statement for the Quarter ended June 30, 2016.
```
（匹配）

为自定义 DLP 策略创建内容匹配分类器

您创建的自定义分类器将添加到创建自定义 DLP 策略时可使用的分类器列表中。

过程

	命令或操作	目的
步骤 1	了解内容匹配分类器如何用于识别潜在的 DLP 违规。	请参阅： • 关于使用内容匹配分类器来定义不允许的内容，第 380 页 • 内容匹配分类器示例，第 380 页
步骤 2	选择**邮件策略 (Mail Policies) > DLP 策略自定义 (DLP Policy Customizations)**，然后点击**添加自定义分类器 (Add Custom Classifier)**。输入分类器名称及说明。	-
步骤 3	输入接近度和最小总分。	请参阅 可疑违规的风险系数的决定因素，第 386 页
步骤 4	选择以下检测规则类型之一，并定义相关联的内容匹配条件： • 词汇或短语 • 词典中的文本 • 正则表达式，或 • 现有的防数据丢失实体	请参阅： • 用于识别敏感内容的分类器检测规则（仅适用于自定义 DLP 策略），第 383 页 • 使用敏感 DLP 术语的自定义词典（仅适用于自定义 DLP 策略），第 385 页 • 用于识别标识号的正则表达式，第 383 页
步骤 5	（可选）通过点击**添加规则 (Add Rule)**，添加其他规则。	有关权重和最高得分的信息，请参阅可疑违规的风险系数的决定因素，第 386 页。
步骤 6	如果包括多条规则，请指定是必须匹配**全部 (All)** 规则，还是匹配**任何 (Any)** 规则即可。	此设置位于“规则”(Rules) 部分顶部。
步骤 7	提交并确认更改。	—

下一步做什么

在自定义 DLP 策略中使用自定义内容分类器。请参阅创建自定义 DLP 策略（高级），第 379 页。

用于识别敏感内容的分类器检测规则（仅适用于自定义 DLP 策略）

内容匹配分类器需要用于在邮件或文档中检测 DLP 违规的规则。分类器可以使用以下一条或多条检测规则：

- **字词或短语**。分类器应检测的一系列字词或短语。请使用逗号或换行符来分隔多个条目。
- **正则表达式**。用于为邮件或附件定义搜索模式的正则表达式。您也可定义要从匹配中排除的模式，以避免误报。有关详细信息，请参阅用于识别标识号的正则表达式，第 383 页和用于识别标识号的正则表达式，第 383 页。
- **词典**。相关字词和短语的词典。设备包含预定义的词典，您也可创建自己的词典。请参阅使用敏感 DLP 术语的自定义词典（仅适用于自定义 DLP 策略），第 385 页。
- **实体**。这是用于识别常见敏感数据类型（例如信用卡号、地址、社会保险号或美国银联转帐号）的预定义模式。有关实体的说明，请依次转至**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**，然后依次点击**添加 DLP 策略 (Add DLP Policy)**、**隐私保护 (Privacy Protection)**、**显示策略说明 (Display Policy Descriptions)**。

用于识别标识号的正则表达式

一些策略模板要求对一个或多个内容匹配分类器进行自定义，这涉及创建正则表达式以搜索可能链接到机密信息（例如自定义帐号、患者标识号或学生 ID）的标识号。您可以使用 **Perl 兼容正则表达式 (PCRE2)** 语法为内容匹配分类器或 DLP 策略模板添加正则表达式。只有在设备上启用了 DLP 功能时才会验证正则表达式的 PCRE2 兼容性。

注释 正则表达式区分大小写，因此它们应包含大写和小写字符，例如 `[a-zA-Z]`。如果仅使用特定的字母，您可相应地定义正则表达式。

模式越不具体（例如 8 位数的号码），您就越有可能希望策略搜索额外的字词和短语，以区分随机的 8 位数号码与实际客户号码。

在为分类器创建正则表达式时，请使用下表作为指南：

元件	说明
正则表达式 (abc)	对于分类器的正则表达式，如果其中的指令序列与一个字符串的任何部分匹配，则该正则表达式与该字符串匹配。 例如，正则表达式 **ACC** 与字符串 **ACCOUNT** 以及 **ACCT** 匹配。
[ ]	使用方括号可指示一组字符。可以逐个定义字符，也可使用范围来定义字符。 例如，**[a-z]** 与 a 到 z 的所有小写字母匹配，而 **[a-zA-Z]** 与 A 到 Z 的所有大写及小写字母匹配。**[xyz]** 仅与字母 x、y 或 z 匹配。

元件	说明
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。 反斜线字符也作为标记的开头，例如 \d。 **重要说明**：反斜线也是解析器的特殊转义字符。因此，如果您想在正则表达式中包括一个反斜线，则必须使用两个反斜线。这样，在解析后，将仅保留一个“真正的”反斜线，这个反斜线将传递到正则表达式系统。
\d	与一个数字 (0-9) 匹配的标记。要与多个数字匹配，请输入一个括在 {} 中的整数以定义数值长度。 例如，\d 仅与 5 之类的单个数字匹配，而与 55 不匹配。使用 \d\{2\} 表示与 55 等包含两个数字的数值匹配，而与 5 不匹配。
\D	与任何非数字字符匹配的标记。要与多个非数字字符匹配，请输入一个括在 {} 中的整数以定义长度。
\w	与任何字母数字字符和下划线（a-z、A-Z、0-9 以及 _）匹配的标记。
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“\d\{8\}”与 12345678 和 11223344 匹配，但与 8 不匹配。
或 (|)	替换或“或”运算符。如果 A 和 B 是正则表达式，则表达式“A|B”将与任何与“A”或“B”匹配的字符串匹配。这可用来在正则表达式中组合数字模式。 例如，表达式“foo|bar”将与 foo 或 bar 匹配，但与 foobar 不匹配。

用于识别标识号的正则表达式的示例

用于说明标识号或帐号中的数字及字母模式的简单正则表达式可能如下所示：

- 8 位数的数值：`\d{8}`
- 在各组数值之间以连字符分隔的标识代码：`\d{3}-\d{4}-\d`
- 以单个大写或小写字母开头的标识代码：`[a-zA-Z]\d\{7\}`
- 以 3 个数字开头并且后跟 9 个大写字母的标识代码：`\d{3}[A-Z]{9}`
- 使用 | 可定义两个要搜索的不同数字模式：`\d{3}[A-Z]{9}|\d{2}[A-Z]{9}-\d`

使用敏感 DLP 术语的自定义词典（仅适用于自定义 DLP 策略）

AsyncOS 附带一组预定义词典，但您也可创建自定义 DLP 词典，以指定要让 DLP 扫描功能匹配的术语。

可以通过多种方式创建自定义 DLP 词典：

- 直接添加自定义 DLP 词典，第 385 页
- 以文本文件的形式创建 DLP 词典，第 385 页然后导入 DLP 词典，第 386 页。
- 导出 DLP 词典，第 385 页 从另一个邮件安全设备，然后导入 DLP 词典，第 386 页。

直接添加自定义 DLP 词典

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。

步骤 2 在**高级设置 (Advanced Settings)** 部分，点击**自定义词典 (Custom DLP Dictionaries)** 旁的链接。

步骤 3 点击**添加词典 (Add Dictionary)**。

步骤 4 为自定义词典输入一个名称。

步骤 5 将新词典条目（字词和短语）输入到词条列表中。

词典词条区分大小写，并可包含非 ASCII 字符。

输入多个条目时，请使用换行符来分隔各个条目。

步骤 6 点击 **Add**。

步骤 7 提交并确认更改。

以文本文件的形式创建 DLP 词典

您可以采用文本文件形式在本地计算机上创建自己的词典，然后将其导入到设备上。对于词典文本文件中的每个词条，请使用换行符。词典词条区分大小写，并可包含非 ASCII 字符。

导出 DLP 词典

注释 预定义的 DLP 词典不可导出。

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。

步骤 2 点击“高级设置”(Advanced Settings) 下的**自定义 DLP 词典 (Custom DLP Dictionaries)** 部分的链接。

步骤 3 点击**导出词典 (Export Dictionary)**。

步骤 4 选择要导出的词典。

步骤 5 为该词典输入一个文件名。

步骤 6 选择将导出的词典保存到什么位置，可以保存在本地计算机上，也可以保存在设备上的配置目录中。

步骤 7 为该文件选择一种编码方式。

步骤 8 点击**提交 (Submit)** 并保存该文件。

导入 DLP 词典

准备工作

如果您要导入一个文件，而该文件使您从邮件安全设备上的非 DLP 词典中导出的，必须首先从文本文件中拆分出权重值，并将所有正则表达式转换为词汇或短语。

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。

步骤 2 在**高级设置 (Advanced Settings)** 部分，点击**自定义词典 (Custom DLP Dictionaries)** 旁的链接。

步骤 3 点击**导入词典 (Import Dictionary)**。

步骤 4 选择一个要从本地计算机或该设备上的配置目录中导入的文件。

步骤 5 选择一种编码方式。

步骤 6 点击 **Next**。

系统将显示“导入成功”(Success) 的消息，并且导入的词典将显示在“添加词典”(Add Dictionary) 页面中。但是，操作过程尚未完成。

步骤 7 命名并编辑词典。

步骤 8 点击 **Submit**。

可疑违规的风险系数的决定因素

当设备扫描邮件以确定是否包含 DLP 违规时，会对邮件指定风险系数得分。此得分指示该邮件发生 DLP 违规的可能性。得分为 0 表示邮件几乎肯定不包含违规。得分为 100 表示邮件几乎肯定包含违规。

对于基于预定义模板的 DLP 策略

不能查看或修改通过预定义模板创建的 DLP 策略的风险因素得分参数。但是，如果对于某一特定 DLP 策略存在过多误报匹配，则可调整该策略的严重性标度。请参阅关于评估违规严重性，第 388 页。对于基于没有内容匹配分类器的模板的策略（如 SOX（萨班斯 - 奥克斯利法案 (Sarbanes-Oxley)）模板），当某一邮件违反该策略时，扫描引擎将始终返回一个值为“75”的风险因素。

对于自定义 DLP 策略

在为自定义 DLP 策略创建内容匹配分类器时，您需指定用来确定风险系数得分的值：

- **接近度**。规则匹配项在邮件或附件中必须达到何种接近度才算作违规。例如，如果在一封较长邮件的开头附近出现类似于社会保险号的数字模式，并且末尾的发件人签名中出现地址，则假设它们不相关，且此数据不算匹配项。
- **最小总分**。将敏感内容标记为 DLP 违规所需达到的最小风险系数得分。如果邮件的匹配项得分未达到最小总分，则将其数据视为不敏感。

- **权重**。对于您创建的每个自定义规则，您可指定“权重”以指示该规则的重要性。得分是通过将检测规则匹配项数与规则权重相乘计算而得。如果某一规则有两个实例，其权重为 10，则得分结果为 20。如果某条规则对于分类器而言比其他规则更重要，则应为其指定较大的权重。
- **最大得分**。某一规则的最高得分将阻止某一低权重规则的大量匹配歪曲扫描的最终得分。

为了计算风险因素，分类器会将某一检测规则的匹配数量与该规则的权重相乘。如果此值超过该检测规则的最高得分，则分类器将使用该最高得分值。如果分类器有多条检测规则，则它会将其所有检测规则的得分累加为一个值。分类器会使用下表所示的对数刻度将检测规则得分 (10 - 10000) 映射到刻度 10 - 100，以创建风险系数：

表 *38:* 根据检测规则得分计算风险系数得分的方式

规则得分	风险系数
10	18
20	28
30	33
50	41
100	50
150	56
300	65
500	72
1000	82
10000	100

查看使用了自定义内容分类器的策略

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略自定义 (DLP Policy Customizations)**。

步骤 2 在**自定义分类器 (Custom Classifiers)** 部分中，点击“自定义分类器”(Custom Classifiers) 表的标题中的**策略 (Policies)** 链接。

根据 DLP 策略过滤邮件

为了改善性能或准确度，您可根据以下条件对 DLP 策略进行限制，使其仅应用于特定的邮件：

选项	说明
按发件人和收件人过滤	您可对 DLP 策略进行限制，使其应用于包含或不包含您使用下列其中一项指定的收件人或发件人的邮件： • 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` 请使用换行符或逗号来分隔多个条目。 AsyncOS 首先会将外发邮件的收件人或发件人与外发邮件策略匹配，然后将发件人或收件人与您为该邮件策略启用的 DLP 策略中指定的发件人和收件人过滤器匹配。 例如，您可能希望不允许所有发件人向合作伙伴域中的收件人以外的收件人发送特定类型的信息。您应为该信息创建一个 DLP 策略，包括一个用于免除合作伙伴域中所有用户的过滤器，然后将这个 DLP 策略包括在应用于所有发件人的外发邮件策略中。
按附件类型过滤	您可对 DLP 策略进行限制，以便仅扫描包含或不包含特定附件类型的邮件。请选择附件类别，然后选择预定义的文件类型，或指定未列出的文件类型。如果指定非预定义文件类型，则 AsyncOS 会根据附件的扩展名来搜索该文件类型。 您还可以将 DLP 扫描限制为具有最小文件大小的附件。
按邮件标记过滤 (Filtering by Message Tag)	如果希望将 DLP 策略限制为包含特定短语的邮件，可以使用邮件或内容过滤器搜索传出邮件中是否包含该短语，然后向该邮件中插入自定义邮件标记。有关详细信息，请参阅内容过滤器操作，第 242 页和 使用邮件过滤器实施邮件策略，第 117 页

关于评估违规严重性

当 DLP 扫描引擎检测到潜在 DLP 违规时，它将计算一个风险因素得分，表示该实例实际上是 DLP 违规的可能性。策略将对该风险因素得分与该策略中定义的严重性标度进行比较，以确定严重性级别（例如，“低”[Low] 或“关键”[Critical]）。可为各个严重性级别的违规指定要采取的操作（除“忽略”[Ignore] 以外，不会为该选项采取任何操作）。可以调整达到各个严重性级别所需的风险因素得分。

调整严重性刻度

所有策略都具有默认的严重性刻度。您可以为每个策略调整此刻度。

例如，在默认情况下，如果一项违规的风险系数得分介于 90 与 100 之间，则其严重性级别为“严重”。但是，对于与特定策略匹配的违规，您可能想提高潜在数据丢失的敏感度。对于此 DLP 策略，可将严重性级别“严重”更改为风险系数得分介于 75 与 100 之间的所有违规。

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。
步骤 2 点击策略名称进行编辑。
步骤 3 在**严重性设置** 部分，点击**编辑刻度**。
步骤 4 使用刻度的箭头来调整严重性级别的得分。
步骤 5 点击 **Done**。
步骤 6 在“严重性刻度”(Severity Scale) 表中，确认得分与您的期望相符。
步骤 7 点击 **Submit**。

排列邮件 DLP 策略用于违规匹配的顺序

如果某个 DLP 违规与外发邮件策略中启用的多个 DLP 策略匹配，则将仅使用列表中的第一个匹配 DLP 策略。

步骤 1 在“DLP 策略管理器”(DLP Policy Manager) 页面上，点击**编辑策略顺序 (Edit Policy Order)**。
步骤 2 点击您想要移动的策略所对应的行，并将其拖动到顺序中的新位置。
步骤 3 当您完成重新排列策略顺序后，请提交并确认更改。

将 DLP 策略与传出邮件策略关联

将 DLP 策略与默认的外发邮件策略关联

当没有任何外发邮件策略与发件人或收件人匹配时，将使用默认的外发邮件策略。

准备工作

完成防数据丢失的设置方式，第 375 页的表格中到此处为止的所有活动。例如，请确保已创建要包括在默认的外发邮件策略中的 DLP 策略。

步骤 1 依次选择**邮件策略 (Mail Policies) > 外发邮件策略 (Outgoing Mail Policies)**。
步骤 2 在表的**默认策略 (Default Policy)** 行中，点击 **DLP** 列中的**禁用 (Disabled)** 链接。
步骤 3 选中**启用 DLP（自定义设置）(Enable DLP [Customize Settings])**。
步骤 4 选择要为默认外发邮件策略启用的 DLP 策略。
步骤 5 提交并确认更改。

下一步做什么

为其他外发邮件策略选择 DLP 策略。请参阅使用外发邮件策略向发件人和收件人指定 DLP 策略，第 390 页。

使用外发邮件策略向发件人和收件人指定 DLP 策略

通过在外发邮件策略中启用 DLP 策略，指定将哪些 DLP 策略应用于哪些发件人和收件人。只能在外发邮件策略中使用 DLP 策略。

准备工作

为默认的外发邮件策略配置 DLP 策略设置。请参阅将 DLP 策略与默认的外发邮件策略关联，第 389 页。

步骤 1 依次选择**邮件策略 (Mail Policies) > 外发邮件策略 (Outgoing Mail Policies)**。

步骤 2 点击表中任何一行的 DLP 列中的链接。

步骤 3 选择要与此外发邮件策略相关联的 DLP 策略。

步骤 4 提交更改。

步骤 5 根据需要，为其他外发邮件策略重复上述步骤。

步骤 6 确认您的更改。

关于编辑或删除 DLP 策略的重要信息

操作	信息
编辑 DLP 策略	如果重命名一个策略，则必须在外发邮件策略中重新启用该策略。
删除 DLP 策略	如果删除一个策略，并且该 DLP 策略已用于一个或多个外发邮件策略，则您会收到通知。删除 DLP 策略会将其从这些邮件策略中移除。

邮件操作

您应指定当邮件安全设备检测到传出邮件中存在可能的 DLP 违规时，它应采取的主要和次要操作。可以针对不同的违规类型和严重程度分配不同的操作。

主要操作包括：

- 投递
- 丢弃
- 隔离

辅助操作包括：

- 如果您选择传送邮件，则向策略隔离区发送一个副本。该副本与原始邮件完全一样，其中包含邮件 ID。隔离副本不仅提供了另一种监控 DLP 违规的方法，还允许在部署前测试 DLP 系统。从隔离区释放该副本时，设备会将该副本传送给收件人，而该收件人已接收了原始邮件。
- 对邮件进行加密。设备仅对邮件正文进行加密。不会对邮件信头进行加密。
- 改动包含 DLP 违规的邮件的主题信头。
- 向邮件添加免责声明文本。
- 将邮件发送到备用目标邮件主机。
- 将邮件副本发送（密件抄送）给其他收件人。（例如，您可以将包含严重 DLP 违规的邮件复制到合规官的邮箱以供检查。）
- 将 DLP 违规通知邮件发送给发件人或其他联系人（例如经理或 DLP 合规官）。请参阅创建 DLP 通知，第 393 页。

注释 这些操作并不互相排斥：您可以在不同的 DLP 策略中组合这些操作，以满足不同用户组的各种处理需求。您也可以在同一个策略中基于不同严重性级别配置不同的处理操作。例如，您可能希望隔离包含严重 DLP 违规的邮件并向合规官发送通知，但您希望传送严重性级别较低的邮件。

定义要针对 DLP 违规采取的操作（邮件操作）

准备工作

- 至少创建一个专用的隔离区，用于存放违反 DLP 策略的邮件（或邮件副本）。

  这可以是邮件安全设备上的本地隔离区，也可以是安全管理设备上的集中隔离区。

  有关信息，请参阅集中化的策略、病毒和病毒爆发隔离区，第 685 页

- 如果您希望在传送邮件前对其进行加密，请确保已设置加密配置文件。请参阅思科邮件加密，第 399 页
- 要在传送包含 DLP 违规或疑似违规的邮件时包括免责声明文本，请在**邮件策略 (Mail Policies) > 文本资源 (Text Resources)** 中指定免责声明文本。有关信息，请参阅免责声明模板，第 491 页
- 要向 DLP 违规的发件人或其他人员（例如合规官）发送通知，请先创建 DLP 通知模板。请参阅创建 DLP 通知，第 393 页。

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略自定义 (DLP Policy Customizations)**。

步骤 2 在**邮件操作 (Message Actions)** 部分，点击**添加邮件操作 (Add Message Action)**。

步骤 3 为该邮件操作输入一个名称。

步骤 4 输入对该邮件操作的说明。

步骤 5 选择是丢弃、传送还是隔离包含 DLP 违规的邮件。

注释 如果您选择“传送”(Deliver)，则可选择将该邮件的副本发送到策略隔离区。该邮件副本与原始邮件完全一样，其中包含邮件 ID。

步骤 6 如果要在传送后或者从隔离区释放时对邮件进行加密，请选中**启用加密 (Enable Encryption)** 复选框，并选择下列选项：

- **加密规则 (Encryption Rule)**。始终对邮件进行加密，或者仅在首先尝试通过 TLS 连接发送邮件失败时对其进行加密。
- **加密配置文件 (Encryption Profile)**。使用指定的加密配置文件对邮件进行加密，并传送该邮件（如果您使用的是思科 IronPort 加密装置或托管密钥服务）。
- **加密邮件主题 (Encrypted Message Subject)**。加密邮件的主题。使用值 `$Subject` 可保留现有的邮件主题。

步骤 7 如果您选择“隔离”(Quarantine) 操作，请选择要用于包含 DLP 违规的邮件的策略隔离区。

步骤 8 如果您想要使用下列任何选项来修改邮件，请点击**高级 (Advanced)**：

- 添加自定义信头
- 修改邮件主题
- 将其传送到备用主机
- 将副本发送（密件抄送）给其他收件人
- 发送 DLP 通知邮件

步骤 9 提交并确认更改。

查看和编辑邮件操作

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略自定义 (DLP Policy Customizations)**。

步骤 2 在**邮件操作 (Message Actions)** 部分，选择操作：

目标	请
查看每一项操作所分配到的邮件策略	点击“邮件操作”(Message Actions) 表的标题中的**策略 (Policies)** 链接。
查看您为每一项操作输入的说明	点击“邮件操作”(Message Actions) 表的标题中的**说明 (Description)** 链接。
查看或编辑邮件操作的详细信息	点击邮件操作的名称。
删除邮件操作	点击您要删除的邮件操作旁边的垃圾桶图标。 如果该邮件操作已用于一个或多个 DLP 策略，您会收到一条确认消息通知。

目标	请
复制邮件操作 您可使用此功能在更改邮件操作前创建备份副本，或用作相似的新邮件操作的起点。	点击您要复制的邮件操作旁边的**复制 (Duplicate)** 图标。

步骤 3 提交并确认所有更改。

创建 DLP 通知

使用此过程可创建通知模板，用于在邮件中包含违反组织防数据丢失策略的信息时发送相应通知。您可将此通知发送给违反 DLP 策略的邮件的发件人，或发送到其他地址（例如经理或 DLP 合规官的邮箱）。

准备工作

- 熟悉DLP 通知模板变量定义，第 393 页。您可借助这些变量，以每项违规的特定详细信息来自定义通知。

步骤 1 依次选择**邮件策略 (Mail Policies) > 文本资源 (Text Resources)**。

步骤 2 点击**添加文本资源 (Add Text Resource)**。

步骤 3 对于**类型 (Type)**，请选择 **DLP 通知模板 (DLP Notification Template)**。

DLP 变量不可用于纯文本通知模板。

步骤 4 请输入通知文本和变量。

此通知应该向其收件人指出，外发邮件可能包含违反组织防数据丢失策略的敏感数据。

下一步做什么

在 DLP 策略管理器上，在 DLP 策略的邮件操作中，指定此 DLP 通知模板。

DLP 通知模板变量定义

使用下列变量可在通知中包括有关每项 DLP 违规的特定信息。

变量	替换内容
$DLPPolicy	替换为违反的邮件 DLP 策略的名称。
$DLPSeverity	替换为违规严重性。可以是“低”(Low)、“中”(Medium)、“高”(High) 或“严重”(Critical)。
$DLPRiskFactor	替换为邮件敏感资料的风险系数（得分 0 - 100）。

变量	替换内容
$To	替换为邮件“收件人:”(To:) 信头（不是“信封收件人”[Envelope Recipient]）。
$From	替换为邮件“发件人:”(From:) 信头（不是“信封收件人”[Envelope Recipient]）。
$Subject	替换为原始邮件的主题。
$Date	替换为当前日期，采用 MM/DD/YYYY 格式。
$Time	替换为本地时区中的当前时间。
$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。
$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。
$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<”。
$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“None”。
$filenames	替换为邮件附件文件名的逗号分隔列表。
$filetypes	替换为邮件附件文件类型的逗号分隔列表。
$filesizes	替换为邮件附件文件大小的逗号分隔列表。
$remotehost	替换为将邮件发送到思科设备的系统的主机名。
$AllHeaders	替换为邮件信头。
$EnvelopeFrom	替换为邮件的信封发件人（信封来源，<MAIL FROM>）。
$Hostname	替换为思科设备的主机名。
$bodysize	替换为邮件的大小（以字节为单位）。
$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。
$remoteip	替换为将邮件发送给思科设备的系统的 IP 地址。
$recvlistener	替换为接收邮件的侦听程序的昵称。
$dropped_filenames	与 $filenames 相同，但显示已丢弃的文件的列表。
$dropped_filename	仅返回最近丢弃的文件名。
$recvint	替换为接收邮件的接口的昵称。

变量	替换内容
$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。
$Time	替换为本地时区中的当前时间。
$orgid	替换为 SenderBase 组织 ID（整数值）。
$enveloperecipients	替换为邮件的所有信封收件人（信封目标，<RCPT TO>）。
$dropped_filetypes	与 $filetypes 相同，但显示已丢弃的文件类型的列表。
$dropped_filetype	仅返回最近丢弃的文件的文件类型。

在邮件跟踪中显示敏感 DLP 数据

DLP 部署可以记录违反 DLP 策略的内容及其周围的内容，您可以随后在“邮件跟踪”中查看这些内容。此内容可能包含敏感数据（例如信用卡号和社会保险号）。

准备工作

启用“邮件跟踪”(Message Tracking)。请参阅 启用邮件跟踪，第 677 页

步骤 1 选择**安全服务 > 数据丢失预防**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选中**启用匹配内容日志记录 (Enable Matched Content Logging)** 复选框。

步骤 4 提交并确认更改。

下一步做什么

指定哪些管理用户可以查看此信息。请参阅控制对“邮件跟踪”中敏感信息的访问权限，第 727 页。

关于更新 DLP 引擎和内容匹配分类器

设备上思科 DLP 引擎和预定义内容匹配分类器的更新与其他安全服务的更新无关。

确定 DLP 引擎的当前版本

步骤 1 依次选择**安全服务 > 防数据丢失**。

步骤 2 查看**当前 DLP 版本文件 (Current DLP Version Files)** 部分。

注释　还可以使用 `dlpstatus` CLI 命令查看 DLP 引擎的当前版本。有关详细信息，请参阅用于思科邮件安全设备的 *AsyncOS CLI* 参考指南。

手动更新 DLP 引擎和内容匹配分类器

准备工作

请参阅以下内容：

- （如适用）集中（集群式）设备上的 DLP 更新，第 397 页

步骤 1 选择 **安全服务 > 数据丢失预防**。

步骤 2 在**当前 DLP 版本文件 (Current DLP Version Files)** 部分中，点击**立即更新 (Update Now)**。

仅当有可供下载的新更新时，此按钮才可用。

注释　还可以使用 `dlpupdate` CLI 命令更新 DLP 引擎。有关详细信息，请参阅思科邮件安全设备 *AsyncOS CLI* 参考指南。

启用自动更新（不建议）

使用此过程可使设备能够定期查找并下载更新。

注释　思科建议您不要启用自动更新。这些更新可能会更改 DLP 策略中使用的内容匹配分类器。而是先手动下载 DLP 更新并在实验室环境中测试这些更新，然后再更新生产环境中使用的设备。

准备工作

- 在**安全设置 (Security Settings) > 服务更新 (Service Updates)** 页面上，确保已针对所有服务更新启用自动更新并指定更新间隔。
- 请参阅集中（集群式）设备上的 DLP 更新，第 397 页。

步骤 1 选择**安全服务 > 防数据丢失**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选中**启用自动更新 (Enable automatic updates)** 复选框。

步骤 4 提交并确认更改。

集中（集群式）设备上的 DLP 更新

请注意以下提示：

- 无法为集群式部署中的设备启用自动 DLP 更新。
- DLP 更新始终在计算机级别执行，与在集群、计算机或组级别配置的 DLP 无关。
- 检查设备的 DLP 引擎状态只能在计算机级别使用 **dlpstatus** CLI 命令来执行。

处理 DLP 事件邮件及数据

注释 根据适用于您的部署的情况，另请参阅安全管理设备的文档。

目标	请
使用条件（例如DLP策略名称、违规严重性以及采取的操作）来搜索包含DLP违规的邮件，并查看所找到的邮件的详细信息	请参阅邮件跟踪，第 677 页。
查看或管理已隔离为疑似 DLP 违规的邮件	请参阅处理策略、病毒或爆发隔离区中的邮件，第 693 页。
查看 DLP 事件摘要	请参阅使用邮件安全监控，第637页中有关DLP事件摘要报告的信息。
查看关于在外发邮件中发现的 DLP 违规的信息	请参阅使用邮件安全监控，第637页中有关DLP事件报告的信息。

防数据丢失故障排除

DLP 无法在邮件附件中检测违规

问题

使用预定义的 DLP 策略时，DLP 无法在邮件附件中检测违规。这可能是由以下原因引起的：

- 预定义 DLP 策略中接近度参数的值较小

注释 您无法更改预定义 DLP 策略的接近度。

- 预定义 DLP 策略中定义的高严重性标度参数

解决方案

- 创建自定义策略，并根据需要调整接近度。请参阅 创建自定义 DLP 策略（高级），第 379 页
- 降低预定义 DLP 策略的严重性标度参数。请参阅 调整严重性刻度，第 388 页

第 19 章

思科邮件加密

本章包含以下部分：

思科邮件加密概述

AsyncOS 支持使用加密技术保护入站和出站邮件的安全。要使用此功能，可以创建加密配置文件为密钥服务器指定加密邮件和连接信息的特征。密钥服务器可以是：

- 思科注册信封服务（托管服务），或
- 思科加密设备（本地托管的服务器）

接下来，创建内容过滤器、邮件过滤器和防数据丢失策略确定要加密的邮件。

1. 符合过滤器条件的外发邮件放置在用于加密处理的邮件安全设备上的队列中。
2. 对邮件进行加密后，用于加密的密钥会存储在在加密配置文件中指定的密钥服务器中，并且加密的邮件会排队等待传输。
3. 如果存在禁止加密队列中邮件的临时情况（例如，临时 C 系列正忙或 CRES 不可用），则会对邮件重新排队并稍后重试。

注释 还可以设置设备以首先尝试在加密之前通过 TLS 连接发送邮件。有关详细信息，请参阅使用 TLS 连接作为加密备用项， 第 406 页。

如何通过本地密钥服务器加密邮件

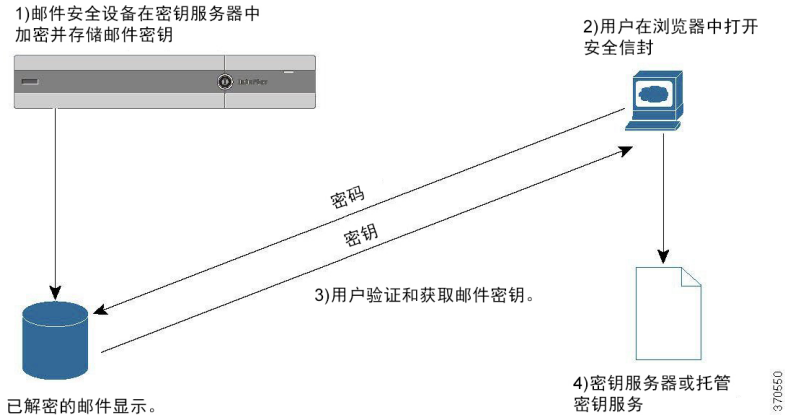
表 *39:* 如何通过本地密钥服务器加密邮件

步骤	请	更多信息
第 1 步	设置网络中的 Cisco IronPort 加密设备。	请参阅 设置和安装，第 17 页
第 2 步	启用邮件加密。	在邮件安全设备上启用邮件加密，第 401 页创建 Services Bridge 报价。
第 3 步	通过创建加密配置文件，指定要使用的加密密钥服务器以及用于加密邮件的安全设置。	配置密钥服务如何处理加密邮件，第 402 页。
第 4 步	定义要使设备对邮件进行加密，邮件必须满足的条件。	确定要加密的邮件，第 405 页。
第 5 步	确定什么时候对邮件工作流程中的邮件进行加密。	• 使用内容过滤器加密并立即传送邮件，第 406 页。 或 • 在传送时使用内容过滤器加密邮件，第 407 页。
第 6 步	（可选）标记进行额外安全保护的邮件。	将加密信头添加到邮件，第 408 页。
第 7 步	定义要为其加密邮件的用户组。	创建邮件策略。 请参阅 邮件策略，第 223 页
第 8 步	将您定义的加密操作与定义的用户组相关联。	将内容过滤器与邮件策略相关联。 请参阅 邮件策略，第 223 页

加密工作流程

当使用邮件加密时，思科邮件安全设备会加密邮件，并将邮件密钥存储在本地密钥服务器或托管密钥服务中。当收件人打开加密邮件时，密钥服务会对收件人进行身份验证，并且解密的邮件将会显示。

图 *34:* 加密工作流程



打开加密邮件的基本工作流程如下：

1. 当配置加密配置文件时，可以为邮件加密指定参数。对于加密的邮件，邮件安全设备会在本地密钥服务器或托管密钥服务（思科注册信封服务）上创建并存储邮件密钥。
2. 收件人可在浏览器中打开安全信封。
3. 当收件人在浏览器中打开加密的邮件时，可能需要输入密码以验证收件人的身份。密钥服务器会返回与邮件关联的加密密钥。

注释 当第一次打开加密的邮件时，收件人需要注册到密钥服务以打开安全信封。在注册后，收件人可以在不进行验证的情况下打开加密的邮件，具体取决于在加密配置文件配置的设置。加密配置文件可以指定不需要密码，但是某些功能将不可用。

4. 此时将显示解密的邮件。

使用邮件安全设备加密邮件

要使用邮件安全设备进行加密，必须配置加密配置文件。可以使用 encryptionconfig CLI 命令或通过 GUI 中的“安全服务”>“Cisco IronPort 邮件加密”启用并配置加密配置文件。

注释 如果在设备上启用了 PXE 和 S/MIME 加密，AsyncOS 会首先使用 S/MIME 然后再使用 PXE 来加密邮件。

在邮件安全设备上启用邮件加密

步骤 1 依次点击**安全服务 (Security Services) > Cisco IronPort 邮件加密 (Cisco IronPort Email Encryption)**。

步骤 2 点击**启用 (Enable)**。

步骤 3 （可选）点击**编辑设置 (Edit Settings)** 配置以下选项：

- 要加密的最大邮件大小。思科建议的邮件大小为 10 MB。设备将加密的最大邮件大小为 25 MB。

  注释 对大于建议的 10 MB 限制的邮件进行加密可能会减慢设备的性能。如果您使用的是思科注册的信封服务，则邮件收件人将无法回复具有大于 10 MB 的附件的加密邮件。

- 加密帐户管理员的邮件地址。调配加密配置文件时，此邮件地址会自动注册到加密服务器。
- 配置代理服务器。

配置密钥服务如何处理加密邮件

如果使用密钥服务，则可以创建一个或多个加密配置文件。如果要为不同的邮件组使用不同的安全级别，则可能需要创建不同的加密配置文件。例如，您可能希望以高安全性发送包含敏感资料的邮件，但是以中等安全性发送其他邮件。在这种情况下，可创建高安全性加密配置文件以与包含某些关键字（例如“机密”）的邮件关联，并为其他外发邮件创建另一加密配置文件。

可以将加密配置文件分配给自定义用户角色，以允许分配给该角色的委派管理员将加密配置文件与其 DLP 策略和内容过滤器配合使用。当配置 DLP 策略和内容过滤器时，只有管理员、操作员和委派的用户可以使用加密配置文件。未分配给自定义角色的加密配置文件可供具有邮件或 DLP 策略权限的所有委派管理员使用。有关详细信息，请参阅分配管理任务，第 723 页。

注释 可以为托管密钥服务配置多个加密配置文件。如果贵组织有多个品牌，这样使您可以参考存储在PXE信封的密钥服务器中的不同徽标。

加密配置文件会存储以下设置：

- **密钥服务器设置**。指定密钥服务器和信息以用于连接到该密钥服务器。
- **信封设置**。指定有关邮件信封的详细信息，例如安全级别、是否返回已读回执、邮件在超时之前排队进行加密的时间长度、要使用的加密算法类型以及是否启用在浏览器中运行的解密小程序。
- **邮件设置**。指定有关邮件的详细信息，例如是否启用安全邮件转发和安全的全部回复。
- **通知设置**。指定要用于文本和 HTML 通知的通知模板，以及加密失败通知。在创建加密配置文件时，在文本资源中创建模板并选择模板。还可以本地化信封并为加密失败通知指定邮件主题。有关通知的详细信息，请参阅加密通知模板，第 500 页和退回和加密失败通知模板，第 499 页。

步骤 1 在“邮件加密配置文件”(Email Encryption Profiles) 部分中，点击**添加加密配置文件 (Add Encryption Profile)**。

步骤 2 输入加密配置文件的名称。

步骤 3 点击**使用者 (角色) (Used By (Roles))** 链接，选择要为其分配对加密配置文件访问权限的自定义用户角色，然后点击**确定 (OK)**。

分配给此自定义角色的委派管理员可以将该加密配置文件用于任何 DLP 策略以及它们负责的内容过滤器。

步骤 4 在“密钥服务器设置”(Key Server Settings) 部分中，从以下密钥服务器中进行选择：

- 思科加密设备（网内）
- 思科注册信封服务（托管密钥服务）

步骤 5 如果选择思科加密设备（本地密钥服务），请输入以下设置：

- **内部 URL**。此 URL 由思科邮件安全设备用于联系网络中的思科加密设备。
- **外部 URL**。当收件人的邮件访问思科加密设备上的密钥和其他服务时，会使用该URL。收件人使用此URL提出入站 HTTP 或 HTTPS 请求。

步骤 6 如果选择思科注册信封服务，请为托管密钥服务输入该 URL。密钥服务 URL 为 https://res.cisco.com。

步骤 7 在“密钥服务器设置”(Key Server Settings) 下点击**高级 (Advanced)**，以指定在收件人打开信封时是使用 HTTP 还是 HTTPS 来传输信封的加密负载。选择以下其中一项：

- **将密钥服务与 HTTP 配合使用**。当收件人打开信封时，使用 HTTP 从密钥服务传输加密的负载。如果您使用的是思科注册信封服务，这是在第 6 步中指定的 URL。如果您使用的是思科加密设备，这是在第 5 步中指定的外部 URL。
- 由于已加密负载，因此通过 HTTP 传输它是安全的，而且比通过 HTTPS 传输更加快速。这会提供比通过 HTTPS 发送图像请求更好的性能。
- **将密钥服务与 HTTPS 配合使用**。当收件人打开信封时，使用 HTTPS 从密钥服务传输加密的负载。如果您使用的是思科注册信封服务，这是在第 6 步中指定的 URL。如果您使用的是思科加密设备，这是在第 5 步中指定的外部 URL。
- **为负载传输指定一个单独的 URL**。如果不希望将密钥服务器用于加密的负荷，则可以使用另一个URL并指定是使用 HTTP 或还是 HTTPS 进行负载传输。

步骤 8 在“信封设置”(Envelope Settings) 部分中，选择邮件安全级别：

- **高安全性**。收件人必须始终输入密码才能打开加密邮件。
- **中等安全性**。如果已缓存收件人凭证，则收件人不需要输入凭证便可打开加密邮件。
- **不需要密码**。这是最低级别的加密邮件安全性。收件人不需要输入密码就能打开加密的邮件。您仍可为不受密码保护的信封启用阅读回执、安全的全部回复和安全邮件转发功能。

步骤 9 要允许用户通过点击其徽标来打开贵组织的 URL，可以添加指向徽标的链接。从以下选项中选择：

- **无链路**。未向邮件信封添加有效链接。
- **自定义链接 URL**。输入 URL，将有效链接添加到邮件信封。

步骤 10 （可选）启用阅读回执。如果启用该选项，则收件人打开安全信封时，发件人将收到回执。

步骤 11 （可选）在“信封设置”(Envelope Settings) 下点击**高级 (Advanced)** 以配置以下设置：

- 输入邮件超时之前，可以在加密队列中存在的时间长度（以秒为单位）。邮件超时后，设备将退回该邮件并向发件人发送通知。

- 选择一种加密算法：
  - **ARC4**。ARC4 是最常用的选项，提供强大的加密，并且最大限度减少邮件收件人的解密延迟。
  - **AES**。AES 提供更强大的加密，但是还需要更长时间进行解密，为收件人产生延迟。AES 通常用于政府和银行应用。
- 启用或禁用解密小序。启用此选项可导致在浏览器环境中打开邮件附件。禁用此选项会导致在密钥服务器中解密邮件附件。如果禁用此选项，则打开邮件可能需要更长时间，但是不依赖于浏览器环境。

步骤 12 在“邮件设置”(Message Settings) 部分中，执行以下操作：

- 要启用安全的全部回复功能，请选中**启用安全的全部回复 (Enable Secure Reply All)** 复选框。
- 要启用安全邮件转发功能，请选中**启用安全邮件转发 (Enable Secure Message Forwarding)** 复选框。

步骤 13 （可选）如果选择了思科注册信封服务并且此服务支持信封本地化，可启用信封的本地化。在“通知设置”(Notification Settings) 部分中，选中**使用本地化信封 (Use Localized Envelope)** 复选框。

注释 如果启用信封的本地化，则不能选择加密邮件 HTML 或文本通知。

如果要设置信封的默认区域设置，请参阅配置信封的默认区域设置，第 404 页。

步骤 14 选择 HTML 和文本通知模板。

注释 密钥服务器基于收件人的邮件应用使用 HTML 或文本通知。必须为两者都配置通知。

执行以下操作：

a) 选择一个 HTML 通知模板。从在文本资源中配置的 HTML 通知中进行选择。如果没有配置模板，系统将使用默认模板。
b) 选择一个文本通知模板。从在文本资源中配置的文本通知中进行选择。如果没有配置模板，系统将使用默认模板。

注释 如果使用本地化信封，这些选项将不可用。

步骤 15 输入加密失败通知的主题信头。如果加密过程超时，则设备会发送通知。

步骤 16 为邮件正文选择加密失败通知模板。从在文本资源中配置的加密失败通知模板中进行选择。如果没有配置模板，系统将使用默认模板。

步骤 17 提交并确认更改。

步骤 18 如果使用思科注册信封服务，则必须执行额外的调配设备步骤。调配设备会通过托管密钥服务注册加密配置文件。要调配设备，请点击要注册的加密配置文件的**调配 (Provision)** 按钮。

配置信封的默认区域设置

信封的默认区域设置为“英语”(English)。如果选择了思科注册信封服务且该服务支持信封的本地化，则可以将信封的区域设置更改为下列任一项：

- 英语

- 法语
- 德语
- 日语
- 葡萄牙语
- 西班牙语

准备工作

- 在思科注册信封服务作为密钥服务类型且启用了信封本地化的情况下，创建加密配置文件。请参阅配置密钥服务如何处理加密邮件，第 402 页。
- 确保思科注册信封服务支持信封的本地化。

步骤 1 依次点击**安全服务 (Security Services)** > **Cisco IronPort 邮件加密 (Cisco IronPort Email Encryption)**。

步骤 2 打开现有的加密配置文件。

步骤 3 在**通知设置 (Notification Settings)** 部分中，从**本地化信封 (Localized Envelopes)** 下拉列表中选择区域设置。

步骤 4 点击 **Submit**。

步骤 5 点击**确认更改**。

更新为 PXE 引擎的最新版本

思科邮件加密设置页面会显示PXE引擎的最新版本以及设备使用的域映射文件。您可以使用**安全服务 > 服务更新**页（或 CLI 中的 updateconfig 命令）将邮件安全设备配置为自动更新 PXE 引擎。有关详细信息，请参阅服务更新，第 761 页。

还可以使用“IronPort 邮件加密设置”(IronPort Email Encryption Settings) 页面中“PXE 引擎更新”(PXE Engine Updates) 部分的**立即更新 (Update Now)** 按钮（或 CLI 中的 **`encryptionupdate`** 命令）手动更新引擎。

确定要加密的邮件

创建加密配置文件后，需要创建确定应加密哪些邮件的传出邮件内容过滤器。内容过滤器扫描传出的邮件，并确定邮件是否与指定的条件匹配。内容过滤器确定邮件与相应条件匹配后，思科邮件安全设备会加密邮件并将生成的密钥发送到密钥服务器。它会使用在加密配置文件中指定的设置来确定要使用的密钥服务器和其他加密设置。

还可以在防数据丢失扫描后放行了邮件时，对邮件进行加密。有关详细信息，请参阅定义要针对 DLP 违规采取的操作（邮件操作），第 391 页。

使用 TLS 连接作为加密备用项

根据为域指定的目标控制，如果 TLS 连接可用，则邮件安全设备可以安全地通过 TLS 连接中继邮件而不是加密它。设备会根据目标控制中的 TLS 设置（“必需”(Required)、“首选”(Preferred) 或“无”(None)）以及在加密内容过滤器中定义的操作，确定是加密邮件还是通过 TLS 连接发送邮件。

创建内容过滤器时，可以指定是始终加密邮件还是首先尝试通过 TLS 连接发送邮件，并且如果 TLS 连接不可用，则对邮件进行加密。下表显示了当加密控制过滤器首先尝试通过 TLS 连接发送邮件时，邮件安全设备如何基于域目标控制的 TLS 设置发送邮件。

表 *40: ESA* 设备上的 *TLS* 支持

目标控制 TLS 设置	TLS 连接可用时的操作	TLS 连接不可用时的操作
无	加密信封并发送	加密信封并发送
首选 TLS	通过 TLS 发送	加密信封并发送
需要 TLS	通过 TLS 发送	重试/退回邮件

有关在目标控制中启用 TLS 的详细信息，请参阅配置网关以接收邮件，第 61 页。

使用内容过滤器加密并立即传送邮件

准备工作

- 要了解为内容过滤器构建条件的概念，请参阅内容过滤器概述，第 235 页。
- （可选）请参阅将加密信头添加到邮件，第 408 页。

步骤 1 依次转到**邮件策略 (Mail Policies) > 传出邮件内容过滤器 (Outgoing Content Filters)**。

步骤 2 在“过滤器”(Filters) 部分，点击**添加过滤器 (Add Filter)**。

步骤 3 在“条件”(Conditions) 部分，点击**添加条件 (Add Condition)**。

步骤 4 添加一个条件以过滤要加密的邮件。例如，要加密敏感材料，可以添加一个条件来识别主题或正文中包含特定字词或短语（例如“机密”）的邮件。

步骤 5 点击 **OK**。

步骤 6 或者，点击**添加操作 (Add Action)**，然后选择**添加信头 (Add Header)** 将加密信头插入邮件以指定一个额外的加密设置。

步骤 7 在“操作”(Actions) 部分，点击**添加操作 (Add Action)**。

步骤 8 从**添加操作 (Add Action)** 列表中选择**立即加密并发送（最终操作）(Encrypt and Deliver Now (Final Action))**。

步骤 9 选择是始终加密符合条件的邮件还是仅在尝试通过 TLS 连接发送邮件失败时加密邮件。

步骤 10 选择加密配置文件以与内容过滤器相关联。

加密配置文件会指定有关要使用的密钥服务器、安全性级别、邮件信封格式的设置，以及其他邮件设置。将加密配置文件与内容过滤器相关联时，内容过滤器会使用存储的设置来加密邮件。

步骤 11 输入邮件的主题。

步骤 12 点击 **OK**。

下图中的内容过滤器显示了在邮件正文中搜索 ABA 内容的内容过滤器。为内容过滤器定义的操作指定将加密并传送邮件。

图 *35:* 加密内容过滤器

步骤 13 添加加密操作后，点击**提交 (Submit)**。

步骤 14 确认您的更改。

下一步做什么

添加内容过滤器后，需要将该过滤器添加到传出邮件策略中。您可能希望在默认策略中启用该内容过滤器，也可以选择将该过滤器应用到特定邮件策略，具体取决于组织的需求。有关使用邮件策略的信息，请参阅邮件策略概述，第 223 页。

在传送时使用内容过滤器加密邮件

在传送时创建内容过滤器来加密邮件，这表示邮件继续下一阶段的处理，而且当所有处理完成后，将加密并传送邮件。

准备工作

- 要了解为内容过滤器构建条件的概念，请参阅内容过滤器概述，第 235 页。
- （可选）请参阅将加密信头添加到邮件，第 408 页。

步骤 1 依次转到**邮件策略 (Mail Policies) > 传出邮件内容过滤器 (Outgoing Content Filters)**。

步骤 2 在“过滤器”(Filters) 部分，点击**添加过滤器 (Add Filter)**。

步骤 3 在“条件”(Conditions) 部分，点击**添加条件 (Add Condition)**。

步骤 4 添加一个条件以过滤要加密的邮件。例如，要加密敏感材料，可以添加一个条件来识别主题或正文中包含特定字词或短语（例如“机密”）的邮件。

步骤 5 点击 **OK**。

步骤 6 或者，点击**添加操作 (Add Action)**，然后选择**添加信头 (Add Header)** 将加密信头插入邮件以指定一个额外的加密设置。

步骤 7 在“操作”(Actions) 部分，点击**添加操作 (Add Action)**。

步骤 8 从**添加操作 (Add Action)** 列表中选择**传送时加密 (Encrypt on Delivery)**。

步骤 9 选择是始终加密符合条件的邮件还是仅在尝试通过 TLS 连接发送邮件失败时加密邮件。

步骤 10 选择加密配置文件以与内容过滤器相关联。

加密配置文件会指定有关要使用的密钥服务器、安全性级别、邮件信封格式的设置，以及其他邮件设置。将加密配置文件与内容过滤器相关联时，内容过滤器会使用存储的设置来加密邮件。

步骤 11 输入邮件的主题。

步骤 12 点击 **OK**。

步骤 13 添加加密操作后，点击**提交 (Submit)**。

步骤 14 确认您的更改。

下一步做什么

添加内容过滤器后，需要将该过滤器添加到传出邮件策略中。您可能希望在默认策略中启用该内容过滤器，也可以选择将该过滤器应用到特定邮件策略，具体取决于组织的需求。有关使用邮件策略的信息，请参阅邮件策略概述，第 223 页。

将加密信头添加到邮件

AsyncOS 支持使用内容过滤器或邮件过滤器将 SMTP 信头插入邮件，从而将加密设置添加到邮件。加密信头可以覆盖在关联的加密配置文件中定义的加密设置，而且它可以将指定的加密功能应用到邮件。

注释 必须设置 Cisco Ironport 设备来处理标记的邮件。

步骤 1 依次转到**邮件策略 (Mail Policies) > 传出邮件内容过滤器 (Outgoing Content Filters)** 或**传入内容过滤器 (Incoming Content Filters)**。

步骤 2 在“过滤器”(Filters) 部分，点击**添加过滤器 (Add Filter)**。

步骤 3 在“操作”(Actions) 部分，点击**添加操作 (Add Action)**，然后选择**添加/编辑信头 (Add/Edit Header)** 将加密信头插入邮件以指定一个额外的加密设置。

例如，如果希望注册的信封在发送后的 24 小时内过期，请键入 X-PostX-ExpirationDate 作为信头名称，并且键入 +24:00:00 作为信头值。

加密信头

下表显示可以添加到邮件的加密信头。

表 *41:* 邮件加密信头

MIME 信头	说明	值
X-PostX-Reply- Enabled	指示是否为邮件启用安全回复，并在邮件栏中显示“回复”(Reply) 按钮。此信头会将加密设置添加到邮件。	有关是否显示“回复”(Reply) 按钮的布尔值。设置为 true 可显示该按钮。默认值为 false。
X-PostX-Reply-All-Enabled	指示是否为邮件启用安全的“全部回复”，并在邮件栏中显示“全部回复”(Reply All) 按钮。此信头会覆盖默认配置文件设置。	有关是否显示“全部回复”(Reply All) 按钮的布尔值。设置为 true 可显示该按钮。默认值为 false。
X-PostX-Forward-Enabled	指示是否启用安全邮件转发，并在邮件栏中显示“转发”(Forward) 按钮。此信头会覆盖默认配置文件设置。	有关是否显示“转发”(Forward) 按钮的布尔值。设置为 true 可显示该按钮。默认值为 false。
X-PostX-Send-Return-Receipt	指示是否启用阅读回执。当收件人打开安全信封时，发件人将收到回执。此信头会覆盖默认配置文件设置。	有关是否发送阅读回执的布尔值。设置为 true 可显示该按钮。默认值为 false。
X-PostX-Expiration Date	在发送之前定义注册信封的到期日期。密钥服务器会在到期日期之后限制对注册信封的访问。注册信封会显示消息指明邮件已过期。此信头会将加密设置添加到邮件。 如果使用思科注册信封服务，则可以登录到网站 http://res.cisco.com 并使用邮件管理功能设置、调整或消除发送邮件后的邮件到期日期。	包含相对日期或时间的字符串值。将 +HH:MM:SS 格式用于相对小时、分钟和秒，将 +D 格式用于相对日期。默认情况下，没有到期日期。
X-PostX-ReadNotification Date	在发送前定义注册信封的“阅读”日期。如果注册信封未在此日期之前阅读，则本地密钥服务器生成通知。具有此信头的注册信封不使用思科注册信封服务，只有使用一个本地密钥服务器。此信头会将加密设置添加到邮件。	包含相对日期或时间的字符串值。将 +HH:MM:SS 格式用于相对小时、分钟和秒，将 +D 格式用于相对日期。默认情况下，没有到期日期。
X-PostX-Suppress-Applet-For-Open	指示是否禁用解密小程序。解密小应用程序会导致在浏览器环境中打开邮件附件。禁用此小应用程序会导致在密钥服务器中解密邮件附件。如果禁用此选项，则打开邮件可能需要更长时间，但是它们不依赖于浏览器环境。此信头会覆盖默认配置文件设置。	指示是否禁用解密小程序的布尔值。设置为 true 可禁用小程序。默认值为 false。

MIME 信头	说明	值
X-PostX-Use-Script	指示是否发送无 JavaScript 的信封。无 JavaScript 的信封是不包括用于在收件人计算机本地打开信封的 JavaScript 的注册信封。收件人必须使用在线打开方法或通过转发打开方法查看邮件。如果收件人域的网关剥离 JavaScript 并使加密消息不可打开，可使用此信头。此信头会将加密设置添加到邮件。	用于指明是否包含 JavaScript 小程序的布尔值。设置为 false 可发送无 JavaScript 的信封。默认值为 true。
X-PostX-Remember-Envelope-Key-Checkbox	指示是否允许通过信封特定的密钥缓存来离线打开信封。通过信封密钥缓存，当收件人输入正确的密码并选中“记住此信封的密码”复选框时，会在收件人计算机上缓存特定信封的解密密钥。随后，收件人不需要重新输入密码，便可在计算机上重新打开信封。此信头会将加密设置添加到邮件。	用于指明是否启用密钥缓存并显示“记住此信封的密码”(Remember the password for this envelope) 复选框的布尔值。默认值为 false。

加密信头示例

本部分提供 XML 信头的示例。

启用信封密钥缓存进行离线打开

要在启用了信封密钥缓存的情况下发送注册信封，请将以下信头插入邮件中：

```
X-PostX-Remember-Envelope-Key-Checkbox: true
```

“记住此信封的密码”(Remember the password for this envelope) 复选框会在显示注册信封中。

启用无 JavaScript 的信封

要发送无 JavaScript 的注册信封，请将以下信头插入邮件中：

```
X-PostX-Use-Script: false
```

当收件人打开 securedoc.html 附件时，会显示具有“在线打开”(Open Online) 链接的注册信封，并且“打开”(Open) 按钮已禁用。

启用邮件到期

要配置邮件，以便其在发送后的 24 小时过期，请将以下信头插入邮件中：

```
X-PostX-ExpirationDate: +24:00:00
```

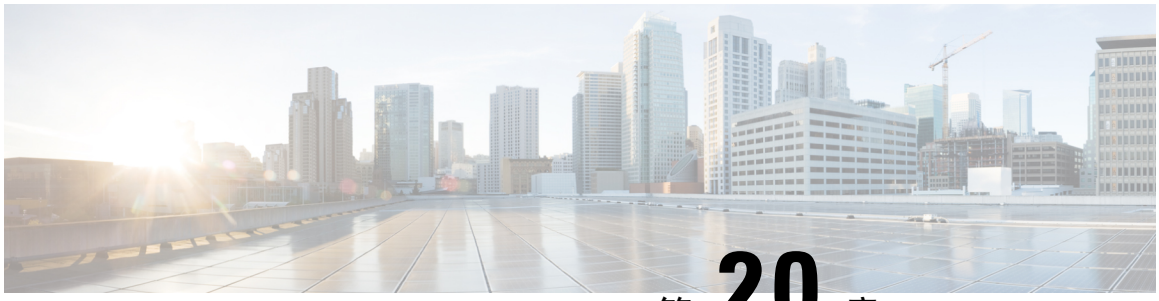
在发送后的24小时内，收件人可以打开并查看加密邮件的内容。随后，注册信封会显示消息指明信封已过期。

禁用解密小程序

要禁用解密小程序并在密钥服务器中解密邮件附件，请将以下信头插入邮件中：

```
X-PostX-Suppress-Applet-For-Open: true
```

注释 当禁用了解密小程序时，可能需要更长时间打开邮件，但是这不依赖于浏览器环境。



第 20 章

S/MIME 安全服务

本章包含以下部分：

S/MIME 安全服务概述

安全/多用途互联网邮件扩展 (S/MIME) 是一种基于标准的用于发送和接收经过验证的安全邮件的方法。S/MIME 使用公钥/私钥对来对邮件加密或签名。这样，

- 如果邮件进行了加密，则只有邮件收件人才能打开加密的邮件。
- 如果邮件进行了签名，则邮件收件人可验证发件人的域的身份，并可确保邮件在传输过程中未被修改。

有关 S/MIME 的详细信息，请查看以下 RFC：

- RFC 5750：安全/多用途互联网邮件扩展 (S/MIME) 版本 3.2 - 证书处理
- RFC 5751：安全/多用途互联网邮件扩展 (S/MIME) 版本 3.2 - 邮件规范
- RFC 3369：邮件语法加密

邮件安全设备中的 S/MIME 安全服务

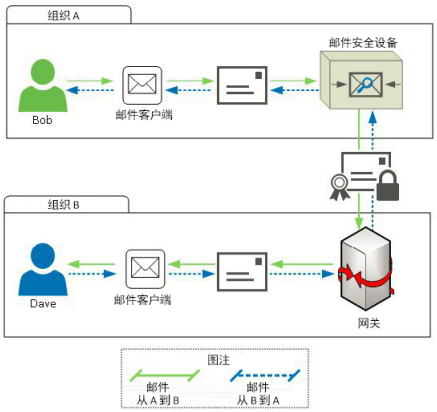
组织可能希望使用 S/MIME 安全地通信，而无需所有最终用户都拥有自己的证书。对于此类组织，邮件安全设备支持使用标识组织（而不是单个用户）的证书在网关级别执行 S/MIME 安全服务（签名、加密、验证和解密）。

邮件安全设备为企业到企业 (B2B) 和企业到消费者 (B2C) 场景提供以下 S/MIME 安全服务：

- 使用 S/MIME 对邮件签名、加密或签名并加密。请参阅使用 S/MIME 签名并/或加密传出邮件，第 416 页。
- 使用 S/MIME 验证、解密邮件或解密并验证邮件。请参阅使用 S/MIME 验证、解密或解密并验证传入的邮件，第 425 页。

了解 S/MIME 安全服务的工作方式

场景：企业到企业



组织 A 和 B 希望它们之间传输的所有邮件都使用 S/MIME 签名和加密。组织 A 配置了邮件安全设备，在网关级别执行 S/MIME 安全服务。组织 B 配置了第三方应用，在网关级别执行 S/MIME 安全服务。

注释 当前示例假设组织 B 使用第三方应用来执行 S/MIME 安全服务。实际上，可以使用能在网关级别执行 S/MIME 安全服务的任何应用或设备（包括邮件安全设备）。

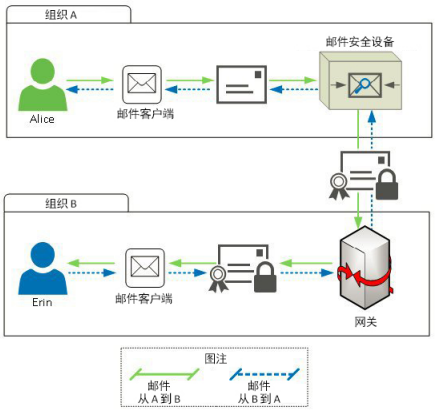
组织 A 向组织 B 发送邮件：

1. Bob（组织 A）使用邮件客户端向 Dave（组织 B）发送未签名和加密的邮件。
2. 组织 A 中的邮件安全设备对邮件签名并加密，然后将其发送到组织 B。
3. 组织 B 网关的第三方应用解密并验证该邮件。
4. Dave 收到未加密和签名的邮件。

组织 B 向组织 A 发送邮件：

1. Dave（组织 B）使用邮件客户端向 Bob（组织 A）发送未签名和加密的邮件。
2. 组织 B 网关的第三方应用对邮件签名并加密，然后将其发送到组织 A。
3. 组织 A 中的邮件安全设备解密并验证该邮件。
4. Bob 收到未加密和签名的邮件。

场景：企业到消费者



组织 A 和 B 希望它们之间传输的所有邮件都使用 S/MIME 签名和加密。组织 A 配置了邮件安全设备，在网关级别执行 S/MIME 安全服务。组织 B 配置了所有用户的邮件客户端来执行 S/MIME 安全服务。

组织 A 向组织 B 发送邮件：

1. Alice（组织 A）使用邮件客户端向 Erin（组织 B）发送未签名和加密的邮件。
2. 组织 A 中的邮件安全设备对邮件签名并加密，然后将其发送到组织 B。
3. 组织 B 的邮件客户端解密并验证该邮件，然后为 Erin 显示邮件内容。

组织 B 向组织 A 发送邮件：

1. Erin（组织 B）使用邮件客户端对邮件签名并加密，然后将其发送给 Alice（组织 A）。
2. 组织 A 中的邮件安全设备解密并验证该邮件。
3. Alice 收到未加密和签名的邮件。

使用 S/MIME 签名并/或加密传出邮件

注释 您可以使用邮件安全设备签名、加密及签名并加密传出和传入的邮件。

邮件安全设备中的 S/MIME 签名和加密工作流程

S/MIME 签名工作流程

以下过程介绍邮件安全设备如何执行 S/MIME 签名。

1. 对邮件应用哈希算法，以创建邮件摘要。
2. 利用设备的 S/MIME 证书私钥对邮件摘要加密。
3. 利用加密的邮件摘要和设备的 S/MIME 证书公钥创建 PKCS7 签名。
4. 通过将 PKCS7 签名附加到邮件中，对邮件签名。
5. 将签名的邮件发送给收件人。

S/MIME 加密工作流程

以下过程介绍邮件安全设备如何执行 S/MIME 加密。

1. 创建一个伪随机的会话密钥。
2. 使用该会话密钥对邮件正文加密。
3. 使用收件人（网关或消费者）的 S/MIME 证书公钥对该会话密钥加密。
4. 将加密的会话密钥附加到邮件中。
5. 将加密的邮件发送给收件人。

注释 如果在设备中启用了 PXE 和 S/MIME 加密，邮件安全设备将首先使用 S/MIME 对邮件加密，然后再使用 PXE 加密。

如何使用 S/MIME 签名、加密或签名并加密传出邮件

步骤	请	更多信息
第 1 步	了解 S/MIME 证书要求。	请参阅S/MIME 证书要求，第 430 页。

步骤	请	更多信息
第 2 步	根据您的要求，执行以下操作之一： • 要执行 S/MIME 签名，请设置 S/MIME 签名证书。 • 要执行 S/MIME 加密，请设置收件人 S/MIME 证书的公钥。 • 要执行 S/MIME 签名并加密，请分别设置 S/MIME 签名证书和收件人 S/MIME 证书的公钥。	请参阅： • 设置用于 S/MIME 签名的证书，第 417 页 • 设置用于 S/MIME 加密的公钥，第 420 页
第 3 步	创建一个配置文件用于签名、加密或签名并加密邮件。	请参阅创建签名、加密或签名和加密邮件的 S/MIME 发送配置文件，第 422 页。
第 4 步	定义设备要对邮件签名、加密或签名并加密，邮件所必须满足的条件。	请参阅确定要签名、加密或签名并加密的邮件，第 423 页。
第 5 步	确定在邮件工作流程中对邮件签名、加密或签名并加密的时间。	请参阅： • 使用内容过滤器签名、加密或签名并加密及立即传送邮件，第 424 页 • 传送时使用内容过滤器签名并/或加密邮件，第 424 页
第 6 步	定义要对其邮件签名或加密的用户组。	创建邮件策略。 请参阅 邮件策略，第 223 页
第 7 步	将定义的签名或加密操作与定义的用户组相关联。	将内容过滤器与邮件策略相关联。 请参阅 邮件策略，第 223 页

注释 如果要使用 CLI 执行 S/MIME 签名、加密或签名并加密，请使用 **smimeconfig** 命令。请参阅《适用于思科邮件安全设备的 *AsyncOS CLI* 参考指南》。

设置用于 S/MIME 签名的证书

要对邮件签名，必须设置 S/MIME 证书。邮件安全设备允许您使用以下方法之一设置 S/MIME 签名证书。

- 使用设备创建自签名 S/MIME 证书。请参阅创建自签名 S/MIME 证书，第 418 页。
- 将现有的 S/MIME 证书导入到设备。请参阅导入 S/MIME 签名证书，第 419 页。

注释 要将签名邮件发送给组织内或测试环境中的用户，思科建议使用自签名 S/MIME 证书。要将签名邮件发送给外部用户或生产环境中的用户，请使用从可信颁发机构获取的有效 S/MIME 证书。

要了解 S/MIME 的证书要求，请参阅S/MIME 证书要求，第 430 页。

创建自签名 S/MIME 证书

您可以使用 Web 界面或 CLI 生成符合 RFC 5750（安全/多用途互联网邮件扩展 (S/MIME) 版本 3.2 - 证书处理）要求的自签名 S/MIME 证书。

注释 要将签名邮件发送给组织内或测试环境中的用户，思科建议使用自签名 S/MIME 证书。

步骤 1 依次点击**网络 (Network)** > **证书 (Certificates)**。

步骤 2 点击 **Add Certificate**。

步骤 3 选择**创建自签名 S/MIME 证书 (Create Self-Signed S/MIME Certificate)**。

步骤 4 为自签名证书输入以下信息：

公共名称	**完全限定域名。**
组织	组织精确的法定名称。
组织单位	组织的部门。
城市(地区)	组织法定所在的城市。
省/市/自治区	组织法定所在的省/市/自治区、县或区域。
国家/地区	组织法定所在国家/地区的双字母 ISO 缩写。
过期前的持续时间	证书到期之前的天数。
主题备用名称(域)	如果配置了此字段，则来自指定域的所有用户均可发送签名邮件。 计划从中发送签名邮件的域的名称。示例包括 domain.com 和 *.domain.net。对于多个条目，请使用逗号分隔值列表。
主题备用名称(邮件)	如果配置了此字段，则只有指定用户可以发送签名邮件。 计划发送签名邮件的用户的邮件地址，例如 user@somedomain.com。对于多个条目，请使用逗号分隔值列表。
私钥大小	生成证书签名请求 (CSR) 的私钥大小。

注释　S/MIME 签名证书可能包含“主题备用名称(域)”(Subject Alternative Name (Domains)) 和“主题备用名称(邮件)”(Subject Alternative Name (Email))。

步骤 5 点击**下一步 (Next)** 查看证书和签名信息。

步骤 6 根据您的要求，执行以下操作：

- 为证书输入一个名称。
- 如果您要将自签名证书的 CSR 提交给证书颁发机构，请点击**下载证书签名请求**，以将 PEM 格式的 CSR 保存到本地或网络计算机。

步骤 7 提交并确认更改。

下一步做什么

注释　在 CLI 中，使用 **certconfig** 命令可生成自签名 S/MIME 证书。

导入 S/MIME 签名证书

如果已有用来签名邮件的 S/MIME 证书，可以通过导入将其添加到设备中。

准备工作

请确保计划导入的 S/MIME 证书符合S/MIME 证书要求，第 430 页中所述的要求。

步骤 1 依次点击**网络 (Network)** > **证书 (Certificates)**。

步骤 2 点击 **Add Certificate**。

步骤 3 选择**导入证书 (Import Certificate)**。

步骤 4 输入指向网络或本地计算机中的证书文件的路径。

步骤 5 输入该文件的密码。

步骤 6 点击**下一步 (Next)** 查看证书的信息。

步骤 7 为证书输入一个名称。

步骤 8 提交并确认更改。

下一步做什么

注释　在 CLI 中，使用 **certconfig** 命令可导入 S/MIME 证书。

设置用于 S/MIME 加密的公钥

只有将收件人 S/MIME 证书的公钥添加到设备中，才能对邮件加密。根据组织的策略和流程，可以使用下列方法之一将公钥添加到设备：

- 请求收件人使用电子通道（例如邮件）发送公钥。然后，可以使用 Web 界面或 CLI 添加公钥。

  有关添加公钥的说明，请参阅添加用于 S/MIME 加密的公钥，第 420 页。

- 使用 Web 界面或 CLI 启用公钥搜集，并请求收件人发送签名的邮件。邮件安全设备可从签名邮件中搜集公钥。

  有关从传入的签名邮件中搜集公钥的说明，请参阅搜集公钥，第 420 页。

添加用于 S/MIME 加密的公钥

准备工作

- 确保公钥符合S/MIME 证书要求，第 430 页中所述的要求。
- 确保公钥为 PEM 格式。

步骤 1 依次点击**邮件策略 (Mail Policies)** > **公钥 (Public Keys)**。

步骤 2 点击**添加公钥 (Add Public Key)**。

步骤 3 输入公钥的名称。

步骤 4 输入公钥。

步骤 5 提交并确认更改。

下一步做什么

注释 在 CLI 中，使用 **smimeconfig** 命令可添加公钥。

S/MIME 搜集的公钥

您可以将邮件安全设备配置为从传入的 S/MIME 签名邮件中检索（搜集）公钥，并利用搜集到的密钥将加密邮件发送给其所有者（企业或消费者）。

在“邮件流策略”(Mail Flow Policies) 中可以启用公钥搜集。“S/MIME 搜集的公钥”(S/MIME Harvested Public Keys) 页面将列出搜集的所有公钥。

搜集公钥

您可以将邮件安全设备配置为从传入的 S/MIME 签名邮件中检索（搜集）公钥，并利用搜集到的密钥将加密邮件发送给其所有者（企业或消费者）。

注释 默认情况下，不会从过期或自签名 S/MIME 证书中搜集公钥。

准备工作

确保发件人 S/MIME 证书的公钥符合S/MIME 证书要求，第 430 页中所述的要求。

步骤 1 依次点击**邮件策略 (Mail Policies)** > **邮件流策略 (Mail Flow Policies)**。

步骤 2 创建新的邮件流策略或修改现有的邮件流策略。

步骤 3 向下滚动至**安全功能 (Features)** 部分。

步骤 4 在“S/MIME 公钥搜集”(S/MIME Public Key Harvesting) 下，执行以下操作：

- 启用 S/MIME 公钥搜集。
- （可选）选择传入的签名邮件验证失败时是否搜集公钥。
- （可选）选择是否搜集更新的公钥。

注释 如果设备在 48 小时内收到来自同一个域或邮件的多个更新公钥，将发出风险通告。

步骤 5 提交并确认更改。

下一步做什么

注释 设备中搜集的公钥存储库的大小为 512 MB。如果存储库已满，邮件安全设备将自动删除未使用的公钥。

在 CLI 中，使用 **listenerconfig** 命令可启用密钥搜集。

下一步

请求收件人将签名邮件发送给邮件安全设备管理员。邮件安全设备将从签名的邮件中搜集公钥，并在“邮件策略”(Mail Policies) >“搜集的公钥”(Harvested Public Keys) 页面显示它们。

管理 S/MIME 发送配置文件

S/MIME 发送配置文件允许您定义参数，例如：

- 要使用的 S/MIME 模式，例如签名、加密等。
- 适用于签名的 S/MIME 证书
- 要使用的 S/MIME 签名模式，例如不透明或独立。
- 设备中收件人 S/MIME 证书的公钥不可用时采取的操作。

例如，一家组织要求发送给它们的所有邮件都进行签名，另一家组织要求发送给它们的所有邮件都进行签名并加密。在此情况下，必须创建两个发送配置文件，一个用于仅签名，另一个用于签名并加密。

您也可以使用 Web 界面或 CLI 创建、编辑、删除、导入、导出和搜索 export 搜索配置文件。

创建签名、加密或签名和加密邮件的 S/MIME 发送配置文件

步骤 1 依次点击**邮件策略 (Mail Policies)** > **发送配置文件 (Sending Profiles)**。

步骤 2 点击**添加配置文件 (Add Profile)**。

步骤 3 配置以下字段：

S/MIME 配置文件名称 (S/MIME Profile Name)	输入发送配置文件的名称。
S/MIME 模式 (S/MIME Mode)	选择 S/MIME 模式。可能的值包括： • **Sign** • **加密** • **签名/加密 (Sign/Encrypt)**。签名，然后加密 • **三重 (Triple)**。登录，加密，然后再签名 **注释** 如果使用以下 S/MIME 模式之一，当签名失败时，邮件将退回给发件人：**签名 (Sign)**、**签名/加密 (Sign/Encrypt)** 或**三重 (Triple)**。
签名证书	选择要使用的签名证书。 **注释** 只有在选择以下 S/MIME 模式之一时，才需要设置此字段：**签名 (Sign)**、**签名/加密 (Sign/Encrypt)** 或**三重 (Triple)**。
S/MIME 签名模式 (S/MIME Sign Mode)	选择 S/MIME 签名的模式。可能的值包括： • **不透明 (Opaque)**。不透明签名的邮件包含组合成单一部分的邮件和签名，并且只能通过验证签名阅读。 • **独立 (Detached)**。签名信息与签名的文本分开。这种 MIME 类型是多部分签名/签名的第二部分包含应用程序/(x-)pkcs7 签名的 MIME 子类型。 **注释** 只有在选择以下 S/MIME 模式之一时，才需要设置此字段：**签名 (Sign)**、**签名/加密 (Sign/Encrypt)** 或**三重 (Triple)**。

S/MIME 配置文件名称 (S/MIME Profile Name)	输入发送配置文件的名称。
S/MIME 操作 (S/MIME Action)	选择收件人的公钥不可用时邮件安全设备必须采取的行动。可能的值包括： • **退回 (Bounce)**。如果其中任意收件人的公钥不可用，则将该邮件退回给发件人。 • **丢弃 (Drop)**。如果其中任意收件人的公钥不可用，则丢弃该邮件。 • **拆分 (Split)**。拆分邮件。如果邮件发往的收件人的公钥不可用，将以不加密形式传送邮件；如果邮件发往的收件人的公钥可用，将以加密形式传送邮件。 **示例**：假设您要将邮件发送到 bob@example1.com 和 dave@example2.com，且 dave@example2.com 的公钥不可用。在此情况下，如果您选择了**拆分 (Split)**，邮件安全设备将： • 加密该邮件后，将其传送到 bob@example1.com。 • 将该邮件传送到 dave@example2.com，但不对其加密。 **注释** 只有在选择以下 S/MIME 模式之一时，才需要设置此字段：**加密 (Encrypt)**、**签名/加密 (Sign/Encrypt)** 或**三重 (Triple)**。

步骤 4 提交并确认更改。

下一步做什么

注释 在 CLI 中，使用 **smimeconfig** 命令可创建发送配置文件。

编辑 S/MIME 发送配置文件

步骤 1 依次点击**邮件策略 (Mail Policies)** > **发送配置文件 (Sending Profiles)**。

步骤 2 点击要修改的发送配置文件。

步骤 3 编辑创建签名、加密或签名和加密邮件的 S/MIME 发送配置文件 ，第 422 页中所述的字段。

步骤 4 提交并确认更改。

确定要签名、加密或签名并加密的邮件

创建发送配置文件后，您需要创建一个传出内容过滤器，用于确定应该对哪些邮件执行签名、加密或者签名和加密操作。内容过滤器扫描传出的邮件，并确定邮件是否与指定的条件匹配。一旦内容过滤器确定邮件与条件匹配，邮件安全设备将对该邮件签名、加密或签名并加密。

使用内容过滤器签名、加密或签名并加密及立即传送邮件

准备工作

了解构建内容过滤器条件的概念。请参阅内容过滤器的工作原理，第 235 页。

步骤 1 依次转到**邮件策略 (Mail Policies) > 传出邮件内容过滤器 (Outgoing Content Filters)**。

步骤 2 在“过滤器”(Filters) 部分，点击**添加过滤器 (Add Filter)**。

步骤 3 在“条件”(Conditions) 部分，点击**添加条件 (Add Condition)**。

步骤 4 添加一个条件，以过滤要签名、加密或签名并加密的邮件。例如，要加密敏感材料，可以添加一个条件来识别主题或正文中包含特定字词或短语（例如“机密”）的邮件。

步骤 5 点击 **OK**。

步骤 6 在“操作”(Actions) 部分，点击**添加操作 (Add Action)**。

步骤 7 从**添加操作 (Add Action)** 列表中选择 **S/MIME 签名/加密 (最终操作) (S/MIME Sign/Encrypt (Final Action))**。

步骤 8 选择要与内容过滤器关联的发送配置文件。

步骤 9 点击 **OK**。

步骤 10 提交并确认更改。

下一步做什么

添加内容过滤器后，需要将该过滤器添加到传出邮件策略中。您可能希望在默认策略中启用该内容过滤器，也可以选择将该过滤器应用到特定邮件策略，具体取决于组织的需求。有关使用邮件策略的信息，请参阅邮件策略概述，第 223 页。

传送时使用内容过滤器签名并/或加密邮件

创建传送邮件时要对其签名、加密或签名加密的内容过滤器，也就是说，该邮件将进入下一个处理阶段，并且在所有处理完成后，该邮件已得到签名、加密或签名并加密，并被传送。

准备工作

- 了解构建内容过滤器条件的概念。请参阅内容过滤器概述，第 235 页。

步骤 1 依次转到**邮件策略 (Mail Policies) > 传出邮件内容过滤器 (Outgoing Content Filters)**。

步骤 2 在“过滤器”(Filters) 部分，点击**添加过滤器 (Add Filter)**。

步骤 3 在“条件”(Conditions) 部分，点击**添加条件 (Add Condition)**。

步骤 4 添加一个条件，以过滤要签名、加密或签名并加密的邮件。例如，要加密敏感材料，可以添加一个条件来识别主题或正文中包含特定字词或短语（例如“机密”）的邮件。

步骤 5 点击 **OK**。

步骤 6 在“操作”(Actions) 部分，点击**添加操作 (Add Action)**。

步骤 7 从**添加操作 (Add Action)** 列表中选择 **传送时 S/MIME 签名/加密 (S/MIME Sign/Encrypt on Delivery)**。

步骤 8 选择要与内容过滤器关联的发送配置文件。

步骤 9 点击 **OK**。

步骤 10 提交并确认更改。

下一步做什么

添加内容过滤器后，需要将该过滤器添加到传出邮件策略中。您可能希望在默认策略中启用该内容过滤器，也可以选择将该过滤器应用到特定邮件策略，具体取决于组织的需求。有关使用邮件策略的信息，请参阅邮件策略概述，第 223 页。

使用 S/MIME 验证、解密或解密并验证传入的邮件

注释 可以使用邮件安全设备 S/MIME 安全服务验证、解密或解密并验证传出和传入的邮件。

邮件安全设备中的 S/MIME 验证和解密工作流程

S/MIME 验证工作流程

以下过程介绍邮件安全设备如何执行 S/MIME 验证。

1. 对签名邮件应用哈希算法，以创建邮件摘要。
2. 使用发件人 S/MIME 证书的公钥解密附加到签名邮件的 PKCS7 签名，并获得邮件摘要。
3. 对比生成的邮件摘要与从该签名邮件中检索到的的邮件摘要。如果邮件摘要匹配，该邮件将通过验证。
4. 使用证书颁发机构验证发件人域的 S/MIME 证书。

S/MIME 解密工作流程

以下过程介绍邮件安全设备如何执行 S/MIME 解密。

1. 使用设备 S/MIME 证书的私钥解密会话密钥
2. 使用会话密钥解密邮件正文。

如何使用 S/MIME 验证、解密或解密并验证传入的邮件

步骤	请	更多信息
第 1 步	了解 S/MIME 证书要求。	请参阅S/MIME 证书要求，第 430 页。

步骤	请	更多信息

第 2 步	根据您的要求，执行以下操作之一：
	• 要执行 S/MIME 解密，请将组织的 S/MIME 证书（包含执行解密所需的私钥）添加到设备中。
	• 要执行 S/MIME 验证，请将执行验证所需的发件人 S/MIME 证书的公钥添加到设备中。
	• 要执行 S/MIME 解密和验证，请将以下信息添加到设备中：
	  • 将组织的 S/MIME 证书（包含执行解密所需的私钥）添加到设备。
	  • 发件人域的证书颁发机构。
	  • 执行验证所需的发件人 S/MIME 证书的公钥。
		请参阅
		• 设置解密邮件的证书，第 426 页
		• 设置验证签名邮件的公钥，第 427 页
		• 导入自定义证书颁发机构列表，第 520 页

第 3 步	使用 S/MIME 配置验证、解密、解密和验证传入邮件的邮件流策略。	请参阅启用 S/MIME 解密和验证，第 429 页。
第 4 步	（可选）定义邮件安全设备将对解密或验证的邮件采取的操作。	请参阅配置针对 S/MIME 解密或验证的邮件的操作，第 430 页。

注释 如果要使用 CLI 执行 S/MIME 验证、解密或解密并验证，请依次使用 **listenerconfig** > hostaccess 命令。有关更多详细信息，请参阅 CLI 在线帮助。

设置解密邮件的证书

您必须将组织的 S/MIME 证书（包含执行解密所需的私钥）添加到设备中。

准备工作

- 通过下列方式之一，与发件人（企业或消费者）共享设备 S/MIME 证书的公钥：
  - 使用电子通道（例如邮件）发送公钥。
  - 请求发件人通过密钥搜集检索公钥。

发件人可以使用此公钥将加密的邮件发送到您的设备。

注释 在 B2C 场景下，如果组织的 S/MIME 证书是域证书，则某些邮件客户端（例如 Microsoft Outlook）可能无法使用组织的 S/MIME 证书公钥发送加密的邮件。这是因为，这些邮件客户端不支持使用域证书的公钥进行加密。

- 请确保计划导入的 S/MIME 证书符合S/MIME 证书要求，第 430 页中所述的要求。

步骤 1 依次点击**网络 (Network)** > **证书 (Certificates)**。

步骤 2 点击 **Add Certificate**。

步骤 3 选择**导入证书 (Import Certificate)**。

步骤 4 输入指向网络或本地计算机中的证书文件的路径。

步骤 5 输入该文件的密码。

步骤 6 点击**下一步 (Next)** 查看证书的信息。

步骤 7 为证书输入一个名称。

步骤 8 提交并确认更改。

下一步做什么

注释 在 CLI 中，使用 **certconfig** 命令可添加 S/MIME 证书。

设置验证签名邮件的公钥

只有将发件人 S/MIME 证书的公钥添加到设备中，才能验证签名的邮件。根据组织的策略和流程，可以使用下列方法之一将公钥添加到设备：

- 请求发件人使用电子通道（例如邮件）发送其公钥。然后，可以使用 Web 界面或 CLI 添加公钥。

  有关添加公钥的说明，请参阅添加用于 S/MIME 加密的公钥，第 420 页。

- 通过密钥搜集检索公钥。请参阅搜集公钥，第 420 页。

添加用于 S/MIME 验证的公钥

准备工作

- 确保公钥符合S/MIME 证书要求，第 430 页中所述的要求。
- 确保公钥为 PEM 格式。

步骤 1 依次点击**邮件策略 (Mail Policies)** > **公钥 (Public Keys)**。

步骤 2 点击**添加公钥 (Add Public Key)**。

步骤 3 输入公钥的名称。

步骤 4 输入公钥。

步骤 5 提交并确认更改。

下一步做什么

注释 在 CLI 中，使用 **smimeconfig** 命令可添加公钥。

搜集用于 S/MIME 验证的公钥

您可以将邮件安全设备配置为从传入的 S/MIME 签名邮件中检索（搜集）公钥，并利用搜集到的密钥来验证其所有者（企业或消费者）的签名邮件。

注释 默认情况下，不会从过期或自签名 S/MIME 证书中搜集公钥。

1. 使用 Web 界面或 CLI 启用公钥搜集。请参阅启用公钥搜集，第 428 页。
2. 请求发件人发送签名邮件。
3. 搜集完成后，将搜集的公钥添加到设备。请参阅添加用于 S/MIME 验证的搜集公钥，第 429 页。

此步骤是为了确保邮件在网关级别进行验证。

启用公钥搜集

步骤 1 依次点击**邮件策略 (Mail Policies)** > **邮件流策略 (Mail Flow Policies)**。

步骤 2 创建新的邮件流策略或修改现有的邮件流策略。

步骤 3 向下滚动至**安全功能 (Features)** 部分。

步骤 4 在“S/MIME 公钥搜集”(S/MIME Public Key Harvesting) 下，执行以下操作：

- 启用 S/MIME 公钥搜集。
- （可选）选择传入的签名邮件验证失败时是否搜集公钥。
- （可选）选择是否搜集更新的公钥。

注释 如果设备在 48 小时内收到来自同一个域或邮件的多个更新公钥，将发出风险通告。

步骤 5 提交并确认更改。

下一步做什么

注释 设备中搜集的公钥存储库的大小为512MB。如果使用的存储库已满，邮件安全设备将自动删除未使用的公钥。

在 CLI 中，使用 **listenerconfig** 命令可启用密钥搜集。

添加用于 S/MIME 验证的搜集公钥

步骤 1 依次点击**邮件策略 (Mail Policies)** > **搜集的公钥 (Harvested Public Keys)**。

步骤 2 点击搜集的目标用途的公钥，并复制该公钥。

步骤 3 将该公钥添加到设备。请参阅添加用于 S/MIME 验证的公钥，第 427 页。

步骤 4 提交并确认更改。

启用 S/MIME 解密和验证

步骤 1 依次点击**邮件策略 (Mail Policies)** > **邮件流策略 (Mail Flow Policies)**。

步骤 2 创建新的邮件流策略或修改现有的邮件流策略。

步骤 3 向下滚动至**安全功能 (Features)** 部分。

步骤 4 在“S/MIME 验证/解密”(S/MIME Decryption/Verification) 下，执行以下操作：

- 启用 S/MIME 解密和验证。
- 选择在 S/MIME 验证后是保留还是删除邮件中的数字签名。如果不希望终端用户了解 S/MIME 网关验证，请选择**删除 (Remove)**。

对于三重封装的邮件，仅保留或删除内部签名。

步骤 5 提交并确认更改。

下一步做什么

提示 如果在邮件流策略中启用了 S/MIME 解密和验证，则传送所有 S/MIME 邮件，不考虑解密和验证的状态。如果要配置处理 S/MIME 解密或验证的邮件的操作，可以使用邮件过滤器规则 smime-gateway-verified 和 smime-gateway。有关详细信息，请参阅配置针对 S/MIME 解密或验证的邮件的操作，第 430 页。

配置针对 S/MIME 解密或验证的邮件的操作

在邮件安全设备执行 S/MIME 解密、验证或两者后，您可能希望根据结果采取不同的操作。您可以使用邮件过滤器规则 smime-gateway-verified 和 smime-gateway，基于解密和/或验证的结果对邮件执行操作。有关详细信息，请参阅 使用邮件过滤器实施邮件策略，第 117 页

注释 此外，还可以使用内容过滤器条件 - **S/MIME 网关邮件 (S/MIME Gateway Message)** 和 **S/MIME 网关已验证 (S/MIME Gateway Verified)**，基于解密、验证或两者的结果对邮件执行操作。有关详细信息，请参阅 内容过滤器，第 235 页

示例：隔离验证、解密（或两者）失败的 S/MIME 邮件

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"); }
```

S/MIME 证书要求

签名的证书要求

签名的 S/MIME 证书必须包含以下信息：

公共名称	完全限定域名。
组织	组织精确的法定名称。
组织单位	组织的部门。
城市(地区)	组织法定所在的城市。
省/市/自治区	组织法定所在的省/市/自治区、县或区域。
国家/地区	组织法定所在国家/地区的双字母 ISO 缩写。
过期前的持续时间	证书到期之前的天数。
主题备用名称(域)	计划从中发送签名邮件的域的名称。示例包括 domain.com 和 *.domain.net。对于多个条目，请使用逗号分隔值列表。
主题备用名称(邮件)	计划发送签名邮件的用户的邮件地址，例如 user@somedomain.com。对于多个条目，请使用逗号分隔值列表。
私钥大小	为 CSR 生成的私钥的大小。

公共名称	完全限定域名。
密钥使用	主要用作决定证书用途的限制方法。如果指定了密钥使用延长期，则必须设置以下位：digitalSignature 和 nonRepudiation。 如果未指定密钥使用延长期，则接收客户端必须假定已设置 digitalSignature 和 nonRepudiation 位。

有关 S/MIME 证书的详细信息，请参阅“RFC 5750：安全/多用途互联网邮件扩展 (S/MIME) 版本 3.2 - 证书处理”。

加密的证书要求

加密的 S/MIME 证书必须包含以下信息：

公共名称	完全限定域名。
组织	组织精确的法定名称。
组织单位	组织的部门。
城市(地区)	组织法定所在的城市。
省/市/自治区	组织法定所在的省/市/自治区、县或区域。
国家/地区	组织法定所在国家/地区的双字母 ISO 缩写。
过期前的持续时间	证书到期之前的天数。
主题备用名称(域)	计划将加密邮件发送到的域的名称。示例包括 domain.com 和 *.domain.net。对于多个条目，请使用逗号分隔值列表。 如果计划将加密邮件发送给域中的所有用户，则公钥应包括 SAN 域。
主题备用名称(邮件)	计划作为加密邮件收件人的用户的邮件地址，例如，user@somedomain.com。对于多个条目，请使用逗号分隔值列表。
私钥大小	为 CSR 生成的私钥的大小。
密钥使用	主要用作决定证书用途的限制方法。必须指定密钥使用延长期，并且必须设置以下位：keyEncipherment。

有关 S/MIME 证书的详细信息，请参阅“RFC 5750：安全/多用途互联网邮件扩展 (S/MIME) 版本 3.2 - 证书处理”。

管理公钥

邮件安全设备需要：

- 收件人的 S/MIME 加密证书的公钥，用于加密传出邮件。
- 发件人的 S/MIME 签名证书的公钥，用于验证传入的签名邮件。

您可以通过以下方式向设备添加公钥：

- 如果您有 PEM 格式的目标公钥，可以使用 Web 界面或 CLI 进行添加。请参阅添加公钥，第 432 页。
- 如果您的目标公钥包含在导出文件中，可以将导出文件复制到 /configuration 目录，再使用 Web 界面或 CLI 将其导入。请参阅从现有导出文件中导入公钥，第 432 页。

此外，邮件安全设备还支持密钥搜集（自动从从传入的签名邮件中检索公钥）。有关详细信息，请参阅S/MIME 搜集的公钥，第 420 页。

添加公钥

准备工作

- 确保公钥符合S/MIME 证书要求，第 430 页中所述的要求。
- 确保公钥为 PEM 格式。

步骤 1 依次点击**邮件策略 (Mail Policies)** > **公钥 (Public Keys)**。

步骤 2 点击**添加公钥 (Add Public Key)**。

步骤 3 输入公钥的名称。

步骤 4 输入公钥。

步骤 5 提交并确认更改。

下一步做什么

注释 在 CLI 中，使用 **smimeconfig** 命令可添加公钥。

从现有导出文件中导入公钥

准备工作

将导出文件复制到设备的 /configuration 目录。有关创建导出文件的说明，请参阅导出公钥，第 433 页。

步骤 1 依次点击**邮件策略 (Mail Policies)** > **公钥 (Public Keys)**。

步骤 2 点击**导入公钥 (Import Public Keys)**。

步骤 3 选择导出文件，然后点击**提交 (Submit)**。

注释 如果要导入包含大量公钥的文件，则导入过程可能需要较长的时间。确保相应地调整 Web 界面或 CLI 的不活动超时时间。

步骤 4 确认您的更改。

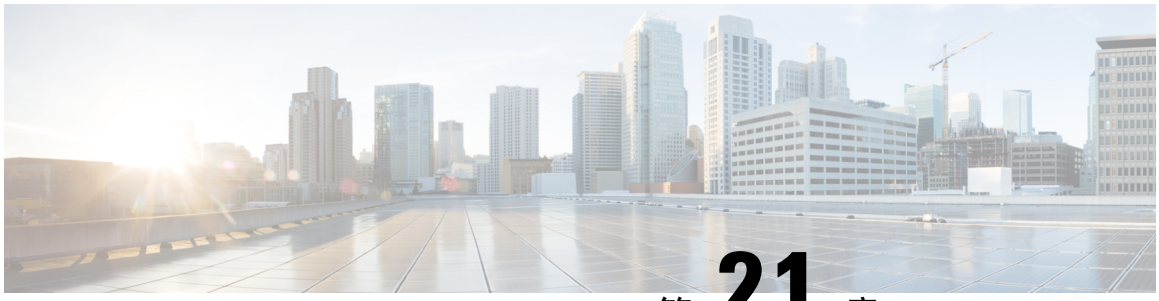
导出公钥

将设备中的所有公钥一起导出到一个文本文件中，存储在 /configuration 目录中。

步骤 1 依次选择**邮件策略 (Mail Policies)** > **公钥 (Public Keys)**。

步骤 2 点击**导出公钥 (Export Public Keys)**。

步骤 3 输入文件名称并点击**提交 (Submit)**。



第 21 章

自动修补 Office 365 邮箱中的邮件

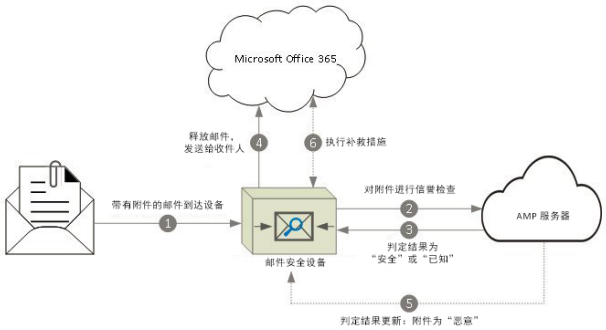
本章包含以下部分：

当威胁判决变为恶意时对传递给最终用户的邮件执行补救措施

文件在任何时候都可以变成恶意的, 即使它已经到达用户的邮箱。AMP 可以识别这一点, 新的信息涌现, 并推动追溯警报到您的装置。有了这个版本, 你得到的不仅仅是警报。如果您的组织使用 Office 365 管理邮箱, 则可以将设备配置为在威胁判决更改时对用户邮箱中的邮件执行自动补救操作。例如, 当附件的判决从 "清除" 更改为 "恶意" 时, 您可以将设备配置为从收件人邮箱中删除邮件。

工作流程

图 *36:* 邮箱自动修复工作流



1. 包含附件的邮件将发送至设备。
2. 设备将查询 AMP 服务器以评估附件的信誉。
3. AMP 服务器将判定发送给设备。判定为安全或未知。
4. 设备将邮件释放发给收件人。
5. 经过一段时间后，设备将从 AMP 服务器收到判定更新。新判定为恶意。
6. 设备对驻留在收件人邮箱中的邮件（带有恶意附件）执行配置的修复操作。

当威胁判定变为恶意时，如何对传递给最终用户的邮件执行补救操作

	请	更多信息
第 1 步	查看先决条件。	必备条件，第 437 页

	请	更多信息
第 2 步	将邮件安全设备注册为 Azure AD（Azure 管理门户）上的应用。	将您的设备注册为 Azure AD 上的应用，第 437 页
第 3 步	在设备上配置 Office 365 邮箱设置。	在思科邮件安全设备上配置 Office 365 邮箱设置，第 439 页
第 4 步	将您的设备配置为在威胁判定变为恶意时，对传递给最终用户的邮件执行补救操作。	配置当威胁判定更改为恶意时，对发送给终端用户的邮件执行的补救操作，第 440 页

必备条件

文件信誉服务和文件分析服务的功能密钥

确保您已：

- 向设备添加文件信誉服务和文件分析服务的功能密钥。
- 在设备上启用了文件信誉和分析功能。请参阅文件信誉过滤和文件分析：，第 353 页。

Office 365 帐户

请确保您拥有将设备注册到 Azure AD 所需的以下帐户：

- Office 365 企业帐户
- 与您的 Office 365 企业帐户关联的 Azure AD 订用

有关详情，请联系您的 Office 365 管理员。

安全通信证书

若要确保 Office 365 服务与设备之间的通信安全，必须以下列方式之一设置证书：创建自签名证书或从受信任的 CA 获取证书。

您必须具有：

- 采用 .crt 或 .p12 格式的公钥。请确保 emailAddress 设置为 Office 365 管理员的邮件地址 (<admin_username>@<domain>.com)。
- 采用 .pem 格式的关联私钥，密钥大小至少为 2048 位。

注释 此版本不支持带密码的私钥。

将您的设备注册为 Azure AD 上的应用

Office 365 服务使用 Azure Active Directory (Azure AD) 提供对用户邮箱的安全访问。要使您的设备能够访问 Office 365 邮箱，您必须使用 Azure AD 注册您的设备。以下是使用 Azure AD 注册设备需要

执行的概要步骤。有关详细说明，请参阅 Microsoft 文档 (https://msdn.microsoft.com/en-us/office/office365/howto/add-common-consent-manually)。

准备工作

执行 必备条件，第 437 页 中描述的任务。

步骤 1 使用 Office 365 业务帐户凭证登录到 Azure 管理门户。

步骤 2 将新应用添加到链接到 Office 365 订用的目录中。添加新应用时，请确保：

- 选择应用类型作为 Web 应用和/或 Web API。
- 指定以下参数：
  - 登录 URL。这是用户可以登录并使用您的设备的 URL，例如，`https://<company_domain.com>/ManualRegistration` 。
  - App ID URI。Microsoft Azure AD 可用于您的设备的唯一 URI，例如 `https://<company_domain.com>`。

步骤 3 配置应用所需的应用和权限。在新创建的应用的“配置”选项卡下，将 Office 365 Exchange Online 添加为应用，并设置以下权限：

- 应用权限
  - 以任何用户的方式发送邮件
  - 读取并写入所有邮箱中的邮件
  - 读取所有邮箱中的邮件
  - 使用具有所有邮箱完全访问权限的 Exchange Web Services
- 委派的权限
  - 以用户的方式发送邮件
  - 读取和写入用户邮件
  - 阅读用户邮件
  - 通过 Exchange Web Services 作为登录用户访问邮箱

步骤 4 通过使用公钥证书中的密钥凭证更新应用清单，确保 Office 365 服务与设备之间的通信安全。执行以下步骤：

a) 在 Windows PowerShell 提示符下，从公钥证书中获取 `$base64Thumbprint`、`$base64Value` 和 `$keyid` 的值。请参阅以下示例。

在 Windows PowerShell 提示符下，导航到包含公钥证书的目录，然后运行以下内容：

示例：

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import(".\mycer.cer")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)
$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)
$keyid = [System.Guid]::NewGuid().ToString()
```

运行上述命令后，运行以下命令以提取它们的值：

- `$keyid`
- `$base64Value`
- `$base64Thumbprint`

b) 从 Azure 管理门户下载应用清单。

c) 使用文本编辑器打开下载的清单，并用以下 JSON 替换空的 KeyCredentials 属性：

示例：

```
"keyCredentials": [
     {
        "customKeyIdentifier" : "$base64Thumbprint_from_step_1",
        "keyId": "$keyid_from_step1",
        "type": "AsymmetricX509Cert",
        "usage": "Verify",
        "value": "$base64Value_from_step1"
     }
],
```

在上面的 JSON 代码片段中，确保用步骤 a 中获得的值替换 `$base 64Thumbprint`、`$base 64Value` 和 `$keyid` 的值。必须在单行中输入每个值。

d) 保存您的更改并将修改后的清单上传到 Azure 管理门户。

步骤 5 在使用 Azure AD 注册您的设备后，请记下 Azure 管理门户中的以下详细信息：

- “配置”选项卡中的客户端 ID。
- 从“查看终结点”>“应用端点”页面中的租户 ID。租户 ID 是此页上列出的所有 URL 上都可用的唯一值。例如，此页上列出的 URL 为：
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/federationmetadata/2007-06/federationmetadata.xml
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/wsfed
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/saml2

在这种情况下，租户 ID 为 abcd1234-bcdd-469d-8545-a0662708cbc3。

在思科邮件安全设备上配置 Office 365 邮箱设置

准备工作

确保：

- 在设备上启用了文件信誉和分析功能。请参阅文件信誉过滤和文件分析： ，第 353 页。
- 已获取 .pem 格式的证书私钥。请参阅安全通信证书，第 437 页。
- 以下参数的值：
  - 在 Azure 管理门户上注册的应用的客户端 ID 和租户 ID。请参阅将您的设备注册为 Azure AD 上的应用，第 437 页的步骤 5。
  - 证书指纹 ($base64Thumbprint)。请参阅将您的设备注册为 Azure AD 上的应用，第 437 页的步骤 4。

步骤 1 登录到设备。

步骤 2 依次点击**系统管理** > **邮箱设置**。

步骤 3 点击**启用**。

步骤 4 选择**启用 Office 365 邮箱设置**。

步骤 5 输入下列详细信息：

- 在 Azure 管理门户上注册的应用的客户端 ID 和租户 ID。
- 证书指纹（$base 64Thumbprint 的值）。

步骤 6 上传证书的私钥。点击**选择文件**，然后选择 .pem 文件。

步骤 7 提交并确认更改。

步骤 8 验证设备是否能够连接到 Office 365 服务。

1. 点击**检查连接**。
2. 输入 Office 365 邮件地址。该地址必须是 Office 365 域中的有效邮件地址。
3. 点击**测试连接**。

弹出窗口将显示您的设备是否能够连接到 Office 365 服务。如果连接失败，请验证：

- 客户端 ID、租户 ID 和指纹的值是正确的。
- 上传的私钥是正确的，并且尚未过期。

配置当威胁判定更改为恶意时，对发送给终端用户的邮件执行的补救操作

准备工作

确保已在设备上配置了 Office 365 邮箱设置。请参阅在思科邮件安全设备上配置 Office 365 邮箱设置，第 439 页。

步骤 1 选择**邮件策略** > **传入邮件策略**。

步骤 2 点击邮件策略的**高级恶意软件防护 (Advanced Malware Protection)** 列中的链接进行修改。

步骤 3 选择**启用邮箱自动补救**。

步骤 4 指定当威胁判定更改为恶意时，对发送给终端用户的邮件将执行的操作。根据您的要求，选择下列补救操作之一：

- 转发到某个邮件地址。选择此选项可将包含恶意附件的邮件转发给指定用户，例如邮件管理员。
- 删除邮件。选择此选项可从终端用户的邮箱中永久删除包含恶意附件的邮件。
- 转发到邮件地址并删除该邮件。选择此选项可将包含恶意附件的邮件转发给指定用户（例如邮件管理员），并从终端用户的邮箱中永久删除该邮件。

注释 由于 Office 365 服务不支持删除这些文件夹中的邮件，因此无法删除来自某些文件夹（例如，已删除邮件）的邮件。

步骤 5 提交并确认更改。

监控邮箱补救结果

您可以使用邮箱自动补救报告页面（**监控** > **邮箱自动补救**）查看邮箱补救结果的详细信息。使用此报告可以查看详细信息，如：

- 对其邮箱执行的补救操作成功或不成功的收件人的列表
- 对邮件执行的修复操作
- 与 SHA-256 哈希关联的文件名

在以下情景中，**对其邮箱执行的补救操作不成功的收件人**字段会更新：

- 收件人不是有效的 Office 365 用户，或者收件人不属于您的设备上配置的 Office 365 域帐户。
- 包含附件的邮件在邮箱中不再可用，例如，终端用户删除了邮件。
- 当设备尝试执行配置的补救操作时，您的设备与 Office 365 服务之间存在连接问题。

点击 SHA-256 哈希可查看邮件跟踪中的相关邮件。

查看邮件跟踪中的邮箱修复详细信息

要在邮件跟踪中显示邮箱修复详细信息，

- 必须启用邮件跟踪。请参阅 邮件跟踪，第 677 页
- 必须配置 Office 365 邮箱设置（**系统管理** > **邮箱设置**）。请参阅在思科邮件安全设备上配置 Office 365 邮箱设置，第 439 页。
- 必须配置邮箱修复操作（**安全服务** > **邮箱自动修复**）。请参阅配置当威胁判定更改为恶意时，对发送给终端用户的邮件执行的补救操作，第 440 页。

有关所显示数据的详细信息，请参阅邮件跟踪详细信息，第 681 页。

邮箱修复疑难解答

无法检查设备和 Office 365 服务之间的连接

问题

尝试在“邮箱设置”页面（**系统管理** > **邮箱设置**）上检查设备与 Office 365 服务之间的连接时，您会收到一条错误消息：连接不成功。

解决方案

根据服务器的响应，执行以下操作之一：

错误消息	原因和解决方案
`The SMTP address has no mailbox associated with it`	输入的邮件地址不属于 Office 365 域。 请输入有效的邮件地址，然后再次检查连接。
`Application with identifier '<client_id>' was not found in the directory <tenant_id>`	输入的客户端 ID 无效。 修改“邮箱设置”页面上的客户端 ID，然后再次检查连接。
`No service namespace named '<tenant_id>' was found in the data store.`	输入的租户 ID 无效。 修改“邮箱设置”页上的租户 ID，然后再次检查连接。
`Error validating credentials. Credential validation failed`	输入的证书指纹无效。 修改“邮箱设置”页面上的证书指纹，然后再次检查连接。
`Error validating credentials. Client assertion contains an invalid signature.`	输入了错误的证书指纹，或者上传了无效或不正确的证书私钥。 核实： • 输入了正确的指纹。 • 已上传了正确的证书私钥。 • 证书私钥未到期。 • 设备的时区与证书私钥中的时区匹配。

查看日志

邮箱补救信息发布到下列日志：

- 邮件日志 (mail_logs)。邮箱补救过程启动的时间发布到此日志。
- 邮箱自动补救日志（3月）。有关补救状态、执行的操作、错误等信息都将发布到此日志中。

警报

警报：检测到设备和 Office 365 服务之间的连接问题

问题

您收到一个信息级别警报，指示设备和 Office 365 服务之间存在连接问题，而设备无法执行配置的修复操作。

解决方案

执行以下操作：

- 检查可能阻止设备和 Office 365 服务之间通信的网络问题。

查看设备的网络设置。请参阅更改网络设置，第 796 页。

- 检查防火墙是否存在问题。请参阅 防火墙资讯，第 1005 页
- 检查 Office 365 服务是否正常运行。

未执行配置补救操作

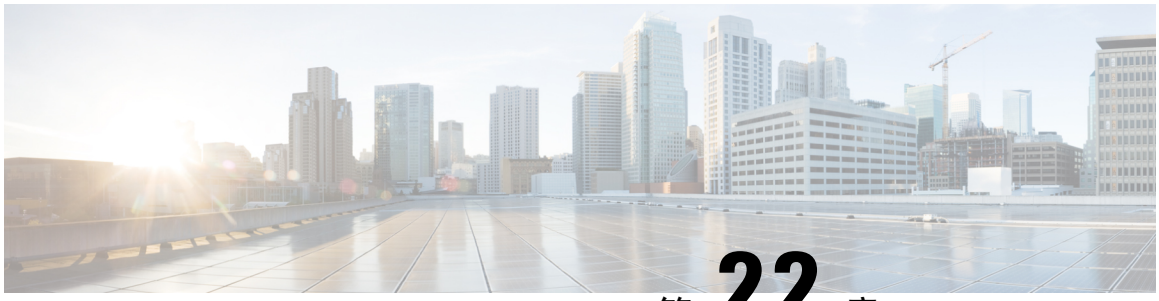
问题

从 AMP 服务器收到追溯警报后，没有对 Office 365 邮箱中的恶意邮件执行配置的补救操作。

解决方案

执行以下操作：

- 测试设备和 Office 365 服务之间的连接。请参阅在思科邮件安全设备上配置 Office 365 邮箱设置，第 439 页中的步骤 8。
- 检查是否收到以下警报：检测到设备和 Office 365 服务之间的连接问题。请参阅警报，第 442 页。



第 22 章

电邮验证

本章包含以下部分：

邮件验证概述

AsyncOS 支持邮件验证和签名，防止邮件伪造。AsyncOS 支持发件人策略框架 (SPF)、发件人 ID 框架 (SIDF)、DomainKey 识别邮件 (DKIM)、基于域的邮件验证、报告和合规 (DMARC) 以及伪造邮件检测，以验证传入邮件。AsyncOS 支持使用 DomainKey 和 DKIM 签名验证出站邮件。

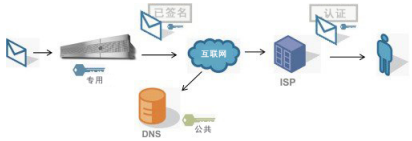
DomainKey 和 DKIM 身份验证

利用 DomainKey 或 DKIM 邮件验证，发件人可使用公钥加密方法签署邮件。之后，可通过将已验证的域与邮件 From:（或 Sender:）中的域进行对比检测伪造。

DomainKey 和 DKIM 包括两个主要部分：签名和验证。AsyncOS 支持 DomainKey 流程的“签名”部分，支持 DKIM 的签名和验证流程。您还可以对退回和延迟邮件使用 DomainKey 和 DKIM 签名。

DomainKey 和 DKIM 验证工作流程

图 *37:* 验证工作流程



1. 管理员（域所有者）发布公钥到 DNS 命名空间。
2. 管理员在出站邮件传输代理 (MTA) 上加载私钥。
3. 使用各自的私钥对该域中授权用户提交的邮件进行数字签名。将签名作为 DomainKey 或 DKIM 签名信头插入到邮件中，然后传输该邮件。
4. 接收 MTA 从信头中提取 DomainKey 或 DKIM 签名，从邮件中提取声称的发送域（通过 Sender: 或 From: 信头）。从声称的签名域（从 DomainKey 或 DKIM 信头字段）提取公钥。
5. 使用公钥判断 DomainKey 或 DKIM 签名是否由相应的私钥生成。

要测试外发 DomainKey 签名，可以使用 Yahoo! 或 Gmail 地址，因为这些服务是免费的，并可验证 DomainKey 签名的传入邮件。

AsyncOS 中的 DomainKey 和 DKIM 签名

通过域配置文件在 AsyncOS 中实施 DomainKey 和 DKIM 签名，通过邮件流策略（通常为外发“中继”策略）启用这些签名。有关详细信息，请参阅“配置网关以接收邮件”一章。签署邮件是设备在发送邮件前执行的最后一项操作。

域配置文件将域与域密钥信息（签名密钥和相关信息）关联。由于邮件通过设备上的邮件流策略发送，因此，使用域配置文件中指定的签名密钥对匹配任何域配置文件的发件人邮件地址进行DomainKey签名。如果同时启用 DKIM 和 DomainKey 签名，使用 DKIM 签名。可通过 domainkeysconfig CLI 命令，或通过GUI中的“邮件策略”>“域配置文件和邮件策略”>“签名密钥”页面，实施DomainKey和 DKIM 配置文件。

DomainKey和DKIM签名的工作原理为：域所有者生成两个密钥，一个存储在公共DNS（与该域关联的 DNS 文本记录）的公钥，一个存储在设备上对从该域发送（起源）的邮件进行签名的私钥。

在发送邮件（出站）的侦听程序上收到邮件后，设备会检查是否存在任何域配置文件。如果在设备上创建（并为邮件流策略实施了）域配置文件，设备将扫描邮件是否包含有效的 Sender: 或 From: 地址。如果两者都存在，则“发件人：”信头始终用于域密钥和DKIM签名，即使不使用“发件人：”信头进行DKIM签名，也会需要该信头。当仅存在“发件人：”信头时，在时，DomainKey或DKIM签名配置文件不匹配。“发件人：”信头仅在以下情况下使用：

- 没有“发件人：”信头。
- 选择 Web 界面的“DKIM 全局设置”页面的“使用‘发件人：’信头进行 DKIM 签名”。

注释 从 Async0S 10.0 和更高版本中，可以选择是否要使用 Web 界面的“DKIM 全局设置”页面中的“使用‘发件人：’信头进行 DKIM 签名”。将“发件人：”信头与 DKIM 签名配合使用以进行正确的 DMARC 验证非常重要。

如果找不到有效的地址，则不对邮件签名，并将此事件记录到邮件日志中。

注释 如果创建 DomainKey 和 DKIM 配置文件（并在邮件流策略中启用签名），AsyncOS 将同时使用 DomainKey 和 DKIM 签名对外发邮件签名。

如果找到有效的发送地址，则将发送地址与现有的域配置文件匹配。如果找到匹配，则对邮件签名。否则，不进行签名直接发送邮件。如果邮件已经有 DomainKey（“DomainKey-Signature:”信头），则仅当在初始签名后添加新发件人地址时才对邮件签名。如果邮件有现有的 DKIM 签名，在邮件中添加新 DKIM 签名。

AsyncOS 支持基于域对邮件签名，支持管理（创建新的输入现有）签名密钥。

本文档配置说明介绍的是最常见的签名和验证用途。此外，也可以在入站邮件的邮件流策略上启用 DomainKey 和 DKIM 签名，或者在出站邮件的邮件流策略上启用 DKIM 验证。

注释 在集群环境中配置域配置文件和签名密钥时，请注意域密钥配置文件设置和签名密钥设置是关联的。因此，如果复制、移动或删除签名密钥，系统会在相关配置文件上执行相同的操作。

配置 DomainKey 和 DKIM 签名

签名密钥

签名密钥是设备上存储的私钥。创建签名密钥时，需要指定密钥大小。密钥越大越安全；但是，密钥较大也可能会影响性能。设备支持大小在 512 位和 2048 位之间的密钥。768 - 1024 位密钥被视为安全密钥，也是当今大部分发件人使用的密钥。较长的密钥可能会影响性能，且系统不支持超过 2048 位的密钥。有关创建签名密钥的详细信息，请参阅创建或编辑签名密钥，第 453 页。

如果您输入现有密钥，只需将其粘贴到表单。另一种使用现有签名密钥的方法是，将密钥导入为文本文件。有关添加现有签名密钥的详细信息，请参阅导入或输入现有签名密钥，第 454 页。

输入后，密钥可在域配置文件中使用，并显示在域配置文件的“签名密钥”(Signing Key) 下拉列表中。

导出和导入签名密钥

您可以将设备上的签名密钥导出到文本文件中。导出密钥会将当前设备上的所有密钥放入一个文本文件。有关导出密钥的详细信息，请参阅导出签名密钥，第 453 页。

您还可以导入已经导出的密钥。

注释 导入密钥会替换当前设备上的所有密钥。

有关详细信息，请参阅导入或输入现有签名密钥，第 454 页。

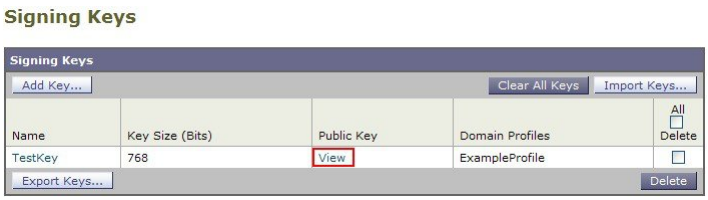
公共密钥

将签名密钥与域配置文件相关联后，可以创建包含公钥的DNS文本记录。可通过域配置文件列表中“DNS 文本记录”(DNS Text Record) 列中的“生成”(Generate) 链接（或通过 CLI 中的 **domainkeysconfig -> profiles -> dnstxt** 命令）执行此操作：

有关生成 DNS 文本记录的详细信息，请参阅生成 DNS 文本记录，第 455 页。

您可以通过“签名密钥”(Signing Keys) 页面上的“视图”(View) 链接查看公钥:

图 *38:*“签名密钥”*(Signing Keys)* 页面上的查看公钥链接



域配置文件

域配置文件将发件人域与签名密钥，以及签名需要的其他信息关联。

- 域配置文件的名称。
- 域名（应添加到“d=”信头的域）。
- 选择器（选择器用于构建公钥查询。在 DNS 查询类型中，此值被添加到发送域命名空间“_domainkey.”的前面）。
- 规范化方法（准备信头和内容向签名算法演示的方法）。AsyncOS 对 DomainKey 支持“simple”和“nofws”，对 DKIM 支持“relaxed”和“simple”。
- 签名密钥（有关详细信息，请参阅签名密钥，第 447 页）。
- 要签名的信头和正文长度列表（仅限 DKIM）。
- 要在签名的信头中添加的标签列表（仅限 DKIM）。这些标签存储以下信息：
  - 代表其对邮件签名的用户或代理（例如，邮递列表管理器）。
  - 检索公钥使用的查询方法逗号分隔列表。
  - 创建签名的时间戳。
  - 以秒为单位表示的签名到期时间。
  - 签署邮件时显示的栏分隔的信头字段列表（即，|）。
- 要在签名中添加的标签（仅限 DKIM）。

- 配置文件用户列表（允许使用域配置文件进行签名的地址）。

注释 地址中由配置文件用户指定的域必须与“域”(Domain) 字段中指定的域匹配。

可以在现有的所有域配置文件中搜索特定术语。有关详细信息，请参阅搜索域配置文件，第 456 页。

此外，您还可以选择是否：

- 使用 DKIM 签名对系统生成的邮件进行签名
- 使用“发件人”信头进行 DKIM 签名

有关说明，请参阅编辑 DKIM 全局设置，第 457 页。

导出和导入域配置文件

您可以将设备上的现有域配置文件导出到文本文件。导出域配置文件会将当前设备上的所有域配置文件放入一个文本文件中。请参阅导出域配置文件，第 456 页。

可以导入之前导出的域配置文件。导入域配置文件会替换当前设备上的所有域配置文件。请参阅导入域配置文件，第 456 页。

对外发邮件启用签名

在出站邮件的邮件流策略上启用 DomainKey 和 DKIM 签名。有关详细信息，请参阅“配置网关以接收邮件”一章。

步骤 1 在“邮件流策略”(Mail Flow Policies) 页面（从“邮件策略”(Mail Policies) 菜单）上，点击 RELAYED 邮件流策略（外发）。

步骤 2 在“安全功能”(Security Features) 部分，通过选择“开”(On) 启用 DomainKey/DKIM 签名。

步骤 3 提交并确认更改。

对退回和延迟邮件启用签名

除对出站邮件签名外，您可能还需要对退回和延迟邮件签名。您可以通过签名提醒收件人从公司收到的退回和延迟邮件是合法的。要对退回和延迟邮件启用 DomainKey 和 DKIM 签名，请对与公共侦听程序关联的退回配置文件启用 DomainKey/DKIM 签名。

步骤 1 在与签名出站邮件的目标公共侦听程序关联的退回配置文件上，找到硬退回和延迟警告邮件。

步骤 2 启用“对退回和延迟邮件启用域密钥签名”(Use Domain Key Signing for Bounce and Delay Messages)。

注释 必须完成配置 DomainKey/DKIM 签名 (GUI)，第 450 页上列出的所有步骤，才能实现对退回和延迟邮件签名。

域配置文件中的 From: 地址必须与用作退回返回地址的地址匹配。要确保这些地址匹配，可以为退回配置文件配置返回地址（“系统管理 > 返回地址”(System Administration > Return Addresses)），然后在域配置文件的“配置文件用户”(Profile Users) 中使用这一名称。例如，可以为退回返回地址配置 MAILER-DAEMON@example.com 返回地址，并添加 MAILER-DAEMON@example.com 作为域配置文件中的配置文件用户。

配置 DomainKey/DKIM 签名 (GUI)

步骤 1 创建新私钥或导入现有的私钥。有关创建或导入签名密钥的信息，请参阅签名密钥，第 447 页。

步骤 2 创建域配置文件，并将密钥与该域配置文件关联。有关创建域配置文件的信息，请参阅域配置文件，第 448 页。

步骤 3 创建 DNS 文本记录。有关创建 DNS 文本记录的信息，请参阅生成 DNS 文本记录，第 455 页。

步骤 4 在出站邮件的邮件流策略上启用 DomainKey/DKIM 签名，如果尚未启用（请参阅对外发邮件启用签名，第 449 页）。

步骤 5 或者，对退回和延迟邮件启用 DomainKey/DKIM 签名。有关对退回和延迟邮件启用签名的消息，请参阅对退回和延迟邮件启用签名，第 449 页。

步骤 6 发送邮件。对源域与域配置文件匹配的邮件进行 DomainKey/DKIM 签名。此外，如果配置签署退回和延迟邮件，则对退回或延迟邮件签名。

注释 如果创建 DomainKey 和 DKIM 配置文件（并在邮件流策略中启用签名），AsyncOS 将同时使用 DomainKey 和 DKIM 签名对外发邮件签名。

创建用于 DomainKeys 签名的域配置文件

步骤 1 依次选择**邮件策略 (Mail Policies) > 签名配置文件 (Signing Profiles)**。

步骤 2 在**域签名配置文件 (Domain Signing Profiles)** 部分，点击**添加配置文件 (Add Profile)**。

步骤 3 输入配置文件的名称。

步骤 4 对于**域密钥类型 (Domain Key Type)**，请选择**域密钥 (Domain Keys)**。

页面随即显示其他选项。

步骤 5 输入域名。

步骤 6 输入选择器。选择器是添加至“_domainkey”命名空间前面的任意名称，用于帮助支持每个发送域的多个并发公钥。在 DNS 命名空间和额外规定不能包含分号的邮件信头中，选择器值和长度必须合法。

步骤 7 选择规范化（不转发空格或 simple）。

步骤 8 如已创建签名密钥，请选择签名密钥。否则，跳到下一步。必须创建（或导入）至少一个签名密钥，才能从列表中选择签名密钥。请参阅创建或编辑签名密钥，第 453 页。

步骤 9 输入将使用域配置文件进行签名的用户（邮件地址、主机等）。

步骤 10 提交并确认更改。

步骤 11 此时，应在外发邮件流策略上启用 DomainKeys/DKIM 签名（如果尚未启用）（请参阅对外发邮件启用签名，第 449 页）。

注释 如果同时创建 DomainKey 和 DKIM 配置文件，AsyncOS 将在外发邮件上执行 DomainKey 和 DKIM 签名。

创建用于 DKIM 签名的新域配置文件

步骤 1 依次选择**邮件策略 (Mail Policies) > 签名配置文件 (Signing Profiles)**。

步骤 2 在**域签名配置文件 (Domain Signing Profiles)** 部分，点击**添加配置文件 (Add Profile)**。

步骤 3 输入配置文件的名称。

步骤 4 对于**域密钥类型 (Domain Key Type)**，请选择 **DKIM**。

页面随即显示其他选项。

步骤 5 输入域名。

步骤 6 输入选择器。选择器是添加至“_domainkey”命名空间前面的任意名称，用于帮助支持每个发送域的多个并发公钥。在 DNS 命名空间和额外规定不能包含分号的邮件信头中，选择器值和长度必须合法。

步骤 7 为标题选择规范化。从以下选项中选择：

- **Relaxed**。“relaxed”信头规范化算法执行以下操作：将信头名称更改为小写、展开信头、将线性空格缩减为单个空格、删除前导和结尾空格。
- **Simple**。不对信头做更改。

步骤 8 为正文选择规范化。从以下选项中选择：

- **Relaxed**。“relaxed”信头规范化算法执行以下操作：删除正文结尾的空行、空格缩减为行中的单个空格、删除行中的行尾空格。
- **简单**、删除正文结尾的空行。

步骤 9 如已创建签名密钥，请选择签名密钥。否则，跳到下一步。必须创建（或导入）至少一个签名密钥，才能从列表中选择签名密钥。请参阅创建或编辑签名密钥，第 453 页。

步骤 10 选择要签名的信头列表。可选择以下信头：

- **All**。AsyncOS 对签名时存在的所有信头签名。如果不想在传输过程中添加或删除信头，可能需要签署所有信头。
- **Standard**。如果想要在传输中添加或删除信头，可能需要选择标准信头。AsyncOS 仅对以下标准信头签名（如果邮件不存在信头，DKIM 签名指示信头的值为空）：

- 来源
- Sender、Reply To-
- Subject
- Date、Message-ID
- To、Cc
- MIME-Version
- Content-Type、Content-Transfer-Encoding、Content-ID、Content-Description
- Resent-Date、Resent-From、Resent-Sender、Resent-To、Resent-cc、Resent-Message-ID
- In-Reply-To、References
- List-Id、List-Help、List-Unsubscribe、LIst-Subscribe、List-Post、List-Owner、List-Archive

注释　选择“Standard”时，可添加更多要签名的信头。

步骤 11 指定如何对邮件正文签名。您可以选择对邮件正文签名，和/或要签名的字节数量。选择以下选项之一：

- **Whole Body Implied**。不要使用“l=”标签确定正文长度。对整封邮件签名，不允许做任何更改。
- **Whole Body Auto-determined**。对整封邮件签名，允许传输过程中在正文结尾附加一些额外数据。
- **Sign first _ bytes**。对达到指定字节数的邮件正文签名。

步骤 12 选择您要在邮件签名的信头字段中添加的标签。这些标签中存储的信息可用于邮件签名验证。选择以下其中一个或多个选项：

- “**i**”标签。代表其对邮件签名的用户或代理（例如，邮递列表管理器）的身份。在 @ 符号前面输入域名，例如，域@example.com。
- “**q**”标签。用于检索公钥的查询方法冒号分隔列表。目前，唯一的有效值是 dns/txt。
- “**t**”标签。创建签名时的时间戳。
- “**x**”标签。签名到期的绝对日期和时间。指定签名的到期时间（以秒为单位）。默认值为 31536000 秒。
- “**z**”标签。签署邮件时显示的栏分隔的信头字段列表（即，|）。这包括信头字段的名称及其值。例如：

z=From:admin@example.come|To:joe@example.com|
Subject:test%20message|Date:Date:August%2026,%202011%205:30:02%20PM%20-0700

步骤 13 输入将使用域配置文件进行签名的用户（邮件地址、主机等）。

注释　创建域配置文件时，请注意使用层次结构确定与特定用户关联的配置文件。例如，为 example.com 创建配置文件，为 joe@example.com 创建另一个配置文件。从 joe@example.com 发送邮件时，使用 joe@example.com 的配置文件。但是，从 adam@example.com 时发送邮件时，使用 example.com 的配置文件。

步骤 14 提交并确认更改。

步骤 15 此时，应在外发邮件流策略上启用DomainKeys/DKIM签名（如果尚未启用）（请参阅对外发邮件启用签名，第 449 页）。

注释 如果同时创建 DomainKey 和 DKIM 配置文件，AsyncOS 将在外发邮件上执行 DomainKey 和 DKIM 签名。

创建或编辑签名密钥

创建新签名密钥

必须为进行 DomainKey 和 DKIM 签名的域配置文件提供签名密钥。

步骤 1 依次选择**邮件策略 (Mail Policies) > 签名密钥 (Signing Keys)**。

步骤 2 点击**添加密钥 (Add Key)**。

步骤 3 输入密钥名称。

步骤 4 点击**生成 (Generate)** 并选择密钥大小。

步骤 5 提交并确认更改。

注释 您可能需要编辑域配置文件来分配一个密钥，如果尚未生成密钥。

编辑现有签名密钥

步骤 1 依次选择**邮件策略 (Mail Policies) > 签名密钥 (Signing Keys)**。

步骤 2 点击目标签名密钥。

步骤 3 按照创建新签名密钥，第 453 页中的说明编辑目标字段。

注释 为增强安全性，如果已在 FIPS 模式中启用设备敏感数据加密，您将无法查看私钥。如果要编辑私钥，可以粘贴私钥或生成新的私钥。

步骤 4 提交并确认更改。

导出签名密钥

设备上的所有密钥集中导出到一个文本文件中。

步骤 1 依次选择**邮件策略 (Mail Policies) > 签名密钥 (Signing Keys)**。

步骤 2 点击**导出密钥 (Export Keys)**。

注释 为增强安全性，如果已在 FIPS 模式中启用设备敏感数据加密，签名密钥导出时将进行加密。

步骤 3 输入文件名称并点击**提交 (Submit)**。

导入或输入现有签名密钥

粘贴密钥

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名密钥 (Signing Keys)**。
步骤 2 点击**添加密钥 (Add Key)**。
步骤 3 将密钥粘贴到“粘贴密钥”(Paste Key) 字段（必须是 PEM 格式，且必须只能是 RSA 密钥）。
步骤 4 提交并确认更改。

从现有导出文件导入密钥

注释 要获取密钥文件，请参阅导出签名密钥，第 453 页。

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名密钥 (Signing Keys)**。
步骤 2 点击**导入密钥 (Import Keys)**。
步骤 3 选择包含导出的签名密钥的文件。
步骤 4 点击 **Submit**。系统将警告您导入将会替换现有的所有签名密钥。文本文件中的密钥均被导入。
步骤 5 点击 **Import**。

删除签名密钥

删除所选的签名密钥

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名密钥 (Signing Keys)**。
步骤 2 选中每个要删除签名密钥右侧的复选框。
步骤 3 点击 **Delete**。
步骤 4 确认删除。

删除所有签名密钥

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名密钥 (Signing Keys)**。
步骤 2 点击“签名密钥”(Signing Keys) 页面上的**清除所有密钥 (Clear All Keys)**。

步骤 3 确认删除。

生成 DNS 文本记录

步骤 1 依次选择**邮件策略 (Mail Policies) > 签名配置文件 (Signing Profiles)**。

步骤 2 在“域签名配置文件”(Domain Signing Profiles) 部分的“DNS 文本记录”(DNS Text Record) 列中，点击相应域配置文件的**生成 (Generate)** 链接。

步骤 3 选中与要包含在 DNS 文本记录中的属性对应的复选框。

步骤 4 点击**重新生成 (Generate Again)** 使用所做更改重新生成密钥。

步骤 5 DNS 文本记录显示在窗口底部的文本字段中（可在该位置执行复制）。有时候可生成多字符串 DNS 文本记录。请参阅多字符串 DNS 文本记录，第 455 页。

步骤 6 点击 **Done**。

多字符串 DNS 文本记录

如果生成 DNS 文本记录的签名密钥的密钥大小超过 1024 位，可能会生成多字符串 DNS 文本记录。这是因为 DNS 文本记录的单个字符串中不允许超过 255 个字符。DKIM 验证可能会失败，因为某些 DNS 服务器不接受，也不提供多字符串 DNS 文本记录。

为避免出现这种情况，建议使用双引号将多字符串 DNS 文本记录分成不超过 255 个字节的短字符串。下面便是一例：

```
s._domainkey.domain.com. IN TXT "v=DKIM1;"
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE"
"A4Vbhjq2n/3DbEk6EHdeVXlIXFT7OEl81amoZLbvwMX+bej"
"CdxcsFV3uS7G8oOJSWBP0z++nTQmy9ZDWfaiopU6k7tzoi"
"+oRDlKkhCQrM4oP2B2F5sTDkYwPY3Pen2jgC2OgbPnbo3o"
"m3c1wMWgSoZxoZUE4ly5kPuK9fTtpeJHNiZAqkFICiev4yrkL"
"R+SmFsJn9MYH5+lchyZ74BVm+16Xq2mptWXEwpiwOxWI"
"YHXsZo2zRjedrQ45vmgb8xUx5ioYY9/yBLHudGc+GUKTj1i4"
"mQg48yCD/HVNfsSRXaPinliEkypH9cSnvgvWuIYUQz0dHU;"
```

DKIM 实施对如此拆分的 DNS 文本记录组合为完整原始单个字符串，然后再进行处理。

测试域配置文件

创建签名密钥、将其与域配置文件关联、生成并将 DNS 文本插入授权 DNS 后，可以测试域配置文件。

步骤 1 依次选择**邮件策略 (Mail Policies) > 签名配置文件 (Signing Profiles)**。

步骤 2 在**域签名配置文件 (Domain Signing Profiles)** 部分的“测试配置文件”(Test Profile) 列中，点击域配置文件的**测试 (Test)** 链接。

步骤 3 页面顶部将显示一条消息，表明测试成功还是失败。如果测试失败，屏幕将显示警告消息，包括错误文本。

导出域配置文件

设备上的所有域配置文件集中导出到一个文本文件中。

步骤 1 依次选择**邮件策略 (Mail Policies) > 签名配置文件 (Signing Profiles)**。
步骤 2 点击**导出域配置文件 (Export Domain Profiles)**。
步骤 3 输入文件名称并点击**提交 (Submit)**。

导入域配置文件

步骤 1 依次选择**邮件策略 (Mail Policies) > 签名配置文件 (Signing Profiles)**。
步骤 2 点击**导入域配置文件 (Import Domain Profiles)**。
步骤 3 选择包含导出的域配置文件的文件。
步骤 4 点击 **Submit**。系统将警告您导入将会替换现有的所有域配置文件。文本文件中的所有域配置文件均被导入。
步骤 5 点击 **Import**。

删除域配置文件

删除所选域配置文件

步骤 1 依次选择**邮件策略 (Mail Policies) > 签名配置文件 (Signing Profiles)**。
步骤 2 选中每个要删除域配置文件右侧的复选框。
步骤 3 点击 **Delete**。
步骤 4 确认删除。

删除所有域配置文件

步骤 1 依次选择**邮件策略 (Mail Policies) > 签名配置文件 (Signing Profiles)**。
步骤 2 点击**清除所有配置文件 (Clear All Profiles)**。
步骤 3 确认删除。

搜索域配置文件

步骤 1 依次选择**邮件策略 (Mail Policies) > 签名配置文件 (Signing Profiles)**。

步骤 2 在“查找域配置文件”(Find Domain Profiles) 部分，指定搜索词。

步骤 3 点击**查找配置文件 (Find Profiles)**。

步骤 4 搜索将扫描每个域配置文件的以下字段：邮件、域、选择器和签名密钥名称。

注释 如果不输入搜索词语，搜索引擎将返回所有域配置文件。

编辑 DKIM 全局设置

可以使用 DKIM 全局设置来选择是否：

- 使用 DKIM 签名对系统生成的邮件进行签名。设备将签署以下邮件：
  - 思科 IronPort 垃圾邮件隔离区通知
  - 内容过滤器生成的通知
  - 配置消息
  - 支持请求
- 使用“发件人”信头进行 DKIM 签名

步骤 1 依次选择**邮件策略 (Mail Policies) > 签名配置文件 (Signing Profiles)**。

步骤 2 在“DKIM 全局设置”下，点击**编辑设置**。

步骤 3 根据您的要求，配置以下字段：

- 系统生成的邮件的 DKIM 签名
- 对 DKIM 签名使用 From 信头

注释 如果您没有对 DKIM 签名使用 From 信头，或如果缺少有效的 From 信头，则将使用 Sender 信头。对于 DKIM 签名邮件的 DMARC 验证，必须在 DKIM 签名过程中使用 From 信头。

步骤 4 提交并确认更改。

域密钥和日志记录

执行 DomainKey 签名时，类似下文的行目将添加到邮件日志中：

```
Tue Aug 28 15:29:30 2007 Info: MID 371 DomainKeys: signing with dk-profile - matches
user123@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DomainKeys: cannot sign - no profile matches
user12@example.com
```

执行 DKIM 签名时，类似下文的行目将添加到邮件日志中：

```
Tue Aug 28 15:29:54 2007 Info: MID 372 DKIM: signing with dkim-profile - matches
user@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DKIM: cannot sign - no profile matches
user2@example.com
```

使用 DKIM 如何验证传入的邮件

使用 DKIM 如何验证传入的邮件

	请	更多信息
第 1 步	创建用于使用 DKIM 验证邮件的配置文件。	创建 DKIM 验证配置文件，第 459 页
第 2 步	（可选）创建用于使用 DKIM 验证传入邮件的自定义邮件流策略。	使用邮件流策略定义传入邮件规则，第 93 页
第 3 步	将邮件流策略配置为使用 DKIM 验证传入的邮件。	在邮件流策略上配置 DKIM 验证，第 461 页
第 4 步	定义邮件安全设备在已验证邮件上执行哪些操作。	配置面向 DKIM 已验证邮件的操作，第 462 页
第 5 步	将操作与特定发件人或收件人群组关联。	配置邮件策略，第 228 页

AsyncOS 执行的 DKIM 验证检查

配置 AsyncOS 设备进行 DKIM 验证时，设备将执行以下检查：

步骤 1 AsyncOS 检查传入邮件的 DKIM 签名字段、签名信头的语法，有效的标签值和所需的标签。如果签名未通过这些检查，AsyncOS 返回 *permfail*。

步骤 2 签名检查完成后，设备从公共 DNS 记录检索公钥，并验证文本记录。如果在此过程中出错，AsyncOS 返回 *permfail*。如果公钥的 DNS 查询无法获得响应，设备返回 *tempfail*。

步骤 3 检索公钥后，AsyncOS 将检查散列值并验证签名。如果在此过程中失败，AsyncOS 返回 *permfail*。

步骤 4 如果检查全部通过，AsyncOS 返回 *pass*。

注释 当邮件正文超过指定的长度时，AsyncOS 返回以下判定：

```
dkim = pass (partially verified [x bytes])
```

其中，*X* 表示验证的字节数。

最终验证结果输入为 *Authentication-Results* 信头。例如，您可能获得类似下文之一的信头：

```
Authentication-Results: example1.com

header.from=From:user123@example.com; dkim=pass (signature verified)

Authentication-Results: example1.com
```

```
header.from=From:user123@example.com; dkim=pass (partially verified [1000 bytes])

Authentication-Results: example1.com

header.from=From:user123@example.com; dkim=permfail (body hash did not verify)
```

注释 当前 DKIM 验证在第一个有效签名位置停止。无法使用检测到的最后一个签名进行验证。此功能可能会在未来版本中提供。

当域在 DKIM 测试模式 (`t=y`) 中具有其 DNS TXT 记录时，设备将彻底跳过任何 DKIM 验证和操作。

管理 DKIM 验证配置文件

DKIM 验证配置文件是邮件安全设备的邮件流策略验证 DKIM 签名使用的参数列表。例如，您可以创建两个验证配置文件，一个在查询超时前留出 30 秒的时间，一个在查询超时前仅留出 3 秒的时间。您可以将第二个验证配置文件分配给 Throttled 邮件流策略，防止在 DDoS 情况下出现连接耗竭。验证配置文件包括以下信息：

- 验证配置文件的名称。
- 可接受的最小和最大公钥大小。默认密钥大小分别为 512 和 2048 位。
- 邮件中要验证的最大签名数量。如果邮件中签名的数量超过定义的最大数量，设备将跳过验证剩余的签名，并继续处理邮件。默认为 5 个签名。
- 发件人系统时间和检验器系统时间之间允许的最大时间差（以秒为单位）。例如，如果邮件签名在 05:00:00 到期，检验器的系统时间是 05:00:30，那么如果允许的时间差是 60 秒，邮件签名将继续有效，如果允许的时间差是 10 秒，签名将无效。默认值为 60 秒。
- 一个表明是否使用正文长度参数的选项。
- 在临时失败情况下执行的 SMTP 操作。
- 在永久失败情况下执行的 SMTP 操作。

可以按配置文件名称在现有的所有验证配置文件中搜索。

可以将 DKIM 验证配置文件导出为设备配置目录中的文本文件。导出验证配置文件时，当前设备上的所有配置文件均放入一个文本文件。有关详细信息，请参阅导出 DKIM 验证配置文件，第 460 页。

可以导入之前导出的 DKIM 验证配置文件。导入 DKIM 验证配置文件会替换当前设备上的所有 DKIM 验证配置文件。有关详细信息，请参阅导入 DKIM 验证配置文件，第 460 页。

创建 DKIM 验证配置文件

步骤 1 依次点击**邮件策略 (Mail Policies) > 验证配置文件 (Verification Profiles)**。

步骤 2 点击**添加配置文件 (Add Profile)**。

步骤 3 输入配置文件的名称。

步骤 4 选择设备接受的最小签名密钥大小。

步骤 5 选择设备接受的最大签名密钥大小。

步骤 6 选择要在一封邮件中验证的最大签名数量。默认为 5 个签名。

步骤 7 选择密钥查询超时前留出的秒数。默认值为 10 秒。

步骤 8 选择发件人系统时间和检验器系统时间之间允许的最大时间差（以秒为单位）。默认值为 60 秒。

步骤 9 选择是否在签名中使用正文长度参数验证邮件。

步骤 10 选择邮件安全设备在验证邮件签名出现临时失败时接受还是拒绝邮件。如果希望设备拒绝邮件，可以选择配置设备发送默认 451 SMTP 响应代码或其他 SMTP 响应代码和文本。

步骤 11 选择邮件安全设备在验证邮件签名出现永久失败时接受还是拒绝邮件。如果希望设备拒绝邮件，可以选择配置设备发送默认 451 SMTP 响应代码或其他 SMTP 响应代码和文本。

步骤 12 提交更改。

新的配置文件随即显示在 DKIM 验证配置文件表中。

步骤 13 确认您的更改。

步骤 14 此时应在传入邮件流策略上启用 DKIM 验证，并选择要使用的验证配置文件。

导出 DKIM 验证配置文件

设备上的所有 DKIM 验证配置文件导出为一个文本文件，并保存在设备的 configuration 目录中。

步骤 1 依次选择**邮件策略 (Mail Policies) > 验证配置文件 (Verification Profiles)**。

步骤 2 点击**导出配置文件 (Export Profiles)**。

步骤 3 输入文件名称并点击**提交 (Submit)**。

导入 DKIM 验证配置文件

步骤 1 依次选择**邮件策略 (Mail Policies) > 验证配置文件 (Verification Profiles)**。

步骤 2 点击**导入配置文件 (Import Profiles)**。

步骤 3 选择包含 DKIM 验证配置文件的文件。

步骤 4 点击 **Submit**。系统将警告您导入将会替换现有的所有 DKIM 验证配置文件。

步骤 5 点击 **Import**。

删除 DKIM 验证配置文件

删除所选的 DKIM 验证配置文件

步骤 1 依次选择**邮件策略 (Mail Policies) > 验证配置文件 (Verification Profiles)**。

步骤 2 选中每个要删除 DKIM 验证配置文件右侧的复选框。

步骤 3 点击 **Delete**。

步骤 4 确认删除。

删除所有 DKIM 验证配置文件

步骤 1 依次选择**邮件策略 (Mail Policies) > 验证配置文件 (Verification Profiles)**。

步骤 2 点击**清除所有配置文件 (Clear All Profiles)**。

步骤 3 确认删除。

搜索 DKIM 验证配置文件

在所有 DKIM 验证配置文件中搜索配置文件名称中的特定术语：

步骤 1 依次选择**邮件策略 (Mail Policies) > 验证配置文件 (Verification Profiles)**。

步骤 2 在**搜索 DKIM 验证配置文件 (Search DKIM Verification Profiles)** 部分，指定搜索词。

步骤 3 点击**查找配置文件 (Find Profiles)**。

搜索将扫描每个 DKIM 验证配置文件的配置文件名称。

如果不输入搜索词，搜索引擎将返回所有 DKIM 验证配置文件。

在邮件流策略上配置 DKIM 验证

在传入邮件的邮件流策略上启用 DKIM 验证。

步骤 1 依次选择**邮件策略 (Mail Policies) > 邮件流策略 (Mail Flow Policies)**。

步骤 2 点击要执行验证的侦听程序的传入邮件策略。

步骤 3 在邮件流策略的“安全功能”(Security Features) 部分，选择**开 (On)** 启用 DKIM 验证。

步骤 4 选择要用于策略的 DKIM 验证配置文件。

步骤 5 确认您的更改。

DKIM 验证和日志记录

执行 DKIM 验证时，类似下文的行目将添加到邮件日志中：

```
mail.current:Mon Aug 6 13:35:38 2007 Info: MID 17 DKIM: no signature

mail.current:Mon Aug 6 15:00:37 2007 Info: MID 18 DKIM: verified pass
```

配置面向 DKIM 已验证邮件的操作

验证 DKIM 邮件时，系统会向邮件添加 *Authentication-Results* 信头，但不论验证结果如何仍会接受邮件。要配置基于这些验证结果的操作，可以创建内容过滤器对DKIM已验证邮件执行操作。例如，如果 DKIM 验证失败，您可能希望将邮件配置为对其进行投递、退回、丢弃或发送到隔离区。要执行此操作，必须配置一个使用内容过滤器的操作。

步骤 1 选择**邮件策略 > 传入内容过滤器**。

步骤 2 点击**添加过滤器 (Add Filter)**。

步骤 3 在“条件”(Conditions) 部分，点击**添加条件 (Add Condition)**。

步骤 4 从条件列表中选择 **DKIM 验证 (DKIM Authentication)**。

步骤 5 选择 DKIM 条件。选择以下选项之一：

- **Pass**。邮件通过验证测试。
- Neutral。验证未执行。
- **Temperror**。出现可解决的错误。
- **Permerror**。出现不可解决的错误。
- **Hardfail**。验证测试失败。
- **None**。邮件未签名。

步骤 6 选择与条件关联的操作。例如，如果 DKIM 验证失败，您可能希望通知收件人和退回邮件。或者，如果 DKIM 验证通过，您可能希望立即投递邮件，无需进一步处理。

步骤 7 提交新的内容过滤器。

步骤 8 在相应的传入邮件策略上启用内容过滤器。

步骤 9 确认您的更改。

SPF 和 SIDF 验证概述

AsyncOS 支持发件人策略框架 (SPF) 和发件人 ID 机制 (SIDF) 验证。SPF 和 SIDF 是基于 DNS 记录验证邮件真实性的方法。通过 SPF 和 SIDF，互联网域的所有者可使用特定格式的 DNS 文本记录指定哪些计算机获得传输该域邮件的权限。然后，应允的邮件收件人使用发布的 SPF 记录在邮件传输过程中测试发送邮件传输代理身份的授权。

使用 SPF/SIDF 验证时，发件人发布指定哪些主机可使用其名称的 SPF 记录，应允的邮件收件人使用发布的 SPF 记录在邮件传输过程中测试发送邮件传输代理身份的授权。

注释 由于 SPF 检查要求解析和评估，AsyncOS 的性能可能会受到影响。此外，请注意 SPF 检查会增加 DNS 基础设施的负担。

使用 SPF 和 SIDF 时，请注意 SIDF 类似于 SPF，但有一些差异。要了解 SIDF 和 SPF 两者之间差异的完整说明，请参阅 RFC 4406。在本文档中，两个术语一起讨论，除非出现仅适用一种验证类型的情况。

注释 AsyncOS 不支持用于传入中继的 SPF。

有关有效 SPF 记录的说明

要在设备上使用 SPF 和 SIDF，请根据 RFC 4406、4408 和 7208 发布 SPF 记录。查阅 RFC 4407 了解如何确定 PRA 身份。您还可以访问以下网站，了解创建 SPF 和 SIDF 记录时的常见错误：

http://www.openspf.org/FAQ/Common_mistakes

有效的 SPF 记录

要通过 SPF HELO 检查，请为每个发送 MTA（独立于域）添加“v=spf1 a －all”SPF 记录。如果不添加此记录，针对 HELO 身份的 HELO 检查可能会返回 None 判定结果。如果您发现目标至您所在域的 SPF 发件人返回大量 None 判定，这些发件人可能没有为每个发送 MTA 添加“v=spf1 a －all”SPF 记录。

有效的 SIDF 记录

要支持 SIDF 机制，您需要同时发布“v=spf1”和“spf2.0”记录。例如，您可能会有类似下文示例的 DNS 记录：

```
example.com. TXT "v=spf1 +mx a:colo.example.com/28 -all"

smtp-out.example.com TXT "v=spf1 a -all"

example.com. TXT "spf2.0/mfrom,pra +mx a:colo.example.com/28 -all"
```

SIDF 不验证 HELO 身份，因此在这种情况下，不需要为每个发送 MTA 发布 PF v2.0 记录。

注释 如果选择不支持 SIDF，请发布“spf2.0/pra ~all”记录。

检测 SPF 记录

除查阅 RFC 以外，在邮件安全设备上实施 SPF 验证之前，最好检测 SPF 记录。openspf.org website 上有多款测试工具可供选择：

http://www.openspf.org/Tools

您可以使用以下工具找出邮件未通过 SPF 记录检查的原因：

http://www.openspf.org/Why

此外，您可以在测试侦听程序上启用 SPF，使用思科的 trace 命令（或从 GUI 执行跟踪）查看 SPF 结果。使用跟踪，您可以轻松检测各个发送 IP。

如何使用 SPF/SDIF 验证传入邮件

	请	更多信息
第 1 步	（可选）创建用于使用 SPF/SDIF 验证传入邮件的自定义邮件流策略。	使用邮件流策略定义传入邮件规则，第 93 页
第 2 步	将邮件流策略配置为使用 SPF/SDIF 验证传入邮件。	启用 SPF 和 SIDF，第 464 页
第 3 步	定义邮件安全设备在已验证邮件上执行哪些操作。	确定对 SPF/SIDF 已验证邮件执行的操作，第 468 页
第 4 步	将操作与特定发件人或收件人群组关联。	配置邮件策略，第 228 页
第 5 步	（可选）测试邮件验证的结果。	测试 SPF/SIDF 结果，第 470 页

注意 虽然思科坚决支持全球邮件验证，但目前思科建议谨慎处理 SPF/SIDF 验证失败。思科强烈建议客户隔离未通过 SPF/SIDF 验证的邮件，不要退回这些邮件，直到更多组织能够对授权的邮件发送基础设施进行更为严格的掌控。

注释 AsyncOS 命令行界面 (CLI) 可提供比网络界面更多的 SPF 级别控制设置。根据 SPF 判定，设备可以在 SMTP 会话中接受或拒绝每个侦听程序上的邮件。可以在使用 listenerconfig 命令编辑侦听程序主机访问表的默认设置时修改 SPF 设置。有关这些设置的详细信息，请参阅通过 CLI 启用 SPF 和 SIDF，第 465 页。

启用 SPF 和 SIDF

要使用 SPF/SIDF，必须在传入侦听程序上启用针对邮件流策略的 SPF/SIDF。可以在侦听程序上从默认邮件流策略启用 SPF/SIDF，也可以对特定传入邮件流策略启用。

步骤 1 依次选择**邮件策略 > 邮件流策略 (Mail Policies > Mail Flow Policy)**。

步骤 2 点击**默认策略参数 (Default Policy Parameters)**。

步骤 3 查看默认策略参数中的“安全功能”(Security Features) 部分。

步骤 4 在 **SPF/SIDF 验证 (SPF/SIDF Verification)** 部分，点击**开 (On)**。

步骤 5 设置一致性级别（默认值为 SIDF-compatible）。通过此选项确定要使用的 SPF 或 SIDF 验证标准。除 SIDF 一致性之外，您可以选择包含 SPF 和 SIDF 的 SIDF-compatible。

SPF/SIDF 一致性级别

一致性级别	说明
SPF	SPF/SIDF 验证基于 RFC4408 和 RFC7208 进行操作。 - 未执行 purported responsible address (PRA) 身份验证。 **注**：选择此一致性选项测试 HELO 身份。
SIDF	SPF/SIDF 验证基于 RFC4406。 - 在与标准完全一致的情况下，确定 PRA 身份。 - SPF v1.0 记录被视为 spf2.0/mfrom,pra。 - 对于不存在的域或格式错误的身份，返回 Fail 判定。
SIDF 兼容	SPF/SIDF 验证基于 RFC4406，但以下冲突除外： - SPF v1.0 记录被视为 spf2.0/mfrom。 - 对于不存在的域或格式错误的身份，返回 None 判定。 **注**：此一致性选项应 OpenSPF 社区 (www.openspf.org) 要求推出。

注释 更多设置，请查看 CLI。有关详细信息，请参阅通过 CLI 启用 SPF 和 SIDF，第 465 页。

步骤 6 如选择一致性级别 SIDF-compatible，请配置验证是否在邮件中存在 Resent-Sender: 或 Resent-From: 信头时将 PRA 身份的 Pass 结果降级为 None。您可能会出于安全考虑选择此选项。

步骤 7 如果您选择一致性级别 SPF，可以配置是否执行 HELO 身份测试。您可以使用此选项通过禁用 HELO 检查提高性能。此选项非常实用，因为 spf-passed 过滤器规则首先检查 PRA 或 MAIL FROM 身份。设备仅对 SPF 一致性级别执行 HELO 检查。

通过 CLI 启用 SPF 和 SIDF

AsyncOS CLI 为每个 SPF/SIDF 一致性级别支持更多控制设置。配置侦听程序主机访问表的默认设置时，可以选择侦听程序的 SPF/SIDF 一致性级别和设备基于 SPF/SIDF 验证结果执行的 SMTP 操作（ACCEPT 或 REJECT）。您还可以定义设备拒绝邮件时发送的 SMTP 响应。

根据一致性级别，设备执行 HELO 身份、MAIL FROM 身份或 PRA 身份检查。针对每个身份检查的下列 SPF/SIDF 验证结果，指定设备继续会话 (ACCEPT) 还是终止会话 (REJECT)：

- **无**。由于缺少信息无法执行验证。
- **Neutral**。域所有者未表明客户端是否有权使用特定身份。
- **SoftFail**。域所有者认为主机无权使用特定身份，但无意发表明确意见。
- **Fail**。客户端无权使用特定身份发送邮件。
- **TempError**。验证过程中出现瞬时错误。

- **PermError**。验证过程中出现持久错误。

如出现 Pass 结果，设备将接受邮件，除非您将 SIDF Compatible 一致性级别配置为在邮件中存在 Resent-Sender: 或 Resent-From: 信头时将 PRA 身份的 Pass 结果降级为 None。设备之后将执行 PRA 检查返回 None 时指定的 SMTP 操作。

如选择不定义身份检查的 SMTP 操作，设备自动接受所有验证结果，包括 Fail。

如果身份验证结果匹配任何已启用身份检查的 REJECT 操作，设备将终止会话。例如，管理员配置侦听程序基于所有 HELO 身份检查结果接受邮件，包括 Fail，同时配置其拒绝 MAIL FROM 身份检查获得 Fail 结果的邮件。如果邮件未通过 HELO 身份检查，会话将继续，因为设备接受该结果。如果邮件稍后未通过 MAIL FROM 身份检查，侦听程序将终止会话，然后返回针对 REJECT 操作的 STMP 响应。

SMTP 响应是设备根据 SPF/SIDF 验证结果拒绝邮件时返回的代码编号和消息。TempError 结果返回与其他验证结果不同的 SMTP 响应。对于 TempError，默认响应代码为 451，默认消息文本为 `#4.4.3 Temporary error occurred during SPF verification`。对于所有其他验证结果，默认响应代码为 550，默认消息文本为 `#5.7.1 SPF unauthorized mail is prohibited`。您可以为 TempError 和其他验证结果指定自定义响应代码和文本消息。

或者，如果对 Neutral、SoftFail 或 Fail 验证结果执行 REJECT 操作，可将设备配置为返回来自 SPF 发布程序域的第三方响应。默认情况下，设备返回以下响应：

```
550-#5.7.1 SPF unauthorized mail is prohibited.

550-The domain example.com explains:

550 <Response text from SPF domain publisher>
```

要启用这些 SPF/SIDF 设置，请使用 `listenerconfig -> edit` 子命令并选择侦听器。然后使用 `hostaccess -> default` 子命令编辑主机访问表的默认设置。

以下 SPF 控制设置可用于主机访问表：

通过 CLI 实现的 SPF 控制设置

一致性级别	可用的 SPF 控制设置

仅限 SPF	• 是否执行 HELO 身份
	• 根据以下身份检查结果采取的 SMTP 操作：
	  • HELO 身份（如已启用）
	  • MAIL FROM 身份
	• REJECT 操作返回的 SMTP 响应代码和文本
	• 验证超时时间（以秒为单位）

一致性级别	可用的 SPF 控制设置

SIDF 兼容	• 是否执行 HELO 身份检查
	• 如果邮件中存在 Resent-Sender: 或 Resent-From: 信头，验证是否将 PRA 身份的 Pass 结果降级为 None
	• 根据以下身份检查结果采取的 SMTP 操作：
	  • HELO 身份（如已启用）
	  • MAIL FROM 身份
	  • PRA 身份
	• REJECT 操作返回的 SMTP 响应代码和文本
	• 验证超时时间（以秒为单位）

SIDF Strict	• 根据以下身份检查结果采取的 SMTP 操作：
	  • MAIL FROM 身份
	  • PRA 身份
	• REJECT 操作返回的 SMTP 响应代码和文本
	• 验证超时时间（以秒为单位）

设备执行 HELO 身份检查，接受 None 和 Neutral 验证结果并拒绝所有其他结果。所有身份类型的 SMTP 操作 CLI 提示符均相同。用户没有定义针对 MAIL FROM 身份的 SMTP 操作。设备自动接受所有身份验证结果。设备对所有 REJECT 结果均使用默认拒绝代码和文本。

还可以在命令行界面中使用 `listenerconfig` 命令配置此功能。

接收的 SPF 信头

对 AsyncOS 进行 SPF/SIDF 验证配置时，设备会在邮件中添加 SPF/SIDF 验证信头 (`Received-SPF`)。`Received-SPF` 信头包含以下信息：

- **验证结果** - SPF 验证结果（请参阅验证结果，第 468 页）。
- **身份** - SPF 验证检查的身份：HELO、MAIL FROM、PRA。
- **接收方** - 验证主机名（检查执行方）。
- **客户端 IP 地址** - SMTP 客户端的 IP 地址。
- **信封发件人** - 信封发件人邮箱。（注意，此地址可能与 MAIL FROM 身份不同，因为 MAIL FROM 身份不能空。）
- **x-sender** - HELO、MAIL FROM 或 PRA 身份的值。
- **x-conformance** - 一致性级别（请参阅表 - *SPF/SIDF* 一致性级别）以及 PRA 检查降级的执行情况。

以下示例展示如何向通过 SPF/SIDF 检查的邮件添加信头：

```
Received-SPF: Pass identity=pra; receiver=box.example.com;

client-ip=1.2.3.4; envelope-from="alice@fooo.com";
```

```
x-sender="alice@company.com"; x-conformance=sidf_compatible
```

注释 spf-status 和 spf-passed 过滤器规则使用 received-SPF 信头判断 SPF/SIDF 验证状态。

确定对 SPF/SIDF 已验证邮件执行的操作

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。可以使用以下邮件和内容过滤器规则确定 SPF/SIDF 已验证邮件的状态，并基于验证结果对邮件执行相应的操作：

- spf-status。此过滤器规则根据 SPF/SIDF 状态确定操作。可以为每个 SPF/SIDF 有效返回值指定不同的操作。
- spf-passed。此过滤器规则将 SPF/SIDF 结果表示为布尔值。

注释 spf-passed 过滤器规则仅适用于邮件过滤器。

要处理更为精细的结果时，可以使用 spf-status 规则，要创建简单布尔值时，可使用 spf-passed 规则。

验证结果

如使用 spf-status 过滤器规则，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")
```

注释 只能使用 spf-status 邮件过滤器规则检查 HELO、MAIL FROM 和 PRA 身份验证结果。不能使用 spf-status 内容过滤器规则检查身份。spf-status 内容过滤器仅检查 PRA 身份。

您可能会收到以下任何一种验证结果。

- None - 由于缺少信息无法执行验证。
- Pass - 客户端获得使用特定身份发送邮件的授权。
- Neutral - 域所有者未表明客户端是否有权使用特定身份。
- SoftFail - 域所有者认为主机无权使用特定身份，但无意发表明确意见。

- Fail - 客户端无权使用特定身份发送邮件。
- TempError - 验证过程中出现瞬时错误。
- PermError - 验证过程中出现持久错误。

在 CLI 中使用 spf-status 过滤器规则

以下示例展示 spf-status 邮件过滤器的实际应用：

```
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");

}

.
```

GUI 中的 spf-status 内容过滤器规则

您还可以从 GUI 的内容过滤器中启用 spf-status 规则。但是，使用 spf-status 内容过滤器规则时无法检查 HELO、MAIL FROM 和 PRA 身份。

要从 GUI 添加 spf-status 内容过滤器规则，请依次点击**邮件策略** > **传入内容过滤器**。然后从“添加条件”(Add Condition) 对话框添加 SPF 验证过滤器规则。为该条件指定一个或多个验证结果。

添加 SPF 验证条件后，请指定基于 SPF 状态执行的操作。例如，如果 SPF状态为 SoftFail，可能需要隔离邮件。

使用 spf-passed 过滤器规则

`spf-passed` 规则将 SPF 验证的结果显示为布尔值。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");

}
```

注释 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。

测试 SPF/SIDF 结果

测试SPF/SIDF 验证结果，并使用这些结果确定如何处理SPF/SIDF 失败，因为不同组织实施SPF/SIDF 的方式不同。结合使用内容过滤器、邮件过滤器和“邮件安全监控 - 内容过滤器”(Email Security Monitor - Content Filters) 报告，测试 SPF/SIDF 验证的结果。

对 SPF/SIDF 验证的依赖程度决定 SPF/SIDF 结果的测试精细程度。

SPF/SIDF 结果基本粒度测试

要获得针对传入邮件 SPF/SIDF 验证结果的基本衡量，可以使用内容过滤器和“邮件安全监控 - 内容过滤器”(Email Security Monitor - Content Filters) 页面。此测试可获得每种类型 SPF/SIDF 验证结果的邮件数量。

步骤 1 在传入侦听程序的邮件流策略上启用 SPF/SIDF 验证，并使用内容过滤器配置要执行的操作。有关启用 SPF/SIDF 的详细信息，请参阅启用 SPF 和 SIDF，第 464 页。

步骤 2 为每种类型的 SPF/SIDF 验证创建 **spf-status** 内容过滤器。使用命名约定表明验证类型。例如，对通过 SPF/SIDF 已验证邮件使用“SPF-Passed”，或对由于验证过程中出现瞬时错误而未能通过验证的邮件使用“SPF-TempErr”。有关创建 **spf-status** 内容过滤器的信息，请参阅GUI 中的 spf-status 内容过滤器规则，第 470 页。

步骤 3 处理大量 SPF/SIDF 验证邮件后，点击**监控 > 内容过滤器**可查看触发每种类型 SPF/SIDF 验证内容过滤器的邮件数量。

SPF/SIDF 结果精细粒度测试

要获得更全面的 SPF/SIDF 验证结果信息，可只对特定发件人组启用 SPF/SIDF 验证，查看这些特定发件人的验证结果。然后，为该特定组创建邮件策略，并在邮件策略上启用 SPF/SIDF 验证。有关创建内容过滤器和查看内容过滤器报告的信息，请参阅SPF/SIDF 结果基本粒度测试，第 471 页。如果发现验证有效，可参考 SPF/SIDF 验证决定丢弃或退回指定发件人组的邮件。

步骤 1 创建 SPF/SIDF 验证邮件流策略。对传入侦听程序上的邮件流策略启用 SPF/SIDF 验证。有关启用 SPF/SIDF 的信息，请参阅启用 SPF 和 SIDF，第 464 页。

步骤 2 创建 SPF/SIDF 验证的发件人组，并使用命名约定表明 SPF/SIDF 验证。有关创建发件人组的信息，请参阅“配置网关以接收邮件”一章。

步骤 3 为每种类型的 SPF/SIDF 验证创建 **spf-status** 内容过滤器。使用命名约定表明验证类型。例如，对通过 SPF/SIDF 已验证邮件使用“SPF-Passed”，或对由于验证过程中出现瞬时错误而未能通过验证的邮件使用“SPF-TempErr”。有关创建 **spf-status** 内容过滤器的信息，请参阅GUI 中的 spf-status 内容过滤器规则，第 470 页。

步骤 4 处理大量 SPF/SIDF 验证邮件后，点击**监控 > 内容过滤器**可查看触发每种类型 SPF/SIDF 验证内容过滤器的邮件数量。

DMARC 验证

基于域的邮件验证、报告和合规 (DMARC) 是旨在降低邮件滥用可能性的技术规范。DMARC 规范了邮件收件人如何使用 SPF 和 DKIM 机制执行邮件验证。要通过 DMARC 验证，邮件必须至少通过这些验证机制之一，且验证 ID 必须符合 RFC 5322。

邮件安全设备使您能够：

- 使用 DMARC 验证传入的邮件。

- 定义配置文件覆盖（接受、隔离或拒绝）域所有者的策略。
- 向域所有者发送反馈报告，帮助改善身份验证配置。
- 如果 DMARC 汇总报告超过 10 MB 或 DMARC 记录的 RUA 标签上指定的大小，向域所有者发送投递错误报告。

AsyncOS 可以处理符合 DMARC 规范的邮件，例如 2013 年 3 月 31 日提交给 Internet 工程任务组 (IETF) 的邮件。有关详细信息，请访问 http://tools.ietf.org/html/draft-kucherawy-dmarc-base-02。

注释 邮件安全设备不会对带有不正确格式的 DMARC 记录的域的邮件执行 DMARC 验证。但是，该设备可以接收和处理此类邮件。

DMARC 验证工作流程

下文介绍 AsyncOS 如何执行 DMARC 验证。

1. AsyncOS 上配置的侦听程序收到 SMTP 连接。
2. AsyncOS 对邮件进行 SPF 和 DKIM 验证。
3. AsyncOS 从 DNS 获取发件人域的 DMARC 记录。
   - 如果未找到记录，AsyncOS 将跳过 DMARC 验证并继续处理。
   - 如果 DNS 查找失败，AsyncOS 将根据指定的 DMARC 验证配置文件执行操作。
4. 根据 DKIM 和 SPF 验证结果，AsyncOS 对邮件执行 DMARC 验证。

注释 如果 SPF 和 DKIM 验证已启用，DMARC 验证重新使用 DKIM 和 SPF 验证结果。

5. 根据 DMARC 验证结果和指定的 DMARC 验证配置文件，AsyncOS 接受、隔离或拒绝邮件。如果邮件并未因 DMARC 验证失败而被拒绝，AsyncOS 将继续处理。
6. AsyncOS 发送相应的 SMTP 响应并继续处理。
7. 如果启用发送汇总报告，AsyncOS 将收集 DMARC 验证数据，并在发送给域所有者的每日报告中添加这些数据。有关 DMARC 汇总反馈报告的详细信息，请参阅DMARC 汇聚报告，第 477 页。

注释 如果汇总报告超过 10 MB或 DMARC 记录的 RUA 标签指定的大小，AsyncOS 会向域所有者发送投递错误报告。

使用 DMARC 如何验证传入的邮件

使用 DMARC 如何验证传入的邮件

	请	更多信息
第 1 步	根据个人需求，创建新的 DMARC 验证配置文件或修改默认DMARC验证配置文件。	创建 DMARC 验证配置文件，第 473 页 编辑 DMARC 验证配置文件，第 474 页
第 2 步	（可选）根据需求配置DMARC全局设置。	配置全局 DMARC 设置，第 475 页
第 3 步	将邮件流策略配置为使用 DMARC 验证传入的邮件。	对邮件流策略配置 DMARC 验证，第 476 页
第 4 步	（可选）配置 DMARC 反馈报告的返回地址。	配置 DMARC 反馈报告的返回地址，第 477 页
第 5 步	（可选）请查看以下信息： • DMARC 验证和传入邮件报告 • 使用邮件跟踪查看 DMARC 验证失败的邮件	• “DMARC 验证”页面，第 654 页 • “传入邮件”页面，第 644 页 • 搜索邮件，第 678 页

管理 DMARC 验证配置文件

DMARC 验证配置文件是邮件安全设备的邮件流策略验证 DMARC 使用的一系列参数。例如，您可能要创建一个严格配置文件，拒绝来自特定域的不合规邮件，一个非严格配置文件，隔离来自另一个域的所有不合规邮件。

DMARC 验证配置文件包括以下信息：

- 验证配置文件的名称。
- DMARC 记录中的策略被拒时执行的邮件操作。
- DMARC 记录中的策略被隔离时执行的邮件操作。
- 临时失败情况下执行的邮件操作。
- 永久失败情况下执行的邮件操作。

创建 DMARC 验证配置文件

使用此过程创建新 DMARC 验证配置文件。

注释 默认情况下，AsyncOS 提供默认 DMARC 验证配置文件。如不想创建新 DMARC 验证配置文件，可以使用默认 DMARC 验证配置文件。默认 DMARC 验证配置文件位于**邮件策略** > **DMARC (Mail Policies > DMARC)** 页面。有关编辑默认 DMARC 验证配置文件的说明，请参阅编辑 DMARC 验证配置文件，第 474 页。

步骤 1 依次选择**邮件策略** > **DMARC (Mail Policies > DMARC)**。

步骤 2 点击**添加配置文件 (Add Profile)**。

步骤 3 输入配置文件的名称。

步骤 4 设置 AsyncOS 在 DMARC 记录中的策略被拒时执行的邮件操作。选择以下其中一个选项：

- **无操作 (No Action)**。AsyncOS 对 DMARC 验证失败的邮件不采取任何操作。
- **隔离 (Quarantine)**。AsyncOS 将 DMARC 验证失败的邮件隔离到指定隔离区。
- **拒绝 (Reject)**。AsyncOS 拒绝所有 DMARC 验证失败的邮件，并返回指定的 SMTP 代码和响应。默认值分别为 `550 和 #5.7.1 DMARC unauthenticated mail is prohibited`。

步骤 5 设置 AsyncOS 在 DMARC 记录中的策略被隔离时执行的邮件操作。选择以下其中一个选项：

- **无操作 (No Action)**。AsyncOS 对 DMARC 验证失败的邮件不采取任何操作。
- **隔离 (Quarantine)**。AsyncOS 将 DMARC 验证失败的邮件隔离到指定隔离区。

步骤 6 设置 AsyncOS 对 DMARC 验证过程中发生临时失败的邮件执行的邮件操作。选择以下其中一个选项：

- **接受 (Accept)**。AsyncOS 接受在 DMARC 验证过程中发生临时失败的邮件。
- **拒绝 (Reject)**。AsyncOS 拒绝在 DMARC 验证过程中发生临时失败的邮件，并返回指定 SMTP 代码和响应。默认值分别为 `451 和 #4.7.1 Unable to perform DMARC verification`。

步骤 7 设置 AsyncOS 对 DMARC 验证过程中发生永久失败的邮件执行的邮件操作。选择以下其中一个选项：

- **接受 (Accept)**。AsyncOS 接受在 DMARC 验证过程中发生永久失败的邮件。
- **拒绝 (Reject)**。AsyncOS 拒绝在 DMARC 验证过程中发生永久失败的邮件，并返回指定 SMTP 代码和响应。默认值分别为 `550 和 #5.7.1 DMARC verification failed`。

步骤 8 提交并确认更改。

编辑 DMARC 验证配置文件

步骤 1 依次选择**邮件策略** > **DMARC (Mail Policies > DMARC)**。

步骤 2 点击目标验证配置文件名称。

步骤 3 按照创建 DMARC 验证配置文件，第 473 页中的说明编辑目标字段。

步骤 4 提交并确认更改。

导出 DMARC 验证配置文件

可以将设备上的所有 DMARC 验证配置文件导出到 configuration 目录下的一个文本文件中。

步骤 1 依次选择**邮件策略** > **DMARC (Mail Policies > DMARC)**。

步骤 2 点击**导出配置文件 (Export Profiles)**。

步骤 3 输入文件名称。

步骤 4 点击 **Submit**。

导入 DMARC 验证配置文件

步骤 1 依次选择**邮件策略** > **DMARC (Mail Policies > DMARC)**。

步骤 2 点击**导入配置文件 (Import Profiles)**。

步骤 3 选择包含 DMARC 验证配置文件的文件。

步骤 4 点击 **Submit**。系统将警告您导入将会替换现有的所有 DMARC 验证配置文件。

步骤 5 点击 **Import**。

步骤 6 确认您的更改。

删除 DMARC 验证配置文件

步骤 1 依次选择**邮件策略** > **DMARC (Mail Policies > DMARC)**。

步骤 2 选择要删除的验证配置文件。

步骤 3 点击 **Delete**。

步骤 4 确认删除。

配置全局 DMARC 设置

步骤 1 依次选择**邮件策略** > **DMARC (Mail Policies > DMARC)**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 更改下表中定义的设置。

DMARC 全局设置

全局设置	说明
特定发件人绕行地址列表	对来自特定发件人的邮件跳过 DMARC 验证。从下拉列表中选择一个地址列表。 注释 您可以通过选择“仅允许完整邮件地址”(Allow only full Email Addresses) 选项来只选择创建的地址列表。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，第 100 页。
绕过验证具有信头的邮件	对包含特定信头的邮件绕过 DMARC 验证。例如，使用此选项对来自发送邮件列表和信任转发器的邮件绕过 DMARC 验证。 输入一个信头或用逗号分隔的多个信头。
安排报告生成	希望 AsyncOS 生成 DMARC 汇总报告的时间。例如，可以选择在非峰值时段生成汇总报告，避免影响邮件流。

全局设置	说明
生成报告的实体	生成 DMARC 汇总报告的实体。这有助于收到 DMARC 汇总报告的域所有者确定生成报告的实体。 输入有效的域名。
报告的其他联系信息	其他联系信息，例如，组织的客户支持详细信息，如果收到 DMARC 汇总报告的域所有者要与生成报告的实体联系。
将所有汇总报告的副本发送到	将所有 DMARC 汇总报告的副本发送到特定用户，例如，分析汇总报告的内部用户。 输入一个邮件地址或用逗号分隔的多个地址。
错误报告	如果 DMARC 汇总报告超过 10 MB 或 DMARC 记录的 RUA 标签上指定的大小，向域所有者发送投递错误报告。 选中复选框。

步骤 4 提交并确认更改。

对邮件流策略配置 DMARC 验证

步骤 1 依次选择**邮件策略 (Mail Policies)** > **邮件流策略 (Mail Flow Policies)**。

步骤 2 点击要执行验证的侦听程序的传入邮件策略。

步骤 3 在邮件流策略的“安全功能”(Security Features) 部分，选择**开 (On)** 启用 DMARC 验证

步骤 4 选择要用于策略的 DMARC 验证配置文件。

步骤 5 （可选）启用将 DMARC 汇总反馈报告发送至已启用 DMARC 域的 RUA 标签中的邮件发送地址。

汇总反馈报告每天都会生成。

步骤 6 提交并确认更改。

DMARC 验证日志

邮件日志会在 DMARC 验证的以下阶段添加日志消息。

- 在邮件上尝试 DMARC 验证
- DMARC 验证完成
- DMARC 验证详细信息包括 DKIM 和 SPF 调整结果
- 跳过针对邮件的 DMARC 验证
- DMARC 记录被获取和解析，或 DNS 失败
- 为域交付 DMARC 汇总报告失败
- 为域生成错误报告

- 为域交付错误报告成功
- 为域交付错误报告失败

配置 DMARC 反馈报告的返回地址

步骤 1 依次选择**系统管理 > 返回地址 (System Administration > Return Addresses)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 提供 DMARC 汇总反馈报告的返回地址。

步骤 4 提交并确认更改。

DMARC 汇聚报告

DMARC 依赖反馈机制以安全和可扩展的方式实施域所有者策略。此反馈机制可帮助域所有者改善身份验证部署。

如使用 AsyncOS 执行 DMARC 验证，并已在邮件流策略中启用发送汇总反馈报告，AsyncOS 将每天生成汇总反馈报告，并将其发送给域所有者。这些报告采用 XML 格式并存档为 GZip 文件。

注释 AsyncOS 生成的所有 DMARC 汇总反馈报告均符合 DMARC。

DMARC 汇总反馈报告包含以下部分：

- 报告发件人的元数据（如邮件地址和报告 ID 编号）。
- 已发布 DMARC 策略的详细信息。
- DMARC 策略处理的详细信息（例如，源 IP 地址和处置摘要）。
- 域 ID
- DMARC 验证结果和验证概述。

DMARC 汇聚反馈报告示例

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <version>1.0</version>
  <report_metadata>
    <org_name>cisco.com</org_name>
    <email>noreply-dmarc-support@cisco.com</email>
    <extra_contact_info>http://cisco.com/dmarc/support</extra_contact_info>
    <report_id>b1d925$4ecceab=0694614b826605cd@cisco.com</report_id>
    <date_range>
      <begin>1335571200</begin>
      <end>1335657599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>example.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
```

```
    <p>none</p>
    <sp>none</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>1.1.1.1</source_ip>
      <count>2</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>fail</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
   <envelope_from>example.com</envelope_from>
      <header_from>example.com</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>example.com</domain>
     <selector>ny</selector>
        <result>fail</result>
      </dkim>
      <dkim>
        <domain>example.net</domain>
<selector></selector>
        <result>pass</result>
      </dkim>
      <spf>
        <domain>example.com</domain>
<scope>mfrom</scope>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
</feedback>
```

伪造邮件检测

邮件伪造（也称为欺骗、CEO 欺诈或商业电子邮件妥协）指如下过程：改变邮件信头以隐藏发件人的真实身份，从而使邮件看似是您认识的人发来的邮件。假设，欺诈者冒充组织管理人员向员工发送伪造信息，要求提供客户清单及其个人身份信息 (PII)。此员工不知道发件人的真实身份，提供了客户清单及其 PII。欺诈者使用 PII 执行身份盗窃。

思科邮件安全设备可以检测使用伪造发件人地址（“发件人:”信头）的欺诈邮件，并对此类邮件执行指定操作。例如，设备可以检测使用伪造发件人地址的邮件，并将“发件人:”信头替换为信封发件人。在这种情况下，员工将看到真实发件人（欺诈者）的邮件地址，而不是伪造的邮件地址。

设置伪造邮件检测

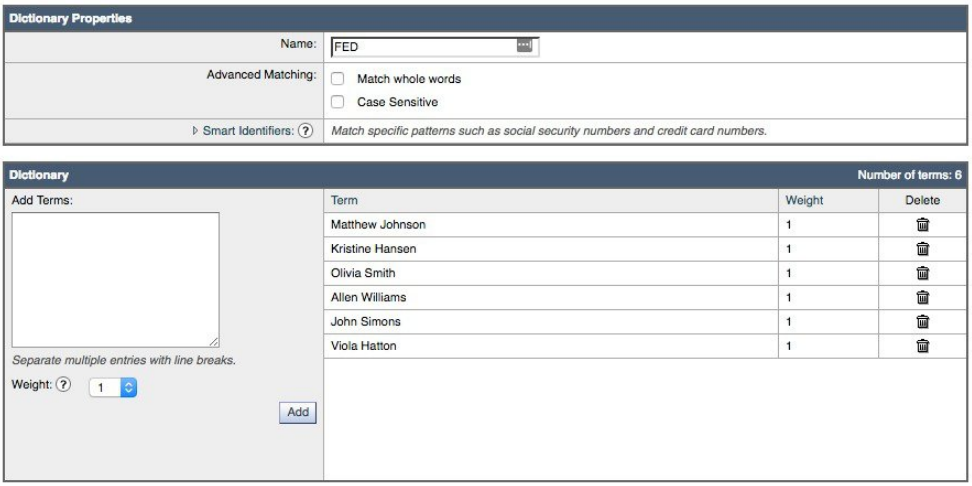
1. 标识组织中其邮件很可能是伪造的用户（例如，管理人员）。创建新的内容字典，并将已标识用户的姓名添加到该词典。

   在创建内容字典时，

- 输入用户名而不是电子邮件地址。例如，输入“Olivia Smith”而不是“olivia.smith@example.com”。
- 请勿配置高级匹配和智能标识符。
- 请勿为使用的术语选择权重。
- 请勿使用正则表达式。

下图显示了为伪造邮件检测创建的内容字典示例。

图 *39:* 伪造邮件检测的内容词典



有关配置内容字典的说明，请参见添加词典，第 484 页。

2. 创建传入内容或邮件过滤器以检测伪造邮件以及设备对这些邮件执行的操作。使用下列内容：
   - **条件/规则：**伪造邮件检测（请参阅内容过滤器条件，第 236 页和邮件过滤器规则，第 118 页）
   - **操作：**基于您的要求的伪造邮件检测或任何其他操作。（请参阅内容过滤器条件，第236页和邮件过滤器规则，第 118 页。）
3. 将新创建的内容过滤器添加到传入邮件策略。请参阅根据每个用户执行邮件策略的方法，第224页。

监控伪造邮件检测结果

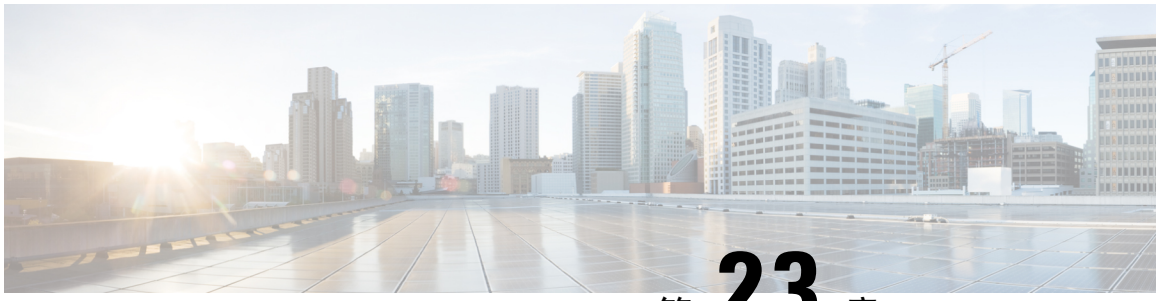
要查看有关检测到的伪造邮件的数据，请参阅“伪造邮件匹配项”报告页面（**监控 > 伪造邮件匹配项**）。此报告页面包括以下报告：

- **伪造邮件匹配项排行榜**。显示内容字典中与传入邮件中的伪造“发件人：”信头匹配的前十个用户。
- **伪造邮件匹配项：详细信息**.显示内容词典中与传入邮件中的伪造“发件人：”信头匹配所有用户的列表，对于给定用户，还会显示匹配的邮件的数量。点击该数字可查看邮件跟踪中的邮件列表。

在邮件跟踪中显示伪造邮件检测详细信息

要在邮件跟踪中显示设备检测到的伪造邮件的详细信息，请确保：

- 邮件跟踪服务已启用。请参阅邮件跟踪，第 677 页。
- 用于检测伪造邮件的内容或邮件筛选器可正常运行。



第 23 章

文本资源

本章包含以下部分：

文本资源概述

本章介绍如何创建和管理各种文本资源，例如内容词典、免责声明和模板。

内容词典

内容词典是一些字词或条目组，它们可与设备上的实体扫描功能结合使用，可用于内容过滤器和邮件过滤器。使用您定义的词典扫描邮件、邮件信头和邮件附件以查找词典中包括的术语，从而根据您的企业策略采取相应的措施。例如，您可以构建一个机密或亵渎字词列表，然后使用过滤器规则扫描包含列表中的字词的邮件，以删除、存档或隔离邮件。

AsyncOS 操作系统具备使用 GUI（“邮件策略”(Mail Policies) > “词典”(Dictionaries)）或 CLI 的 **dictionaryconfig** 命令定义总共 100 个内容词典的能力。您可以创建、删除和查看词典；从词典添加和删除条目；并导入和导出整个词典。

您可以使用内容词典对照邮件或内容过滤器来扫描邮件，以按照您的企业策略采取相应的措施。您可以创建、删除和查看词典；从词典添加和删除条目；并导入和导出整个词典。您还可以确定每个词典的大小写和词边界检测。例如，您可以构建一个机密或亵渎字词列表，然后使用过滤器规则扫描邮件中是否含有列表中的字词，以删除或存档包含匹配字词的邮件。您可以在词典中添加“权重”术语，以便某些属于可以更轻松地触发过滤器操作。

词典中可以包含非 ASCII 字符。

请注意，为了实现高效处理，以下内容词典条目将视为字词：

- 仅包含字母数字字符的条目
- 包含以下字符的邮件地址：0-9、A-Z、a-z、点、下划线、连字符和 @ 符号
- 包含以下字符的域名：0-9、A-Z、a-z、点、下划线、连字符和 at 符号

如果希望设备将这些单词处理为正则表达式，请将单词放在括号内，例如 (user@example.com)。

文本资源

文本资源是文本对象，例如免责声明、通知模板和防病毒模板。可以创建新对象以在 AsyncOS 的各种组件中使用。可以导入和导出文本资源。

邮件免责声明标记

通过邮件免责声明标记，可以向邮件中添加免责声明文本资源。例如，可以向从您的企业内发送的每封邮件附加版权声明、促销邮件或免责声明。

内容词典

内容词典是一些字词或条目组，它们可与设备上的实体扫描功能结合使用，可用于内容过滤器和邮件过滤器。使用您定义的词典扫描邮件、邮件信头和邮件附件以查找词典中包括的术语，从而根据您的企业策略采取相应的措施。例如，您可以构建一个机密或亵渎字词列表，然后使用过滤器规则扫描包含列表中的字词的邮件，以删除、存档或隔离邮件。

AsyncOS 操作系统具备使用 GUI（“邮件策略”(Mail Policies) > “词典”(Dictionaries)）或 CLI 的 **dictionaryconfig** 命令定义总共 100 个内容词典的能力。您可以创建、删除和查看词典；从词典添加和删除条目；并导入和导出整个词典。

您可以使用内容词典对照邮件或内容过滤器来扫描邮件，以按照您的企业策略采取相应的措施。您可以创建、删除和查看词典；从词典添加和删除条目；并导入和导出整个词典。您还可以确定每个词典的大小写和词边界检测。例如，您可以构建一个机密或亵渎字词列表，然后使用过滤器规则扫描邮件中是否含有列表中的字词，以删除或存档包含匹配字词的邮件。您可以在词典中添加“权重”术语，以便某些属于可以更轻松地触发过滤器操作。

词典中可以包含非 ASCII 字符。

请注意，为了实现高效处理，以下内容词典条目将视为字词：

- 仅包含字母数字字符的条目
- 包含以下字符的邮件地址：0-9、A-Z、a-z、点、下划线、连字符和 @ 符号
- 包含以下字符的域名：0-9、A-Z、a-z、点、下划线、连字符和 at 符号

如果希望设备将这些单词处理为正则表达式，请将单词放在括号内，例如 (user@example.com)。

词典内容

词典中的字词按照每行一个文本字符串的形式创建，条目可以是纯文本形式，也可以是正则表达式的形式。词典中还可以包含非 ASCII 字符。定义正则表达式词典可以提高匹配术语的灵活性，但这

样要求您了解如何正确界定字词。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/

注释 要在词典条目的开头使用特殊字符 #，可以使用字符类 [#] 以防止将该字符处理为注释。

对于每个术语，可以指定“权重”，以便某些术语可以更轻松地触发过滤器条件。当 AsyncOS 扫描邮件中的内容词典术语时，会通过将术语实例数乘以术语权重来为邮件“评分”。如果一个术语的实例数为 2，权重为 3，则得分为 6。然后，AsyncOS 会将此得分与一个与内容或邮件过滤器关联的阈值进行比较，以确定邮件是否应触发过滤操作。

您还可以为内容词典添加智能标识符。智能标识符是在数据中搜索对应于通用数字模式的模式的算法，例如社会保险号和美国银联转帐号。这些标识符对于策略的实施很有用。有关正则表达式的详细信息，请参阅“使用邮件过滤器实施邮件策略”一章中的“规则中的正则表达式”。有关智能标识符的详细信息，请参阅“使用邮件过滤器实施邮件策略”一章中的“智能标识符”。

注释 包含非 ASCII 字符的词典可能在您的终端 CLI 中无法正常显示。查看和更改包含非 ASCII 字符的词典的最佳方式是将词典导出到文本文件中，编辑该文本文件，然后将新文件重新导入设备。有关详细信息，请参阅将词典作为文本文件导入和导出，第 483 页。

字词边界和双字节字符集

在某些语言（双字节字符集）中，字词、字词边界或大小写的概念是不存在的。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。因此，您可能需要禁止字词边界的实施。

将词典作为文本文件导入和导出

默认情况下，内容词典功能还包括位于设备的配置词典中的以下文本文件：

- **config.dtd**
- **profanity.txt**
- **proprietary_content.txt**
- **sexual_content.txt**

这些文本文件旨在与内容词典功能结合使用，以帮助您创建新词典。这些内容词典已进行加权，并使用智能标识符来更好检测数据和触发过滤器中的模式（如果这些模式指示合规性问题）。

注释 导入和导出词典不会保留“匹配完整字词”(Match Whole Words) 和“区分大小写”(Case Sensitive) 设置。此设置仅在配置文件中保留。

有关访问配置目录的详细信息，请参阅FTP、SSH 和 SCP 访问，第 979 页。

您还可以创建自己的词典文件并将其导入到设备中。向字典添加非 ASCII 字符的最佳方式是在设备下的文本文件中将术语添加到词典中，将该文件移动到设备上，然后将该文件作为新词典导入。有关导入词典的详细信息，请参阅导入词典，第 485 页。有关导出词典的详细信息，请参阅导出词典，第 485 页。

⚠

注意 这些文本文件包含一些人员可能认为淫秽、下流或冒犯的术语。如果将输入从这些文件导入您的内容词典，则仅当您以后查看已在设备上配置的内容词典时才会显示这些术语。

添加词典

步骤 1 依次导航到**邮件策略 (Mail Policies)** > **词典 (Dictionaries)** 页面。

步骤 2 点击**添加词典 (Add Dictionary)**。

步骤 3 输入词典名称。

步骤 4 （可选）配置高级匹配。

注释 当您在配置文件中保存**匹配完整字词 (Match Whole Words)** 和**区分大小写 (Case Sensitive)** 设置时，AsyncOS 会保留这些设置。当导入和导出词典时，AsyncOS 不保留这些设置。

步骤 5 （可选）向词典添加智能标识符。

智能标识符是在数据中搜索对应于通用数字模式的模式的算法，例如社会保险号和美国银联转帐号。有关智能标识符的详细信息，请参阅“使用邮件过滤器实施邮件策略”一章。

步骤 6 将新词典条目添加到术语列表中。

如果您要添加多个新条目，并且希望这些条目以均等的可能性触发过滤器操作，请将每个新术语放在其自己的行中。

注释 开头或结尾带有正则表达式“.*”的内容词典条目会导致系统在发现“word”MIME 部分的匹配项时锁定。思科系统公司建议您不要在内容词典条目的开头或结尾处使用“.*”。

步骤 7 为术语指定权重。

您可以为词典术语“加权”，以便该术语相较于其他术语更有可能触发过滤器操作。有关如何使用此权重确定过滤器操作的详细信息，请参阅“使用邮件过滤器实施邮件策略”一章中的“内容词典的阈值评分”。

步骤 8 点击 **Add**。

步骤 9 提交并确认更改。

删除词典

准备工作

请注意，AsyncOS 会将引用已删除的词典的任何邮件过滤器标记为无效。AsyncOS 会将引用已删除的词典的任何内容过滤器保留为启用状态，但会将其评估为 false。

步骤 1 依次导航到**邮件策略 (Mail Policies)** > **词典 (Dictionaries) 页面**。

步骤 2 点击词典列表中要删除的词典旁边的垃圾桶图标。

确认消息会列出当前引用该词典的所有过滤器。

步骤 3 在确认邮件中点击**删除 (Delete)**。

步骤 4 确认您的更改。

导入词典

准备工作

确认要导入的文件在设备的配置目录中是否存在。

步骤 1 依次导航到**邮件策略 (Mail Policies)** > **词典 (Dictionaries)** 页面。

步骤 2 点击**导入词典 (Import Dictionary)**。

步骤 3 选择要从其导入的位置。

步骤 4 选择要导入的文件。

步骤 5 选择要为词典术语使用的默认权重。

AsyncOS 会为未指定权重的所有术语分配一个默认权重。导入文件后，可以对权重进行编辑。

步骤 6 选择一种编码方式。

步骤 7 点击 **Next**。

步骤 8 命名并编辑词典。

步骤 9 提交并确认更改。

导出词典

步骤 1 依次导航到**邮件策略 (Mail Policies)** >“词典”(Dictionaries) 页面。

步骤 2 点击**导出词典 (Export Dictionary)**。

步骤 3 选择要导出的词典。

步骤 4 为导出的词典输入文件名。

这是在设备的配置目录中创建的文件的名称。

步骤 5 选择要导出到的位置。

步骤 6 选择文本文件的编码。

步骤 7 提交并确认更改。

使用和测试内容词典过滤器规则

词典可与各种 dictionary-match() 邮件过滤器规则和内容过滤器一起使用。

词典匹配过滤器规则

如果邮件正文中包含名为 *dictionary_name* 的内容词典中的任何正则表达式，则名为 `dictionary-match(<dictionary_name>)` 的邮件过滤器规则（及其对等规则）将被评估为 true。如果该词典不存在，此规则将其评估为 false。

请注意，`dictionary-match()` 规则的作用与 `body-contains()` 正文扫描规则类似：它只扫描邮件正文和附件，而不扫描信头。

要扫描信头，可以使用适当的 `*-dictionary-match()` 类型规则（有针对特定信头的规则，例如 `subject-dictionary-match()`，也有更通用一些的规则，`header-dictionary-match()`，在该规则中，可以指定包含自定义信头的任何信头）。有关词典匹配的详细信息，请参阅“使用邮件过滤器实施邮件策略”一章中的“词典规则”。

表 *42*: 内容词典的邮件过滤器规则

规则	语法	说明
词典匹配	`dictionary-match (<dictionary_name>)`	邮件中是否包含与指定词典中列出的所有正则表达式匹配的字词？

在以下示例中，将创建一个使用 `dictionary-match()` 规则的新邮件过滤器，以在设备扫描包含名为“secret_words”的词典（在上一示例中创建）中的任何字词的邮件时秘密抄送管理员。请注意，由于设置的作用，只有包含完全匹配打小鸡的完整字词“`codename`”的邮件才会针对此过滤器被评估 true。

```
bcc_codenames:

if (dictionary-match ('secret_words'))

{

bcc('administrator@example.com');

}
```

在本例中，我们将邮件发送到策略隔离区：

```
quarantine_codenames:

if (dictionary-match ('secret_words'))

{
```

```
quarantine('Policy');

}
```

词典条目示例

表 *43:* 词典条目示例

描述	示例
通配符	
锚点	以 foo $ 结尾，以 ^ foo 开头
邮件地址（不要遗漏句点）	**foo@example.com**, **@example.com** **example.com$**（结尾）**@example.***
主题	**邮件主题**（请记住，在邮件主题中使用 ^ 锚点时，这些主题往往会加上“RE:”或“FW:”等前缀）

测试内容词典

`trace` 函数可以提供有关使用 `dictionary-match()` 规则的邮件过滤器的快速反馈。有关详细信息，请参阅使用测试邮件调试邮件流：追踪，第 935 页。您还可以使用 `quarantine()` 操作测试过滤器，如上面的 `quarantine_codenames` 过滤器示例所示。

了解文本资源

文本资源是可以附加到邮件或作为邮件发送的文本模板。文本资源可以是以下类型之一：

- **消息免责声明** - 添加到邮件的文本。有关详细信息，请参阅免责声明模板，第 491 页。
- **通知模板** - 作为通知发送的邮件，与 notify() 和 notify-bcc() 操作一起使用。有关详细信息，请参阅通知模板，第 496 页。
- **防病毒通知模板** - 在邮件中发送病毒时作为通知发送的邮件。您可以为容器（附加原始邮件）创建模板，或者作为不使用附加的邮件发送的通知创建模板。有关详细信息，请参阅防病毒通知模板，第 496 页。
- **退回和加密失败通知模板** - 邮件被退回或邮件加密失败时作为通知发送的邮件。有关详细信息，请参阅退回和加密失败通知模板，第 499 页。
- **加密通知模板** - 将设备配置为加密传出邮件时发送的邮件。该邮件会通知收件人他们已收到加密邮件并提供阅读说明。有关详细信息，请参阅加密通知模板，第 500 页。

您可以使用 CLI (**textconfig**) 或 GUI 来管理文本资源，包括：添加、删除、编辑、导入和导出。有关使用 GUI 管理文本资源的信息，请参阅文本资源管理概述，第 488 页。

文本资源中可以包含非 ASCII 字符。

注释 包含非 ASCII 字符的文本资源可能在您的终端 CLI 中无法正常显示。要查看和更改包含非 ASCII 字符的文本资源，请将文本资源导出到文本文件中，编辑该文本文件，然后将新文件重新导入设备。有关详细信息，请参阅将词典作为文本文件导入和导出，第 483 页。

将文本资源作为文本文件导入和导出

您必须有权访问设备上的配置目录。导入的文本文件必须存在于设备的配置目录中。导出的文本文件防止在配置目录中。

有关访问配置目录的详细信息，请参阅FTP、SSH 和 SCP 访问，第 979 页。

要向文本资源添加非 ASCII 字符，请在设备下的文本文件中将术语添加到文本资源中，将该文件移动到设备上，然后将该文件作为新文本资源导入。有关导入文本资源的详细信息，请参阅导入文本资源，第 489 页。有关导出文本资源的信息，请参阅导出文本资源，第 489 页。

文本资源管理概述

可以使用 GUI 或 CLI 管理文本资源。本节重点介绍 GUI。

在 CLI 中使用 **textconfig** 命令管理文本资源。

文本资源管理包括以下任务：

- 添加
- 编辑和删除
- 导出和导入
- 为所有文本资源类型定义纯文本邮件
- 为某些文本资源类型定义基于 HTML 的邮件

添加文本资源

步骤 1 依次导航到**邮件策略 (Mail Policies)** > **文本资源 (Text Resources)**

步骤 2 点击**添加文本资源 (Add Text Resource)**。

步骤 3 在**名称 (Name)** 字段中输入文本资源的名称。

步骤 4 从**类型 (Type)** 字段中选择文本资源类型。

步骤 5 在**文本 (Text)** 或 **HTML 和纯文本 (HTML and Plain Text)** 字段中输入邮件文本。

如果文本资源仅允许纯文本邮件，请使用**文本 (Text)** 字段。如果文本资源允许 HTML 和纯文本邮件，请使用 **HTML 和纯文本 (HTML and Plain Text)** 字段。

步骤 6 提交并确认更改。

删除文本资源

准备工作

注意删除文本资源所带来的影响：

- 引用已删除的文本资源的所有邮件过滤器都将被标记为无效。
- 引用已删除的文本资源的所有内容过滤器都将留为启用状态，但是会被评估为 false。

步骤 1 在**邮件策略 (Mail Policies)** > **文本资源 (Text Resources)** 页面中，点击要删除的文本资源的“删除”(Delete) 列下的垃圾桶图标。屏幕上将显示一条确认消息。

步骤 2 点击**删除 (Delete)** 删除文本资源。

步骤 3 确认您的更改。

导入文本资源

准备工作

确保要导入的文件在设备的配置目录中。

步骤 1 在**邮件策略 (Mail Policies)** > **文本资源 (Text Resources)** 页面上，点击**导入文本资源 (Import Text Resource)**。

步骤 2 选择要导入的文件。

步骤 3 指定编码。

步骤 4 点击 **Next**。

步骤 5 选择名称，进行编辑，然后选择文本资源类型。

步骤 6 提交并确认更改。

导出文本资源

准备工作

请注意，导出文本资源时，会在设备的配置目录中创建一个文本文件。

步骤 1 在**邮件策略 (Mail Policies)** > **文本资源 (Text Resources)** 页面上，点击**导出文本资源 (Export Text Resource)**。

步骤 2 选择要导出的文本资源。

步骤 3 输入文本资源的文件名。

步骤 4 选择文本文件的编码。

步骤 5 点击**提交 (Submit)** 以在配置目录中创建包含文本资源的文本文件。

基于 HTML 的文本资源概述

可以使用基于 HTML 的邮件和纯文本邮件（例如免责声明）创建一些文本资源。将包含基于 HTML 的邮件和纯文本邮件的文本资源应用于某邮件时，基于 HTML 的文本资源邮件会应用于该邮件的文本/html 部分，纯文本邮件会应用于该邮件的文本/纯文本部分。

当添加或编辑基于 HTML 的文本资源时，GUI 提供富文本编辑功能，您无需手动输入 HTML 代码即可输入富文本。

添加和编辑基于 HTML 的文本资源时，请考虑以下信息：

- 您可以选择基于 HTML 版本自动生成邮件的纯文本版本，也可以独立定义纯文本版本。
- 点击**代码视图 (Code View)** 按钮，可以在富文本编辑器和 HTML 代码之间切换。
- 要在 GUI 中输入富文本编辑器不支持的 HTML 代码，请切换到代码视图并手动键入 HTML 代码。例如，您可能希望执行此操作以使用 **<img src>** HTML 标记插入对外部服务器上的图像文件的引用。

导入和导出基于 HTML 的文本资源

可以从文本文件导出和导入基于 HTML 的文本资源。将基于 HTML 的文本资源导出到文件中时，该文件包含每个版本的文本资源的以下部分：

- `[html_version]`
- `[text_version]`

这些部分的顺序不重要。

例如，导出的文件可能包含以下文本：

```
[html_version]
 <p>Sample <i>message.</i></p>
 [text_version]
 Sample message.
```

导出和导入基于 HTML 的文本资源时，请考虑以下规则和指南：

- 导出其纯文本邮件基于 HTML 版本自动生成的基于 HTML 的文本资源时，导出的文件不包含 `[text_version]` 部分。
- 从文本文件导入时，如果文本资源类型支持 HTML 邮件，则 [html_version] 部分下的所有 HTML 代码在创建的文本资源中都将转化为 HTML 邮件。类似地，`[text_version]` 部分下的所有文本在创建的文本资源中都将转化为纯文本邮件。
- 从包含空的或不存在的 `[html_version]` 部分的文件导入以创建基于 HTML 的文本资源时，设备会使用 `[text_version]` 部分的文本创建 HTML 好纯文本邮件。

使用文本资源

所有类型的文本资源都按照相同的方式创建，即使用“文本资源”页面或 textconfig CLI 命令。创建后，每种类型按照不同的方式使用。免责声明和通知模板与过滤器和侦听程序一起使用，而防病毒通知模板与邮件策略和防病毒设置一起使用。

免责声明模板

对于侦听程序收到的部分或所有邮件，设备可以在文本（标题或页脚）以上或以下添加默认免责声明。可以使用以下方法向设备的邮件添加免责声明：

- 通过侦听程序，使用 GUI 或 `listenerconfig` 命令（请参阅通过侦听程序添加免责声明文本，第 491 页）。
- 使用内容过滤器操作，`Add Disclaimer Text`（请参阅内容过滤器操作，第 242 页）。
- 使用邮件过滤器操作，`add-footer()`（请参阅“使用邮件过滤器实施邮件策略”一章。）。
- 使用防数据丢失配置文件（请参阅数据防泄漏，第 373 页）。
- 为爆发过滤器使用邮件修改来改变尝试对邮件进行网络钓鱼或恶意软件分配的用户（请参阅修改邮件，第 311 页）。为此类通知添加的免责声明在文本上方添加。

例如，可以向从您的企业内发送的每封邮件附加版权声明、促销邮件或免责声明。

使用免责声明文本之前，必须创建免责声明模板。使用 GUI 中的“文本资源”页面（请参阅添加文本资源，第 488 页）或 `textconfig` 命令（请参阅《适用于思科邮件安全设备的 AsyncOS 的 CLI 参考指南》）创建和管理要使用的一组文本字符串。

通过侦听程序添加免责声明文本

创建了免责声明文本资源后，请选择要附加到侦听程序接收的邮件的文本字符串。可以在邮件上方或下方添加免责声明文本。此功能在公共（入站）和私有（出站）侦听程序上均可用。

如果发送包含文本和 HTML 的邮件（Microsoft Outlook 将此类邮件称为“多部分替代”），则设备将会在邮件的两个部分为免责声明打上印记。但是，如果邮件中包含签名内容，则不会对该内容进行修改，因为修改将使签名无效，而是会利用免责声明印记创建一个新的部分，即“Content-Disposition inline attachment.”有关多部分邮件的详细信息，请参阅“使用邮件过滤器实施邮件策略”一章中的“邮件正文与邮件附件”。

通过过滤器添加免责声明

您还可以使用过滤器操作 `add-footer()` 或内容过滤器操作“添加免责声明文本”(Add Disclaimer Text) 向邮件的免责声明附加预定义的特定文本字符串。例如，下列邮件过滤器规则会将名为 `legal.disclaimer` 文本字符串附加到从 LDAP 组“Legal:”中的用户发送的所有邮件。

```
Add-Disclaimer-For-Legal-Team:

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

{

add-footer('legal.disclaimer');

}
```

免责声明和过滤器操作变量

您还可以使用邮件过滤器操作变量（有关详细信息，请参阅“使用邮件过滤器实施邮件策略”一章中的“操作变量”）。

以下变量可用于免责声明模板：

表 *44:* 防病毒通知变量

变量	替换内容
$To	替换为邮件“收件人:”(To:) 信头（不是“信封收件人”[Envelope Recipient]）。
$From	替换为邮件“发件人:”(From:) 信头（不是“信封收件人”[Envelope Recipient]）。
$Subject	替换为原始邮件的主题。
$Date	替换为当前日期，采用 MM/DD/YYYY 格式。
$Time	替换为本地时区中的当前时间。
$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。
$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。
$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<”。
$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<”。
$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“None”。
$filenames	替换为邮件附件文件名的逗号分隔列表。
$filetypes	替换为邮件附件文件类型的逗号分隔列表。
$filesizes	替换为邮件附件文件大小的逗号分隔列表。
$remotehost	替换为向邮件安全设备发送邮件的系统的主机名。
$AllHeaders	替换为邮件信头。
$EnvelopeFrom	替换为邮件的信封发件人（信封来源，<MAIL FROM>）。
$Hostname	替换为邮件安全设备的主机名。
$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。
$enveloperecipients	替换为邮件的所有信封收件人（信封目标，<RCPT TO>）。
$bodysize	替换为邮件的大小（以字节为单位）。

变量	替换内容
$FilterName	返回正在处理的过滤器的名称。
$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）。
$DLPPolicy	替换为违反的邮件 DLP 策略的名称。
$DLPSeverity	替换为违规严重性。可以是“低”(Low)、“中”(Medium)、“高”(High)或“严重”(Critical)。
$DLPRiskFactor	替换为邮件敏感资料的风险系数（得分 0 - 100）。
$threat_category	替换为爆发过滤器威胁的类型，例如网络钓鱼、病毒、诈骗或恶意软件。
$threat_type	替换为爆发过滤器威胁类别的子类别。例如，可以是慈善诈骗、财务网络钓鱼尝试、伪交易等。
$threat_description	替换为爆发过滤器威胁的描述。
$threat_level	替换为邮件的威胁等级（得分 0 - 5）。
$threat_verdict	替换为“是”(Yes)或“否”(No)，具体取决于邮件修改威胁级别阈值。如果邮件的病毒或非病毒威胁级别大于或等于邮件修改威胁级别阈值，则此变量的值设置为“是”(Yes)。

要在免责声明中使用邮件过滤器操作变量，请创建邮件免责声明（通过 GUI 的“文本资源”页面或 **textconfig** 命令）并引用该变量：

通过将页脚添加为内联的、UTF-8 编码的引用可打印附件，add-footer() 操作支持非 ASCII 文本。

免责声明设置标记和多个编码

AsyncOS 包含一个用于修改具有不同字符编码的免责声明印记工作原理的设置。默认情况下，AsyncOS 会尝试将其附加的免责声明放置在邮件的正文内。如果正文部分和免责声明的编码不同，则可以使用在 **localeconfig** 命令内配置的设置配置其行为。要了解此设置，将邮件视为包含多个部分很有用：

收件人：joe@example.com 发件人： mary@example.com 主题：您好！	报头
<blank line>	
您好：	正文部分

此邮件已经过扫描…	第一个附件部分
Example.zip	第二个附件部分

第一个空白行之后的邮件正文可以包含许多 MIME 部分。第二个和以下部分通常成为“附件”，而第一个部分通常称为“正文”或“文本”。

免责声明可以作为附件（如上所述）或作为正文的一部分包括在邮件中。

收件人：joe@example.com 发件人： mary@example.com 主题：您好！	报头
<blank line>	
您好：	正文部分
此邮件已经过扫描…	免责声明现在包括在正文部分中
Example.zip	第一个附件部分

通常情况下，如果邮件正文和免责声明之间存在编码不匹配，则 AsyncOS 会尝试按照与邮件正文相同的编码方式对整个邮件进行编码，以便免责声明将包括在正文（“内联”）中，而不是以独立附件的形式包括在内。换句话说，如果免责声明的编码与正文的编码匹配，或者，如果在免责声明中的文本包含可以内联显示的字符（在正文中），则免责声明将内联包括在内。例如，可以具有仅包含 US-ASCII 字符的 ISO-8859-1 编码免责声明；这样，这些字符就可以正常“内联”显示。

但是，如果免责声明不能与正文结合使用，则可以使用 localeconfig 命令将 AsyncOS 配置为尝试促进或转换正文文本以匹配免责声明的编码，以便免责声明可以包括在邮件的正文中：

```
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: Only try encoding from
message body


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]>

Footers or headings are added in-line with the message body whenever
possible. However, if the footer or heading 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 footer or
heading. If that fails, and if the message body's encoding is USASCII,
the system can try to edit the message body to use the footer's
or heading's encoding. Should the system try to impose the footer's
or headings's encoding on the message body? [N]> y

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

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

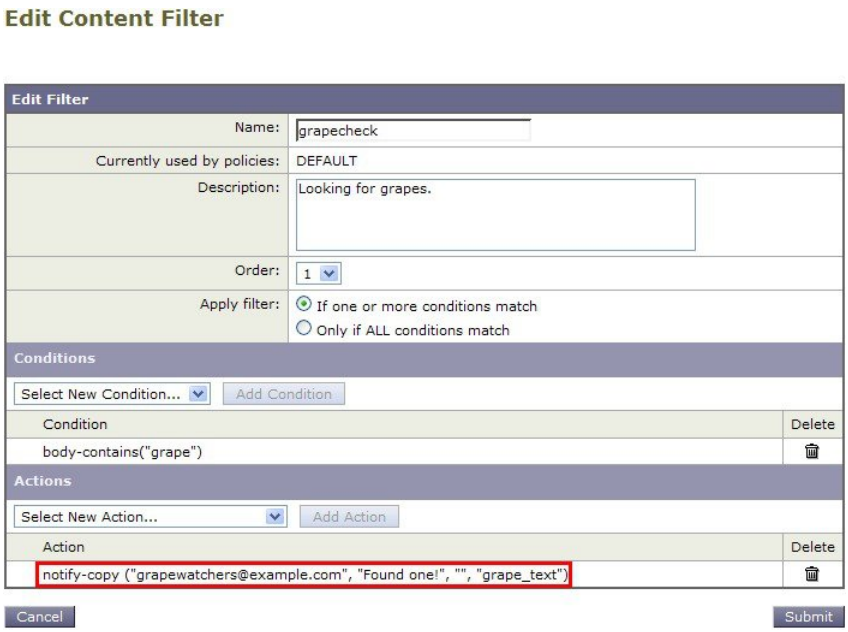
有关 `localeconfig` 命令的详细信息，请参阅“将设备配置为接收邮件”一章。

通知模板

通知模板与 **`notify()`** 和 **`notify-copy()`** 过滤器操作一起使用。通知模板可以包含非 ASCII 文本和操作变量（请参阅“使用邮件过滤器实施邮件策略”一章中的“操作变量”），包括防病毒通知使用的防病毒相关的变量。例如，可以使用 **`$Allheaders`** 操作变量包括原始邮件对的信头。您可以为通知配置“发件人:”(From:) 地址，请参阅为设备生成的邮件配置返回地址，第 775 页。

创建通知模板后，即可在内容和邮件过滤器中引用该模板。下图显示一个内容过滤器，其中 **`notify-copy()`** 过滤器操作设置为将“grape_text”通知发送至“grapewatchers@example.com:”

图 *40*: 内容过滤器中的通知示例



防病毒通知模板

有两种类型的防病毒通知模板：

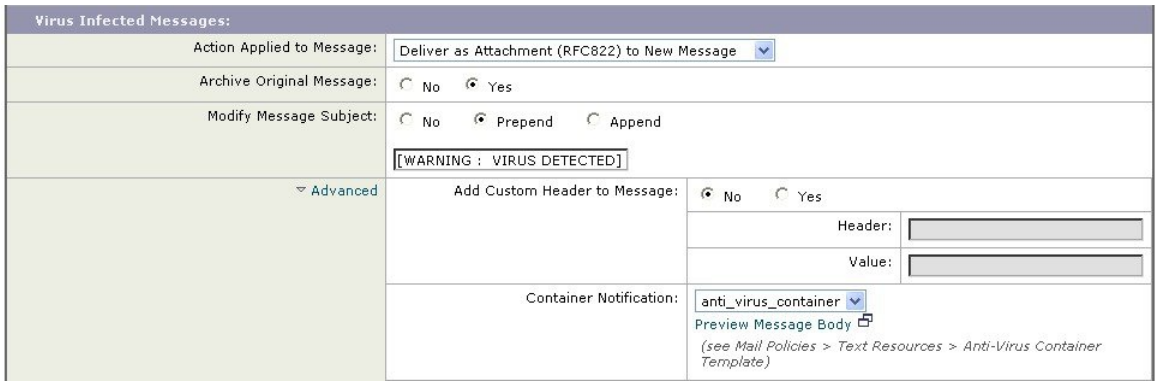
- **防病毒通知模板**。防病毒通知模板在原始邮件未附加到病毒通知时使用。
- **防病毒容器模板**。容器模板在原始邮件作为附件发送时使用。

防病毒通知模板的使用方式与通知模板基本相同，只是防病毒通知模板是与防病毒引擎而非过滤器一起使用。可以在编辑邮件策略时指定要发送的自定义通知。您可以为防病毒通知配置“发件人：”(From:) 地址。有关信息，请参阅为设备生成的邮件配置返回地址，第 775 页。

自定义防病毒通知模板

下图显示指定了自定义防病毒通知的邮件策略。

图 *41:* 邮件策略中的防病毒容器模板通知示例



防病毒通知变量

当创建防病毒通知时，可以使用下表中列出的任意通知变量：

表 *45:* 防病毒通知变量

变量	替换内容
$To	替换为邮件“收件人:”(To:) 信头（不是“信封收件人”[Envelope Recipient]）。
$From	替换为邮件“发件人:”(From:) 信头（不是“信封收件人”[Envelope Recipient]）。
$Subject	替换为原始邮件的主题。
$AV_VIRUSES	替换为在邮件中的任意位置发现的所有病毒的列表： “Unix/Apache.Trojan”，“W32/Bagel-F”
$AV_VIRUS_TABLE	替换为 MIME 部分/附件名称以及各个部分的病毒的表格： “HELLO.SCR”：“W32/Bagel-F” <unnamed part of the message>：“Unix/Apache.Trojan”
$AV_VERDICT	替换为防病毒判定。
$AV_DROPPED_TABLE	替换为删除的附件的表格。每行都包括一个部分或文件名，后跟与该部分关联的病毒列表： “HELLO.SCR”：“W32/Bagel-f”，“W32/Bagel-d” “Love.SCR”：“Netsky-c”，“W32/Bagel-d”
$AV_REPAIRED_VIRUSES	替换为发现和修复的所有病毒的列表。
$AV_REPAIRED_TABLE	替换为发现和修复的所有部分和病毒的表格：“HELLO.SCR”：“W32/Bagel-F”

变量	替换内容
$AV_DROPPED_PARTS	替换为删除的文件名的列表。 “HELLO.SCR”，“CheckThisOut.exe”
$AV_REPAIRED_PARTS	替换为修复的文件名或部分的列表。
$AV_ENCRYPTED_PARTS	替换为加密的文件名或部分的列表。
$AV_INFECTED_PARTS	替换为包含病毒的文件的文件名读好分隔列表。
$AV_UNSCANNABLE_PARTS	替换为不可扫描的文件名或部分的列表。
$Date	替换为当前日期，采用 MM/DD/YYYY 格式。
$Time	替换为本地时区中的当前时间。
$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。
$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。
$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<”。
$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<”。
$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“None”。
$filenames	替换为邮件附件文件名的逗号分隔列表。
$filetypes	替换为邮件附件文件类型的逗号分隔列表。
$filesizes	替换为邮件附件文件大小的逗号分隔列表。
$remotehost	替换为向邮件安全设备发送邮件的系统的主机名。
$AllHeaders	替换为邮件信头。
$EnvelopeFrom	替换为邮件的信封发件人（信封来源，<MAIL FROM>）。
$Hostname	替换为邮件安全设备的主机名。

注释 变量名称不区分大小写。例如，在文本资源中指定“$to”等同于指定“$To”。如果“AV_”变量在原始邮件中为空，则会取代字符串 <None>。

定义文本资源后，使用**邮件策略 (Mail Policies)** > **传入/传出邮件策略 (Incoming/Outgoing Mail Policies)** > **编辑防病毒设置 (Edit Anti-Virus Settings)** 页面或 **`policyconfig -> edit -> antivirus`** 命令指定原始邮件要作为“已修复”(Repaired)、“不可扫描”(Unscannable)、“已加密”(Encrypted) 或“具有病毒特征”(Virus Positive) 邮件的 RFC 822 附件包括在内。有关详细信息，请参阅发送自定义警报通知，第 263 页。

退回和加密失败通知模板

退回和加密失败通知模板的使用方式与通知模板基本相同，只是退回和加密失败通知模板是与退回通知和邮件加密失败通知一起使用。您可以在编辑退回配置文件时指定发送自定义退回通知，在编辑加密配置文件时指定发送自定义邮件加密失败通知。

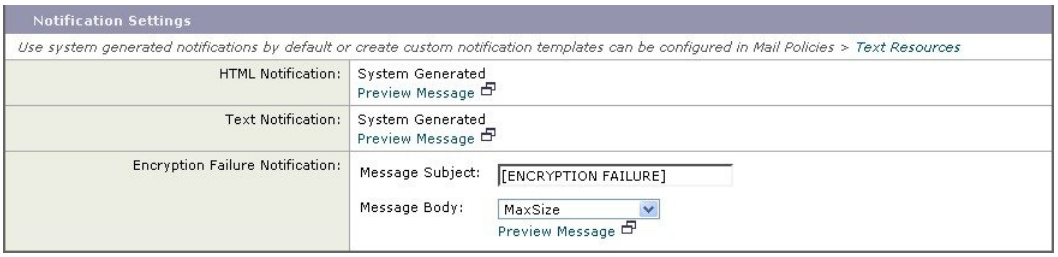
下图显示了在退回配置文件中指定的退回通知模板。

图 *42:* 退回配置文件中的退回通知示例

注释 必须使用 RFC-1891 DSN 才能使用自定义模板。

下图显示了在加密配置文件中指定的加密失败模板。

图 *43:* 加密配置文件中的加密失败通知示例



退回和加密失败通知变量

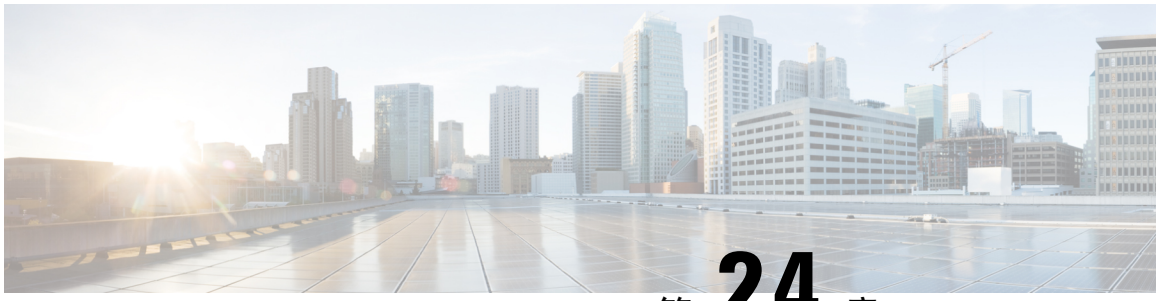
创建退回或加密失败通知时，可以使用下表中列出的任意通知变量：

表 *46:* 退回通知变量

变量	替换内容
$Subject	原始邮件的主题。
$Date	替换为当前日期，采用 MM/DD/YYYY 格式。
$Time	替换为本地时区中的当前时间。
$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。
$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。
$BouncedRecipient	退回的收件人地址
$BounceReason	此通知的原因
$remotehost	替换为向邮件安全设备发送邮件的系统的主机名。

加密通知模板

加密通知模板在您将思科邮件加密配置为级加密出站邮件时使用。该通知会通知收件人他们已收到加密邮件并提供阅读说明。可以指定要随加密邮件一起发送的自定义加密通知。创建加密配置文件时，可以指定 HTML 和文本加密通知。因此，如果要创建自定义配置文件，则应创建文本和 HTML 通知。



第 24 章

使用 SMTP 服务器验证收件人

本章包含以下部分：

SMTP Call-Ahead 收件人验证概述

SMTP Call-Ahead 收件人验证功能会在接受收件人的传入邮件之前查询外部 SMTP 服务器。使用此功能可在无法使用 LDAP 接受或收件人访问表 (RAT) 时验证收件人。例如，假设您为许多邮箱托管邮件，每个邮箱都使用单独的域，并且您的 LDAP 基础设施不允许查询 LDAP 服务器来验证每个收件人。在这种情况下，邮件安全设备可以查询 SMTP 服务器，并在继续进行 SMTP 会话之前验证收件人。

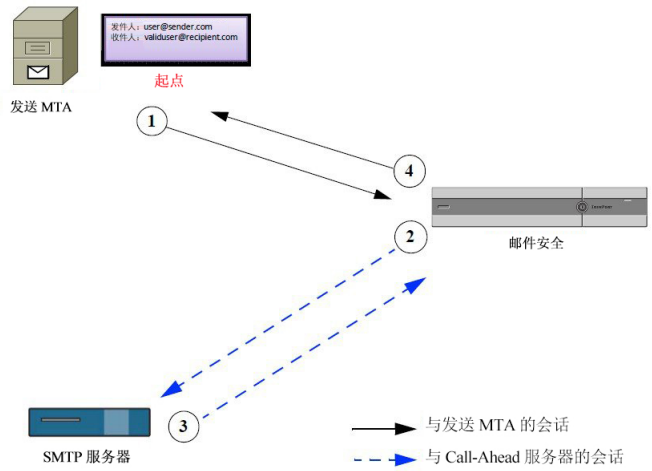
可以使用 SMTP Call-Ahead 收件人验证来减少对无效收件人的邮件的处理。通常，无效收件人的邮件会先通过工作队列，然后才会被删除。相反，在邮件管道的传入/接收部分中可以删除或退回无效的邮件，无需其他处理。

SMTP Call-Ahead 收件人验证工作流程

当配置邮件安全设备进行 SMTP Call-Ahead 收件人验证时，邮件安全设备会暂停与发送 MTA 的 SMTP 会话，同时对 SMTP 服务器进行“Call-Ahead”以验证收件人。当设备查询 SMTP 服务器时，会将 SMTP 服务器的响应返回到邮件安全设备，您可以根据配置的设置，选择接受该邮件或删除具有代码和自定义响应的连接。

下图显示了 SMTP Call-Ahead 验证对话的基本工作流程。

图 *44: SMTP Call Ahead* 服务器对话工作流程



1. 发送 MTA 启动 SMTP 会话。
2. 邮件安全设备将查询发送到SMTP服务器来验证收件人 *validuser@recipient.com* 时，会暂停 SMTP 会话。

注释 如果配置了 SMTP 路由或 LDAP 路由查询，这些路由将用于查询 SMTP 服务器。

3. SMTP 服务器会将查询响应返回到邮件安全设备。
4. 邮件安全设备将恢复 SMTP 会话并向发送 MTA 发送响应，以便基于 SMTP 服务器响应（以及在 SMTP Call-Ahead 配置文件中配置的设置）继续会话或删除连接。

由于邮件管道中的处理顺序，如果特定收件人的邮件被 RAT 拒绝，则不会进行 SMTP Call-Ahead 收件人验证。例如，如果在 RAT 中指定仅接受 *example.com* 的邮件，则在进行 SMTP Call-Ahead 收件人验证之前，会拒绝 *recipient@domain2.com* 的邮件。

注释 如果在 HAT 中配置了目录搜集攻击预防 (DHAP)，请注意 SMTP Call-Ahead 服务器拒绝将计入指定的每小时最大无效收件人中包含的拒绝数。您可能需要调整该数量以考虑其他 SMTP 服务器拒绝。有关 DHAP 的详细信息，请参阅“将网关配置为接收邮件”一章。

如何使用外部 SMTP 服务器验证收件人

	请	更多信息
第 1 步	确定设备如何连接到SMTP服务器并解释服务器的响应。	配置 Call-Ahead 服务器配置文件，第 503 页

	请	更多信息
第 2 步	将公共侦听程序配置为使用SMTP服务器验证收件人	启用侦听程序以通过SMTP服务器验证传入邮件，第 505 页
第 3 步	（可选）更新LDAP路由查询以确定将邮件路由到其他主机时使用的 SMTP 服务器。	配置 LDAP 路由查询设置，第 506 页
第 4 步	（可选）将设备配置为忽略对特定收件人的 Call-Ahead 验证	对特定用户或用户组忽略 SMTP Call-Ahead 验证，第 507 页

配置 Call-Ahead 服务器配置文件

配置 SMTP Call-Ahead 服务器配置文件时，指定设置来确定邮件安全设备如何与 SMTP 服务器建立连接，以及如何解释从 SMTP 服务器发回的响应。

步骤 1 依次点击**网络 (Network)** > **SMTP Call-Ahead**。

步骤 2 点击**添加配置文件 (Add Profile)**。

步骤 3 输入配置文件的设置。有关详细信息，请参阅表 - *SMTP Call-Ahead* 服务器配置文件设置。

步骤 4 为配置文件配置高级设置。有关详细信息，请参阅表 - *SMTP Call-Ahead* 服务器配置文件高级设置。

步骤 5 提交并确认更改。

SMTP Call-Ahead 服务器配置文件设置

在配置 SMTP Call-Ahead 服务器配置文件时，需要配置设置以确定邮件安全设备如何与 SMTP 服务器建立连接。

表 *47: SMTP Call-Ahead* 服务器配置文件设置

设置	说明
配置文件名称	Call-Ahead 服务器配置文件的名称。

设置	说明
Call-Ahead 服务器类型	选择以下一种方法用于连接到 Call-Ahead 服务器： • **使用传送主机**。选择此选项可指定将传送电子邮件地址的主机用于 SMTP Call-Ahead 查询。例如，如果邮件收件人地址为 *recipient@example.com*，则对与 *example.com* 相关的 SMTP 服务器执行 SMTP 查询。如果配置了 SMTP 路由或 LDAP 路由查询，这些路由用于确定要查询的 SMTP 服务器。有关配置 LDAP 路由查询的详细信息，请参阅配置 LDAP 路由查询设置，第 506 页。 • **静态 Call-Ahead 服务器**。使用此选项可创建要查询的 Call-Ahead 服务器的静态列表。如果不希望 Call-Ahead 服务器的名称和位置经常更改，则可使用此选项。使用此选项时，邮件安全设备会以循环方式查询主机，并且从列出的第一个静态 Call-Ahead 服务器开始。 **注释** 请注意，在选择静态 Call-Ahead 服务器类型时，不会将任何 SMTP 路由用于查询。相反，会执行 MX 查找，然后对主机执行 A 查找以获取静态服务器的 Call-Ahead IP 地址。
静态 Call-Ahead 服务器	如果选择使用静态 Call-Ahead 服务器类型，请在此字段中输入主机和端口组合的列表。使用以下语法列出服务器和端口： ironport.com:25 使用逗号分隔多个条目。

下表介绍 SMTP Call-Ahead 服务器配置文件高级设置：

表 *48: SMTP Call-Ahead* 服务器配置文件高级设置

设置	说明
接口	用于启动与 SMTP 服务器的 SMTP 会话的接口。 选择使用“管理接口”(Management interface) 还是“自动”(Auto)。如果选择“自动”(Auto)，则邮件安全设备会尝试自动检测要使用的接口。Cisco IronPort 接口会尝试通过以下方式连接到 SMTP 服务器： • 如果 Call-Ahead 服务器与配置的其中一个接口位于同一子网中，则匹配的接口会发起连接。 • 所有配置的 SMTP 路由均用于路由查询。 • 否则，将使用与默认网关位于同一子网的接口。
MAIL FROM 地址	用于与 SMTP 服务器进行 SMTP 会话的“MAIL FROM:”地址。
验证请求超时	等待从SMTP服务器返回结果的秒数。此超时值用于可能涉及联系多个 Call-Ahead 服务器的单个收件人验证请求。请参阅Call-Ahead 服务器响应，第 505 页。

设置	说明
验证失败操作	收件人验证请求失败（由于超时、服务器故障、网络问题或未知响应）时采取的措施。可以配置希望邮件安全设备如何处理不同的响应。请参阅Call-Ahead 服务器响应，第 505 页。
暂时失败操作	收件人验证请求临时失败（并且远程 SMTP 服务器返回 4xx 响应）时采取的措施。当邮箱已满、邮箱不可用或者该服务不可用时会出现该情况。 请参阅Call-Ahead 服务器响应，第 505 页。
每个会话的最大收件人数	要在单个 SMTP 会话中验证的最大收件人数。 指定介于 1 和 25,000 之间的会话数。
每个服务器的最大连接数	到单个 Call-Ahead SMTP 服务器的最大连接数。 指定介于 1 和 100 之间的连接数。
缓存	SMTP 响应的缓存大小。指定介于 100 和 1,000,000 之间的条目数。
缓存 TTL	条目在缓存中的生存时间值。本字段的默认值为 900 秒。指定介于 60 和 86400 之间的秒数。

Call-Ahead 服务器响应

SMTP 服务器可能返回以下响应：

- **2xx**：如果从 Call-Ahead 服务器收到以 2 开头的 SMTP 代码，则表示已接受收件人。例如，响应 250 表示允许继续进行邮寄操作。
- **4xx**：以 4 开头的 SMTP 代码表示在处理 SMTP 请求时发生临时故障。稍后重试可能回成功处理。例如，响应 451 表示请求的操作已中止或处理时出现本地错误。
- **5xx**：以 5 开头的 SMTP 代码表示处理 SMTP 请求时发生永久故障。例如，响应 550 表示尚未进行请求的操作或邮箱不可用。
- **超时**。如果 Call-Ahead 服务器未返回任何响应，可以配置在出现超时之前可尝试进行重试的时间。
- **连接错误**。如果与 Call-Ahead 服务器的连接发生故障，可以配置是接受还是拒绝收件人地址的连接。
- **自定义响应**。您可以进行配置，在发生验证失败和临时失败时，以自定义 MTP 响应（代码和文本）来拒绝连接。

启用侦听程序以通过 SMTP 服务器验证传入邮件

创建 SMTP Call-Ahead 服务器配置文件后，需要在侦听程序上将其启用以便侦听程序通过 SMTP 服务器验证传入邮件。SMTP Call-Ahead 功能仅在公共侦听程序中可用，因为收件人验证不是专用侦听程序必需的。

步骤 1 依次转到**网络 (Network)** > **侦听程序 (Listeners)**。

步骤 2 点击要在其中启用 SMTP Call-Ahead 功能的侦听程序的名称。

步骤 3 在 **SMTP Call-Ahead 配置文件 (SMTP Call Ahead Profile)** 字段中，选择要启用的 SMTP Call-Ahead 配置文件。

步骤 4 提交并确认更改。

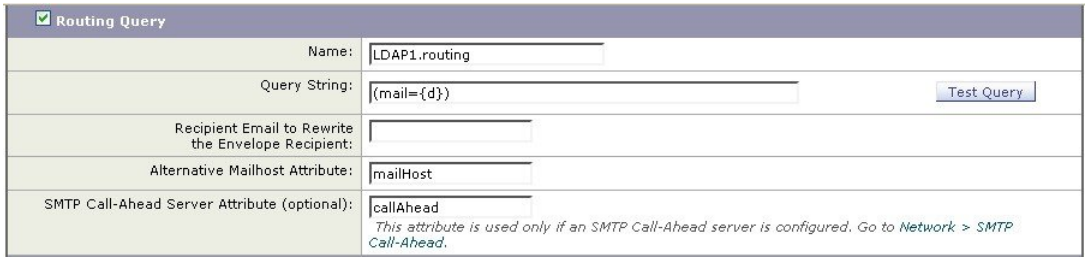
配置 LDAP 路由查询设置

如果使用 LDAP 路由查询将邮件路由到其他邮件主机，则 AsyncOS 使用备用邮件主机属性来确定要查询的 SMTP 服务器。但是，有时您可能不希望出现该情况。例如，在以下方案中，请注意邮件主机属性 (mailHost) 的 SMTP 地址与 SMTP Call-Ahead 服务器属性 (callAhead) 中列出的服务器不同：

```
dn: mail=cisco.com, ou=domains
mail: cisco.com
mailHost: smtp.mydomain.com
policy: ASAV
callAhead: smtp2.mydomain.com,smtp3.mydomain.com:9025
```

在这种情况下，可以使用 **SMTP Call-Ahead** 字段创建路由查询，将 SMTP Call-Ahead 查询定向到 callAhead 属性中列出的服务器。例如，可以创建具有以下属性的路由查询：

图 *45:* 为 *SMTP Call-Ahead* 配置的 *LDAP* 路由查询



在此查询中，{d} 表示收件人地址的域部分，SMTP Call-Ahead 服务器属性会返回 Call-Ahead 服务器的值以及应当用于查询的端口：smtp2.mydomain.com，在端口 9025 上为 smtp3.mydomain.com。

注释 本示例显示的只是配置查询以便使用 LDAP 路由查询将 SMTP Call-Ahead 查询定向到正确的 SMTP 服务器的一种方式。不需要使用在本例中介绍的查询字符串或特定 LDAP 属性。

SMTP Call-Ahead 查询路由

当路由 SMTP Call-Ahead 查询时，AsyncOS 会按以下顺序检查信息：

1. 检查域名。
2. 检查 LDAP 路由查询。

3. 检查 SMTP 路由。
4. 执行 DNS 查找（首先执行 MX 查找，然后执行 A 查找）。

如果没有 LDAP 路由查询或没有为该域配置 SMTP 路由，则上一状态的结果将传递到下一阶段。在任何没有 SMTP 路由的情况下，都会执行 DNS 查找。

如果 LDAP 路由查询用于 SMTP Call-Ahead 查询并且还配置了 SMTP 路由，则路由行为取决于路由查询返回的值。

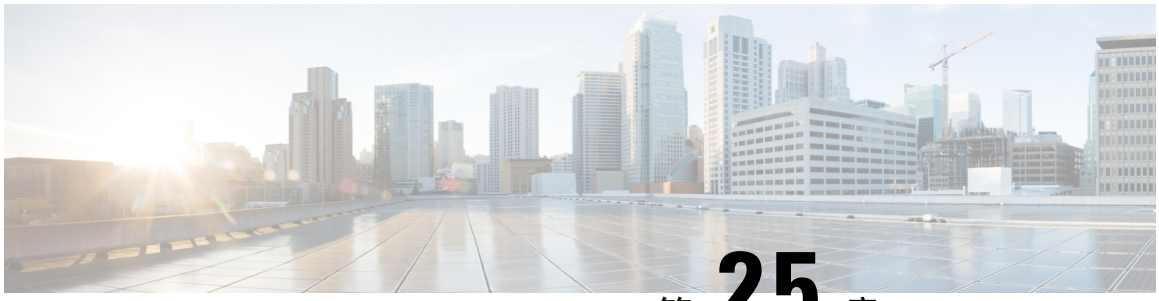
- 如果 LDAP 路由查询返回没有端口的单个主机名，则 SMTP Call-Ahead 查询会应用 SMTP 路由。如果 SMTP 路由仅列出目标主机作为主机名，则会执行 DNS 查找以获取 SMTP 服务器的 IP 地址。
- 如果 LDAP 路由查询返回具有端口的单个主机名，则会使用 SMTP 路由，但是会使用 LDAP 查询返回的端口来替代在 SMTP 路由中指定的任何端口。如果 SMTP 路由仅列出目标主机作为主机名，则会执行 DNS 查找以获取 SMTP 服务器的 IP 地址。
- 如果 LDAP 路由查询返回具有或没有端口的多个主机，则会应用 SMTP 路由，但是会使用 LDAP 路由查询返回的端口来替代 SMTP 路由中提供的端口。如果 SMTP 路由仅列出目标主机作为主机名，则会执行 DNS 查找以获取 SMTP 服务器的 IP 地址。

对特定用户或用户组忽略 SMTP Call-Ahead 验证

您可能希望对侦听程序启用 SMTP Call-Ahead 验证，但是对特定用户或用户组跳过 SMTP Call-Ahead 验证。

您可能希望对在 SMTP Call-Ahead 查询期间不能延迟其邮件的收件人跳过 SMTP Call-Ahead 验证。例如，可以为已知有效并且很可能需要立即关注的客户服务别名添加 RAT 条目。

要通过 GUI 配置忽略 SMTP Call-Ahead 验证，请在添加或编辑 RAT 条目时选择**忽略 SMTP Call-Ahead**。



第 25 章

加密与其他 MTA 的通信

本章包含以下部分：

加密与其他 MTA 的通信概述

企业网关（或邮件传输代理，即MTA）通常以明码形式通过互联网进行通信。换而言之，这些通信并不加密。在有些情况下，恶意代理在不知道发件方或接收方身份信息的情况下即可拦截这种通信。通信可由第三方监控，甚至修改。

传输层安全 (TLS) 是改进版本的安全套接字层 (SSL) 技术。该机制广泛用于对通过互联网的 SMTP 会话加密。AsyncOS 支持 STARTTLS 扩展到 SMTP (Secure SMTP over TLS)，相关介绍请参阅 RFC 3207（取代 RFC 2487）

AsyncOS 中的 TLS 实施通过加密来确保隐私安全。因此，您可以从证书颁发机构服务导入 X.509 证书和私钥，也可以创建自签名证书在设备上使用。AsyncOS 支持对公共和私有侦听程序、接口上的安全 HTTP (HTTPS) 管理访问、LDAP 接口以及所有外发 TLS 连接使用单独的 TLS 证书。

使用 TLS 加密 SMTP 会话的方法

使用 TLS 加密 SMTP 会话的方法

	请	更多信息
第 1 步	从权威证书颁发机构获取 X.509 证书和私钥。	证书的使用，第 510 页

	请	更多信息
第 2 步	在邮件安全设备上安装证书	通过如下方法之一安装证书： • 创建自签名 证书，第 512 页 • 导入证书，第 513 页
第 3 步	对接收邮件和/或传送邮件启用 TLS	• 在侦听程序的 HAT 中启用 TLS，第 515 页 • 传送时启用 TLS 和证书验证，第 517 页
第 4 步	（可选）自定义设备的受信任证书颁发机构列表，使用该列表验证远程域的证书，建立域凭证。	管理证书颁发机构列表，第 519 页
第 5 步	（可选）将邮件安全设备配置为，在无法将邮件传送给需要 TLS 连接的域时发送警报。	必要 TLS 连接失败时发送警报，第 519 页

证书的使用

要使用 TLS，邮件安全设备必须具有用于接收和传送邮件的 X.509 证书和匹配的私钥。您可以对 SMTP 接收和传送使用同一证书，对接口上的 HTTPS 服务、LDAP 接口以及所有到目标域的外发 TLS 连接使用不同的证书，或对这些对象使用同一证书。

使用 certconfig 配置证书后，您可以在 Web 界面的“网络”>“证书”页面上查看完整证书列表，或在 CLI 中使用 print 命令查看此列表。请注意，print 命令不显示中间证书。

⚠

注意 设备随附用于测试 TLS 和 HTTPS 功能的演示证书，但使用本证书启用其中任一服务都是不安全的，因此不推荐用于一般用途。使用默认演示证书启用其中一项服务时，CLI 将打印一条警告消息。

部署自签名证书

无法在邮件安全设备和另一台计算机之间交换自签名证书时（例如，因为该计算机不在您所在的域而无法进行交换），可使用签名证书。公司安全部门可能还有其他需求。

	请	更多信息
第 1 步	如果您在集群中部署，请按照说明执行操作。	证书和集中管理，第 511 页
第 2 步	生成自签名证书和证书签名请求 (CSR)。	创建自签名 证书，第 512 页
第 3 步	将生成的证书发送到权威证书颁发机构进行签署。	关于发送证书签名请求 (CSR) 到证书颁发机构，第 513 页

	请	更多信息
第 4 步	上传签名证书。	上传证书颁发机构签署的证书，第 513 页
第 5 步	确保签署证书的证书颁发机构属于受信任的颁发机构。	管理证书颁发机构列表，第 519 页
第 6 步	如有可能，可以使用中间证书。	中间证书，第 512 页

部署自签名证书

通常，可以针对受公司防火墙保护的设备之间的通信使用自签名证书。公司安全部门可能还有其他需求。

	请	更多信息
第 1 步	如果您在集群中部署，请按照说明执行操作。	证书和集中管理，第 511 页
第 2 步	从邮件安全设备生成自签名证书。	创建自签名 证书，第 512 页
第 3 步	导出自签名证书。	导出证书，第 514 页
第 4 步	将自签名证书导入与邮件安全设备通信的计算机。	参阅另一台计算机的相关文档。
第 5 步	从另一台计算机生成并导出自签名证书。	参阅另一台计算机的相关文档。
第 6 步	将自签名证书从另一台计算机导入邮件安全设备。	导入证书，第 513 页 或 参阅本指南中有关配置与该计算机通信的章节。 例如，要配置与思科 AMP Threat Grid 设备的安全通信，请参阅配置本地文件分析服务器，第 357 页中配置高级设置的说明。

证书和集中管理

证书通常使用本地计算机的主机名作为证书的常用名称。如果邮件安全设备在某个集群内，您需要在计算机级别为每个集群成员导入一张证书，但可以在集群级别安装的通配符证书或使用者备用名称 (SAN) 证书除外。每个集群成员的证书必须使用相同的证书名称，这样当成员的侦听程序与其他计算机通信时，集群才能够引用此证书。

中间证书

除根证书验证之外，AsyncOS还支持使用中间证书验证。中间证书是受信任根证书机构颁发的证书，可用于创建额外的证书，从而有效创建一系列连锁信任。例如，godaddy.com可能颁发了一张证书，而该机构又被某一受信任的根证书颁发机构授予了颁发证书的权限。那么，由 godaddy.com 颁发的证书必须同时经过 godaddy.com 的私钥和受信任的根证书颁发机构的私钥的验证。

创建自签名 证书

在以下情况下，您可能需要在设备上创建自签名证书：

- 使用 TLS 加密与其他 MTA 的 SMTP 会话（入站和出站会话）。
- 在设备上启用 HTTPS 服务，以使用 HTTPS 访问 GUI。
- LDAP 服务器需要客户端证书将自签名证书用作 LDAPS 的客户端证书。
- 实现设备与思科 AMP Threat Grid 设备之间的安全通信。
- 实现设备与思科 AMP Threat Grid 设备之间的安全通信。

要使用 CLI 创建自签名证书，请使用 certconfig 命令。

步骤 1 依次选择**网络 (Network) > 证书 (Certificates)**。

步骤 2 点击 **Add Certificate**。

步骤 3 选择**创建自签名证书 (Create Self-Signed Certificate)**。

步骤 4 为自签名证书输入以下信息：

公共名称	**完全限定域名。**
组织	组织精确的法定名称。
组织单位	组织的部门。
城市(地区)	组织法定所在的城市。
省/市/自治区	组织法定所在的省/市/自治区、县或区域。
国家/地区	组织法定所在国家/地区的双字母 ISO 缩写。
过期前的持续时间	证书到期之前的天数。
私钥大小	为 CSR 生成的私钥的大小。仅支持 2048 位和 1024 位。

步骤 5 点击 **Next**。

步骤 6 为证书输入一个名称。默认情况下，AsyncOS 将分配之前输入的常用名称。

步骤 7 如果您需要提交此证书作为证书签名请求 (CSR)，请点击**下载证书签名请求**将本 CSR 以 PEM 格式保存到本地或网络计算机。

步骤 8 提交并确认更改。

关于发送证书签名请求 (CSR) 到证书颁发机构

证书颁发机构是颁发用于验证身份的数字证书和分配公钥的第三方组织或公司。由于证书由有效的受信任实体颁发，因此多了一层保证。您可以从权威证书颁发机构购买证书和私钥。思科不优先推荐服务。

邮件安全设备可以创建自签名证书并生成证书签名请求 (CSR) 以提交给证书颁发机构来获得公共证书。证书颁发机构则返回私钥签名的可信任公共证书。使用网络界面中的“网络”>“证书”页面或使用 certconfig 命令（CLI 中）可以创建自签名证书、生成 CSR 以及安装受信任公共证书。

如果您是第一次获取或创建证书，请在互联网上搜索“certificate authority services SSL Server Certificates”，并选择最能满足组织需求的服务。按照服务的说明获得证书。

后续操作

请参阅部署自签名证书，第 510 页。

上传证书颁发机构签署的证书

证书颁发机构返回私有密钥签名的受信任公共证书后，请将此证书上传至设备。

您可以将证书用于公共或专用侦听程序、IP 接口的 HTTPS 服务、LDAP 接口或所有指向目标域的外发 TLS 连接。

步骤 1 将证书上传至设备之前，确保您收到的受信任公共证书为 PEM 格式，或其格式可以转换为 PEM 格式。（OpenSSL 随附的转换工具，可以从 http://www.openssl.org 免费获取此软件。）

步骤 2 将签名证书上传到设备：

注释 上传证书颁发机构的证书将覆盖现有的自签名证书。

a) 依次选择**网络 (Network) > 证书 (Certificates)**。
b) 点击您发送到证书颁发机构进行签署的证书的名称。
c) 输入该文件在本地计算机或网盘上的路径。

步骤 3 您还可以上传与自签名证书相关的中间证书。

下一步做什么

相关主题

- 部署自签名证书，第 510 页

导入证书

AsyncOS 支持在设备上使用从其他计算机导入的 PKCS #12 格式证书。

要使用 CLI 导入证书，请运行 **certconfig** 命令。

注释 如果您部署签名证书，请不要使用此程序导入签名证书，而应参阅上传证书颁发机构签署的证书，第 513 页。

步骤 1 依次选择**网络 (Network) > 证书 (Certificates)**。

步骤 2 点击 **Add Certificate**。

步骤 3 选择**导入证书 (Import Certificate)** 选项。

步骤 4 输入指向网络或本地计算机中的证书文件的路径。

步骤 5 输入该文件的密码。

步骤 6 点击**下一步 (Next)** 查看证书的信息。

步骤 7 为证书输入一个名称。

默认情况下 AsyncOS 会分配常用名称。

步骤 8 提交并确认更改。

下一步做什么

- 如果您部署自签名证书，请参阅部署自签名证书，第 511 页。

导出证书

AsyncOS 支持导出证书，并将其保存为 PKCS #12 格式。

注释 如果您部署签名证书，请不要使用此程序生成证书签名请求 (CSR)，而应参阅部署自签名证书，第 510 页。

步骤 1 导航至**网络** > **证书**页面。

步骤 2 点击**导出证书 (Export Certificate)**。

步骤 3 选择要导出的证书。

步骤 4 输入证书的文件名称。

步骤 5 为证书文件输入密码并确认密码。

步骤 6 点击 **Export**。

步骤 7 将文件保存到本地或网络计算机。

步骤 8 您可以导出更多证书，或点击**取消 (Cancel)** 返回“网络”(Network) >“证书”(Certificates) 页面。

下一步做什么

- 如果您部署自签名证书，请参阅部署自签名证书，第 511 页。

在侦听程序的 HAT 中启用 TLS

必须在需要加密的所有侦听程序上启用 TLS。您可能希望在面向互联网的侦听程序（即公共侦听程序）上启用 TLS，但不在内部系统的侦听程序（即专用侦听程序）上启用 TLS。或者，您可能希望对所有侦听程序启用加密。

您可以对侦听程序上的 TLS 指定以下设置。

侦听程序的 TLS 设置

TLS 设置	含义
1.否	不允许对传入连接使用 TLS。到侦听程序的所有连接均不需要加密的 SMTP 会话。这是设备上所配置侦听程序的默认设置。
2.首选	允许对从 MTA 到侦听程序的传入连接使用 TLS。
3.必要	允许对从 MTA 到侦听程序的传入连接使用 TLS，且设备对除 NOOP、EHELO 或 QUIT 之外的其他命令均回应错误消息，直至收到 STARTTLS 命令。此行为由 RFC 3207 指定，后者定义安全 SMTP 在传输层安全的 SMTP 服务扩展。“需要”TLS 意味着发件人不愿意使用 TLS 加密的邮件在发送之前将被设备拒绝，从而阻止邮件以明码形式传送。

默认情况下，私有和公共侦听程序均不启用 TLS 连接。必须在侦听程序的 HAT 中对入站（接收）或出站（发送）邮件启用 TLS。此外，在所有私有和公共侦听程序的默认邮件流策略设置中，tls 均设为“off”。

创建侦听程序时，您可以为各个公共侦听程序分配用于 TLS 连接的特定证书。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，第 66 页。

使用 GUI 为公共或私有侦听程序分配用于 TLS 连接的证书

步骤 1 依次导航至“网络”(Network) >“侦听程序”(Listeners) 页面。

步骤 2 点击要编辑侦听程序的名称。
步骤 3 在“证书”(Certificate) 字段，选择证书。
步骤 4 提交并确认更改。

使用 CLI 为公共或私有侦听程序分配用于 TLS 连接的证书

步骤 1 使用 `listenerconfig -> edit` 命令选择要配置的侦听程序。
步骤 2 使用 `certificate` 命令查看可用的证书。
步骤 3 根据提示选择您要分配给侦听程序的证书。
步骤 4 完成侦听程序配置后，发出 `commit` 命令启用更改。

日志记录

当侦听程序需要 TLS 却无法使用 TLS 时，邮件安全设备会在邮件日志中进行记录。设备会在满足以下条件时更新邮件日志：

- 侦听程序的 TLS 设为“必需”。
- 邮件安全设备已发出“Must issue a STARTTLS command first”命令。
- 连接在未收到任何成功收件人的情况下关闭。

TLS 连接失败原因的相关信息将记录在邮件日志中。

GUI 示例：更改侦听程序 HAT 的 TLS 设置

步骤 1 依次导航到“邮件策略”(Mail Policies) >“邮件流策略”(Mail Flow Policies) 页面。
步骤 2 选择要修改策略的侦听程序，然后点击要编辑策略的名称链接。（您还可以编辑默认策略参数。）
步骤 3 在“TLS”字段的“加密和身份验证”(Encryption and Authentication) 部分，选择侦听程序的 TLS 级别。
步骤 4 提交并确认更改

设备已使用您选择的 TLS 设置更新侦听程序的邮件流策略。

CLI 示例：更改侦听程序 HAT 的 TLS 设置

步骤 1 使用 `listenerconfig -> edit` 命令选择要配置的侦听程序。
步骤 2 使用 `hostaccess -> default` 命令来编辑侦听程序的默认 HAT 设置。

步骤 3 屏幕显示以下问题时，请选择下文其中一个选项来更改 TLS 设置：

```
Do you want to allow encrypted TLS connections?

1. No

2. Preferred

3. Required

[1]> 3

You have chosen to enable TLS. Please use the 'certconfig' command to

ensure that there is a valid certificate configured.
```

步骤 4 请注意，此示例要求您使用 `certconfig` 命令确保存在可用于侦听程序的有效证书。如果您尚未创建任何证书，侦听程序将使用设备上预先安装的演示证书。为便于测试，您可以使用演示证书启用 TLS，但此操作不安全，不建议用于一般用途。使用 `listenerconfig -> edit -> certificate` 命令为侦听程序分配证书。配置 TLS 后，此设置将反映在 CLI 的侦听程序摘要中：

```
Name: Inboundmail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain map: disabled

TLS: Required
```

步骤 5 发出 `commit` 命令启用更改。

传送时启用 TLS 和证书验证

可以使用“目标控制”(Destination Controls) 页面或 `destconfig` 命令，对目标至特定域的邮件传送启用 TLS。

除 TLS 之外，您可以要求对域的服务器证书进行验证。此域验证将基于建立域凭证时使用的数字证书。验证过程涉及到两个验证要求：

- SMTP 会话的颁发者证书链以受信任证书颁发机构 (CA) 颁发的证书结尾
- 证书中列出的常用名称 (CN) 与接收计算机的 DNS 名称或邮件的目标域匹配。

  -或者-

  邮件的目标域与证书使用者备用名称 (subjectAltName) 扩展名中的其中一个 DNS 名称匹配，如 RFC 2459 所述。匹配支持通配符，如 RFC 2818 第 3.1 节所述。

受信任 CA 是颁发用于验证身份的数字证书和分配公钥的第三方组织或公司。由于证书由有效的受信任实体颁发，因此多了一层保证。

您可以将邮件安全设备配置为通过 TLS 连接将邮件发送到域，替代信封加密。有关详细信息，请参阅“思科邮件加密”一章。

您可以为设备指定用于所有外发 TLS 连接的证书。要指定证书，请点击“目标控制”(Destination Controls) 页面上的**编辑全局设置 (Edit Global Settings)**，或在 CLI 中使用 `destconfig -> setup` 命令。证书是全局设置，非按域设置。

使用“目标控制”(Destination Controls) 页面或 `destconfig` 命添加域时，可以为给定域指定 5 个不同的 TLS 设置。除指定与域的交换是否需要使用或首选使用 TLS 编码之外，您还可以指定是否有必要进行域验证。有关这些设置的说明，请参阅下表：

表 *49*: 传送 *TLS* 设置

TLS 设置	含义
默认	使用“目标控制”(Destination Controls) 页面或 `destconfig -> default` 子命令设置的、用于从侦听程序到该域 MTA 的外发连接的默认 TLS 设置。 如果您对问题“Do you wish to apply a specific TLS setting for this domain?”回答“no”，则设置“Default”值。
1.否	不对从接口到该域 MTA 的外发连接协商 TLS。
2.首选	对从邮件安全设备接口到该域 MTA 的外发连接协商 TLS。但是，如果 TLS 协商失败（在收到 220 响应之前），SMTP 事务将以“明码形式”（不加密）继续。不进行任何验证证书是否来自受信任证书颁发机构的尝试。如果在收到 220 响应后出错，SMTP 事务不会恢复为明码形式。
3.必要	对从邮件安全设备接口到该域 MTA 的外发连接协商 TLS。不进行任何验证域证书的尝试。如果协商失败，设备不会通过连接发送电子邮件。如果协商成功，设备将通过加密会话传送电子邮件。
4.首选（验证）	对从邮件安全设备到该域 MTA 的外发连接协商 TLS。设备将尝试验证域证书。 验证可能有三种结果： • 协商 TLS，并验证证书。邮件通过加密会话传送。 • 协商 TLS，但不验证证书。邮件通过加密会话传送。 • 不进行 TLS 连接，因此不验证证书。邮件以纯文本形式传送。

如果友好相邻表中没有针对给定收件人域的特定条目，或者如果存在特定条目但该条目没有特定TLS设置，则设备将选择用户使用“目标控制”页面或 `destconfig -> default` 子命令设置的任何行为（“无”、“首选”、“必需”、“首选(验证)”或“必需(验证)”）。

必要 TLS 连接失败时发送警报

您可以指定，如果向需要 TLS 连接的域发送邮件时 TLS 协商失败，邮件安全设备否发送警报。警报邮件包含失败 TLS 协商的目标域名称。邮件安全设备会向接收系统警报类型的警告严重级别警报的所有收件人发送警报。可以通过 GUI 中的“系统管理”>“警报”页面（或 CLI 中的 alertconfig 命令）管理警报收件人。

启用 TLS 连接警报

步骤 1 依次导航到“邮件策略”(Mail Policies) >“目标控制”(Destination Controls) 页面。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 针对“Send an alert when a required TLS connection fails.”点击**启用 (Enable)** 选项。

此设置为全局设置，而不是按域的设置。有关设备所尝试传送邮件的信息，请参阅“监控”(Monitor) >“邮件跟踪”(Message Tracking) 页面或邮件日志。

步骤 4 提交并确认更改。

下一步做什么

您还可以在命令行界面中运行 destconfig -> setup 命令，通过 CLI 启用 TLS 连接警报来配置此设置。

日志记录

当域需要 TLS 但无法使用 TLS 时，邮件安全设备会在邮件日志实例中进行记录。日志中将提供有关 TLS 连接为何无法使用的信息。满足以下任一条件时，设备将更新邮件日志：

- 远程 MTA 不支持 ESMTP（例如，无法解析来自邮件安全设备的 EHLO 命令）。
- 远程 MTA 支持 ESMTP，但“STARTTLS”不在其告知的 EHLO 响应扩展名列表中。
- 邮件安全设备发出 STARTTLS 命令时，远程 MTA 告知“STARTTLS”扩展名，但回应错误。

管理证书颁发机构列表

在验证某远程域的证书以建立域凭证时，设备使用存储的受信任证书颁发机构。您可以将设备配置为使用以下受信任证书颁发机构：

- **预装列表**。设备具有受信任证书颁发机构的预装列表。此列表称为系统列表。
- **用户定义的列表**。您可以自定义受信任证书颁发机构列表，然后将列表导入设备。

验证远程域的证书时，您可以使用系统列表或自定义列表，也可以同时使用这两个列表。

可以在 GUI 中使用“网络”>“证书”>“编辑证书颁发机构”页面管理列表，或在 CLI 中使用 certconfig > certauthority 命令管理列表。

在“网络”(Network) > “证书”(Certificates) > “编辑证书颁发机构”(Edit Certificate Authorities) 页面，您可以执行以下任务：

- **查看证书颁发机构的系统列表**（预装）。有关详细信息，请参阅查看证书颁发机构预装列表，第 520 页。
- **选择是否使用系统列表**。您可以启用或禁用系统列表。有关详细信息，请参阅禁用系统证书颁发机构列表，第 520 页。
- **选择是否使用自定义证书颁发机构列表**。您可以启用设备使用自定义列表，然后从文本文件中导入列表。有关详细信息，请参阅导入自定义证书颁发机构列表，第 520 页。
- **将证书颁发机构列表导出至文件**。您可以将证书颁发机构系统列表或自定义列表导出至文本文件。有关详细信息，请参阅导出证书颁发机构列表，第 521 页。

查看证书颁发机构预装列表

步骤 1 依次导航至“网络”(Network) > “证书”(Certificates) 页面。

步骤 2 在“证书颁发机构”(Certificate Authorities) 部分，点击**编辑设置 (Edit Settings)**。

步骤 3 点击**查看系统证书颁发机构 (View System Certificate Authorities)**。

禁用系统证书颁发机构列表

预安装的系统证书颁发机构列表无法从设备上删除，但是，您可以启用或禁用此列表。您可能想要禁用此列表，以便只允许设备使用自定义列表验证远程主机的证书。

步骤 1 依次导航至“网络”(Network) > “证书”(Certificates) 页面。

步骤 2 在“证书颁发机构”(Certificate Authorities) 部分，点击**编辑设置 (Edit Settings)**。

步骤 3 对“系统列表”(System List) 点击**禁用 (Disable)** 选项。

步骤 4 提交并确认更改。

导入自定义证书颁发机构列表

您可以创建颁发证书颁发机构自定义列表，并将列表导入设备。此文件必须是PEM格式，且包括您希望设备信任的证书颁发机构的证书。

步骤 1 依次导航至“网络”(Network) > “证书”(Certificates) 页面。

步骤 2 在“证书颁发机构”(Certificate Authorities) 部分，点击**编辑设置 (Edit Settings)**。

步骤 3 对于“自定义列表”(Custom List)，点击**启用 (Enable)**。

步骤 4 输入本地或网络计算机上自定义列表的完整路径。

步骤 5 提交并确认更改。

导出证书颁发机构列表

如果您只想在系统中使用部分受信任证书颁发机构，或者要编辑现有的自定义列表，您可以将列表导出至 .txt 文件，然后通过添加或删除证书颁发机构对列表进行编辑。列表编辑完成后，请将此文件重新导入设备作为自定义列表。

步骤 1 依次导航至“网络”(Network) >“证书”(Certificates) 页面。

步骤 2 在“证书颁发机构”(Certificate Authorities) 部分，点击**编辑设置 (Edit Settings)**。

步骤 3 点击**导出列表 (Export List)**。

AsyncOS 随即显示“导出证书颁发机构列表”(Export Certificate Authority List) 页面。

步骤 4 选择要导出的列表。

步骤 5 输入列表的文件名。

步骤 6 点击 **Export**。

AsyncOS 随即显示一个对话框，询问您是否要打开列表或将列表另存为 .txt 文件。

为 HTTPS 启用证书

您可以在 GUI 中使用**网络 > IP 接口**，或在 CLI 中使用 **`interfaceconfig`** 命令，对 IP 接口上的 HTTPS 服务启用证书。

步骤 1 导航至**网络 > IP 接口**页面。

步骤 2 选择您要启用 HTTPS 服务的接口。

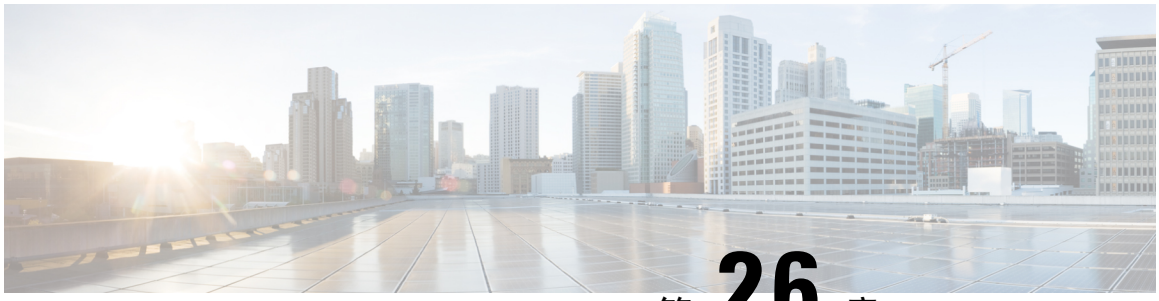
步骤 3 选中“设备管理”下的 **HTTPS** 复选框，并输入端口号。

步骤 4 提交并确认更改。

下一步做什么

注释 在设备上预先安装的演示证书。为便于测试，您可以使用演示证书启用 HTTPS 服务，但此操作不安全，不建议用于一般用途。

您可以在 GUI 使用系统设置向导启用 HTTPS 服务。有关详细信息，请参阅设置和安装，第 17 页。



第 26 章

配置路由和传送功能

本章包含以下部分：

路由本地域的邮件

在配置网关以接收邮件，第 61 页中，您为企业网关配置自定义了服务 SMTP 连接的专用和公共侦听程序。这些侦听程序经过自定义来处理特定连接（通过 HAT 修改）和接收特定域的邮件（通过公共侦听程序的 RAT 修改）。

设备将本地域的邮件路由到通过网络 > SMTP 路由页（或 smtproutes 命令）指定的主机。此功能类似于 sendmail mailertable 功能。

注释 如果已按照“设置和按照”一章中的说明完成了 GUI 中的“系统设置向导”(System Setup Wizard)（或命令行界面中的 systemsetup 命令）并确认了更改，即在设备中为当时输入的每个 RAT 条目定义了第一个 SMTP 路由条目。

SMTP 路由概述

SMTP 路由允许您将特定域的所有邮件重定向到其他邮件交换 (MX) 主机。例如，可以从 example.com 映射到 groupware.example.com。此映射会导致“信封收件人”地址中带有 @example.com 的所有邮件都发送至 groupware.example.com。系统先在 groupware.example.com 中执行“MX”查找，然后在主机中执行“A”查找，就像正常的邮件传送一样。此备用 MX 主机不需要在 DNS MX 记录中列出，甚至无需成为其邮件正在被重定向的域的成员。AsyncOS 操作系统最多支持为设备配置四万 (40,000) 个 SMTP 路由映射。（请参阅SMTP 路由限制，第 525 页）

此功能还允许使用主机“通配”。如果您指定不完整域，例如 .example.com，则以 example.com 结尾的任何域均会与该条目匹配。例如，fred@foo.example.com 和 wilma@bar.example.com 均与该映射匹配。

如果在 SMTP 路由表中没有找到主机，则使用 DNS 执行 MX 查询。不会对照 SMTP 路由表对结果重新进行检查。如果 foo.domain 的 DNS MX 条目为 bar.domain，则发送到 foo.domain 的任何邮件都将传送到主机 bar.domain。如果为 bar.domain 创建了到其他主机的映射，则地址为 foo.domain 的邮件不受影响。

换句话说，递归条目不受影响。如果有一个条目将 a.domain 重定向到 b.domain，然后又有一个条目将 b.domain 的邮件重定向到 a.domain，则不会导致邮件循环。这种情况下，地址为 a.domain 的邮件将传送到 b.domain 指定的 MX 主机；相反，地址为 b.domain 的邮件将传送到 a.domain 指定的 MX 主机。

对于每次邮件传送，都会自上而下读取 SMTP 路由表。选出与映射最匹配的条目例如，如果 SMTP 路由表中的 host1.example.com 和 .example.com 都存在映射，则使用 host1.example.com 的条目，因为该条目更具体，即使它出现在不太具体的 .example.com 条目之后亦无妨。否则，系统将在“信封收件人 (Envelope Recipient)”的域中定期执行 MX 查询。

默认 SMTP 路由

此外，还可以使用特殊关键字 ALL 定义默认 SMTP 路由。如果域与 SMTP 路由列表中先前的映射不匹配，则会默认重定向到 ALL 条目指定的 MX 主机。

打印 SMTP 路由条目时，默认 SMTP 路由将作为 ALL: 列出。无法删除默认 SMTP 路由，只能清除为其输入的任何值。

通过“网络”(Network) > “SMTP 路由”(SMTP Routes) 页面或 smtproutes 命令配置默认 SMTP 路由。

定义 SMTP 路由

使用“网络”(Network) > “SMTP 路由”(SMTP Routes) 页面（或 smtproutes 命令）构建路由。创建新的路由时，首先指定要为其创建永久路由的域或部分域。然后指定目标主机。目标主机可以采用完全限定的主机名或 IP 地址形式输入。IP 地址可以是互联网协议版本 4 (IPv4) 或版本 6 (IPv6)。

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

另外，还可以指定 /dev/null 的专门目标主机，以删除与该条目匹配的邮件。（因此，实际上，为默认路由指定 /dev/null 可确保不会再传送设备收到的邮件。）

接收域可以具有多个目标主机，每个目标主机均分配有优先级便会，就像 MX 记录一样。编号最小的目标主机识别为接收域的主要目标主机。所列出的其他目标主机将作为备用主机。

具有相同优先级的目标将以“轮询”方式使用。该轮询过程基于 SMTP 连接，且不一定基于邮件。此外，如果一个或多个目标主机没有响应，邮件将传送到可访问的主机之一。如果所有配置的目标主机不响应，邮件将排队接收域，并且稍后尝试向目标主机进行传送。（它不使用 MX 记录进行故障转移）。

在使用 CLI 中的 smtproutes 命令构造路由时，可以通过以下方法确定每个目标主机的优先级：在主机或 IP 地址后加上 /pri=，后跟介于 0 和 65535 之间的整数用于分配优先级（0 表示最高优先级）。例如，host1.example.com/pri=0 的优先级高于 host2.example.com/pri=10。使用逗号分隔多个条目。

SMTP 路由限制

最多可以定义 40,000 个路由。根据此限制，ALL 最后一个默认路由将计入路由数量。因此，最多可定义 39,999 个自定义路由和一个使用特殊关键字 ALL 的路由。

SMTP 路由和 DNS

使用特殊关键字 USEDNS 可指示设备执行 MX 查找，确定特定域接下来的跳跃。在需要将子域的邮件路由到特定主机时，此功能非常有用。例如，如果发往 example.com 的邮件被发送到公司的 Exchange 服务器，您可能会看到类似以下 SMTP 路由的信息：

example.com exchange.example.com

但是，对于发往各种子域 (foo.example.com) 的邮件，请添加类似于以下的 SMTP 路由：

.example.com USEDNS

SMTP 路由和警报

从设备发送到通过“系统管理”>“警报”页面（或 alertconfig 命令）指定的地址的警报遵循为这些目标定义的 SMTP 路由。

SMTP 路由、邮件传送和邮件拆分

传入：如果一封邮件有 10 个收件人，并且这些收件人都在同一台 Exchange 服务器中，则 AsyncOS 将打开一个 TCP 连接，只向邮件存储区提供一封邮件，而不是 10 封独立邮件。

传出：工作原理类似，但如果一封邮件将发送到 10 个不同域中的 10 个收件人，则 AsyncOS 会打开 10 个通往 10 个 MTA 的连接，并向其中每个 MTA 传送一封邮件。

分拆：如果一封传入邮件有 10 个收件人，它们分别位于不同的传入策略组（10 个组）中，则即使 10 个收件人都在同一台 Exchange 服务器中，系统也会对邮件进行拆分。因此，10 封不同的邮件将通过单一 TCP 连接进行传送 。

SMTP 路由和出站 SMTP 身份验证

如果已创建出站 SMTP 身份验证配置文件，则可以将其应用于 SMTP 路由。利用此功能，即可在设备部署于网络边缘的邮件中继服务器之后时，对外发邮件进行身份验证。有关出站 SMTP 身份验证的详细信息，请参阅传出 SMTP 身份验证 ，第 618 页。

使用 GUI 管理发送出站邮件的 SMTP 路由

使用“网络”(Network) >“SMTP 路由”(SMTP Routes) 页面管理设备。在表中添加、修改和删除映射。可以导出或导入 SMTP 路由条目。

添加 SMTP 路由

步骤 1 点击“网络”(Network) >“SMTP 路由 (SMTP Routes)”页面中的**添加路由 (Add Route)**。

步骤 2 输入一个接收域。这可以是主机名、域、IPv4 地址或 IPv6 地址。

步骤 3 输入目标主机。这可以是主机名、IPv4 地址或 IPv6 地址。通过点击**添加行 (Add Row)** 并在新行中输入下一个目标主机，可添加多个目标主机。

注释 可以通过向目标主机添加“:<端口号>”来指定端口号： example.com:25。

步骤 4 如果添加多个目标主机，请输入介于 0 和 65535 之间的整数，为主机分配优先级。0 是最高优先级。有关详细信息，请参阅定义 SMTP 路由 ，第 524 页。

步骤 5 提交并确认更改。

导出 SMTP 路由

与主机访问表 (HAT) 和收件人访问表 (RAT) 类似，也可以通过导出和导入文件来修改 SMTP 路由映射。导出 SMTP 路由的步骤：

步骤 1 点击“SMTP 路由 (SMTP Routes)”页面中的**导出 SMTP 路由 (Export SMTP Routes)**。

步骤 2 输入文件名称并点击**提交 (Submit)**。

导入 SMTP 路由

与主机访问表 (HAT) 和收件人访问表 (RAT) 类似，也可以通过导出和导入文件来修改 SMTP 路由映射。导入 SMTP 路由的步骤：

步骤 1 点击“SMTP 路由”(SMTP Routes) 页面中的**导入 SMTP 路由 (Import SMTP Routes)**。

步骤 2 选择包含导出的 SMTP 路由的文件。

步骤 3 点击 **Submit**。系统将向您发出警告，告知导入将替代所有现有的 SMTP 路由。文本文件中的所有 SMTP 路由都会导入。

步骤 4 点击 **Import**。

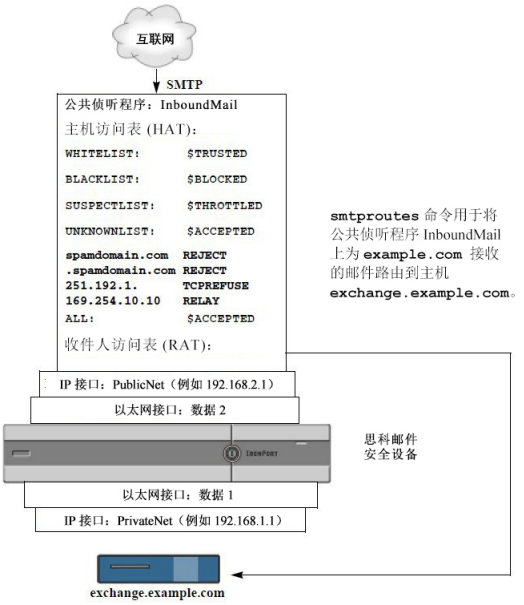
您可以在文件中加入“注释”。以“#”字符开头的行被视为注释，AsyncOS 会忽略注释。例如：

```
# this is a comment, but the next line is not

ALL:
```

下一步做什么

此时，我们的“邮件网关”(Email Gateway) 配置类似于以下：

图 *46:* 为公共侦听程序定义的 ***SMTP*** 路由



重写地址

AsyncOS 提供多种方法来重写邮件管道中的信封发件人和收件人地址。例如，可以使用重写地址将发送的邮件重定向至合作伙伴域或隐藏（屏蔽）内部基础设施。

下表概述了用于重写发件人和收件人邮件地址的各种功能。

表 *50:* 重写地址的方法

原始地址	切换到	特性	作用范围
*@anydomain	user@domain	别名表（请参阅创建别名表，第 528 页）	• 仅信封收件人 • 适用于全局范围 • 将别名映射到邮件地址或其他别名
*@olddomain	*@newdomain	域映射（请参阅域映射功能，第 544 页）	• 仅信封收件人 • 按侦听程序应用
*@olddomain	*@newdomain	伪装（请参阅配置伪装，第 535 页）	• 信封发件人以及“收件人:”、“发件人:”和/或“抄送:”信头 • 按侦听程序应用

创建别名表

别名表提供一种机制，将邮件重定向至一个或多个收件人。可以通过与一些Unix 系统上某个 sendmail 配置的 `/etc/mail/aliases` 功能类似的方式，构建用户名别名和其他别名的映射表。

当侦听程序接受的邮件的信封收件人（也称为目标信封或 `RCPT TO`）与别名表中定义的别名匹配时，该邮件的信封收件人地址会被重写。

注释 在检查 RAT 之后以及过滤邮件之前，侦听程序会检查别名表并修改收件人。请参阅“了解邮件管道”一章。

注释 别名表功能实际上会重写邮件的信封收件人。这与 `smtproutes` 命令不同（请参阅定向退回的邮件，第 550 页），它不重写邮件的信封收件人，而只是将邮件重新路由到指定的域。

从命令行配置别名表

别名表在以下部分中定义：每个部分以域上下文为标题，标题是域列出该部分与，后面是映射列表。

域上下文一个或多个域或部分域的列表，这些域通过逗号分隔并且括在方括号中（“[”和“]”）。按照RFC 1035 第 2.3.1 节“首选名称语法”中的定义，域是包含字母、数字、连字符和句点的字符串。部分域（例如 .example.com）是以句点开头的域。以与部分域匹配的子字符串结尾的所有域都被视为匹配项。例如，域上下文 `.example.com` 将与 `mars.example.com` 和 `venus.example.com` 匹配。在域上下文下方是一个映射列表，该列表由别名后跟一个收件人列表组成。映射的结构如下：

表 *51:* 别名表语法

左侧 (LHS)	分隔符	右侧 (RHS)
要匹配的一个或多个别名的列表	冒号（“:”）	一个或多个收件人地址或别名的列表

左侧的一个别名可以包含以下格式：

`username`	指定要匹配的别名。必须在该表中指定一个前导的“域”属性。缺少此参数将导致出错。
`user@domain`	指定要匹配的确切的邮件地址。

在左侧的单个行中，可以输入多个别名，并用逗号分隔开。

右侧的每个收件人可以是完整的 `user@domain` 邮件地址，也可以是其他别名。

别名文件可包含没有隐含域的“全局”别名（全局应用而不是应用到特定域的别名），和/或其中的别名具有一个或多个隐含域的域上下文。

可以创建别名的“链”（或递归条目），但是它们必须以完整邮件地址结束。

支持 `/dev/null` 的特殊目标丢弃该邮件，以便与 sendmail 配置的上下文兼容。如果邮件通过别名表映射到 `/dev/null`，被丢弃的计数器将增加。（请参阅“通过 CLI 管理和监控”一章。）收件人被接受，但未排队。

导出和导入别名表

要导入别名表，请先参阅FTP、SSH 和 SCP 访问，第 979 页以确保可以访问该设备。

使用 `aliasconfig` 命令的 `export` 子命令保存任何现有别名表。会将一个文件（您指定了其名称）写入侦听程序的 `/configuration` 目录。可以在 CLI 外修改此文件，然后将其重新导入。（如果文件中存在格式错误的条目，则尝试导入文件时会打印错误。）

将别名表文件放置在 `/configuration` 目录中，然后使用 `aliasconfig` 命令的 `import` 子命令上传文件。

使用每行开头的数字符号 (#) 为表中的行添加注释。

请记住在导入别名表文件之后发出 `commit` 命令，以使配置更改生效。

从别名表中删除条目

如果通过命令行界面 (CLI) 从别名表中删除条目，则系统会提示先选择一个域组。选择“ALL (任何域)”(ALL (any domain)) 条目以查看适用于所有域的带编号的别名列表。然后选择要删除的别名数量。

别名表示例

注释 此示例表中的所有条目已注释掉。

```
# sample Alias Table file
# copyright (c) 2001-2005, IronPort Systems, Inc.
#
# Incoming Envelope To addresses are evaluated against each
# entry in this file from top to bottom. The first entry that
# matches will be used, and the Envelope To will be rewritten.
#
# Separate multiple entries with commas.
#
# Global aliases should appear before the first domain
# context. For example:
#
# admin@example.com: administrator@example.com
# postmaster@example.net: administrator@example.net
#
# This alias has no implied domain because it appears
# before a domain context:
#
# someaddr@somewhere.dom: specificperson@here.dom
#
# The following aliases apply to recipients @ironport.com and
# any subdomain within .example.com because the domain context
# is specified.
#
# Email to joe@ironport.com or joe@foo.example.com will
# be delivered to joseph@example.com.
#
# Similarly, email to fred@mx.example.com will be
```

```
# delivered to joseph@example.com
#
# [ironport.com, .example.com]
#
# joe, fred: joseph@example.com
#
# In this example, email to partygoers will be sent to
# three addresses:
#
# partygoers: wilma@example.com, fred@example.com, barney@example.com
#
# In this example, mail to help@example.com will be delivered to
# customercare@otherhost.dom. Note that mail to help@ironport.com will
# NOT be processed by the alias table because the domain context
# overrides the previous domain context.
#
# [example.com]
#
# help: customercare@otherhost.dom
#
# In this example, mail to nobody@example.com is dropped.
#
# nobody@example.com: /dev/null
#
# "Chains" may be created, but they must end in an email address.
# For example, email to "all" will be sent to 9 addresses:
#
# [example.com]
#
# all: sales, marketing, engineering
# sales: joe@example.com, fred@example.com, mary@example.com
# marketing:bob@example.com, advertising
```

```
# engineering:betty@example.com, miles@example.com, chris@example.com

# advertising:richard@example.com, karen@advertising.com
```

aliasconfig 命令示例

在本示例中，使用 aliasconfig 命令来构造别名表。首先，指定了 **example.com** 的域上下文。然后，将构建别名 **customercare**，以便发送到 customercare@example.com 的任何邮件重定向到 bob@example.com、frank@example.com 和 sally@example.com.。接下来，构建 **admin** 的全局别名，以便将发送到 admin 的邮件重定向到 administrator@example.com。最后，打印别名表以进行确认。

请注意，在打印该表时，admin 的全局别名显示在 example.com 的第一个域上下文之前。

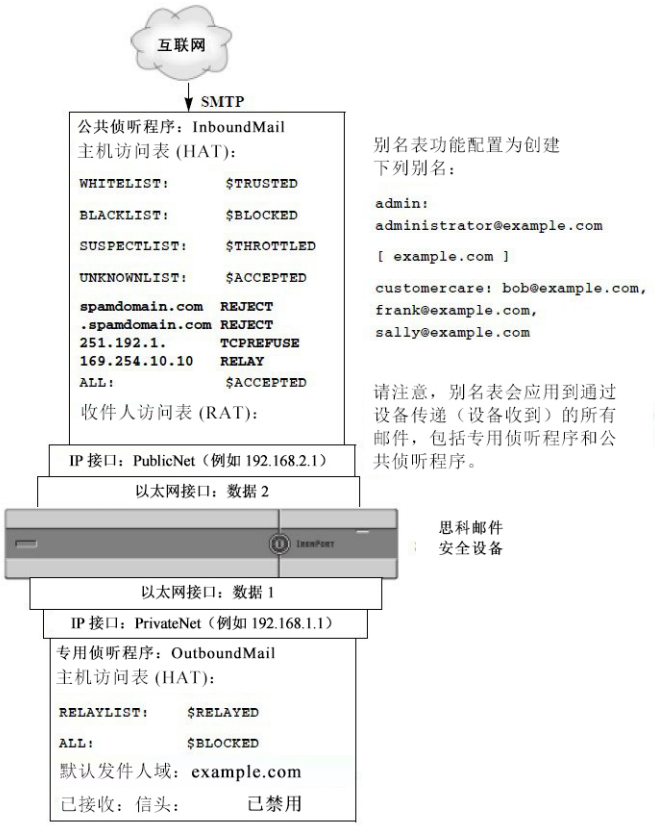
```
mail3.example.com> aliasconfig

No aliases in table.

Choose the operation you want to perform:

- NEW - Create a new entry.

- IMPORT - Import aliases from a file.

[]> new


How do you want your aliases to apply?

1. Globally

2. Add a new domain context


[1]> 2

Enter new domain context.

Separate multiple domains with commas.

Partial domains such as .example.com are allowed.

[]> example.com


Enter the alias(es) to match on.

Separate multiple aliases with commas.

Allowed aliases:

- "user" - This user in this domain context.

- "user@domain" - This email address.

[]> customercare


Enter address(es) for "customercare".

Separate multiple addresses with commas.
```

```
[]> bob@example.com, frank@example.com, sally@example.com

Adding alias customercare: bob@example.com,frank@example.com,sally@example.com
Do you want to add another alias? [N]> n
There are currently 1 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]> new
How do you want your aliases to apply?
1. Globally
2. Add a new domain context
3. example.com
[1]> 1
Enter the alias(es) to match on.
Separate multiple aliases with commas.
Allowed aliases:
- "user@domain" - This email address.
- "user" - This user for any domain
- "@domain" - All users in this domain.
- "@.partialdomain" - All users in this domain, or any of its sub domains.
[]> admin
Enter address(es) for "admin".
Separate multiple addresses with commas.
[]> administrator@example.com
Adding alias admin: administrator@example.com
Do you want to add another alias? [N]> n
```

```
There are currently 2 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]> print
admin: administrator@example.com
[ example.com ]
customercare: bob@example.com, frank@example.com, sally@example.com
There are currently 2 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]>
```

此时，我们的“邮件网关”配置类似于以下：

图 *47:* 为设备定义的别名表



配置伪装

伪装是根据构建的表重写侦听程序处理的邮件中的信封发件人（也称为发件人或 MAIL FROM）以及“收件人：”、“发件人：”和/或“抄送：”信头的一项功能。该功能的一个典型实施示例是允许从一个站点托管多个域的“虚拟域”。另一个典型实施是通过从邮件信头的字符串中“拆离”子域来“隐藏”网络基础设施。伪装功能适用于专用和公共侦听程序。

注释 “伪装”功能在侦听程序上配置，与为整个系统配置的别名表功能不同。

侦听程序会检查伪装表中的匹配项，并在邮件处于工作队列中、紧接着 LDAP 收件人接受查询之后以及在 LDAP 路由查询之前修改收件人。请参阅“了解邮件管道”一章。

“伪装”功能实际上会重写已接收的邮件的信封发件人地址以及“收件人:”(To:)、“发件人:”(From:)和“抄送:”(CC:) 字段。可以通过以下两种方式之一为创建的每个侦听程序指定不同的伪装参数：

- 通过所创建映射的静态表
- 通过 LDAP 查询。

此部分介绍静态表方法。表格式与一些 Unix 系统中 sendmail 配置的 /etc/mail/genericstable 功能是向前兼容的。有关 LDAP 伪装查询的详细信息，请参阅LDAP 查询，第 585 页。

伪装和 altsrchost

通常，伪装功能会重写信封发件人，并且要对邮件执行的任何后续操作都将从伪装地址“触发”。但是，从 CLI 运行 altscrchost 命令时，将从原始地址（而不是经修改的伪装地址）触发 altsrchost 映射。

有关详细信息，请参阅使用虚拟网关™ 技术为所有托管的域配置邮件网关，第 570 页和回顾：邮件管道，第 581 页。

配置静态伪装表

使用 listenerconfig 命令的 edit -> masquerade 子命令配置映射到静态伪装表。或者，可以导入包含映射的文件。请参阅导入伪装表，第 537 页。该子命令会创建和维护将输入地址、用户名和域映射到新地址和域的表。有关 LDAP 伪装查询的详细信息，请参阅LDAP 查询，第 585 页。

将邮件注入系统时，会参照此表，而且如果在信头中找到匹配则会覆盖邮件。

域伪装表按如下方式构建：

表 *52:* 伪装表语法

左侧 (LHS)	分隔符	右侧 (RHS)
要匹配的一个或多个用户名和/或域的列表	空格（空格或制表符）	重写的用户名和/或域

下表列出了伪装表中的有效条目：

左侧 (LHS)	右侧 (RHS)
`username`	`username@domain`
该条目指定要匹配的用户名。与左侧所列用户名匹配的传入邮件将与右侧的地址匹配并重写。右侧必须是一个完整的地址。	
`user@domain`	`username@domain`
该条目指定要匹配的确切地址。与左侧所列完整地址匹配的传入邮件将通过右侧所列地址重写。右侧必须是一个完整的地址。	
`@domain`	`@domain`
此条目指定具有指定域的所有地址。左侧的原始域将替换为右侧的域，并将用户名保留不变。	
`@.partialdomain`	`@domain`
此条目指定具有指定域的所有地址。左侧的原始域将替换为右侧的域，并将用户名保留不变。	

左侧 (LHS)	右侧 (RHS)
所有	@domain
ALL 条目与不包含域名的地址匹配且通过右侧的地址重写它们。右侧必须是以“@”开头的域。此条目始终具有最低优先级，不论在表中的什么位置都是如此。 **注释** 仅可将 ALL 条目用于专用侦听程序。	

- 规则按其在伪装表中的显示顺序进行匹配。
- 默认情况下，信头中“发件人：”(From:)、“收件人：”(To:) 和“抄送：”(CC:) 字段中的地址将在接收时匹配和重写。还可以配置选项来匹配和重写信封发件人。使用 config 命令启用和禁用信封发件人，并确定要重写的信头。
- 您可以使用每行开头的数字符号 (#) 为表中的行添加注释。从 # 开始到行尾的所有内容都将被视为注释并被忽略。
- 伪装表限于 400,000 个条目，无论是通过 new 子命令还是从文件导入它们都是如此。

专用侦听程序的伪装表示例

```
# sample Masquerading file

@.example.com @example.com # Hides local subdomains in the header

sales sales_team@success.com

@techsupport tech_support@biggie.com

user@localdomain user@company.com

ALL @bigsender.com
```

导入伪装表

可以导入传统 sendmail /etc/mail/genericstable 文件。要导入 genericstable 文件，请先参阅FTP、SSH 和 SCP 访问，第 979 页以确保可以访问该设备。

将 genericstable 文件放置在配置目录中，然后使用 masquerade 子命令的 import 子命令上传文件。按以下顺序使用命令：

```
listenerconfig -> edit -> listener_number -> masquerade -> import
```

或者，可以使用 export 子命令下载现有配置。系统会将一个文件（您指定了其名称）写入配置目录。可以在 CLI 外修改此文件，然后再将其导入。

使用 import 子命令时，请确保该文件仅包含有效的条目。如果存在无效条目（例如，一个左侧没有对应的右侧），则在导入文件时 CLI 会报告语法错误。如果在导入过程中存在语法错误，则不会导入整个文件中的任何映射。

请记住在导入 genericstable 文件之后发出 commit 命令，以使侦听程序的配置更改生效。

伪装示例

在本示例中，使用 `listenerconfig` 的 `masquerade` 子命令在 PrivateNet 接口上为名为“OutboundMail”的专用侦听程序构建域名伪装表。

首先，将 LDAP 用于伪装的选项将被拒绝。（有关配置 LDAP 伪装查询的信息，请参阅LDAP 查询，第 585 页。）

然后，**`@.example.com`** 的部分域记法将映射到 **`@example.com`**，以便从 `.example.com` 的子域中的任何计算机发送的邮件都映射到 `example.com`。然后，用户名 **`joe`** 将映射到域 **`joe@example.com`**。接下来，将打印域伪装表以确认两个条目，然后导出得到名为 `masquerade.txt` 的文件。使用 `config` 子命令禁用在“抄送:”(CC:) 字段中禁用重写地址，最后，确认更改。

```
mail3.example.com> listenerconfig

Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> edit

Enter the name or number of the listener you wish to edit.

[]> 2

Name: OutboundMail

Type: Private

Interface: PrivateNet (192.168.1.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 600 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Footer: None

LDAP: Off

Choose the operation you want to perform:
```

```
- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should
be accepted or bounced/dropped.

- LDAPROUTING - Configure an LDAP query to reroute messages.

- LDAPGROUP - Configure an LDAP query to determine whether a sender or

recipient is in a specified group.

- SMTPAUTH - Configure an SMTP authentication.

[]> masquerade

Do you want to use LDAP for masquerading? [N]> n

Domain Masquerading Table

There are currently 0 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[]> new


Enter the source address or domain to masquerade.

Usernames like "joe" are allowed.

Full addresses like "user@example.com" are allowed.
```

```
Full addresses with subdomain wildcards such as "username@.company.com" are allowed.
Domains like @example.com and @.example.com are allowed.
Hosts like @training and @.sales are allowed.
[]> @.example.com
Enter the masqueraded address or domain.
Domains like @example.com are allowed.
Full addresses such as user@example.com are allowed.
[]> @example.com
Entry mapping @.example.com to @example.com created.
Domain Masquerading Table
There are currently 1 entries.
Masqueraded headers: To, From, Cc
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]> new

Enter the source address or domain to masquerade.
Usernames like "joe" are allowed.
Full addresses like "user@example.com" are allowed.
Full addresses with subdomain wildcards such as "username@.company.com" are allowed.
Domains like @example.com and @.example.com are allowed.
Hosts like @training and @.sales are allowed.
[]> joe
Enter the masqueraded address.
Only full addresses such as user@example.com are allowed.
[]> joe@example.com
Entry mapping joe to joe@example.com created.
```

```
Domain Masquerading Table

There are currently 2 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[]> print

@.example.com @example.com

joe joe@example.com

Domain Masquerading Table

There are currently 2 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[]> export

Enter a name for the exported file:

[]> masquerade.txt

Export completed.

Domain Masquerading Table

There are currently 2 entries.
```

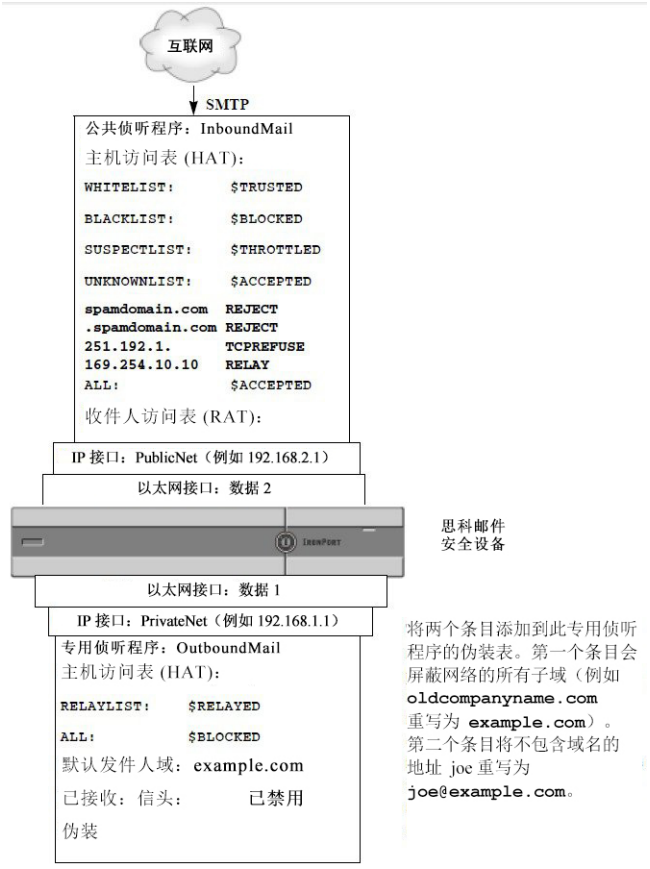
```
Masqueraded headers: To, From, Cc
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.

[]> config
Do you wish to masquerade Envelope Sender?
[N]> y
Do you wish to masquerade From headers?
[Y]> y
Do you wish to masquerade To headers?
[Y]> y
Do you wish to masquerade CC headers?
[Y]> n
Do you wish to masquerade Reply-To headers?
[Y]> n
Domain Masquerading Table
There are currently 2 entries.
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]>
Name: OutboundMail
Type: Private
```

```
Interface: PrivateNet (192.168.1.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 600 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should
be accepted or bounced/dropped.

- LDAPROUTING - Configure an LDAP query to reroute messages.

- LDAPGROUP - Configure an LDAP query to determine whether a sender or
recipient is in a specified group.

- SMTPAUTH - Configure an SMTP authentication.


[]>

Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.
```

```
- DELETE - Remove a listener.

- SETUP - Change global settings.

[]>
```

现在，我们的企业网关配置如下所示：

图 *48:* 为专用侦听程序定义的伪装



域映射功能

可以为侦听程序配置“域映射”。对于配置的每个侦听程序，可以构建一个域映射表，以便为匹配域映射表中某个域的邮件中的每个收件人重写信封收件人。此功能类似于 sendmail“域表”或 Postfix“虚拟表”功能。仅信封收件人受影响；此功能不会重写 To: 信头。

注释 域映射功能的处理在 RAT 之前且在评估默认域之后立即发生。请参阅“了解邮件管道”一章。

域映射功能的一个常见实施是接受多个旧域的传入邮件。例如，如果您的公司收购了另一家公司，您可以在设备上构建一个域映射以接收所获得的域的邮件，并将信封收件人重写到您公司的当前域。

注释 可以配置多达 20,000 个单独的唯一域映射。

表 *53:* 域映射表语法示例

左侧	右侧	备注
`username@example.com`	**username2@example.net**	仅右侧的完整地址
`user@.example.com`	**user2@example.net**	
`@example.com`	**user@example.net** 或 **@example.net**	完整地址或完全限定域名。
`@.example.com`	**user@example.net** 或 **@example.net**	

在以下示例中，使用 `listenerconfig` 命令的 `domainmap` 子命令为公共侦听程序“InboundMail”创建域映射。发往 `oldcompanyname.com` 域及其任何子域的邮件将映射到 `example.com` 域然后将打印映射以供确认。将此示例与在侦听程序的 RAT 中放置两个域的配置进行对比：域映射功能实际上会将 `joe@oldcomapanyname.com` 的信封收件人重写为 `joe@example.com`，而在侦听程序的 RAT 中放置域 `oldcompanyname.com` 仅会为 `joe@oldcompanyname.com` 接受邮件并将其路由路由，不会重写信封收件人。此外，将此示例与别名表功能进行对比。别名表必须解析为明确的地址；它们无法构建为将“*any username*`@domain`”映射到“*the same username*`@newdomain`”。

```
mail3.example.com> listenerconfig

Currently configured listeners:

1. Inboundmail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public

2. Outboundmail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> edit

Enter the name or number of the listener you wish to edit.
```

```
[]> 1

Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- RCPTACCESS - Modify the Recipient Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

[]> domainmap

Domain Map Table

There are currently 0 Domain Mappings.

Domain Mapping is: disabled

Choose the operation you want to perform:

- NEW - Create a new entry.

- IMPORT - Import domain mappings from a file.
```

```
[]> new

Enter the original domain for this entry.
Domains such as "@example.com" are allowed.
Partial hostnames such as "@.example.com" are allowed.
Email addresses such as "test@example.com" and "test@.example.com"
are also allowed.
[]> @.oldcompanyname.com
Enter the new domain for this entry.
The new domain may be a fully qualified
such as "@example.domain.com" or a complete
email address such as "test@example.com"
[]> @example.com
Domain Map Table
There are currently 1 Domain Mappings.
Domain Mapping is: enabled
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display all domain mappings.
- IMPORT - Import domain mappings from a file.
- EXPORT - Export domain mappings to a file.
- CLEAR - Clear all domain mappings.
[]> print
@.oldcompanyname.com --> @example.com
Domain Map Table
There are currently 1 Domain Mappings.
Domain Mapping is: enabled
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
```

```
- PRINT - Display all domain mappings.

- IMPORT - Import domain mappings from a file.

- EXPORT - Export domain mappings to a file.

- CLEAR - Clear all domain mappings.

[]>

Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Enabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- RCPTACCESS - Modify the Recipient Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

[]>
```

导入和导出域映射表

要导入或导出域映射表，请先参阅FTP、SSH 和 SCP 访问，第 979 页以确保可以访问该设备。

创建要映射的域条目的文本文件。用空格（制表符或空格）分隔各个条目。使用每行开头的数字符号 (#) 为表中的行添加注释。

将文件放置在配置目录中，然后使用 domain 子命令的 `import` 子命令上传文件。按以下顺序使用命令：

```
listenerconfig ->  edit ->  inejctor_number -> domainmap -> import
```

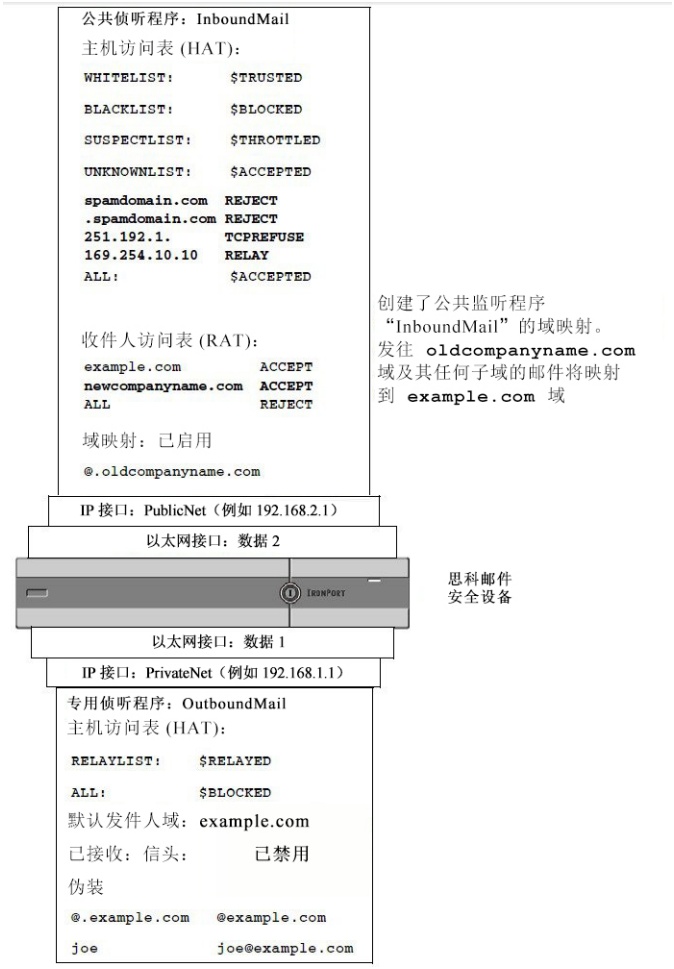
或者，可以使用 `export` 子命令下载现有配置。系统会将一个文件（您指定了其名称）写入配置目录。可以在 CLI 外修改此文件，然后再将其导入。

使用 `import` 子命令时，请确保该文件仅包含有效的条目。如果存在无效条目（例如，一个左侧没有对应的右侧），则在导入文件时 CLI 会报告语法错误。如果在导入过程中存在语法错误，则不会导入整个文件中的任何映射。

请记住在导入域映射表文件之后发出 `commit` 命令，以使侦听程序的配置更改生效。

现在，我们的企业网关配置如下所示：

图 *49:* 为公共侦听程序定义的域映射



定向退回的邮件

退回的邮件是任何邮件传送都不可避免的部分。设备可以通过多种高度可配置的方式处理退回的邮件。

请注意，本部分介绍了如何控制设备生成外发退回的方式（根据传入邮件）。要控制设备如何控制传入退回（基于外发邮件），请使用退回验证（请参阅退回验证，第 558 页）。

处理无法传送的邮件

AsyncOS 操作系统将无法传送的邮件（或“退回邮件”）划分到以下类别中：

“会话”退回：
远程域在初始 **SMTP** 会话期间退回邮件。

软退回	暂时无法传送的邮件。例如，用户的邮箱可能已满。可以稍后再尝试发送这些邮件。（例如，SMTP 4XX 错误代码。）
硬退回	永远无法传送的邮件。例如，该域的用户不再存在。将不会重试发送这些邮件。（例如，SMTP 5XX 错误代码。）
“延迟”（或“非会话”）退回： **远程域接受要传送的邮件，但是稍后将其退回。**	
软退回	暂时无法传送的邮件。例如，用户的邮箱可能已满。可以稍后再尝试发送这些邮件。（例如，SMTP 4XX 错误代码。）
硬退回	永远无法传送的邮件。例如，该域的用户不再存在。将不会重试发送这些邮件。（例如，SMTP 5XX 错误代码。）

使用 GUI 中“网络”(Network) 菜单上的“退回配置文件”(Bounce Profiles) 页面（或 `bounceconfig` 命令）配置 AsyncOS 如何处理所创建的每个侦听程序的硬和软会话退回。创建退回配置文件，然后通过网络 > 侦听程序页面（或 `listenerconfig` 命令）将配置文件应用到每个侦听程序。还可以使用邮件过滤器，将退回配置文件分配给特定邮件。（有关详细信息，请参阅使用邮件过滤器实施邮件策略，第 117 页。）

有关软退回和硬退回的说明

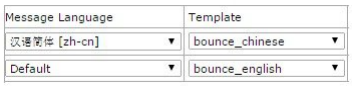
- 对于会话软退回，软退回事件定义定义为收件人传送暂时失败事件。单个收件人可能导致多个软退信事件。可以使用“退回配置文件”页面或 bounceconfig 命令配置每个软退回事件的参数。（请参阅退回配置文件参数，第 551 页。）
- 默认情况下，系统会生成退回邮件并将其发送给每个硬退回收件人的原始发件人。（该邮件会发送到在邮件信封的信封发件人地址中定义的地址。“信封发件人”(Envelope From) 通常也称作“信封发件人”(Envelope Sender)。）可以禁用此功能，并改为根据日志文件了解有关硬退回的信息。（请参阅“日志记录”一章。）
- 在队列中达到最长时间或达到最大重试次数（只要发生任一种情况）后，软退回将变成硬退回。

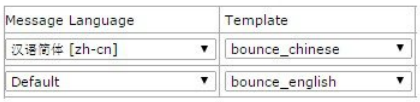
退回配置文件参数

当配置退回配置文件时，下列参数将控制如何根据邮件处理会话退回：

表 *54:* 退回配置文件参数

最大重试次数 (Maximum number of retries)	系统在将软退回邮件作为硬退回邮件处理之前，应尝试重新连接到收件人主机以重新传送软退回邮件的次数。默认值为 100 次重试。
在队列中的最大秒数 (Maximum number of seconds in queue)	系统在将软退回邮件作为硬退回邮件处理之前，应尝试连接到收件人主机以重新传送软退回邮件的时间。默认值为 259,200 秒（72 小时）。

在重试发送邮件前等待的初始秒数 (Initial number of seconds to wait before retrying a message)	在第一次尝试重新传送软退回邮件之前，系统应等待的时间。默认值为60秒。将初始重试时间设置为较高的值可降低软退回尝试的频率。相反，要增加频率，可减小该值。
在重试发送邮件前等待的最大秒数 (Maximum number of seconds to wait before retrying a message)	在尝试重新传送软退回邮件之前，系统应等待的最长时间。默认值为 3600 秒（1 小时）。这不是每个后续尝试之间的时间间隔；相反，它是用于控制重试次数的另一个参数。初始重试时间间隔被限制为不能超过最大重试时间间隔。如果计算出的重试时间间隔超过最大重试时间间隔，则改为使用最大重试时间间隔。
发送硬退回邮件	指定是否发送退回邮件以进行硬退回。如果启用此选项，则可以选择退回邮件的格式。默认情况下，退回邮件使用 DSN 格式 (RFC 1894)。 您还可以根据原始邮件（主题和正文）的语言发送自定义的退回邮件。例如，您可能希望对中文邮件以中文发送退回邮件，而对其他语言的所有邮件以英文发送退回邮件。 在**通知模板**下，点击**添加行**，然后选择邮件语言以及要使用的模板。 **注释** 请确保不要删除默认条目（**邮件语言** 设置为**默认**）。您可以更改默认条目的退回通知模板。 在下列情况下，邮件语言被视为默认值： • 如果邮件语言不同于在其他通知模板条目中所选的语言。 • 如果思科邮件安全设备不支持该邮件语言。 • 如果设备无法检测邮件语言。 • 如果邮件内容（主题和正文）少于 50 字节。 在配置上述示例（对中文邮件以中文发送退回邮件，而对其他语言的所有邮件以英文发送退回邮件）时，通知模板表应如下所示：  此外，还可以选择是否解析退回响应中的DSN状态字段。如果选择“是”，则设备会在退回响应中搜索DSN状态代码(RFC 3436)，并在传送状态通知的“状态”字段中使用此代码。

发送延迟警告邮件	指定是否发送延迟传送的警告邮件。如果启用此选项，您可以根据原始邮件（主题和正文）的语言配置自定义延迟警告邮件。例如，您可能希望对中文邮件以中文发送延迟警告邮件，而对其他语言的所有邮件以英文发送延迟警告邮件。 在**通知模板**下，点击**添加行**，然后选择邮件语言以及要使用的模板。 **注释** 请确保不要删除默认条目（**邮件语言** 设置为**默认**）。您可以更改默认条目的退回通知模板。 在下列情况下，邮件语言被视为默认值： • 如果邮件语言不同于在其他通知模板条目中所选的语言。 • 如果思科邮件安全设备不支持该邮件语言。 • 如果设备无法检测邮件语言。 • 如果邮件内容（主题和正文）少于 50 字节。 在配置上述示例（对中文邮件以中文发送延迟警告邮件，而对其他语言的所有邮件以英文发送延迟警告邮件）时，通知模板表应如下所示：  您还可以指定邮件之间的最小时间间隔以及重试发送的最大次数。
指定退回的收件人 (Specify Recipient for Bounces)	可以将邮件退回到备用地址而不是默认的信封发件人地址。
对退回邮件和延迟邮件使用 DomainKeys 签名 (Use DomainKeys signing for bounce and delay messages)	可以选择将 DomainKeys 配置文件用于签名退回和延迟邮件。有关 DomainKeys 的信息，请参阅DomainKey 和 DKIM 身份验证，第 445 页。
全局设置	
通过“退回配置文件”(Bounce Profiles) 页面上的编辑全局设置 (Edit Global Settings) 链接，或通过 CLI 中的 `bounceconfig` 命令编辑默认退回配置文件来配置这些设置。	
在重试连接无法访问的主机前等待的初始秒数 (Initial number of seconds to wait before retrying an unreachable host)	系统在重试连接无法访问的主机之前， 应等待的时间。默认值为 60 秒。

两次重试某个无法访问的主机之间允许的最大间隔 (Max interval allowed between retries to an unreachable host)	在重试连接无法访问的主机之前，系统应等待的最长时间。默认值为 3600 秒（1 小时）。当初始传送由于主机关闭而失败时，将以最小重试秒数值开始，而对于后续每次重试连接到关闭的主机，将增加持续时间，直至达到此最大秒数值。

硬退回和状态命令

启用硬退回邮件生成功能后，status 和 status detail 命令中的以下计数器将在设备每次为传送生成硬退回邮件时增加计数：

Counters:	Reset	Uptime	Lifetime
Receiving			
Messages Received	0	0	0
Recipients Received	0	0	0
Gen. Bounce Recipients	0	0	0

有关详细信息，请参阅“通过 CLI 监控和管理”一章。当禁用硬退回邮件生成功能时，如果收件人硬退回，则这些计数器都不会增加计数。

注释 邮件信封的信封发件人地址与邮件信头中的“发件人:”(From:) 不同。AsyncOS 可以配置为将硬退回硬件发送到与信封发件人地址不同的邮件地址。

会话退回和 SMTP 路由邮件过滤器操作

SMTP 路由映射和邮件过滤器操作不适用于路由因会话退回而由设备生成的 SMTP 退回邮件。当设备收到会话退回邮件时，会生成一个回到原始邮件信封发件人的 SMTP 退回邮件。在这种情况下，设备实际上是在生成邮件，因此用于注入邮件以进行中继的任何 SMTP 路由都不适用。

退回配置文件示例

考虑以下使用不同退回配置文件参数的两个示例：

表 *55:* 示例 *1*：退回配置文件参数

参数	值
最大重试次数 (Max number of retries)	2

参数	值
队列中的最大秒数 (Max number of seconds in queue)	259,200 秒（72 小时）
在重试发送邮件前的初始秒数 (Initial number of seconds before retrying)	60 秒
在重试之前等待的最大秒数 (Max number of seconds to wait before retrying)	60 秒

在示例 1 中，第一次收件人传送尝试在 t=0 处执行，即在邮件注入设备后立即进行。通过将默认初始重试时间设置为 60 秒，将在 t=60（即大约一分钟后）时立即进行第一次重试尝试。计算了重试时间间隔，并且确定使用 60 秒的最大重试时间间隔。因此，第二次重试尝试在大约 t=120 时执行。紧接此重试尝试之后，系统会为该收件人生成硬退回邮件，因为最大重试次数是 2。

表 *56:* 示例 *2*：退回配置文件参数

参数	值
最大重试次数 (Max number of retries)	100
队列中的最大秒数 (Max number of seconds in queue)	100 秒
在重试发送邮件前的初始秒数 (Initial number of seconds before retrying)	60 秒
在重试之前等待的最大秒数 (Max number of seconds to wait before retrying)	120 秒

在示例 2 中，第一次传送尝试在 t=0 处执行，第一次重试在 t=60 时执行。系统在下一次传送尝试之前（安排发生在 t=120 时）立即硬退回邮件，因为在队列中超出了 100 秒的最长时间。

传送状态通知格式

默认情况下，系统生成的退回邮件为硬退回和软退回使用传送状态通知 (DSN) 格式。DSN 是 RFC 1894 定义的格式（请参阅 http://www.faqs.org/rfcs/rfc1894.html），该格式“定义了可由邮件传输代理 (MTA) 使用的 MIME 内容类型，或用于报告尝试将邮件传送给一个或多个收件人的结果的电子邮件网关”。默认情况下，传送状态通知包括有关传送状态的说明和原始邮件（如果邮件大小小于 10K）。如果邮件大小大于 10K，则传送状态通知仅包括邮件信头。如果邮件信头大小超过 10K，则传送状态通知会截断邮件信头。如果要在 DNS 中年包含大小超过 10K 的邮件（或邮件信头），可以在 bounceconfig 命令中使用 max_bounce_copy 参数（此参数仅在 CLI 中可用）。

延迟警告邮件

系统生成的队列中时间邮件（延迟通知邮件）也使用DSN格式。通过使用“网络”菜单上的“退回配置文件”页面（或 bounceconfig 命令）编辑现有退回配置文件或创建新的退回配置文件，并更改以下项的默认值来更改默认参数：

- 发送延迟警告邮件之间的最短时间间隔。
- 发送给每个收件人的延迟警告邮件的最大数量。

延迟警告邮件和硬退回

请注意，如果为“在队列中的最长时间”设置和“发送延迟警告邮件”的最短时间间隔设置都设置了很短的持续时间，则可能同时为同一邮件接收延迟警告和硬退回。如果选择启用发送延迟警告邮件的功能，则思科系统公司建议使用这些设置的默认值作为最小值。

此外，在处理过程中，设备产生的延迟警告邮件和退回邮件可能延迟多达 15 分钟。

创建新的退回配置文件

在以下示例中，使用“退回配置文件”页创建了名为 bouncepr1 的退回配置文件。在此配置文件，所有硬退回邮件均发送到备用地址 bounce-mailbox@example.com。已启用延迟警告邮件。将为每个收件人发送一封警告邮件，而且接受警告邮件之间的 4 小时（14400 秒）默认值。

编辑默认退回配置文件

可以通过在点击其在“退回配置文件”(Bounce Profiles) 列表中的名称来编辑任何退回配置文件。还可以编辑默认退回配置文件。在本示例中，会编辑默认配置文件以将 `maximum number of seconds to wait before retrying unreachable hosts` 从 3600（一个小时）增大到 10800（三个小时）：

Minimalist 退回配置文件示例

在以下示例中，创建了名为 minimalist 的退回配置文件。在此配置文件中，当邮件退回时不会重试发送邮件（最大重试次数为零），而且指定了重试之前的最长等待时间。已禁用硬退回邮件，而且不会发送软退回警告。

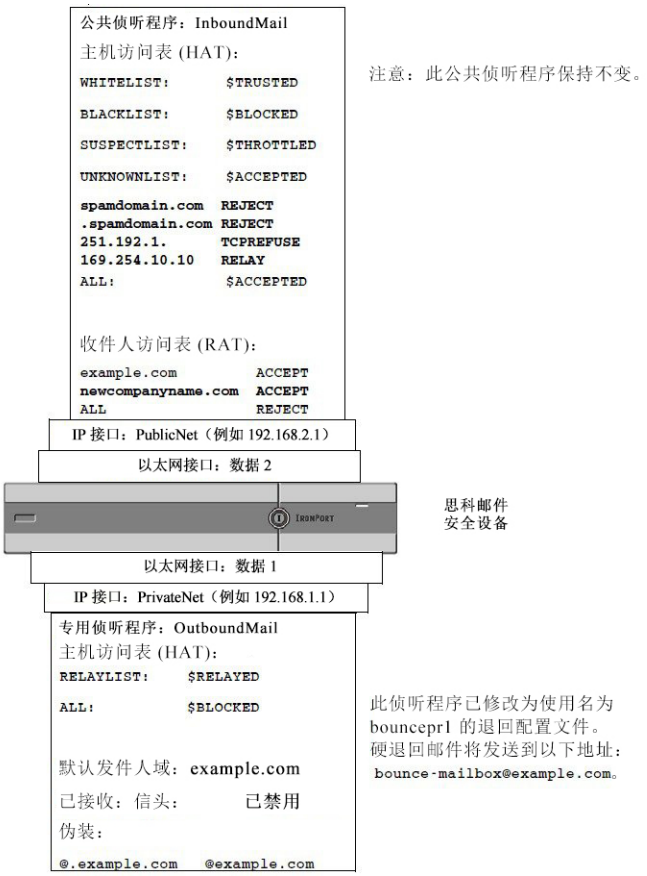
将退回配置文件应用到侦听程序

创建退回配置文件后，可以使用**网络 > 侦听程序**页面或 **`listenerconfig`** 命令将该配置文件应用到侦听程序。

在以下示例中，bouncepr1 配置文件将应用到 OutgoingMail 侦听程序。

此时，我们的“邮件网关”(Email Gateway) 配置类似于以下：

图 *50:* 将退回配置文件应用到专用侦听程序



使用目标控制来控制邮件传送

未受控制的大量邮件传送还会使收件人域不堪重负。AsyncOS 通过定义设备将打开的连接数量或设备将向每个目标域发送的邮件数量，使您可以完全控制邮件传送。

使用“目标控制”功能（GUI 中的“邮件策略”>“目标控制”或 CLI 中的 destconfig 命令），可以控制：

速率限制

- 并发连接数 (Concurrent Connections)：设备将尝试打开的到远程主机的同时连接数。
- 每个连接最大邮件数 (Maximum Messages Per Connection)：设备在启动新的连接之前，将发送到目标域的邮件数。
- 收件人 (Recipients)：设备在指定时间段内将向指定的远程主机发送的收件人数。
- 限制 (Limits)：如何应用按目标或 MGA 主机名指定的限制。

TLS

- 是否接受、允许或需要与远程主机的 TLS 连接（请参阅控制 TLS，第 560 页）。
- 将邮件传送到需要 TLS 连接的远程主机时，如果 TLS 协商失败，是否发送警报。此设置为全局设置，而不是按域的设置。
- 分配 TLS 证书以用于与远程主机的所有出站 TLS 连接。

退回验证

- 是否通过退回验证执行地址标记（请参阅退回验证，第 565 页）。

退回配置文件

- 设备将哪个退回配置文件用于指定的远程主机（默认退回配置文件通过“网络”(Network)>“退回配置文件”(Bounce Profiles) 页面设置）。

还可以控制未指定的域的默认设置。

确定使用哪个接口传送邮件

除非通过 `deliveryconfig` 命令或通过邮件过滤器 (`alt-src-host`) 指定输出接口，或通过使用虚拟网关，否则根据 AsyncOS 路由表来选择输出接口。基本上，选择“自动”(auto) 就表示由 AsyncOS 来决定。

更详细地说：本地地址通过将接口网掩码应用到接口 IP 地址来识别。这两个地址都通过“网络”(Network)>“接口”(Interfaces) 页面或 `interfaceconfig` 命令（或在系统设置期间）进行设置。如果地址空间重叠，则使用更具体的网络掩码。如果目标地址是本地地址，则通过适当的本地接口发送数据包。

如果目标地址不是本地地址，则将数据包发送到默认路由器（通过“网络”(Network) >“路由”(Routing) 页面或使用 `setgateway` 命令设置）。默认路由器的 IP 地址为本地地址。输出接口通过用于为本地地址选择输出接口的规则来决定。例如，AsyncOS 会选择包括默认路由器的 IP 地址的最具体 IP 地址和网络掩码。

路由表通过“网络”(Network) >“路由”(Routing) 页面（或通过 `routeconfig` 命令）配置。路由表中匹配的条目优先于默认路由。更具体的路由优先于较笼统的路由。

默认传送限制

每个出站目标域都有自己的出站队列。因此，每个域都有在目标控制表中指定的一组单独的并发限制。此外，未在目标控制表中明确列出的每个唯一域都使用在该表中设置的另一组“默认”限制。

使用目标控制

使用 GUI 中的“邮件策略”>“目标控制”页面或 CLI 中的 destconfig 命令创建、编辑和删除目标控制条目。

控制互联网协议地址的版本

可以配置将哪一版本的互联网协议地址用于连接到某个域。邮件安全设备支持互联网协议版本 4 (IPv4) 和版本 6 (IPv6)。可以在设备上配置一个侦听程序，以使用一个或两个版本的协议。

如果为 IPv4 或 IPv6 指定了“必需”(Required) 设置，设备将使用指定版本的地址协商与该域的连接。如果该域不使用该 IP 地址版本，则无法发送邮件。如果为 IPv4 或 IPv6 指定了“首选”(Preferred) 设置，设备将首先尝试使用指定版本的地址协商与该域的连接，如果通过第一个版本的地址无法访问，则回退到另一个版本的地址。

控制域的连接、邮件和收件人数量

您可能希望限制设备如何传送邮件，以避免来自设备的邮件使远程主机或您自己的内部群件服务器负载过重。

对于每个域，可以分配最大连接数、最大出站邮件数和最大收件人数，使系统在指定时间段内不超过这些数量。这个“友好相邻”表通过“目标控制”功能（**邮件策略 > 目标控制**或 `destconfig` 命令 - 之前的 `setgoodtable` 命令）定义。可以使用以下语法指定域名：

```
domain.com
```

或

```
.domain.com
```

此语法使 AsyncOS 可以为子域（如 sample.server.domain.com）指定目标控制，而且无分别需输入每个完整的子域地址。

对于连接、邮件和收件人，设置所定义的限制是为每个虚拟网关地址还是为整个系统强制实施。（虚拟网关地址限制控制每个 IP 接口的并发连接数。系统级的限制控制设备允许的总连接数。）

您还可以设置是否为整个域强制执行定义的限制。

注释 当前系统默认值是每个域 500 个连接，每个连接 50 封邮件。

这些值在下表中进行了说明。

表 *57:* 目标控制表中的值

字段	说明
并发连接数	设备与指定主机建立的最大出站连接数。（请注意，域可包含内部群件主机。）

字段	说明
每个连接的最大邮件数 (Maximum Messages Per Connection)	在发起新的连接之前，允许从设备到指定主机的单个出站连接发送的最大邮件数。
接管者	在指定时间段内允许的最大收件人数。“无”(None) 表示指定域没有收件人限制。 设备将统计收件人数的最短时间段（介于 1 和 60 分钟之间）。将该时间段指定为“0”可禁用该功能。 **注释** 如果更改收件人限制，则 AsyncOS 会重置队列中已有的所有邮件的计数器。设备会根据新的收件人限制传送邮件。
应用限制 (Apply Limits)	指定是否为整个域应用（强制执行）限制。 此设置会应用到连接、邮件和收件人限制。 指定限制将应用到系统级还是每个虚拟网关地址。 **注释** 如果配置了 IP 地组址，但是尚未配置虚拟网关，请不要按各个虚拟网关来配置应用限制。此设置仅旨在用于配置为使用虚拟网关的系统。有关配置虚拟网关的信息，请参阅使用虚拟网关™ 技术为所有托管的域配置邮件网关，第 570 页。

注释 如果按各个虚拟网关地址应用限制，仍可以有效实施系统级限制，方法是：将虚拟网关限制设置为所需的系统级限制，并将其除以可能的虚拟网关数。例如，如果配置了四个虚拟网关地址，并且不希望打开超过 100 个与域 `yahoo.com` 的同步连接，则将虚拟网关限制设置为 25 个同步连接。

对所有域执行 `delivernow` 命令时，会重置在 `destconfig` 命令中跟踪的所有计数器。

控制 TLS

还可以按域配置 TLS（传输层安全）。如果指定了“必需”(Required) 设置，则会该域协商从设备侦听程序到 MTA 的 TLS 连接。如果协商失败，则不会通过该连接发送任何邮件。有关详细信息，请参阅传送时启用 TLS 和证书验证，第 517 页。

可以指定在将邮件传送到需要 TLS 连接的域时，如果 TLS 协商失败，设备是否发送警报。警报邮件包含失败 TLS 协商的目标域名称。设备会将警报邮件发送给系统警报类型设置接收警告严重性级别警报的所有收件人。可以通过 GUI 中的“系统管理”>“警报”页面（或 CLI 中的 alertconfig 命令）管理警报收件人。

要启用 TLS 连接警报，请点击“目标控制”页面上的**编辑全局设置**或使用 destconfig -> setup 子命令。此设置为全局设置，而不是按域的设置。有关设备所尝试传送邮件的信息，请参阅“监控”(Monitor) >“邮件跟踪”(Message Tracking) 页面或邮件日志。

必须指定用于所有外发 TLS 连接的证书。使用“目标控制”页面上的**编辑全局设置**或 destconfig -> setup 子命令来指定证书。有关获取证书的信息，请参阅证书的使用，第 510 页。

有关警报的详细信息，请参阅“系统管理”一章。

控制退回验证标记

可以指定是否标记所发送的邮件已进行退回验证。可以为默认目标以及特定目标指定该设置。思科建议为默认目标启用退回验证，然后为特定排除项创建新目标。有关详细信息，请参阅退回验证，第 565 页。

控制退回

除了控制连接数以外，收件人将传送至远程主机及，还可以指定用于该域的退回配置文件。如果已指定，退回配置文件将显示在 destconfig 命令的第五列中。如果不指定退回配置文件，将使用默认退回配置文件。有关详细信息，请参阅创建新的退回配置文件，第 556 页。

添加新的目标控制条目

步骤 1 点击**添加目标 (Add Destination)**。

步骤 2 配置条目。

步骤 3 提交并确认更改。

导入和导出目标控制配置

如果管理多个域，可以创建一个配置文件来定义所有域的目标控制条目并将其导入到设备上。配置文件的格式类似于 Windows INI 配置文件。域的参数将分组在一个部分中，并以域名作为该部分的名称。例如，使用部分名称 [example.com] 为域 `example.com` 分组参数。未定义的任何参数都将继承自默认目标控制条目。可以通过在配置文件中包含 `[DEFAULT]` 部分来定义默认目标控制条目的参数。

导入该配置文件会覆盖设备的所有目标控制条目（默认条目除外），除非配置文件包含 `[DEFAULT]` 部分。其他所有现有目标控制条目都会被删除。

可以在配置文件中为域定义以下任何参数。`[DEFAULT]` 部分需要除 `bounce_profile` 参数以外的所有参数。

表 *58:* 目标控制配置文件参数

参数名	说明
ip_sort_pref	为该域指定互联网协议版本。 输入以下其中一个值： • 对于“首选 IPv6”(IPv6 Preferred)，输入 PREFER_V6 • 对于“IPv6 必需”(IPv6 Required)，输入 REQUIRE_v6 for “IPv6 Required” • 对于“首选 IPv4”(IPv4 Preferred)，输入 PREFER_V4 • 对于“IPv4 必需”(IPv6 Required)，输入 REQUIRE_v4 for “IPv6 Required”
max_host_concurrency	设备与指定主机建立的最大出站连接数。 如果为某个域定义了此参数，还必须定义 limit_type 和 limit_apply 参数。
max_messages_per_connection	在发起新的连接之前，允许从设备到指定主机的单个出站连接发送的最大邮件数。
recipient_minutes	设备将统计收件人数的最时间段（介于 1 和 60 分钟之间）。如果不应当应用任何收件人限制，请将其保留未定义状态。
recipient_limit	在指定时间段内允许的最大收件人数。如果不应当应用任何收件人限制，请将其保留未定义状态。 如果您为某个域定义该参数，也必须定义 recipient_minutes、limit_type 和 limit_apply 参数。
limit_type	指定将限制应用到整个域还是为该域指定的每个邮件交换 IP 地址。 输入以下其中一个值： • 0（或 host），表示域 • 1（或 MXIP），表示邮件交换 IP 地址
limit_apply	指定限制将应用到系统级还是每个虚拟网关地址。 输入以下其中一个值： • 0（或 system）表示系统范围 • 1（或 VG），表示虚拟网关
bounce_validation	指定是否打开退回验证地址标记功能。 输入以下其中一个值： • 0（或 off） • 1（或 on）

参数名	说明
table_tls	为该域指定 TLS 设置。有关详细信息，请参阅传送时启用 TLS 和证书验证，第 517 页。 输入以下其中一个值： • 0（或 off） • 1（或 on），表示“首选” • 2（或 required），表示“必需” • 3（或 on_verify），表示“首选（验证）” • 4（或 require_verify），表示“所需（验证）” 字符串不区分大小写。
bounce_profile	要使用的退回配置文件的名称。这不可在 [DEFAULT] 目标控制条目中使用。
send_tls_req_alert	是否在必需的 TLS 连接失败时发送警报。 输入以下其中一个值： • 0（或 off） • 1（或 on） 这是全局设置，仅可在 [DEFAULT] 目标控制条目中使用。
certificate	用于外发 TLS 连接的证书。这是全局设置，仅可在 [DEFAULT] 目标控制条目中使用。 **注释** 如果不指定证书，AsyncOS 将分配演示证书，但是使用该演示证书是不安全的，因此建议不要将其用于一般用途。

以下示例显示了用于域 example1.com 和 example2.com 的一个配置文件，以及相应的默认目标控制条目：

```
[DEFAULT]

ip_sort_pref = PREFER_V6

max_host_concurrency = 500

max_messages_per_connection = 50

recipient_minutes = 60

recipient_limit = 300

limit_type = host

limit_apply = VG

table_tls = off

bounce_validation = 0

send_tls_req_alert = 0
```

```
certificate = example.com
[example1.com]
ip_sort_pref = PREFER_V6
recipient_minutes = 60
recipient_limit = 100
table_tls = require_verify
limit_apply = VG
bounce_profile = tls_failed
limit_type = host
[example2.com]
table_tls = on
bounce_profile = tls_failed
```

以上示例会为 example1.com 和 example2.com 生成以下目标控制条目。

```
example1.com

IP Address Preference: IPv6 Preferred
Maximum messages per connection: 50
Rate Limiting:
500 concurrent connections
100 recipients per 60 minutes
Limits applied to entire domain, across all virtual gateways
TLS: Required (Verify)

Bounce Profile: tls_failed

example2.com

IP Address Preference: IPv6 Preferred
Maximum messages per connection: Default
Rate Limiting: Default
TLS: Preferred
Bounce Profile: tls_failed
```

使用“目标控制”页面上的**导入表**按钮或 `destconfig -> import` 命令导入配置文件。此外，还可使用“目标控制”页面上的**导出表**按钮或 `destconfig -> export` 命令将目标控制条目导出为 INI 文件。AsyncOS 在导出的 INI 文件中包含 `[Default]` 域。

目标控制和 CLI

可以使用 CLI 中的 destconfig 命令配置目标控制条目。在思科邮件安全设备 AsyncOS CLI 参考指南中介绍了此命令。

退回验证

“退回”邮件是接收 MTA 发送的新邮件，其使用原始邮件的信封发件人作为新的信封收件人。该退回（通常）会发送回信封收件人，并且当原始邮件不可传送（通常由于不存在收件人地址）时，具有空白的信封发件人 (MAIL FROM: <>)。

越来越多的垃圾邮件发送者通过错误定向的退回攻击来攻击邮件基础设施。这些攻击使用由未知的合法邮件服务器发送的大量退回邮件。基本上，垃圾邮件发送者采用的发送过程是：通过开放中继和“僵尸”网络将邮件发送到各个域中多个可能无效的地址（信封收件人）。在这些邮件中，会伪造信封发件人，以便垃圾邮件看似来自合法的域（这称为“Joe job”）。

反过来，对于具有无效信封收件人的每个传入邮件，接收邮件服务器会生成一个新邮件（退回邮件），并将其发送到无辜域中的信封发件人（其信封发件人地址是伪造的）。因此，此目标域会接收到大量“错误定向”的退回邮件，邮件有可能数以百万计。这种类型的分布式拒绝服务攻击可能会使邮件基础设施瘫痪，并使其无法成为发送或接收合法邮件的目标。

为了抵御这些错误定向退回攻击，AsyncOS 提供了退回验证。当启用该功能后，退回验证会为通过设备发送的邮件标记信封发件人地址。然后，会检查设备接收到的任何退回邮件的信封收件人，以查看是否存在此标记。对于合法退回邮件（应包含此标记），将移除标记并进行传送。不包含此标记的退回邮件将予以单独处理。

请注意，可以使用退回验证来基于外发邮件管理传入退回邮件。要控制设备如何生成外发退回邮件（基于传入邮件），请参阅定向退回的邮件，第 550 页。

概述：标记和退回验证

在启用退回验证的情况下发送邮件时，设备将重写邮件中的信封发件人地址。例如，MAIL FROM: joe@example.com 将变为 MAIL FROM: prvs=joe=123ABCDEFG@example.com。示例中的 123... 字符串是设备发送邮件时添加到信封发件人的“退回验证标记”。该标记使用在“退回验证”设置中定义的密钥生成（有关指定密钥的详细信息，请参阅退回验证地址标签密钥，第 566 页）。如果退回此邮件，退回邮件中的信封收件人地址通常会包含该退回验证标记。

可以在系统级启用或禁用退回验证标记作为默认设置。此外，还可以为特定域启用或禁用退回验证标记。在大多数情况下，默认启用该设置，然后列出要在目标控制表中排除的特定域（请参阅使用目标控制，第 559 页）。

如果邮件已包含标记的地址，AsyncOS 不会添加另一个标记（以免设备将退回邮件传送到 DMZ 中的一个设备）。

处理传入退回邮件

将传送包含有效标记的退回邮件。编辑会被删除，并且恢复信封收件人。在域映射进入邮件管道后会立即发生这种情况。可以定义设备如何处理未标记或标记无效的退回邮件 - 拒绝它们还是添加自定义信头。有关详细信息，请参阅配置退回验证设置，第 567 页。

如果退回验证标记不存在，用于生成该标记的密钥已更改，或者邮件存在时间超过七天，则该邮件将根据为退回验证定义的设置进行处理。

例如，以下邮件日志显示了设备拒绝的一封退回邮件：

```
Fri Jul 21 16:02:19 2006 Info: Start MID 26603 ICID 125192

Fri Jul 21 16:02:19 2006 Info: MID 26603 ICID 125192 From: <>

Fri Jul 21 16:02:40 2006 Info: MID 26603 ICID 125192 invalid bounce, rcpt address
<bob@example.com> rejected by bounce verification.
Fri Jul 21 16:03:51 2006 Info: Message aborted MID 26603 Receiving aborted by sender

Fri Jul 21 16:03:51 2006 Info: Message finished MID 26603 aborted
```

注释 将非退回邮件传送到您自己的内部邮件服务器（Exchange 等）时，应该为该内部域禁用退回验证标记功能。

AsyncOS 将退回邮件视为具有空 Mail From 地址 (<>) 的邮件。对于可能包含带有标记的信封收件人的非退回邮件，AsyncOS 会应用更宽松的策略。在这种情况下，AsyncOS 会忽略七天密钥到期日期并且还会尝试查找与旧密钥的匹配项。

退回验证地址标签密钥

标记密钥是生成退回验证标记时设备所使用的文本字符串。理想情况下，您将在所有设备中使用相同的密钥，以便离开域的所有邮件一致地进行标记。这样，如果一台设备标记一个外发邮件中的信封发件人，则会验证并传送一个传入退回邮件，即使退回邮件由不同的设备接收也是如此。

标记具有七天的宽限期。例如，可以选择在 7 天内多次更改标记密钥。在这种情况下，设备将尝试使用存在时间不超过七天的所有以前的密钥来验证已标记的邮件。

接受合法的无标记退回邮件

AsyncOS 还包括一个与退回验证相关的 HAT 设置，用于考虑无标记的退回邮件是否有效。默认设置为“否”，这表示没有标记的退回邮件被视为无效，并且设备会拒绝该邮件或根据在**邮件策略 > 退回验证**页上选择的操作来应用客户信头。如果选择“是”(Yes)，设备将没有标记的退回邮件视为有效并接受它们。在以下情况下可能会使用该设置：

假设您的某个用户希望向邮件列表发送邮件。但是，该邮件列表仅接受来自一组固定信封发件人的邮件。在这种情况下，不会接受来自您的用户的标记邮件（因为标记会定期更改）。

步骤 1 将该用户尝试向其发送邮件的域添加到目标控制表，并为该域禁用标记功能。此时，用户便可顺利地发送邮件了。

步骤 2 但是，要正确支持接收来自该域的退回邮件（因为它们没有标记），可以为该域创建一个发件人组，并在“接受”邮件流策略中启用“将无标记的退回视为有效”(Consider Untagged Bounces to be Valid) 参数。

使用退回验证防止退回邮件风暴

步骤 1 输入标记密钥。有关详细信息，请参阅配置退回验证地址标记密钥，第 567 页。

步骤 2 编辑退回验证设置。有关详细信息，请参阅配置退回验证设置，第 567 页。

步骤 3 通过目标控制启用退回验证。有关详细信息，请参阅使用目标控制，第 559 页。

配置退回验证地址标记密钥

退回验证地址标记密钥列表会显示当前密钥和过去使用过的所有未清除密钥。添加新密钥的步骤：

步骤 1 在**邮件策略 > 退回验证**页面上，点击**新建密钥**。

步骤 2 输入文本字符串，然后点击**提交 (Submit)**。

步骤 3 **确认**更改。

清除密钥

可以通过从下拉菜单中选择要清除的规则，然后点击**清除 (Purge)** 来清除旧地址标记密钥。

配置退回验证设置

退回验证设置可确定在接收无效退回时要采取的操作。

步骤 1 选择**邮件策略 > 退回验证**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选择是拒绝无效退回邮件，还是向邮件添加自定义信头。如果要添加信头，请输入信头名称和值。

步骤 4 或者，启用智能例外。此设置允许从退回验证处理（即使将单个侦听程序用于传入和外发邮件时）中自动免除传入邮件以及由内部邮件服务器生成的退回邮件。

步骤 5 提交并确认更改。

使用 CLI 配置退回验证

可以使用 CLI 中的 bvconfig 和 destconfig 命令来配置退回验证。在《思科邮件安全设备 *AsyncOS CLI* 参考指南》中介绍了这些命令。

退回验证和集群配置

退回验证在集群配置中工作，只要两个设备使用同一个“退回密钥”即可。当使用相同的密钥时，任一系统都能够接受合法的邮件退回。修改的信头标记/密钥不特定于每台设备。

设置邮件传送参数

deliveryconfig 命令会设置在从设备传送邮件时使用的参数。

设备使用多个邮件协议接受邮件：SMTP 和 QMQP。但是，所有外发邮件都使用 SMTP 传送，因此 deliveryconfig 命令不需要指定该协议。

注释 本部分介绍的一些功能或命令将会影响路由优先顺序或者会受路由优先顺序的影响。有关详细信息，请参阅“分配网络和 IP 地址”附录。

默认传送 IP 接口

默认情况下，系统使用 IP 接口组进行邮件传送。可以设置当前配置的任何 IP 接口或 IP 接口组。如果未确定具体的接口，AsyncOS 与收件人主机通信时，将使用与 SMTP HELO 命令中的默认传送接口关联的主机名。要配置 IP 接口，请使用 interfaceconfig 命令。

以下是有关使用自动选择方法选择邮件传送接口的规则：

- 如果远程邮件服务器与配置的接口位于同一子网中，则流量通过匹配的接口输出。
- 当设置为自动选择时，使用 routeconfig 配置的静态路由将生效。
- 否则，将使用与默认网关位于同一子网的接口。如果所有 IP 地址都有到目标的对应路由，则系统会使用可用的最高效接口。

可能的传送功能

注意 如果启用此功能，这邮件传送将不可靠，并且可能导致邮件丢失。此外，您的设备将不符合 RFC 5321 标准。有关详细信息，请参阅http://tools.ietf.org/html/rfc5321#section-6.1.。

当启用可能的传送功能时，AsyncOS 会将在传送邮件正文后，但在收件人主机确认收到该邮件之前超时的所有邮件视为“可能的传送”。如果其收件人主机持续出现阻止确认回执的错误，此功能可防止收件人收到多个邮件副本。AsyncOS 会在邮件日志中将此收件人记录为可能的传送，并将邮件计为已完成。

默认最大并发数

还可以指定设备为进行出站邮件传送而建立的最大并发连接数。（系统级的默认值为与单独的域建立 10,000 个连接。）该限制与每个侦听程序的最大出站邮件传送并发数一起受监控（对于专用侦听程序，每个侦听程序的默认连接数为 600，对于公共侦听程序，默认连接数为 1000）。将该值设置为低于默认值可避免网关控制较弱的网络。例如，一些防火墙不支持大量连接，这在一些环境中可能导致拒绝服务 (DoS) 警告。

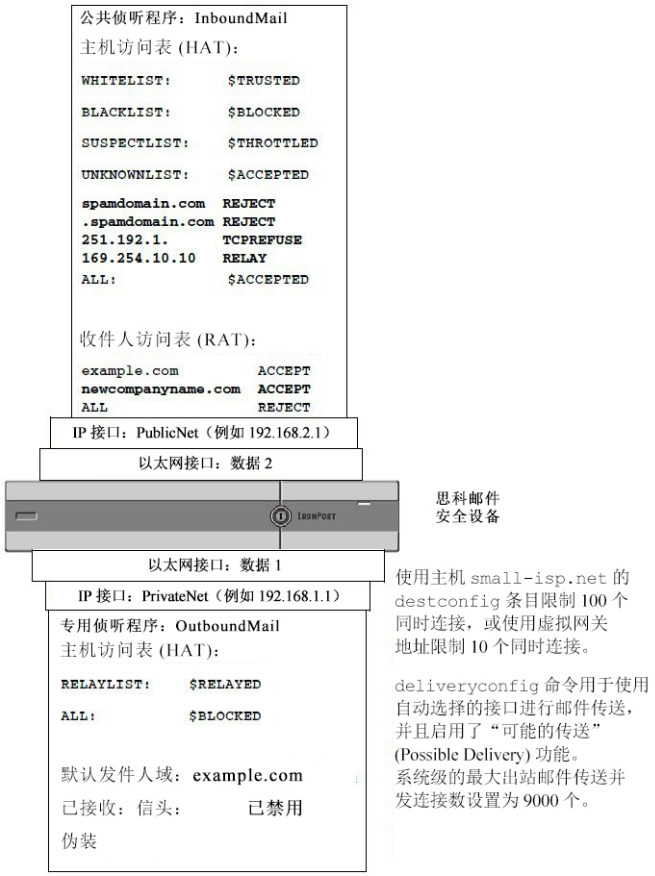
deliveryconfig 示例

在以下示例中，使用 `deliveryconfig` 命令将默认接口设置为“自动”，并且启用了“可能的传送”。系统级的最大出站邮件传送连接数设置为 9000 个。

```
mail3.example.com> deliveryconfig

Choose the operation you want to perform:

- SETUP - Configure mail delivery.

[]> setup

Choose the default interface to deliver mail.

1. Auto

2. PublicNet2 (192.168.3.1/24: mail4.example.com)

3. Management (192.168.42.42/24: mail3.example.com)

4. PrivateNet (192.168.1.1/24: mail3.example.com)

5. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Enable "Possible Delivery" (recommended)? [Y]> y

Please enter the default system wide maximum outbound message delivery

concurrency

[10000]> 9000

mail3.example.com>
```

现在，我们的邮件网关配置如下所示：

图 *51:* 设置目标和传送参数



使用虚拟网关™ 技术为所有托管的域配置邮件网关

本部分介绍虚拟网关™技术及其优势，如何设置虚拟网关地址，以及如何监控和管理虚拟网关地址。

思科虚拟网关技术允许为托管的所有域配置企业邮件网关（具有不同的 IP 地址、主机名和域），并为这些域创建单独的公司邮件策略实施和反垃圾邮件策略，同时托管在同一物理设备中。所有邮件安全设备型号中的可用虚拟网关地址数都为 255。

概述

思科开发了一种独特的虚拟网关技术，旨在帮助确保公司能通过邮件与其客户可靠地进行通信。虚拟网关技术使用户可以将设备分隔成多个虚拟网关地址，以用于发送和接收邮件。每个虚拟网关地址都具有不同的 IP 地址、主机名和域以及邮件队列。

为每个虚拟网关地址分配不同的 IP 地址和主机名可确保通过该网关传送的邮件由收件人主机正确识别，并防止重要邮件被作为垃圾邮件阻止。设备具有智能，可 SMTP HELO 命令中为每个虚拟网关地址指定正确的主机名。这可确保在接收互联网服务提供商 (ISP) 执行反向 DNS 查找时，设备可匹配通过该虚拟网关地址发送的邮件的 IP 地址。由于许多 ISP 使用反向 DNS 查找来检测未经请求的

邮件，因此该功能非常有用。如果反向 DNS 查找中的 IP 地址与发送主机的 IP 地址不匹配，则 ISP 可以假设发件人是非法的，并且通常会丢弃该邮件。虚拟网关技术可确保反向DNS查找始终能够匹配发送 IP 地址，避免邮件被意外阻止。

此外，还会为每个虚拟网关地址中的邮件分配单独的邮件队列。如果某个收件人主机正在阻止来自一个虚拟网关地址的邮件，则发往该主机的邮件将一直位于队列中并最终会超时。但是未被阻止的其他虚拟网关队列中发往同一域的邮件将会正常传送。尽管这些队列单独进行处理以用于传送，但系统管理、日志记录和报告功能仍将所有虚拟网关队列作为一个整体来提供相关的全面视图。

设置虚拟网关地址

在设置思科虚拟网关地址之前，必须分配用来发送邮件的一组 IP 地址。（有关详细信息，请参阅“分配网络和 IP 地址”附录。）还应确保正确配置 DNS 服务器，以便将 IP 地址解析为有效的主机名。正确配置的 DNS 服务器可确保在收件人主机执行反向 DNS 查找时，将其解析为有效的 IP/主机名对。

创建新的 IP 接口以与虚拟网关配合使用

确定了 IP 地址和主机名后，配置虚拟网关地址的第一步是使用 GUI 中的“网络”>“IP 接口”页面或 CLI 中的 interfaceconfig 命令通过 IP/主机名对创建新的 IP 接口。

配置了 IP 接口之后，可以选择将多个 IP 接口整合为接口组；然后可以将这些组分配到特定的虚拟网关地址，系统在传送邮件时会以“轮询”方式循环使用这些虚拟网关地址。

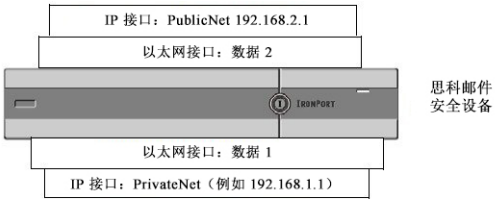
创建了所需的 IP 接口后，可以通过两个选项来设置虚拟网关地址并定义将从每个 IP 接口或接口组将发送哪些邮件活动：

- 可以使用 altsrchost 命令将来自特定发件人 IP 地址或信封发件人地址信息的邮件映射到主机 IP 接口（虚拟网关地址）或接口组以进行传送。
- 使用邮件过滤器时，可以设置特定主机 IP 接口以使用特定你主机 IP 接口（虚拟网关地址）或接口组来传送标记的邮件。请参阅修改源主机（虚拟网关地址）操作，第 180 页。（此方法比上述方法更加灵活和强大。）

有关创建 IP 接口的详细信息，请参阅“访问设备”附录。

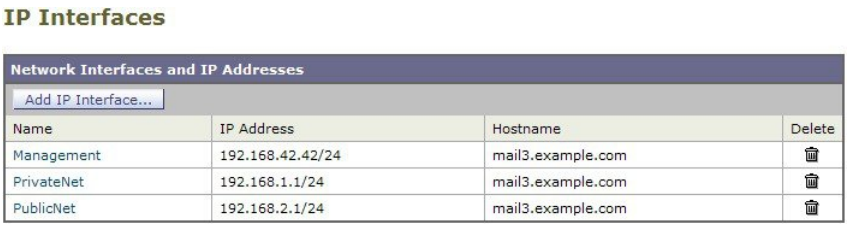
到目前为止，我们已将邮件网关配置与定义的以下接口配合使用，如下图中所示。

图 *52:* 公共和专用接口示例



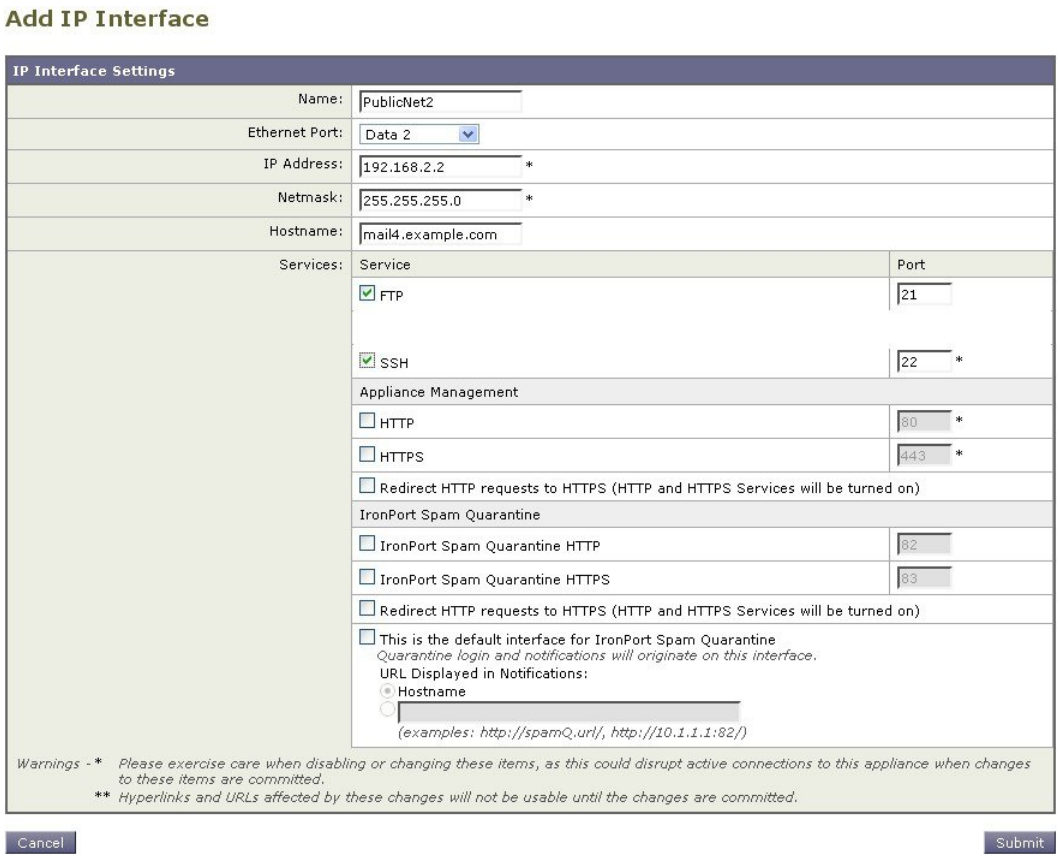
在下面的示例中，“IP 接口”(IP Interfaces) 页面确认除 Management 接口外，还配置了两个接口（PrivateNet 和 PublicNet）。

图 *53:* “*IP* 接口”页面



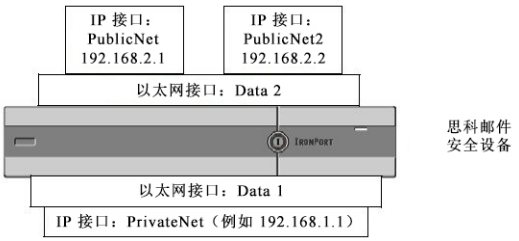
接下来，使用“添加 IP 接口”(Add IP Interface) 页面在 Data2 以太网接口上创建名为 PublicNet2 的新接口。使用的 IP 地址为 192.168.2.2，且指定了主机名 mail4.example.com。然后为 FTP（端口 21）和 SSH（端口 22）启用了服务。

图 *54:* 添加 *IP* 接口 *(Add IP Interface)* 页面



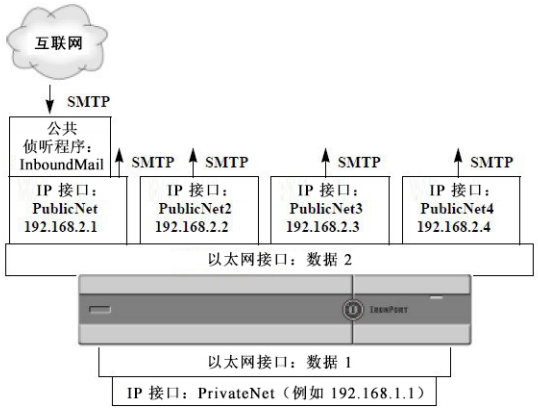
现在，我们的邮件网关配置如下所示：

图 *55:* 添加另一个公共接口



使用虚拟网关地址时，还可使用如下图中所示的配置。

图 *56:* 在一个以太网接口上配置四个虚拟网关地址



请注意，可以使用四个不同的IP接口来传送邮件，其中仅有一个公共侦听程序配置用于接受来自互联网的邮件。

将邮件映射到 IP 接口以进行传送

`altsrchost` 命令提供最简单、最直接的方法，将每个设备分隔到多个IP接口（虚拟网关地址），以便从这些接口传送邮件。但是，需要更强大的功能和更大的灵活性以便将邮件映射到特定虚拟网关的用户，应该研究邮件过滤器的使用。有关详细信息，请参阅使用邮件过滤器实施邮件策略，第 117 页。

`altsrchost` 命令允许在邮件传送期间基于以下一项来控制要使用的 IP 接口或接口组：

- 发件人的 IP 地址
- 信封发件人地址

要指定系统将通过其传送邮件的 IP 接口或接口组，可以创建映射密钥，以便将发件人的 IP 地址或信封发件人地址与 IP 接口或接口组（指定的接口名称或组名称）进行配对。

AsyncOS 会将 IP 地址和信封发件人地址与映射密钥进行比较。如果 IP 地址或信封发件人地址与其中一个密钥匹配，则会将相应的 IP 地址用于出站传送。如果没有匹配项，则使用默认出站接口。

系统可以匹配以下任一密钥并采用按以下顺序的优先级：

发件人的 IP 地址	发件人的 IP 地址必须完全匹配。 示例：`192.168.1.5`
完全格式化的信封发件人	信封发件人必须确切匹配整个地址。 示例：`username@example.com`
用户名	系统将用户名语法与信封发件人地址中 `@` 符号之前的部分进行匹配。必须包含 `@` 符号。示例：`username@`
域	系统将域名语法与信封发件人地址中从 `@` 符号开始的部分进行匹配。必须包含 `@` 符号。示例：`@example.com`

注释 侦听程序会检查 `altsrchost` 表中的信息并在检查伪装信息之后且在检查邮件过滤器之前，将邮件定向到特定接口。

在 CLI 中使用 `altsrchost` 命令中的以下子命令在虚拟网关中创建映射：

语法	说明
`new`	手动创建新的映射。
`print`	显示当前映射列表。
`delete`	从表中删除一个映射。

导入 altsrchost 文件

与 HAT、RAT、smtproutes 以及伪装和别名表一样，可以通过导出和导入文件来修改 altsrchost 条目。

步骤 1 使用 altsrchost 命令的 export 子命令将现有条目导出到文件（文件名称由您指定）。

步骤 2 在 CLI 外，获取该文件。（有关详细信息，请参阅FTP、SSH 和 SCP 访问，第 979 页。）

步骤 3 通过文本编辑器，在文件中创建新的条目。规则在 altsrchost 表中的显示顺序非常重要。

步骤 4 保存文件并将其放置在接口的“altsrchost”目录中，以便可以将其导入。（有关详细信息，请参阅FTP、SSH 和 SCP 访问，第 979 页。）

步骤 5 使用 altsrchost 的 import 子命令导入编辑后的文件。

altsrchost 限制

可以定义多达 1,000 个 altsrchost 条目。

具有 altsrchost 命令有效映射的文本文件示例

```
# Comments to describe the file

@example.com DemoInterface

paul@ PublicInterface

joe@ PublicInterface

192.168.1.5, DemoInterface

steve@example.com PublicNet
```

`Import` 和 `export` 子命令会逐行运行，并且将发件人 IP 地址或信封发件人地址行映射到接口名称。该密钥必须采用第一块使用非空格字符，后跟位于第二块非空格字符中的接口名称的形式，两者用逗号 (,) 或空格 ( ) 分隔开。注释行以数字符号 (#) 开头并将被忽略。

通过 CLI 添加 altsrchost 映射

在下面的示例中，将打印 `altsrchost` 表以显示不存在映射。然后，会创建两个条目：

- 来自名为 `@exchange.example.com` 组件服务器主机的邮件将映射到 PublicNet 接口。
- 来自 IP 地址为 192.168.35.35 发件人 IP 地址（例如，市场营销活动邮件系统）的邮件将映射到 PublicNe2t 接口。

最后，将打印 `altsrchost` 映射以供确认，并确认更改。

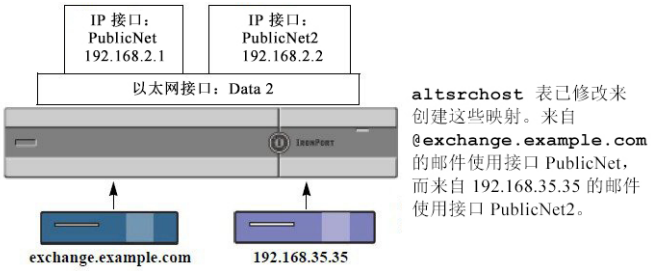
```
mail3.example.com> altsrchost

There are currently no mappings configured.

Choose the operation you want to perform:

- NEW - Create a new mapping.

- IMPORT - Load new mappings from a file.

[]> new

Enter the Envelope From address or client IP address for which you want to set up a
Virtual Gateway mapping. Partial addresses such as "@example.com" or "user@" are
allowed.

[]> @exchange.example.com

Which interface do you want to send messages for @exchange.example.com from?

1. PublicNet2 (192.168.2.2/24: mail4.example.com)

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail4.example.com)

[1]> 4

Mapping for @exchange.example.com on interface PublicNet created.
```

```
Choose the operation you want to perform:

- NEW - Create a new mapping.

- EDIT - Modify a mapping.

- DELETE - Remove a mapping.

- IMPORT - Load new mappings from a file.

- EXPORT - Export all mappings to a file.

- PRINT - Display all mappings.

- CLEAR - Remove all mappings.


[]> new


Enter the Envelope From address or client IP address for which you want to set up a
Virtual Gateway mapping. Partial addresses such as "@example.com" or "user@" are
allowed.


[]> 192.168.35.35

Which interface do you want to send messages for 192.168.35.35 from?

1. PublicNet2 (192.168.2.2/24: mail4.example.com)

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail4.example.com)

[1]> 1


Mapping for 192.168.35.35 on interface PublicNet2 created.

Choose the operation you want to perform:

- NEW - Create a new mapping.

- EDIT - Modify a mapping.

- DELETE - Remove a mapping.

- IMPORT - Load new mappings from a file.

- EXPORT - Export all mappings to a file.

- PRINT - Display all mappings.

- CLEAR - Remove all mappings.

[]> print

1. 192.168.35.35 -> PublicNet2

2. @exchange.example.com -> PublicNet
```

```
Choose the operation you want to perform:

- NEW - Create a new mapping.

- EDIT - Modify a mapping.

- DELETE - Remove a mapping.

- IMPORT - Load new mappings from a file.

- EXPORT - Export all mappings to a file.

- PRINT - Display all mappings.

- CLEAR - Remove all mappings.

[]>

mail3.example.com> commit

Please enter some comments describing your changes:


[]> Added 2 altsrchost mappings

Do you want to save the current configuration for rollback? [Y]> n

Changes committed: Fri May 23 11:42:12 2014 GMT
```

下图 展示本例中配置更改的图示：

图 *57:* 示例：选择要使用的 *IP* 接口或接口组



监控虚拟网关地址

尽管每个虚拟网关地址具有自己的邮件队列用于传送，但系统管理、日志记录和报告功能仍将所有虚拟网关队列作为一个整体来提供相关的全面视图。要监控每个虚拟网关队列的收件人主机状态，请使用 hoststatus 和 hostrate 命令。请参阅“使用 CLI 进行管理和监控”一章中的“读取可用的监控组件”部分。

hoststatus 命令会返回有关与特定收件人主机相关的邮件操作的监控信息。

如果使用虚拟网关技术，则还会显示有关每个虚拟网关地址的信息。该命令要求输入要返回的主机信息的域。此外还提供在 AsyncOS 缓存中存储的 DNS 信息以及从收件人主机返回的最后一个错误。返回的数据是从上一个 resetcounters 命令运行以来累加的。

返回的统计信息分为两类：计量器和测量器。此外，返回的其他数据包括：上次活动、MX 记录和最后的 5XX 错误。

管理每个虚拟网关地址的传送连接

某些系统参数需要系统和虚拟网关地址级别的设置

例如，一些收件人 ISP 会限制允许每个客户端主机具有的连接数量。因此，管理与 ISP 的关系非常重要，尤其是在通过多个虚拟网关地址传送邮件时。

有关 destconfig 命令以及虚拟网关地址如何受影响的信息，请参阅使用目标控制来控制邮件传送，第 557 页。

在创建一“组”虚拟网关地址时，虚拟网关的好邻居表设置会应用到该组，即使该组包含 254 个 IP 地址也是如此。

例如，假设您创建了包含 254 个出站 IP 地址的组并将其设置为通过“轮询”方式使用每个地址，并且假设 small-isp.com 的好邻居表对于系统允许 100 个同时连接，而对于虚拟网关地址允许 10 个连接。此配置绝不会为该组中的 254 个 IP 地址总计打开超过 10 个连接；该组被视为一个虚拟网关地址。

使用全局取消订用

为了确保特定收件人、收件人域或 IP 地址永远不会接收到来自设备的邮件，请使用 AsyncOS 全局取消订用功能。unsubscribe 命令允许在全局取消订用列表中添加和删除地址，以及启用和禁用此功能。AsyncOS 根据“全局取消订阅”用户、域、邮件地址和 IP 地址的列表来检查所有收件人地址。如果收件人与列表中的一个地址匹配，则该收件人会被删除或硬退回，并且全局取消订阅 (GUS) 计数器的计数会增加。（日志文件将记录匹配的收件人已被删除或硬退回。）在尝试向收件人发送邮件之前会立即进行 GUS 检查，从而检查系统发送的所有邮件。

注释 全局取消订阅不是用于更换名称删除和对邮件列表进行常规维护。该功能旨在作为一种故障防护机制，确保不会将邮件传送到不适当的实体。

全局取消订阅不可超过 10,000 个地址的上限。全局取消订阅地址可以具有以下四种格式之一：

表 *59:* 全局取消订用语法

username@example.com	完全格式化的邮件地址 此语法用于阻止特定域中的特定收件人。
username@	用户名 用户名语法将阻止所有域中具有指定用户名的所有收件人。该语法是用户名后跟 at 符号 (@)。

@example.com	域 域语法用于阻止发往特定域的所有收件人。该语法是在特定域前面加上 at 符号 (@)。
@.example.com	部分域 部分域语法用于阻止发往特定域及其所有子域的所有收件人。
10.1.28.12	IP 地址 IP 地址语法用于阻止发往特定 IP 地址的所有收件人。如果通过单个IP地址托管多个域，则此语法非常有用。该语法由常用的点号分隔的八位IP地址构成。

使用 CLI 添加全局取消订用地址

在本例中，将地址 user@example.net 添加到了全局取消订阅列表，并且该功能配置为硬退回邮件。发送到此地址的邮件将被退回；设备将在邮件传送之前立即退回邮件。

```
mail3.example.com> unsubscribe

Global Unsubscribe is enabled. Action: drop.

Choose the operation you want to perform:

- NEW - Create a new entry.

- IMPORT - Import entries from a file.

- SETUP - Configure general settings.

[]> new

Enter the unsubscribe key to add. Partial addresses such as

"@example.com" or "user@" are allowed, as are IP addresses. Partial hostnames such as

"@.example.com" are allowed.

[]> user@example.net

Email Address 'user@example.net' added.

Global Unsubscribe is enabled.

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import entries from a file.
```

```
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]> setup
Do you want to enable the Global Unsubscribe feature? [Y]> y
Would you like matching messages to be dropped or bounced?
1. Drop
2. Bounce
[1]> 2
Global Unsubscribe is enabled. Action: bounce.
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]>

mail3.example.com> commit
Please enter some comments describing your changes:
[]> Added username “user@example.net” to global unsubscribe
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

导入和导出全局取消订用文件

与 HAT、RAT、smtproutes、静态伪装表、别名表、域映射表以及 altsrchost 条目一样，可以通过导出和导入文件来修改全局取消订用条目。

步骤 1 使用 unsubscribe 命令的 export 子命令将现有条目导出到某个文件（您指定其名称）。

步骤 2 在 CLI 外，获取该文件。（有关详细信息，请参阅FTP、SSH 和 SCP 访问，第 979 页。）

步骤 3 通过文本编辑器，在文件中创建新的条目。

通过新行分隔文件中的条目。从所有标准操作系统返回表达是可接受的（<CR>、<LF> 或 <CR><LF>）。注释行以数字符号 (#) 开头并且会被忽略。例如，以下文件排除了单个收件人邮件地址 (test@example.com)、特定域 (@testdomain.com) 中的所有收件人、在多个域中具有相同名称 (testuser@) 的用户以及在特定 IP 地址 (11.12.13.14) 中的所有收件人。

```
# this is an example of the global_unsubscribe.txt file
test@example.com
@testdomain.com
testuser@
11.12.13.14
```

步骤 4 保存文件并将其放置在接口的配置目录中，以便可以将其导入。（有关详细信息，请参阅FTP、SSH 和 SCP 访问，第 979 页。）

步骤 5 使用 unsubscribe 的 import 子命令导入编辑后的文件。

回顾：邮件管道

下表提供了有关如何通过系统路由邮件（从接收到路由再到传送）的概述。每项功能都按顺序（从上到下）处理，并且简要地进行了总结。表 - 邮件安全设备的邮件管道：路由和传送功能中的阴影区域表示工作队列中发生的处理。

可以使用 trace 命令可以测试此管道中功能的大多数配置。有关详细信息，请参阅“故障排除”一章中的“使用测试邮件调试邮件流：跟踪”。

注释 对于外发邮件，在病毒爆发过滤器阶段之后会进行防数据丢失扫描。

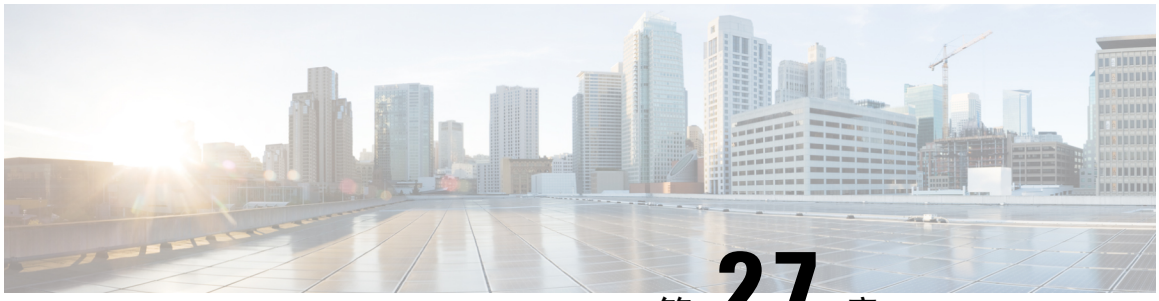
表 *60:* 邮件安全设备的邮件管道：接收邮件功能

特性	说明
主机访问表 (HAT) 主机 DNS 发件人验证组 信封发件人验证 发件人验证例外表 邮件流策略	ACCEPT、REJECT、RELAY 或 TCPREFUSE 连接 最大出站连接数 每个 IP 地址的最大并发入站连接数 每个连接的最大邮件大小和最大邮件数 每小时内每封邮件的最大收件人数 TCP 侦听队列大小 TLS：否/首选/必需 SMTP AUTH：否/首选/必需 删除具有格式不正确的 MAIL FROM 信头的邮件 始终接受或拒绝来自发件人验证例外表中的 Mail From 条目。 SenderBase 开/关（IP 配置/流量控制）
已接收信头	将已接收的信头添加到接受的邮件：开/关。
默认域	为没有域的用户地址添加默认域。
退回验证	用于验证传入退回邮件是否合法。
域名Map	为匹配域映射表中某个域的邮件中的每个收件人重写信封收件人。
收件人访问表 (RAT)	（仅限公共侦听程序）接受或拒绝 RCPT TO 中的收件人以及自定义 SMTP 响应。允许特殊收件人绕过限制。
别名表	重写信封收件人。（已配置的系统范围。aliasconfig 不是 listenerconfig 的子命令。）
LDAP 收件人接受	收件人接受的 LDAP 验证发生在 SMTP 会话过程中。如果在 LDAP 目录中找到收件人，则会删除或退回邮件。可以将 LDAP 验证配置为在工作队列中执行。

表 *61:* 邮件安全设备的邮件管道：路由和传送功能

邮件队列	**LDAP** 收件人接受		对收件人接受的 LDAP 验证在工作队列中执行。如果在 LDAP 目录中找到收件人，则会删除或退回邮件。可以将 LDAP 验证配置为 SMTP 会话中执行。
	化妆 或 **LDAP** 伪装		伪装发生在工作队列中；它会在静态表中或通过 LDAP 查询重写信封发件人、“收件人:”(To:)、“发件人:”(From:) 和/或“抄送:”(CC:) 信头。
	LDAP 路由		将对邮件路由或地址重写执行 LDAP 查询。组 LDAP 查询与邮件过滤器规则 mail-from-group 和 rcpt-to-group 结合使用。
	邮件过滤器*		邮件过滤器在邮件“拆分”之前应用。* 可将邮件发送到隔离区。
	反垃圾邮件**	按收件人扫描	反垃圾邮件扫描引擎会检查邮件，并返回判定以进一步进行处理。
	防病毒*		防病毒扫描会检查邮件中是否存在病毒。会对邮件进行扫描并有选择地进行修复（如果可能）。* 可将邮件发送到隔离区。
	高级恶意软件保护		高级恶意软件保护会执行文件信誉扫描和文件分析，以便检测附件是否存在恶意软件。
	内容过滤器*		会应用内容过滤器。* 可将邮件发送到隔离区。
	爆发过滤器*		爆发过滤器功能有助于防止病毒爆发。* 可将邮件发送到隔离区。
	虚拟网关		通过特定 IP 接口或 IP 接口组发送邮件。
	传送限制		1.设置默认传送接口。 2.设置最大出站连接数。
	基于域的限制		按域定义：每个虚拟网关以及整个系统的最大出站连接数；要使用的退回配置文件；用于传送的 TLS 首选项：否/首选/必需
	基于域的路由		根据域路由邮件，不重写信封收件人。
	全局取消订用		根据特定列表（配置的系统级列表）丢弃收件人。
	退回配置文件		无法发送的邮件处理。可按侦听程序、目标控制条目以及通过邮件过滤器进行配置。

* 这些功能可将邮件发送到称为隔离区的特定队列。



第 27 章

LDAP 查询

本章包含以下部分：

LDAP 查询概述

如果在网络基础设施的 LDAP 目录中（例如，在 Microsoft Active Directory、SunONE Directory Server 或 OpenLDAP 目录中）存储用户信息，则可以将设备配置为查询 LDAP 服务器以接受、路由和验证邮件。可以将设备配置为与一个或多个 LDAP 服务器配合使用。

以下部分概述了可以执行的 LDAP 查询的类型；LDAP 如何与设备配合使用以验证、接受和路由邮件；以及如何将设备配置为与 LDAP 配合使用。

了解 LDAP 查询

如果在网络基础设施的 LDAP 目录中存储用户信息，则可以将设备配置为查询 LDAP 服务器以用于实现以下目的：

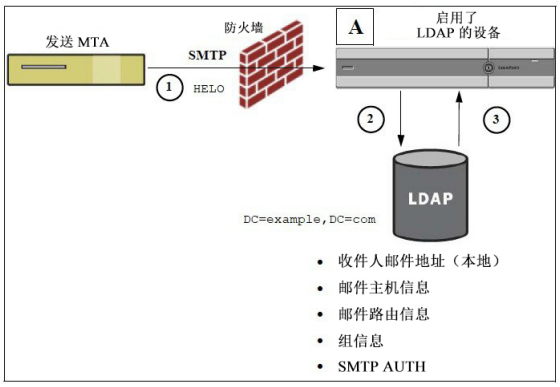
- **接受查询**。可以使用现有 LDAP 基础设施来定义如何处理传入邮件的收件人邮件地址（在公共侦听程序中）。有关详细信息，请参阅使用接受查询进行收件人验证，第 601 页。
- **路由（别名设置）**。可以将设备配置为根据网络中 LDAP 目录中的可用信息，将邮件路由至相应地址和/或邮件主机。有关详细信息，请参阅使用路由查询将邮件发送到多个目标地址，第 602 页。
- **证书身份验证**。可以创建查询来检查客户端证书的有效性，以便验证用户的邮件客户端与邮件安全设备之间的 SMTP 会话。有关详细信息，请参阅检查客户端证书的有效性，第 631 页。
- **伪装**。可以伪装信封发件人（对于传出邮件）和邮件信头（对于传入邮件，如“收件人:”(To:)、“回复:”(Reply To:)、“发件人:”(From:) 或“抄送:”(CC:)）。有关伪装的更多信息，请参阅使用伪装查询重写信封发件人，第 603 页。
- **组查询**。可以将设备配置为根据 LDAP 目录中的组对邮件执行操作。为此，可以将组查询与邮件过滤器相关联。可以对与定义的LDAP组匹配的邮件执行适用于邮件过滤器的任何邮件操作。有关详细信息，请参阅使用组 LDAP 查询确定收件人是否为组成员，第 604 页。
- **基于域的查询**。可以创建基于域的查询，以便设备在单个侦听程序中为不同的域执行不同的查询。当邮件安全设备运行基于域的查询时，它会根据域确定要使用的查询，并且会查询与该域关联的 LDAP 服务器。
- **链查询**。可以创建链查询来使设备按顺序执行一系列查询。在配置链查询时，设备会按顺序运行每个查询，直到 LDAP 设备返回一个积极的结果。对于链式路由查询，设备会按顺序对每个重写的邮件地址重新运行相同的配置链查询。
- **目录搜集预防**。可以将设备配置为使用 LDAP 目录来抵御目录搜集攻击。可以在 SMTP 会话期间或在工作队列中配置目录搜集攻击预防。如果在 LDAP 目录中找不到收件人，可以配置系统以执行延迟退回或彻底删除邮件。因此，垃圾邮件发送者无法区分有效和无效的邮件地址。请参阅将 LDAP 用于目录搜集攻击预防，第 609 页。
- **SMTP 身份验证**。AsyncOS 支持 SMTP 身份验证。SMTP 身份验证是用于验证连接到 SMTP 服务器的客户端的一种机制。可以使用该功能使贵组织中的用户可以使用邮件服务器发送邮件，即使他们利用远程连接（例如在家中或在旅行时）也是如此。有关详细信息，请参阅配置AsyncOS 进行 SMTP 身份验证，第 612 页。
- **外部身份验证**。可以将设备配置为使用 LDAP 目录来验证登录到设备的用户。有关详细信息，请参阅为用户配置外部 LDAP 身份验证，第 619 页。
- **垃圾邮件隔离区最终用户身份验证**。可以将设备配置为在用户登录最终用户隔离区时对其进行验证。有关详细信息，请参阅对垃圾邮件隔离区的终端用户进行身份验证，第 621 页。
- **垃圾邮件隔离区别名合并**。如果为垃圾邮件使用邮件通知，则此查询会合并最终用户别名，以便最终用户不会根据每个别名邮件地址都收到隔离区通知。有关详细信息，请参阅垃圾邮件隔离区别名整合查询，第 623 页。

了解 LDAP 如何与 AsyncOS 配合使用

使用 LDAP 目录时，可以将设备与 LDAP 目录服务器配合使用，以接受收件人、路由邮件和/或伪装邮件信头。还可以将 LDAP 组查询与邮件过滤器配合使用，以创建规则来处理设备接收的邮件。

下图展示设备如何与 LDAP 配合使用：

图 *58: LDAP* 配置



1. 发送 MTA 通过 SMTP 将邮件发送到公共侦听程序。
2. 设备通过**系统管理 > LDAP**页面（或通过全局 **ldapconfig** 命令）查询定义的 LDAP 服务器。
3. 将从 LDAP 目录接收数据，而且根据在**系统管理 > LDAP** 页面（或在 **ldapconfig** 命令中）定义由侦听程序使用的查询：
   - 邮件将路由到新的收件人地址，或者被删除或退回
   - 邮件将路由到新收件人的相应邮件主机
   - “发件人:”(From:)、“收件人:”(To:) 和“抄送:”(CC:) 邮件信头将根据查询重写
   - 执行 **rcpt-to-group** 或 **mail-from-group** 邮件过滤器规则（与配置的组查询配合使用）定义的进一步操作。

注释 可以将设备配置为连接到多个 LDAP 服务器。当这样做时，可以配置用于负载平衡或故障转移的 LDAP 配置文件设置。有关使用多个 LDAP 服务器的详细信息，请参阅将 AsyncOS 配置为与多个 LDAP 服务器配合使用，第 625 页。

将 Cisco IronPort 设备配置为与 LDAP 服务器配合使用

配置设备以与 LDAP 目录配合使用时，必须完成以下步骤以配置 AsyncOS 设备的接受、路由、别名和伪装设置：

步骤 1 配置 LDAP 服务器配置文件。服务器配置文件包含用于启用 AsyncOS 以连接到 LDAP 服务器（或多个服务器）的信息，例如：

- 发送查询的服务器和端口的名称，
- 基本 DN，以及
- 有关绑定到服务器的身份验证要求

有关配置服务器配置文件的详细信息，请参阅创建 LDAP 服务器配置文件以存储有关 LDAP 服务器的信息，第 588 页。

配置 LDAP 服务器配置文件时，可以配置 AsyncOS 以连接到一个或多个 LDAP 服务器。

有关配置 AsyncOS 以连接到多个服务器的信息，请参阅将 AsyncOS 配置为与多个 LDAP 服务器配合使用，第 625 页。

步骤 2 **配置 LDAP 查询**。在 LDAP 服务器配置文件中配置 LDAP 查询。配置的查询应根据特定 LDAP 实施和方案进行定制。

有关的可以创建的 LDAP 查询类型的信息，请参阅了解 LDAP 查询，第 586 页。

有关编写查询的信息，请参阅处理 LDAP 查询，第 594 页。

步骤 3 **在公共侦听程序或专用侦听程序中启用 LDAP 服务器配置文件**。必须在侦听程序上启用 LDAP 服务器配置文件，以指示侦听程序在接受、路由或发送邮件时运行 LDAP 查询。

有关详细信息，请参阅启用 LDAP 查询以在特定侦听程序中运行，第 590 页。

注释 在配置组查询时，需要执行额外的步骤来配置 AsyncOS，以便与 LDAP 服务器配合使用。有关配置组查询的信息，请参阅使用组 LDAP 查询确定收件人是否为组成员，第 604 页。当配置最终用户身份验证或垃圾邮件通知整合查询时，必须启用 LDAP 最终用户对垃圾邮件隔离区的访问。有关垃圾邮件隔离区的详细信息，请参阅“垃圾邮件隔离区”章节。

创建 LDAP 服务器配置文件以存储有关 LDAP 服务器的信息

配置 AsyncOS 以使用 LDAP 目录时，您需要创建 LDAP 服务器配置文件来存储有关 LDAP 服务器的信息。

步骤 1 在“系统管理”(System Administration) > “LDAP”页面上，点击**添加 LDAP 服务器配置文件 (Add LDAP Server Profile)**。

步骤 2 输入服务器配置文件的名称。

步骤 3 输入 LDAP 服务器的主机名。

可以输入多个主机名以配置用于故障转移或负载均衡的 LDAP 服务器。使用逗号分隔多个条目。有关详细信息，请参阅将 AsyncOS 配置为与多个 LDAP 服务器配合使用，第 625 页。

步骤 4 选择身份验证方法。可以使用匿名身份验证或指定用户名和密码。

步骤 5 选择 LDAP 服务器类型：Active Directory、OpenLDAP 或“未知或其他 (Unknown or Other)”。

步骤 6 输入端口号。

对于 Active Directory 或任何未知/其他服务器类型，默认端口为 3268（不使用 SSL 时）和 3269（使用 SSL 时）。

对于 Open LDAP 服务器类型，默认端口为 389（不使用 SSL 时）和 636（使用 SSL 时）。

步骤 7 输入 LDAP 服务器的基础 DN（可分辨名称）。

如果通过用户名和密码进行身份验证，则用户名必须包含具有该密码的条目的完整DN。例如，某个用户是营销团队的成员，其邮件地址为 joe@example.com。此用户的条目类似于以下条目：

```
uid=joe, ou=marketing, dc=example dc=com
```

步骤 8 选择在与 LDAP 服务器通信时是否使用 SSL。

步骤 9 在“高级”(Advanced) 下，输入缓存生存时间。此值表示保留缓存的时长。

步骤 10 输入保留缓存条目的最大数量。

注释 此缓存按 LDAP 服务器进行维护。如果要配置多个 LDAP 服务器，则必须设置更小的 LDAP 缓存值以提高性能。此外，如果设备中各种进程的内存使用量较高，则增加此值可能会降低系统性能。

步骤 11 输入最大并发连接数。

如果配置用于负载均衡的 LDAP 服务器配置文件，则这些连接会分布在列出的 LDAP 服务器之间。例如，如果配置 10 个并发连接并且通过三台服务器对连接进行负载均衡，则 AsyncOS 会与每台服务器建立 10 个连接，总共建立 30 个连接。

注释 最大并发连接数包括用于 LDAP 查询的 LDAP 连接。但是，如果为垃圾邮件隔离区使用 LDAP 身份验证，则设备可能会打开更多连接。

步骤 12 通过点击“测试服务器”按钮测试服务器连接。如果指定了多个 LDAP 服务器，则会对它们全部进行测试。测试结果会显示在“连接状态”(Connection Status) 字段中。有关详细信息，请参阅测试LDAP服务器，第 589 页。

步骤 13 通过标记相应复选框并填写字段来创建查询。可以选择“接受”(Accept)、“路由”(Routing)、“伪装表”(Masquerade)、“组”(Group)、“SMTP 身份验证”(SMTP Authentication)、“外部身份验证”(External Authentication)、“垃圾邮件隔离区终端用户身份验证”(Spam Quarantine End-User Authentication) 和“垃圾邮件隔离区别名合并”(Spam Quarantine Alias Consolidation)。

注释 要允许设备在您接收或发送邮件时运行 LDAP 查询，必须在适当的侦听程序上启用 LDAP 查询。有关详细信息，请参阅启用 LDAP 查询以在特定侦听程序中运行，第 590 页。

步骤 14 通过点击**测试查询 (Test Query)** 按钮测试查询。

输入测试参数并点击“运行测试”。测试结果会显示在“连接状态”(Connection Status) 字段中。如果对查询定义或属性进行任何更改，请点击**更新 (Update)**。有关详细信息，请参阅测试 LDAP 服务器，第 589 页。

注释 如果将 LDAP 服务器配置为允许与空密码进行绑定，则查询可以使用空密码字段通过测试。

步骤 15 提交并确认更改。

注释 尽管服务器配置的数量不受限制，但是可以仅为每台服务器配置一个收件人接受、一个路由、一个伪装和一个组查询。

测试 LDAP 服务器

使用“添加/编辑 LDAP 服务器配置文件”页面上的“测试服务器”按钮（或 CLI 中 ldapconfig 命令的 test 子命令）测试与 LDAP 服务器的连接。AsyncOS 会显示消息，指明与服务器端口的连接是成功还是失败。如果配置了多台 LDAP 服务器，则 AsyncOS 会测试每台服务器并显示各个测试结果。

启用 LDAP 查询以在特定侦听程序中运行

要允许设备在您接收或发送邮件时运行 LDAP 查询，必须在适当的侦听程序上启用 LDAP 查询。

配置 LDAP 查询的全局设置

LDAP 全局设置定义设备如何处理所有 LDAP 流量。

步骤 1 在**系统管理 > LDAP** 页面上，点击**编辑设置**。

步骤 2 选择用于 LDAP 流量的 IP 接口。默认情况下，设备会自动选择接口。

步骤 3 选择用于 LDAP 接口的 TLS 证书（通过**网络 > 证书**页或 CLI 中的 **certconfig** 命令添加的 TLS 证书在列表中提供，请参阅加密与其他 MTA 的通信概述，第 509 页）。

步骤 4 如果要验证 LDAP 服务器证书，请选择适当的选项。

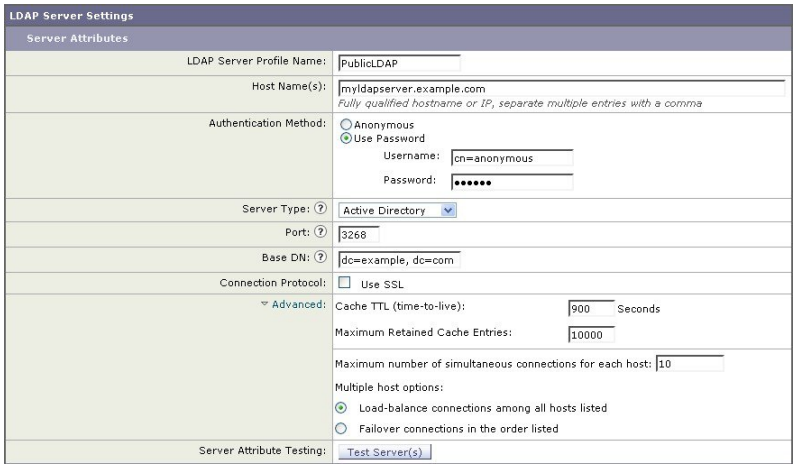
步骤 5 提交并确认更改。

创建 LDAP 服务器配置文件示例

在下面的示例中，“系统管理”(System Administration) > “LDAP”页面用于为要绑定到的设备定义 LDAP 服务器，并为收件人接受、路由和伪装配置查询。

注释 LDAP 连接具有 60 秒的连接尝试超时（包括 DNS 查找、连接本身，以及如果适用，设备自身的身份验证绑定）。在第一次失败后，AsyncOS 会立即开始尝试同一服务器中的其他主机（如果以逗号分隔的列表形式指定了多个主机）。如果服务器中只有一个主机，AsyncOS 会继续尝试连接到它。

图 *59:* 配置 *LDAP* 服务器配置文件 *(1/2)*

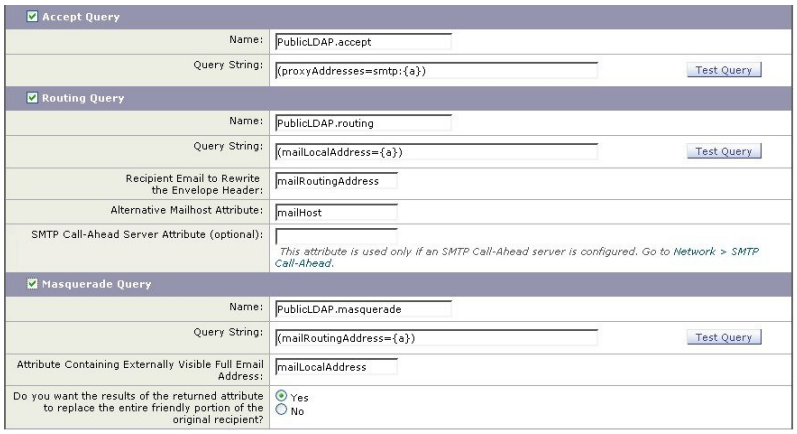


首先，为 myldapserver.example.com LDAP 服务器指定昵称“PublicLDAP”。连接数量设置为 10（默认值），而且多个 LDAP 服务器（主机）负载均衡选项将保留默认设置。可以通过提供一个用逗号

分隔的名称列表，在此处指定多个主机。查询将定向到端口 3268（默认值）。对于此主机，未启用 SSL 作为连接协议。定义了 example.com 的基本 DN (dc=example,dc=com)。缓存存活时间设置为 900 秒，缓存条目的最大数量为 10000，而且身份验证方法设置为密码。

定义了用于收件人接受、邮件路由和伪装的查询。确保查询名称区分大小写，必须完全一致才能返回正确的结果。

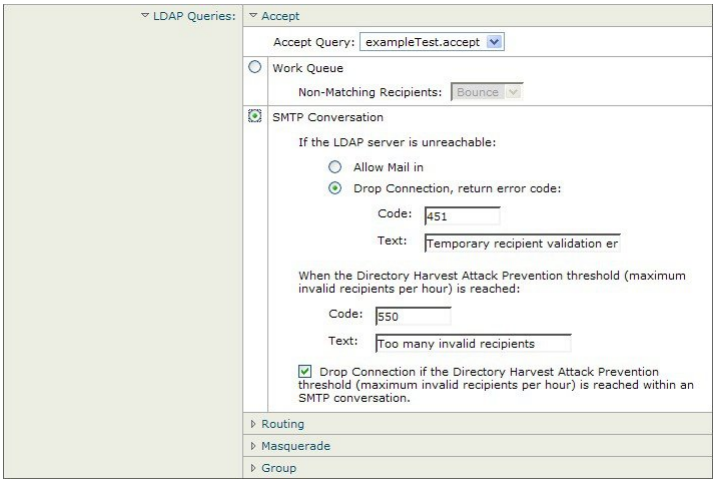
图 *60:* 配置 *LDAP* 服务器配置文件 *(2/2)*



在公共侦听程序上启用 LDAP 查询

在本例中，公共侦听程序“InboundMail”更新为将 LDAP 查询用于收件人接受。此外，收件人接受配置为在 SMTP 会话期间发生（有关详细信息，请参阅使用接受查询进行收件人验证，第 601 页）。

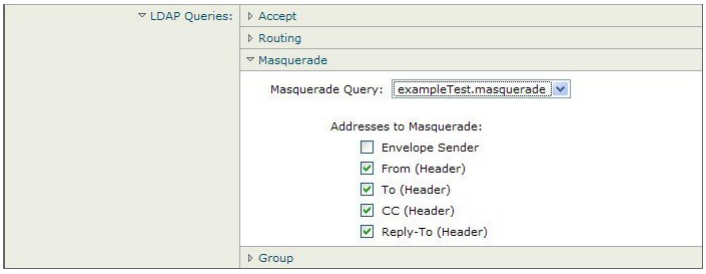
图 *61:* 在侦听程序上启用接受和路由查询



在专用侦听程序上启用 LDAP 查询

在本例中，专用侦听程序“OutboundMail”更新为将 LDAP 查询用于伪装。伪装的字段包括：“发件人”(From)、“收件人”(To)、“抄送”(CC) 和“回复”(Reply-To)。

图 *62*: 在侦听程序上启用伪装查询



对 Microsoft Exchange 5.5 的增强支持

AsyncOS 包含一个配置选项，可用于为 Microsoft Exchange 5.5 提供支持。如果使用较高版本的 Microsoft Exchange，则不需要启用此选项。在配置 LDAP 服务器时，可选择通过在 `ldapconfig -> edit -> server -> compatibility` 子命令（仅通过 CLI 可用）中出现提示时回答“y”来启用 Microsoft Exchange 5.5 支持。

```
mail3.example.com> ldapconfig

Current LDAP server configurations:

1. PublicLDAP: (ldapexample.com:389)


Choose the operation you want to perform:

- NEW - Create a new server configuration.

- EDIT - Modify a server configuration.

- DELETE - Remove a server configuration.


[]> edit

Enter the name or number of the server configuration you wish to edit.

[]> 1

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Choose the operation you want to perform:

- SERVER - Change the server for the query.
```

```
- LDAPACCEPT - Configure whether a recipient address should be accepted or
bounced/dropped.

- LDAPROUTING - Configure message routing.

- MASQUERADE - Configure domain masquerading.

- LDAPGROUP - Configure whether a sender or recipient is in a specified group.

- SMTPAUTH - Configure SMTP authentication.

[]> server

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com


Microsoft Exchange 5.5 Compatibility Mode: Disabled

Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.

- PORT - Configure the port.

- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.

- COMPATIBILITY - Set LDAP protocol compatibility options.

[]> compatibility
Would you like to enable Microsoft Exchange 5.5 LDAP compatibility mode? (This is not
recommended for versions of Microsoft Exchange later than 5.5, or other LDAP servers.)


[N]> y

Do you want to configure advanced LDAP compatibility settings? (Typically not required)

[N]>

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Microsoft Exchange 5.5 Compatibility Mode: Enabled (attribute "objectClass")

Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.
```

```
- PORT - Configure the port.

- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.

- COMPATIBILITY - Set LDAP protocol compatibility options.

[]>
```

处理 LDAP 查询

在 LDAP 服务器配置文件中为您要执行的每种类型的 LDAP 查询创建一个条目。在创建 LDAP 查询时，必须输入 LDAP 服务器的查询语法。请注意，构建的查询应进行定制并且特定于 LDAP 目录服务的特殊实施，特别是在通过对象类和属性扩展了目录以满足目录的独特需求时。

LDAP 查询的类型

- **接受查询**。有关详细信息，请参阅使用接受查询进行收件人验证，第 601 页。
- **路由查询**。有关详细信息，请参阅使用路由查询将邮件发送到多个目标地址，第 602 页。
- **证书身份验证查询**。有关详细信息，请参阅检查客户端证书的有效性，第 631 页。
- **伪造查询**。有关详细信息，请参阅使用伪装查询重写信封发件人，第 603 页。
- **组查询**。有关详细信息，请参阅使用组 LDAP 查询确定收件人是否为组成员，第 604 页。
- **基于域的查询**。有关详细信息，请参阅使用基于域的查询路由到特定域，第 607 页。
- **链查询**。有关详细信息，请参阅使用链查询执行一系列 LDAP 查询，第 608 页。

还可以为以下目的配置查询：

- **目录搜集预防**。有关详细信息，请参阅了解 LDAP 查询，第 586 页。
- **SMTP 身份验证**。有关详细信息，请参阅配置 AsyncOS 进行 SMTP 身份验证，第 612 页。
- **外部身份验证**。有关详细信息，请参阅为用户配置外部 LDAP 身份验证，第 619 页。
- **垃圾邮件隔离区终端用户身份验证查询**。有关详细信息，请参阅对垃圾邮件隔离区的终端用户进行身份验证，第 621 页。
- **垃圾邮件隔离区别名整合查询**。有关详细信息，请参阅垃圾邮件隔离区别名整合查询，第 623 页。

指定的搜索查询适用于在系统上配置的所有侦听程序。

基本可区别名称 (DN)

目录的根级别称为基本。基本的名称为 DN（可分辨名称）。Active Directory 的基本 DN 格式（以及按照 RFC 2247 的标准）会将 DNS 域转换为域组成部分 (dc=)。例如，example.com 的基本 DN 为：dc=example，dc=com。请注意，DNS 名称的每个部分均按顺序表示。这可能会或不会反映您的配置的 LDAP 设置。

如果目录中包含多个域，则您可能会发现不便为查询输入单个 BASE。在本例中，在配置 LDAP 服务器设置时，请将基本 DN 设置为“无”(NONE)。但是，这会让搜索效率低下。

LDAP 查询语法

LDAP 路径中允许有空格，而且不需要加引号。CN 和 DC 语法不区分大小写。

Cn=First Last,oU=user,dc=domain,DC=COM

为查询输入的变量名称区分大小写，且必须与 LDAP 实施匹配才能正常工作。例如，在提示符处输入 **mailLocalAddress** 执行的查询与输入 **maillocaladdress** 所执行的查询是不同的。

令牌：

可以在 LDAP 查询中使用以下令牌：

- {a} 用户名@域名
- {d} 域名
- {dn} 可区别名称
- {g} 组名称
- {u} 用户名
- {f} MAIL FROM: 地址

注释 {f} 令牌仅在接受查询中有效。

例如，可以使用以下查询接受 Active Directory LDAP 服务器的邮件：

(|(mail={a})(proxyAddresses=smtp:{a}))

注释 在侦听程序上启用 LDAP 功能之前，Cisco Systems 强烈建议使用“LDAP”页面的测试功能（或 **ldapconfig** 命令的 **test** 子命令）来测试所构建的所有查询，并确保返回预期结果。有关详细信息，请参阅测试 LDAP 查询，第 599 页。

安全 LDAP (SSL)

可以指示 AsyncOS 在与 LDAP 服务器通信时使用 SSL。如果将 LDAP 服务器配置文件配置为使用 SSL：

- AsyncOS 将使用通过 CLI 中的 certconfig 配置的 LDAPS 证书（请参阅创建自签名 证书，第 512 页）。

  可能必须将 LDAP 服务器配置为支持使用 LDAPS 证书。

- 如果未配置 LDAPS 证书，则 AsyncOS 将使用演示证书。

路由查询 (Routing Queries)

LDAP 路由查询没有递归限制；路由完全由数据驱动。但是，AsyncOS 会检查循环参考数据以防止无限循环地进行路由。

允许客户端匿名绑定到 LDAP 服务器

可能需要配置LDAP目录服务器以允许匿名查询。（即，客户端可匿名绑定到服务器并执行查询。）有关配置 Active Directory 以允许匿名查询的具体说明，请参阅以下 URL 的“Microsoft 知识库文章 - 320528”：

```
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B320528
```

或者，可以配置一个“用户”，将其专用于身份验证和执行查询，而不是打开 LDAP 目录服务器以从任何客户端进行匿名查询。

此处提供相应步骤的摘要，特别是：

- 如何设置 Microsoft Exchange 2000 服务器以允许“匿名”身份验证。
- 如何设置 Microsoft Exchange 2000 服务器以允许“匿名绑定”。
- 如何使用“匿名绑定”和“匿名”身份验证设置 AsyncOS 以从 Microsoft Exchange 2000 服务器检索 LDAP 数据。

必须为 Microsoft Exchange 2000 服务器提供特定权限，以便允许“匿名”或“匿名绑定”身份验证，从而查询用户邮件地址。当 LDAP 查询用于确定进入 SMTP 网关的传入邮件的有效性时，该操作非常有用。

匿名身份验证设置

通过下面的设置说明，可以将特定数据提供给 Microsoft Windows Active Directory 中未经身份验证的 Active Directory 和 Exchange 2000 服务器查询。如果希望允许“匿名绑定”到 Active Directory，请参阅Active Directory 的匿名绑定设置，第 597 页。

步骤 1 确定所需的 Active Directory 权限。

使用 ADSI Edit 管理单元或 LDP 实用程序时，必须修改以下 Active Directory 对象属性的权限：

- 要根据其进行查询的域的域命名上下文根。
- 包含要根据其查询邮件信息的用户的所有 OU 和 CN 对象。

下表显示了要应用到所需容器的所需权限。

用户对象	权限	遗产	权限类型
所有人	列出内容	容器对象	对象

用户对象	权限	遗产	权限类型
所有人	列出内容	组织单位对象	对象
所有人	读取公共信息	用户对象	特性
所有人	读取电话和邮件选项	用户对象	特性

步骤 2 设置 Active Directory 权限

- 打开 Windows 2000 支持工具中的 ADSIEdit。
- 找到**域命名上下文 (Domain Naming Context)** 文件夹。此文件夹包含域的 LDAP 路径。
- 右键点击**域命名上下文 (Domain Naming Context)** 文件夹，然后点击**属性 (Properties)**。
- 点击 **Security**。
- 点击 **Advanced**。
- 点击 **Add**。
- 点击**用户对象 (User Object)**“Everyone”，然后点击**确定 (OK)**。
- 点击**权限类型 (Permission Type)** 选项卡。
- 点击**应用到 (Apply onto)** 框中的**继承 (Inheritance)**。
- 点击以选中**权限 (Permission)** 对应的“允许”(Allow) 复选框。

步骤 3 配置思科邮件网关

使用命令行界面 (CLI) 中的 **`ldapconfig`** 创建包含下列信息的 LDAP 服务器条目。

- Active Directory 或 Exchange 服务器的主机名
- 端口 3268
- 与域的根命名上下文匹配的基本 DN
- 匿名身份验证类型

Active Directory 的匿名绑定设置

通过下面的设置说明，可以将特定数据提供给 Microsoft Windows Active Directory 中 Active Directory 和 Exchange 2000 服务器的匿名绑定查询。Active Directory 服务器的匿名绑定将发送用户名 anonymous 且密码为空。

注释 如果将某个密码发送到 Active Directory 服务器并且尝试匿名绑定，则身份验证可能会失败。

步骤 1 确定所需的 Active Directory 权限。

使用 ADSI Edit 管理单元或 LDP 实用程序时，必须修改以下 Active Directory 对象属性的权限。

- 要根据其进行查询的域的域命名上下文根。
- 包含要根据其查询邮件信息的用户的所有 OU 和 CN 对象。

下表显示了要应用到所需容器的所需权限。

用户对象	权限	遗产	权限类型
ANONYMOUS LOGON	列出内容	容器对象	对象
ANONYMOUS LOGON	列出内容	组织单位对象	对象
ANONYMOUS LOGON	读取公共信息	用户对象	特性
ANONYMOUS LOGON	读取电话和邮件选项	用户对象	特性

步骤 2 设置 Active Directory 权限

- 打开 Windows 2000 支持工具中的 ADSIEdit。
- 找到**域命名上下文 (Domain Naming Context)** 文件夹。此文件夹包含域的 LDAP 路径。
- 右键点击**域命名上下文 (Domain Naming Context)** 文件夹，然后点击**属性 (Properties)**。
- 点击 **Security**。
- 点击 **Advanced**。
- 点击 **Add**。
- 点击**用户对象 (User Object)**“ANONYMOUS LOGON”，然后点击**确定 (OK)**。
- 点击**权限类型 (Permission Type)** 选项卡。
- 点击**应用到 (Apply onto)** 框中的**继承 (Inheritance)**。
- 点击以选中**权限 (Permission)** 对应的**允许 (Allow)** 复选框。

步骤 3 配置思科邮件网关

使用**系统管理 > LDAP** 页（或 CLI 中的 **`ldapconfig`**）创建包含下列信息的 LDAP 服务器条目。

- Active Directory 或 Exchange 服务器的主机名
- 端口 3268
- 与域的根命名上下文匹配的基本 DN
- 基于密码的身份验证类型，使用 cn=anonymous 作为用户且密码为空

Active Directory 实施说明

- Active Directory 服务器在端口 3268 和 389 上接受 LDAP 连接。用于访问全局目录的默认端口是 3268。
- Active Directory 服务器在端口 636 和 3269 上接受 LDAPS 连接。Microsoft 在 Windows Server 2003 及更高版本上支持 LDAPS。
- 设备应连接到还作为全局目录的域控制器，以便使用同一台服务器对不同的基本 DN 执行查询。
- 在 Active Directory 中，可能需要为“Everyone”组授予对目录对象的读取权限，以便实现成功的查询。这包括域命名上下文的根。
- 通常，在许多 Active Directory 实施中 mail 属性条目的值具有匹配的“ProxyAddresses”属性条目值。
- 基础设施中可相互识别的 Microsoft Exchange 环境通常在彼此之间路由邮件，不会路由回原始 MTA。

测试 LDAP 查询

使用每个查询类型对应的“添加 LDAP 服务器配置文件”(Add LDAP Server Profile)/“编辑 LDAP 服务器配置文件”(Edit LDAP Server Profile) 页面上的“测试查询 (Test Query) 按钮（或 CLI 中的 `test` 子命令）来测试对配置的 LDAP 服务器的查询。除了显示结果之外，AsyncOS 还显示有关查询连接测试每个阶段的详细信息。可以测试每个查询类型。

`ldaptest` 命令以批处理命令的形式提供，例如：

```
ldaptest LDAP.ldapaccept foo@ironport.com
```

如果在 LDAP 服务器属性的“主机名”(Host Name) 字段中输入了多个主机，则设备会在每个 LDAP 服务器上测试查询。

表 *62:* 测试 *LDAP* 查询

查询类型	如果收件人匹配 (PASS)...	如果收件人不匹配 (FAIL)...
收件人接受（接受，`ldapaccept`）	接受邮件.	收件人无效：会话、延迟退回或根据侦听程序设置删除邮件。DHAP: 删除。
路由（路由，`ldaprouting`）	根据查询设置进行路由。	继续处理邮件。
伪装（伪装，`masquerade`）	使用查询定义的变量映射修改信头。	继续处理邮件。
组成员身份（组，`ldapgroup`）	为邮件过滤器规则返回“true”。	为邮件过滤器规则返回“false”。

查询类型	如果收件人匹配 (PASS)...	如果收件人不匹配 (FAIL)...
SMTP Auth （SMTP 身份验证，`smtpauth`）	从 LDAP 服务器返回密码，并将其用于身份验证；发生 SMTP 身份验证。	不会进行任何密码匹配；SMTP 身份验证尝试失败。
外部身份验证 (`externalauth`)	单独为绑定、用户记录和用户的组成员身份分别返回“match positive”。	单独为绑定、用户记录和用户的组成员身份分别返回“match negative”。
垃圾邮件隔离区终端用户身份验证 (`isqauth`)	为终端用户帐户返回“match positive”。	不会进行任何密码匹配；终端用户身份验证尝试失败。
垃圾邮件隔离区别名整合 (`isqalias`)	返回将整合的垃圾邮件通知发送到的邮件地址。	不会进行任何垃圾邮件通知整合。

注释 为查询输入的变量名称区分大小写，且必须与 LDAP 实施匹配才能正常工作。例如，在提示符处输入 **mailLocalAddress** 执行的查询与输入 **maillocaladdress** 执行的查询是不同的。思科系统公司强烈建议使用 ldapconfig 命令的 test 子命令来测试所构建的所有查询，并确保返回正确结果。

排除 LDAP 服务器连接故障

如果设备无法连接 LDAP 服务器，将会显示下列错误之一：

- `Error: LDAP authentication failed: <LDAP Error "invalidCredentials" [0x31]>`
- `Error: Server unreachable: unable to connect`
- `Error: Server unreachable: DNS lookup failure`

请注意，可能由于在服务器配置中输入了错误的端口或端口无法在防火墙中打开，无法连接到服务器。LDAP 服务器通常通过端口 3268 或 389 通信。Active Directory 使用端口 3268 访问在多服务器环境中使用的全局目录（有关详细信息，请参阅“防火墙信息”附录。）在 AsyncOS 4.0 中，添加了通过 SSL 与 LDAP 服务器通信（通常通过端口 636）的功能。有关详细信息，请参阅安全 LDAP (SSL)，第 595 页。

也可能由于输入的主机名无法解析，无法连接服务器。

可以使用“添加/编辑 LDAP 服务器配置文件”页面上的测试服务器（或 CLI 中 `ldapconfig` 命令的 `test` 子命令）测试与 LDAP 服务器的连接。有关详细信息，请参阅测试 LDAP 服务器，第 589 页。

如果LDAP服务器无法访问:

- 如果在工作队列中启用了 LDAP 接受、伪装或路由，则邮件会保留在工作队列中。
- 如果未启用 LDAP 接受，但在过滤器中使用了其他查询（组策略检查等），则过滤器求值为 False。

使用接受查询进行收件人验证

可以使用现有 LDAP 基础设施来定义如何处理传入邮件的收件人邮件地址（在公共侦听程序中）。设备下次查询目录服务器时，在目录中对用户数据的更改会更新。可以指定缓存的大小以及设备存储其检索到的数据的时间。

注释 您可能希望绕过对特殊收件人的 LDAP 接受查询（例如 administrator@example.com）。可以在收件人访问表 (RAT) 中配置此设置。有关配置此设置的信息，请参阅“配置网关以接收邮件”一章。

接受查询示例

下表显示了接受查询示例。

表 *63:* 常规 *LDAP* 实施的 *LDAP* 查询字符串示例：接受

查询内容：	收件人验证

OpenLDAP	`(mailLocalAddress={a})`
	`(mail={a})`
	`(mailAlternateAddress={a})`

Microsoft Active Directory 通讯录 **Microsoft Exchange**	`(|(mail={a})(proxyAddresses=smtp:{a}))`

SunONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

Lotus NotesLotus Domino	`(|(|(mail={a})(uid={u}))(cn={u}))` `(|(ShortName={u})(InternetAddress={a})(FullName={u}))`

还可以验证用户名（左侧）。如果目录不包含要接受其邮件的所有域，则该验证非常有用。将接受查询设置为 (uid={u})。

为 Lotus Notes 配置接受查询

请注意，LDAPACCEPT 和 Lotus Notes 存在潜在问题。如果 Notes LDAP 包含具有如下属性的人员：

```
mail=juser@example.com

cn=Joe User

uid=juser

cn=123456

location=New Jersey
```

Lotus 会接受此人各种不同格式邮件地址而不是指定地址的邮件，例如“Joe_User@example.com”-其在 LDAP 中不存在。因此 AsyncOS 可能找不到该用户的所有有效的用户邮件地址。

一个可能的解决方案是尝试发布其他格式的地址。请联系 Lotus Notes 管理员以获得更多详细信息。

使用路由查询将邮件发送到多个目标地址

AsyncOS 支持别名扩展（具有多个目标地址的 LDAP 路由）。AsyncOS 会将原始邮件替换为针对每个别名目标的新的单独邮件（例如，recipient@yoursite.com 可能会替换为发送到 newrecipient1@hotmail.com 和 recipient2@internal.yourcompany.com 等的新的单独邮件）。路由查询有时在其他邮件处理系统中称为别名查询。

路由查询示例

表 *64:* 常规 *LDAP* 实施的 *LDAP* 查询字符串示例：路由

查询内容：	路由到其他邮件主机
OpenLDAP	`(mailLocalAddress={a})`
Microsoft Active Directory 通讯录 **Microsoft Exchange**	可能不适用

SunONE Directory Server	`(mail={a})`
	`(mailForwardingAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailRoutingAddress={a})`
	`(otherMailbox={a})`
	`(rfc822Mailbox={a})`

Active Directory 实施可以具有与 `proxyAddresses` 属性对应的多个条目，但是由于 AD 会将该属性值格式化为 `smtp:user@domain.com`，因此该数据无法用于 LDAP 路由/别名扩展。每个目标地址必须在单独的 `attribute:value` 对中。基础设施中可相互识别的 Microsoft Exchange 环境通常在彼此之间路由邮件，不会路由回原始 MTA。

路由：MAILHOST 和 MAILROUTINGADDRESS

对于路由查询，MAILHOST 的值不能是 IP 地址；它必须是可解析的主机名。这通常需要使用内部 DNSconfig。

MAILHOST 对于路由查询是可选的。如果未设置 MAILHOST，则 MAILROUTINGADDRESS 是必需项。

使用伪装查询重写信封发件人

伪装是根据构建的查询重写邮件中的信封发件人（也称为发件人或 MAIL FROM）以及 To:、From: 和/或CC: 信头的一项功能。该功能的一个典型实施示例是允许从一个站点托管多个域的“虚拟域”。另一个典型实施是通过从邮件信头的字符串中“拆离”子域来“隐藏”网络基础设施。

伪装查询示例

表 *65:* 常规 *LDAP* 实施的 *LDAP* 查询字符串示例：伪装

查询内容：	伪装
OpenLDAP	`(mailRoutingAddress={a})`
Microsoft Active Directory 通讯录	`(proxyaddresses=smtp:{a})`

SunONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

伪装“友好名称”

在一些用户环境中，LDAP 目录服务器方案除了存储邮件路由地址或本地邮件地址外，可能还存储“友好名称”。AsyncOS 允许通过“友好地址”来伪装信封发件人（对于传出邮件）和邮件信头（对于传入邮件，如“收件人:”(To:)、“回复:”(Reply To:)、“发件人:”(From:) 或“抄送:”(CC:)）- 即使友好地址包含有效地址中通常不允许的特殊字符（例如引号、空格和逗号）也是如此。

当通过 LDAP 查询使用伪装信头时，现在可以选择配置是否将整个友好邮件字符串替换为 LDAP 服务器中的结果。请注意，即使启用了该行为，也只能将 user@domain 部分用于信封发件人（友好名称是非法的）。

与常规 LDAP 伪装一样，如果 LDAP 查询返回空结果（长度为零或全部为空格），则不会发生伪装。

要启用此功能，请在为侦听程序配置基于 LDAP 的伪装查询（通过“LDAP”页面或 `ldapconfig` 命令）时，对以下问题回答“y”：

```
Do you want the results of the returned attribute to replace the entire
friendly portion of the original recipient? [N]
```

例如，考虑以下 LDAP 条目示例：

属性	值
mailRoutingAddress	admin\@example.com
mailLocalAddress	joe.smith\@example.com
mailFriendlyAddress	“Administrator for example.com”，<joe.smith\@example.com>

如果启用了此功能，则 (mailRoutingAddress={a}) 的 LDAP 查询和 (mailLocalAddress) 的伪装属性将导致以下替换：

原始地址（发件人、收件人、抄送、回复）	伪装的信头	伪装的信封发件人
admin@example.com	发件人：“Administrator for example.com”，<joe.smith@example.com>	MAIL FROM：<joe.smith@example.com>

使用组 LDAP 查询确定收件人是否为组成员

可以定义对 LDAP 服务器的查询以确定收件人是否为 LDAP 目录所定义的组的成员。

步骤 1 创建使用 rcpt-to-group 或 mail-from-group 规则对邮件执行操作的邮件过滤器。

步骤 2 然后，使用**系统管理 > LDAP** 页面（或 **ldapconfig** 命令）为要绑定到的设备定义 LDAP 服务器并为组成员配置查询。

步骤 3 使用**网络 > 侦听程序**页面（或 **listenerconfig -> edit -> ldapgroup** 子命令）为侦听程序启用组查询。

组查询示例

表 *66:* 常规 *LDAP* 实施的 *LDAP* 查询字符串示例：组

查询内容：	**Group**
OpenLDAP	默认情况下，OpenLDAP 不支持 memberOf 属性。LDAP 管理员可以将此属性或类似属性添加到方案。
Microsoft Active Directory	`(&(memberOf={g})(proxyAddresses=smtp:{a}))`
SunONE Directory Server	`(&(memberOf={g})(mailLocalAddress={a}))`

例如，假定您的 LDAP 目录将“营销”组的成员归类为 ou=Marketing。可以使用此分类来处理以特殊方式发送给或来自该组成员的邮件。第 1 步会创建邮件过滤器以对邮件执行操作，并且第 2 步和第 3 步会启用 LDAP 查询机制。

配置组查询

在下面的示例中，来自营销组成员的邮件（如 LDAP 组“营销”所定义）将传输到备用传输主机 `marketingfolks.example.com`。

步骤 1 首先，会创建邮件过滤器以对与组成员身份积极匹配的邮件执行操作。在本示例中，使用 `mail-from-group` 规则创建了过滤器。其信封发件人在 LDAP 组“marketing-group1”中的所有邮件都通过备用传输主机进行传输（过滤器 `alt-mailhost` 操作）。

组成员身份字段变量 (groupName) 将在第 2 步中定义。组属性“groupName”使用值 `marketing-group1` 定义。

```
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.
MarketingGroupfilter:
if (mail-from-group == "marketing-group1") {
alt-mailhost ('marketingfolks.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.

[]>
```

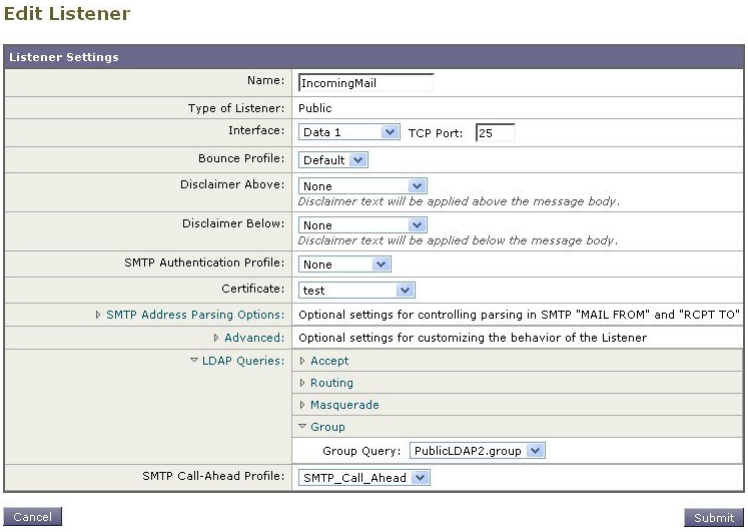
有关 `mail-from-group` 和 `rcpt-to-group` 邮件过滤器规则的详细信息，请参阅邮件过滤器规则，第 118 页。

步骤 2 接下来，使用“添加 LDAP 服务器配置文件”(Add LDAP Server Profile) 页面为要绑定到的设备定义 LDAP 服务器，并为组成员身份配置初始查询。

步骤 3 接下来，公共侦听程序“InboundMail”更新为将 LDAP 查询用于组路由。使用“编辑侦听程序”(Edit Listener) 页面启用上面指定的 LDAP 查询。

由于此查询，侦听程序所接受的邮件会触发对 LDAP 服务器的查询以确定组成员身份。PublicLDAP2.group 查询先前通过**系统管理 > LDAP** 页定义。

图 ***63:*** 在侦听程序上指定组查询



步骤 4 提交并确认更改。

示例：使用组查询跳过垃圾邮件和病毒检查

由于邮件过滤器是渠道的早期阶段运行，因此可以使用组查询跳过对指定组的病毒和垃圾邮件检查。例如，您希望 IT 组接收所有邮件并跳过垃圾邮件和病毒检查。在 LDAP 记录中，创建一个使用 DN 作为组名称的组条目。组名称中包含下列 DN 条目：

cn=IT, ou=groups, o=sample.com

通过下列组查询创建 LDAP 服务器配置文件：

(&(memberOf={g})(proxyAddresses=smtp:{a}))

然后在侦听程序中启用此查询，以便在侦听程序收到邮件时，会触发组查询。

要为 IT 组的成员跳过病毒和垃圾邮件过滤，可以创建以下邮件过滤器，从而将传入邮件与 LDAP 组进行比较。

```
[]> - NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

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

IT_Group_Filter:

if (rcpt-to-group == "cn=IT, ou=groups, o=sample.com"){

skip-spamcheck();

skip-viruscheck();

deliver();

}

.
1 filters added.
```

注释 此邮件过滤器中的 rcpt-to-group 反映作为组名称输入的 DN：cn=IT，ou=groups，o=sample.com。确认在邮件过滤器中使用了正确的组名称，以确保过滤器与 LDAP 目录中的名称匹配。

侦听程序所接受的邮件会触发对 LDAP 服务器的查询以确定组成员身份。如果邮件收件人是 IT 组的成员，则邮件过滤器会跳过病毒和垃圾邮件检查并将邮件发送给收件人。要启用该过滤器以检查 LDAP 查询的结果，必须在 LDAP 服务器上创建 LDAP 查询并在侦听程序上启用该 LDAP 查询。

使用基于域的查询路由到特定域

基于域的查询是按类型分组的 LDAP 查询，它们与域相关联，并且分配给特定侦听程序。如果有不同的 LDAP 服务器与不同的域关联，但是要为同一侦听程序上的所有 LDAP 服务器运行查询，则可能需要使用基于域的查询。例如，公司“MyCompany”收购了公司“HisCompany”和公司“HerCompany”，而且 MyCompany 保留其域 MyCompany.example.com 以及所收购公司的域 HisCompany.example.com 和 HerCompany.example.com，其为与每个域相关联的员工维护不同的 LDAP 服务器。要接受这三个域的邮件，MyCompany 会创建基于域的查询。这允许 MyCompany.example.com 在同一侦听程序上接受 Mycompany.example.com、HisCompany.example.com 和 HerCompany.example.com 的邮件。

步骤 1 为要在基于域的查询中使用的域创建服务器配置文件。对于每个服务器配置文件，配置要用于基于域的查询的查询（接受、路由等）。有关详细信息，请参阅创建 LDAP 服务器配置文件以存储有关 LDAP 服务器的信息，第 588 页。

步骤 2 创建基于域的查询。创建基于域的查询时，从每个服务器配置文件中选择查询，并使设备根据“Envelope To”字段中的域确定要运行的查询。有关创建查询的详细信息，请参阅创建基于域的查询，第 608 页。

步骤 3 在公共或专用侦听程序上启用基于域的查询。有关配置侦听程序的详细信息，请参阅“配置网关以接收邮件”一章。

注释 还可以启用对垃圾邮件隔离区的LDAP最终用户访问或垃圾邮件通知启用基于域的查询。有关详细信息，请参阅“垃圾邮件隔离区”一章。

创建基于域的查询

从“系统管理”(System Administration)>“LDAP”>“LDAP 服务器配置文件”(LDAP Server Profiles)页面创建基于域的查询。

步骤 1 从“LDAP 服务器配置文件 (LDAP Server Profiles)”页面上，点击**高级 (Advanced)**。

步骤 2 点击**添加域分配 (Add Domain Assignments)**。

步骤 3 输入基于域的查询的名称。

步骤 4 选择查询类型。

注释 创建基于域的查询时，无法选择不同类型的查询。选择某种查询类型后，设备将使用可用服务器配置文件中该类型的查询来填充查询字段。

步骤 5 在“域分配 (Domain Assignments)”字段中，输入域。

步骤 6 选择要与域关联的查询。

步骤 7 继续添加行，直到将所有域添加到查询。

步骤 8 如果所有其他查询失败，可以输入默认查询。如果不希望输入默认查询，请选择**无 (None)**。

步骤 9 通过点击“测试查询”按钮并在测试参数字段中输入要测试的用户登录名和密码或者邮件地址，以测试查询。结果会显示在“连接状态”(Connection Status) 字段中。

步骤 10 或者，如果在接受查询使用 {f} 令牌，则可以将信封发件人地址添加到测试查询。

注释 创建了基于域的查询后，需要将其与公共或专用侦听程序相关联。

步骤 11 提交并确认更改。

使用链查询执行一系列 LDAP 查询

链查询是设备连续尝试运行的一系列LDAP查询。设备会尝试运行“链”中的每个查询，直到LDAP服务器返回正面响应（或者“链”中最后一个查询返回负面响应或失败）。对于链接的路由查询，设备会按顺序对每个重写的邮件地址重新运行已配置的相同链查询。如果 LDAP 目录中的条目使用不同的属性存储相似（或相同）的值，则链查询会非常有用。例如，您可能已经使用属性 maillocaladdress 和 mail 存储用户邮件地址。为了确保查询根据这两个属性行，可以使用链查询。

步骤 1 为要在链查询中使用的每个查询创建服务器配置文件。对于每个服务器配置文件，配置要用于链查询的查询。有关详细信息，请参阅创建 LDAP 服务器配置文件以存储有关 LDAP 服务器的信息，第 588 页。

步骤 2 创建链查询。有关详细信息，请参阅创建链查询，第 609 页。

步骤 3 在公共或专用侦听程序上启用链查询。有关配置侦听程序的详细信息，请参阅“配置网关以接收邮件”一章。

注释 还可以启用对垃圾邮件隔离区的LDAP最终用户访问或垃圾邮件通知启用基于域的查询。有关详细信息，请参阅“垃圾邮件隔离区”一章。

创建链查询

从“系统管理”(System Administration)>“LDAP”>“LDAP 服务器配置文件”(LDAP Server Profiles)页面创建链查询。

步骤 1 从“LDAP 服务器配置文件 (LDAP Server Profiles)”页面上，点击**高级 (Advanced)**。

步骤 2 点击**添加链查询 (Add Chain Query)**。

步骤 3 添加链查询的名称。

步骤 4 选择查询类型。

创建链查询时，无法选择不同类型的查询。选择某种查询类型后，设备将使用可用服务器配置文件中该类型的查询来填充查询字段。

步骤 5 选择查询以添加到链查询。

设备会按照配置顺序运行查询。因此，如果将多个查询添加到链查询，则可能需要对它们进行排序，以便更常规的查询在更具体的查询之后。

步骤 6 通过点击“测试查询”按钮并在测试参数字段中输入要测试的用户登录名和密码或者邮件地址，以测试查询。结果会显示在“连接状态”(Connection Status) 字段中。

步骤 7 或者，如果在接受查询使用 {f} 令牌，则可以将信封发件人地址添加到测试查询。

注释 创建了链查询后，需要将其与公共或专用侦听程序相关联。

步骤 8 提交并确认更改。

将 LDAP 用于目录搜集攻击预防

当恶意发件人尝试向具有通用名称的收件人发送邮件时，邮件网关通过验证该位置具有有效有效的收件人进行响应。当大规模执行时，恶意发件人通过“搜集”要发送垃圾邮件的有效地址，可以确定向谁发送邮件。

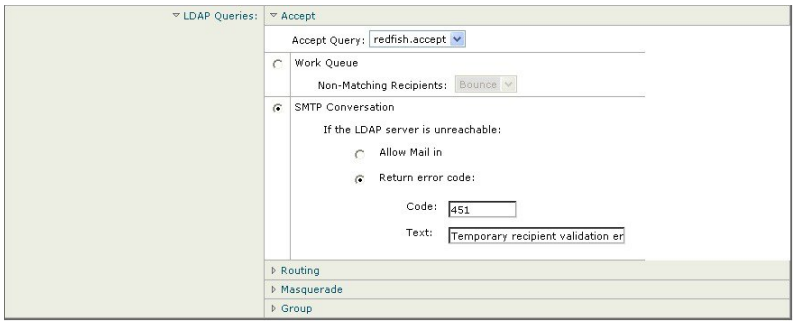
当使用 LDAP 接受验证查询时，邮件安全设备可以检测和阻止目录搜集攻击 (DHA)。可以在 SMTP 会话期间或在工作队列中配置 LDAP 接受以阻止目录搜集攻击。

SMTP 会话期间的目录搜集攻击预防

可以通过仅输入收件人访问表 (RAT) 中的域并在 SMTP 会话中执行 LDAP 接受验证来阻止 DHA。

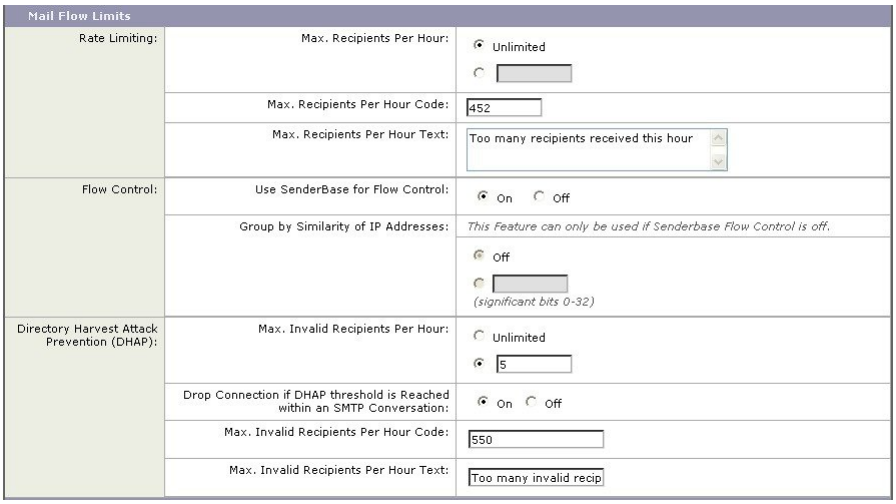
要在 SMTP 会话期间删除邮件，请为 LDAP 接受配置 LDAP 服务器配置文件。然后，配置侦听程序以在 SMTP 会话期间执行 LDAP 接受查询。

图 *64:* 配置 *SMTP* 会话期间的接受查询



为侦听程序配置了 LDAP 接受查询后，必须在与侦听程序关联的邮件流策略中配置 DHAP 设置。

图 *65:* 配置邮件流策略以删除 *SMTP* 会话中的连接



在与侦听程序关联的邮件流策略中，配置以下目录搜集攻击预防设置：

- **每小时的最大无效收件人数量 (Max. Invalid Recipients Per hour)**。此侦听程序每小时将从远程主机接收的最大无效收件人数。此阈值表示 RAT 拒绝总数与在 SMTP 会话中删除或在工作队列中退回的无效 LDAP 收件人邮件的总数相结合的结果。例如，将阈值配置为 5，且计数器检测两个 RAT 拒绝和三个到无效 LDAP 收件人的已删除邮件。此时，设备确定已达到阈值，并放弃连接。默认情况下，公共侦听程序的每小时最大收件人数量为 25。对于专用侦听程序，默认情况下的每小时最大收件人数量无限制。将其设置为“无限制”(Unlimited) 表示不为邮件流策略启用 DHAP。

- **如果在 SMTP 会话中达到 DHAP 阈值，则放弃连接 (Drop Connection if DHAP Threshold is reached within an SMTP conversation)**。将设备配置为在达到目录搜集攻击预防阈值时放弃连接。
- **每小时最大收件人数代码 (Max. Recipients Per Hour Code)**。指定在放弃连接时使用的代码。默认代码为 550。
- **每小时最大收件人数文本 (Max. Recipients Per Hour Text)**。指定用于放弃的连接的文本。默认文本为“无效收件人过多”(Too many invalid recipients)。

如果达到阈值，当收件人无效时，邮件的信封发件人不会收到退回邮件。

工作队列中的目录搜集攻击防御

可以通过仅输入收件人访问表 (RAT) 中的域并在工作队列中执行 LDAP 接受来阻止大多数 DHA。该技术可防止恶意发件人在 SMTP 会话期间知道收件人是否有效。（如果配置了接受查询，系统会接受邮件并在工作队列中执行 LDAP 接受验证。）但是，当收件人无效时，邮件的信封发件人仍会收到退回邮件。

在工作队列中配置 Directory Harvest Prevention

要阻止目录搜集攻击，首先应配置 LDAP 服务器配置文件，并启用 LDAP 接受。启用了 LDAP 接受查询后，将侦听程序配置为使用接受查询且为不匹配收件人的退回件：

接下来，配置邮件流策略以定义系统将根据特定时段的发送 IP 地址允许的无效收件人地址数。当超过该数字时，系统会将这种情况视为 DHA 并发送警报邮件。警报邮件将包含以下信息：

```
LDAP: Potential Directory Harvest Attack from host=('IP-address', 'domain_name
'), dhap_limit=n, sender_group=sender_group,


listener=listener_name, reverse_dns=(reverse_IP_address, 'domain_name
', 1), sender=envelope_sender, rcpt=envelope_recipients
```

系统将退回邮件，直到达到在邮件流策略中指定的阈值，然后以静默方式接收和丢弃其余邮件，从而通知合法发件人地址是错误的，但是避免恶意发件人确定哪些收件人被接受。

此无效收件人计数器的功能类似于 AsyncOS 中当前提供的速率限制功能：启用该功能并定义限制作为公共侦听程序 HAT 中邮件流策略的一部分（包括 HAT 的默认邮件流策略）。

还可以在命令行界面中使用 `listenerconfig` 命令配置此功能。

在 GUI 中编辑任何邮件流策略时也会显示该功能，只要在对应的侦听程序上配置了 LDAP 查询即可：

输入每小时无效收件人数量可为该邮件流策略启用 DHAP。默认情况下，公共侦听程序允许每小时 25 个无效收件人。对于专用侦听程序，默认情况下的每小时最大无效收件人数量无限制。将其设置为“无限制”(Unlimited) 表示不为邮件流策略启用 DHAP。

配置 AsyncOS 进行 SMTP 身份验证

AsyncOS 支持 SMTP 身份验证。SMTP 身份验证是用于验证连接到 SMTP 服务器的客户端的一种机制。

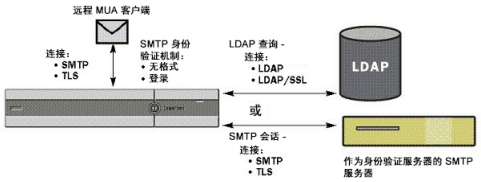
该机制的实用之处是：使给定组织中的用户可以使用该实体的邮件服务器发送邮件，即使他们利用远程连接（例如在家中或在旅行时）也是如此。邮件用户代理(MUA)可以在尝试发送邮件时发出身份验证请求（挑战/响应）。

用户还可以使用 SMTP 身份验证进行传出邮件中继。这允许设备在不位于网络边缘的配置中与中继服务器建立安全连接。

AsyncOS 支持两种验证用户凭据的方法：

- 可以使用 LDAP 目录。
- 您可以使用其他 SMTP 服务器（SMTP Auth 转发和 SMTP Auth 传出）。

图 *66: SMTP Auth* 支持：*LDAP* 目录存储或 *SMTP* 服务器



然后使用配置的 SMTP 身份验证方法，通过 smtpauthconfig 命令创建 SMTP Auth 配置文件以在 HAT 邮件流策略中使用（请参阅在侦听程序上启用 SMTP 身份验证，第 615 页）。

配置 SMTP 身份验证

如果要通过 LDAP 服务器进行身份验证，请在“添加 LDAP 服务器配置文件”或“编辑 LDAP 服务器配置文件”页面上（或在 **`ldapconfig`** 命令中）选择 SMTPAUTH 查询类型以创建 SMTP 身份验证查询。对于配置的每个 LDAP 服务器，可以配置一个 SMTPAUTH 查询以用作 SMTP 身份验证配置文件。

有两种 SMTP 身份验证查询：LDAP 绑定和密码作为属性。当使用密码作为属性时，设备会获取 LDAP 目录中的密码字段。密码可以以纯文本、加密或散列的形式存储。使用 LDAP 绑定时，设备将尝试使用客户端提供的凭据登录到 LDAP 服务器。

指定密码作为属性

根据 RFC 2307，OpenLDAP 中的约定是：用花括号将编码类型括起来作为编码密码的前缀（例如，“{SHA}5en6G6MezRroT3XKqkdPOmY/BfQ=”）。在本例中，应用 SHA 后，密码部分是纯文本密码的 base64 编码。

在获取密码之前，设备与 MUA 协商 SASL 机制，而且设备和 MUA 会决定采用的方法（支持 LOGIN、PLAIN、MD5、SHA、SSHA 和 CRYPT SASL 机制）。然后，设备会查询 LDAP 数据库以获取密码。在 LDAP 中，密码可以具有扩展花括号中的前缀。

- 如果没有前缀，则设备假设密码是以纯文本形式存储在 LDAP 中。
- 如果有前缀，设备将获取哈希密码，对 MUA 提供的用户名和/或密码执行哈希，然后比较哈希版本。根据将散列机制类型附加到密码字段中的散列密码的 RFC 2307 约定，设备支持 SHA1 和 MD5 散列类型。
- 诸如 OpenWave LDAP 服务器等一些 LDAP 服务器不会在加密密码之前附加加密类型前缀；相反，它们将加密类型存储为单独的 LDAP 属性。在这些情况下，可以指定将密码与 SMTP 会话中包含的密码进行比较时设备将使用的默认 SMTP AUTH 加密方法。

设备从 SMTP Auth 交换中获取任意用户名，并将其转换为获取明文或哈希密码字段的 LDAP 查询。然后，它对在 SMTP Auth 凭证中提供的密码执行必要的哈希并将结果与其从 LDAP 检索到的结果（如有哈希类型标记，则将其删除）进行比较。如果结果匹配，则表示 SMTP Auth 会话将继续。匹配失败将产生错误代码。

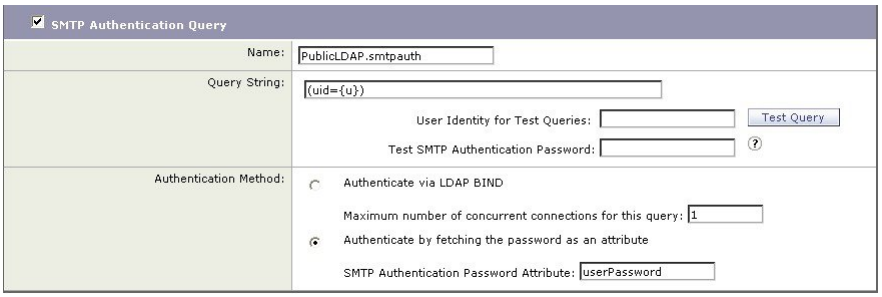
配置 SMTP 身份验证查询

表 *67: SMTP Auth LDAP* 查询字段

名称	查询的名称。
查询字符串	可以选择是通过 LDAP 绑定进行身份验证，还是获取密码作为属性。 **绑定**：尝试使用客户端提供的凭据登录到 LDAP 服务器（这称为 LDAP 绑定）。 指定 SMTP Auth 查询将使用的最大并发连接数。此号码不应超过在上述 LDAP 服务器属性中指定的数量。请注意，为了避免绑定身份验证出现大量会话超时，请增加此处的最大并发连接数（通常接近可分配到 SMTP Auth 的所有连接数）。新的连接将用于每个绑定身份验证。连接的其余部分将与其他 LDAP 查询类型共享。 **密码作为属性**：要通过获取密码进行身份验证，请在下面的 SMTP Auth 密码属性字段中指定密码。 指定用于任何一种身份验证的 LDAP 查询。Active Directory 示例查询：(&(samaccountname={u})(objectCategory=person)(objectClass=user))
SMTP 身份验证密码属性	如果选择了“通过获取密码作为属性进行身份验证”，可以在此处指定密码属性。

在下面的示例中，“系统管理”(System Administration)>“LDAP”页面用于编辑名为“PublicLDAP”的 LDAP 配置以包括 SMTPAUTH 查询。将构建查询字符串 (uid={u}) 来匹配 userPassword 属性。

图 *67: SMTP* 身份验证查询



当配置了 SMTPAUTH 配置文件后，可以指定侦听程序使用该查询进行 SMTP 身份验证。

通过另一个 SMTP 服务器进行 SMTP 身份验证（带转发的 SMTP 身份验证）

可以配置设备来验证提供给与其他 SMTP 服务器进行的其他 SMTP 身份验证会话的用户名和密码。

身份验证服务器不是传输邮件的服务器；相反，它只对 SMTP 身份验证请求做出响应。如果身份验证成功，则可通过专用邮件服务器继续进行 SMTP 邮件传输。此功能有时称为“带转发的 SMTP 身份验证”，因为仅会将凭据转发（或“代理”）到另一个 SMTP 服务器进行身份验证。

步骤 1 依次选择**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**。

步骤 2 点击**添加配置文件 (Add Profile)**。

步骤 3 为 SMTP 身份验证配置文件输入唯一的名称。

步骤 4 对于**配置文件类型 (Profile Type)**，选择**转发 (Forward)**。

步骤 5 点击 **Next**。

步骤 6 输入转发服务器的主机名/IP 地址和端口。选择用于转发身份验证请求的转发接口。指定最大同时连接数。然后，可以配置是否需要 TLS 以从设备连接到转发服务器。此外，如果可用，还可以选择要使用的 SASL 方法（PLAIN 或 LOGIN）。此选择配置用于每个转发服务器。

步骤 7 提交并确认更改。

步骤 8 创建了身份验证配置文件后，可以在侦听程序上启用该配置文件。有关详细信息，请参阅在侦听程序上启用SMTP身份验证，第 615 页。

通过 LDAP 进行 SMTP 身份验证

要创建基于 LDAP 的 SMTP 身份验证配置文件，必须先前已使用“系统管理”(System Administration) >“LDAP”页面创建了与 LDAP 服务器配置文件相结合的 SMTP 身份验证查询。然后，可以使用此配置文件创建 SMTP 身份验证配置文件。有关创建 LDAP 配置文件的详细信息，请参阅了解 LDAP 查询，第 586 页。

步骤 1 依次选择**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**。

步骤 2 点击**添加配置文件 (Add Profile)**。

步骤 3 为 SMTP 身份验证配置文件输入唯一的名称。

步骤 4 对于“配置文件类型”(Profile Type)，选择 **LDAP**。

步骤 5 点击 **Next**。

步骤 6 选择要用于此身份验证配置文件的 LDAP 查询。

步骤 7 从下拉菜单中选择默认加密方法。可以从 SHA、Salted SHA、Crypt、Plain 或 MD5 中进行选择。如果 LDAP 服务器在加密密码前面加上加密类型前缀，请将“无”保持选中状态。如果 LDAP 服务器将加密类型作为单独的实体（例如，OpenWave LDAP 服务器）保存，请从菜单中选择一种加密方法。如果 LDAP 查询使用的是绑定，则不会使用默认加密设置。

步骤 8 点击 **Finish**。

步骤 9 提交并确认更改。

步骤 10 创建了身份验证配置文件后，可以在侦听程序上启用该配置文件。有关详细信息，请参阅在侦听程序上启用SMTP身份验证，第 615 页。

在侦听程序上启用 SMTP 身份验证

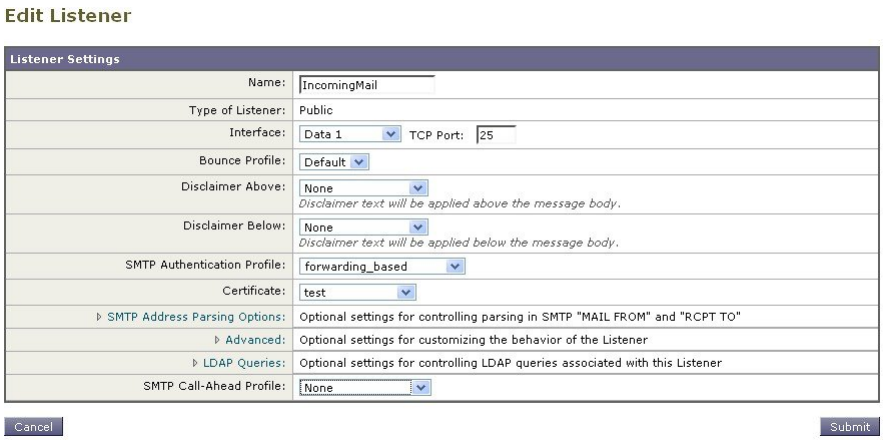
在使用**网络 > SMTP 身份验证**页面创建了用于指定要执行的 SMTP 身份验证类型（基于 LDAP 或基于 SMTP 转发）的 SMTP 身份验证“配置文件”后，必须使用**网络 > 侦听程序**页面（或 **`listenerconfig`** 命令）将该配置文件与侦听程序相关联。

注释 经过身份验证的用户将在其当前邮件流策略中获得 RELAY 连接行为。

可以在配置文件中指定多个转发服务器。SASL 机制 CRAM-MD5 和 DIGEST-MD5 在设备和转发服务器之间不受支持。

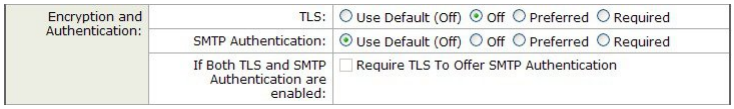
在下面的示例中，编辑了侦听程序“InboundMail”以使用通过“编辑侦听程序”(Edit Listener) 页面配置的 SMTPAUTH 配置文件。

图 *68:* 通过“编辑侦听程序”*(Edit Listener)* 页面选择 *SMTP* 身份验证配置文件



配置了某个侦听程序以使用配置文件后，可以更改主机访问表的默认设置，以使侦听程序允许、禁止或要求 SMTP 身份验证：

图 *69:* 在邮件流策略上启用 *SMTP* 身份验证



编号	说明
1.	“SMTP 身份验证”(SMTP Authentication) 字段为 SMTP 身份验证提供侦听程序级别的控制。如果选择“否”(No)，则不会在侦听程序上启用身份验证，不管配置任何其他 SMTP 身份验证设置都是如此。
2.	如果在第二个提示符（“SMTP 身份验证：”[SMTP Authentication:]）选择“必填”(Required)，则不会发出任何 AUTH 关键字，直到协商 TLS（客户端发出第二个 EHLO 命令）为止。

SMTP 身份验证和 HAT 策略设置

由于在 SMTP 身份验证协商开始之前发件人分为适当的发件人组，因此主机访问表 (HAT) 设置不会受到影响。当连接远程邮件主机时，设备会先确定应用哪个发件人组并对该发件人组施加邮件策略。例如，如果远程 MTA“suspicious.com”在您的 SUSPECTLIST 发件人组中，则会应用 THROTTLE 策略，不管“suspicious.com”的 SMTPAUTH 协商结果如何都是如此。

但是，不使用 SMTPAUTH 进行身份验证的发件人将得到与“正常”发件人不同的对待。成功 SMTPAUTH 会话的连接行为会更改为“RELAY”，从而有效地绕过收件人访问表 (RAT) 和 LDAPACCEPT。这允许发件人通过设备中转邮件。如上所述，应用的任何速率限制或限制都将继续有效。

HAT 延迟的拒绝

当配置了 HAT 延迟的拒绝时，根据 HAT 发件人组喝邮件流策略配置将被丢弃的连接可能仍能够成功进行身份验证并获得 RELAY 邮件流策略授权。

配置是否在邮件收件人级别执行 HAT 拒绝。默认情况下，HAT 拒绝的连接将关闭，并且在 SMTP 会话开始处显示标语消息。

当邮件因 HAT“拒绝”(Reject) 设置而被拒绝时，AsyncOS 可在邮件收件人级别 (RCPT TO)（而不是在 SMTP 会话开始时）执行拒绝。通过此方式拒绝邮件会延迟邮件拒绝并退回邮件，以便 AsyncOS 保留更多有关已拒绝邮件的详细信息。例如，可以通过被阻止的邮件的地址和每个收件人地址查看邮件。延迟 HAT 拒绝还可以降低发送 MTA 将执行多次重试的可能性。

在启用 HAT 延迟拒绝后，将发生以下行为：

- MAIL FROM 命令将被接受，但不会创建邮件对象。
- 所有 RCPT TO 命令都将被拒绝，并显示一段文本，阐明发送邮件的权限已被拒绝。
- 如果发送 MTA 通过 SMTP AUTH 进行身份验证，则它们将被授予“中继”(RELAY) 策略，并且允许它们正常传送邮件。

可以使用 `listenerconfig --> setup` CLI 命令配置延迟拒绝。默认情况下禁用此行为。

下表显示了如何为 HAT 配置延迟拒绝。

```
example.com> listenerconfig

Currently configured listeners:

1. listener1 (on main, 172.22.138.17) QMQP TCP Port 628 Private

2. listener2 (on main, 172.22.138.17) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> setup

Enter the global limit for concurrent connections to be allowed across all listeners.

[300]>

[...]


By default HAT rejected connections will be closed with a banner
message at the start of the SMTP conversation. Would you like to do the rejection at the
message recipient level instead for more detailed logging of rejected mail?
```

```
[N]> y

Do you want to modify the SMTP RCPT TO reject response in this case?

[N]> y

Enter the SMTP code to use in the response. 550 is the standard code.

[550]> 551

Enter your custom SMTP response. Press Enter on a blank line to finish.

Sender rejected due to local mail policy.

Contact your mail admin for assistance.
```

使用客户端证书对 SMTP 会话进行身份验证

邮件安全设备支持使用客户端证书对邮件安全设备与用户邮件客户端之间的 SMTP 会话进行身份验证。

当创建 SMTP 身份验证配置文件时，选择要用于验证证书的证书身份验证 LDAP 查询。还可以指定客户端证书不可用时，邮件安全设备是否退回 SMTP AUTH 命令以对用户进行身份验证。

如果贵组织使用客户端证书对用户进行身份验证，则可以选择使用 SMTP 身份验证查询来检查没有客户端证书的用户是否只要其记录指定为允许便可发送邮件。

传出 SMTP 身份验证

SMTP 身份验证还可用于使用用户名和密码为出站邮件中继提供验证。创建“传出”SMTP 身份验证配置文件，然后将配置文件附加到 ALL 域的 SMTP 路由。在每个邮件传输尝试中，设备使用必要的凭据登录到上游邮件中继。SMTP 身份验证支持以下授权协议：PLAIN 和 LOGIN。

步骤 1 创建传出 SMTP 身份验证配置文件。

1. 依次选择**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**。
2. 点击**添加配置文件 (Add Profile)**。
3. 为 SMTP 身份验证配置文件输入唯一的名称。
4. 对于配置文件类型，选择**传出 (Outgoing)**。
5. 点击 **Next**。
6. 为身份验证配置文件输入身份验证用户名和密码。
7. 点击 **Finish**。

步骤 2 配置 SMPT 路由以使用在步骤 1 中创建的传出 SMTP 身份验证配置文件。

1. 依次选择**网络 (Network) > SMTP 路由 (SMTP Routes)**。
2. 点击**接收域 (Receiving Domain)** 列中的**所有其他域 (All Other Domains)** 链接。
3. 为 SMTP 路由输入目标主机的名称。这是用于发送传出邮件的外部邮件中继的主机名。
4. 从下拉菜单中选择传出 SMTP 身份验证配置文件。

5. 提交并确认更改。

记录和 SMTP 身份验证

当在设备上配置了 SMTP 身份验证机制（基于 LDAP、基于 SMTP 转发服务器或 SMTP 传出）时，以下事件将记录在邮件日志中：

- [仅供参考] 成功的 SMTP 身份验证尝试 - 包括进行了身份验证的用户和使用的机制。（不会记录纯文本密码。）
- [仅供参考] 未成功的 SMTP 身份验证尝试 - 包括进行了身份验证的用户和使用的机制。
- [警告] 无法连接到身份验证服务器 - 包括服务器名称和机制。
- [警告] 等待身份验证请求期间转发服务器（与上游注入设备通信）超时所引起的超时事件。

为用户配置外部 LDAP 身份验证

可以将设备配置为使用网络上的LDAP目录对管理用户进行身份验证，方法是允许他们通过其LDAP用户名和密码进行登录。为 LDAP 服务器配置了身份验证查询后，在 GUI 的**系统管理 > 用户**页面中（或在 CLI 中使用 **userconfig** 命令）为设备启用使用外部身份验证的功能。

步骤 1 **创建查询以查找用户帐户**。在 LDAP 服务器配置文件中，创建一个查询以在 LDAP 目录中搜索用户帐户。

步骤 2 **创建组成员身份查询**。创建查询来确定用户是否为某个目录组的成员。

步骤 3 **设置外部身份验证以使用 LDAP 服务器**。启用设备以将 LDAP 服务器用于用户身份验证，并将用户角色分配给 LDAP 目录中的组。有关详细信息，请参阅“分配管理任务”一章中的“添加用户”。

注释 使用“LDAP”页面上的“测试查询”(Test Query) 按钮（或 **ldaptest** 命令）验证查询是否返回了预期结果。有关详细信息，请参阅测试 LDAP 查询，第 599 页。

用户帐户查询

为了验证外部用户，AsyncOS 会使用查询搜索 LDAP 目录中的用户记录以及包含用户全名的属性。根据选择的服务器类型，AsyncOS 会输入默认查询和默认属性。如果在 LDAP 用户记录的 RFC 2307 中定义了属性（shadowLastChange、shadowMax 和 shadowExpire），则可以选择使设备拒绝帐户过期的用户。在用户记录所在的域级别需要基本 DN。

下表显示了 AsyncOS 在 Active Directory 服务器上搜索用户帐户时使用的默认查询字符串和用户全名属性。

表 *68:* 默认用户帐户查询字符串和属性：*Active Directory*

服务器类型	**Active Directory**
Base DN	[空白]（需要使用特定的基本 DN 来查找用户记录。）
查询字符串	(&(objectClass=user)(sAMAccountName={u}))
包含用户全名的属性	displayName

下表显示了 AsyncOS 在 OpenLDAP 服务器上搜索用户帐户时使用的默认查询字符串和用户全名属性。

表 *69:* 默认用户帐户查询字符串和属性：*OpenLDAP*

服务器类型	**OpenLDAP**
Base DN	[空白]（需要使用特定的基本 DN 来查找用户记录。）
查询字符串	(&(objectClass=posixAccount)(uid={u}))
包含用户全名的属性	gecos

组成员身份查询

AsyncOS 还使用查询来确定用户是否为某个目录组的成员。目录组成员身份中的成员身份会确定系统中的用户权限。在 GUI 的“系统管理”>“用户”页面上（或 CLI 中的 userconfig）启用外部身份验证时，将用户角色分配给 LDAP 目录中的组。用户角色会确定用户在系统中所具有的权限，并且对于在外部进行身份验证的用户，角色将分配给目录组而不是各个用户。例如，可以为 IT 目录组中的用户分配“管理员 (Administrator)”角色，并且为“支持 (Support)”目录中的用户分配“服务中心用户 (Help Desk User)”角色。

如果用户属于具有不同用户角色的多个 LDAP 组，AsyncOS 会为用户授予最受限制角色的权限。例如，如果用户属于具有“操作人员 (Operator)”权限的组和具有“服务中心用户 (Help Desk User)”权限的组，则 AsyncOS 会为该用户授予“服务中心用户 (Help Desk User)”角色的权限。

配置 LDAP 配置文件以查询组成员身份时，输入可以找到组记录的目录级别的基本 DN，保存组成员用户名的属性，以及包含组名的属性。根据为 LDAP 服务器配置文件选择的服务器类型，AysncOS 会输入用户名和组名属性的默认值，以及默认查询字符串。

注释 对于 Active Directory 服务器，用于确定用户是否是组成员的默认查询字符串是 (&(objectClass=group)(member={u}))。但是，如果 LDAP 方案在“memberof”列表中使用可分辨名称而不是用户名，则可以使用 {dn} 而不是 {u}。

下表显示了 AsyncOS 在 Active Directory 服务器上搜索组成员身份信息时使用的默认查询字符串和属性。

表 *70:* 默认组成员查询字符串和属性：*Active Directory*

服务器类型	**Active Directory**
Base DN	[空白]（需要使用特定的基本 DN 来查找组记录。）
可确定用户是否为某个组的成员的查询字符串	(&(objectClass=group)(member={u})) **注释** 如果 LDAP 方案在 memberOf 列表中使用可分辨名称而不是用户名，则可以将 {u} 替换为 {dn}。
保存每个成员的用户名（或用户记录的 DN）的属性	成员
包含组名的属性	cn

下表显示了 AsyncOS 在 OpenLDAP 服务器上搜索组成员身份信息时使用的默认查询字符串和属性。

表 *71:* 默认组成员查询字符串和属性：*OpenLDAP*

服务器类型	**OpenLDAP**
Base DN	[空白]（需要使用特定的基本 DN 来查找组记录。）
可确定用户是否为某个组的成员的查询字符串	(&(objectClass=posixGroup)(memberUid={u}))
保存每个成员的用户名（或用户记录的 DN）的属性	memberUid
包含组名的属性	cn

对垃圾邮件隔离区的终端用户进行身份验证

垃圾邮件隔离区最终用户身份验证查询会在用户登录垃圾邮件隔离区时对他们进行验证。令牌 {u} 指定了该用户（它表示用户的登录名）。令牌 {a} 指定用户的邮件地址。LDAP 查询不会从邮件地址中剥离“SMTP:”；AsyncOS 会剥离地址中的该部分。

如果希望垃圾邮件隔离区将 LDAP 查询用于最终用户访问，请选中“指定为活动查询”(Designate as the active query) 复选框。如果有现有的有效查询，则禁用此选项。打开**系统管理 > LDAP** 页面后，有效查询旁边会显示一个星号 (*)。

根据服务器类型，AsyncOS 会将以下默认查询字符串之一用于最终用户身份验证查询：

- **Active Directory:** (sAMAccountName={u})
- **OpenLDAP**: (uid={u})
- **未知或其他**：[空白]

默认情况下，Active Directory 服务器的主邮件属性为 proxyAddresses，OpenLDAP 服务器的主邮件属性为 mail。可以输入自己的查询和邮件属性。要通过 CLI 创建查询，请使用 ldapconfig 命令的 isqauth 子命令。

注释 如果希望用户使用其完整邮件地址登录，请将 (mail=smtp:{a}) 用于查询字符串。

Active Directory 最终用户身份验证设置示例

此部分显示 Active Directory 服务器和最终用户身份验证查询的设置示例。此示例为 Active Directory 服务器、mail 和 proxyAddresses 邮件属性使用密码身份验证，为 Active Directory 服务器的最终用户身份验证使用默认查询字符串。

表 *72: LDAP* 服务器和垃圾邮件隔离区最终用户身份验证设置示例：*Active Directory*

身份验证方法	使用密码（需要创建一个低权限用户以绑定用于搜索，或配置匿名搜索。）
服务器类型	Active Directory
端口	3268
Base DN	[空白]
连接协议	[空白]
查询字符串	(sAMAccountName={u})
邮件属性	mail,proxyAddresses

OpenLDAP 最终用户身份验证设置示例

本部分介绍 OpenLDAP 服务器和最终用户身份验证查询设置示例。此示例为 OpenLDAP 服务器、mail 和 mailLocalAddress 邮件属性使用匿名身份验证，为 OpenLDAP 服务器的最终用户身份验证使用默认查询字符串。

表 *73: LDAP* 服务器和垃圾邮件隔离区最终用户身份验证设置示例：*OpenLDAP*

身份验证方法	匿名
服务器类型	OpenLDAP
端口	389
Base DN	[空白]（某些较早的方案需要使用特定的基本 DN。）
连接协议	[空白]

身份验证方法	匿名
查询字符串	(uid={u})
邮件属性	mail,mailLocalAddress

垃圾邮件隔离区别名整合查询

如果您使用垃圾邮件通知，垃圾邮件隔离区别名合并查询会合并邮件别名，以便收件人无需为每个邮件别名接收隔离区通知。例如，收件人可能收到以下邮件地址的邮件：john@example.com、jsmith@example.com 和 john.smith@example.com。使用别名合并时，对于发送给所有用户别名的邮件，收件人将在选定的主要邮件地址收到一条垃圾邮件通知。

要将邮件整合到主邮件地址，请创建查询来搜索收件人的备用邮件别名，然后在“邮件属性 (Email Attribute)”字段中输入收件人的主邮件地址的属性。

如果希望垃圾邮件隔离区将LDAP查询用于垃圾邮件通知，请选中“指定为活动查询”(Designate as the active query) 复选框。如果有现有的有效查询，则禁用此选项。打开“系统管理”(System Administration) >“LDAP”页面时，会在有效查询旁边会显示一个星号 (*)。

对于 Active Directory 服务器，默认查询字符串为 (|(proxyAddresses={a})(proxyAddresses=smtp:{a}))，默认邮件属性为 mail。对于 OpenLDAP 服务器，默认查询字符串为 (mail={a})，默认邮件属性为 mail。可以定义自己的查询和邮件属性，包括逗号分隔的多个属性。如果您输入多个邮件属性，思科建议输入一个使用单个值的唯一属性（例如 mail）作为第一个邮件属性，而不是输入一个具有多个可以更改的值的属性，例如 proxyAddresses。

要在 CLI 中创建查询，请使用 ldapconfig 命令的 isqalias 子命令。

Active Directory 别名合并设置示例

此部分显示 Active Directory 服务器和别名合并查询的设置示例。此示例将匿名身份验证用于 Active Directory 服务器，将别名合并的查询字符串用于 Active Directory 服务器，并且使用了 mail 邮件属性。

表 *74: LDAP* 服务器和垃圾邮件隔离区别名合并设置示例：*Active Directory*

身份验证方法	匿名
服务器类型	Active Directory
端口	3268
Base DN	[空白]
连接协议	使用 SSL

身份验证方法	匿名
查询字符串	(|(mail={a})(mail=smtp:{a}))
邮件属性	mail

注释 本示例仅用于演示。查询和 OU 或树设置可能因环境和配置而异。

OpenLDAP 别名整合设置示例

此部分显示 OpenLDAP 服务器和别名整合查询的设置示例。此示例将匿名身份验证用于 OpenLDAP 服务器，将别名整合的查询字符串用于 OpenLDAP 服务器，并且使用了 mail 邮件属性。

表 *75: LDAP* 服务器和垃圾邮件隔离区别名整合设置示例：*OpenLDAP*

身份验证方法	匿名
服务器类型	OpenLDAP
端口	389
Base DN	[空白]（某些较早的方案需要使用特定的基本 DN。）
连接协议	使用 SSL
查询字符串	(mail={a})
邮件属性	mail

注释 本示例仅用于演示。查询和 OU 或树设置可能因环境和配置而异。

用户可分辨名称设置示例

此部分显示 Active Directory 服务器和用户可分辨名称查询的设置示例。此示例为 Active Directory 服务器使用匿名身份验证，并且为 Active Directory 服务器的用户可分辨名称检索使用查询字符串。

表 *76: LDAP* 服务器和垃圾邮件隔离区别名整合设置示例：*Active Directory*

身份验证方法	匿名
服务器类型	Active Directory

身份验证方法	匿名
端口	3268
Base DN	[空白]
连接协议	使用 SSL
查询字符串	`(proxyAddresses=smtp:{a})`

注释 本示例仅用于演示。查询和 OU 或树设置可能因环境和配置而异。

将 AsyncOS 配置为与多个 LDAP 服务器配合使用

配置 LDAP 配置文件时，可以配置设备以连接到列表中的多个 LDAP 服务器。要使用多个 LDAP 服务器，必需将 LDAP 服务器配置为包含相同的信息、使用相同结构并且使用相同的身份验证信息。（存在可以整合记录的第三方产品）。

将设备配置为连接到冗余 LDAP 服务器时，可以配置 LDAP 配置以进行故障转移或负载均衡。

可以使用多个 LDAP 服务器以获得以下结果：

- **故障转移**。当配置 LDAP 配置文件以进行故障转移时，如果设备无法连接到第一台 LDAP 服务器，则会故障转移到列表中的下一台 LDAP 服务器。
- **负载均衡**。配置 LDAP 配置文件以实现负载均衡时，设备会在执行 LDAP 查询期间在列出的 LDAP 服务器之间分发连接。

可以在“系统管理”>“LDAP”页面上，或使用 CLI 的 ldapconfig 命令配置冗余 LDAP 服务器。

测试服务器和查询

使用“添加 LDAP 服务器配置文件”(Add LDAP Server Profile) 或“编辑 LDAP 服务器配置文件”(Edit LDAP Server Profile) 页面上的**测试服务器 (Test Server[s])** 按钮或（CLI 中的 **`test`** 子命令）测试到 LDAP 服务器的连接。如果使用多个 LDAP 服务器，则 AsyncOS 会测试每台服务器并显示每台服务器的各个结果。AsyncOS 还将在每台 LDAP 服务器上测试查询并显示各个结果。

故障切换

要确保 LDAP 查询得到解决，可以配置 LDAP 配置文件以进行故障切换。如果与 LDAP 服务器的连接失败，或者查询返回特定的错误代码（例如，“不可用”或“忙”），则设备将尝试查询列表中指定的下一台 LDAP 服务器。

设备会在指定的时间段内尝试连接到 LDAP 服务器列表中的第一台服务器。如果设备无法连接到列表中的第一台 LDAP 服务器，或者查询返回特定错误代码（例如，“不可用”或“忙”），则设备

将尝试连接到列表中的下一台 LDAP 服务器。默认情况下，设备始终尝试连接到列表中的第一台服务器，而且，会尝试按照列出的顺序连接到后续每台服务器。为确保设备在默认情况下连接到主 LDAP 服务器，请务必将其输入为 LDAP 服务器列表中的第一台服务器。

如果设备连接到第二个或后续的 LDAP 服务器，它将保持连接到该服务器的状态，直到出现超时。出现超时后，它会尝试重新连接到列表中的第一台服务器。

注释 只有查询指定 LDAP 服务器的尝试才会进行故障转移。尝试查询与未故障转移的指定的 LDAP 服务器关联的建议或后续服务器。

配置设备进行 LDAP 故障切换

要配置设备进行 LDAP 故障转移，请在 GUI 中完成以下步骤：

步骤 1 从“系统管理”(System Administration) > “LDAP”中，选择要编辑的 LDAP 服务器配置文件。

步骤 2 从 LDAP 服务器配置文件中，配置以下设置：

编号	说明
1	列出 LDAP 服务器。
2	配置最大连接数。

步骤 3 配置其他 LDAP 设置并确认更改。

负载均衡

要在一组 LDAP 服务器中分发 LDAP 连接，可以配置用于负载均衡的 LDAP 配置文件。

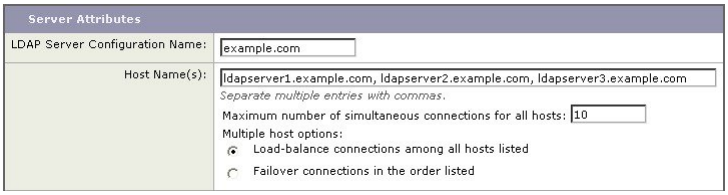
为负载均衡配置 LDAP 配置文件时，设备会在列出的 LDAP 服务器之间分发连接。如果连接失败或超时，设备会确定哪些 LDAP 服务器可用，并重新连接到可用的服务器。设备会基于配置的最大连接数确定要建立的并发连接数。

如果其中一台所列的 LDAP 服务器未响应，设备将在剩余的 LDAP 服务器之间分发的连接。

为设备配置负载均衡

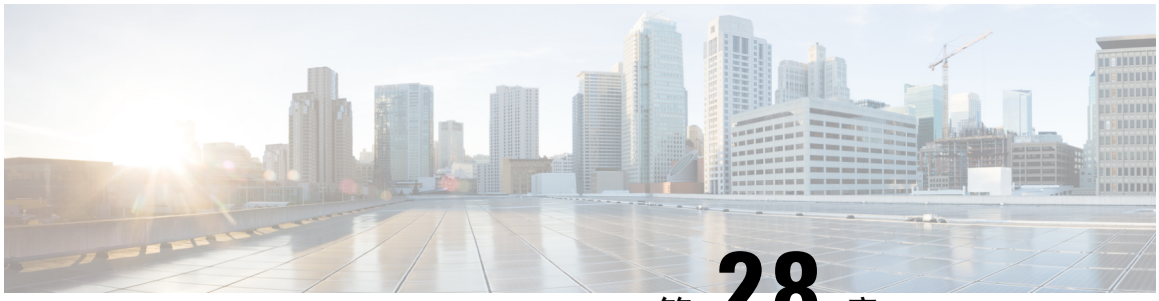
步骤 1 从**系统管理 > LDAP** 中，选择要编辑的 LDAP 服务器配置文件。

步骤 2 从 LDAP 服务器配置文件中，配置以下设置：



编号	说明
1	列出 LDAP 服务器
2	配置最大连接数

步骤 3 配置其他 LDAP 设置并确认更改。



第 28 章

使用客户端证书对 SMTP 会话进行身份验证

本章包含以下部分：

证书和 SMTP 身份验证概述

邮件安全设备支持使用客户端证书对邮件安全设备与用户邮件客户端之间的 SMTP 会话进行身份验证。当应用尝试连接到设备发送邮件时，邮件安全设备可以请求用户的邮件客户端提供客户端证书。设备在收到客户端证书后，将确认证书是否有效、未过期且未被撤销。如果证书有效，邮件安全设备则允许通过 TLS 从邮件应用建立 SMTP 连接。

如果组织需要其用户对邮件客户端使用通用访问卡 (CAC)，可以使用此功能配置邮件安全设备，以请求 CAC 和 ActivClient 中间件应用将向设备提供的证书。

您可以将邮件安全设备配置为，需要用户在发送邮件时提供证书，但仍允许对特定用户例外。对于这些用户，您可以将设备配置为使用 SMTP 身份验证 LDAP 查询验证用户。

用户必须将其邮件客户端配置为通过安全连接 (TLS) 发送邮件，并接受设备提供的服务器证书。

如何使用客户端证书验证用户

表 *77:* 如何使用客户端证书验证用户

	请	更多信息
第 1 步	为 LDAP 服务器定义一个证书查询。	检查客户端证书的有效性，第 631 页
第 2 步	创建基于证书的 SMTP 身份验证配置文件。	使用客户端证书验证通过 TLS 的 SMTP 连接，第 632 页

	请	更多信息
第 3 步	配置一个监听程序，以使用证书 SMTP 身份验证配置文件。	通过使用 Web 界面创建侦听程序侦听连接请求， 第 66 页
第 4 步	将 RELAYED 邮件流策略修改为需要 TLS、客户端证书和 SMTP 身份验证。	从设备建立 TLS 连接， 第 632 页

如何使用 SMTP 身份验证 LDAP 查询验证用户

表 *78:* 如何使用 *SMTP* 身份验证 *LDAP* 查询验证用户

	请	更多信息
第 1 步	为您的服务器定义一个 SMTP 身份验证查询，使用允许查询字符串和 Bind 作为身份验证方法。	使用 LDAP 目录验证用户， 第 631 页
第 2 步	创建基于 LDAP 的 SMTP 身份验证配置文件。	配置 AsyncOS 进行 SMTP 身份验证， 第 612 页
第 3 步	配置一个监听程序，以使用 LDAP SMTP 身份验证配置文件。	如果不允许用户使用基于 LDAP 的 SMTP 身份验证验证连接，可以选择在记录所有活动时设备是拒绝连接还是临时允许连接。
第 4 步	将 RELAYED 邮件流策略修改为需要 TLS 和 SMTP 身份验证。	从设备建立 TLS 连接， 第 632 页

如果客户端证书无效，如何使用 LDAP SMTP 身份验证查询验证用户

表 *79:* 如何使用客户端证书或 *LDAP SMTP* 身份验证查询验证用户

	请	更多信息
第 1 步	为您的服务器定义一个 SMTP 身份验证查询，使用允许查询字符串和 Bind 作为身份验证方法。	使用 LDAP 目录验证用户， 第 631 页
第 2 步	为 LDAP 服务器定义一个基于证书的查询。	检查客户端证书的有效性， 第 631 页
第 3 步	创建基于证书的 SMTP 身份验证配置文件	使用客户端证书验证通过 TLS 的 SMTP 连接， 第 632 页
第 4 步	创建 LDAP SMTP 身份验证配置文件。	配置 AsyncOS 进行 SMTP 身份验证， 第 612 页
第 5 步	配置一个侦听程序，以使用证书 SMTP 身份验证配置文件。	通过使用 Web 界面创建侦听程序侦听连接请求， 第 66 页

	请	更多信息
第 6 步	1. 将 RELAYED 邮件流策略修改为使用以下设置： 2. 首选 TLS 3. 需要 SMTP 身份验证 4. SMTP 身份验证需要 TLS	从设备建立 TLS 连接，第 632 页

检查客户端证书的有效性

证书身份验证 LDAP 查询将检查客户端证书的有效性，以便验证用户的邮件客户端与邮件安全设备之间的SMTP会话。创建此查询时，需为身份验证选择一系列证书字段，指定用户 ID 属性（默认值为 uid），并输入查询字符串。

例如，搜索证书通用名称和序列号的查询字符串可能如下所示：**`(&(objectClass-posixAccount)(caccn={cn})(cacserial={sn})`**。创建查询之后，即可在证书 SMTP 身份验证配置文件中使用它。此 LDAP 查询支持 OpenLDAP、Active Directory 和 Oracle Directory。

有关配置 LDAP 的详细信息，请参阅LDAP 查询，第 585 页。

步骤 1 依次选择**系统管理 (System Administration) > LDAP**。

步骤 2 创建新 LDAP 配置文件。有关详细信息，请参阅创建 LDAP 服务器配置文件以存储有关 LDAP 服务器的信息，第 588 页。

步骤 3 选中**证书身份验证查询 (Certificate Authentication Query)** 复选框。

步骤 4 输入查询名称。

步骤 5 输入查询字符串，以验证用户的证书。例如，**`(&(objectClass=user)(cn={cn}))`**。

步骤 6 输入用户 ID 属性，例如 **`sAMAccountName`**。

步骤 7 提交并确认更改。

使用 LDAP 目录验证用户

SMTP 身份验证 LDAP 查询包含允许查询字符串，允许邮件安全设备检查是否允许用户的邮件客户端根据用户在 LDAP 目录中的记录通过设备发送邮件。这样，如果用户没有客户端证书，只要其记录指定允许发送，就能发送邮件。

此外，还可以根据其他属性过滤结果。例如，查询字符串 `(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))` 将确认用户是否符合以下任意条件：

- 未向用户出具 CAC (`caccn=*`)
- 免除 CAC (`cacexempt=*`)
- 如果用户没有 CAC，暂时可以发送邮件的时段在将来会过期 (`cacemergency>={t}`)

有关使用 SMTP 身份验证查询的详细信息，请参阅配置 AsyncOS 进行 SMTP 身份验证，第 612 页。

步骤 1 依次选择**系统管理 (System Administration) > LDAP**。

步骤 2 定义一个 LDAP 配置文件。有关详细信息，请参阅创建 LDAP 服务器配置文件以存储有关 LDAP 服务器的信息，第 588 页。

步骤 3 为该 LDAP 配置文件定义一个 SMTP 身份验证查询。

步骤 4 选中“SMTP 身份验证查询”(SMTP Authentication Query) 复选框。

步骤 5 输入查询名称。

步骤 6 输入字符串，以查询用户的 ID。例如 `(uid={u})`。

步骤 7 选择 LDAP BIND 作为身份验证方法。

步骤 8 输入允许查询字符串。例如 `(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`。

步骤 9 提交并确认更改。

使用客户端证书验证通过 TLS 的 SMTP 连接

基于证书的 SMTP 身份验证配置文件允许邮件安全设备使用客户端证书验证通过 TLS 的 SMTP 连接。创建配置文件时，需选择用于验证证书的证书身份验证 LDAP 查询。还可以指定客户端证书不可用时，邮件安全设备是否退回 **SMTP AUTH** 命令以对用户进行身份验证。

有关使用 LDAP 验证 SMTP 连接的信息，请参阅配置 AsyncOS 进行 SMTP 身份验证，第 612 页。

步骤 1 依次选择**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**。

步骤 2 点击**添加配置文件 (Add Profile)**。

步骤 3 输入 SMTP 身份验证配置文件的名称。

步骤 4 为“配置文件类型”(Profile Type) 选择**证书 (Certificate)**。

步骤 5 点击 **Next**。

步骤 6 输入配置文件名称。

步骤 7 选择要用于此 SMTP 身份验证配置文件的证书 LDAP 查询。

注释 如果客户端证书不可用，请不要选择该选项来允许 SMTP AUTH 命令。

步骤 8 点击 **Finish**。

步骤 9 提交并确认更改。

从设备建立 TLS 连接

如果客户端证书有效，RELAYED 邮件流策略的“验证客户端证书”选项会指引邮件安全设备建立到用户邮件应用的 TLS 连接。如果您为“首选 TLS”(TLS Preferred) 设置选择此选项，当用户没有

证书时，设备仍允许非TLS连接；但在用户具有的证书无效时，将拒绝连接。对于“需要TLS”(TLS Required) 设置，选择此选项将要求用户具备有效证书，设备才能允许连接。

要使用客户端证书验证用户的 SMTP 会话，请选择以下设置：

- TLS - 必需
- 验证客户端证书
- 需要 SMTP 身份验证

注释 虽然需要 SMTP 身份验证，但邮件安全设备不会使用 SMTP 身份验证 LDAP 查询，因为它正在使用证书身份验证。

要使用 SMTP 身份验证查询代替客户端证书验证用户的 SMTP 会话，请为 RELAYED 邮件流策略选择以下设置：

- TLS - 必需
- 需要 SMTP 身份验证

如果您需要邮件安全设备对某些用户请求客户端证书，而允许其他用户进行基于 LDAP 的 SMTP 身份验证，请为 RELAYED 邮件流策略选择以下设置：

- TLS - 首选
- 需要 SMTP 身份验证
- 提供 SMTP 身份验证需要 TLS

更新已撤销证书的列表

在证书验证过程中，邮件安全设备会检查已撤销证书列表（称为“证书撤销列表”），以确保用户的证书未被撤销。您可以在服务器上保留此列表的最新版本，邮件安全设备将按您创建的计划下载该列表。

步骤 1 依次转到**网络 (Network) > CRL 源 (CRL Sources)**。

步骤 2 针对 SMTP TLS 连接启用 CRL 检查：

a) 点击“全局设置”(Global Settings) 下的“编辑设置”(Edit Settings)。

b) （可选）如果要选择所有选项，请选中**全局设置**复选框：

- 对入站 SMTP TLS 进行 CRL 检查。
- 对出站 SMTP TLS 进行 CRL 检查
- 对 Web 界面进行 CRL 检查

c) 选中复选框“对入站 SMTP TLS 进行 CRL 检查”、“对出站 SMTP TLS 进行 CRL 检查”或“对 Web 界面进行 CRL 检查”选项。

d) 提交更改。

步骤 3 点击**添加 CRL 来源 (Add CRL Source)**。

步骤 4 输入 CRL 来源的名称。

步骤 5 选择文件类型。可以是 ASN.1 或 PEM。

步骤 6 输入 URL 作为文件的主要来源，包括文件名。例如 **`https://crl.example.com/certs.crl`**

步骤 7 如果设备无法联系主要来源，也可以输入一个次要来源。

步骤 8 指定下载的 CRL 来源的计划。

步骤 9 启用 CRL 来源。

步骤 10 提交并确认更改。

使用客户端证书验证用户的 SMTP 会话

步骤 1 依次转到**系统管理 > LDAP**，配置 LDAP 服务器配置文件。

步骤 2 为该 LDAP 配置文件定义一个证书查询。

a) 输入查询名称。
b) 选择要验证的证书字段，例如序列号和通用名称。
c) 输入查询字符串。例如，**`(&(caccn={cn})(cacserial={sn}))`**。
d) 输入用户 ID 字段，例如 uid。
e) 提交更改。

步骤 3 依次转到**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**。

a) 输入配置文件名称。
b) 选择要使用的证书 LDAP 查询。
c) 如果客户端证书不可用，请不要选择该选项来允许 **`SMTP AUTH`** 命令。
d) 提交更改。

步骤 4 要配置侦听程序以使用您创建的证书 SMTP 身份验证配置文件，请依次转到**网络 (Network) > 侦听程序 (Listeners)**。

步骤 5 将 RELAYED 邮件流策略修改为需要 TLS、客户端证书和 SMTP 身份验证。

注释 虽然需要 SMTP 身份验证，但邮件安全设备不会使用 SMTP AUTH 命令，因为它正在使用证书身份验证。邮件安全设备需要邮件应用提供客户端证书来验证用户。

步骤 6 提交并确认更改。

使用 SMTP AUTH 命令来验证用户的 SMTP 会话

邮件安全设备可以使用 SMTP AUTH 命令，代替客户端证书来验证用户的 SMTP 会话。如果您的用户无法使用 SMTP AUTH 验证连接，可以选择在记录所有活动时设备是拒绝连接还是临时允许连接。

步骤 1 依次转到**系统管理 (System Administration) > LDAP**，配置 LDAP 服务器配置文件。

步骤 2 为该 LDAP 配置文件定义一个 SMTP 身份验证查询。

a) 输入查询名称。
b) 输入查询字符串。例如，`(uid={u})`。
c) 选择 LDAP Bind 作为身份验证方法。
d) 输入允许查询字符串。例如，`(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`。
e) 提交更改。

步骤 3 依次转到**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**，配置 LDAP SMTP 身份验证配置文件。

a) 输入配置文件名称。
b) 选择要使用的 SMTP 身份验证 LDAP 查询。
c) 如果允许用户使用 SMTP AUTH 命令及选择监控和报告用户的活动，请选择“使用 LDAP 检查”(Check with LDAP)。
d) 提交更改。

步骤 4 要配置监听程序以使用您创建的证书SMTP身份验证配置文件，请依次转到**网络 (Network) > 监听程序 (Listeners)**。

步骤 5 将 RELAYED 邮件流策略修改为需要 TLS 和 SMTP 身份验证。

步骤 6 提交并确认更改。

使用客户端证书或 SMTP AUTH 验证用户的 SMTP 会话

此配置要求邮件安全设备对具有客户端证书的用户请求客户端证书，同时允许没有客户端证书或无法使用证书发送邮件的用户使用 SMTP AUTH。

严禁不允许使用 SMTP AUTH 命令的用户进行任何尝试。

步骤 1 依次转到**系统管理 (System Administration) > LDAP**，配置 LDAP 服务器配置文件。

步骤 2 为该配置文件定义一个 SMTP 身份验证查询。

a) 输入查询名称。
b) 输入查询字符串。例如，`(uid={u})`。
c) 选择 LDAP Bind 作为身份验证方法。
d) 输入允许查询字符串。例如，`(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`。

步骤 3 为该 LDAP 配置文件定义一个证书查询。

a) 输入查询名称。
b) 选择要验证的客户端证书字段，例如序列号和通用名称。
c) 输入查询字符串。例如，`(&(caccn={cn})(cacserial={sn}))`。
d) 输入用户 ID 字段，例如 uid。
e) 提交更改。

步骤 4 依次转到**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**，配置 LDAP SMTP 身份验证配置文件。

a) 输入配置文件名称。
b) 选择要使用的 SMTP 身份验证 LDAP 查询。
c) 如果允许用户使用 SMTP AUTH 命令及选择拒绝连接，请选择“使用 LDAP 检查”(Check with LDAP)。
d) 输入自定义 SMTP AUTH 响应。例如 525, “Dear user, please use your CAC to send email.”
e) 提交更改。

步骤 5 配置证书 SMTP 身份验证配置文件。

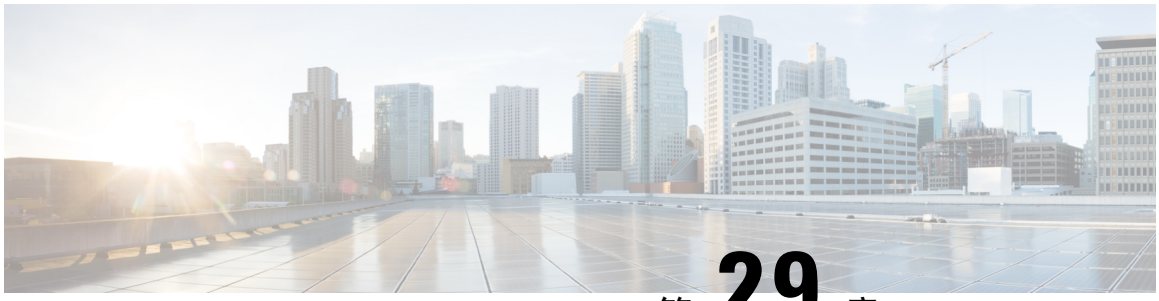
a) 输入配置文件名称。
b) 选择要使用的证书 LDAP 查询。
c) 如果客户端证书不可用，选择该选项可允许使用 SMTP AUTH 命令。
d) 如果用户没有客户端证书，请选择供设备使用的 LDAP SMTP 身份验证配置文件。
e) 提交更改。

步骤 6 要配置侦听程序以使用您创建的证书SMTP身份验证配置文件，请依次转到**网络 (Network)>侦听程序 (Listeners)**。

步骤 7 将 RELAYED 邮件流策略修改为选择以下选项：

- 首选 TLS
- 需要 SMTP 身份验证
- SMTP 身份验证需要 TLS

步骤 8 提交并确认更改。



第 29 章

使用邮件安全监控

本章包含以下部分：

邮件安全监控概述

邮件安全监控功能可收集邮件传送过程中各个步骤的数据。数据库根据 IP 地址识别和记录各个邮件发件人，同时与 SenderBase 信誉服务进行交互以获取实时身份信息。您可以即时报告任何邮件发件人的本地邮件流量历史记录，并显示包括互联网中发件人全局记录的配置文件。通过邮件安全监控器功能，安全团队可以“封闭循环”监控向用户发送邮件的人员、用户发送和接收的邮件数量以及安全策略的有效性。

本章介绍如何执行以下操作：

- 访问邮件监控器功能，以监控入站和出站邮件流。
- 通过查询发件人的 SenderBase 信誉分数 (SBRS)，制定邮件流策略决策（更新白名单、黑名单和灰名单）。您可以查询网络所有者、域，甚至个人 IP 地址。
- 报告邮件流、系统状态以及发送到网络和从网络发送的邮件。

对于传入邮件的任何给定邮件发件人，邮件安全监控器数据库都会捕获关键参数，例如：

- 邮件量
- 连接历史记录
- 接受与拒绝的连接
- 接受率和调节限制
- 发件人信誉过滤器匹配项
- 可疑垃圾邮件和明确识别的垃圾邮件的反垃圾邮件数
- 防病毒扫描检测到的具有病毒特征的邮件数

有关反垃圾邮件扫描的详细信息，请参阅反垃圾邮件，第 269 页；有关防病毒扫描的详细信息，请参阅防病毒，第 253 页。

邮件安全监控器功能还会捕获有关特定邮件触发哪个内容过滤器的信息，包括向其发送或从其发送邮件的内部用户（邮件收件人）。

邮件安全监控器功能仅在 GUI 中可用，让您了解邮件流量和设备状态（包括隔离区、工作队列和病毒爆发）。设备会识别发件人何时超出正常流量配置文件的范围。系统会在界面中突出显示超出范围的发件人，允许您采取纠正措施，将该发件人分给给某个发件人组，或者完善发件人的访问配置文件；或者，您可以让 AsyncOS 的安全服务继续反应和响应。出站邮件具有类似的监控功能，让您了解邮件队列中排名靠前的域以及接收主机的状态（请参阅“传送状态详细信息”(Delivery Status Details) 页面，第 651 页）。

注释 邮件安全监控器功能不会报告重新启动设备时存在于工作队列中的邮件的信息。

邮件安全监控和集中管理

要查看汇总报告数据，请部署思科内容安全管理设备。

您无法汇总集群设备的邮件安全监控器报告。所有报告均限于计算机级别。这意味着，它们无法在组或集群级别运行 - 只能在单个计算机上运行。

“存档报告”(Archived Reports) 页面的情况同样如此 - 实际上，每台计算机都有自己的存档。因此，“生成报告”(Generate Report) 功能会在所选计算机上运行。

“计划报告”(Scheduled Reports) 页面不限于计算机级别；因此，可以跨多台计算机共享设置。各个计划报告就如同交互式报告一样在计算机级别运行，因此，如果您在集群级别配置计划报告，则集群中的每台计算机都将发送自己的报告。

“预览此报告”(Preview This Report) 按钮始终依据登录主机运行。

“邮件安全监控器”页面

邮件安全监控器功能包括“监控”(Monitor) 菜单上的所有页面，但“隔离区”(Quarantines) 页面除外。

您可使用 GUI 中的这些页面监控连接到设备的侦听程序的域。您可以对设备的“邮件流”进行监控、排序、分析和分类，区分大批量合法邮件发件人和潜在“垃圾邮件发件人”（大量垃圾邮件发件人）或病毒发件人。此外，这些页面还可以帮助排除系统入站连接故障（包括域的 SBRS 得分和最近发件人组匹配等重要信息）。

这些页面可帮助您对与设备相关以及与存在于网关范围之外的服务相关的邮件分类，例如 SenderBase 信誉服务、反垃圾邮件扫描服务、防病毒扫描安全服务、内容过滤器和病毒爆发过滤器。

对于任何邮件安全监控页面，通过点击页面右上角的“可打印 PDF”(Printable PDF) 链接，可以生成打印机友好格式的 .PDF 版本。有关生成英语以外的其他语言的 PDF 的信息，请参阅有关报告的注意事项，第 667 页。

通过**导出 (Export)** 链接可以将图表及其他数据导出为 CSV（逗号分隔值）格式。

导出的 CSV 数据将以 GMT 显示所有邮件跟踪和报告数据（不考虑邮件安全设备中的设置）。GMT 时间转换是为了允许独立于设备使用数据，或从分布于多个时区的设备中引用数据的情况。

注释 如果导出本地化 CSV 数据，则标题在某些浏览器中可能不会正常呈现。发生此情况是因为某些浏览器可能未使用本地化文本的正确字符集。要解决此问题，您可以将文件保存到磁盘，然后使用“文件”(File) >“打开”(Open) 打开文件。打开文件时，请选择字符集以显示本地化文本。

有关自动导出报告数据的详细信息，请参阅检索 CSV 数据，第 665 页。

搜索和邮件安全监控

许多邮件安全监控器页面都包含搜索表单。您可以搜索不同类型的项目：

- IP 地址（IPv4 和 IPv6）
- domain
- 网络所有者
- 内部用户
- 目标域
- 内部发件人域
- 内部发件人 IP 地址
- 传出域传送状态

对于域、网络所有者和内部用户搜索，请选择是完全匹配搜索文本还是查找以输入文本开头的项目（例如，以“ex”开头将匹配“example.com”）。

对于 IPv4 地址搜索，所输入的文本始终解释为最多四个点分十进制格式的 IP 八位组的开头。例如，输入“17”将会在 17.0.0.0 至 17.255.255.255 的范围内搜索，因此 17.0.0.1 匹配搜索结果，而 172.0.0.1 不匹配。对于完全匹配搜索，只要输入全部四个八位组即可。IP 地址搜索还支持 CIDR 格式 (17.16.0.0/12)。

对于 IPv6 地址搜索，AsyncOS 支持以下格式：

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

所有搜索都必须在页面中当前选择的时间范围内。

查看报告中所含邮件的详细信息

只有报告和跟踪都在本地执行（并非在思科内容安全管理设备中集中执行）时，此功能才有效。

步骤 1 点击报告页面上某个表格中的任何蓝色编号。

（并非所有表格都有这些链接。）

该编号中包含的邮件显示在“邮件跟踪”(Message Tracking) 中。

步骤 2 向下滚动可查看列表。

“我的控制面板”页面

您可以创建自定义邮件安全报告页和，方法是组合现有报告页中的图表（图形）和表格。

目标	请
将模块添加到自定义报告页面。	**1.** 依次转到**监控 > 邮件或网络 > 报告 > 我的控制面板**，通过点击模块右上角的 **[X]** 删除不需要的任何示例模块。 **2.** 执行以下操作之一： • 点击模块块中的 **[+]** 按钮（位于“监控”菜单的报告页），将其添加到您的自定义报告中。 • 依次转到**监控 > 邮件或网络 > 报告 > 我的控制面板**，点击其中一个部分的 **[+]** 按钮，然后选择要添加的报告模块。您可能需要检查**每个部分的 + 报告模块**，以找到查找的报告。 **3.** 添加的模块使用默认设置。如果添加已自定义的模块（例如，通过添加、删除或重新排序列，），可在添加这些模块后对其自定义。原始模块的时间范围无法保留。 **4.** 如果添加包含单独图例的图表（例如，“概述 (Overview)”页面中的图形），请单独添加图例。如果需要，请将其拖放到其描述的数据的旁边。 注意： • 某些报告页面的部分模块，只能通过上述某种方法使用。如果无法使用一种方法添加模块，请尝试其他方法。 • 您只能将每个模块添加一次；如果已经将特定模块添加到报告，则用于添加模块的选项将不可用。
查看自定义报告页面	**1.** 依次选择**监控 > 邮件或网络 > 报告> 我的控制面板**。 **2.** 对于“时间范围”部分中的报告：针对所有报告页面所选的时间范围会应用到“我的控制面板”页面中的所有模块。选择要查看的时间范围。 新添加的模块显示在相关部分顶部。

目标	请
在自定义报告页面上重新排列模块	将模块拖放到所需的位置。
从自定义报告页面中删除模块	点击模块右上角的 [X]。

“概述”页面

“概述”(Overview) 页面会概括介绍设备的邮件活动，包括隔离区和病毒爆发过滤器状态的概述（在页面的“系统概述”[System Overview] 部分）。此外，“概述”(Overview) 页面还包括传入和传出邮件的图表和详细邮件计数。可以使用此页面来监控进出网关的所有邮件的流量。

“概述”(Overview) 页面重点介绍了设备与 SenderBase 信誉服务相集成以处理传入邮件（例如，由信誉过滤拦截的邮件）的方式。在**概述 (Overview)** 页面中，可以执行以下操作：

- 查看出入网关的所有邮件的邮件趋势图。
- 查看随着时间的推移显示以下信息的图表：尝试发送的邮件数、被发件人信誉过滤 (SBRS) 拦截的邮件数、包含无效收件人的邮件数、标记为垃圾邮件的邮件数、标记为具有病毒特征的邮件数和正常邮件数。
- 查看系统状态和本地隔离区的摘要。
- 根据威胁操作中心 (TOC) 提供的信息，查看当前的病毒和非病毒爆发信息。

“概述”(Overview) 页面分为两部分：“系统概述”(System Overview) 与“传入和传出邮件”(Incoming and Outgoing Mail) 图表及概要。

系统概况

“概述”(Overview) 页面的“系统概述”(System Overview) 部分用作系统控制面板，提供有关设备的详细信息，包括系统和工作队列状态、隔离区状态和病毒爆发活动。

状态

本部分概括介绍设备和入站邮件处理的当前状态。

系统状态 (System Status)：以下其中一种状态：

- 在线
- 保留资源
- 传输挂起
- 接收挂起
- 工作队列暂停
- 离线

有关详细信息，请参阅 使用 CLI 进行管理和监控，第 805 页。

传入邮件：平均每小时传入邮件的速率。

工作队列：工作队列中等待处理的邮件数。

点击“系统状态详细信息”(System Status Details) 链接可导航至“系统状态”(System Status) 页面。

系统隔离区

本部分显示有关按设备上的磁盘使用情况排名前三的隔离区的信息，包括隔离区的名称、隔离区的满溢程度（磁盘空间）和隔离区中当前的邮件数。

点击“本地隔离区”(Local Quarantines) 链接可导航到“本地隔离区”(Local Quarantines) 页面。

防病毒爆发(VOF)

此部分显示威胁操作中心 (TOC) 报告的爆发状态。此外还显示病毒爆发隔离区的状态，包括其满溢程度（磁盘空间）和隔离区中的邮件数。仅当已在设备上启用爆发过滤器功能时，才会显示病毒爆发隔离区。

注释 为使威胁级别指示器正常工作，您需要将防火墙上的端口 80 对“**downloads.ironport.com**”开放。或者，如果您已指定本地更新服务器，则威胁级别指示器将尝试使用该地址。如果您已通过“服务更新”(Services Updates) 页面配置了下载代理，则威胁级别指示器也将正确更新。有关详细信息，请参阅服务更新，第 761 页。

点击“病毒爆发详细信息”(Outbreak Details) 链接可查看外部威胁防御运营中心网站。请注意，为使此链接正常工作，您的设备必须能够访问互联网。请注意，“单独的窗口”图标表示点击后将以单独窗口打开链接。您可能需要配置浏览器的弹出窗口阻止程序设置才能允许显示这些窗口。

传入和传出摘要与图形

“传入和传出邮件”(Incoming and Outgoing) 摘要部分提供访问系统中所有邮件活动实时状况的权限，其中包括传入和传出邮件图表和邮件摘要。通过“时间范围”(Time Range) 菜单，可以选择报告的时间范围。所有邮件安全监控页面都将使用您选择的时间范围。下面介绍了邮件的各种类型或类别（请参阅邮件分类，第 643 页）。

邮件趋势图显示了邮件流量的视觉表达，而摘要表提供了相同信息的数字细分表达。摘要表包括每种类型邮件的比例和实际数量，包括尝试发送的邮件总数、威胁邮件数和正常邮件数。

传出邮件图表和摘要显示了出站邮件的类似信息。

邮件安全监控中的邮件计数注意事项

邮件安全监控器用于对传入邮件进行计数的方法取决于每封邮件的收件人数量。例如，从example.com发送给三个收件人的传入邮件将计为三封来自该发件人的邮件。

由于发件人信誉过滤拦截的邮件实际不会进入工作队列，因此，设备无权访问传入邮件的收件人列表。在这种情况下，使用倍数来估算收件人数量。此倍数由思科确定，并且是通过对现有客户数据大量取样调查得出。

邮件分类

“概述”(Overview) 和“传入邮件”(Incoming Mail) 页面报告的邮件分类如下：

- **由信誉过滤拦截：**由 HAT 策略拦截的所有连接数乘以一个固定倍数（请参阅邮件安全监控中的邮件计数注意事项，第 642 页），再加上由收件人限制拦截的所有收件人数。
- **无效收件人：**会话 LDAP 拒绝以及所有 RAT 拒绝所拒绝的所有收件人。
- **检测到的垃圾邮件：**反垃圾邮件扫描引擎检测到的具有垃圾邮件或可疑垃圾邮件特征，以及既有垃圾邮件特征又有病毒特征的总邮件数。
- **检测到的病毒邮件：**被检测为具有病毒特征，但不是垃圾邮件的邮件总数和百分比。

  注释 如果将防病毒设置配置为发送不可扫描或加密的邮件，则将这些邮件计入正常邮件，且不具有病毒特征。否则，邮件将被计入具有病毒特征的邮件。

- **由高级恶意软件防护检测 (Detected by Advanced Malware Protection)：**通过文件信誉过滤发现邮件附件是恶意的。该值不包括判定更新或由文件分析发现为恶意的文件。
- **带恶意 URL 的邮件：**URL 过滤发现邮件中的一个或多个 URL 是恶意的。
- **由内容过滤器拦截：**由内容过滤器拦截的邮件总数。
- **由 DMARC 拦截：**执行 DMARC 验证后拦截的邮件总数。
- **S/MIME 验证/解密失败 (S/MIME Verification/Decryption Failed)：**S/MIME 验证、解密或两者均失败的邮件总数。
- **S/MIME 验证/解密成功 (S/MIME Verification/Decryption Successful)：**成功通过 S/MIME 验证、解密或解密和验证的邮件总数。
- **正常邮件：**已被接受且被视为无病毒和垃圾邮件的邮件-考虑到每个收件人的扫描操作（例如，正在按照单独的邮件策略处理的拆分邮件）时接受的对正常邮件最准确的表达。但是，由于标记为垃圾邮件或病毒特征并且仍然提交了的邮件不进行计数，因此所传送邮件的实际数量可能不同于正常邮件的计数。
- 灰色邮件
  - **营销邮件：**专业营销组织（例如 Amazon.com）发送的广告邮件总数。
  - **社交网络邮件：**社交网络、交友网站、论坛等发送的通知邮件总数。示例包括 LinkedIn 和 CNET 论坛。
  - **批量邮件：**无法识别的营销组织（例如技术媒体公司 TechTarget）发送的广告邮件总数。

  点击与上述任何灰色邮件类别对应的数字，可通过“邮件跟踪”(Message Tracking) 查看属于该类别的邮件列表。

  注释 如果邮件与邮件过滤器匹配并且未被过滤器丢弃或退回，则被视为正常。邮件过滤器丢弃或退回的邮件不计入总数。

邮件分类方法

当邮件通过邮件管道时，可应用于多个类别。例如，可将邮件标记为具有垃圾邮件、病毒或恶意软件特征；也可以匹配内容过滤器。各种判定遵循以下优先规则：病毒爆发过滤器隔离（在此情况下，在从隔离区发行邮件并再次通过工作队列进行处理之前，不会对邮件进行计数），接下来是具有垃圾邮件特征、具有病毒特征、具有恶意软件特征，以及匹配内容过滤器。

例如，如果某个邮件被标记为具有垃圾邮件特征，并且您的反垃圾邮件设置被设置为丢弃具有垃圾邮件特征的邮件，则该邮件将被丢弃，垃圾邮件计数器会增加。此外，如果反垃圾邮件设置被设置为允许具有垃圾邮件特征的邮件继续在邮件通道中通行，并且后续内容过滤器将会丢弃、退回或隔离该邮件，则垃圾邮件计数器仍会增加。仅当该邮件不具有垃圾邮件、病毒或恶意软件特征时，内容过滤器才会增加。

“传入邮件”页面

传入邮件页面提供一种报告机制，即报告连接到您的设备的所有远程主机的邮件安全监控功能正在收集的实时信息。这可以让您收集有关向您发送邮件的 IP 地址、域和组织（网络所有者）的详细信息。也可以基于 IP 地址、域以及向您发送邮件的组织执行发件人配置文件搜索。

“传入邮件”(Incoming Mail) 页面包含三个视图：“域”(Domain)、“IP 地址”(IP Address) 和“网络所有者”(Network Owner)，并提供在选定视图环境中连接到系统的远程主机的快照。

它会显示已向设备上配置的所有公共侦听程序发送邮件的排名靠前的域（或者 IP 地址或网络所有者，具体取决于视图）的表（传入邮件详细信息）。您可以监控流入网关的所有邮件流。您可以点击任何域/IP/网络所有者，以在“发件人配置文件”(Sender Profile) 页面（这是特定于您点击的域/IP/网络所有者的“传入邮件”[Incoming Mail] 页面）上深入访问有关此发件人的详细信息。

默认情况下，并非所有可用列都会显示。您可以通过点击表下方的“列”(Columns) 链接显示一组不同的信息。例如，您可以显示默认情况下隐藏的“由高级恶意软件保护检测”列。

“传入邮件”(Incoming Mail) 页面扩展以包含一组页面（“传入邮件”[Incoming Mail]、“发件人配置文件”[Sender Profiles] 和“发件人组报告”[Sender Group Report]）。从**传入邮件 (Incoming Mail)** 页面可以执行如下操作：

- 对已向您发送邮件的 IP 地址、域或组织（网络所有者）执行搜索。
- 查看“发件人组”(Sender Groups) 报告以根据特定的发件人组和邮件流量策略操作监控连接。有关详细信息，请参阅发件人组报告，第 648 页。
- 查看有关向您发送邮件的发件人的详细统计数据，包括按安全服务（发件人信誉过滤、反垃圾邮件、防病毒、灰色邮件等）细分的尝试发送的邮件数量。
- 按已向您发送大量垃圾邮件或病毒邮件（如反垃圾邮件或防病毒安全服务所确定）的发件人排序。
- 使用 SenderBase 信誉服务深入了解并检查特定 IP 地址、域和组织之间的关系，以获取有关发件人的详细信息。
- 深入了解特定发件人，以从 SenderBase 信誉服务获取有关发件人的详细信息，包括发件人的 SenderBase 信誉分数和域最新匹配的发件人组。将发件人添加到发件人组。
- 深入了解已发送大量垃圾邮件或病毒邮件（如反垃圾邮件或防病毒安全服务所确定）的特定发件人。

- 收集到有关域的信息后，即可通过从域、IP地址或网络所有者页面点击“添加到发件人组”(Add to Sender Group) 将 IP 地址、域或组织添加到现有发件人组（如有必要）。请参阅配置网关以接收邮件，第 61 页。

传入邮件

“传入邮件”(Incoming Mail) 页面提供访问系统中配置的所有公共侦听程序的实时活动的权限，其中包括两部分：汇总接收的顶部发件人域的邮件趋势图（按威胁邮件总数、正常邮件总数和灰色邮件总数）和“传入邮件详细信息”(Incoming Mail Details) 列表。

有关“传入邮件详细信息”(Incoming Mail Details) 列表中包含的数据的说明，请参阅传入邮件详细信息列表，第 645 页。

邮件趋势图中的时间范围说明

邮件安全监控器功能不断记录有关流入网关的邮件的数据。数据每60秒更新一次，但是，所显示的内容比当前系统时间滞后延迟 120 秒。您可以指定要包含在显示的结果中的时间范围。由于数据实时监控，因此信息会在数据库中定期更新和汇总。

从下表的时间范围选项中进行选择。

表 *80:* 邮件安全监控功能可用的时间范围

在 GUI 中选择的以下时间范围	...定义如下：
小时	最近 60 分钟 + 最多 5 分钟
天	最近 24 小时 + 最近 60 分钟
星期	最近 7 天 + 当日的耗用小时数
30 天	最近 30 天 + 当日的耗用小时数
90 天	最近 90 天 + 当日的耗用小时数
过去	00:00 到 23:59（午夜到下午 11:59）
上一日历月	当月第一天 00:00 至当月最后一天 23:59
自定义范围	通过指定的开始日期和时刻与结束日期和时刻框定的时间范围

如果已启用集中报告，则显示的时间范围选项将会不同。有关详细信息，请参阅有关“集中报告模式”的信息：在思科内容（M 系列）安全管理设备上集中管理服务，第 969 页

传入邮件详细信息列表

根据所选的视图，“传入邮件”(Incoming Mail) 页面底部的“已接收的外部域”(External Domains Received) 列表中将列出已连接到设备公共侦听程序的顶部发件人。点击列标题可对数据进行排序。有关各种类别的说明，请参阅邮件分类，第 643 页。

系统通过执行双重 *DNS* 查找，获取和验证远程主机 IP 地址（即域）的有效性。有关双向 DNS 查找和发件人验证的详细信息，请参阅配置网关以接收邮件，第 61 页。

“发件人详细信息”(Sender Detail) 列表有两个视图：“摘要”(Summary) 和“全部”(All)。

默认“发件人详细信息”(Sender Detail) 视图显示每个发件人尝试发送的邮件总数，并包括按类别的细分（与“概述”(Overview) 页面上“传入邮件摘要”(Incoming Mail Summary) 图表中的类别相同）。

“由信誉过滤拦截 (Stopped by Reputation Filtering)”值的计算取决于多种因素：

- 此发件人的“受限制”邮件数量。
- 被拒绝或被 TCP 拒绝的连接数量（可能是部分计数）。
- 每个连接的邮件数量的保守倍数。

当设备处于重负载下时，不会根据每个发件人来记录被拒绝的连接的准确计数，而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接的计数。在这种情况下，显示的值可以解释为“基准”，换句话说，大于等于该值才会拦截许多邮件。

注释 “概述 (Overview)”页面上“由信誉过滤拦截 (Stopped by Reputation Filtering)”总数始终基于所有被拒绝连接的完整计数。因负载原因，只有按发件人连接的计数受限。

可以显示的附其他列如下：

拒绝的连接 (Connections Rejected)：HAT 策略拦截的所有连接。当设备处于重负载下时，不会根据每个发件人来记录被拒绝的连接的准确计数，而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接的计数。

接受的连接 (Connections Accepted)：接受的所有连接

由收件人限制拦截 (Stopped by Recipient Throttling)：这是“由信誉过滤拦截”(Stopped by Reputation Filtering) 的组成部分。表示由于超出下列任何 HAT 限制而拦截的收件人邮件的数量：每小时的最大收件人数、每封邮件的最大收件人数或每个连接的最大邮件数。此值加上与被拒绝或被 TCP 拒绝的收件人邮件估算值就得到了“由信誉过滤拦截 (Stopped by Reputation Filtering)”的值。

由高级恶意软件防护检测 (Detected by Advanced Malware Protection)：通过文件信誉过滤发现带有恶意附件的邮件。该值不包括判定更新或由文件分析发现为恶意的文件。

威胁总数 (Total Threat)：威胁邮件（由发件人信誉拦截、作为无效收件人拦截、垃圾邮件以及病毒）的总数。

点击表格底部的“列”(Column) 链接，可显示或隐藏列。

点击列标题链接可排序列表。列标题旁边的小三角形，表示该数据当前排序所依据的列。

“没有域信息”

已连接至设备并且无法通过双重 DNS 查找进行验证的域将自动分组到名为“没有域信息”的特殊域。可以控制通过发件人验证来管理此类未验证主机的方式。请参阅配置网关以接收邮件，第 61 页。

可以通过“显示的项目”(Items Displayed) 菜单选择要在列表中显示的发件人数。

查询详细信息

对于“邮件安全监控器”(Email Security Monitor) 表中列出的发件人，请点击发件人（或“没有域信息”(No Domain Information) 链接）以深入了解特定发件人的详细信息。结果显示在“发件人配置文件”(Sender Profile) 页面上，其中包含来自 SenderBase 信誉服务的实时信息。从“发件人配置文件”(Sender Profile) 页面中，您可以深入了解有关特定 IP 地址或网络所有者的详细信息（请参阅填充了数据的报告页面：发件人配置文件页面，第 647 页）。

您还可以查看另一个报告，即“发件人组”(Sender Groups) 报告，方法是点击“传入邮件”(Incoming Mail) 页面底部的“发件人组”(Sender Groups) 报告链接。有关发件人组报告的详细信息，请参阅发件人组报告，第 648 页。

填充了数据的报告页面：发件人配置文件页面

如果点击了“传入邮件”(Incoming Mail) 页面“传入邮件详细信息”(Incoming Mail Details) 表格中的某个发件人，将列出生成的“发件人配置文件”*(Sender Profile)* 页面及特定 IP 地址、域或组织（网络所有者）的数据。“发件人配置文件”(Sender Profile) 页面显示发件人的详细信息。您可以通过点击“传入邮件”(Incoming Mail) 或其他“发件人配置文件”(Sender Profile) 页面中的指定项目，访问任何网络所有者、域或 IP 地址的“发件人配置文件”(Sender Profile) 页面。网络所有者是包含域的实体；域是包含 IP 地址的实体。有关此关系及其如何与 SenderBase 信誉服务关联的详细信息，请参阅配置网关以接收邮件，第 61 页。

针对 IP 地址、网络所有者和域显示的“发件人配置文件”(Sender Profile) 页面略有不同。不管是哪个页面，其中都包含来自该发件人的传入邮件的图形和摘要表。图表下方是列示与该发件人关联的域或 IP 地址的表格（各个 IP 地址的“发件人配置文件”(Sender Profile) 页面不包含详细列表），以及包含该发件人的当前 SenderBase、发件人组和网络信息的信息部分。

- 网络所有者配置文件页面包含网络所有者以及与该网络所有者关联的域和 IP 地址的信息。
- 域配置文件页面包含与该域关联的域和 IP 地址。
- IP 地址配置文件页面只包含有关该 IP 地址的信息。

每个发件人配置文件页面底部的“当前信息”(Current Information) 表格中都包含以下数据：

- 来自 SenderBase 信誉服务的**全局**信息，包括：
  - IP 地址、域名和/或网络所有者
  - 网络所有者类别（仅网络所有者）
  - CIDR 范围（仅 IP 地址）
  - IP 地址、域和/或网络所有者的日流量和月流量
  - 自上次从此发件人收到第一封邮件以来的天数
  - 上一个发件人组以及是否进行了 DNS 验证（仅 IP 地址发件人配置文件页面）

日流量用于衡量某个域在最近 24 小时内发送了多少邮件。SenderBase 流量类似于用来衡量地震的里氏震级，使用以 10 为底数的对数标尺计算邮件数量。该标尺的最大理论值设置为 10，等同于 100% 的实际邮件数量（大约为每天 100 亿封邮件）。使用该对数标尺时，流量每增加 1 个单位，实际数量就会增加 10 倍。

月流量的计算方法与日流量相同，只是百分比基于最近 30 天发送的邮件数量来计算。

- 平均流量（仅 IP 地址）
- 生命周期流量/30 天流量（仅 IP 地址配置文件页面）
- Bonded 发件人状态（仅限 IP 地址配置文件页面）
- SenderBase 信誉得分（仅 IP 地址配置文件页面）
- 自第一封邮件以来的天数（仅限网络所有者和域配置文件页面）
- 与此网络所有者关联的域的数量（仅网络所有者和域配置文件页面）
- 此网络所有者中的 IP 地址的数量（仅网络所有者和域配置文件页面）
- 用于发送邮件的 IP 地址的数量（仅网络所有者页面）

点击“SenderBase 的更多信息”(More from SenderBase) 链接可看到一个页面，其中包含由 SenderBase 信誉服务提供的所有信息。

- **邮件流量统计数据**信息，包含在您指定的时间范围内收集的有关该发件人的邮件安全监控信息。
- 有关此网络所有者控制的域和 IP 地址的**详细信息**，将显示在网络所有者配置文件页面。有关域中的 IP 地址的详细信息，将显示在域页面。

  从域配置文件页面中，可深入了解特定 IP 地址，也可深入查看组织配置文件页面。您还可以通过点击“IP 地址”(IP Addresses) 表底部的“列”(Columns) 链接，为该表中的每个发件人地址显示“已经过 DNS 验证”(DNS Verified) 状态、SBRS（SenderBase 信誉分数）和“上一发件人组”(Last Sender Group)。您还可以隐藏该表中的任何列。

  从网络所有者配置文件页面中，您可以通过点击“域”(Domains) 表底部的“列”(Columns) 链接，显示该表中各域的“拒绝的连接”(Connections Rejected)、“接受的连接”(Connections Accepted)、“由收件人限制拦截”(Stopped by Recipient Throttling) 以及“由高级恶意软件防护检测”(Detected by Advanced Malware Protection) 等信息。还可以隐藏该表中的任何列。

  如果您是系统管理员，在其中每个页面，都可以选择将网络所有者、域或 IP 地址添加到发件人组，方法是点击实体的复选框（如果需要），然后点击“添加到发件人组”(Add to Sender Group)。

  此外，也可以点击发件人“当前信息”(Current Information) 表中“发件人组信息”(Sender Group Information) 下方的**添加到发件人组 (Add to Sender Group)** 链接，再点击“添加到发件人组”(Add to Sender Group)，将该发件人添加到发件人组。有关将发件人添加到发件人组的详细信息，请参阅配置网关以接收邮件，第 61 页。当然，您不必进行任何更改 - 可以让安全服务来处理传入邮件。

发件人配置文件搜索

在“快速搜索”(Quick Search) 方框中键入 IP 地址、域或组织名称，以搜索特定发件人。

系统将显示包含发件人信息的“发件人配置文件”(Sender Profile) 页面。请参阅填充了数据的报告页面：发件人配置文件页面，第 647 页。

发件人组报告

“发件人组 (Sender Groups)”报告按发件人组和邮件流量策略操作提供连接摘要，使您能够查看 SMTP 连接和邮件流策略趋势。“按发件人组的邮件流量 (Mail Flow by Sender Group)”列表显示每个发件人组的连接的百分比和数量。“按邮件流量策略操作的连接 (Connections by Mail Flow Policy

Action)”图表显示每个邮件流量策略操作的连接的百分比。此页面概述了主机访问表 (HAT) 策略的有效性。有关 HAT 的详细信息，请参阅配置网关以接收邮件，第 61 页。

传出目标

“传出邮件目标”(Outgoing Destinations) 页面提供有关您的公司发送邮件所至的域的信息。该页面包含两部分。页面的上半部分包含图形，这些图形在页面的上半部分描绘按传出威胁邮件划分的排名靠前的目标，以及按传出正常邮件划分的排名靠前的目标。页面下半部分显示一个图表，包含按收件人总数（默认设置）排序的所有列。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式。

“外发目标”(Outgoing Destinations) 页面可用于回答以下类型的问题：

- 设备将邮件发送到哪些域？
- 向每个域发送多少邮件？
- 该邮件中有多少是正常的、具有垃圾邮件特征、具有病毒特征、具有恶意软件特征或由内容过滤器拦截？
- 传送了多少邮件以及被目标服务器硬性退回了多少邮件？

传出邮件发件人

“传出邮件发件人”(Outgoing Senders) 页面提供有关正从网络内的 IP 地址和域发送的邮件数量和类型的信息。查看此页面时，可以按域或 IP 地址查看结果。如果您要查看每个域正在发送的邮件的数量，则可能要按域查看结果；如果要查看哪些 IP 地址发送的病毒邮件最多或者正在触发内容过滤器，则可能要按 IP 地址查看结果。

该页面包含两部分。页面左侧是一个描绘按威胁邮件总数排名靠前的发件人的图形。威胁邮件总数包括具有垃圾邮件特征、病毒特征的邮件，恶意软件邮件或触发了内容过滤器的邮件数量。页面右侧是一个图形，在页面上半部分显示按正常邮件数量排名靠前的发件人。页面下半部分显示一个图表，其中显示按邮件总数（默认设置）排序的所有列。

注释 此页面未显示有关邮件发送的信息。可以使用“传送状态”(Delivery Status) 页面跟踪传送信息，例如，退回的来自特定域的邮件数。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式。

“传出发件人”(Outgoing Senders) 页面可用于回答以下类型的问题：

- 哪些 IP 地址正在发送最具病毒特征、垃圾邮件特征的邮件或恶意软件邮件？
- 哪些 IP 地址触发内容过滤器的频率最高？
- 哪些域发送的邮件最多？

“地理分布”页面

可以使用“地理分布”报告页面查看：

- 以图形格式显示的基于来源国家/地区的传入邮件连接排行榜。
- 基于源国家/地区的传入邮件连接总数（采用表格格式）

您可以点击特定地理位置的传入邮件连接数来查看邮件跟踪中的相关消息。

“邮件总数”列仅显示在 SMTP 连接级别接受的邮件。

注释 报告生成期间：

- 如果将一个或多个传入邮件连接检测为私有 IP 地址，则这些传入邮件连接将在报告中归类为“私有 IP 地址”。
- 如果将一个或多个传入邮件连接检测为非有效 SBRS 得分，则这些传入邮件连接将在报告中归类为“无国家/地区信息”。

“传送状态”(Delivery Status) 页面

如果您怀疑向特定收件人域进行传送有问题，或者如果要收集有关虚拟网关地址的信息，则“监控”(Monitor) >“传送状态”(Delivery Status) 页面会提供有关与特定收件人域相关的邮件操作的监控信息。

“**传送状态**”**页面**显示的信息与 CLI 中的 tophosts 命令所示的信息相同。（有关详细信息，请参阅使用 CLI 进行管理和监控，第 805 页中的“确定邮件队列的构成”）

此页面显示系统在过去三个小时内传送的邮件的前 20、50 或 100 个收件人域列表。可以通过点击每项统计数据列标题中的链接，按最新主机状态、有效收件人（默认）、连接超时、发送的收件人、软退回事件以及硬退回收件人进行排序。

- 要搜索特定域，请在“域名：”(Domain Name:) 字段中键入域的名称，然后点击**搜索 (Search)**。
- 要深入查看所示的域，请点击域名链接。

结果显示在“传送状态详细信息”(Delivery Status Details) 页面中。

注释 收件人域的任何活动都会导致该域处于“活动”状态，因此会出现在概述页面中。例如，如果邮件由于传送问题而保持处于出站队列中，则该收件人域会继续列在传出邮件概述中。

重试传送

点击**重试所有传送 (Retry All Delivery)**，可立即重试计划稍后传送的邮件。“重试所有传送”(Retry All Delivery) 允许您重新安排立即传送队列中的邮件。标记为“已关闭”的所有域以及任何已计划或软退回的邮件会加入队列等候立即传送。

要重试传送到特定目标域，请点击域名链接。在“传送状态详细信息”(Delivery Status Details) 页面，点击**重试传送 (Retry Delivery)**。

您也可以在 CLI 中使用 delivernow 命令来重新安排立即传送邮件。有关详细信息，请参阅安排邮件立即传送，第 825 页。

“传送状态详细信息”(Delivery Status Details) 页面

使用“**传送状态详细信息**”**页面**可以查找有关特定收件人域的统计数据。此页面显示的信息与 CLI 内的**hoststatus** 命令所示的信息相同：邮件状态、计数器和计量器。（有关详细信息，请参阅使用 CLI 进行管理和监控，第 805 页）要搜索特定域，请在“域名:”字段中键入域的名称，然后点击**搜索**。如果使用的是 **altsrchost** 功能，则会显示虚拟网关地址信息。

“内部用户”页面

“内部用户”页面按邮件地址提供有关内部用户发送和接收的邮件的信息（一个用户可能列出了多个邮件地址 - 报告中不合并邮件地址）。

该页面包含两部分：

- 描述按正常传入和传出邮件排名靠前用户和收到灰色邮件的靠前用户的图表。
- 用户邮件流量详细信息

您可以选择报告时间范围（小时、天、周或月）。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式。您还可以通过点击表下方的“列”(Columns) 链接显示隐藏表列或隐藏默认列。

“用户邮件流量详细信息”(User Mail Flow Details) 列表将每个邮件邮件地址收到和发送的邮件细分为“正常”(Clean)、“检测到垃圾邮件”(Spam Detected)（仅限传入）、“检测到病毒”(Virus Detected) 和“内容过滤器匹配”(Content Filter Matches)。您可以通过点击列标题对列表排序。

使用“内部用户”(Internal Users) 报告，您可以回答以下类型的问题：

- 谁发送的外部邮件最多？
- 谁接收的正常邮件最多？
- 谁接收的灰色邮件最多？
- 谁接收的垃圾邮件最多？
- 谁在触发哪些内容过滤器？
- 谁的邮件被内容过滤器捕获？

入站内部用户是基于“收件人: (Rcpt To:)”地址为其接收邮件的用户。出站内部用户基于“发件人: (Mail From:)”地址，在跟踪内部网络中的发件人所发送邮件的类型时非常有用。

请注意，某些出站邮件（如退回邮件）的发件人为空。它们计数在出站和“未知”下面。

点击内部用户可查看该用户的“内部用户”(Internal User) 详细信息页面。

点击表下方的“列”链接可显示默认隐藏的列，例如“由高级恶意软件防护检测到的传入邮件”列或“由高级恶意软件防护检测到的传出邮件”列。

“内部用户详细信息”(Internal User Details)

“内部用户详细信息”(Internal User detail) 页面显示有关指定用户的详细信息，包括显示每个类别（检测到垃圾邮件、检测到病毒、由高级恶意软件保护检测到、由内容过滤器拦截、检测到灰色邮件和正常）邮件数量的传入和传出邮件明细。或者，对于传入邮件，您可以点击表下方的“列”(Columns) 链接来显示“由高级恶意软件防护检测到的传入邮件”(Incoming Detected by Advanced Malware Protection) 列。该值反映包含被文件信誉过滤确定为恶意的附件的邮件数量。它不包括判定更新或由文件分析发现为恶意的文件。此外，还会显示传入和传出内容过滤器及 DLP 策略匹配项。

点击内容过滤器的名称可在相应的内容过滤器信息页面上查看该过滤器的详细信息（请参阅“内容过滤器”(Content Filters) 页面，第 653 页）。您可以使用此方法获取也发送或接收与该特定内容过滤器匹配的邮件的用户列表。

搜索特定的内部用户

您可以通过“内部用户”(Internal Users) 页面和“内部用户详细信息”(Internal User detail) 页面底部的搜索表单搜索特定内部用户（邮件地址）。选择是完全匹配搜索文本还是查找以输入的文本开头的项目（例如，以“ex”开头将匹配“example.com”）。

“DLP 事件”页面

“DLP 事件 (DLP Incidents)”页面显示有关在传出邮件中发生的防数据丢失 (DLP) 策略违规事件的信息。设备使用在“传出邮件策略 (Outgoing Mail Policies)”表中启用的 DLP 邮件策略来检测用户发送的敏感数据。违反 DLP 策略的每个外发邮件均报告为一个事件。

使用“DLP 事件”(DLP Incidents) 报告，您可以回答以下类型的问题：

- 用户发送什么类型的敏感数据？
- 这些 DLP 事件具有什么样的严重性？
- 发送了多少封邮件？
- 丢弃了多少封邮件？
- 是谁在发送这些邮件？

“DLP 事件”(DLP Incidents) 页面包含两个主要部分：

- DLP 事件趋势图，按严重性（低、中、高、关键）和策略匹配项汇总排名靠前的 DLP 事件，以及
- “DLP 事件详细信息”(DLP Incidents Details) 列表。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式；或通过点击**可打印 (PDF) (Printable (PDF))** 链接导出为 PDF 格式。有关生成英语以外的其他语言的 PDF 的信息，请参阅有关报告的注意事项，第 667 页。

点击 DLP 策略的名称，可查看有关策略检测到的 DLP 事件的详细信息。您可以使用此方法获取发送了包含策略检测到的敏感数据的邮件的用户列表。

DLP 事件详细信息

当前在设备的传出邮件策略中启用的 DLP 策略列于“DLP 事件”(DLP Incidents) 页面底部的“DLP 事件详细信息”(DLP Incidents Details) 表中。点击 DLP 策略的名称可查看更多详细信息。

“DLP 事件详细信息”表显示了每个策略的 DLP 事件总数，并按严重性级别细分。严重性级别还包括已退回的邮件数，以及在清除、已发送的加密或删除的邮件中传递的邮件数。点击列标题可对数据进行排序。

“DLP 策略详细信息”页面

如果点击“DLP 事件详细信息 (DLP Incidents Details)”表中某个 DLP 策略的名称，则随之打开的“DLP 策略详细信息 (DLP Policy Detail)”页面会显示该策略的 DLP 事件数据。该页面根据严重性显示有关 DLP 事件的图形。

该页面还包括一个位于页面底部的“按发件人的事件 (Incidents by Sender)”列表，其中列出发送违反 DLP 策略的邮件的每个内部用户。该列表还按用户显示每个策略的 DLP 事件总数，按严重级别进行细分，并且显示邮件是以明文形式发送、以加密形式发送还是已经丢弃。可以使用“按发件人的事件”(Incidents by Sender) 表，了解哪些用户可能正在将组织的敏感数据发送给网络以外的人员。

点击发件人名称，将打开“内部用户”(Internal Users) 页面。有关详细信息，请参阅“内部用户”页面，第 651 页。

“内容过滤器”(Content Filters) 页面

“内容过滤器”(Content Filters) 页面通过两种形式显示排名靠前的传入和传出邮件内容过滤器匹配项（匹配邮件数量最多的内容过滤器）：条形图和列表。使用“内容过滤器”(Content Filters) 页面，可以按内容过滤器或按用户查看企业策略，并回答以下类型的问题：

- 传入或传出邮件触发哪些内容过滤器的次数最多？
- 哪些用户在发送或接收触发特定内容过滤器的邮件方面排名靠前？

您可以点击列表中内容过滤器的名称，以在“内容过滤器详细信息”(Content Filter detail) 页面上查看有关该过滤器的详细信息。

内容过滤器详细信息

“内容过滤器详细信息”(Content Filter detail) 页面随时间推移显示该过滤器的匹配项，以及按内容用户划分的匹配项。

在“按内部用户划分的匹配项”(Matches by Internal User) 部分中，您可以点击用户的名称来查看该内部用户的（邮件地址）“内部用户”(Internal User) 详细信息页面（请参阅“内部用户详细信息”(Internal User Details)，第 652 页）。

“DMARC 验证”页面

“DMARC 验证”(DMARC Verification) 页面显示 DMARC 验证失败的排名靠前的域，以及 AsyncOS 对 DMARC 验证失败的邮件执行的操作的详细信息。可以使用此报告优化 DMARC 设置并回答以下类型的问题：

- 哪些域发送的不符合 DMARC 的邮件数量最多？
- 对于每个域，AsyncOS 对 DMARC 验证失败的邮件执行什么操作？

“DMARC 验证”(DMARC Verification) 页面包含：

- 条形图，显示按 DMARC 验证失败次数排名靠前的域。
- 对于每个域，用表格显示以下信息：
  - 已拒绝、已隔离或已接受但未采取任何操作的邮件数量。点击数值可查看选定类别下的邮件的列表。
  - 通过 DMARC 验证的邮件的数量。
  - DMARC 验证尝试总数。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式；或通过点击**可打印 (PDF) (Printable (PDF))** 链接导出为 PDF 格式。

“宏检测”页面

可以使用“宏检测”报告页面查看：

- 以图形和表格格式显示的按文件类型排名靠前的启用宏的传入附件。
- 以图形和表格格式显示的按文件类型排名靠前的启用宏的传出附件。

您可以点击启用宏的附件数量，以在邮件跟踪中查看相关邮件。

注释 在生成报告期间：

- 如果在存档文件中检测到一个或多个宏，则“存档文件”文件类型将递增一。不计算存档文件中启用了宏的附件数量。
- 如果在嵌入文件中检测到一个或多个宏，则父文件类型将递增一。不计算嵌入文件中启用宏的附件数量。

“病毒爆发过滤器”页面

“爆发过滤器”(Outbreak Filters) 页面显示设备上的爆发过滤器的当前状态和配置，以及有关近期病毒爆发和因爆发过滤器而隔离的邮件的信息。使用此页面可以监控对针对性病毒、诈骗和网络钓鱼攻击的防御。

“按类型划分的威胁”(Threats By Type) 部分显示设备接收的不同类型的威胁邮件。

“威胁摘要”(Threat Summary) 部分按恶意软件、网络钓鱼、垃圾邮件和病毒显示威胁邮件的细分。点击数值可使用“邮件跟踪”(Message Tracking) 查看该数值中包含的所有邮件的列表。

“过去一年爆发摘要 (Past Year Outbreak Summary)”会列出过去一年的全局及局部爆发，以便将局部网络趋势与全局趋势进行比较。全球爆发列表是所有爆发情况（包括病毒和非病毒）的超集，而局部爆发仅限于影响设备的病毒爆发。局部爆发数据不包括非病毒威胁。全局爆发数据会显示由威胁操作中心检测到的超出当前为爆发隔离区配置的阈值的所有爆发。本地病毒爆发数据显示在此设备上检测到的超出当前为爆发隔离区配置的阈值的所有病毒爆发。局部保护总时间始终基于威胁操作中心检测到各个病毒爆发的时间与主要供应商发布防病毒特征码的时间之间的差异。请注意，并非每个全局爆发都会影响设备。值“--”表示保护时间不存在，或防病毒供应商未提供特征码时间（某些供应商可能不报告特征码时间）。这并不表示保护时间为零，而是表示计算保护时间所需的信息不可用。

“隔离的邮件 (Quarantined Messages)”部分汇总爆发过滤器隔离情况，是测量爆发过滤器捕获的潜在威胁邮件数的有用计量器。隔离的邮件在放行时计数。通常，邮件在防病毒和反垃圾邮件规则可用之前会被隔离。放行时，它们会被防病毒和反垃圾邮件软件进行扫描并确定是阳性还是正常邮件。由于爆发跟踪的动态性质，当邮件处于隔离区中时，用于隔离邮件的规则（甚至关联的爆发）可能会更改。在释放时对邮件计数（而不是在进入隔离区时计数）可避免计数增加和降低引起的混乱。

威胁详细信息列表会显示有关特定爆发的信息，包括威胁类别（病毒、欺诈或网络钓鱼）、威胁名称、威胁说明和确定的邮件数。对于病毒爆发，“过去一年的病毒爆发 (Past Year Virus Outbreaks)”包括爆发名称和ID、首次全局出现病毒爆发的时间和日期、爆发过滤器提供的保护时间以及隔离的邮件数。您可以通过左侧菜单选择要显示的全局或本地病毒爆发以及邮件数。您可以通过点击列标题对列表排序。点击数值可使用“邮件跟踪”(Message Tracking) 查看该数值中包含的所有邮件的列表。

首次全局出现时间由威胁防御运营中心根据 SenderBase（全球最大的邮件和网络流量监控网络）中的数据确定。保护时间是基于威胁防御运营中心检测到每个威胁的时间与主要供应商发布防病毒签名的时间之间的时间差。

值“--”表示保护时间不存在，或防病毒供应商未提供特征码时间（某些供应商可能不报告特征码时间）。这并不表示保护时间为零。相反，这表示计算保护时间所需的信息不可用。

“来自传入邮件的命中邮件”(Hit Messages from Incoming Messages) 部分显示病毒附件、其他威胁（非病毒）和正常传入邮件的百分比和数量。

“按威胁级别划分的命中邮件”(Hit Messages by Threat Level) 部分根据威胁级别（级别 1 到 5）显示传入威胁邮件（病毒和非病毒）的百分比和数量。

“位于病毒爆发隔离区的邮件”(Messages resided in Outbreak Quarantine) 部分根据持续时间显示位于病毒爆发隔离区中的威胁邮件的数量。

“排名靠前的已重写 URL”(Top URL's Rewritten) 部分根据出现次数显示排名前 10 位的已重写 URL 的列表。使用“显示的项目”(Items Displayed) 下拉菜单可查看更多已重写URL。点击数值可在“邮件跟踪”(Message Tracking) 页面上查看包含所选已重写 URL 的所有邮件的列表。

使用“爆发过滤器”(Outbreak Filters) 页面可回答如下问题：

- 有多少邮件被隔离？它们属于什么类型的威胁？
- 为病毒爆发提供爆发过滤器功能的交付期是多久？

- 我的本地病毒爆发如何与全局病毒爆发进行比较？

“病毒类型”(Virus Types) 页面

“病毒类型”(Virus Types) 页面提供发送到网络以及从网络发出的病毒的概述。“病毒类型”(Virus Types) 页面显示已由设备中运行的病毒扫描引擎检测到的病毒。您可能希望使用此报告针对特定病毒采取特定操作。例如，如果发现收到已知嵌入 PDF 文件中的大量病毒，则您可能要创建过滤器操作来隔离具有 PDF 附件的邮件。

如果运行多个病毒扫描引擎，则“病毒类型 (Virus Types)”页面包括来自所有启用的病毒扫描引擎的结果。显示在该页面上的病毒的名称由病毒扫描引擎确定。如果多个扫描引擎检测到某个病毒，则同一病毒可能具有多个对应的条目。

“病毒类型”(Virus Types) 页面提供从网络发出或发送到网络的病毒的概述。“检测到的排名靠前的传入病毒”(Top Incoming Virus Detected) 部分以降序显示已发送到网络的病毒的图表视图。“检测到的排名靠前的传出病毒”(Top outgoing Virus Detected) 部分以降序显示从网络发出的病毒的图表视图。

注释 要查看哪些主机将感染病毒的邮件发送到您的网络，您可以转至“传入邮件”(Incoming Mail) 页面，指定同一报告周期并按具有病毒特征排序。同样，要查看哪些 IP 地址在您的网络中发送了病毒阳性邮件，可查看“传出邮件发件人”(Outgoing Senders) 页面，并按病毒阳性邮件排序。

“病毒类型详细信息”(VirusTypes Details) 列表显示有关特定病毒的信息，包括受感染的传入和传出邮件及受感染的邮件总数。受感染的传入邮件的详细信息列表显示病毒名称以及感染此病毒的传入邮件的数量。同样，传出邮件显示病毒名称以及感染此病毒的传出邮件的数量。您可以按“传入邮件数”(Incoming Messages)、“传出邮件数”(Outgoing Messages) 和“受感染邮件总数”(Total Infected Messages) 对病毒类型详细信息进行排序。

“URL 过滤”页面

- 仅当启用了 URL 过滤时，才会填充 URL 过滤报告模块。
- URL 过滤报告适用于传入和传出邮件。
- 只有 URL 过滤引擎（作为反垃圾邮件/爆发过滤器扫描一部分或通过邮件/内容过滤器）扫描的邮件会包含在这些模块中。但是，并非所有结果都一定具体归因于 URL 过滤功能。
- 排名靠前的URL类别模块包括在已扫描的邮件中发现的所有类别，不管这些邮件是否匹配内容或邮件过滤器。
- 每封邮件都只能与一个 URL 信誉级别相关。对于具有多个 URL 的邮件，统计数据会反映邮件中任何 URL 的最低信誉。
- 在“安全服务 (Security Services)”>“URL 过滤 (URL Filtering)”中配置的全局白名单中的 URL 不包含在报告中。

  在各个过滤器的白名单中使用的 URL 会包含在报告中。

- 恶意 URL 是爆发过滤器确定为信誉不佳的 URL。不确定 URL 是爆发过滤器确定需要点击时间保护的 URL。因此，不确定 URL 已被重写，从而重定向到思科网络安全代理。

- 基于 URL 类别的过滤器的结果会反映在内容和邮件过滤器报告中。
- 思科网络安全代理的点击时间 URL 评估结果不会反映在报告中。

“网络交互跟踪”页面

- 只有启用了网络交互跟踪功能，才能填充网络交互跟踪报告。
- 网络交互跟踪报告模块不会实时更新，而是每 30 分钟刷新一次。此外，点击重写的 URL 后，网络交互跟踪报告最长可能需要两小时，才会报告此事件。
- 网络交互跟踪报告不会实时更新。点击云重定向的重写URL后，网络交互跟踪报告最长可能需要两小时，才会报告此事件。
- 网络交互跟踪报告适用于传入和传出邮件。
- 这些模块中仅包含终端用户（通过策略或爆发过滤器）点击的云重定向重写 URL。
- “网络交互跟踪”(Web Interaction Tracking) 页面包括以下报告：

终端用户点击的排名靠前的重写恶意 URL。点击某个 URL，可查看包含以下信息的详细报告：

- 点击了重写恶意 URL 的终端用户列表。
- 点击该 URL 的日期和时间。
- 该 URL 由策略还是爆发过滤器重写。
- 点击重写的URL时采取的操作（允许、阻止或未知）。请注意，如果由爆发过滤器重写URL，且最终判定不可用，则状态显示为未知。

点击重写的恶意 URL 的排名靠前的终端用户

网络交互跟踪详细信息。包括以下信息：

- 所有云重定向重写 URL（恶意和非恶意）的列表。点击某个 URL 可查看详细报告。
- 点击云重定向重写的 URL 时采取的操作（允许、阻止或未知）。

要显示数据，请执行以下操作：

- 选择**传入邮件策略 > 爆发过滤器**配置爆发过滤器，并启用邮件修改和 URL 重写。
- 为内容过滤器配置“**重定向到思科安全代理**”操作。

请注意，如果终端用户点击某个URL时，其判定（正常或恶意）未知，则状态将显示为未知。这可能是因为，需要进一步审查该 URL，或用户点击时网络服务器停止服务或无法访问。

- 终端用户点击重写的 URL 的次数。点击数字可查看包含可点击的 URL 的所有邮件列表。
- 在使用网络交互跟踪报告时，请记住以下限制：
  - 如果已将内容或邮件过滤器配置为重写恶意 URL 后传送邮件并通知其他用户（例如管理员），则原始收件人的网络交互跟踪数据将增加，即使获得通知的用户点击的是重写的 URL 也不例外。
  - 如果使用 Web 界面将包含重写 URL 的被隔离邮件副本发送给用户（例如管理员），则原始收件人的网络交互跟踪数据将增加，即使接收邮件副本的用户点击的是重写的URL也不例外。
  - 在任何时候，如果您计划修改设备时间，请确保系统时间与协调世界时 (UTC) 同步。

伪造邮件匹配项报告

请参阅监控伪造邮件检测结果，第 479 页。

文件信誉和文件分析报告

对于以下报告，请参阅文件信誉和文件分析报告与跟踪，第 368 页：

- 高级恶意软件保护
- 文件分析
- AMP 判定更新

邮箱自动修复报告

您可以使用“邮箱自动修复”报告页面（**监控** > **邮箱自动修复**）查看邮箱修复结果的详细信息。使用此报告可以查看详细信息，如：

- 其邮箱修复成功或不成功的收件人列表
- 对邮件执行的修复操作
- 与 SHA-256 哈希关联的文件名

点击 SHA-256 哈希以在邮件跟踪中查看相关邮件。

有关详细信息，请参阅 自动修补 Office 365 邮箱中的邮件，第 435 页

“TLS 连接”页面

“TLS 连接”(TLS Connections) 页面显示所收发邮件的 TLS 连接的整体使用情况。该报告还显示使用 TLS 连接发送邮件的每个域的详细信息。

“TLS 连接 (TLS Connections)”页面可用于确定以下信息：

- 总体而言，传入和传出连接的哪个部分使用 TLS？
- 我与哪些合作伙伴成功建立了 TLS 连接？
- 我未与哪些合作伙伴成功建立 TLS 连接？
- 哪些合作伙伴的 TLS 证书存在问题？
- 某个合作伙伴使用 TLS 的邮件占总邮件的百分比是多少？

“TLS 连接”(TLS Connections) 页面分为传入连接部分和传出连接部分。每个部分都包含图表、摘要和详细信息表。

图形显示指定时间范围内的传入或传出 TLS 加密和未加密连接的视图。该图形显示邮件总数、加密和未加密邮件的数量，以及成功和失败的 TLS 加密邮件的数量。需要 TLS 的连接图表和仅首选 TLS 的连接图表有所不同。

此表显示发送或接收加密邮件的域的详细信息。对于每个域，您可以查看成功和失败的必需 TLS 连接和首选 TLS 连接的数量、TLS 连接尝试总数（无论成功还是失败）以及未加密连接总数。您也可

以查看尝试 TLS 的所有连接的百分比以及成功发送的加密邮件的总数，无论 TLS 是首选还是必需。您可以通过点击此表底部的“列”(Columns) 链接来显示或隐藏列。

入站 SMTP 身份验证页面

“入站 SMTP 身份验证 (Inbound SMTP Authentication)”页面显示如何使用客户端证书和 SMTP AUTH 命令对邮件安全设备与用户的邮件客户端之间的 SMTP 会话进行验证。如果设备接受证书或 SMTP AUTH 命令，则其将会建立到邮件客户端的 TLS 连接，客户端将使用该连接发送邮件。由于设备无法跟踪每个用户进行的尝试，因此报告会基于域名和域 IP 地址显示有关 SMTP 身份验证的详细信息。

使用此报告可确定以下信息：

- 总体而言，多少入站连接使用 SMTP 身份验证？
- 多少连接使用客户端证书？
- 多少连接使用 SMTP AUTH？
- 当尝试使用 SMTP 身份验证时，哪些域无法连接？
- 当 SMTP 身份验证失败时，多少连接成功使用回退？

“入站 SMTP 身份验证 (Inbound SMTP Authentication)”页面包括已接收连接的图表，尝试 SMTP 身份验证连接的邮件收件人图表,以及包含身份验证连接尝试详细信息的表格。

“接收的连接 (Received Connections)”图表显示来自在指定的时间范围内尝试使用 SMTP 身份验证对连接进行身份验证的邮件客户端的传入连接。该图形显示设备已接收的连接总数、未尝试使用 SMTP 身份验证进行身份验证的连接数、使用客户端证书对连接进行身份验证成功和失败的连接数，以及使用 SMTP AUTH 命令进行身份验证失败和成功的连接数。

“已接收的收件人”(Received Recipients) 图形显示了收件人的数量，这些收件人的邮件客户端尝试对其与邮件安全设备的连接进行身份验证以使用 SMTP 身份验证来发送邮件。该图形还显示其连接已进行身份验证的收件人数和其连接未进行身份验证的收件人数。

“SMTP 身份验证详细信息”(SMTP Authentication details) 表显示了域的详细信息，这些域的用户尝试对其与邮件安全设备的连接进行身份验证以发送邮件。对于每个域，您可以查看使用客户端证书进行的成功或失败的连接尝试数、使用 SMTP AUTH 命令进行的成功或失败的连接尝试数，以及在其客户端证书连接尝试失败后回退到 SMTP AUTH 的连接尝试数。可以使用页面顶部的链接按域名或域 IP 地址显示此信息。

速率限制页面

通过按信封发件人的速率限制可以根据发件人地址按各个发件人的时间间隔限制邮件收件人数。“速率限制 (Rate Limits)”报告显示最显著超过该限制的发件人。

使用此报告有助于确定以下内容：

- 可能被用于批量发送垃圾邮件的受侵害用户帐户。
- 组织中的失控应用程序，这些应用程序使用邮件发送通知、警报、自动声明等内容。
- 组织中具有大量邮件活动的来源，用于内部计费或资源管理目的。
- 可能不会被视为垃圾邮件的大量入站邮件流量的来源。

请注意，包含内部发件人（例如内部用户或传出邮件发件人）的统计信息的其他报告仅测量已发送的邮件数；它们不会向大量收件人表明少数邮件的发件人的身份。

“按事件划分的排名靠前的危害”图表显示最频繁尝试向超过配置限制的收件人发送邮件的信封发件人。每次尝试被视为一个事件。此图表汇聚来自所有侦听程序的事件计数。

“按拒绝的收件人排名靠前的入侵者 (Top Offenders by Rejected Recipients)”图表显示将邮件发送给超出所配置限制的最大数量收件人的信封发件人。此图表汇总所有侦听程序的收件人计数。

要按信封发件人配置速率限制或修改现有速率限制，请参阅使用邮件流策略定义传入邮件规则，第 93 页。

系统容量页面

“系统容量”(System Capacity) 页面提供有关系统负载的详细说明，包括工作队列中的邮件、花费在工作队列中的平均时间、传入和传出邮件（总量、大小和数量）、总体 CPU 使用率、按功能的 CPU 使用率和内存页面交换信息。

“系统容量”(System Capacity) 页面可用于确定以下信息：

- 确定设备超出建议容量的时间以及需要配置优化或额外设备的时间。
- 确定系统行为方面指向即将发生的容量问题的历史趋势。
- 确定系统的哪个部分正在使用大部分资源，以协助进行故障排除。

监控设备以确保容量适合邮件量是十分重要的。随着时间的推移，邮件量会不可避免地增加，适当的监控可确保主动添加容量或进行配置更改。监控系统容量的最有效方式是跟踪总量、工作队列中的邮件以及资源节约模式下的事件。

- **邮件量**：请务必了解环境中的“正常”邮件量和“正常”峰值。随着时间的推移跟踪此数据以测量邮件量增长。可以使用“传入邮件 (Incoming Mail)”和“外发邮件 (Outgoing Mail)”页面随着时间的推移跟踪邮件量。有关详细信息，请参阅系统容量 - 传入邮件，第 661 页和系统容量 - 传出邮件，第 661 页。
- **工作队列**：工作队列旨在充当“缓冲器”-吸收和过滤垃圾邮件攻击并处理正常邮件的不正常增加情况。但是，工作队列也是系统不堪重负的最佳指示器，长时间的频繁工作队列备份可能表示容量问题。您可以使用“工作队列”(WorkQueue) 页面跟踪邮件花在工作队列中的平均时间以及工作队列中的活动。有关详细信息，请参阅系统容量 - 工作队列，第 660 页。
- **资源节约模式**：当设备变得过载时，会进入资源节约模式 (RCM)，并发送“关键”(CRITICAL) 系统警报。这旨在保护设备，使其可以处理任何邮件积压情况。设备不能频繁进入 RCM 模式，只能在邮件量非常大或不正常增加时才能进入 RCM 模式。频繁的 RCM 警报可以表示系统变得过载。请参阅系统容量 - 系统负载，第 661 页。

系统容量 - 工作队列

“工作队列”(Workqueue) 页面显示邮件在工作队列中花费的平均时间，不含花费在垃圾邮件隔离区或策略、病毒或爆发隔离区中的任何时间。您可以查看时间段，从一小时到一个月。此平均值可以帮助确定延迟邮件传送的短期事件和确定系统上工作负载的长期趋势。

注释 如果邮件从隔离区释放到工作队列中，“工作队列中的平均时间”指标将忽略此时间。这可以防止因延长花在隔离区中的时间而出现重复计数和错误的统计信息。

此报告也显示指定时间段内的工作队列中的邮件量，并且显示相同时间段内工作队列中的最大邮件数量。工作队列中的最大邮件数图表还显示工作队列阈值级别。

工作队列图中的偶尔出现峰值是正常的，符合预期。如果工作队列中的邮件数长时间保持高于配置的阈值，可能表示存在容量问题。这种情况下，请考虑调整阈值级别或审核系统配置。

有关更改工作队列阈值级别的说明，请参阅为系统运行状况参数配置阈值 ， 第 775 页。

提示 在查看工作队列页面时，可能要测量工作队列备份的频率，并记下超过 10,000 个邮件的工作队列备份。

系统容量 - 传入邮件

传入邮件页面显示传入连接、传入邮件总数、平均邮件大小和传入邮件总大小。您可以将结果限制到指定的时间范围。了解环境中的正常邮件量和峰值趋势至关重要。您可以使用传入邮件页面随着时间的推移跟踪邮件量增长并规划系统容量。您可能还希望比较传入邮件数据与发件人配置文件数据，以查看从特定域发送到网络的邮件量的趋势。

注释 传入连接数增加不一定会影响系统负载。

系统容量 - 传出邮件

传出邮件页面显示传出连接、传出邮件总数、平均邮件大小和传出邮件总大小。您可以将结果限制到指定的时间范围。了解环境中的正常邮件量和峰值趋势至关重要。您可以使用传出邮件页面随着时间的推移跟踪邮件量增长并规划系统容量。您可能还要将“传出邮件”(Outgoing Mail) 数据与“外发目标”(Outgoing Destinations) 数据进行比较，以查看从特定域或 IP 地址发送的邮件量的趋势。

系统容量 - 系统负载

系统负载报告显示如下信息：

- CPU 总体使用情况
- 内存页面交换
- 资源节约活动

CPU 总体使用情况

邮件安全设备经过优化，可使用空闲 CPU 资源来提高邮件吞吐量。高 CPU 使用率并不一定表示存在系统容量问题。如果高 CPU 使用率与持续的大容量内存页面交换一同出现，则可能表示存在容量问题。

注释 此图还显示 CPU 的阈值级别。如果要更改阈值级别，请在 Web 界面中依次使用**系统管理 (System Administration)** > **系统运行状况 (System Health)** 页面或在 CLI 中使用 **healthconfig** 命令。请参阅为系统运行状况参数配置阈值，第 775 页。

该页面还包含一个图，用于显示不同功能（包括邮件处理、垃圾邮件和病毒引擎、报告和隔离）使用的 CPU 量。按功能显示的 CPU 图表可指示产品的哪些部分占用系统上的大多数资源。如果需要优化设备，则此图有助于确定哪些功能可能需要调整或禁用。

内存页面交换

内存页面交换图显示系统必须切换到磁盘的频率。此图还显示内存页面交换的阈值级别。如果要更改阈值级别，请在 Web 界面中依次使用**系统管理 (System Administration)** > **系统运行状况 (System Health)** 页面或在 CLI 中使用 **healthconfig** 命令。请参阅为系统运行状况参数配置阈值，第 775 页。

资源节约活动

资源节约活动图显示设备进入资源节约模式 (RCM) 的次数。例如，如果图中显示 n 次，则意味着设备进入了 RCM n 次，并已退出至少 n-1 次。

设备不能频繁进入 RCM 模式，只能在邮件量非常大或不正常增加时才能进入 RCM 模式。如果资源节约活动图显示您的设备经常进入 RCS，则可能表明系统过载。

内存页面交换说明

该系统旨在定期交换内存，因此进行一些内存交换是适当的，并不表示设备存在问题。除非系统一致地大容量交换内存，否则内存交换正常，并且是预期行为（尤其在 C170 和 C190 设备上）。为提高性能，您可能需要将设备添加到网络或调整配置以确保实现最大吞吐量。

系统容量 - 全部

“全部”(All) 页面将以前的所有系统容量报告整合在一个页面上，以便查看不同报告之间的关系。例如，您可能会发现在进行过量内存交换时，邮件队列很高。这可能是表示存在容量问题。您可能希望将此页面另存为 PDF 文件，以保留系统性能快照供以后参考（或与支持人员共享）。有关生成英语以外的其他语言的 PDF 的信息，请参阅有关报告的注意事项，第 667 页。

“系统状态”页面

系统状态页面详细展示了系统的所有实时邮件和 DNS 活动。显示的信息与使用 CLI 中的 status detail 和 **dnsstatus** 命令得到的信息一样。有关详细信息，请参阅中的“监控详细邮件状态”（对于

status detail 命令）或“检查 DNS 状态”（对于 **dnsstatus** 命令）。 使用 CLI 进行管理和监控，第 805 页

“系统状态”(System Status) 页面由四个部分组成：系统状态 (System Status)、计量器 (Gauges)、速率 (Rates) 和计数器 (Counters)。

系统状态

“系统状态”(System Status) 部分显示“邮件系统状态”(Mail System Status) 和“版本信息”(Version Information)。

邮件系统状态

“邮件系统状态”(Mail System Status) 部分包括：

- 系统状态（有关系统状态的详细信息，请参阅状态，第 641 页）
- 上次报告状态的时间。
- 设备的正常运行时间。
- 系统中最早的邮件，包括尚未排队等待传送的邮件。

版本信息

“版本信息”(Version Information) 部分包括：

- 设备型号名称。
- 安装的 AsyncOS 操作系统的版本和构建日期。
- AsyncOS 操作系统的安装日期。
- 您连接到的系统的序列号。

如果要联系思科客户支持，此信息非常有用。（请参阅使用技术支持，第 954 页。）

规格

“计量器”(Gauges) 部分显示队列和资源利用率。

- 邮件处理队列
- 队列中正在处理的收件人
- 队列空间
- CPU使用率

邮件网关设备是指 AsyncOS 进程所占用的 CPU 百分比。CASE 指多个项目，包括反垃圾邮件扫描引擎和病毒爆发过滤器进程。

- 常规资源利用率
- 日志磁盘利用率

比率

“速率”(Rates) 部分显示收件人处理率。

- 邮件处理率

- 完成比率

计数器

可以重置系统统计数据的累积邮件监控计数器，并查看上次重置计数器的时间。重置操作会影响系统计数器以及每个域的计数器。重置不会影响与重试计划相关的传送队列中的邮件计数器。

注释 只有管理员或操作员组中的用户帐户有权重置计数器。您在访客组中创建的用户帐户将无法重置计数器。有关详细信息，请参阅处理用户帐户，第 723 页。

点击“重置计数器”(Reset Counters) 可重置计数器。此按钮提供与 CLI 中的 **resetcounters** 命令相同的功能。有关详细信息，请参阅重置邮件监控计数器，第 819 页。

- 邮件处理事件数量
- 完成事件
- 域密钥事件
- DNS 状态

“大量邮件”页面

注释 “大量邮件”(High Volume Mail) 页面显示仅来自使用报头重复规则的邮件过滤器的数据。

“大量邮件 (High Volume)”页面包含以下条形图形式的报告：

- **排名靠前的主题**。您可以使用此图表了解 AsyncOS 接收的排名靠前的邮件主题。
- **排名靠前的信封发件人**。您可以使用此图表了解 AsyncOS 接收的排名靠前的邮件信封发件人。
- **按匹配数排名靠前的邮件过滤器**。您可以使用此图表了解排名靠前的邮件过滤器（使用“报头重复”(Header Repeats) 规则）匹配项。

“大量邮件”(High Volume Mail) 页面还用表格显示排名靠前的邮件过滤器以及各个邮件过滤器的匹配数。点击数值可使用“邮件跟踪”(Message Tracking) 查看该数值中包含的所有邮件的列表。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式；或通过点击**可打印 (PDF) (Printable (PDF))** 链接导出为 PDF 格式。

“邮件过滤器”页面

“邮件过滤器”(Message Filters) 页面以两种形式显示有关排名靠前的邮件过滤器匹配项（匹配邮件数量最多的邮件过滤器）：条形图和表格。

使用条形图，您可以查找传入和传出邮件触发次数最多的邮件过滤器。表格显示排名靠前的邮件过滤器以及各个的邮件过滤器的匹配数。点击数值可使用“邮件跟踪”(Message Tracking) 查看该数值中包含的所有邮件的列表。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式；或通过点击**可打印 (PDF) (Printable (PDF))** 链接导出为 PDF 格式。

检索 CSV 数据

您可以检索用于邮件安全监控器中构建图表和图形的CSV格式的数据。CSV数据可以通过两种方式访问：

- **通过邮件传送的 CSV 报告**。您可以生成通过邮件传送或存档的 CSV 报告。当您要为“邮件安全监控器”(Email Security Monitor) 页面上显示的每个表分隔报告时，或者当您要将 CSV 数据发送给无权访问内部网络的用户时，这种传送方式非常有用。

  逗号分隔值 (CSV) 报告类型是 ASCII 文本文件，其中包含计划报告的表格数据。每个 CSV 文件最多可以包含 100 行。如果某个报告包含多个类型的表格，则会为每个表格创建单独的 CSV 文件。单个报告的多个 CSV 文件将压缩成单个 .zip 文件以作为存档文件存储选项，或全部附加到不同的邮件进行传送。

  有关配置计划报告或按需报告的信息，请参阅报告概述，第 666 页。

- **通过 HTTP 检索的 CSV 文件**。可以通过 HTTP 检索邮件安全监控功能中用来生成图表的数据。如果计划通过其他工具进一步对数据执行分析，这种传送方法则非常有用。您可以自动检索这些数据（例如通过可下载原始数据的自动脚本），处理数据，然后在其他某些系统中显示结果。

通过自动化流程检索 CSV 数据

获取所需的HTTP查询的最简单方法是将其中一个邮件安全监控器页面配置为显示所需的数据类型。然后，可以复制**导出 (Export)** 链接。这是下载 URL。像这样实现数据检索自动化时，需要注意的是下载 URL 中的哪些参数应当修复，哪些应当更改（见下文）。

下载 URL 的编码方式使其能够复制到可执行相同查询（使用适当的 HTTP 身份验证）并获得类似数据集的外部脚本。脚本可以使用基本 HTTP 身份验证或 Cookie 身份验证。当通过自动化过程检索 CSV 数据时，请记住以下几点：

- 时间范围选择（过去的小时、天、星期等）与再次使用该 URL 的时间有关。如果您复制 URL 以检索“上一天”的 CSV 数据集，当您下次使用该 URL 时，您将获得一个新的数据集，涵盖从您再次发送该 URL 算起的“上一天”。日期范围选择予以保留并显示在 CSV 查询字符串中（例如，date_range=current_day）。
- 数据集的过滤和分组首选项。过滤器予以保留并显示在查询字符串中。请注意，报告中的过滤器十分罕见 - 例如，“病毒爆发”(Outbreaks) 报告中的“全局/本地”(Global/Local) 病毒爆发选择器。
- CVS 下载可以返回所选时间范围内表中所有行的数据。
- CVS 下载可以返回表中按时间戳和密钥排列的行的数据。您可以在单独的步骤中执行进一步排序，例如，通过电子表格应用。
- 第一行包括与报告中显示的显示名称匹配的列标题。请注意，系统也会显示时间戳（请参阅时间戳，第 666 页）和密钥（请参阅按键，第 666 页）。

示例 URL

http://example.com/monitor/content_filters?format=csv&sort_col_ss_0_0_0=
MAIL_CONTENT_FILTER_INCOMING.RECIPIENTS_MATCHED&section=ss_0_0_0
&date_range=current_day&sort_order_ss_0_0_0=desc&report_def_id=mga_content_filters

添加基本 HTTP 身份验证凭证

要为 URL 指定基本 HTTP 身份验证凭据：

http://example.com/monitor/

变成：

http://username:password@example.com/monitor/

文件格式

下载的文件采用 CSV 格式，且具有 .csv 文件扩展名。文件标题具有默认文件名，以报告名称开头，之后是报告部分。

时间戳

导出流数据将显示每个原始时间“间隔”的开始和结束时间戳。提供两个开始时间戳，两个结束时间戳 - 一个为数字格式，另一个是人类可读的字符串格式。时间戳为 GMT 时间，如果您的设备分布于多个时区，则更方便进行日志汇总。

请注意，在该数据与来自其他来源的数据合并的少数情况下，导出文件不包含时间戳。例如，病毒爆发详细信息导出可以合并报告数据与威胁防御运营中心 (TOC) 数据，使时间戳不相关，因为没有时间间隔。

按键

导出还包括报告表密钥，甚至在密钥在报告中不可见的情况下也是如此。在显示密钥的情况下，报告中显示的显示名称用作列标题。否则，显示“key0”、“key1”等列标题。

流传输

大多数报告会将其数据传输回客户端，因为数据量可能会非常大。但是，有些导出会返回整个结果集，而不是流数据。当报告数据与非报告数据（例如爆发详细信息）汇聚在一起时，通常会出现这种情况。

报告概述

AsyncOS 中的报告涉及三个基本操作：

- 您可以创建要每日、每周或每月运行的计划报告。
- 可以立即生成报告（“按需”报告）。
- 可以查看之前运行的报告的存档版本（计划和按需）。

通过“监控”(Monitor) >“计划的报告”(Scheduled Reports) 页面可配置计划的报告和按需报告。通过“监控”(Monitor) >“存档报告”(Archived Reports) 页面查看存档报告。

您的设备将保留生成的最近报告，所有报告总计最多1000个版本。可以根据需要为报告定义任意数量的收件人，包括零个收件人。如果不指定邮件收件人，则系统仍会将报告存档。但是，如果需要将报告发送到大量地址，则创建邮件列表而不是列出各个收件人更加方便。

默认情况下，设备会存档每个计划报告的12个最新报告。报告存储在设备的/saved_reports目录中。（有关详细信息，请参阅FTP、SSH 和 SCP 访问，第 979 页。）

计划的报告类型

您可以选择以下报告类型：

- 内容过滤器
- 发送状态
- DLP 事件概要
- 内容摘要
- 传入邮件概要
- 内部用户概要
- 外发目标
- 外发邮件概要
- 传出发件人：域 (Outgoing Senders: Domains)
- 组
- 系统容量
- TLS 连接
- 病毒爆发过滤器
- 病毒类型

每个报告都包含对应的“邮件安全监控器”(Email Security Monitor) 页面的摘要。因此，例如，“内容过滤器”报告提供“**监控**”>“**内容过滤器**”页面上显示的信息的摘要。“执行摘要”报告是基于“**监控**”>“**概述**”页面。

有关报告的注意事项

PDF 格式的内容过滤器报告限制为最多 40 个内容过滤器。您可以通过 CSV 格式的报告获得完整列表。

注释 要在 Windows 计算机上生成中文、日语或韩语 PDF，您还必须从 Adobe.com 下载适用的字体包并将其安装在本地计算机上。

设置报告的返回地址

要设置报告的返回地址，请参阅为设备生成的邮件配置返回地址，第 775 页。在 CLI 中，请使用 **addressconfig** 命令。

管理报告

您可以创建、编辑、删除和查看存档的计划报告。您还可以立即运行报告（按需报告）。以下报告类型可用：“内容过滤器”(Content Filters)、“DLP 事件摘要”(DLP Incident Summary)、“执行摘要”(Executive Summary)、“传入邮件摘要”(Incoming Mail Summary)、“内部用户摘要”(Internal Users Summary)、“传出邮件摘要”(Outgoing Mail Summary)、“发件人组”(Sender Groups) 和“爆发过滤器”(Outbreak Filters)。下面介绍如何管理和查看这些报告。

注释 当处于集群模式下时，您无法查看报告。您可以在处于计算机模式下时查看报告。

“监控”(Monitor) >“计划报告”(Scheduled Reports) 页面显示设备上已创建的计划报告的列表。

计划的报告

计划报告可以安排为每日、每周或每月运行。您可以选择运行报告的时间。无论何时运行报告，它都只包含您指定的时间段的数据，例如，过去 3 天或上个日历月。请注意，安排在凌晨 1 点运行的每日报告将包含前一天的数据（午夜到午夜）。

设备随附一组默认计划报告，您可以使用、修改或删除其中任何报告。

将报告计划为自动生成

步骤 1 在“监控”(Monitor) >“计划报告”(Scheduled Reports) 页面上，点击**添加计划报告 (Add Scheduled Report)**。

步骤 2 选择报告类型。根据您选择的报告类型，有不同的选项可供使用。

有关可用的计划报告类型的详细信息，请参阅计划的报告类型，第 667 页。

步骤 3 为报告输入描述性标题。AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建具有相同名称的多个报告。

步骤 4 选择报告数据的时间范围。（此选项对于“爆发过滤器”[Outbreak Filters] 报告不可用。）

步骤 5 选择报告的格式：

- PDF。创建用于传送和/或存档的 PDF 格式文档。您可以通过点击“预览 PDF 报告”(Preview PDF Report) 立即以 PDF 文件形式查看报告。

  有关生成英语以外的其他语言的 PDF 的信息，请参阅有关报告的注意事项，第 667 页。

- CSV。创建以逗号分隔值形式包含列表式数据的 ASCII 文本文件。每个 CSV 文件最多可以包含 100 行。如果报告包含多种类型的表格，则会为每个表格创建一个单独的 CSV 文件。

步骤 6 指定报告选项（如果可用）。有些报告没有报告选项。

步骤 7 指定安排和传送选项。如果您不指定邮件地址，则仅存档报告，而不向任何收件人发送报告。

注释 如果您是将报告发送到外部帐户（例如 Yahoo 或 Gmail 等），则可能需要将报告返回地址添加到外部帐户的白名单中，以防止将报告邮件错误地分类为垃圾邮件。

步骤 8 点击 **Submit**。确认您的更改。

编辑计划的报告

步骤 1 点击“服务”(Services) >“集中报告”(Centralized Reporting) 页面上列表中的报告标题。

步骤 2 进行更改。

步骤 3 提交并确认更改。

删除计划的报告

步骤 1 在“服务”(Services) >“集中报告”(Centralized Reporting) 页面上，选中与要删除的报告对应的复选框。

注释 选择“全部”(All) 复选框可删除所有计划报告。

步骤 2 点击 **Delete**。

步骤 3 确认删除，然后提交更改。

任何已删除报告的存档版本都不会自动删除。

存档的报告

“监控”(Monitor) >“存档报告”(Archived Reports) 页面列出可用的存档报告。您可以通过点击“报告标题”(Report Title) 列中的报告名称来查看报告。您可以通过点击**立即生成报告 (Generate Report Now)** 来立即生成报告。

使用“显示”(Show) 菜单可过滤列出的报告类型。点击列标题可对列表进行排序。

自动删除存档报告 - 每份计划报告最多保留 30 个实例（最多 1000 份报告），添加新报告的同时，删除旧报告，使报告数量保持在 1000 份。30 个实例限制适用于单个计划报告，不适用于报告类型。

生成按需报告

您可以在不计划报告的情况下生产报告。这些按需报告仍然基于指定的时间范围，但是可以立即生成。

步骤 1 点击“存档的报告”(Archived Reports) 页面中的**立即生成报告 (Generate Report Now)**。

步骤 2 选择报告类型，并在需要时编辑标题。AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建具有相同名称的多个报告。

有关可用的计划报告类型的详细信息，请参阅计划的报告类型 ，第 667 页。

步骤 3 选择报告数据的时间范围。（此选项对“病毒爆发”(Virus Outbreak) 报告不可用。）

如果创建自定义范围，则范围将显示为链接。要修改范围，请点击该链接。

步骤 4 选择报告的格式。

- PDF。创建用于传送和/或存档的 PDF 格式文档。您可以通过点击“预览 PDF 报告”(Preview PDF Report) 立即以 PDF 文件形式查看报告。

  有关生成英语以外的其他语言的 PDF 的信息，请参阅有关报告的注意事项，第 667 页。

- CSV。创建以逗号分隔值形式包含列表式数据的 ASCII 文本文件。每个 CSV 文件最多可以包含 100 行。如果报告包含多种类型的表格，则会为每个表格创建一个单独的 CSV 文件。指定任何报告选项。

步骤 5 选择是否对报告进行存档（如果存档，则该报告将显示在“存档报告”[Archived Reports] 页面上）。

步骤 6 指定是否通过邮件发送报告以及向哪些邮件地址发送报告。

步骤 7 点击**传送此报告 (Deliver this Report)** 可生成报告，并将其传送给收件人或存档。

步骤 8 确认您的更改。

邮件报告故障排除

邮件跟踪链接导致出现意外结果

问题

从报告深入了解邮件跟踪中的详细信息，会产生意外结果。

解决方案

如果报告和邮件跟踪不同时启用、不能正常工作、不能在本地存储数据（相对于在安全管理设备上集中存储数据），就会出现这种情况。每个功能（报告和邮件跟踪）的数据仅在该功能已启用且在设备上正常工作时存储，不受另一功能（报告或邮件跟踪）是否已启用且正常工作影响。因此，报告可能包括邮件跟踪中不可用的数据，反之亦然。

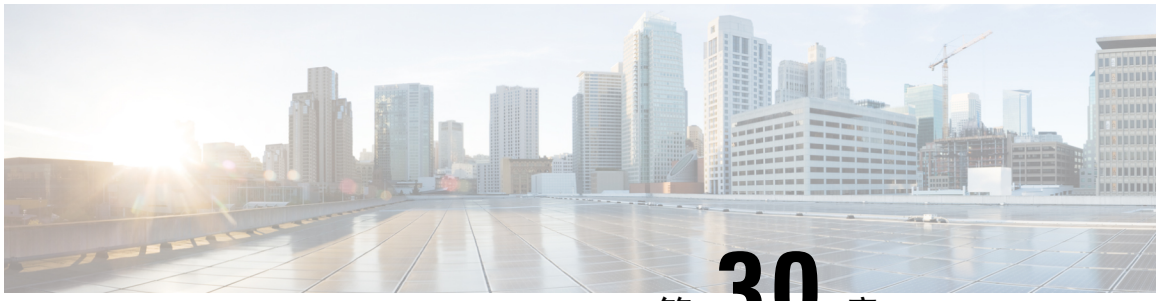
云端的文件分析详细信息不完整

问题

对于从组织中其他邮件安全设备上传的文件，无法在公共云中获取完整的文件分析结果。

解决方案

务必将所有要共享文件分析结果数据的设备分组到一起。请参阅（仅公共云文件分析服务）配置设备组，第 361 页。必须在该组中的每台设备上完成此配置。



第 30 章

FIPS 管理

本章包含以下部分：

FIPS 管理概述

联邦信息处理标准 (FIPS) 140 是美国和加拿大联邦政府共同开发且公开发布的标准，其中规定了政府机构用于保护敏感但非保密性信息的密码模块的要求。思科 IronPort 邮件安全设备使用思科 SSL 密码工具套件实现 FIPS 140-2 1 级合规性。

Cisco SSL 密码工具包是一个 GGSG 批准的加密套件，其中包括 作为 OpenSSL FIPS 支持增强版的 Cisco SSL 以及符合 FIPS 标准的思科通用加密模块。思科通用加密模块是一个软件库，供邮件安全设备用于对 SSH 等协议的 FIPS 验证密码算法。

FIPS 模式下的配置更改

设备处于 FIPS 模式时，邮件安全设备使用 Cisco SSL 和符合 FIPS 标准的证书进行通信。有关详细信息，请参阅将设备切换到 FIPS 模式， 第 672 页。

为了符合 FIPS 级别 1 标准，邮件安全设备会对配置进行以下更改：

- **SMTP 接收和传送**。在邮件安全设备上的公共侦听程序与远程主机之间通过 TLS 进行的传入和传出 SMTP 会话使用 TLS 第 1.0 版、1.1 版或 1.2 版及 FIPS 密码套件。在 FIPS 模式下可以使用 sslconfig 修改密码套件。TLS v1 在 FIPS 模式下支持的唯一版本的 TLS。

- **Web 界面**。与邮件安全设备的 Web 界面进行的 HTTPS 会话使用 TLS 第 1.0 版、1.1 版或 1.2 版和 FIPS 密码套件。这还包括与垃圾邮件隔离区和其他 IP 接口的 HTTPS 会话。在 FIPS 模式下可以使用 sslconfig 修改密码套件。
- **证书**。FIPS 模式会限制设备使用的证书类型。证书必须使用以下签名算法之一：SHA-224、SHA-256、SHA-384 和 SHA-512，以及长度为 2048 位的 RSA 密钥。设备不会导入不使用其中一种算法的证书。如果设备使用任何不符合标准的证书，则无法切换到FIPS模式。它将显示错误消息。有关详细信息，请参阅管理证书和密钥，第 674 页。
- **DKIM 签名和验证**。用于 DKIM 签名和验证的 RSA 密钥的长度必须为 2048 位。如果设备使用任何不符合标准的 RSA 密钥，则无法切换到 FIPS 模式。它将显示错误消息。当验证 DKIM 签名时，如果签名不使用符合 FIPS 标准的密钥，设备会返回永久故障。请参阅 管理用于 DKIM 签名和验证的密钥，第 675 页
- **LDAPS**。邮件安全设备与 LDAP 服务器之间的 TLS 事务（包括使用 LDAP 服务器进行外部身份验证）使用 TLS 第 1 版和 FIPS 加密套件。如果 LDAP 服务器使用 MD5 散列存储密码，则由于 MD5 不符合 FIPS 标准，因此 SMTP 身份验证查询会失败。
- **日志**。SSH2 是允许通过 SCP 推动日志的唯一协议。对于与 FIPS 管理相关的错误消息，请阅读信息级别的 FIPS 日志。
- **集中管理**。对于集群化设备，FIPS 模式只能在集群级别打开。
- **SSL 密码**。在 FIPS 模式下仅支持以下 SSL 密码：AES256-SHA:AES128-SHA:DES-CBC3-SHA。

将设备切换到 FIPS 模式

使用 fipsconfig CLI 命令将设备切换到 FIPS 模式。

注释 只有管理员可以使用此命令。将设备从非 FIPS 模式切换到 FIPS 模式后，需要重新启动。

准备工作

确保设备没有不符合FIPS标准的任何对象（例如，密钥长度为512位的DKIM验证配置文件）。要启用 FIPS 模式，必须修改所有不符合 FIPS 标准的对象以符合 FIPS 要求。请参阅FIPS 模式下的配置更改，第 671 页。有关检查设备是否包含不符合 FIPS 标准的对象的说明，请参阅检查 FIPS 模式合规性，第 674 页。

程序

```
mail.example.com> fipsconfig
FIPS mode is currently disabled.
Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> setup
To finalize FIPS mode, the appliance will reboot immediately. No commit will be required.
Are you sure you want to enable FIPS mode and reboot now ? [N]> y
Do you want to enable encryption of sensitive data in configuration file when FIPS mode is
 enabled? Changing the value will result in system reboot [N]> n
Enter the number of seconds to wait before forcibly closing connections.
```

```
[30]>
System rebooting.  Please wait while the queue is being closed...
Closing CLI connection.
Rebooting the system...
```

在 FIPS 模式下加密敏感数据

使用 fipsconfig 命令加密设备中的敏感数据（例如密码和密钥）。如果启用此选项，

- 将对设备中的以下重要安全参数进行加密和存储：
  - 证书私钥
  - RADIUS 密码
  - LDAP 绑定密码
  - 本地用户的密码哈希
  - SNMP 密码
  - DK/DKIM 签名密钥
  - 外发 SMTP 身份验证密码
  - PostX 加密密钥
  - PostX 加密代理密码
  - FTP 推送日志订用的密码
  - IPMI LAN 密码
  - 更新程序服务器 URL

注释 所有用户（包括管理员）都无法查看配置文件中的敏感信息。

- 如果设备的物理安全受到威胁，设备中的交换空间将进行加密以避免任何未经授权的访问或调查攻击。

程序

```
mail.example.com> fipsconfig
FIPS mode is currently enabled.
Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> setup
To finalize FIPS mode, the appliance will reboot immediately. No commit will be required.
Are you sure you want to disable FIPS mode and reboot now ? [N]> n
Do you want to enable encryption of sensitive data in configuration file when FIPS mode is
 enabled? Changing the value will result in system reboot [N]> y
Enter the number of seconds to wait before forcibly closing connections.
[30]>
System rebooting.  Please wait while the queue is being closed...
Closing CLI connection.
Rebooting the system...
```

检查 FIPS 模式合规性

使用 fipsconfig 命令检查设备是否包含任何不符合 FIPS 标准的对象。

程序

```
mail.example.com> fipsconfig
FIPS mode is currently disabled.
Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> fipscheck
All objects in the current configuration are FIPS compliant.
FIPS mode is currently disabled.
```

管理证书和密钥

AsyncOS 允许使用证书和私钥对加密设备与外部计算机之间的通信。可以上传现有证书和密钥对、生成自签名证书或生成证书签名请求 (CSR)，从而提交到证书颁发机构以获得公共证书。证书颁发机构将返回由私钥签名的可信公共证书，然后，可以将该证书上传到设备。

当设备处于 FIPS 模式时，可以继续

设备的 FIPS 模式为设备使用的证书施加了许多限制，以便设备符合 FIPS 标准。证书必须使用以下签名算法之一：SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512。

设备不会导入不使用其中一种算法的证书。如果在侦听程序中使用了任何不符合标准的证书，则设备还无法切换到 FIPS 模式。它将显示错误消息。

当设备处于 FIPS 模式时，设备的非 FIPS 状态将显示在 CLI 和 GUI 中。当选择用于某项功能（例如监听程序或目标控制）的证书时，设备不会显示不符合标准的证书作为选项。

有关在设备上使用证书的详细信息，请参阅证书的使用，第 510 页。

可以将符合 FIPS 标准的证书与以下任何服务配合使用：

- **SMTP 接收和传送**。使用**网络 > 侦听程序**页面（或 listenerconfig -> edit -> certificate CLI 命令）为需要使用 TLS 加密的任何侦听程序分配证书。您可能希望在面向互联网的侦听程序（即公共侦听程序）上启用TLS，或者为包括内部系统在内所有侦听程序（即专用侦听程序）启用加密。
- **目标控制**。使用**邮件策略 > 目标控制**页面（或 destconfig CLI 命令）分配证书作为用于邮件传送的所有外发 TLS 连接的全局设置。
- **接口**。使用**网络 > IP 接口**页面（或 interfaceconfig CLI 命令）为某个接口（包括管理接口）中的 HTTPS 服务启用证书。
- **LDAP**。使用**系统管理 (System Administration) > LDAP** 页面为需要 TLS 连接的所有 LDAP 流量分配证书。设备还可以将 LDAP 用于对用户的外部身份验证。

管理用于 DKIM 签名和验证的密钥

有关 DomainKeys 和 DKIM 如何在邮件安全设备上运行的概述，请参阅电邮验证，第 445 页。

相关主题

- DKIM 签名，第 675 页
- DKIM 验证，第 675 页

DKIM 签名

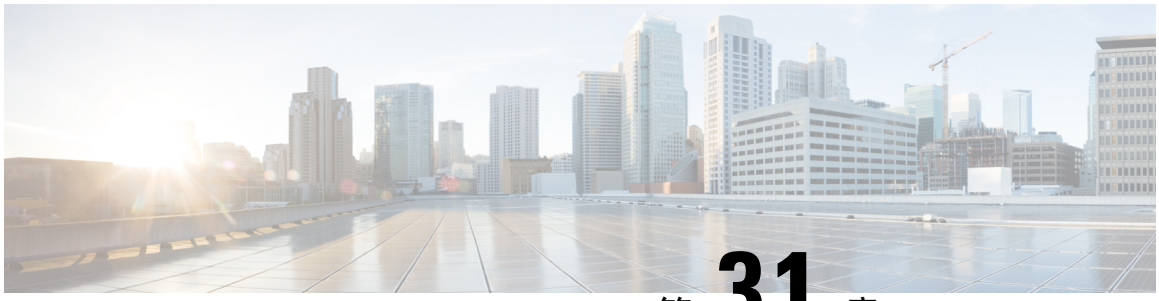
当创建 DKIM 签名密钥时，需要指定密钥大小。邮件安全设备的 FIPS 模式支持 2048 位的密钥大小。密钥越长越安全；但是，较长的密钥可能会影响性能。

如果设备使用任何不符合标准的 RSA 密钥，则无法切换到 FIPS 模式。它将显示错误消息。

在使用**邮件策略 (Mail Policies) > 域配置文件 (Domain Profiles)** 页面创建或编辑域配置文件时，符合 FIPS 标准的签名密钥可用于域配置文件，并且会显示在“签名密钥”(Signing Key) 列表中。将签名密钥与域配置文件相关联后，可以创建包含公钥的 DNS 文本记录。为此，可以通过域配置文件列表中“DNS 文本记录”列的“生成”链接（或通过 CLI 中的 domainkeysconfig -> profiles -> dnstxt）。

DKIM 验证

设备要求邮件使用符合 FIPS 标准的密钥来验证 DKIM 签名。如果签名不使用符合 FIPS 标准的密钥，则设备会返回永久故障。



第 31 章

邮件跟踪

本章包含以下部分：

邮件跟踪概览

邮件跟踪可提供邮件流的的详细视图，帮助解决支持中心呼叫。例如，如果邮件未能如期投递，您可以判断邮件是否包含病毒、被放入垃圾邮件隔离区，还是位于邮件流的其他位置。

您可以搜索一封匹配指定条件的特定邮件或一组邮件。

注释 使用邮件跟踪无法读取邮件内容。

启用邮件跟踪

注释 仅保留启用本功能之后所处理邮件的邮件跟踪数据。

准备工作

- 要在邮件跟踪中搜索和显示附件名称，并在日志文件中查看附件名称，您必须至少配置和启用一个正文扫描过程，例如邮件过滤器或内容过滤器。
- 日志文件必须配置为记录主题信头，才能实现按主题搜索。有关详细信息，请参阅日志记录，第 855 页。

- 如果要设置集中跟踪：请将安全管理设备设置为支持对此邮件安全设备进行集中邮件跟踪。请参阅《思科内容安全管理设备用户指南》。

步骤 1 依次点击**服务 > 集中式服务 > 邮件跟踪(Services > Centralized Services > Message Tracking)**。

即使您不计划集中使用此服务，也请使用此路径。

步骤 2 选择**启用邮件跟踪服务 (Enable Message Tracking Service)**。

步骤 3 如果在运行系统设置向导后首次启用邮件跟踪，请阅读终端用户许可协议，并点击**接受**。

步骤 4 选择邮件跟踪服务：

选项	说明
本地跟踪	在此设备使用邮件跟踪。
集中跟踪	使用安全管理设备为包括本设备在内的多个邮件安全设备跟踪邮件。

步骤 5 （可选）选中该复选框可保存被拒绝连接的信息。

为获得最佳性能，请禁用此设置。

步骤 6 提交并确认更改。

下一步做什么

如果您选择了本地跟踪：

- 选择可以访问DLP违规相关内容的用户。请参阅控制对“邮件跟踪”中敏感信息的访问权限，第 727 页。
- （可选）请调整用于存储邮件的磁盘空间分配。请参阅管理磁盘空间，第 758 页。

搜索邮件

步骤 1 选择**邮件 > 邮件跟踪 > 邮件跟踪**。

步骤 2 输入搜索条件。

- 要查看所有选项，请点击**高级 (Advanced)** 链接。
- 跟踪不支持通配符或正则表达式。
- 跟踪搜索不区分大小写。
- 查询是“AND”搜索，除非另行说明：查询返回满足搜索字段中指定的所有条件的邮件。例如，如果为信封收件人和主题行参数指定文本字符串，查询将仅返回与指定信封收件人和主题行的两者匹配的邮件。

- 搜索条件包括：

选项	说明
信封发件人	选择**起始字符 (Begins With)**、**为 (Is)** 或**包含 (Contains)**，然后输入要查找邮件发件人的邮件地址、用户名或域。 可以输入任何字符。不会针对输入执行验证。
信封收件人	选择**起始字符 (Begins With)**、**为 (Is)** 或**包含 (Contains)**，然后输入要查找邮件收件人的邮件地址、用户名或域。 您可以输入任何字符。不会针对输入执行验证。
主题	选择**开头 (Begins With)**、**是 (Is)** 或**包含 (Contains)**，然后在邮件主题行中输入要搜索的文本字符串。 **警告**：不要在法规禁止这类跟踪的环境中使用此种搜索。
邮件接收时间 (Message Received)	指定日期和时间范围。 如果未指定日期，查询将返回所有日期的数据。如果只指定时间范围，查询将返回所有可用日期该时间范围的数据。 使用邮件安全设备收到邮件的本地日期和时间。
高级选项：	
发件人 IP 地址/域/网络所有者 (Sender IP Address/ Domain / Network Owner)	指定远程主机的 IP 地址、域或网络所有者。 您可以仅在被拒连接中搜索，也可以搜索所有邮件。
附件	选择**开头 (Begins With)**、**是 (Is)** 或**包含 (Contains)**，然后输入要查找的一个附件的 ASCII 或 Unicode 文本字符串。系统不删除所输入文本的前导空格和结尾空格 只有执行下列操作后，才能按附件文件名搜索邮件： • 使用邮件过滤器扫描正文 • 使用内容过滤器扫描正文 • 高级恶意软件防护 (AMP) 扫描。 有关基于 SHA-256 哈希识别文件的详细信息，请参阅通过 SHA-256 散列标识文件，第 368 页。
邮件事件	选择一个或多个邮件处理事件。例如，您可以搜索已投递、被隔离或硬退回的邮件。 使用“OR”运算符添加邮件事件：选择多个事件查找满足任何指定条件的邮件。

选项	说明
邮件 ID 信头	输入 SMTP 邮件 ID 信头的文本字符串。 此 RFC 822 邮件信头是邮件的唯一标识，初次创建邮件时，即在邮件中插入该信头。
思科 IronPort MID:	输入要搜索的邮件编号。IronPort MID 唯一标识邮件安全设备上的每封邮件。
思科 IronPort 主机	选择一台邮件安全设备，将邮件搜索范围限制为该设备处理的邮件，或选择所有设备。

步骤 3 点击**搜索 (Search)** 提交查询。

查询结果将显示在页面底部。

处理邮件跟踪搜索结果

请注意以下问题：

- 只有邮件安全设备中已记录邮件，且安全管理设备检索到邮件时，结果中才会显示邮件。根据日志大小和轮询频率，邮件的发送时间与其实际在跟踪和报告结果中的显示时间可能存在小的差距。
- 有关涉及高级恶意软件防护的搜索（文件信誉扫描和文件分析）的信息，请参阅关于邮件跟踪和高级恶意软件保护功能，第 370 页。

使用搜索结果可以执行以下操作：

- 显示超过 250 个搜索结果，方法是返回搜索条件，点击“高级”(Advanced)，滚动到“查询设置”(Query Settings)，然后将结果最大数量设为 1000。
- 从搜索结果部分的右上角选择选项，可在每页显示更多结果。
- 从搜索结果部分的右上角在多个搜索结果页面之间导航。
- 将光标悬停在搜索结果中要添加为条件的某一值上，可缩小搜索结果范围。显示橙色高亮时，可以点击该值按该条件缩小搜索范围。可通过此操作在搜索条件中添加更多条件。例如，如果搜索发送到特定收件人的邮件，可以点击搜索结果中的发件人姓名，查找在最初指定的时间范围内从该发件人发送给该收件人（并满足任何其他条件）的所有邮件。
- 如果超过1000封邮件匹配您的搜索条件，则您可以点击“全部导出”（位于搜索结果部分右上角的链接），将多达 50,000 个搜索结果导出为逗号分隔值文件，并在其他应用中处理这些数据。
- 在邮件行中点击“显示详细信息”(Show Details) 可查看该邮件的更多详细信息。系统随即打开新的浏览器窗口，显示邮件的详细信息。
- 对于已隔离的邮件，可以点击邮件跟踪搜索结果中的链接，查看邮件被隔离的原因等详细信息。

注释 如果点击报告页面上的链接来查看邮件跟踪中的邮件详细信息，但结果没有达到预期，这可能是因为查阅时没有同时启用报告和跟踪。

邮件跟踪详细信息

项目	说明
信封和信头概要部分：	
接收时间	邮件安全设备收到邮件的时间。 日期和时间显示为邮件安全设备上配置的本地时间。
MID	唯一 IronPort 邮件 ID。
邮件大小	邮件的大小
主题	邮件的主题行。 如果邮件没有主题，或如果日志文件未配置为记录主题信头，跟踪结果中主题行的值可能为“（无主题）”。有关详细信息，请参阅日志记录，第 855 页
信封发件人	SMTP 信封中的发件人地址。
信封收件人	如果部署使用别名表进行别名扩展，搜索将查找扩展的收件人地址，而不是原始信封地址。有关别名表的详细信息，请参阅“配置路由和传送功能”一章中的“创建别名表”。 在任何其他情况下，邮件跟踪查询将查找原始信封收件人地址。
邮件 ID 信头	RFC 822 邮件信头。
SMTP 身份验证用户 ID	发件人的 SMTP 身份验证用户名，如果发件人使用 SMTP 身份验证发送邮件。否则，该值为“N/A”。

项目	说明
附件	附加到邮件的文件的名称。 搜索结果中将显示采用查询的名称，且至少包含一个附件的邮件。 对于某些附件，可能不跟踪。由于性能原因，附件名称的扫描只作为其他扫描操作（例如邮件或内容过滤、DLP 或免责声明印记）的一部分进行。只有通过正文扫描，且仍附带附件的邮件，才能获得其附件名称。附件名称不会出现在搜索结果中的情况包括（但不限于）： • 如果系统只使用内容过滤器，并且邮件被删除或其附件被反垃圾邮件或防病毒过滤器隔离 • 如果在进行正文扫描之前，邮件拆分策略从某些邮件中删除了附件。 由于性能原因，不会搜索附件中文件的名称，例如 OLE 对象或 ZIP 文件等存档。
发送主机摘要部分 **反向 DNS 主机名**	发送主机的名称，由反向 DNS (PTR) 查找验证。
IP 地址	发送主机的 IP 地址
SBRS 得分	SenderBase 信誉得分。范围是 10（可能是可信发件人）到 -10（绝对垃圾邮件发送者）。得分“无 (None)”表示处理该邮件时，无此主机的相关信息。 有关 SBRS 的详细信息，请参阅发件人信誉过滤，第 75 页
处理详细信息部分 **摘要信息** （如果显示下面选项卡之一，则此信息将显示在某个选项卡中。摘要信息始终显示。）	“摘要”选项卡显示处理邮件过程中记录的状态事件。 条目包括有关邮件策略处理的信息，例如，反垃圾邮件和防病毒扫描以及其他事件（邮件分流和内容或邮件过滤器添加的自定义日志条目等）。 如果邮件已投递，则显示投递的详细信息。 处理详细信息中将突出显示最后记录的事件。

项目	说明
“DLP 匹配内容”(DLP Matched Content) 选项	仅对 DLP 策略捕获的邮件显示此选项。 此选项卡包括匹配相关信息，以及触发 DLP 策略匹配的敏感内容。 必须配置设备才能显示此信息。请参阅在邮件跟踪中显示敏感 DLP 数据，第 395 页。 若要控制对此选项卡的访问，请参阅控制对“邮件跟踪”中敏感信息的访问权限，第 727 页。
“URL 详细信息”选项卡	此选项卡仅向由URL信誉和URL类别内容过滤器以及病毒爆发过滤器捕获的邮件显示。 此选项卡显示以下信息： • 与 URL 关联的信誉得分或类别 • 对 URL 执行的操作（重写、去除或重定向） • 如果邮件包含多个 URL，显示哪一个 URL 触发了过滤器操作。 必须配置设备才能显示此信息。请参阅在邮件跟踪中显示 URL 详细信息，第 336 页。 若要控制对此选项卡的访问，请参阅控制对“邮件跟踪”中敏感信息的访问权限，第 727 页。

检查邮件跟踪数据的可用性

您可以确定邮件跟踪数据包括的日期范围，并可识别这些数据中缺少的任何间隔。

步骤 1 依次选择**监视 > 邮件跟踪**。

步骤 2 在搜索框的右上角查找**数据时间范围: (Data in time range:)**。

步骤 3 点击**数据时间范围: (Data in time range:)** 的值。

关于邮件跟踪和升级

全新的邮件跟踪功能可能不适用于在升级前处理的邮件，因为可能没有为这些邮件保留所需的数据。有关邮件跟踪数据和升级的可能限制，请参阅所用版本的版本说明。

邮件跟踪故障排除

搜索结果中不显示的附件

问题

搜索结果中找不到且未显示附件名称。

解决方案

请参阅启用邮件跟踪，第 677 页（）中的配置要求。另请参阅邮件跟踪详细信息，第 681 页中的附件名称搜索限制。

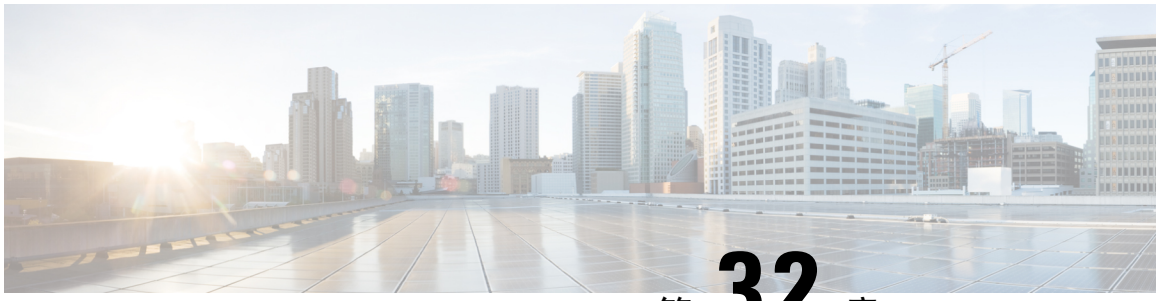
搜索结果中缺少预期邮件

问题

搜索结果中不包括本应满足条件的邮件。

解决方案

- 搜索的结果，特别是涉及邮件事件的搜索，取决于您的设备配置。例如，如果搜索未经过滤的URL类别，将找不到结果，即使邮件包含此类别的URL。确认您是否已正确配置邮件安全设备来实现预期的行为。例如，检查邮件策略、内容和邮件过滤器及隔离区设置。
- 如果点击报告中的链接后缺少预期的信息，请参阅邮件报告故障排除，第 670 页。



第 32 章

集中化的策略、病毒和病毒爆发隔离区

本章包含以下部分：

策略、病毒和病毒爆发隔离区概述

“策略、病毒和病毒爆发隔离区”包含所有非垃圾邮件隔离区，其中包括文件分析隔离区。

当邮件安全设备在传入或传出邮件中检测到潜在恶意软件或组织不允许的内容时，可以将这些邮件发送到隔离区，而不是立即将其删除。隔离区会在邮件安全设备或思科内容安全管理设备上安全保留这些邮件一段时间，以便人们审核邮件或者等待更新来更好地评估邮件的安全性。

例如，组织中利用非垃圾邮件隔离区的方式包括：

- **策略实施**。请人力资源专员或法律部门审核可能包含攻击性、机密或其他不许可信息的邮件。
- **病毒隔离区**。存储标记为已感染、已加密或防病毒扫描引擎无法扫描的邮件，以防病毒传播给您的用户。
- **预防爆发**。暂存被爆发过滤器标记为可能属于爆发或小规模恶意软件攻击的邮件，直到发布防病毒或反垃圾邮件更新。
- **文件分析隔离区**。存储可能包含恶意软件、已发送进行分析的带附件邮件，直到作出判断。

集中隔离区概述

可以将邮件安全设备中某些过滤器、策略和扫描操作处理的邮件放在隔离区中临时保存，以供后续操作。您可以集中来自思科内容安全管理设备上的多个邮件安全设备的隔离区。

集中隔离区的优势包括以下几点：

- 可以集中于一处来管理多个邮件安全设备的被隔离邮件。
- 隔离的邮件存储在防火墙后，而不是DMZ中，从而降低安全风险。

- 集中的隔离区可以被备份为安全管理设备上的标准备份功能的一部分。

防病毒扫描、爆发过滤器和高级恶意软件保护（文件分析）都有一个专用的隔离区。可创建策略隔离区来暂存被邮件过滤、内容过滤和防数据丢失策略拦截的邮件。

有关隔离区的详细信息，请参阅邮件安全设备的相应文档。

隔离区类型

隔离区类型	隔离区名称	默认情况下是否由系统创建？	说明	更多信息
高级恶意软件防护	文件分析	是	暂存发送进行文件分析的邮件，直到作出判断。	• 管理策略、病毒和病毒爆发隔离区，第 687 页 • 处理策略、病毒或爆发隔离区中的邮件，第 693 页
病毒	病毒	是	暂存可能传输防病毒引擎确定的恶意软件的邮件。	
爆发	爆发	是	暂存爆发过滤器拦截的可能是垃圾邮件或恶意软件的邮件。	
策略	策略	是	暂存邮件过滤器、内容过滤器和 DLP 邮件操作拦截的邮件。 系统已为您创建了默认策略隔离区。	
	未分类	是	只有邮件过滤器、内容过滤器或 DLP 邮件操作中指定的隔离区被删除后，才会暂存邮件。 无法向此隔离区指定任何过滤器或邮件操作。	
	（您创建的策略隔离区）	否	您创建的用于邮件过滤器、内容过滤器和 DLP 邮件操作的策略隔离区。	
垃圾邮件	垃圾邮件	是	暂存垃圾邮件或可疑垃圾邮件，以供邮件的收件人或管理员审核。 垃圾邮件隔离区不包括在策略、病毒和爆发隔离区的分组当中，并且与所有其他隔离区分开管理。	垃圾邮件隔离区，第 701 页

管理策略、病毒和病毒爆发隔离区

策略、病毒和爆发隔离区的磁盘空间分配

有关策略、病毒和爆发隔离区的磁盘空间信息，请参阅管理磁盘空间，第 758 页。

即使隔离区已集中，策略、病毒和爆发隔离区仍会占用邮件安全设备中的部分磁盘空间。

多个隔离区中的邮件与单一隔离区中的邮件占用相同的磁盘空间。

如果爆发过滤器和集中隔离区都启用：

- 使用邮件安全设备中本已分配给本地策略、病毒和爆发隔离区的所有磁盘空间（而不是在爆发隔离区暂存邮件副本），以便在爆发规则每次更新时扫描这些邮件。
- 安全管理设备上用于特定受管

邮件在隔离区中的保留时间

在以下情况下，将自动从隔离区中删除邮件：

- 正常到期 - 隔离区中的邮件达到配置的保留时间。您为每个隔离区中的邮件指定一个保留时间。每封邮件都有自己特定的到期时间，显示在隔离区列表中。除非出现本主题中描述的其他情况，否则邮件存储时间为指定时间。

  注释 病毒爆发过滤器隔离区中邮件的正常保留时间在每个邮件策略的“病毒爆发过滤器”(Outbreak Filters) 部分配置，而不是爆发隔离区。

- 提前到期 - 在到达配置的保留时间之前，强制从隔离区中删除邮件。在以下条件下可能发生这种情况：
  - 达到策略、病毒和爆发隔离区的磁盘空间分配，第687页中定义的所有隔离区的大小限制。

    如果达到大小限制，将处理最早的邮件（无论哪个隔离区），并针对每封邮件执行默认操作，直到所有隔离区的大小再次低于大小限制。该策略为先进先出 (FIFO)。多个隔离区中邮件的到期时间将以其最新到期时间为准。

    （可选）可以配置免除因磁盘空间不足而被放行或删除的各个隔离区。如果将所有隔离区都配置为免除，当磁盘空间达到容量时，将传送隔离区中的邮件以便为新邮件腾出空间。

    在磁盘空间达到里程碑时，您将会收到警报。请参阅关于隔离区磁盘空间使用量的警报，第 692 页。

- 您删除仍存放邮件的隔离区。

从隔离区中自动删除邮件时，将针对该邮件执行默认操作。请参阅自动处理的隔离邮件的默认操作，第 688 页。

注释 除上述场景之外，也可以根据扫描操作（爆发过滤器或文件分析）的结果从隔离区自动删除邮件。

保留时间中时间调整的影响

- 夏令时和设备时区更改不会影响保留时间。
- 如果更改隔离区的保留时间，只有新邮件采用新的到期时间。
- 如果更改系统时钟，则过去已到期的邮件将在下一个最适当的时间到期。
- 系统时钟更改不适用于当前到期的邮件。

自动处理的隔离邮件的默认操作

出现邮件在隔离区中的保留时间，第 687 页中所述的任何情况时，将针对策略、病毒或爆发隔离区中的邮件执行默认操作。

主要默认操作有两个：

- 删除-删除邮件。
- 放行-放行邮件进行传送。

放行后，可能会重新扫描邮件中的威胁。有关详细信息，请参阅关于重新扫描隔离的邮件，第 698 页。

此外，对于在预期保留时间到达之前被放行的邮件，还会对它们执行其他操作，例如添加X-Header。有关详细信息，请参阅配置策略、病毒和爆发隔离区，第 688 页。

检查系统创建的隔离区的设置

在使用隔离区之前，请自定义默认隔离区的设置，包括未分类隔离区。

配置策略、病毒和爆发隔离区

开始之前

- 如果要编辑现有的隔离区，请参阅关于编辑策略、病毒和爆发隔离区设置，第 690 页。
- 了解如何自动管理隔离区中的邮件，包括保留时间和默认操作。请参阅邮件在隔离区中的保留时间，第 687 页和自动处理的隔离邮件的默认操作，第 688 页。
- 确定您希望哪些用户有权访问每个隔离区，并相应地创建用户和自定义用户角色。有关详细信息，请参阅可访问策略、病毒和爆发隔离区的用户组，第 693 页。

步骤 1 选择监控 > 策略、病毒和爆发隔离区。

步骤 2 执行以下操作之一：

- 点击**添加策略隔离区 (Add Policy Quarantine)**.
- 点击要编辑的隔离区。

步骤 3 输入信息。

记住以下几点：

- 文件分析隔离区的默认保留时间为一小时，不建议您进行更改。
- 如果您不希望在指定的保留期结束之前处理此隔离区中的邮件，即使隔离区磁盘空间已满也如此，请取消选择**通过在空间溢出后对邮件应用默认操作来释放空间 (Free up space by applying default action on messages upon space overflow)**。

  对于所有隔离区，请勿选择此选项。系统必须能够通过删除至少一个隔离区中的邮件来释放空间。
- 如果选择**放行 (Release)** 作为默认操作，可以指定其他操作以应用于保留期间到期前被放行的邮件：

选项	信息
修改主题 (Modify Subject)	键入文本，以添加和指定是否将其添加到原始邮件主题的开头或结尾。 例如，您可能希望警告收件人，该邮件可能包含不当内容。 **注释** 要正常显示使用非 ASCII 字符的主题，必须根据 RFC 2047 进行表示。
添加 X-Header (Add X-Header)	X 报头可提供对邮件采取的操作的记录。这可能会非常有用，例如在处理有关传送特定邮件的原因的查询时。 输入名称和值。 示例： 名称 = Inappropriate-release-early 值 = True
拆离附件 (Strip Attachments)	拆离附件可防范这些文件当中存在病毒。

步骤 4 指定可以访问此隔离区的用户：

用户	信息
本地用户	本地用户列表仅包含具有可以访问隔离区的角色的用户。 该列表不包括具有管理员权限的用户，因为所有管理员都对隔离区具有完全访问权限。
以外部方式进行身份验证的用户 (Externally Authenticated Users)	您必须已配置外部身份验证。

用户	信息
自定义用户角色	仅当您已创建至少一个具有隔离区访问权限的自定义用户角色时，才会看到此选项。

步骤 5 提交并确认更改。

下一步做什么

创建将邮件移到隔离区的邮件与内容过滤器及 DLP 邮件操作。

关于编辑策略、病毒和爆发隔离区设置

注释

- 不能重命名隔离区。
- 另请参阅邮件在隔离区中的保留时间，第 687 页。

要更改隔离区设置，请从“设备配置”页面选择监控 > 策略、病毒和爆发隔离区，然后点击隔离区名称。

确定策略隔离区分配到的过滤器和邮件操作

您可以查看邮件过滤器、内容过滤器、防数据丢失 (DLP) 邮件操作、与策略隔离区相关的 DMARC 验证配置文件。

步骤 1 依次选择**监控 > 策略、病毒和病毒爆发隔离区**。

步骤 2 点击要检查的策略隔离区的名称。

步骤 3 滚动到页面底部，查看**关联邮件过滤器 (Associated Message Filters)/内容过滤器 (Content Filters)/DLP 邮件操作 (DLP Message Actions)**。

关于删除策略隔离区

- 删除策略隔离区之前，请查看它是否与任何有效过滤器或邮件操作相关。请参阅确定策略隔离区分配到的过滤器和邮件操作，第 690 页。
- 即使策略隔离区已被分配到过滤器或邮件操作，也可以将其删除。
- 如果删除的隔离区不为空，则对所有邮件应用隔离区中定义的默认操作，即使已选择磁盘满时不删除邮件的选项亦不例外。请参阅自动处理的隔离邮件的默认操作，第 688 页。

- 在删除与过滤器或邮件操作关联的隔离区后，该过滤器或邮件操作后续隔离的所有邮件都将发送到未分类隔离区。在删除隔离区之前，应自定义未分类隔离区的默认设置。
- 无法删除未分类隔离区.

监控隔离区状态、容量和活动

查看内容	请
为所有非垃圾邮件隔离区分配的总空间	选择，并查看页面的第一部分。 要更改分配，请参阅管理磁盘空间，第 758 页。
所有非垃圾邮件隔离区的当前可用空间	选择监控 > 策略、病毒和病毒爆发隔离区，并查看下方的表格。
所有隔离区当前使用的总空间	选择**监控 (Monitor) > 系统状态 (System Status)**，并查找**隔离区使用的队列空间 (Queue Space Used by Quarantine)**。 选择
每个隔离区当前使用的空间	选择**监控 > 策略、病毒和病毒爆发隔离区**，点击隔离区名称，并直接在隔离区名称下的表格行中查找此信息。
所有隔离区当前的总邮件数	选择**监控 (Monitor) > 系统状态 (System Status)**，并查找**隔离区中的有效邮件 (Active Messages in Quarantine)**。 选择
每个隔离区当前的邮件数	选择**监控 > 策略、病毒和病毒爆发隔离区**，并查看隔离区的表格行。
所有隔离区的总 CPU 使用量	选择**监控 (Monitor) > 系统状态 (System Status)**，并查看 **CPU 使用量 (CPU Utilization)** 部分。 选择。
邮件最后进入每个隔离区的日期和时间（策略隔离区之间的移动除外）	选择**监控 > 策略、病毒和爆发隔离区**，并查看隔离区的表格行。
策略隔离区的创建日期	选择**监控 > 策略、病毒和病毒爆发隔离区**，点击隔离区名称，并直接在隔离区名称下的表格行中查找此信息。 对于系统创建的隔离区，创建日期和创建者名称不可用。
策略隔离区创建者的名称	
与策略隔离区关联的过滤器和邮件操作	请参阅确定策略隔离区分配到的过滤器和邮件操作，第 690 页。

策略隔离区性能

除了硬盘驱动器空间外，策略隔离区中存储的邮件还使用系统内存。在单一设备的策略隔离区中存储成千上万的邮件，可能会由于内存耗用过大，导致设备性能下降。设备需要更多时间来隔离、删除和放行邮件，导致邮件处理速度减缓和邮件管道备份。

思科建议策略隔离区中存储的邮件平均少于 20,000 封，以确保思科安全设备按正常速度处理邮件。

要查看隔离区的邮件数，请参阅监控隔离区状态、容量和活动，第 691 页。

关于隔离区磁盘空间使用量的警报

当策略、病毒和爆发隔离区的容量达到或超过 75%、85% 和 95% 时，系统将发送警报。将邮件放到隔离区时，系统会进行检查。例如，如果添加邮件会使隔离区使用量达到或超过总容量的 75%，则系统会发送警报。

有关警报的详细信息，请参阅告警信息，第 777 页。

策略隔离区和日志记录

AsyncOS 会逐个记录被隔离的所有邮件：

Info: MID 482 quarantined to "Policy" (message filter:policy_violation)

导致邮件被隔离的邮件过滤器或爆发过滤器的功能规则放在括号中。系统会针对放置邮件的每个隔离区生成单独的日志条目。

AsyncOS 还会逐个记录从隔离区删除的邮件：

Info: MID 483 released from quarantine "Policy" (queue full)

Info: MID 484 deleted from quarantine "Anti-Virus" (expired)

从所有隔离区移除邮件后，无论是永久删除还是计划传送，系统会逐个记录邮件，例如

Info: MID 483 released from all quarantines

Info: MID 484 deleted from all quarantines

重新放入邮件时，系统会用新的邮件 ID (MID) 创建新邮件对象。这些信息将使用现有的日志邮件及新 MID“byline”进行记录，例如：

Info: MID 483 rewritten to 513 by Policy Quarantine

关于向其他用户分配邮件处理任务

可以向其他管理用户分配邮件审查和处理任务。例如：

- 人力资源团队可以审查和管理策略隔离区。
- 法律团队可以管理机密资料隔离区。

在指定隔离区的设置时，可向这些用户分配访问权限。要将用户添加到隔离区，这些用户必须已存在。

每个用户可访问所有、部分隔离区或不能访问隔离区。无权查看隔离区的用户在 GUI 或 CLI 隔离区列表的任何位置，都不会看到它们存在的任何提示。

可访问策略、病毒和爆发隔离区的用户组

允许管理用户访问隔离区时，他们可执行的操作取决于其用户组：

- 管理员或邮件管理员组的用户可以创建、配置、删除和集中隔离区，并可管理被隔离的邮件。
- 操作员、访客、只读操作员和服务中心用户组的用户，以及具有隔离区管理权限的自定义用户角色可以搜索、查看和处理隔离区中的邮件，但不能更改隔离区的设置，创建、删除或集中隔离区。可在每个隔离区中指定哪些用户可以访问该隔离区。
- 技术人员组的用户无法访问隔离区。

邮件跟踪和防数据丢失等相关功能的访问权限也会影响管理用户在“隔离区 (Quarantine)”页面看到的选项和信息。例如，如果用户无权访问邮件跟踪，则该用户看不到邮件跟踪链接和被隔离邮件的信息。

终端用户无权查看或访问策略、病毒和病毒爆发隔离区。

关于集群配置中的策略、病毒和病毒爆发隔离区

部署时，只能在计算机级别利用集中管理功能配置策略、病毒和爆发隔离区。

关于集中策略、病毒和病毒爆发隔离区

可以在思科内容安全管理设备上集中策略、病毒和病毒爆发隔离区。有关详细信息，请参阅 集中策略、病毒和病毒爆发隔离区

处理策略、病毒或爆发隔离区中的邮件

查看隔离区中的邮件

目标	请
查看隔离区中的所有邮件	选择**监控 > 策略、病毒和病毒爆发隔离区**。 在相关隔离区的行中，点击表格**邮件 (Messages)** 列的蓝色编号。
查看爆发隔离区中的邮件	选择**监控 > 策略、病毒和病毒爆发隔离区**。 在相关隔离区的行中，点击表格**邮件 (Messages)** 列的蓝色编号。 请参阅“按规则摘要管理”链接，第 699 页[仅限新 Web 界面]。
在隔离区的邮件列表中导航	点击“上一页 (Previous)”、“下一页 (Next)”、页码或双箭头链接。双箭头可带您转至列表的第一页 (<<) 或最后一页 (>>)。

目标	请
排序隔离区的邮件列表	点击列标题（可能包含多个项目的列或“在其他隔离区中”的列除外）。
调整表列	拖动列标题之间的分隔符。
查看导致邮件被隔离的内容。	请参阅查看匹配的内容，第 697 页。

隔离的邮件和国际字符集

如果邮件的主题中包含国际字符集的字符（双字节、可变长度和非 ASCII 编码），则“策略隔离区 (Policy Quarantine)”页面将以非 ASCII 字符的解码形式显示主题行。

查找策略、病毒和病毒爆发隔离区中的邮件

注释
- 用户只能查找和查看其有权访问的隔离区的邮件。
- 策略、病毒和爆发隔离区中的搜索找不到垃圾邮件隔离区中的邮件。

步骤 1 [仅限新 Web 界面] 点击相应隔离区的蓝色数字链接。

提示 [仅限新 Web 界面] 对于病毒爆发隔离区，还可以查找每个病毒爆发规则隔离的所有邮件：点击“病毒爆发”表格行中的**规则摘要**，然后点击相关规则。

步骤 2 选择**监控 > 策略、病毒和病毒爆发隔离区** 。

步骤 3 点击**搜索整个隔离区 (Search Across Quarantines)** 按钮。

提示 对于爆发隔离区，还可以查找每个爆发规则隔离的所有邮件：点击“爆发 (Outbreak)”表格行中的**管理规则摘要**，然后点击相关规则。

步骤 4 （可选）输入其他搜索条件。

- 对于“信封发件人”(Envelope Sender) 和“信封收件人”(Envelope Recipient)：可以输入任何字符。不会针对输入执行验证。
- 搜索结果仅包括与您指定的所有条件都匹配的邮件。例如，如果您指定了“信封收件人 (Envelope Recipient)”和“主题 (Subject)”，则只会返回与“信封收件人 (Envelope Recipient)”和“主题 (Subject)”中指定的术语都匹配的邮件。

下一步做什么

可以按使用隔离区列表的方式使用搜索结果。有关详细信息，请参阅手动处理隔离区中的邮件，第 695 页。

手动处理隔离区中的邮件

手动处理邮件意味着，从“邮件操作 (Message Actions)”页面手动选择适用于邮件的邮件操作。

可以针对邮件执行以下操作：

- 删除
- 放行
- 延迟从隔离区计划退出
- 将邮件副本发送到您指定的邮件地址
- 在不同隔离区之间移动邮件

通常，在进行以下活动时可以针对显示的列表中的邮件执行操作。但是，并不是所有情况下都能执行所有操作。

- 从**监控 > 策略、病毒和病毒爆发隔离区**或页面上的隔离区列表中，点击隔离区中的邮件数。
- 点击**搜索整个隔离区**。
- 点击一个隔离区名称，并在隔离区中搜索。

通过以下方式，可以一次对多封邮件执行这些操作：

- 从邮件列表顶部的拾取列表中选择一个选项。
- 选择页面中列出的每封邮件旁边的复选框。
- 选择邮件列表顶部表格标题中的复选框。这样，操作将应用到屏幕上可见的所有邮件。其他页面上的邮件不受影响。

对于爆发隔离区中的邮件，还可以使用其他选项。请参阅《适用于邮件安全设备的 *AsyncOS*》的在线帮助或用户指南中有关病毒爆发过滤器的章节中的

发送邮件副本

只有管理员组的用户才能发送邮件副本。

要发送邮件副本，请在“副本发送目标: (Send Copy To:)”字段输入邮件地址，然后点击**提交 (Submit)**。发送邮件副本不会导致对该邮件执行任何其他操作。

关于在策略隔离区之间移动邮件

在一台设备上，您可以手动在不同策略隔离区之间移动邮件。

将邮件移到其他隔离区时：

- 到期时间不变。邮件保留原隔离区的保留时间。
- 邮件被隔离的原因（包括匹配的内容及其他相关详细信息）不会更改。
- 如果某个邮件存在于多个隔离区中，将该邮件移到已存有该邮件副本的目标时，移动的邮件副本的到期时间和隔离原因将覆盖目标隔离区原有邮件副本的相应信息。

多个隔离区中的邮件

如果一个或多个其他隔离区都存在某封邮件，则隔离区邮件列表的“在其他隔离区”(In other quarantines) 列将显示“是”(Yes)，无论您是否有权访问其他隔离区。

一封邮件在多个隔离区中：

- 不传送，除非它所在的所有隔离区都将其放行。如果任何隔离区中删除了该邮件，则永不会传送该邮件。
- 不会从任何隔离区删除，除非从其所在的全部隔离区都删除或放行该邮件。

由于想要放行邮件的用户可能无权访问其驻留的所有隔离区，所以以下规则适用：

- 在从邮件驻留的所有隔离区放行邮件之前，不会从任何隔离区放行该邮件。
- 如果某个邮件在任何隔离区中标记为“已删除 (Deleted)”，则无法从其所在的任何其他隔离区中传送该邮件。（仍可以放行。）

如果邮件在多个隔离区中排队，而用户无权访问一个或多个其他隔离区：

- 系统将通知用户，其有权访问的各个隔离区中是否存在该邮件。
- GUI 仅显示用户有权访问的隔离区的预定退出时间。（对于特定邮件，每个隔离区有单独的退出时间。）
- 系统不会告知用户存有该邮件的其他隔离区的名称。
- 用户不会看到导致邮件放入其无权访问的隔离区的匹配内容。
- 放行邮件只会影响用户有权访问的队列。
- 如果该邮件也在用户不可访问的其他隔离区排队，该邮件将留在隔离区中保持不变，直到具有访问其余隔离区所需权限的用户采取操作（或直到该邮件通过提前或正常到期被放行）。

邮件详细信息和查看邮件内容

点击邮件的主题行，可查看邮件内容和访问“隔离的邮件 (Quarantined Message)”页面。

“隔离的邮件 (Quarantined Message)”页面包含两部分：隔离区详细信息和邮件详细信息。

在“隔离的邮件”页面，可以阅读邮件、选择邮件操作发送邮件副本或者检测病毒。另外，还可以查看从隔离区放行邮件时，是否由于“传送时加密 (Encrypt on Delivery)”过滤器操作对邮件加密。

“邮件详细信息 (Message Details)”部分只显示邮件正文、邮件信头和附件。仅显示前 100 K 邮件正文。如果邮件更长，显示前 100 K，后面为省略号 (...)。实际的邮件不会截断。这些信息仅用于显示。通过点击“邮件详细信息”底部“邮件部分”中的 [邮件正文]，可以下载邮件正文。此外，还可以通过点击附件的文件名下载任何邮件附件。

如果您查看的邮件包含病毒，而您的计算机上安装了桌面防病毒软件，则防病毒软件可能报告发现了病毒。这并非对您计算机的威胁，可以安全忽略。

要查看有关邮件的更多详细信息，请点击**邮件跟踪 (Message Tracking)** 链接。

注释 对于特殊爆发隔离区，可使用其他功能。请参阅病毒爆发隔离区 ，第 698 页。

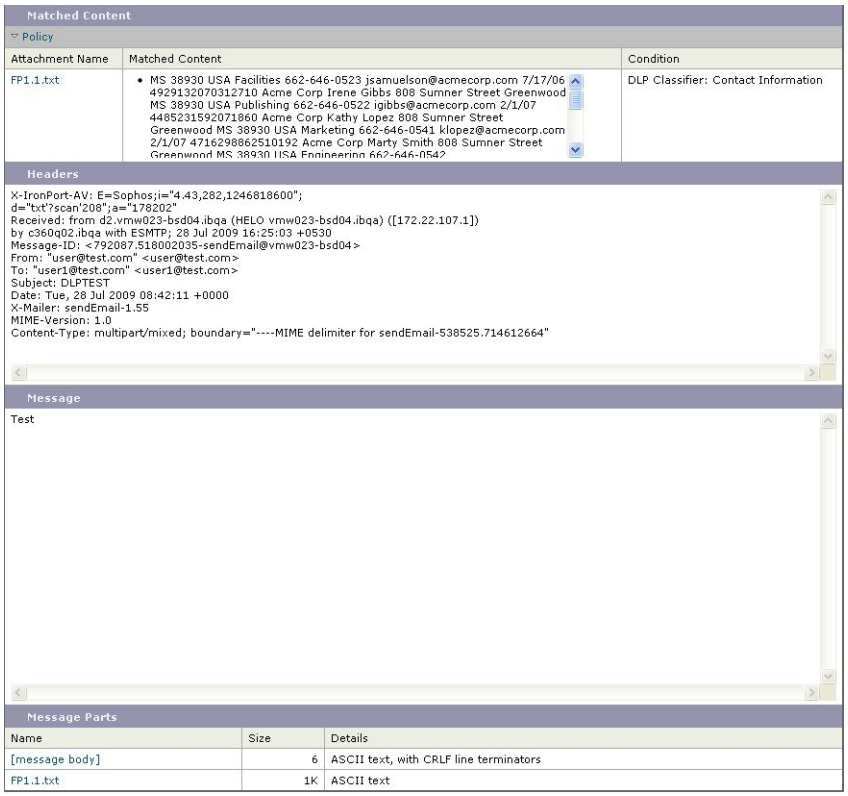
查看匹配的内容

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，匹配内容将以黄色突出显示，DLP 策略违规匹配除外。另外，还可以使用 $MatchedContent 操作变量在邮件主题中包括来自邮件或内容过滤器匹配的匹配内容。

如果附件包含匹配的内容，将显示附件内容以及其被隔离的原因，是由于 DLP 策略违规、内容过滤器条件、邮件过滤器条件，还是图像分析结果。

查看触发了邮件或内容过滤器规则的本地隔离区的邮件时，GUI 可能显示实际上未触发过滤器操作的内容（及已触发过滤器操作的内容）。应将 GUI 显示作为查找内容匹配的指南，但它不一定反映确切的内容匹配。发生这种情况，是因为 GUI 比过滤器使用的内容匹配逻辑更宽松。此问题仅适用于邮件正文中的突出显示。在邮件各个部分列出匹配字符串的表以及相关过滤器规则是正确的。

图 *70:* 在策略隔离区查看的匹配内容



下载附件

通过点击“邮件部分 (Message Parts)”或“匹配内容 (Matched Content)”部分的附件文件名，可以下载邮件附件。AsyncOS 显示警告，表示附件来自未知来源，可能包含病毒，并询问您是否要继续。下载可能包含病毒的附件，风险自负。您还可以点击“邮件部分”部分的 [message body] 下载邮件正文。

病毒检测

要检测邮件中有无病毒，请点击**开始检测 (Start Test)**。使用隔离区暂存邮件，直到确定您的防病毒签名已更新。

检测病毒会发送邮件副本到防病毒引擎，而不是邮件本身。返回并在“隔离区 (Quarantines)”区域上方显示防病毒引擎的结果。

关于重新扫描隔离的邮件

将邮件从其被隔离的所有队列中放行后，将根据为最初隔离邮件的设备和邮件策略启用的功能，进行以下重新扫描。

- 防病毒引擎重新扫描从策略和病毒隔离区放行的邮件。
- 反垃圾邮件和防病毒引擎重新扫描从爆发隔离区放行的邮件。（有关重新扫描病毒爆发隔离区邮件的信息，请参阅）
- 重新扫描从文件分析隔离区放行的邮件中的威胁。
- 从策略、病毒和爆发隔离区放行后，由文件信誉服务重新扫描带附件的邮件。

重新扫描后，如果生成的结果与上次处理邮件时生成的结果相符，则不会再次隔离邮件。相反，如果结果不同，可能会将邮件发送到其他隔离区。

这样是为了防止邮件无限期循环返回隔离区。例如，假定邮件已进行加密，因此发送到病毒隔离区。如果管理员放行该邮件，防病毒引擎仍无法对其解密；但是，应不会再隔离邮件，否则将会创建循环，邮件将永不会从隔离区中放行。由于两次结果相同，所以第二次系统会绕开病毒隔离区。

病毒爆发隔离区

输入有效的爆发过滤器功能许可密钥后，则存在爆发隔离区。根据设定的阈值，爆发过滤器功能将邮件发送到爆发隔离区。有关详细信息，请参阅。

爆发隔离区功能与其他隔离区类似—可以搜索邮件、放行或删除邮件等。

- 标准
- 规则摘要

爆发隔离区包含其他隔离区不可用的一些附加功能：“按规则管理摘要”(Manage by Rule Summary) 链接、查看邮件详细信息时“发送到思科”(Send to Cisco) 功能、以及按预定退出时间对搜索结果中的邮件排序的选项。

如果爆发过滤器功能的许可证到期，将无法向爆发隔离区添加更多邮件。一旦隔离区中当前的邮件过期，爆发隔离区变空，GUI 的隔离区列表将不再显示它们。

重新扫描爆发隔离区中的邮件

如果新发布的规则认为被隔离的邮件不再是威胁，系统将自动放行爆发隔离区中的邮件。

如果在设备上启用了反垃圾邮件和防病毒功能，扫描引擎将根据适用于邮件的邮件流策略扫描从爆发隔离区放行的每封邮件。

“按规则摘要管理”链接

点击隔离区列表中爆发隔离区旁边的“管理规则 (Manage by Rule)”链接，可查看“管理规则摘要 (Manage by Rule Summary)”页面。根据导致邮件被隔离的爆发规则，可以对隔离区中的所有邮件执行邮件操作（放行、删除、延迟退出）。这非常适合清理爆发隔离区中的大量邮件。有关更多信息，请参阅“病毒爆发隔离区和管理规则摘要”视图下的主题

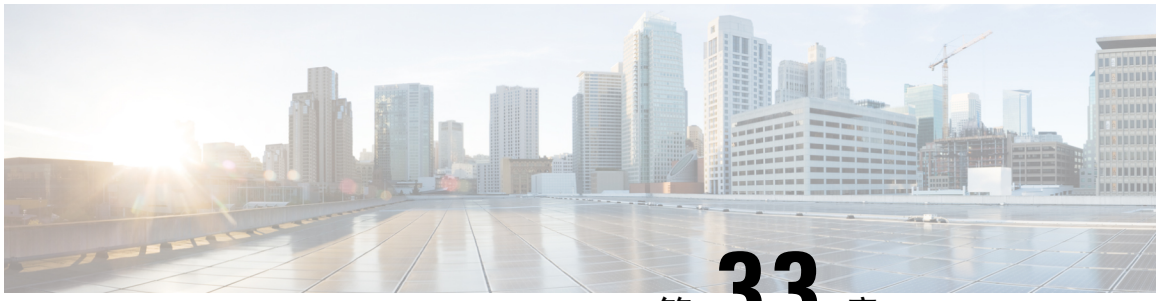
向思科系统公司报告误报或可疑邮件

查看爆发隔离区中邮件的详细信息时，可以将邮件发送到思科报告误报或可疑邮件。

步骤 1 导航到爆发隔离区中的邮件。

步骤 2 在“邮件详细信息 (Message Details)”部分，选择**将副本发送到思科系统 (Send a Copy to Cisco Systems)** 复选框。

步骤 3 点击 **Send**。



第 33 章

垃圾邮件隔离区

本章包含以下部分：

垃圾邮件隔离区概述

垃圾邮件隔离区（也称为 ISQ、最终用户隔离区和 EUQ）为担忧“错误判断”（即合法的邮件被设备认为是垃圾邮件）的组织提供安全保护机制。当设备确定某个邮件是垃圾邮件或是可疑垃圾邮件时，您可能希望让收件人或管理员查看该邮件，然后再传输或删除该邮件。为此，垃圾邮件隔离区会存储邮件。

邮件安全设备的管理用户可查看垃圾邮件隔离区中的所有邮件。最终用户（通常是邮件收件人）可在略微不同的 Web 界面中查看各自的隔离邮件。

垃圾邮件隔离区与策略、病毒和爆发隔离区分隔。

本地与外部垃圾邮件隔离区

本地垃圾邮件隔离区在邮件安全设备上存储垃圾邮件和可疑垃圾邮件。外部垃圾邮件隔离区可在独立的思科内容安全管理设备上存储这些邮件。

如果满足以下条件，请考虑使用外部垃圾邮件隔离区：

- 希望在某个位置集中存储和管理来自多个邮件安全设备的垃圾邮件。
- 希望存储的垃圾邮件数量超过邮件安全设备可承载的范围。
- 希望定期备份垃圾邮件隔离区及其邮件。

设置本地垃圾邮件隔离区

下表演示如何将邮件发送到垃圾邮件隔离区

过程

	命令或操作	目的
步骤 1	启用反垃圾邮件功能（如果尚未启用）。	
步骤 2	启用和配置隔离区设置。	
步骤 3	调整为垃圾邮件隔离区分配的磁盘空间	有关详细信息，请参阅 管理磁盘空间，第 758 页
步骤 4	启用对隔离区的浏览器访问。	有关详细信息，请参阅 配置浏览器访问垃圾邮件隔离区的 IP 接口，第 703 页
步骤 5	配置邮件安全设备以将垃圾邮件发送到隔离区。	有关详细信息，请参阅 • 配置隔离区垃圾邮件的邮件策略，第 704 页 • 限制邮件被隔离的收件人，第 704 页
步骤 6	指定信头中不含这些信息的邮件的默认字符编码。	有关详细信息，请参阅 确保邮件文本正确显示，第 704 页

设置集中垃圾邮件隔离区

过程

	命令或操作	目的
步骤 1	在安全管理设备上，配置垃圾邮件隔离区浏览器界面。	配置浏览器访问垃圾邮件隔离区的 IP 接口，第 703 页
步骤 2	确保邮件安全设备配置为发送邮件到垃圾邮件隔离区。	在邮件安全设备文档中，了解有关配置反垃圾邮件和邮件策略的信息。设置本地垃圾邮件隔离区部分的表中包含指向相关部分的链接。
步骤 3	在邮件安全设备中，启用和配置外部垃圾邮件隔离区。	请参阅您所用版本的邮件安全设备的文档。
步骤 4	在邮件安全设备上，禁用本地隔离区。	有关禁用本地垃圾邮件隔离区，以激活外部垃圾邮件隔离区的信息，请参阅邮件安全设备文档。

配置浏览器访问垃圾邮件隔离区的 IP 接口

当管理员和最终用户访问垃圾邮件隔离区时，将打开独立的浏览器窗口。

步骤 1 依次选择**管理设备 (Management Appliance) > 网络 (Network) > IP 接口 (IP Interfaces)**。

步骤 2

步骤 3 点击接口名称（例如，我们将使用“管理 (Management)”接口）。

步骤 4 在“垃圾邮件隔离区 (Spam Quarantine)”部分，配置垃圾邮件隔离区的访问设置：

- 默认情况下，HTTP 使用端口 82，HTTPS 使用端口 83。
- 指定通知和垃圾邮件隔离区浏览器窗口显示的 URL。

  如果不希望向最终用户显示安全管理设备的主机名，可以指定一个备用主机名。

步骤 5 提交并确认更改。

下一步做什么

确保 DNS 服务器可以解析为访问垃圾邮件隔离区指定的主机名。

配置对垃圾邮件隔离区的管理用户访问权限

所有具有管理员权限的用户均可更改垃圾邮件隔离区设置，并查看和管理垃圾邮件隔离区中的邮件。无需为管理员用户配置垃圾邮件隔离区访问权限。

如果为具有以下角色的用户配置访问垃圾邮件隔离区的权限，他们可以查看、释放和删除垃圾邮件隔离区中的邮件：

- Operator
- 只读操作员 (Read-only operator)
- 服务中心用户 (Help desk user)
- 访客
- 具有垃圾邮件隔离区权限的自定义用户角色

这些用户不能访问垃圾邮件隔离区设置。

开始之前

创建有权访问垃圾邮件隔离区的用户或自定义用户角色。有关详细信息，请参阅see 分配管理任务，第 723 页

步骤 1 如果还没有编辑垃圾邮件隔离区设置页面，请执行以下操作：

a) 选择**监控 > 垃圾邮件隔离区**。

b) 点击“垃圾邮件隔离区”部分的“隔离区名称”列中的**编辑设置** 。

步骤 2 点击要添加的用户类型的链接：本地、外部身份验证或自定义角色。

如果已添加了用户或角色，请点击用户名或角色查看所有符合条件的用户或角色。

步骤 3 选择要添加的用户或角色。

未列出具有管理员权限的用户，因为他们自动具有访问垃圾邮件隔离区的完整权限。

步骤 4 点击 **OK**。

步骤 5 提交并确认更改。

配置隔离区垃圾邮件的邮件策略

一旦启用了垃圾邮件隔离区，即可配置向该隔离区发送垃圾邮件或可疑垃圾邮件的邮件策略。在邮件策略中必须启用反垃圾邮件扫描，以便将邮件发送到垃圾邮件隔离区。

步骤 1 在**邮件策略 > 传入邮件策略**页，点击相应邮件策略的“反垃圾邮件”列中的链接。

步骤 2 在“反垃圾邮件设置 (Anti-Spam Settings)”部分，选择**使用 IronPort 反垃圾邮件服务 (Use IronPort Anti-Spam service)**。

步骤 3 在“确认为垃圾邮件设置 (Positively-Identified Spam Settings)”部分，为**将此操作应用于邮件 (Apply This Action to Message)** 部分选择**垃圾邮件隔离区 (Spam Quarantine)**。

步骤 4 配置对可疑垃圾邮件和营销邮件的设置。

步骤 5 提交并确认更改。

限制邮件被隔离的收件人

在邮件安全设备可以使用多个邮件策略（“邮件策略”>“传入邮件策略”），以指定邮件不会被隔离的收件人地址列表。为邮件策略配置反垃圾邮件设置时，选择“传送”(Deliver)或“丢弃”(Drop)，而不是隔离。

确保邮件文本正确显示

AsyncOS 尝试根据邮件信头中指定的编码确定邮件的字符集。但是，如果信头中指定的编码与实际文本不符，则在垃圾邮件隔离区中查看邮件时，邮件不会正确显示。这种情况较可能发生在垃圾邮件中。

要确保为这些邮件正确显示邮件文本，请参阅。

指定默认编码

如果传入邮件中没有信头指定的字符集编码，则可以配置设备以指定默认编码。

这样，有助于确保这些类型的邮件在垃圾邮件隔离区中正确显示。但是，指定默认编码可能会导致使用其他字符集的邮件无法正确显示。此设置仅适用于信头中未指定编码的邮件。通常，只有在希望属于此类别的大多数邮件采用一种特定编码时，才需要设置默认编码。

例如，如果大多数隔离的邮件未在邮件信头中指定邮件的字符集编码为日语 (ISO-2022-JP)，则可以在“扫描行为”页将编码设置为**日语 (ISO-2022-JP)**。

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

步骤 2 在“全局设置 (Global Settings)”下，点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 在**未指定信息时使用的编码 (Encoding to use when none is specified)** 下拉列表中，选择所需的编码类型。

步骤 4 点击 **Submit**。

步骤 5 点击**确认更改**。

垃圾邮件隔离区语言

每个用户都可从窗口右上角的“选项 (Options)”菜单中选择垃圾邮件隔离区的语言。

编辑垃圾邮件隔离区页面

使用安全列表和阻止列表基于发件人控制邮件发送

管理员和终端用户可以使用安全列表和阻止列表来帮助确定哪些邮件是垃圾邮件。安全列表指定永不被视为垃圾邮件来源的发件人和域。阻止列表指定始终被视为垃圾邮件来源的发件人和域。

可以允许终端用户（邮件用户）管理自己邮件帐户的安全列表和阻止列表。例如，某个终端用户可能会收到其不再感兴趣的邮件列表发来的邮件。他可以决定将此发件人添加到其阻止列表中，以防来自该邮件列表的邮件发送到他的收件箱。另一方面，终端用户可能发现特定发件人的邮件被发送到其垃圾邮件隔离区，而他们不希望这些邮件被视为垃圾邮件。为了确保这些发件人的邮件不会被隔离，他们可以将这些发件人添加到安全列表。

终端用户和管理员所做的更改对彼此可见，并且双方可以相互更改。

安全列表和阻止列表的邮件处理

发件人在安全列表或阻止列表中不会阻碍设备扫描邮件病毒，或确定邮件是否符合内容相关的邮件策略的条件。即使邮件发件人在收件人的安全列表中，但根据其他扫描设置和结果，该邮件也可能不会发送给最终用户。

启用安全列表和阻止列表后，设备会立即对照安全列表/阻止列表数据库扫描邮件，然后才进行反垃圾邮件扫描。如果设备检测到与安全列表或阻止列表条目匹配的发件人或域，当邮件中包含多个收件人时（且这些收件人的安全列表/阻止列表设置不同），该邮件将进行分流。例如，将一封邮件发

送给收件人 A 和收件人 B。收件人 A 将发件人放在安全列表中，而收件人 B 的安全列表或阻止列表中都没有该发件人的条目。这种情况下，邮件可能拆分成两封邮件，使用两个邮件 ID。发送给收件人 *A* 的邮件标记为安全，信头为 *X-SLBL-Result-Safelist*，并跳过反垃圾邮件扫描，而发往收件人 *B* 的邮件将由反垃圾邮件扫描引擎扫描。然后，两封邮件将继续在管道中前行（通过反病毒扫描、内容策略等），并受任何配置的设置约束。

如果邮件发件人或域位于阻止列表中，发送行为将取决于在启用安全列表/阻止列表功能时指定的阻止列表操作。与安全列表发送类似，如果不同收件人的安全列表/阻止列表设置不同，邮件也将分流。然后，根据阻止列表操作设置，隔离或删除被阻止列表分流的邮件。如果阻止列表操作配置为隔离，将对邮件进行扫描，最终进行隔离。如果阻止列表操作配置为删除，则在安全列表/阻止列表扫描后立即删除邮件。

由于安全列表和阻止列表保留在垃圾邮件隔离区中，所以发送行为还取决于其他反垃圾邮件设置。例如，如果在主机访问表 (HAT) 中配置了“接受”邮件流策略以跳过反垃圾邮件扫描，则在该监听程序中收到邮件的用户，其安全列表和阻止列表设置将不会应用于该监听程序上收到的邮件。同样，如果创建了针对特定邮件收件人跳过反垃圾邮件扫描的邮件流策略，则这些收件人将不会应用其安全列表和阻止列表设置。

启用安全列表和阻止列表

开始之前

- 必须启用垃圾邮件隔离区。请参阅设置集中垃圾邮件隔离区，第 702 页。
- 配置邮件安全设备以使用外部安全列表/阻止列表。有关设置外部垃圾邮件隔离区的说明，请参阅邮件安全设备文档。

步骤 1 依次选择**监控 > 垃圾邮件隔离区**。

步骤 2 在**终端用户安全列表/阻止列表（垃圾邮件隔离区）(End-User Safelist/Blocklist (Spam Quarantine))** 部分，选择**启用 (Enable)**。

步骤 3 选择**启用终端用户安全列表/阻止列表功能 (Enable End User Safelist/Blocklist Feature)**。

步骤 4 为“阻止列表操作”选择**隔离区**或**删除**。

步骤 5 指定**每个用户的列表项的最大数目 (Maximum List Items Per User)**。

这是针对每个收件人、每个列表的地址或域的最大数目。如果允许每个用户存在大量列表项，则可能会使系统性能下降。

步骤 6 选择更新频率。此值决定在使用外部垃圾邮件隔离区的邮件安全设备上，AsyncOS 更新安全列表/阻止列表的频率。有关此设置的意义，请参阅外部垃圾邮件隔离区和安全列表/阻止列表，第 707 页。

步骤 7 提交并确认更改。

外部垃圾邮件隔离区和安全列表/阻止列表

如果在安全管理设备中使用外部垃圾邮件隔离区，则安全列表/阻止列表将保存在管理设备上。这样，将提供单一位置来管理所有设备的安全和阻止的发件人。

由于邮件安全设备在处理传入邮件时会评估安全列表和阻止列表中的发件人，所以必须将安全管理设备中存储的安全列表和阻止列表发送到邮件安全设备，以应用于传入邮件。在安全管理设备上配置安全列表/阻止列表功能时，可配置这些更新的频率。

有关在安全管理设备上使用外部安全列表和阻止列表的详细信息，请参阅下的主题和《思科内容安全管理设备用户指南》。

向安全列表和阻止列表中添加发件人和域（管理员）

通过垃圾邮件隔离区界面管理安全列表和阻止列表。

另外，还可以查看是否有许多收件人（贵组织中的最终用户）都将特定发件人或域列入白名单或黑名单。

管理员可以查看和使用每个最终用户查看和使用的相同条目的超集。

开始之前

- 确保您可以访问垃圾邮件隔离区。请参阅访问垃圾邮件隔离区（管理用户），第 719 页。
- 启用对安全列表/阻止列表的访问权限。请参阅启用安全列表和阻止列表，第 706 页。
- （可选）要导入安全列表/阻止列表（而不是使用此部分的步骤建立这些列表），请使用备份和恢复安全列表/阻止列表，第 710 页中所述的过程。
- 了解安全列表和阻止列表条目所需的格式。请参阅安全列表和阻止列表条目的语法，第 708 页。

步骤 1 使用浏览器，访问垃圾邮件隔离区。

步骤 2 请登录。

步骤 3 选择页面右上角的**选项 (Options)** 下拉菜单。

步骤 4 选择**安全列表 (Safelist)** 或**阻止列表 (Blocklist)**。

步骤 5 （可选）搜索发件人或收件人。

步骤 6 执行以下一项或多项操作：

目标	请
为收件人添加多个发件人	1. 选择**查看方式: 收件人 (View by: Recipient)** 2. 点击**添加 (Add)**，或针对某个收件人点击**编辑 (Edit)**。 3. 输入或编辑收件人的邮件地址。 4. 输入发件人的邮件地址和域。 每个条目单独为一行，或使用逗号分隔各个条目。 5. 点击 **Submit**。
为发件人添加多个收件人	1. 选择**查看方式: 发件人 (View by: Sender)** 2. 点击**添加 (Add)**，或针对某个发件人点击**编辑 (Edit)**。 3. 输入或编辑发件人的地址或域。 4. 输入收件人的邮件地址。 每个条目单独为一行，或使用逗号分隔各个条目。 5. 点击 **Submit**。
删除与某个收件人相关的所有发件人 删除与某个发件人相关的所有收件人	1. 选择**查看方式 (View by)** 选项。 2. 点击垃圾箱图标以删除整个表格行。
删除某个收件人的个别发件人 删除某个发件人的个别收件人	1. 选择“查看方式 (View by)”选项。 2. 针对单个收件人或发件人点击**编辑 (Edit)**。 3. 在文本框中添加或删除条目。必须至少留下一个条目。 4. 点击 **Submit**。

安全列表和阻止列表条目的语法

可以使用下列格式向安全列表和阻止列表中添加发件人：

- user@domain.com
- server.domain.com
- domain.com
- [10.1.1.0]
- [ipv6:2001:DB8:1::1]
- user@[1.2.3.4]
- user@[ipv6:2001:db8::1]

同一个条目（例如发件人地址或域）不能同时包含在安全列表和阻止列表中。但是，您可以在将一个域列入安全列表的同时，将属于该域的发件人的邮件地址列入阻止列表，反之亦然。在这种情况下，两种规则都适用。例如，如果 *example.com* 位于安全列表中，可以将 *george@example.com* 列入

阻止列表。这种情况下，设备会发送来自 *example.com* 且发件人不是 *george@example.com* 的所有邮件（此发件人的邮件被视为垃圾邮件），而不扫描垃圾邮件。

不能对使用以下语法的子域范围执行允许或阻止操作：*.domain.com*。但是，可以阻止使用以下语法的特定域：*server.domain.com*。

清除所有安全列表和阻止列表

如果需要删除所有安全列表和阻止列表条目，包括所有发件人和所有收件人，请按照备份和恢复安全列表/阻止列表，第 710 页中的程序导入不含条目的文件。

关于最终用户访问安全列表和阻止列表

最终用户可通过垃圾邮件隔离区访问其安全列表和阻止列表。要配置最终用户对垃圾邮件隔离区的访问权限，请参阅设置终端用户通过网络浏览器访问垃圾邮件隔离区的权限，第 714 页。

可能需要为最终用户提供垃圾邮件隔离区的 URL 及以下说明（如果适用）。

向安全列表添加条目（终端用户）

注释 列入安全列表的发件人的邮传送情况取决于系统中配置的其他设置。请参阅安全列表和阻止列表的邮件处理，第 705 页。

最终用户可通过两种方式向安全列表中添加发件人：

将隔离邮件的发件人添加到安全列表

如果邮件已发送到垃圾邮件隔离区，终端用户可以将发件人添加到安全列表。

步骤 1 在垃圾邮件隔离区，选中邮件旁边的复选框。

步骤 2 从下拉菜单中选择**放行并添加至安全列表**。

可以将指定邮件的信封发件人和信头发件人都添加至安全列表，而放行的邮件可直接转至目标队列，跳过电子邮件管道中的任何其他工作队列处理。

将发件人添加到不含隔离邮件的安全列表

步骤 1 通过浏览器访问垃圾邮件隔离区。

步骤 2 选择页面右上角的**选项 (Options)** 下拉菜单。

步骤 3 选择**安全列表 (Safelist)**。

步骤 4 在“安全列表 (Safelist)”对话框中，输入邮件地址或域。可以输入多个域和邮件地址，并以逗号分隔。

步骤 5 点击**添加到列表 (Add to List)**。

将发件人添加到阻止列表（终端用户）

根据管理员定义的安全列表/阻止列表操作设置，列入阻止列表的发件人所发送的邮件可能会被拒绝或隔离。

注释 只能按照以下过程添加阻止列表条目。

步骤 1 登录到垃圾邮件隔离区。

步骤 2 选择页面右上角的**选项 (Options)** 下拉菜单。

步骤 3 输入要添加到阻止列表的域或邮件地址。可以输入多个域和邮件地址，并以逗号分隔。

步骤 4 点击**添加到列表 (Add to List)**。

同步多个邮件安全设备上的安全列表/阻止列表（没有安全管理设备的部署）

如果使用的多个不含安全管理设备的邮件安全设备，可能需要手动在不同邮件安全设备之间同步安全列表/阻止列表及其配置设置。

可以按照备份和恢复安全列表/阻止列表，第 710 页中所述的步骤导出和导入 .csv 文件，然后使用 FTP 上传和下载文件。

备份和恢复安全列表/阻止列表

在升级设备或运行安装向导之前，应备份安全列表/阻止列表数据库。安全列表/阻止列表信息未包含在含有设备配置设置的主 XML 配置文件中。

另外，还可以使用此程序保存安全列表/阻止列表的副本，以同步多个邮件安全设备。

步骤 1 选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 配置文件 (Configuration File)**。

步骤 2 滚动到**终端用户安全列表/阻止列表数据库（垃圾邮件隔离区）(End-User Safelist/Blocklist Database (Spam Quarantine))** 部分。

目标	请
导出安全列表/阻止列表	请注意 .csv 文件的路径和文件名，并根据需要进行修改。 点击 **Backup Now**。 设备将使用以下命名约定将 .csv 文件保存到设备的 /configuration 目录： *slbl*<序列号><时间戳>*.csv*
导入安全列表/阻止列表	**注意** 此过程将覆盖所有用户的安全列表和阻止列表中的全部现有条目。 点击**选择要恢复的文件 (Select File to Restore)**。 从配置目录的文件列表中选择所需文件。 选择要恢复的安全列表/阻止列表备份文件。 点击 **Restore**。

安全列表和阻止列表故障排除

要排除安全列表和阻止列表的问题，可以查看日志文件或系统警报。

当邮件由于安全列表/阻止列表设置被锁定时，该操作将记录到ISQ_log文件或反垃圾邮件日志文件。列入安全列表的邮件以信头 *X-SLBL-Result-Safelist* 在安全列表中进行标记。列入阻止列表的邮件以信头 *X-SLBL-Result-Blocklist* 在阻止列表中进行标记。

创建或更新数据库时，或者修改数据库或运行安全列表/阻止列表进程出错时，将发送警报。

有关警报的详细信息，请参阅告警信息，第 777 页。

有关日志文件的详细信息，请参阅日志记录，第 855 页。

列入安全列表的发件人的邮件未传送

问题

列入安全列表的发件人的邮件未发送。

解决方案

可能原因：

- 此邮件被恶意软件删除或内容违规。请参阅安全列表和阻止列表的邮件处理，第 705 页。
- 如果有多台设备，并且最近才将发件人添加至安全列表，则处理该邮件时，安全列表/阻止列表可能尚未同步。请参阅外部垃圾邮件隔离区和安全列表/阻止列表，第 707 页和同步多个邮件安全设备上的安全列表/阻止列表（没有安全管理设备的部署），第 710 页。

为终端用户配置垃圾邮件管理功能

目标	请参阅
了解终端用户访问垃圾邮件管理功能采用的不同身份验证方法的优点和局限性。	配置终端用户访问垃圾邮件隔离区的权限，第 714 页 和小节
允许终端用户直接通过浏览器访问垃圾邮件隔离区。	访问垃圾邮件管理功能的终端用户的身份验证选项，第 712 页
如果发给用户的邮件被传送到垃圾邮件隔离区，将向用户发送通知。 通知可能包括访问垃圾邮件隔离区的链接。	通知终端用户被隔离的邮件，第 716 页
允许用户指定以下发件人的电子邮件地址和域：他们认为安全的发件人，及他们知道会发送垃圾邮件或其他不需要邮件的发件人。	使用安全列表和阻止列表基于发件人控制邮件发送，第 705 页

访问垃圾邮件管理功能的终端用户的身份验证选项

注释 邮箱身份验证不允许用户查看发到邮件别名的邮件。

对于终端用户垃圾邮件隔离区访问	请
直接通过网络浏览器，需要身份验证 和 通过通知中的链接，需要身份验证	1. 在“终端用户隔离区访问”设置中，选择 **LDAP**，**SAML 2.0** 或**邮箱 (IMAP/POP)**。 2. 在“垃圾邮件通知 (Spam Notifications)”设置中，取消选择**启用登录时无需隔离区访问凭证 (Enable login without credentials for quarantine access)**。
直接通过网络浏览器，需要身份验证 和 通过通知中的链接，不需要身份验证	1. 在“终端用户隔离区访问”设置中，选择 **LDAP**，**SAML 2.0** 或**邮箱 (IMAP/POP)**。 2. 在“垃圾邮件通知 (Spam Notifications)”设置中，取消选择**启用登录时无需隔离区访问凭证 (Enable login without credentials for quarantine access)**。
仅通过通知中的链接，不需要身份验证	在“终端用户隔离区访问 (End User Quarantine Access)”设置中，选择**无 (None)** 作为身份验证方法。

对于终端用户垃圾邮件隔离区访问	请
无访问权限	在“终端用户隔离区访问 (End User Quarantine Access)”设置中，取消选择**启用终端用户隔离区访问 (Enable End-User Quarantine Access)**。

LDAP 身份验证过程

1. 用户在网络 UI 登录页输入其用户名和密码。
2. 垃圾邮件隔离区连接到指定 LDAP 服务器，执行匿名搜索或作为使用指定“服务器登录”DN 和密码通过身份验证的用户执行搜索。对于 Active Directory，通常需要在“全局目录端口”（在 6000s 中）连接服务器，并需要创建一个权限低的 LDAP 用户，以便垃圾邮件隔离区可以绑定来执行搜索。
3. 然后，垃圾邮件隔离区将使用指定 BaseDN 和查询字符串搜索用户。找到用户的 LDAP 记录时，垃圾邮件隔离区将提取该记录的 DN，并尝试使用该用户记录的 DN 和他们最初输入的密码绑定至目录。如果此密码检查成功，则用户正确通过身份验证，但垃圾邮件隔离区仍需要确定为该用户显示哪些邮箱内容。
4. 邮件使用收件人的信封地址存储在垃圾邮件隔离区中。在用户密码通过 LDAP 验证后，垃圾邮件隔离区会从 LDAP 记录中检索“主邮件属性”，以确定他们应为之显示隔离邮件的哪个信封地址。“主邮件属性”可以包含多个邮件地址，然后使用它们来确定应为通过身份验证的用户显示隔离区中的哪些信封地址。

IMAP/POP 身份验证过程

1. 根据邮件服务器配置，用户向网络用户界面登录页输入其用户名 (joe) 或邮件地址 (joe@example.com) 与密码。可以修改“登录页消息 (Login Page Message)”，以便告知用户应输入完整的邮件地址，还是仅用户名（请参阅配置终端用户访问垃圾邮件隔离区的权限，第 714 页）。
2. 垃圾邮件隔离区连接到 IMAP 或 POP 服务器，并使用输入的登录信息（用户名或邮件地址）和密码尝试登录到 IMAP/POP 服务器。如果接受密码，则用户被视为通过身份验证，而垃圾邮件隔离区会立即从 IMAP/POP 服务器注销。
3. 一旦用户通过身份验证，垃圾邮件隔离区将根据邮件地址列出该用户的邮件：
   - 如果配置了垃圾邮件隔离区来指定附加到裸用户名（例如 joe）的域，将附加此域，并使用完全限定的邮件地址在隔离区中搜索匹配的信封。
   - 否则，垃圾邮件隔离区使将用输入的邮件地址搜索匹配的信封。

有关 IMAP 的详细信息，请参阅华盛顿大学网站：

http://www.washington.edu/imap/

设置终端用户通过网络浏览器访问垃圾邮件隔离区的权限

过程

	命令或操作	目的
步骤 1	了解终端用户访问垃圾邮件管理功能采用的不同身份验证方法的优点和局限性。	请参阅思科内容安全管理设备指南中的使用 *SAML 2.0* 的 *SSO* 部分
步骤 2	如果使用 LDAP 验证终端用户，请配置 LDAP 服务器配置文件，包括**系统管理 > LDAP > LDAP 服务器配置文件**页上的**垃圾邮件隔离区终端用户身份验证查询**设置。 **示例：** `If you will authenticate end users using SAML 2.0 (SSO), configure the settings on the` **`System Administration`** `>` **`SAML`** `page.`	
步骤 3	配置终端用户访问垃圾邮件隔离区的权限。	配置终端用户访问垃圾邮件隔离区的权限，第 714 页
步骤 4	确定终端用户访问垃圾邮件隔离区的 URL。	确定最终用户访问垃圾邮件隔离区的 URL，第 715 页

配置终端用户访问垃圾邮件隔离区的权限

无论是否启用终端用户访问权限，管理用户都可以访问垃圾邮件隔离区。

开始之前

请参阅访问垃圾邮件管理功能的终端用户的身份验证选项，第 712 页中的要求。

步骤 1 选择**监控 >垃圾邮件隔离区**。

步骤 2 点击“垃圾邮件隔离区部分“隔离区名称”列中的**垃圾邮件隔离区**链接。

步骤 3 向下滚动到**终端用户隔离区访问权限**部分。

步骤 4 选择**启用终端用户隔离区访问权限**。

步骤 5 指定终端用户尝试查看自己的隔离邮件时，对他们进行身份验证的方法。

选择此选项	更多信息
无	-

选择此选项	更多信息
邮箱(IMAP/POP)	对于不使用 LDAP 目录进行身份验证的站点，隔离区可以根据保留用户邮箱的基于标准的 IMAP 或 POP 服务器来验证用户邮件地址和密码。 在登录到垃圾邮件隔离区时，终端用户输入其完整的邮件地址和邮箱密码。 如果 POP 服务器在标题中通告支持 APOP，则出于安全考虑（例如，避免以明文形式发送密码），思科设备将仅使用 APOP。如果部分或所有用户不支持 APOP，则应重新配置 POP 服务器，以便不进行 APOP 通告。 如果已将服务器配置为使用 SSL，请选择“SSL”。如果用户仅输入了用户名，可以指定域以自动补充完整的邮件地址。为登录用户输入信封的域，以便“将域附加到非限定用户名”。
LDAP	请按照本主题“准备工作”部分所引用的部分中介绍的操作，配置 LDAP 设置。
SAML 2.0	为垃圾邮件隔离启用单点登录。 在使用此选项之前，请确保已配置了“管理设备”>“系统管理”>“SAML”页面上的所有设置。请参阅《思科内容安全管理设备指南》中的使用 *SAML 2.0* 的 *SSO*。

步骤 6 指定在释放邮件前，是否显示邮件正文。

如果选中此复选框，用户可能无法通过垃圾邮件隔离区页面查看邮件正文。相反，要查看已隔离邮件的正文，用户必须释放该邮件并在其邮件应用（例如 Microsoft Outlook）中查看邮件正文。可以出于政策和法规合规性要求而使用此功能 - 例如，如果法规要求存档所有已查看的邮件。

步骤 7 提交并确认更改。

确定最终用户访问垃圾邮件隔离区的 URL

最终用户直接访问垃圾邮件隔离区所使用的 URL 基于计算机的主机名和启用隔离区的 IP 接口上配置的设置（HTTP/S 和端口号）。例如，HTTP://mail3.example.com:82。

终端用户查看的邮件

通常，终端用户只能在垃圾邮件隔离区中查看自己的邮件。

根据访问方法（通过通知或直接通过网络浏览器）和身份验证方法（LDAP 或 IMAP/POP），用户可以在垃圾邮件隔离区中查看多个邮件地址的邮件。

使用 LDAP 身份验证时，如果主邮件属性具有多个 LDAP 目录值，则所有值（地址）均与该用户关联。因此，对于 LDAP 目录中的终端用户，隔离区中包含发往所有与该用户关联的邮件地址的已隔离邮件。

如果身份验证方法为 IMAP/POP 或用户直接通过通知访问隔离区，则隔离区将仅显示该用户邮件地址（或通知发送到的地址）的邮件。

有关发送到用户所属别名的邮件的信息，请参阅收件人电子邮件的邮件列表别名和垃圾邮件通知，第 717 页。

通知终端用户被隔离的邮件

如果垃圾邮件隔离区中存在用户的垃圾邮件和可疑垃圾邮件，可以将系统配置为向部分或所有这些用户发送通知邮件。

默认情况下，垃圾邮件通知会列出用户的被隔离邮件。此外，通知还包括用户可点击的链接，通过链接可查看其在垃圾邮件隔离区被隔离的邮件。这些链接不会过期。用户可以查看被隔离的邮件，并决定将它们传输到收件箱还是删除。

注释 在群集配置中，只能在计算机级别选择哪些用户可以收到通知。

开始之前

- 最终用户要管理通知中列出的邮件，必须能够访问垃圾邮件隔离区。请参阅配置终端用户访问垃圾邮件隔离区的权限，第 714 页。
- 了解使用通知管理垃圾邮件的身份验证选项。请参阅访问垃圾邮件管理功能的终端用户的身份验证选项，第 712 页。
- 如果最终用户收到多个别名的电子邮件，请参阅收件人电子邮件的邮件列表别名和垃圾邮件通知，第 717 页。

步骤 1 依次选择 **监控 > 垃圾邮件隔离区**。

步骤 2 点击“垃圾邮件隔离区部分“隔离区名称”列中的**垃圾邮件隔离区**链接。

步骤 3 向下滚动至**垃圾邮件通知 (Spam Notifications)** 部分。

步骤 4 选择**启用垃圾邮件通知 (Enable Spam Notification)**。

步骤 5 指定选项。

要自定义邮件正文，请执行以下操作：

a) （可选）自定义默认文本和变量。

要插入变量，请将光标置于希望插入变量的位置，然后点击右侧“邮件变量 (Message Variables)”列表中的变量名称。或键入变量。

以下邮件变量将扩展为特定最终用户的实际值：

- **新邮件数** (%new_message_count%) - 自用户上次登录后的新邮件数。
- **总邮件数** (%total_message_count%) - 用户在垃圾邮件隔离区的邮件数。
- **邮件过期前的天数** (%days_until_expire%)
- **隔离区 URL** (%quarantine_url%) - 用于登录到隔离区和查看邮件的 URL。
- **用户名** (%username%)

- **新邮件表** (%new_quarantine_messages%) - 用户的新隔离邮件的列表，显示发件人、邮件主题、日期和放行邮件的链接。用户点击邮件主题可查看垃圾邮件隔离区中的邮件。
- **不带主题的新邮件表** (%new_quarantine_messages_no_subject%) - 与新邮件表类似，但仅在每封邮件的主题位置显示“查看邮件”链接。

b) 如果在此页面的“最终用户隔离区访问 (End User Quarantine Access)”部分启用了身份验证方法，请执行以下操作：

- 要使用户在点击通知中的链接访问垃圾邮件隔离区时自动登录，请选择**启用登录时无需隔离区访问凭证 (Enable login without credentials for quarantine access)**。最终用户可以释放邮件,只需点击通知中的“释放 (Release)”链接即可。
- 如果需要用户在点击通知中的链接访问垃圾邮件隔离区时进行登录，请取消选择此选项。最终用户不能通过点击通知中的“释放”(Release) 来释放邮件。

c) 点击**预览邮件 (Preview Message)** 可确认邮件是否符合预期。

步骤 6 提交并确认更改。

下一步做什么

要确保最终用户收到这些通知，请考虑建议他们将垃圾邮件隔离区通知电子邮件的“发件人:(From:)”地址添加到其邮件应用（例如 Microsoft Outlook 或 Mozilla Thunderbird）的垃圾邮件设置中的“白名单”。

收件人电子邮件的邮件列表别名和垃圾邮件通知

通知可以发送给拥有隔离邮件的各个信封收件人，包括邮件列表和其他别名。每个邮件列表都会收到一个摘要。如果将通知发送到邮件列表，列表中的所有订阅者都将收到通知。属于多个邮件别名的用户、属于收到通知的 LDAP 组的用户或使用多个邮件地址的用户，都可能收到多个垃圾邮件通知。下表显示了用户可能收到多个通知的案例。

表 *81:* 每个地址/别名的通知

用户	邮件地址	别名	通知
Sam	sam@example.com	—	1
May	mary@example.com	dev@example.com qa@example.com pm@example.com	4
Joe	joe@example.com、admin@example.com	hr@example.com	3

如果使用 LDAP 身份验证，可以选择不向邮件列表别名发送通知。或者，如果选择向邮件列表别名发送垃圾邮件通知，可以防止有时出现的多个通知。请参阅垃圾邮件隔离区别名整合查询，第 623 页。

通过点击通知中的链接访问垃圾邮件隔离区的用户，不会看到最终用户可能拥有的任何其他别名被隔离的邮件，除非设备针对电子邮件通知使用的是垃圾邮件隔离区别名整合查询。如果将通知发送到设备处理后展开的分发列表，则多个收件人可能都有权访问该列表的相同隔离区。

这意味着，邮件列表的所有订阅者都将收到通知，并可以登录到隔离区以释放或删除邮件。这种情况下，最终用户访问隔离区查看通知中提到的邮件时，可能会发现这些邮件已被其他用户删除。

注释 如果不使用 LDAP 且不希望最终用户收到多个电子邮件通知，请考虑禁用通知，改为允许最终用户直接访问隔离区和通过 LDAP 或 POP/IMAP 进行身份验证。

测试通知

可以通过以下方法测试通知：配置测试邮件策略，并仅针对一位用户隔离垃圾邮件。然后，配置垃圾邮件隔离区通知设置：选中**启用垃圾邮件通知 (Enable Spam Notification)** 复选框，但不选择**启用最终用户隔离区访问 (Enable End-User Quarantine Access)**。这样，只有在**将退回邮件发送到 (Deliver Bounced Messages To)** 字段配置的管理员会收到隔离区的新垃圾邮件通知。

垃圾邮件通知故障排除

用户收到多个通知

问题

用户针对一封邮件收到多个垃圾邮件通知。

解决方案

可能原因：

- 用户有多个电子邮件地址，并且该垃圾邮件发送到了其中多个地址。
- 用户是收到该垃圾邮件的一个或多个电子邮件别名的成员。要尽可能减少重复及了解更多信息，请参阅收件人电子邮件的邮件列表别名和垃圾邮件通知，第 717 页。

收件人未收到通知

问题

收件人未收到垃圾邮件通知。

解决方案

- 如果通知被发送到“将退回邮件传送到：”(Deliver Bounce Messages To:) 地址，而不是垃圾邮件收件人，这意味着垃圾邮件通知已启用，但垃圾邮件隔离区访问未启用。请参阅访问垃圾邮件管理功能的终端用户的身份验证选项，第 712 页。
- 让用户检查其电子邮件客户端的垃圾邮件设置。

管理垃圾邮件隔离区的邮件

此部分介绍如何处理本地或外部垃圾邮件隔离区中的邮件。

管理用户可以查看和管理垃圾邮件隔离区的所有邮件。

访问垃圾邮件隔离区（管理用户）

管理用户可以查看和管理垃圾邮件隔离区的所有邮件。

访问垃圾邮件隔离区（管理用户）

选择**监控 > 垃圾邮件隔离区**，然后点击“邮件”列中的编号。

在垃圾邮件隔离区中搜索邮件

步骤 1 指定信封收件人。

注释 可以输入部分地址。

步骤 2 选择搜索结果应与输入的收件人完全匹配，还是结果中应包含输入的条目、以该条目开头或结尾。

步骤 3 输入要搜索的日期范围。点击日历图标以选择日期。

步骤 4 指定“发件人: (From:)”地址，然后选择搜索结果应包含输入的值，与该值完全匹配，还是以该值开头或结尾。

步骤 5 点击 **Search**。页面“搜索 (Search)”部分下将显示符合搜索条件的邮件。

搜索超大邮件集合

如果垃圾邮件隔离区有大量邮件，而且没有具体定义搜索术语，则查询可能需要很长时间才能返回信息，也可能会超时。

系统将提示确认是否要重新提交搜索。请注意，同时运行多个大型搜索可能会影响性能。

查看垃圾邮件隔离区中的邮件

邮件列表显示垃圾邮件隔离区中的邮件。可以选择一次显示的邮件数量。可以点击列标题对显示排序。再次点击同一列可反向排序。

点击邮件主题可查看邮件，包括正文和信头。邮件会显示在“邮件详细信息(Message Details)”页面中。显示邮件的前 20K 信息。如果邮件更长，邮件将在 20K 处截断，您可以通过邮件底部的链接下载邮件。

在“邮件详细信息”页面，可以删除邮件（选择**删除**）或选择**释放**以释放邮件。释放邮件可发送该邮件。

要查看有关邮件的更多详细信息，请点击**邮件跟踪 (Message Tracking)** 链接。

请注意以下提示：

- **查看带附件的邮件**

  查看包含附件的邮件时，将显示邮件的正文，然后是附件列表。

- **查看 HTML 邮件**

  垃圾邮件隔离区会尝试尽可能地呈现基于 HTML 的邮件。不显示图像。

- **查看编码的邮件**

  Base64 编码的邮件将先解码，然后显示。

发送垃圾邮件隔离区中的邮件

如果要放行邮件以进行发送，请点击要释放的一封或多封邮件旁边的复选框，再从下拉菜单中选择**放行**。然后点击**提交**。

点击标题行中的复选框，可自动选择页面中当前显示的所有邮件。

放行的邮件会直接转到目标队列，跳过邮件管道中的任何其他工作队列处理。

删除垃圾邮件隔离区中的邮件

可以将垃圾邮件隔离区配置为：经过一段时间后自动删除邮件。此外，还可以将垃圾邮件隔离区配置为：一旦隔离区达到最大容量，自动删除最早的邮件。也可以手动删除垃圾邮件隔离区中的邮件。

要删除特定邮件，请点击要删除的邮件旁边的复选框，然后从下拉菜单中选择**删除 (Delete)**。然后点击**提交**。点击标题行中的复选框，可自动选择页面当前显示的所有邮件。

要删除垃圾邮件隔离区中的所有邮件，请禁用隔离区（请参阅关于禁用外部垃圾邮件隔离区，第 721 页），然后点击**删除所有邮件 (Delete All Messages)** 链接。链接尾部括号中的数字为垃圾邮件隔离区中的邮件数。

垃圾邮件隔离区的磁盘空间

默认情况下，垃圾邮件隔离区中的邮件经过一段时间后将自动删除。如果隔离区已满，将删除较早的垃圾邮件。

关于禁用外部垃圾邮件隔离区

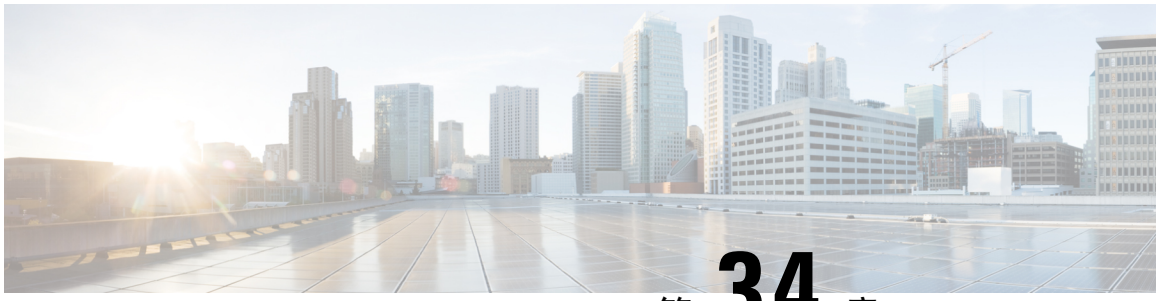
如果禁用垃圾邮件隔离区：

- 如果被禁用的垃圾邮件隔离区中存在邮件，可以选择删除所有邮件。
- 为隔离垃圾邮件设置的所有邮件策略将改为发送邮件。可能需要调整上的邮件策略。
- 要完全禁用外部垃圾邮件隔离区，请在邮件安全设备和安全管理设备上都禁用该外部垃圾邮件隔离区。

只禁用邮件安全设备上的外部垃圾邮件隔离区不会删除外部隔离区或其邮件与数据。

垃圾邮件隔离区功能故障排除

- 安全列表和阻止列表故障排除，第 711 页
- 垃圾邮件通知故障排除，第 718 页
- 确保邮件文本正确显示，第 704 页



第 34 章

分配管理任务

本章包含以下部分：

处理用户帐户

思科设备提供两种添加用户帐户的方法：在思科设备上创建用户帐户；使用您自己的集中身份验证系统（可以是 LDAP 或 RADIUS 目录）启用用户身份验证。可以在 GUI 中的**系统管理 > 用户**页面上（或使用 CLI 中的**userconfig**命令）管理用户和指向外部身份验证源的连接。有关使用外部目录对用户进行身份验证的信息，请参阅外部身份验证， 第 736 页。

或者，您可以通过以下方法为特定用户角色启用双因素身份验证：

- Web 界面中的“系统管理”>“用户”页面。请参阅双因素身份验证， 第 739 页。
- CLI 中的 `userconfig > twofactorauth` 命令。请参阅《用于思科邮件安全设备的 *AsyncOS CLI* 参考指南》。

admin 是系统的默认用户帐户，具有所有管理权限。不能删除 admin 用户帐户，但可以更改密码以及锁定该帐户。

在创建新用户帐户时，可将该用户分配给某一预定义或自定义用户角色。每个角色包含系统之内不同级别的权限。

虽然对可在该设备上创建的用户帐户数量并无限制，但不能使用系统保留的名称来创建用户帐户。例如，不能创建名为“operator”或“root”的用户帐户。

用户角色

表 *82:* 用户角色列表

用户角色	说明
admin	admin 用户是系统的默认用户帐户，并且拥有完全管理权限。此处列出 admin 用户帐户是出于方便考虑，但该帐户不能通过用户角色分配，也不能编辑或删除，只能更改密码。 只有 admin 用户可以发出 **resetconfig** 和 revert 命令。
管理员	具有“管理员 (Administrator)”角色的用户帐户具有系统的所有配置设置的完全访问权限。不过，只有 admin 用户有权访问 **resetconfig** 和 **revert** 命令。 **注释** AsyncOS 不支持多个管理员同时通过 GUI 配置邮件安全设备。
技术人员	具有“技术人员”(Technician) 角色的用户帐户可以执行系统升级、重新引导设备，以及管理功能密钥。为对设备进行升级，“技术人员”(Technician) 还可以执行以下操作： • 暂停邮件传送和接收。 • 查看工作队列和侦听程序的状态。 • 保存及通过邮件发送配置文件。 • 备份安全列表和阻止列表。“技术人员”(Technician) 不能恢复这些列表。 • 断开设备与集群的连接。 • 启用或禁用对思科技术支持的远程服务访问权限。 • 提交支持请求。
操作员	具有“操作员 (Operator)”角色的用户帐户无法执行以下操作： • 创建或编辑用户帐户。 • 发出 **resetconfig** 命令。 • 升级设备。 • 发出 **systemsetup** 命令或运行“系统设置”(System Setup) 向导。 • 发出 **adminaccessconfig** 命令。 • 执行某些隔离区功能（包括创建、编辑、删除和集中隔离区）。 • 在启用 LDAP 进行外部身份验证的情况下，修改除用户名和密码以外的 LDAP 服务器配置文件设置。 除上述情况外，他们所拥有的权限与管理员角色相同。
访客	具有“访客”(Guest) 角色的用户帐户只能查看状态信息和报告。如果在隔离区中启用了访问权限，则具有“访客”(Guest) 角色的用户还可管理隔离区中的邮件。具有“访客 (Guest)”角色的用户不能访问邮件跟踪。

用户角色	说明
只读操作员	具有“只读操作员 (Read-Only Operator)”角色的用户帐户有权查看配置信息。具有“只读操作员”(Read-Only Operator) 角色的用户可以执行和提交更改，以了解如何配置功能，但不能确认更改。如果在隔离区中启用了访问权限，则具有此角色的用户可以管理隔离区中的邮件。 具有此角色的用户不能访问以下信息： • 文件系统、FTP 或 SCP。 • 用于创建、编辑、删除或集中隔离区的设置。
网络管理员用户	具有“服务中心用户”(Help Desk User) 角色的用户帐户只能执行以下操作： • 邮件跟踪。 • 管理隔离区中的邮件。 具有此角色的用户不能访问系统的其余部分，包括CLI。需要启用每个隔离区中的访问权限，然后具有此角色的用户才能管理它们。
自定义用户角色	具有自定义用户角色的用户帐户只能访问分配给该角色的邮件安全功能。这些功能可以是 DLP 策略、邮件策略、报告、隔离区、本地邮件跟踪、加密配置文件和跟踪调试工具的任意组合。此类用户不能访问系统配置功能，包括全局启用功能。只有管理员可以定义自定义用户角色。有关详细信息，请参阅管理授权管理的自定义用户角色，第 728 页。 **注释** 分配了自定义角色的用户不能访问 CLI。

除“服务中心用户”角色和自定义用户角色（他们只能访问 GUI）以外，上表中定义的所有角色均可访问 GUI 和 CLI。

如果使用 LDAP 目录验证用户，可以将目录组分配给用户角色（而不是单个用户）。将目录组分配给用户角色后，该组中的每个用户都会获得为该用户角色定义的权限。有关详细信息，请参阅外部身份验证，第 736 页。

管理用户

“用户”(Users) 页面列出系统的现有用户，包括用户名、完整名称和用户类型或组。

从“用户”(Users) 页面，可以执行以下操作：

- 添加新用户。有关详细信息，请参阅添加用户，第 726 页。
- 删除用户。有关详细信息，请参阅删除用户，第 727 页。
- 编辑用户，如更改用户的密码，以及锁定和解锁用户帐户。有关详细信息，请参阅编辑用户，第 726 页。
- 强制用户更改密码。请参阅强制用户更改其密码，第 726 页。
- 配置本地帐户的用户帐户和密码设置。有关详细信息，请参阅配置受限制的用户帐户和密码设置，第 736 页。

- 使设备能够使用 LDAP 或 RADIUS 目录对用户进行身份验证。有关详细信息，请参阅外部身份验证，第 736 页。
- 对特定用户角色启用双因素身份验证。有关详细信息，请参阅双因素身份验证，第 739 页。
- 启用非管理员对“邮件跟踪”(Message Tracking) 中的“DLP 匹配内容”(DLP Matched Content) 的访问权限。有关详细信息，请参阅控制对“邮件跟踪”中敏感信息的访问权限，第 727 页。

添加用户

准备工作

- 确定要使用的用户角色。
  - 有关预定义用户角色的说明，请参阅用户角色，第 724 页。
  - 要创建自定义角色，请参阅管理授权管理的自定义用户角色，第 728 页。
- 指定密码要求。请参阅配置受限制的用户帐户和密码设置，第 736 页。

步骤 1 依次选择**系统管理 (System Administration) > 用户 (Users)**。

步骤 2 点击**添加用户 (Add User)**。

步骤 3 为用户输入登录名。某些词语是保留词语（如“operator”或“root”）。

步骤 4 输入用户的完整名称。

步骤 5 选择预定义或自定义用户角色。

步骤 6 生成或输入密码。

步骤 7 提交并确认更改。

编辑用户

使用以下过程执行更改密码等操作。

步骤 1 依次选择**系统管理 (System Administration) > 用户 (Users)**。

步骤 2 在“用户 (Users)”列表中点击用户名。

步骤 3 更改该用户。

步骤 4 提交并确认更改。

强制用户更改其密码

步骤 1 依次选择**系统管理 (System Administration) > 用户 (Users)**。

步骤 2 从“用户”(Users) 列表中选择用户。

步骤 3 点击**强制密码更改**。

步骤 4 选择用户是必须在下次登录时更改密码，还是必须在指定持续时间（以天为单位）之后更改密码。

步骤 5 （可选）如果在指定持续时间后强制更改密码，请设置在密码到期后重置密码的宽限期（以天为单位）。

步骤 6 点击 **OK**。

步骤 7 提交并确认更改。

删除用户

步骤 1 在“用户”(Users) 列表中，点击用户名所对应的垃圾桶图标。

步骤 2 在出现的警告对话框中点击**删除 (Delete)**，确认删除。

步骤 3 确认您的更改。

控制对“邮件跟踪”中敏感信息的访问权限

您可能希望限制对可能包含敏感信息的邮件详细信息的管理访问：

- 违反防数据丢失 (DLP) 策略的邮件可能包含公司机密信息或个人信息（包括信用卡号和健康记录）等信息。默认情况下，对设备具有访问权限的所有用户都可以看到此内容。
- 由爆发过滤器或基于 URL 信誉或类别的内容过滤器捕获的 URL 也可能被视为是敏感的。默认情况下，只有具有管理员权限的用户才能查看此内容。

这些敏感内容显示在“邮件跟踪”结果中所列邮件的“邮件详细信息”页面上的专用选项卡中。

您可以根据管理用户的用户角色将这些选项卡及其内容向管理用户隐藏。虽然有一个选项可以向具有管理员角色的用户隐藏此敏感内容，但具有管理员角色的任何用户都可以更改这些权限，从而可以随时查看这些敏感信息。

准备工作

确保您已满足这些功能的先决条件。请参阅在邮件跟踪中显示 URL 详细信息，第 336 页。

步骤 1 依次转到**系统管理 (System Administration) > 用户 (Users)** 页面。

步骤 2 在**对邮件跟踪中敏感信息的访问**下，点击**编辑设置**。

步骤 3 选择要为其授予每种敏感信息的访问权限的角色。

无权访问“邮件跟踪”(Message Tracking) 的自定义角色永远不能查看此信息，因此不会列出。

步骤 4 提交并确认更改。

管理授权管理的自定义用户角色

可以设计自定义用户角色，以及向用户授权与其在组织内的角色一致的特定职责，允许这些授权的管理员仅访问他们负责的邮件安全功能，而不能访问与其角色无关的系统配置功能。通过授权管理，用户可以比预定义的管理员、操作员和服务中心用户角色更灵活地控制对设备上的邮件安全功能的访问。

例如，您可能有负责管理邮件安全设备上特定域的邮件策略的用户，但您不希望这些用户访问系统管理和安全服务配置功能，这些功能是由预定义的管理员和操作员角色授权的。您可以为邮件策略管理员创建自定义用户角色，这些邮件策略管理员可向这些用户授予对其所管理的邮件策略的访问权限，以及对其他邮件安全功能（他们可以使用这些功能管理由这些策略处理的邮件）的访问权限，如“邮件跟踪”(Message Tracking) 和策略隔离区。

使用 GUI 中的**系统管理 > 用户角色**页（或 CLI 中的 **`userconfig -> role`** 命令）定义自定义用户角色，以及管理他们负责的邮件安全功能，如邮件策略、DLP 策略、邮件报告和隔离区。有关授权的管理员可以管理的邮件安全功能的完整列表，请参阅分配访问权限，第 729 页。还可以在使用**系统管理 > 用户**页添加或删除本地用户帐户时创建自定义角色。有关详细信息，请参阅在添加用户帐户时定义自定义用户角色，第 733 页。

您应确保在创建自定义用户角色时，该角色的职责不会与其他授权的管理员的职责重叠过多。例如，如果多个授权的管理员负责同一内容过滤器，并在不同的邮件策略中使用该内容过滤器，则由一个授权的管理员对该过滤器所做的更改，可能会对由其他授权的管理员管理的邮件策略造成意想不到的副作用。

如果您已创建了自定义用户角色，则可以像任何其他用户角色一样，向他们分配本地用户和外部身份验证组。有关详细信息，请参阅处理用户帐户，第 723 页。请注意，分配给自定义角色的用户不能访问 CLI。

“帐户权限”页面

在某一授权的管理员登录到设备时，“帐户权限”(Account Privileges) 页面将显示指向该授权的管理员所负责的安全功能的链接，及其访问权限的简短说明。授权的管理员可以通过选择“选项”(Options) 菜单中的“帐户权限”(Account Privileges) 返回到此页面。授权的管理员还可以使用位于网页顶部的菜单访问其所管理的功能。

下图显示了具有对邮件策略、邮件报告、邮件跟踪和隔离区的访问权限的授权的管理员“帐户权限”页面。

图 *71:* 授权的管理员的“帐户权限”*(Account Privileges)* 页面

分配访问权限

在创建自定义用户角色时，您应定义对授权的管理员所负责的安全功能的访问权限的级别。

可供授权的管理员管理的安全功能包括：

- 传入和传出邮件策略，以及内容过滤器。
- 防数据丢失 (DLP) 策略。
- 邮件报告。
- 邮件跟踪。
- 跟踪调试工具。
- 垃圾邮件、策略、病毒和爆发隔离区。
- 思科邮件加密配置文件。

在定义自定义用户角色的访问权限级别之后，您需要分配授权的管理员将要负责的特定邮件策略、内容过滤器、DLP 策略、隔离区或加密配置文件。

例如，您可以创建两个负责不同 DLP 策略的不同 DLP 策略管理员角色。其中一个角色仅负责与公司保密性和可接受的使用有关的 DLP 违规，而另一个角色则负责与隐私保护有关的 DLP 违规。除了 DLP 策略访问权限以外，还可以为这些自定义用户角色分配跟踪邮件数据以及查看隔离区和报告的权限。他们可以使用邮件跟踪搜索与他们所负责的策略相关的 DLP 违规。

可以通过点击“用户角色”(User Roles) 页面上“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 表中已分配权限的链接，查看可将哪些职责分配给自定义用户角色。请参阅更新自定义用户角色的职责，第 734 页。

邮件策略和内容过滤器

邮件策略和内容过滤器访问权限定义授权的管理员对邮件安全设备上的传入和传出邮件策略及内容过滤器的访问权限级别。可将特定的邮件策略和内容过滤器分配给自定义用户角色，仅允许属于此角色的授权的管理员，与操作员和管理员一起，管理邮件策略和内容过滤器。

具有此访问权限的所有授权的管理员可以查看默认传入和传出邮件策略，但如果他们具有完全访问权限，只能编辑这些策略。

具有访问权限的所有授权的管理员可以创建新内容过滤器，以与其邮件策略一起使用。由某一授权的管理员创建的内容过滤器可供分配到该自定义用户角色的其他授权的管理员使用。未分配给任何自定义用户角色的内容过滤器都是公共的，并且可由所有具有邮件策略访问权限的授权的管理员查看。默认情况下，由操作员或管理员创建的内容过滤器是公共的。授权的管理员可以启用或禁用针对已分配给其自定义用户角色的所有现有的内容过滤器，但不能修改或删除公共内容过滤器。

如果某一授权的管理员删除了由他们自己的邮件策略以外的其他邮件策略使用的某一内容过滤器，或者如果该内容过滤器已分配给其他自定义用户角色，则 AsyncOS 不会从系统中删除该内容过滤器。相反，AsyncOS 将会取消内容过滤器与自定义角色的链接，并将其从该授权的管理员的邮件策略中删除。内容过滤器仍可用于其他自定义用户角色和邮件策略。

授权的管理员可在其内容过滤器中使用任何文本资源或词典，但他们不能访问 GUI 中的“文本资源”(Text Resources) 或“词典”(Dictionaries) 页面来查看或修改它们。授权的管理员也不能创建新文本资源或词典。

对于传出邮件策略，授权的管理员可以启用或禁用 DLP 策略，但他们不能自定义 DLP 设置，除非他们还具有 DLP 策略权限。

可为自定义用户角色分配对邮件策略和内容过滤器的以下访问权限级别之一：

- **无访问权限 (No access)**：授权的管理员不能查看或编辑邮件安全设备上的邮件策略和内容过滤器。
- **查看分配内容、编辑分配内容 (View assigned, edit assigned)**：授权的管理员可以查看和编辑分配给自定义用户角色的邮件策略及内容过滤器，还可创建新内容过滤器。授权的管理员可以编辑策略的“反垃圾邮件”(Anti-Spam)、“防病毒”(Anti-Virus) 和“爆发过滤器”(Outbreak Filters) 设置。他们可为策略启用其内容过滤器，以及禁用分配给策略的所有现有内容过滤器，而无论他们是否负责该策略。授权的管理员不能修改邮件策略的名称或其发件人、收件人或组。授权的管理员可以修改分配给其自定义用户角色的邮件策略的内容过滤器的顺序。
- **查看所有，编辑已分配 (View all, edit assigned)**：授权的管理员可以查看设备上的所有邮件策略和内容过滤器，但他们只能编辑分配给该自定义用户角色的邮件策略和内容过滤器。

查看所有，编辑所有（完全访问权限）(View all, edit all (full access))：授权的管理员具有对设备上所有邮件策略和内容过滤器的完全访问权限，包括默认邮件策略，并能创建新邮件策略。授权的管理员可以修改所有邮件策略的发件人、收件人和组。他们还可以对邮件策略重新排序。

可以使用“邮件安全管理器”(Email Security Manager) 或“用户角色”(User Roles) 页面上的“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 表，将单个邮件策略和内容过滤器分配给自定义用户角色。

有关使用“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 表分配邮件策略和内容过滤器的信息，请参阅更新自定义用户角色的职责，第 734 页。

DLP 策略

DLP 策略访问权限通过邮件安全设备上的 DLP 策略管理器定义授权的管理员对 DLP 策略的访问权限级别。可将 DLP 策略分配给特定的自定义用户角色，除了操作员和管理员以外，还允许授权的管

理员管理这些策略。具有DLP访问权限的授权的管理员还可以从“防数据丢失全局设置”(Data Loss Prevention Global Settings) 页面导出 DLP 配置文件。

如果某一授权的管理员还具有邮件策略权限，则他们可以自定义DLP策略。授权的管理员可以使用其 DLP 策略的任何自定义 DLP 词典，但他们无法查看或修改自定义 DLP 词典。

可为自定义用户角色分配对 DLP 策略的以下访问权限级别之一：

- **无访问权限**：授权的管理员不能查看或编辑邮件安全设备上的 DLP 策略。
- **查看已分配，编辑已分配**：授权的管理员可以使用DLP策略管理器查看和编辑分配给自定义用户角色的 DLP 策略。授权的管理员不能对 DLP 策略管理器中的 DLP 策略进行重命名或重新排序。授权的管理员可以导出 DLP 配置。
- **查看所有，编辑已分配**：授权的管理员可以查看和编辑分配给自定义用户角色的DLP策略。他们可以导出 DLP 配置。他们还可以查看未分配给自定义用户角色的所有 DLP 策略，但他们不能编辑这些策略。授权的管理员不能对 DLP 策略管理器中的 DLP 策略重新排序，也不能重命名策略。
- **查看所有，编辑所有（完全访问权限）**：授权的管理员具有对设备上的所有DLP策略的完全访问权限，包括能够创建新策略。授权的管理员可对 DLP 策略管理器中的 DLP 策略重新排序。他们不能更改设备所使用的 DLP 模式。

可以使用DLP策略管理器或“用户角色”页面上的“授权管理的自定义用户角色”表，将各个DLP策略分配给自定义用户角色。

有关 DLP 策略和 DLP 策略管理器的详细信息，请参阅数据防泄漏，第 373 页。

有关使用“授权管理的自定义用户角色”列表分配DLP策略的详细信息，请参阅更新自定义用户角色的职责，第 734 页。

邮件报告

邮件报告访问权限根据自定义用户角色对邮件策略、内容过滤器和DLP策略的访问权限，定义授权的管理员可以查看哪些报告和“邮件安全监控”页面。这些报告没有针对已分配的策略进行过滤；授权的管理员可以查看不属于负责的邮件和 DLP 策略的报告。

可为自定义用户角色分配对邮件报告的以下访问权限级别之一：

- **无访问权限 (No access)**：授权的管理员不能查看邮件安全设备上的报告。
- **查看相关报告 (View relevant reports)**：授权的管理员可以查看“邮件安全监控”(Email Security Monitor) 页面上与其邮件策略、内容过滤器和 DLP 策略访问权限相关的报告。具有邮件策略和内容过滤器访问权限的授权的管理员可以查看以下“邮件安全监控”(Email Security Monitor) 页面：
  - 概述
  - 传入邮件
  - 外发目标
  - 外发邮件发件人
  - 内部用户
  - 内容过滤器
  - 病毒爆发

- 病毒类型
- 存档的报告

具有 DLP 策略访问权限的授权的管理员可以查看以下“邮件安全监控”(Email Security Monitor) 页面：

- 概述
- DLP 事件
- 存档的报告

- **查看所有报告 (View all reports)**：授权的管理员可以查看邮件安全设备上的所有报告和“邮件安全监控”(Email Security Monitor) 页面。

有关邮件报告和邮件安全监控的详细信息，请参阅使用邮件安全监控，第 637 页一章。

邮件跟踪

邮件跟踪访问权限定义分配给自定义用户角色的授权的管理员是否有权访问邮件跟踪；如果已在**系统管理 > 用户**页面上启用了“DLP 追踪策略”选项，并且自定义用户角色也具有 DLP 策略访问权限，则还包括可能违反组织的 DLP 策略的邮件内容。

授权的管理员只能搜索分配给他们的 DLP 策略的 DLP 违规。

有关邮件跟踪的详细信息，请参阅邮件跟踪，第 677 页。

有关允许授权的管理员访问查看“邮件跟踪”(Message Tracking) 中匹配的 DLP 内容的信息，请参阅控制对“邮件跟踪”中敏感信息的访问权限，第 727 页。

跟踪

跟踪访问权限定义分配给自定义用户角色的授权的管理员是否可以使用“跟踪”(Trace) 调试通过系统的邮件流。具有访问权限的授权的管理员可以运行“跟踪”(Trace) 和查看所有生成的输出。跟踪结果不会根据授权的管理员的邮件或 DLP 策略权限进行过滤。

有关使用跟踪的详细信息，请参阅使用测试邮件调试邮件流：追踪，第 935 页。

隔离区

隔离区访问权限定义授权的管理员是否可以管理已分配的隔离区。授权的管理员可以查看已分配的隔离区中的所有邮件，并对它们进行操作，如放行或删除邮件，但不能更改隔离区的配置（例如大小、保留时间等），或者创建或删除隔离区。

可以使用“监控”(Monitor) > “隔离区”(Quarantines) 页面或“用户角色”(User Roles) 页面上的“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 表，将任何隔离区分配给自定义用户角色。

有关将隔离区管理任务分配给管理用户的更多信息，请参阅关于向其他用户分配邮件处理任务，第 692 页和配置对垃圾邮件隔离区的管理用户访问权限，第 703 页。

有关使用“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 列表分配隔离区的信息，请参阅更新自定义用户角色的职责，第 734 页。

加密配置文件：

加密配置文件访问权限定义授权的管理员是否可在编辑内容过滤器或DLP策略时，使用分配给自己的自定义用户角色的加密配置文件。加密配置文件只能分配给具有邮件或DLP策略访问权限的自定义用户角色。未分配给自定义角色的加密配置文件可供具有邮件或DLP策略权限的所有委派管理员使用。授权的管理员不能查看或修改任何加密配置文件。

在使用“安全服务”(Security Services)>“IronPort邮件加密”(IronPort Email Encryption)页面创建或编辑加密配置文件时，可以分配加密配置文件。

定义自定义用户角色

可以使用GUI中的“用户角色”页（或CLI中的userconfig -> role命令）定义新用户角色和分配其访问权限。“用户角色”(User Roles)页面显示设备上的所有现有自定义用户角色，以及每个角色的访问权限。

步骤1 依次选择**系统管理 (System Administration) > 用户角色 (User Roles)**。

步骤2 点击**添加用户角色 (Add User Role)**。

步骤3 为用户角色输入一个名称。

步骤4 为用户角色及其权限输入一段说明。

步骤5 选择用户角色的访问权限。（有关各种类型访问权限的详细信息，请参阅分配访问权限，第729页。）

步骤6 提交并确认更改。

在添加用户帐户时定义自定义用户角色

在在邮件安全设备上添加或编辑本地用户帐户时，可以创建新自定义用户角色。

有关添加用户帐户的详细信息，请参阅管理用户，第725页。

步骤1 依次转到**系统管理 (System Administration) > 用户 (Users)**页面。

步骤2 点击 **Add User**（**添加用户**）。

步骤3 在创建用户帐户时，选择“自定义角色”(Custom Roles)。

步骤4 选择**添加角色 (Add Role)**。

步骤5 为新角色输入名称。

步骤6 提交新用户帐户。

AsyncOS显示一条通知，表示已添加新用户帐户和自定义用户角色。

步骤7 依次转到**系统管理 (System Administration) > 用户角色 (User Roles)**页面。

步骤8 在“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration)表中，点击自定义用户角色的名称。

步骤 9 为用户角色及其权限输入一段说明。

步骤 10 选择用户角色的访问权限。（有关各种类型访问权限的详细信息，请参阅分配访问权限，第 729 页。）

步骤 11 提交并确认更改。

更新自定义用户角色的职责

步骤 1 依次转到**系统管理 (System Administration) > 用户角色 (User Roles)** 页面。

步骤 2 点击您要更新的自定义用户角色的访问权限的名称。

AsyncOS 将显示一个列表，其中包括设备上可用的所有邮件策略、内容过滤器、DLP 策略或隔离区，以及任何其他已分配的自定义用户角色的名称。

步骤 3 选择您希望已分配的授权的管理员负责的邮件策略、内容过滤器、DLP 策略或隔离区。

步骤 4 提交并确认更改。

编辑自定义用户角色

步骤 1 依次转到**系统管理 (System Administration) > 用户角色 (User Roles)** 页面。

步骤 2 在“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 列表中，点击用户角色的名称。

步骤 3 对该用户角色进行更改。

步骤 4 提交并确认更改。

复制自定义用户角色

您可能希望创建多个具有相似访问权限的自定义用户角色，但为不同的用户组分配不同的职责。例如，如果邮件安全设备处理多个域的邮件，您可能希望创建多个具有相似访问权限、但适用于基于该域的不同邮件策略的自定义用户角色。这样可使授权的管理员能够管理自己的域的邮件策略，而不干扰其他授权的管理员的职责。

步骤 1 依次转到**系统管理 (System Administration) > 用户角色 (User Roles)** 页面。

步骤 2 点击与您希望在“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 列表中复制的用户角色相对应的复制图标。

步骤 3 更改自定义用户角色的名称。

步骤 4 进行新自定义用户角色所需的所有访问权限更改。

步骤 5 提交并确认更改。

删除自定义用户角色

在删除某一自定义角色后，用户将变为未分配状态，并且没有对设备的访问权限。如果删除分配给一个或多个用户的自定义用户角色，则您不会收到警告消息。您应重新分配先前分配给已删除的自定义用户角色的所有用户。

步骤 1 依次转到**系统管理 (System Administration) > 用户角色 (User Roles)** 页面。

步骤 2 点击与您希望在“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 列表中删除的用户角色相对应的垃圾桶图标。

步骤 3 在出现的警告对话框中点击**删除 (Delete)**，确认删除。

步骤 4 确认您的更改。

密码

更改密码

管理用户可以通过位于 GUI 顶部的“选项”>“更改密码”链接更改他们自己的密码。

提交新密码后，系统会立即将您注销并转到登录屏幕。

在 CLI 中，使用 passphrase 或 passwd 命令更改密码。如果忘记了管理员用户帐户的密码，请联系您的客户支持提供商重置密码。

为了安全起见，passphrase 命令要求输入旧密码。

注释 密码更改会立即生效，并且不会要求您确认更改。

锁定和解锁用户帐户

锁定用户帐户可防止本地用户登录设备。通过以下方式之一可锁定用户帐户：

- 如果某一用户超过了“本地用户帐户和密码设置”部分中定义的最大尝试登录失败次数，AsyncOS 将锁定该用户帐户。
- 管理员可以为了安全目的，使用“系统管理”(System Administration) >“用户”(Users) 页面手动锁定用户帐户。

在“编辑用户 (Edit User)”页面查看用户帐户时，AsyncOS 将显示用户帐户被锁定的原因。

要解锁用户帐户，请通过点击“用户”(Users) 列表中的用户名打开用户帐户，然后点击**解锁帐户 (Unlock Account)**。

要手动锁定本地用户帐户，请通过点击“用户”(Users) 列表中的用户名打开用户帐户，然后点击**锁定帐户 (Lock Account)**。AsyncOS 将显示一条消息，表示用户无法登录到设备，并询问是否要继续。

如果用户在已配置的尝试次数后未能成功登录，您还可以将所有本地用户帐户配置为锁定。有关详细信息，请参阅配置受限制的用户帐户和密码设置，第 736 页。

注释 如果锁定 admin 帐户，则只能在以管理员身份登录后通过串行通信连接到串行控制台端口将其解锁。即使在 admin 帐户被锁定时，admin 用户也可以使用串行控制台端口访问设备。有关使用串行控制台端口访问设备的详细信息，请参阅连接到设备，第 24 页。

配置受限制的用户帐户和密码设置

可以通过定义用户帐户和密码限制来实施组织密码策略。用户帐户和密码限制适用于在思科设备上定义的本地用户。可以配置以下设置：

- **用户帐户锁定 (User account locking)**。可以定义导致用户帐户锁定的登录尝试失败次数。
- **密码有效期规则**。可以定义密码的有效期，在该期限之后，用户登录后需要更改密码。
- **密码规则**。可以定义用户可选择的密码类型，例如哪些字符是可选的或必需的。

可以在“本地用户帐户和密码设置”部分的“系统管理”>“用户”页面上定义用户帐户和密码限制。

外部身份验证

如果您将用户信息存储在网络上的 LDAP 或 RADIUS 目录中，则可将思科设备配置为使用外部目录对登录到该设备的用户进行身份验证。要将设备设置为使用外部目录进行身份验证，请使用 GUI 中的“系统管理”>“用户”页，或 CLI 中的 userconfig 命令和 external 子命令。

在启用外部身份验证后，并且用户登录到邮件安全设备时，该设备会先确定该用户是否是系统定义的“admin”帐户。如果不是，则该设备将检查配置的第一个外部服务器，以确定该用户是否是在那里定义的。如果该设备无法连接到第一个外部服务器，则它将检查列表中的下一个外部服务器。

对于 LDAP 服务器，如果用户在任何外部服务器上的身份验证失败，则该设备会尝试将该用户，对其进行身份验证。如果用户不存在于任何外部服务器或设备上，或者如果用户输入错误的密码，则对该设备的访问将被拒绝。

如果外部 RADIUS 服务器无法联系，将尝试列表中的下一个服务器。如果所有服务器都无法联系，则设备会尝试将用户作为在邮件安全设备上定义的本地用户进行身份验证。但是，如果外部RADIUS 服务器因故拒绝用户，如密码不正确或是用户缺习，则对该设备的访问将被拒绝。

启用 LDAP 身份验证

除了使用 LDAP 目录对用户进行身份验证以外，还可以将 LDAP 组分配给思科用户角色。例如，您可以将IT组中的用户分配给“管理员”(Administrator)用户角色，此外，您还可以将“支持”(Support)组中的用户分配给“服务中心用户”(Help Desk User) 角色。如果用户属于具有不同用户角色的多个 LDAP 组，AsyncOS 会为用户授予最受限制角色的权限。例如，如果用户属于具有“操作人员 (Operator)”权限的组和具有“服务中心用户 (Help Desk User)”权限的组，则 AsyncOS 会为该用户授予“服务中心用户 (Help Desk User)”角色的权限。

注释 如果外部用户更改其 LDAP 组的用户角色，则该用户应从设备注销，然后重新登录。该用户将具有其新角色的权限。

准备工作

定义一个 LDAP 服务器配置文件和一个 LDAP 服务器的外部身份验证查询。有关详细信息，请参阅LDAP 查询，第 585 页

步骤 1 依次选择**系统管理 (System Administration) > 用户 (Users)**。

步骤 2 向下滚动到**外部身份验证 (External Authentication)** 部分。

步骤 3 点击**启用 (Enable)**。

步骤 4 选中**启用外部身份验证 (Enable External Authentication)** 复选框。

步骤 5 为身份验证类型选择 **LDAP**。

步骤 6 在网络用户界面中输入存储外部身份验证凭证的时间长度。

步骤 7 选择对用户进行身份验证的 LDAP 外部身份验证查询。

步骤 8 输入超时前设备等待服务器响应的秒数。

步骤 9 输入希望设备验证的 LDAP 目录中的组名称，然后选择该组中用户的角色。

步骤 10 （可选）点击**添加行**添加另一个目录组。为设备验证的每个目录组重复执行步骤 9 和 10。

步骤 11 提交并确认更改。

启用 RADIUS 身份验证

您还可以使用 RADIUS 目录对用户进行身份验证，以及将用户组分配给角色。RADIUS 服务器应支持“类”(CLASS) 属性，AsyncOS 将使用该属性将 RADIUS 目录中的用户分配给用户角色。AsyncOS 支持两种用于与 RADIUS 服务器通信的身份验证协议：密码身份验证协议 (PAP) 和质询握手身份验证协议 (CHAP)。

要将 RADIUS 用户分配给思科用户角色，请先在包含字符串值 <radius-group> 的 RADIUS 服务器上设置CLASS属性，该字符串值将映射到思科用户角色。“类(CLASS)”属性可以包含字母、数字和短划线，但不能以短划线开头。AsyncOS 不支持“类 (CLASS)”属性中的多个值。如果 RADIUS 用户属于某一个组，而该组不含“类”(CLASS) 属性，或者包含未映射的“类”(CLASS) 属性，则这些 RADIUS 用户不能登录到设备。

如果设备无法与 RADIUS 服务器通信，用户可以使用设备上的本地用户帐户登录。

注释 如果外部用户更改了其 RADIUS 组的用户角色，则该用户应注销设备，然后重新登录。该用户将获得新角色的权限。

步骤 1 在**系统管理** > **用户**页面中，点击**启用**。

步骤 2 如果尚未启用，请选中“启用外部身份验证”选项。

步骤 3 输入 RADIUS 服务器的主机名。

步骤 4 输入 RADIUS 服务器的端口号。默认端口号为 1812。

步骤 5 输入 RADIUS 服务器的共享密钥密码。

步骤 6 输入超时前设备等待服务器响应的秒数。

步骤 7 （可选）点击**添加行 (Add Row)** 添加另一台 RADIUS 服务器。为每个 RADIUS 服务器重复步骤 3 - 6。

注释 最多可以添加十个 DNS 服务器。

步骤 8 输入 AsyncOS 在再次与 RADIUS 服务器联系以在“外部身份验证缓存超时”(External Authentication Cache Timeout) 字段中再次进行身份验证之前，存储外部身份验证凭证的秒数。默认值为零 (0)。

注释 如果 RADIUS 服务器使用一次性密码（例如基于令牌创建的密码），请输入零 (0)。如果该值设置为零，在当前会话期间，AsyncOS 不会再次联系 RADIUS 服务器进行身份验证。

步骤 9 配置组映射：

设置	说明
将通过外部身份验证的用户映射到多个本地角色。	AsyncOS 将基于 RADIUS“类”(CLASS) 属性将 RADIUS 用户分配给设备角色。“类 (CLASS)”属性要求： • 最少 3 个字符 • 最多 253 个字符 • 不含冒号、逗号或换行符 • 每个 RADIUS 用户有一个或多个映射的“类 (CLASS)”属性（有了此设置，AsyncOS 可拒绝访问没有映射“类 (CLASS)”属性的 RADIUS 用户。） 对于具有多个“类 (CLASS)”属性的 RADIUS 用户，AsyncOS 将分配限制性最高的角色。例如，如果 RADIUS 用户有两个“类 (CLASS)”属性，分别映射到“操作员”和“只读操作员”角色，则 AsyncOS 会将 RADIUS 用户分配到“只读操作员”角色，因为该角色比“操作员”角色限制性高。 下面是设备角色限制性由低到高的顺序： • admin • 管理员 • 技术人员 • 操作员 cloudadmin • 只读操作员 (Read-only Operator) • 网络管理员用户 • 访客
将所有外部身份验证的用户映射为管理员角色。	AsyncOS 将 RADIUS 用户分配到“管理员”角色。

步骤 10 选择是将所有外部身份验证的用户映射到“管理员”(Administrator) 角色，还是映射到不同的设备用户角色类型。

步骤 11 如果将用户映射到不同的角色类型，请按照“组名称”(Group Name) 或“目录”(Directory) 字段中 RADIUS“类”(CLASS) 属性中的定义，输入组名称，并从“角色”(Role) 字段中选择设备角色类型。可以通过点击**添加行 (Add Row)** 添加更多角色映射。

有关用户角色类型的详细信息，请参阅处理用户帐户，第 723 页。

步骤 12 提交并确认更改。

双因素身份验证

可以使用 RADIUS 目录为特定用户角色配置双因素身份验证。设备支持以下与 RADIUS 服务器通信的身份验证协议：

- 密码身份验证协议 (PAP)

- 质询握手身份验证协议 (CHAP)

可以为以下用户角色启用双因素身份验证：

- 预定义
- custom

该功能已在以下设备上进行了测试：

- RSA 身份验证管理器 v8.2
- FreeRADIUS v1.1.7 及更高版本
- ISE v1.4 及更高版本

启用双因素身份验证

准备工作

请确保从 IT 管理员那里获得了双因素身份验证所需的 RADIUS 服务器详细信息。

步骤 1 在**系统管理 > 用户**页上，点击“双因素身份验证”下的**启用**。
步骤 2 输入 RADIUS 服务器的主机名或 IP 地址。
步骤 3 输入 RADIUS 服务器的端口号。
步骤 4 输入 RADIUS 服务器的共享密钥密码。
步骤 5 输入超时之前等待服务器响应的秒数。
步骤 6 选择相应的身份验证协议。
步骤 7 （可选）点击**添加行 (Add Row)** 添加另一台 RADIUS 服务器。对每个 RADIUS 服务器重复步骤 2 到 6。

注释 最多可以添加十个 DNS 服务器。

步骤 8 选择要为其启用双因素身份验证的所需用户角色。
步骤 9 提交并确认更改。

启用双因素身份验证后，当用户输入用户名和密码后，系统会提示输入密码，以便登录到该设备。

禁用双因素身份验证

准备工作

确保设备已启用双因素身份验证。

步骤 1 在**系统管理 > 用户**页面上，点击“双因素身份验证”下的**编辑全局设置**
步骤 2 取消选择**启用双因素身份验证**。

步骤 3 提交并确认更改。

配置对邮件安全设备的访问

AsyncOS 提供多种管理员控制措施，用于管理用户对邮件安全设备的访问，包括 Web UI 会话的超时，以及一个访问列表（它指定了用户和组织的代理服务器可通过其访问设备的 IP 地址）。

配置基于 IP 的网络访问

可以通过为直接连接到设备的用户以及通过反向代理连接的用户（如果组织为远程用户使用反向代理）创建访问列表，控制用户通过哪些 IP 地址访问邮件安全设备。

直接连接

可以为可连接到邮件安全设备的计算机指定 IP 地址、子网或 CIDR 地址。用户可以从使用访问列表中 IP 地址的任何计算机访问设备。如果用户尝试从列表中未包括的地址连接设备，将被拒绝访问。

通过代理连接

如果组织的网络在远程用户的计算机与邮件安全设备之间使用反向代理服务器，AsyncOS 将允许您创建访问列表，其中包含可连接到设备的代理的 IP 地址。

即使使用反向代理，AsyncOS 仍会对照允许用户连接的 IP 地址列表验证远程用户计算机的 IP 地址。要将远程用户的 IP 地址发送到邮件安全设备，代理需要在其连接设备的请求中包括 x-forwarded-for HTTP 信头。

x-forwarded-for 信头是非 RFC 标准的 HTTP 信头，格式如下：

x-forwarded-for: client-ip, proxy1, proxy2,...CRLF。

此信头的值是逗号分隔值形式的 IP 地址列表，其中最左侧的地址是远程用户计算机的地址，之后是转发连接请求的各个后续代理的地址。（信头名称是可配置的。）邮件安全设备根据访问列表中允许的用户和代理 IP 地址，从信头和连接代理的 IP 地址开始匹配远程用户的 IP 地址。

注释 AsyncOS 仅支持 x-forwarded-for 信头中的 IPv4 地址。

限制网络访问时的重要预防措施

警告！如果满足下列条件之一，在提交和确认网络访问更改后，可能会丧失对设备的访问权限：

- 如果选择**仅允许特定连接**，并且不包括列表中当前计算机（PC、集群环境中的邮件安全设备或安全管理设备等）的 IP 地址。
- 如果选择**仅允许通过代理的特定连接 (Only Allow Specific Connections Through Proxy)**，当前连接到设备的代理的 IP 地址不在代理列表中，并且源 IP 信头的值不在允许的 IP 地址列表中。

- 如果选择**仅允许直接或通过代理的特定连接 (Only Allow Specific Connections Directly or Through Proxy)**，且
  - 源 IP 信头的值不在允许的 IP 地址列表中

    或

  - 源 IP 信头的值不在允许的 IP 地址列表中，且连接到设备的代理的 IP 地址不在允许的代理列表中。

创建访问列表

通过 GUI 或使用 **adminaccessconfig > ipaccess** CLI 命令，可创建网络访问列表。

准备工作

请确保更改网络访问设置不会导致您自己无法登录到设备。请参阅限制网络访问时的重要预防措施，第 741 页。

步骤 1 依次选择**系统管理 (System Administration) > 网络访问 (Network Access)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选择访问列表的控制模式：

选项	说明
允许全部	此模式允许与设备的所有连接。 此模式为默认操作模式。
仅允许特定连接	如果用户的 IP 地址与访问列表中所含的 IP 地址、IP 范围或 CIDR 范围匹配，此模式则允许该用户连接到设备。
仅允许通过代理的特定连接 (Only Allow Specific Connections Through Proxy)	如果满足以下条件，此模式允许用户通过反向代理连接到设备： • 访问列表“代理服务器 (Proxy Server)”字段的 IP 地址中包含连接代理的 IP 地址。 • 代理的连接请求中包含 **x-forwarded-header** HTTP 信头。 • **x-forwarded-header** 的值为空。 • 远程用户的 IP 地址包含在 x-forwarded-header 中，并与访问列表中为用户定义的 IP 地址、IP 范围或 CIDR 范围匹配。
仅允许直接或通过代理的特定连接 (Only Allow Specific Connections Directly or Through Proxy)	如果用户的 IP 地址与访问列表中包含的 IP 地址、IP 范围或 CIDR 范围匹配，则此模式允许用户通过反向代理连接或直接连接到设备。通过代理连接的条件与“仅允许通过代理的特定连接 (Only Allow Specific Connections Through Proxy)”模式相同。

步骤 4 输入允许用户连接的目标设备的 IP 地址。

可以输入 IP 地址、IP 地址范围或 CIDR 范围。使用逗号分隔多个条目。

步骤 5 如果允许通过代理连接，请输入以下信息：

1. 允许连接到设备的代理的 IP 地址。使用逗号分隔多个条目。
2. 代理发送到设备的源 IP 信头的名称，其中包含远程用户计算机和转发请求的代理服务器的 IP 地址。默认情况下，该信头的名称为 x-forwarded-for。

步骤 6 请确保您未配置在提交并落实更改后将会导致您自己无法登录到设备的更改。

步骤 7 提交并确认更改。

配置会话超时

配置 Web UI 会话超时

可以指定用户因不活动而被 AsyncOS 注销前可以登录到邮件安全设备的 Web UI 的时间。此 Web UI 会话超时适用于：

- 所有用户，包括管理员
- HTTP 和 HTTPS 会话
- 思科垃圾邮件隔离区

AsyncOS 注销用户后，设备会将用户的 Web 浏览器重定向到登录页。

步骤 1 依次选择**系统管理 (System Administration) > 网络访问 (Network Access)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 在 **Web UI 不活动超时时间 (Web UI Inactivity Timeout)** 字段中，输入用户可在注销之前保持不活动状态的分钟数。可以定义 5 到 1440 分钟之间的超时期限。

步骤 4 提交并确认更改。

下一步做什么

也可以使用 CLI 中的 adminaccessconfig 命令来配置 Web UI 会话超时。请参阅《适用于思科邮件安全设备的 *AsyncOS CLI* 参考指南》。

配置 CLI 会话超时

可以指定用户因不活动而被 AsyncOS 注销前可以登录邮件安全设备的 CLI 的时间。CLI 会话超时适用于：

- 所有用户，包括管理员
- 仅适用于使用安全外壳 (SSH)、SCP和直接串行连接的连接

注释 在 CLI 会话超时时的所有未提交的配置更改都将丢失。请确保在进行配置更改后立即提交它们。

步骤 1 依次选择**系统管理 (System Administration) > 网络访问 (Network Access)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 在 **CLI 不活动超时时间 (CLI Inactivity Timeout)** 字段中，输入用户可在注销之前保持不活动状态的分钟数。可以定义 5 到 1440 分钟之间的超时期限。

步骤 4 提交并确认更改。

下一步做什么

也可以使用 CLI 中的 adminaccessconfig 命令来配置 CLI 会话超时。请参阅《适用于思科邮件安全设备的 *AsyncOS CLI* 参考指南》。

向管理用户显示消息

在登录前显示消息

可将邮件安全设备配置为在用户尝试通过 SSH、FTP 或 Web UI 登录到该设备前显示一条消息。登录横幅是可自定义的文本，显示在登录提示的上方。可以使用登录横幅显示设备的内部安全信息或最佳实践说明。例如，您可以创建一段简单说明，指出禁止未经授权使用该设备，或者有关组织有权审核用户对该设备所做更改的详细警告。

可以使用 CLI 中的 adminaccessconfig > banner 命令创建登录横幅。登录横幅的最大长度是 2000 个字符，以适合 80x25 的控制台。可从设备上 /data/pub/configuration 目录中的文件导入登录横幅。在创建横幅之后，请确认您的更改。

在登录后显示消息

可将 AsyncOS 配置为在用户通过 SSH、FTP 或 Web UI 成功登录到设备后显示一个欢迎横幅。可以使用欢迎横幅显示设备的内部安全信息或最佳实践说明。

可以使用 CLI 中的 adminaccessconfig > welcome 命令创建欢迎横幅。欢迎横幅的最大长度为 1600 个字符。

可从设备 /data/pub/configuration 目录中的文件导入欢迎横幅。在创建横幅之后，请确认您的更改。

有关详细信息，请参阅适用于思科邮件安全设备的 *AsyncOS* 的 *CLI* 参考指南。

管理安全外壳 (SSH) 密钥

可将 sshconfig 命令用于：

- 向/从系统上已配置的用户帐户（包括 admin 帐户）的 authorized_keys 文件添加/删除安全外壳 (SSH) 公共用户密钥。这将允许使用 SSH 密钥而不是密码质询队用户帐户进行身份验证。
- 编辑以下 SSH 服务器配置设置：
  - 公钥身份验证算法 (Public Key Authentication Algorithms)
  - 加密算法 (Cipher Algorithms)
  - KEX 算法 (KEX Algorithms)
  - MAC 方法 (MAC Methods)
  - 最小服务器密钥大小 (Minimum Server Key Size)。

注释 要配置主机密钥，以便在将日志文件从思科设备 SCP 推送到其他主机时使用，请使用 **logconfig -> hostkeyconfig**。有关详细信息，请参阅日志记录，第 855 页。

使用 **hostkeyconfig**，可以扫描远程主机的密钥，并将它们添加到思科设备。

示例：安装新公钥

在下面的示例中，将为管理员账户安装一个新公钥：

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]> userkey
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new
Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
[-paste public key for user authentication here-]
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]>
```

示例：编辑 SSH 服务器配置

下面的示例显示了如何编辑 SNMP 服务器配置。

```
mail.example.com> sshconfig
Choose the operation you want to perform:
```

```
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]> sshd
ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
        ssh-dss
        ssh-rsa
Cipher Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        arcfour256
        arcfour128
        aes128-cbc
        3des-cbc
        blowfish-cbc
        cast128-cbc
        aes192-cbc
        aes256-cbc
        arcfour
        rijndael-cbc@lysator.liu.se
MAC Methods:
        hmac-md5
        hmac-sha1
        umac-64@openssh.com
        hmac-ripemd160
        hmac-ripemd160@openssh.com
        hmac-sha1-96
        hmac-md5-96
Minimum Server Key Size:
        1024
KEX Algorithms:
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]> setup
Enter the Public Key Authentication Algorithms do you want to use
[rsa1,ssh-dss,ssh-rsa]> rsa1
Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,
cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se]> aes192-ctr
Enter the MAC Methods do you want to use
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
hmac-md5-96]> hmac-sha1
Enter the Minimum Server Key Size do you want to use
[1024]> 2048
Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,
diffie-hellman-group1-sha1]> diffie-hellman-group-exchange-sha1
ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
Cipher Algorithms:
        aes192-ctr
MAC Methods:
        hmac-sha1
Minimum Server Key Size:
        2048
KEX Algorithms:
        diffie-hellman-group-exchange-sha1
```

```
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]>
```

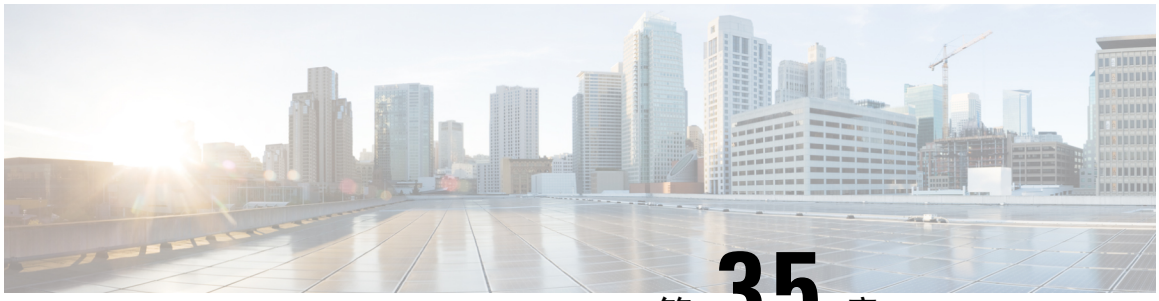
远程 SSH 命令执行

CLI 允许通过远程执行 SSH 命令来运行命令。例如，如果已为思科设备上的“管理员”(admin) 帐户配置 SSH 公钥，则可以从未质询的远程主机运行以下命令：

```
# ssh admin@mail3.example.com status

Enter "status detail" for more information.

Status as of: Mon Jan 20 17:24:15 2003

Last counter reset: Mon Jan 20 17:08:21 2003

System status: online

[rest of command deleted]
```

监控管理用户访问权限

目标	请
查看设备的所有活动用户的会话详细信息	点击页面右上角的**选项 > 活动会话** 在命令行界面中，使用 w、whoami 和 who 命令。
查看最近登录到设备的用户。 还将显示远程主机的 IP 地址，以及登录、注销和总时间。	在命令行界面，使用 last 命令。



第 35 章

系统管理

本章包含以下部分：

注释 本部分介绍的一些功能或命令将会影响路由优先顺序或者会受路由优先顺序的影响。有关详细信息，请参阅附录 *B* “*IP* 地址接口和路由”。

设备管理

以下任务可让您轻松管理设备中的常用功能。

关闭或重新引导设备

在关闭或重新引导设备后，可以稍后重新启动设备，而不会丢失传送队列中的任何邮件。

可以在 CLI 中使用 shutdown 或 reboot 命令，也可以使用 Web 界面：

步骤 1 依次选择**系统管理 (System Administration)** > **关闭/暂停 (Shutdown/Suspend)**。

步骤 2 在**系统操作 (System Operations)** 部分，从**操作 (Operation)** 下拉列表中选择 **关闭 (Shutdown)** 或**重新引导 (Reboot)**。

步骤 3 输入等待的秒数，以允许打开的连接在被强制关闭之前完成。

默认延迟为三十 (30) 秒。

步骤 4 点击**确认 (Commit)**。

暂停邮件接收和传送

AsyncOS 允许您暂停邮件的接收和传送。您可以暂停：

- 接收某特定侦听程序或多个侦听程序上的邮件。
- 传送所有邮件或发送至某特定域或多个域的邮件。

使用 CLI 中的 suspend 命令或使用 Web 界面：

步骤 1 依次选择**系统管理 (System Administration)** > **关闭/暂停 (Shutdown/Suspend)**。

步骤 2 暂停接收某特定侦听程序或多个侦听程序上的邮件。

在**邮件操作 (Mail Operations)** 部分，选择要暂停的功能和/或侦听程序。如果设备有多个侦听程序，可以暂停各个侦听程序上的邮件接收。

步骤 3 暂停传送所有邮件或发送至某特定域或多个域的邮件。根据您的要求，执行以下操作之一：

1. 要暂停所有邮件的传送，请在**指定域/子域 (Specify Domain(s)/Subdomain(s))** 字段中，输入 All，然后按 **Enter**。
2. 要暂停传送至特定域或子域的邮件，请在**指定域/子域 (Specify Domain(s)/Subdomain(s))** 字段中，输入域或子域名称或 IP 地址，然后按 **Enter**。使用逗号分隔文本添加多个条目。

步骤 4 输入等待的秒数，以允许打开的连接在被强制关闭之前完成。

如果没有打开的连接，系统将立即变为离线状态。

默认延迟为 30 秒。

步骤 5 点击**确认 (Commit)**。

下一步做什么

当您准备恢复暂停的服务时，请参阅恢复暂停的邮件的接收和传送，第 751 页。

恢复暂停的邮件的接收和传送

使用“关闭/暂停”页面或 resume 命令恢复暂停的邮件的接收和传送。

步骤 1 依次选择**系统管理 (System Administration)** > **关闭/暂停 (Shutdown/Suspend)**。

步骤 2 在**邮件操作 (Mail Operations)** 部分，选择要恢复的功能和/或侦听程序。

如果设备有多个侦听程序，可以恢复各个侦听程序上的邮件接收。

步骤 3 恢复传送所有邮件或发送至某特定域或多个域的邮件。

在**指定域/子域 (Specify Domain(s)/Subdomain(s))** 字段中，点击目标条目上的关闭图标。

步骤 4 点击**确认 (Commit)**。

重置为出厂默认设置

注意 如果您无法使用串行接口或管理接口上的默认设置通过默认的 Admin 用户帐户重新连接到 Web 界面或 CLI，则请勿重置为出厂默认设置。

物理传输设备时，您可能需要先使用出厂默认设置。重置为出厂设置是极其具有破坏性的，仅当传输装备或最近重新进行了排序以解决配置问题时才重置为出厂设置。重置为出厂默认设置会断开您与 Web 界面或 CLI 的连接，从而禁用您用来连接至设备（FTP、SSH、HTTP、HTTPS）的服务，甚至会删除您已创建的其他用户帐户。您可以通过如下方式重置为出厂默认设置：

- 在 Web 界面上，点击**系统管理 > 配置文件**页上的“重置”按钮，或点击**系统管理 > 系统设置向导**中的“重置配置”按钮。
- 在 CLI 上，使用 **resetconfig** 命令。

注释 仅当设备处于离线状态时，**resetconfig** 命令才有效。重置为出厂设置后，设备将恢复在线状态。

后续步骤

- 运行“系统设置向导”(System Setup Wizard)。有关详细信息，请参阅 使用系统设置向导，第 29 页
- 打开邮件传送以恢复邮件传送。

显示 AsyncOS 的版本信息

要确定设备上当前安装的 AsyncOS 版本，请使用 Web 界面上“监控”菜单上的“系统概述”页面（请参阅系统状态，第 663 页），或使用 CLI 中的 version 命令。

功能密钥

添加和管理功能密钥

对于物理设备，功能密钥既特定于设备的序列号，又特定于要启用的功能（您不能在一个系统上重用另一个系统的密钥）。

要在 CLI 中使用功能密钥，请使用 **featurekey** 命令。

步骤 1 依次选择**系统管理 (System Administration) > 功能密钥 (Feature Keys)**。

步骤 2 执行操作：

目标	请
查看活动功能密钥的状态	查看 **<序列号> 的功能密钥 (Feature Keys for <serial number>)** 部分。
查看已为设备签发但又尚未激活的功能密钥	查看**待处理激活 (Pending Activation)** 部分。 如果您启用了自动下载和激活，则功能密钥不会出现在此列表中。
检查最近签发的功能密钥	单击“待处理激活”(Pending Activation) 部分的**检查新密钥 (Check for New Keys)** 按钮。 如果您尚未启用功能密钥的自动下载和激活，或者需要在下一次自动检查之前下载功能密钥，则此按钮很有用。
激活签发的功能密钥	在**待处理激活 (Pending Activation)** 列表中选择该密钥，并点击**激活选定的密钥 (Activate Selected Keys)**。
添加新功能密钥	使用**功能激活 (Feature Activation)** 部分。

自动执行功能密钥下载和激活

您可以将设备设置为自动检查、下载和激活为此设备签发的功能密钥。

步骤 1 依次选择**系统管理 (System Administration) > 功能密钥设置 (Feature Keys Settings)**。

步骤 2 点击**编辑功能密钥设置 (Edit Feature Key Settings)**。

步骤 3 要查看新功能密钥的检查频率，请点击 (?) 帮助按键。

步骤 4 指定设置。

步骤 5 提交并确认更改。

过期的功能密钥

如果功能密钥将要到期，设备会在密钥到期之前的 90 天、60 天、30 天、15 天、5 天、1 天以及在密钥到期时发出警报。要接收这些警报，请确保您已订用系统警报。有关详细信息，请参阅告警信息，第 777 页。

如果您尝试访问（通过 Web 界面）的功能的功能密钥已过期，请与您的思科代表或支持组织联系。

思科邮件安全虚拟设备许可证

要设置和许可邮件安全虚拟设备，请参阅思科内容安全虚拟设备安装指南。本文档可从中指定的位置获得。

注释 安装虚拟设备许可证之前，无法打开技术支持隧道或运行系统设置向导。

虚拟设备许可证到期

虚拟设备许可证到期之后，设备将会继续传送邮件，但不会获得 180 天的安全服务。在此期间，不会进行安全服务更新。

许可证到期之前的 180 天、150 天、120 天、90 天、60 天、30 天、15 天、5 天、1 天和 0 秒将会发出警报，并且在宽限期结束之前会按照相同的间隔发出警报。这些警报属于“系统”(System)类型，严重性级别为“严重”(Critical)。要确保收到这些警报，请参阅添加警报收件人，第 778 页。

这些警报也会记录在系统日志中。

各个功能密钥可能会先于虚拟设备许可证到期。当这些密钥接近其到期日期时，您也会收到警报。

管理配置文件

设备中的所有配置设置均可通过当个配置文件管理。该文件以XML（可扩展标记语言）格式维护。

可以通过多种方式使用此文件：

- 可以将配置文件保存到其他系统，以备份和保存重要的配置数据。如果在配置设备时出错，可以“回滚”到最近保存的配置文件。
- 可以下载现有的配置文件，快速查看设备的整个配置。（许多新浏览器具有直接显示 XML 文件的功能。）这样，可以帮助您解决当前配置中可能存在的细微错误（例如排字错误）。
- 可以下载现有的配置文件，对其更改，再将其上传到同一设备。这实际上是“绕过”CLI和Web界面更改配置。
- 可以通过 FTP 访问上传整个配置文件，也可以将整个配置文件的一部分直接粘贴到 CLI 中。
- 由于文件是 XML 格式，所以还会提供描述配置文件中所有 XML 实体的相关 DTD（文档类型定义）。可以下载 DTD 先验证 XML 配置文件，再进行上传。（XML 验证工具可随时在互联网上获取。）

使用 XML 配置文件管理多个设备

- 可以从一个设备下载现有的配置文件，对其更改，再将其上传到另一台设备。这样，您可以更轻松地管理多台设备的安装。目前，您尚不能将配置文件从C/X系列设备加载到M系列设备。
- 可以将从一台设备下载的现有配置文件分为多个子部分。可以修改所有设备间通用的部分（在多设备环境中）并在更新子部分时将其加载到其他设备。

例如，可以在测试环境中使用设备来测试“全局取消订阅”(Global Unsubscribe) 命令。如果您认为已经正确配置了“全局取消订阅”(Global Unsubscribe) 列表，则可以将“全局取消订阅”(Global Unsubscribe) 配置部分从测试部分加载到所有生产设备。

管理配置文件

要在您的设备上管理配置文件，请依次点击“系统管理”>“配置文件”。

“配置文件”(Configuration File) 页面包含以下部分：

- **当前配置 (Current Configuration)** - 用于保存和导出当前配置文件。
- **加载配置 (Load Configuration)** - 用于加载完整或部分配置文件。
- **最终用户安全列表/阻止列表数据库(垃圾邮件隔离区)** - 有关信息，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，第 705 页和备份和恢复安全列表/阻止列表，第 710 页。
- **重置配置 (Reset Configuration)** - 用于将当前配置重置回出厂默认设置（应在重置配置之前先保存配置）。

注释 具有加密密码的配置文件以未加密的 PEM 格式随附私钥和证书。

保存和导出当前的配置文件

使用**系统管理** > **配置文件**页面的**当前配置**部分，可以将当前配置保存到您的本地计算机，或是保存到设备上（位于 FTP/SCP 根目录下的 configuration 目录中），也可以通过邮件将其发送至指定的地址。

以下信息不随配置文件一起保存：

- 与 URL 过滤功能使用的服务进行安全通信所用的证书。
- “联系技术支持”(Contact Technical Support) 页面上保存的 CCO 用户 ID 和合同 ID。

可以通过选中**屏蔽配置文件中的密码**复选框来屏蔽用户的密码。屏蔽密码会使初始加密的密码在导出或保存的文件中替换为“*****”。但请注意，无法将包含屏蔽密码的配置文件重新加载到 AsyncOS。

可以通过选中**加密配置文件中的密码**复选框来加密用户的密码。下面列出了将要加密的配置文件中的重要安全参数。

- 证书私钥
- RADIUS 密码
- LDAP 绑定密码
- 本地用户的密码哈希
- SNMP 密码
- DK/DKIM 签名密钥
- 外发 SMTP 身份验证密码
- PostX 加密密钥
- PostX 加密代理密码
- FTP 推送日志订阅的密码
- IPMI LAN 密码
- 更新程序服务器 URL

可以使用 saveconfig 命令在命令行界面中配置此参数。

通过邮件发送配置文件

使用“系统管理”>“配置文件”中的“通过邮件将文件发送至”字段或使用 mailconfig 命令通过邮件将当前配置文件以附件形式发送给用户。

加载配置文件

使用**系统管理 (System Administration) > 配置文件 (Configuration File)** 页面的“加载配置”(Load Configuration) 部分将新配置信息加载到设备中.可以使用 `loadconfig` 命令在命令行界面中配置此参数。

可以使用以下三种方法之一加载信息：

- 将信息放在 `configuration` 目录，然后上传。
- 直接从本地计算机上传配置文件。
- 直接粘贴配置信息。

注释 无法加载包含屏蔽密码的配置文件。

在集群模式下，可以选择加载集群或设备的配置。有关加载集群配置的说明，请参阅在集群设备中加载配置，第 928 页。

无论使用哪种方法，在配置顶部必须包括以下标记：

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

... your configuration information in valid XML

</config>
```

结束的 `</config>` 标记应跟随配置信息。对照设备上 `configuration` 目录中的 DTD（文档类型定义）解析和验证 XML 语法中的值。DTD 文件名为 `config.dtd`。如果使用 `loadconfig` 命令时命令行报告验证错误，则未加载更改。可以下载 DTD 先在设备之外验证配置文件，再上传它们。

使用任何导入方法，均可导入整个配置文件（最高级别标记之间定义的信息：`<config></config>`）或配置文件的完整和唯一子部分，只要其中包含声明标记（如上），并括在 `<config></config>` 标记中即可。

“完整”表示 DTD 定义的特定小节的完整开始和结束标记都包括在内。例如，上传或粘贴如下内容：

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

<autosupport_enabled>0</autosu

</config>
```

将会在上传时引发验证错误。但使用如下内容：

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

<autosupport_enabled>0</autosupport_enabled>

</config>
```

则不会出现此问题。

“唯一”表示要上传或粘贴的配置文件的子部分对于该配置非常明确。例如，系统可能只有一个主机名，所以允许上传以下代码（包括声明和 <config></config> 标记）：

```
<hostname>mail4.example.com</hostname>
```

。但是，系统可能定义了多个侦听程序，并为每个侦听程序定义了不同的收件人访问表，所以仅上传以下代码：

```
<rat>
       <rat_entry>
              <rat_address>ALL</rat_address>
         <access>RELAY</access>
     </rat_entry>
</rat>
```

会被视为不明确，所以不允许上传，即使是“完整”语法亦不例外。

注意 上传或粘贴配置文件或配置文件的子部分时，可能会清除待处理的未确认更改。

如果配置文件分配的磁盘空间量小于设备上当前存储的数据量，则时间最长的数据将被删除，以满足配置文件中指定的配额。

空标记与忽略的标记

上传或粘贴一部分配置文件时，请务必小心。如果不带标记，在加载配置文件时则不会修改其在配置中的值。但是，如果包括空标记，则其配置将被清除。

例如，上传如下内容：

```
<listeners></listeners>
```

将会从系统中移除所有侦听程序！

注意 上传或粘贴配置文件的子部分时，可能会从 Web 界面或 CLI 断开自己并损坏大量配置数据。如果无法使用其他协议、串行接口或管理端口上的默认设置重新连接到设备，请勿使用此命令禁用服务。此外，如果不确定 DTD 定义的确切配置语法，请勿使用此命令。务必先备份配置数据，再加载新的配置文件。

关于加载日志订用密码的注意事项

如果尝试加载的配置文件包含需要密码的日志订用（例如，将使用FTP推送的日志订用），loadconfig 命令不会警告您缺少密码。FTP 推送失败，系统将生成警报，直到使用 logconfig 命令配置正确的密码。

关于字符集编码的注意事项

XML 配置文件的“编码”属性必须是“ISO-8859-1”，无论您使用哪种字符集离线操作文件。请注意，只要发出 showconfig、saveconfig 或 mailconfig 命令，都需要在文件中指定编码属性：

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

目前，只能加载此编码的配置文件。

重置当前的配置

重置当前配置会使您的设备恢复到原始出厂默认设置。在重置之前，请保存您的配置。集群环境中不支持通过 GUI 中的词按钮重置配置。

请参阅重置为出厂默认设置，第 751 页。

查看配置文件

您只能使用 showconfig 命令查看配置文件详细信息。showconfig 命令可将当前配置打印到屏幕。

```
mail3.example.com> showconfig


Do you want to include passphrases? Please be aware that a configuration without
passphrases will fail when reloaded with loadconfig.
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
Product: IronPort model number Messaging Gateway Appliance(tm)
Model Number: model number
Version: version of AsyncOS installed
Serial Number: serial number

Current Time: current time and date

[The remainder of the configuration file is printed to the screen.]
```

“配置文件”(Configuration File) 页

管理磁盘空间

（仅限虚拟设备）增加可用磁盘空间

对于运行 ESXi 5.5 和 VMFS 5 的虚拟设备，最多可以分配 2 TB 磁盘空间。对于运行 ESXi 5.1 的设备，限制为 2 TB。

要向虚拟设备实例添加磁盘空间，请执行以下操作：

注释 不支持减少磁盘空间。请参阅 VMWare 文档中的相关信息。

准备工作

仔细确定所需的磁盘空间增加。

步骤 1 减少邮件安全设备实例。

步骤 2 使用 VMWare 提供的实用程序或管理工具增加磁盘空间。

有关更改虚拟磁盘配置的信息，请参阅 VMWare 文档。发布时，可在以下位置获取 ESXi 5.5 的此信息：http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html。

步骤 3 依次转至**系统管理 (System Administration) > 磁盘管理 (Disk Management)**，并确认所做的更改是否已生效。

查看和分配磁盘空间使用情况

您可以通过在设备上您的部署所用的功能之间分配磁盘空间来优化磁盘的使用。

目标	请
• 查看磁盘空间配额和每项服务的当前使用情况 • 您可以随时重新分配设备上的磁盘空间	依次转至**系统管理 (System Administration) > 磁盘管理 (Disk Management)**。
管理数据卷	• 为了报告和跟踪服务和垃圾邮件隔离区，最早的数据将自动删除。 • 对于“策略”(Policy)、“病毒”(Virus) 和“爆发”(Outbreak) 隔离区，将执行在隔离区中配置的默认操作。请参阅自动处理的隔离邮件的默认操作，第 688 页。 • 对于“其他”(Miscellaneous) 配额，必须手动删除数据以将使用量将至您设置的新配额以下。请参阅管理“其他”配额的磁盘空间，第 759 页。

管理“其他”配额的磁盘空间

“其他 (Miscellaneous)”配额包括系统数据和用户数据。无法删除系统数据。您可以管理以下文件类型的用户数据：

管理	请
日志文件	依次转至**系统管理 (System Administration) > 日志订用 (Log Subscriptions)**，并且： • 查看哪些日志目录使用的磁盘空间最多。 • 确认是否需要将生成的所有日志订用。 • 确认日志级别的详细程度是否超出必要。 • 如果可行，降低回滚文件的大小。
数据包捕获	依次转至**帮助和支持 (Help and Support)**（屏幕右上侧附近）> **数据包捕获 (Packet Capture)**。
配置文件 （这些文件不太可能占用太多磁盘空间。）	通过 FTP 转至设备的 /data/pub 目录。 要配置通过 FTP 访问设备，请参阅 FTP、SSH 和 SCP 访问，第 979 页
配额大小	依次转至**系统管理 (System Administration) > 磁盘管理 (Disk Management)**。

确保收到有关磁盘空间的警报

当“其他”(Miscellaneous) 磁盘使用量达到配额的 75% 时，将开始接收警告级别的系统警报。在收到这些警报时，您应采取措施。

要确保收到这些警报，请参阅告警信息，第 777 页。

磁盘空间和集中管理

磁盘空间管理只能在计算机模式下进行，不能在组或集群模式下进行。

托管安全服务

“服务概述”页面列出以下引擎的当前服务和规则版本：

- Graymail
- McAfee
- Sophos

您可以在“服务概述”页面执行以下任务：

- 手动更新引擎。有关详细信息，请参阅 手动更新引擎，第 761 页
- 回滚到引擎的上一版本。有关详细信息，请参阅 回滚到以前版本的引擎，第 761 页

自动更新列显示特定引擎的自动更新的状态。如果要启用或禁用自动更新，请转到特定引擎的**全局设置**页面。

当为特定服务引擎禁用自动更新时，您将定期收到警报。如果要更改警报间隔，请使用“安全服务”>“服务更新”页面中的**禁用的自动引擎更新的警报间隔**选项。

注释 对于应用了回滚的引擎，自动更新将被禁用。

手动更新引擎

步骤 1 转到**安全服务** > **服务概述**页面。

步骤 2 点击**可用更新**列中的**更新**，以获取服务引擎的最新服务或规则版本。

注释 只有存在特定引擎的新更新时，**更新**选项才可用。

回滚到以前版本的引擎

步骤 1 转到**安全服务** > **服务概述**页。

步骤 2 点击**修改版本**列中的**更改**。

步骤 3 选择更新所需的规则和服务版本，然后点击**应用**。

设备会将引擎回滚到上一个版本。

注释 服务更新以包的形式包含服务版本和规则版本。

点击**应用**后，将自动禁用特定引擎的自动更新。要启用自动更新，请转到特定引擎的“全局设置”页面。

查看日志

有关引擎回滚和禁用自动更新的信息将发布到以下日志：

- **更新程序日志**：包含关于引擎回滚和自动更新引擎的信息。大多数信息处于信息或调试级别。

  有关详细信息，请参阅更新程序日志示例，第 893 页。

服务更新

以下服务需要更新以获得最高效率：

- 功能密钥
- McAfeee 防病毒定义
- PXE 引擎
- Sophos 防病毒定义
- IronPort 反垃圾邮件规则
- 爆发过滤器规则
- 时区规则
- URL 类别（用于 URL 过滤功能。有关详细信息，请参阅将来的 URL 类别集变更，第 351 页）
- 注册客户端（用于更新与用于URL过滤功能的基于云的服务进行通信所需的证书。有关信息，请参阅关于与思科网络安全服务的连接，第 329 页。）
- Graymail 规则

注释 DLP 引擎和内容匹配分类器的设置在**安全服务 > 防数据丢失**页面上处理。有关详细信息，请参阅关于更新 DLP 引擎和内容匹配分类器，第 395 页。

服务更新设置用于接收更新（（DLP 更新除外）的所有服务。不能为任何单个服务（DLP 更新除外）指定特有的设置。

要设置网络和设备以获取这些重要更新，请参阅设置以获取升级和更新，第 762 页。

设置以获取升级和更新

分配升级和更新的选项

将 AsyncOS 升级和更新文件分配至您的设备的方式有如下几种：

- 每台设备都可直接从思科更新服务器下载文件。此为默认方法。
- 您可以从思科下载一次文件，然后从网络中的服务器将其分配到设备。请参阅从本地服务器升级和更新，第 763 页。

要选择和配置某种方法，请参阅配置服务器设置以下载升级和更新，第 765 页。

将您的网络配置为从思科服务器下载升级和更新

设备直接连接到思科更新服务器，以查找并下载升级和更新：

图 *72*: 数据流更新方法

思科更新服务器使用动态 IP 地址。如果您有很强的防火墙策略，可能需要改为配置静态位置。有关详细信息，请参阅配置设备以在严格的防火墙环境中获取升级和更新，第 763 页。

创建一个防火墙规则以允许从端口 80 和 443 的思科更新服务器下载升级。

配置设备以在严格的防火墙环境中获取升级和更新

思科 IronPort 升级和更新服务器使用动态 IP 地址。如果您有很强的防火墙策略，可能需要为更新和 AsyncOS 升级配置静态位置。

步骤 1 请与思科客户支持联系，获取静态 URL 地址。

步骤 2 创建一个防火墙规则以允许从端口 80 的静态 IP 地址下载升级和更新。

步骤 3 依次选择**安全服务 (Security Services) > 服务更新 (Service Updates)**。

步骤 4 点击**编辑更新设置**。

步骤 5 在“编辑更新设置”页面的“更新服务器(映像)”部分，选择“本地更新服务器”并在“基本 URL”字段中输入在第 1 步中收到的静态 URL，以获取 AsyncOS 升级和 McAfee 防病毒定义。

步骤 6 确认已为“更新服务器(列表)”(Update Servers (list)) 部分选中“IronPort 更新服务器”(IronPort Update Servers)。

步骤 7 提交并确认更改。

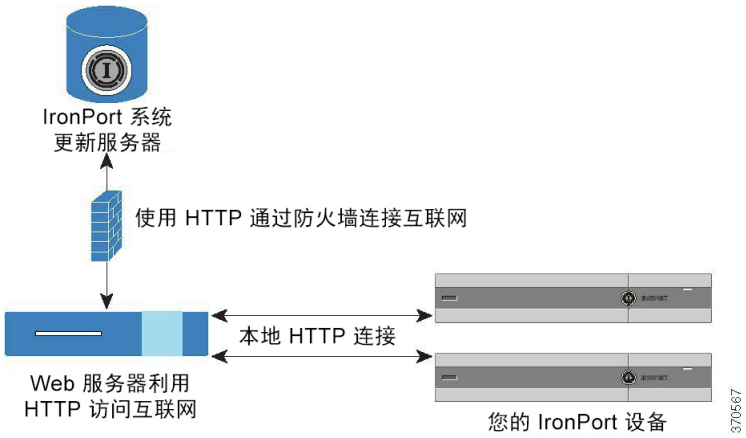
从本地服务器升级和更新

可以将 AsyncOS 升级映像下载到本地服务器并从您自己的网络内托管升级，无需直接从思科的更新服务器获得升级。使用此功能，升级映像将通过 HTTP 下载到网络中有权访问互联网的任何服务器。如果选择下载升级映像，即可配置内部 HTTP 服务器（“更新管理器”）将 AsyncOS 映像托管到您的设备。

如果您的设备无权访问互联网，或是贵组织限制访问来镜像用于下载的站点，请使用本地服务器。将 AsyncOS 升级从本地服务器下载至每台设备通常比从 Cisco IronPort 服务器下载速度要快。

注释 思科建议仅将本地服务器用于 AsyncOS 升级。如果为安全更新映像使用本地更新服务器，则本地服务器不会从 Cisco IronPort 自动接收安全更新，因此，您网络内的设备无法始终拥有最新的安全服务。

图 *73:* 远程更新方法



步骤 1 配置本地服务器，以检索和提供升级文件。

步骤 2 下载升级文件。

步骤 3 在 GUI 中使用**安全服务 > 服务更新**页或在 CLI 中使用 **updateconfig** 命令将设备配置为使用本地服务器。

步骤 4 使用**系统管理 > 系统升级**页面或在 CLI 中使用 upgrade 命令升级设备。

从本地服务器升级和更新的硬件和软件要求

要下载 AsyncOS 升级和更新文件，您的内部网络中必须有系统可满足以下条件：

- 对系统更新服务器的互联网访问权限。
- Web 浏览器（请参阅浏览器要求，第 13 页）。

注释 对于此版本，如果您需要配置防火墙设置以允许通过 HTTP 访问此地址，则必须使用 DNS 名称而不是特定 IP 地址对其进行配置。

要托管 AsyncOS 更新文件，您的内部网络中必须有服务器可满足以下条件：

- Web 服务器（例如 Microsoft IIS (Internet Information Services) 或 Apache 开源服务器），该服务器应：
  - 支持目录或文件名显示超出 24 个字符
  - 已启用目录浏览
  - 配置为匿名（无身份验证）或基本（“简单”）身份验证
  - 至少包含 350MB 可用磁盘空间，用于每个 AsyncOS 更新映像

在本地服务器上托管升级映像

在设置本地服务器后，转至 http://updates.ironport.com/fetch_manifest.html 以下载升级映像的压缩文件。要下载映像，请输入您的序列号（对于物理设备）或 VLN（对于虚拟设备）以及设备的版本号。然后，系统将显示您可用的升级列表。点击要下载的升级版本，在本地服务器上解压根目录中的 ZIP 文件，但目录结构应保持完整。要使用升级映像，请在“编辑更新设置”页面中（或在 CLI 中使用 updateconfig）将设备配置为使用本地服务器。

本地服务器还会托管 XML 文件，用于将网络中设备的可用 AsyncOS 升级限制为下载的升级映像。此文件称为“证明”。证明文件位于升级映像 ZIP 文件的 asyncos 目录内。解压了本地服务器根目录中的 ZIP 文件后，在“编辑更新设置”页面中（或在 CLI 中使用 updateconfig）输入 XML 的完整 URL，包括文件名。

有关远程升级的详细信息，请参阅知识库或联系思科支持提供商。

通过代理服务器进行更新

默认情况下，设备配置为直接连接到思科更新服务器接收更新。此连接通过 HTTP 在端口 80 上进行，并且内容已加密。如果不希望在防火墙中打开此端口，可以定义代理服务器以及设备可以从其接收更新的规则的特定端口。

如果选择使用代理服务器，可以指定一个可选的身份验证和端口。

注释 如果定义了代理服务器，该代理服务器将自动用于配置为使用代理服务器的所有服务更新。无法为任何单个服务的更新关闭代理服务器。

配置服务器设置以下载升级和更新

指定将升级和更新下载至设备所需的服务器和连接信息。

可以为 AsyncOS 升级和服务更新使用相同或不同的设置。

准备工作

确定设备将直接从思科下载升级和更新，还是在网络的本地服务器中托管这些映像。然后，设置您的网络以支持所选的方式。查看设置以获取升级和更新，第 762 页下的所有主题。

步骤 1 依次选择**安全服务 (Security Services) > 服务更新 (Service Updates)**。

步骤 2 点击**编辑更新设置 (Edit Update Settings)**。

步骤 3 输入选项：

设置	说明
更新服务器（映像）	选择要从 Cisco IronPort 更新服务器还是从网络的本地服务器下载 Cisco IronPort AsyncOS 升级映像和服务更新。默认设置为使用 Cisco IronPort 更新服务器下载升级和更新。 为为升级和更新使用相同设置，请在可见字段中输入信息。 如果选择本地更新服务器，请输入用于下载升级和更新的服务器的基本 URL 和端口号。如果服务器需身份验证，则也可以输入有效用户名和密码。 要单独为 AsyncOS 升级和 McAfee 防病毒定义输入单独的设置，请点击**点击以为 AsyncOS 使用不同设置 (Click to use different settings for AsyncOS)** 链接。 **注释** 智能多重扫描需要另一台本地服务器来为第三方反垃圾邮件规则下载更新。
更新服务器（列表）	为确保只有适合您的部署的升级和更新才可为每台设备所用，Cisco IronPort 会生成相关文件的证明列表。 选择从 Cisco IronPort 更新服务器还是本地网络服务器下载可用的升级和服务更新列表（证明 XML 文件）。 系统提供了独立的部分来为更新和 AsyncOS 升级指定服务器。升级和更新都默认选择从 Cisco IronPort 更新服务器下载。 如果选择本地更新服务器，请输入指向每个列表的证明 XML 文件的完整路径，包括文件名和服务器的 HTTP 端口号。如果将端口字段留空，AsyncOS 将使用端口 80。如果服务器需要身份验证，请输入有效的用户名和密码。
自动更新	为 Sophos 和 McAfee 防病毒定义、思科反垃圾邮件规则、思科智能多重扫描规则、PXE 引擎更新、病毒爆发过滤器规则和时区规则启用自动更新和升级间隔（设备检查更新的频率）。 包括后缀 s、m 或 h，以表示秒、分钟或小时。输入 0（零）将禁用自动更新。 **注释** 只能使用**安全服务 > 防数据丢失**页面为 DLP 启用自动更新。但首先必须先为所有服务启用自动更新。有关详细信息，请参阅关于更新 DLP 引擎和内容匹配分类器，第 395 页。
禁用的自动引擎更新的警报间隔	在针对特定引擎禁用“自动更新”功能时，输入要发送警报的特定频率。 包括后缀 m、h 或 d，表示月份、小时或天。默认值为 30 天。
接口	选择联系列出的安全组件更新的更新服务器时所用的网络接口。将显示可用的代理数据接口。默认情况下，设备选择一个接口使用。
HTTP 代理服务器	用于 GUI 中列出的服务的可选代理服务器。 如果指定代理服务器，则使用它来更新所有服务。
HTTPS 代理服务器	使用 HTTPS 的可选代理服务器。如果定义了 HTTPS 代理服务器，将使用它来更新 GUI 中列出的服务。

步骤 4 提交并确认更改。

配置自动更新

步骤 1 依次导航至**安全服务 (Security Services) > 服务更新 (Service Updates)** 页面，然后点击**编辑更新设置 (Edit Update Settings)**。

步骤 2 选中该复选框以启用自动更新。

步骤 3 输入更新间隔（两次更新之间的等待时间）。为分钟添加后缀 **m**，为小时添加后缀 **h**。最大更新间隔为 1 小时。

配置设备以验证更新程序服务器证书的有效性

每当设备与更新程序服务器进行通信时，邮件安全设备均可检查思科更新程序服务器证书的有效性。如果配置了此选项并且验证失败，则不会下载更新，并在更新程序日志中记录详细信息。

使用 updateconfig 命令配置此选项。以下示例显示了如何配置此选项。

```
mail.example.com> updateconfig
Service (images):                                   Update URL:
-------------------------------------------------------------------------------------------
Feature Key updates                                 http://downloads.ironport.com/asyncos
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> validate_certificates
Should server certificates from Cisco update servers be validated?
[Yes]>
Service (images):                                   Update URL:
-------------------------------------------------------------------------------------------
Feature Key updates                                 http://downloads.ironport.com/asyncos
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates          Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------------------
```

```
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>
```

将设备配置为信任代理服务器通信

如果使用非透明代理服务器，则可以添加 CA 证书用于为设备的代理证书签名。这样，设备将会信任代理服务器通信。

使用 updateconfig 命令配置此选项。以下示例显示了如何配置此选项。

```
mail.example.com> updateconfig
...
...
...
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> trusted_certificates
Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
[]> add
Paste certificates to be trusted for secure updater connections, blank to quit
Trusted Certificate for Updater:
Paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MMIICiDCCAfGgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhMCSU4x
DDAKBgNVBAgTA0tBUjENM.........................................
-----END CERTIFICATE-----
.
Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
- LIST - List trusted certificates for updates.
- DELETE - Delete a trusted certificate for updates.
[]>
```

升级 AsyncOS

过程

	命令或操作	目的
步骤 1	如果尚未执行此操作，请配置适用于所有更新和升级下载的设置，并构建网络以支持和（可选）分发这些下载。	设置以获取升级和更新，第 762 页

	命令或操作	目的
步骤 2	了解升级何时可用并确定是否安装。	可用升级通知，第 769 页
步骤 3	每次升级之前都请执行必要以及建议的任务。	升级 AsyncOS 的准备工作，第 770 页 升级集群中的计算机，第 918 页
步骤 4	执行升级。	下载和安装升级，第 770 页

关于升级集群系统

如果您要升级集群计算机，请参阅升级集群中的计算机，第 918 页。

有关升级过程的批量命令

《思科邮件安全设备 *AsyncOS CLI* 参考指南》中记录了升级操作程序的批处理命令，该指南位于以下网址：http://www.cisco.com/en/US/products/ps10154/prod_command_reference_list.html。

可用升级通知

默认情况下，当设备有 AsyncOS 升级时，具有管理员和技术人员权限的用户将在 Web 界面顶部看到通知。

在集群化的计算机上，操作仅适用于您登录的计算机。

目标	请
查看有关最新升级的详细信息	将鼠标悬停在升级通知上方。
查看所有可用升级的列表	点击通知中的向下箭头。
关闭当前的通知。 有新升级之前，设备不会显示其他通知。	点击向下箭头，然后选择**清除通知 (Clear the notification)**，再点击**关闭 (Close)**。
防止将来通知（仅限有管理员权限的用户。）	转至**管理设备 (Management Appliance) > 系统管理 (System Administration) > 系统升级 (System Upgrade)**。

可用升级通知

默认情况下，当设备有 AsyncOS 升级时，具有管理员和技术人员权限的用户将在 Web 界面顶部看到通知。

在集群化的计算机上，操作仅适用于您登录的计算机。

目标	请
查看有关最新升级的详细信息	将鼠标悬停在升级通知上方。
查看所有可用升级的列表	点击通知中的向下箭头。
关闭当前的通知。 有新升级之前，设备不会显示其他通知。	点击向下箭头，然后选择**清除通知 (Clear the notification)**，再点击**关闭 (Close)**。
防止将来通知（仅限有管理员权限的用户。）	转至**管理设备 (Management Appliance) > 系统管理 (System Administration) > 系统升级 (System Upgrade)**。

升级 AsyncOS 的准备工作

作为一种最佳实践，思科建议按照如下步骤做好升级准备工作。

步骤 1 机下保存 XML 配置文件。如果出于任何原因需要恢复到升级之前的版本，将需要此文件。

步骤 2 如果要使用“安全列表/阻止列表”(Safelist/Blocklist) 功能，请机下导出该列表。

步骤 3 暂停所有侦听程序。如果从 CLI 执行升级，请使用 suspendlistener 命令。如果从 GUI 执行升级，则会自动暂停监听程序。

步骤 4 等待队列清空。可以使用 workqueue 命令查看工作队列中的邮件数，或使用 CLI 中的 rate 命令监控设备上的邮件吞吐量。

注释 升级后重新启用侦听程序。

下载和安装升级

您可以通过单一操作下载并安装，或者在后台下载，稍后再进行安装。

注释 在一次操作中从本地服务器（而不是思科 IronPort 服务器）下载并升级 AsyncOS 时，升级将在下载时即时安装。升级开始时，标语将显示 10 秒。显示此标语时，您可以选择按 Ctrl - C 在下载开始前退出升级过程。

准备工作

- 选择是直接从思科下载升级，还是在网络的服务器中托管升级映像。然后，设置您的网络以支持所选的方式。然后，将设备配置为从您所选的来源获取升级。请参阅设置以获取升级和更新，第 762 页 和 配置服务器设置以下载升级和更新，第 765 页。
- 如果要立即安装升级，请遵循升级 AsyncOS 的准备工作，第 770 页中的说明操作。
- 如果要在集群化系统中安装升级，请参阅升级集群中的计算机，第 918 页。

- 如果只下载升级，则在准备好要安装之前无前提条件。

步骤 1 依次选择**系统管理 (System Administration) > 系统升级 (System Upgrade)**。

步骤 2 点击**升级选项 (Upgrade Options)**。

系统将分析“状态日志”(Status Logs) 中的历史数据（最多三个月），以确定设备的运行状况并就是否可以升级设备提出建议。

注释 对于要执行此分析的系统“状态日志”(Status Logs) 必须包含至少一个月的记录数据。

步骤 3 根据分析结果，执行以下操作之一：

- 如果分析检测到系统在最近几个月内出现以下问题之一，请按照显示的建议操作。
  - 资源节约模式
  - 邮件处理延迟
  - 高 CPU 使用
  - 高内存使用
  - 高内存页面交换
- 如果系统无法执行分析（由于“状态日志”(Status Logs) 中的数据不足），则不提供建议。在这种情形下，仅当设备最近未出现任何问题时再考虑升级设备。
- 如果分析未检测到任何问题，请转至第 4 步。

步骤 4 选择一个选项：

目标	请
在一次操作中下载并安装升级	点击**下载并安装 (Download and Install)**。 如果您已下载安装程序，系统将提示您会覆盖现有的下载。
下载升级安装程序	点击**仅下载 (Download only)**。 如果您已下载安装程序，系统将提示您会覆盖现有的下载。 安装程序在后台下载，而不会中断服务。
安装已下载的升级安装程序	点击**安装**。 只有下载安装程序后，才会显示此选项。 “安装 (Install)”选项下方将标注要安装的 AsyncOS 版本。

步骤 5 除非安装的是先前下载的安装程序，否则请从可用升级列表中选择一个 AsyncOS 版本。

步骤 6 如果要安装：

a) 选择是否将当前配置保存到设备上的 configuration 目录。

b) 选择是否屏蔽配置文件中的密码。

注释 无法使用 GUI 中的“配置文件”页面面或 CLI 中的 loadconfig 命令加载带屏蔽密码的配置文件。

c) 如果要将通过邮件发送配置文件的副本，请输入要将该文件发送到的邮件地址。使用逗号分隔多个邮件地址。

步骤 7 点击**继续**。

步骤 8 如果要安装：

a) 请准备好在这个过程中响应提示。

流程暂停，直到您做出响应。

进度条显示在页面顶部附近。

b) 在提示符下，点击**立即重启 (Reboot Now)**。

c) 大约 10 分钟后，请再次访问设备并登录。

如果认为需要循环设置设备电源，以解决升级问题，则请在您重启后经过至少 20 分钟再执行此操作。

下一步做什么

- 如果流程中断，必须重新开始该流程。
- 如果已下载但未安装升级：

  在准备安装升级时，请从开始按照这些说明执行操作，包括“准备工作 (Before You Begin)”部分的必备条件，但请选择“安装 (Install)”选项。

- 如果已安装升级：
  - 重新启用（恢复）侦听程序。
  - 为新系统保存配置文件。有关信息，请参阅管理配置文件，第 754 页。
- 升级完成后，请重新启用侦听程序。

查看后台下载状态、取消或删除后台下载

步骤 1 依次选择**系统管理 (System Administration) > 系统升级 (System Upgrade)**。

步骤 2 点击**升级选项 (Upgrade Options)**。

步骤 3 选择一个选项：

目标	请
查看下载状态	在页面中间查找。 如果没有正在进行的下载，且无完成的下载等待安装，则不会看到下载状态信息。
取消下载	点击页面中间的**取消下载 (Cancel Download)** 按钮。 只有正在进行下载时，才会显示此选项。

目标	请
删除已下载的安装程序	点击页面中间的**删除文件 (Delete File)** 按钮。 只有下载安装程序后，才会显示此选项。

步骤 4 （可选）查看升级日志。

启用远程电源循环

只有在 80 - 和 90 - 系列硬件上，才能远程重置设备机箱的电源。

如果您希望能够远程重置设备电源，必须事先按照本节所述的过程启用和配置此功能。

准备工作

- 使用线缆将专用的远程电源循环 (RPC) 端口直接连接到安全网络。有关信息，请参阅《硬件安装指南》。
- 确保设备可以远程访问；例如，通过防火墙打开任何必要的端口。
- 此功能需要专用的远程电源循环接口使用唯一的 IPv4 地址。此接口仅可按照本节所述的过程配置，而不能使用 **ipconfig** 命令配置。
- 要循环设置设备电源，需要使用可管理设备（这些设备支持智能平台管理接口 (IPMI) 版本 2.0）的第三方工具。确保您已准备好使用这些工具。
- 有关访问命令行界面的详细信息，请参阅 CLI 参考指南。

步骤 1 使用 SSH 或串行控制台端口访问命令行界面。

步骤 2 使用具有“管理员 (Administrator)”访问权限的帐户登录。

步骤 3 输入以下命令：

```
remotepower
setup
```

步骤 4 按照提示指定以下信息：

1. 此功能的专用 IP 地址，以及网络掩码和网关。
2. 执行电源循环命令所需的用户名和密码。

   这些凭证与用来访问设备的其他凭证不同。

步骤 5 输入 commit 保存更改。

步骤 6 测试您的配置，以确定是否可以远程管理设备电源。

步骤 7 确保您输入的凭证可供您无限期使用。例如，将此信息存储在安全位置，并确保可能需要执行此任务的管理员可访问所需的凭证。

恢复到之前版本的 AsyncOS

AsyncOS 提供将 AsyncOS 操作系统恢复到供应急之用的之前的合格内部版本。

恢复的影响

在设备上使用 revert 命令是一项极具破坏性的操作。此命令会销毁所有配置日志和数据库。仅会保留管理接口上的网络信息保留，其余网络配置都将删除。此外，在重新配置设备之前，恢复操作还会中断邮件处理。由于此命令会破坏网络配置，因此在您希望发出 revert 命令时，可能需要对设备进行物理本地访问。

注意 您必须具有想要恢复到的版本的配置文件。配置文件不向后兼容。

在虚拟设备上恢复 AsyncOS 可能会影响许可证

如果从适用于邮件的 AsyncOS 9.0 恢复到适用于邮件的 AsyncOS 8.5，则许可证不更改。

如果从适用于邮件的 AsyncOS 9.0 恢复到适用于邮件的 AsyncOS 8.0，则不会再有设备不使用安全功能传送邮件的 180 天宽限期。

功能密钥到期日期在任何情况下都不会更改。

恢复 AsyncOS

步骤 1 确保您拥有想要恢复到的版本的配置文件。配置文件不向后兼容。为此，可以通过邮件将该文件发送给自己或通过 FTP 发送文件。有关信息，请参阅通过邮件发送配置文件，第 755 页。

步骤 2 在其他计算机上保存设备当前配置的备份副本（不屏蔽密码）。

注释 这不是您在恢复后要加载的配置文件。

步骤 3 如果使用“安全列表/阻止列表 (Safelist/Blocklist)”功能，请将“安全列表/阻止列表 (Safelist/Blocklist)”数据库导出到其他计算机。

步骤 4 等待邮件队列清空。

步骤 5 登录到您要恢复的设备的 CLI。

在运行 revert 命令时，系统将发出许多警告提示。接受这些警告提示之后，将会立即执行恢复操作。因此，在完成恢复前的步骤之前，请勿开始恢复过程。

步骤 6 从 CLI 中发出 **`revert`** 命令。

注释 恢复过程非常耗时。可能需要 15-20 分钟才会完成恢复，并可重新通过控制台访问设备。

步骤 7 等待设备重启两次。

步骤 8 计算机重启两次之后，请使用串行控制台并使用 **interfaceconfig** 命令配置具有可访问 IP 地址的接口。

步骤 9 在配置的某个接口上启用 FTP 或 HTTP。

步骤 10 以 FTP 传送您创建的 XML 配置文件，或将其粘贴到 GUI 界面。

步骤 11 加载您要恢复到的版本的 XML 配置文件。

步骤 12 如果使用“安全列表/阻止列表 (Safelist/Blocklist)”功能，请导入并恢复“安全列表/阻止列表 (Safelist/Blocklist)”数据库。

步骤 13 确认您的更改。

现在，应使用所选的 AsyncOS 版本运行恢复的设备。

为设备生成的邮件配置返回地址

在以下情况下，可以为 AsyncOS 生成的邮件配置信封发件人：

- 反病毒通知
- 退回
- DMARC 反馈
- 通知（notify() 和 notify-copy() 过滤器操作）
- 隔离去通知（以及隔离区管理中的“发送副本”(Send Copy)
- 报告
- 其他所有邮件。

您可以指定返回地址的显示名称、用户名和域名。还可以选择对于域名使用“虚拟网关 (Virtual Gateway)”域。

可以在 GUI 中或是在 CLI 中使用 addressconfig 命令修改系统生成的邮件的返回地址.

步骤 1 依次导航至“系统管理”(System Administration) >“返回地址”(Return Addresses) 页面。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 对您要修改的一个或多个地址进行更改

步骤 4 提交并确认更改。

为系统运行状况参数配置阈值

根据贵组织的要求，您可以为设备的各个运行状况参数（例如CPU使用、队列中的最大邮件数，等等）配置阈值。您还可以将设备配置为在达到指定的阈值时发送警报。

注释 要使用 CLI 为系统运行状况参数配置阈值，请使用 healthconfig 命令。有关详细信息，请参阅 CLI 内联帮助或《适用于思科邮件安全设备的 *AsyncOS CLI* 参考指南》。

准备工作

请仔细确定阈值。

步骤 1 依次点击**系统管理 (System Administration)** > **系统运行状况 (System Health)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 配置以下选项：

- 为 CPU 使用指定阈值级别（以百分比形式）。

  此外，还要指定在当前的 CPU 使用达到配置的阈值时是否要接收警报。发送第一个警报之后，如果 CPU 使用在 15 分钟内达到了自 5% 触发第一个警报起的运行平均值，则会再发送一个警报。

  注释 这些警报的触发条件只有邮件处理过程中的 CPU 使用情况。

- 为内存页面交换指定阈值级别（以页面数形式）。

  此外，还要指定在交换的页面数达到配置的阈值时是否要接收警报。发送第一个警报之后，如果内存页面交换在 15 分钟内达到了由 150% 触发第一个警报的值，则会再发送一个警报。例如，如果阈值设置为 5000，

  - 当内存页面交换达到 5002 时，发送第一个警报。
  - 当内存页面交换在 15 分钟内达到 7510 时，则会再发送一个警报。

- 为队列中邮件的最大数指定阈值级别（以邮件数形式）。

  此外，还要指定在队列内的邮件数达到配置的阈值时是否要接收警报。发送第一个警报之后，如果队列内的邮件数在15分钟内达到了由150%触发第一个警报的值，则会再发送一个警报。例如，如果阈值设置为1000，

  - 当队列内的邮件最大数达到 1002 时，发送第一个警报。
  - 当队列内的邮件最大数在 15 分钟内达到 1510 时，则会再发送一个警报。

注释 此功能的所有警报均属于“系统警报”(System Alert) 类别。

步骤 4 提交并确认更改。

下一步做什么

如果已为此功能配置了警报，请确保要订购系统警报。有关说明，请参阅添加警报收件人，第 778 页。

检查邮件安全设备的运行状况

可以使用运行状况检查功能检查邮件安全设备的运行状况。执行运行状况检查时，系统将分析当前“状态日志”(Status Logs) 中的历史数据（最多三个月）以确定设备的运行状况。

注释 对于要执行此分析的系统“状态日志”(Status Logs) 必须包含至少一个月的记录数据。

要执行运行状况检查，请

- 在 Web 界面上，依次转至**系统管理 (System Administration)** > **系统运行状况 (System Health)** 页面，然后点击**执行运行状况检查 (Run Health Check)**。
- 在 CLI 上，运行命令：**`healthconfig`**。

分析结果将指明系统在最近几个月内是否遇到了如下一个或多个问题：

- 资源节约模式
- 邮件处理延迟
- 高 CPU 使用
- 高内存使用
- 高内存页面交换

如果运行状况检查指明您的设备遇到了上述一个或多个问题，请考虑查看和优化您的系统配置。有关详细信息，请参阅：
http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118881-technote-esa-00.html。

告警信息

警报邮件是自动生成的标准邮件，其中包含设备上发生的事件的相关信息。这些事件的重要性（或严重性）级别可以从“微小”到“重要”不等，通常有关于设备上的特定组件或功能。警告由设备生成。您可以在更为精细的级别指定将哪些警报邮件发送给哪些用户以及为哪些严重性级别的事件发送警报。通过 GUI 中的“系统管理”>“警报”页面（或 CLI 中的 alertconfig 命令）管理警报。

警报严重性

可以针对以下严重性级别发送警报：

- 严重：需要立即注意。
- 警告 (Warning)：需要进一步监控并可能需要立即注意的问题或错误
- 参考：此设备的例行运行当中生成的信息

自动支持

为了使思科能够更好地支持和设计未来的系统变更，可以将配置为向思科系统发送系统生成的所有警报邮件的副本。此功能称为“自动支持”，是允许我们的团队主动支持您的需求的有效方式。“自动支持”还发送每周报告，说明系统正常运行时间、**`status`** 命令的输出和使用的 AsyncOS 版本。

默认情况下，设置为接收“参考”(Information) 严重性级别的“系统”(System) 警报类型的警报收件人，会收到发往思科的每封邮件的副本。如果您不希望内部每周发送警报邮件，可以禁用此功能。要启用或禁用此功能，请参阅配置警报设置，第 779 页。

警报传送

由于警报邮件可用来通知设备中的问题，因此不使用 AsyncOS 正常的邮件传送系统发送它们。相反，警报邮件通过独立而并行的邮件系统传递，即便在 AsyncOS 存在重大系统故障时也会运行。

警报邮件系统与 AsyncOS 的配置不同，也就是说，警报邮件可能与其他邮件传送的行为稍有不同：

- 警报邮件通过标准 DNS MX 和 A 记录查找传送。
  - 它们不使用 SMTP 路由。
  - 它们确实会缓存 DNS 条目 30 分钟，缓存每 30 分钟刷新一次，所以如果 DNS 出现故障，警报将停止。
- 警报邮件不通过工作队列传递，所以不对它们病毒扫描或垃圾邮件。另外，它们也不受邮件过滤器或内容过滤器约束。
- 警报邮件不通过传送队列传递，因此不受退回配置文件或目标控制限制的影响。

警报邮件示例

```
Date: 23 Mar 2005 21:10:19 +0000

To: joe@example.com

From: IronPort C60 Alert [alert@example.com]

Subject: Critical-example.com: (Anti-Virus) update via http://newproxy.example.com
failed

The Critical message is:

update via http://newproxy.example.com failed

Version: 4.5.0-419

Serial Number: XXXXXXXXXXXX-XXXXXXX

Timestamp: Tue May 10 09:39:24 2005

For more information about this error, please see
http://support.ironport.com

If you desire further information, please contact your support provider.
```

添加警报收件人

通过警报引擎，可以精细控制向哪些警报收件人发送哪些警报。例如，可以将系统配置为仅将特定警报发送给某警报收件人，将某警报收件人配置为仅在发送“系统”(System)（警报类型）的“重要”(Critical)（严重性）信息时接收通知。

注释 如果在系统设置期间启用了“自动支持”，则指定的邮件地址将默认接收所有严重性和类型的警报。可以随时更改此配置。

步骤 1 依次选择**系统管理 (System Administration) > 警报 (Alerts)**。

步骤 2 点击“**添加接收人**”。

步骤 3 输入收件人的邮件地址。可以输入多个地址，并以逗号分隔。

步骤 4 （可选）如果您要接收思科支持人员发来的软件版本和重要支持通知警报，请选中**版本和支持通知 (Release and Support Notifications)** 复选框。

步骤 5 选择此收件人将接收的警报类型和严重性。

步骤 6 提交并确认更改。

配置警报设置

以下设置适用于所有警报。

注释 使用 alertconfig CLI 命令定义要在设备上保存的警报数量以供日后查看。

步骤 1 点击“警报”(Alerts) 页面中的**编辑设置 (Edit Settings)**。

步骤 2 输入“信头源:”地址以在发送警报时使用，或选择“自动生成”(Automatically Generated)(“alert@<hostname>”)。

步骤 3 如果您要指定发送两次重复警报间隔的秒数，请选中该复选框。有关详细信息，请参阅发送重复警告，第 780 页。

- 指定 AsyncOS 发送重复警报前等待的初始秒数。
- 指定 AsyncOS 发送重复警报前等待的最大秒数。

步骤 4 可以通过选中“IronPort 自动支持”(IronPort AutoSupport) 选项来启用“自动支持”。有关“自动支持”的详细信息，请参阅自动支持，第 777 页。

- 如果启用了“自动支持”，则每周向设置为接收“参考”(Information) 级别系统警报的警报收件人发送“自动支持”报告。可以通过该复选框禁用此功能。

步骤 5 提交并确认更改。

警告信设置

警告设置可控制警报的常规行为和配置，包括：

- 发送警告时的 RFC 2822 信头源:（输入地址或使用默认的“alert@<hostname>”）。也可以在 CLI 中使用 alertconfig -> from 命令设置此项。
- 发送重复警报前等待的初始秒数。
- 发送重复警报前等待的最大秒数。

- “自动支持”的状态（启用或禁用）。
- 每周向设置为接收“参考”(Information) 级别系统警报的警报收件人发送“自动支持”状态报告。

发送重复警告

可以指定 AsyncOS 发送重复警报前等待的初始秒数。如果将此值设置为 0，不会发送重复警报摘要，而是毫无任何延迟地发送所有重复警报（这样可能导致短时间内发送大量邮件）。发送每个警报后，发送重复警报之间等待的秒数（警报间隔）将增加。增加值是等待的秒数加上最后间隔的两倍。因此，如果等待 5 秒，警报发送时间将是 5 秒、15 秒、35 秒、75 秒、155 秒、315 秒，以此类推。

最终，间隔可能变得很大。您可以通过“发送重复警报前等待的最大秒数 (maximum number of seconds to wait before sending a duplicate alert)”字段，设置间隔之间等待的秒数限值。例如，如果将初始值设置为 5 秒，最大值为 60 秒，则在 5 秒、15 秒、35 秒、60 秒、120 秒时发送警报，以此类推。

查看最近的警报

邮件安全设备会保存最新的警报，因此如果丢失或删除了警报邮件，可以在 GUI 和 CLI 中进行查看。这些警报无法从设备下载。

要查看最新警报的列表，请点击“警报”页面上的**查看顶部警报**按钮或使用 CLI 中的 displayalerts 命令。可以在 GUI 中按日期、级别、文本和收件人排列警报。

默认情况下，设备最多保存 50 条警报以显示在**顶部警报 (Top Alerts)** 窗口中。使用 CLI 中的 alertconfig -> setup 命令编辑设备保存的警报数。如果要禁用此功能，请将警报数更改为 0。

风险通告说明

下表按类别列出了警报，包括警报名称（使用的内部描述符）、警报的实际文本、说明、严重性（重要，参考或警告）以及邮件文本中所包含的参数（如果有）。参数值在警报的实际文本将被替换。例如，以下警报邮件可能会在邮件文本中提到“$ip”。生成警报时，“$ip”将替换为实际的 IP 地址。

反垃圾邮件警报

下表包含可通过 AsyncOS 生成的各种反垃圾邮件警报的列表，包括对警报和警报严重性的说明。

表 *83:* 可能的反垃圾邮件警报列表

警报名称	邮件和描述	参数
AS.SERVER.ALERT	$engine anti-spam - $message $tb 严重。反垃圾邮件引擎失败时发送。	“**engine**”- 反垃圾邮件引擎的类型。 “**message**”- 日志邮件。 “**tb**”- 事件的回溯。
AS.TOOL.INFO_ALERT	更新 - $engine - $message 信息。反垃圾邮件引擎出现问题时发送。	“**engine**”- 反垃圾邮件引擎名称 “**message**”- 邮件

警报名称	邮件和描述	参数
AS.TOOL.ALERT	更新 - $engine - $message	“**engine**”- 反垃圾邮件引擎名称 “**message**”- 邮件
	严重。当更新因用来管理反垃圾邮件引擎的某个工具出现问题而中止时发送。	

防病毒警报

下表包含可通过 AsyncOS 生成的各种防病毒警报的列表，包括对警报和警报严重性的说明：

表 *84:* 可能的防病毒警报列表

警报名称	邮件和描述	参数
AV.SERVER.ALERT /AV.SERVER.CRITICAL	$engine antivirus - $message $tb	“**engine**”- 防病毒引擎的类型。 “**message**”- 日志邮件。 “**tb**”- 事件的回溯。
	严重。防病毒扫描引擎出现严重问题时发送。	
AV.SERVER.ALERT.INFO	$engine antivirus - $message $tb	“**engine**”- 防病毒引擎的类型。 “**message**”- 日志邮件。 “**tb**”- 事件的回溯。
	信息。当防病毒扫描引擎出现参考事件时发送。	
AV.SERVER.ALERT.WARN	$engine antivirus - $message $tb	“**engine**”- 防病毒引擎的类型。 “**message**”- 日志邮件。 “**tb**”- 事件的回溯。
	警告。防病毒扫描引擎出现问题时发送。	
MAIL.ANTIVIRUS.ERROR_MESSAGE	MID $mid antivirus $what error $tag	“**mid**”- MID “**what**”- 发生的错误。 “**tag**”- 病毒爆发名称（如果已设置）。
	严重。如果防病毒扫描在扫描邮件时发生错误，则发送。	
MAIL.SCANNER. PROTOCOL_MAX_RETRY	MID $mid 已破坏，无法由 $engine 进行扫描。	“**mid**”- MID “**engine**”- 正在使用的引擎
	严重。因为邮件被破坏，所以扫描引擎尝试扫描邮件失败。当超出最大重试次数时，邮件将在不由引擎处理的情况下进行处理。	

目录搜集攻击预防 (DHAP) 警报

下表包含可通过 AsyncOS 生成的各种 DHAP 警报的列表，包括对警报和警报严重性的说明。

表 *85:* 可能的目录搜集攻击预防警报列表

警报名称	邮件和描述	参数
LDAP.DHAP_ALERT	LDAP：检测到潜在的目录搜集攻击。有关此攻击的详细信息，请参阅系统邮件日志。	
	警告。检测到可能的目录搜集攻击时发送。	

硬件风险通告

下表包含可通过 AsyncOS 生成的各种硬件警报的列表，包括对警报和警报严重性的说明。

表 *86:* 可能的硬件警报列表

警报名称	邮件和描述	参数
INTERFACE.ERRORS	端口 $port: 检测到 $in_err 输入错误、$out_err 输出错误、$col 冲突，请检查媒体设置。	“**port**”- 接口名称。 “**in_err**”- 自上一封邮件以来的输入错误数。 “**out_err**”- 自上一封邮件以来的输出错误数。 “**col**”- 自上一封邮件以来的数据包冲突数。
	警告。检测到接口错误时发送。	
MAIL.MEASUREMENTS_FILESYSTEM	$file 系统分区的处于 $capacity% 容量	“**file_system**”- 文件系统的名称 “**capacity**”- 文件系统满溢的程度（采用百分比形式）。
	警告。当磁盘分区接近容量 (75%) 时发送。	
MAIL.MEASUREMENTS_FILESYSTEM.严重	$file 系统分区的处于 $capacity% 容量	“**file_system**”- 文件系统的名称 “**capacity**”- 文件系统满溢的程度（采用百分比形式）。
	严重。当磁盘分区达到 90% 容量（以及 95%、96%、97% 等）时发送。	
SYSTEM.RAID_EVENT_ALERT	RAID 事件发生：$error	“**error**”- RAID 错误的文本。
	警告。发生严重 RAID 事件时发送。	
SYSTEM.RAID_EVENT_ALERT_INFO	RAID 事件发生：$error	“**error**”- RAID 错误的文本。
	信息。发生 RAID 事件时发送。	

垃圾邮件隔离区警报

下表包含可通过 AsyncOS 生成的各种垃圾邮件隔离区警报的列表，包括警报和警报严重性说明。

表 *87:* 可能的垃圾邮件隔离区警报列表

警报名称	邮件和描述	参数
ISQ.CANNOT_CONNECT_OFF_BOX	ISQ：无法在 $host:$port 连接到机下隔离区 信息。当 AsyncOS 无法连接到（机下）IP 地址时发送。	“**host**”- 机下隔离区的地址 “**port**”- 在机下隔离区连接到的端口
ISQ.CRITICAL	ISQ: $msg 严重。发生严重垃圾邮件隔离区错误时发送。	“**msg**”- 要显示的邮件
ISQ.DB_APPROACHING_FULL	ISQ：超过 $threshold% 的数据库为满 警告。垃圾邮件隔离区数据库接近满状态时发送。	“**threshold**”- 开始发送警报时达到的满状态阈值（以百分比形式）
ISQ.DB_FULL	ISQ：数据库已满 严重。垃圾邮件隔离区数据库已满时发送。	
ISQ.MSG_DEL_FAILED	ISQ：因以下原因未能删除 MID $mid（收件人为 $rcpt）：$reason 警告。未能成功从垃圾邮件隔离区删除邮件时发送。	“**mid**”- MID “**rcpt**”- 收件人或“全部” “**reason**”- 未删除邮件的原因
ISQ.MSG_NOTIFICATION_FAILED	ISQ：未能发送通知邮件：$reason 警告。未成功发送通知邮件时发送。	“**reason**”- 未发送通知的原因
ISQ.MSG_QUAR_FAILED	警告。未成功隔离邮件时发送。	
ISQ.MSG_RLS_FAILED	ISQ：因以下原因未能将 MID $mid 发布到 $rcpt：$reason 警告。未成功发布邮件时发送。	“**mid**”- MID “**rcpt**”- 收件人或“全部” “**reason**”- 未发布邮件的原因
ISQ.MSG_RLS_FAILED_UNK_RCPTS	ISQ：因以下原因未能发布 MID $mid：$reason 警告。因收件人未知而未成功发布邮件时发送。	“**mid**”- MID “**reason**”- 未发布邮件的原因

警报名称	邮件和描述	参数
ISQ.NO_EU_PROPS	ISQ：无法检索 $user 的属性。设置默认值	“**user**”- 最终用户名称
	信息。当 AsyncOS 无法检索用户相关信息时发送。	
ISQ.NO_OFF_BOX_HOST_SET	ISQ：在未设置主机的情况下设置机下 ISQ	
	信息。当 AsyncOS 配置为引用未定义的外部隔离区时发送。	

安全列表/阻止列表警报

下表包含可通过 AsyncOS 生成的各种安全列表/阻止列表警报的列表，包括对警报和警报严重性的说明

表 *88:* 可能的安全列表/阻止列表警报列表

警报名称	邮件和描述	参数
SLBL.DB.RECOVERY_FAILED	SLBL：无法恢复最终用户安全列表/阻止列表数据库：“$error”。	“**error**”- 错误原因
	严重。无法恢复安全列表/阻止列表数据库。	
SLBL.DB.SPACE_LIMIT	SLBL：最终用户安全列表/阻止列表数据库超出了允许的磁盘空间：$current of $limit。	“**current**”- 已使用的空间量（以 MB 为单位）
	严重。安全列表/阻止列表数据库超出了允许的磁盘空间。	“**limit**”- 配置的限制（以 MB 为单位）

系统警告

下表包含可通过 AsyncOS 生成的各种系统警报的列表，包括对警报和警报严重性的说明。

表 *89:* 可能的系统警报的列表

组件/警报名称	邮件和描述	参数
AMP.ENGINE.ALERT	请参阅 确保接收有关高级恶意软件防护问题的警报，第 367 页	-
AsyncOS API 警报	请参阅《使用思科邮件安全设备的 *AsyncOS API* - 入门指南》的“警报”部分。	-
邮箱自动修复警报	请参阅“警报”部分 自动修补 Office 365 邮箱中的邮件，第 435 页	-

组件/警报名称	邮件和描述	参数
COMMON.APP_FAILURE	应用故障发生：$error 警告。出现未知应用故障时发送。	“**error**”- 错误（通常为回溯）的文本。
COMMON.ENGINE_AUTO_UPDATE_ENABLED	<$level>: <$class> 信息：已为特定引擎 <$engine> 启用了自动更新。现在，您将收到此引擎的自动引擎更新。	“**$engine**”- 服务引擎的名称。值可以为： • Sophos • McAfee • Graymail
COMMON.ENGINE_AUTO_UPDATE_DISABLED	<$level>: <$class> 信息：已为特定引擎 <$engine> 禁用了自动更新。除非在特定引擎的“全局设置”页面中启用了自动更新，否则不会收到此引擎的任何自动更新。	“**$engine**”- 服务引擎的名称。值可以为： • Sophos • McAfee • Graymail
COMMON.KEY_EXPIRED_ALERT	您的“$feature”密钥已经到期。请联系您的授权思科销售代表。 警告。功能密钥过期时发送。	“**feature**”- 即将到期的功能的名称。
COMMON.KEY_EXPIRING_ALERT	您的“$feature”密钥将于 $days 天内到期。请联系您的授权思科销售代表。 警告。功能密钥即将到期时发送。	“**feature**”- 即将到期的功能的名称。 “**days**”- 功能将要到期的天数。
COMMON.KEY_FINAL_EXPIRING_ALERT	这是最终通知。您的“$feature”密钥将于 $days 天内到期。请联系您的授权思科销售代表。 警告。以功能密钥即将到期的最终通知形式发送。	“**feature**”- 即将到期的功能的名称。 “**days**”- 功能将要到期的天数。
KEYS.GRACE_EXPIRING_ALERT	思科邮件安全设备已经到期的所有安全服务许可证。设备将在 $days 天内不使用安全服务继续传送邮件。 要续订安全服务许可证，请联系您的授权思科销售代表。 严重。从宽限期开始针对虚拟设备许可证到期定期发送。	“**days**”- 发送警报时宽限期内所剩的天数。 有关宽限期的详细信息，请参阅虚拟设备许可证到期，第 753 页。

组件/警报名称	邮件和描述	参数
KEYS.GRACE_FINAL_EXPIRING_ALERT	这是最终通知。思科邮件安全设备已经到期的所有安全服务许可证。设备将在1天内不使用安全服务继续传送邮件。 要续订安全服务许可证，请联系您的授权思科销售代表。 严重。虚拟设备许可证到期之前的一天发送。	有关宽限期的详细信息，请参阅虚拟设备许可证到期，第 753 页。
KEYS.GRACE_EXPIRED_ALERT	您的宽限期已经到期。所有安全服务均已到期，因此您的设备无法运行。采用新许可证之前，设备不再传送邮件。 要续订安全服务许可证，请联系您的授权思科销售代表。 严重。当虚拟设备的宽限期到期时发送。	有关宽限期的详细信息，请参阅虚拟设备许可证到期，第 753 页。
DNS.BOOTSTRAP_FAILED	无法启动 DNS 解析器。无法联系根服务器。 警告。当设备无法与根 DNS 服务器通信时发送。	
COMMON.INVALID_FILTER	无效 class：$error 警告。当遇到无效过滤器时发送。	“**class**”-“Filter”、“SimpleFilter”等。 “**error**”- 其他有关为何过滤器无效的信息。
IPBLOCKD.HOST_ADDED_TO_WHITELIST IPBLOCKD.HOST_ADDED_TO_BLACKLIST IPBLOCKD.HOST_REMOVED_FROM_BLACKLIST	由于 SSH DOS 攻击，已将 $ip 的主机添加到黑名单。 已将 $ip 的主机永久添加到 ssh 白名单。 已从黑名单删除 $ip 的主机 警告。 对于尝试通过 SSH 连接到设备，但未提供有效凭证的 IP 地址，如果两分钟内失败尝试次数大于 10 次，则将其添加到 SSH 黑名单。 如果用户从同一 IP 地址成功登录，则将该 IP 地址添加到白名单。 白名单的地址即使在黑名单中，也允许它们访问。 条目将于大约一天后自动从该黑名单删除。	“**ip**”- 尝试从其进行登录的 IP 地址。

组件/警报名称	邮件和描述	参数
LDAP.GROUP_QUERY_FAILED_ALERT	LDAP：失败的组查询 $name，过滤器中的比较将评估为 false	“**name**”- 查询的名称。
	严重。当 LDAP 组查询失败时发送。	
LDAP.HARD_ERROR	LDAP：$name 内因 $why 原因发生工作队列处理错误	“**name**”- 查询的名称。 “**why**”- 错误发生的原因。
	严重。当LDAP查询完全失败时（尝试所有服务器之后）发送。	
LOG.ERROR.*	严重。各种日志记录错误。	
MAIL.FILTER.RULE_MATCH_ALERT	MID $mid 匹配 $rule_name 规则。\n 详细信息：$details	“**mid**”- 邮件的唯一识别号。 “**rule_name**”- 匹配的规则的名称。 “**details**”- 有关邮件或规则的详细信息。
	信息。每当标头请求规则被评价为 true 时发送。	
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	扫描各个收件人期间LDAP组查询失败，可能是 LDAP 错误配置或服务器不可访问所致。	
	严重。扫描各个收件人期间LDAP组查询失败时发送。	
MAIL.QUEUE.ERROR.*	严重。各种邮件队列硬错误。	
MAIL.RES_CON_START_ALERT.内存	此系统（主机名：$hostname）已进入“资源节约”模式，以防止快速消耗重要系统资源。此系统的 RAM 利用率超出了 $memory_threshold_start% 的资源节约阈值。此系统允许的接收速率将随着 RAM 利用率越来越接近 $memory_threshold_halt% 而逐渐降低。	“**hostname**”- 主机的名称。 “**memory_threshold_start**”- 启动内存缓送技术时的百分比阈值。 “**memory_threshold_halt**”- 系统因内存过满而将中止时的百分比阈值。
	严重。当 RAM 使用率超过系统资源节约阈值时发送。	
MAIL.RES_CON_START_ALERT.QUEUE_SLOW	此系统（主机名：$hostname）已进入“资源节约”模式，以防止快速消耗重要系统资源。队列出现过载，无法保持当前吞吐量。	“**hostname**”- 主机的名称。
	严重。当邮件队列过载及企业系统资源节约时发送。	

组件/警报名称	邮件和描述	参数
MAIL.RES_CON_START_ALERT.QUEUE	此系统（主机名：$hostname）已进入“资源节约”模式，以防止快速消耗重要系统资源。此系统的队列利用率超出了 $queue_threshold_start% 的资源节约阈值。此系统允许的接收速率将随着队列利用率越来越接近 $queue_threshold_halt% 而逐渐降低。	“**hostname**”- 主机的名称。 “**queue_threshold_start**”- 启动内存缓送技术时的百分比阈值。 “**queue_threshold_halt**”- 系统因队列过满而将中止时的百分比阈值。
	严重。当队列利用率超过系统资源节约阈值时发送。	
MAIL.RES_CON_START_ALERT.WORKQ	此系统（主机名：$hostname）已进入“资源节约”模式，以防止快速消耗重要系统资源。当前工作队列大小超出 $suspend_threshold 的阈值，因此侦听程序已挂起。工作队列大小下降到 $resume_threshold 时，侦听程序将会恢复。使用系统 CLI 上的“tarpit”命令可以改变这些阈值。	“**hostname**”- 主机的名称。 “**suspend_threshold**”- 侦听程序挂起的工作队列大小下限。 “**resume_threshold**”- 侦听程序恢复的工作队列大小上限。
	信息。由于工作队列过大暂停监听程序时发送。	
MAIL.RES_CON_START_ALERT	此系统（主机名：$hostname）已进入“资源节约”模式，以防止快速消耗重要系统资源。	“**hostname**”- 主机的名称。
	严重。当设备进入“资源节约”模式时发送。	
MAIL.RES_CON_STOP_ALERT	由于资源利用率已下降到节约阈值以下，因此此系统（主机名：$hostname）已退出“资源节约”模式。	“**hostname**”- 主机的名称。
	信息。当设备退出“资源节约”模式时发送。	
MAIL.SDS.CATEGORY_CHANGE	请参阅将来的 URL 类别集变更，第 351 页。	-
MAIL.SDS.CERTIFICATE_INVALID	请参阅URL 过滤故障排除，第 336 页。	
MAIL.SDS.ERROR_FETCHING_CERTIFICATE		
MAIL.WORK_QUEUE_PAUSED_NATURAL	工作队列已暂停，$num 个邮件，$reason	“**num**”- 工作队列中的邮件数。 “**reason**”- 工作队列暂停的原因。
	严重。当工作队列暂停时发送。	
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	工作队列已恢复，$num 个邮件	“**num**”- 工作队列中的邮件数。
	严重。当工作队列恢复时发送。	

组件/警报名称	邮件和描述	参数
NTP.NOT_ROOT	未以根用户身份运行，无法调整系统时间	
	警告。当设备由于 NTP 未以根用户身份运行而无法调整时间时发送。	
QUARANTINE.ADD_DB_ERROR	无法隔离 MID $mid - 隔离系统不可用	“**mid**”- MID
	严重。无法将邮件发送至隔离区时发送。	
QUARANTINE.DB_UPDATE_FAILED	无法更新隔离区数据库（当前版本：$version；目标版本：$target_version）	“**version**”- 检测到的方案版本。 “**target_version**”- 目标方案版本。
	严重。无法更新隔离区数据库时发送。	
QUARANTINE.DISK_SPACE_LOW	$file_system 分区空间不足导致隔离区系统不可用。	“**file_system**”- 文件系统的名称
	严重。当隔离区磁盘空间已满时发送。	
QUARANTINE.THRESHOLD_ALERT	隔离区“$quarantine”处于 $full% 满状态	“**quarantine**”- 隔离区的名称。 “**full**”- 隔离区满溢程度的百分比。
	警告。当隔离区达到容量的 5%、50% 或 75% 时发送。	
QUARANTINE.THRESHOLD_ALERT.SERIOUS	隔离区“$quarantine”处于 $full% 满状态	“**quarantine**”- 隔离区的名称。 “**full**”- 隔离区满溢程度的百分比。
	严重。当隔离区达到容量的 95% 时发送。	
REPORTD.DATABASE_OPEN_FAILED_ALERT	打开数据库时，报告系统遇到严重错误。为了防止中断其他服务，应在此计算机上禁用报告。请与客户支持联系以启用报告。错误消息如下：$err_msg	“**err_msg**”- 出现的错误邮件
	严重。当报告引擎无法打开数据库时发送。	
REPORTD.AGGREGATION_DISABLED_ALERT	“由于日志记录磁盘空间不足，对所收集报告数据的处理功能已禁用。磁盘使用量超过 $threshold 百分比。报告事件的记录很快将会受限，如果未释放磁盘空间（通过删除旧日志等方法），还可能会丢失报告数据。磁盘使用量下降到 $threshold 百分比以下时，报告数据的满状态处理将会自动重新启动。	“**threshold**”- 阈值
	警告。当系统磁盘空间不足时发送。当日志条目的磁盘使用量超过日志使用阈值时，报告禁用聚合并发送警报。	

组件/警报名称	邮件和描述	参数
REPORTING.CLIENT.UPDATE_FAILED_ALERT	报告客户端：报告系统在延长的一段时间 ($duration) 内无响应。 警告。当报告引擎无法保存报告数据时发送。	“**duration**”- 客户端一直在尝试联系报告后台守护程序的时长。此为一个采用人可读格式的字符串 (’1h 3m 27s’)。
REPORTING.CLIENT.JOURNAL.FULL	报告客户端：报告系统无法保持生成数据的速率。生成的所有新数据都将丢失。 严重。当报告引擎无法存储新数据时发送。	
REPORTING.CLIENT.JOURNAL.一	报告客户端：报告系统现在无法处理新数据。 信息。当报告引擎再次能够存储新数据时发送。	
PERIODIC_REPORTS.REPORT_TASK.BUILD_FAILURE	生成定期报告“$report_title”时出错。此订用已从调度程序删除。 严重。当报告引擎无法生成报告时发送。	“**report_title**”- 报告标题
PERIODIC_REPORTS.REPORT_TASK.EMAIL_FAILURE	以邮件发送定期报告“$report_title”时失败。此订用已从调度程序删除。 严重。当无法通过邮件发送报告时发送。	“**report_title**”- 报告标题
PERIODIC_REPORTS.REPORT_TASK.ARCHIVE_FAILURE	存档定期报告“$report_title”时失败。此订用已从调度程序删除。 严重。当报告无法存档时发送。	“**report_title**”- 报告标题
SENDERBASE.ERROR	处理对查询 $query 的响应时出错：响应为 $response 信息。处理 SenderBase 的响应出错时发送。	“**query**”- 查询地址。 “**response**”- 收到的响应的原始数据。
SMTPAUTH.FWD_SERVER_FAILED_ ALERT	SMTP 身份验证：无法到达转发服务器 $ip 时出错，原因为 $why 警告。无法访问 SMTP 身份验证转发服务器时发送。	“**ip**”- 远程服务器的 IP。 “**why**”- 错误发生的原因。
SMTPAUTH.LDAP_QUERY_FAILED	SMTP 身份验证：LDAP 查询失败，有关详细信息，请参阅 LDAP 调试日志。 警告。当 LDAP 查询失败时发送。	

组件/警报名称	邮件和描述	参数
SYSTEM.HERMES_SHUTDOWN_FAILURE. 重新启动	准备${what}时，无法以温和的方式停止邮件服务器：${error}$what:=reboot 警告。关闭正在重启的系统出现问题时发送。	“**error**”- 发生的错误。
SYSTEM.HERMES_SHUTDOWN_FAILURE. SHUTDOWN	准备${what}时，无法以温和的方式停止邮件服务器：${error}$what:=shut down 警告。关闭系统出现问题时发送。	“**error**”- 发生的错误。
SYSTEM.LOGIN_FAILURES_LOCK_ALERT	$Numlogins 次连续登录失败后，用户“$user”被锁定。上次从 $rhost 进行登录尝试 信息：当因失败登录尝试次数达到最大值而导致用户帐户被锁定时发送	“user”- 用户名称 “numlogins”- 配置的警报阈值 “rhost”- 远程主机的地址
SYSTEM.RCPTVALIDATION.UPDATE_FAILED	更新收件人验证数据时出错：$why 严重。当收件人验证更新失败时发送。	“why”- 错误邮件。
SYSTEM.SERVICE_TUNNEL.已禁用	技术支持：服务隧道已被禁用 信息。禁用为“思科支持服务”(Cisco Support Services) 创建的隧道时发送。	
SYSTEM.SERVICE_TUNNEL.ENABLED	技术支持：服务隧道已启用，端口 $port 信息。启用为“思科支持服务”(Cisco Support Services) 创建的隧道时发送。	“**port**”- 用于服务隧道的端口。
IPBLOCKD.HOST_ADDED_TO_WHITELIST IPBLOCKD.HOST_ADDED_TO_BLACKLIST IPBLOCKD.HOST_REMOVED_FROM_BLACKLIST	由于 SSH DOS 攻击，已将 $ip 的主机添加到黑名单。 已将 $ip 的主机永久添加到 ssh 白名单。 已从黑名单删除 $ip 的主机 警告。 对于尝试通过 SSH 连接到设备，但未提供有效凭证的 IP 地址，如果两分钟内失败尝试次数大于 10 次，则将其添加到 SSH 黑名单。 如果用户从同一 IP 地址成功登录，则将该 IP 地址添加到白名单。 白名单的地址即使在黑名单中，也允许它们访问。 条目将于大约一天后自动从该黑名单删除。	“**ip**”- 尝试从其进行登录的 IP 地址。

组件/警报名称	邮件和描述	参数
WATCHDOG_RESTART_ALERT_MSG	<$level>: <$class>, <$hostname>: $subject $text 警告。 思科邮件安全设备使用监控器服务监控以下引擎的运行状况： • 反垃圾邮件 • 防病毒 • 防恶意软件防护 • Graymail 如果上述任何一个引擎在某一持续时间内都没有响应监控器服务，则监控器服务将重启引擎，并向管理员发送警报。	“**subject**”- 特定于引擎的监控器警报主题 “**text**”- 特定于引擎的监控器警报文本
MAIL.IMH.GEODB_UPDATE_COUNTRIES'	警告。地理位置更新 - 受支持的国家/地区列表已更改。 增加的国家/地区 - <$added> 删除的国家/地区 - <$deleted> 相应地检查您的 HAT 发件人组、邮件过滤器和内容过滤器设置。	“added”- 添加了以下国家/地区：<iso_code1>:<country_name1>,<iso_code2>:<country_name2>, “deleted”- 删除了以下国家/地区：<iso_code1>:<country_name1>:<iso_code2>:<country_name2>,

更新程序警报

下表包含可由 AsyncOS 生成的各种更新程序警报。

表 *90:* 可能的更新程序警报列表

警报名称	邮件和描述	参数
UPDATER.APP.UPDATE_ABANDONED	发布新版本后，$app 才会丢弃更新。$app 应用尝试并失败了 $attempts 次后才成功完成更新。这可能是由于网络配置问题或临时中断所致	“**app**”- 应用名称。 “**attempts**”- 尝试次数。
	警告。应用正在丢弃更新。	
UPDATER.UPDATER.MANIFEST_FAILED_ALERT	更新程序已至少 $threshold 无法与更新程序服务器通信。	“**threshold**”- 人可读阈值字符串。
	警告。未能获取服务器证明。	

警报名称	邮件和描述	参数
UPDATER.UPDATER_RELEASE_NOTIFICATION	$mail_text 警告。发布通知。	“**mail_text**”- 通知文本。 “**notification_subject**”- 通知文本。
UPDATER.UPDATERD.UPDATE_FAILED	出现未知错误：$traceback 严重。未能运行更新。	“**traceback**”- 回溯。

病毒爆发过滤器警报

下表包含可通过 AsyncOS 生成的各种病毒爆发过滤器警报的列表，包括对警报和警报严重性的说明。请注意，爆发过滤器也可以在隔离区（具体是指爆发隔离区）的系统警报中引用。

表 *91:* 可能的病毒爆发过滤器警报列表

警报名称	邮件和描述	参数
VOF.GTL_THRESHOLD_ALERT	爆发过滤器规则更新警报：$text 上次在 $date $time 更新的所有规则。 信息。当病毒爆发过滤器阈值发生更改时发送。	“**text**”- 更新警报文本。 “**time**”- 上次更新时间。 “**date**”- 上次更新日期。
AS.UPDATE_FAILURE	$engine 更新不成功。这可能是由于瞬态网络或 DNS 问题、引起更新传输错误的 HTTP 代理配置或 downloads.ironport.com 不可用造成的。这种失败造成设备上产生的特定错误是：$error 警告。当反垃圾邮件引擎或 CASE 规则无法更新时发送。	“**engine**”- 无法更新的引擎。 “**error**”- 发生的错误。

将警报集群化

下表包含可通过 AsyncOS 生成的各种系统警报的列表，包括对警报和警报严重性的说明：

表 *92:* 可能的集群警报列表

警报名称	邮件和描述	参数
CLUSTER.CC_ERROR.AUTH_ERROR	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=计算机似乎不在集群中 严重。发生身份验证错误时发送。如果计算机不是集群成员，可能会出现这种情况。	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。

警报名称	邮件和描述	参数
CLUSTER.CC_ERROR.DROPPED	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=现有连接被丢弃 警告。与集群的连接被丢弃时发送。	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR.FAILED	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=连接失败 警告。与集群的连接失败时发送。	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR.FORWARD_FAILED	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=邮件转发失败，无上游连接 严重。设备无法将数据转发到集群中的计算机时发送。	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR.NOROUTE	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=未发现路由 严重。计算机无法获取到集群中另一计算机的路由时发送。	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR.SSH_KEY	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=主机密钥无效 严重。存在无效 SSH 主机密钥时发送。	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR.TIMEOUT	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=操作超时 警告。指定的操作超时时发送。	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP	连接到集群计算机 $name 时出错 - $error - $why 严重。设备为集群中的另一计算机获取有效 IP 地址时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。

警报名称	邮件和描述	参数
CLUSTER.CC_ERROR_NOIP.AUTH_ERROR	连接到集群计算机 $name 时出错 - $error - whyerror:=计算机似乎不在集群中 严重。连接到集群中的计算机出现身份验证错误时发送。如果计算机不是集群成员，可能会出现这种情况。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP.植入的文件	连接到集群计算机 $name 时出错 - $error - whyerror:=现有连接被丢弃 警告。计算机无法为集群内的另一计算机获取有效 IP 地址并且与集群的连接丢弃时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP.发生故障	连接到集群计算机 $name 时出错 - $error - whyerror:=连接失败 警告。出现未知连接失败并且计算机无法为集群内的另一计算机获取有效 IP 地址时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP.FORWARD_FAILED	连接到集群计算机 $name 时出错 - $error - whyerror:=邮件转发失败，无上游连接 严重。计算机无法为集群内的另一计算机获取有效IP地址并且设备无法将设备转发至计算机时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP.NOROUTE	连接到集群计算机 $name 时出错 - $error - whyerror:=未发现路由 严重。计算机无法为集群内的另一计算机获取有效IP地址并且无法获取至计算机的路由时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP.SSH_KEY	连接到集群计算机 $name 时出错 - $error - whyerror:=主机密钥无效 严重。计算机无法为集群内的另一计算机获取有效 IP 地址并且无法获取有效 SSH 主机密钥时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP.TIMEOUT	连接到集群计算机 $name 时出错 - $error - whyerror:=操作超时 警告。计算机无法为集群内的另一计算机获取有效 IP 地址并且指定操作超时时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。

警报名称	邮件和描述	参数
CLUSTER.SYNC.PUSH_ALERT	覆盖计算机 $name 上的 $sections 严重。当配置数据不同步并且已发送至远程主机时发送。	“**name**”- 计算机的主机名和/或序列号。 “**sections**”- 正在发送的集群部分的列表。

更改网络设置

本节介绍用于配置设备网络操作的功能。通过这些功能，可以直接访问在使用系统设置向导，第 29 页中使用系统设置向导（或 **systemsetup** 命令）配置的主机名、DNS 和路由设置。

本节讨论以下功能：

- **sethostname**
- DNS 配置（GUI 以及 **dnsconfig** 命令）
- 路由配置（GUI 以及通过 **routeconfig** 和 **setgateway** 命令）
- **dnsflush**
- 密码
- 网络接入
- 登录标识

更改系统主机名

主机名用于识别系统。您必须输入完全限定的主机名。要更改主机名，请执行以下操作：

- 在 Web 界面上，依次点击“网络”>“IP 接口”，点击“管理”，然后在“主机名”中更改主机名。
- 在 CLI 中，使用 sethostname 命令。

注释 确认更改后，新主机名才会生效。

配置域名系统 (DNS) 设置

可以通过 GUI 的“网络”菜单的“DNS”页面或 dnsconfig 命令为设备配置 DNS 设置。

可以配置以下设置：

- 使用 Internet 的 DNS 服务器还是自己的服务器，以及具体使用的服务器
- 用于 DNS 通信的接口
- 反向 DNS 查找超时前等待的秒数
- 清除 DNS 缓存

指定 DNS 服务器

AsyncOS 可以使用 Internet 根 DNS 服务器、您自己的 DNS 服务器，或 Internet 根 DNS 服务器和您指定的授权 DNS 服务器。使用 Internet 根服务器时，可以指定用于特定域的备用服务器。由于备用 DNS 服务器适用于单个域，所有它必须对该域拥有授权（提供限定的 DNS 记录）。

不使用 Internet 的 DNS 服务器时，AsyncOS 支持“拆分”DNS 服务器。如果您要使用自己的内部服务器，还可以指定例外域及关联的 DNS 服务器。

设置“拆分 DNS”时，还应设置 in-addr.arpa (PTR) 条目。例如，如果要将“.eng”查询重定向到名称服务器 1.2.3.4，并且所有 .eng 条目均在 172.16 网络内，则应将“eng,16.172.in-addr.arpa”指定为拆分 DNS 配置中的域。

多个条目和优先级

对于输入的每个 DNS 服务器，都可以指定一个数字优先级。AsyncOS 将尝试使用优先级最接近 0 的 DNS 服务器。如果该 DNS 服务器没有响应，AsyncOS 将尝试使用下一个优先级的服务器。如果为相同优先级的 DNS 服务器指定了多个条目，则系统在每次执行查询时会随机列出该优先级的 DNS 服务器。然后，系统会等待简短时间让第一个查询到期或“超时”，然后会等待稍长一点的时间让第二个查询到期或“超时”，以此类推。所等待的时长取决于已配置的 DNS 服务器及优先级的确切总数。在任何特定优先级，所有 IP 地址的超时长度相同。第一个优先级的超时时间最短，后续每个优先级的超时时间依次延长。而且，超时期限约为 60 秒。如果有一个优先级，则该优先级每台服务器的超时将为 60 秒。如果有两个优先级，则第一个优先级每台服务器的超时将为 15 秒；第二个优先级每台服务器的超时将为 45 秒。对于三个优先级，超时分别为 5 秒、10 秒、45 秒。

例如，假设您配置了四台 DNS 服务器，其中两台为优先级 0，一台为优先级 1，另一台为优先级 2：

表 *93: DNS* 服务器、优先级和超时间隔示例

优先级	服务器	超时（秒）
0	1.2.3.4、1.2.3.5	5、5
1	1.2.3.6	10
2	1.2.3.7	45

AsyncOS 将在优先级为 0 的两台服务器之间随机选择。如果一台优先级 0 的服务器关闭，则使用另一台。如果优先级为 0 的两台服务器均关闭，则使用优先级为 1 的服务器 (1.2.3.6)，最后是优先级为 2 (1.2.3.7) 的服务器。

两台优先级为 0 的服务器的超时期限相同，优先级为 1 的服务器稍长，优先级为 2 的服务器更长。

使用 Internet 根服务器

AsyncOS DNS 解析器旨在容纳高性能邮件传送所需的大量并行 DNS 连接。

注释 如果选择将默认 DNS 服务器设置为 Internet 根服务器之外的其他服务器，则该服务器必须能够递归解析其不属于授权服务器的域的查询。

反向 DNS 查询超时

设备尝试对连接到侦听程序来收发邮件的所有远程主机执行“双重DNS查找”。即系统通过执行双重 DNS 查找，获取和验证远程主机 IP 地址的有效性。其中包括对连接主机的 IP 地址的反向 DNS (PTR) 查询，之后是对 PTR 查询结果的正向 DNS (A) 查询。然后，系统将检查 A 查询结果是否与 PTR 查询结果匹配。如果结果不匹配或 A 记录不存在，则系统将仅使用 IP 地址来匹配主机访问表 (HAT) 中的条目。此特定超时期限仅适用于此查询，与多个条目和优先级，第 797 页中讨论的通用 GNS 超时无关。

默认值为 20 秒。可以全局禁用所有侦听程序中的反向 DNS 查询超时，方法是输入“0”作为秒数。

如果该值设置为 0 秒，则不尝试反向 DNS 查询，而是立即返回标准超时响应。这样也可以防止在接收主机的证书具有映射至主机 IP 查询的公共名称 (CN) 时设备将邮件传送至需要 TLS 验证的连接的域。

DNS 警报

有时，重启设备时，系统会生成警报，其中包含“无法引导DNS缓存”的消息。这些消息表示系统无法与其主 DNS 服务器通信，如果在建立网络连接前 DNS 子系统已上线，则可能在启动时出现这种情况。如果其他时候出现此消息，可能表示存在网络问题或 DNS 配置未指向有效的服务器。

清除 DNS 缓存

GUI 中的“清除缓存”按钮或 dnsflush 命令（有关 dnsflush 命令的详细信息，请参阅《思科邮件安全设备 AsyncOS CLI 参考指南》）将清除 DNS 缓存中的所有信息。更改本地 DNS 系统后，您可能会选择使用此功能。该命令会立即生效，并且重新填充缓存时可能导致性能临时下降。

通过图形用户界面配置 DNS 设置

步骤 1 依次选择**网络 (Network) > DNS**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选择使用 Internet 的根 DNS 服务器还是自己的内部 DNS 服务器还是 Internet 的根 DNS 服务器，并指定备用 DNS 服务器。

步骤 4 如果您要使用自己的 DNS 服务器，请输入服务器 ID 并点击**添加行 (Add Row)**。对于每个服务器重复上述步骤。在输入自己的 DNS 服务器时，还请指定优先级。有关详细信息，请参阅指定 DNS 服务器，第 797 页。

步骤 5 如果您要为某些域指定备用 DNS 服务器，请输入域名和备用 DNS 服务器 IP 地址。点击**添加行 (Add Row)** 添加其他域。

注释 可以为单个 DNS 服务器输入多个域名，只需使用逗号分隔域名即可。也可以输入多个 DNS 服务器，方法也是使用逗号分隔 IP 地址。

步骤 6 选择用于 DNS 通信的接口。
步骤 7 输入取消反向 DNS 查询之前等待的秒数。
步骤 8 也可以点击**清除缓存 (Clear Cache)** 清除 DNS 缓存。
步骤 9 提交并确认更改。

配置 TCP/IP 通信路由

有些网络环境需要使用标准默认网关以外的通信路由。

邮件安全设备可以使用互联网协议版本 4 (IPv4) 和互联网协议版本 6 (IPv6) 静态路由。

可以使用 CLI 中的 routeconfig 命令或使用以下过程管理静态路由。

步骤 1 依次选择**网络 (Network) > 路由 (Routing)**。
步骤 2 针对要创建的静态路由类型（IPv4 或 IPv6）点击**添加路由 (Add Route)**。
步骤 3 输入路由名称。
步骤 4 输入目标 IP 地址。
步骤 5 输入网关 IP 地址。
步骤 6 提交并确认更改。

配置默认网关

可以使用 CLI 中的 setgateway 命令或使用以下过程配置默认网关。

步骤 1 依次选择**网络 (Network) > 路由 (Routing)**。
步骤 2 针对要修改的互联网协议版本点击路由列表中的**默认路由 (Default Route)**。
步骤 3 更改网关 IP 地址。
步骤 4 提交并确认更改。

配置 SSL 设置

可以使用“SSL 配置设置”页面或 sslconfig 命令为设备配置 SSL 设置。

步骤 1 依次点击**系统管理 (System Administration) > SSL 配置设置 (SSL Configuration Settings)**。
步骤 2 点击**编辑设置 (Edit Settings)**。
步骤 3 根据您的要求，执行以下操作：

- 设置 GUI HTTPS SSL 设置。在 GUI HTTPS 下，指定要使用的 SSL 方法和密码。
- 设置入站 SMTP SSL 设置。在入站 SMTP 下，指定要使用的 SSL 方法和密码。
- 设置出站 SMTP SSL 设置。在出站 SMTP 下，指定要使用的 SSL 方法和密码。

请记住：

- 不能同时启用 SSL v2 和 TLS v1 方法。但是，可以结合 SSL v3 方法启用这些方法。
- 您不能同时启用 TLS v1.0 和 v1.1 方法。但是，可以结合 TLS v1.2 方法启用这些方法。

步骤 4 点击 **Submit**。

步骤 5 点击**确认更改**。

禁用 SSLv3 以增强安全性

为了增强安全性，可以针对以下服务禁用 SSLv3：

- 更新程序
- URL 过滤
- 终端用户隔离区
- LDAP

使用 CLI 中的 sslv3config 命令对以上服务禁用或启用 SSLv3。以下示例显示了如何针对终端用户隔离区禁用 SSLv3。

```
mail.example.com> sslv3config
     Current SSLv3 Settings:
     ---------------------------------------------------
                 UPDATER     :     Enabled
              WEBSECURITY    :     Enabled
                     EUQ     :     Enabled
                    LDAP     :     Enabled
     ---------------------------------------------------
Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.
[]> setup
Choose the service to toggle SSLv3 settings:
1. EUQ Service
2. LDAP Service
3. Updater Service
4. Web Security Service
[1]>
Do you want to enable SSLv3 for EUQ Service ? [Y]>n
Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.
[]>
```

系统时间

要在设备上设置系统时间，请设置使用的时区，或者选择一个 NTP 服务器和查询接口，然后使用 GUI 中“系统管理”菜单中的“时区”或“时间设置”页面或使用 CLI 中的以下命令：ntpconfig、settime 和 settz。

也可以在**系统管理 > 时间设置**页面上或使用 tzupdate CLI 命令验证 AsyncOS 使用的时区文件。

选择时区

“时区”(Time Zone) 页面（通过 GUI 中的“系统管理”[System Administration] 菜单可用）显示设备的时区。可以选择特定的时区或 GMT 偏移。

步骤 1 在**系统管理 (System Administration) > 时区 (Time Zone)** 页面中点击**编辑设置 (Edit Settings)**。

步骤 2 从下拉菜单中选择区域、国家/地区和时区。

步骤 3 提交并确认更改。

选择 GMT 偏移

步骤 1 在**系统管理 (System Administration) > 时区 (Time Zone)** 页面中点击**编辑设置 (Edit Settings)**。

步骤 2 从区域列表中选择“GMT 偏移时间 (GMT Offset)”。

步骤 3 在“时区”(Time Zone) 列表中选择偏移。偏移是指为了达到 GMT（本初子午线）所必须增加/减去的小时数。小时前缀减号（“-”）表示本初本初子午线以东。加号（“+”）表示本初子午线以西。

步骤 4 提交并确认更改。

编辑时间设置

可以使用以下方法之一编辑设备的时间设置：

（推荐）使用网络时间协议 (NTP) 设置设备系统时间

这是建议的时间保留方法，特别是您的设备与其他设备集成时更是如此。所有集成设备应使用同一台 NTP 服务器。

步骤 1 依次导航至“系统管理”(System Administration) >“时间设置”(Time Settings) 页面。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 在“时间保留方法”(Time Keeping Method) 部分，选择“使用网络时间协议”(Use Network Time Protocol)。

步骤 4 输入 NTP 服务器地址，然后点击**添加行 (Add Row)**。可以添加多个 NTP 服务器。
步骤 5 要从列表中删除 NTP 服务器，请点击该服务器对应的垃圾桶图标。
步骤 6 为 NTP 查询选择一个接口。这是 NTP 查询应该源于的 IP 地址。
步骤 7 提交并确认更改。

手动设置设备系统时间

通常不建议使用此时间保留方法。而是使用网络时间协议服务器。

步骤 1 依次导航至“系统管理”(System Administration) >“时间设置”(Time Settings) 页面。
步骤 2 点击**编辑设置 (Edit Settings)**。
步骤 3 在“时间保留方法”(Time Keeping Method) 部分，选择“手动设置时间”(Set Time Manually)。
步骤 4 输入月、日、年、小时、分钟和秒数。
步骤 5 选择上午或下午
步骤 6 提交并确认更改。

自定义视图

使用收藏夹页面

（仅限通过本地身份验证的管理用户。）可以创建最常用的页面的快速访问列表。

目标	请
将页面添加到收藏夹列表	导航到要添加的页面，然后从窗口右上角附近的“我的收藏夹 (My Favorites)”菜单选择**将此页添加到我的收藏夹 (Add This Page To My Favorites)**。 更改“我的收藏夹 (My Favorites)”时不需要确认。
收藏夹重新排序	依次选择**我的收藏夹 (My Favorites) > 查看我的所有收藏夹 (View All My Favorites)**，并按所需的顺序拖动收藏夹。
删除收藏夹	依次选择**我的收藏夹 (My Favorites) > 查看我的所有收藏夹 (View All My Favorites)**，并删除收藏夹。
转到收藏夹页面	从窗口右上角附近的**我的收藏夹 (My Favorites)** 菜单选择一个页面。
查看或构建自定义报告页面	请参阅“我的控制面板”页面，第 640 页。

设置用户首选项

本地用户可以定义特定于每个帐户的首选项设置，例如语言。当用户首次登录设备时，默认应用这些设置。存储每个用户的首选项设置，无论用户从哪个客户机登录到设备，首选项设置都相同。

如果用户更改了这些设置，但未确认这些更改，那么当用户重新登录时，这些设置将恢复为默认值。

注释 外部验证的用户不能使用此功能。这些用户可以直接从“选项”(Options) 菜单中选择语言。

步骤 1 使用想要定义其首选项设置的用户帐户登录到设备。

步骤 2 依次选择**选项 (Options) > 首选项 (Preferences)**。“选项”(Options) 菜单位于窗口的右上角。

步骤 3 点击**编辑首选项 (Edit Preferences)**。

步骤 4 配置设置：

首选项设置	说明
语言显示 (Language Display)	AsyncOS for Web 在 Web 界面和 CLI 中使用的语言。
登录页面	用户登录到设备后显示的页面。
显示的报告时间范围 (Reporting Time Range Displayed)（默认）	“报告 (Reporting)”选项卡上为报告显示的默认时间范围。
显示的报告行数 (Number of Reporting Rows Displayed)	默认情况下为每份报告显示的数据行数。

步骤 5 提交并确认更改。

步骤 6 点击页面底部的**返回上一页 (Return to previous page)** 链接。

覆盖 Internet Explorer 兼容模式

为了使 Web 界面呈现更好的效果，思科建议您启用 Internet Explorer 兼容模式覆盖。

注释 如果启用此功能违反了您的组织策略，可以将其禁用。

步骤 1 依次点击**系统管理 (System Administration)** > **常规设置 (General Settings)**。

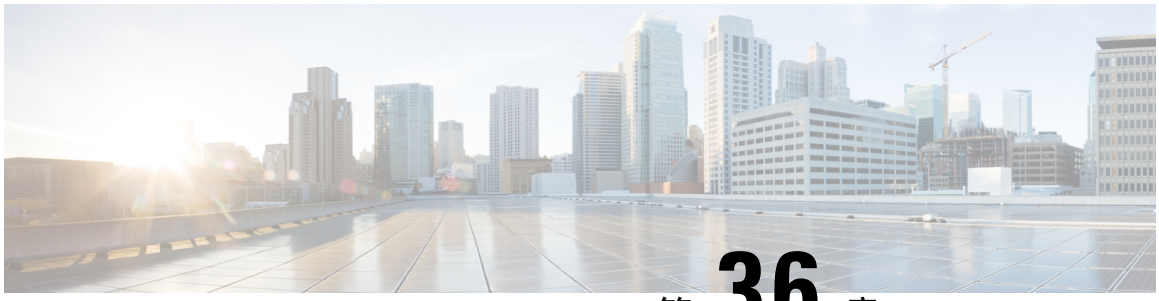
步骤 2 选中**覆盖 IE 兼容模式 (Override IE Compatibility Mode)** 复选框。

步骤 3 提交并确认更改。

配置 HTTP 信头长度的最大值

现在，可以使用 CLI 中的 `adminaccessconfig > maxhttpheaderfieldsize` 命令来配置发送到设备的 HTTP 请求的 HTTP 信头长度最大值。

HTTP 信头字段大小的默认值为 4096 (4 KB)，最大值为 33554432 (32 MB)。



第 36 章

使用 CLI 进行管理和监控

本章包含以下部分：

使用 CLI 进行管理和监控概述

使用 CLI 管理和监控邮件安全设备的过程包含以下类型的任务：

- 监控邮件活动。
  - 设备在邮件管道中处理的邮件、收件人和退回收件人的原始数量。
  - 邮件传送或邮件退回的每小时速率基于过去一分钟、五分钟或 15 分钟时段
- 监控系统资源。示例：
  - 内存使用率
  - 磁盘空间
  - 连接数
- 使用简单网络管理协议 (SNMP) 监控可能的系统功能障碍。示例：
  - 风扇故障
  - 更新失败
  - 异常高的设备温度
- 管理管道中的邮件。示例：
  - 删除队列中的收件人
  - 将邮件重定向到另一台主机
  - 通过删除收件人或重定向邮件清除该队列
  - 暂停或恢复邮件接收、传送或工作队列处理

- 找到特定邮件

读取可用的监控组件

读取事件计数器

计数器提供系统中运行的各个事件的总数。对于每个计数器，可以查看自重置计数器以来、自上次系统重新启动以来以及在系统的整个生命周期中生成的事件总数。

每次发生事件时的计数器增量，其通过三个版本显示：

重置	自上次通过 resetcounters 命令重置计数器
正常运行时间	自上次系统重新启动
使用时间	在思科设备整个生命周期中的总计

下表列出了在监控思科设备时可用的计数器及其说明。

注释 这是完整的列表。显示的计数器因所选的显示选项或命令而异。此列表仅供参考。

表 *94:* 计数器

统计	说明
接受	在接收队列中接收的邮件。
接收的邮件数量	
已经接收的收件人数量	所有已接收邮件的收件人。
生成的退回收件人数量	系统为其生成退回并将其插入传送队列中的收件人。
拒绝	由于收件人访问表 (RAT) 或意外协议协商（包括过早出现连接终止）而被拒绝接收到传送队列的收件人。
拒绝的收件人数量	
删除的邮件数量	由于过滤器删除操作条件匹配或已被 Black Hole 排队侦听程序接收而被拒绝接收到传送队列中的邮件。定向到别名表中的 /dev/null 条目的邮件也被视为丢弃的邮件。被反垃圾邮件过滤功能（如果已在系统中启用）删除的邮件也会记入此计数器。
队列	

统计	说明
软退回事件的数量	软退回事件的数量 - 多次软退回的邮件具有多个软退回事件。
完成	全部硬退回的收件人、已传送收件人和已删除收件人的总计。从传送队列中删除的任何收件人。
已经完成的收件人数量	
硬退回的收件人	所有 DNS 硬退回、5XX 硬退回、过滤器硬退回、到期硬退信和其他硬退回的总计。将邮件传送给收件人的尝试失败，导致传送立即终止。
DNS 硬退回	尝试将邮件传送给收件人时遇到的 DNS 错误。
5XX 硬退回	当尝试将邮件传送给收件人时，目标邮件服务器返回“5XX”响应代码。
过期的硬退回	超出传送队列中允许的最长时间或最大连接尝试次数的邮件收件人。
内容过滤的硬退回	收件人传送已被匹配的过滤器bounce操作预占。被反垃圾邮件过滤功能（如果已在系统中启用）删除的邮件也会记入此计数器。
其他硬退回	在邮件传送或通过 bouncerecipients 命令明确退回邮件收件人期间出现的意外错误。
发送的收件人数量	邮件已成功传送给收件人。
已删除的收件人	通过 deleterecipients 命令明确删除的邮件收件人总数或全局取消订用命中数。
全局取消订用命中数	邮件收件人因匹配全局取消订用设置而被删除。
当前的 ID	分配给插入传送队列中的邮件的最后一个邮件ID。MID与思科设备接收到的每封邮件关联，并可在邮件日志中进行跟踪。MID 会在 231 处重置为零。
邮件ID(MID)	
注入连接 ID (ICID)	分配给侦听程序接口连接的最后注入连接 ID 。ICID 会在 231 处回滚（重置为零）。
传送连接 ID (DCID)	已分配给目标邮件服务器连接的最后传送连接 ID。DCID 会在 231 处回滚（重置为零）。

读取系统计量器

计量器会显示系统资源（如内存、磁盘空间或活动连接）的当前利用率。

下表列出了在监控设备时可用的计量器及其说明。

注释 这是完整的列表。显示的计量器因所选的显示选项或命令而异。此列表仅供参考。

表 *95:* 规格

统计	说明
系统计量器	
内存使用率	系统使用的物理随机访问内存的百分比。
CPU使用率	CPU 使用率百分比
硬盘 I/O 使用率	使用的磁盘 I/O 的百分比。 注释 磁盘I/O利用率计量器不根据已知值的比例显示读数。相反，它会显示到目前为止系统发现的 I/O 利用率，并且根据上次重新启动以来的最大值进行调整。因此，如果计量器显示 100%，则表示系统达到启动以来最高级别的 I/O 利用率（不一定表示使用了整个系统 100% 的物理磁盘 I/O）。
保留资源	介于 0 和 60 或 999 之间的值。介于 0 和 60 之间的数字表示系统降低其接受邮件的程度，从而避免快速消耗关键系统资源。数字越高表示减少接受的程度越大。零表示不降低接受程度。如果此计量器显示999，则系统已进入“资源节约模式”，不会接受任何邮件。每当系统进入或退出资源节约模式时，都会发送警报邮件。
磁盘利用率：日志	用于日志的磁盘百分比，在状态日志中显示为 LogUsd，而在 XML 状态中显示为 log_used。
连接计量器	
当前的入站连接数	侦听程序接口的当前入站连接数。
当前的出站连接数	与目标邮件服务器的当前出站连接。
队列计量器	
正在处理的收件人	传送队列中的邮件收件人。未尝试发送的收件人和已尝试发送过的收件人的总计。

统计	说明
未尝试发送的收件人	有效收件人的子类别。队列中未尝试向其传送的邮件收件人。
已经尝试发送过的收件人	有效收件人的子类别。队列中已尝试向其传送单位由于软退回事件而失败的邮件收件人。
工作队列中的邮件数量	在排队之前，等待由别名表扩展、伪装、反垃圾邮件、防病毒扫描、邮件过滤器和 LDAP 查询处理邮件数量。
隔离区中的邮件	任何隔离区中的独特邮件数量，加上已释放或删除但尚未执行操作的邮件。例如，如果释放病毒爆发中的所有隔离邮件，则病毒爆发的邮件总数将立即变为零，但是，此字段仍会反映隔离的邮件，直到传送所有这些邮件。
内存中的目标	内存中的目标域数量。对于具有需要传送的邮件的每个域，将在内存中创建目标对象。在传送了该域的所有邮件后，会将目标对象再保留 3 个小时。在 3 小时后，如果没有任何新邮件发往该域，则该对象将过期，因此不再报告该目标（例如，在 tophosts 命令中）。如果仅将邮件传送到一个域，此计数器将为“1”。如果您从未收到或发送任何邮件（或设备在数小时内未处理任何邮件），则计数器将为“0”。 如果使用虚拟网关，则每个虚拟网关的目标域都将具有单独的目标对象。（例如，如果从 3 个不同的虚拟网关传送到 yahoo.com，yahoo.com 将统计为 3 个目标对象 ）。
K字节已使用	已使用的队列存储（按 KB 计）。
隔离区中的 KB 数	用于隔离的邮件的队列存储。该值的计算方式为：邮件大小加上每个收件人对应的30字节，并且根据上面统计的“隔离区中的邮件”进行求和。请注意，此计算通常会过高估计使用的空间。
K字节(空闲的)	剩余的队列存储（按 KB 计）。

读取已传送和已退回邮件的速率

所有速率均显示为在进行查询的特定时间点，每小时发生某个事件的平均速率。将为三个时间间隔计算速率：过去一 (1) 分钟、过去五 (5) 分钟和过去十五 (15) 分钟内的每小时平均速率。

例如，如果思科设备在 1 分钟内接收 100 个收件人，则这 1 分钟间隔的速率将是每小时 6,000。5 分钟间隔的速率为每小时 1,200 个，而 15 分钟的速率为每小时 400 个。计算速率以指示当一分钟时段的速率继续时，该小时的平均速率是什么。因此，每分钟 100 封邮件会产生比 15 分钟 100 封邮件更高的速率。

下表列出了在监控思科设备时可用的速率及其说明。

注释 这是完整的列表。显示的速率因所选的显示选项或命令而异。此列表仅供参考。

表 *96:* 比率

统计	说明
接收的邮件数量	每小时将邮件插入传送队列的速率。
已经接收的收件人数量	每小时插入传送队列的所有邮件的收件人数的速率。
软退回事件的数量	每小时软退回事件数量的速率。（软退回多次的邮件具有多个软退回事件。）
已经完成的收件人数量	全部硬退回的收件人数量、已传送收件人和已删除收件人的总计的速率。从传送队列中删除的任何收件人都被视为已完成。
硬退回的收件人	每小时内所有 DNS 硬退回、5XX 硬退回、过滤器硬退回、到期硬退回和其他硬退回的总计的速率。导致传送立即终止的将邮件传送给收件人尝试失败被视为硬退回。
发送的收件人数量	每小时成功将邮件发送给收件人的速率。

使用 CLI 监控

监控邮件状态

您可能想要监控思科设备上邮件操作的状态。status 命令将返回监控到的有关邮件操作的信息子集。统计数据以下列两种形式中的一种返回：计数器和计量器。计数器提供系统中运行的各个事件的总数。对于每个计数器，您可以查看自计数器重置以来、自系统上次重新引导以来以及在系统的整个生命周期所发生的事件总数。计量器会显示系统资源（如内存、磁盘空间或活动连接）的当前利用率。

有关每个项目的说明，请参阅使用 CLI 进行管理和监控概述 ， 第 805 页。

表 *97:* 邮件状态

统计	说明
状态时间	显示当前系统时间和日期。
上次重置计数器	显示上次重置计数器的时间。
系统状态	在线、离线、接收暂停或传送暂停。请注意，仅当暂停所有侦听程序时，状态才会成为“接收暂停”。当所有侦听程序的接收和传送均暂停时，状态成为“离线”。

统计	说明
时间最长的邮件	显示等待由系统传送的最早邮件。
功能	显示通过 featurekey 命令在系统上安装的任何特殊功能。

示例

```
mail3.example.com> status

Status as of:              Thu Oct 21 14:33:27 2004 PDT
Up since:                    Wed Oct 20 15:47:58 2004 PDT (22h 45m 29s)
Last counter reset:        Never
System status:             Online
Oldest Message:             4 weeks 46 mins 53 secs
Counters:                     Reset          Uptime        Lifetime
  Receiving
    Messages Received      62,049,822         290,920      62,049,822
    Recipients Received    62,049,823         290,920      62,049,823
  Rejection
    Rejected Recipients     3,949,663          11,921       3,949,663
    Dropped Messages       11,606,037             219      11,606,037
  Queue
    Soft Bounced Events     2,334,552          13,598       2,334,552
  Completion
    Completed Recipients   50,441,741         332,625      50,441,741
  Current IDs
    Message ID (MID)                                      99524480
    Injection Conn. ID (ICID)                             51180368
    Delivery Conn. ID (DCID)                              17550674
Gauges:                                 Current
  Connections
    Current Inbound Conn.                     0
    Current Outbound Conn.                   14
  Queue
    Active Recipients                     7,166
    Messages In Work Queue                    0
    Messages In Quarantine               16,248
    Kilobytes Used                      387,143
      Kilobytes In Quarantine           338,206
    Kilobytes Free                   39,458,745
mail3.example.com>
```

监控详细的邮件状态

status detail 命令返回有关邮件操作的完整受监控信息。返回的统计数据以下列三种类别中的一种返回：计数器、速率和计量器。计数器提供系统中运行的各个事件的总数。对于每个计数器，可以查看自重置计数器以来、自上次系统重新启动以来以及在系统的整个生命周期中生成的事件总数。计量器会显示系统资源（如内存、磁盘空间或活动连接）的当前利用率。所有速率均显示为在进行查询的特定时间点，每小时发生某个事件的平均速率。将为三个时间间隔计算速率：过去一 (1) 分钟、过去五 (5) 分钟和过去十五 (15) 分钟内的每小时平均速率。有关每个项目的说明，请参阅使用 CLI 进行管理和监控概述 ， 第 805 页。

示例

```
mail3.example.com> status detail
Status as of:           Thu Jun 30 13:09:18 2005 PDT
Up since:               Thu Jun 23 22:21:14 2005 PDT (6d 14h 48m 4s)
Last counter reset:            Tue Jun 29 19:30:42 2004 PDT
System status:                 Online
Oldest Message:                No Messages
Feature - IronPort Anti-Spam:  17 days
Feature - Sophos:              Dormant/Perpetual
Feature - Outbreak Filters: Dormant/Perpetual
Feature - Central Mgmt:        Dormant/Perpetual
Counters:                       Reset          Uptime        Lifetime
  Receiving
    Messages Received       2,571,967          24,760       3,113,176
    Recipients Received     2,914,875          25,450       3,468,024
    Gen. Bounce Recipients      2,165               0           7,451
  Rejection
    Rejected Recipients     1,019,453             792       1,740,603
    Dropped Messages        1,209,001              66       1,209,028
  Queue
    Soft Bounced Events        11,236               0          11,405
  Completion
    Completed Recipients    2,591,740          49,095       3,145,002
      Hard Bounced Recipients   2,469               0           7,875
        DNS Hard Bounces          199               0           3,235
        5XX Hard Bounces        2,151               0           4,520
        Expired Hard Bounces      119               0             120
        Filter Hard Bounces         0               0               0
        Other Hard Bounces          0               0               0
      Delivered Recipients  2,589,270          49,095       3,137,126
      Deleted Recipients            1               0               1
        Global Unsub. Hits          0               0               0
    DomainKeys Signed Msgs         10               9              10
  Current IDs
    Message ID (MID)                                          7615199
    Injection Conn. ID (ICID)                                 3263654
    Delivery Conn. ID (DCID)                                  1988479
Rates (Events Per Hour):      1-Minute       5-Minutes      15-Minutes
  Receiving
    Messages Received             180             300             188
    Recipients Received           180             300             188
  Queue
    Soft Bounced Events             0               0               0
  Completion
    Completed Recipients          360             600             368
      Hard Bounced Recipients       0               0               0
      Delivered Recipients        360             600             368
Gauges:                              Current
  System
    RAM Utilization                       1%
    CPU Utilization
      MGA                                 0%
      AntiSpam                            0%
      AntiVirus                           0%
    Disk I/O Utilization                  0%
    Resource Conservation                 0
  Connections
    Current Inbound Conn.                 0
    Current Outbound Conn.                0
  Queue
    Active Recipients                     0
      Unattempted Recipients              0
```

```
  Attempted Recipients                0
Messages In Work Queue                0
Messages In Quarantine               19
Destinations In Memory                3
Kilobytes Used                      473
  Kilobytes In Quarantine           473
Kilobytes Free                39,845,415
```

注释 新安装的设备中可能存在这样的情况：最早的邮件计数器显示邮件，但是实际上计数器中未显示任何收件人。如果远程主机正在连接且接收邮件的速度非常缓慢（即接收一封邮件需花费数分钟的时间），您可能会发现收件人接收的计数器显示“0”，但是最早的邮件计数器显示“1”。这是因为最早的邮件计数器会显示正在进行的邮件。如果连接最终断开，则会重置计数器。

监控邮件主机的状态

如果您怀疑特定收件人主机存在传送问题或要在虚拟网关地址上收集信息，则hoststatus 命令会显示此信息。hoststatus 命令会返回有关与特定收件人主机相关的邮件操作的监控信息。该命令要求您输入要返回的主机信息的域。此外还提供在 AsyncOS 缓存中存储的 DNS 信息以及从收件人主机返回的最后一个错误。返回的数据是从上一个 resetcounters 命令运行以来累加的。返回的统计数据以下列两种类别显示：计数器和计量器。有关每个项目的说明，请参阅使用 CLI 进行管理和监控概述，第 805 页。

此外，还会返回特定于 hoststatus 命令的其他数据。

表 *98: hoststatus* 命令中的其他数据

统计	说明
挂起的出站连接	与目标邮件主机的挂起或“起始”连接，与开放和有效连接相对。挂起的出站连接是尚未到达协议问候阶段的连接。
时间最长的邮件	此域传送队列中最早有效收件人的时限。此计数器对于确定邮件在队列中由于软退回事件和/或关闭的主机而无法传送的时间非常有用。
最后的行为	每次尝试向该主机传送邮件时，此字段便会更新。
已排序的 IP 地址	此字段包含 IP 地址的 TTL（生存时间）、根据 MX 记录的首选项以及实际地址。MX 记录会指定域的邮件服务器 IP 地址。域可以具有多个 MX 记录。每个 MX 记录邮件服务器均分配有优先级。具有最低优先级数字的 MX 记录将成为首选项。
最后的 5XX 错误	此字段包含主机返回的最新“5XX”状态代码和说明。该项仅在存在 5XX 错误时显示。
MX 记录	MX 记录会指定域的邮件服务器 IP 地址。域可以具有多个 MX 记录。每个 MX 记录邮件服务器均分配有优先级。最有最低优先级数字的 MX 记录将成为首选项。

统计	说明
此主机的 SMTP 路由	如果为此域定义了 SMTP 路由，它们将列出在此处。
最后的 TLS 错误	此字段包含有关最近外发 TLS 连接错误的说明以及设备尝试建立的 TLS 连接类型。仅当出现 TLS 错误时，才会显示该信息。

虚拟网关

仅当设置了虚拟网关地址时，才会显示以下虚拟网关信息（请参阅配置网关以接收邮件，第 61 页）。

表 *99: hoststatus* 命令中的其他虚拟网关数据

统计	说明
主机 up/down	与同名全局 hoststatus 字段具有相同的定义 - 根据虚拟网关地址跟踪。
最后的行为	与同名全局 hoststatus 字段具有相同的定义 - 根据虚拟网关地址跟踪。
接管者	此字段还对应与全局 hoststatus 命令相同的定义。有效收件人字段 - 按虚拟网关地址跟踪。
最后的 5XX 错误	此字段包含主机返回的最新 5XX 状态代码和说明。该项仅在存在 5XX 错误时显示。

示例

```
mail3.example.com> hoststatus

Recipient host:
[]> aol.com
Host mail status for: 'aol.com'
Status as of:          Tue Mar 02 15:17:32 2010
Host up/down:         up
Counters:
  Queue
    Soft Bounced Events                        0
  Completion
    Completed Recipients                       1
      Hard Bounced Recipients                  1
        DNS Hard Bounces                       0
        5XX Hard Bounces                       1
        Filter Hard Bounces                    0
        Expired Hard Bounces                   0
        Other Hard Bounces                     0
      Delivered Recipients                     0
      Deleted Recipients                       0
Gauges:
  Queue
    Active Recipients                          0
      Unattempted Recipients                   0
      Attempted Recipients                     0
```

```
    Connections
      Current Outbound Connections              0
      Pending Outbound Connections              0
Oldest Message         No Messages
Last Activity          Tue Mar 02 15:17:32 2010
Ordered IP addresses: (expiring at Tue Mar 02 16:17:32 2010)
    Preference   IPs
    15           64.12.137.121    64.12.138.89     64.12.138.120
    15           64.12.137.89     64.12.138.152    152.163.224.122
    15           64.12.137.184    64.12.137.89     64.12.136.57
    15           64.12.138.57     64.12.136.153    205.188.156.122
    15           64.12.138.57     64.12.137.152    64.12.136.89
    15           64.12.138.89     205.188.156.154  64.12.138.152
    15           64.12.136.121    152.163.224.26   64.12.137.184
    15           64.12.138.120    64.12.137.152    64.12.137.121
MX Records:
    Preference   TTL        Hostname
    15           52m24s     mailin-01.mx.aol.com
    15           52m24s     mailin-02.mx.aol.com
    15           52m24s     mailin-03.mx.aol.com
    15           52m24s     mailin-04.mx.aol.com
    Last 5XX Error:
    ----------
    550 REQUESTED ACTION NOT TAKEN: DNS FAILURE
 (at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10
    ----------
Last TLS Error:             Required - Verify
    ----------
    TLS required, STARTTLS unavailable
    (at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10
Virtual gateway information:
============================================================
example.com (PublicNet_017):
    Host up/down:         up
    Last Activity         Wed June 22 13:47:02 2005
    Recipients            0
```

注释 仅在使用 altsrchost 功能时，才会显示虚拟网关地址信息。

确定邮件队列的组成

要获取有关邮件队列的即时信息并确定特定收件人主机是否存在传送问题（例如队列组成），请使用 tophosts 命令。tophosts 命令将返回队列中前 20 个收件人主机的列表。可以按不同的统计数据排列该列表，包括有效收件人、输出连接、传送的收件人、软退回事件和硬退回的收件人。有关每个项目的说明，请参阅使用 CLI 进行管理和监控概述，第 805 页。

示例

```
mail3.example.com> tophosts

Sort results by:
1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Soft Bounced Events
```

```
5. Hard Bounced Recipients
[1]> 1
Status as of:         Mon Nov 18 22:22:23 2003
                    Active    Conn.   Deliv.   Soft      Hard
#  Recipient Host   Recip     Out     Recip.   Bounced   Bounced
1  aol.com          365       10      255      21         8
2  hotmail.com      290        7      198      28        13
3  yahoo.com        134        6      123      11        19
4  excite.com        98        3       84       9         4
5  msn.com           84        2       76      33        29
mail3.example.com>
```

显示实时活动

思科设备提供实时监控功能，以便查看系统中邮件活动的进度。rate 命令会返回有关邮件操作的实时监控信息。信息按您指定的时间间隔定期更新。使用 Ctrl+C 组合键可停止 **rate** 命令。

该数据显示在下表中：

表 *100: rate* 命令中的数据

统计	说明
输入连接数	入站连接的数量。
出去的TCP连接数	出站连接的数量。
已经接收的收件人数量	系统中接收的收件人总数。
完成的收件人	完成的收件人总数。
Delta	自上次数据更新以来，已接收收件人与已完成收件人之间的差异。
使用的队列	邮件队列的大小（以 KB 计）。

示例

```
mail3.example.com> rate

Enter the number of seconds between displays.
[10]> 1
Hit Ctrl-C to return to the main prompt.
Time     Connections Recipients          Recipients               Queue
             In   Out   Received    Delta  Completed    Delta     K-Used
23:37:13    10     2   41708833        0   40842686        0         64
23:37:14     8     2   41708841        8   40842692        6        105
23:37:15     9     2   41708848        7   40842700        8         76
23:37:16     7     3   41708852        4   40842705        5         64
23:37:17     5     3   41708858        6   40842711        6         64
23:37:18     9     3   41708871       13   40842722       11         67
23:37:19     7     3   41708881       10   40842734       12         64
23:37:21    11     3   41708893       12   40842744       10         79
^C
```

hostrate 命令会返回有关特定邮件主机的实时监控信息。此信息是 status detail 命令的子集。（请参阅监控详细的邮件状态，第 811 页。）

表 *101: hostrate* 命令中的数据

统计	说明
主机状态	特定主机的当前状态：up、down 或 unknown。
当前输出连接数	当前与主机的出站连接数量。
队列中正在处理的收件人	队列中发送到特定主机的有效收件人总数。
队列中正在处理的收件人增量	自上次已知主机状态以来，队列中发送到特定主机的有效收件人总数的差异。
传送的收件人增量	自上次已知主机状态以来，队列中发送到特定主机的已传送收件人总数的差异。
硬退回收件人增量	自上次已知主机状态以来，队列中发送到特定主机的硬退回收件人总数的差异。
软退回事件增量	自上次已知主机状态以来，队列中发送到特定主机的软退回收件人总数的差异。

使用 Ctrl+C 组合键可停止 hostrate 命令。

示例

```
mail3.example.com> hostrate
Recipient host:
[]> aol.com
Enter the number of seconds between displays.
[10]> 1
    Time   Host  CrtCncOut  ActvRcp ActvRcp  DlvRcp HrdBncRcp SftBncEvt
           Status                    Delta   Delta     Delta     Delta
23:38:23       up          1         0       0         4         0         0
23:38:24       up          1         0       0         4         0         0
23:38:25       up          1         0       0        12         0         0
^C
```

监控入站邮件连接

您可能希望监控连接到思科设备的主机，以识别大量发件人或对系统的入站连接进行故障排除。topin 命令提供连接到系统的远程主机的快照。它会显示一个表，其中每个行对应连接到特定侦听程序的每个远程 IP 地址。从同一 IP 地址到不同侦听程序的两个连接会在下表中产生 2 个行，该表描述了使用 topin 命令时显示的字段。

表 *102: topin* 命令中的数据

统计	说明
远程主机名	远程主机的主机名，衍生自反向 DNS 查找。
远程 IP 地址	远程主机的 IP 地址。
监听程序	接收连接的设备上侦听程序的昵称。
入站连接数量	在命令运行时打开的来自具有指定IP地址的远程主机的并发连接数。

系统会执行反向 DNS 查找来查找远程主机名，然后执行正向 DNS 查找来验证该名称。如果正向查找不会产生原始 IP 地址，或者如果反向 DNS 查找失败，则该表会在主机名列中显示 IP 地址。有关发件人验证过程的详细信息，请参阅验证发件人，第 102 页。

示例

```
mail3.example.com> topin

Status as of:                  Sat Aug 23 21:50:54 2003
#  Remote hostname             Remote IP addr.   listener        Conn. In
1  mail.remotedomain01.com     172.16.0.2        Incoming01            10
2  mail.remotedomain01.com     172.16.0.2        Incoming02            10
3  mail.remotedomain03.com     172.16.0.4        Incoming01             5
4  mail.remotedomain04.com     172.16.0.5        Incoming02             4
5  mail.remotedomain05.com     172.16.0.6        Incoming01             3
6  mail.remotedomain06.com     172.16.0.7        Incoming02             3
7  mail.remotedomain07.com     172.16.0.8        Incoming01             3
8  mail.remotedomain08.com     172.16.0.9        Incoming01             3
9  mail.remotedomain09.com     172.16.0.10       Incoming01             3
10 mail.remotedomain10.com     172.16.0.11       Incoming01             2
11 mail.remotedomain11.com     172.16.0.12       Incoming01             2
12 mail.remotedomain12.com     172.16.0.13       Incoming02             2
13 mail.remotedomain13.com     172.16.0.14       Incoming01             2
14 mail.remotedomain14.com     172.16.0.15       Incoming01             2
15 mail.remotedomain15.com     172.16.0.16       Incoming01             2
16 mail.remotedomain16.com     172.16.0.17       Incoming01             2
17 mail.remotedomain17.com     172.16.0.18       Incoming01             1
18 mail.remotedomain18.com     172.16.0.19       Incoming02             1
19 mail.remotedomain19.com     172.16.0.20       Incoming01             1
20 mail.remotedomain20.com     172.16.0.21       Incoming01             1
```

检查 DNS 状态

dnsstatus 命令会返回一个计数器，以显示 DNS 查找统计数据和缓存信息。对于每个计数器，可以查看自上次重置计数器以来、自上次系统重新启动以来以及在系统生命周期中的事件总数。

下表列出了可用的计数器。

表 *103: dnsstatus* 命令中的数据

统计	说明
DNS 请求	发送到用于解析域名的系统 DNS 缓存的顶级非递归请求。
网络请求数	发送到用于检索 DNS 信息的网络（非本地）的请求。
缓存命中数	发送到在其中找到并返回记录的 DNS 缓存的请求。
缓存丢失数	发送到在其中未找到记录的 DNS 缓存的请求。
缓存排斥数	发送到在其中找到记录但域未知的 DNS 缓存的请求。
缓存过期	发送到在其中找到记录的 DNS 缓存的请求。 在缓存中，考虑使用，并且由于过于陈旧而放弃。 许多条目可存在于缓存中，即使它们的生存时间 (TTL) 已过也是如此。只要这些条目未使用，它们就不会包含在到期计数器中。当清理缓存时，有效和无效（过旧）条目都会被删除。刷新操作不会更改到期计数器。

示例

```
mail3.example.com> dnsstatus
Status as of: Sat Aug 23 21:57:28 2003
Counters:                    Reset          Uptime        Lifetime
  DNS Requests         211,735,710       8,269,306     252,177,342
  Network Requests     182,026,818       6,858,332     206,963,542
  Cache Hits           474,675,247      17,934,227     541,605,545
  Cache Misses         624,023,089      24,072,819     704,767,877
  Cache Exceptions      35,246,211       1,568,005      51,445,744
  Cache Expired            418,369           7,800         429,015
mail3.example.com>
```

重置邮件监控计数器

resetcounters 命令会重置累加的邮件监控计数器。重置会影响全局计数器以及每个主机计数器。重置不会影响与重试计划相关的传送队列中的邮件计数器。

注释 还可以在 GUI 中重置计数器。请参阅“系统状态”页面，第 662 页。

示例

```
mail3.example.com> resetcounters
Counters reset: Mon Jan 01 12:00:01 2003
```

识别有效的 TCP/IP 服务

要识别邮件安全设备使用的有效 TCP/IP 服务，请在命令行界面中使用 tcpservices 命令。

管理邮件队列

通过思科 AsyncOS，可以对邮件队列中的邮件执行操作。可以删除、退回、暂停或重定向邮件队列中的邮件。还可以找到、删除和存档队列中的旧邮件。

删除队列中的收件人

如果不希望传送给特定收件人或要清除邮件队列，请使用 deleterecipients 命令。deleterecipients 命令支持通过删除等待传送的特定收件人来管理邮件传送队列。要删除的收件人将通过作为收件人目标的收件人主机或邮件发件人（由邮件信封的“信封发件人”(Envelope From) 行中指定的特定地址确定）来识别。此外，可以同时删除传送队列中的所有邮件。

注释 要执行 deleterecipients 功能，建议将思科设备置于离线状态或暂停传送（请参阅暂停邮件接收和传送，第 750 页）。

注释 尽管该功能在所有状态下均受支持，但是在执行该功能期间可能会传送一些邮件。

收件人主机和发件人的匹配必须是完全相同的字符串匹配。不接受通配符。deleterecipients 命令会返回已删除邮件的总数。此外，如果配置了邮件日志订用（仅限 IronPort 文本格式，则邮件删除事件会记录为单独的行。

示例

```
mail3.example.com> deleterecipients
Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]>
```

思科设备为您提供了根据需要删除收件人的选项。以下示例显示按收件人主机删除收件人、按信封发件人地址删除收件人以及删除队列中的所有收件人。

按收件人域删除

```
Please enter the hostname for the messages you wish to delete.
[]> example.com
Are you sure you want to delete all messages being delivered to "example.com"? [N]> Y
Deleting messages, please wait.
100 messages deleted.
```

按 Envelope From 地址删除

```
Please enter the Envelope From address for the messages you wish to delete.
[]> mailadmin@example.com
Are you sure you want to delete all messages with the Envelope From address of
"mailadmin@example.com"? [N]> Y
Deleting messages, please wait.
100 messages deleted.
```

全部删除

```
Are you sure you want to delete all messages in the delivery queue (all active recipients)?
 [N]> Y
Deleting messages, please wait.
1000 messages deleted.
```

退回队列中的收件人

与 deleterecipients 命令一样，bouncerecipients 命令允许通过硬退回等待传送的特定收件人来管理邮件传送队列。邮件退回遵循在 bounceconfig 命令中指定的常规退回邮件配置。

注释 要执行 bouncerecipients 功能，建议将思科设备置于离线或暂停传送状态（请参阅暂停邮件接收和传送，第 750 页）。

注释 尽管该功能在所有状态下均受支持，但是在执行该功能期间可能会传送一些邮件。

收件人主机和发件人的匹配必须是完全相同的字符串匹配。不接受通配符。bouncerecipients 命令会返回退回邮件的总数。

注释 bouncerecipients 功能是资源密集型，可能需要几分钟才能完成。如果处于离线或暂停传送状态，则仅在通过 resume 命令将思科 AsyncOS 恢复为在线状态之后，才会开始退回邮件的实际发送（如果开启硬退回生成）。

示例

```
mail3.example.com> bouncerecipients
Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]>
```

目标收件人主机或邮件信封的信封发件人行所示的特定地址识别的邮件发件人可对要退回的收件人进行识别。或者，传送队列中的所有邮件都可以立即退回。

按收件人主机退回

```
Please enter the hostname for the messages you wish to bounce.
[]> example.com
Are you sure you want to bounce all messages being delivered to "example.com"? [N]> Y
Bouncing messages, please wait.
100 messages bounced.
```

按 Envelope From 地址退回

```
Please enter the Envelope From address for the messages you wish to bounce.
[]> mailadmin@example.com
Are you sure you want to bounce all messages with the Envelope From address of
"mailadmin@example.com"? [N]> Y
Bouncing messages, please wait.
100 messages bounced.
```

全部退回

```
Are you sure you want to bounce all messages in the queue? [N]> Y
Bouncing messages, please wait.
1000 messages bounced.
```

重定向队列中的邮件

redirectrecipients 命令允许邮件传送队列中的所有邮件重定向至另一个中继主机。请注意，将收件人重定向至未准备好从此主机接受大量 SMTP 邮件的主机或 IP 地址会导致退回邮件，并且可能导致邮件丢失。

注意 将邮件重定向至以 /dev/null 作为其目标的接收域会导致丢失邮件。如果将邮件定向至此类域，则 CLI 不会显示警告。在重定向邮件之前，请检查接收域的 SMTP 路由。

示例

以下示例会将所有邮件定向至 example2.com 主机。

```
mail3.example.com> redirectrecipients
Please enter the hostname or IP address of the machine you want to send all mail to.
[]> example2.com
WARNING: redirecting recipients to a host or IP address that is not prepared to accept large
 volumes of SMTP mail from this host will cause messages to bounce and possibly result in
the loss of mail.
Are you sure you want to redirect all mail in the queue to "example2.com"? [N]> y
Redirecting messages, please wait.
246 recipients redirected.
```

根据队列中的收件人显示邮件

使用 showrecipients 命令按收件人主机或信封发件人地址显示邮件传送队列中的邮件。还可以显示队列中的所有邮件。

示例

```
mail3.example.com> showrecipients
Please select how you would like to show messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 3
Showing messages, please wait.
MID/     Bytes/    Sender/                 Subject
[RID]    [Atmps]   Recipient
1527     1230      user123456@ironport.com Testing
[0]      [0]       9554@example.com
1522     1230      user123456@ironport.com Testing
[0]      [0]       3059@example.com
1529     1230      user123456@ironport.com Testing
[0]      [0]       7284@example.com
1530     1230      user123456@ironport.com Testing
[0]      [0]       8243@example.com
1532     1230      user123456@ironport.com Testing
[0]      [0]       1820@example.com
1531     1230      user123456@ironport.com Testing
[0]      [0]       9595@example.com
1518     1230      user123456@ironport.com Testing
[0]      [0]       8778@example.com
1535     1230      user123456@ironport.com Testing
[0]      [0]       1703@example.com
1533     1230      user123456@ironport.com Testing
[0]      [0]       3052@example.com
1536     1230      user123456@ironport.com Testing
[0]      [0]       511@example.com
```

以下示例显示了队列中所有收件人主机的邮件。

暂停邮件传送

要临时暂停邮件传送以进行维护或故障排除，请使用 suspenddel 命令。suspenddel 命令将思科 AsyncOS 置为暂停传送状态。此状态具有以下特征：

- 停止出站邮件传送。
- 接受入站邮件连接。
- 继续日志传输。
- CLI 保持可访问。

suspenddel 命令可使打开的出站连接关闭，并阻止打开任何新的连接。suspenddel 命令会立即开始，并允许成功关闭任何已建立的连接。使用 resumedel 命令从暂停传送状态恢复为正常操作。

注释 在系统重新启动过程中会保留“传送暂停”状态。如果使用 suspenddel 命令，然后重新启动设备，则必须在重新启动后使用 resumedel 命令恢复传送。

示例

```
mail3.example.com> suspenddel
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
```

恢复邮件传送

resumedel 命令会在使用 suspenddel 命令后将思科 AsyncOS 恢复为正常操作状态。

语法

resumedel

```
mail3.example.com> resumedel
Mail delivery resumed.
```

暂停接收邮件

要临时暂停所有侦听程序接收邮件，请使用 suspendlistener 命令。当暂停接收时，系统不会接受与侦听程序特定端口的连接。

此行为在此 AsyncOS 版本中已更改。在以前的版本中，系统会接受连接，做出以下响应并断开连接：

- SMTP: 421 *hostname* Service not available, closing transaction channel
- QMQP: ZService not available

注释 在系统重新启动过程中会保留“接收暂停”状态。如果使用 suspendlistener 命令，然后重新启动设备，则必须使用 resumelistener 命令，然后才使侦听程序恢复接收邮件。

语法

```
suspendlistener mail3.example.com> suspendlistener
Choose the listener(s) you wish to suspend.
Separate multiple entries with commas.
1. All
2. InboundMail
3. OutboundMail
[1]> 1
```

```
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Waiting for listeners to exit...
Receiving suspended.
mail3.example.com>
```

恢复接收邮件

resumelistener 命令会在使用 suspendlistener 命令后将思科 AsyncOS 恢复为正常操作状态。

语法

```
resumelistener
```

```
mail3.example.com> resumelistener
Choose the listener(s) you wish to resume.
Separate multiple entries with commas.
1. All
2. InboundMail
3. OutboundMail
[1]> 1
Receiving resumed.
mail3.example.com>
```

恢复邮件的传送和接收

恢复命令将恢复传送和接收。

语法

```
resume
```

```
mail3.example.com> resume
Receiving resumed.
Mail delivery resumed.
mail3.example.com>
```

安排邮件立即传送

对于安排延迟交付的收件人和主机，可以使用 delivernow 命令立即重试。delivernow 命令允许重新安排立即传送队列中的邮件。记下的所有域和任何已安排或软退回的邮件都会排队以进行立即传送。

可以调用 delivernow 命令用于队列（已安排和活动）中的所有收件人或特定收件人。当选择特定收件人时，必须输入安排立即传送的收件人的域名。系统会匹配整个字符串的字符和长度。

语法

```
delivernow
```

```
mail3.example.com> delivernow
```

```
Please choose an option for scheduling immediate delivery.
1. By recipient host
2. All messages
[1]> 1
Please enter the domain to schedule for immediate delivery.
[]> recipient.example.com
Rescheduling all messages to recipient.example.com for immediate delivery.
mail3.example.com>
```

暂停工作队列

LDAP 收件人访问处理、伪装、LDAP 重新路由、邮件过滤器、反垃圾邮件和防病毒扫描引擎都在“工作队列”中执行。有关处理流程，请参阅配置路由和传送功能，第 523 页，有关“工作队列中的邮件”(Messages in Work Queue) 计量器的说明，请参阅读取系统计量器，第 808 页。可以使用 workqueue 命令手动暂停邮件处理的工作队列部分。

例如，假设要更改 LDAP 服务器配置的配置，而许多邮件都在工作队列中。或许您要从退回转换到根据 LDAP 收件人访问查询来删除邮件。又或许您要暂停队列，同时手动检查最新的防病毒扫描引擎定义文件（通过 antivirusupdate 命令）。通过 workqueue 命令可以暂停和恢复工作队列，以在执行其他配置更改时停止处理。

当暂停和恢复工作队列时，系统会记录事件。例如，

```
Sun Aug 17 20:01:36 2003 Info: work queue paused, 1900 msgs S
Sun Aug 17 20:01:39 2003 Info: work queue resumed, 1900 msgs
```

在以下示例中，工作队列将暂停：

```
mail3.example.com> workqueue
Status as of:  Sun Aug 17 20:02:30 2003 GMT
Status:   Operational
Messages: 1243
Choose the operation you want to perform:
- STATUS - Display work queue status
- PAUSE - Pause the work queue
- RATE - Display work queue statistics over time
[]> pause
Manually pause work queue?  This will only affect unprocessed messages.  [N]> y
Reason for pausing work queue:
[]> checking LDAP server
Status as of:  Sun Aug 17 20:04:21 2003 GMT
Status:   Paused by admin: checking LDAP server
Messages: 1243
```

注释 输入原因是可选的。如果不输入原因，系统会将原因记录为“由用户手动暂停”。

在以下示例中，工作队列将恢复：

```
mail3.example.com> workqueue
Status as of:  Sun Aug 17 20:42:10 2003 GMT
Status:   Paused by admin: checking LDAP server
Messages: 1243
Choose the operation you want to perform:
- STATUS - Display work queue status
```

```
- RESUME - Resume the work queue
- RATE - Display work queue statistics over time
[]> resume
Status:   Operational
Messages: 1243
```

查找并存档较早的邮件

有时，由于无法传送，旧邮件会保留在队列中。您可能希望删除和存档这些邮件。为此，请使用 showmessage CLI 命令显示给定邮件 ID 的邮件。使用 oldmessage CLI 命令显示系统中最早的非隔离邮件。然后，您可以选择性使用 removemessage 安全删除给定邮件 ID 的邮件。此命令仅可删除工作队列、重试队列或目标队列中的邮件。如果邮件不在任何这些队列中，则其无法删除。

您还可以使用 archivemessage[mid] CLI 命令将给定邮件 ID 的邮件存档到配置目录中的 mbox 文件内。

您无法使用 oldmessage 命令获取隔离区中某个邮件的邮件 ID。但是，如果知道邮件 ID，则可以显示或存档指定的邮件。由于邮件不在工作队列、重试队列或目标队列中，因此无法通过 removemessage 命令删除该邮件。

注释 您无法在思科垃圾邮件隔离区中对邮件执行其中任何队列管理命令。

语法

```
archivemessage
```

```
example.com> archivemessage
Enter the MID to archive and remove.
[0]> 47
 MID 47 has been saved in file oldmessage_47.mbox in the configuration directory
example.com>
```

语法

```
oldmessage
```

```
example.com> oldmessage
MID 9: 1 hour 5 mins 35 secs old
Received: from example.com ([172.16.0.102])
  by example.com with SMTP; 14 Feb 2007 22:11:37 -0800
From: user123@example.com
To: 4031@test.example2.com
Subject: Testing
Message-Id: <20070215061136.68297.16346@example.com>
```

跟踪系统中的邮件

findevent CLI 命令可简化使用 onbox 邮件日志文件跟踪系统中的邮件的过程。findevent CLI 命令允许通过搜索邮件ID或根据主题信头、信封发件人或信封收件人匹配的正则表达式来搜索整个邮件日志中的特定邮件。可以显示当前日志文件或所有日志文件的结果，也可以按日期显示日志文件。按日期查看日志文件时，可以指定某个日期或日期范围。

确定要查看其日志的邮件后，findevent命令会显示该邮件ID的日志信息，包括拆分信息（拆分日志邮件、退回和系统生成的邮件）。以下示例显示了 findevent CLI 命令如何跟踪主题信头中包含“Confidential”的邮件的接收和传送情况：

```
example.com>
findevent
Please choose which type of search you want to perform:
1. Search by envelope FROM
2. Search by Message ID
3. Search by Subject
4. Search by envelope TO
[1]> 3
Enter the regular expression to search for.
[]> confidential
Currently configured logs:
1. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to use for message tracking.
[]> 1
Please choose which set of logs to search:
1. All available log files
2. Select log files by date list
3. Current log file
[3]> 3
The following matching message IDs were found. Please choose one to
show additional log information:
1. MID 4 (Tue Jul 31 17:37:35 2007) sales: confidential
[1]> 1
Tue Jul 31 17:37:32 2007 Info: New SMTP ICID 2 interface Data 1 (172.19.1.86) address
10.251.20.180 reverse dns host unknown verified no
Tue Jul 31 17:37:32 2007 Info: ICID 2 ACCEPT SG None match ALL SBRS None
Tue Jul 31 17:37:35 2007 Info: Start MID 4 ICID 2
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 From: <user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 RID 0 To: <ljohnson@example02.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 Subject 'sales: confidential'
Tue Jul 31 17:37:35 2007 Info: MID 4 ready 4086 bytes from <user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 matched all recipients for per-recipient policy DEFAULT
 in the inbound table
Tue Jul 31 17:37:35 2007 Info: ICID 2 close
Tue Jul 31 17:37:37 2007 Info: MID 4 interim verdict using engine: CASE spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 using engine: CASE spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 interim AV verdict using Sophos CLEAN
Tue Jul 31 17:37:37 2007 Info: MID 4 antivirus negative
Tue Jul 31 17:37:37 2007 Info: MID 4 queued for delivery
Tue Jul 31 17:37:37 2007 Info: Delivery start DCID 0 MID 4 to RID [0]
Tue Jul 31 17:37:37 2007 Info: Message done DCID 0 MID 4 to RID [0]
Tue Jul 31 17:37:37 2007 Info: MID 4 RID [0] Response '/null'
Tue Jul 31 17:37:37 2007 Info: Message finished MID 4 done
```

使用 SNMP 监控系统运行状况和状态

AsyncOS 操作系统通过 SNMP（简单网络管理协议）支持系统状态监控。此版本可实现 RFC 1213 和 1907 中定义的 MIB-II 只读子网。（有关 SNMP 的详细信息，请参阅 RFC 1065、1066 和 1067。）请注意：

- 默认情况下，SNMP 已**关闭**。
- 未实施 SNMP SET 操作（配置）。
- AsyncOS 支持 SNMPv1、v2 和 v3。
- 当启用 SNMPv3 时，必需进行邮件身份验证和加密。用于身份验证和加密的密码应不同。加密算法可以是 AES（推荐）或 DES。身份验证算法可以是 SHA-1（推荐）或 MD5。在您下次运行 snmpconfig 命令时，该命令会“记住”您的密码。
- SNMPv3 用户名为：v3get

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 ironport mail.example.com
```

- 如果仅使用 SNMPv1 或 SNMPv2，则必须设置社区字符串。社区字符串的默认值不是 public。
- 对于 SNMPv1 和 SNMPv2，必须指定在其中接受 SNMP GET 请求的网络。
- 要使用陷阱，SNMP 管理器（不包括在 AsyncOS 中）必须正在运行，并且其 IP 地址输入为陷阱目标。（可以使用主机名，但是如果这样，陷阱仅在 DNS 正常运行时才有效。）

使用 snmpconfig 命令以启用并配置设备 SNMP 监控。选择并配置接口的值以后，设备会响应 SNMPv3 GET 请求。这些第 3 版请求必须包含匹配密码。默认情况下，第 1 版和第 2 版请求会被拒绝。如果启用，第 1 版和第 2 版请求必须具有匹配的社区字符串。

MIB 文件

以下思科邮件安全设备的 MIB 文件可在 http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html 找到。使用最新可用的 MIB 文件。

- ASYNCOS-MAIL-MIB.txt - 思科设备的企业 MIB 文件的 SNMPv2 兼容说明。
- AsyncOS-SMI.txt (IRONPORT-SMI.txt) - 一种“管理信息结构”(SMI) 文件，用于定义思科内容安全产品中 ASYNCOS-MAIL-MIB 的角色。

硬件对象

符合智能平台管理接口规格 (IPMI) 的硬件传感器会报告温度、风扇速度以及电源状态等信息。

在问题变得严重之前，轮询硬件状态并识别可能的硬件故障是明智之举。距离临界值 10% 以内的温度可能会产生令人担心的问题。

有关设备电源数量和操作温度范围等信息，请参阅对应您的设备型号的指南。有关硬件指南的位置，请参阅文档，第 8 页。

硬件陷阱

当状态更改时，发送状态更改陷阱。每隔 5 秒发送一次风扇故障和高温陷阱。其他陷阱是故障条件警报陷阱 - 当状态更改（从正常变为故障）时，就会发送一次。

例如，在 C170 设备上，如果达到以下阈值，会发送陷阱：

表 *104: C170* 设备上的硬件陷阱：温度和硬件条件

型号	高温 (CPU)	高温（环境）	高温（背板）	高温（侧板）	风扇故障	电源	RAID	链接
C170	90C	47C	NA	NA	0 RPM	状态更改	状态更改	状态更改

要查看您设备上的可用陷阱和阈值，请从命令行接口运行 snmpconfig 命令。

请注意，故障条件警报陷阱表示单个组件的严重故障，但是可能不会导致整个系统故障。例如，设备上多个风扇或电源中的单个风扇或电源发生故障，而设备仍会继续运行。

相关主题

- 示例：snmpconfig 命令 ，第 830 页

SNMP 陷阱

当满足一个或多个条件时，SNMP 能够发送陷阱或通知来告知管理应用（通常是 SNMP 管理控制台）。陷阱是网络数据包，其中包含与发送陷阱的系统的组件相关的数据。当在 SNMP 代理上满足某个条件时（此情况下是邮件安全设备）就会生成陷阱。在满足条件后，SNMP 代理就会形成 SNMP 数据包并将其发送到运行 SNMP 管理控制台软件的主机。

要启用并配置 SNMP 陷阱，可使用 snmpconfig 命令。

要指定多个陷阱目标：提示陷阱目标时，最多可以输入 10 个逗号分隔的 IP 地址。

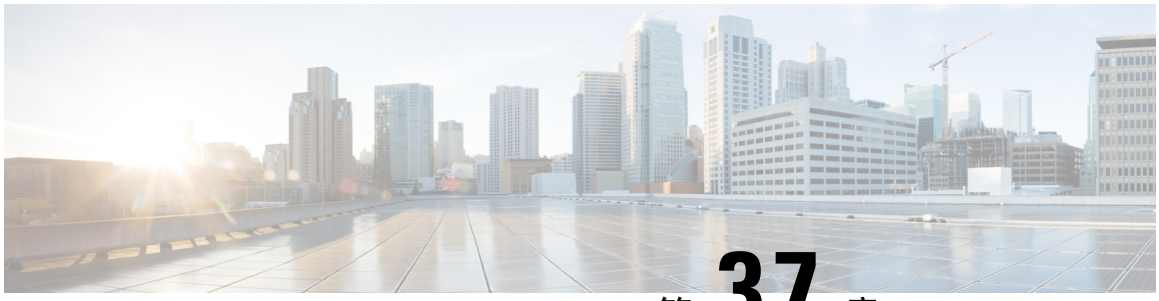
示例：snmpconfig 命令

在以下示例中，snmpconfig 命令用于 C690 硬件设备以在 161 端口上的“PublicNet”接口上启用 SNMP。对 GET 请求输入版本 1 和 2 的社区字符串 public。

```
esa.example.com> snmpconfig
Current SNMP settings:
SNMP Disabled.
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP
Do you want to enable SNMP?
[Y]>
Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: esa.example.com)
[1]>
Which port shall the SNMP daemon listen on interface "Management"?
```

```
[161]>
Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2
Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2
Enter the SNMPv3 authentication passphrase.
[]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[]>
Enter the SNMPv3 privacy passphrase.
[]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[]>
Service SNMP V1/V2c requests?
[N]> Y
Enter the SNMP V1/V2c community string.
[ironport]> public
Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>
From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>
Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 203.0.113.1
Enter the Trap Community string.
[ironport]> tcomm
Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
[N]> Y
Do you want to disable any of these traps?
[Y]> n
Do you want to enable any of these traps?
[Y]> y
Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 1,7,12
What threshold would you like to set for CPU utilization?
[95]>
What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>
What threshold would you like to set for memory utilization?
[95]>
Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3
```

```
Enter the System Contact string.
[snmp@localhost]> esa-admin@example.com
Current SNMP settings:
Listening on interface "Management" 198.51.100.1  port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: esa-admin@example.com
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>
esa.example.com> commit
Please enter some comments describing your changes:
[]> Enable and configure SNMP
Changes committed: Fri Nov 06 18:13:16 2015 GMT
esa.example.com>
```



第 37 章

SenderBase网络参与

本章包含以下部分：

SenderBase 网络参与概述

SenderBase 是一项邮件信誉服务，旨在帮助邮件管理员调查发件人，识别合法的邮件来源并阻止垃圾邮件。

参与 SenderBase 网络的客户允许思科收集有关其组织的邮件流量汇总统计数据，从而提高该服务对所有用户的实用性。参与本着自愿原则。思科仅收集有关邮件属性的摘要数据以及思科设备如何处理不同类型邮件的信息。例如，思科不会收集邮件正文或邮件主题。个人身份信息和可识别组织的信息将予以保密。

与 SenderBase 共享统计数据

步骤 1 依次转到**安全服务 (Security Services) > SenderBase**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 标记复选框，以启用与 SenderBase 信息服务共享统计数据。

选中此复选框，将以全局方式为设备启用该功能。启用后，使用情景自适应扫描引擎(CASE)收集和报告数据（无论是否启用思科反垃圾邮件扫描）。在 CLI 中，使用 **senderbaseconfig** 命令可以配置相同的设置

步骤 4 （可选）启用与 SenderBase 信息服务共享统计数据的代理服务器。

如果定义了代理服务器来检索规则更新，还可以在提供的其他字段中配置连接到代理服务器时通过验证的用户名、密码和特定端口。要编辑这些设置，请参阅配置服务器设置以下载升级和更新， 第 765 页。可以在 CLI 中使用 **senderbaseconfig** 命令配置相同的设置。

常见问题解答

思科了解您的隐私至关重要，因此我们在设计和运行服务时，时刻谨记要保护您的隐私。如果您注册 SenderBase 网络参与，思科将收集有关您组织邮件流量的汇总统计数据，但不会收集或使用任何个人身份信息。思科收集的任何可识别您的用户或组织的信息，都将被视为机密信息。

我为什么应该参与？

参与 SenderBase 网络对我们有帮助，也对您有帮助。要阻止垃圾邮件、病毒和目录搜集攻击等基于邮件的威胁影响您的组织，与我们共享数据就非常重要。例如，在以下情况下，您的参与尤其重要：

- 专门针对您组织的邮件攻击，在这种情况下，您提供的数据是为您提供保护的主要信息来源。
- 您的组织是首批要遭受一种全新全球邮件攻击的袭击的对象之一，在这种情况下，您与我们共享的数据可显著提高我们响应新威胁的速度。

我需要共享哪些数据？

数据是有关邮件属性及思科设备处理不同类型邮件的方式的汇总信息。我们不收集邮件的完整正文。同样，提供给思科的可识别您的用户或组织的信息将被视为机密信息。（请参阅以下思科采取哪些措施来确保我共享的数据安全？，第 837 页）。

下表介绍了“人性化”格式的日志条目示例。

表 *105:* 按思科设备共享的统计信息

项目	示例数据
MGA 标识符	MGA 10012
Timestamp	从 2005 年 7 月 1 日 8 AM 到 8:05 AM 的数据
软件版本号	MGA 4.7.0 版本
规则集版本号	反垃圾邮件规则集 102
防病毒更新间隔	每 10 分钟更新一次
隔离区大小	500 MB
隔离区邮件计数	隔离区中当前有 50 封邮件
病毒得分阈值	发送要在威胁级别 3 或更高级别隔离的邮件
进入隔离区的邮件的病毒评估分数总和	120
进入隔离区的邮件计数	30 (产生平均得分 4)
最大隔离时间	12 小时

项目	示例数据
按进入和退出隔离区的原因统计的爆发隔离区邮件数量(与防病毒结果关联)	50 封邮件由于 .exe 规则进入隔离区 30封邮件由于手动放行离开隔离区，并且30封全部具有病毒特征
按离开隔离区后采取的操作细分的爆发隔离区邮件计数	10 封邮件在离开隔离区后删除了附件
邮件保留在隔离区中的总时间	20 小时

表 *106:* 按发件人 *IP* 地址共享的统计数据

项目	示例数据
设备内各个阶段的邮件计数	通过防病毒引擎检测：100 通过反垃圾邮件引擎检测：80
反垃圾邮件和防病毒分数总和以及判定结果	2,000（检测到的所有邮件的反垃圾邮件得分总和）
符合不同反垃圾邮件和防病毒规则组合条件的邮件数量	100 封邮件命中规则 A 和 B 50 封邮件仅命中规则 A
连接数	20 个 SMTP 连接
收件人总数和无效收件人数量	收件人总计 50 名 10 名无效收件人
哈希文件名：(a)	在名为 <one-way-hash>.zip 的存档附件内找到一个 <one-way-hash>.pif 文件
混淆文件名：(b)	在 aaaaaaa.zip 文件内找到一个 aaaaaaa0.aaa.pif 文件。
URL 主机名 (c)	在发往 www.domain.com 的邮件中找到一个链接
混淆 URL 路径 (d)	在发往主机名 www.domain.com 的邮件内找到一个链接，其中包含路径 aaa000aa/aa00aaa。

项目	示例数据
按垃圾邮件和病毒扫描结果统计的邮件数	10 封具有垃圾邮件特征 10 封无垃圾邮件特征 5 封具有可疑垃圾邮件特征 4 封具有病毒特征 16 封无病毒特征 5 封无法扫描病毒
按不同反垃圾邮件和防病毒判定结果统计的邮件数	500 封垃圾邮件，300 封 ham
按大小范围统计的邮件数	125 个在 30K-35K 范围内
不同扩展名类型的计数	300 个“.exe”附件
附件类型、实际文件类型和容器类型的关联统计信息	100 个附件具有“.doc”扩展名，但实际上是“.exe” 50 个附件的“.exe”扩展名在 zip 内
扩展名和实际文件类型与附件大小的关联统计信息	30 个附件为“.exe”，大小在 50-55K 范围内
上传到文件信誉服务（AMP 云）的附加文件数	1110 个文件上传到文件信誉服务
上传到文件信誉服务（AMP 云）的文件的判定结果	发现 10 个文件为恶意性质 发现 100 个文件为清洁文件 1000 个文件属于信誉服务未知文件
上传到文件信誉服务（AMP 云）的文件的信誉得分	50 个文件的信誉得分为 37 50 个文件的信誉得分为 57 1 个文件的信誉得分为 61 9 个文件的信誉得分为 99
上传到文件信誉服务（AMP 云）的文件的名称	example.pdf testfile.doc
文件信誉服务（AMP 云）检测到的恶意软件威胁的名称	Trojan-Test

(a) 文件名将以单向散列 (MD5) 编码。

(b) 文件名将以混淆形式发送，其中所有小写 ASCII 字母 ([a-z]) 将替换为“a”，所有大写 ASCII 字母 ([A-Z]) 将替换为“A”，任何多字节 UTF-8 字符将替换为“x”（为其他字符集保密），所有

ASCII 数字 ([0–9]) 将替换为“0”，保留所有其他单字节字符（空格、标点符号等）。例如，文件名 Britney1.txt.pif 将显示为 Aaaaaaa0.aaa.pif。

(c) URL 主机名指向提供内容的网络服务器，与 IP 地址相似。无机密信息，例如用户名和密码。

(d) 主机名之后的 URL 信息将混淆处理，以确保不会透露用户的任何个人信息。

从 AsyncOS 8.5 for Email 及更高版本起，如果 IronPort 反垃圾邮件或智能多次扫描功能密钥处于活动状态，并启用了 SenderBase 网络参与，则 AsyncOS 将执行以下操作以提高产品的效率：

- 收集有关邮件中特定信头重复的信息，对收集的信息加密，并将加密的信息作为信头添加到各个邮件中。

  您可以将这些处理的邮件送交思科进行分析。每封邮件由人工分析师审核，并用于增强产品的效果。有关将邮件提交给思科进行分析的说明，请参阅向思科报告分类错误的邮件，第 281 页。

- 发送随机邮件示例到 CASE 进行反垃圾邮件扫描，不考虑其发件人的 SBRS。CASE 扫描这些邮件，并利用结果改善产品的效果。只有在 AsyncOS 空闲时，才会执行此操作。因此，此反馈机制不会对邮件处理造成任何重大影响。

思科采取哪些措施来确保我共享的数据安全？

如果您同意参与 SenderBase 网络:

- 从您的思科设备发送的数据都将通过安全协议 HTTPS 发送到思科 SenderBase 网络服务器。
- 所有客户数据均在思科谨慎处理。这些数据存储在安全的位置，只有需要访问它们来改善公司邮件安全产品与服务或提供客户支持的思科员工和承包商才能访问这些数据。
- 在根据这些数据生成报告或统计数据时，不会在思科系统之外共享可识别邮件收件人或客户公司的任何信息。

共享数据是否会影响我的思科设备的性能？

思科认为，这对大多数用户的性能影响非常之小。我们在邮件传送过程中记录已存在的数据。然后，在设备中汇总客户数据，并将它们批量发送到 SenderBase（通常每 5 分钟一批）。预计通过 HTTPS 传输的数据总大小不足典型公司邮件流量带宽的 1%。

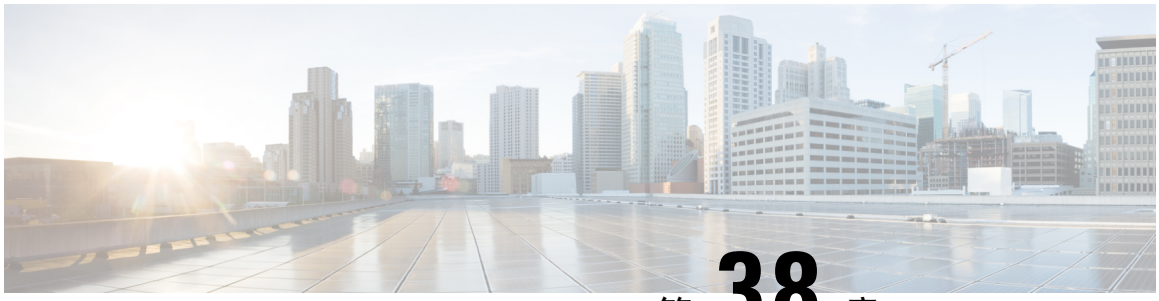
启用后，使用情景自适应扫描引擎(CASE)收集和报告数据（无论是否启用思科反垃圾邮件扫描）。

注释 如果您选择参与 SenderBase 网络，系统将针对每封邮件执行“正文扫描”。无论过滤器或应用于邮件的其他操作是否将触发正文扫描，都会执行此操作。有关正文扫描的详细信息，请参阅正文扫描规则，第 142 页。

如果您还有其他问题，请与思科客户支持部门联系。请参阅思科支持社区，第 9 页。

我是否可通过其他方式共享数据？

如果客户希望采取更多操作来帮助思科提供优质安全服务，可使用命令来共享其他数据。这种更高级别的数据共享还将在邮件中提供纯文本形式的附件文件名，以及URL的主机名。如果您有兴趣了解此功能，请告诉您的系统工程师或联系思科客户支持部门。



第 38 章

GUI 中的其他任务

本章包含以下部分：

图形用户界面 (GUI)

图形用户界面 (GUI) 是基于 Web 的界面，可替代某些命令行界面 (CLI) 命令用于系统监控和配置。通过 GUI，您可以使用基于 Web 的简单界面监控系统，而不必学习 AsyncOS 命令语法。为接口启用 HTTP 和/或 HTTPS 服务后，才能访问 GUI 和登录。有关详细信息，请参阅“访问设备”一章。

在接口上启用 GUI

默认情况下，系统出厂设置为在“管理”(Management) 接口上启用 HTTP。

要启用GUI，请在命令行界面中执行interfaceconfig命令，对要连接的接口进行编辑，然后启用HTTP服务和/或安全 HTTP 服务。

注释 也可使用“网络”>“IP 接口”页面启用接口上的 GUI；若在任何其他接口上启用了 GUI，则可在此页面上禁用 GUI。有关详细信息，请参阅IP接口，第 979 页。

注释 要在接口上启用安全 HTTP，必须安装证书。有关详细信息，请参阅“启用 HTTPS 的证书”。

对于 HTTP 和 HTTPS 服务，请分别指定需要启用服务的端口。在默认情况下，HTTP 在端口 80 上启用，HTTPS 则在端口 443 上启用。如果在一个端口上启用两种服务，用户可以自动将 HTTP 请求重定向到安全服务。

此外，所有尝试（通过 HTTP 或 HTTPS）在该接口上访问 GUI 的用户（请参阅 处理用户帐户，第 723 页）必须通过标准的用户名和密码登录页面进行自我身份验证。

注释 您必须先使用 commit 命令保存更改，然后才能访问 GUI。

在以下示例中，在 Data 1 接口上启用了 GUI。使用 interfaceconfig 命令在端口 80 上启用 HTTP，在端口 443 上启用 HTTPS。（HTTP 暂时使用演示证书，直至 certconfig 命令可以运行。有关详细信息，请参阅“在思科设备上安装证书”。）端口 80 的 HTTP 请求配置为自动重定向到 Data1 接口的端口 443。

GUI 中的系统信息

- 在**系统概览**页面，用户能够：
  - 查看显示某些关键系统状态和性能信息的历史图片及表格。
  - 查看设备上安装的 AsyncOS 操作系统的版本。
  - 查看关键统计子集。
- **系统状态**页面详细展示了系统的所有实时邮件和 DNS 活动。用户还可以重置系统统计的计数器，并查看计数器的最后一次重置时间。

从 GUI 收集 XML 状态

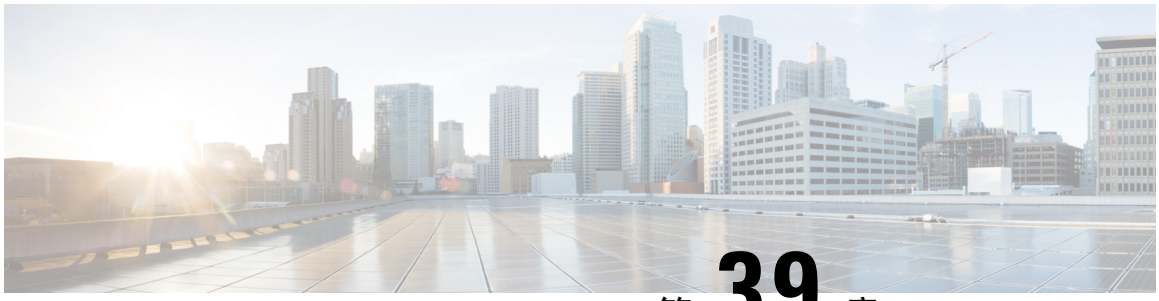
通过 XML 页面查看状态，或以程序化方式访问 XML 状态信息。

XML状态功能提供了用于访问邮件监控统计信息的程序化方法。请注意，某些较新的浏览器也能直接显示 XML 数据。

此表中来自 GUI 页面的信息也可像动态 XML 输出一样，通过访问对应的 URL 获得：

GUI 页面名称	对应的 XML 状态 URL
邮件状态	http:// *hostname* /xml/status
指定主机的主机邮件状态	http:// *hostname* /xml/hoststatus?hostname= *host*
DNS 状态	http:// *hostname* /xml/dnsstatus
最高传入域	http:// *hostname* /xml/topin
传出域排行榜[1]	http:// *hostname* /xml/tophosts

[1] 该页面的默认排序方式为按在线收件人的数量排列。用户可以通过将“?sort= order”添加至 URL 来更改顺序，其中 order 是 conn_out、deliv_recip、soft_bounced 或 hard_bounced。



第 39 章

高级网络配置

本章包含以下部分：

以太网接口上的媒体设置

以太网接口的媒体设置可使用 etherconfig 命令访问。每个以太网接口连同其当前设置一起列出。选择接口后，将会显示可能的介质设置。有关示例，请参阅编辑介质设置示例，第 841 页。

使用 etherconfig 编辑以太网接口上的介质设置

etherconfig 命令可用于设置以太网接口的双工设置（全/半）以及速度（10/100/1000 Mbps）。默认情况下，接口会自动选择介质设置；但某些情况下，您可能希望覆盖此设置。

注释 如果您已按照“设置和安装”一章中的说明完成了 GUI 的系统设置向导（或命令行界面 systemsetup 命令）并确认了更改，则默认的以太网接口设置应已在设备上配置。

某些设备包含一个光纤网络接口选项。如果可用，您会在这些设备上的可用接口列表中看到另外两个以太网接口（Data 3 和 Data 4）。这些千兆光纤接口可以与异类配置中的铜缆（Data 1、Data 2 和管理）接口配对。请参阅网络接口卡配对/组合，第 842 页。

编辑介质设置示例

```
mail3.example.com> etherconfig

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
```

```
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.

[]> media
Ethernet interfaces:
1. Data 1 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6d
2. Data 2 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6e
3. Management (Autoselect: <100baseTX full-duplex>) 00:02:b3:c7:a2:da

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]> edit
Enter the name or number of the ethernet interface you wish to edit.
[]> 2
Please choose the Ethernet media options for the Data 2 interface.
1. Autoselect
2. 10baseT/UTP half-duplex
3. 10baseT/UTP full-duplex
4. 100baseTX half-duplex

5. 100baseTX full-duplex


6. 1000baseTX half-duplex
7. 1000baseTX full-duplex
[1]> 5
Ethernet interfaces:
1. Data 1 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6d
2. Data 2 (100baseTX full-duplex: <100baseTX full-duplex>) 00:06:5b:f3:ba:6e
3. Management (Autoselect: <100baseTX full-duplex>) 00:02:b3:c7:a2:da
Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]>
```

网络接口卡配对/组合

NIC 配对可用于组合任何两个物理数据端口，以在从 NIC 到上游以太网端口的数据路径出现故障时提供备用以太网接口。配对主要是配置以太网接口，以便有一个主接口和一个备用接口。如果主接口发生故障（例如，如果 NIC 和上游节点之间的载体中断），则备用接口变为活动状态，并发送警报。当主接口重新启用后，此接口将自动变为活动状态。在本产品的文档中，NIC 配对与 NIC 组合是同义词。

注释 NIC 配对在邮件安全虚拟设备上不可用。

您可以创建多个 NIC 配对，以为您提供足够的数据端口。创建配对时，可以组合任意两个数据端口。例如：

Data 1 和 Data 2

Data 3 和 Data 4

Data 2 和 Data 3

其他

某些思科设备包含一个光纤网络接口选项。如果可用，您会在这些设备上的可用接口列表中看到另外两个以太网接口（Data 3 和 Data 4）。这些千兆光纤接口可以与异类配置中的铜缆（Data 1、Data 2 和管理）接口配对。

NIC 配对和 VLAN

VLAN（请参阅虚拟局域网 (VLAN)，第 844 页）仅在主接口上允许。

NIC 对命名

在创建 NIC 对时，必须指定用于引用该对的名称。在 4.5 之前的 AsyncOS 版本中创建的 NIC 对将在升级后自动接收默认名称“Pair 1”。

因 NIC 配对生成的任何警报都将按名称引用特定的 NIC 对。

NIC 配对和现有侦听程序

如果在为其指定了侦听程序的接口上启用 NIC 配对，系统会提示您删除、重新分配或禁用指定给备用接口的所有侦听程序。

通过 etherconfig 命令启用 NIC 配对

注释 NIC 配对在邮件安全虚拟设备上不可用。

```
mail3.example.com> etherconfig

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
```

```
[]> pairing

Paired interfaces:

Choose the operation you want to perform:

- NEW - Create a new pairing.

[]> new

Please enter a name for this pair (Ex: "Pair 1"):

[]> Pair 1

Warning: The backup (Data 2) for the NIC Pair is currently configured with one or more
IP addresses. If you continue, the Data 2 interface will be deleted.

Do you want to continue? [N]> y

The interface you are deleting is currently used by listener "OutgoingMail".

What would you like to do?

1. Delete: Remove the listener and all its settings.

2. Change: Choose a new interface.

3. Ignore: Leave the listener configured for interface "Data 2" (the listener will be
disabled until you add a new interface named "Data 2" or edit the listener's settings).


[1]>

Listener OutgoingMail deleted for mail3.example.com.

Interface Data 2 deleted.

Paired interfaces:

1. Pair 1:


Primary (Data 1) Active, Link is up

Backup (Data 2) Standby, Link is up

Choose the operation you want to perform:

- DELETE - Delete a pairing.

- STATUS - Refresh status.

[]>
```

虚拟局域网 (VLAN)

您可以在设备的任意物理网络端口上配置多个虚拟局域网 (VLAN)。

可以使用 VLAN 来：

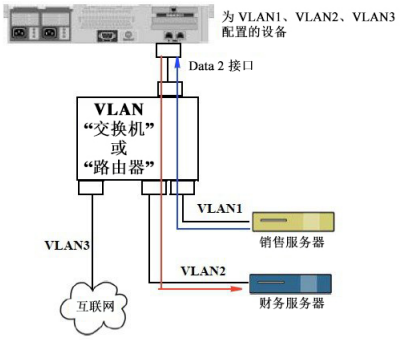
- 将设备可连接的网络数增加到超过设备上的物理接口数。
- 允许在现有侦听程序的独立“端口”上定义更多网络。
- 出于安全考虑对网络进行分段，以简化管理或增加带宽。

使用案例示例：

直接因 VLAN 限制而无法通信的两个邮件服务器可以通过邮件安全设备发送邮件。设备上的 Data 2 接口通过 VLAN1 和 VLAN2 配置。蓝线显示从销售网络 (VLAN1) 发送至设备的邮件。设备按照正常方式处理该，然后在传送时，以目的 VLAN2 信息（红线）标记数据包。

使用 VLAN 加速设备之间的通信

图 *74:* 使用 *VLAN* 加速设备之间的通信



关于配置 VLAN

可以在设备上的任意物理网络端口上配置多个 VLAN，包括“数据”和“管理”端口以及某些设备型号上提供的光纤数据端口。AsyncOS 最多支持 30 个 VLAN。

物理端口不需要为了进入 VLAN 而配置 IP 地址。在其上创建 VLAN 的物理端口可以有一个用来接收非 VLAN 流量的 IP，以便可以在同一接口上同时拥有 VLAN 和非 VLAN 流量。

VLAN 可与 NIC 配对（在配对的 NIC 上提供）和直接服务器返回 (DSR) 配合使用。

VLAN 显示为以：“VLAN DDDD”格式标记的动态“数据端口”，其中“DDDD”是 ID，是长度最多为 4 位数的整数（例如 VLAN 2 或 VLAN 4094）。VLAN ID 在设备上必须是唯一的。

管理 VLAN

可以通过 etherconfig 命令创建、编辑和删除 VLAN。创建 VLAN 后，可以通过“网络”>“接口”页面或 CLI 中的 interfaceconfig 命令配置该 VLAN。请记得要确认所有更改。

通过 etherconfig 命令创建新的 VLAN

在本例中，在 Data 1 端口上创建两个 VLAN（名为 VLAN 31 和 VLAN 34）：

```
mail3.example.com> etherconfig

Choose the operation you want to perform:
```

```
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> vlan
VLAN interfaces:
Choose the operation you want to perform:
- NEW - Create a new VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 34
Enter the name or number of the ethernet interface you wish bind to:
1. Data 1
2. Data 2
3. Management
[1]> 1

VLAN interfaces:
1. VLAN 34 (Data 1)
Choose the operation you want to perform:

- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 31
Enter the name or number of the ethernet interface you wish bind to:
1. Data 1
2. Data 2
3. Management
```

```
[1]> 1

VLAN interfaces:

1. VLAN 31 (Data 1)

2. VLAN 34 (Data 1)

Choose the operation you want to perform:

- NEW - Create a new VLAN.

- EDIT - Edit a VLAN.

- DELETE - Delete a VLAN.

[]>

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.

[]>
```

通过 interfaceconfig 命令在 VLAN 上创建 IP 接口

在本例中，在 VLAN 31 以太网接口上创建新的 IP 接口。

对接口进行更改可能会断开您与设备的连接。

```
mail3.example.com> interfaceconfig

Currently configured interfaces:

1. Data 1 (10.10.1.10/24: example.com)

2. Management (10.10.0.10/24: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]> new
```

```
Please enter a name for this IP interface (Ex: "InternalNet"):

[]> InternalVLAN31

Would you like to configure an IPv4 address for this interface (y/n)? [Y]>

IPv4 Address (Ex: 10.10.10.10):

[]> 10.10.31.10

Netmask (Ex: "255.255.255.0" or "0xffffff00"):

[255.255.255.0]>

Would you like to configure an IPv6 address for this interface (y/n)? [N]>

Ethernet interface:

1. Data 1

2. Data 2

3. Management

4. VLAN 31

5. VLAN 34

[1]> 4

Hostname:

[]> mail31.example.com

Do you want to enable SSH on this interface? [N]>

Do you want to enable FTP on this interface? [N]>

Do you want to enable HTTP on this interface? [N]>

Do you want to enable HTTPS on this interface? [N]>

Currently configured interfaces:

1. Data 1 (10.10.1.10/24: example.com)

2. InternalVLAN31 (10.10.31.10/24: mail31.example.com)

3. Management (10.10.0.10/24: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]>
```

使用 Web 界面配置 VLAN

使用 etherconfig 命令创建 VLAN 后，可以使用“网络”>“侦听程序”页对其进行配置。

直接服务器返回

直接服务器返回(DSR)是一种为轻量级负载均衡机制提供支持的方式，以实现共享同一虚拟 IP(VIP)的多个邮件安全设备之间的负载均衡。

DSR 通过在设备的“环回”以太网接口上创建的 IP 接口实现。

注释 为邮件安全设备配置负载均衡不在本文档的范围之内。

启用直接服务器返回

通过在每个参与设备上启用“环回”以太网接口来启用 DSR。接下来，使用 CLI 中的 **interfaceconfig** 命令或 GUI 中的“网络”(Network)>“接口”(Interfaces)页面通过虚拟 IP(VIP)在环回接口上创建 IP 接口。最后，使用 CLI 中的 **listenerconfig** 命令或 GUI 中的“网络”(Network)>“侦听程序”(Listeners)页面在新 IP 接口上创建侦听程序。请记得要确认所有更改。

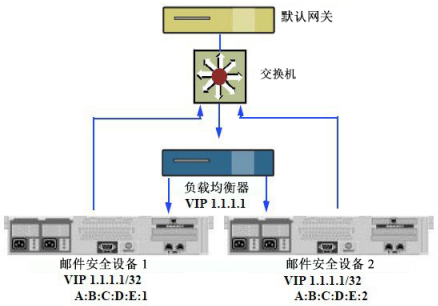
注释 使用环回接口可以防止设备针对该特定接口发出 ARP 应答

当启用 DSR 时，以下规则适用：

所有系统都使用同一虚拟 IP (VIP) 地址

所有系统必须与负载均衡器位于同一交换机和子网上

图 *75:* 使用 ***DSR*** 实现交换机上多个邮件安全设备之间的负载均衡



使用 DSR 实现交换机上多个邮件安全设备之间的负载均衡

通过 etherconfig 命令启用环回接口

启用后，环回接口将像其他任何接口（例如 Data 1）一样被跟踪：

```
mail3.example.com> etherconfig

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.


[]> loopback

Currently configured loopback interface:

Choose the operation you want to perform:


- ENABLE - Enable Loopback Interface.

[]> enable

Currently configured loopback interface:


1. Loopback

Choose the operation you want to perform:

- DISABLE - Disable Loopback Interface.

[]>

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.

[]>
```

通过 interfaceconfig 命令在环回接口上创建 IP

在环回接口上创建 IP 接口：

```
mail3.example.com> interfaceconfig

Currently configured interfaces:
```

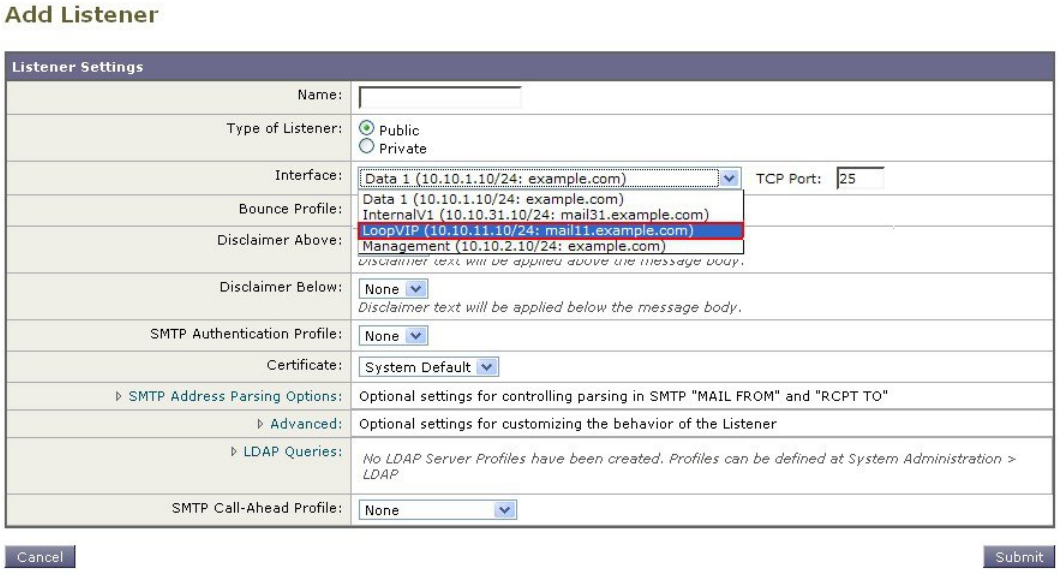
```
1. Data 1 (10.10.1.10/24: example.com)
2. InternalV1 (10.10.31.10/24: mail31.example.com)
3. Management (10.10.0.10/24: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> new
Please enter a name for this IP interface (Ex: "InternalNet"):
[]> LoopVIP
Would you like to configure an IPv4 address for this interface (y/n)? [Y]>
IPv4 Address (Ex: 10.10.10.10):
[]> 10.10.1.11
Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> 255.255.255.255
Would you like to configure an IPv6 address for this interface (y/n)? [N]>
Ethernet interface:
1. Data 1
2. Data 2
3. Loopback
4. Management
5. VLAN 31
6. VLAN 34
[1]> 3
Hostname:
[]> example.com
Do you want to enable SSH on this interface? [N]>

Do you want to enable FTP on this interface? [N]>

Do you want to enable HTTP on this interface? [N]>
Do you want to enable HTTPS on this interface? [N]>
```

```
Currently configured interfaces:

1. Data 1 (10.10.1.10/24: example.com)

2. InternalV1 (10.10.31.10/24: mail31.example.com)

3. LoopVIP (10.10.1.11/24: example.com)

4. Management (10.10.0.10/24: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]>
```

在新 IP 接口上创建侦听程序

通过 GUI 或 CLI 在新 IP 接口上创建侦听程序。例如，下图显示了 GUI 的“添加侦听程序”页面上可用的新创建的 IP 接口。

图 *76*: 在新环回 *IP* 接口上创建侦听程序



以太网接口的最大传输单位

最大传输单位 (MTU) 是以太网接口将接受的最大数据单位。可以通过 etherconfig 命令降低以太网接口的 MTU。默认的 MTU 大小是 1500 字节，这是以太网可以接受的最大 MTU。

要编辑接口的 MTU，请：

```
mail3.example.com> etherconfig

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.

[]> mtu

Ethernet interfaces:

1. Data 1 mtu 1400

2. Data 2 default mtu 1500

3. Management default mtu 1500

Choose the operation you want to perform:

- EDIT - Edit an ethernet interface.

[]> edit

Enter the name or number of the ethernet interface you wish to edit.

[]> 2

Please enter a non-default (1500) MTU value for the Data 2 interface.

[]> 1200

Ethernet interfaces:

1. Data 1 mtu 1400

2. Data 2 mtu 1200

3. Management default mtu 1500

Choose the operation you want to perform:

- EDIT - Edit an ethernet interface.

[]>
```

接受或拒绝包含组播地址的 ARP 应答

您现在可指定是接受还是拒绝包含组播地址的 ARP 应答。使用 MULTICAST 子命令配置此功能。

以下示例显示如何将设备配置为接受包含组播地址的 ARP 应答：

```
mail.example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> multicast
ARP replies with a multicast address will be rejected.
Choose the operation you want to perform:
- ACCEPT - Accept ARP replies with a multicast address.
[]> accept
ARP replies with a multicast address will be accepted.
```

第 40 章

日志记录

本章包含以下部分：

概述

了解日志文件和日志订阅

日志是收集 AsyncOS 邮件操作重要信息的有效方法，非常节省空间。这些日志将记录设备上发生的活动的相关信息。日志中的信息会因您查看的日志（例如，退回日志或传送日志）而异。

大多数日志采用纯文本 (ASCII) 格式记录；但为保证资源效率，传送日志采用二进制格式。ASCII 文本信息在任何文本编辑器中均可读。

思科提供 M 系列内容安全管理设备，作为来自多个邮件安全设备的日志的集中报告和跟踪工具。请联系您的思科代表，了解详情。

日志订用可将日志类型与名称、日志记录级别和其他约束（例如大小和目标信息）关联起来；同一日志类型允许存在多个订用。

日志类型

日志类型指明了在生成的日志中记录的信息，例如，消息数据、系统统计信息、二进制或文本数据。创建日志订用时，您可选择日志类型。有关详细信息，请参阅日志订阅，第 896 页。

AsyncOS 会生成以下日志类型：

表 *107:* 日志类型

记录	说明
文本邮件日志	文本邮件日志记录邮件系统操作的相关信息。例如，邮件接收、邮件传送尝试、打开和关闭的连接、退回、TLS 连接等。
qmail格式邮件日志	qmail格式传送日志记录的邮件系统操作信息与下文中的传送日志相同，但会将信息存储为 qmail 格式。
投递日志	传送日志记录邮件安全设备的邮件传送操作的重要信息，例如，有关每次收件人传送的信息以及传送尝试时的退回相关信息。日志消息为“无状态”消息，这意味着所有相关信息都会逐条记录在每条日志消息中，用户无需参考上一条日志消息即可了解当前传送尝试的相关信息。传送日志以二进制格式记录，以提高资源效率。必须使用提供的实用程序对传送日志文件进行后处理，将其转换为 XML 或 CSV（逗号分隔值）格式。转换工具位置： https://supportforums.cisco.com/document/33721/cisco-ironport-systems-contributed-tools
反弹日志	退回日志记录有关退回的收件人的信息。为每个退回的收件人记录如下信息：邮件 ID、收件人 ID、源信封地址、目标信封地址、收件人退回的原因以及来自收件人主机的响应代码。此外，针对每个退回的收件人邮件，您还可以选择记录固定大小的信息。此大小以字节为单位，默认为零。
状态日志	此类日志文件记录 CLI 状态命令中的系统统计信息，包括 status detail 和 dnsstatus 命令。记录期限使用 logconfig 中的 setup 子命令设置。状态日志中的每个计数器或记录的速率为从上次重置计数器起至当前的值。
域名调试日志	域调试日志记录客户端和服务器在邮件安全设备与指定收件人主机SMTP会话期间的通信。此类日志可用来调试特定收件人主机存在的问题。必须在日志文件中指定要记录的SMTP会话总数。随着会话记录的增加，此数目会逐渐减少。可以通过删除或编辑日志订用，在记录所有会话之前停止域调试。
注入调试日志	注入调试日志记录邮件安全设备和连接到系统的指定主机之间的SMTP会话。注入调试日志对于排除邮件安全设备和互联网上某主机之间的通信问题很有帮助。
系统日志	系统日志记录以下信息：引导信息、虚拟设备许可证到期警报、DNS状态信息和用户使用 commit 命令输入的备注。系统日志对于排查设备的基本状态很有用。
CLI审核日志	CLI 审核日志会记录系统中的所有 CLI 活动。
FTP服务器日志	FTP 日志会记录有关在界面上启用的FTP服务的信息。其中包含连接详细信息和用户活动。
GUI 日志	请参阅 HTTP 日志。

记录	说明
HTTP日志	HTTP 日志记录接口上启用的 HTTP 和/或安全 HTTP 服务的相关信息。由于图形用户界面 (GUI) 通过 HTTP 访问，因此 HTTP 日志实质上等同于CLI审核日志的GUI。日志会记录会话数据（新会话和过期的会话）和在 GUI 中访问的页面。 这些日志还包括有关SMTP事务的信息，例如，从设备上邮件发送的计划报告的信息。
NTP 日志	NTP 日志记录设备与配置的所有 NTP（网络时间协议）服务器之间的会话。有关详细信息，请参阅“系统管理”章节的“编辑网络时间协议 (NTP) 配置（计时方法）”部分。
LDAP调试日志	LDAP 调试日志用于调试LDAP安装。（请参阅章节“LDAP查询”。）此类日志将记录有关邮件安全设备发送到LDAP服务器的查询的实用信息。
反垃圾邮件日志	反垃圾邮件日志记录系统反垃圾邮件扫描功能的状态，包括最新反垃圾邮件规则更新的接收状态。此外，日志还将记录所有与情景自适应扫描引擎相关的日志。
反垃圾邮件归档	如启用反垃圾邮件扫描功能，此类日志将存档经过扫描且与“存档邮件”操作有关的邮件。日志文件为 mbox 格式。有关反垃圾邮件引擎的详细信息，请参阅“反垃圾邮件”一章。
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。
防病毒日志	防病毒日志记录系统防病毒扫描功能的状态，包括最新防病毒身份文件更新的接收状态。
防病毒归档	如启用防病毒引擎，此类日志将记录经过扫描并与“存档邮件”操作关联的邮件。日志文件为 mbox 格式。有关详细信息，请参阅“防病毒”一章。
AMP 引擎日志	AMP引擎日志记录系统高级恶意软件保护功能的状态。有关详细信息，请参阅 文件信誉过滤和文件分析：，第 353 页
AMP 存档	如已将邮件策略配置为对高级恶意软件保护引擎发现附件无法扫描或包含恶意软件的邮件进行存档，此类邮件会存档至此处。日志文件为mbox格式。
Scaning 日志	扫描日志包含扫描引擎的所有 LOG 和 COMMON 消息（请参阅告警信息，第 777 页）。这类消息通常是应用故障、发送的警报，失败的警报和日志错误消息。此日志不适用于系统范围警报。

记录	说明
垃圾邮件隔离区日志	垃圾邮件隔离区日志记录与垃圾邮件隔离区进程相关的操作。
垃圾邮件隔离区 GUI 日志	垃圾邮件隔离区日志记录与垃圾邮件隔离区相关的操作，例如，通过 GUI 进行的配置、最终用户身份验证和最终用户操作（发出邮件等）。
SMTP 会话日志	SMTP 会话日志记录传入和传出 SMTP 会话的所有信息。
安全/阻止列表日志	安全列表/阻止列表日志会记录有关安全列表/阻止列表设置和数据库的数据。
报告日志	报告日志会记录与集中报告服务的进程相关的操作。
路由查询日志	报告查询日志会记录与设备上运行的报告查询相关的操作。
更新程序日志	更新程序日志记录与系统服务更新相关的事件，例如 McAfee 防病毒定义更新。
跟踪日志	跟踪记录记录与跟踪服务进程相关的操作。跟踪日志是邮件日志的子集。
身份验证日志	身份验证日志记录成功的用户登录和失败的登录尝试。
配置历史记录日志	配置历史记录日志记录以下信息：邮件安全设备上发生的变更以及变更发生的时间。每次用户提交更改时，都会创建一份新的配置历史记录日志。
升级日志	有关升级下载和安装的状态信息。
API 日志	API 日志记录与思科邮件安全设备 AsyncOS API 相关的各种事件，例如： • API 启动或停止 • 到 API 的连接失败或关闭（在响应后） • 身份验证成功或失败 • 请求包含错误 • 与 AsyncOS API 进行网络配置更改通信时出现错误

日志类型特征

下表汇总了每种日志类型的不同特征。

表 *108:* 日志类型比较

						包含								
	事务	无状态	记录为文本	记录为mbox文件	记录为二进制	定期状态信息	邮件接收信息	传送信息	单个硬退回	单个软退回	注入SMTP会话	信头日志记录	传送SMTP会话	配置信息
邮件日志	•		•			•	•	•	•	•				
qmail 格式传送日志		•			•		•	•	•					
传送日志		•			•		•	•	•					
反弹日志	•		•						•	•				
状态日志		•	•			•								
域名调试日志	•		•					•	•	•				
注入调试日志	•		•				•							
系统日志	•		•			•								
CLI审核日志	•		•			•								
FTP服务器日志	•		•			•								
HTTP日志	•		•			•								
NTP 日志	•		•			•								
LDAP 日志	•		•											
反垃圾邮件日志	•		•			•								

						包含								
反垃圾邮件归档				•										
灰色邮件引擎日志	•		•			•								
灰色邮件存档				•										
防病毒日志	•		•			•								
防病毒归档				•										
AMP 引擎日志	•		•			•								
AMP 存档				•										
Scaning 日志	•		•			•								
垃圾邮件隔离区	•		•			•								
垃圾邮件隔离区 GUI	•		•			•								
安全/阻止列表日志	•		•			•								
报告日志	•		•		•									
路由查询日志	•		•		•									
更新程序日志			•											
跟踪日志	•				•	•	•	•	•	•				
身份验证日志	•		•											

						包含								
配置历史记录日志	•		•											
API 日志	•		•											

日志检索方法

可根据以下其中一个文件传输协议检索日志文件。在日志订用过程中，当使用GUI或logconfig命令创建或编辑日志订用时，可以设置协议。

注释 在某个日志上使用日志推送方法时，该日志在本地无法用于故障排除或者通过 CLI 进行搜索。

表 *109:* 日志传输协议

手动下载	使用这种方法，随时可以通过在“日志订用”(Log Subscriptions) 页面点击日志目录链接，然后点击要访问的日志文件，来访问日志文件。根据使用的浏览器，可以在浏览器窗口中查看文件、打开文件，或将文件另存为文本文件。此方法使用 HTTP(S) 协议，也是默认的检索方法。 **注释** 使用此方法无法检索集群中任何计算机的日志，而不管是何级别（计算机、组或集群级别），即使在 CLI 中指定此方法亦是如此。
FTP 推送	此方法可将日志文件定期推送到远程计算机上的 FTP 服务器。订用要求提供远程计算机的用户名、密码和目标目录。日志文件将根据您设置的回滚计划进行传输。
SCP 推送	此方法可将日志文件定期推送到远程计算机上的 SCP 服务器。此方法要求在远程计算机上存在使用 SSH1 或 SSH2 协议的 SSH SCP 服务器。订用要求提供远程计算机的用户名、密码和目标目录。日志文件将根据您设置的回滚计划进行传输。
Syslog Push	此方法会将日志消息发送到远程系统日志服务器。此方法符合 RFC 3164 标准。必须提交系统日志服务器的主机名，并选择使用 UDP 还是 TCP 传输日志。使用的端口是514。可为日志选择设备；但是，日志类型的默认值已在下拉菜单中预先选择。只有基于文本的日志可以使用系统日志推送进行传输。

日志文件名和目录结构

AsyncOS 会根据日志订阅名称为每个日志订阅创建目录。日志文件在目录中的实际名称由指定的日志文件名、启动日志文件的时间戳以及单字符状态代码组成。可使用以下公式创建日志文件名：

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

状态代码可以是 .current 或 .s（表示已保存）。只能传送或删除已保存状态的日志文件。

日志回滚和传输计划

日志文件由日志订阅创建，并根据满足的第一个用户指定的条件进行回滚（并调用，如选择基于推送的检索选项）：最大文件大小或计划回滚。在 CLI 中使用 logconfig 命令，或在 GUI 中使用“日志订用”页面配置最大文件大小和计划回滚的时间间隔。此外，还可以在 GUI 中使用**立即回滚**按钮，或在 CLI 中使用 rollovernow 命令对选定的日志订阅进行回滚。有关计划回滚的详细信息，请参阅滚动更新日志订用，第 900 页。

设备会对使用手动下载检索的日志进行保存，直至日志达到指定的最大数量（默认为 10 个文件）或直至系统需要更多的日志文件存储空间。

默认启用的日志

邮件安全设备预配置了很多默认启用的日志订用（其他日志可根据您应用的许可证密钥进行配置）。默认情况下，检索方法是“手动下载”(Manually Download)。

所有预配置日志订用的日志级别均为 3，但 error_logs 日志订用除外。此类日志的级别为 1，以便其中仅包含错误。有关详细信息，请参阅日志级别，第 896 页。有关创建新日志订用或修改现有日志订用的信息，请参阅日志订阅，第 896 页。

日志类型

日志文件中的时间戳

以下日志文件包括日志自身的开始和结束日期、AsyncOS 的版本以及 GMT 偏移（以秒为单位，且仅在日志开头显示）：

- 防病毒日志
- LDAP 日志
- 系统日志
- 邮件日志

使用文本邮件日志

这类日志包含有关邮件接收、邮件传送以及退回的详细信息。此外，每分钟还会将状态信息写入邮件日志。这些日志是非常有用的信息来源，可用于了解特定邮件的传输及分析系统性能。

这些日志无需任何特殊配置。但是，必须正确配置系统才能查看附件名称，而且不一定会记录附件名称。有关信息，请参阅启用邮件跟踪，第 677 页和邮件跟踪概览，第 677 页。

下表显示了文本邮件日志中显示的信息：

表 *110:* 文本邮件日志统计信息

统计	说明
ICID	注入连接 ID。目标至系统的 SMTP 连接的数字标识符，通过此连接可发送 1 到上千封邮件。
DCID	传输连接 ID。目标至另一服务器的 SMTP 连接的数字标识符，每个连接可发送 1 至成千上万封邮件，且每个连接会在一次邮件传送中传送部分或全部 RID。
RCID	RPC 连接 ID。目标至垃圾邮件隔离区的 RPC 连接的数字标识符。可使用此标识符追踪发往/发自垃圾邮件隔离区的邮件。
MID	邮件 ID：当邮件流经日志时，该 ID 用于跟踪邮件。
RID	收件人 ID：为每个邮件收件人分配一个 ID。
新	启动新连接。
开始	已开始新的邮件。

解释文本邮件日志

使用以下示例作为解释日志文件的指南。

注释 日志文件中的行目没有编号。下文出于方便对各行进行了编号。

表 *111:* 文本邮件日志详细信息

1	`Mon Apr 17 19:56:22 2003 Info:`
	`New SMTP ICID 5 interface Management (10.1.1.1)`
	`address 10.1.1.209 reverse dns host remotehost.com verified yes`

2	`Mon Apr 17 19:57:20 2003 Info:` `Start MID 6 ICID 5`
3	`Mon Apr 17 19:57:20 2003 Info:` `MID 6 ICID 5 From: <sender@remotehost.com>`
4	`Mon Apr 17 19:58:06 2003 Info:` `MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>`
5	`Mon Apr 17 19:59:52 2003 Info:` `MID 6 ready 100 bytes from <sender@remotehost.com>`
6	`Mon Apr 17 19:59:59 2003 Info: ICID 5 close`

7	Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25
8	Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID [0]
9	Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0]
10	Mon Mar 31 20:11:03 2003 Info: DCID 8 close

可参考下表来阅读上文介绍的日志文件。

表 *112:* 文本邮件日志详细信息示例

行号	说明
1	发起到系统的新连接，并且分配注入 ID (ICID)“5”。此连接是在管理 IP 接口上接收的，从 10.1.1.209 远程主机发起。
2	客户端发出 MAIL FROM 命令后，为邮件分配邮件 ID (MID) 6。
3	识别和接受发件人地址。
4	识别收件人，并且分配收件人 ID (RID)“0”。
5	接受 MID 5，将其写入磁盘并确认。
6	接收成功，接收连接断开。
7	邮件传送过程随后开始。系统为其分配了从 192.168.42.42 到 10.5.3.25 的传输连接 ID (DCID)“8”。
8	开始到 RID“0”的邮件传送。
9	从 MID 6 到 RID“0”的传送成功。
10	传送连接断开。

文本邮件日志条目示例

以下是不同情景中的日志条目示例。

邮件注入和传送

系统在邮件安全设备中注入一封发送至单个收件人的邮件。已成功传输该邮件。

```
Wed Jun 16 21:42:34 2004 Info: New SMTP ICID 282204970 interface mail.example.com
(1.2.3.4) address 2.3.4.5 reverse dns host unknown verified no

Wed Jun 16 21:42:34 2004 Info: ICID 282204970 SBRS None
```

```
Wed Jun 16 21:42:35 2004 Info: Start MID 200257070 ICID 282204970

Wed Jun 16 21:42:35 2004 Info: MID 200257070 ICID 282204970 From: <someone@foo.com>

Wed Jun 16 21:42:36 2004 Info: MID 200257070 ICID 282204970 RID 0 To: <user@example.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Message-ID
'<37gva9$5uvbhe@mail.example.com>'

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Subject 'Hello'

Wed Jun 16 21:42:38 2004 Info: MID 200257070 ready 24663 bytes from <someone@foo.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 antivirus negative

Wed Jun 16 21:42:38 2004 Info: MID 200257070 queued for delivery

Wed Jun 16 21:42:38 2004 Info: New SMTP DCID 2386069 interface 1.2.3.4 address 1.2.3.4

Wed Jun 16 21:42:38 2004 Info: Delivery start DCID 2386069 MID 200257070 to RID [0]

Wed Jun 16 21:42:38 2004 Info: ICID 282204970 close

Wed Jun 16 21:42:38 2004 Info: Message done DCID 2386069 MID 200257070 to RID [0]
[('X-SBRS', 'None')]

Wed Jun 16 21:42:38 2004 Info: MID 200257070 RID [0] Response 2.6.0
<37gva9$5uvbhe@mail.example.com> Queued mail for delivery

Wed Jun 16 21:42:43 2004 Info: DCID 2386069 close
```

成功的邮件传送

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

不成功的邮件传输（硬退回）

有两个收件人的邮件注入邮件安全设备。传输过程中，目标主机返回5XX错误，这表示无法将邮件传输到任何一个收件人。设备会通知发件人，并从队列中删除收件人。

```
Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11 address
64.81.204.225

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0 - Unknown address
error ('550', ['<george@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0 - Unknown address
error ('550', ['<jane@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:32 2003 Info: DCID 3 close
```

成功传送后发生软退回

邮件注入邮件安全设备。在第一次尝试传输时，邮件被软退回并且排队等候将来传输。第二次尝试时，邮件被成功传送。

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]

Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0 - Unknown address
error ('466', ['Mailbox temporarily full.'])[]

Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon Mar 31 20:01:23
2003

Mon Mar 31 20:01:28 2003 Info: DCID 5 close

Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet address 172.17.0.113

Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID [0]

Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]

Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

scanconfig 命令的邮件扫描结果

当邮件无法分解为各个组成部分时（删除附件时），可以使用 scanconfig 命令确定系统行为。可选择的命令包括 Deliver、Bounce 以及 Drop。

下文示例展示的是 `scanconfig` 设为 Deliver 的文本邮件日志。

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From: <test@virus.org>

Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To: <joe@example.com>

Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID '<137398.@virus.org>'

Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test #22'

Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from <test@virus.org>

Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem: Continuation line
seen before first header


Tue Aug 3 16:36:29 2004 Info: ICID 44784 close

Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive 'EICAR-AV-Test'

Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by antivirus

Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done
```

下文示例展示的是 `scanconfig` 设为 drop 的文本邮件日志。

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org
```

```
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To: <joe@example.com>
Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID '<392912.@virus.org>'
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem: Continuation line
seen before first header
Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by filter 'drop_zip_c'
Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done
Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

包含附件的邮件

在本示例中，配置了使用“邮件正文包含”条件的内容过滤器以便识别附件名称：

```
Sat Apr 23 05:05:42 2011 Info: New SMTP ICID 28 interface Management (192.0.2.10)
address 224.0.0.10 reverse dns host test.com verified yes

Sat Apr 23 05:05:42 2011 Info: ICID 28 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0]
SBRS 0.0

Sat Apr 23 05:05:42 2011 Info: Start MID 44 ICID 28
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 From: <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 RID 0 To: <recipient1@example.org>
Sat Apr 23 05:05:42 2011 Info: MID 44 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Sat Apr 23 05:05:42 2011 Info: MID 44 Subject 'Message 001'
Sat Apr 23 05:05:42 2011 Info: MID 44 ready 240129 bytes from <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Sat Apr 23 05:05:42 2011 Info: ICID 28 close
Sat Apr 23 05:05:42 2011 Info: MID 44 interim verdict using engine: CASE
spam negative
Sat Apr 23 05:05:42 2011 Info: MID 44 using engine: CASE spam negative
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Banner.gif'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment '=D1=82=D0=B5=D1=81=D1=82.rst'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Test=20Attachment.docx'
Sat Apr 23 05:05:43 2011 Info: MID 44 queued for delivery
```

请注意，三个附件中的第二附件采用 Unicode 格式。在无法显示 Unicode 的终端上，这些附件以引用的可打印格式显示。

根据发件人的来源国家/地区收到的邮件

在此示例中，日志显示根据特定发件人组的源国家/地区接收的邮件。

```
Thu Apr  6 06:50:18 2017 Info: ICID 73 ACCEPT SG WHITELIST match country[us] SBRS -10.0
country United States
```

生成或重写邮件的日志条目

某些功能可创建新的邮件，如重写/重定向操作（alt-rcpt-to 过滤器、反垃圾邮件 rcpt 重写、bcc() 操作、防病毒重定向等）。浏览日志时，您可能需要检查结果，添加更多 MID 以及 DCID。可能为以下这样的条目：

```
Tue Jun  1 20:02:16 2004 Info: MID 14 generated based on MID 13 by bcc filter 'nonetest'
```

或者：

```
Tue Jan 6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispam

Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by alt-rcpt-to-filter filter
'testfilt'
```

注意一点，“重写”条目可能会出现在表示使用新 MID 的日志行的后面。

发送到垃圾邮件隔离区的邮件

在用户将邮件发送到隔离区时，邮件日志会跟踪进出隔离区的移动，使用 RCID（RPC 连接 ID）标识 RPC 连接。在以下邮件日志中，邮件被标记为垃圾邮件，并发送到垃圾邮件隔离区：

```
Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From: <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To:
<stevel@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.chase.com>'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make
it a reality'

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>

Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient
policy DEFAULT in the inbound table

Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect

Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine
Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative
Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery
Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local
IronPort Spam Quarantine


Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877

Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877

Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done
```

使用传送日志

传送日志记录有关 AsyncOS 邮件传送操作的重要信息。日志消息为“无状态”消息，这意味着所有相关信息都会逐条记录在每条日志消息中，用户无需参考上一条日志消息即可了解当前传送尝试的相关信息。

传送日志记录有关每个收件人的邮件传送操作的所有信息。所有信息以符合逻辑的方式布置，并且使用思科提供的实用程序进行转换后，可供人类进行阅读。转换工具位置：
https://supportforums.cisco.com/document/33721/cisco-ironport-systems-contributed-tools

传送日志以二进制格式记录和传输，以提高资源效率。下表展示传送日志记录的信息：

表 *113:* 传送日志统计信息

统计	说明
传送状态	成功（邮件成功传送）或退回（邮件被硬退回）
Del_time	传送时间
Inj_time	Injection time. del_time - inj_time = 收件人邮件在队列中停留的时间
字节	消息大小
中	消息 ID
Ip	收件人主机 IP。接收或退回收件人邮件的主机的 日IP 地址
来源	源信封，也称为信封发件人或 MAIL FROM
Source_ip	源主机 IP。传入邮件的主机的 IP 地址
代码	来自收件人主机的 SMTP 响应代码
应答	来自收件人主机的 SMTP 响应消息
Rcpt Rid	收件人 ID。收件人 ID 以 <0> 开头，有多个收件人的邮件包含多个收件人 ID
目标	目标信封
尝试	传送尝试的次数

如果传送状态为退回，传送日志中会显示以下附加信息：

表 *114:* 传送日志退回信息

统计	说明
原因	传送过程中，SMTP 响应的 RFC 1893 增强邮件状态代码解释
代码	来自收件人主机的 SMTP 响应代码
Error	来自收件人主机的 SMTP 响应消息

如已设置日志信头（请参阅日志记录邮件信头，第 899 页），传送信息后面会显示信头信息：

表 *115:* 传送日志信头信息

统计	说明
Customer_data	标记所记录信头的开始部分的 XML 标签
标头名称	信头的名称

统计	说明
值	所记录的信头的内容

传送日志条目示例

下文示例展示的是各种类型的传送日志条目。

成功的邮件传送

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

传送状态退回

```
<bounce del_time="Sun Jan 05 08:28:33.073 2003" inj_time="Mon Jan 05 08:28:32.929 2003"

bytes="4074" mid="94157762" ip="0.0.0.0" from="campaign1@yourdomain.com"

source_ip="192.168.102.1 "reason="5.1.0 - Unknown address error" code="550"

error="["Requested action not taken: mailbox unavailable"]">


<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

</bounce>
```

包含日志信头的传送日志条目

```
<success del_time="Tue Jan 28 15:56:13.123 2003" inj_time="Tue Jan 28 15:55:17.696 2003"
bytes="139" mid="202" ip="10.1.1.13" from="campaign1@yourdomain.com"
source_ip="192.168.102.1" code="250" reply="sent">


<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

<customer_data>

<header name="xname" value="sh"/>

</customer_data>

</success>
```

使用退回日志

退回日志记录有关每个退回收件人的所有信息。下表展示退回日志记录的信息：

表 *116:* 退回日志统计信息

统计	说明
Timestamp	退回事件发生的时间
日志级别	此退回日志的明细级别
退回类型	退回或延迟（例如，硬退回或软退回）
MID/RID	邮件 ID 和收件人 ID
来源	源信封
目标	目标信封
原因	传送过程中，SMTP 响应的 RFC 1893 增强邮件状态代码解释
解决方案	来自收件人主机的 SMTP 响应代码和消息

此外，如已指定要记录的邮件大小或已设置**日志信头**（请参阅日志记录邮件信头，第 899 页），退回信息后面会显示邮件和信头信息：

表 *117:* 退回日志信头信息

标头	信头名称和内容
消息	所记录的消息内容

退回日志条目示例

软退回收件人（退回类型 = 延迟）

```
Thu Dec 26 18:37:00 2003 Info: Delayed: 44451135:0
From:<campaign1@yourdomain.com> To:<user@sampledomain.com>


Reason: "4.1.0 - Unknown address error" Response: "('451',
['<user@sampledomain.com> Automated block triggered by suspicious
activity from your IP address (10.1.1.1). Have your system administrator
send e-mail to postmaster@sampledomain.com if you believe this block is
in error'])"
```

硬退回收件人（退回类型 = 退回）

```
Thu Dec 26 18:36:59 2003 Info: Bounced: 45346670:0 From:<campaign1@yourdomain.com>
To:<user2@sampledomain.com>


Reason: "5.1.0 - Unknown address error" Response: "('550', ['There is no such active
account.'])"
```

包含邮件正文和日志信头的退回日志

```
Wed Jan 29 00:06:30 2003 Info: Bounced: 203:0 From:<campaign1@yourdomain.com>
To:<user@sampledomain.com>


Reason:"5.1.2 - Bad destination host" Response: "('000', [])" Headers: ['xname:
userID2333']' Message: Message-Id:



<1u5jak$6b@yourdomain.com>\015\012xname: userID2333\015\012subject:
Greetings.\015\012\015\012Hi Tom:'
```

注释 文本字符串 \015\012 表示换行（例如 CRLF）。

使用状态日志

状态日志记录 CLI 状态命令中的系统统计信息，包括 status、status detail 以及 dnsstatus 命令。记录期限使用 logconfig 中的 setup 子命令设置。状态日志中的每个计数器或记录的速率为从上次重置计数器起至当前的值。

了解状态日志

下表展示状态日志标签和匹配的系统统计信息。

表 *118:* 状态日志统计信息

统计	说明
CPULd	CPU使用率
DskIO	硬盘 I/O 使用率
RAMUtil	内存使用率
QKUsd	已用队列容量 (KB)
QKFre	可用队列容量 (KB)
CrtMID	邮件ID(MID)
CrtICID	注入连接 ID (ICID)
CRTDCID	传送连接 ID (DCID)
InjBytes	已注入的总邮件大小（字节）
InjMsg	注入的邮件数量
InjRcp	注入的收件人数量

统计	说明
GenBncRcp	生成的退回收件人数量
RejRcp	拒绝的收件人数量
DrpMsg	删除的邮件数量
SftBncEvnt	软退回事件的数量
CmpRcp	已经完成的收件人数量
HrdBncRcp	硬退回的收件人
DnsHrdBnc	DNS 硬退回
5XXHrdBnc	5XX 硬退回
FltrHrdBnc	内容过滤的硬退回
ExpHrdBnc	过期的硬退回
OtrHrdBnc	其他硬退回
DlvRcp	发送的收件人数量
DelRcp	已删除的收件人
GlbUnsbHt	全局取消订用命中数
ActvRcp	正在处理的收件人
UnatmptRcp	未尝试发送的收件人
AtmptRcp	已经尝试发送过的收件人
CrtCncIn	当前的入站连接数
CrtCncOut	当前的出站连接数
DnsReq	DNS 请求
NetReq	网络请求数
CchHit	缓存命中数
CchMis	缓存丢失数
CchEct	缓存排斥数
CchExp	缓存过期
CPUTTm	应用的 CPU 使用总时间

统计	说明
CPUETm	应用启动后经过的时间
MaxIO	邮件进程的每秒最大磁盘 I/O 操作数
RamUsd	分配的内存（字节）
SwIn	换入内存。
SwOut	换出内存。
SwPgIn	调入内存。
SwPgOut	调出内存。
MMLen	系统中的总邮件数
DstInMem	内存中的目标对象数
ResCon	资源节省 tarpit 值。由于系统负载繁重，传入邮件接受按此秒数延迟
WorkQ	此为工作队列中的当前邮件数
QuarMsgs	策略、病毒或爆发隔离区中的邮件数量（出现在多个隔离区的邮件只计算一次）
QuarQKUsd	策略、病毒和爆发隔离区邮件使用的千字节数
LogUsd	日志分区的使用百分比
BMLd	防病毒扫描的 CPU 使用百分比
CmrkLd	Cloudmark 反垃圾邮件扫描的 CPU 使用百分比
SophLd	Sophos 反垃圾邮件扫描的 CPU 使用百分比
McafLd	McAfee 防病毒扫描的 CPU 使用百分比
CASELd	CASE 扫描的 CPU 使用百分比
TotalLd	CPU 消耗总量
LogAvail	可用于日志文件的磁盘空间大小
EuQ	垃圾邮件隔离区中邮件的估计数量
EuqRls	垃圾邮件隔离区释放队列中邮件的估计数量
RptLD	报告过程中的 CPU 负载
QtnLd	隔离过程中的 CPU 负载

统计	说明
EncrQ	加密队列中的邮件

状态日志示例

```
Fri Feb 24 15:14:39 2006 Info: Status: CPULd 0 DskIO 0 RAMUtil 2 QKUsd 0 QKFre 8388608
CrtMID 19036 CrtICID 35284 CrtDCID 4861
InjMsg 13889 InjRcp 14230 GenBncRcp 12 RejRcp 6318 DrpMsg 7437 SftBncEvnt 1816 CmpRcp 6813
 HrdBncRcp 18 DnsHrdBnc 2 5XXHrdBnc
15 FltrHrdBnc 0 ExpHrdBnc 1 OtrHrdBnc 0 DlvRcp 6793 DelRcp 2 GlbUnsbHt 0 ActvRcp 0 UnatmptRcp
 0 AtmptRcp 0 CrtCncIn 0 CrtCncOut
0 DnsReq 143736 NetReq 224227 CchHit 469058 CchMis 504791 CchEct 15395 CchExp 55085 CPUTTm
 228 CPUETm 181380 MaxIO 350 RAMUsd
21528056 MMLen 0 DstInMem 4 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 3 AVLd 0 BMLd 0
 CASELd 3 TotalLd 3 LogAvail 17G EuQ 0
EuqRls 0
```

使用域调试日志

域调试日志记录客户端和服务器在邮件安全设备与指定收件人主机 SMTP 会话期间的通信。此日志类型主要用来调试特定收件人主机存在的问题。

表 *119:* 域调试日志统计信息

统计	说明
Timestamp	退回事件发生的时间
日志级别	此退回日志的明细级别
来源	源信封
目标	目标信封
原因	传送过程中，SMTP 响应的 RFC 1893 增强邮件状态代码解释
解决方案	来自收件人主机的 SMTP 响应代码和消息

域调试日志示例

```
Sat Dec 21 02:37:22 2003 Info: 102503993 Sent: 'MAIL FROM:<daily@dailyf-y-i.net>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'RCPT TO:<LLLSMILE@aol.com>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'DATA'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '354 START MAIL INPUT, END WITH "." ON A
LINE BY ITSELF'
```

```
Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '250 OK'
```

使用注入调试日志

注入调试日志记录邮件安全设备和连接到系统的指定主机之间的SMTP会话。可参考注入调试日志，排查邮件安全设备和从互联网发起连接的客户端之间的通信问题。该日志记录两个系统之间传送的所有字节并将这些字节分类为“已发送至”连接主机或“接收自”连接主机。

必须通过指定 IP 地址、IP 范围、主机名或部分主机名，表明要记录的主机对话。日志将记录 IP 范围内的所有连接 IP 地址。而且，在一个部分域内的所有主机都将被记录。系统将在连接的 IP 地址上执行反向 DNS 查询，将 IP 地址转换为主机名。在 DNS 中没有相应 PTR 记录的 IP 地址不存在匹配的主机名。

此外，还必须指定要记录的会话数。

“注入调试”日志的每一行均包含下表中的如下信息。

表 *120:* 注入调试日志统计信息

统计	说明
Timestamp	数据的传输时间
ICID	注入连接 ID 是可与其他日志订用中同一连接关联的唯一标识符
发送数据/接收数据	标记“Sent to”的行是发送到所连接主机的实际数据量。标记“Received from”的行是从所连接主机接收的实际数据量。
IP 地址	所连接主机的 IP 地址

注入调试日志示例

```
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '220 postman.example.com
ESMTP\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'HELO
mail.remotehost.com\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250
postman.example.com\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'MAIL
FROM:<sender@remotehost.com>\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 sender
<sender@remotehost.com> ok\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'RCPT
TO:<recipient@example.com>\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 recipient
<recipient@example.com> ok\015\012'
Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'DATA\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '354 go ahead\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'To:
recipient@example.com\015\012Date: Apr 02 2003 10:09:44\015\012Subject: Test
Subject\015\012From: Sender <sender@remotehost.com>\015\012'
```

```
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'This is the content of the
message'
Wed Apr 2 14:30:04 Info: 6216 Sent to '172.16.0.22': '250 ok\015\012'

Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'QUIT\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '221
postman.example.com\015\012'
```

使用系统日志

表 *121:* 系统日志统计信息

统计	说明
Timestamp	数据的传输时间
消息	记录的事件

系统日志分析

在本示例中，系统日志展示了一些提交条目，包括发出提交命令的用户的名称和用户输入的注释。

```
Wed Sep 8 18:02:45 2004 Info: Version: 4.0.0-206 SN: XXXXXXXXXXXX-XXX

Wed Sep 8 18:02:45 2004 Info: Time offset from UTC: 0 seconds

Wed Sep 8 18:02:45 2004 Info: System is coming up

Wed Sep 8 18:02:49 2004 Info: bootstrapping DNS cache

Wed Sep 8 18:02:49 2004 Info: DNS cache bootstrapped

Wed Sep 8 18:13:30 2004 Info: PID 608: User admin commit changes: SSW:Password

Wed Sep 8 18:17:23 2004 Info: PID 608: User admin commit changes: Completed Web::SSW

Thu Sep 9 08:49:27 2004 Info: Time offset from UTC: -25200 seconds

Thu Sep 9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added a second CLI
log for examples

Thu Sep 9 08:51:53 2004 Info: PID 1237: User admin commit changes: Removed example CLI
log.
```

使用 CLI 审核日志

表 *122: CLI* 审核日志统计信息

统计	说明
Timestamp	数据的传输时间
PID	输入命令的特定 CLI 会话的进程 ID

统计	说明
消息	消息包含输入的 CLI 命令、CLI 输出（包括菜单、列表等）和显示的提示

CLI 审核日志示例

在本例中，CLI 审核日志显示用户对 PID 16434 输入以下 CLI 命令：who、textconfig。

```
Thu Sep 9 14:35:55 2004 Info: PID 16434: User admin entered 'who'; prompt was
'\nmail3.example.com> '


Thu Sep 9 14:37:12 2004 Info: PID 16434: User admin entered 'textconfig'; prompt was
'\nUsername Login Time Idle Time Remote Host What\n======== ========== =========
=========== ====\nadmin Wed 11AM 3m 45s 10.1.3.14 tail\nadmin 02:32PM
0s 10.1.3.14 cli\nmail3.example.com> '


Thu Sep 9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt was '\nThere are
no text resources currently defined.\n\n\nChoose the operation you want to perform:\n-
NEW - Create a new text resource.\n- IMPORT - Import a text resource from a file.\n[]> '
```

使用 FTP 服务器日志

表 *123: FTP* 服务器日志统计信息

统计	说明
Timestamp	数据的传输时间
ID	连接 ID。每个 FTP 连接的单独 ID
消息	日志条目的消息部分可以是日志文件状态信息或 FTP 连接信息（登录、上传、下载、注销等）

FTP 服务器日志示例

在本例中，FTP 服务器日志记录了连接（ID：1）。显示了传入连接的 IP 地址，以及活动（上传和下载文件）和注销。

```
Wed Sep 8 18:03:06 2004 Info: Begin Logfile

Wed Sep 8 18:03:06 2004 Info: Version: 4.0.0-206 SN: 00065BF3BA6D-9WFWC21

Wed Sep 8 18:03:06 2004 Info: Time offset from UTC: 0 seconds

Wed Sep 8 18:03:06 2004 Info: System is coming up

Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds

Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on 172.19.0.86

Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS
```

```
Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes

Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes

Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout
```

使用 HTTP 日志

表 *124: HTTP* 日志统计信息

统计	说明
Timestamp	数据的传输时间
ID	Session ID
req	连接计算机的 IP 地址
user	连接用户的用户名
消息	有关所执行操作的信息。可能包括 GET 或 POST 命令，或系统状态等。

HTTP 日志示例

在本示例中，HTTP 日志展示了管理员用户与 GUI 的交互（运行“系统设置向导”(System Setup Wizard) 等）。

```
Wed Sep 8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting to https port 443

Wed Sep 8 18:17:23 2004 Info: http service listening on 192.168.0.1:80

Wed Sep 8 18:17:23 2004 Info: https service listening on 192.168.0.1:443

Wed Sep 8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds

Wed Sep 8 11:17:24 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg POST
/system_administration/system_setup_wizard HTTP/1.1 303

Wed Sep 8 11:17:25 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/system_administration/ssw_done HTTP/1.1 200

Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/incoming_mail_overview HTTP/1.1 200

Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin&height=190
HTTP/1.1 200

Wed Sep 8 11:18:46 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/classification_graph?injector=&width=325&interval=0&type=recipientsin&height=19
0 HTTP/1.1 200

Wed Sep 8 11:18:49 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/quarantines HTTP/1.1 200
```

使用 NTP 日志

表 *125: NTP* 日志统计信息

统计	说明
Timestamp	数据的传输时间
消息	消息包含目标到服务器的简单网络时间协议 (SNTP) 查询或 adjust: 消息

NTP 日志示例

在本示例中，NTP 日志显示轮询 NTP 主机两次的设备。

```
Thu Sep 9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset -652

Thu Sep 9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us next_poll: 4096

Thu Sep 9 08:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset -1152

Thu Sep 9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us next_poll: 4096
```

使用扫描日志

扫描日志包含设备扫描引擎的所有LOG和COMMON消息。可参阅“系统管理”一章中的“警报”部分，了解 COMMON 和 LOG 警报消息。

表 *126:* 扫描日志统计信息

统计	说明
Timestamp	数据的传输时间
消息	消息包含针对某一扫描引擎的应用故障、发送的警报、失败的警报或日志错误消息。

扫描日志示例

在本示例中，日志显示发送有关 Sophos 防病毒警告警报的设备的历史记录。

```
Wed Feb 23 22:05:48 2011 Info: Internal SMTP system attempting to send a message to
alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos
antivirus - The Anti-Virus database on this system is...' (attempt #0).


Wed Feb 23 22:05:48 2011 Info: Internal SMTP system successfully sent a message to
alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos
antivirus - The Anti-Virus database on this system is...'.


Wed Feb 23 22:05:48 2011 Info: A Anti-Virus/Warning alert was sent to alerts@example.com
with subject "Warning <Anti-Virus> mail3.example.com: sophos antivirus - The Anti-Virus
```

```
database on this system is...".
```

使用反垃圾邮件日志

表 *127:* 反垃圾邮件日志统计信息

统计	说明
Timestamp	数据的传输时间
消息	消息包含反垃圾邮件更新检查，以及检查结果（是否需要引擎或反垃圾邮件规则更新）

反垃圾邮件日志示例

在本例中，反垃圾邮件日志显示反垃圾邮件引擎检查垃圾邮件定义更新和 CASE 更新：

```
Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19103) : case-daemon: server
successfully spawned child process, pid 19111

Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19111) : startup: Region profile:
Using profile global

Fri Apr 13 18:59:59 2007 Info: case antispam - engine (19111) : fuzzy: Fuzzy plugin v7
successfully loaded, ready to roll

Fri Apr 13 19:00:01 2007 Info: case antispam - engine (19110) : uribllocal: running URI
blocklist local

Fri Apr 13 19:00:04 2007 Info: case antispam - engine (19111) : config: Finished loading
configuration
```

使用灰色邮件日志

统计	说明
Timestamp	数据的传输时间
消息	邮件包含有关灰色邮件引擎、状态、配置的信息等。

灰色邮件日志示例

```
Tue Mar 24 08:56:45 2015 Info: graymail [BASE] Logging at DEBUG level

Tue Mar 24 08:56:45 2015 Info: graymail [HANDLER] Initializing request handler

Tue Mar 24 08:56:50 2015 Info: graymail [ENGINE] Loaded graymail scanner library

Tue Mar 24 08:56:50 2015 Info: graymail [ENGINE] Created graymail scanner instance

Tue Mar 24 08:56:50 2015 Info: graymail [HANDLER] Debug mode disabled on graymail process
```

```
Tue Mar 24 08:56:50 2015 Info: graymail [HANDLER] Starting thread WorkerThread_0
```

使用防病毒日志

表 *128:* 防病毒日志统计信息

统计	说明
Timestamp	数据的传输时间
消息	消息包含防病毒更新检查，以及检查结果（是否需要引擎或病毒定义更新）

防病毒日志示例

在本例中，防病毒日志显示 Sophos 防病毒引擎检查病毒定义 (IDE) 更新和引擎本身的更新。

```
Thu Sep 9 14:18:04 2004 Info: Checking for Sophos Update

Thu Sep 9 14:18:04 2004 Info: Current SAV engine ver=3.84. No engine update needed

Thu Sep 9 14:18:04 2004 Info: Current IDE serial=2004090902. No update needed.
```

您可以将此暂时设置为调试级别，帮助诊断防病毒引擎为什么对给定邮件做出了特定判断。调试日志记录信息非常冗长，请谨慎使用。

使用 AMP 引擎日志

AMP 引擎日志包含以下内容的详细信息：

- 发送到文件信誉服务器的文件信誉查询和从文件信誉服务器收到的响应。
- 文件分析，如果文件已上传到文件分析服务器。文件分析的状态会定期记录，直到从文件分析服务器收到响应。

AMP 引擎日志条目示例

以下是基于某些方案的 AMP 引擎日志条目示例：

文件信誉和文件分析服务器的初始化

```
Wed Oct 5 15:17:31 2016 Info: File reputation service initialized successfully
Wed Oct 5 15:17:31 2016 Info: The following file type(s) can be sent for File Analysis:
Microsoft Windows / DOS Executable, Microsoft Office 97-2004 (OLE), Microsoft Office 2007+
 (Open XML), Other potentially malicious file types, Adobe Portable Document Format (PDF).
 To allow analysis of new file type(s), go to Security Services > File Reputation and
Analysis.
Wed Oct 5 15:17:31 2016 Info: File Analysis service initialized successfully
```

文件信誉服务器未配置

```
Tue Oct 4 23:15:24 2016 Warning: MID 12 reputation query failed for attachment 'Zombies.pdf'
 with error "Cloud query failed"
```

文件信誉查询的初始化

```
Fri Oct 7 09:44:04 2016 Info: File reputation query initiating. File Name = 'mod-6.exe',
MID = 5, File Size = 1673216 bytes,
File Type = application/x-dosexec
```

统计	说明
文件名	其 SHA-256 哈希标识符发送到文件信誉服务器的文件的名称。 如果文件名不可用，则显示为“未知”。
MID	用于跟踪通过邮件管道传递的邮件的邮件 ID。
文件大小	将其 SHA-256 哈希标识符发送到文件信誉服务器的文件的大小。
文件类型	将其 SHA-256 哈希标识符发送到文件信誉服务器的文件的类型。 以下是支持的文件类型： • Microsoft Windows / DOS Executable • Microsoft Office 97-2004 (OLE) • Microsoft Office 2007+ (Open XML) • 其他潜在恶意文件类型 • Adobe 便携式文档格式 (PDF)

从文件信誉服务器收到的文件信誉查询响应

```
Fri Oct 7 09:44:06 2016 Info: Response received for file reputation query from Cloud. File
Name = 'mod-6.exe', MID = 5, Disposition = MALICIOUS, Malware = W32.061DEF69B5-100.SBX.TG,
Reputation Score = 73, sha256 =
061def69b5c100e9979610fa5675bd19258b19a7ff538b5c2d230b467c312f19, upload_action = 2
```

统计	说明
文件名	其 SHA-256 哈希标识符发送到文件信誉服务器的文件的名称。 如果文件名不可用，则显示为“未知”。
MID	用于跟踪通过邮件管道传递的邮件的邮件 ID。

统计	说明
处理结果	文件信誉处理值为： • 恶意 • 正常 • 文件未知 - 信誉得分为零时。 • 判定未知 - 处置为“文件未知”，且值为非零时。
恶意软件	恶意软件威胁的名称。
信誉得分	文件信誉服务器分配给文件的信誉得分。 如果文件处置是**判定未知**，设备将根据信誉得分和阈值调整文件声誉判定。
上传操作	文件信誉服务器推荐的对给定文件应用的上传操作值： • 0 - 无需发送上传 • 1 - 发送文件进行上传。 **注释** 当上传操作值为“1”时，设备将上传该文件。 • 2 - 不发送文件进行上传 • 3 - 仅发送元数据进行上传

已上传文件进行分析以及文件分析过程

```
Wed Sep 28 11:31:58 2016 Info: File uploaded for analysis. SHA256:
e7ae35a8227b380ca761c0317e814e4aaa3d04f362c6b913300117241800f0ea

Wed Sep 28 11:36:58 2016 Info: File Analysis is running for SHA:
e7ae35a8227b380ca761c0317e814e4aaa3d04f362c6b913300117241800f0ea

Fri Oct 7 07:39:13 2016 Info: File Analysis complete. SHA256:
16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc, Submit Timestamp:
1475825466, Update Timestamp: 1475825953, Disposition: 3 Score: 100, run_id: 194926004
Details: Analysis is completed for the File
SHA256[16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc]
Spyname:[W32.16454AFF50-100.SBX.TG]
```

统计	说明
SHA256	相应文件的 SHA-256 散列标识符。
提交时间戳	设备将文件上传到文件分析服务器的日期和时间。
更新时间戳	文件的文件分析完成的日期和时间

统计	说明
处理结果	文件信誉处置值包括： • 1 - 未检测到恶意软件 • 2 - 正常 • 3 - 恶意软件
得分	文件分析服务器分配给文件的分析分数。
运行 ID	文件分析服务器为特定文件分析分配给文件的数字值 (ID)。
Details	如果在文件分析期间报告错误，则显示其他信息，否则会指示文件的最终分析已完成。
间谍软件名称	威胁的名称（如果在文件分析期间在文件中发现恶意软件）。

未上传文件进行分析

```
Wed Sep 14 12:27:52 2016 Info: File not uploaded for analysis. MID = 0 File
SHA256[a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82] file
mime[text/plain] Reason: No active/dynamic contents exists
```

统计	说明
MID	用于跟踪通过邮件管道传递的邮件的邮件 ID。
文件 MIME	文件的 MIME 类型。
原因	以下是即使 upload_action 设置为“1”，文件也未上传到文件分析服务器的原因值之一： • 文件已由另一个节点上传 - 文件已通过其他设备上传到文件分析服务器。 • 正在进行文件分析 - 文件已被选中进行上传且上传正在进行中。 • 文件已上传到文件分析服务器 • 不是支持的文件类型 • 文件大小超出范围 - 上传文件大小超过文件分析服务器设置的阈值限制。 • 上传队列已满 • 文件分析服务器错误 • 不存在活动/动态内容 • 一般/未知错误

由于文件上传限制，跳过文件上传而不进行文件分析

```
Tue Jun 20 13:22:56 2017 Info: File analysis upload skipped. SHA256:
b5c7e26491983baa713c9a2910ee868efd891661c6a0553b28f17b8fdc8cc3ef,Timestamp[1454782976]
details[File SHA256[b5c7e26491983baa713c9a2910ee868efd891661c6a0553b28f17b8fdc8cc3ef] file
mime[application/pdf], upload priority[Low] not uploaded, re-tries[3], backoff[986]
discarding ...]
Tue Jun 20 13:22:56 2017 Critical: The attachment could not be uploaded to the
```

```
File Analysis server because the appliance exceeded the upload limit
```

统计	说明
SHA256	相应文件的 SHA-256 散列标识符。
Timestamp	文件无法上传到文件分析服务器的日期和时间。
Details	文件分析服务器错误的详细信息。
文件 MIME	文件的 MIME 类型。
上传优先级	上传优先级值为： • 高 - 针对所有选定的文件类型，PDF 文件类型除外。 • 低 - 仅针对 PDF 文件类型
重新尝试	对给定文件执行的上传尝试次数。 **注释** 最多可以对给定文件执行三次上传尝试。
退避 (x)	设备在尝试将文件上传到文件分析服务器之前需要等待的秒数 (x)。当设备达到每日上传限制时会发生此情况。
关键 (原因)	无法将附件上传到文件分析服务器，因为设备超出了上传限制。

由于文件分析服务器错误，跳过文件上传而不进行文件分析

```
Sat Feb 6 13:22:56 2016 Info:SHA256:
69e17e213732da0d0cbc48ae7030a4a18e0c1289f510e8b139945787f67692a5,Timestamp[1454959409]
details[Server Response HTTP code:[502]]
```

统计	说明
SHA256	相应文件的 SHA-256 散列标识符。
Timestamp	尝试将文件上传到文件分析服务器的日期和时间。
Details	有关文件分析服务器错误的信息。

文件追溯判定已收到

```
Fri Oct 7 07:39:13 2016 Info: Retrospective verdict received. SHA256:
16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc, Timestamp: 1475832815.7,
Verdict: MALICIOUS, Reputation Score: 0, Spyname: W32.16454AFF50-100.SBX.
```

统计	说明
SHA256	相应文件的 SHA-256 散列标识符。
Timestamp	从文件分析服务器接收文件追溯判定的日期和时间。

统计	说明
判定	文件追溯判定值是恶意的或安全的。
声誉得分	文件信誉服务器分配给文件的信誉得分。
Spyname	威胁的名称（如果在文件分析期间在文件中发现恶意软件）。

使用垃圾邮件隔离区日志

表 *129:* 垃圾邮件日志统计信息

统计	说明
Timestamp	数据的传输时间
消息	消息包含所采取的操作（隔离邮件、从隔离区释放的邮件等）。

垃圾邮件隔离区日志示例

在本示例中，日志展示从隔离区释放至 admin@example.com 的邮件 (MID 8298624)。

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for all

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624 (skipping work
queue)

Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to admin@example.com

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625 (skipping work
queue)

Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to admin@example.com
```

使用垃圾邮件隔离区 GUI 日志

表 *130:* 垃圾邮件 *GUI* 日志统计信息

统计	说明
Timestamp	数据的传输时间
消息	消息包含所采取的操作，包括用户身份验证等。

垃圾邮件隔离区 GUI 日志示例

在本示例中，日志显示了成功的身份验证、登录和注销：

```
Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port 82
```

```
Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1, port 83

Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin

Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCfO session:10.251.23.228

Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228

Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin
```

使用 LDAP 调试日志

表 *131: LDAP* 调试日志统计信息

统计	说明
Timestamp	数据的传输时间
消息	LDAP 调试消息

LDAP 调试日志示例

注释 日志文件中的行目没有编号。下文出于方便对各行进行了编号。

1	`Thu Sep  9 12:24:56 2004 Begin Logfile`
2	`Thu Sep  9 12:25:02 2004 LDAP:` `Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa`
3	`Thu Sep  9 12:25:02 2004 LDAP:` `Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa`
4	`Thu Sep  9 12:25:02 2004 LDAP:` `Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa`
5	`Thu Sep  9 12:28:08 2004 LDAP: Clearing LDAP cache`
6	`Thu Sep  9 13:00:09 2004 LDAP:` `Query '(&(ObjectClass={g})(mailLocalAddress={a}))' to server sun (sun.qa:389)`

7	`Thu Sep  9 13:00:09 2004 LDAP:`
	`After substitute, query is '(&(ObjectClass=inetLocalMailRecipient)`
	`(mailLocalAddress=rroute.d00002b.loc@ldap.route.local.add00002.qa))'`

8	`Thu Sep  9 13:00:09 2004 LDAP: connecting to server`

9	Thu Sep 9 13:00:09 2004 LDAP: connected
10	Thu Sep 9 13:00:09 2004 LDAP: Query (&(ObjectClass=inetLocalMailRecipient) (mailLocalAddress=rroute.d00002b.loc@ldap.route.local.add00002.qa)) returned 1 results
11	Thu Sep 9 13:00:09 2004 LDAP: returning: [<LDAP:>]

可参考本日志阅读上文介绍的日志文件。

表 *132: LDAP* 调试日志详细信息示例

行号	说明
1	日志文件已初始化。
2 3 4	侦听程序配置为使用 LDAP 进行伪装，具体使用名为“sun.masquerade”的 LDAP 查询。 侦听程序在 LDAP 服务器上查询地址 employee@routing.qa，找到匹配项，生成伪装地址 employee@mail.qa，并根据伪装配置将该地址写入邮件信头和/或源信封。
5	用户手动运行 ldapflush。
6	查询随即发送至端口 389 sun.qa。查询模板为 (&(ObjectClass={g})(mailLocalAddress={a}))。 {g} 将替换为调用筛选器中指定的组名，rcpt-to-group 或 mail-from-group 规则均可。 {a} 将替换为具体地址。
7	这便是查询在发送到 LDAP 服务器之前的样态，接下来将发生（前面介绍的）替换。
8	此时与服务器的连接并没有建立，请建立连接。
9	发送至服务器的数据。
10	结果是空正值，这表示返回了一条记录，但因为查询没有请求任何字段，因此没有要报告的数据。查询检查数据库中是否存在匹配项时，这些数据将用于组和接受查询。

使用安全列表/阻止列表日志

下表显示在安全列表/阻止列表日志中记录的统计信息。

表 *133:* 安全列表/阻止列表日志统计信息

统计	说明
Timestamp	数据的传输时间。
消息	消息包含采取的操作，包括用户身份验证等。

安全列表/阻止列表日志示例

在本示例中，安全列表/阻止列表日志显示每两隔小时创建数据库快照的设备。它还显示何时将发件人添加到数据库中。

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007 Info: Version:
6.0.0-425 SN: XXXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007 Info: Time offset from UTC:
10800 seconds Fri Sep 28 14:22:33 2007 Info: System is coming up.


Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been created.

.........................

Mon Oct 1 14:16:09 2007 Info: SLBL: The database snapshot has been created.

Mon Oct 1 14:37:39 2007 Info: SLBL: The database snapshot has been created.

Mon Oct 1 15:31:37 2007 Warning: SLBL: Adding senders to the database failed.

Mon Oct 1 15:32:31 2007 Warning: SLBL: Adding senders to the database failed.

Mon Oct 1 16:37:40 2007 Info: SLBL: The database snapshot has been created.
```

使用报告日志

下表显示在报告日志中记录的统计信息。

表 *134:* 报告日志统计信息

统计	说明
Timestamp	数据的传输时间。
消息	消息包含采取的操作，包括用户身份验证等。

报告日志示例

在本示例中，报告日志显示在信息日志级别设置的设备。

```
Wed Oct 3 13:39:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:39:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:40:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-40

Wed Oct 3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%). Not found: 1692

Wed Oct 3 13:40:53 2007 Info: Period hour using 36800 (KB)

Wed Oct 3 13:40:53 2007 Info: Period day using 2768 (KB)

Wed Oct 3 13:40:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:40:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533 seconds

Wed Oct 3 13:41:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-41

Wed Oct 3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%). Not found: 1692

Wed Oct 3 13:41:53 2007 Info: Period hour using 36800 (KB)

Wed Oct 3 13:41:53 2007 Info: Period day using 2768 (KB)

Wed Oct 3 13:41:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:41:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:42:03 2007 Info: Update 2 registered appliance at 2007-10-03-13-42
```

使用报告查询日志

下表显示在报告查询日志中记录的统计信息。

表 *135:* 报告查询日志统计信息

统计	说明
Timestamp	数据的传输时间。
消息	消息包含采取的操作，包括用户身份验证等。

报告查询日志示例

在本示例中，报告查询日志显示从 2007 年 8 月 29 日到 10 月 10 日期间运行每日持续邮件流量查询的设备。

```
Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804479.

Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804480.
```

```
Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610228.

Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610229 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.

DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTENT_FILTER',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_PROCESSED'] for rollup period "day" with
interval range 2007-08-29 to 2007-10-01
with key constraints

None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM'] returning results from
0 to 2 sort_ascending=False.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610229.

Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610230 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.

TOTAL_HARD_BOUNCES', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval
range 2007-08-29 to
2007-10-01 with key constraints None sorting on
['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES'] returning
results from 0 to 2 sort_ascending=False.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

使用更新程序日志

表 ***136:*** 更新程序日志统计信息

统计	说明
Timestamp	数据的传输时间。
消息	消息包含系统服务更新信息，AsyncOS 更新检查以及下一次更新的计划日期和时间。

更新程序日志示例

在本示例中，日志显示设备使用全新 McAfee 防病毒定义进行更新。

```
Fri Sep 19 11:07:51 2008 Info: Starting scheduled update

Fri Sep 19 11:07:52 2008 Info: Acquired server manifest, starting update 11

Fri Sep 19 11:07:52 2008 Info: Server manifest specified an update for mcafee

Fri Sep 19 11:07:52 2008 Info: mcafee was signalled to start a new update

Fri Sep 19 11:07:52 2008 Info: mcafee processing files from the server manifest

Fri Sep 19 11:07:52 2008 Info: mcafee started downloading files

Fri Sep 19 11:07:52 2008 Info: mcafee downloading remote file
"http://stage-updates.ironport.com/mcafee/dat/5388"
```

```
Fri Sep 19 11:07:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:12:52
2008

Fri Sep 19 11:08:12 2008 Info: mcafee started decrypting files

Fri Sep 19 11:08:12 2008 Info: mcafee decrypting file
"mcafee/dat/5388" with method "des3_cbc"

Fri Sep 19 11:08:17 2008 Info: mcafee started decompressing files

Fri Sep 19 11:08:17 2008 Info: mcafee started applying files

Fri Sep 19 11:08:17 2008 Info: mcafee applying file "mcafee/dat/5388"

Fri Sep 19 11:08:18 2008 Info: mcafee verifying applied files

Fri Sep 19 11:08:18 2008 Info: mcafee updating the client manifest

Fri Sep 19 11:08:18 2008 Info: mcafee update completed

Fri Sep 19 11:08:18 2008 Info: mcafee waiting for new updates

Fri Sep 19 11:12:52 2008 Info: Starting scheduled update

Fri Sep 19 11:12:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:17:52
2008

Fri Sep 19 11:17:52 2008 Info: Starting scheduled update

Fri Sep 19 11:17:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:22:52
2008
```

更新程序日志示例

在此示例中，日志显示禁用的自动更新，以及应用于 Sophos 防病毒定义的备份。

```
Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “postx”

Fri Mar 10 15:05:55 2017 Debug: postx updates disabled

Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “postx”

Fri Mar 10 15:05:55 2017 Trace: command session starting

Fri Mar 10 15:05:55 2017 Info: Automatic updates disabled for engine Sophos engine

Fri Mar 10 15:05:55 2017 Info: Sophos: Backup update applied successfully

Fri Mar 10 15:05:55 2017 Info: Internal SMTP system attempting to send a message to
abshastr@ironport.com
with subject ‘Automatic updates are now disabled for sophos’ attempt #0).

Fri Mar 10 15:05:55 2017 Debug: amp feature key disabled

Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “amp”

Fri Mar 10 15:05:55 2017 Debug: amp feature key disabled
```

了解跟踪日志

跟踪日志记录有关 AsyncOS 的邮件操作的信息。此类日志消息包含在邮件日志中。

设备消息跟踪组件将使用跟踪日志创建消息跟踪数据库。由于构建数据库的过程中会使用日志文件，因此跟踪日志是动态的。跟踪日志中的信息不是供人类阅读或分析的。

您还可以使用思科安全管理设备查看多个邮件安全设备提供的跟踪信息。

使用身份验证日志

身份验证日志记录成功的用户登录和失败的登录尝试。

表 *137:* 身份验证日志统计信息

统计	说明
Timestamp	数据的传输时间。
消息	消息包含尝试登录到设备的用户的用户名，以及用户的身份验证情况。

身份验证日志示例

在本示例中，日志显示用户“admin”、“joe”以及“dan”的登录尝试。

```
Wed Sep 17 15:16:25 2008 Info: Begin Logfile

Wed Sep 17 15:16:25 2008 Info: Version: 6.5.0-262 SN: XXXXXXX-XXXXX

Wed Sep 17 15:16:25 2008 Info: Time offset from UTC: 0 seconds

Wed Sep 17 15:18:21 2008 Info: User admin was authenticated successfully.

Wed Sep 17 16:26:17 2008 Info: User joe failed authentication.

Wed Sep 17 16:28:28 2008 Info: User joe was authenticated successfully.

Wed Sep 17 20:59:30 2008 Info: User admin was authenticated successfully.

Wed Sep 17 21:37:09 2008 Info: User dan failed authentication.
```

由于密码错误导致双因素身份验证登录失败的示例

在此示例中，日志显示由于输入的密码不正确导致双因素身份验证登录失败。

```
Thu Mar 16 05:47:47 2017 Info: Trying RADIUS server example.cisco.com

Thu Mar 16 05:48:18 2017 Info: Two-Factor RADIUS Authentication failed.

Thu Mar 16 05:48:48 2017 Info: An authentication attempt by the user **** from
21.101.210.150 failed
```

由于超时导致双因素身份验证登录失败的示例

在此示例中，日志显示由于超时而导致的双因素身份验证登录失败。

```
Thu Mar 16 05:46:04 2017 Info: Trying RADIUS server example.cisco.com

Thu Mar 16 05:46:59 2017 Info: RADIUS server example.cisco.com communication error. No
valid responses from server (timeout).

Thu Mar 16 05:46:59 2017 Info: Two-Factor Authentication RADIUS servers timed out.
Authentication could fail due to this.
```

双因素身份验证登录成功示例

在本示例中，日志显示双因素身份验证登录成功。

```
Thu Mar 16 05:49:05 2017 Info: Trying RADIUS server example.cisco.com

Thu Mar 16 05:49:05 2017 Info: Two-Factor RADIUS Authentication was successful.

Thu Mar 16 05:49:05 2017 Info: The user admin successfully logged on from 21.101.210.150
using an HTTPS connection.
```

使用配置历史记录日志

配置历史记录日志包含一个配置文件以及一个额外部分，其中列出了用户名、有关用户在配置中的什么位置进行更改的说明以及用户在提交更改时输入的备注。每次用户提交更改时，都会创建一个包含更改后的配置文件的新日志。

配置历史记录日志示例

在本示例中，配置历史记录日志会显示用户（管理员）向定义允许哪些本地用户登录系统的表添加了访客用户。

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<!--

XML generated by configuration change.

Change comment: added guest user

User: admin

Configuration are described as:

This table defines which local users are allowed to log into the system.

Product: Cisco IronPort M160 Messaging Gateway(tm) Appliance

Model Number: M160

Version: 6.7.0-231

Serial Number: 000000000ABC-D000000

Number of CPUs: 1

Memory (GB): 4

Current Time: Thu Mar 26 05:34:36 2009

Feature "Cisco IronPort Centralized Configuration Manager": Quantity = 10, Time
```

```
Remaining = "25 days"

Feature "Centralized Reporting": Quantity = 10, Time Remaining = "9 days"

Feature "Centralized Tracking": Quantity = 10, Time Remaining = "30 days"

Feature "Centralized Spam Quarantine": Quantity = 10, Time Remaining = "30 days"

Feature "Receiving": Quantity = 1, Time Remaining = "Perpetual"

-->

<config>
```

日志订阅

配置日志订用

使用“系统管理”(System Administration) 菜单的“日志订阅”(Log Subscriptions)（或在 CLI 中使用 **logconfig** 命令）配置日志订阅。日志订阅创建存储 AsyncOS 活动信息（包括错误）的日志文件。日志订阅将检索或传送（推送）到另一台计算机。通常，日志订阅具有以下属性：

表 *138:* 日志文件属性

属性	说明
日志类型	定义记录的信息类型和日志订用的格式。有关详细信息，请参阅表：日志类型。
Name	供将来参考使用的日志订阅的昵称。
按文件大小回滚	回滚之前文件可以达到的最大大小。
按时间回滚	设置文件回滚的时间间隔。
日志级别	设置每个日志订阅的明细级别。
检索方法	定义从邮件安全设备获取日志订阅的方法。
日志文件名	作为文件写入磁盘时的实际名称。如使用多个邮件安全设备，日志文件名应唯一，以便标识生成日志文件的系统。

日志级别

日志级别决定日志中提供的信息量。日志可以是五种级别中的一种。设置的明细级别越高，创建的日志文件越大，对系统性能的影响也越大。除包含较低级别日志中的所有信息之外，较高级别日志中还包含其他信息。随着明细级别的增加，系统的性能会有所下降。

注释 可以为所有邮件日志类型选择日志级别。

表 *139:* 日志级别

日志级别	说明
Critical	最低的明细设置。仅记录错误。使用此设置不会监视性能和其他重要活动，但日志文件不会在短时间内达到最大大小。此日志级别相当于系统日志级别“警报”。
Warning	所有错误和系统创建的警告。使用此设置不会监视性能和其他重要活动。此日志级别相当于系统日志级别“警告”。
信息	信息设置可以捕获系统每一秒的操作。例如，打开的连接数或传送尝试次数。该信息级别是推荐的日志级别设置。此日志级别相当于系统日志级别“信息”。
调试	如要查明错误的原因，请使用调试日志级别。可临时使用该设置，然后返回默认级别。此日志级别相当于系统日志级别“调试”。
跟踪	建议仅将“跟踪”日志级别供开发人员使用。使用此级别会造成严重的系统性能下降，建议不要使用。此日志级别相当于系统日志级别“调试”(Debug)。

在 GUI 中创建日志订用

步骤 1 依次选择**系统管理 (System Administration) > 日志订用 (Log Subscriptions)**。

步骤 2 点击**添加日志订用 (Add Log Subscription)**。

步骤 3 选择日志类型，输入日志名称（用于日志目录）以及日志文件的名称。

步骤 4 指定 AsyncOS 在执行日志文件回滚前日志文件可达到的最大大小，以及回滚的时间间隔。有关回滚日志文件的详细信息，请参阅滚动更新日志订用，第 900 页。

步骤 5 选择日志级别。可用的选项包括重要、警告、信息、调试或跟踪。

步骤 6 配置日志检索方法。

步骤 7 提交并确认更改。

编辑日志订阅

步骤 1 依次选择**系统管理 (System Administration) > 日志订阅 (Log Subscriptions)**。

步骤 2 点击“日志设置”(Log Settings) 列中的日志名称。

步骤 3 更改日志订阅。

步骤 4 提交并确认更改。

配置日志记录的全局设置

系统在文本邮件日志和状态日志中定期记录系统测量数据。使用**系统管理 > 日志订用**页的“全局设置”部分中的**编辑设置**按钮（或在 CLI 中使用 `logconfig -> setup` 命令）进行配置：

- 系统测量频率。系统记录性能指标的时间间隔，以秒为单位。
- 是否记录邮件 ID 信头。
- 是否记录远程响应状态代码。
- 是否记录原始邮件的主题信头。
- 应为每封邮件记录的信头列表。

所有日志均可以选择包括以下三种数据：

1. 邮件 ID

   如配置此选项，每封邮件都会记录邮件 ID 信头（如果有）。注意，此邮件 ID 可能来自接收的邮件或可能由 AsyncOS 生成。例如：

   ```
   Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
   ```

2. 远程响应

   如配置此选项，每封邮件均会记录远程响应状态代码（如果有）。例如：

   ```
   Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as 9C8B425DA7'
   ```

   远程响应字符串是在传输 SMTP 对话期间响应 DATA 命令后收到的人类可读的文本。在本示例中，连接主机发出数据命令后的远程响应是“queued as 9C8B425DA7”。

   ```
   [...]

   250 ok hostname

   250 Ok: queued as 9C8B425DA7
   ```

   空格、标点（以及 250 响应中的 OK 字符）是从字符串开头部分截取的。只有空格是从字符串结尾部分截取的。例如，邮件安全设备对 DATA 命令默认回应字符串：250 Ok: Message MID accepted。因此，如果远程主机也是邮件安全设备，日志将记录字符串 "Message MID accepted"。

3. 源主题信头

   启用此选项后，日志将记录每封邮件的源主题信头。

   ```
   Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2

   Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>

   Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>
   ```

```
Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'

Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
```

日志记录邮件信头

有时，当邮件通过系统时，有必要记录邮件信头的存在性及其内容。可以在“日志订用”的“全局设置”页面（或在 CLI 中通过 logconfig -> logheaders 子命令）指定要记录的信头。邮件安全设备会在文本邮件日志、传送日志和退回日志中记录指定的邮件信头。如果信头存在，系统记录信头的名称和值。如果信头不存在，则不在日志中记录任何内容。

注释 在处理要记录的邮件的过程中，系统会评估存在于邮件中的所有信头，不管是否为日志记录指定了信头都是如此。

SMTP 协议的 RFC 位于 http://www.faqs.org/rfcs/rfc2821.html 并定义用户定义的信头。

如果已通过 logheaders 命令配置了要记录的信头，则在传输信息之后将显示信头信息：

表 *140: Log Headers*

信头名称	信头的名称
值	所记录的信头的内容

例如，指定“date, x-subject”作为要记录的信头会导致邮件日志中显示以下行目：

```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0]
[('date', 'Tue, 31 May 2005 10:13:18 -0700'), ('x-subject', 'Logging this header')]
```

使用 GUI 配置日志记录的全局设置

步骤 1 依次选择**系统管理 (System Administration) > 日志订用 (Log Subscriptions)**。

步骤 2 向下滚动至**全局设置 (Global Settings)** 部分。

步骤 3 点击**编辑设置 (Edit Settings)**。

步骤 4 指定系统测量频率、是否在邮件日志中包含邮件 ID 信头、是否包含远程响应以及是否包含每封邮件的源主题信头等信息。

步骤 5 输入想要在日志中包含的所有其他信头。

步骤 6 提交并确认更改。

滚动更新日志订用

为防止设备上的日志文件过大，当文件达到用户指定的最大大小或经过一定时间间隔后，AsyncOS 将执行“回滚”、对日志文件存档，并创建新文件来存储传入的日志数据。根据日志订用定义的检索方法，较旧的日志文件将存储设备上，以供检索或发送至外部计算机。有关如何从设备检索日志文件的详细信息，请参阅日志检索方法，第 861 页。

AsyncOS 在回滚日志文件时会执行以下操作：

- 使用回滚时间戳和表示日志文件已保存的字母“**s**”扩展名，对当前日志文件重命名。
- 创建新的日志文件，并使用“**current**”扩展名表明文件为当前文件。
- 将刚刚保存的日志文件发送至远程主机（如使用基于推送的检索方法）。
- 从同一订用传送过去不成功的日志文件（如使用基于推送的检索方法）。
- 超出当前保存的文件总数（如使用基于轮询的检索方法）时，删除日志订用中时间最早的文件。

  创建或编辑订用时，可使用 GUI 中的**系统管理 > 日志订用**页面，或在 CLI 中使用 logconfig 命令定义日志订用的回滚设置。触发日志文件回滚的两个设置为：

- 最大文件大小。
- 时间间隔。

按文件大小回滚

当日志文件达到最大文件大小时，AsyncOS 执行日志文件回滚，防止文件占用的磁盘空间过多。定义回滚的最大文件大小时，可使用后缀 m 表示兆字节，使用 k 表示千字节。例如，如希望 AsyncOS 在日志文件达到10 兆字节时进行回滚，可输入 10m。

按时间回滚

如希望定期执行回滚，可选择以下时间间隔之一：

- **无**。AsyncOS 仅在日志文件达到最大文件大小时执行回滚。
- **自定义时间间隔**。AsyncOS 将在上次回滚后经过指定的一段时间再执行回滚。创建计划回滚的自定义时间间隔时，可以 d、h 以及 m 为后缀，分别输入天数、时数以及分钟数。
- **每日回滚**。AsyncOS 每天在指定时间执行回滚。如选择每日回滚，请输入希望 AsyncOS 执行回滚的 24 时制时间，即 HH:MM。

  仅 GUI 提供每日回滚选项。如要在 CLI 中使用 logconfig 命令配置每日回滚，请选择“每周回滚”选项，并使用星号 (*) 指定 AsyncOS 应在每一天执行回滚。

- **每周回滚**。AsyncOS 将在每周的某一天或某几天的指定时间执行回滚。例如，您可以将 AsyncOS 设置为在每周三和每周五的午夜执行日志文件回滚。要配置每周回滚，请选择每周执行回滚的日期和 24 小时制时间 (HH:MM)。

  如使用 CLI，可以使用破折号 (-) 指定天数范围、使用星号 (*) 指定每周的每一天，或逗号 (,) 分隔多个日期和时间。

  下表展示如何使用 CLI 在周三和周五的午夜 (00:00) 对日志订用进行文件回滚。

表 *141: CLI* 中的每周日志回滚设置

Do you want to configure time-based log files rollover? [N]> y
Configure log rollover settings:
1. Custom time interval.
2. Weekly rollover.
[1]> 2
1. Monday
2. Tuesday
3. Wednesday
4. Thursday
5. Friday
6. Saturday
7. Sunday
Choose the day of week to roll over the log files. Separate multiple days with comma, or use "*" to specify every day of a week. Also you can use dash to specify a range like "1-5":
[]> **3, 5**
Enter the time of day to rollover log files in 24-hour format (HH:MM). You can specify hour as "*" to match every hour, the same for minutes. Separate multiple times of day with comma:
[]> **00:00**

按需回滚日志订阅

要使用 GUI 即时回滚日志订阅，请执行以下操作：

步骤 1 在“系统管理”(System Administration) > “日志订阅”(Log Subscriptions) 页面上，选中要回滚日志右侧的复选框。

步骤 2 或者，您通过选中“全部”(All) 复选框选择所有日志进行回滚。

步骤 3 选中一个或多个要回滚的日志后，**立即回滚 (Rollover Now)** 按钮随即启用。点击**立即回滚 (Rollover Now)** 按钮可回滚所选日志。

在 GUI 上查看最近的日志条目

准备工作

要通过 GUI 查看日志，必须在管理接口上启用 HTTP 或 HTTPS 服务。

步骤 1 依次选择**系统管理 (System Administration) > 日志订阅 (Log Subscriptions)**。

步骤 2 在表的**日志文件 (Log Files)** 列中，选择日志订阅。

步骤 3 登录。

步骤 4 选择一个要在浏览器中查看的日志文件或将其保存到磁盘。

在 CLI 中查看最近的日志条目（tail 命令）

AsyncOS 支持 tail 命令，该命令会显示在设备上配置的日志的最新条目。发出 tail 命令并选择当前配置的日志的编号以查看它。使用 Ctrl-C 退出 tail 命令。

示例

在以下示例中，tail 命令用于查看系统日志。（此日志跟踪 commit 命令中的用户注释以及其他信息。）tail 命令还接受参数形式的日志名称：tail mail_logs。

```
mail3.example.com> tail

Currently configured logs:


1. "antispam" Type: "Anti-Spam Logs" Retrieval: Manual Download

2. "antivirus" Type: "Anti-Virus Logs" Retrieval: Manual Download

3. "asarchive" Type: "Anti-Spam Archive" Retrieval: Manual Download

4. "authentication" Type: "Authentication Logs" Retrieval: Manual Download

5. "avarchive" Type: "Anti-Virus Archive" Retrieval: Manual Download

6. "bounces" Type: "Bounce Logs" Retrieval: Manual Download

7. "cli_logs" Type: "CLI Audit Logs" Retrieval: Manual Download

8. "encryption" Type: "Encryption Logs" Retrieval: Manual Download
```

```
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download

10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: Manual Download

11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: Manual Download

12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: Manual Download

13. "gui_logs" Type: "HTTP Logs" Retrieval: Manual Download

14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download

15. "reportd_logs" Type: "Reporting Logs" Retrieval: Manual Download

16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: Manual Download

17. "scanning" Type: "Scanning Logs" Retrieval: Manual Download

18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: Manual Download

19. "sntpd_logs" Type: "NTP logs" Retrieval: Manual Download

20. "status" Type: "Status Logs" Retrieval: Manual Download

21. "system_logs" Type: "System Logs" Retrieval: Manual Download

22. "trackerd_logs" Type: "Tracking Logs" Retrieval: Manual Download

23. "updater_logs" Type: "Updater Logs" Retrieval: Manual Download


Enter the number of the log you wish to tail.

[]> 19

Press Ctrl-C to stop.

Mon Feb 21 12:25:10 2011 Info: PID 274: User system commit changes: Automated Update for
Quarantine Delivery Host

Mon Feb 21 23:18:10 2011 Info: PID 19626: User admin commit changes:

Mon Feb 21 23:18:10 2011 Info: PID 274: User system commit changes: Updated filter logs
config

Mon Feb 21 23:46:06 2011 Info: PID 25696: User admin commit changes: Receiving
suspended.

^Cmail3.example.com>
```

配置主机密钥

使用 `logconfig -> hostkeyconfig` 子命令管理从邮件安全设备向其他服务器推送日志时与 SSH 搭配使用的主机密钥。SSH 服务器必须具有一对主机密钥：一个私钥和一个公钥。私有主机密钥位于 SSH 服务器上，不能由远程计算机读取。公共主机密钥可分配给需要与 SSH 服务器交互的任何客户端计算机。

注释 要管理用户密钥，请参阅管理安全外壳 (SSH) 密钥 ，第 745 页。

`hostkeyconfig` 子命令会执行以下功能：

表 *142:* 管理主机密钥 - 子命令列表

命令	描述
新	添加新密钥。
Edit	修改现有密钥。
Delete	删除现有密钥。
扫描	自动下载主机密钥。
打印	定义密钥。
Host	显示系统主机密钥。此值将存入远程系统的“known_hosts”文件。
指纹	显示系统主机密钥指纹。
User	显示将日志推送到远程计算机的系统帐户的公共密钥。此密钥与设置 SCP 推送订阅时显示的密钥相同。此值将存入远程系统的“authorized_keys”文件。

在下文示例中，AsyncOS 扫描主机密钥并为主机添加密钥：

```
mail3.example.com> logconfig

Currently configured logs:

[ list of logs ]

Choose the operation you want to perform:

- NEW - Create a new log.

- EDIT - Modify a log subscription.

- DELETE - Remove a log subscription.

- SETUP - General settings.

- LOGHEADERS - Configure headers to log.

- HOSTKEYCONFIG - Configure SSH host keys.

[]> hostkeyconfig

Currently installed host keys:

1. mail3.example.com ssh-dss [ key displayed ]

Choose the operation you want to perform:
```

```
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> scan
Please enter the host or IP address to lookup.
[]> mail3.example.com
Choose the ssh protocol type:
1. SSH1:rsa
2. SSH2:rsa
3. SSH2:dsa
4. All
[4]>
SSH2:dsa
mail3.example.com ssh-dss
[ key displayed ]
SSH2:rsa
mail3.example.com ssh-rsa
[ key displayed ]
SSH1:rsa
mail3.example.com 1024 35
[ key displayed ]

Add the preceding host key(s) for mail3.example.com? [Y]>
Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed ]
2. mail3.example.com ssh-rsa [ key displayed ]
3. mail3.example.com 1024 35 [ key displayed ]
Choose the operation you want to perform:
```

```
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]>
Currently configured logs:
[ list of configured logs ]
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>
```

第 41 章

使用集群进行集中管理

本章包含以下部分：

使用集群进行集中管理概述

思科集中管理功能允许同时管理和配置多台设备，减少管理时间，并确保网络中的配置一致。您无需购买额外的硬件来管理多台设备。集中管理功能可提高网络内的可靠性、灵活性和可扩展性，从而可以实现全局管理，同时又能遵从本地策略。

集群是一组共享配置信息的计算机。在集群内，计算机（思科设备）划分为组；每个集群至少包含一个组。一台特定计算机是且仅是一个组的成员。管理员用户可以在集群范围内、组范围内或每台计算机上配置不同的系统元素，从而基于网络、地域、业务部或其他逻辑关系细分思科设备。

集群按点对点架构形式实施；集群内没有主从关系。您可以登录到任何计算机来控制和管理集群。（但是，某些配置命令受限。请参阅限制的命令，第 920 页。）

用户数据库在集群内的所有计算机之间共享。也就是说，整个集群只有一组用户和一个管理员用户（具有相关密码）。加入集群的所有计算机将共享一个管理员密码，该密码称为集群的*admin*密码。

注释 如果群集中的设备超过 20 个，可能会导致群集通信出现错误。

集群要求

- 集群中的计算机必须在 DNS 中具有可解析的主机名。或者，可以改为使用 IP 地址，但不能将两者混合使用。

  请参阅DNS 和主机名解析，第 924 页。集群通信通常使用计算机的 DNS 主机名发起。

- 集群必须全部由运行相同版本 AsyncOS 的计算机组成。

  有关如何升级集群成员的信息，请参阅升级集群中的计算机，第 918 页。

- 计算机可以通过 SSH（通常在端口 22 中）或集群通信服务 (CCS) 加入集群。

  请参阅集群通信，第 924 页。

- 计算机加入集群后，即可通过 SSH 或集群通信服务进行通信。使用的端口是可配置的。通常在端口 22 中启用 SSH，而且 CCS 默认在端口 2222 中启用，但可以在其他端口上配置这些服务。

  除了必须为设备打开的正常防火墙端口之外，通过 CCS 通信的集群化计算机必须能够通过 CCS 端口相互连接。请参阅集群通信，第 924 页。

- 您必须使用命令行界面 (CLI) 命令 **clusterconfig** 创建、加入或配置计算机的集群。

  创建集群后，可通过 GUI 或 CLI 管理非集群的配置设置。

  请参阅创建和加入集群，第 910 页和通过 GUI 管理集群，第 921 页。

- 如果您在设备上启用了双因素身份验证，则可以使用预共享密钥将其加入集群计算机。使用 CLI 中的 `clusterconfig > prepjoin` 命令配置此设置。

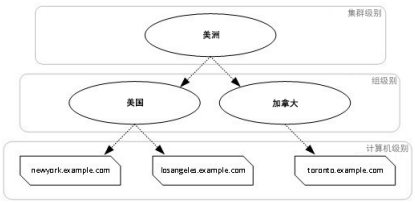
  或

  在创建或加入集群之前，请在邮件安全设备上禁用双因素身份验证。有关详细信息，请参阅禁用双因素身份验证，第 740 页。

集群组织

在集群内，配置信息可分为 3 组或 3 个级别。最顶层的级别描述集群设置，中间的级别描述组设置，最底层的级别描述计算机特定的设置。

图 *77:* 集群级别层次结构



在每个级别中，都有一个或多个可为其配置设置的特定成员，我们称其为模式。模式是指特定级别的指定成员。例如，“美国”组表示图中的两个组模式之一。级别是一般术语，模式是特定术语；模式这一称谓始终由名称而来。上图中描述的集群有六种模式。

虽然设置在指定级别进行配置，但总是针对特定模式配置。无需为一个级别内的所有模式配置设置。集群模式是一种特殊情况。由于只能存在一个集群，所以为集群模式配置的所有设置都可以称为在集群级别配置。

通常，应在集群级别配置大多数设置。但是，已在较低级别专门配置的设置将覆盖在较高级别配置的设置。因此，可以使用组模式或计算机模式设置覆盖集群模式设置。

例如，您可以首先在集群模式下配置友好相邻表；集群中的所有计算机都将使用该配置。然后，还可以在计算机模式下为计算机 newyork 配置此表。在这种情况下，集群中的所有其他计算机仍将使用在集群级别定义的友好相邻表，但计算机 newyork 将以其单独的计算机模式设置覆盖集群设置。

覆盖特定组或计算机集群设置的功能为您提供了极大的灵活性。但是，如果您发现自己在计算机模式下单独配置了许多设置，将失去集群预期提供的很多管理便利性。

初始配置设置

对于大多数功能，当您开始配置新模式的设置时，默认情况下，这些设置最初均为空。在一种模式下，设置为空与无设置之间有所不同。例如，有一个非常简单的集群，其中包含一个组和一台计算机。假设您在集群级别配置了一个 LDAP 查询。在组或计算机级别未配置设置：

集群	(ldap queries: a, b, c)
Group	
Machine	

现在，假设您为该组创建了新的 LDAP 查询设置。结果类似如下：

集群	(ldap queries: a, b, c)
Group	(ldap queries: None)
Machine	

现在，组级别设置将覆盖集群级别设置；不过新的组设置初始为空。组模式实际上没有配置自己的任何 LDAP 查询。请注意，此组中的计算机将从组中继承 LDAP 查询的“空”集。

接下来，可以将 LDAP 查询添加到该组中，例如：

集群	(ldap queries: a, b, c)
Group	(ldap queries: d)
Machine	

现在，集群级别配置了一组查询，而组中有另一组查询。计算机将继承该组中的查询。

创建和加入集群

无法在图形用户界面 (GUI) 中创建或加入集群。您必须使用命令行界面 (CLI) 创建、加入或配置计算机的集群。创建集群后，可通过 GUI 或 CLI 更改配置设置。

注意 如果您在设备上启用了双因素身份验证，则可以使用预共享密钥将其加入集群计算机。使用 CLI 中的 `clusterconfig prepjoin` 命令配置此设置。

或

在创建或加入集群之前，请禁用邮件安全设备上的双因素身份验证。有关详细信息，请参阅禁用双因素身份验证，第 740 页。

clusterconfig 命令

计算机只能通过 `clusterconfig` 命令创建或加入集群。

- 创建新集群后，该集群的所有初始设置都将从创建该集群的计算机中继承。如果计算机之前在“独立”模式下配置，则在创建集群时将使用其独立设置。
- 在计算机加入集群后，该计算机所有可集群化的设置都将从集群级别继承。换句话说，除了特定于计算机的某些设置（IP 地址等）外，其他一切都将丢失，并替换为要加入的且为该计算机所选的集群和/或组中的设置。如果计算机之前在“独立”模式下配置，则在创建集群时将使用其独立设置，而不会保留计算机级别的任何设置。

如果当前的计算机尚不属于某个集群，发送 `clusterconfig` 命令可提供加入现有集群或创建新集群的选项。

这时，可以将计算机添加到新集群中。这些计算机可通过 SSH 或 CCS 进行通信。

```
newyork.example.com> clusterconfig

Do you want to join or create a cluster?

1. No, configure as standalone.

2. Create a new cluster.

3. Join an existing cluster over SSH.

4. Join an existing cluster over CCS.

[1]> 2

Enter the name of the new cluster.

[]> americas

New cluster committed: Wed Jun 22 10:02:04 2005 PDT

Creating a cluster takes effect immediately, there is no need to commit.
```

```
Cluster americas

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>
```

加入现有集群

在要添加到集群的主机中，发出 clusterconfig 命令可加入现有集群。可以选择通过 SSH 或 CCS（集群通信服务）加入集群。

要将主机加入现有集群，必须：

- 可以验证集群中计算机的 SSH 主机密钥
- 知道集群中计算机的 IP 地址，并能够连接到到集群中的此计算机（例如，通过 SSH 或 CCS）
- 知道属于该集群的某台计算机中 admin 用户的管理员密码

通过 SSH 加入现有集群

下表演示如何使用 SSH 选项将计算机 losangeles.example.com 添加到集群。

```
losangeles.example.com> clusterconfig


Do you want to join or create a cluster?

1. No, configure as standalone.

2. Create a new cluster.

3. Join an existing cluster over SSH.

4. Join an existing cluster over CCS.

[1]> 3
```

```
While joining a cluster, you will need to validate the SSH host key of the remote
machine to which you are joining. To get the public host key

fingerprint of the remote host, connect to the cluster and run: logconfig ->
hostkeyconfig -> fingerprint.


WARNING: All non-network settings will be lost. System will inherit the values set at
the group or cluster mode for the non-network settings. Ensure that the cluster
settings are compatible with your network settings (e.g. dnsconfig settings)

Do you want to enable the Cluster Communication Service on
losangeles.example.com? [N]> n

Enter the IP address of a machine in the cluster.

[]> IP address is entered

Enter the remote port to connect to. The must be the normal admin ssh
port, not the CCS port.

[22]> 22

Enter the admin passphrase for the cluster.
The administrator passphrase for the clustered machine is entered

Please verify the SSH host key for IP address:

Public host key fingerprint: xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx

Is this a valid key for this host? [Y]> y

Joining cluster group Main_Group.

Joining a cluster takes effect immediately, there is no need to commit.

Cluster americas

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>
```

```
(Cluster americas)>
```

通过 CCS 加入现有集群

如果无法使用 SSH，请使用 CCS 替代 SSH。CCS 唯一的优势是，通过该端口只会进行集群通信（无用户登录、SCP 等）。要通过 CCS 将其他计算机添加到现有集群，请使用 clusterconfig 的子命令 `prepjoin` 准备要添加到集群的计算机。在本例中，在计算机 newyork 中发出 `prepjoin` 命令，准备要添加到集群中的计算机 losangeles。

`prepjoin` 命令涉及：通过在要添加到集群的主机的 CLI 中键入 `clusterconfig prepjoin print` 获取该主机的用户密钥，然后将该密钥复制到当前位于集群中的主机的命令行。

计算机成为集群的一部分后，使用 `clusterconfig` 命令可以针对该集群配置各种设置。

```
Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]> prepjoin

Prepare Cluster Join Over CCS

No host entries waiting to be added to the cluster.

Choose the operation you want to perform:

- NEW - Add a new host that will join the cluster.

[]> new

Enter the hostname of the system you want to add.

[]> losangeles.example.com

Enter the serial number of the host mail3.example.com.

[]> unique serial number is added

Enter the user key of the host losangeles.example.com. This can be obtained by typing
"clusterconfig prepjoin print" in the CLI on mail3.example.com. Press enter on a blank
```

```
line to finish.

unique user key from output of prepjoin print is pasted
Host losangeles.example.com added.
Prepare Cluster Join Over CCS
1. losangeles.example.com (serial-number)
Choose the operation you want to perform:
- NEW - Add a new host that will join the cluster.
- DELETE - Remove a host from the pending join list.
[]>

(Cluster Americas)> clusterconfig
Cluster americas
Choose the operation you want to perform:
- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- LISTDETAIL - List the machines in the cluster with detail.
- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.
- PREPJOIN - Prepare the addition of a new machine over CCS.
[]>
```

使用预共享密钥通过 SSH 加入现有集群

下表演示如何使用预共享密钥通过 SSH 将计算机 (testmachine.example.com) 加入集群 (test_cluster)。

```
testmachine.example.com> clusterconfig

Do you want to join or create a cluster?
1. No, configure as standalone.
2. Create a new cluster.
```

```
3. Join an existing cluster over SSH.

4. Join an existing cluster over CCS.

[1]> 3


While joining a cluster, you will need to validate the SSH host key of the remote
machine to which you are joining. To get the public host key

fingerprint of the remote host, connect to the cluster and run: logconfig ->
hostkeyconfig -> fingerprint.


WARNING: All non-network settings will be lost. System will inherit the values set at
the group or cluster mode for the non-network settings. Ensure that the cluster
settings are compatible with your network settings (e.g. dnsconfig settings)

Do you want to enable the Cluster Communication Service on
testmachine.example.com? [N]>

Enter the IP address of a machine in the cluster.

[]> IP address entered

Enter the remote port to connect to. The must be the normal admin ssh
port, not the CCS port.

[22]>

Would you like to join this appliance to a cluster using pre-shared keys?
Use this option if you have enabled two-factor authentication on the appliance.) [Y]> yes

To join this appliance to a cluster using pre-shared keys, log in to the cluster machine,
run the clusterconfig > prepjoin > command, enter the
following details, and commit your changes.
Host: pod1226-esa07.ibesa
Serial Number: 42291A18D741EDB4C601-BC14E5579F34
User Key:

ssh-dss
AAAAB3NzaC1kc3MAAACBAJ6Xm+ja4aau9n4DOcJs/gGwEDEUWgERYchhgWApKt6IW+s58I7knGM81rQgQbNdNCO58D
EqaVGmP0Vyb0TTpgvh6f0mr80OuTgWh9bqg4uiOJvbKvlTvDt0o7//mTklm159zr2KT/qFH+9L5i+8iIMX62R5y+a
6E8JV0BrJCNAAAAFQCmK+WOu9HSribsC0f/5dVoADdxEwAAAIA5p7NR74rlSrs0JWWYItNAtE1SamAN+gqCOdUWGPPHT
qdrtBIlPQ9tfFoThZElqY4Tx8lku9laasoRLruQ2Z36R3bQGzIn4jzQqujvvbxTvLK9eLoSr8yFbEE3ZvuUo0+vhDn
LIDX2N65AQSQsTaOrKX+yQZ8yAVt48CsctpsDrgAAAIAVROGlWoSl8g3FFm2eRTa+/oZ+cMjv+pSZiZoiUCoaIlouc
u1ZDpN413QBnf6p/3D8wVD8m5uo8O4N/HXasAMektZvGoP4Sf+shItPuISRv3lrMTEYsD0sqVcMc7vIXUeD2jpOk7MB
ooVkTZB/rdTbNMfXrhDkNJ2IAPQQiUKVnw==

Before you proceed to the next step, make sure you add the ‘Host’, Serial Number’ and
‘User Key’
details to the cluster machine.

Would you like to continue? [Y]> yes

Joining cluster group Main_Group.

Joining a cluster takes effect immediately, there is no need to commit.

Cluster test_cluster

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.
```

```
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- LISTDETAIL - List the machines in the cluster with detail.
- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.
- PREPJOIN - Prepare the addition of a new machine over CCS.
[]>
(Cluster test_cluster)>
```

添加组

所有集群必须至少包含一个组。在创建新集群时，系统会自动创建一个名为 **Main_Group** 的默认组。但是，您可以决定在集群中创建其他组。本示例展示了如何在现有集群中创建其他组以及向新组分配计算机。

步骤 1 发出 **clusterconfig** 命令。

步骤 2 选择 **addgroup** 子命令，并输入新组的名称。

步骤 3 使用 **setgroup** 子命令选择新组的计算机。

管理集群

通过 CLI 管理集群

对于属于集群的计算机，CLI 可以切换到不同的模式。重申一下，模式是指某个级别特定的指定成员。

CLI模式完全决定修改配置设置的位置。对于用户登录到的计算机“登录主机”，默认为“计算机”模式。

使用 clustermode 命令可在不同模式之间切换。

表 *143:* 管理集群

命令示例	说明
`clustermode`	提示切换集群模式
`clustermode group northamerica`	将“northamerica”组切换到组模式
`clustermode machine losangeles.example.com`	将计算机“losangeles”切换到计算机模式

CLI 中的提示变为指示当前模式。

```
(Cluster Americas)>
```

或

```
(Machine losangeles.example.com)>
```

在计算机模式下，提示将包括计算机的完全限定域名。

复制和移动设置

所有非受限（请参阅限制的命令，第920页）的命令都有新的操作：**CLUSTERSHOW**和**CLUSTERSET**。**CLUSTERSHOW**用于显示配置命令的模式（请参阅添加的新操作，第 919 页）。**CLUSTERSET**操作允许在不同模式或不同级别（例如，从一台计算机到到一个组）之间移动或复制当前的设置（可通过当前的命令配置）。

*copy*将保留当前模式的设置。*move*将重置（清除）当前模式的配置；例如，在移动后，当前模式将没有配置任何设置。

例如，如果您为组**northamerica**配置了“友好相邻表”设置（**destconfig**命令），并且希望整个集群都采用这些设置，则可以在**destconfig**命令内使用**clusterset**操作，将当前设置复制（或移动）到集群模式。（请参阅测试新配置，第 917 页。）

注意 移动或复制配置设置避免时务必小心，以避免从属关系不一致。例如，如果要将配置了免责声明标记的侦听程序移动或复制到其他计算机，而新计算机没有配置相同的免责声明，则在新计算机中不会启用免责声明标记。

测试新配置

使用集群最有利的方面之一，就是测试新的配置设置。首先，在独立环境下，在计算机模式下进行更改。然后，对所做的配置满意后，将这些配置更改上移到集群模式，以用于所有计算机。

以下示例显示了在一台计算机上更改侦听程序设置，准备好后再将设置发布到集群其余部分的步骤。由于侦听程序通常在集群级别配置，所以示例首先是将配置下拉到一台计算机的计算机模式，然后才进行更改并测试。您应在一台计算机上测试此类型的试验性更改，然后再对集群中的其他计算机进行更改。

步骤 1 使用 **clustermode cluster** 命令更改到集群模式。

切记，**clustermode** 命令是用来将模式更改到集群、组和计算机级别的 CLI 命令。

步骤 2 键入 **listenerconfig** 可查看为集群配置的侦听程序设置。

步骤 3 选择用于试验的计算机，然后使用 clusterset 命令将设置从集群“向下”复制到计算机模式。

步骤 4 使用 clustermode 命令导航到试验计算机的计算机模式，例如：

```
clustermode machine newyork.example.com
```

步骤 5 在计算机模式下，在试验计算机中发出 listenerconfig 命令，以专门针对试验计算机进行更改。

步骤 6 确认更改。

步骤 7 在试验计算机上继续试验配置更改，切记要确认更改。

步骤 8 在准备好将新设置应用到所有其他计算机后，使用 clusterset 命令将设置上移到集群模式。

步骤 9 确认更改。

永久退出集群（删除）

使用 clusterconfig 的 REMOVEMACHINE 操作，可从集群中永久删除计算机。从集群中永久删除计算机后，其配置将“趋于扁平”，适用范围与其之前属于集群成员时相同。例如，如果只有一个集群模式的“全局取消订用”(Global Unsubscribe) 表，则从集群中删除该计算机后，该“全局取消订用”(Global Unsubscribe) 表数据将复制到计算机的本地配置中。

升级集群中的计算机

集群不允许连接的计算机采用不同版本的 AsyncOS。

在安装 AsyncOS 升级之前，需要通过 clusterconfig 命令断开集群中每台计算机。升级所有计算机后，可以通过 clusterconfig 命令重新连接集群。将计算机升级到相同版本时，可以运行两个不同的集群。此外，还可以在“GUI 升级”(GUI Upgrades) 页面升级集群中的计算机。

可以在后台下载升级，这样在准备好安装升级之前，无需断开集群计算机。

注释 如果在从集群断开每台计算机之前就使用升级命令，AsyncOS 将断开集群中的所有计算机。Cisco Systems 建议先从集群中断开每台计算机，再进行升级。然后，其他计算机可以继续作为集群运行，直到每台计算机均已断开和升级。

步骤 1 在集群中的某台计算机上，使用 clusterconfig 的 disconnect 操作。例如，要断开计算机 losangeles.example.com，请键入 type clusterconfig disconnect losangeles.example.com。无需 commit。

步骤 2 或者，在升级过程中，使用 suspendlistener 命令停止接受新连接和消息。

步骤 3 发出 upgrade 命令，将 AsyncOS 升级到更新的版本。

注释 忽略有关断开集群中的所有计算机的任何警告或确认提示。由于您已断开计算机，AsyncOS 此时不会断开集群中的其他计算机。

步骤 4 选择计算机的 AsyncOS 版本。升级完成后，计算机将重启。

步骤 5 在升级计算机中使用 resume 命令，以开始接受新消息。

步骤 6 针对集群中的每台计算机，重复步骤 1 - 5。

注释 从集群中断开某台计算机后，将无法使用它来更改其他计算机的配置。虽然仍可以修改集群配置，但断开计算机后请勿进行更改，因为设置无法同步。

步骤 7 在升级了所有计算机后，针对每台升级的计算机使用 clusterconfig 的 reconnect 操作，以便重新连接。例如，要重新连接计算机 losangeles.example.com，请键入 clusterconfig reconnect losangeles.example.com。请注意，只能将计算机连接到运行相同版本 AsyncOS 的集群。

CLI 命令支持

所有命令均为集群感知

AsyncOS 中的所有 CLI 命令现在都是集群可感知的。在集群模式下发出某些命令时，其行为可能稍有变化。例如，在属于集群的计算机中发出以下命令时，它们的行为有所变化：

commit 和 clearchanges 命令

提交

commit 命令将确认在集群所有三个级别进行的全部更改，不考虑您当前所处的模式。

commitdetail

commitdetail 命令提供将配置应用到集群内的所有计算机时，有关配置变更的详细信息。

clearchanges

clearchanges (clear) 命令将清除集群所有三个级别的全部更改，不考虑您当前所处的模式。

添加的新操作

CLUSTERSHOW

在每个命令中，现在都有一个 CLUSTERSHOW 操作，允许您查看配置命令的模式。

当输入 CLI 命令要执行的操作将会被较低级的现有设置覆盖时，您将会看到通知。例如，如果您在集群模式下输入命令，可能会看到如下通知：

```
Note: Changes to these settings will not affect the following groups and machines
because they are overriding the cluster-wide settings:

East_Coast, West_Coast

facilities_A, facilities_B, receiving_A
```

如果您正在编辑组模式的设置，也会显示类似的消息。

限制的命令

大多数 CLI 命令及其对应的 GUI 页面可在任何模式（集群、组或计算机）下运行。但是，有些命令和页面仅限于一种模式。

系统界面（GUI 和 CLI）始终会明确指出命令受限及其受限方式。切换到配置命令的适当模式非常方便。

- 在 GUI 中，可使用“更改模式”(Change Mode) 菜单或“当前定义此功能设置的位置:”(Settings for this features are currently defined at:) 链接切换模式。
- 在 CLI 中，可使用 clustermode 命令切换模式。

表 *144:* 仅限于集群模式的命令

clusterconfig	sshconfig
clustercheck	userconfig
passwd	

如果尝试在组或计算机级别运行上述某个命令，系统将为您提供警告消息，并允许您切换到适当的模式。

注释 passwd 命令是特殊情况，因为它需要能被访客用户使用。如果访客用户在集群模式下在一台计算机上发出 passwd 密码，则它不会输出警告消息，而只是以静默方式操作集群级别的数据，而不会更改用户的模式。所有其他用户将会遇到上面提到的情况（与其他受限的配置命令保持一致）。

以下命令仅限于计算机模式：

antispamstatus	etherconfig	resume	suspenddel
antispamupdate	featurekey	resumedel	suspendlistener
antivirusstatus	hostrate	resumelistener	techsupport

antivirusupdate	hoststatus	rollovernow	tophosts
bouncerecipients	interfaceconfig	routeconfig	topin
deleterecipients	ldapflush	sbstatus	trace
delivernow	ldaptest	setgateway	version
diagnostic	nslookup	sethostname	vofflush
dnsflush	quarantineconfig	settime	vofstatus
dnslistflush	rate	shutdown	workqueue
dnslisttest	reboot	status	
dnsstatus	resetcounters	suspend	

如果尝试在集群或组级别运行上述某个命令，系统将为您提供警告消息，并允许您切换到适当的模式。

而且，以下命令还限于登录主机（即您登录到的特定计算机）。这些命令要求有权访问本地文件系统。

表 *145:* 限于登录主机模式的命令

最后一个	resetconfig	tail	upgrade
ping	supportrequest	telnet	who

通过 GUI 管理集群

虽然从GUI无法创建或加入集群或管理集群特定的设置（相当于**clusterconfig**命令），但可以在 GUI 内浏览集群中的计算机，并在集群、组和计算机之间创建、删除、复制和移动设置（即相当于执行 **clustermode** 和 **clusterset** 命令）。

“传入邮件概述”(Incoming Mail Overview) 页面是限于登录主机的命令示例，因为您查看的邮件流量监控数据存储在本地计算机中。要查看其他计算机的传入邮件概述报告，必须登录到该计算机的GUI。

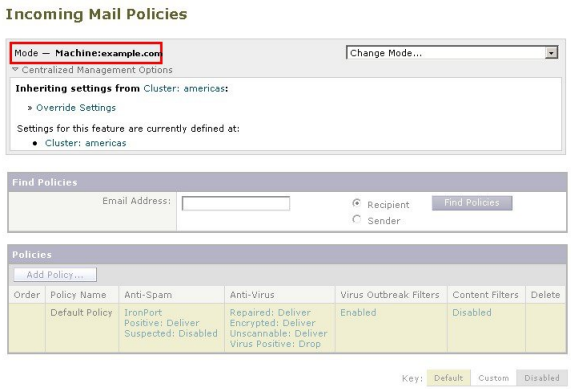
如果设备上启用了集群，请注意浏览器地址字段中的 URL。URL 中将包含相应的单词 **machine**、**group** 或 **cluster**。例如，首次登录时，“传入邮件概述”(Incoming Mail Overview) 页面的 URL 将显示为：

https:// *hostname***machine**/*serial_number* **/monitor/incoming_mail_overview**

注释 “监控”(Monitor) 菜单中的“传入邮件概述”(Incoming Mail Overview) 和“传入邮件详细信息”(Incoming Mail Details) 页面仅限于登录计算机。

“邮件策略”(Mail Policies)、“安全服务”(Security Services)、“网络”(Network,) 和“系统管理”(System Administration) 选项卡包含不限于本地计算机的页面。如果点击“邮件策略”(Mail Policies) 选项卡，GUI 中的集中管理信息将发生变化。

图 *78: GUI* 中的集中管理功能：未定义设置



在上图中，计算机将从集群模式继承当前功能的所有配置设置。继承的设置为浅灰色（预览）。您可以保留这些设置，也可以更改它们，覆盖此计算机的集群级别设置。

注释 继承的设置（预览显示）始终显示从集群继承的设置。在启用或禁用组和集群级别之间的从属服务时，请务必小心。有关详细信息，请参阅复制和移动设置，第 917 页。

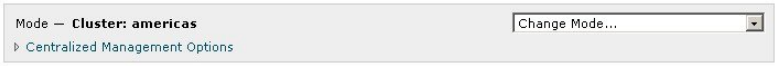
如果点击“覆盖设置”(Override Settings) 链接，您将转到该功能的新页面。在此页面，可为计算机模式创建新的配置设置。可以从默认设置开始，如果您已在其他模式下配置了设置，也可以将那些设置复制到此计算机。

图 *79: GUI* 中的集中管理功能：创建新设置

或者，如图“*GUI* 中的集中管理功能：未定义设置”中所示，也可以导航到已定义此配置设置的模式。这些模式列在“当前定义此功能设置的位置:”(Settings for this feature are currently defined at:) 下的集中管理框的下半部分。此处只会列出实际定义了设置的模式。当您查看在其他模式下定义（并继承）的设置页面时，该页面将为您显示相关设置。

如果点击列出的模式之一（例如，图“*GUI* 中的集中管理功能：未定义设置”中显示的“集群: 美洲”链接），您将会转到一个新页面，从中可查看和管理该模式的设置的新页面。

图 *80: GUI* 中的集中管理功能：定义的设置



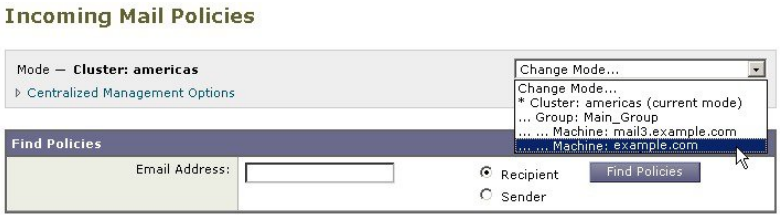
对于为特定模式定义的设置，每个页面将以最小化状态显示集中管理框。点击“集中管理选项”(Centralized Management Options) 链接可展开该框，显示当前页面中针对当前模式可使用的选项列表。点击“管理设置”(Manage Settings) 按钮，可以将当前设置复制或移动到其他模式，或完全删除这些设置。

例如，在下图中，点击“集中管理选项”链接后将显示以下可用的选项。

图 *81: GUI* 中的集中管理功能：管理设置

该框的右侧是“更改模式”(Change Mode) 菜单。此菜单显示当前模式，并提供随时导航到任何其他模式（集群、组或计算机）的功能。

图 *82:*“更改模式”*(Change Mode)* 菜单



当您导航至代表另一模式的页面时，集中管理方框左侧的“Mode -”文本将短暂闪烁黄色，提醒您模式已更改。

某些选项卡中的部分页面仅限于计算机模式。但是，与仅限于当前登录主机的“传入邮件概述”(Incoming Mail Overview) 页面不同，这些页面可用于集群中的任何计算机。

图 *83:* 集中管理功能：受限计算机

从“更改模式”(Change Mode) 菜单可选择要管理的计算机。您将看到文本短暂地闪烁，以提醒您模式已更改。

集群通信

集群中的计算机使用网状网络相互通信。默认情况下，所有计算机彼此相互连接。如果一条链接中断，不会阻碍其他计算机接收更新。

默认情况下，使用 SSH 保护集群之间的所有通信。每台计算机在内存中保留一份路由表，如果链接断开或恢复，则根据需要在内存内进行更改。每台计算机还会定期（每隔 1 分钟）对集群中其他计算机执行“ping”操作。这样可确保链接状态最新，即使路由器或 NAT 超时，也会保持连接。

注释 如果您的设备处于集群模式，并且您计划远程访问另一设备的数据（与配置无关，例如查看隔离区中的邮件或以较快的速率刷新报告）；将有可以生成警报和错误的群集重新连接尝试。设备将自动重新连接，不需要手动干预。

DNS 和主机名解析

计算机加入集群需要 DNS。集群通信通常使用计算机的 DNS 主机名发起（不是计算机接口的主机名）。主机名不可解析的计算机无法与集群中的任何其他计算机实际通信，即使从技术上属于集群的一部分也不例外。

您的 DNS 必须配置为：主机名指向启用了 SSH 或 CCS 的设备中正确的 IP 接口。这一点非常重要。如果 DNS 指向其他未启用 SSH 或 CCS 的 IP 地址，将找不到该主机。请注意，集中管理功能使用“主要主机名”，而不是按接口的主机名（与使用 sethostname 命令的设置相同）。

如果使用IP地址连接到集群中的其他计算机，则连接到的计算机必须能够反向查找连接的IP地址。如果反向查找由于 IP 地址不在 DNS 中超时，计算机将无法连接到集群。

集群、完全限定域名和升级

更改 DNS 可能会导致升级 AsyncOS 后连接丢失。请注意，如果需要更改集群中某台计算机的完全限定域名（而非集群中某台计算机接口的主机名），则必须通过 sethostname 更改主机名设置，并在升级 AsyncOS 之前更新该计算机的 DNS 记录。

集群通信安全

集群通信安全 (CCS) 是一种与定期 SSH 服务类似的安全外壳服务。思科实施 CCS，是为了打消使用定期 SSH 进行集群通信的顾虑。两台计算机之间的 SSH 通信将在同一端口打开定期登录（admin 等）。许多管理员不愿意在其集群计算机中打开定期登录。

提示：切勿启用“集群通信服务”(Cluster Communication Services)（即使是默认设置），除非您加入集群的部分计算机之间拥有防火墙阻止端口 22。集群在所有计算机之间使用全网状的 SSH 隧道（在端口 22 上）。如果您已同意在任何计算机中启用 CCS，请从集群中删除所有计算机并重新开始。删除集群中的最后一台计算机将删除集群。

CCS 提供增强功能，借此管理员可以打开集群通信，但不是 CLI 登录。默认情况下禁用该服务。当系统提示您启用其他服务时，系统将提示您通过 interfaceconfig 命令启用 CCS。例如：

```
Do you want to enable SSH on this interface? [Y]>

Which port do you want to use for SSH?

[22]>

Do you want to enable Cluster Communication Service on this interface?

[N]> y

Which port do you want to use for Cluster Communication Service?

[2222]>
```

CCS 的默认端口号为 2222。如果愿意，可以将此端口更改为其他开放、未使用的端口号。在完成加入且加入的计算机获得集群中的所有配置数据后，将会出现以下问题：

```
Do you want to enable Cluster Communication Service on this interface? [N]> y


Which port do you want to use for Cluster Communication Service?

[2222]>
```

集群一致性

具有“集群感知”的计算机将不断验证与集群内其他计算机的网络连接。这种验证通过定期向集群中的其他计算机发送“ping”进行。

如果尝试与特定计算机通信总是失败，则尝试进行通信的计算机将记录一条消息，指出远程主机已断开连接。系统会向管理员发送风险通告，说明远程主机已断开连接。

即使计算机关闭，仍会继续发送 ping 验证。当计算机重新加入集群网络后，系统将发送同步命令，这样以前脱机的任何计算机都能下载任何更新。同步命令还可确定一端（而不是另一端）是否有任何更改。如果是，以前关闭的计算机将以静默方式下载更新。

断开连接/重新连接

计算机可以从集群断开连接。有时，您可能想要故意断开计算机，例如要升级计算机。此外，还可能会意外断开连接，例如由于电源故障或其他软件或硬件错误。如果一台设备在会话中尝试打开的 SSH 连接数超过允许的最大值，也可能会出现中断。从集群断开的计算机仍可以直接访问和配置，但在断开的计算机重新连接之前，对其进行的任何更改将不会再应用到集群内的其他计算机。

在计算机重新连接到集群后，它将立即尝试重新连接所有计算机。

理论上，集群中断开连接的两台设备可以同时向其本地数据库确认类似的更改。计算机在重新连接到集群后，将尝试同步这些更改。如果存在冲突，将记录最近的更改（取代任何其他更改）。

在确认期间，设备会检查更改的每个变量。确认数据包括版本信息、序列识别号和可比较的其他信息。如果您发现要更改的数据与以前的更改存在冲突，允许您选择放弃更改。例如，您可能会看到如下信息：

```
(Machine mail3.example.com)> clustercheck

This command is restricted to "cluster" mode. Would you like to switch to "cluster"

mode? [Y]> y

Checking Listeners (including HAT, RAT, bounce profiles)...

Inconsistency found!

Listeners (including HAT, RAT, bounce profiles) at Cluster enterprise:

mail3.example.com was updated Mon Sep 12 10:59:17 2005 PDT by 'admin' on

mail3.example.com

test.example.com was updated Mon Sep 12 10:59:17 2005 PDT by 'admin' on

mail3.example.com

How do you want to resolve this inconsistency?

1. Force entire cluster to use test.example.com version.


2. Force entire cluster to use mail3.example.com version.

3. Ignore.

[1]>
```

如果选择不放弃更改，它们将保持不变（但未确认）。您可以查看针对当前设置的更改，并决定如何继续。

还可以随时使用 `clustercheck` 命令确认集群的运行是否正确。

```
losangeles> clustercheck

Do you want to check the config consistency across all machines in the cluster? [Y]> y

Checking losangeles...

Checking newyork...

No inconsistencies found.
```

相互依赖的设置

建议您不要在云端邮件安全设备中配置以下设置。

在集中管理环境下，有些相互依赖的设置是在不同模式下配置的。灵活的配置模式允许在多种模式下配置设置，而继承规则控制在每台计算机中使用哪些设置。但是，有些设置对其他设置具有依赖性，且从属设置配置的可用性不仅限于相同模式的设置。因此，可以针对引用不同级别下为特定计算机所配置的设置的级别配置设置。

相互依赖的设置最常见的示例就是页面中从不同集群部分提取数据的特定字段。例如，以下功能可以在不同模式下配置：

- 使用 LDAP 查询
- 使用词典或文本资源
- 使用退回或 SMTP 身份验证配置文件。

在集中管理中，存在受限和非受限的命令。（请参阅限制的命令，第 920 页。）非受限命令通常是可跨集群共享的配置命令。

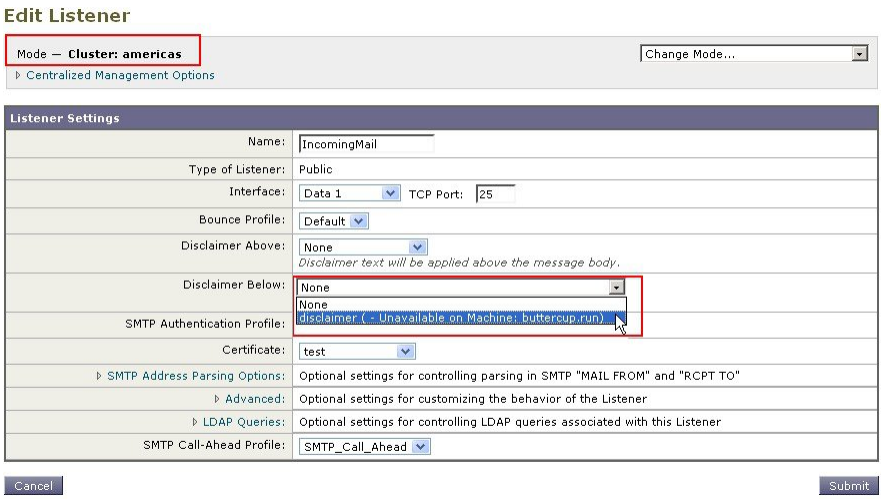
listenerconfig 命令就是为集群中的所有计算机配置的命令示例。非受限命令表示可在集群的所有计算机中镜像，且无需修改计算机特定数据的命令。

另一方面，受限命令是仅适用于特定模式的命令。例如，不能针对特定计算机配置用户 - 整个集群中只能设置一个用户。（否则，将无法使用相同登录信息登录到远程计算机。）同样，由于只能在每台计算机的基础上维护邮件流量监控数据、系统概述计数器和日志文件，所以这些命令和页面必须限于计算机。

您会发现，虽然整个集群中配置的计划报告可以相同，但报告的视图则取决于计算机。因此，在GUI的单个“计划报告”(Scheduled Reports)页面，必须在集群模式下执行配置，但查看报告则必须是计算机模式。

“系统时间”页面包含 **settz**、**ntpconfig** 和 **settime** 命令，其中既有受限命令，也有非受限命令。在这种情况下，settime必须仅限于计算机模式（因为时间设置是计算机特定的），而 **settz** 和 **ntpconfig** 可在集群或组模式下配置。

图 *84:* 相互依赖的设置示例



在此图示中，侦听程序“IncomingMail”引用仅在计算机级别配置的“免责声明”(disclaimer)页脚。可用页脚资源下拉列表显示，该页脚在集群中也可使用的计算机“buttercup.run”中不可用。针对此难题，有两种解决方案：

- 将页脚“免责声明”(disclaimer)从计算机级别提升到集群级别
- 将侦听程序降低到计算机级别，以消除相互依赖关系

为了充分实现集中管理系统的功能最大化，优先选择前一种解决方案。在为属于集群的计算机量身定制配置时，请注意设置之间的相互依赖关系。

在集群设备中加载配置

AsyncOS 允许在集群的设备中加载集群配置。在以下场景下，可以加载集群配置：

- 如果要从内部部署环境迁移到托管环境，并想要将内部部署的集群配置迁移到托管环境。
- 如果集群中的设备关闭或需要淘汰，您希望将此设备的配置加载到计划添加到集群的新设备中。
- 如果要向集群中添加更多设备，您希望将集群中现有的一台设备的配置加载到新添加的设备中。
- 如果要将备份配置加载到集群中。

根据您的需求，可以从有效的集群配置文件中加载集群配置或设备配置。

注释 在集群中的设备上无法加载独立设备的配置。

准备工作

- 确保您具有有效且完整的 XML 配置。请参阅加载配置文件，第 755 页。
- 为计划将配置加载到的设备的当前配置创建备份。请参阅保存和导出当前的配置文件，第 755 页。
- 创建集群设置，并在设置中包含您计划使用的所有设备。请参阅创建和加入集群，第 910 页。

注释 您可以将所有设备安排在一个组下。确保集群通信的接口在您的设置与 XML 配置中，具有相同的名称及 SSH 和 CCS 设置。

步骤 1 点击**系统管理 (System Administration)** > **配置文件 (Configuration File)**。

步骤 2 从**模式 (Mode)** 下拉菜单中选择集群。

步骤 3 根据您要加载集群配置还是设备配置，执行以下任一操作：

- **加载集群配置**
  1. 在“加载配置”(Load Configuration) 部分，从下拉列表中选择**集群 (Cluster)**。
  2. 加载集群配置，并点击**加载 (Load)**。请参阅加载配置文件，第 755 页。
  3. 向集群中的设备分配已加载的配置中的组，并将选定组中设备的设备配置复制到各自的设备当中。使用**组配置 (Group Configuration)** 和**设备配置 (Appliance Configuration)** 下拉列表。

     如果您不希望复制设备配置，请从**设备配置 (Appliance Configuration)** 下拉列表中选择**不复制 (Don't Copy)**。

     1. 检查配置。点击**审核**。
     2. 点击**确认**。
     3. 点击**继续 (Continue)**。

- **加载设备配置**

1. 在“加载配置”部分，从下拉列表中选择**集群中的设备**。
2. 加载配置，并点击**加载 (Load)**。请参阅加载配置文件，第 755 页。请注意，在集群中的设备上无法加载独立设备的配置。
3. 从已加载的配置中选择设备配置，并在要将配置加载到的集群中选择目标设备。使用下拉列表。
4. 点击 **OK**。
5. 点击**继续 (Continue)**。
6. 要将设备配置加载到更多设备，请重复步骤 **a** 到步骤 **e**。

步骤 4 检查集群中的设备的网络设置，然后确认更改。

最佳实践和常见问题解答

最佳实践

在创建集群时，您当时所登录到的计算机将作为第一台计算机自动添加到该集群，并会添加到 Main_Group。其计算机级别设置会尽可能有效地迁移到集群级别。无组级别的设置，唯一留在计算机级别的设置就是在集群级别没有意义和无法集群化的设置。例如 IP 地址、功能密钥等。

尽可能多的在集群级别保留设置。如果集群中只有一台计算机需要不同的设置，可将集群设置复制到该计算机的计算机级别。不要移动该设置。如果移动没有出厂默认值的设置（例如 HAT 表、SMTPROUTES 表、LDAP 服务器配置文件等），继承集群设置的系统会有空白表，并可能无法处理邮件。

要让该计算机重新继承集群设置，请管理 CM 设置并删除计算机设置。只有在看到以下显示时，才会知道计算机要覆盖集群设置：

配置定义:

To inherit settings from a higher level: Delete Settings for this feature at this mode.

You can also Manage Settings.

该特征的设置也可以定义在：

```
Cluster: xxx
```

或以下显示：

删除配置:

```
Cluster: xxx
Machine: yyyy.domain.com
```

复制与移动

什么时候复制：当您希望集群有设置，而组或计算机无设置或具有不同的设置时。

什么时候移动：但您希望集群完全没有设置，而组或计算机有设置时。

良好的 CM 设计实践

在 LIST 您的 CM 计算机时，您可能希望看到如下信息：

cluster = CompanyName

Group Main_Group:

Machine lab1.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Machine lab2.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Group Paris:

Machine lab3.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Machine lab4.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Group Rome:

Machine lab5.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Machine lab6.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

请注意，不要丢失对所做更改级别的跟踪。例如，如果将 Main_Group 的名称（使用 RENAMEGROUP）更改为 London，它将显示如下所示的信息：

cluster = CompanyName

Group London:

Machine lab1.cable.nu (Serial #: 000F1FF7B3F0-CF2SX51)

...

但是，许多管理员可能会对此配置感到困惑，因为它们开始是在组级别更改London系统，然后又停止使用集群级别作为基本设置的正常配置级别。

提示：最好不要使用与集群相同的名称作为组名，例如集群 London、组 London。如果您使用站点名称作为组名，则最好不要使用引用某个位置的集群名称。

如上所述，正确的方法是在集群级别保留尽可能多的设置。大多数情况下，应在Main_Group中保留计算机的主站点或主要集合，并对其他站点使用组合。即使您认为两个站点“平等”，这一点也不例外。请记住，CM 没有主/次或主/从服务器 - 集群中的所有计算机是对等的。

提示：如果使用额外的组，则可以在将这些额外计算机加入集群之前轻松地准备组。

在集群设置中访问垃圾邮件或策略隔离区的最佳实践

从登录的设备访问集群中其他设备的垃圾邮件或策略隔离区，可能会导致登录设备上的CPU利用率过高。为了避免出现这种情况，可以通过登录各自的设备访问垃圾邮件或策略隔离区。

过程：配置示例集群

要配置此示例集群，在运行 clusterconfig 之前，请在所有设备上退出全部 GUI。在任意一台主站点计算机中运行 clusterconfig。然后，就能将其他仅需要尽可能最大共享设置（支持仅限计算机的设置，例如 IP 地址）的本地和远程计算机加入此集群。使用 clusterconfig 命令无法将远程计算机加入集群，必须在远程计算机上使用 CLI 并运行 clusterconfig（“加入现有集群”）。

在我们上面的示例中，我们登录到 lab1，运行 clusterconfig，并创建一个名为 CompanyName 的集群。我们只有一台具有相同需求的计算机，因此我们登录到 lab2 并针对现有配置运行 saveconfig（继承 lab1 的大多数设置后，它将发生巨大变化。）然后，在 lab2 中可以使用 clusterconfig 加入现有集群。如果此站点还有其他计算机需要类似的策略和设置，请重复上述操作。

运行 CONNSTATUS，确认 DNS 解析是否正确。在计算机加入集群后，新计算机将继承 lab1 的几乎所有设置，早期的设置将丢失。如果是生产计算机，您则需要估计是否仍可使用新配置（而不是先前配置）来处理邮件。如果从集群中删除它们，它们不会恢复到以前的专用配置。

接下来，我们来看例外的计算机数量。如果只有一台，它应会收到几个额外计算机级别的设置，您无需为其创建额外的组。将其加入集群，并开始将设置向下复制到计算机级别。如果此计算机是现有的生产计算机，则必须备份配置，并考虑邮件处理的变化，如上所述。

如果有两台或更多台例外计算机，就像在我们的示例中，需要确定这两台计算机之间是否共享不与集群共享的任何设置。在这种情况下，需要为它们创建一个或多个组。否则，可以为每台计算机进行计算机级别的设置，这样则无需创建额外的组。

在我们的情况下，我们需要从已属于集群的任意计算机的 CLI 中运行 clusterconfig，并选择 ADDGROUP。此操作要执行两次，针对 Paris 和 Rome 各执行一次。

现在，即可开始使用 GUI 和 CLI 为集群和所有组构建配置设置（即使组中还没有计算机）。对于计算机特定的设置，只有在计算机加入集群后才能为它们创建。

创建覆盖或例外设置的最佳方式是，将更高级别（例如集群）的设置向下复制到较低（例如组）级别。

例如，在创建集群后，我们的 dnsconfig 设置起初如下所示：

Configured at mode:

Cluster: Yes

Group Main_Group: No

Group Paris: No

Group Rome: No

Machine lab2.cable.nu: No

如果我们将 DNS 设置“复制到组”，将如下所示：

Configured at mode:

Cluster: Yes

Group Main_Group: No

Group Paris: Yes

Group Rome: No

Machine lab2.cable.nu: No

现在，您可以编辑 Paris 组级别的 DNS 设置，而 Paris 组的其他计算机将继承这些设置。除非非 Paris 计算机具有特定于计算机的设置，否则它们将继承集群设置。除了 DNS 设置，为 SMTPROUTES 创建组级别设置则非常常见。

提示 使用各种菜单中的 CLI CLUSTERSET 功能时，可以使用一项 GUI 无法提供的特殊选项将设置复制到所有组。

侦听程序将自动从组或集群中完全继承，通常您只需在集群的第一个系统中创建侦听程序。这样可以显著减少管理工作。但是，要使用此功能，整个组或集群的接口的名称必须完全相同。

一旦组级别定义的设置正确，即可将计算机加入集群，使它们成为此组的成员。需要两个步骤：

首先，要将我们剩余的 4 个系统加入集群，需要在每个系统中运行 clusterconfig。集群越庞大和复杂，加入所需的时间就越长，可能需要几分钟。可以使用 LIST 和 CONNSTATUS 子命令监控加入的进度。加入完成后，可以使用 SETGROUP 将计算机从 Main_Group 移至 Paris 和 Rome。有一种情况无法避免，即添加到集群的所有计算机最初将继承 Main_Group 设置，而不是 Paris 和 Rome 的设置。如果新系统已在运行中，这样可能会影响邮件流量。

提示 切勿将实验计算机加入与生产计算机相同的集群。对于实验系统，使用新的集群名称。这样可增加一层保护，防止出现意外变更（例如，有人更改实验系统会意外丢失生产邮件）。

使用 CM 设置（而不是集群默认设置）的 GUI 选项摘要

覆盖设置，开始使用默认设置。例如，SMTPROUTES 配置的默认设置是一个空白表，然后您可以从头开始构建。

覆盖设置，但开始使用当前继承自集群 xxx 或组 yyy 的设置副本。例如，您可能希望在组级别获得一份新的 SMTPROUTES 表副本（初始与集群表相同）。同一组 (SETGROUP) 中包含的所有思科设备都将获得此表。不在该组的计算机仍将使用集群级别设置。在此表的独立副本中更改SMTPROUTES不会影响其他组、继承集群设置的计算机或在单个计算机级别定义设置的计算机。这是最常见的选择。

管理设置，“集中管理选项”(Centralized Management Options) 的子菜单。在此菜单中，可以复制如上设置，也可以移动或删除设置。如果将 SMTPROUTES 移到组或计算机级别，路由表将在集群级别为空，但在更具体的级别仍然存在。

管理设置。继续我们的SMTPROUTES示例，使用删除选项也会导致集群的SMTPROUTES表为空。如果您先前在组级别或计算机级别为 SMTPROUTES 配置了定义，这没什么问题。但最好不要删除集群级别设置，而仅依赖于组或计算机设置。集群范围的设置作为新添加计算机的默认设置，它们非常有用，保留它们可减少一项您必须维护的组或站点设置。

设置和配置问题

问：我有一台以前配置的独立计算机，将其加入了现有集群。我的设置会发生什么情况？

答：当计算机加入集群时，该计算机所有可集群化的设置都将从该集群级别继承。在加入集群后，所有本地配置的非网络设置将丢失，被集群及任何关联组的设置覆盖。（其中包括用户/密码表；密码和用户在集群内共享）。

问：我有一台集群计算机，并从集群中（永久）删除了该计算机。我的设置会发生什么情况？

答：从集群中永久删除计算机后，其配置层次结构将“趋于扁平”，计算机的运行方式将与其之前属于该集群成员时相同。该计算机继承的所有设置将在独立设置中应用于计算机。

例如，如果只有一个集群模式的“全局取消订用”(Global Unsubscribe) 表，则从集群中删除计算机后，该“全局取消订用”(Global Unsubscribe) 表的数据将复制到计算机的本地配置中。

一般问题

问：日志文件是否汇集在集中管理的计算机中？

答：不是。日志文件仍然为每台计算机单独保留。出于跟踪和报告目的，可使用安全管理设备汇集多个计算机中的邮件日志。

问：用户访问的工作原理是什么？

答：思科设备针对整个集群共享一个数据库。特别是，整个集群只有一个 admin 帐户（和密码）。

问：我应该如何将数据中心集群化？

答：理想地讲，数据中心是集群内的一个“组”，不是自己的集群。但是，如果数据中心自身之间共享的数据不多，最好是每个数据中心设置独立的集群。

问：如果系统脱机，然后重新连接，会发生什么情况？

答：在重新连接到集群后，系统将尝试同步。

网络问题

问：集中管理功能是“对等”架构还是“主/从”架构？

答：由于每台计算机都包含所有计算机的所有数据（包括其不会使用的所有计算机特定的设置），所以可以将集中管理视为点对点架构。

问：如何设置一个框，才不会使其成为一个点？我想要“从属”系统。

答：使用这种架构无法创建真正的“从属”计算机。但是，可以在计算机级别禁用 HTTP (GUI) 和 SSH (CLI) 访问。这样，则只能通过 clusterconfig 命令配置没有 GUI 或 CLI 访问权限的计算机（也就是说，它永远不能作为登录主机）。这与拥有从属计算机类似，但该配置在重新打开登录访问权限后即失效。

问：是否可以创建多个分段的集群？

答：可以注册隔离的“孤岛”集群；实际上，有些情况下创建此类集群比较有利，例如出于性能考虑的情况。

问：我想重新配置加入集群的某台设备的 IP 地址和主机名。如果这样做，在运行重启命令前是否会丢失 GUI/CLI 会话？

答：请按以下步骤操作：

1. 添加新 IP 地址。
2. 将侦听程序移到新地址上
3. 离开集群

4. 更改主机名
5. 确保从任何计算机查看时，clusterconfig 连接列表中都不会显示旧计算机名称
6. 确保所有 GUI 会话均已注销
7. 确保任何接口上都未启用 CCS（通过 interfaceconfig 或“网络”>“侦听程序”检查）
8. 将计算机再次添加到集群中

问：是否可以在集群级别应用目标控制功能？还是只能在本地计算机级别应用？

答：可以在集群级别设置；但是限制在计算机级别设置。因此，如果限制为 50 个连接，则 50 就是为集群中每台计算机设置的限制。

规划与配置

问：在设置集群时，如何才能最大限度地提高效率和减少问题？

1. 初始规划
   - 尝试在集群级别配置尽可能多的设置。
   - 仅对例外情况按计算机进行管理。
   - 比方说，您有多个数据中心，则可使用组来共享既不是集群也不必特别于计算机的属性。
   - 对于每台设备上的接口和侦听程序，使用相同的名称。
2. 注意受限命令。
3. 了解设置之间的相互依赖关系。

   例如，listenerconfig 命令（即使在集群级别）依赖于仅在计算机级别存在的接口。如果并不是集群中所有计算机的计算机级别都存在该接口，该侦听程序将被禁用。

   请注意，删除接口还会影响 listenerconfig。
4. 注意您的设置！

   切记，先前配置的计算机在加入集群后将丢失其独立设置。如果要重新应用以前在计算机级别配置的某些设置，请务必在加入集群之前记下所有设置。

   切记，“断开连接的”计算机仍是集群的一部分。在计算机重新连接后，您在其脱机状态下所做的任何更改将与集群的其余计算机同步。

   请记住，如果从集群中永久删除某台计算机，该计算机将保留其属于集群时的所有设置。但是，如果您改变主意将其重新加入集群，该计算机将丢失全部独立设置。

   使用 saveconfig 命令可记录设置。

第 42 章

测试和故障排除

本章包含以下部分：

使用测试邮件调试邮件流：追踪

您可以使用**系统管理 > 跟踪**页面（与 CLI 中的 trace 命令等效）通过模拟发送测试邮件来利用系统调试邮件流。“跟踪”页面（和 **trace** CLI 命令）会模拟一封邮件被侦听程序接受，并会打印一份已被系统当前配置（包括未被确认的更改）“触发”或受其影响的功能摘要。测试消息实际上并未发送。“跟踪”页面（以及 **trace** CLI 命令）是一种强大的故障排除和调试工具，尤其是在结合思科设备的许多高级功能的情况下，其功能会更强大。

注释 追踪不适用于测试文件信誉扫描。

“跟踪”页面（和 **trace** CLI 命令）会提示您提供下表所列的输入参数。

表 *146:*“跟踪”页面的输入

值	说明	示例
源 IP 地址	输入远程客户端的 IP 地址，以模拟远程域的源。该地址可以是互联网协议版本 4 (IPv4) 或版本 6 (IPv6) 地址。 注：trace 命令会提示用户输入 IP 地址和完全限定域名。它不会尝试根据该 IP 地址反查其是否与完全限定域名匹配。trace 命令不允许完全限定域名字段为空，因此不可能在 DNS 反向匹配不正确的情况下进行测试。	**203.45.98.109** **2001:0db8:85a3::8a2e:0370:7334**
源 IP 的完全限定域名	输入完全限定远程域名以进行模拟。如果完全限定域名字段为空，则会对源 IP 地址执行反向 DNS 查询。	**smtp.example.com**
用于跟踪行为的监听程序	从系统内配置的监听程序列表中选择，作为模拟发送测试消息的目标。	**InboundMail**
SenderBase 网络所有者组织 ID	输入 SenderBase 网络所有者的唯一标识号，或让系统查找与源 IP 地址相关联的网络所有者 ID。如果用户通过 GUI 将网络所有者添加至发件人组，就能够查看此信息。	**34**
SenderBase 信誉得分（SBRS 得分）	输入要为被欺骗的域提供的 SBRS 得分，或者允许系统查找与源 IP 地址关联的 SBRS 得分。这有助于使用 SBRS 得分对策略进行测试。请注意，手动输入的 SBRS 得分不会传递至上下文自适应扫描引擎 (CASE)。有关详细信息，请参阅编辑侦听程序的发件人信誉过滤得分阈值，第 77 页。	**-7.5**
信封发件人	输入测试消息的信封发件人。	**admin@example.net**
信封收件人	输入测试消息的收件人列表。使用逗号分隔多个条目。	**joe** **frank@example.com**
消息内容	输入测试消息的消息内容，包括标题。在输入消息内容时，请在分隔行末尾输入句号。请注意，“标题”也是消息内容的一部分（由空行隔开），如果遗漏标题或格式输入不当，则可能导致无法达到预期的跟踪结果。	**收件人：1@example.com** 发件人：ralph 主题：测试 **this is a test message** **.**

输入值后，请点击**开始跟踪**。将显示系统上配置的、对消息有影响的所有功能汇总。

用户可以从本地文件系统上传邮件内容。（在 CLI 中，用户可使用已上传至 **/configuration** 目录下的邮件内容进行测试。有关放置文件以导入思科设备的详细信息，请参阅FTP、SSH 和 SCP 访问，第 979 页。）

汇总显示后，系统会提示用户查看结果消息并重新运行测试消息。如果输入另一封测试邮件，则“跟踪”页面和 trace 命令使用上表中您输入的任何先前值。

注释 按次序执行下表中所列的使用 trace 命令测试的配置项。这对了解功能配置之间的互相影响有很大帮助。例如，通过域映射功能转换的收件人地址在由 RAT 评估时会影响该地址。根据别名表对受 RAT 影响的收件人求值时，又会对该地址产生影响，等等。

表 *147:* 执行跟踪时查看输出

trace 命令部分	**输出**
主机访问表 (HAT) 及邮件流策略处理	对用户指定的监听程序的主机访问表设置进行处理。系统报告 HAT 中与用户输入的远程 IP 地址及远程域名匹配的条目。用户可以查看默认邮件流策略和发件人组，以及与给定条目一致的内容。 如果思科设备配置为拒绝连接（通过 REJECT 或 TCPREFUSE 访问规则），则 trace 命令会在处理过程中退出。 有关更多设置 HAT 参数的信息，请参阅 了解预定义发件人组和邮件流策略，第 90 页。
信封发件人地址处理 这些部分汇总了设备配置对用户提供的信封发件人的影响。（即设备配置如何解释 MAIL FROM 命令。）**trace** 命令会在此部分之前打印“**正在处理 MAIL FROM：**”。	
默认域	如果用户指定某监听程序更改其接收消息的默认发件人域，则对信封发件人所作的任何更改都会显示在此部分中。 有关详细信息，请参阅配置网关以接收邮件，第 61 页。
化妆	如果用户指定要转换某消息的信封发件人，则所作更改会在此处注明。用户使用 **listenerconfig -> edit -> masquerade -> config subcommands** 子命令，在专用侦听程序上对信封发件人启用伪装。 有关详细信息，请参阅配置路由和传送功能，第 523 页。
信封收件人处理 这些部分汇总了设备配置对用户提供的信封收件人的影响。（即设备配置如何解释 RCPT TO 命令。）trace 命令会在此部分之前打印“正在处理收件人列表：”。	

trace 命令部分	输出
默认域	如果用户指定某监听程序更改其接收消息的默认发件人域，则对信封收件人所作的任何更改都会显示在此部分中。 有关详细信息，请参阅配置网关以接收邮件，第 61 页。
域映射转换	域映射功能可将收件人地址转换为其他地址。如果用户指定了任何域映射更改，并且用户指定的收件人地址在更改范围内，则此部分中会显示出转换过程。 有关详细信息，请参阅配置路由和传送功能，第 523 页。
收件人访问表 (RAT)	除策略及参数外，此部分还会显示出与 RAT 内的条目匹配的每个信封收件人。（例如，指定某收件人忽略监听程序 RAT 中的限制。） 有关指定您接受的收件人的详细信息，请参阅配置网关以接收邮件，第 61 页。
别名表	此部分会显示出与设备上配置的别名表内条目匹配的每个信封收件人（以及随后向一个或多个收件人地址的转换）。 有关详细信息，请参阅配置路由和传送功能，第 523 页。
Pre-Queue 消息操作 这些部分汇总了设备在收到消息内容后、将消息列入工作队列之前，对每个消息的影响。该处理工作在将最终的 **250 ok** 命令返回到远程 MTA 之前进行。 **trace** 命令在此部分之前列显“邮件正在处理：”。	
虚拟网关	**altsrchost** 命令基于信封发件人的完整地址、域/域名或 IP 地址的匹配，向指定接口分配消息。如果信封发件人与 **altsrchost** 命令中的条目相匹配，则该信息会显示在此部分中。 请注意，此时分配的虚拟网关地址可能会由以下消息过滤器的处理所覆盖。 有关详细信息，请参阅配置路由和传送功能，第 523 页。
退回配置文件	退回配置文件在处理过程中的三个不同时间使用。这是第一次出现。如果处理过程中要为监听程序分配退回配置文件，则会在此时分配。该信息会显示在此部分中。 有关详细信息，请参阅配置路由和传送功能，第 523 页。
工作队列操作 下面的一组功能将针对工作队列中的消息执行。这组操作发生在客户端接收消息后、将消息列入目标队列等待发送之前。“工作队列中的邮件”由 status 和 status detail 命令进行报告。	

trace 命令部分	输出
化妆	如果用户指定要隐藏消息的收件人、发件人以及抄送标题（通过从监听程序输入的静态表或通过 LDAP 队列），则所作更改会在此处注明。用户使用 **listenerconfig -> edit -> masquerade -> config** 子命令，在专用侦听程序上对邮件信头启用伪装。 有关详细信息，请参阅配置路由和传送功能，第 523 页。
LDAP 路由	如果监听程序上启用了 LDAP 队列，则此部分会显示 LDAP 的接收结果、重编路由、伪装以及组队列。 有关详细信息，请参阅LDAP 查询，第 585 页。
消息过滤器处理	此时，通过测试消息对系统内启用的所有消息过滤器进行求值。对每个过滤器的规则求值，如果最终结果为“真”，则按顺序执行该过滤器内的每步操作。过滤器可能会包含其他过滤器，将其作为一种操作，且过滤器的嵌套是不受限的。如果规则评估为“false”，并且操作列表与 else 子句关联，则改为评估这些操作。此部分将会显示按顺序处理的消息过滤器的结果。 请参阅使用邮件过滤器实施邮件策略，第 117 页。
邮件策略处理 “邮件策略处理”(mail policy processing) 部分显示了反垃圾邮件、防病毒、爆发过滤器功能以及您提供的所有收件人的声明时间戳。如果多个收件人与电邮安全管理器中的多条策略相匹配，则将为每条匹配的策略重复显示以下部分。字符串：“Message Going to（消息收件人）”将定义收件人和以及匹配的策略。	
反垃圾邮件	本部分显示未标记接受反垃圾邮件扫描处理的消息。如果要在消息送达监听程序之前，对消息进行反垃圾邮件扫描处理，则会在处理消息后显示返回的裁决。如果思科设备配置为根据判定退回或丢弃邮件，则会列显该信息，并且 **trace** 命令处理将停止。 注意：如果反垃圾邮件扫描在系统内不可用，则跳过此步骤。如果反垃圾邮件扫描可用，但未使用功能键启用，则此部分同样会显示该信息。 请参阅反垃圾邮件，第 269 页。

trace 命令部分	输出
防病毒	此部分显示未标记接受防病毒扫描处理的消息。如果要在消息送达监听程序之前，对消息进行防病毒扫描处理，则会在处理消息后显示返回的裁决。如果思科设备配置为“清除”受感染邮件，则会注明该信息。如果该设备配置为根据判定退回或丢弃消息，则会显示出该信息，且 trace 命令的处理停止。 注意：如果防病毒扫描在系统内不可用，则跳过此步骤。如果防病毒扫描可用，但未使用功能键启用，则此部分同样会显示该信息。 请参阅 防病毒，第 253 页。
手工内容过滤	系统上启用的所有内容过滤器此时都会由测试邮件进行评估。对每个过滤器的规则求值，如果最终结果为“真”，则按顺序执行该过滤器内的每步操作。过滤器可能会包含其他过滤器，将其作为一种操作，且过滤器的嵌套是不受限的。按照顺序处理的内容过滤器的结果在此部分打印。 请参阅内容过滤器，第 235 页。
爆发过滤器处理	此部分指明，包含附件的邮件将要绕过爆发过滤器功能。如果邮件将由收件人的爆发过滤器处理，邮件将被处理和评估。如果该设备配置为根据裁决隔离、退回或丢弃消息，则会显示出该信息，且处理会停止。 请参阅病毒爆发过滤器，第 307 页。
页脚印戳	此部分指明是否将页脚文本资源追加到邮件。并显示了文本资源名称。请参阅文本资源，第 481 页中邮件免责声明标记，第 482 页。
发送操作 以下部分显示消息送达时进行的操作。在此部分之前，trace 命令将显示“队列中等待发送的邮件”。	
根据域和用户进行全局退订	如果任何被指定为 trace 命令输入的收件人与全局退订功能中所列的收件人、收件人域或 IP 地址相匹配，则所有退订的收件人地址都会显示在此部分中。 请参阅配置路由和传送功能，第 523 页。
最终结果 全部处理过程显示后，用户会收到最终结果的提示。在 CLI 中，针对问题“是否要查看生成的邮件”回答 **y**，以查看生成的邮件。	

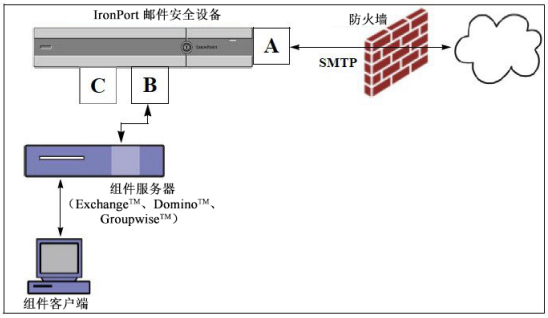
使用侦听程序测试设备

通过“黑洞”侦听程序，可以测试您的邮件生成系统，同时还可以粗略衡量接收性能。黑洞侦听程序的两种类型是排队和非排队。

- 排队侦听程序会将邮件保存到队列，然后立即将其删除。如果希望衡量您的邮件生成系统的整个注入部分的性能，请使用排队侦听程序。
- 非排队侦听程序会接受邮件，然后立即将其删除，不进行保存。如果希望排除邮件生成系统与设备之间的连接故障，请使用非排队侦听程序。

例如，在下图中，可以创建黑洞侦听程序“C”来镜像标记为“B”的专用侦听程序。非排队版本会测试从组件客户端到组件服务器再到设备的系统性能路径。排队版本会测试相同的路径以及设备使邮件入队并为通过 SMTP 传送而做准备的能力。

图 *85:* 企业网关的黑洞侦听程序



在以下示例中，使用 listenerconfig 命令在管理接口上创建名为 BlackHole_1 的黑洞排队侦听程序。然后，编辑侦听程序的主机访问表 (HAT) 以接受来自以下主机的连接：

- **yoursystem.example.com**
- **10.1.2.29**
- **badmail.tst**
- **.tst**

注释 最后的条目 .tst 用于配置侦听程序，以便 .tst 域中的任何主机都可以向名为 BlackHole_1 的侦听程序发送邮件。

示例

```
mail3.example.com> listenerconfig

Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private
```

```
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> new
Please select the type of listener you want to create.
1. Private
2. Public
3. Blackhole
[2]> 3
Do you want messages to be queued onto disk? [N]> y
Please create a name for this listener (Ex: "OutboundMail"):
[]> BlackHole_1
Please choose an IP interface for this Listener.
1. Management (192.168.42.42/24: mail3.example.com)
2. PrivateNet (192.168.1.1/24: mail3.example.com)
3. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1
Choose a protocol.
1. SMTP
2. QMQP
[1]> 1
Please enter the IP port for this listener.
[25]> 25
Please specify the systems allowed to relay email through the IronPort C60.
Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
IP addresses, IP address ranges, and partial IP addressed are allowed.
Separate multiple entries with commas.

[]> yoursystem.example.com, 10.1.2.29, badmail.tst, .tst
Do you want to enable rate limiting per host? (Rate limiting defines
```

```
the maximum number of recipients per hour you are willing to receive from a remote
domain.) [N]> n

Default Policy Parameters

==========================

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 600

Maximum Number Of Messages Per Connection: 10,000

Maximum Number Of Recipients Per Message: 100,000

Maximum Number Of Recipients Per Hour: Disabled

Use SenderBase for Flow Control: No

Spam Detection Enabled: No

Virus Detection Enabled: Yes

Allow TLS Connections: No

Allow SMTP Authentication: No

Require TLS To Offer SMTP authentication: No

Would you like to change the default host access policy? [N]> n

Listener BlackHole_1 created.

Defaults have been set for a Black Hole Queuing listener.

Use the listenerconfig->EDIT command to customize the listener.

Currently configured listeners:

1. BlackHole_1 (on Management, 192.168.42.42) SMTP Port 25 Black Hole Queuing

2. InboundMail (on PublicNet, 192.1681.1) SMTP Port 25 Public

3. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]>
```

注释 请记得要发出 commit 命令，这些更改才能生效。

在配置了黑洞排队侦听程序并修改了 HAT 以接受来自注入系统的连接后，请使用注入系统向设备发送邮件。使用 status、status detail 和 rate 命令监控系统性能。也可以通过图形用户界面 (GUI) 来监控系统。有关详情，请参阅：

- 使用 CLI 监控，第 810 页
- GUI 中的其他任务，第 839 页

排除网络故障

如果怀疑设备存在网络连接问题，请先确认设备是否正常工作。

测试设备的网络连接

步骤 1 连接到系统并以管理员身份登录。成功登录后，将显示以下信息：

```
Last login: day month date hh:mm:ss from IP address

Copyright (c) 2001-2003, IronPort Systems, Inc.

AsyncOS x.x for Cisco


Welcome to the Cisco Messaging Gateway Appliance(tm)
```

步骤 2 使用 status 或 status detail 命令。

```
mail3.example.com> status
```

或

```
mail3.example.com> status detail
```

status 命令将返回监控到的有关邮件操作的信息子集。 返回的统计信息分为两类：计量器和测量器。 有关邮件操作的完整监控信息（包括速率），请使用 status detail 命令。计数器提供系统中运行的各个事件的总数。对于每个计数器，您可以查看自计数器重置以来、自系统上次重新引导以来以及在系统的整个生命周期所发生的事件总数。（有关详细信息，请参阅使用 CLI 监控，第 810 页。）

步骤 3 使用 `mailconfig` 命令向已知的工作地址发送邮件。

`mailconfig` 命令会生成一种可读文件，包括设备可用的所有配置设置。尝试将文件从设备发送到已知工作邮件地址，以确认设备可以通过网络发送邮件。

```
mail3.example.com> mailconfig


Please enter the email address to which you want to send the
configuration file.
```

```
Separate multiple addresses with commas.

[]> user@example.com

Do you want to include passphrases? Please be aware that a configuration without
passphrases will fail when reloaded with loadconfig. [N]> y


The configuration file has been sent to user@example.com.

mail3.example.com>
```

故障排除

确认设备在网络中处于活动状态后，请使用以下命令查明所有网络问题。

- 可以使用 `netstat` 命令显示网络连接（包括传入和传出）、路由表和大量网络接口统计信息，包括以下信息：
  - 活动套接字列表
  - 网络接口状态
  - 路由表内容
  - 侦听队列的大小
  - 数据包流量信息
- 可以使用 `diagnostic -> network -> flush` 命令清空所有网络相关的缓存。
- 可以使用 `diagnostic -> network -> arpshow` 命令显示系统 ARP 缓存。
- 可以使用 `packetcapture` 命令解释和显示 TCP/IP 及其他正在通过计算机连接到的网络传送或接收的数据包。

  要使用 `packetcapture`，请设置网络接口和过滤器。过滤器使用相同的命令格式 UNIX `tcpdump` 命令。使用 start 开始数据包捕获，使用 stop 停止数据包捕获。停止捕获之后，需要使用 SCP 或 FTP 从 /pub/captures 目录下载文件。有关详细信息，请参阅运行数据包捕获，第 957 页。
- 使用 `ping` 命令到达已知工作主机，以确认设备在网络中具有活动连接，并且能够到达特定网段。

  使用 `ping` 命令可以测试网络主机与设备的连接。

```
mail3.example.com> ping


Which interface do you want to send the pings from?

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)
```

```
[1]> 1

Please enter the host you wish to ping.

[]> anotherhost.example.com

Press Ctrl-C to stop.

PING anotherhost.example.com (x.x.x.x): 56 data bytes

64 bytes from 10.19.0.31: icmp_seq=9 ttl=64 time=0.133 ms

64 bytes from 10.19.0.31: icmp_seq=10 ttl=64 time=0.115 ms

^C

--- anotherhost.example.com ping statistics ---

11 packets transmitted, 11 packets received, 0% packet loss

round-trip min/avg/max/stddev = 0.115/0.242/1.421/0.373 ms
```

注释 您必须使用 Control-C 才能结束 ping 命令。

- 使用 `traceroute` 命令测试网络主机与设备的连接性并调试网络跳的路由问题。

```
mail3.example.com> traceroute

Which interface do you want to trace from?

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Please enter the host to which you want to trace the route.

[]> 10.1.1.1

Press Ctrl-C to stop.

traceroute to 10.1.1.1 (10.1.1.1), 64 hops max, 44 byte packets

1 gateway (192.168.0.1) 0.202 ms 0.173 ms 0.161 ms

2 hostname (10.1.1.1) 0.298 ms 0.302 ms 0.291 ms

mail3.example.com>
```

- 使用 `diagnostic -> network -> smtpping` 命令测试远程 SMTP 服务器。
- 使用 `nslookup` 命令检查 DNS 功能。

`nslookup` 命令可以确认设备能够到达并解析来自工作 DNS（域名服务）服务器的主机名和 IP 地址。

```
mail3.example.com> nslookup

Please enter the host or IP to resolve.

[]> example.com


Choose the query type:

1. A

2. CNAME

3. MX

4. NS

5. PTR

6. SOA

7. TXT

[1]>

A=192.0.34.166 TTL=2d
```

表 *148:* 检查 *DNS* 功能：查询类型

查询类型	说明
	主机的 Internet 地址
CNAME	别名的规范名称
墨西哥	邮件交换器
NS	用于指定区域的名称服务器
PTR	如果查询是互联网地址，则指主机名，否则，是指向其他信息的指针
SOA	域的“授权起始点”信息
TXT	文本信息

- 使用 CLI 的 `tophosts` 命令或 GUI，并按“活动收件人”进行排序。

  `tophosts` 命令返回队列中前 20 个收件人主机的列表。此命令可帮助您确定是否已将网络连接问题隔离至您尝试向其发送邮件的单个或一组主机。（有关详细信息，请参阅中的“确定邮件队列的构成”。）

```
mail3.example.com> tophosts

Sort results by:
```

```
1. Active Recipients

2. Connections Out

3. Delivered Recipients

4. Soft Bounced Events

5. Hard Bounced Recipients

[1]> 1

Status as of: Mon Nov 18 22:22:23 2003

ActiveConn.Deliv.SoftHard

# Recipient HostRecipOutRecip.BouncedBounced

1 aol.com36510255218

2 hotmail.com29071982813

3 yahoo.com13461231119

4 excite.com9838494

5 msn.com8427633 29

^C
```

- “向下钻取”以使用 tophosts 命令结果中列出的顶部域中的 `hoststatus` 命令。

  `hoststatus` 命令会返回有关与特定收件人主机相关的邮件操作的监控信息。此外，还会提供 AsyncOS 缓存中存储的 DNS 信息以及从收件人主机返回的最后一条错误。返回的数据是从上一个 `resetcounters` 命令运行以来累加的。（有关详细信息，请参阅 监控邮件主机的状态，第 813 页。）

  使用顶部域中的 `hoststatus` 命令可以将 DNS 解析的性能问题隔离到设备或互联网。例如，如果顶部的活动收件人主机的 `hoststatus` 命令显示了许多待定出站连接，则尝试确定该特定主机是否已关闭或无法到达，或者设备是否无法连接到全部或大多数主机。

- 检查防火墙权限。

  设备可能需要打开以下所有端口才能正常工作：端口 20、21、22、23、25、53、80、123、443 和 628。（请参阅防火墙资讯，第 1005 页。）

- 从网络中的设备向 dnscheck@ironport.com 发送邮件

  将邮件从网络内部发送至 dnscheck@ironport.com 以在系统上执行基本的 DNS 检查。自动回复邮件将对以下四种测试的结果和详细信息加以回应。

DNS PTR 记录 - “信封发件人”的 IP 地址与域的 PTR 记录是否匹配？

DNS A 记录 - 域的 PTR 记录与“信封发件人”的 IP 地址是否匹配？

HELO 匹配 - `SMTP HELO` 命令中列出的域与“信封发件人”的 DNS 主机名是否匹配？

邮件服务器接受延迟退回邮件 - `SMTP HELO` 命令中列出的域是否具有解析该域的 IP 地址的 MX 记录？

排除侦听程序故障

如果您怀疑注入邮件存在问题，请采用以下战略方法：

- 确认您正在从其注入的 IP 地址，然后使用 `listenerconfig` 命令检查允许的主机。

  是否允许 IP 地址连接到您创建的侦听程序？使用 `listenerconfig` 命令检查侦听程序的主机访问表 (HAT)。使用以下命令打印侦听程序的 HAT：

  ```
  listenerconfig -> edit -> listener_number -> hostaccess -> print
  ```

  HAT 可以配置为通过 IP 地址、IP 地址块、主机名或域拒绝连接。有关详细信息，请参阅“指定允许连接的主机”。

  您还可以使用 `limits` 子命令检查侦听程序允许的最大连接数：

  ```
  listenerconfig -> edit -> listener_number -> limits
  ```

- 在您从其注入的计算机中，使用 Telnet 或 FTP 手动连接到设备。例如：

  ```
  injection_machine% telnet appliance_name
  ```

  您还可以使用设备中的 `telnet` 命令从侦听程序连接到实际设备：

  ```
  mail3.example.com> telnet

  Please select which interface you want to telnet from.

  1. Auto

  2. Management (192.168.42.42/24: mail3.example.com)

  3. PrivateNet (192.168.1.1/24: mail3.example.com)

  4. PublicNet (192.168.2.1/24: mail3.example.com)

  [1]> 3

  Enter the remote hostname or IP.

  []> 193.168.1.1

  Enter the remote port.

  [25]> 25

  Trying 193.168.1.1...

  Connected to 193.168.1.1.

  Escape character is '^]'.
  ```

  如果无法从一个接口连接到另一个接口，可能是设备的管理接口以及 Data1 和 Data2 接口连接到网络的方式有问题。有关更多信息，请参阅FTP、SSH 和 SCP 访问，第 979 页。您可以使用 telnet 登录到侦听程序的端口 25 并手动输入 SMTP 命令（如果您熟悉该协议）。

- 检查 IronPort 文本邮件日志和注入调试日志，以检查是否存在接收错误。

注入调试日志记录设备与连接到系统的指定主机之间的 SMTP 会话。注入调试日志对于排除设备与从互联网发起连接的客户端之间的通信问题很有帮助。该日志记录两个系统之间传送的所有字节并将这些字节分类为“已发送至”连接主机或“接收自”连接主机。

有关详细信息，请参阅使用文本邮件日志，第 862 页和使用注入调试日志，第 876 页。

排除从设备传送邮件的故障

如果您怀疑从设备传送邮件存在问题，请采用以下战略方法：

- 确定问题是否是域特定的问题。

  使用 `tophosts` 命令获取有关邮件队列的即时信息并确定特定收件人域是否存在传送问题。

  按“活动收件人”分类时返回的域是否存在问题？

  按“连接输出”分类时，是否有任何域达到了为侦听程序指定的最大连接数？侦听程序默认的最大连接数为 600。默认的系统范围最大连接数为 10,000（通过 `deliveryconfig` 命令设置）。您可以使用以下命令检查侦听程序的最大连接数：

  ```
  listenerconfig -> edit -> listener_number -> limits
  ```

  侦听程序的连接数是否受 `destconfig` 命令（或者系统最大数或虚拟网络地址）的进一步限制？使用此命令检查 `destconfig` 连接限制：

  ```
  destconfig -> list
  ```

- 使用 `hoststatus` 命令。

  使用结果（通过 `tophosts` 命令列出）中列出的顶部域上的 `hoststatus` 命令“向下钻取”。

  主机是否可用并接受连接？

  给定主机的某个特定 MX 记录邮件服务器是否存在问题？

  如果指定的主机存在 5XX 错误（永久负完成回复），则 `hoststatus` 命令会报告该主机返回的最后一个“5XX”状态代码和说明。如果与主机的最后一个传出 TLS 连接失败，则 `hoststatus` 命令会显示失败的原因。

- 配置和/或检查域调试、退回和文本邮件日志来检查收件人主机是否可用。

  域调试日志记录设备与指定收件人主机之间的 SMTP 会话期间的客户端和服务器通信。此日志文件类型可用来调试特定收件人主机存在的问题。

  有关详细信息，请参阅使用域调试日志，第 875 页。

  退回日志记录与每个已退回收件人有关的所有信息。

  有关详细信息，请参阅使用退回日志，第 870 页。

  文本邮件日志包含邮件接收、邮件传送和退回的详细信息。此外，每分钟还会将状态信息写入邮件日志。这些日志是非常有用的信息来源，可用于了解特定邮件的传输及分析系统性能。

  有关详细信息，请参阅使用文本邮件日志，第 862 页。

- 使用 `telnet` 命令从设备连接到问题域：

```
mail3.example.com> telnet

Please select which interface you want to telnet from.

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Enter the remote hostname or IP.

[]> problemdomain.net

Enter the remote port.

[25]> 25
```

- 您可以使用 `tlsverify` 命令按需建立出站 TLS 连接并调试有关目的域的所有 TLS 连接问题。要创建连接，请指定进行验证所参照的域和目的主机。AsyncOS 会根据所需的（验证）TLS 设置检查 TLS 连接。

```
mail3.example.com> tlsverify

Enter the TLS domain to verify against:

[]> example.com

Enter the destination host to connect to. Append the port (example.com:26) if you are

not connecting on port 25:

[example.com]> mxe.example.com:25

Connecting to 1.1.1.1 on port 25.

Connected to 1.1.1.1 from interface 10.10.10.10.

Checking TLS connection.

TLS connection established: protocol TLSv1, cipher RC4-SHA.

Verifying peer certificate.

Verifying certificate common name mxe.example.com.

TLS certificate match mxe.example.com

TLS certificate verified.

TLS connection to 1.1.1.1 succeeded.

TLS successfully connected to mxe.example.com.
```

```
TLS verification completed.
```

排除性能问题

如果您怀疑设备存在性能问题，请采用以下战略方法：

- 使用 rate 和 `hostrate` 命令检查当前的系统活动。

  rate 命令会返回有关邮件操作的实时监控信息。有关详细信息，请参阅显示实时活动，第 816 页。

  `hostrate` 命令会返回特定主机的实时监控信息。

- 使用 status 命令再次确认历史速率，以检查是否存在性能降低问题。
- 使用 `status detail` 命令检查 RAM 利用率。

  您可以使用 `status detail` 命令快速查看系统的 RAM、CPU 和磁盘 I/O 利用率。

  注释 RAM 利用率应始终少于 45%。如果 RAM 利用率超过 45%，设备将进入“资源节约模式；”该模式会启动“后退”算法以防止资源的超订用并发出以下邮件警报：

```
This system (hostname: hostname) has entered a 'resource conservation' mode in order
to
prevent the rapid depletion of critical system resources.


RAM utilization for this system has exceeded the resource conservation threshold of
45%.
The allowed injection rate for this system will be gradually decreased as RAM
utilization approaches 60%.
```

  仅当利用传送性能较差的设备进行攻击性注入时才会出现这种情况。 如果遇到 RAM 利用率超过 45% 的情况，请检查队列中的邮件数并查看特定域是否已关闭或无法传送（通过 `hoststatus` 或 `hostrate` 命令）。此外，还要检查系统的状态并确保传送未处于挂起状态。如果停止注入后 RAM 利用率仍然很高，请与思科客户支持联系。

- 问题是否特定于某个域？

  使用 `tophosts` 命令获取有关邮件队列的即时信息并确定特定收件人域是否存在传送问题。

  检查队列的大小。您可以删除、退回、挂起或重定向邮件队列中的邮件，以管理其大小或处理有问题的特定域的收件人。有关详细信息，请参阅管理邮件队列，第 820 页。使用如下命令：

  - `deleterecipients`
  - `bouncerecipients`
  - `redirectrecipients`
  - `suspenddel / resumedel`
  - `suspendlistener / resumelistener`

使用 tophosts 命令检查软退回和硬退回的数量。按“软退回的事件”（选项 4）或“硬退回的收件人”（选项5）进行分类。如果特定域存在性能问题，请使用上述命令管理到该域的传送。

Web 界面外观和呈现问题

请参阅覆盖 Internet Explorer 兼容模式，第 803 页。

回应警报

警报：C380 或 C680 硬件上的电池充放电已超时（RAID 事件）

问题

您收到 C380 或 C680 硬件“电池充放电超时”（RAID 事件）警报。

解决方案

此警报并不表示一定出了问题。电池自身充放电超时并非意味着 RAID 控制器有任何问题。控制器在随后的充放电过程中可以恢复。请在接下来的 48 小时内监控您的邮件是否出现任何其他 RAID 警报，以确保此问题不是其他问题的副作用所致。如果系统中未出现任何其他 RAID 相关的警报，则可以安全地忽略此警报。

对“其他磁盘使用量接近配额”的警报进行故障排除

问题

您收到“其他磁盘使用量接近配额”的警报。

解决方案

您可以增加配额或删除文件。请参阅管理“其他”配额的磁盘空间，第 759 页。

对硬件问题进行故障排除

硬件设备前面板和/或后面板上的指示灯指示设备的运行状况和状态。有关这些指示灯的说明，请参阅硬件指南，例如《思科 *x90s* 系列内容安全设备的安装和维护指南》，可通过以下网址获取：http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html。

这些文档中还会介绍设备规格，例如温度范围。

远程重置设备电源

如果设备需要硬重置，可以使用第三方智能平台管理界面 (IPMI) 工具远程重启设备机箱。

限制

- 远程电源重新启动仅适用于特定硬件。

  有关特定信息，请参阅启用远程电源循环，第 773 页。

- 如果您希望能够使用此功能，必须在需要使用该功能之前提前将其启用。

  有关详细信息，请参阅启用远程电源循环，第 773 页。

- 仅支持以下 IPMI 命令：

  - **status**、**on**、**off**、**cycle**、**reset**、**diag**、**soft**
  - 发出不受支持的命令将会引发“权限不足”错误。

准备工作

- 获取并设置可使用 IPMI 2.0 版管理设备的实用程序。
- 了解如何使用受支持的 IPMI 命令。请参阅您的 IPMI 工具文档。

步骤 1 使用 IPMI 向分配到“远程电源重新启动”端口（之前配置）的 IP 地址发出支持的电源循环命令，以及所需的凭证。

例如，从支持 IPMI 的 UNIX 类型计算机中可能发出如下命令：

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

其中，**192.0.2.1** 是分配到远程电源重新启动端口的 IP 地址，**remoteresetuser** 和 password 是您在启用此功能时输入的凭证。

步骤 2 等待至少十一分钟，以便设备重启。

使用技术支持

虚拟设备技术支持

获取虚拟设备技术支持的要求在思科内容安全虚拟设备安装指南（可从 http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html 获得）中进行了介绍。

从设备提交或更新支持案例

准备工作

- 如果问题紧急，请勿使用此方法。请改为使用思科客户支持，第 10 页中列出的方法之一与支持人员联系。

仅当遇到类似请求信息或者您有解决方法但希望采用备选方案的问题时再使用以下过程。

- 考虑获取帮助的其他选项：
  - 知识库，第 9 页
  - 思科支持社区，第 9 页
- 要直接从设备访问思科技术支持，您的 Cisco.com 用户 ID 必须与此设备的服务协议合同关联。要查看当前与您的 Cisco.com 配置文件相关的服务合同列表，请访问位于 https://sso.cisco.com/autho/forms/CDClogin.html 的 Cisco.com 配置文件管理器。如果没有 Cisco.com 用户 ID，请注册一个。请参阅注册思科帐户，第 10 页。

  请务必要将您的 Cisco.com 用户 ID 和支持合同 ID 保存在一个安全的位置。
- 使用此过程创建支持请求时，系统会将设备配置文件发送给思科客户支持人员。如果不希望发送设备配置，可以使用其他方法与客户支持人员联系。
- 在集群配置中，支持请求及其保存的值是计算机特定的。
- 设备必须连接到互联网，并可以发送邮件。
- 如果要发送有关现有案例的信息，请确保拥有案例编号。

步骤 1 登录设备。

步骤 2 依次选择**帮助和支持 (Help and Support) > 联系技术支持 (Contact Technical Support)**。

步骤 3 完成表格。

步骤 4 点击 **Send**。

注释　必须在设备上保存 CCO 用户 ID 和上次输入的合同 ID 以供日后使用。

启用思科技术支持人员远程访问

只有思科客户帮助部门才能使用这些方法访问您的设备。

启用对网络连接设备的远程访问

支持部门可通过此过程在设备与 **upgrades.ironport.com** 服务器之间创建的 SSH 隧道访问设备。

准备工作

标识可通过互联网访问的端口。默认端口为 。大多数防火墙配置都允许通过此端口进行的连接。

步骤 1 登录到设备。

步骤 2 在 GUI 窗口的右上角，依次选择**帮助和支持 (Help and Support) > 远程访问 (Remote Access)**。

步骤 3 点击**启用 (Enable)**。

步骤 4 输入信息：

选项	说明
种子字符串	种子字符串用于生成一个安全的共享密码，思科客户支持要使用该密码访问此设备。
安全隧道	选中该复选框以使用安全隧道进行远程访问连接。 输入连接的端口。 默认端口为 25 ，该端口在大多数环境中都适用。

步骤 5 点击 **Submit**。

下一步做什么

当不再需要远程访问支持人员时，请参阅禁用技术支持隧道， 第 956 页。

启用对无直接网络连接设备的远程访问

对于未直接连接互联网的设备，通过连接到互联网的其他设备进行访问。

准备工作

- 设备必须能够通过端口 22 连接到其他已连接互联网的设备。
- 在已连接互联网的设备上，按照启用对网络连接设备的远程访问， 第 955 页中的过程创建通往该设备的支持隧道。

步骤 1 在需要支持的设备的命令行界面中，输入 **techsupport** 命令。

步骤 2 输入 **sshaccess**。

步骤 3 按照提示操作。

下一步做什么

当不再需要支持人员的远程访问时，请参阅以下内容：

禁用技术支持隧道

已启用的 techsupport 隧道连续 7 天保持连接到 upgrades.ironport.com。此后，建立的连接不会断开，但一旦断开，将无法重新连接到隧道。

要手动禁用隧道，请执行以下操作：

步骤 1 登录到设备。

步骤 2 在 GUI 窗口的右上角，依次选择**帮助和支持 (Help and Support) > 远程访问 (Remote Access)**。

步骤 3 点击**禁用 (Disable)**。

禁用远程访问

使用 techsupport 命令创建的远程访问帐户将保持活动状态，直到将其禁用为止。

步骤 1 在命令行界面中，输入 techsupport 命令。

步骤 2 输入 sshaccess。

步骤 3 输入 disable。

检查支持连接的状态

步骤 1 在命令行界面中，输入 techsupport 命令。

步骤 2 输入 status。

运行数据包捕获

数据包捕获允许支持人员查看TCP/IP数据，及传入和传出设备的其他数据包。由此，允许支持部门调试网络设置，了解到达设备或离开设备的网络流量。

步骤 1 依次选择**帮助和支持 (Help and Support) > 数据包捕获 (Packet Capture)**。

步骤 2 指定数据包捕获设置：

a) 在**数据包捕获设置 (Packet Capture Settings)** 部分，点击**编辑设置 (Edit Settings)**。

b) （可选）输入数据包捕获的持续时间、限制和过滤器。

您的支持代表可针对这些设置提供指导。

如果输入的捕获持续时间未指定时间单位，AsyncOS 默认以秒为单位。

在**过滤器**部分：

- 自定义过滤器可以使用 UNIX tcpdump 命令支持的任何语法，例如 host 10.10.10.10 && port 80。
- 客户端 IP 是连接到设备的计算机的 IP 地址，例如通过邮件安全设备发送邮件的邮件客户端。
- 服务器 IP 是设备连接到的计算机的 IP 地址，例如设备向其传送邮件的 Exchange 服务器。
- 可以使用客户端和服务器 IP 地址跟踪特定客户端与特定服务器之间的流量，而将邮件安全设备置于两者之间。

c) 点击 **Submit**。

步骤 3 点击**开始捕获 (Start Capture)**。

- 一次只能运行一个捕获。
- 当数据包捕获运行时，“数据包捕获 (Packet Capture)”页面将显示正在进行的捕获的状态，即显示当前的统计数据，例如文件大小和逝去的时间。
- GUI 仅显示在 GUI 中启动的数据包捕获，不包括从 CLI 启动的捕获。同样，CLI 仅显示在 CLI 中启动运行的当前数据包捕获的状态。
- 数据包捕获文件可拆分为十个部分。如果该文件的大小在数据包捕获结束前达到最大限制，系统将删除文件最早的部分（放弃数据），新部分将从当前的数据包捕获数据开始。每次仅放弃仅数据包捕获文件的 1/10。
- 如果正在运行的捕获从 GUI 启动，将保留在会话之间。（如果正在运行的捕获从 CLI 中启动，当会话结束时，捕获将停止。）

步骤 4 允许捕获运行指定的持续时间；如果允许捕获无限期地运行，可通过点击**停止捕获 (Stop Capture)** 手动停止捕获。

步骤 5 访问数据包捕获文件：

- 点击**管理数据包捕获文件 (Manage Packet Capture Files)** 列表，然后点击**下载文件 (Download File)**。
- 使用 FTP 或 SCP 访问设备 captures 子目录中的文件。

下一步做什么

将文件设为可供支持人员访问：

- 如果允许远程访问您的设备，技术人员可使用 FTP 或 SCP 访问数据包捕获文件。请参阅启用思科技术支持人员远程访问，第 955 页。
- 将该文件通过邮件发送给支持人员。

第 43 章

使用 D 模式优化设备的出站邮件传送

本章包含以下部分：

功能摘要：用于优化出站传送的 D 模式

D 模式是通过功能密钥启用的功能，可针对出站邮件传送优化特定邮件安全设备。特定于入站邮件处理的功能在 D 模式下已禁用。

启用 D 模式的设备独有的功能

- 256 个虚拟网关地址 - 思科虚拟网关技术允许为托管的所有域配置企业邮件网关（具有不同的 IP 地址、主机名和域），并为这些域创建单独的公司邮件策略实施和反垃圾邮件策略，同时托管在同一物理设备中。请参阅有关“自定义侦听程序”的信息，在 配置网关以接收邮件， 第 61 页
- IronPort 邮件合并 (IPMM) - IronPort 邮件合并 (IPMM) 免去了从客户系统生成单独的个性化邮件的负担。通过消除生成数以千计的单独邮件的需求并在邮件生成系统和邮件网关之间传输它们，用户可从降低系统负载以及提高的邮件传送吞吐量中获得益处。有关详细信息，请参阅使用 IronPort 邮件合并 (IPMM) 发送大量邮件， 第 962 页。
- 节约资源的退回设置 - 可以配置启用了 D 模式的设备以检测可能被阻止的目标并退回发往该目标的所有邮件。有关详细信息，请参阅配置节约资源的退回设置， 第 961 页。
- 增强出站传输的性能

在启用了 D 模式的设备中禁用的标准功能

- IronPort 反垃圾邮件扫描和内部或外部垃圾邮件隔离 - 由于反垃圾邮件扫描主要适合传入邮件，因此 IronPort 反垃圾邮件扫描引擎已停用。因此，“反垃圾邮件”一章不适用。
- 爆发过滤器 - 由于爆发过滤器功能用于隔离传入邮件，因此此功能在启用了 D 模式的设备上已禁用。因此，“爆发过滤器“一章中的信息不适用。

- SenderBase 网络参与功能 - 由于 SenderBase 网络参与会报告有关传入邮件的信息，因此该功能在启用了 D 模式的设备上已禁用。因此，有关 SenderBase 网络参与的信息不适用。
- 报告 - 报告有限。某些报告不可用，而且由于性能原因，确实执行的报告设置为在非常有限的级别运行。

注释 在“邮件安全监控概述”报告中针对启用了 D 模式的设备显示的总计可能错误地包括垃圾邮件和疑似垃圾邮件计数，即使这些功能在启用了 D 模式的设备上已禁用也是如此。

- 防数据丢失 - 对外发邮件的 DLP 扫描在启用了 D 模式的设备上已禁用。

适用于启用了 D 模式的设备的标准功能

表 *149:* 在启用了 *D* 模式的设备中包括的 *AsyncOS* 功能

特性	更多信息
防病毒扫描	请参阅 防病毒，第 253 页
域密钥签名	DKIM/域密钥是用于基于发件人使用的签名密钥验证邮件真实性的方法。请参阅 电邮验证，第 445 页
集中管理	请参阅 使用集群进行集中管理，第 907 页
传送限制	对于每个域，可以分配最大连接数和最大收件人数，使系统在指定时间段内不超过这些数量。这个“好邻居”表通过 destconfig 命令定义。 有关详细信息，请参阅使用目标控制来控制邮件传送，第 557 页。
退回验证	验证退回邮件的真实性。请参阅退回验证，第 558 页。
授权管理	请参阅 分配管理任务，第 723 页
跟踪（调试）	请参阅使用测试邮件调试邮件流：追踪，第 935 页。
VLAN, NIC 配对	请参阅 高级网络配置，第 841 页
可选防病毒引擎	可以添加可选的防病毒扫描来确保出站邮件的完整性。请参阅防病毒扫描概述，第 253 页。

设置设备以优化出站邮件传送

步骤 1 应用所提供的功能密钥。在运行系统设置向导之前（在配置设备之前），需要将该密钥应用到思科邮件安全设备。通过“系统管理”>“功能密钥”页面或通过在 CLI 中发出 featurekey 命令，应用密钥。

注释　前述功能密钥包括 30 天试用的 Sophos 或 McAfee 防病毒许可证，可供您用来测试对出站邮件的防病毒扫描。

步骤 2 重新启动设备。

步骤 3 运行系统设置向导（GUI 或 CLI）并配置设备。

请记住，针对出站传送进行了优化的设备不包括反垃圾邮件扫描或爆发过滤器功能。（请忽略这些章节。）

注释　在集群环境中，不能将通过 D 模式功能密钥配置的设备与未通过传送性能包配置的 AsyncOS 设备整合在一起。

配置节约资源的退回设置

为优化出站邮件传送配置了设备后，可以配置系统以检测潜在传送问题并退回发往某个目标的所有邮件。

注释　使用此设置将退回队列中发往被认为无法送达的目标域的所有邮件。传送问题得到解决后，需要重新发送邮件。

启用节约资源的退回设置示例

```
mail3.example.com> bounceconfig

Choose the operation you want to perform:

- NEW - Create a new profile.

- EDIT - Modify a profile.

- DELETE - Remove a profile.

- SETUP - Configure global bounce settings.

[]> setup

Do you want to bounce all enqueued messages bound for a domain if the host is down? [N]>

y
```

使用此功能时， 在连续 10 次尝试连接主机失败后 即将主机视为“关闭”。AsyncOS 每隔 15 分钟扫描一次关闭的主机， 因此在清除队列之前可能进行超过 10 次尝试。

使用 IronPort 邮件合并 (IPMM) 发送大量邮件

注释 IronPort 邮件合并仅适用于启用了 D 模式的设备。

IronPort 邮件合并概述

IronPort 邮件合并 (IPMM) 免去了从客户系统生成单独的个性化邮件的负担。它消除了生成数以千计的单独邮件的需求并在邮件生成系统和邮件网关之间传输它们，从而降低系统负载并提高的邮件传送吞吐量。

通过 IPMM，可使用表示在邮件中位置的变量（可予以替换以实现个性化）创建单个邮件正文。对于每个邮件收件人，只需将收件人邮件地址和变量替换传输到邮件网关。此外，IPMM 可用于发送某些收件人特定“部分”的邮件正文，同时从其他收件人中排除特定部分。（例如，假设需要在邮件末尾针对两个不同国家或地区的收件人包含不同的版权声明。）

邮件合并功能的优势

- 便于邮件管理员使用。消除了为每个收件人创建个性化邮件的复杂性，因为 IPMM 以许多常用语言提供变量替换和抽象界面。
- 减少了邮件生成系统的负载。通过要求一份邮件正文和一个所需替换的表，大多数邮件生成“工作”都可从邮件生成系统分载出去并移至为优化出站邮件传送进行了配置的设备。
- 增加传送吞吐量。通过减少接受和排队数以千计的传入邮件所需的资源，设备可以大大提高出站传送性能。
- 队列存储效率。通过减少为每个邮件收件人存储的信息，用户可以大大提高效率，更好地使用启用了 D 模式的设备上的队列存储。

使用邮件合并

SMTP 注入

IPMM 将 SMTP 作为传输协议进行扩展。无需对设备进行特殊配置。（默认情况下，可为启用了 D 模式的设备上的专用侦听程序启用 IPMM，并为公共侦听程序禁用 IPMM。）但是，如果当前未使用 SMTP 作为注入协议，则必须创建通过启用了 D 模式的设备的接口使用 SMTP 的新专用侦听程序。

使用 listenerconfig 的 setipmm 子命令在侦听程序上启用 IPMM。有关详细信息，请参阅 配置网关以接收邮件，第 61 页

IPMM 通过更改两个命令（MAIL FROM 和 DATA）并添加另一个命令 XDFN 来修改 SMTP。MAIL FROM 命令会替换为 XMRG FROM，并且 DATA 命令会替换为 XPRT。

要生成邮件合并邮件，用于生成邮件的命令需要按特定顺序发出。

1. 初始 EHLO 语句，用于确定发送主机。
2. 每封邮件都以 XMRG FROM: 语句开头，指示发件人地址。
3. 然后定义每个收件人：
4. 编写一个或多个 XDFN 变量分配语句，包括定义部分 (XDFN *PART=1,2,3…) 和任何其他收件人特定的变量。
5. 收件人邮件地址通过 RCPT TO: 语句定义。在 RCPT TO: 之前，但在以前的 XMRG FROM 或 RCPT TO 命令之后的任何变量分配都将映射到此收件人邮件地址。
6. 每个部分都使用 XPRT n 命令定义，并且每个部分以句点 (.) 符号终止，这类似于 DATA 命令。最后一部分通过 XPRT n LAST 命令定义。

变量替换

邮件正文的任何部分（包括邮件信头）可以包含用于替换的变量。变量也可能出现在 HTML 邮件中。变量是用户定义的，必须以和号 (&) 字符开始，并以分号 (;) 字符结束。以星号 (*) 开始的变量名称会被保留，不可使用。

保留的变量

IPMM 包含预定义的五个特殊“保留”变量。

表 *150: IPMM*：保留变量

*FROM	保留变量 *FROM 派生自“Envelope From”参数。“Envelope From”参数由“XMRG FROM:”命令设置。
*TO	保留变量 *TO 派生自信封收件人值，由“RCPT TO:”命令设置。
*PARTS	保留变量 *PARTS 保存一个以逗号分隔的部分列表。它在通过“RCPT TO:”定义收件人之前设置，可确定特定用户将收到哪些“XPRT n”邮件正文块。
*DATE	保留变量 *DATE 将替换为当前日期戳。
*DK	保留变量 *DK 用于指定 DomainKeys 签名配置文件（此配置文件必须已经存在于 AsyncOS 中）。有关创建 DomainKeys 签名配置文件的详细信息，请参阅 电邮验证，第 445 页

邮件示例 1

以下邮件正文（包括信头）示例包含四个完全不同的变量和五个替换位置，在最终邮件中会替换这些变量和位置。请注意，同一变量可在邮件正文中使用多次。此外，还使用了保留变量 &*TO;，该变量将替换为收件人邮件地址。此保留变量不需要作为单独变量传送。本例中的变量以粗体显示。

```
From: Mr.Spacely <spacely@example.com>

To: &first_name;&last_name;&*TO;


Subject: Thanks for Being an Example.Com Customer
```

```
Dear &first_name;,
Thank you for purchasing a &color; sprocket.
```

此邮件只需向设备注入一次。对于每个收件人，需要提供以下其他信息：

- 收件人邮件地址
- 用于变量替换名称-值对

部分组合

SMTP 对每个邮件正文使用一个 DATA 命令，而 IPMM 使用一个或多个 XPRT 命令来构建邮件。各个部分基于每个收件人指定的顺序进行组合。每个收件人可以接收任何或所有邮件部分。可按任意顺序组合各个部分。

特殊变量 *PARTS 保存一个以逗号分隔的部分列表。

例如，以下邮件示例包含两个部分。

第一部分包含邮件信头和一些邮件正文。第二部分包含可根据特定客户变化的优惠。

邮件示例 2，第 1 部分

```
From: Mr. Spacely <spacely@example.com>

To: &first_name; &last_name; &*TO;

Subject: Thanks for Being an Example.Com Customer

Dear &first_name;,

Thank you for purchasing a &color; sprocket.
```

邮件示例 2，第 2 部分

```
Please accept our offer for 10% off your next sprocket purchase.
```

这些邮件部分只需向设备注入一次。在此情况下，每个收件人都需要提供以下附加信息：

- 要包含在最终邮件中的部分排序列表
- 收件人邮件地址
- 用于变量替换名称值对

IPMM 和 DomainKeys 签名

IPMM 支持 DomainKeys 签名。使用 *DK 保留变量可指定 DomainKeys 配置文件。例如：

```
XDFN first_name="Jane" last_name="User" color="red" *PARTS=1,2 *DK=mass_mailing_1
```

在本例中，“mail_mailing_1”是以前配置的 DomainKeys 配置文件的名称。

命令说明

当客户端将 IPMM 邮件注入侦听程序时，它通过以下关键命令使用扩展的 SMTP。

XMRG FROM

语法：

```
XMRG FROM: <sender email address>
```

此命令替换 SMTP MAIL FROM: 命令并指明下面是 IPMM 邮件。IPMM 作业通过 XMRG FROM: 命令启动。

XDFN

语法：

```
XDFN <KEY=VALUE> [KEY=VALUE]
```

XDFN 命令可设置每个收件人的元数据。请注意，可以选择将密钥-值对包含在尖括号或方括号中。

*PARTS 是一个特殊保留变量，用于指示 XPRT 命令定义的索引编号（如下所述）。*PARTS 变量分割为以逗号分隔的整数列表。整数对应于按照 XPRT 命令所定义要发送的正文部分。其他保留变量有：*FROM、*TO 和 *DATE。

XPRT

语法：

```
XPRT index_number LAST

Message

.
```

XPRT 命令会替换 SMTP DATA 命令。该命令接受在发出该命令后传输邮件部分。该命令完成后会在一个行中显示一个句点，后面是返回结果（这与 SMTP DATA 命令的完成方式相同）。

特殊关键字 **LAST** 指示邮件合并作业结束，并且必须用于指定要注入的最后一部分。

在使用 LAST 关键字后，邮件会进行排队，然后开始传送。

有关定义变量的说明

- 在使用 XDFN 命令定义变量时，请注意，实际命令行大小不能超过系统的物理限制。如果使用启用了 D 模式的设备，则该限制为每行 4 KB。其他主机系统可能具有更低的阈值。在非常大的行中定义多个变量时，请务必小心。
- 在定义变量键-值对时，可以使用正斜杠“/”来转义特殊字符。这在邮件正文包含可能错误替换为变量定义的 HTML 字符实体时非常有用。（例如，字符实体 ™ 定义商标字符的 HTML 字符实体。如果创建了命令 XDFN trade=foo，然后创建包含 HTML 字符实体“™”的 IPMM 邮件，则组合后的邮件将包含变量替换 (“foo”) 而不是商标字符。此概念还适用于和号字符“&”，有时会在包含 GET 命令的 URL 中使用该字符。

IPMM 会话示例

以下是邮件示例 2 的 IPMM 会话示例（如上所示）。邮件将发送到本示例中的两个收件人：“Jane User”和“Joe User”。

在本示例中，**bold** 中键入的内容表示要在与启用了 D 模式的设备进行的手动 SMTP 会话中键入的内容，在 monospaced type 中键入的内容表示 SMTP 服务器的响应，而斜体键入内容表示注释或变量。

已建立连接:

```
220 ESMTP


EHLO foo


250 - ehlo responses from the listener enabled for IPMM
```

会话已开始：

```
XMRG FROM:<user@domain.com> [Note: This replaces the MAIL FROM: SMTP command.]

250 OK
```

为每个收件人设置了变量和部分：

```
XDFN first_name="Jane" last_name="User" color="red" *PARTS=1,2

[Note: This line defines three variables (first_name, last_name, and color) and then
uses the *PARTS reserved variable to define that the next recipient defined will receive
message parts numbers 1 and 2.]

250 OK

RCPT TO:<jane@company.com>

250 recipient <jane@company.com> ok

XDFN first_name="Joe" last_name="User" color="black" *PARTS=1

[Note: This line defines three variables (first_name, last_name, and color) and then
uses the *PARTS reserved variable to define that the next recipient defined will receive
message parts numbers 1 only.]

RCPT TO:<joe@company1.com>

250 recipient <joe@company1.com> ok
```

Next, part 1 is transmitted:

```
XPRT 1 [Note: This replaces the DATA SMTP command.]

354 OK, send part

From: Mr. Spacely <spacely@example.com>

To: &first_name; &last_name; &*TO;

Subject: Thanks for Being an Example.Com Customer

&*DATE;
```

```
Dear &first_name;,

Thank you for purchasing a &color; sprocket.

.
```

然后，第 2 部分终止。请注意，LAST 关键字用于将第 2 部分识别为最后一个要组合的部分：

```
XPRT 2 LAST

Please accept our offer for 10% off your next sprocket purchase.

.

250 Ok, mailmerge message enqueued
```

“250 Ok, mailmerge message queued”说明该邮件已被接受。

根据本示例，收件人 Jane User 将收到以下邮件：

```
From: Mr. Spacely <spacely@example.com>

To: Jane User <jane@company.com>

Subject: Thanks for Being an Example.Com Customer

message date

Dear Jane,

Thank you for purchasing a red sprocket.

Please accept our offer for 10% off your next sprocket purchase.
```

收件人 Joe User 将收到以下邮件：

```
From: Mr. Spacely <spacely@example.com>

To: Joe User <joe@company1.com>

Subject: Thanks for Being an Example.Com Customer

message date

Dear Joe,

Thank you for purchasing a black sprocket.
```

代码示例

思科使用常用编程语言创建了库，以抽象化将 IPMM 邮件注入为 IPMM 启用的设备侦听程序的任务。请联系思科客户支持，获取有关如何使用 IPMM 库的示例。对该代码进行了广泛的注释，以解释其语法。

第 44 章

在思科内容（M 系列）安全管理设备上集中管理服务

本章包含以下部分：

思科内容安全管理设备服务概述

思科内容安全管理设备（M 系列设备）是外部或“机下”位置，为多个邮件安全设备上的某些服务提供单一界面。

安全管理设备附带以下功能：

- 外部垃圾邮件隔离区。为最终用户暂存垃圾邮件和可疑垃圾邮件，并允许用户和管理员在做出最终决定前审核标记为垃圾邮件的邮件。
- 集中策略、病毒和爆发隔离区。在防火墙后提供单一位置，用来存储和管理防病毒扫描、爆发过滤器和策略隔离的邮件。
- 集中报告。运行关于来自多个邮件安全设备的汇聚数据的报告。
- 集中跟踪。跟踪经过多个邮件安全设备的邮件。

有关配置和使用思科内容安全管理设备的完整信息，请参阅《思科内容安全管理设备用户指南》。

注意 如果您在邮件安全设备上启用了双因素身份验证，则可以使用预共享密钥将其添加到安全管理设备。使用 CLI 中的 `smaconfig > add` 命令配置此设置。

或

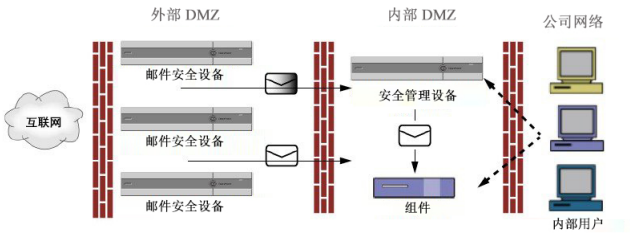
在将邮件安全设备添加到安全管理设备之前，请在邮件安全设备上禁用双因素身份验证。有关详细信息，请参阅禁用双因素身份验证，第 740 页。

网络规划

思科内容安全管理设备可以让您将最终用户界面（例如，邮件应用）与驻留在您的各种 DMZ 上的更加安全的网关系统分隔开来。使用两层防火墙可灵活地进行网络规划，这样最终用户就不用直接连接到外部 DMZ 了。

下图显示纳入安全管理设备和多个 DMZ 的典型网络配置。

图 *86:* 利用思科内容安全管理设备的典型网络配置



大型企业数据中心可以分享一个安全管理设备，将其用作一个或多个邮件安全设备的外部垃圾邮件隔离区。与此同时，远程办公室可以在邮件安全设备上维护本地垃圾邮件隔离区，以供本地使用。

使用外部垃圾邮件隔离区

邮件流和外部垃圾邮件隔离区

如果您的网络配置方式与网络规划，第 970 页中所述的方式相同，则外部 DMZ 中的设备会收到来自互联网的传入邮件。正常邮件会直接发送到内部 DMZ 中的邮件传输代理 (MTA)（组件），最终发送给企业网络内的最终用户。

垃圾邮件和可疑垃圾邮件（取决于邮件流策略设置）发送到安全管理设备上的垃圾邮件隔离区。然后，最终用户访问该隔离区，选择删除垃圾邮件并放行其认为应传送给他们的邮件。垃圾邮件隔离区中剩余的邮件经过一段时间（可配置）后将自动删除。

从安全管理设备的外部隔离区放行的邮件将返回到原始邮件安全设备以便传送。在传送前，这些邮件通常不通过以下进程：HAT 和其他策略或扫描设置、RAT、域例外、别名、传入过滤器、伪装、退回验证和工作队列。

邮件安全设备配置为向安全管理设备发送邮件，将自动期望接收从安全管理设备放行的邮件，并且在重新接收这些邮件时不重新处理。为此，安全管理设备的 IP 地址必须更改。如果安全管理设备的 IP 地址发生改变，接收邮件安全设备将像处理任何其他传入邮件一样处理该邮件。应在安全管理设备上始终使用相同的 IP 地址进行接收和传送。

安全管理设备接受来自在垃圾邮件隔离区设置中指定的 IP 地址的邮件以进行隔离。要在安全管理设备上配置垃圾邮件隔离区，请参阅《思科内容安全管理设备用户指南》。

安全管理设备放行的邮件传送到在垃圾邮件隔离区设置中定义的主要主机和辅助主机（内容安全设备或其他组件主机）（请参阅《思科内容安全管理设备用户指南》）。因此，无论向安全管理设备传送邮件的邮件安全设备的数量如何，所有放行的邮件、通知和警报都将发送到一台主机（组件或内容安全设备）。请注意，不要让负责传送来自安全管理设备的邮件的主要主机负担过重。

从本地垃圾邮件隔离区迁移到外部隔离区

如果您当前正在使用本地垃圾邮件隔离区或邮件安全设备，但是想要迁移到安全管理设备上托管的外部垃圾邮件隔离区（同时保留对本地隔离区中邮件的访问权限），则在过渡期间，您应阻止新邮件进入本地隔离区。

请考虑下列可能的策略：

- 配置反垃圾邮件设置 - 在邮件策略中配置反垃圾邮件设置，将安全管理设备指定为备用主机。此操作会将新垃圾邮件发送到外部隔离区，但仍允许访问本地隔离区。
- 设置更短的过期时间 - 将本地隔离区中的“保留天数 (之后自动删除)”(Schedule Delete After) 设置配置为更短的期限。
- 删除所有剩余的邮件 - 要删除本地隔离区中的所有剩余邮件，请禁用隔离区，然后点击本地隔离区页面中的“全部删除”(Delete All) 链接（请参阅删除垃圾邮件隔离区中的邮件，第 720 页）。只有还含有邮件的本地垃圾邮件隔离区被禁用，此链接才可用。

现在，您可以启用外部隔离区并禁用本地隔离区。

注释 如果本地隔离区和外部隔离区均启用，则使用本地隔离区。

启用外部垃圾邮件隔离区和外部安全列表/阻止列表

您只能在邮件安全设备上启用一个外部垃圾邮件隔离区。

准备工作

- 审查邮件流和外部垃圾邮件隔离区，第 970 页中的信息。
- 查看从本地垃圾邮件隔离区迁移到外部隔离区，第 971 页中的信息，并基于此采取操作。
- 将安全管理设备配置为支持集中垃圾邮件隔离区和安全列表/阻止列表功能。请参阅安全管理设备文档。
- 如果之前已为邮件安全设备配置了其他外部垃圾邮件隔离区，请先禁用该外部垃圾邮件隔离区设置。

在每个邮件安全设备上完成以下程序。

步骤 1 依次选择**安全服务 (Security Services) > 集中服务 (Centralized Services) > 垃圾邮件隔离区 (Spam Quarantine)**。

步骤 2 点击**配置**。

步骤 3 选择**启用外部垃圾邮件隔离区 (Enable External Spam Quarantine)**。

步骤 4 在“名称”(Name) 字段中，输入安全管理设备的名称。

名称不是很重要，仅供参考。例如，输入安全管理设备的主机名。

步骤 5 输入 IP 地址和端口号。

它们必须匹配“垃圾邮件隔离区设置”(Spam Quarantines Settings) 页面中在安全管理设备上指定的 IP 地址和端口号（**管理设备 [Management Appliance] > 集中服务 [Centralized Services] > 垃圾邮件隔离区 [Spam Quarantine]**。）

步骤 6 （可选）选中该复选框以启用**外部安全列表/阻止列表 (External Safelist/Blocklist)** 功能，并指定适当的阻止列表操作。

步骤 7 提交并确认更改。

步骤 8 对每个邮件安全设备重复此程序。

禁用本地垃圾邮件隔离区以激活外部隔离区

如果在启用外部垃圾邮件隔离区之前使用的是本地垃圾邮件隔离区，则必须禁用本地隔离区，才能将邮件发送到外部隔离区。

准备工作

执行启用外部垃圾邮件隔离区和外部安全列表/阻止列表，第 971 页中的所有指导，包括“准备工作”部分的信息。

步骤 1 选择**监控 (Monitor) > 垃圾邮件隔离区 (Spam Quarantine)**。

步骤 2 在“垃圾邮件隔离区”(Spam Quarantine) 部分，点击**垃圾邮件隔离区 (Spam Quarantine)** 链接。

步骤 3 取消选择**启用垃圾邮件隔离区 (Enable Spam Quarantine)**。

忽略所有由于此更改导致的调整邮件策略警告。如果已配置外部隔离区设置，邮件策略则自动将邮件发送到外部垃圾邮件隔离区。

步骤 4 提交并确认更改。

外部垃圾邮件隔离区故障排除

邮件安全设备重新处理从外部隔离区释放的邮件

问题：邮件安全管理设备不必重新处理从安全管理设备释放的邮件。

解决方案：如果安全管理设备的IP地址发生改变，则会发生这种情况。请参阅邮件流和外部垃圾邮件隔离区，第 970 页。

关于集中策略、病毒和病毒爆发隔离区

集中化的策略、病毒和病毒爆发隔离区

您可以在安全管理设备上集中策略、病毒和爆发隔离区。邮件由邮件安全设备处理，但存储在安全管理设备上的隔离区中。

集中策略、病毒和爆发隔离区提供以下优势：

- 管理员可以集中于一处来管理多个邮件安全设备的被隔离邮件。
- 隔离的邮件存储在防火墙后，而不是 DMZ 中，从而降低安全风险。
- 集中隔离区可使用安全管理设备上的标准备份功能进行备份。

有关完整信息，请参阅安全管理设备的用户指南或联机帮助。

集中策略、病毒和爆发隔离区的限制和局限性

- 在每个邮件安全设备上，所有策略、病毒和爆发隔离区都必须集中管理，或必须存储在本地。
- 因为在安全管理设备中未提供扫描引擎，您无法手动测试策略、病毒或爆发隔离区中的邮件是否含有病毒。

在集群配置中集中策略、病毒和病毒爆发隔离区的要求

可以在集群设备的任何级别启用集中策略、病毒和爆发隔离区。

要求：

- 在特定级别（计算机、组或集群）在邮件安全设备上启用集中策略、病毒和爆发隔离区之前，属于同一级别的所有设备都必须先添加到安全管理设备。
- 内容和邮件过滤器及DLP邮件操作必须在同一级别配置，且它们在低于该级别的任何级别不会被覆盖。
- 集中策略、病毒和爆发隔离区设置必须在同一级别配置，且它们在低于所配置级别的任何级别不会被覆盖。
- 确保要用于与安全管理设备进行通信的接口在组或集群中的所有设备上拥有相同的名称。

例如：

如果要在集群或组级别启用集中策略、病毒和爆发隔离区，但连接到集群的邮件安全设备的这些设置是在计算机级别定义的，则您必须删除在计算机级别配置的集中隔离区设置，才能在集群或组级别启用此功能。

关于策略、病毒和爆发隔离区的迁移

当您集中策略、病毒和爆发隔离区时，邮件安全设备上的现有策略、病毒和爆发隔离区将迁移到安全管理设备。

您将在安全管理设备上配置迁移，但是当您确认更改，在邮件安全设备上启用集中策略、病毒和爆发隔离区时，会发生迁移。

在确认更改时，将会出现以下情况：

- 禁用邮件安全设备上的本地策略、病毒和爆发隔离区。所有进入这些隔离区的新邮件都将在安全管理设备上隔离起来。
- 从现有非垃圾邮件隔离区向安全管理设备的迁移开始。
- 删除所有本地策略、病毒和爆发隔离区。如果您配置的是自定义迁移，则选择不迁移的任何本地策略隔离区也会被删除。有关删除策略隔离区的影响，请参阅关于删除策略隔离区，第 690 页。
- 迁移前位于多个隔离区中的邮件，在迁移后将位于对应的集中隔离区。
- 迁移在后台进行。所需的时间取决于隔离区大小和网络。当您在邮件安全设备上启用集中隔离区时，您可以输入一个或多个邮件地址，以便在迁移完成时接收通知。
- 这些邮件将应用集中隔离区中的设置，而不是始发本地隔离区的设置。但是，每封邮件仍沿用初始到期时间。

注释 迁移期间自动创建的所有集中隔离区均采用默认隔离区设置。

集中策略、病毒和爆发隔离区

开始之前

注释 请在维护窗口或非高峰时段执行此过程。

- 您必须先为集中策略、病毒和爆发隔离区配置安全管理设备。请参阅安全管理设备联机帮助或用户指南中“集中策略、病毒和爆发隔离区”一章的“集中策略、病毒和爆发隔离区”部分的表格。
- 如果安全管理设备上分配给集中隔离区的空间比现有本地隔离区占用的总空间小，邮件将根据安全管理设备上的隔离区设置提前到期。在迁移之前，请考虑手动执行操作以减小隔离区空间。有关提前到期的详细信息，请参阅自动处理的隔离邮件的默认操作，第 688 页。
- 如果您已选择自动迁移，或者将自定义迁移配置为在迁移过程中创建集中隔离区，请注意邮件安全设备上的当前隔离区设置，以便将这些设置用作集中隔离区配置准则。
- 如果在集群配置中部署了邮件安全设备，请参阅在集群配置中集中策略、病毒和病毒爆发隔离区的要求，第 973 页。

- 注意在此程序中确认更改时将发生的变化。请参阅关于策略、病毒和爆发隔离区的迁移，第 974 页。

步骤 1 依次选择**安全服务 (Security Services) > 集中服务 (Centralized Services) > 策略、病毒和爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**。

步骤 2 点击**启用 (Enable)**。

步骤 3 输入要用于与安全管理设备通信的接口和端口。

确保可从安全管理设备访问接口和端口。

如果邮件安全设备加入集群，则选择的接口必须在集群中的所有计算机上都可用。

步骤 4 要在迁移完成时收到通知，请输入一个或多个邮件地址。

步骤 5 验证要迁移的隔离区的相关信息，确保这是您所需的内容。

步骤 6 如果要执行自定义迁移，请注意在确认此过程中的更改时将删除任何隔离区。

步骤 7 确认有关内容和邮件过滤器及 DLP 邮件操作的信息将按预期方式更新。

注释 对于集群配置，只有在特定级别已定义过滤器和邮件操作，且它们在低于该级别的任何级别上不会被覆盖，系统才会在该级别自动更新过滤器和邮件操作。迁移后，可能需要使用集中隔离区名称手动重新配置过滤器和邮件操作。

步骤 8 如果需要重新配置迁移映射，请执行以下操作：

a) 返回安全管理设备。

b) 重新配置迁移映射。

在管理设备上，选择要重新映射的隔离区，然后点击**从集中隔离区中删除 (Remove from Centralized Quarantine)**。然后，可以重新映射隔离区。

c) 在安全管理设备上提交新迁移配置。

d) 从开始执行此程序。

重要提示！请务必重新依次加载**安全服务 (Security Services) > 集中服务 (Centralized Services) > 策略、病毒和爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**。

步骤 9 点击 **Submit**。

步骤 10 如果需要重新配置迁移映射，请按照步骤 8 中的过程执行操作。

步骤 11 确认您的更改。

注释 在迁移进行时，避免在邮件安全设备或安全管理设备上进行配置更改。

步骤 12 查看页面顶部可监控迁移状态；如果在配置迁移时输入了邮件地址，请等待邮件通知您迁移完成。

下一步做什么

执行安全管理设备联机帮助或用户指南中“集中策略、病毒和爆发隔离区”主题的表格中所述的剩余任务。

相关主题

- 可访问策略、病毒和爆发隔离区的用户组 ， 第 693 页

关于禁用集中策略、病毒和爆发隔离区

当您在邮件安全设备上禁用集中策略、病毒和爆发隔离区时：

- 邮件安全设备上的本地隔离区会自动启用。
- 系统创建的隔离区以及邮件过滤器、内容过滤器和 DLP 邮件操作所引用的隔离区会在邮件安全设备上自动创建。病毒、爆发和未分类隔离区使用集中隔离区之前使用的设置创建，包括分配的用户角色。所有其他隔离区均采用默认设置创建。
- 新隔离的邮件将立即转到本地隔离区。
- 禁用集中隔离区时其中包含的邮件将保留在原处，直到出现以下情况之一：
  - 手动删除邮件或邮件到期自动删除。
  - 手动释放邮件，或自动释放邮件，前提是同时满足下列条件之一：

* 在安全管理设备上配置了备用释放设备。请参阅安全管理设备的联机帮助或文档。

* 集中隔离区在邮件安全设备上再次启用。

禁用集中策略、病毒和爆发隔离区

开始之前

- 了解禁用集中策略、病毒和爆发隔离区的影响。
- 执行以下操作之一：
  - 处理集中策略、病毒和爆发隔离区中当前的所有邮件。
  - 确保已指定备用放行设备，用来在禁用集中隔离区后处理从集中隔离区放行的邮件。有关信息，请参阅安全管理设备联机帮助或用户指南。

步骤 1 在邮件安全设备上，依次选择**安全服务 (Security Services) > 集中服务 (Centralized Services) > 策略、病毒和爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**。

步骤 2 禁用集中策略、病毒和爆发隔离区。

步骤 3 提交并确认更改。

步骤 4 自定义新创建的本地隔离区的设置。

集中策略、病毒和病毒爆发隔离区故障排除

如果思科内容安全管理设备停止工作

如果在停止工作的安全管理设备上集中策略、病毒和爆发隔离区，应在邮件安全设备上禁用这些集中隔离区。

如果部署替代安全管理设备，则必须在安全管理设备和每个邮件安全设备上重新配置隔离区迁移。请参阅安全管理设备联机帮助或用户指南中“集中策略、病毒和爆发隔离区”一章的“集中策略、病毒和爆发隔离区”部分的表格。

配置集中报告

开始之前

- 在安全管理设备上启用和配置集中报告。请参阅《思科内容安全管理设备用户指南》中的先决条件和说明。
- 确保在安全管理设备上为报告服务分配了充足的磁盘空间。

步骤 1 依次点击**安全服务 (Security Services) > 报告 (Reporting)**。

步骤 2 在“报告服务”(Reporting Service) 部分，选择“集中报告”(Centralized Reporting) 选项。

步骤 3 提交并确认更改。

高级恶意软件保护报告的要求

有关安全管理设备上高级恶意软件防护（文件信誉和文件分析）功能的完整报告的所需配置，请参阅您的安全管理设备软件版本的联机帮助或用户指南的邮件报告章节中有关高级恶意软件防护报告的信息。

更改集中报告后报告信息的可用性

在邮件安全设备上启用集中报告时：

- 邮件安全设备上用于每月报告的现有数据不会传输到安全管理设备。
- 邮件安全设备上的存档报告不可用。
- 邮件安全设备仅存储一周的数据。
- 每月和每年报告的新数据存储在安全管理设备上。
- 邮件安全设备上的排定报告暂停。
- 您再也无法在邮件安全设备上访问排定报告配置页面。

关于禁用集中报告

如果在邮件安全设备上禁用集中报告，则邮件安全设备会开始存储新的每月报告数据，计划报告恢复，并且您可以访问它的存档报告。禁用集中报告后，设备仅显示过去一小时和一天的数据，但不

是过去一周或一个月。这种情况是暂时的。在累积足够的数据后，设备将显示过去一周和一个月的报告。如果邮件安全设备重新回到集中报告模式，它将在交互式报告中显示上一周的数据。

配置集中邮件跟踪

开始之前

注释　您不能在邮件安全设备上启用集中和本地跟踪。

步骤 1 依次点击**安全服务 (Security Services) > 邮件跟踪 (Message Tracking)**。

步骤 2 在“邮件跟踪服务”(Message Tracking Service) 部分，点击**编辑设置 (Edit Settings)**。

步骤 3 选中**启用邮件跟踪服务 (Enable Message Tracking Service)** 复选框。

步骤 4 选择“集中跟踪”(Centralized Tracking) 选项。

步骤 5 （可选）选中该复选框可保存被拒绝连接的信息。

注释　保存被拒绝连接的跟踪信息，会对安全管理设备的性能造成负面影响。

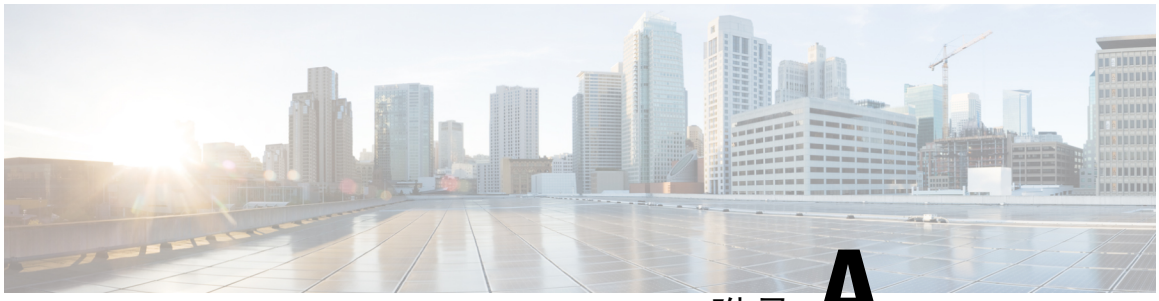
步骤 6 提交并确认更改。

后续操作

要使用集中跟踪，您必须在邮件安全设备和安全管理设备上启用该功能。要在安全管理设备上启用集中跟踪，请参阅《思科内容安全管理设备用户指南》。

使用集中服务

有关使用集中服务的说明，请参阅《思科内容安全管理设备用户指南》。



附录 A

FTP、SSH 和 SCP 访问

本附录包含以下部分：

IP接口

IP 接口包含到网络的各个连接所需要的网络配置数据。可以为一个物理以太网接口配置多个 IP 接口。您可以向 IP 接口分配互联网协议第 4 版 (IPv4) 和/或第 6 版 (IPv6)。

表 *151:* 在接口上默认启用的服务

		是否默认为启用？	
服务	默认端口	管理接口 设备上的 Data1 接口的默认设置。[2]	创建的新接口
FTP	21	否	否
SSH	22	是	否
HTTP	80	是	否
HTTPS	443	是	否

2

- 如果您需要通过图形用户界面 (GUI) 访问设备，则必须在接口上启用 HTTP 和/或 HTTPS。
- 如果需要访问设备来上传或下载配置文件，则必须在接口上启用 FTP。
- 您也可以使用安全复制 (scp) 来上传或下载文件。

您可以通过 IP 接口配置对垃圾邮件隔离区的 HTTP 或 HTTPS 访问。

对于邮件传输和虚拟网关，每个 IP 接口都可作为一个具有特定 IP 地址和主机名的虚拟网关地址。也可以将接口“连接”到不同组中（通过 CLI），系统在传输邮件时将遍历这些组。

连接或组合虚拟网关，对于在多个接口之间均衡大型邮件活动的负载非常有用。还可以创建VLAN，并像配置任何其他接口（通过 CLI）一样配置它们。有关详细信息，请参阅 高级网络配置 ， 第 841 页

AsyncOS 如何选择默认IP接口

AsyncOS 根据 IP 接口在**网络 > IP 接口**页下或在 `ifconfig` CLI 命令中的显示最低的 IP 地址选择默认 IP 接口。使用列表中驻留在所述子网上的第一个 IP 接口。

如果同一子网中有多个 IP 地址被配置为默认网关，则使用编号最小的 IP 地址。例如，如果在同一子网中配置了以下 IP 地址，

- `10.10.10.2/24`
- `10.10.10.30/24`
- `10.10.10.100/24`
- `10.10.10.105/24`

AsyncOS 将选择 `10.10.10.2/24` 作为默认 IP 接口。

配置对邮件安全设备的 FTP 访问

步骤 1 使用**网络 > IP 接口**页面或 `interfaceconfig` 命令为接口启用 FTP 访问。

危险 通过 `interfaceconfig` 命令禁用服务，可以断开与CLI的连接，具体取决于与设备的连接方式。如果无法使用其他协议、串行接口或管理端口上的默认设置重新连接到设备，请勿使用此命令禁用服务。

步骤 2 提交并确认更改。

步骤 3 通过 FTP 访问接口。确保为该接口使用的 IP 地址正确。例如：

```
$ ftp 192.168.42.42
```

注释 许多浏览器还允许通过 FTP 访问接口。

步骤 4 浏览到尝试完成的特定任务所在的目录。通过 FTP 访问接口后，可以浏览以下目录以复制和添加（“GET”和“PUT”）文件。请参阅下表。

FTP、SSH 和 SCP 访问

Directory Name	说明
/configuration	以下命令中的数据导出到和/或从中导入（保存）的目录： • 虚拟网关映射 (`altsrchost`) • XML 格式的配置数据 (`saveconfig`, `loadconfig`) • 主机访问表 (HAT) (`hostaccess`) • 收件人访问表 (RAT) (`rcptaccess`) • SMTP 路由条目 (`smtproutes`) • 别名表 (`aliasconfig`) • 伪装表 (`masquerade`) • 邮件**过滤器** (`filters`) • 全局取消订用数据 (`unsubscribe`) • `trace` 命令的测试邮件 • 通过以下格式保存的安全列表/阻止列表备份文件：*slbl<timestamp><serial number>.csv*
/antivirus	保存防病毒引擎日志文件的目录。您可以查看此目录中的日志文件，手动查找上次成功下载的病毒定义文件 (`scan.dat`)。

Directory Name	说明
/configuration /system_logs /cli_logs /status /reportd_logs reportqueryd_logs /ftpd_logs /mail_logs /asarchive /bounces /error_logs /avarchive /gui_logs /sntpd_logs /RAID.output /euq_logs /scanning /antispam /antivirus /euqgui_logs /ipmitool.output	通过 `logconfig` 和 `rollovernow` 命令为**日志记录**自动创建。有关每个日志的详细说明，请参阅日志记录，第 855 页。 有关各个日志文件类型之间的差异，请参阅“日志文件类型比较”。

步骤 5 使用 FTP 程序从相应目录上传和下载文件。

安全复制 (scp) 访问权限

如果您的客户端操作系统支持安全复制 (`scp`) 命令，则您可以将文件复制到上表列出的目录中，或者从这些目录复制文件。例如，在以下示例中，文件 `/tmp/test.txt` 会从客户机复制到主机名为 `mail3.example.com` 的设备的配置目录中。

请注意，该命令会提示输入用户 (admin) 的密码。此示例仅用于参考；特定操作系统的安全复制实施可能有所不同。

```
% scp /tmp/test.txt admin@mail3.example.com:configuration

The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.
```

```
DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.

Are you sure you want to continue connecting (yes/no)? yes


Warning: Permanently added 'mail3.example.com ' (DSA) to the list of known hosts.

admin@mail3.example.com's passphrase: (type the passphrase)

test.txt 100% |***************************| 1007 00:00

%
```

在本例中，从设备复制了相同文件到客户机：

```
% scp admin@mail3.example.com:configuration/text.txt .

admin@mail3.example.com's passphrase: (type the passphrase)

test.txt 100% |***************************| 1007 00:00

%
```

您可以使用安全复制 (scp) 来代替 FTP 将文件传输到思科设备或从该设备进行传输。

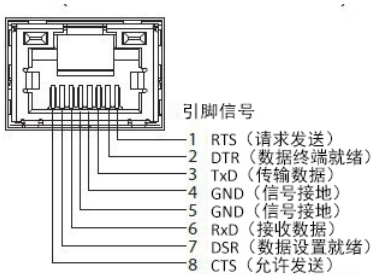
注释 只有操作员或管理员组的用户可以使用安全复制 (scp) 访问设备。有关详细信息，请参阅添加用户，第 726 页。

通过串行连接访问邮件安全设备

如果通过串行连接连接至设备，请针对控制台端口使用以下信息。

有关此端口的完整信息，请参阅设备的硬件安装指南。

80 和 90 系列硬件的串行端口引脚详细信息



70 系列硬件的串行端口引脚详细信息

下图展示串行端口连接器的引脚编号，下表定义串行端口连接器的引脚分配情况和接口信号。

FTP、SSH 和 SCP 访问

图 *87:* 串行端口的引脚编号

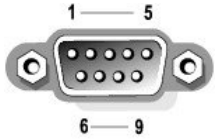
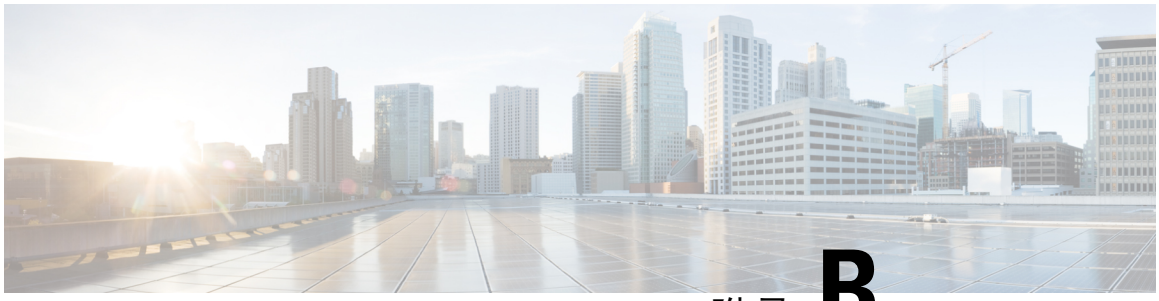


表 *152:* 串行端口引脚分配

引脚	信号	DTE	定义
1	DCD		数据载体检测
2	新加坡		串行输入
3	SOUT		串行输出
4	DTR		数据终端就绪
5	接地线	n/a	信号接地
6	DSR		数据设置就绪
7	RTS		请求发送
8	CTS		允许发送
9	RI		振铃指示器
外壳	n/a	n/a	机箱接地线



附录 B

分配网络和 IP 地址

本附录包含以下部分：

以太网接口

思科内容安全设备在系统的后面板上最多提供四个以太网接口，具体取决于配置（您是否具有可选的光纤网络接口）。它们的标签为：

- 管理
- Data1
- Data2
- Data3
- Data4

选择 IP 地址和网络掩码

当您配置网络时，内容安全设备必须能够选择一个唯一的接口来发送传出的数据包。此要求促使针对以太网接口的 IP 地址和网络掩码做出一些决策。此规则是指一个网络上只能有一个接口（通过将网络掩码应用到接口的 IP 地址来确定）。

IP 地址标识任何给定网络中的物理接口。一个物理以太网接口可以有多个 IP 地址，用来接受数据包。包含多个 IP 地址的以太网接口可以通过该接口发送数据包，以其任一 IP 地址作为数据包中的源地址。实施虚拟网关技术时需使用此属性。

网络掩码的作用是将 IP 地址划分为网络地址和主机地址。网络地址可视为 IP 地址的网络部分（位数与网络掩码匹配）。主机地址是 IP 地址的剩余数位。由 4 个 8 位二进制数构成的地址中的有效位数有时以无类域间路由 (CIDR) 方式表示，短划线后面跟随位数 (1-32)。

网络掩码可以这种方式表示，只统计二进制中的位数，因此 255.255.255.0 将变成“/24”，而 255.255.240.0 将变成“/20”。

接口配置示例

此部分显示了基于某些典型网络的接口配置示例。此示例使用两个名为 Int1 和 Int2 的接口。对于内容安全设备，这些接口名称可以表示三个接口中的任何两个接口（管理 [Management]、数据 1 [Data1]、数据 2 [Data2]）。

网络 1：

独立接口必须出现在独立网络中。

接口	IP 地址	Netmask	网络地址
Int1	192.168.1.10	255.255.255.0	192.168.1.0/24
Int2	192.168.0.10	255.255.255.0	192.168.0.0/24

发往 192.168.1.X 的数据在 Int1 传出（X 是 1 到 255 中除了您自己的地址外的任何数字，此例中为 10）。发往 192.168.0.X 的任何数据在 Int2 传出。发往不是采用这些格式的某个其他地址的任何数据包（最有可能是通过广域网或互联网传出）会发送到默认网关，默认网关必须在上述其中一个网络上。然后，默认网关会继续转发数据包。

网络 2：

两个不同接口的网络地址（IP 地址的网络部分）不能相同。

以太网接口	IP 地址	Netmask	网络地址
Int1	192.168.1.10	255.255.0.0	192.168.0.0/16
Int2	192.168.0.10	255.255.0.0	192.168.0.0/16

这种情况会出现冲突，因为两个不同的太网接口的网络地址相同。如果来自内容安全设备的数据包发送到 192.168.1.11，则无法决定应将哪个以太网接口用于传送数据包。如果两个以太网接口连接到两个单独的物理网络，该数据包可能会传送到错误的网络，并且永远找不到其目的地。内容安全设备不允许您在发生冲突的情况下配置网络。

您可以将两个以太网接口连接到同一个物理网络，但是，您必须精心构建 IP 地址和网络掩码，以使内容安全设备可以选择唯一的传送接口。

IP 地址、接口和路由

如果您选择某个接口，以便在 GUI 或 CLI 中通过该接口执行使您可以选择某个接口的命令或功能（例如升级 AsyncOS 或配置 DNS），则路由（默认网关）优先于所选的接口。

例如，假设您具有已配置三个网络接口的内容安全设备，每个接口在不同的网段上（假定全部为 /24）：

以太网	IP
管理	192.19.0.100
Data1	192.19.1.100
Data2	192.19.2.100

并且您的默认网关是 192.19.0.1。

现在，如果您执行 AsyncOS 升级（或者使您可以选择某个接口的其他命令或功能），并选择 Data1 的 IP (192.19.1.100)，则可以预期所有 TCP 流量将通过 Data1 以太网接口传送。但是，流量不会从设置为默认网关的接口（在此例中为管理接口）传出，而是从 Data1 上标有 IP 源地址的接口传出。

Summary

内容安全设备必须始终能够识别可传送数据包的唯一接口。为了做出此决策，内容安全设备组合使用数据包目标 IP 地址与其以太网接口的网络和 IP 地址设置。下表概括总结了之前的例子：

	相同网络	不同网络
相同物理接口	允许	允许
不同物理接口	不允许	允许

用于连接内容安全设备的策略

请在连接设备时注意以下事项：

- 与邮件流量相比，管理流量（CLI、网络界面、日志传送）通常很少。
- 如果将两个以太网接口连接到同一台网络交换机，但最后却与另一台下游主机上的接口进行通信，或者连接到将所有数据回响到所有端口的网络集线器，那么使用两个接口并不会带来任何优势。
- 通过在 1000Base-T 模式下工作的接口进行的 SMTP 转换略快于通过在 100Base-T 模式下工作的同一接口进行的转换，但只有在理想的情况下才如此。
- 如果传输网络的其他部分存在瓶颈，则无法优化网络连接。与互联网或连接提供商的上游设备进行连接时，最常发生瓶颈。

您选择连接的接口数量以及处理接口的方式应取决于基础网络的复杂程度。如果网络拓扑或数据量不作要求，则不必要连接到多个接口。另外，可以在起初熟悉网关时保持简单连接，然后随着数据量和网络拓扑的需求增长而提高连接性。

附录 C

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、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：

- 反垃圾邮件， 第 269 页
- 防病毒， 第 253 页
- 病毒爆发过滤器， 第 307 页
- 分配管理任务， 第 723 页

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。

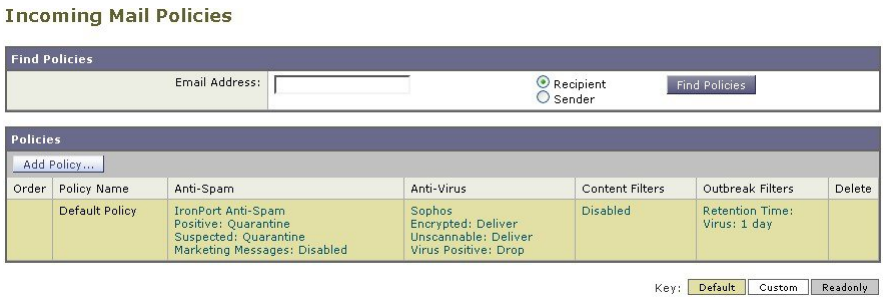
默认情况下，会为默认传入邮件策略启用这些设置：

- 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

图 *88*:“传入邮件策略”页面：全新设备的默认设置



注释 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。

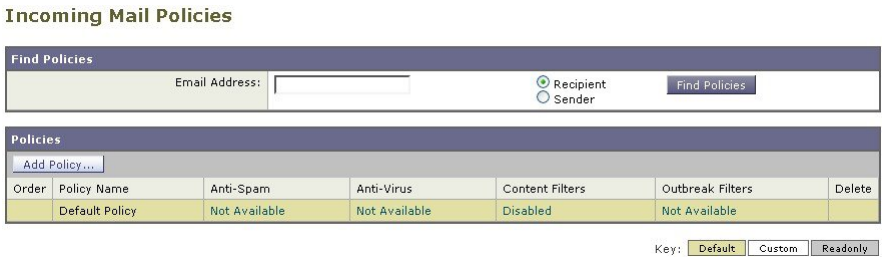
已启用、已禁用和“不可用”

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，点击“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。

图 *89:* 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，请点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严格的设置。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，以便删除确认的垃圾邮件。疑似垃圾邮件将继续被隔离。将启用营销邮件扫描功能，并营销邮件传送至目标收件人。营销邮件的主题将预置文本 [MARKETING]。

步骤 1 点击反垃圾邮件安全服务的链接。

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。可以点击“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，点击**是 (Yes)** 以启用营销邮件扫描。

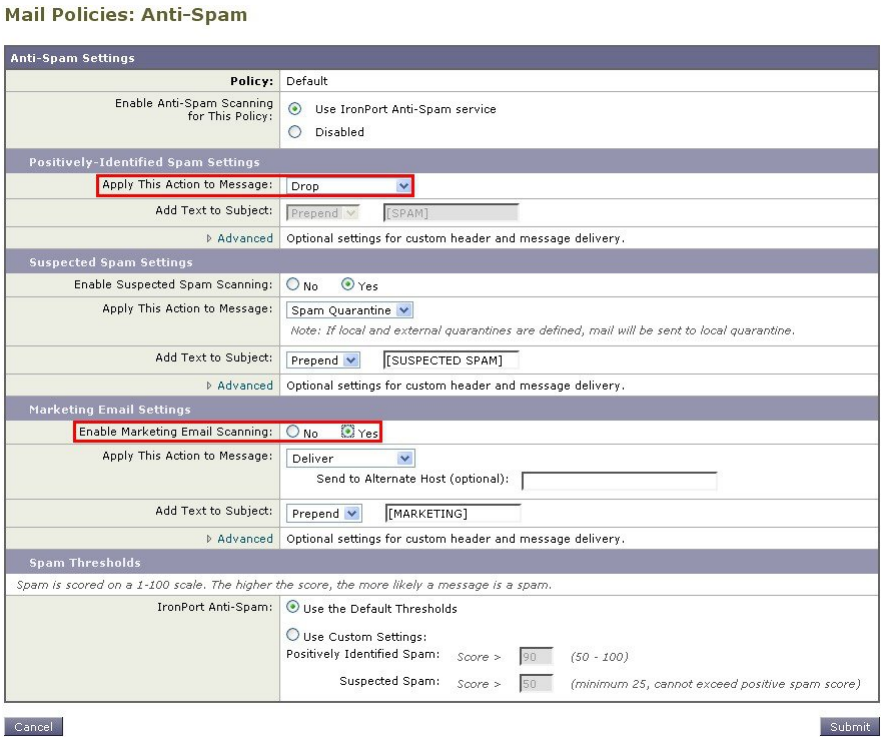
如果启用，则默认操作是传送合法的营销邮件，同时在主题前预置文本 [MARKETING]。

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

步骤 4 点击 **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。

图 *90:*“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，使属于此角色的委派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。

步骤 1 点击**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（进站或外发）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 点击“可编辑者 (角色)”(Editable By (Roles)) 链接并为负责管理邮件策略的委派管理员选择自定义用户角色。

当点击该链接时，AsyncOS 会为具有邮件策略编辑权限的委派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、防病毒和爆发过滤器设置，并为该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。

有关授权管理的详细信息，请参阅分配管理任务，第 723 页。

步骤 4 定义策略的用户。

邮件策略和内容过滤器示例

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，第 226 页。）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

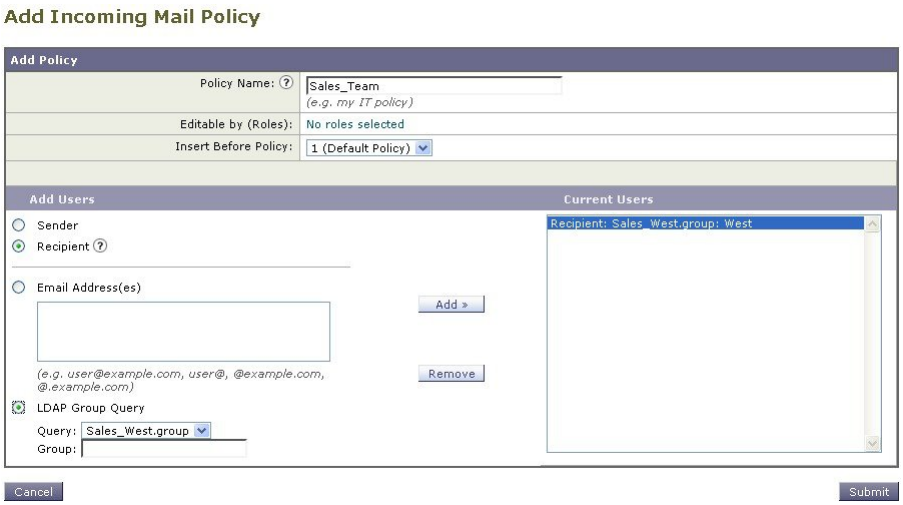
注释 AsyncOS GUI 和 CLI 中的用户条目都不区分大小写。例如，如果输入收件人 Joe@ 作为用户，则发送到 joe@example.com 的邮件与之匹配。

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，则可以将设备配置为查询 LDAP 服务器以接受收件人地址、将邮件路由到备用地址和/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。

如果将设备配置为执行此操作，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，第 585 页。

图 *91:* 为策略定义用户



步骤 5 点击**添加**按钮将用户添加到当前用户列表中。

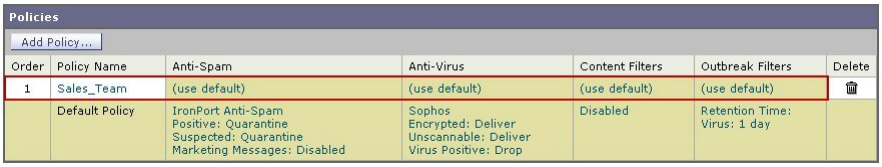
策略可以包含发件人、收件人和 LDAP 查询的组合。

使用**删除**按钮可从当前用户的列表中删除已定义的用户。

步骤 6 添加完用户后，点击**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。

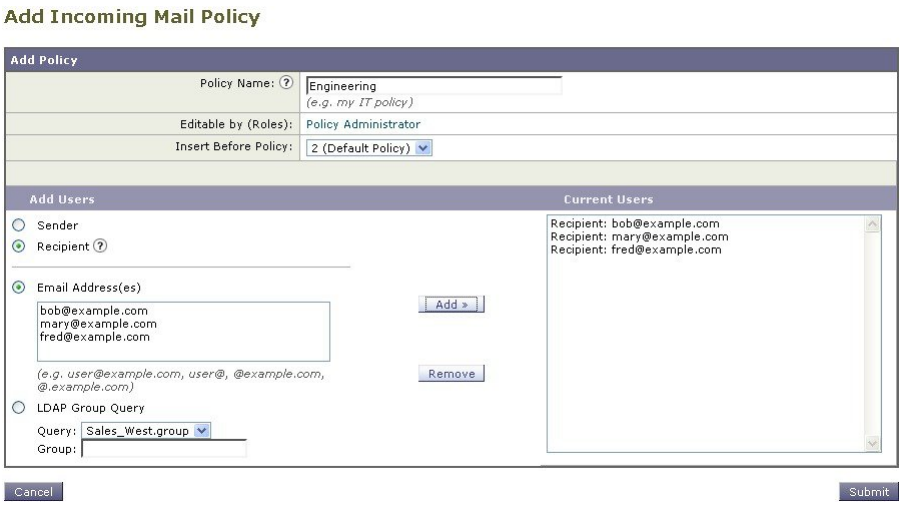
图 *92:* 新添加的策略 - 销售组



步骤 7 再次点击**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：

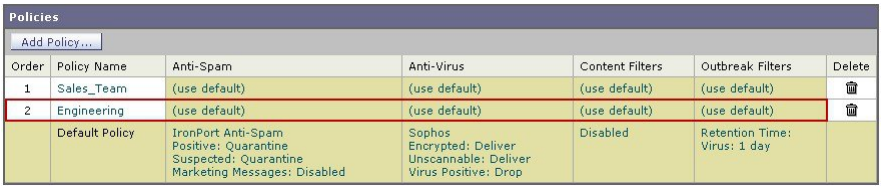
图 *93:* 为工程团队创建策略



步骤 8 为工程策略添加完用户后，点击**提交 (Submit)**。

步骤 9 确认您的更改。

图 *94:* 新添加的策略 - 工程团队



注释 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严格的设置。（请参阅为传入邮件配置默认反垃圾邮件策略，第 991 页。）删除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，请参阅反垃圾邮件，第 269 页。

- 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。爆发过滤器扫描会绕开扩展名为“dwg”的附件文件。

  有关配置爆发过滤器的详细信息，请参阅病毒爆发过滤器，第 307 页。

  为销售团队策略编辑反垃圾邮件策略步骤：

步骤 1 点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，点击**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)。

注释 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，点击**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，点击**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：

步骤 1 点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”不在设备进行附件扫描时可以通过其指纹识别的已知文件列表中。

注释 您不需要在三字母的文件扩展名之前键入句点 (.)。

步骤 4 点击**添加扩展名**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 点击**启用邮件修改 (Enable Message Modification)**。

启用邮件修改使设备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。

注释 必需在邮件策略中启用反垃圾邮件扫描，以便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)**。

这允许设备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释放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。

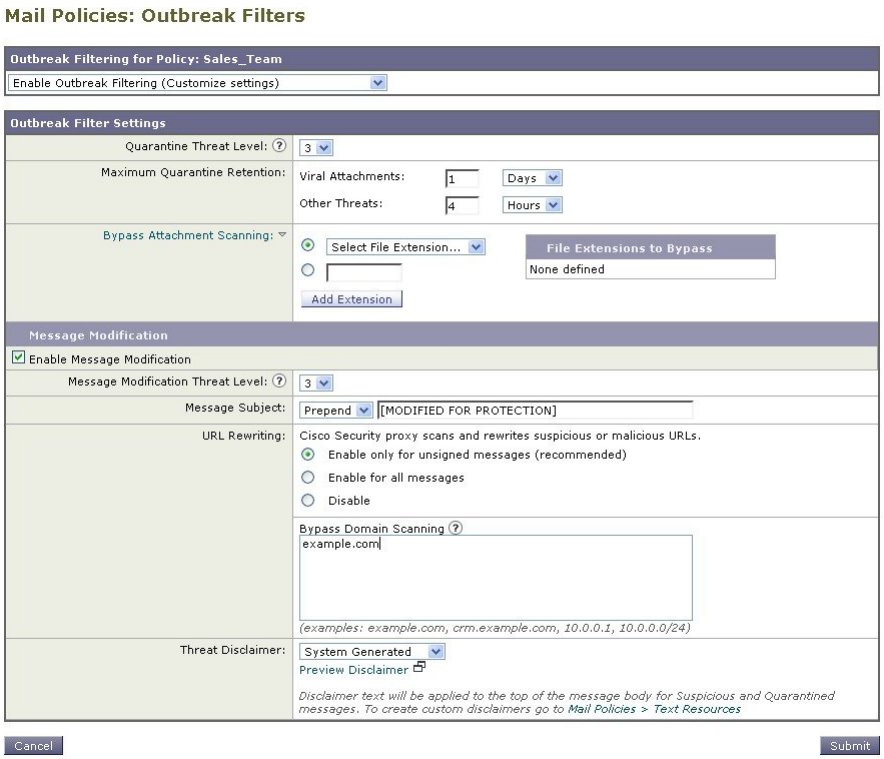
步骤 7 在**绕过域扫描 (Bypass Domain Scanning)** 字段中输入 example.com。

设备不会修改指向 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)。

设备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。

图 *95:* 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 并点击“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。

点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。“主动”策略旨在尽可能减少到达终端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 *153*: 积极和保守的邮件策略设置

	主动设置	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 无法扫描的邮件：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 无法扫描的邮件：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委派管理员进行编辑。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。

步骤 1 点击“邮件策略”(Mail Policies) 选项卡。

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

步骤 3 点击**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 点击**可编辑者 (角色) (Editable By (Roles))** 链接，选择“策略管理员”(Policy Administrator)，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 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 点击“添加条件”。

步骤 8 选择“邮件正文”(Message Body)。

步骤 9 在“包含文本:”字段中，键入 confidential，然后点击**确定**。

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

步骤 10 点击“添加操作”。

步骤 11 选择“发送副本到(Bcc:)”(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 点击 **OK**。

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

步骤 15 点击“添加操作”。

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 点击 **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，因此设备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。

步骤 1 点击**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 点击**可编辑者 (角色) (Editable By (Roles))** 链接，选择“策略管理员”(Policy Administrator)，然后点击**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 点击“添加操作”。

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 点击 **OK**。

步骤 11 提交并确认更改。

注释 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。

步骤 1 点击**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 点击**可编辑者 (角色) (Editable By (Roles))** 链接，选择“策略管理员”(Policy Administrator)，然后点击**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 点击**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 点击 **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 点击“添加操作”。

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。

注释 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 > 词典**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，第 481 页。

步骤 13 点击 **OK**。

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

步骤 14 点击“添加操作”。

步骤 15 选择“退回 (最终操作)”并点击“确定”。

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”。

图 *96:* 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

点击该链接可为各个策略启用和选择内容过滤器。

步骤 1 点击“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，第 992 页中添加的两个策略。请注意，默认情况下会为所有策略禁用内容过滤。

步骤 2 点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，第 235 页中使用“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 点击 **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：

步骤 1 点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 点击 **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。

下一步做什么

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。）

邮件策略和内容过滤器示例

- 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，并且可以由任何委派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，第 723 页。
- 管理员和操作员可以查看和编辑设备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，它们会立即影响设备对所有邮件的处理。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。（请参阅集中化的策略、病毒和病毒爆发隔离区，第 685 页）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释放邮件（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。
- 如果在设备中配置了 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”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)

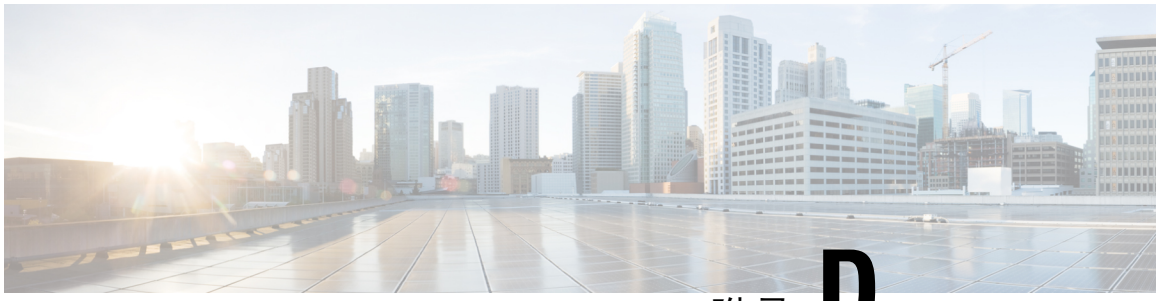
邮件策略和内容过滤器示例

- 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，情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。

图 *97:* 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：
  - **描述 (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。



附录 D

防火墙资讯

本章包含以下部分：

防火墙资讯

下表列出了为确保思科内容安全设备正常运行可能需要打开的端口（这些是默认值）。

表 *154:* 防火墙端口

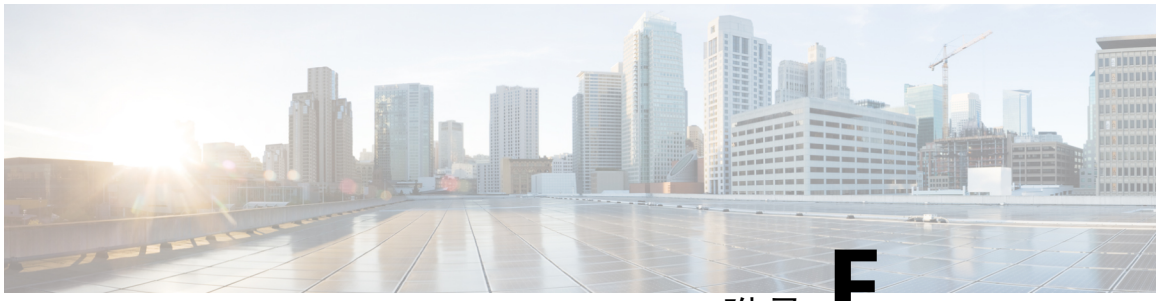
默认端口	协议	输入/输出	**Hostname**	目的
20/21	TCP	输入或输出	AsyncOS IP、FTP 服务器	通过 FTP 汇聚日志文件。 数据端口 TCP 1024 和更高端口也必须全部打开。 有关详细信息，请在知识库中搜索 FTP 端口信息。请参阅知识库，第 9 页。
22	TCP	In	AsyncOS IP	通过 SSH 访问 CLI，整合日志文件。
22	TCP	输出	SSH 服务器	通过 SSH 汇聚日志文件。
22	TCP	输出	SCP 服务器	SCP 推送到日志服务器。
25	TCP	输出	任意	SMTP，用于发送邮件。
25	TCP	In	AsyncOS IP	SMTP，用于接收退回的邮件，或者从防火墙外传入的邮件时。

防火墙资讯

53	UDP/TCP	输出	DNS 服务器	如果配置为使用 Internet 根服务器或防火墙外的其他 DNS 服务器，则使用 DNS。也用于 SenderBase 查询。
80	HTTP	In	AsyncOS IP	通过 HTTP 访问 GUI，进行系统监控。
80	HTTP	输出	downloads.ironport.com	和 McAfee 定义除外。
80	HTTP	输出	updates.ironport.com	AsyncOS 升级和 McAfee 定义。
80	HTTP	输出	cdn-microupdates.cloudmark.com	用于更新到 Intelligent MultiScan 中的第三方垃圾邮件组件。设备还必须连接到 CIDR 范围 208.83.136.0/22，才能更新第三方家庭电话。
82	HTTP	In	AsyncOS IP	用于查看垃圾邮件隔离区。
83	HTTPS	In	AsyncOS IP	用于查看垃圾邮件隔离区。
110	TCP	输出	POP 服务器	垃圾邮件隔离区的最终用户的 POP 身份验证。
123	UDP	输入/输出	NTP 服务器	NTP，如果时间服务器在防火墙外部。
143	TCP	输出	IMAP 服务器	垃圾邮件隔离区的最终用户的 IMAP 身份验证。
161	UDP	In	AsyncOS IP	SNMP 查询。
162	UDP	输出	管理站	SNMP 陷阱。
389 或 3268	LDAP	输出	LDAP 服务器	LDAP，如果 LDAP 目录服务器在防火墙外部。思科垃圾邮件隔离区的 LDAP 身份验证。
6363269	LDAP	输出	LDAP	LDAPS - ActiveDirectory 的全局目录服务器（使用 SSL）。
443	TCP	In	AsyncOS IP	到 GUI 的安全 HTTP (https) 访问，以进行系统监控。
443	TCP	输出	res.cisco.com	验证更新服务器的最新文件。
443	TCP	输出	update-manifests.ironport.com	从更新服务器（用于物理硬件设备）获取最新文件的列表。

443	TCP	输出	update-manifests.sco.cisco.com	从更新服务器（用于虚拟设备）获取最新文件的列表。
443	TCP	输出	phonehome.senderbase.org	接收/发送病毒爆发过滤器。
443	TCP	输出	在命令行界面，运行 websecurityadvancedconfig 命令并接受所有默认值。将显示网络安全服务主机名。	云服务用于获取 URL 信誉和类别信息，以进行URL过滤。
443	TCP	输出	如“安全服务”(Security Services) >“文件信誉和分析”(File Reputation and Analysis) 的“文件信誉”(File Reputation) 部分“高级设置”(Advanced Settings) 的“云服务器池”(Cloud Server Pool) 参数的配置。	如果已配置，则为访问云服务获取文件信誉的端口。默认端口为 32137。有关文件分析服务，请参阅端口 443。
443	TCP	输出	如“安全服务”(Security Services) >“文件信誉和分析”(File Reputation and Analysis) 的“文件分析”(File Analysis) 部分“高级设置”(Advanced Settings) 的配置。	访问云服务以进行文件分析。有关文件信誉服务，请参阅端口 443 或 32137。
443	TCP	输入/输出	outlook.office365.com login.microsoftonline.com.	访问 Office 365 服务以进行邮箱自动修复。
443	TCP	输出	aggregator.cisco.com	对思科聚合服务器的访问。
514	UDP/TCP	输出	系统日志服务器	系统日志记录。
628	TCP	输入/输入	AsyncOS IP	QMQP，如果从外部防火墙注入邮件。
1024 和更高	-	-	-	对于端口 21，请参阅以上信息 (FTP)。
2222	CCS	输入/输入	AsyncOS IP	集群通信服务（用于集中管理）。
7025	TCP	输入和输出	AsyncOS IP	启用此功能时，传递邮件安全设备和安全管理设备之间的策略、病毒和病毒爆发隔离区数据。

防火墙资讯



附录 E

最终用户许可协议

本附录包含以下部分：

思科系统公司最终用户许可协议

重要提示：请认真阅读本最终用户许可协议。很重要的一点是，您应确认是从授权来源购买思科软件或设备，并且您或您所代表的实体（统称为“客户”）已经注册成为思科最终用户许可协议中规定的最终用户。如您还未注册成为最终用户，则无权使用本软件。本最终用户许可协议中的有限担保条款对您不适用。如您是从已授权的渠道购买了本软件，一旦下载、安装或使用思科或思科供应软件即构成接受本协议。

CISCO SYSTEMS, INC.或代替 CISCO SYSTEMS INC. 许可本软件的子公司（“思科”）愿意对您许可本软件，前提条件是您购买的软件来自授权来源，并且您接受本最终用户许可协议中的所有条款和条件，以及本产品随附或订购本产品时提供的附加许可协议中列出的对许可证的任何其他限制（统称“协议”）。如果最终用户许可协议与补充许可协议之间存在任何冲突，应以补充许可协议为准。下载、安装或使用本软件即表示您确认您是从授权渠道购买的本软件并同意受本协议的约束。若您不同意本协议全部条款，则思科不愿意授予您本软件许可，因此 (a) 您不得下载、安装或使用本软件；和 (b) 您可退还本软件（包括未启封的 CD 包和所有书面资料）并获得全额退款。或者，如果本软件与书面材料构成其他产品的组成部分，您可退还全部产品并获得全额退款。只有原始及注册最终用户购买者才享有退货与退款权利，并且该权利从授权渠道购买产品后 30 天失效。在本最终用户许可协议中，“获批来源”指 A) 思科；或 (B) 经思科授权在您所在大区内向最终用户分销/出售思科设备、软件和服务的分销商或系统集成商；或 (C) 由任何该等分销商或系统集成商根据与思科签署的分销商协议条款授权在您所在大区内向最终用户分销/出售思科设备、软件和服务的经销商。

本协议下述条款管辖客户对本软件（定义如下）的使用，除非 *(a)* 客户与思科签订了单独协议以管理客户对本软件的使用；或 *(b)* 本软件包含了单独的“点击接受”许可协议或第三方许可协议，作为安装或下载流程的组成部分以管理客户对本软件的使用。如果前述文件条款之间存在任何抵触，优先顺序应为 *(1)* 经签署后的合同；*(2)* 点击接受协议或第三方协议；和 *(3)* 本协议。在本协议中，“软件”指计算机程序，包括授权来源提供给客户的思科设备中嵌入的固件和计算机程序，以及该固件和计算机程序的升级版、更新版、错误修正版与修改版（统称为“升级版”）；根据思科软件转让或重新许可政策（思科不定期修改后版本）重新许可的程序或前述内容的备份副本。

最终用户许可协议

许可。以遵守本协议条款和条件为前提，思科授予客户非独占性、不可转让许可，允许在客户内部业务中使用客户已向授权渠道支付许可费用的软件和文档。“文档”指该软件授权来源以任何方式（如 CD-ROM、在线提供等）所提供的与本软件相关的书面信息（无论是包含在用户手册、技术手册、培训材料、技术说明或其他材料中）。为使用本软件，客户应输入注册号或产品授权密钥，并在思科的网站在线登记客户的软件副本，以获取必要的许可密钥或许可文件。

客户使用本软件的许可应限于单个硬件机箱或硬件卡，除此以外客户不得在其他地方使用本软件。此外，使用许可权限还应符合相关补充许可协议或采购订单上规定的限制要求，因为此类订单已被授权来源所接受，并且客户已就该订单（“采购订单”）向授权来源支付必要的许可费。

除文档或相关补充许可协议中另有明确规定外，客户仅能使用其持有或租赁的思科设备中嵌入、运行的软件，或（如果相关文档允许在非思科设备上安装的话）为了与客户持有或租赁的思科设备通信使用本软件，以及为了实现客户的内部业务目的使用本软件。未以暗示、禁止反言或其他方式授予其他许可。

对于思科未收取许可费用的评估或测试软件，上述有关支付许可费用的要求不适用。

一般限制要求本协议仅为软件与文档许可协议，并非转让软件与文档的所有权，思科保留本软件与文档副本的所有权利。客户确认本软件与文档中含有思科或其提供商与许可方的商业秘密，包括（但不限于）单个程序的具体内部设计和架构，以及相关接口信息。除非本协议另作明确规定，本软件只能与客户从获批来源购得的思科设备配套使用，客户应无权利且客户明确同意不：

(i) 无权且明确同意不会向他人或实体转让、分配或转授其许可权力（符合思科现行有效的再次许可/转让政策的除外）；无权且明确同意不会在授权渠道以外采购的思科设备上或在二手思科设备上使用本软件；客户确认任何企图转让、分配、转授或使用的行为无效。

(ii) 无权且明确同意不会修正本软件错误、修改本软件或根据本软件制作衍生产品；也不得允许他人实施这种行为；

(iii) 无权且明确同意不会对本软件进行逆向工程、反编译、解码、反汇编或将本软件修改为可读格式。尽管存在该等限制要求，但适用法律明确许可的情况除外，以及根据适用开源协议规定要求思科允许该等活动的除外。

(iv) 无权且明确同意不会公布在本软件上运行的基准测试的结果；

(v) 未征得思科明确书面授权，无权且明确同意不会使用本软件或允许使用本软件向第三方提供服务，无论是以服务机构或分时方式提供服务；或

(vi) 未征得思科事先书面批准，无权且明确同意不会以任何方式向第三方披露、提供本软件和文档中包含的商业秘密。客户应采取合理的安全措施保护该等商业秘密。

在适用法律要求的范围之内，如经客户书面要求，思科应向客户提供实现软件与其他独立创建的程序之间的互操作性所需的界面信息，但客户应支付思科收取的合理费用（如有）。客户应严格遵守该等信息相关的保密义务。思科提供该等信息后应根据适用条款和条件的要求使用该等信息。

软件、升级版或额外副本。尽管本协议中含有其他相反之规定，(1) 客户无权制作或使用额外副本或更新版本，除非客户在制作或取得该副本或更新版本时，已经持有原始软件的有效许可并就更新版本或新增副本向许可资源支付了的恰当的费用；(2) 升级版本仅限用于授权渠道提供的思科设备，且客户是原始最终用户采购方或租赁方，或持有有效许可使用被升级软件，和 (3) 仅限于备份目的制作和使用额外副本。

专有权通知客户同意采用软件中含有的版权通知和其他专有权通知的格式和方法，针对所有形式的软件副本建立并翻印版权、专有权和其他通知。除本协议明确批准外，未经思科事先书面同意，客户不得制作任何本软件的副本。

期限和终止。本协议与本协议授予的许可在协议终止前始终有效。客户销毁本软件和文档的全部副本后即可终止本协议。如果客户未遵守本协议中的任何条款，则本协议中规定的客户权利应立即终止，无需思科另行通知。协议终止后，客户应销毁其持有或控制和软件与文档的全部副本。本协议终止后，“一般限制要求”一节中规定客户应遵守的所有保密义务、禁止与限制要求、责任限制、免责声明和质保限制要求应继续有效。此外，本协议终止后，标题“美国政府最终用户购买者”和“适用于有限担保声明和最终用户许可协议的通用条款”部分的规定仍然有效。

客户记录客户授予思科及其独立会计师权利，可在客户的正常营业时间内检查客户的账簿、记录及账目，以验证客户遵守本协议的情况。如果审计显示客户不符合本协议要求，客户应即时向思科支付恰当的许可费用加上合理的审计费用。

出口、再出口、转让与使用管控思科根据本协议提供的软件、文档和技术或直接产品（以下称为“软件和技术”）受美国法律法规及任何其他适用国家/地区的法律法规的出口控制约束。客户应遵守适用于思科软件和技术的出口、再出口、转让及使用的法律与法规，并将取得所有必要的美国联邦及地方的批准、审批或许可。思科与客户同意向对方提供取得授权或许可相关的其他信息、支持文件与合理要求的协助。有关遵守出口、再出口、转让和使用等方面规定的信息，请访问：

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html.

美国政府最终用户购买人本软件与文档系“商业物品”，该术语定义见《联邦采购条例》（“FAR”）(48 C.F.R.) 2.101，包括“商业计算机软件”和“商业计算机软件文档”，该术语用于 FAR 12.212。符合 FAR 12.212 和 DoD FAR 增刊227.7202-1 至 227.7202-4 的要求。尽管本协议可能并入含有其他相反之 FAR 或合同条款的协议中，客户可向政府最终用户提供具备本协议规定权利的软件与文档。如果本协议为直接与政府签订的协议，则政府最终用户仅根据协议规定的权利即可获得软件与文档。使用软件或文档或二者均使用，将视为政府同意本软件与文档为“商业计算机软件”与“商业计算机软件文档”，并视作政府接受本协议中规定的权利与限制要求。

标识组件；额外条款 本软件可能含有一个及以上的组件或与该等组件一同交付，这些组件可能含有第三方备件，思科在文档、自述文件、第三方点击接受协议或其他地方（如 http://www.cisco.com/）上对该等组件做出了标识（“标识组件”）。该等组件应遵守不同于本协议规定的许可协议条款、质保免责声明、限制保证或其他条款和条件（统称为“额外条款”）的要求。您同意接受任何此类标识组件的适用附加条款。

有限担保。

以符合本协议中的限制要求与条件为前提，思科保证：自向客户发货之日起（如果是授权来源转售而非思科直接销售，则应从思科最初发货后不超过九十 (90) 天起计算），在随后为期 (a) 九十 (90) 天或 (b) 随产品（本软件系组成部分）一同交付的保修卡上明确规定的质保期（如有）内（以二者中较长日期为准），(a) 安装软件的媒介在正常使用的情况下，材料与工艺上无任何瑕疵；和 (b) 本软件完全符合文档要求。思科发运产品的日期见产品包装。除上述规定外，软件将“按原样”提供。本有限保修仅用于首次注册最终用户从授权渠道购买的软件。本有限担保中的客户专属补救措施与思科和其提供商的全部责任为 (i) 替换缺陷媒介和/或 (ii) 根据思科的选择修复、替换本软件或退款，上述两种情况的前提条件是违反本有限担保的错误或缺陷在质保期内已报告给向客户销售软件的授权渠道。思科或向客户提供软件的授权渠道可不要求返还软件和/或文档作为行使补救措施的前提条

最终用户许可协议

件。思科未保证本软件无任何错误，也未保证客户使用本软件时不会出现任何问题或发生中断。此外，由于入侵和攻击网络的新技术的不断发展，思科并不保证本软件或本软件运行的设备、系统或网络无入侵和攻击漏洞。

限制如果本软件、产品或授权使用本软件的设备发生下述情况，则本保修不适用：(a) 被修改；但思科或其授权代表做出的修改除外；(b) 未按思科的指示安装、操作、修理或维护；(c) 受到非正常物理或电气应力、非正常环境条件、不当使用、疏忽或其他事故的影响；或 (d) 仅授予测试、评估、试验或示范许可。本软件保修也不适用于：(e) 任何临时软件模块；(f) 思科软件中心上未公布的软件；(g) 思科在思科软件中心明确“按原样”提供的软件；(h) 授权来源未收到许可费用的软件；和 (i) 授权来源以外的第三方提供的软件。

保修免责声明

除保修条款中规定的外，所有明示或暗示的条款、陈述与保证，包括（但不限于）对适销性、特殊目的适用性、未涉侵权、合格品质、未涉干扰、信息内容准确性等的暗示保修或条款，或因交易过程、法律、惯例或商业习惯产生的暗示保修或条款在此予以排除，但必须符合适用法律的规定，且思科、其提供商和授权商明确否认这种暗示的保修或条款。某种程度上，同样不能排除该等隐含条款、陈述和（或）保证的持续时间仅限于上文“有限担保”一款中明确规定的明示保修期内的情况。由于部分国家或司法管辖区不允许存在暗示保证时限限制，则上述限制要求在该等地区不适用。本保修赋予了客户特定的法律权利，同时客户也可拥有其他司法管辖区内规定的其他权利。即使上述明示保证未能实现其根本目的，该款免责及排除仍然适用。

免责声明 – 责任限制。如果您是在美国、拉丁美洲、加拿大、日本或加勒比地区购买的本软件，尽管本协议中含有其他相反规定，但是，思科、其关联机构、高管、董事、雇员、代理、提供商和授权商对客户应承担的责任（无论是因合同、侵权 [包括过失行为]、违反保修条款或其他形式引起的责任）不得超过授权渠道提供商提供的被索赔软件的购买价格，如果该软件为其他产品的组成部分，则不得超过该产品的购买价格。软件的责任限制为累积计算，并非针对每次事件（即，两次或两次以上的索赔不得提高此限制）。

如果您是在欧洲、中东地区、非洲、亚洲或太平洋地区购买的本软件，尽管本协议中含有其他相反规定，但是，思科、其分公司、高管、董事、雇员、代理、提供商和授权商对客户应承担的责任（无论是因合同、侵权（包括过失行为）、违反保修条款或其他形式引起的责任）不得超过思科提供的被索赔软件的购买价格，如果该软件为其他产品的组成部分，则不得超过该产品的购买价格。软件的责任限制为累积计算，并非针对每次事件（即，两次或两次以上的索赔不得提高此限制）。本协议中的任何内容均不限制(I)思科及其附属公司、高级官员、总监、员工、代理、供应商和许可商由于疏忽对客户造成个人伤害或致死的责任；(II) 思科欺诈性误述的责任；或 (III) 适用法律要求不能排除的思科责任。

免责声明 - 针对间接损害及其他损失的免责声明。 如果您是在美国、拉丁美洲、加勒比地区或加拿大购买的本软件，无论本协议中规定的补救措施是否实现了其基本目的，对于任何收益与利润损失、遗失或损坏数据、业务中断、资本损失，或特殊的、间接性、连带性或惩罚性损害赔偿，思科或其提供商均无需承担任何责任，无论导致前述损失损害的原因与责任推断如何，也无论是否是由于使用本软件造成该等损失损害，即使思科或其提供商曾告知将发生该等损害的可能性。由于某些国家或管辖区不允许限制或排除间接或附带损害，因此，上述限制可能对您不适用。

如果您在日本购买软件，除了由死亡或人身伤害、欺诈性失实陈述引起或与之相关的责任，无论本协议中补救措施是否实现其根本目的或其他目的，在任何情况下，思科及其关联机构、管理人员、董事、员工、代理、提供商及许可方对任何原因造成的任何收益或利润损失、数据丢失或损坏、业务中断、资本损失、特殊、间接、连带、附带或惩罚性损失概不负责，不论责任推断如何，也无论

是否因使用或无法使用软件或其他原因引起，即使思科或任何经批准的源或其提供商或许可方已被告知发生此类损失的可能性。

如果您在欧洲、中东、非洲、亚洲或大洋洲购买软件，在任何情况下，思科及其分公司、管理人员、董事、员工、代理、提供商及许可方对任何收益或利润损失、数据丢失或损坏、业务中断、资本损失、特殊、间接、从属、附带或惩罚性损失概不负责，无论该损失如何造成，包括（但不限于）合同或侵权（包括疏忽）原因，也无论该损失是否因使用或无法使用软件引起，即使在各种情况下思科及其分公司、管理人员、董事、员工、代理、提供商及许可方已被告知发生此类损失的可能性。由于某些国家或管辖区不允许限制或排除间接或附带损害，因此，上述限制可能对您完全不适用。前述排除免责条款不适用于由下列原因引起或与之相关的责任：(I) 死亡或人身伤害；(II) 欺诈性失实陈述；(III) 与适用法律下任何不可免责条款有关的由思科承担的责任。

客户确认并同意，思科已根据本协议中的免责声明和责任限制确定价格和签订本协议，该价格和协议反映了协议各方之间的风险分担（包括合同补救措施可能不能达到其根本目的而且可能导致间接损失的风险），并构成了协议各方议价的重要依据。

管辖法律和司法权。如果您参照经授权来源所接受的采购订单上的地址，在美国、拉丁美洲或加勒比海采购软件，本协议和保证条款（“保证条款”）受美国加州的法律管辖并持解释权，不管是否存在任何法律条款冲突。加州法院和联邦法院对由本协议或保证条款引起的任何索赔享有专属管辖权。如果您在加拿大购买软件，除非当地法律明确禁止，否则本协议和保证条款受加拿大安大略省法律管辖并据其进行解释，不管法律条款是否存在任何冲突；安大略省法庭对由本协议或保证条款引起的任何索赔享有专属管辖权。如果您在欧洲、中东、非洲、亚洲或大洋洲（不包括澳大利亚）购买软件，除非当地法律明确禁止，否则本协议和保证条款受英国法律管辖并据其进行解释，尽管法律条款可能存在任何冲突。英国法庭对由本协议或保证条款引起的任何索赔享有专属管辖权。此外，如果本协议受英国法律管辖，依照《1999 年合同法（第三方权利）》，不属于本协议一方的任何人无权执行或受益于本协议的任何条款。如果您在日本购买软件，除非当地法律明确禁止，本协议和保证条款受日本法律管辖并依据该法律进行解释，尽管法律条款可能存在任何冲突。日本东京地方裁判所对由本协议或保证条款引起的任何索赔享有专属管辖权。如果您在澳大利亚购买软件，除非当地法律明确禁止，本协议和保证条款受澳大利亚新南威尔士州法律管辖并依据该法律进行解释，尽管法律条款可能存在任何冲突。新南威尔士州法院和联邦法院对由本协议或保证条款引起的任何索赔享有专属管辖权。如果您在任何其他国家/地区购买软件，除非当地法律明确禁止，否则本协议和保证条款受美国加州管辖并据其进行解释，尽管法律条款可能存在任何冲突。加州法院和联邦法院对由本协议或保证条款引起的任何索赔享有专属管辖权。

对于上述所有国家/地区，协议各方明确放弃使用《联合国国际货物销售合同公约》。尽管有上述规定，各方可以就任何所谓的违反该方知识产权或专有权利之行为，向适当管辖区的任何法庭寻求临时禁令救济。如果任何部分被发现为无效或不可强制执行，本协议和保证条款的其他条款应继续完全有效。除非本协议另有明确规定，否则本协议构成双方之间关于软件和文档许可的完整协议，并且替代任何《采购订单》或其他内容中包含的任何冲突或附加条款，所有此类条款都将被排除。本协议采用英文书写，双方同意以英语版本为准。

在以下 URL，可获得适用于思科产品的产品保修条款及其他信息：

http://www.cisco.com/go/warranty

思科系统公司内容安全软件终端用户补充许可协议

重要信息：请仔细阅读

最终用户许可协议

这种补充终端用户许可协议（“SEULA”）包含您（此处使用“您”，意味着您和所代表的业务实体或“公司”）与思科之间根据终端用户许可协议（“EULA”）许可的软件产品的其他条款和条件（统称为“协议”）。本SEULA中使用，但未定义的大写术语，与EULA中对其分配的含义相同。如果 EULA 和本 SEULA 的条款和条件在某种程度上存在冲突，则此 SEULA 的条款和条件优先。

除了 EULA 中列出的对您的软件访问和使用的限制之外，您同意始终遵守本 SEULA 中提供的条款和条件。

下载、安装或使用本软件即构成接受本协议，您自己及所代表的业务实体均受本协议绑定约束。若您不同意本协议全部条款，则思科不愿意授予您本软件许可，因此(a)您不得下载、安装或使用本软件；和(b)您可退还本软件（包括未启封的CD包和所有书面资料）并获得全额退款。或者，如果本软件与书面材料构成其他产品的组成部分，您可退还全部产品并获得全额退款。从思科或授权思科经销商购买产品30天后，退货和退款的权利即到期，而且只有您是原始终端用户购买者，此权利才适用。

对于此SEULA，您订购的产品名称和产品说明是以下任意思科系统邮件安全设备（“ESA”）、思科系统网络安全设备（“WSA”）和思科系统安全管理应用（“SMA”）（统称为“内容安全”）及其等效的虚拟设备（“软件”）：

Cisco AsyncOS for Email

Cisco AsyncOS for Web

Cisco AsyncOS for Management

思科邮件反垃圾邮件、Sophos 防病毒

思科邮件爆发过滤器

Cloudmark 反垃圾邮件

思科映像分析器

McAfee 防病毒

思科智能多次扫描

思科数据丢失保护

思科邮件加密

思科电邮传送模式

思科网络使用控制

思科网络信誉

Sophos防恶意软件

Webroot防恶意软件

McAfee 防恶意软件

思科邮件报告

思科邮件跟踪

思科邮件集中式隔离区

思科 Web 报告

思科网络策略和配置管理

使用 Splunk 的思科高级网络安全管理

加密设备的邮件加密

系统生成的批量邮件的邮件加密

加密设备的邮件加密和公钥加密

加密设备的大型附件处理

加密设备的安全邮箱许可证

定义

对于此 SEULA，以下定义适用：

“公司服务”是指为了执行公司的内部业务，向终端用户提供的公司邮件、互联网、安全管理服务。

“终端用户”是指：（1）对于 WSA 和 SMA，为公司授权通过公司服务访问互联网和 SMA 的员工、承包商或其他代理；以及（2）对于 ESA，为公司授权通过公司服务访问或使用邮件服务的员工、承包商或其他代理的电子邮箱。

“订购文档”是指公司与思科或公司与思科经销商之间的购买协议、评估协议、试用，发布前协议或类似的协议，或思科接受的与之相关的任何采购订单的有效条款，包括本协议授予的软件许可证购买条款。

“个人身份信息”是指可用于识别个人的任何信息，包括但不限于个人的姓名、用户名、邮件地址及任何其他个人身份信息。

“服务器”是指网络中的一台物理计算机或设备，管理或为多位用户提供网络资源。

“服务”是指思科软件订用服务。

“服务说明”是指以下网站介绍的软件订用支持服务：http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html

“遥测数据”是指公司的邮件和网络流量示例，包括有关邮件和网络请求属性的信息，以及有关公司的思科硬件产品如何处理不同类型的邮件和网络请求的信息。遥测数据中的邮件元数据和网络请求已进行匿名和模糊处理，以删除任何个人身份信息。

“期限”是指您购买的软件订用的长度，如订购文档中所示。

“虚拟设备”是指思科邮件安全设备、网络安全设备和安全管理设备的虚拟版本。

“虚拟机”是指可像服务器一样运行自己的操作系统和执行应用程序的软件容器。

其他许可条款和条件

许可证授予并同意数据收集条款

软件许可。

最终用户许可协议

使用本软件及文档，公司即同意遵守本协议的条款。只要公司遵从本协议，思科将在软件使用期限内，授予公司非排他性、不能再许可、不可转让的全球许可，仅限用于思科硬件产品；对于虚拟设备，即在虚拟机中，仅与面向终端用户的公司服务条款相关。许可使用本软件的终端用户数，限制为订购文档中规定的终端用户数。如果与提供公司服务相关的终端用户数量超过订购文档中规定的终端用户数量，公司将联系授权渠道购买更多该软件的许可证。有关此许可证的持续时间和范围等详细定义，请参阅订购文档。在软件许可证条款方面，订购文档可取代 EULA。除了此处授予的许可权限外，思科、思科经销商或其各自许可人不向公司授予任何软件的权利、所有权或利益。您对本软件升级的权利受服务说明约束。本协议和服务的有效期相同。

同意和许可使用数据。

根据思科隐私声明 (http://www.cisco.com/web/siteassets/legal/privacy.html)，公司在此同意并允许思科从公司收集和使用遥测数据。思科不会收集或使用遥测数据中的个人身份信息。思科可以与第三方共享整合和匿名的遥测数据，以帮助我们改进用户体验及本软件与其他思科安全产品和服务。公司可以随时禁用本软件中的“SenderBase 网络参与”，从而终止思科收集遥测数据的权限。有关启用或禁用“SenderBase 网络参与”的说明，请参阅软件配置指南。

其他权利和义务说明

请参阅 Cisco Systems Inc. 终端用户许可协议、隐私声明和软件订用支持服务的服务说明。

索 引

符號

A

B

C

D

E

F

G

H

J

K

L

M

N

P

Q

R

S

T

W

X

Y

Z