了解邮件通道

本章包含以下部分：

- 邮件管道概述 ， 第 1 页
- 邮件管道流 ， 第 1 页
- 传入/接收 ， 第 4 页
- 工作队列/路由 ， 第 6 页
- 交付 ， 第 10 页

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、病毒爆发过滤器和隔离。
- 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 *1:* 邮件管道 - 接收邮件连接

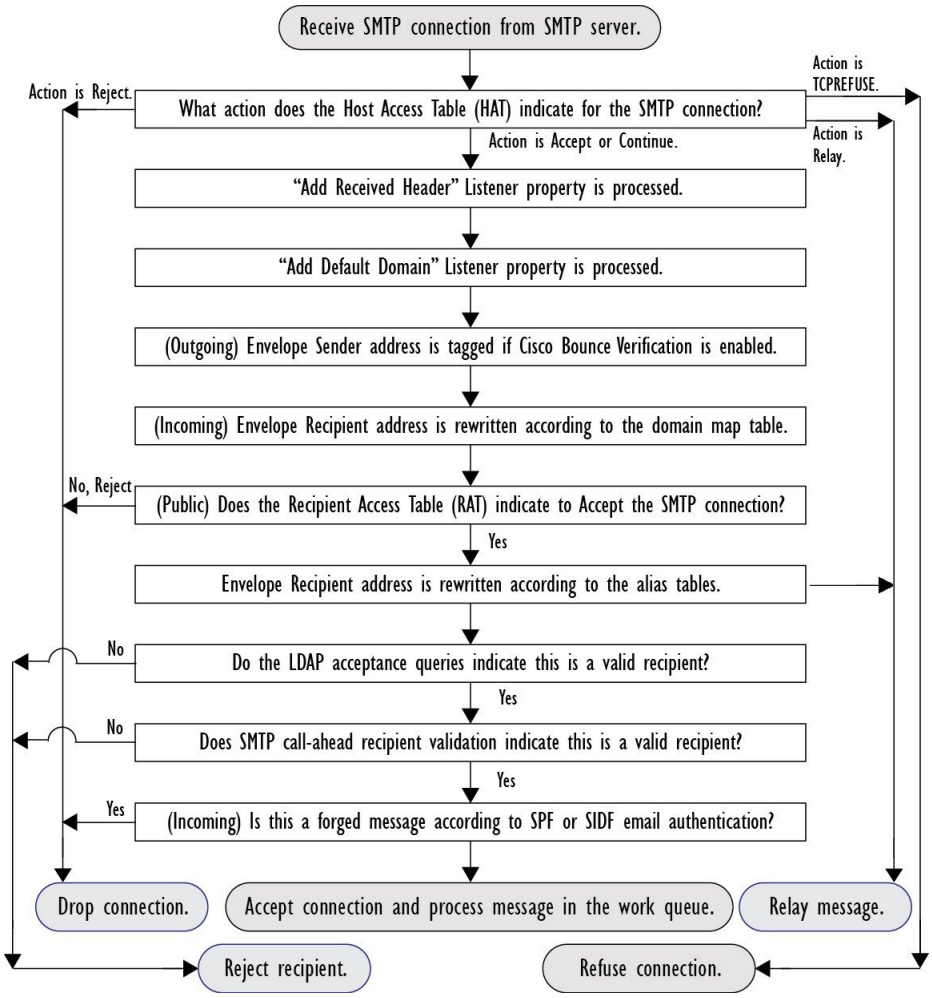


图 *2:* 邮件管道 - 工作队列

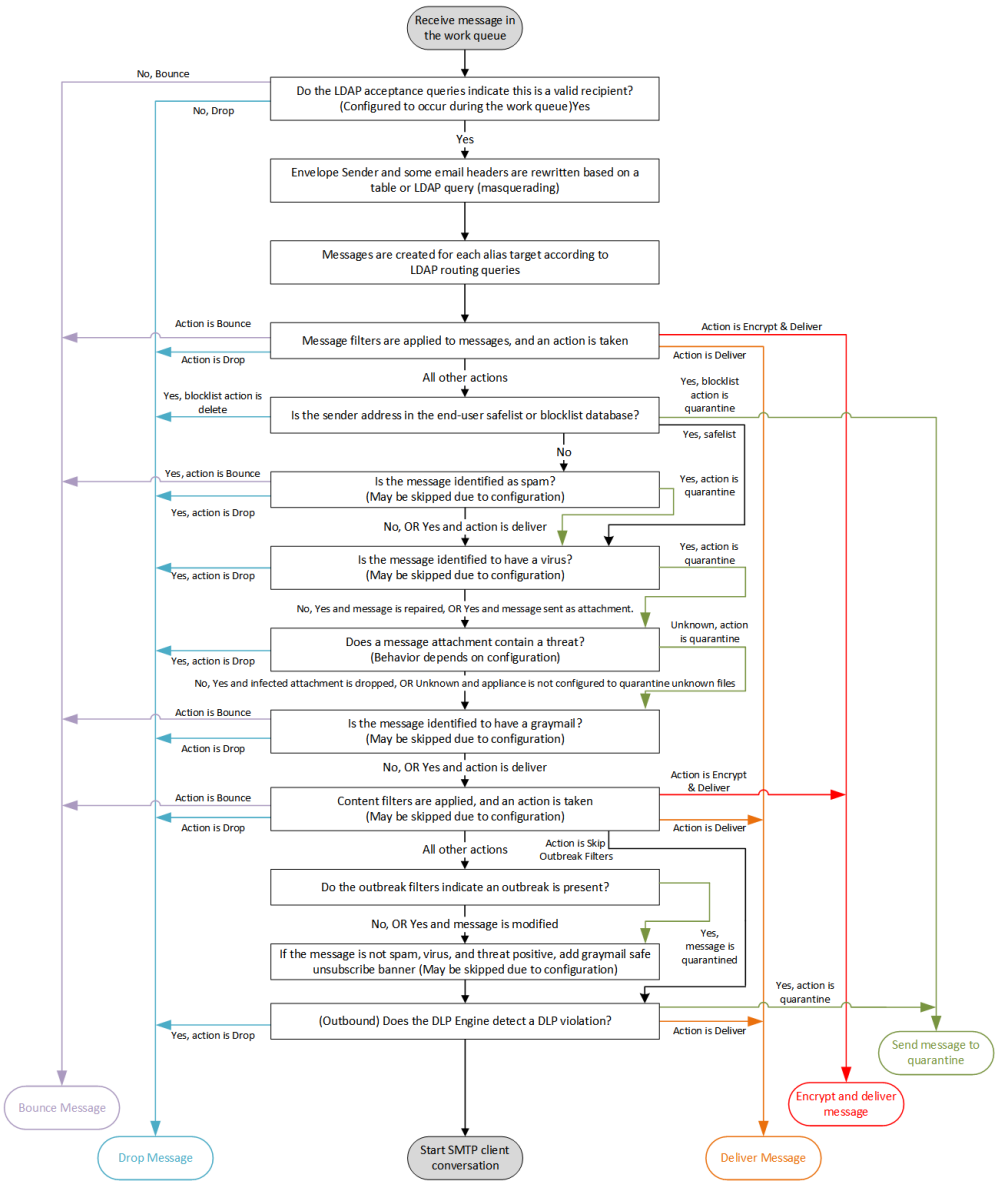
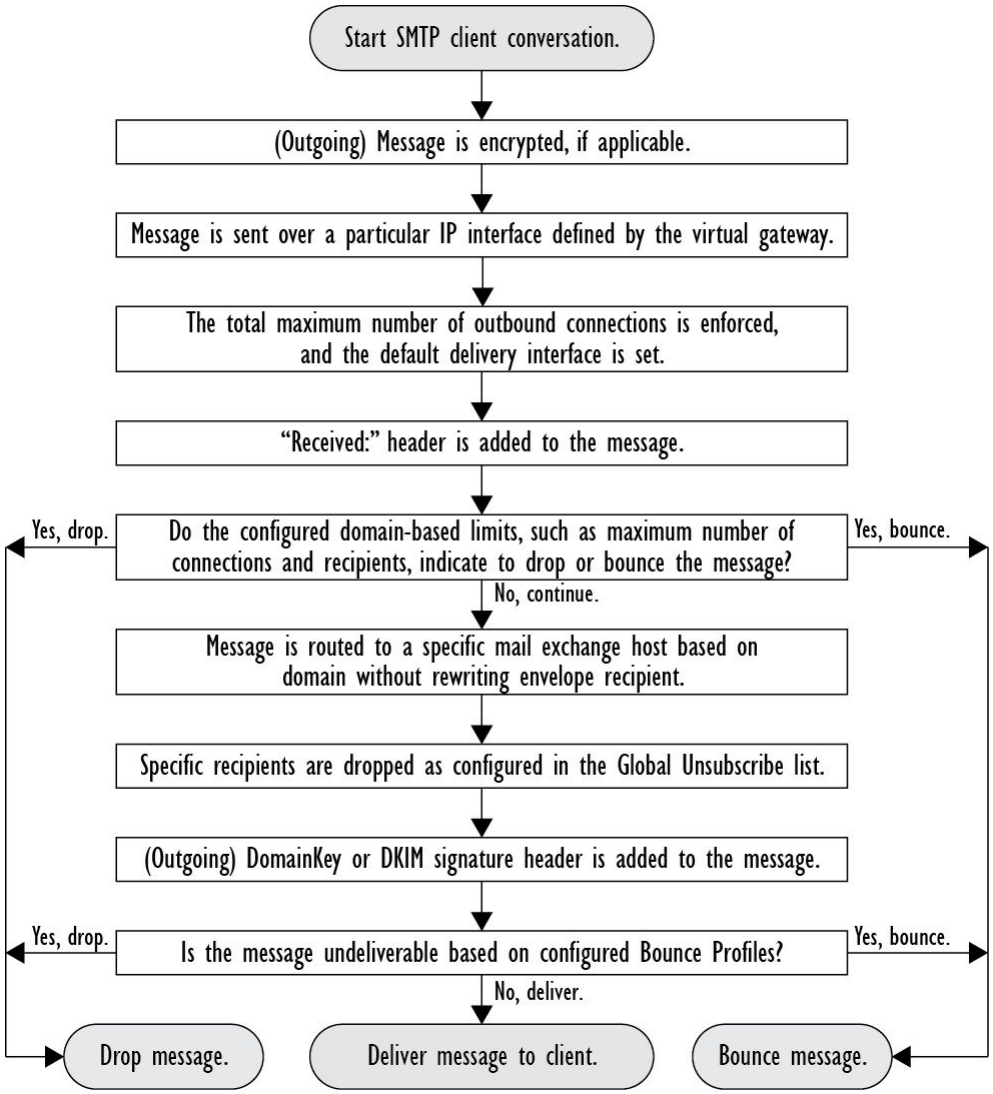

Receive message in the work queue
Do the LDAP acceptance queries indicate this is a valid recipient? (Configured to occur during the work queue)Yes
No, Bounce
No, Drop
Yes
Envelope Sender and some email headers are rewritten based on a table or LDAP query (masquerading)
Messages are created for each alias target according to LDAP routing queries
Message filters are applied to messages, and an action is taken
Action is Bounce
Action is Drop
Action is Encrypt & Deliver
Action is Deliver
All other actions
Is the sender address in the end-user safelist or blocklist database?
Yes, blocklist action is delete
Yes, blocklist action is quarantine
Yes, safelist
No
Is the message identified as spam? (May be skipped due to configuration)
Yes, action is Bounce
Yes, action is Drop
Yes, action is quarantine
No, OR Yes and action is deliver
Is the message identified to have a virus? (May be skipped due to configuration)
Yes, action is Drop
Yes, action is quarantine
No, Yes and message is repaired, OR Yes and message sent as attachment.
Does a message attachment contain a threat? (Behavior depends on configuration)
Unknown, action is quarantine
Yes, action is Drop
No, Yes and infected attachment is dropped, OR Unknown and appliance is not configured to quarantine unknown files
Is the message identified to have a graymail? (May be skipped due to configuration)
Action is Bounce
Action is Drop
No, OR Yes and action is deliver
Content filters are applied, and an action is taken (May be skipped due to configuration)
Action is Encrypt & Deliver
Action is Bounce
Action is Drop
Action is Deliver
All other actions
Action is Skip Outbreak Filters
Do the outbreak filters indicate an outbreak is present?
No, OR Yes and message is modified
Yes, message is quarantined
If the message is not spam, virus, and threat positive, add graymail safe unsubscribe banner (May be skipped due to configuration)
Yes, action is quarantine
(Outbound) Does the DLP Engine detect a DLP violation?
Yes, action is Drop
Action is Deliver
Send message to quarantine
Encrypt and deliver message
Bounce Message
Drop Message
Start SMTP client conversation
Deliver Message

图 *3:* 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。

相关主题

- 主机访问表 (HAT)、发件人组和邮件流策略， 第 5 页
- Received: 信头， 第 5 页
- 默认域， 第 5 页
- 退回验证， 第 5 页
- 域名Map， 第 6 页

• 收件人访问表 (RAT)，第 6 页
• 别名表，第 6 页
• LDAP 收件人接受，第 6 页
• SMTP Call-Ahead 收件人验证，第 6 页

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。

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 Received: 信头。

有关详细信息，请参阅使用侦听程序。

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。

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。

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。

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。

别名表

别名表提供一种将邮件重定向到一个或多个收件人的机制。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。

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。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丢弃邮件。

有关详细信息，请参阅处理 LDAP 查询。

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）继续会话或丢弃连接。

有关详细信息，请参阅使用 SMTP 服务器验证收件人

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、病毒爆发过滤器和隔离。

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。

相关主题

- 邮件管道和安全服务，第 7 页
- LDAP 收件人接受，第 6 页
- 伪装或 LDAP 伪装，第 8 页
- LDAP 路由，第 8 页
- 邮件过滤器，第 8 页
- 邮件安全管理器（按收件人扫描），第 8 页
- 隔离区，第 10 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，而且在从隔离区放行之前，邮件策略已更新为包括防病毒扫描，则该邮件从隔离区放行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。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丢弃邮件。

有关详细信息，请参阅处理 LDAP 查询。

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。

有关通过 LDAP 查询进行伪装的详细信息，请参阅处理 LDAP 查询。

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。

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。

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 ， 第 8 页
- 反垃圾邮件 ， 第 9 页
- 防病毒 ， 第 9 页
- 灰色邮件检测和安全取消订阅 ， 第 9 页
- 文件信誉扫描和文件分析 ， 第 9 页
- 内容过滤器 ， 第 9 页
- 病毒爆发过滤器 ， 第 10 页

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。

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，请参阅管理垃圾邮件和灰色邮件。

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
- 丢弃附件
- 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 10 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。

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，请参阅管理垃圾邮件和灰色邮件。

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：

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。

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。

对“病毒爆发”(Outbreak)隔离区中邮件的处理方式与任何其他隔离区中邮件的处理方式相同。有关隔离区和工作队列的详细信息，请参阅隔离区，第 10 页。

有关详细信息，请参阅病毒爆发过滤器。

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。

相关主题

- 策略、病毒和病毒爆发隔离区
- 垃圾邮件隔离区

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。

相关主题

- 虚拟网关，第 11 页
- 传送限制，第 11 页
- 基于域的限制，第 11 页
- 基于域的路由，第 11 页
- 全局取消订阅，第 11 页
- 退回限制，第 11 页

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。

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。

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。

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。

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。

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。