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

建议您避免添加、更改或删除思科安全邮件云网关上的侦听程序。

该邮件网关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。该邮件网关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”）。

该邮件网关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，侦听程序还定义邮件网关如何与尝试向邮件网关发送邮件的系统通信。

可以创建以下类型的侦听程序：

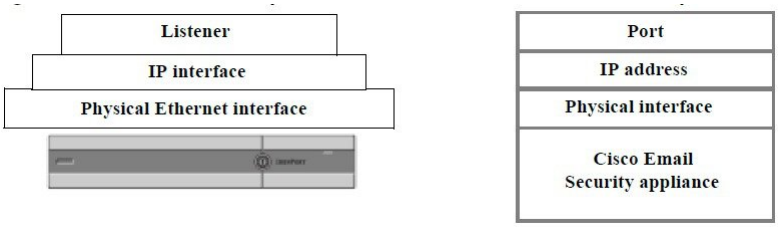
- **公共云**，侦听并接受来自互联网的邮件。公共侦听程序接收来自许多主机的连接，并将邮件定向到有限数量的收件人。
- **私有云**，侦听并接受来自网络内的系统（通常来自内部组件和邮件服务器 (POP/IMAP)）、计划发送给互联网中网络外部的收件人的邮件。专用侦听程序接收来自有限（已知）数量的主机的连接，并将邮件定向到很多收件人。

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, on page 2。
- **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。
- **（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。

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。这使邮件网关能在连接关闭之前拦截垃圾邮件主机。

Figure 1: 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, on page 4。

在使用和配置邮件网关上的侦听程序时，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，将在邮件网关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 IP 信誉得分值。

- **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。
- 为了帮助测试邮件网关和排除故障，可以创建“sinkhole”类型的侦听程序，而不是公共或专用侦听程序。当创建 sinkhole 侦听器时，您可以选择是否在删除邮件前将其写入磁盘。（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邮件网关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邮件网关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邮件网关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邮件网关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。

Figure 2: 多种型号具有两个以上以太网接口的邮件网关上的公共和专用侦听程序

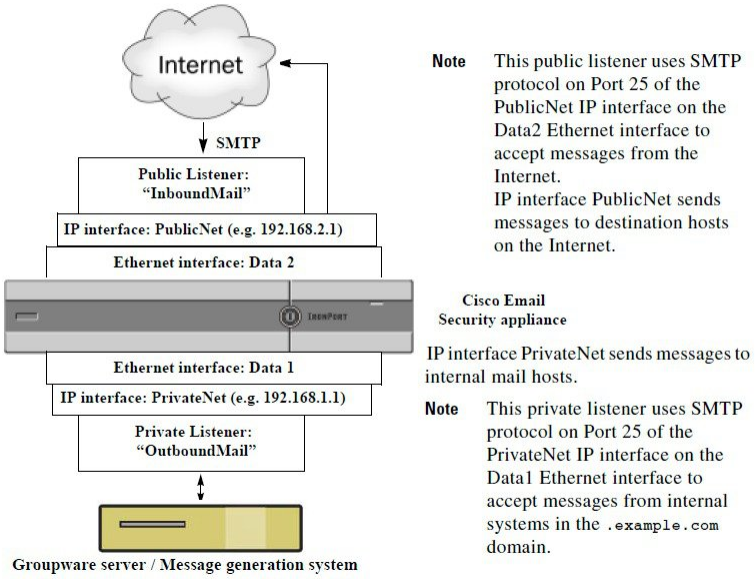
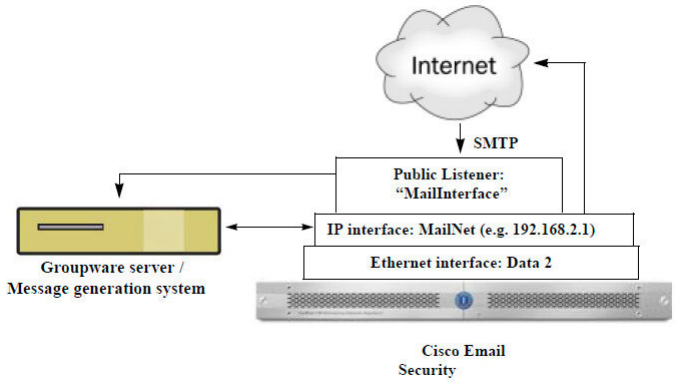


Figure 3: 多种型号仅有两个以太网接口的邮件网关上的公共侦听程序



Note 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邮件网关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。

Procedure

步骤 1 依次选择**网络 (Network)** > **侦听程序 (Listeners)**。

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

步骤 3 更改下表中定义的设置。

Table 1: 侦听程序全局设置

全局设置	说明
最大并发连接数 (Maximum Concurrent Connections)	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为 300，则 IPv4 和 IPv6 连接的总和不能超过 300。
最大并发 TLS 连接数 (Maximum Concurrent TLS Connections)	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为 100，则 IPv4 和 IPv6 TLS 连接的总和不能超过 100。

全局设置	说明
注入计数器重新设置时间 (Injection Counters Reset Period)	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。
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。
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，邮件网关将尝试断开连接，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。

全局设置	说明
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。

What to do next

相关主题

- 包含多种编码的邮件设置, on page 6

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邮件网关的行为：

- 信头
- 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。

Note 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。

通过使用 Web 界面创建侦听程序侦听连接请求

Procedure

步骤 1 依次选择网络 (Network) > 侦听程序 (Listener)。

步骤 2 单击**添加侦听程序 (Add Listener)**。

步骤 3 配置下表中定义的设置。

Table 2: 侦听程序设置

名称	您提供给侦听器的唯一昵称以供将来参考。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 (Interface)	选择要在其上创建侦听程序的已配置邮件网关 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 (Bounce Profile)	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）。
免责声明在上方 (Disclaimer Above)	选择免责声明附于邮件上方或下方（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）。
免责声明在下方 (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 (SMTP Authentication Profile)	指定 SMTP 身份验证配置文件。
证书 (Certificate)	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）。

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邮件网关遵守 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 (Maximum Concurrent Connections)	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。
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 (Add Received Header)	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。 **Note** “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： • **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。单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。

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“账户搜集攻击预防”(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。
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。
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 From 或 CC 信头地址。 有关详细信息，请参阅LDAP 查询概述。
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。

步骤 7 提交并确认更改。

What to do next

相关主题

部分域、默认域和格式不正确的 MAIL FROM, on page 11

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。

Table 3: 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`
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，请参阅适用于思科安全邮件网关的 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。

相关主题

高级 HAT 参数, on page 12

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。无字母的值会被视作字节。标有星号的参数支持下表中所示的变量语法。

Table 4: 高级 ***HAT*** 参数语法

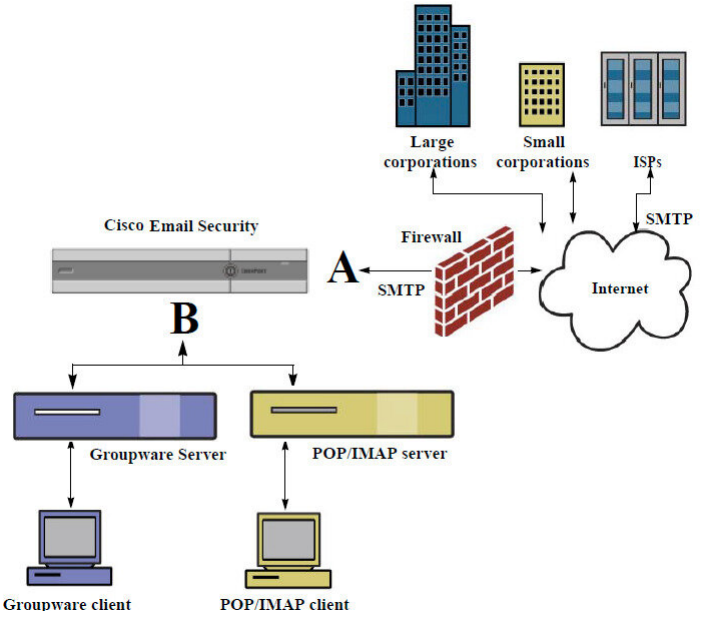
参数	语法	值	示例值
每个连接的最大邮件数 (Maximum messages per connection)	`max_msgs_per_session`	编号	`1000`
每封邮件的最大收件人数 (Maximum recipients per message)	`max_rcpts_per_msg`	编号	`10000` `1k`
最大邮件大小 (Maximum message size)	`max_message_size`	编号	`1048576` `20M`
此侦听程序允许的最大并发连接数量 (Maximum concurrent connections allowed to this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

参数	语法	值	示例值
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 IP 信誉得分 (Define SenderBaseIP 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。

Figure 4: 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的邮件网关上配置了一个公共侦听器 (A) 和一个专用侦听器 (B)。