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 IP 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, on page 2。
- **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, on page 7

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。

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, on page 10。

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邮件网关，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, on page 20。

相关主题

- 默认 HAT 条目, on page 2

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。

Note 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
- IP 信誉服务“组织”分类
- IP 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, on page 3。

当 SMTP 服务器尝试与邮件网关建立 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 IP 信誉得分、域或 IP 地址）时将连接分配给发件人组。

Note 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。

相关主题

- 发件人组语法, on page 3
- 网络所有者、域和 IP 地址定义的发件人组, on page 4
- 按 IP 信誉得分定义发件人组, on page 6
- 通过查询 DNS 列表定义的发件人组, on page 7

发件人组语法

Table 1: 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

`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

语法	含义
.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]	IP 信誉得分。有关详细信息，请参阅按 IP 信誉得分定义发件人组, on page 6。
SBO:n	网络所有者标识号。有关详细信息，请参阅按 IP 信誉得分定义发件人组, on page 6。
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, on page 7。
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，IP 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。邮件网关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。

相关主题

- 根据 HAT 设置策略, on page 5

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。

Table 2: 网络所有者和组织示例

示例类型	网络所有者	组织
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。IP 信誉服务对于细化到组织级别的邮件源具有独特的了解，而邮件网关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“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，则邮件网关对于 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 IP 信誉服务获得。IP 信誉服务提供有关发件人相对规模（ 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，应为其分配更多与邮件网关的连接。
  - 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邮件网关连接的组织。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邮件网关的连接。

邮件流监控功能使用其在 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 IP 信誉得分定义发件人组

邮件网关可以查询 IP 信誉服务来确定 IP 信誉得分。IP 信誉得分是根据 IP 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。

***Table 3: IP* 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
无	没有适用于此发件人的数据（通常是垃圾邮件的来源）

使用 IP 信誉得分，可以将邮件网关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 , on page 12。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 IP 信誉得分的语法。

***Table 4: IP* 信誉得分的语法**

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

Note 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 IP 信誉服务中的唯一标识号。

使用**网络 (Network) > 侦听程序 (Listeners)** 页面或 CLI 中的 `listenerconfig -> setup` 命令来查询 IP 信誉服务。还可以定义在查询 IP 信誉服务时邮件网关应等待的超时值。然后，可以在 GUI 中使用“邮件策略”(Mail Policies) 页面的值或在 CLI 中使用 `listenerconfig -> edit -> hostaccess` 命令配置不同的策略来查询 IP 信誉服务。

Note 您还可以创建邮件过滤器来指定 IP 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，请参阅反垃圾邮件和防病毒章节中的“IP 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。

Note 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）

Note 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 ALLOWED_LIST 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。

Note 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。

- **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 , on page 12。

相关主题

- HAT 变量语法, on page 8

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。）

***Table 5: 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	仅在经过邮件网关验证后，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）。 如果邮件网关无法获取 SenderBase 组织 ID，或者如果 IP 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。

相关主题

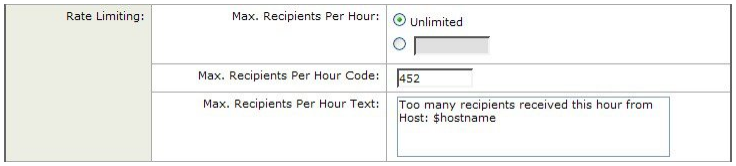
- 使用 HAT 变量, on page 9
- 测试 HAT 变量, on page 9

使用 HAT 变量

Note 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。

Figure 1: 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 地址添加到邮件网关上侦听程序的 $ALLOWED_LIST 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: ALLOWED_LIST, 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。

Table 6: 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
ALLOWED_LIST	将您信任的发件人添加到 Allowed_list 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
BLOCKED_LIST	Blocked_list 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。 • 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。如果此参数过于积极，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 IP 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。有关IP信誉服务方面的详细信息，请参阅IP 信誉服务。	$ACCEPTED
ALL	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, on page 2。	$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。

Table 7: 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。 **Note** 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
ALL	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, on page 2。	$BLOCKED

Note 在仅有两个以太网端口的邮件网关型号上运行“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邮件网关型号，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。

相关主题

- 创建发件人组用于邮件处理 , on page 12
- 将发件人添加到现有发件人组, on page 13
- 重新排列对传入连接所执行规则的顺序, on page 13
- 搜索发件人, on page 14
- 使用邮件流策略定义邮件发件人的访问规则, on page 7
- 定义邮件流策略的默认值, on page 19

创建发件人组用于邮件处理

Procedure

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。

Note 如果您不知道要应用到此发件人组的邮件流策略（或者还没有邮件流策略存在），则使用默认的“继续（无策略）”(CONTINUE [no policy]) 邮件流策略。

步骤 8 （可选）选择一个 DNS 列表。

步骤 9 （可选）包括 IP 信誉得分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, on page 28。

步骤 12 点击**提交 (Submit)** 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 (Add Sender)** 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 (IP Addresses)**，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 (Geolocation)**，选择国家/地区，然后提交更改。

步骤 15 提交并确认更改。

What to do next

相关主题

- 编辑侦听程序的 IP 信誉过滤得分阈值

将发件人添加到现有发件人组

Procedure

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。

Note 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”(Add to Sender Group) 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, on page 3。

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。

What to do next

相关主题

- 避免垃圾邮件过滤器过滤邮件网关生成的邮件
- 如何配置邮件网关以扫描垃圾邮件

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。

Procedure

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 ALLOWED_LIST、BLOCKED_LIST、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”(HAT Overview) 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“查找”(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“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, on page 19。
- 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。）

Procedure

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 (Add Policy)**。

步骤 3 输入下表中描述的信息。

Table 8: 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。

参数	说明
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 横幅	
自定义 SMTP 横幅代码	当与此侦听程序建立连接时，返回的 SMTP 代码。
自定义 SMTP 横幅文本	当与此侦听程序建立连接时，返回的 SMTP 横幅文本。 **Note** 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, on page 8。
自定义 SMTP 拒绝横幅代码	当此侦听程序拒绝连接时，返回的 SMTP 代码。
自定义 SMTP 拒绝横幅文本	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，邮件网关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	
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。 **Note** 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, on page 8。
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	

参数	说明
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, on page 21。
流量控制	
使用 SenderBase 控制流量	为此侦听程序启用对 IP 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。定义一个有效位范围（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。
目录搜集攻击预防 (DHAP)	
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。
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，则邮件网关会放弃与主机的连接。

参数	说明
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。
发件人域信誉验证	
发件人域信誉验证	启用发件人域信誉验证。
加密和身份验证	
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，邮件网关会拒绝连接，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) 选项会指导邮件网关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，邮件网关仍允许非 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，邮件网关才能允许连接。 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, on page 21。 有关将客户端证书用于 TLS 连接的信息，请参阅从邮件网关建立 TLS 连接。

参数	说明
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，请参阅邮件验证。
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，请参阅邮件验证。
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。
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。

参数	说明
DMARC 反馈报告	启用发送 DMA RC 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。 **Note** 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，则邮件网关会接受退回邮件。
信封发件人 DNS 验证	
	请参阅验证发件人, on page 24。
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, on page 26。

Note 如果在HAT中全局启用了反垃圾邮件扫描或防病毒扫描，则邮件网关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

Procedure

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, on page 14。

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的邮件网关，从而覆盖所有现有主机访问表信息。

相关主题

- 将主机访问表配置导出到外部文件, on page 20
- 从外部文件导入主机访问表配置, on page 20

将主机访问表配置导出到外部文件

Procedure

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。这是在邮件网关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。

Procedure

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。

Note 要导入的文件必须在邮件网关的配置目录中。

步骤 5 点击**提交 (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**导入 (Import)**。

步骤 7 确认您的更改。

可以在文件中加入“注释”。以“#”字符开头的行会被视作注释并会被 AsyncOS 忽略。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) 页面会显示邮件网关中的所有地址列表，以及使用地址列表的任何邮件流策略。

Procedure

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**仅限完整的邮件地址 (Full Email Addresses only)**。

步骤 6 选择以下选项之一来创建地址列表：

- 如果要强制在地址列表中使用完整邮件地址，请选择**仅限完整的邮件地址 (Full Email Addresses only)**。
- 如果要强制在地址列表中使用域，请选择**仅限域 (Domains only)**。
- 如果要强制在地址列表使用 IP 地址，请选择**仅限 IP 地址 (IP Addresses only)**。

步骤 7 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@`

  Note 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 8 提交并确认更改。

SenderBase 设置和邮件流策略

为了分类与邮件网关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, on page 4。

“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。）

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 IP 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 有效位功能。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，IP 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。

相关主题

- HAT 有效位功能, on page 22

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。

Note 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 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 , on page 23
- 有效位元 HAT 策略选项 , on page 23
- 注入控制周期性 , on page 23

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”(Mail Policies) > “邮件流策略”(Mail Flow Policies) 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 Cisco Secure Email Gateway的 AsyncOS 的 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）。

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 Cisco Secure Email Gateway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 查找的连接过滤）还可帮助减少通过邮件网关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，以便确定邮件网关如何处理来自未经验证的发件人的邮件：例如，可将邮件网关配置为在 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, on page 24。
- **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, on page 25。

相关主题

- 发件人验证：主机, on page 24
- 发件人验证：信封发件人, on page 25
- 实施发件人验证 - 设置示例, on page 27
- 为来自未经验证的发件人的邮件测试设置, on page 30
- 发件人验证和日志记录, on page 31

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。

邮件网关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，邮件网关将检查 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 记录查找由于临时 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”(Connecting Host DNS Verification) 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, on page 28）。

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 ALLOWED_LIST 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 ALLOWED_LIST 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。

Note 如果 DNS 响应为“ NOERROR”则发件人验证会拒绝没有 MX 记录的域。

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，因为发送到MAIL FROM地址的退回邮件无法发送。使用信封发件人验证，可将邮件网关配置为拒绝 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, on page 26）。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）。

相关主题

- 部分域、默认域和格式不正确的 MAIL FROM, on page 26
- 自定义 SMTP 代码和响应, on page 26
- 发件人验证：信封发件人, on page 25

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。

这些功能相互排斥。

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。每个邮件网关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”(Mail Policies) >“例外表”(Exception Table) 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, on page 29）或 CLI（请参阅《适用于*Cisco Secure Email Gateway* 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, on page 29。

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：

Table 9: 发件人验证：建议的设置

发件人组	策略	包含
UNVERIFIED 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 查找 (PTR) 与正向 DNS 查找 (A) 不匹配。
	ACCEPTED	SMTP 会话期间的信封发件人验证： - 格式错误的 MAIL FROM - 信封发件人在 DNS 中不存在。 - 信封发件人 DNS 无法解析。

相关主题

- 使用 SUSPECTLIST 发件人组限制来自未经验证的发件人的邮件, on page 28
- 对未经验证的发件人实施更严格的限制设置, on page 28
- 定义邮件以使用 ACCEPTED 邮件流策略发送到未经验证的发件人, on page 29
- 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, on page 29
- 在发件人验证例外表中搜索地址, on page 29

使用 SUSPECTLIST 发件人组限制来自未经验证的发件人的邮件

Procedure

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 查找 (PTR) 不匹配正向 DNS 查找 (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

Procedure

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

Procedure

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**开 (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

Procedure

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

Note 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

Procedure

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**查找 (Find)**。

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，可以验证邮件网关设备的行为了。

请注意，测试 DNS 相关的设置不属于本文档的讨论范围。

相关主题

- 发送 MAIL FROM 发件人地址格式不正确的测试邮件, on page 30
- 从发件人验证规则中排除的地址发送邮件, on page 30

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。

Procedure

步骤 1 打开与邮件网关的 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。

Note 如果将邮件网关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：

Procedure

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 打开与邮件网关的 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。

相关主题

- 信封发件人验证, on page 31

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
```

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。