# 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）。

邮件网关将本地域的邮件路由到通过**网络 (Network) > SMTP 路由 (SMTP Routes)** 页面（或 `smtproutes` 命令）指定的主机。此功能类似于 sendmail `mailertable` 功能。

**Note** 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，即在邮件网关中为当时输入的每个 RAT 条目定义了第一个 SMTP 路由条目。

相关主题



# 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邮件网关配置四万 (40,000) 个 SMTP 路由映射。（请参阅SMTP 路由限制, on page 3）

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。

如果未在 SMTP 路由表中找到主机，则使用 DNS 执行 MX 查找。系统不会比照 SMTP 表重新检查结果。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。

每次传送邮件时，从上到下阅读 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。您不能删除默认 SMTP 路由；您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。当您创建新的路由时，首先指定要为其创建永久路由的域或不完整域，然后，指定目标主机。目标主机可以输入为完全限定的主机名或 IP 地址。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` 可确保不会再传送邮件网关收到的邮件。）

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 可指示邮件网关执行 MX 查找，确定特定域接下来的跳跃。当您需要将子域的邮件路由到某台特定主机时，此功能非常有用。例如，如果将发往 example.com 的邮件发送到公司的 Exchange 服务器，您可能会看到类似于以下 SMTP 路由的地址：

example.com exchange.example.com

但对于发送到不同子域 (foo.example.com) 的邮件，请添加如下所示的 SMTP 路由：

.example.com USEDNS

# SMTP 路由和警报

从邮件网关发送到通过“系统管理”(System Administration) > “警报”(Alerts) 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：工作原理相似，但如果将一封邮件发送到 10 个不同的域中的 10 位收件人，则 AsyncOS 将打开与 10 个 MTA 的 10 个连接，并向每个 MTA 传送一封邮件。

拆分：如果一封传入邮件有 10 位收件人并且每位收件人分别属于单独的传入策略组（10 个组），则邮件会进行拆分，即使这 10 位收件人均位于同一台 Exchange 服务器上也是如此。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，即可在邮件网关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。

# 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) 页面管理邮件网关。在表中添加、修改和删除映射。可以导出或导入 SMTP 路由条目。

### 相关主题


- 添加 SMTP 路由, on page 4
- 导出 SMTP 路由, on page 5
- 导入 SMTP 路由, on page 5


## 添加 SMTP 路由

**Procedure**

**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。

**Note** 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, on page 3。

**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，您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：

### Procedure

**步骤 1** 在“SMTP 路由”(SMTP Routes) 页面上点击**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，您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：

### Procedure

**步骤 1** 在“SMTP 路由”(SMTP Routes) 页面上点击**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**提交 (Submit)**。您会收到导入将替换所有现有 SMTP 路由的警告。文本文件中的所有 SMTP 路由均会导入。

**步骤 4** 点击**导入 (Import)**。

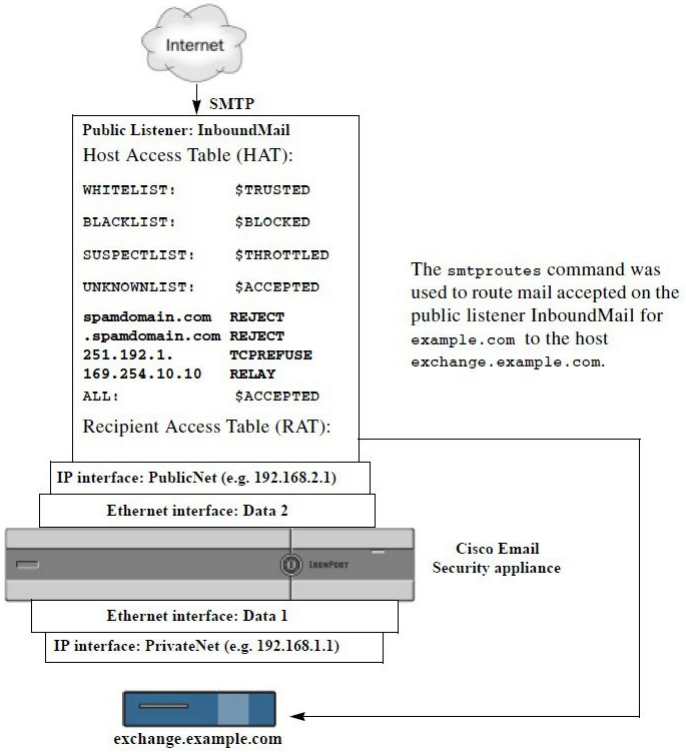
可以在文件中加入“注释”。以“#”字符开头的行会被视作注释并会被 AsyncOS 忽略。例如：

```
# this is a comment, but the next line is not

ALL:
```

### What to do next

此时，我们的“邮件网关”(Email Gateway) 配置类似于以下：

***Figure 1:*** 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。

***Table 1:*** 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, on page 7） | • 仅信封收件人<br>• 适用于全局范围<br>• 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, on page 24） | • 仅信封收件人<br>• 按侦听程序应用 |

| 原始地址 | 切换到 | 特性 | 作用范围 |
|---|---|---|---|
| *@olddomain | *@newdomain | 伪装（请参阅配置伪装, on page 14） | • 信封发件人以及“收件人:”、“发件人:”和/或“抄送:”信头<br>• 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。

**Note** 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。

**Note** 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, on page 30），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。

### 相关主题


- 从命令行配置别名表, on page 7
- 导出和导入别名表 , on page 8
- 从别名表中删除条目, on page 9


# 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：

***Table 2:*** 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。

### 相关主题

- 别名表示例, on page 9
- aliasconfig 命令示例, on page 11

# 导出和导入别名表

要导入别名表，请先参阅FTP、SSH 和 SCP 访问以确保可以访问该邮件网关。

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

**Note** 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。

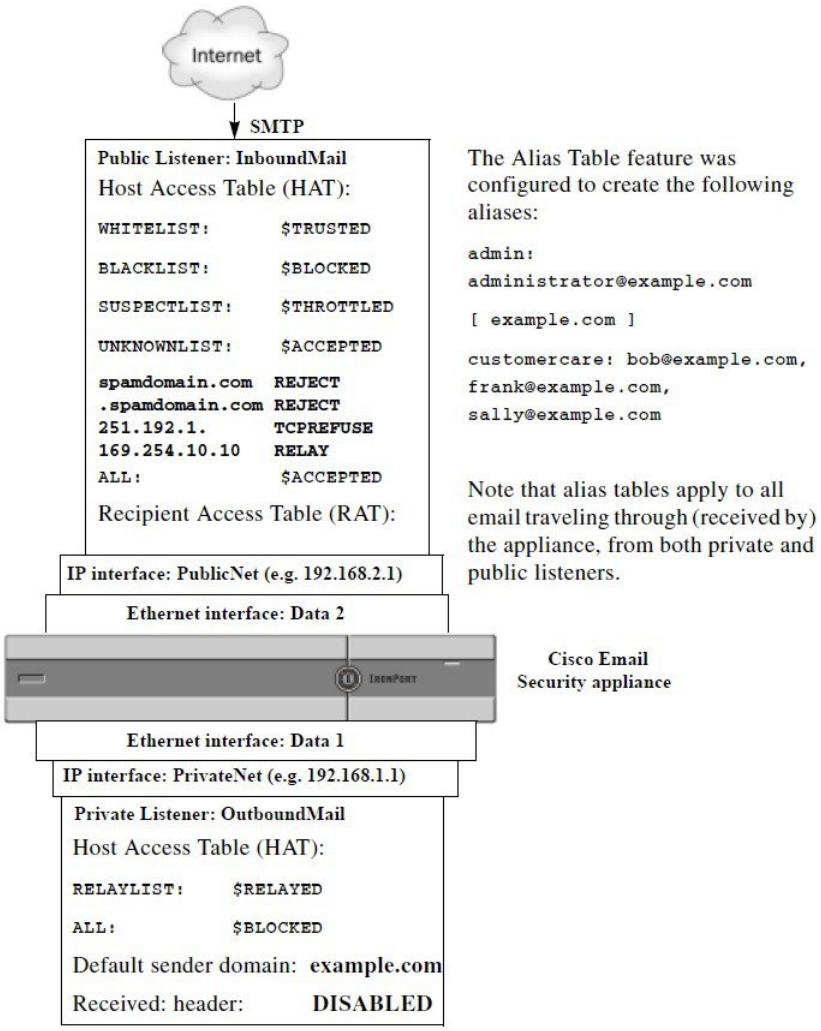
```
mail3.example.com> aliasconfig
No aliases in table.
Choose the operation you want to perform:
- NEW - Create a new entry.
- IMPORT - Import aliases from a file.
[]> new

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：

***Figure 2:*** 为邮件网关定义的别名表




# 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。

**Note** “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。

### 相关主题

- 伪装和 altsrchost, on page 15

# 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 Virtual Gateway™ 技术为所有托管的域配置邮件网关, on page 53和回顾：邮件管道, on page 65。

### 相关主题

- 配置静态伪装表, on page 15
- 专用侦听程序的伪装表示例, on page 16
- 导入伪装表 , on page 16
- 伪装示例 , on page 17

## 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 , on page 16。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。

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：

***Table 3:*** 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。 | |
| 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。<br>**Note** 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 访问以确保可以访问该邮件网关设备。

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。）

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.
```

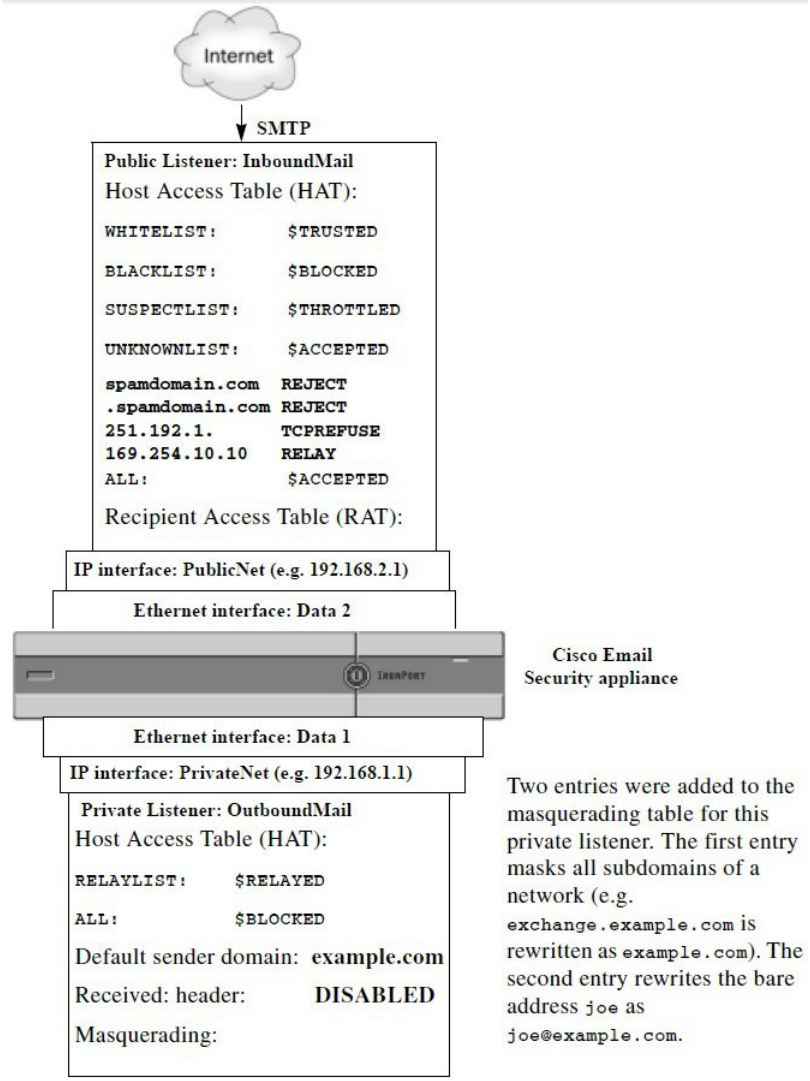
```
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]> export
Enter a name for the exported file:
[]> masquerade.txt
Export completed.
Domain Masquerading Table
There are currently 2 entries.
Masqueraded headers: To, From, Cc
Choose the operation you want to perform:
- NEW - 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：

***Figure 3:*** 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。

**Note** 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，您可以在邮件网关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。

**Note** 可以配置多达 20,000 个单独的唯一域映射。

***Table 4:*** 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**<br>或<br>**@example.net** | 完整地址或完全限定域名。 |
| `@.example.com` | **user@example.net**<br>或<br>**@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.

[]>
```

### 相关主题

- 导入和导出域映射表 , on page 29

# 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 访问以确保可以访问该邮件网关。

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
```

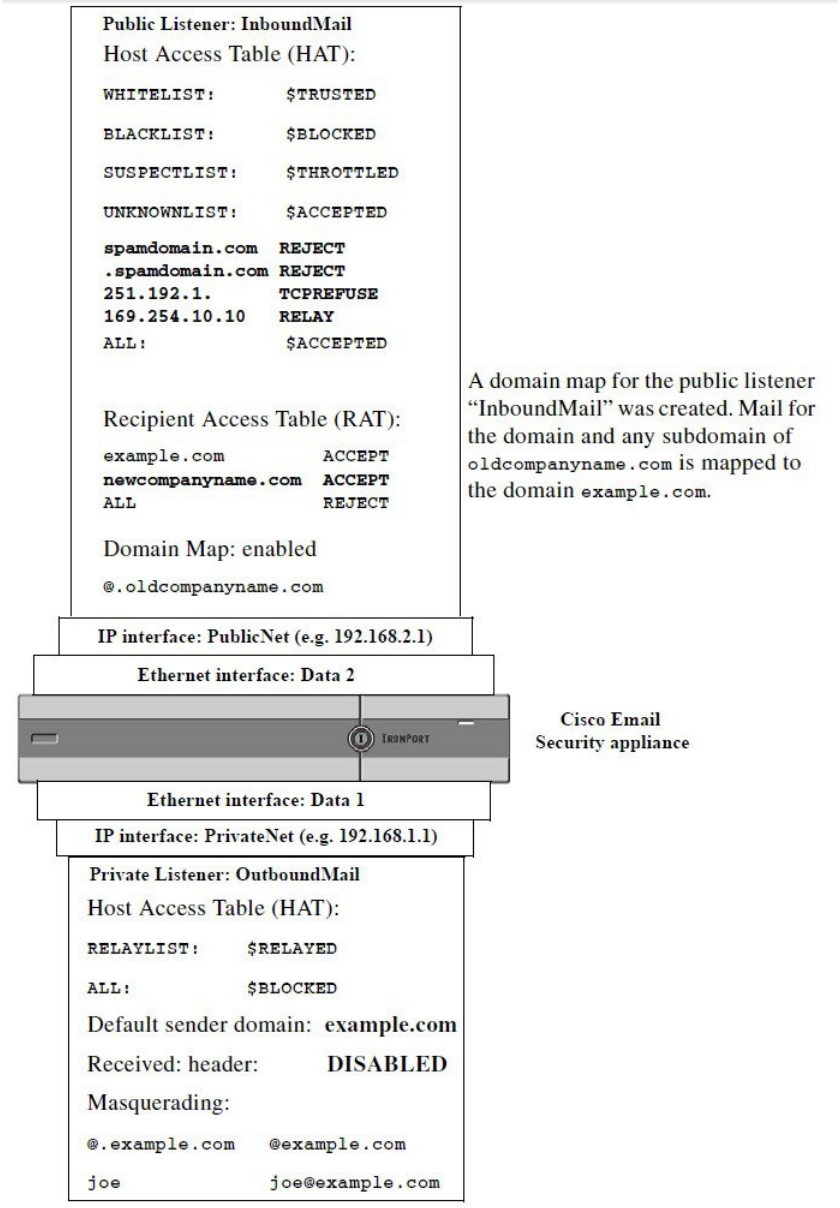
或者，可以使用 `export` 子命令下载现有配置。系统会将一个文件（您指定了其名称）写入配置目录。可以在 CLI 外修改此文件，然后再将其导入。

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：

*Figure 4:* 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。邮件网关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邮件网关生成外发退回的方式（根据传入邮件）。要控制邮件网关如何控制传入退回（基于外发邮件），请使用退回验证（请参阅退回验证, on page 39）。

### 相关主题

- 处理无法传送的邮件, on page 31
- 创建新的退回配置文件, on page 37
- 将退回配置文件应用到侦听程序, on page 37

# 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：**<br>**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：**<br>**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 (Web) > 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。（有关详细信息，请参阅使用邮件过滤器实施邮件策略。）

### 相关主题

- 有关软退回和硬退回的说明, on page 32
- 退回配置文件参数, on page 32
- 硬退回和状态命令, on page 35
- 会话退回和 SMTP 路由邮件过滤器操作, on page 35
- 退回配置文件示例, on page 35
- 传送状态通知格式, on page 36
- 延迟警告邮件, on page 36
- 延迟警告邮件和硬退回, on page 37

# 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”(Bounce Profiles) 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, on page 32。）
- 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。

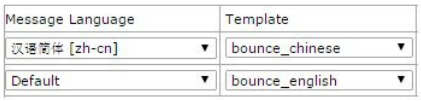
# 退回配置文件参数

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：

***Table 5:*** 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 (Send Hard Bounce Messages)** | 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)。<br><br>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。<br><br>在**通知模板 (Notification Template)** 下，点击**添加行 (Add Row)**，然后选择邮件语言以及要使用的模板。<br><br>**Note** 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。<br><br>在下列情况下，邮件语言被视为默认值：<br>• 如果邮件语言不同于在其他通知模板条目中所选的语言。<br>• 如果邮件网关不支持该邮件语言。<br>• 如果邮件网关无法检测到邮件的语言。<br>• 如果邮件内容（主题和正文）少于 50 字节。<br><br>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：<br><br>  <br><br>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”(Yes)，则邮件网关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 (Send Delay Warning Messages)** | 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。<br>在**通知模板 (Notification Template)** 下，点击**添加行 (Add Row)**，然后选择邮件语言以及要使用的模板。<br>**Note** 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。<br>在下列情况下，邮件语言被视为默认值：<br>• 如果邮件语言不同于在其他通知模板条目中所选的语言。<br>• 如果邮件网关不支持该邮件语言。<br>• 如果邮件网关无法检测到邮件的语言。<br>• 如果邮件内容（主题和正文）少于 50 字节。<br>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：<br>  <br><br>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。 |
| 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` 命令编辑默认回退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，<br>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邮件网关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。

**Note** 邮件信封的信封发件人地址与邮件信头中的 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邮件网关现生成的SMTP退回邮件。当邮件网关现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，邮件网关现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：

*Table 6:* 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 |
| 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，即在邮件注入邮件网关后立即进行。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。

*Table 7:* 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”(Network) 菜单上的“退回配置文件”(Bounce Profiles) 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，邮件网关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。

### 相关主题

- 编辑默认退回配置文件, on page 37
- Minimalist 退回配置文件示例, on page 37

## 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。

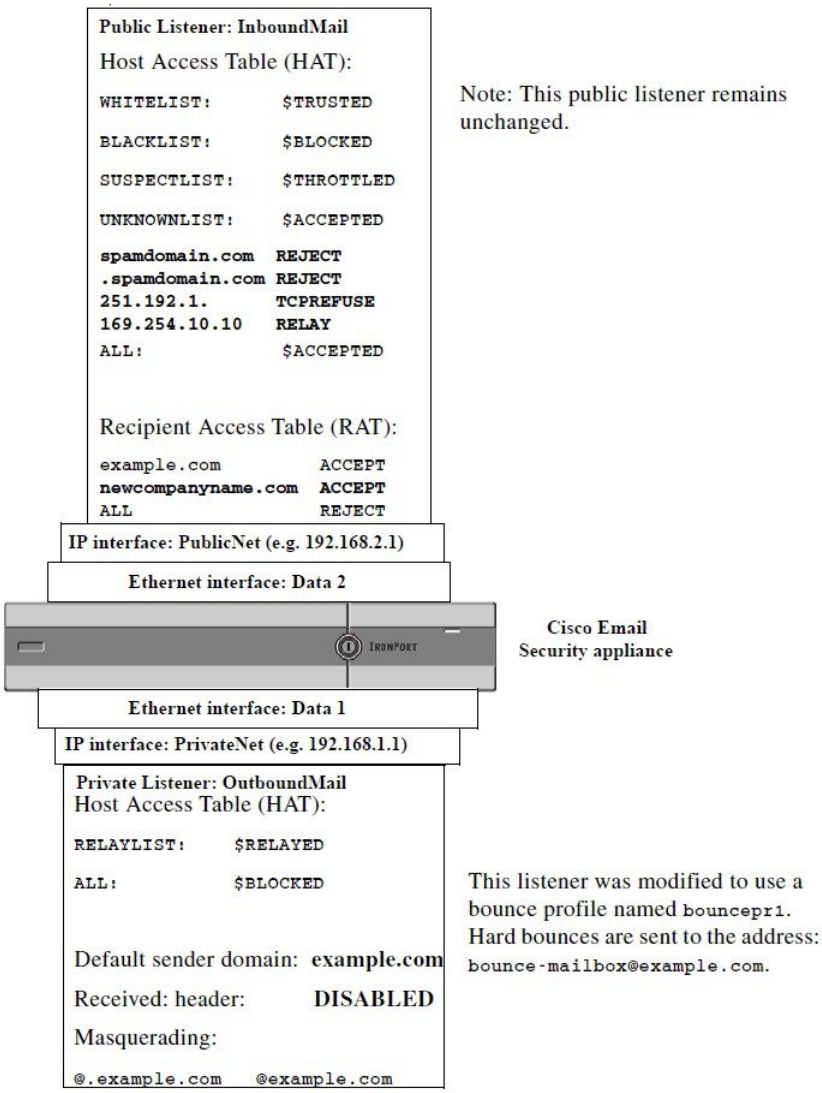
# 将退回配置文件应用到侦听程序

创建退回配置文件后，可以使用**网络 (Web) > 侦听程序 (Listeners)**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：

*Figure 5:* 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 通过定义邮件网关将打开的连接数量或邮件网关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, on page 39
- TLS, on page 39
- 退回验证, on page 39
- 退回配置文件, on page 39

# 速率限制

- 并发连接数 (Concurrent Connections)：邮件网关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)：邮件网关在其启动新的连接之前，将发送到目标域的邮件数。
- 收件人 (Recipients)：邮件网关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, on page 42）。
- 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, on page 47）。

# 退回配置文件

- 设备将哪个退回配置文件供邮件网关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。

### 相关主题

- 确定使用哪个接口传送邮件, on page 39
- 默认传送限制, on page 40
- 使用目标控制, on page 40

# 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”(Mail Policies) > “目标控制”(Destination Controls) 页面或 CLI 中的 destconfig 命令创建、编辑和删除目标控制条目。

### 相关主题


- 控制互联网协议地址的版本, on page 40
- 控制域的连接、邮件和收件人数量, on page 40
- 控制 TLS, on page 42
- 控制退回验证标记, on page 43
- 控制退回, on page 43
- 添加新的目标控制条目, on page 43
- 导入和导出目标控制配置, on page 43
- 目标控制和 CLI, on page 47


## 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。邮件网关支持互联网协议版本 4 (IPv4) 和版本 6 (IPv6)。可以在邮件网关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，邮件网关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，邮件网关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，以避免来自邮件网关的邮件使远程主机或您自己的内部组件服务器负载过重。

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 (Mail Policies) > 目标控制 (Destination Controls)**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。系统级的限制控制邮件网关允许的总连接数。）

您还可以设置是否为整个域强制执行定义的限制。

**Note** 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。

***Table 8:*** 目标控制表中的值

| 字段 | 说明 |
|---|---|
| 并发连接数 (Concurrent Connections) | 邮件网关与指定主机建立的最大出站连接数。（请注意，域可包含内部组件主机。） |
| 每个连接的最大邮件数 (Maximum Messages Per Connection) | 在发起新的连接之前，允许从邮件网关到指定主机的单个出站连接发送的最大邮件数。 |
| 收件人 (Recipients) | 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。<br>邮件网关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。<br>**Note** 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。邮件网关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。<br>此设置会应用到连接、邮件和收件人限制。<br>指定限制将应用到系统级还是每个虚拟网关地址。<br>**Note** 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 Virtual Gateway™ 技术为所有托管的域配置邮件网关, on page 53。 |

**Note** 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，则会该域协商从邮件网关侦听程序到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。

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，邮件网关是否发送警报。警报邮件包含失败TLS协商的目标域名称。邮件网关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”(System Administration)>“警报”(Alerts)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”(Destination Controls)页面上的**编辑全局设置 (Edit Global Settings)** 或使用 destconfig -> setup 子命令。此设置为全局设置，而不是按域的设置。有关邮件网关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。

必须指定用于所有传出 TLS 连接的证书。您可以在 Web 界面中编辑“默认”目标控制条目，或在 CLI 中使用 `destconfig > setup` 子命令指定要用于所有目标控制的证书。有关获取证书的信息，请参阅证书的使用。

您还可以为特定域选择除“默认”目标控制条目中配置的证书以外的其他证书。

您可以通过以下方式之一选择不同证书：

- 编辑相应的目标控制条目，并使用 Web 界面中的**TLS 证书** 选项选择其他证书。
- 在创建或编辑目标控制条目时，使用 `destconfig > 新建` 或 `编辑` 子命令选择证书。

**Note** 您最多可以创建 100 个目标控制条目，其证书与“默认”目标控制条目中配置的证书不同。

有关警报的详细信息，请参阅“系统管理”一章。

### 相关主题

- 在发件人或收件人级别对传出邮件实施 TLS, on page 42

## 在发件人或收件人级别对传出邮件实施 TLS

现有的“目标控制”(Destination Controls)配置允许您按域覆盖TLS模式（例如TLS强制、TLS首选等）。

如果需要根据其他条件（例如发件人、收件人等）对传出邮件实施 TLS，您现在可以使用 **X-ESA-CF-TLS-Mandatory** 信头。

您可以配置“内容过滤器 - 添加/编辑信头”(Content Filter – Add/Edit Header) 操作，以根据任何内容过滤器条件在“信头名称：”(Header Name:) 字段中添加 **X-ESA-CF-TLS-Mandatory** 信头，并将内容过滤器附加到传出邮件策略。

有关如何配置“内容过滤器 - 添加/编辑信头”(Content Filter – Add/Edit Header) 操作以添加“**X-ESA-CF-TLS-Mandatory**”信头的详细信息，请参阅内容过滤器操作。

## 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, on page 47。

## 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, on page 37。

## 添加新的目标控制条目

**Procedure**

**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邮件网关上。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邮件网关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。

***Table 9:*** 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。<br>输入以下其中一个值：<br>• PREFER_V6，表示“首选 IPv6”<br>• 对于“IPv6 必需”(IPv6 Required)，输入 REQUIRE_v6<br>• 对于“首选 IPv4”(IPv4 Preferred)，输入 PREFER_V4<br>• 对于“IPv4 必需”(IPv6 Required)，输入 REQUIRE_v4 |
| max_host_concurrency | 邮件网关与指定主机建立的最大出站连接数。<br>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，允许从邮件网关到指定主机的单个出站连接发送的最大邮件数。 |
| recipient_minutes | 邮件网关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。<br>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。<br>输入以下其中一个值：<br>• 0（或 host），表示域<br>• 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。<br>输入以下其中一个值：<br>• 0（或 system），表示系统范围<br>• 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。<br>输入以下其中一个值：<br>• 0（或 off）<br>• 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。<br>输入以下其中一个值：<br>• 0（或 off ）<br>• 1（或 on），表示“首选”<br>• 2（或 required），表示“必需”<br>• 3（或 on_verify），表示“首选（验证）”<br>• 4（或 require_verify），表示“所需（验证）”<br>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。<br>输入以下其中一个值：<br>• 0（或 off）<br>• 1（或 on）<br>这是全局设置，仅可在 [DEFAULT] 目标控制条目中使用。 |
| certificate | 用于传出TLS连接的证书。如果不指定证书，则使用 [DEFAULT] 目标控制条目中的证书。<br>**Note** 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]
certificate = 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)
TLS Certificate: example.com
Bounce Profile: tls_failed

example2.com

IP Address Preference: IPv6 Preferred
Maximum messages per connection: Default
Rate Limiting: Default
TLS: Preferred
TLS Certificate: example2.com
Bounce Profile: tls_failed
```

使用“目标控制”(Destination Controls) 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 《Cisco Secure Email Gateway AsyncOS CLI 参考指南》 中介绍了该命令。

# 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，退回验证会为通过邮件网关发送的邮件标记信封发件人地址。然后，会检查邮件网关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。要控制邮件网关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, on page 30。

#### 相关主题

- 概述：标记和退回验证, on page 47
- 使用退回验证防止退回邮件风暴, on page 49
- 接受合法的无标记退回邮件, on page 49

# 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，邮件网关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... 字符串是邮件网关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, on page 48）。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, on page 40）。

如果邮件已包含标记的地址，AsyncOS 不会添加另一个标记（以免邮件网关将退回邮件传送到 DMZ 中的一个邮件网关）。

### 相关主题

- 处理传入退回邮件, on page 48
- 退回验证地址标签密钥, on page 48

## 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。可以定义邮件网关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, on page 50。

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邮件网关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
```

**Note** 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邮件网关所使用的文本字符串。理想情况下，您将在所有邮件网关中使用相同的密钥，以便离开域的所有邮件一致地进行标记。这样，如果一个邮件网关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邮件网关接收也是如此。

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，邮件网关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”(No)，这表示没有标记的退回邮件被视为无效，并且邮件网关会拒绝该邮件或根据在**邮件策略 (Mail Policies) > 退回验证 (Bounce Verification)** 页面上选择的操作来应用客户信头。如果选择“是”(Yes)，邮件网关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）。

**Procedure**

**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

**Procedure**

**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, on page 49。

**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, on page 50。

**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, on page 40。

**What to do next**

相关主题

- 配置退回验证地址标记密钥, on page 49
- 配置退回验证设置, on page 50
- 使用 CLI 配置退回验证, on page 50
- 退回验证和集群配置, on page 50

## 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：

**Procedure**

步骤 1 在**邮件策略 (Mail Policies)** > **退回验证 (Bounce Verification)** 页面上，点击**新建密钥 (New Key)**。
步骤 2 输入文本字符串，然后点击**提交 (Submit)**。
步骤 3 **确认**更改。

**What to do next**

相关主题

- 清除密钥, on page 50

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。

**Procedure**

步骤 1 选择**邮件策略 (Mail Policies)** > **退回验证 (Bounce Verification)**。
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《*Cisco Secure Email Gateway 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，只要两个邮件网关使用同一个“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/密钥不特定于每个邮件网关。

# 设置邮件传送参数

deliveryconfig 命令会设置在从邮件网关传送邮件时使用的参数。

邮件网关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。

**Note** 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。

### 相关主题


- 默认传送 IP 接口, on page 51
- 可能的传送功能, on page 51
- 默认最大并发数, on page 51
- deliveryconfig 示例, on page 52


# 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

**Caution** 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，您的邮件网关将不符合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

还可以指定邮件网关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。

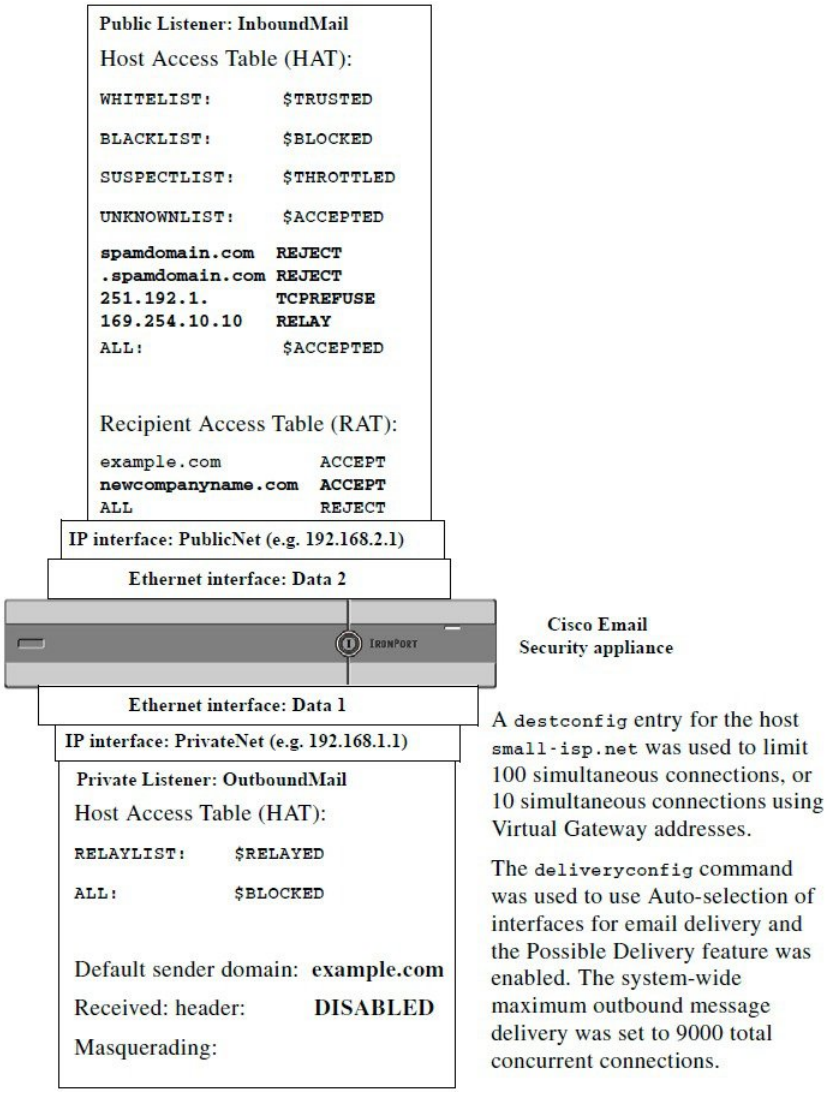
# deliveryconfig 示例

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"? [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：

*Figure 6:* 设置目标和传送参数




# 使用 Virtual Gateway™ 技术为所有托管的域配置邮件网关

本部分介绍 Cisco Virtual Gateway™ 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邮件网关中。所有邮件网关型号中的可用虚拟网关地址数都为 255。

## 相关主题

• 概述, on page 54

# 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邮件网关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。邮件网关具有智能，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，邮件网关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 查询中的 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，并且通常会删除该邮件。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。

### 相关主题



## 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”(Network) > “IP 接口”(IP Interfaces) 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。

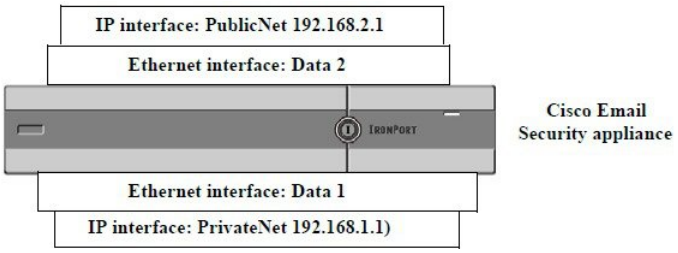
创建了所需的 IP 接口后，可以通过两个选项来设置虚拟网关地址并定义将从每个 IP 接口或接口组将发送哪些邮件活动：

- 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。（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“访问邮件网关”附录。

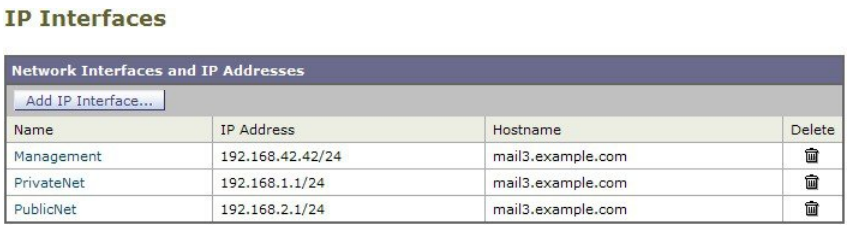
到目前为止，我们已将邮件网关配置与定义的以下接口配合使用，如下图中所示。

***Figure 7:*** 公共和专用接口示例



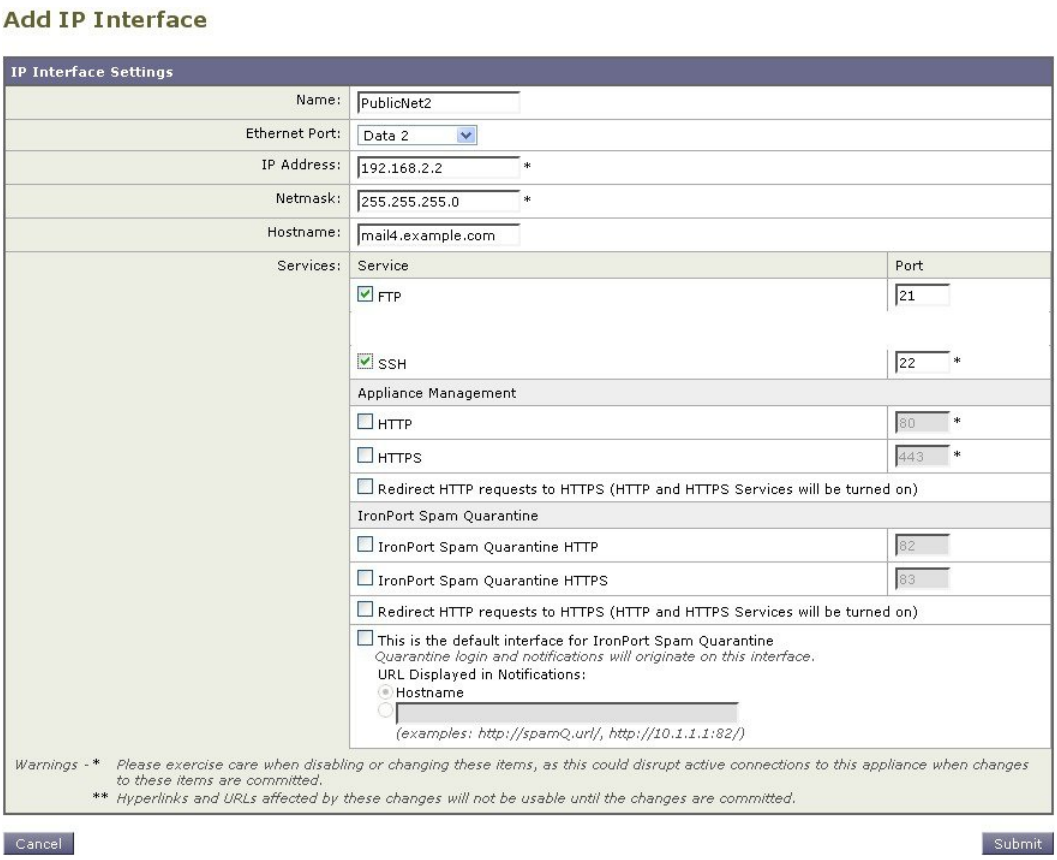

在下面的示例中，“IP 接口”(IP Interfaces) 页面确认除 Management 接口外，还配置了两个接口（PrivateNet 和 PublicNet）。

***Figure 8:“IP 接口”(IP Interface)*** 页面



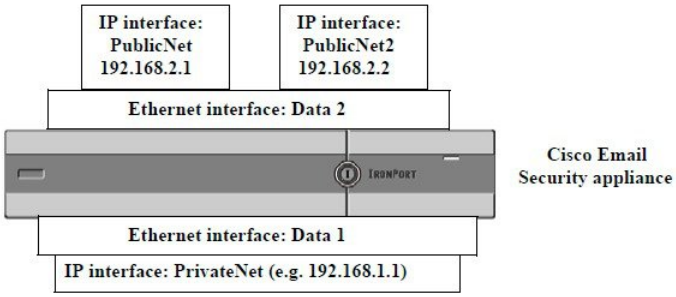

接下来，使用“添加 IP 接口”(Add IP Interface) 页面在 Data2 以太网接口上创建名为 PublicNet2 的新接口。使用的 IP 地址为 192.168.2.2，且指定了主机名 mail4.example.com。然后为 FTP（端口 21）和 SSH（端口 22）启用了服务。

***Figure 9:*** 添加 ***IP*** 接口 ***(Add IP Interface)*** 页面



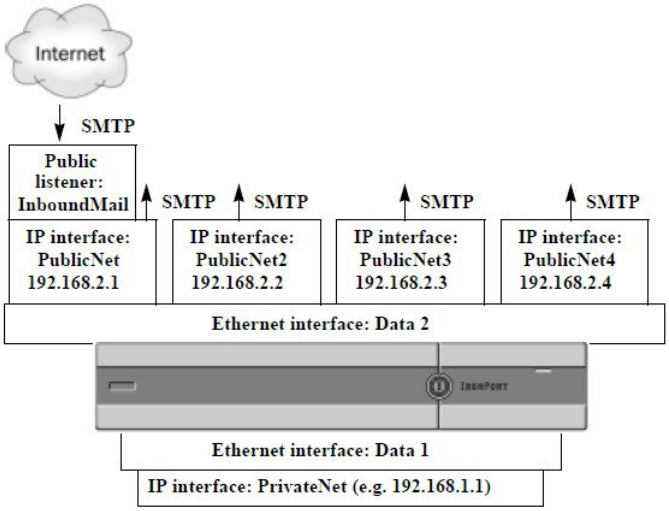

现在，我们的邮件网关配置如下所示：

***Figure 10:*** 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。

*Figure 11:* 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，将每个邮件网关分隔到多个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。

`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。<br>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。<br>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 |

**Note** 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。

**Procedure**

**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。）

**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。）

**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，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。

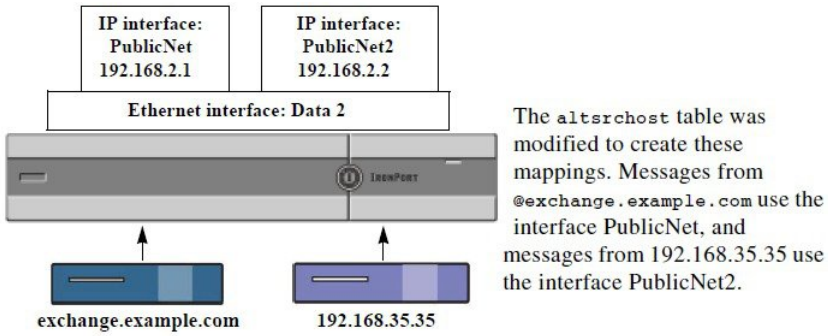
```
mail3.example.com> altsrchost

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：

***Figure 12:*** 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, on page 38。

在创建一“组”虚拟网关地址时，虚拟网关的友好相邻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邮件网关的邮件，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“全局取消订用”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，则该收件人会被丢弃或硬退回，并且全局取消订用(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丢弃或硬退回。）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。

**Note** 全局取消订用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。

全局取消订用不可超过 10,000 个地址的上限。全局取消订用地址可以具有以下四种格式之一：

***Table 10:*** 全局取消订用语法

| | |
|---|---|
| username@example.com | 完全格式化的邮件地址<br>此语法用于阻止特定域中的特定收件人。 |
| username@ | 用户名<br>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<br>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<br>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<br>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。 |

### 相关主题

- 使用 CLI 添加全局取消订用地址, on page 63
- 导入和导出全局取消订用文件, on page 64

# 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用列表，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；邮件网关在传送邮件之前会将其退回。

```
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。

### Procedure

**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。）

**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。）

**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 - *Cisco Secure Email Gateway*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”。

**Note** 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。

***Table 11: Cisco Secure Email Gateway*的邮件管道：接收邮件功能**

| 特性 | 说明 |
|---|---|
| 主机访问表 (HAT)<br>主机 DNS 发件人验证<br>发件人组<br>信封发件人验证<br>发件人验证例外表<br>邮件流策略 | ACCEPT、REJECT、RELAY 或 TCPREFUSE 连接<br>最大出站连接数<br>每个 IP 地址的最大并发入站连接数<br>每个连接的最大邮件大小和最大邮件数<br>每小时内每封邮件的最大收件人数<br>TCP 侦听队列大小<br>TLS：否/首选/必需<br>SMTP AUTH：否/首选/必需<br>丢弃具有格式不正确的 MAIL FROM 信头的邮件<br>始终接受或拒绝来自发件人验证例外表中的 Mail From 条目。<br>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，则会丢弃或退回邮件。可以将 LDAP 验证配置为在工作队列中执行。 |

***Table 12:*** 邮件安全设备的邮件管道：路由和传送功能

| | | | |
|---|---|---|---|
| 工作队列 | **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，则会丢弃或退回邮件。可以将 LDAP 验证配置为 SMTP 会话中执行。 |
| | 伪装<br>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。 |
| | 高级恶意软件防护 | | 高级恶意软件防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。 |
| | 病毒爆发过滤器* | | 病毒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。<br>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。

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。