邮件验证

本章包含以下部分：

- 邮件验证概述, on page 1
- 配置 DomainKey 和 DKIM 签名, on page 3
- 使用 DKIM 如何验证传入的邮件, on page 16
- SPF 和 SIDF 验证概述, on page 22
- 如何使用 SPF/SDIF 验证传入邮件, on page 23
- 启用 SPF 和 SIDF, on page 24
- 确定对 SPF/SIDF 已验证邮件执行的操作, on page 28
- 测试 SPF/SIDF 结果, on page 31
- DMARC 验证, on page 32
- 伪造邮件检测, on page 40

邮件验证概述

AsyncOS 支持邮件验证和签名，防止邮件伪造。AsyncOS 支持发件人策略框架 (SPF)、发件人 ID 框架 (SIDF)、DomainKey 识别邮件 (DKIM)、基于域的邮件验证、报告和合规 (DMARC) 以及伪造邮件检测，以验证传入邮件。AsyncOS 支持使用 DomainKey 和 DKIM 签名验证出站邮件。

相关主题

- DomainKey 和 DKIM 身份验证, on page 1
- SPF 和 SIDF 验证概述, on page 22
- DMARC 验证, on page 32
- 伪造邮件检测, on page 40

DomainKey 和 DKIM 身份验证

利用 DomainKey 或 DKIM 邮件验证，发件人可使用公钥加密方法签署邮件。之后，可通过将已验证的域与邮件 From:（或 Sender:）中的域进行对比检测伪造。

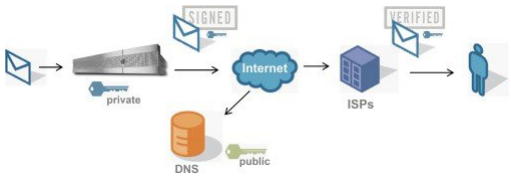
DomainKey 和 DKIM 包括两个主要部分：签名和验证。AsyncOS 支持 DomainKey 流程的“签名”部分，支持 DKIM 的签名和验证流程。您还可以对退回和延迟邮件使用 DomainKey 和 DKIM 签名。

相关主题

- DomainKey 和 DKIM 验证工作流程, on page 2
- AsyncOS 中的 DomainKey 和 DKIM 签名, on page 2

DomainKey 和 DKIM 验证工作流程

Figure 1: 验证工作流程



1. 管理员（域所有者）发布公钥到 DNS 命名空间。
2. 管理员在出站邮件传输代理 (MTA) 上加载私钥。
3. 使用各自的私钥对该域中授权用户提交的邮件进行数字签名。将签名作为 DomainKey 或 DKIM 签名信头插入到邮件中，然后传输该邮件。
4. 接收 MTA 从信头中提取 DomainKey 或 DKIM 签名，从邮件中提取声称的发送域（通过 Sender: 或 From: 信头）。从声称的签名域（从 DomainKey 或 DKIM 信头字段）提取公钥。
5. 使用公钥判断 DomainKey 或 DKIM 签名是否由相应的私钥生成。

要测试外发 DomainKey 签名，可以使用 Yahoo! 或 Gmail 地址，因为这些服务是免费的，并可验证 DomainKey 签名的传入邮件。

AsyncOS 中的 DomainKey 和 DKIM 签名

通过域配置文件在 AsyncOS 中实施 DomainKey 和 DKIM 签名，通过邮件流策略（通常为外发“中继”策略）启用这些签名。有关详细信息，请参阅“配置网关以接收邮件”一章。签署邮件是邮件网关在发送邮件前执行的最后一项操作。

域配置文件将域与域密钥信息（签名密钥和相关信息）关联。由于邮件通过邮件网关上的邮件流策略发送，因此，使用域配置文件中指定的签名密钥对匹配任何域配置文件的发件人邮件地址进行 DomainKey 签名。如果同时启用 DKIM 和 DomainKey 签名，使用 DKIM 签名。可通过 domainkeysconfig CLI 命令，或通过 GUI 中的“邮件策略”>“域配置文件和邮件策略”>“签名密钥”页面，实施 DomainKey 和 DKIM 配置文件。

DomainKey 和 DKIM 签名的工作原理为：域所有者生成两个密钥，一个存储在公共 DNS（与该域关联的 DNS 文本记录）的公共密钥，一个存储在邮件网关上对从该域发送（起源）的邮件进行签名的私钥。

在发送邮件（出站）的侦听程序上收到邮件后，邮件网关会检查是否存在任何域配置文件。如果在邮件网关上创建（并为邮件流策略实施了）域配置文件，则会扫描邮件是否包含有效的 Sender: 或

From: 地址。如果两者都存在，则“发件人：”信头始终用于域密钥和 DKIM 签名，即使不使用“发件人：”信头进行 DKIM 签名，也会需要该信头。当仅存在“发件人：”信头时，在时，DomainKey 或 DKIM 签名配置文件不匹配。“发件人：”信头仅在以下情况下使用：

- 没有“发件人：”信头。
- 选择 Web 界面的“DKIM 全局设置”页面的“使用‘发件人：’信头进行 DKIM 签名”。

Note 从 Async0S 10.0 和更高版本中，可以选择是否要使用 Web 界面的“DKIM 全局设置”页面中的“使用‘发件人：’信头进行 DKIM 签名”。将“发件人：”信头与 DKIM 签名配合使用以进行正确的 DMARC 验证非常重要。

如果找不到有效的地址，则不对邮件签名，并将此事件记录到邮件日志中。

Note 如果创建 DomainKey 和 DKIM 配置文件（并在邮件流策略中启用签名），AsyncOS 将同时使用 DomainKey 和 DKIM 签名对外发邮件签名。

如果找到有效的发送地址，则将发送地址与现有的域配置文件匹配。如果找到匹配，则对邮件签名。否则，不进行签名直接发送邮件。如果邮件已经有 DomainKey（“DomainKey-Signature:”信头），则仅当在初始签名后添加新发件人地址时才对邮件签名。如果邮件有现有的 DKIM 签名，在邮件中添加新 DKIM 签名。

AsyncOS 支持基于域对邮件签名，支持管理（创建新的输入现有）签名密钥。

本文档配置说明介绍的是最常见的签名和验证用途。此外，也可以在入站邮件的邮件流策略上启用 DomainKey 和 DKIM 签名，或者在出站邮件的邮件流策略上启用 DKIM 验证。

Note 在集群环境中配置域配置文件和签名密钥时，请注意域密钥配置文件设置和签名密钥设置是关联的。因此，如果复制、移动或删除签名密钥，系统会在相关配置文件上执行相同的操作。

配置 DomainKey 和 DKIM 签名

相关主题

- 签名密钥, on page 4
- 公共密钥, on page 4
- 域配置文件, on page 5
- 对退回和延迟邮件启用签名, on page 6
- 对外发邮件启用签名, on page 6
- 配置 DomainKey/DKIM 签名 (GUI), on page 6

- 域密钥和日志记录, on page 16

签名密钥

签名密钥是邮件网关上存储的私钥。创建签名密钥时，需要指定密钥大小。密钥越大越安全；但是，密钥较大也可能会影响性能。邮件网关支持大小在 512 位和 2048 位之间的密钥。768 - 1024 位密钥被视为安全密钥，也是当今大部分发件人使用的密钥。较长的密钥可能会影响性能，且系统不支持超过 2048 位的密钥。有关创建签名密钥的详细信息，请参阅创建或编辑签名密钥, on page 10。

如果您输入现有密钥，只需将其粘贴到表单。另一种使用现有签名密钥的方法是，将密钥导入为文本文件。有关添加现有签名密钥的详细信息，请参阅导入或输入现有签名密钥 , on page 11。

输入后，密钥可在域配置文件中使用，并显示在域配置文件的“签名密钥”(Signing Key) 下拉列表中。

相关主题

- 导出和导入签名密钥, on page 4

导出和导入签名密钥

您可以将邮件网关上的签名密钥导出到文本文件中。导出密钥会将当前邮件网关上的所有密钥放入一个文本文件。有关导出密钥的详细信息，请参阅导出签名密钥, on page 11。

您还可以导入已经导出的密钥。

Note 导入密钥会替换当前邮件网关上的所有密钥。

有关详细信息，请参阅导入或输入现有签名密钥 , on page 11。

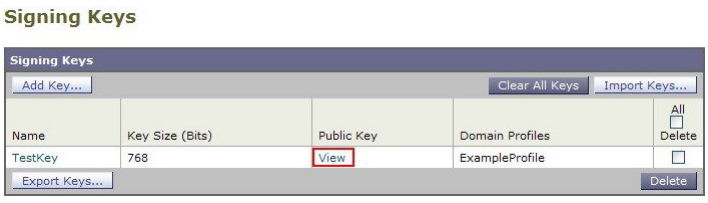
公共密钥

将签名密钥与域配置文件相关联后，可以创建包含公钥的DNS文本记录。可通过域配置文件列表中“DNS 文本记录”(DNS Text Record) 列中的“生成”(Generate) 链接（或通过 CLI 中的 **domainkeysconfig -> profiles -> dnstxt** 命令）执行此操作：

有关生成 DNS 文本记录的详细信息，请参阅生成 DNS 文本记录 , on page 12。

您可以通过“签名密钥”(Signing Keys) 页面上的“视图”(View) 链接查看公钥:

Figure 2: *“签名密钥”(Signing Keys)* 页面上的查看公钥链接



域配置文件

域配置文件将发件人域与签名密钥，以及签名需要的其他信息关联。

- 域配置文件的名称。
- 域名（应添加到“d=”信头的域）。
- 选择器（选择器用于构建公钥查询。在 DNS 查询类型中，此值被添加到发送域命名空间“_domainkey.”的前面）。
- 规范化方法（准备信头和内容向签名算法演示的方法）。AsyncOS 对 DomainKey 支持“simple”和“nofws”，对 DKIM 支持“relaxed”和“simple”。
- 签名密钥（有关详细信息，请参阅签名密钥, on page 4）。
- 要签名的信头和正文长度列表（仅限 DKIM）。
- 要在签名的信头中添加的标签列表（仅限 DKIM）。这些标签存储以下信息：
  - 代表其对邮件签名的用户或代理（例如，邮递列表管理器）。
  - 检索公钥使用的查询方法逗号分隔列表。
  - 创建签名的时间戳。
  - 以秒为单位表示的签名到期时间。
  - 签署邮件时显示的栏分隔的信头字段列表（即，|）。
- 要在签名中添加的标签（仅限 DKIM）。
- 配置文件用户列表（允许使用域配置文件进行签名的地址）。

Note 地址中由配置文件用户指定的域必须与“域”(Domain) 字段中指定的域匹配。

可以在现有的所有域配置文件中搜索特定术语。有关详细信息，请参阅搜索域配置文件, on page 15。

此外，您还可以选择是否：

- 使用 DKIM 签名对系统生成的邮件进行签名
- 使用“发件人”信头进行 DKIM 签名

  有关说明，请参阅编辑 DKIM 全局设置, on page 15。

相关主题

- 导出和导入域配置文件, on page 5

导出和导入域配置文件

您可以将邮件网关上的现有域配置文件导出到文本文件。导出域配置文件会将当前邮件网关上的所有域配置文件放入一个文本文件中。请参阅导出域配置文件, on page 13。

可以导入之前导出的域配置文件。导入域配置文件会替换当前设备上的所有域配置文件。请参阅导入域配置文件, on page 14。

对外发邮件启用签名

在出站邮件的邮件流策略上启用 DomainKey 和 DKIM 签名。有关详细信息，请参阅“配置网关以接收邮件”一章。

Procedure

步骤 1 在“邮件流策略”(Mail Flow Policies) 页面（从“邮件策略”(Mail Policies) 菜单）上，单击 RELAYED 邮件流策略（外发）。

步骤 2 在“安全功能”(Security Features) 部分，通过选择“开”(On) 启用 DomainKey/DKIM 签名。

步骤 3 提交并确认更改。

对退回和延迟邮件启用签名

除对出站邮件签名外，您可能还需要对退回和延迟邮件签名。您可以通过签名提醒收件人从公司收到的退回和延迟邮件是合法的。要对退回和延迟邮件启用 DomainKey 和 DKIM 签名，请对与公共侦听程序关联的退回配置文件启用 DomainKey/DKIM 签名。

Procedure

步骤 1 在与签名出站邮件的目标公共侦听程序关联的退回配置文件上，找到硬退回和延迟警告邮件。

步骤 2 启用“对退回和延迟邮件启用域密钥签名”(Use Domain Key Signing for Bounce and Delay Messages)。

Note 必须完成配置 DomainKey/DKIM 签名 (GUI), on page 6上列出的所有步骤，才能实现对退回和延迟邮件签名。

域配置文件中的 From: 地址必须与用作退回返回地址的地址匹配。要确保这些地址匹配，可以为退回配置文件配置返回地址（系统管理 (System Administration) > 返回地址 (Return Addresses)），然后在域配置文件的“配置文件用户”(Profile Users) 中使用这一名称。例如，可以为退回返回地址配置 MAILER-DAEMON@example.com 返回地址，并添加 MAILER-DAEMON@example.com 作为域配置文件中的配置文件用户。

配置 DomainKey/DKIM 签名 (GUI)

Procedure

步骤 1 创建新私钥或导入现有的私钥。有关创建或导入签名密钥的信息，请参阅签名密钥, on page 4。

步骤 2 创建域配置文件，并将密钥与该域配置文件关联。有关创建域配置文件的信息，请参阅域配置文件, on page 5。

步骤 3 创建 DNS 文本记录。有关创建 DNS 文本记录的信息，请参阅生成 DNS 文本记录 , on page 12。

步骤 4 在出站邮件的邮件流策略上启用 DomainKey/DKIM 签名，如果尚未启用（请参阅对外发邮件启用签名, on page 6）。

步骤 5 或者，对退回和延迟邮件启用 DomainKey/DKIM 签名。有关对退回和延迟邮件启用签名的消息，请参阅对退回和延迟邮件启用签名, on page 6。

步骤 6 发送邮件。对源域与域配置文件匹配的邮件进行 DomainKey/DKIM 签名。此外，如果配置签署退回和延迟邮件，则对退回或延迟邮件签名。

Note 如果创建 DomainKey 和 DKIM 配置文件（并在邮件流策略中启用签名），AsyncOS 将同时使用 DomainKey 和 DKIM 签名对外发邮件签名。

What to do next

相关主题

- 创建用于 DomainKeys 签名的域配置文件, on page 7
- 创建用于 DKIM 签名的新域配置文件, on page 8
- 创建或编辑签名密钥, on page 10
- 导入或输入现有签名密钥 , on page 11
- 测试域配置文件, on page 13
- 编辑 DKIM 全局设置, on page 15

创建用于 DomainKeys 签名的域配置文件

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名配置文件 (Signing Profiles)**。

步骤 2 在**域签名配置文件 (Domain Signing Profiles)** 部分，单击**添加配置文件 (Add Profile)**。

步骤 3 输入配置文件的名称。

步骤 4 对于**域密钥类型 (Domain Key Type)**，请选择**域密钥 (Domain Keys)**。

页面随即显示其他选项。

步骤 5 输入域名。

步骤 6 输入选择器。选择器是添加到“_domainkey”命名空间前面的任意名称，用于帮助支持每个发送域的多个并发公钥。在DNS命名空间和额外规定不能包含分号的邮件信头中，选择器值和长度必须合法。

步骤 7 选择规范化（不转发空格或 simple）。

步骤 8 如已创建签名密钥，请选择签名密钥。否则，跳到下一步。必须创建（或导入）至少一个签名密钥，才能从列表中选择签名密钥。请参阅创建或编辑签名密钥, on page 10。

步骤 9 输入将使用域配置文件进行签名的用户（邮件地址、主机等）。

步骤 10 提交并确认更改。

步骤 11 此时，应在外发邮件流策略上启用 DomainKeys/DKIM 签名（如果尚未启用）（请参阅对外发邮件启用签名, on page 6）。

Note 如果同时创建 DomainKey 和 DKIM 配置文件，AsyncOS 将在外发邮件上执行 DomainKey 和 DKIM 签名。

创建用于 DKIM 签名的新域配置文件

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名配置文件 (Signing Profiles)**。

步骤 2 在**域签名配置文件 (Domain Signing Profiles)** 部分，单击**添加配置文件 (Add Profile)**。

步骤 3 输入配置文件的名称。

步骤 4 对于**域密钥类型 (Domain Key Type)**，请选择 **DKIM**。

页面随即显示其他选项。

步骤 5 输入域名。

步骤 6 输入选择器。选择器是添加到“_domainkey”命名空间前面的任意名称，用于帮助支持每个发送域的多个并发公钥。在DNS命名空间和额外规定不能包含分号的邮件信头中，选择器值和长度必须合法。

步骤 7 为标题选择规范化。从以下选项中选择：

- **Relaxed**。“relaxed”信头规范化算法执行以下操作：将信头名称更改为小写、展开信头、将线性空格缩减为单个空格、删除前导和结尾空格。
- **Simple**。不对信头做更改。

步骤 8 为正文选择规范化。从以下选项中选择：

- **Relaxed**。“relaxed”信头规范化算法执行以下操作：删除正文结尾的空行、空格缩减为行中的单个空格、删除行中的行尾空格。
- **简单**、删除正文结尾的空行。

步骤 9 如已创建签名密钥，请选择签名密钥。否则，跳到下一步。必须创建（或导入）至少一个签名密钥，才能从列表中选择签名密钥。请参阅创建或编辑签名密钥, on page 10。

步骤 10 选择要签名的信头列表。可选择以下信头：

- **All**。AsyncOS对签名时存在的所有信头签名。如果不想在传输过程中添加或删除信头，可能需要签署所有信头。

- **Standard**。如果想要在传输中添加或删除信头，可能需要选择标准信头。AsyncOS 仅对以下标准信头签名（如果邮件不存在信头，DKIM 签名指示信头的值为空）：
  - 发件人
  - Sender、Reply To-
  - 主题
  - Date、Message-ID
  - To、Cc
  - MIME-Version
  - Content-Type、Content-Transfer-Encoding、Content-ID、Content-Description
  - Resent-Date、Resent-From、Resent-Sender、Resent-To、Resent-cc、Resent-Message-ID
  - In-Reply-To、References
  - List-Id、List-Help、List-Unsubscribe、LIst-Subscribe、List-Post、List-Owner、List-Archive

Note 选择“Standard”时，可添加更多要签名的信头。

步骤 11 指定如何对邮件正文签名。您可以选择对邮件正文签名，和/或要签名的字节数量。选择以下选项之一：

- **Whole Body Implied**。不要使用“l=”标签确定正文长度。对整封邮件签名，不允许做任何更改。
- **Whole Body Auto-determined**。对整封邮件签名，允许传输过程中在正文结尾附加一些额外数据。
- **Sign first _ bytes**。对达到指定字节数的邮件正文签名。

步骤 12 选择您要在邮件签名的信头字段中添加的标签。这些标签中存储的信息可用于邮件签名验证。选择以下其中一个或多个选项：

- “**i**”标签。代表其对邮件签名的用户或代理（例如，邮递列表管理器）的身份。在@符号前面输入域名，例如，域@example.com。
- “**q**”标签。用于检索公钥的查询方法冒号分隔列表。目前，唯一的有效值是 dns/txt。
- “**t**”标签。创建签名时的时间戳。
- “**x**”标签。签名到期的绝对日期和时间。指定签名的到期时间（以秒为单位）。默认值为 31536000 秒。
- “**z**”标签。签署邮件时显示的栏分隔的信头字段列表（即，|）。这包括信头字段的名称及其值。例如：

z=From:admin@example.come|To:joe@example.com|
Subject:test%20message|Date:Date:August%2026,%202011%205:30:02%20PM%20-0700

步骤 13 输入将使用域配置文件进行签名的用户（邮件地址、主机等）。

Note 创建域配置文件时，请注意使用层次结构确定与特定用户关联的配置文件。例如，为 example.com 创建配置文件，为 joe@example.com 创建另一个配置文件。从 joe@example.com 发送邮件时，使用 joe@example.com 的配置文件。但是，从 adam@example.com 时发送邮件时，使用 example.com 的配置文件。

步骤 14 提交并确认更改。

步骤 15 此时，应在外发邮件流策略上启用 DomainKeys/DKIM 签名（如果尚未启用）（请参阅对外发邮件启用签名, on page 6）。

Note 如果同时创建 DomainKey 和 DKIM 配置文件，AsyncOS 将在外发邮件上执行 DomainKey 和 DKIM 签名。

创建或编辑签名密钥

- 创建新签名密钥, on page 10
- 编辑现有签名密钥, on page 10

创建新签名密钥

必须为进行 DomainKey 和 DKIM 签名的域配置文件提供签名密钥。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名密钥 (Signing Keys)**。

步骤 2 单击**添加密钥 (Add Key)**。

步骤 3 输入密钥名称。

步骤 4 单击**生成 (Generate)** 并选择密钥大小。

步骤 5 提交并确认更改。

Note 您可能需要编辑域配置文件来分配一个密钥，如果尚未生成密钥。

编辑现有签名密钥

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名密钥 (Signing Keys)**。

步骤 2 单击目标签名密钥。

步骤 3 按照创建新签名密钥, on page 10中的说明编辑目标字段。

步骤 4 提交并确认更改。

导出签名密钥

邮件网关上的所有密钥集中导出到一个文本文件中。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名密钥 (Signing Keys)**。

步骤 2 单击**导出密钥 (Export Keys)**。

步骤 3 输入文件名称并单击**提交 (Submit)**。

导入或输入现有签名密钥

相关主题

- 粘贴密钥 , on page 11
- 从现有导出文件导入密钥 , on page 11

粘贴密钥

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名密钥 (Signing Keys)**。

步骤 2 单击**添加密钥 (Add Key)**。

步骤 3 将密钥粘贴到“粘贴密钥”(Paste Key) 字段（必须是 PEM 格式，且必须只能是 RSA 密钥）。

步骤 4 提交并确认更改。

从现有导出文件导入密钥

Note 要获取密钥文件，请参阅导出签名密钥, on page 11。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名密钥 (Signing Keys)**。

步骤 2 单击**导入密钥 (Import Keys)**。

步骤 3 选择包含导出签名密钥的文件。

步骤 4 单击**提交 (Submit)**。系统将警告您导入将会替换现有的所有签名密钥。文本文件中的密钥均被导入。

步骤 5 点击导入。

删除签名密钥

相关主题

- 删除所选的签名密钥 , on page 12
- 删除所有签名密钥 , on page 12

删除所选的签名密钥

Procedure

步骤 1 依次选择邮件策略 **(Mail Policies)** > 签名密钥 **(Signing Keys)**。
步骤 2 选中每个要删除签名密钥右侧的复选框。
步骤 3 单击删除 **(Delete)**。
步骤 4 确认删除。

删除所有签名密钥

Procedure

步骤 1 依次选择邮件策略 **(Mail Policies)** > 签名密钥 **(Signing Keys)**。
步骤 2 单击“签名密钥”(Signing Keys) 页面上的清除所有密钥 **(Clear All Keys)**。
步骤 3 确认删除。

生成 DNS 文本记录

Procedure

步骤 1 依次选择邮件策略 **(Mail Policies)** > 签名配置文件 **(Signing Profiles)**。
步骤 2 在“域签名配置文件”(Domain Signing Profiles) 部分的“DNS 文本记录”(DNS Text Record) 列中，单击相应域配置文件的生成 **(Generate)** 链接。
步骤 3 选中与要包含在 DNS 文本记录中的属性对应的复选框。
步骤 4 单击重新生成 **(Generate Again)** 使用所做更改重新生成密钥。
步骤 5 DNS 文本记录显示在窗口底部的文本字段中（可在该位置执行复制）。有时候可生成多字符串 DNS 文本记录。请参阅多字符串 DNS 文本记录, on page 13。

步骤 6 单击**完成 (Done)**。

What to do next

相关主题

- 多字符串 DNS 文本记录, on page 13

多字符串 DNS 文本记录

如果生成 DNS 文本记录的签名密钥的密钥大小超过 1024 位，可能会生成多字符串 DNS 文本记录。这是因为 DNS 文本记录的单个字符串中不允许超过 255 个字符。DKIM 验证可能会失败，因为某些 DNS 服务器不接受，也不提供多字符串 DNS 文本记录。

为避免出现这种情况，建议使用双引号将多字符串 DNS 文本记录分成不超过 255 个字节的短字符串。下面便是一例：

```
s._domainkey.domain.com. IN TXT "v=DKIM1;"
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE"
"A4Vbhjq2n/3DbEk6EHdeVXlIXFT7OEl81amoZLbvwMX+bej"
"CdxcsFV3uS7G8oOJSWBP0z++nTQmy9ZDWfaiopU6k7tzoi"
"+oRDlKkhCQrM4oP2B2F5sTDkYwPY3Pen2jgC2OgbPnbo3o"
"m3c1wMWgSoZxoZUE4ly5kPuK9fTtpeJHNiZAqkFICiev4yrkL"
"R+SmFsJn9MYH5+lchyZ74BVm+16Xq2mptWXEwpiwOxWI"
"YHXsZo2zRjedrQ45vmgb8xUx5ioYY9/yBLHudGc+GUKTj1i4"
"mQg48yCD/HVNfsSRXaPinliEkypH9cSnvgvWuIYUQz0dHU;"
```

DKIM 实施对如此拆分的 DNS 文本记录组合为完整原始单个字符串，然后再进行处理。

测试域配置文件

创建签名密钥、将其与域配置文件关联、生成并将 DNS 文本插入授权 DNS 后，可以测试域配置文件。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名配置文件 (Signing Profiles)**。

步骤 2 在**域签名配置文件 (Domain Signing Profiles)** 部分的“测试配置文件”(Test Profile) 列中，单击域配置文件的**测试 (Test)** 链接。

步骤 3 页面顶部将显示一条消息，表明测试成功还是失败。如果测试失败，屏幕将显示警告消息，包括错误文本。

导出域配置文件

邮件网关上的所有域配置文件集中导出到一个文本文件中。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名配置文件 (Signing Profiles)**。
步骤 2 单击**导出域配置文件 (Export Domain Profiles)**。
步骤 3 输入文件名称并单击**提交 (Submit)**。

导入域配置文件

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名配置文件 (Signing Profiles)**。
步骤 2 单击**导入域配置文件 (Import Domain Profiles)**。
步骤 3 选择包含导出域配置文件的文件。
步骤 4 单击**提交 (Submit)**。系统将警告您导入将会替换现有的所有域配置文件。文本文件中的所有域配置文件均被导入。
步骤 5 点击**导入**。

删除域配置文件

相关主题

- 删除所选域配置文件 , on page 14
- 删除所有域配置文件 , on page 15

删除所选域配置文件

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名配置文件 (Signing Profiles)**。
步骤 2 选中每个要删除域配置文件右侧的复选框。
步骤 3 单击**删除 (Delete)**。
步骤 4 确认删除。

删除所有域配置文件

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名配置文件 (Signing Profiles)**。

步骤 2 单击**清除所有配置文件 (Clear All Profiles)**。

步骤 3 确认删除。

搜索域配置文件

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名配置文件 (Signing Profiles)**。

步骤 2 在“查找域配置文件”(Find Domain Profiles) 部分，指定搜索词。

步骤 3 单击**查找配置文件 (Find Profiles)**。

步骤 4 搜索将扫描每个域配置文件的以下字段：邮件、域、选择器和签名密钥名称。

Note 如果不输入搜索词语，搜索引擎将返回所有域配置文件。

编辑 DKIM 全局设置

可以使用 DKIM 全局设置来选择是否：

- 使用 DKIM 签名对系统生成的邮件进行签名。邮件网关将签署以下邮件：
  - 思科 IronPort 垃圾邮件隔离区通知
  - 内容过滤器生成的通知
  - 配置消息
  - 支持请求
- 使用“发件人”信头进行 DKIM 签名

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **签名配置文件 (Signing Profiles)**。

步骤 2 在“DKIM 全局设置”(DKIM Global Settings) 下，单击**编辑设置 (Edit Settings)**。

步骤 3 根据您的要求，配置以下字段：

- 系统生成的邮件的 DKIM 签名
- 对 DKIM 签名使用 From 信头

Note 如果您没有对 DKIM 签名使用 From 信头，或如果缺少有效的 From 信头，则将使用 Sender 信头。对于 DKIM 签名邮件的 DMARC 验证，必须在 DKIM 签名过程中使用 From 信头。

步骤 4 提交并确认更改。

域密钥和日志记录

执行 DomainKey 签名时，类似下文的行目将添加到邮件日志中：

```
Tue Aug 28 15:29:30 2007 Info: MID 371 DomainKeys: signing with dk-profile - matches
user123@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DomainKeys: cannot sign - no profile matches
user12@example.com
```

执行 DKIM 签名时，类似下文的行目将添加到邮件日志中：

```
Tue Aug 28 15:29:54 2007 Info: MID 372 DKIM: signing with dkim-profile - matches
user@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DKIM: cannot sign - no profile matches
user2@example.com
```

使用 DKIM 如何验证传入的邮件

使用 DKIM 如何验证传入的邮件

	相应操作	更多信息
第 1 步	创建用于使用 DKIM 验证邮件的配置文件。	创建 DKIM 验证配置文件, on page 18
第 2 步	（可选）创建用于使用 DKIM 验证传入邮件的自定义邮件流策略。	使用邮件流策略定义传入邮件规则
第 3 步	将邮件流策略配置为使用 DKIM 验证传入的邮件。	在邮件流策略上配置 DKIM 验证, on page 20
第 4 步	定义邮件网关在已验证邮件上执行哪些操作。	配置面向 DKIM 已验证邮件的操作, on page 21
第 5 步	将操作与特定发件人或收件人群组关联。	配置邮件策略

相关主题

- AsyncOS 执行的 DKIM 验证检查, on page 17
- 管理 DKIM 验证配置文件, on page 17
- 在邮件流策略上配置 DKIM 验证, on page 20
- 配置面向 DKIM 已验证邮件的操作, on page 21

AsyncOS 执行的 DKIM 验证检查

配置 AsyncOS 设备进行 DKIM 验证时，邮件网关将执行以下检查：

Procedure

步骤 1 AsyncOS 检查传入邮件的 DKIM 签名字段、签名信头的语法，有效的标签值和所需的标签。如果签名未通过这些检查，AsyncOS 返回 *permfail*。

步骤 2 签名检查完成后，设备从公共DNS记录检索公钥，并验证文本记录。如果在此过程中出错，AsyncOS 返回 *permfail*。如果公钥的 DNS 查询无法获得响应，设备返回 *tempfail*。

步骤 3 检索公钥后，AsyncOS 将检查散列值并验证签名。如果在此过程中失败，AsyncOS 返回 *permfail*。

步骤 4 如果检查全部通过，AsyncOS 返回 *pass*。

Note 当邮件正文超过指定的长度时，AsyncOS 返回以下判定：

```
dkim = pass (partially verified [x bytes])
```

其中，*X* 表示验证的字节数。

最终验证结果输入为 *Authentication-Results* 信头。例如，您可能获得类似下文之一的信头：

```
Authentication-Results: example1.com

header.from=From:user123@example.com; dkim=pass (signature verified)

Authentication-Results: example1.com

header.from=From:user123@example.com; dkim=pass (partially verified [1000 bytes])

Authentication-Results: example1.com

header.from=From:user123@example.com; dkim=permfail (body hash did not verify)
```

Note 当前 DKIM 验证在第一个有效签名位置停止。无法使用检测到的最后一个签名进行验证。此功能可能会在未来版本中提供。

当域在 DKIM 测试模式 (`t=y`) 中具有其 DNS TXT 记录时，邮件网关将彻底跳过任何 DKIM 验证和操作。

管理 DKIM 验证配置文件

DKIM 验证配置文件是邮件网关的邮件流策略验证 DKIM 签名使用的参数列表。例如，您可以创建两个验证配置文件，一个在查询超时前留出 30 秒的时间，一个在查询超时前仅留出 3 秒的时间。您可以将第二个验证配置文件分配到受限制邮件流策略，以防止在 DDoS 情况下连接匮乏。验证配置文件包括以下信息：

- 验证配置文件的名称。
- 可接受的最小和最大公钥大小。默认密钥大小分别为 512 和 2048 位。

- 邮件中要验证的最大签名数量。如果邮件中签名的数量超过定义的最大数量，邮件网关将跳过验证剩余的签名，并继续处理邮件。默认为 5 个签名。
- 发件人系统时间和检验器系统时间之间允许的最大时间差（以秒为单位）。例如，如果邮件签名在 05:00:00 到期，检验器的系统时间是 05:00:30，那么如果允许的时间差是 60 秒，邮件签名将继续有效，如果允许的时间差是 10 秒，签名将无效。默认值为 60 秒。
- 一个表明是否使用正文长度参数的选项。
- 在临时失败情况下执行的 SMTP 操作。
- 在永久失败情况下执行的 SMTP 操作。

可以按配置文件名称在现有的所有验证配置文件中搜索。

可以将 DKIM 验证配置文件导出为邮件网关配置目录中的文本文件。导出验证配置文件时，当前邮件网关上的所有配置文件均放入一个文本文件。有关详细信息，请参阅导出 DKIM 验证配置文件, on page 19。

可以导入之前导出的DKIM验证配置文件。导入DKIM验证配置文件会替换当前设备上的所有DKIM验证配置文件。有关详细信息，请参阅导入 DKIM 验证配置文件, on page 19。

相关主题

- 创建 DKIM 验证配置文件, on page 18
- 导出 DKIM 验证配置文件, on page 19
- 导入 DKIM 验证配置文件, on page 19
- 删除 DKIM 验证配置文件, on page 19
- 搜索 DKIM 验证配置文件, on page 20

创建 DKIM 验证配置文件

Procedure

步骤 1 依次单击**邮件策略 (Mail Policies)** > **验证配置文件 (Verification Profiles)**。

步骤 2 单击**添加配置文件 (Add Profile)**。

步骤 3 输入配置文件的名称。

步骤 4 选择邮件网关接受的最小签名密钥大小。

步骤 5 选择邮件网关接受的最大签名密钥大小。

步骤 6 选择要在一封邮件中验证的最大签名数量。默认为 5 个签名。

步骤 7 选择密钥查询超时前留出的秒数。默认值为 10 秒。

步骤 8 选择发件人系统时间和检验器系统时间之间允许的最大时间差（以秒为单位）。默认值为 60 秒。

步骤 9 选择是否在签名中使用正文长度参数验证邮件。

步骤 10 选择邮件网关在验证邮件签名出现临时失败时接受还是拒绝邮件。如果希望邮件网关拒绝邮件，可以选择配置设备发送默认 451 SMTP 响应代码或其他 SMTP 响应代码和文本。

步骤 11 选择邮件网关在验证邮件签名出现永久失败时接受还是拒绝邮件。如果希望邮件网关拒绝邮件，可以选择配置设备发送默认 451 SMTP 响应代码或其他 SMTP 响应代码和文本。

步骤 12 提交更改。

新的配置文件随即显示在 DKIM 验证配置文件表中。

步骤 13 确认您的更改。

步骤 14 此时应在传入邮件流策略上启用 DKIM 验证，并选择要使用的验证配置文件。

导出 DKIM 验证配置文件

邮件网关上的所有 DKIM 验证配置文件导出为一个文本文件，并保存在邮件网关的 configuration 目录中。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **验证配置文件 (Verification Profiles)**。

步骤 2 单击**导出配置文件 (Export Profiles)**。

步骤 3 输入文件名称并单击**提交 (Submit)**。

导入 DKIM 验证配置文件

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **验证配置文件 (Verification Profiles)**。

步骤 2 单击**导入配置文件 (Import Profiles)**。

步骤 3 选择包含 DKIM 验证配置文件的文件。

步骤 4 单击**提交 (Submit)**。系统将警告您导入将会替换现有的所有 DKIM 验证配置文件。

步骤 5 点击**导入**。

删除 DKIM 验证配置文件

相关主题

- 删除所选的 DKIM 验证配置文件 , on page 20
- 删除所有 DKIM 验证配置文件, on page 20

删除所选的 DKIM 验证配置文件

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **验证配置文件 (Verification Profiles)**。
步骤 2 选中每个要删除 DKIM 验证配置文件右侧的复选框。
步骤 3 单击**删除 (Delete)**。
步骤 4 确认删除。

删除所有 DKIM 验证配置文件

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **验证配置文件 (Verification Profiles)**。
步骤 2 单击**清除所有配置文件 (Clear All Profiles)**。
步骤 3 确认删除。

搜索 DKIM 验证配置文件

在所有 DKIM 验证配置文件中搜索配置文件名称中的特定术语：

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **验证配置文件 (Verification Profiles)**。
步骤 2 在**搜索 DKIM 验证配置文件 (Search DKIM Verification Profiles)** 部分，指定搜索词。
步骤 3 单击**查找配置文件 (Find Profiles)**。

搜索将扫描每个 DKIM 验证配置文件的配置文件名称。

如果不输入搜索词，搜索引擎将返回所有 DKIM 验证配置文件。

在邮件流策略上配置 DKIM 验证

在传入邮件的邮件流策略上启用 DKIM 验证。

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 单击要执行验证的侦听程序的传入邮件策略。

步骤 3 在邮件流策略的“安全功能”(Security Features) 部分，选择**开 (On)** 启用 DKIM 验证。

步骤 4 选择要用于策略的 DKIM 验证配置文件。

步骤 5 确认您的更改。

What to do next

相关主题

- DKIM 验证和日志记录, on page 21

DKIM 验证和日志记录

执行 DKIM 验证时，类似下文的行目将添加到邮件日志中：

```
mail.current:Mon Aug 6 13:35:38 2007 Info: MID 17 DKIM: no signature

mail.current:Mon Aug 6 15:00:37 2007 Info: MID 18 DKIM: verified pass
```

配置面向 DKIM 已验证邮件的操作

验证 DKIM 邮件时，系统会向邮件添加 *Authentication-Results* 信头，但不论验证结果如何仍会接受邮件。要配置基于这些验证结果的操作，可以创建内容过滤器对DKIM已验证邮件执行操作。例如，如果 DKIM 验证失败，您可能希望将邮件配置为对其进行传送、退回、丢弃或发送到隔离区。要执行此操作，必须配置一个使用内容过滤器的操作。

Procedure

步骤 1 选择**邮件策略 (Mail Policies) > 传入内容过滤器 (Incoming Content Filters)**。

步骤 2 单击**添加过滤器 (Add Filter)**。

步骤 3 在“条件”(Conditions) 部分，单击**添加条件 (Add Condition)**。

步骤 4 从条件列表中选择 **DKIM 验证 (DKIM Authentication)**。

步骤 5 选择 DKIM 条件。选择以下选项之一：

- **Pass**。邮件通过验证测试。
- Neutral。验证未执行。
- **Temperror**。出现可解决的错误。
- **Permerror**。出现不可解决的错误。
- **Hardfail**。验证测试失败。

- **None**。邮件未签名。

步骤 6 选择与条件关联的操作。例如，如果 DKIM 验证失败，您可能希望通知收件人和退回邮件。或者，如果 DKIM 验证通过，您可能希望立即传送邮件，无需进一步处理。

步骤 7 提交新的内容过滤器。

步骤 8 在相应的传入邮件策略上启用内容过滤器。

步骤 9 确认您的更改。

SPF 和 SIDF 验证概述

AsyncOS 支持发件人策略框架 (SPF) 和发件人 ID 机制 (SIDF) 验证。SPF 和 SIDF 是基于 DNS 记录验证邮件真实性的方法。通过 SPF 和 SIDF，互联网域的所有者可使用特定格式的 DNS 文本记录指定哪些计算机获得传输该域邮件的权限。然后，应允的邮件收件人使用发布的 SPF 记录在邮件传输过程中测试发送邮件传输代理身份的授权。

使用 SPF/SIDF 验证时，发件人发布指定哪些主机可使用其名称的 SPF 记录，应允的邮件收件人使用发布的 SPF 记录在邮件传输过程中测试发送邮件传输代理身份的授权。

Note 由于 SPF 检查要求解析和评估，AsyncOS 的性能可能会受到影响。此外，请注意 SPF 检查会增加 DNS 基础设施的负担。

使用 SPF 和 SIDF 时，请注意 SIDF 类似于 SPF，但有一些差异。要了解 SIDF 和 SPF 两者之间差异的完整说明，请参阅 RFC 4406。在本文档中，两个术语一起讨论，除非出现仅适用一种验证类型的情况。

Note AsyncOS 不支持用于传入中继的 SPF。

相关主题

- 有关有效 SPF 记录的说明, on page 22

有关有效 SPF 记录的说明

要在邮件网关上使用 SPF 和 SIDF，请根据 RFC 4406、4408 和 7208 发布 SPF 记录。查阅 RFC 4407 了解如何确定 PRA 身份。您还可以访问以下网站，了解创建 SPF 和 SIDF 记录时的常见错误：

http://www.openspf.org/FAQ/Common_mistakes

相关主题

- 有效的 SPF 记录, on page 23

• 有效的 SIDF 记录, on page 23
• 检测 SPF 记录, on page 23

有效的 SPF 记录

要通过 SPF HELO 检查，请为每个发送 MTA（独立于域）添加“v=spf1 a －all”SPF 记录。如果不添加此记录，针对 HELO 身份的 HELO 检查可能会返回 None 判定结果。如果您发现目标至您所在域的 SPF 发件人返回大量“无”(None) 判定，这些发件人可能没有为每个发送 MTA 添加“v=spf1 a －all”SPF 记录。

有效的 SIDF 记录

要支持 SIDF 机制，您需要同时发布“v=spf1”和“spf2.0”记录。例如，您可能会有类似下文示例的 DNS 记录：

```
example.com. TXT "v=spf1 +mx a:colo.example.com/28 -all"

smtp-out.example.com TXT "v=spf1 a -all"

example.com. TXT "spf2.0/mfrom,pra +mx a:colo.example.com/28 -all"
```

SIDF 不验证 HELO 身份，因此在这种情况下，不需要为每个发送 MTA 发布 PF v2.0 记录。

Note 如果选择不支持 SIDF，请发布“spf2.0/pra ~all”记录。

检测 SPF 记录

除查阅 RFC 以外，在邮件网关上实施 SPF 验证之前，最好检测 SPF 记录。openspf.org website 上有多款测试工具可供选择：

http://www.openspf.org/Tools

您可以使用以下工具找出邮件未通过 SPF 记录检查的原因：

http://www.openspf.org/Why

此外，您可以在测试侦听程序上启用 SPF，使用思科的 trace 命令（或从 GUI 执行跟踪）查看 SPF 结果。使用跟踪，您可以轻松检测各个发送 IP。

如何使用 SPF/SDIF 验证传入邮件

	相应操作	更多信息
第 1 步	（可选）创建用于使用 SPF/SIDF 验证传入邮件的自定义邮件流策略。	使用邮件流策略定义传入邮件规则

	相应操作	更多信息
第 2 步	将邮件流策略配置为使用 SPF/SIDF 验证传入邮件。	启用 SPF 和 SIDF, on page 24
第 3 步	定义邮件网关在已验证邮件上执行哪些操作。	确定对 SPF/SIDF 已验证邮件执行的操作, on page 28
第 4 步	将操作与特定发件人或收件人群组关联。	配置邮件策略
第 5 步	（可选）测试邮件验证的结果。	测试 SPF/SIDF 结果, on page 31

Caution 虽然思科坚决支持全局邮件验证，但目前思科建议谨慎处理 SPF/SIDF 验证失败。思科强烈建议客户隔离未通过 SPF/SIDF 验证的邮件，不要退回这些邮件，直到更多组织能够对授权的邮件发送基础设施进行更为严格的掌控。

Note AsyncOS 命令行界面 (CLI) 可提供比网络界面更多的 SPF 级别控制设置。根据 SPF 判定，邮件网关可以在 SMTP 会话中接受或拒绝每个侦听程序上的邮件。可以在使用 listenerconfig 命令编辑侦听程序主机访问表的默认设置时修改 SPF 设置。有关这些设置的详细信息，请参阅通过 CLI 启用 SPF 和 SIDF, on page 25。

启用 SPF 和 SIDF

要使用 SPF/SIDF，必须在传入侦听程序上启用针对邮件流策略的 SPF/SIDF。可以在侦听程序上从默认邮件流策略启用 SPF/SIDF，也可以对特定传入邮件流策略启用。

Procedure

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

步骤 2 单击**默认策略参数 (Default Policy Parameters)**。

步骤 3 查看默认策略参数中的“安全功能”(Security Features) 部分。

步骤 4 在 **SPF/SIDF 验证 (SPF/SIDF Verification)** 部分，单击**开 (On)**。

步骤 5 设置一致性级别（默认值为 SIDF-compatible）。通过此选项确定要使用的 SPF 或 SIDF 验证标准。除 SIDF 一致性之外，您可以选择包含 SPF 和 SIDF 的 SIDF-compatible。

SPF/SIDF 一致性级别

一致性级别	说明
SPF	SPF/SIDF 验证基于 RFC4408 和 RFC7208 进行操作。 - 未执行 purported responsible address (PRA) 身份验证。 **说明**：选择此一致性选项测试 HELO 身份。
SIDF	SPF/SIDF 验证基于 RFC4406。 - 在与标准完全一致的情况下，确定 PRA 身份。 - SPF v1.0 记录被视为 spf2.0/mfrom,pra。 - 对于不存在的域或格式错误的身份，返回 Fail 判定。
SIDF 兼容	SPF/SIDF 验证基于 RFC4406，但以下冲突除外： - SPF v1.0 记录被视为 spf2.0/mfrom。 - 对于不存在的域或格式错误的身份，返回 None 判定。 **说明**：此一致性选项应 OpenSPF 社区 (www.openspf.org) 要求推出。

Note 更多设置，请查看 CLI。有关详细信息，请参阅通过 CLI 启用 SPF 和 SIDF, on page 25。

步骤 6 如选择一致性级别 SIDF-compatible，请配置验证是否在邮件中存在 Resent-Sender: 或 Resent-From: 信头时将 PRA 身份的 Pass 结果降级为 None。您可能会出于安全考虑选择此选项。

步骤 7 如果您选择一致性级别 SPF，可以配置是否执行 HELO 身份测试。您可以使用此选项通过禁用 HELO 检查提高性能。此选项非常实用，因为 spf-passed 过滤器规则首先检查 PRA 或 MAIL FROM 身份。邮件网关仅对 SPF 一致性级别执行 HELO 检查。

What to do next

相关主题

- 接收的 SPF 信头, on page 27
- 通过 CLI 启用 SPF 和 SIDF, on page 25

通过 CLI 启用 SPF 和 SIDF

AsyncOS CLI 为每个 SPF/SIDF 一致性级别支持更多控制设置。配置侦听程序主机访问表的默认设置时，可以选择侦听程序的 SPF/SIDF 一致性级别和邮件网关基于 SPF/SIDF 验证结果执行的 SMTP 操作（ACCEPT 或 REJECT）。您还可以定义邮件网关拒绝邮件时发送的 SMTP 响应。

根据一致性级别，邮件网关执行 HELO 身份、MAIL FROM 身份或 PRA 身份检查。针对每个身份检查的下列 SPF/SIDF 验证结果，指定邮件网关继续会话 (ACCEPT) 还是终止会话 (REJECT)：

- **None**。由于缺少信息无法执行验证。

- **Neutral**。域所有者未表明客户端是否有权使用特定身份。
- **SoftFail**。域所有者认为主机无权使用特定身份，但无意发表明确意见。
- **Fail**。客户端无权使用特定身份发送邮件。
- **TempError**。验证过程中出现瞬时错误。
- **PermError**。验证过程中出现持久错误。

如果邮件中存在 Resent-Sender: 或 Resent-From: 报头，除非您配置 SIDF 兼容一致性级别以将 PRA 身份的“通过”结果降级为“无”，否则邮件网关会对“通过”结果接受邮件。之后，邮件网关会执行 PRA 检查返回“无”时所指定的 SMTP 操作。

如果您选择不对身份检查定义 SMTP 操作，则邮件网关会自动接受所有验证结果，包括“失败”。

如果身份验证结果与任何已启用的身份检查的REJECT操作相匹配，则邮件网关会终止会话。例如，管理员根据所有 HELO 身份检查结果（包括“失败”）将侦听程序配置为接受邮件，但同时将侦听程序配置为拒绝来自 MAIL FROM 身份检查的“失败”结果的邮件。如果邮件未通过 HELO 身份检查，由于邮件网关接受该结果，因此会话将继续。如果接下来邮件未通过 MAIL FROM 身份检查，则侦听程序会终止会话并对 REJECT 操作返回 STMP 响应。

SMTP 响应是邮件网关根据 SPF/SIDF 验证结果拒绝邮件时返回的代码数字和消息。TempError 结果返回与其他验证结果不同的 SMTP 响应。对于 TempError，默认响应代码为 451，默认消息文本为 `#4.4.3 Temporary error occurred during SPF verification`。对于所有其他验证结果，默认响应代码为 550，默认消息文本为 `#5.7.1 SPF unauthorized mail is prohibited`。可以为 TempError 和其他验证结果指定您自己的响应代码和消息文本。

或者，如果对“不确定”、“软失败”或“失败”验证结果执行 REJECT 操作，则您可以将邮件网关配置为返回来自 SPF 发布者域的第三方响应。默认情况下，邮件网关会返回以下响应：

```
550-#5.7.1 SPF unauthorized mail is prohibited.

550-The domain example.com explains:

550 <Response text from SPF domain publisher>
```

要启用这些 SPF/SIDF 设置，请使用 `listenerconfig -> edit` 子命令并选择侦听器。然后使用 `hostaccess -> default` 子命令编辑主机访问表的默认设置。

以下 SPF 控制设置可用于主机访问表：

通过 CLI 实现的 SPF 控制设置

一致性级别	可用的 SPF 控制设置

仅限 SPF	• 是否执行 HELO 身份检查
	• 根据以下身份检查结果执行 SMTP 操作：
	  • HELO 身份（如已启用）
	  • MAIL FROM 身份
	• 对 REJECT 操作返回的 SMTP 响应代码和文本
	• 验证超时（秒）

SIDF Compatible	• 是否执行 HELO 身份检查
	• 如果邮件中存在 Resent-Sender: 或 Resent-From: 信头，是否将 PRA 身份的“通过”结果降级为“无”
	• 根据以下身份检查结果执行 SMTP 操作：
	  • HELO 身份（如已启用）
	  • MAIL FROM 身份
	  • PRA 身份
	• 对 REJECT 操作返回的 SMTP 响应代码和文本。
	• 验证超时（秒）

SIDF Strict	• 根据以下身份检查结果执行 SMTP 操作：
	  • MAIL FROM 身份
	  • PRA 身份
	• SPF REJECT 操作的情况下返回的 SMTP 响应代码。
	• 验证超时（秒）

邮件网关执行 HELO 身份检查并接受“无”和“不确定”验证结果并拒绝其他验证结果。SMTP 操作的 CLI 提示与所有身份类型的 CLI 提示相同。用户不对 MAIL FROM 身份定义 SMTO 操作。邮件网关自动接受所有该身份的验证结果。邮件网关对所有 REJECT 结果均使用默认拒绝代码和文本。

还可以在命令行界面中使用 `listenerconfig` 命令配置此功能。

接收的 SPF 信头

对 AsyncOS 进行 SPF/SIDF 验证配置时，设备会在邮件中添加 SPF/SIDF 验证信头 (`Received-SPF`)。`Received-SPF` 信头包含以下信息：

- **验证结果** - SPF 验证结果（请参阅验证结果, on page 29）。
- **身份** - SPF 验证检查的身份：HELO、MAIL FROM、PRA。
- **接收方** - 验证主机名（检查执行方）。
- **客户端 IP 地址** - SMTP 客户端的 IP 地址。
- **信封发件人** - 信封发件人邮箱。（注意，此地址可能与 MAIL FROM 身份不同，因为 MAIL FROM 身份不能空。）
- **x-sender** - HELO、MAIL FROM 或 PRA 身份的值。
- **x-conformance** - 一致性级别（请参阅表 - *SPF/SIDF* 一致性级别）以及 PRA 检查降级的执行情况。

以下示例展示如何向通过 SPF/SIDF 检查的邮件添加信头：

```
Received-SPF: Pass identity=pra; receiver=box.example.com;

client-ip=1.2.3.4; envelope-from="alice@fooo.com";

x-sender="alice@company.com"; x-conformance=sidf_compatible
```

Note `spf-status` 和 `spf-passed` 过滤器规则使用 received-SPF 信头判断 SPF/SIDF 验证状态。

确定对 SPF/SIDF 已验证邮件执行的操作

收到 SPF/SIDF 验证邮件时，您可能会根据 SPF/SIDF 验证结果采取不同的操作。可以使用以下邮件和内容过滤器规则确定 SPF/SIDF 已验证邮件的状态，并基于验证结果对邮件执行相应的操作：

- `spf-status`。此过滤器规则根据 SPF/SIDF 状态确定操作。可以为每个 SPF/SIDF 有效返回值指定不同的操作。
- `spf-passed`。此过滤器规则将 SPF/SIDF 结果表示为布尔值。

Note `spf-passed` 过滤器规则仅适用于邮件过滤器。

要处理更为精细的结果时，可以使用 `spf-status` 规则，要创建简单布尔值时，可使用 spf-passed 规则。

相关主题

- 验证结果, on page 29
- 在 CLI 中使用 spf-status 过滤器规则, on page 29
- GUI 中的 spf-status 内容过滤器规则, on page 30
- 使用 spf-passed 过滤器规则, on page 31

验证结果

如使用 spf-status 过滤器规则，可以使用以下语法检查 SPF/SIDF 验证结果：

```
if (spf-status == "Pass")
```

如果您希望在一个条件中检查多个状态判断，可以使用以下语法：

```
if (spf-status == "PermError, TempError")
```

此外，您还可以使用以下语法，根据 HELO、MAIL FROM 以及 PRA 身份检查验证结果：

```
if (spf-status("pra") == "Fail")
```

Note 只能使用 spf-status 邮件过滤器规则检查 HELO、MAIL FROM 和 PRA 身份验证结果。不能使用 spf-status 内容过滤器规则检查身份。spf-status 内容过滤器仅检查 PRA 身份。

您可能会收到以下任何一种验证结果。

- None - 由于缺少信息无法执行验证。
- Pass - 客户端获得使用特定身份发送邮件的授权。
- Neutral - 域所有者未表明客户端是否有权使用特定身份。
- SoftFail - 域所有者认为主机无权使用特定身份，但无意发表明确意见。
- Fail - 客户端无权使用特定身份发送邮件。
- TempError - 验证过程中出现瞬时错误。
- PermError - 验证过程中出现持久错误。

在 CLI 中使用 spf-status 过滤器规则

以下示例展示 spf-status 邮件过滤器的实际应用：

```
skip-spam-check-for-verified-senders:

if (sendergroup == "TRUSTED" and spf-status == "Pass"){
skip-spamcheck();
}
quarantine-spf-failed-mail:
if (spf-status("pra") == "Fail") {
if (spf-status("mailfrom") == "Fail"){
# completely malicious mail
quarantine("Policy");
} else {
```

```
if(spf-status("mailfrom") == "SoftFail") {
# malicious mail, but tempting
quarantine("Policy");
}
}
} else {
if(spf-status("pra") == "SoftFail"){
if (spf-status("mailfrom") == "Fail"
or spf-status("mailfrom") == "SoftFail"){
# malicious mail, but tempting
quarantine("Policy");
}
}
}
stamp-mail-with-spf-verification-error:
if (spf-status("pra") == "PermError, TempError"
or spf-status("mailfrom") == "PermError, TempError"
or spf-status("helo") == "PermError, TempError"){
# permanent error - stamp message subject
strip-header("Subject");
insert-header("Subject", "[POTENTIAL PHISHING] $Subject");
}
.
```

GUI 中的 spf-status 内容过滤器规则

您还可以从 GUI 的内容过滤器中启用 spf-status 规则。但是，使用 spf-status 内容过滤器规则时无法检查 HELO、MAIL FROM 和 PRA 身份。

要从 GUI 添加 spf-status 内容过滤器规则，请依次单击**邮件策略 (Mail Policies) > 传入内容过滤器 (Incoming Content Filters)**。然后从“添加条件”(Add Condition) 对话框添加 SPF 验证过滤器规则。为该条件指定一个或多个验证结果。

添加 SPF 验证条件后，请指定基于 SPF 状态执行的操作。例如，如果 SPF状态为 SoftFail，可能需要隔离邮件。

使用 spf-passed 过滤器规则

spf-passed 规则将 SPF 验证的结果显示为布尔值。以下示例展示使用 spf-passed 规则隔离未标记为 spf-passed 的邮件：

```
quarantine-spf-unauthorized-mail:

if (not spf-passed) {


quarantine("Policy");

}
```

Note 不同于 spf-status 规则，spf-passed 规则将 SPF/SIDF 验证值简化为简单的布尔值。以下验证结果在 spf-passed 规则中被视为未通过：None、Neutral、Softfail、TempError、PermError 以及 Fail。要基于更为精细的结果对邮件执行操作，请使用 spf-status 规则。

测试 SPF/SIDF 结果

测试 SPF/SIDF 验证结果，并使用这些结果确定如何处理 SPF/SIDF 失败，因为不同组织实施 SPF/SIDF 的方式不同。结合使用内容过滤器、邮件过滤器和“邮件安全监控 - 内容过滤器”(Email Security Monitor - Content Filters) 报告，测试 SPF/SIDF 验证的结果。

对 SPF/SIDF 验证的依赖程度决定 SPF/SIDF 结果的测试精细程度。

相关主题

- SPF/SIDF 结果基本粒度测试, on page 31
- SPF/SIDF 结果精细粒度测试, on page 32

SPF/SIDF 结果基本粒度测试

要获得针对传入邮件 SPF/SIDF 验证结果的基本衡量，可以使用内容过滤器和“邮件安全监控 - 内容过滤器”(Email Security Monitor - Content Filters) 页面。此测试可获得每种类型 SPF/SIDF 验证结果的邮件数量。

Procedure

步骤 1 在传入侦听程序的邮件流策略上启用 SPF/SIDF 验证，并使用内容过滤器配置要执行的操作。有关启用 SPF/SIDF 的详细信息，请参阅启用 SPF 和 SIDF, on page 24。

步骤 2 为每种类型的 SPF/SIDF 验证创建 **spf-status** 内容过滤器。使用命名约定表明验证类型。例如，对通过 SPF/SIDF 已验证邮件使用“SPF-Passed”，或对由于验证过程中出现瞬时错误而未能通过验证的邮件使用“SPF-TempErr”。有关创建 **spf-status** 内容过滤器的信息，请参阅 GUI 中的 spf-status 内容过滤器规则, on page 30。

步骤 3 处理大量 SPF/SIDF 验证邮件后，单击**监控 (Monitor)** > **内容过滤器 (Content Filters)** 可查看触发每种类型 SPF/SIDF 验证内容过滤器的邮件数量。

SPF/SIDF 结果精细粒度测试

要获得更全面的 SPF/SIDF 验证结果信息，可只对特定发件人组启用 SPF/SIDF 验证，查看这些特定发件人的验证结果。然后，为该特定组创建邮件策略，并在邮件策略上启用 SPF/SIDF 验证。有关创建内容过滤器和查看内容过滤器报告的信息，请参阅 SPF/SIDF 结果基本粒度测试, on page 31。如果发现验证有效，可参考 SPF/SIDF 验证决定丢弃或退回指定发件人组的邮件。

Procedure

步骤 1 创建 SPF/SIDF 验证邮件流策略。对传入侦听程序上的邮件流策略启用 SPF/SIDF 验证。有关启用 SPF/SIDF 的信息，请参阅启用 SPF 和 SIDF, on page 24。

步骤 2 创建 SPF/SIDF 验证的发件人组，并使用命名约定表明 SPF/SIDF 验证。有关创建发件人组的信息，请参阅“配置网关以接收邮件”一章。

步骤 3 为每种类型的 SPF/SIDF 验证创建 **`spf-status`** 内容过滤器。使用命名约定表明验证类型。例如，对通过 SPF/SIDF 已验证邮件使用“SPF-Passed”，或对由于验证过程中出现瞬时错误而未能通过验证的邮件使用“SPF-TempErr”。有关创建 **`spf-status`** 内容过滤器的信息，请参阅 GUI 中的 spf-status 内容过滤器规则, on page 30。

步骤 4 处理大量 SPF/SIDF 验证邮件后，单击**监控 (Monitor)** > **内容过滤器 (Content Filters)** 可查看触发每种类型 SPF/SIDF 验证内容过滤器的邮件数量。

DMARC 验证

基于域的邮件验证、报告和合规 (DMARC) 是旨在降低邮件滥用可能性的技术规范。DMARC 规范了邮件收件人如何使用 SPF 和 DKIM 机制执行邮件验证。要通过 DMARC 验证，邮件必须至少通过这些验证机制之一，且验证 ID 必须符合 RFC 5322。

邮件网关允许您：

- 使用 DMARC 验证传入的邮件。
- 定义配置文件覆盖（接受、隔离或拒绝）域所有者的策略。
- 向域所有者发送反馈报告，帮助改善身份验证配置。
- 如果 DMARC 汇总报告超过 10 MB 或 DMARC 记录的 RUA 标签上指定的大小，向域所有者发送传送错误报告。

AsyncOS 可以处理符合 DMARC 规范的邮件，例如 2013 年 3 月 31 日提交给 Internet 工程任务组 (IETF) 的邮件。有关详细信息，请访问 http://tools.ietf.org/html/draft-kucherawy-dmarc-base-02。

Note 邮件网关不会对带有不正确格式的DMARC记录的域的邮件执行DMARC验证。但是，该邮件网关可以接收和处理此类邮件。

相关主题

- DMARC 验证工作流程, on page 33
- 使用 DMARC 如何验证传入的邮件, on page 33

DMARC 验证工作流程

下文介绍 AsyncOS 如何执行 DMARC 验证。

1. AsyncOS 上配置的侦听程序收到 SMTP 连接。
2. AsyncOS 对邮件进行 SPF 和 DKIM 验证。
3. AsyncOS 从 DNS 获取发件人域的 DMARC 记录。
   - 如果未找到记录，AsyncOS 将跳过 DMARC 验证并继续处理。
   - 如果 DNS 查找失败，AsyncOS 将根据指定的 DMARC 验证配置文件执行操作。
4. 根据 DKIM 和 SPF 验证结果，AsyncOS 对邮件执行 DMARC 验证。

Note 如果 SPF 和 DKIM 验证已启用，DMARC 验证重新使用 DKIM 和 SPF 验证结果。

5. 根据 DMARC 验证结果和指定的 DMARC 验证配置文件，AsyncOS 接受、隔离或拒绝邮件。如果邮件并未因 DMARC 验证失败而被拒绝，AsyncOS 将继续处理。
6. AsyncOS 发送相应的 SMTP 响应并继续处理。
7. 如果启用发送汇总报告，AsyncOS 将收集 DMARC 验证数据，并在发送给域所有者的每日报告中添加这些数据。有关 DMARC 汇总反馈报告的详细信息，请参阅 DMARC 汇聚报告, on page 39。

Note 如果汇总报告超过 10 MB或 DMARC 记录的 RUA 标签指定的大小，AsyncOS 会向域所有者发送传送错误报告。

使用 DMARC 如何验证传入的邮件

使用 DMARC 如何验证传入的邮件

	相应操作	更多信息
第 1 步	根据个人需求，创建新的 DMARC 验证配置文件或修改默认 DMARC 验证配置文件。	创建 DMARC 验证配置文件, on page 35 编辑 DMARC 验证配置文件, on page 36
第 2 步	（可选）根据需求配置 DMARC 全局设置。	配置全局 DMARC 设置, on page 37
第 3 步	将邮件流策略配置为使用 DMARC 验证传入的邮件。	对邮件流策略配置 DMARC 验证, on page 38
第 4 步	（可选）配置 DMARC 反馈报告的返回地址。	配置 DMARC 反馈报告的返回地址, on page 38
第 5 步	（可选）请查看以下信息： • DMARC 验证和传入邮件报告 • 使用邮件跟踪查看 DMARC 验证失败的邮件	• “DMARC 验证”页面 • “传入邮件”页面 • 在旧界面上搜索邮件

相关主题

- 管理 DMARC 验证配置文件, on page 34
- DMARC 汇聚报告, on page 39
- 配置全局 DMARC 设置, on page 37
- 对邮件流策略配置 DMARC 验证, on page 38
- 配置 DMARC 反馈报告的返回地址, on page 38

管理 DMARC 验证配置文件

DMARC 验证配置文件是邮件网关的邮件流策略验证 DMARC 使用的一系列参数。例如，您可能要创建一个严格配置文件，拒绝来自特定域的不合规邮件，一个非严格配置文件，隔离来自另一个域的所有不合规邮件。

DMARC 验证配置文件包括以下信息：

- 验证配置文件的名称。
- DMARC 记录中的策略被拒时执行的邮件操作。
- DMARC 记录中的策略被隔离时执行的邮件操作。
- 临时失败情况下执行的邮件操作。
- 永久失败情况下执行的邮件操作。

相关主题

- 创建 DMARC 验证配置文件, on page 35
- 编辑 DMARC 验证配置文件, on page 36
- 导出 DMARC 验证配置文件, on page 36
- 导入 DMARC 验证配置文件, on page 36

- 删除 DKIM 验证配置文件, on page 19

创建 DMARC 验证配置文件

使用此步骤创建新 DMARC 验证配置文件。

Note 默认情况下，AsyncOS 提供默认 DMARC 验证配置文件。如不想创建新 DMARC 验证配置文件，可以使用默认 DMARC 验证配置文件。默认 DMARC 验证配置文件位于**邮件策略 (Mail Policies) > DMARC** 页面。有关编辑默认 DMARC 验证配置文件的说明，请参阅编辑 DMARC 验证配置文件, on page 36。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DMARC**。

步骤 2 单击**添加配置文件 (Add Profile)**。

步骤 3 输入配置文件的名称。

步骤 4 设置 AsyncOS 在 DMARC 记录中的策略被拒时执行的邮件操作。选择以下其中一个选项：

- **无操作 (No Action)**。AsyncOS 对 DMARC 验证失败的邮件不采取任何操作。
- **隔离 (Quarantine)**。AsyncOS 将 DMARC 验证失败的邮件隔离到指定隔离区。
- **拒绝 (Reject)**。AsyncOS 拒绝所有 DMARC 验证失败的邮件，并返回指定的 SMTP 代码和响应。默认值分别为 `550 和 #5.7.1 DMARC unauthenticated mail is prohibited`。

步骤 5 设置 AsyncOS 在 DMARC 记录中的策略被隔离时执行的邮件操作。选择以下其中一个选项：

- **无操作 (No Action)**。AsyncOS 对 DMARC 验证失败的邮件不采取任何操作。
- **隔离 (Quarantine)**。AsyncOS 将 DMARC 验证失败的邮件隔离到指定隔离区。

步骤 6 设置 AsyncOS 对 DMARC 验证过程中发生临时失败的邮件执行的邮件操作。选择以下其中一个选项：

- **接受 (Accept)**。AsyncOS 接受在 DMARC 验证过程中发生临时失败的邮件。
- **拒绝 (Reject)**。AsyncOS 拒绝在 DMARC 验证过程中发生临时失败的邮件，并返回指定 SMTP 代码和响应。默认值分别为 `451 和 #4.7.1 Unable to perform DMARC verification`。

步骤 7 设置 AsyncOS 对 DMARC 验证过程中发生永久失败的邮件执行的邮件操作。选择以下其中一个选项：

- **接受 (Accept)**。AsyncOS 接受在 DMARC 验证过程中发生永久失败的邮件。
- **拒绝 (Reject)**。AsyncOS 拒绝在 DMARC 验证过程中发生永久失败的邮件，并返回指定 SMTP 代码和响应。默认值分别为 `550 和 #5.7.1 DMARC verification failed`。

步骤 8 提交并确认更改。

编辑 DMARC 验证配置文件

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DMARC**。
步骤 2 单击目标验证配置文件名称。
步骤 3 按照创建 DMARC 验证配置文件, on page 35中的说明编辑目标字段。
步骤 4 提交并确认更改。

导出 DMARC 验证配置文件

可以将邮件网关上的所有 DMARC 验证配置文件导出到 configuration 目录下的一个文本文件中。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DMARC**。
步骤 2 单击**导出配置文件 (Export Profiles)**。
步骤 3 输入文件名称。
步骤 4 点击**提交**。

导入 DMARC 验证配置文件

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DMARC**。
步骤 2 单击**导入配置文件 (Import Profiles)**。
步骤 3 选择包含 DMARC 验证配置文件的文件。
步骤 4 单击**提交 (Submit)**。系统将警告您导入将会替换现有的所有 DMARC 验证配置文件。
步骤 5 单击**导入 (Import)**。
步骤 6 确认您的更改。

删除 DMARC 验证配置文件

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DMARC**。
步骤 2 选择要删除的验证配置文件。

步骤 3 单击**删除 (Delete)**。

步骤 4 确认删除。

配置全局 DMARC 设置

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DMARC (Mail Policies > DMARC)**。

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

步骤 3 更改下表中定义的设置。

DMARC 全局设置

全局设置	说明
特定发件人绕行地址列表	对来自特定发件人的邮件跳过 DMARC 验证。从下拉列表中选择一个地址列表。 **Note** 使用完整邮件地址或域创建的地址列表只能用于绕过 DMARC 验证。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。
绕过验证具有信头的邮件	对包含特定信头的邮件绕过 DMARC 验证。例如，使用此选项对来自发送邮件列表和信任转发器的邮件绕过 DMARC 验证。 输入一个信头或用逗号分隔的多个信头。
安排报告生成	您希望 AsyncOS 生成 DMARC 汇总报告的时间。例如，可以选择在非峰值时段生成汇总报告，避免影响邮件流。
生成报告的实体	生成 DMARC 汇总报告的实体。这有助于收到 DMARC 汇总报告的域所有者确定生成报告的实体。 输入有效的域名。
报告的其他联系信息	其他联系信息，例如，组织的客户支持详细信息，如果收到DMARC 汇总报告的域所有者要与生成报告的实体联系。
将所有汇总报告的副本发送到	将所有 DMARC 汇总报告的副本发送到特定用户，例如，分析汇总报告的内部用户。 输入一个邮件地址或用逗号分隔的多个地址。
错误报告	如果 DMARC 汇总报告超过 10 MB 或 DMARC 记录的 RUA 标签上指定的大小，向域所有者发送传送错误报告。 选中复选框。

步骤 4 提交并确认更改。

对邮件流策略配置 DMARC 验证

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 单击要执行验证的侦听程序的传入邮件策略。

步骤 3 在邮件流策略的“安全功能”(Security Features) 部分，选择**开 (On)** 启用 DMARC 验证

步骤 4 选择要用于策略的 DMARC 验证配置文件。

步骤 5 （可选）启用将 DMARC 汇总反馈报告发送到已启用 DMARC 域的 RUA 标签中的邮件发送地址。

每天都会生成汇聚返回报告。

步骤 6 提交并确认更改。

What to do next

相关主题

- DMARC 验证日志, on page 38

DMARC 验证日志

邮件日志会在 DMARC 验证的以下阶段添加日志消息。

- 在邮件上尝试 DMARC 验证
- DMARC 验证完成
- DMARC 验证详细信息包括 DKIM 和 SPF 调整结果
- 跳过针对邮件的 DMARC 验证
- DMARC 记录被获取和解析，或 DNS 失败
- 为域交付 DMARC 汇总报告失败
- 为域生成错误报告
- 为域交付错误报告成功
- 为域交付错误报告失败

配置 DMARC 反馈报告的返回地址

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > **返回地址 (Return Addresses)**。

步骤 2 单击**编辑设置 (Edit Settings)**。

步骤 3 提供 DMARC 汇总反馈报告的返回地址。

步骤 4 提交并确认更改。

DMARC 汇聚报告

DMARC 依赖反馈机制以安全和可扩展的方式实施域所有者策略。此反馈机制可帮助域所有者改善身份验证部署。

如使用 AsyncOS 执行 DMARC 验证，并已在邮件流策略中启用发送汇总反馈报告，AsyncOS 将每天生成汇总反馈报告，并将其发送给域所有者。这些报告采用 XML 格式并存档为 GZip 文件。

Note AsyncOS 生成的所有 DMARC 汇总反馈报告均符合 DMARC。

DMARC 汇总反馈报告包含以下部分：

- 报告发件人的元数据（如邮件地址和报告 ID 编号）。
- 已发布 DMARC 策略的详细信息。
- DMARC 策略处理的详细信息（例如，源 IP 地址和处置摘要）。
- 域 ID
- DMARC 验证结果和验证概述。

相关主题

- DMARC 汇总反馈报告示例, on page 39

DMARC 汇总反馈报告示例

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <version>1.0</version>
  <report_metadata>
    <org_name>cisco.com</org_name>
    <email>noreply-dmarc-support@cisco.com</email>
    <extra_contact_info>http://cisco.com/dmarc/support</extra_contact_info>
    <report_id>b1d925$4ecceab=0694614b826605cd@cisco.com</report_id>
    <date_range>
      <begin>1335571200</begin>
      <end>1335657599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>example.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>none</p>
    <sp>none</sp>
    <pct>100</pct>
  </policy_published>
  <record>
```

```
    <row>
      <source_ip>1.1.1.1</source_ip>
      <count>2</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>fail</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
   <envelope_from>example.com</envelope_from>
      <header_from>example.com</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>example.com</domain>
     <selector>ny</selector>
        <result>fail</result>
      </dkim>
      <dkim>
        <domain>example.net</domain>
<selector></selector>
        <result>pass</result>
      </dkim>
      <spf>
        <domain>example.com</domain>
<scope>mfrom</scope>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
</feedback>
```

伪造邮件检测

邮件伪造（也称为欺骗、CEO 欺诈或商业电子邮件妥协）指如下过程：改变邮件信头以隐藏发件人的真实身份，从而使邮件看似是您认识的人发来的邮件。假设，欺诈者冒充组织管理人员向员工发送伪造信息，要求提供客户清单及其个人身份信息 (PII)。此员工不知道发件人的真实身份，提供了客户清单及其 PII。欺诈者使用 PII 执行身份盗窃。

邮件网关可以检测使用伪造发件人地址（“发件人:”信头）的欺诈邮件，并对此类邮件执行指定操作。例如，邮件网关可以检测使用伪造发件人地址的邮件，并将“发件人：”信头替换为信封发件人。在这种情况下，员工将看到真实发件人（欺诈者）的邮件地址，而不是伪造的邮件地址。

相关主题

- 设置伪造邮件检测, on page 40
- 监控伪造邮件检测结果, on page 42
- 在邮件跟踪中显示伪造邮件检测详细信息, on page 42

设置伪造邮件检测

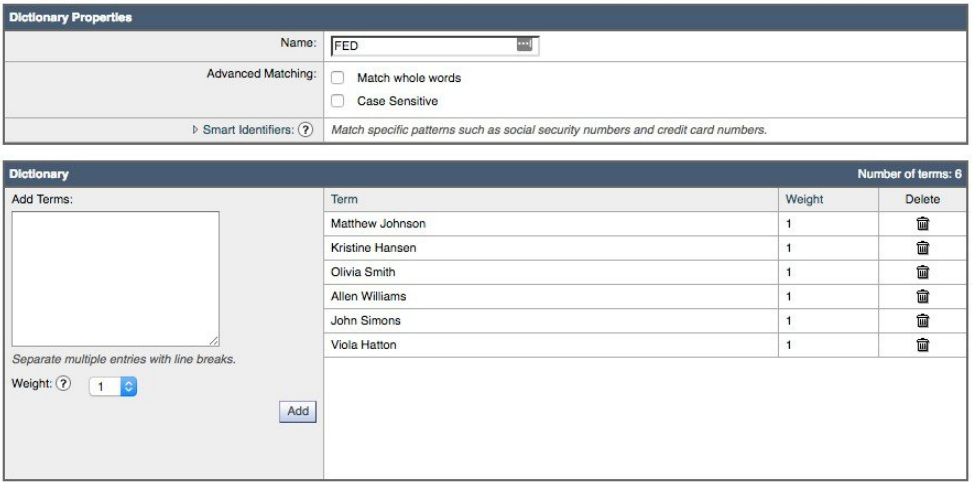
1. 标识组织中其邮件很可能是伪造的用户（例如，管理人员）。创建新的内容字典，并将已标识用户的姓名添加到该词典。

在创建内容字典时，

- 输入用户名而不是电子邮件地址。例如，输入“Olivia Smith”而不是“olivia.smith@example.com”。
- 请勿配置高级匹配和智能标识符。
- 请勿为使用的术语选择权重。
- 请勿使用正则表达式。

下图显示了为伪造邮件检测创建的内容字典示例。

Figure 3: 伪造邮件检测的内容词典



有关配置内容字典的说明，请参见添加词典。

2. 创建传入内容或邮件过滤器以检测伪造邮件以及邮件网关对这些邮件执行的操作。使用下列内容：
   - **条件/规则：**伪造邮件检测（请参阅内容过滤器条件和邮件过滤器规则）

Note 如果要跳过针对特定发件人的邮件的伪造邮件检测过滤器，请从**例外列表**下拉列表中选择地址列表。只能选择使用完整邮件地址创建的地址列表。有关添加例外地址列表的详细信息，请参阅为传入连接规则使用发件人地址列表。

   - **操作：**基于您的要求的伪造邮件检测或任何其他操作。（请参阅内容过滤器条件和邮件过滤器规则。）
3. 将新创建的内容过滤器添加到传入邮件策略。请参阅根据每个用户执行邮件策略的方法。

监控伪造邮件检测结果

要查看有关检测到的伪造邮件的数据，请参阅“伪造邮件匹配项”(Forged Email Matches) 报告页面（**监控 (Monitor)** > **伪造邮件匹配项 (Forged Email Matches)**）。此报告页面包括以下报告：

- **伪造邮件匹配项排行榜**。显示内容字典中与传入邮件中的伪造“发件人：”信头匹配的前十个用户。
- **伪造邮件匹配项: 详细信息**. 显示内容词典中与传入邮件中的伪造“发件人：”信头匹配所有用户的列表，对于给定用户，还会显示匹配的邮件的数量。单击该数字可查看邮件跟踪中的邮件列表。

在邮件跟踪中显示伪造邮件检测详细信息

要在邮件跟踪中显示邮件网关检测到的伪造邮件的详细信息，请确保：

- 邮件跟踪服务已启用。请参阅邮件跟踪。
- 用于检测伪造邮件的内容或邮件过滤器可正常运行。

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。