# 排除常见邮件安全设备错误

## 目录


[简介](#)

[ESA上常见的配置错误有哪些？](#)

[HAT](#)

[策略](#)

[传入中继](#)

[DNS](#)


## 简介

本文档介绍思科邮件安全设备(ESA)上的常见配置错误。

## 环境

- 产品：思科邮件安全设备(ESA)
- 软件:AsyncOS for ESA（版本因部署而异）
- 范围:将此指南应用于入站和出站邮件策略（如果适用）；在更改之前查看每个部分。

## 先决条件

- 对ESA的管理访问（GUI或CLI）
- 能够审核邮件日志和邮件跟踪以进行验证
- 如果使用基于SBRS的发件人组，则启用信誉服务SenderBase信誉得分SBRS
- 主机访问表(HAT)在邮件策略评估之前对连接主机进行分类的意识，这将影响后续控制如何应用

## 一般验证

- 使用Monitor > Overview和message tracking确认预期的发件人组分类、策略匹配以及更改后的传送结果。成功表示更改后会显示预期的发件人组、策略和传送结果。
- 在收紧信誉或过滤设置后，在7-144天内监控隔离区和误报，并根据需要针对已知业务合作伙伴进行调整。

# 邮件安全设备(ESA)上的常见配置错误

使用这些检查可以识别和更正邮件安全设备(ESA)上的常见配置错误。 每个子部分使用一致的问题、原因、解决方法和检验模式，以便快速诊断和纠正问题。

# 主机访问表(HAT)

## 症状

- 由于基于信誉的发件人组过于宽松，垃圾邮件被接受。
- 由于连接控制过于严格，合法邮件被限制或阻止。

## 原因

- 发件人组配置有不适当的SenderBase信誉得分(SBRS)范围或域名系统(DNS)验证设置。

## 分辨率

1. 请勿向允许列表添加正的SBRS值（例如，+5或+7）。对于基于SBRS的允许列表，仅使用从9.0到10.0的分数，并使用邮件跟踪进行验证。
2. 仅在需要时配置未知发件人列表和DNS验证功能。如果不需要，请禁用UNKNOWNLIST、Envelope SenderDNS Verification和Connecting HostDNS Verification。

---



注意：ESA用户界面将传统术语UNKNOWNLIST用于未知发件人列表。

---

3. 要避免每个策略设置不一致，请配置全局默认值：选择Mail Policies > Mail Flow Policies > Default Policy Parameters，并在其中设置邮件大小和其他默认参数。
4. 为大多数发件人（例如3）设置一个合理的默认最大连接值，并将其应用为新邮件流策略的默认值；根据需要针对已知的大容量发件人进行调整。
5. 根据您的风险承受能力配置阻止列表SBRS范围。在许多部署中，阻止SBRS -10.0到–2.0可能会导致低误报率。通过邮件跟踪进行验证，并根据业务合作伙伴进行调整。

# 策略

### 症状/影响

- 邮件被意外扫描或隔离，因为非默认邮件策略会覆盖全局默认值。
- 出站邮件会触发不必要的反垃圾邮件/爆发过滤器操作，从而增加处理时间和误报。
- 邮件显示为空白，因为已去除受感染的附件，并且邮件正文仅包含删除的内容。

### 原因

- 非默认策略可复制或覆盖默认反垃圾邮件、防病毒、内容过滤器或爆发过滤器设置，无需特定要求。
- 出站策略应用以入站为中心的扫描功能。

### 分辨率

1. 为其应用到的收件人命名邮件策略（例如，Inbound_Executions）以及为其所执行的操作命名内容过滤器（例如，Q_basic_attachments和Dspoferss）。
2. 对于非默认策略，请选择Use Default Settings for Anti-Spam、Anti-Virus、Content Filters和Outbreak Filters，除非需要记录的例外。
3. 清除丢弃感染病毒的附件的复选框，以避免传送包含可能显示为空的已剥离内容的邮件。
4. 对于出站防病毒操作，请通知发件人而不是收件人。
5. 在出站邮件策略上禁用爆发过滤器和反垃圾邮件，除非存在显式出站使用案例。

### 验证

- 使用邮件跟踪确认目标邮件策略已匹配，并且默认扫描设置将继承到预期位置。
- 发送受控出站测试邮件，并确认除非通过例外配置反垃圾邮件/爆发过滤器未应用。

## 传入中继

### 症状

- 内部邮件服务器被视为外部发件人，这可能会导致意外限制、过滤或基于信誉的操作。

### 原因

- 内部邮件服务器IP地址或网络未配置为传入中继，或者传入中继功能被禁用。
- 内部中继主机未分类为专用HAT发送方组，这可能导致意外的连接限制或目录搜集攻击防御

(DHAP)行为。

### 分辨率

1. 在GUI中，选择Mail Policies > Incoming Relays，然后添加内部邮件服务器IP地址或网络。
2. 确保启用传入中继功能（不要只向表中添加条目）。
3. 为前一个列表中允许列表中列出的内部中继创建专用主机访问表(HAT)发件人组，以用于报告目的。在根据需要保持启用反垃圾邮件和防病毒扫描的同时，配置无速率限制和目录搜集攻击防御(DHAP)（如果适当）。DHAP限制简单邮件传输协议(SMTP)会话期间无效收件人枚举尝试。
4. 如果基于非中继流量的信誉丢弃邮件，请添加一个邮件过滤器，在必要时对中继邮件应用等效处理。示例：

```
Drop_Low_Reputation_Relayed_Mail:
if reputation <= -2.0
{ drop(); }
```

### 验证

- 在Monitor > Overview中，确认内部服务器不再显示为不受信任的外部发件人。
- 在邮件跟踪/邮件日志中，确认应用了预期的发件人组（例如，内部中继发件人组）。

---



注意：如果重新注入邮件（例如，通过入站策略重新处理用户间邮件），请根据需要免除过滤器的重新注入接口。重新注入通过策略评估发送回邮件，因此过滤器可以再次匹配同一邮件，除非排除该接口。

---

## DNS

### 症状

- DNS解析器选择或拆分：DNS配置导致传送失败、SMTP事务或基于DNS的检查失败。

### 环境

- 适用于需要公共DNS解析、仅内部DNS解析或内部域和服务水平分割DNS的部署。

## 症状

- 消息跟踪显示MX、AAA、PTRR或信誉相关查询的DNSlookup失败/超时。
- 由于重复的DNS重试，邮件传送延迟。

## 原因

- ESA配置为使用无法解析所需公共记录、所需内部记录或两者兼有的解析程序。
- 根据源网络，水平分割DNS为同一域返回不同的答案，它是必需的，但内部域或服务不实施。

## 分辨率

根据ESA解析记录的位置配置域名系统(DNS)解析：公共互联网、内部专用域或两者：

1.当ESA主要需要公共DNS记录且策略允许时，请使用公共递归解析器。

2.当ESA必须解析仅内部区域、内部邮件交换(MXX)记录、轻量级目录访问协议(LDAPP)记录或其他专用服务时，请使用内部DNS或水平分割DNS。

3.如果设备主要解析Internet邮件记录，并且没有内部专用区域或策略限制，则公共DNS是合适的。

根据需要使用内部DNS或拆分DNS

- 仅限内部使用的域
- InternalMXX记录
- 水平分割DNS（根据源网络对同一域使用不同的答案）
- 合规性或安全策略需要内部递归解析器
- 路由所需的专用DNS区域
- 轻型目录访问协议(LDAPP)所需的专用DNS区域
- ESA使用的内部服务所需的专用DNS区域

## 验证

- 确认ESA可以解析所需的公共和内部主机名（如果适用），并且基于DNS的邮件传送和信誉检查成功进行邮件跟踪。

# 邮件和内容过滤器

最常见的错误是在不需要匹配条件时在过滤器中添加匹配条件。

- 空白条件：当过滤器必须为给定邮件策略中的每封邮件运行时，请将此条件留空。
- 评估行为：在asyncOS邮件过滤器中，空条件评估为true，因此过滤器对到达它的每个邮件运行。
- 范围：通过将过滤器附加到适当的传入或传出邮件策略来控制范围。
- Order:邮件过滤器按顺序评估邮件属性和操作。内容过滤器通常由调用它们的邮件策略来确定。

示例：

- 当目标是针对特定用户或组时，通常不需要在邮件过滤器中使用rcpt-to条件。首选基于收件人的传入邮件策略，并在要求完全映射到收件人或收件人组时将内容过滤器应用于该策略。对于策略匹配无法表示要求的异常，请保留rcpt-to条件。
- 如果目的是阻止特定连接类型，则通常会在丢弃连接之前测试其是否存在。将过滤器配置为直接删除目标附件类型；仅当需要不同操作（具体取决于附件是否存在）时，才使用附件存在测试。
- 仅当邮件必须绕过剩余过滤器时，才使用deliver()。deliver()操作停止进一步的过滤器处理，然后传送消息；要传递邮件而不跳过其余过滤器，请勿配置显式deliver()操作（隐式传递适用）。

# 开放式中继防御

## 症状/影响

- 第三方中继测试报告设备接受格式错误或危险的收件人地址。
- Publicblocklists列出发送IP，因为SMTP地址解析允许常用于验证开放中继的模式。

## 原因

- 简单邮件传输协议SMTP地址解析和字符处理允许无效的地址格式（例如，双@符号）或地址文字，即直接写入地址而非域名的IP地址。

## 分辨率

某些服务会测试消息传输代理(MTA)是否接受可能指示开放中继条件的错误地址。配置严格的解析

和拒绝行为，以便ESA在SMTP会话期间拒绝这些地址。

- 在ALLOWLIST前添加用于报告的中继测试源的专用HAT发件人组。适当时，配置无速率限制和无目录搜集攻击防御(DHAP)，同时根据需要保持启用反垃圾邮件和防病毒。
- 启用Strict Address Parsing（默认设置为Loose）以防止地址中出现双@符号。
- 拒绝（不删除）无效字符以防止接受格式错误的地址。
- 拒绝（不接受）地址文字，并输入以下字符：*%!\\/?

### 验证

- 运行外部中继测试并确认ESA在SMTP会话期间拒绝格式错误的收件人地址。
- 使用邮件跟踪确认中继测试发件人组已匹配，并且邮件已按照预期扫描设置进行处理。

## 相关信息

- 获取技术支持和文档
- ReviewAsyncOSS forESA用户指南
- 邮件安全设备(ESA)安装和配置指南（HAT、邮件策略和邮件过滤器）

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。