

# 由思科电子邮件安全工具(ESA)的垃圾邮件获得到您的组织里

## 目录

### [简介](#)

### [方法](#)

- [1. 合法消息/营销邮件](#)
- [2. 反垃圾邮件没有正确地更新](#)
- [3. 邮件策略或消息过滤器](#)
- [4. 邮件流量策略](#)
- [5. 消息是垃圾邮件](#)

## 简介

本文描述发送消息到新闻组电子邮件能加入您的组织的五个方法。

## 方法

### 1. 合法消息/营销邮件

合法消息由用户选择或他们的名称被出售对另一个组织。在第一个案件中用户将需要采取步骤从列表取消预订。如果它是后者，再请送消息给[spam@access.ironport.com](mailto:spam@access.ironport.com)，因此反垃圾邮件定义可以更新全局，改善整体垃圾邮件捕获速率您的ESA。启用在流入的邮件策略的营销邮件可能帮助改变“销售”在“垃圾邮件的”此消息的观念。

### 2. 反垃圾邮件没有正确地更新

反垃圾邮件禁用或功能键超时。要确认反垃圾邮件是否更新，请去**GUI > Security Services > IronPort反垃圾邮件**。在此面板内您在最后6个小时之内应该看到更新到规则集或引擎。并且从在顶部的此选项卡的内部您能保证反垃圾邮件服务启用。对于功能键状态的回顾您可以去检查的系统管理选项卡>功能键反垃圾邮件密钥的状况。

### 3. 邮件策略或消息过滤器

如果反垃圾邮件安全引擎为一特定发送方或收件人禁用每项一项客户邮件策略，垃圾邮件能进入您的组织。另一个方式跳过垃圾邮件过滤是通过消息过滤(CLI：**过滤器命令**)。

## 4. 邮件流量策略

使用消息的ICID，消息分类。在这种情况下很可能反垃圾邮件安全功能被关闭，改写邮件策略。您能通过查看邮件日志确定此，在您首先将需要查看ICID了解的日志内哪SenderGroup消息分类了到。从那里相关的邮件流量策略的回顾。如果有很多条目在您的WhiteList，您可能需要检查进来发现的某些消息他们是否乘反垃圾邮件引擎扫描。打开消息的报头并且寻找报头X IronPort垃圾邮件，此报头出现意味着消息通过引擎。

## 5. 消息是垃圾邮件

消息是实际垃圾邮件。您确认了消息乘反垃圾邮件引擎扫描了使用消息跟踪功能(在消息跟踪，请寻找“案件”)。如果案件判决是负的，并且视为消息是垃圾邮件，请送原始消息给 [spam@access.ironport.com](mailto:spam@access.ironport.com)。这可能是再设计一个新的垃圾邮件威胁发布的或一个更旧的威胁的一个事例。

处理垃圾邮件提交自动，并且手动程序和那里是您的特定提交的没有反馈。在任意时候您能与Cisco TAC联系和请求评估和答复。