# 反垃圾邮件、防病毒、Graymail和爆发过滤器的最佳实践指南

## 目录



## 概述

以垃圾邮件、恶意软件和被混和的攻击的形式，组织面对的绝大多数的威胁、攻击和讨厌通过电子邮件来。Cisco的电子邮件安全工具(ESA)包括几个不同的技术和功能切断这些威胁在网关，在他们加入组织前。本文将描述最佳实践途径配置反垃圾邮件、防病毒、Graymail和爆发过滤器，在入站和出站电子邮件流。

## 反垃圾邮件

反垃圾邮件保护寻址各种各样的已知威胁包括垃圾邮件、网络钓鱼和僵死攻击，以及难对检测低音量，短期的电子邮件威胁例如[“419"诈欺](#)。另外，反垃圾邮件保护识别新和演变的被混和的威胁例如分配有恶意的内容的垃圾邮件攻击通过下载URL或可执行。

Cisco电子邮件安全提供以下反垃圾邮件解决方案：

- IronPort反垃圾邮件过滤(IPAS)
- Cisco智能多扫描过滤(IMS)

您在一项特定的邮件策略准许和启用在您的ESA的两解决方案，但是能只使用一。为此最佳实践文档，我们使用IMS功能的目的。

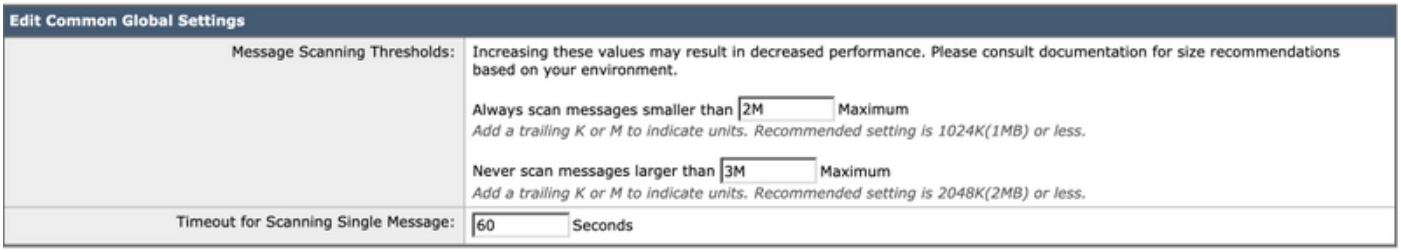
## 验证功能键

- 在ESA，请导航到**系统管理>功能键**
- 寻找智能多扫描许可证并且确保它是活跃的。

## 启用智能多扫描(IMS)全局

- 在ESA，请导航对**安全服务> IMS和Graymail**
- 点击在**IMS全局设置的Enablebutton** ：

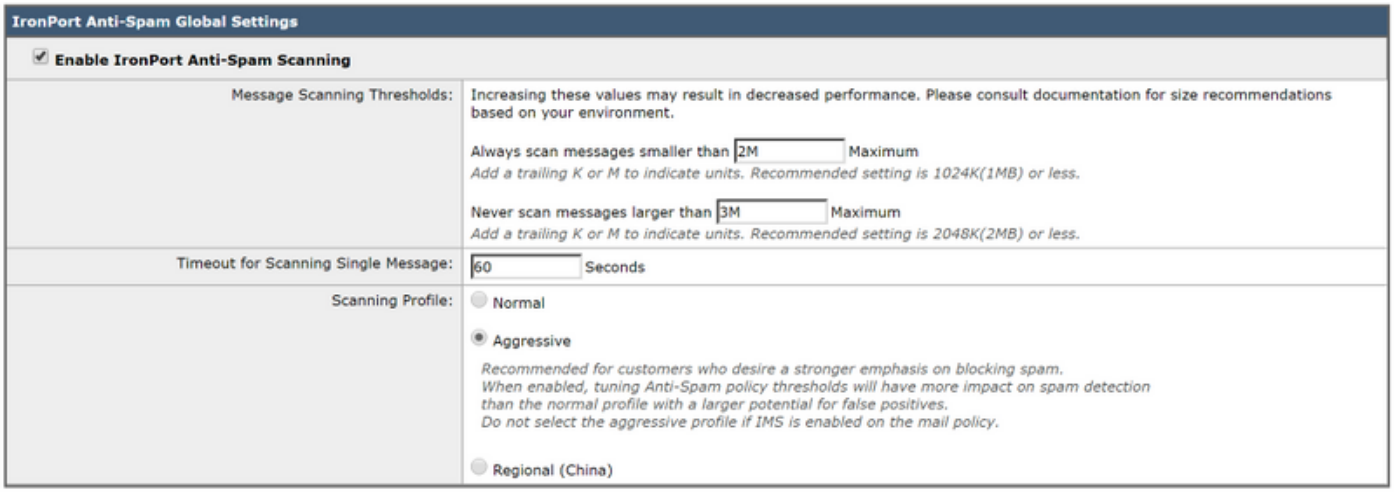

- 寻找**普通的全局设置**并且单击**编辑全局设置**
- 您能配置多设置。 推荐的设置在下面镜像显示：




- 点击**Submitand进行您的更改。**

如果没有一IMS许可证订阅：

- 导航对**安全服务> IronPort反垃圾邮件**
- 点击在**IronPort反垃圾邮件概述的Enablebutton**
- 单击**编辑全局设置**
- 您能配置多设置。 推荐的设置在下面镜像显示：

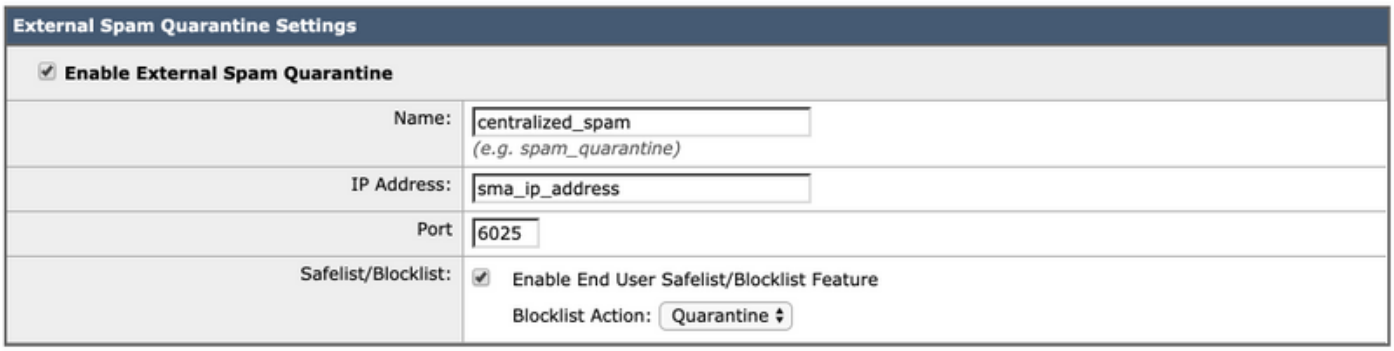



- Cisco推荐选择希望对阻塞垃圾邮件的一个强重点的客户的**积极的**扫描配置文件。
- 点击**Submitand进行您的更改**

## 启用集中化垃圾邮件检疫

因为反垃圾邮件有选项发送检疫，请注意垃圾邮件检疫设置：

- 导航对**安全服务>垃圾邮件检疫**
- 单击**Configurebutton**把您带对以下页。
- 您能通过检查**enablebox**启用检疫和指向在SecurityManagement设备将集中的检疫(SMA) byfilling在SMANAMEAND **IP地址**。 推荐的设置如下所示：



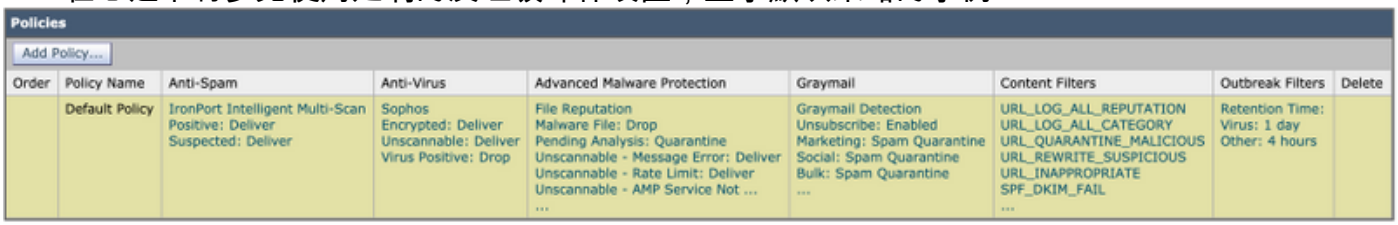

- 点击**Submitand进行您的更改**

关于安装和集中化检疫的更多信息，请参考最佳实践文档：
[集中化策略的最佳实践、病毒和爆发检疫设置和迁移从ESA到SMA]

## 配置在策略的反垃圾邮件

一旦智能多扫描配置全局，您能当前应用智能多扫描邮寄策略：

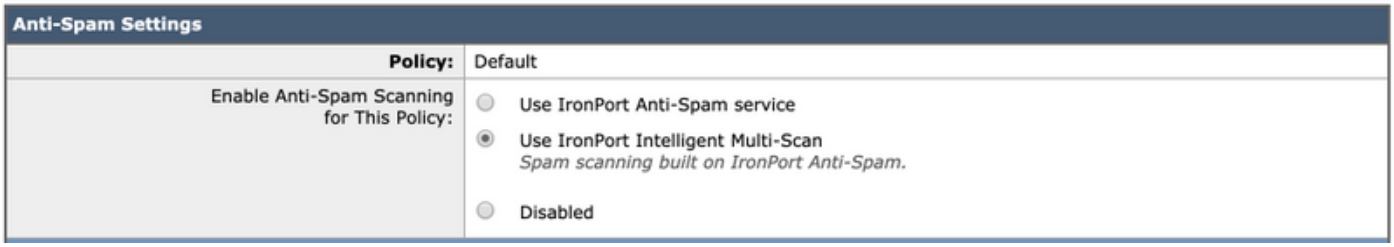
- 导航**邮寄策略>流入的邮件策略**
- 默认情况下流入的邮件策略使用IronPort反垃圾邮件设置。
- 单击在反**垃圾邮件下的**蓝色链路将允许该特定的策略使用定制的反垃圾邮件设置。
- 在您之下将参见使用定制的反垃圾邮件设置，显示默认策略的示例：




自定义一项流入的邮件策略的反垃圾邮件设置通过单击在反**垃圾邮件下的**蓝色链路您希望定制的策略的。

您能选择您希望为此策略启用的反垃圾邮件扫描选项。

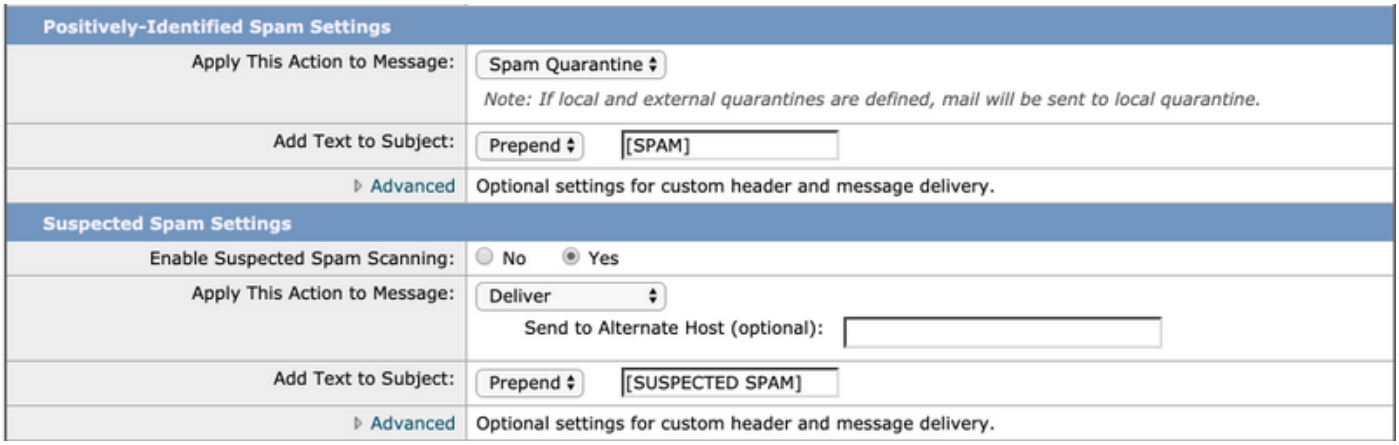
- 为此最佳实践文档，请在使用**IronPort**智能多扫描旁边单击单选按钮：



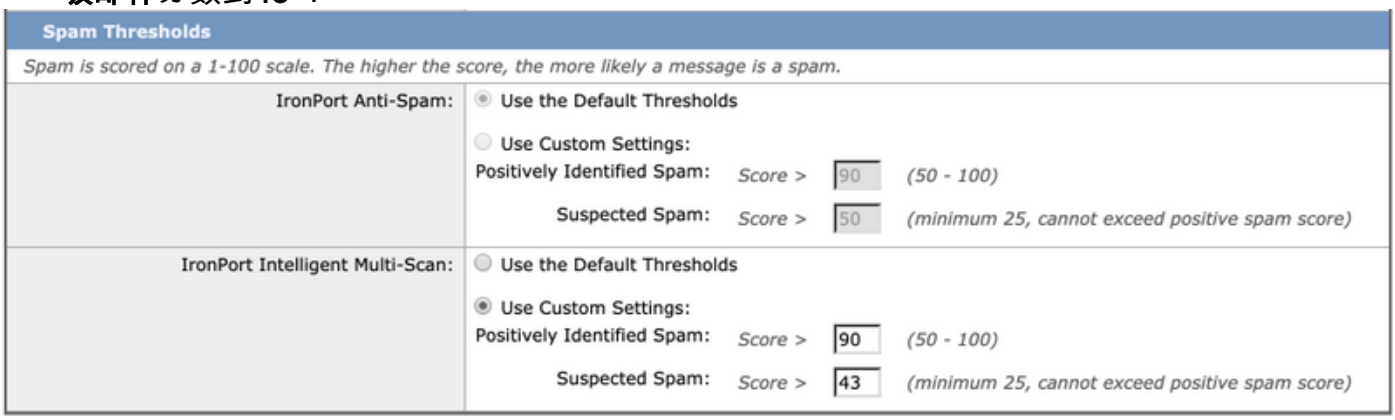

下两个部分包括正**识别的垃圾邮件设置**和**怀疑的垃圾邮件设置**：

- 建议的最佳实践是配置在正**识别的垃圾邮件**设置的**检疫**操作与被加在前面的文本**[SPAM]**被添加到主题和;

- 应用**传送， Suspected垃圾邮件设置的**操作与被加在前面的文本**[SUSPECTED SPAM]**添加了到主题：




- **垃圾邮件门限值设置**可以更改，并且推荐的设置是定制正**识别的垃圾邮件**分数到**90**和**怀疑的垃圾邮件**分数到**43** ：




- 点击**Submitand进行您的更改**

# 防病毒

抗病毒防护通过三分之二当事人引擎提供– Sophos和McAfee。这些引擎将过滤所有已知有恶意的威胁，下降，清洗或者检疫他们如配置。

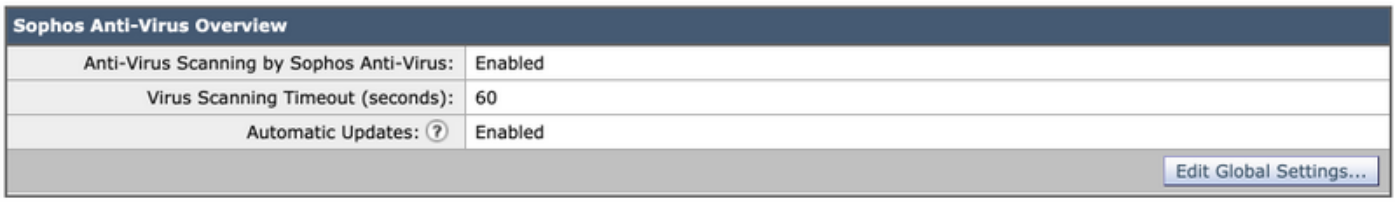
## 验证功能键

检查两个功能键启用和激活：

- 去**系统管理>功能键**
- 确保**Sophos防病毒，**并且**McAfee**许可证是活跃的。

## Enable (event)抗病毒扫描

- 导航对**安全服务>防病毒- Sophos**
- 点击**Enablebutton**。
- 确保**自动更新启用，**并且Sophos抗病毒文件更新优良工作。如果需要，**当前请**单击**更新**立即启动文件更新：





- 点击**Submitand进行您的更改**。

如果McAfee许可证是活跃的，请导航对**安全服务>防病毒- McAfee**

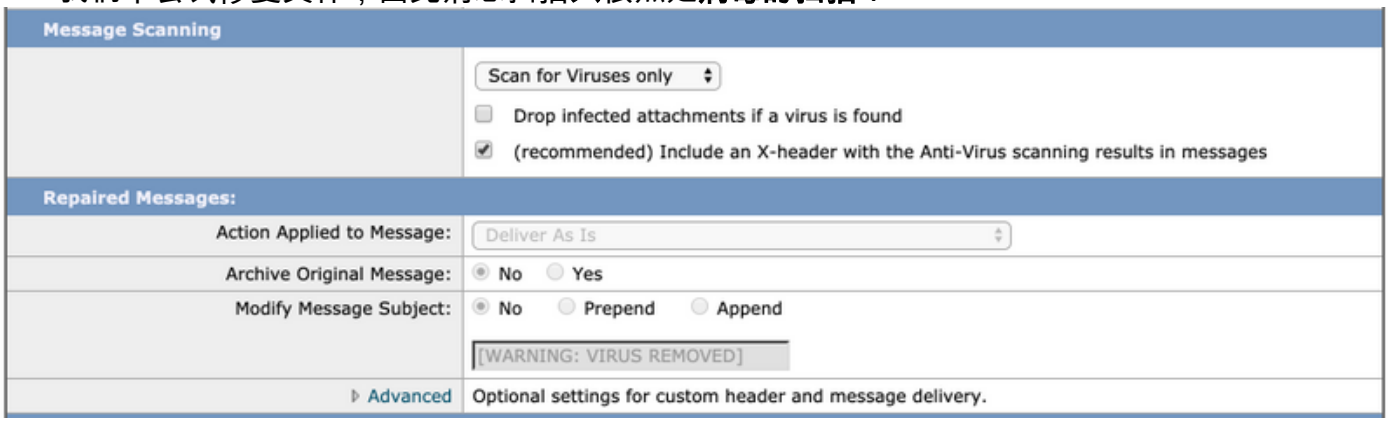
- 点击**Enablebutton**。
- 确保**自动更新启用**，并且McAfee抗病毒文件更新优良工作。如果需要，**当前请**单击**更新**立即启动文件更新。
- 点击**Submitand进行您的更改**

## 配置在邮件策略的防病毒

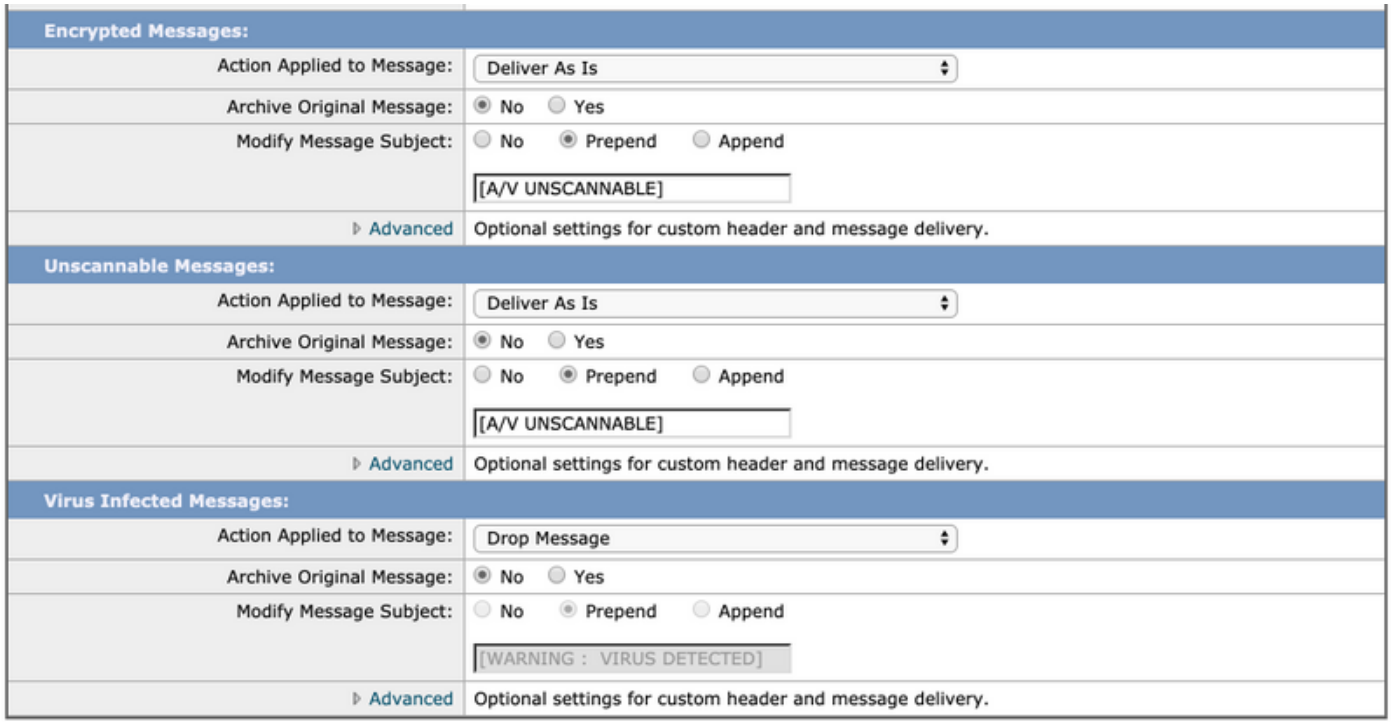
在流入的邮件策略，推荐下列：

- 导航**邮寄策略>流入的邮件策略**
- 一项流入的邮件策略的自定义**抗病毒**设置通过单击在防病毒下的蓝色链路您希望定制的策略的。
- 您能选择您希望为此策略启用的抗病毒扫描选项。
- 为此最佳实践文档，请选择**McAfee**和**Sophos防病毒**：


- 我们不尝试修复文件，因此消息扫描**只**依然是**病毒的扫描**：




- **加密的**和**Unscannable消息的**推荐的操作是**传送如现状**与他们的注意的一已修改标题栏。
- 防病毒的推荐的策略是**丢弃**所有**感染病毒的消息**如下面镜像所显示：




- 点击**Submitand进行您的更改**

一项相似的策略为流出的邮件策略建议使用，然而，我们不推荐正在修改在出站电子邮件的标题栏。

# Graymail

在电子邮件安全工具的graymail管理解决方案包括两个组件：一个集成graymail扫描引擎和一基于网云的取消预订服务。使用取消预订服务， graymail管理解决方案允许组织识别graymail使用集成graymail引擎和实行相应的策略控制和为最终用户提供一容易机制从不需要的消息取消预订。

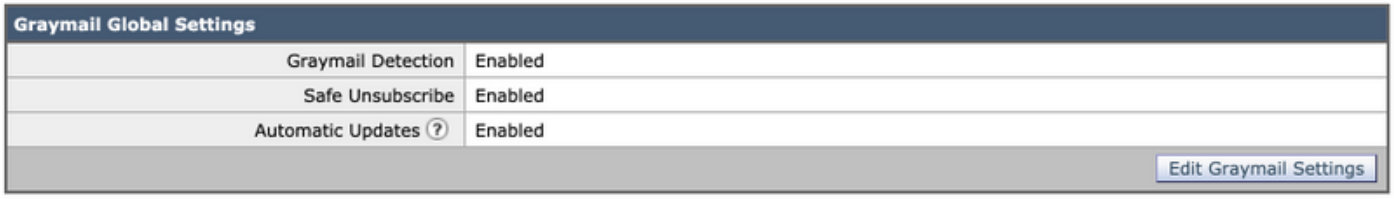
Graymail类别包括营销电子邮件、社会网络电子邮件和大批电子邮件。高级选项包括添加一个自定义报头，发送对一台备选主机和归档消息。对于此最佳实践，我们将启用默认邮件策略的Graymail的安全取消预订功能。

## 验证功能键

- 在ESA，请导航到**系统管理>功能键**
- 寻找**Graymail安全Unsubscription**并且确保它是活跃的。

## 启用Graymail和安全取消预订服务

- 在ESA，请导航对**安全服务> IMS和Graymail**
- 点击**编辑**在**Graymail全局设置的**Graymail Settingsbutton
- 选择所有选项-**启动Graymail检测**，**启用取消预订的安全**并且**启用自动更新**：



- 点击**Submitand进行您的更改**

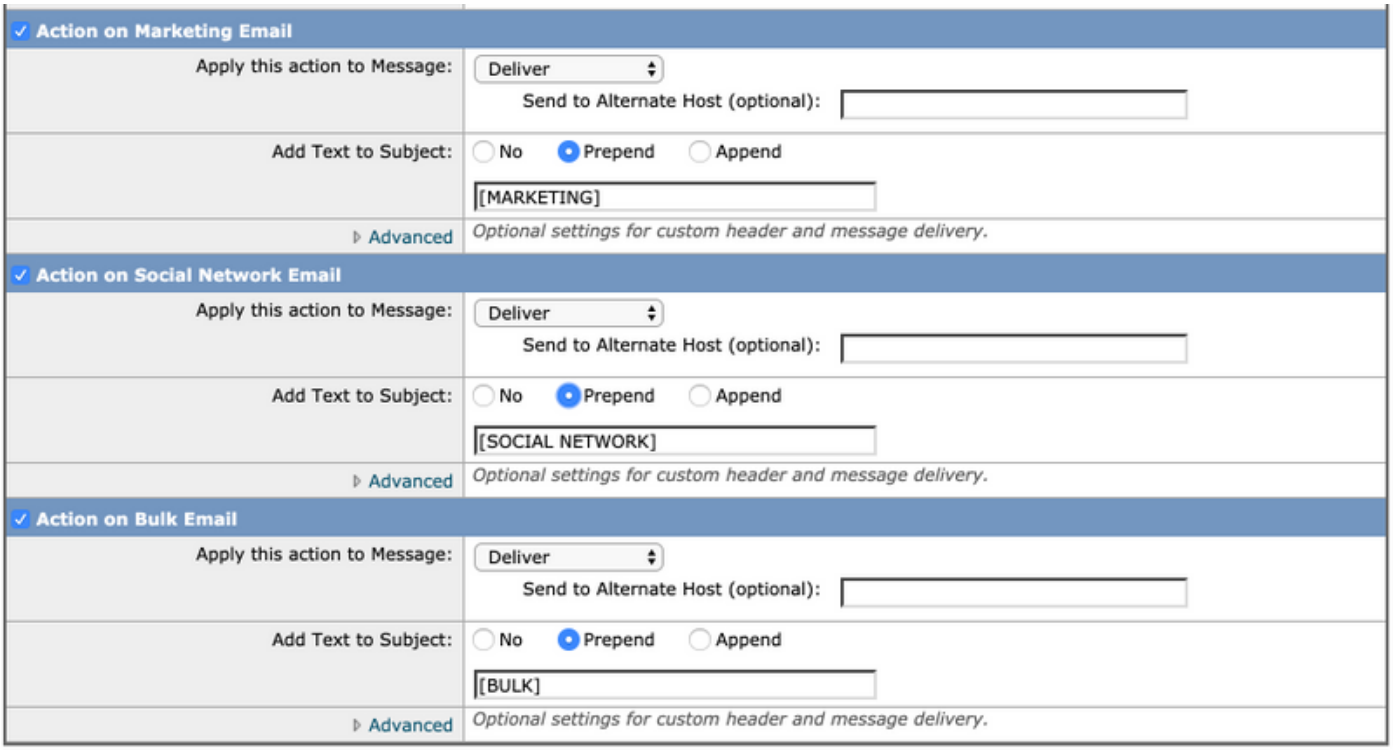
## 配置Graymail和安全取消预订在策略

一旦Graymail和安全Unsubscribe配置全局，您能当前运用这些服务邮寄策略。

- 导航**邮寄策略>流入的邮件策略**
- 单击在**Graymail下的**蓝色链路将允许该特定的策略使用定制的Graymail设置。
- 您能选择您希望为此策略启用的Graymailoptions。
- 为此最佳实践文档，请在**Enable (event)**此策略的Graymail检测旁边单击单选按钮并且**启用此策略的Graymail取消订阅**：


下三个部分包括**在营销电子邮件设置的在社会网络电子邮件设置的操作，在大批电子邮件设置的操作**和**操作**。

- 建议的最佳实践是启用所有和保持操作和**传送**与加在前面文本被添加到主题关于类别如下所示：




- 点击**Submitand进行您的更改**

流出的邮件策略在**已禁用**情况应该安排Graymail保持。

# 爆发过滤器

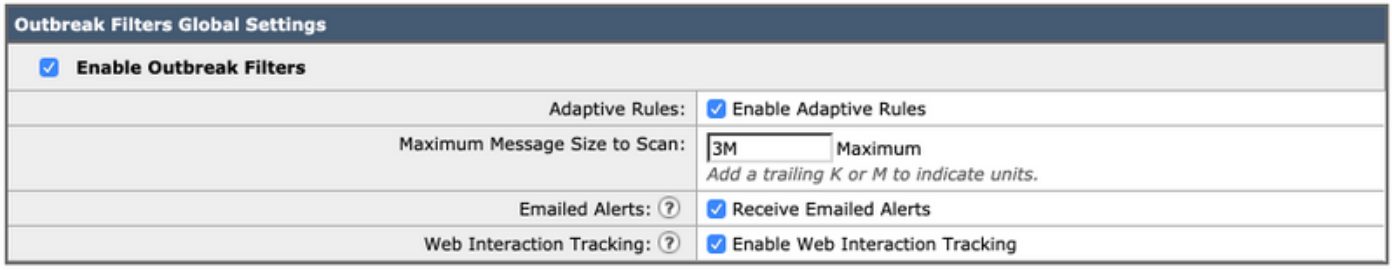
爆发过滤器在反垃圾邮件引擎结合触发， URL扫描和检测技术等等正确地标记例如真的垃圾邮件类别–，网络钓鱼电子邮件和诈欺电子邮件的外部落并且处理他们适当地以用户通知或检疫的项目里。

## 验证功能键

- 在ESA，请导航到**系统管理>功能键**
- 寻找**爆发过滤器**并且确保它是活跃的。

## 启用爆发过滤器服务

- 在ESA，请导航到**安全服务>爆发过滤器**
- 点击在**爆发过滤器概述的Enablebutton**
- 您能配置多设置。 推荐的设置在下面镜像显示：

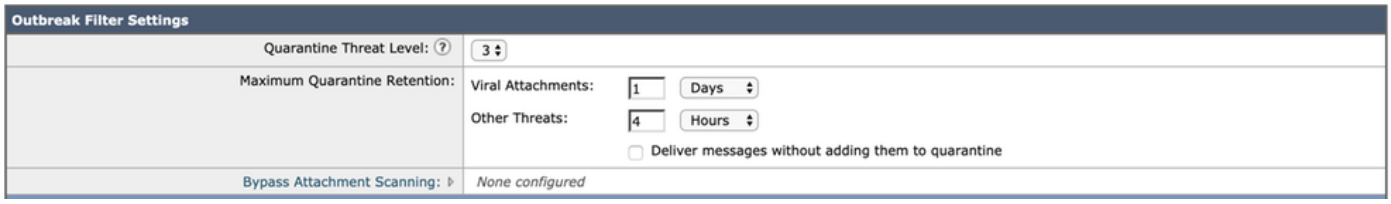



- 点击**Submitand进行您的更改**。

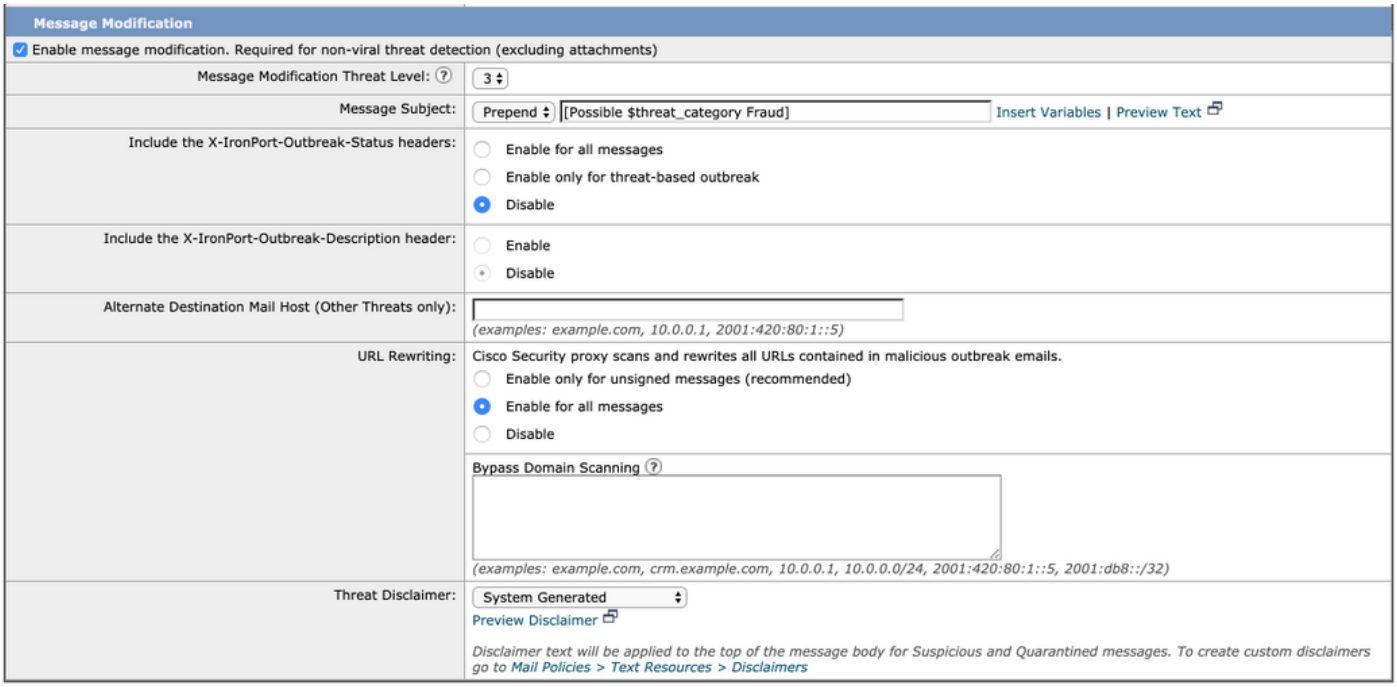
## 配置在策略的爆发过滤器

一旦爆发Filtershas配置全局，您能当前运用此功能tomail策略。

- 导航**邮寄策略>流入的邮件策略**
- 单击在**爆发过滤器下的**蓝色链路将允许该特定的策略使用定制的爆发过滤器设置。
- 为此最佳实践文档，我们保持与默认值的爆发过滤器设置：




- 如果他们视为有恶意，可疑或者phish，爆发过滤器能重写URL。选择**启用留言修改**检测和重写URL基于威胁。
- 确保**重写**选项的**URL**是所有消息的**Enable (event)**如显示的跟随：




- 点击**Submitand进行您的更改**

流出的邮件策略在**已禁用**情况应该安排**爆发过滤器**保持。

## 结论

本文打算描述默认或者最佳实践配置反垃圾邮件、防病毒、Graymail和爆发过滤器的在电子邮件安全工具(ESA)。 所有这些过滤器是可用的在入站和出站电子邮件策略，并且配置和过滤在两个推荐–，当保护的大多数是为入站时，过滤出站流提供防护中继的电子邮件或内部恶意攻击。