

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](#)

[反垃圾邮件](#)

[验证功能键](#)

[启用智能多扫描\(IMS\)全局](#)

[启用集中化垃圾邮件检疫](#)

[配置在策略的反垃圾邮件](#)

[防病毒](#)

[验证功能键](#)

[启用抗病毒扫描](#)

[配置在邮件策略的防病毒](#)

[Graymail](#)

[验证功能键](#)

[启用Graymail和安全取消预订服务](#)

[配置Graymail和安全取消预订在策略](#)

[爆发过滤器](#)

[验证功能键](#)

[启用爆发过滤器服务](#)

[配置在策略的爆发过滤器](#)

[结论](#)

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，以及难以检测低音量，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，请导航到**安全服务> IMS和Graymail**
- 点击在IMS全局设置的Enablebutton：

IMS Global Settings	
Ironport Intelligent Multi-Scan:	Enabled
Regional Scanning:	Off
Edit IMS Settings	

- 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：

Edit Common Global Settings	
Message Scanning Thresholds:	<p>Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.</p> <p>Always scan messages smaller than <input type="text" value="2M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</i></p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</i></p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds

- 点击Submitand进行您的更改。

如果没有—IMS许可证订阅：

- 导航到**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：

IronPort Anti-Spam Global Settings	
<input checked="" type="checkbox"/> Enable IronPort Anti-Spam Scanning	
Message Scanning Thresholds:	<p>Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.</p> <p>Always scan messages smaller than <input type="text" value="2M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</i></p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</i></p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds
Scanning Profile:	<p><input type="radio"/> Normal</p> <p><input checked="" type="radio"/> Aggressive <i>Recommended for customers who desire a stronger emphasis on blocking spam. When enabled, tuning Anti-Spam policy thresholds will have more impact on spam detection than the normal profile with a larger potential for false positives. Do not select the aggressive profile if IMS is enabled on the mail policy.</i></p> <p><input type="radio"/> Regional (China)</p>

- 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**Configure**按钮把您带到以下页。
- 您能通过检查**enable**box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：

External Spam Quarantine Settings	
<input checked="" type="checkbox"/> Enable External Spam Quarantine	
Name:	<input type="text" value="centralized_spam"/> <small>(e.g. spam_quarantine)</small>
IP Address:	<input type="text" value="sma_ip_address"/>
Port:	<input type="text" value="6025"/>
Safelist/Blocklist:	<input checked="" type="checkbox"/> Enable End User Safelist/Blocklist Feature Blocklist Action: <input type="button" value="Quarantine"/>

- 单击**Submit**and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：

Policies								
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	IronPort Intelligent Multi-Scan Positive: Deliver Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not ...	Graymail Detection Unsubscribe: Enabled Marketing: Spam Quarantine Social: Spam Quarantine Bulk: Spam Quarantine ...	URL_LOG_ALL_REPUTATION URL_LOG_ALL_CATEGORY URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SPF_DKIM_FAIL ...	Retention Time: Virus: 1 day Other: 4 hours	

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：

Anti-Spam Settings	
Policy:	Default
Enable Anti-Spam Scanning for This Policy:	<input type="radio"/> Use IronPort Anti-Spam service
	<input checked="" type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i>
	<input type="radio"/> Disabled

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]添加到主题：

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine <input type="button" value="v"/> <i>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</i>
Add Text to Subject:	Prepend <input type="button" value="v"/> <input type="text" value="[SPAM]"/>
<input type="button" value="Advanced"/> Optional settings for custom header and message delivery.	
Suspected Spam Settings	
Enable Suspected Spam Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> <input type="text" value="[SUSPECTED SPAM]"/>
<input type="button" value="Advanced"/> Optional settings for custom header and message delivery.	

- 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：

Spam Thresholds	
<i>Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.</i>	
IronPort Anti-Spam:	<input checked="" type="radio"/> Use the Default Thresholds <input type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="50"/> (minimum 25, cannot exceed positive spam score)
IronPort Intelligent Multi-Scan:	<input type="radio"/> Use the Default Thresholds <input checked="" type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="43"/> (minimum 25, cannot exceed positive spam score)

- 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：

Sophos Anti-Virus Overview	
Anti-Virus Scanning by Sophos Anti-Virus:	Enabled
Virus Scanning Timeout (seconds):	60
Automatic Updates: ?	Enabled

[Edit Global Settings...](#)

Current Sophos Anti-Virus files			
File Type	Last Update	Current Version	New Update
Sophos Anti-Virus Engine	Wed Nov 6 10:04:30 2019	3.2.07.377.1_5.68	Not Available
Sophos IDE Rules	Wed Nov 6 12:03:56 2019	2019110602	Not Available

No updates in progress. [Update Now](#)

- 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：

Anti-Virus Settings	
Policy:	DEFAULT
Enable Anti-Virus Scanning for This Policy:	<input checked="" type="radio"/> Yes <input checked="" type="checkbox"/> Use McAfee Anti-Virus <input checked="" type="checkbox"/> Use Sophos Anti-Virus <input type="radio"/> No

- 我们不尝试修复文件，因此消息扫描只依然是病毒的扫描：

Message Scanning	
	Scan for Viruses only <input type="button" value="v"/> <input type="checkbox"/> Drop infected attachments if a virus is found <input checked="" type="checkbox"/> (recommended) Include an X-header with the Anti-Virus scanning results in messages
Repaired Messages:	
Action Applied to Message:	<input type="text" value="Deliver As Is"/>
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append
	<input type="text" value="[WARNING: VIRUS REMOVED]"/>
Advanced	Optional settings for custom header and message delivery.

- 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：

Encrypted Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Unscannable Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Virus Infected Messages:	
Action Applied to Message:	Drop Message
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING : VIRUS DETECTED]
▶ Advanced	Optional settings for custom header and message delivery.

- 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：

Graymail Global Settings	
Graymail Detection	Enabled
Safe Unsubscribe	Enabled
Automatic Updates ?	Enabled
Edit Graymail Settings	

- 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：

Graymail Settings	
Policy:	DEFAULT
Enable Graymail Detection for This Policy:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable Graymail Unsubscribing for This Policy:	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Perform this action for: <input checked="" type="radio"/> All Messages (Recommended) <input type="radio"/> Unsigned Messages

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：

✓ Action on Marketing Email	
Apply this action to Message:	Deliver <input type="text" value="Send to Alternate Host (optional):"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [MARKETING]
Advanced	Optional settings for custom header and message delivery.
✓ Action on Social Network Email	
Apply this action to Message:	Deliver <input type="text" value="Send to Alternate Host (optional):"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [SOCIAL NETWORK]
Advanced	Optional settings for custom header and message delivery.
✓ Action on Bulk Email	
Apply this action to Message:	Deliver <input type="text" value="Send to Alternate Host (optional):"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [BULK]
Advanced	Optional settings for custom header and message delivery.

- 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**Enable**button
- 您能配置多设置。推荐的设置在下面镜像显示：

Outbreak Filters Global Settings	
<input checked="" type="checkbox"/> Enable Outbreak Filters	
Adaptive Rules:	<input checked="" type="checkbox"/> Enable Adaptive Rules
Maximum Message Size to Scan:	<input type="text" value="3M"/> Maximum <small>Add a trailing K or M to indicate units.</small>
Emailed Alerts: (?)	<input checked="" type="checkbox"/> Receive Emailed Alerts
Web Interaction Tracking: (?)	<input checked="" type="checkbox"/> Enable Web Interaction Tracking

- 点击**Submit**and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：

Outbreak Filter Settings	
Quarantine Threat Level: (?)	<input type="text" value="3"/>
Maximum Quarantine Retention:	Viral Attachments: <input type="text" value="1"/> Days Other Threats: <input type="text" value="4"/> Hours <input type="checkbox"/> Deliver messages without adding them to quarantine
Bypass Attachment Scanning: ▾	None configured

- 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：

Message Modification	
<input checked="" type="checkbox"/> Enable message modification. Required for non-viral threat detection (excluding attachments)	
Message Modification Threat Level: ?	3
Message Subject:	Prepend [Possible \$threat_category Fraud] Insert Variables Preview Text
Include the X-IronPort-Outbreak-Status headers:	<input type="radio"/> Enable for all messages <input type="radio"/> Enable only for threat-based outbreak <input checked="" type="radio"/> Disable
Include the X-IronPort-Outbreak-Description header:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Alternate Destination Mail Host (Other Threats only):	<input type="text"/> <small>(examples: example.com, 10.0.0.1, 2001:420:80:1::5)</small>
URL Rewriting:	Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails. <input type="radio"/> Enable only for unsigned messages (recommended) <input checked="" type="radio"/> Enable for all messages <input type="radio"/> Disable
	Bypass Domain Scanning ? <input type="text"/> <small>(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24, 2001:420:80:1::5, 2001:db8::/32)</small>
Threat Disclaimer:	System Generated Preview Disclaimer <small>Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies > Text Resources > Disclaimers</small>

- 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。