

反垃圾郵件、防病毒、灰色郵件和爆發過濾器的最佳實踐指南

目錄

[概觀](#)

[反垃圾郵件](#)

[驗證功能金鑰](#)

[全域性啟用智慧多掃描\(IMS\)](#)

[啟用集中垃圾郵件隔離區](#)

[在策略中配置反垃圾郵件](#)

[防病毒](#)

[驗證功能金鑰](#)

[啟用防病毒掃描](#)

[在郵件策略中配置防病毒](#)

[灰色郵件](#)

[驗證功能金鑰](#)

[啟用灰色郵件和安全取消訂閱服務](#)

[在策略中配置灰色郵件和安全取消訂閱](#)

[爆發過濾器](#)

[驗證功能金鑰](#)

[啟用爆發過濾器服務](#)

[在策略中配置爆發過濾器](#)

[結論](#)

概觀

企業通過電郵面臨的絕大多數威脅、攻擊和騷擾都以垃圾郵件、惡意軟體和混合攻擊的形式出現。思科的電子郵件安全裝置(ESA)包括多種不同的技術和功能，可在這些威脅進入組織之前在網關將其隔離。本文檔將介紹在入站和出站電子郵件流上配置反垃圾郵件、防病毒、灰色郵件和爆發過濾器的最佳方法。

反垃圾郵件

反垃圾郵件保護可應對各種已知威脅，包括垃圾郵件、網路釣魚和殭屍攻擊，以及難以檢測的低容量、短壽命電子郵件威脅(如[419」詐騙](#))。此外，反垃圾郵件保護可識別新的和不斷發展的混合威脅，例如通過下載URL或執行檔分發惡意內容的垃圾郵件攻擊。

思科電子郵件安全提供以下反垃圾郵件解決方案：

- IronPort反垃圾郵件過濾(IPAS)
- 思科智慧多掃描過濾(IMS)

您可以在您的ESA上許可和啟用這兩個解決方案，但只能在特定郵件策略中使用一個。為了編寫本最佳實踐文檔，我們將使用IMS功能。

驗證功能金鑰

- 在ESA上，導航到**系統管理 > 功能金鑰**
- 查詢智慧多掃描許可證，並確保其處於活動狀態。

全域性啟用智慧多掃描(IMS)

- 於其ESA中，導覽成長至**安全服務> IMS和Graymail**
- 按一下其**啟用IMS全域性設置上的按鈕**：

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

- 查詢「**Common Global Settings(通用全域性設定)**」和按一下**編輯全域性設定**
- 此處您可以設定多個設定。其建議設定是顯示在其影象如下：

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

- 按一下**Submit**和 **提交 更改**。

如果您沒有IMS許可證訂用：

- 導航到**安全服務> IronPort Anti-Spam**
- 按一下其**啟用ironPort Anti-Spam上的按鈕**
- 按一下**編輯全域性設定**
- 此處您可以設定多個設定。其建議設定是顯示在其影象如下：

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>

- 思科建議為希望重點阻止垃圾郵件的客戶選擇**主動掃描配置檔案**。
- 按一下**Submit**和 **提交 變更**

啟用集中垃圾郵件隔離區

由於反垃圾郵件具有傳送到隔離區的選項，因此確保設定垃圾郵件隔離區非常重要：

- 導覽至**Security Services > Spam Quarantine**
- 按一下其 **設定** 按鈕 將 獲取 您 成長至 其 摺疊欠款 頁面。
- 此處 您 可以 啟用 其 隔離 依據 檢查 其 **啟用** 框 和 第e 隔離 成長至 是 集中 於 安全管理A裝置 (SMA) 依據 填充 在 sma**名稱** 和 **IP 地址**。其 建議 設定 是 顯示 如下：

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

- 按一下 **Submit** 和 **提交 變更**

有關設定和集中隔離區的詳細資訊，請參閱最佳實踐文檔：

[集中策略、病毒和爆發隔離區設定以及從ESA遷移到SMA的最佳實踐](#)

在策略中配置反垃圾郵件

一次 智慧 多個 - 掃描 有 已 configured 全域性 中， 您 可以 現在 應用 智慧 多個 - 掃描 成長至 mail 策略：

- 導覽至**Mail Policies > Incoming Mail Policies**
- 預設情況下，傳入郵件策略使用IronPort反垃圾郵件設定。
- 按一下**Anti-Spam**下的藍色連結將允許該特定策略使用自定義的反垃圾郵件設定。
- 下面是一個使用自定義反垃圾郵件設定的預設策略的示例：

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	

通過按一下要自定義的策略的**Anti-Spam**下的藍色連結，為傳入郵件策略自定義反垃圾郵件設定。

此處 您 可以 選擇 其 Anti-Spam 掃描 選項 您 願望 成長至 啟用 對於 此 政策。

- 對於 其 用途 的 此 最佳 行為 冰 文檔， 按一下 其 無線電 按鈕 下一頁 成長至 使用 **IronPort 智慧 多功能掃描**：

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

接下來的兩節包括已確定的垃圾郵件設定和疑似垃圾郵件設定：

- 建議的最佳做法是在主題和主題中新增了預置文本[SPAM]時，對**Proved-Identified Spam**設定

配置Quarantine操作；

- 在主題中新增了預置文本[SUSPECTED SPAM]時，應用到Deliver作為可疑垃圾郵件設定的操作：

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine <input type="button" value="v"/> <small>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</small>
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.

- 垃圾郵件閾值設定可以更改，建議設定是將Positive-Identified Spam score自定義為90，將Suspected Spam score自定義43:

Spam Thresholds	
<small>Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.</small>	
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)

- 按一下Submit和 提交 變更

防病毒

防病毒保護通過兩個第三方引擎 — Sophos和McAfee提供。這些引擎將過濾所有已知的惡意威脅，按照配置刪除、清除或隔離它們。

驗證功能金鑰

要檢查兩個功能鍵是否已啟用並處於活動狀態：

- 轉至系統管理 > 功能鍵
- 確保Sophos Anti-Virus和McAfee許可證均處於活動狀態。

啟用防病毒掃描

- 導覽 成長至 安全 服務> 防病毒 — Sophos
- 按一下 其 啟用按鈕。
- 確保Automatic Update已啟用，並且Sophos Anti-Virus檔案更新工作正常。如有必要，請單擊 Update Now以立即啟動檔案更新：

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](#)

- 按一下Submit和 提交 更改。

如果McAfee許可證也處於活動狀態，請導航 成長至 安全 服務> 防病毒 — McAfee

- 按一下 其 啟用 按鈕。
- 確保Automatic Update已啟用，並且McAfee Anti-Virus檔案更新工作正常。如有必要，請單擊 Update Now以立即啟動檔案更新。
- 按一下Submit和 提交 變更

在郵件策略中配置防病毒

對於傳入郵件策略，建議執行以下操作：

- 導覽至Mail Policies > Incoming Mail Policies
- 通過按一下要自定義的策略的Anti-Virus下的藍色連結，為傳入郵件策略自定義Anti-Virus設定。
- 此處 您 可以 選擇 其 Anti — 病毒 掃描 選項 您 願望 成長至 啟用 對於 此 政策。
- 對於 其 用途 的 此best p反應冰 文檔，選擇McAfee和Sophos Anti-Virus:

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

- 我們不嘗試修復檔案，因此郵件掃描將保留為Scan for Virtuals：

Message Scanning	
	Scan for Viruses only ▾ <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:	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
	[WARNING: VIRUS REMOVED]
Advanced	Optional settings for custom header and message delivery.

- Encrypted和Unscannable Messages的建議操作是Deliver As-Is，並修改主題行以引起注意。
- 防病毒的建議策略是Drop所有受病毒感染的郵件，如下圖所示：

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.

- 按一下 **Submit** 和 **提交 變更**

建議對傳出郵件策略使用類似的策略，但是，我們不建議修改傳出郵件上的主題行。

灰色郵件

郵件安全裝置中的灰色郵件管理解決方案包括兩個元件：整合的灰色郵件掃描引擎和基於雲的取消訂閱服務。灰色郵件管理解決方案允許組織使用整合的灰色郵件引擎識別灰色郵件，應用適當的策略控制，並為終端使用者提供一種簡單的機制，使用取消訂閱服務取消訂閱不需要的郵件。

灰色郵件類別包括行銷電子郵件、社交網路電子郵件和批次電子郵件。高級選項包括新增自定義報頭、傳送到備用主機和存檔消息。為了達到此最佳實踐，我們將為預設郵件策略啟用 Graymail 的安全取消訂閱功能。

驗證功能金鑰

- 在 ESA 上，導航到 **系統管理 > 功能金鑰**
- 查詢 **Graymail Safe Unsubscription** 並確保其處於活動狀態。

啟用灰色郵件和安全取消訂閱服務

- 於其 ESA 中，導覽 成長至 **安全 服務 > IMS 和 Graymail**
- 按一下其 **編輯灰色郵件設定 Graymail Global Settings** 上的按鈕
- 選擇所有選項 — **Enable Graymail Detection**、**Enable Safe Unsubscribe** 和 **Enable Automatic Updates**:

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

- 按一下Submit和 提交 變更

在策略中配置灰色郵件和安全取消訂閱

Once Graymail 和安全取消訂閱 有 已 configured 全域性 中， 您 可以 現在 應用這些服務 成長至 mail 策略。

- 導覽至Mail Policies > Incoming Mail Policies
- 按一下灰色郵件下的藍色連結將允許該特定策略使用自定義的灰色郵件設定。
- 此處 您 可以 選擇 《格雷郵報》選項 您 願望 成長至 啟用 對於 此 政策。
- 對於 其用途 的 此 最佳p反應冰 文檔， 按一下 其 無線電 按鈕 下一頁 要為此策略啟用灰色郵件檢測和為此策略啟用Graymail取消訂閱：

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

接下來的三個部分包括Action on Marketing Email Settings、Action on Social Network Email Settings和Action on Bulk Email Settings。

- 建議的最佳做法是啟用所有這些功能，並保持如下所示類別的Delivered操作，即主題新增了預置文本：

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

- 按一下Submit和 提交 變更

傳出郵件策略應使灰色郵件保持為禁用狀態。

爆發過濾器

爆發過濾器將反垃圾郵件引擎、URL掃描和檢測技術等中的觸發器組合在一起，以正確標籤不屬於真正垃圾郵件類別的專案（例如網路釣魚郵件和詐騙電子郵件），並使用使用者通知或隔離區適當

處理它們。

驗證功能金鑰

- 在ESA上，導航到**系統管理 > 功能金鑰**
- 查詢**爆發過濾器**並確保其處於活動狀態。

啟用爆發過濾器服務

- 於其ESA中，導覽成長至 **安全 服務> 爆發過濾器**
- 按一下其 **啟用爆發過濾器概述**上的按鈕
- 此處您可以設定多個設定。其建議設定是顯示在其影象如下：

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

- 按一下Submit和 **提交 更改**。

在策略中配置爆發過濾器

病毒爆發過濾器有已 configured 全域性中，您可以現在將此功能應用於 mail 策略。

- 導覽至**Mail Policies > Incoming Mail Policies**
- 按一下**爆發過濾器**下的藍色連結將允許該特定策略使用自定義的爆發過濾器設定。
- 對於其用途的此最佳行為冰文檔中，我們將使用預設值保留爆發過濾器設定：

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

- 如果爆發過濾器認為它們是惡意、可疑或網路釣魚的，則它們可以重寫它們。選擇**Enable message modification**以檢測和重寫基於URL的威脅。
- 確保所有郵件的**URL Rewriting**選項為**Enable**，如下所示：

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 <input #"="" type="text" value="[[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:	<input type="text" value="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>

- 按一下Submit和 提交 變更
傳出郵件策略應使爆發過濾器保持為禁用狀態。

結論

本文檔旨在描述郵件安全裝置(ESA)中的反垃圾郵件、防病毒、灰色郵件和爆發過濾器的預設或最佳實踐配置。所有這些過濾器都可用於入站和出站郵件策略，並且都建議對兩者進行配置和過濾——雖然大部分保護用於入站，但過濾出站流可提供針對中繼郵件或內部惡意攻擊的保護。