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

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。

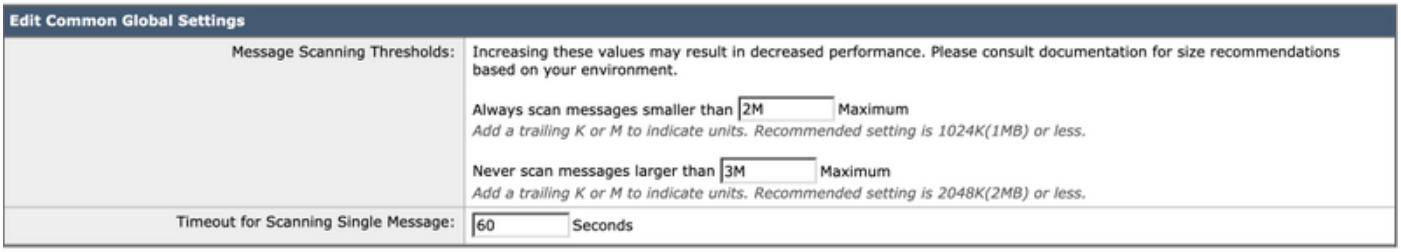
驗證功能金鑰

- 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**:

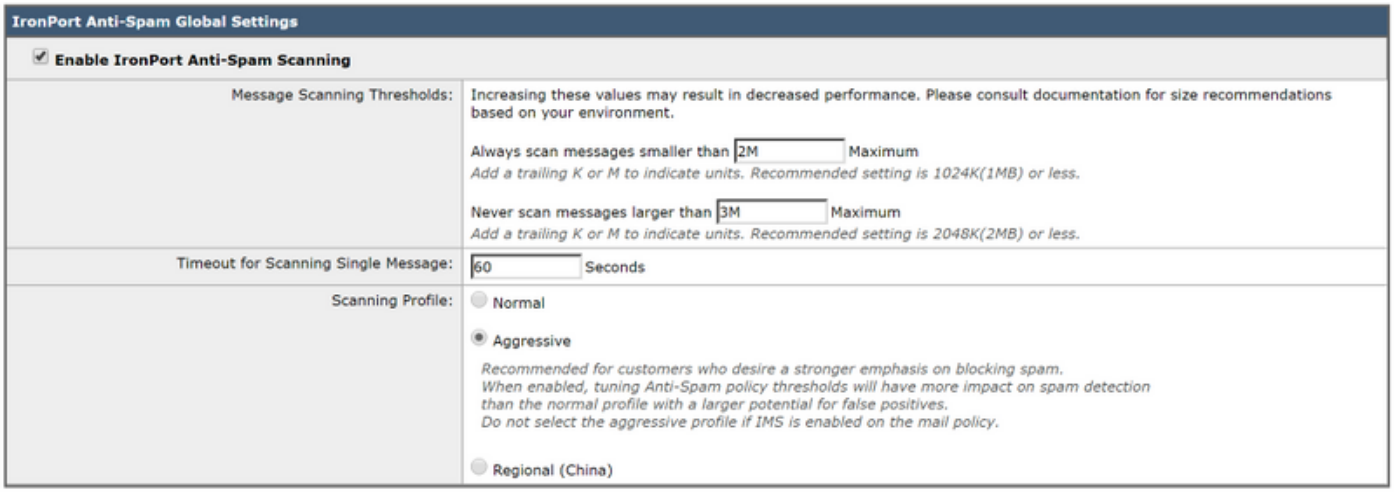
- 查詢「Common Global Settings(**通用全域性設定)**」和 按一下**編輯全域性設定**
- 此處 您 可以 設定 多個 設定。 其 建議 設定 是 顯示 在 其 影象 如下：



- 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：

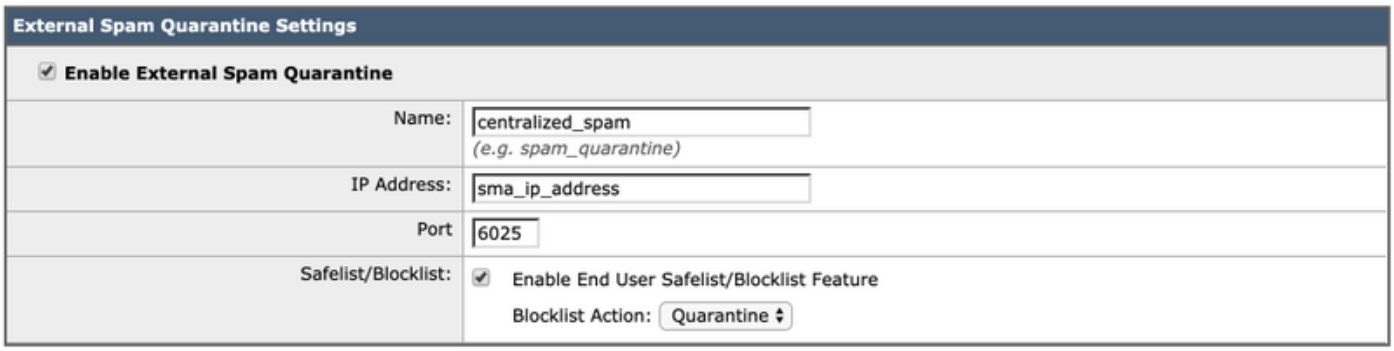


- 思科建議為希望重點阻止垃圾郵件的客戶選擇**主動掃描**配置檔案。
- 按一下**Submit**和 **提交 變更**

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ing 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：



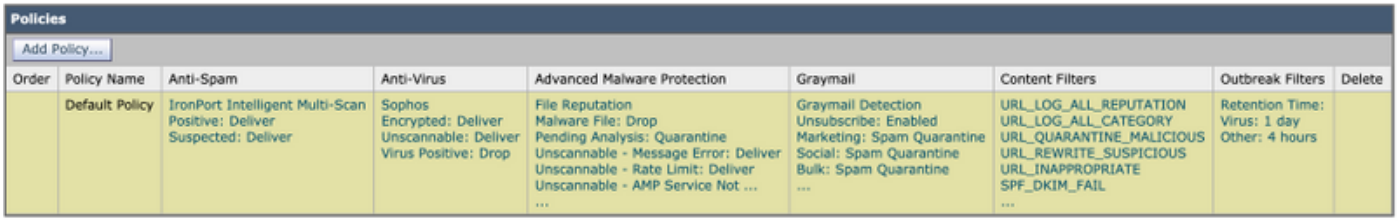
- 按一下**Submit**和 **提交 變更**

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：

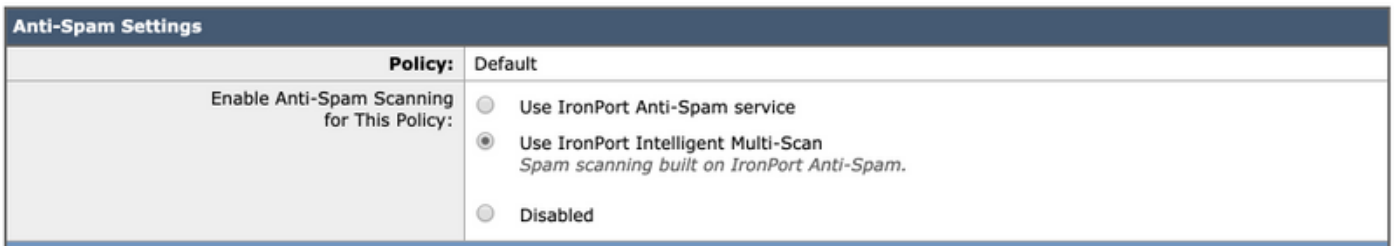
- 導覽至**Mail Policies > Incoming Mail Policies**
- 預設情況下，傳入郵件策略使用IronPort反垃圾郵件設定。
- 按一下**Anti-Spam**下的藍色連結將允許該特定策略使用自定義的反垃圾郵件設定。
- 下面是一個使用自定義反垃圾郵件設定的預設策略的示例：



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：**

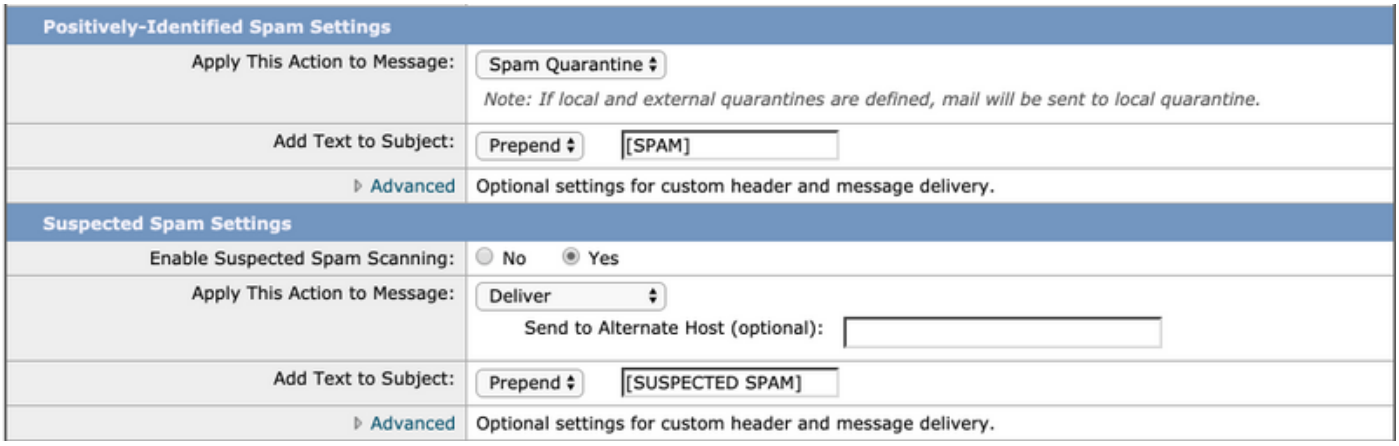


接下來的兩節包括已確**定的垃圾郵件設定和**疑似垃**圾郵件設定：**

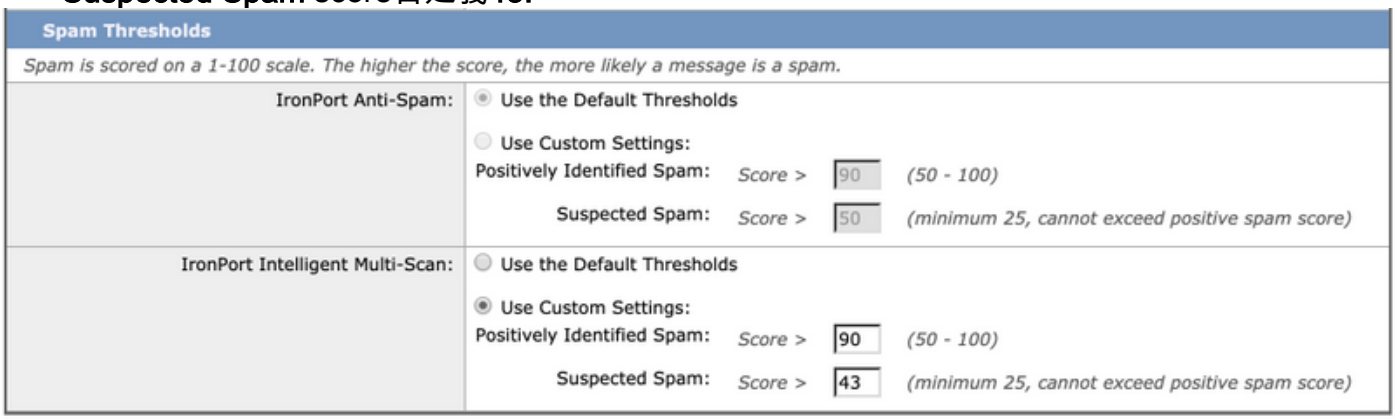
- 建議的最佳做法是在主題和主題中新增了預置文本**[SPAM]**時，對**Proved-Identified Spam**設定

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：



- **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:**



- 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。

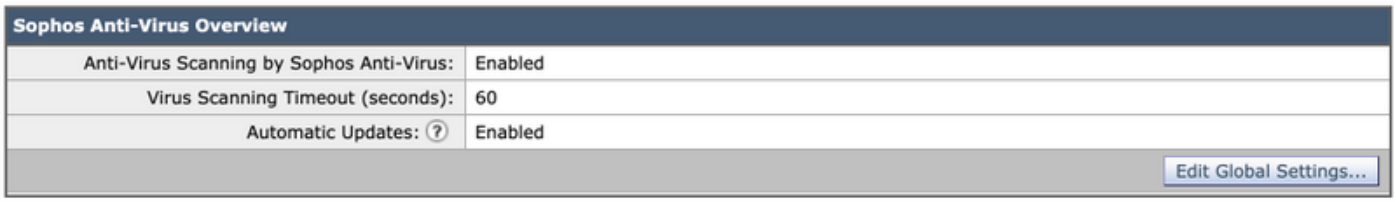
驗證功能金鑰

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：



- 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**

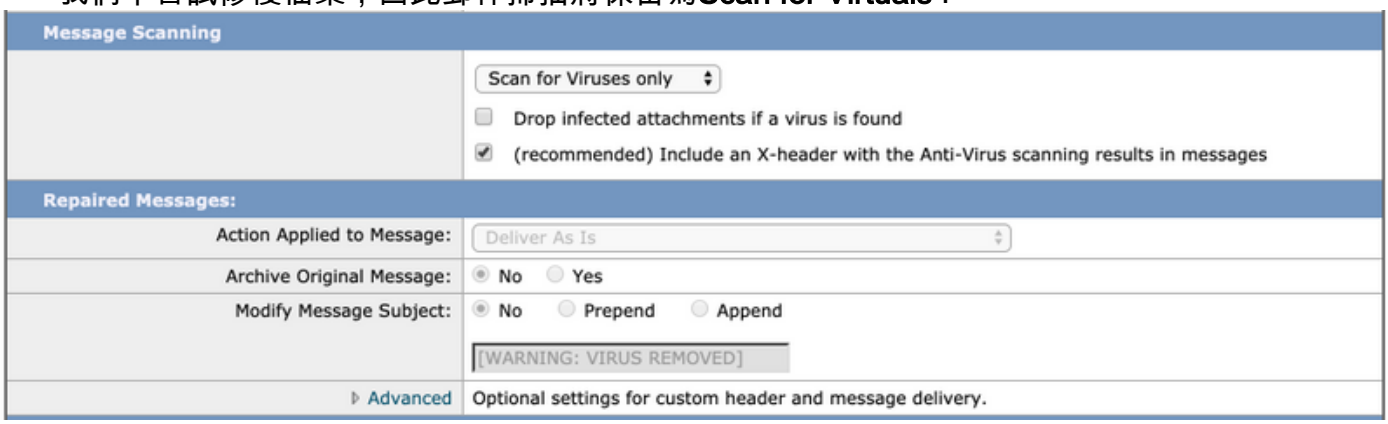
- 按一下 其 **啟用**按鈕。
- 確保**Automatic Update**已啟用，並且McAfee Anti-Virus檔案更新工作正常。如有必要，請單擊**Update Now**以立即啟動檔案更新。
- 按一下**Submit**和 **提交 變更**

在郵件策略中配置防病毒

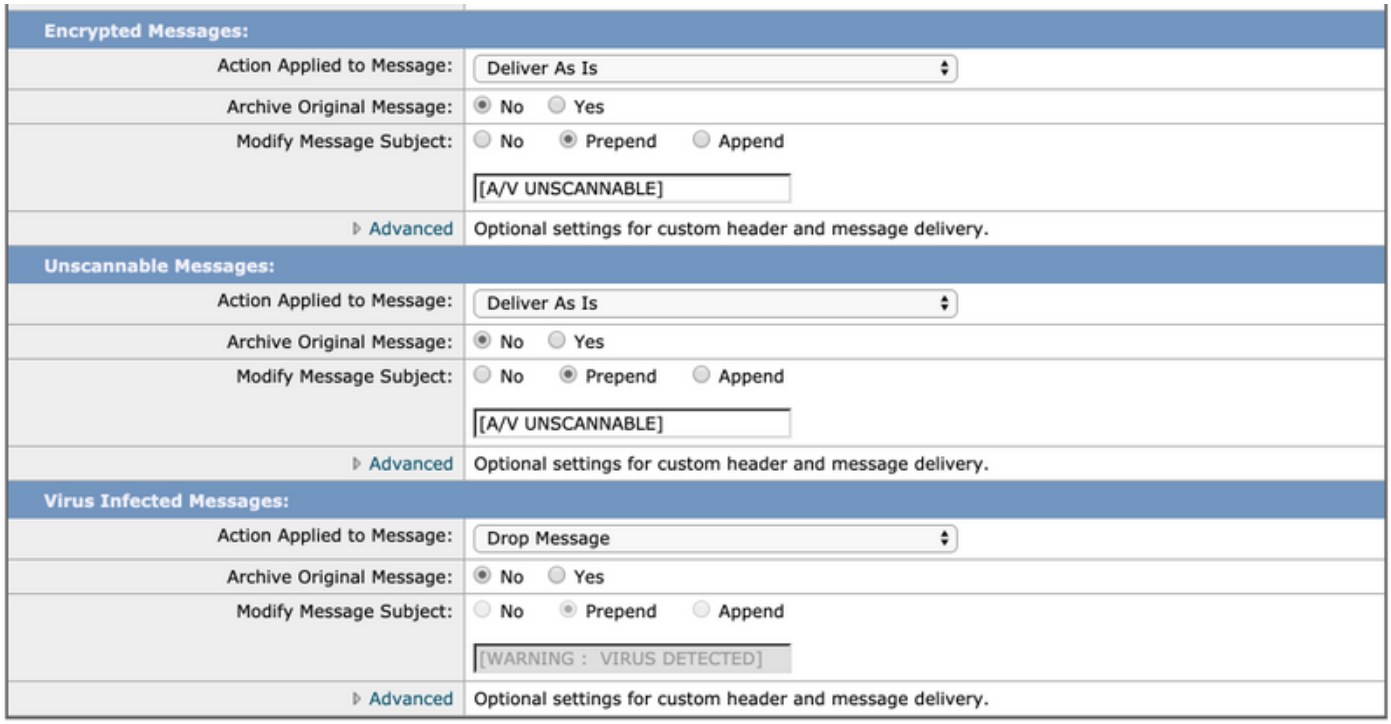
對於傳入郵件策略，建議執行以下操作：

- 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**:

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



- **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：



- 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。

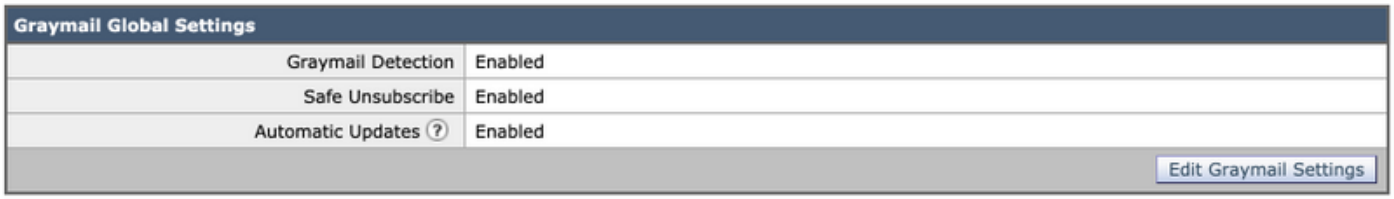
灰色郵件類別包括行銷電子郵件、社交網路電子郵件和批次電子郵件。高級選項包括新增自定義報頭、傳送到備用主機和存檔消息。為了達到此最佳實踐，我們將為預設郵件策略啟用Graymail的安全取消訂閱功能。

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**:



- 按一下Submit和 **提交 變更**

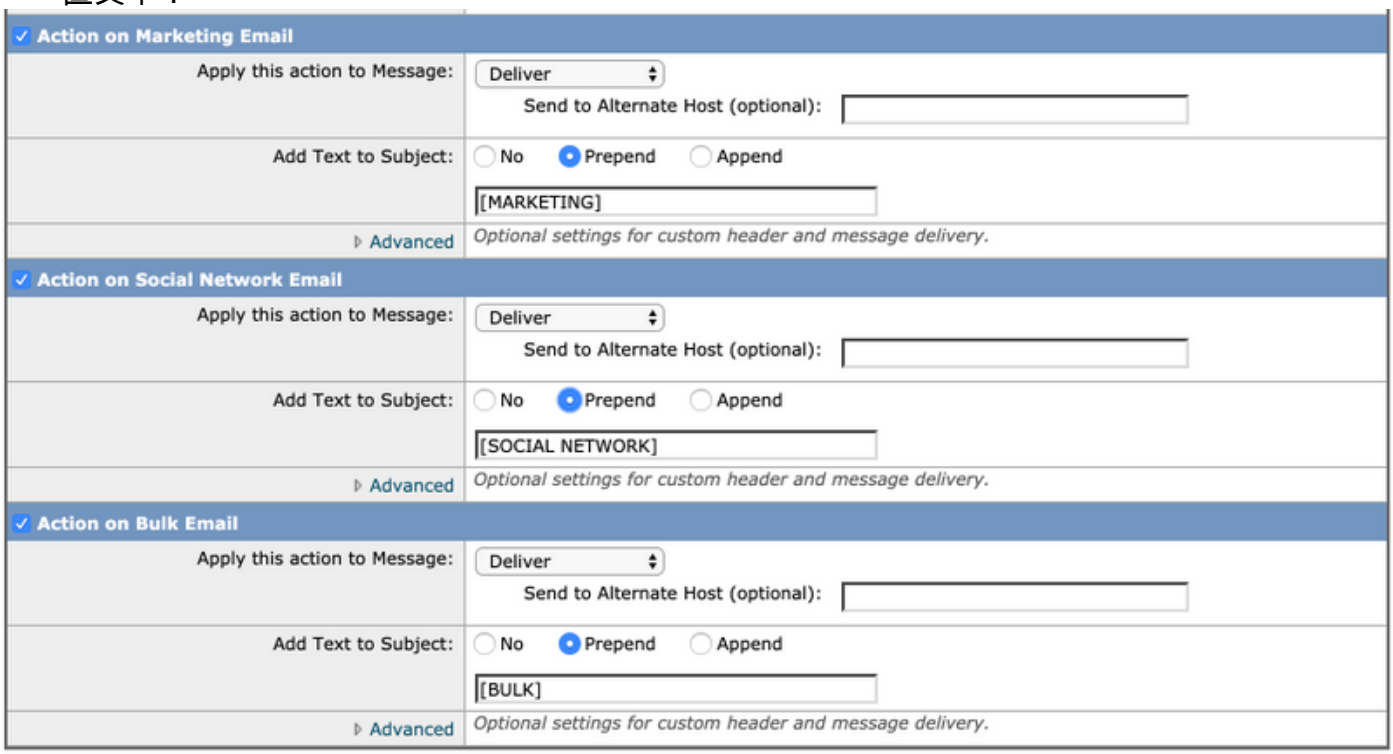
在策略中配置灰色郵件和安全取消訂閱

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**:

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：



- 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

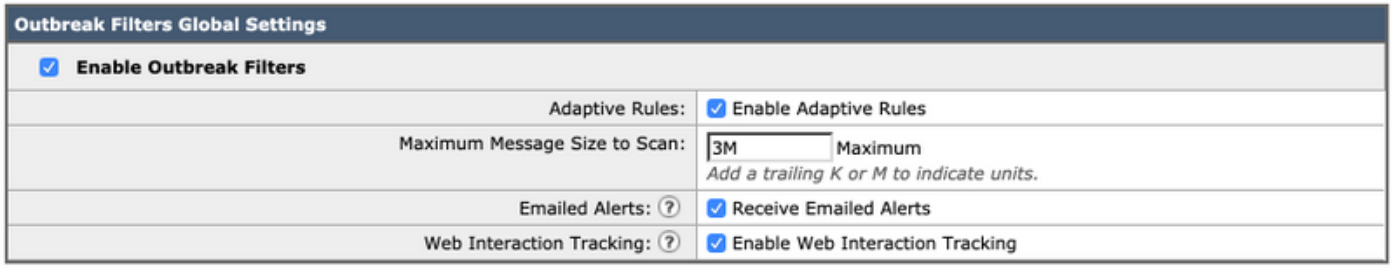
處理它們。

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：

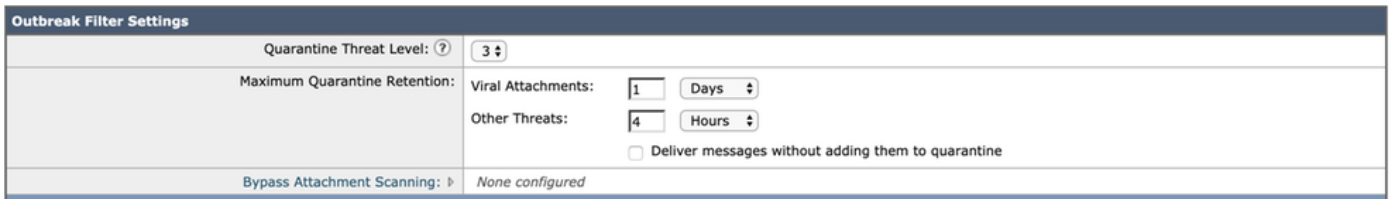


- 按一下Submit和 **提交 更改。**

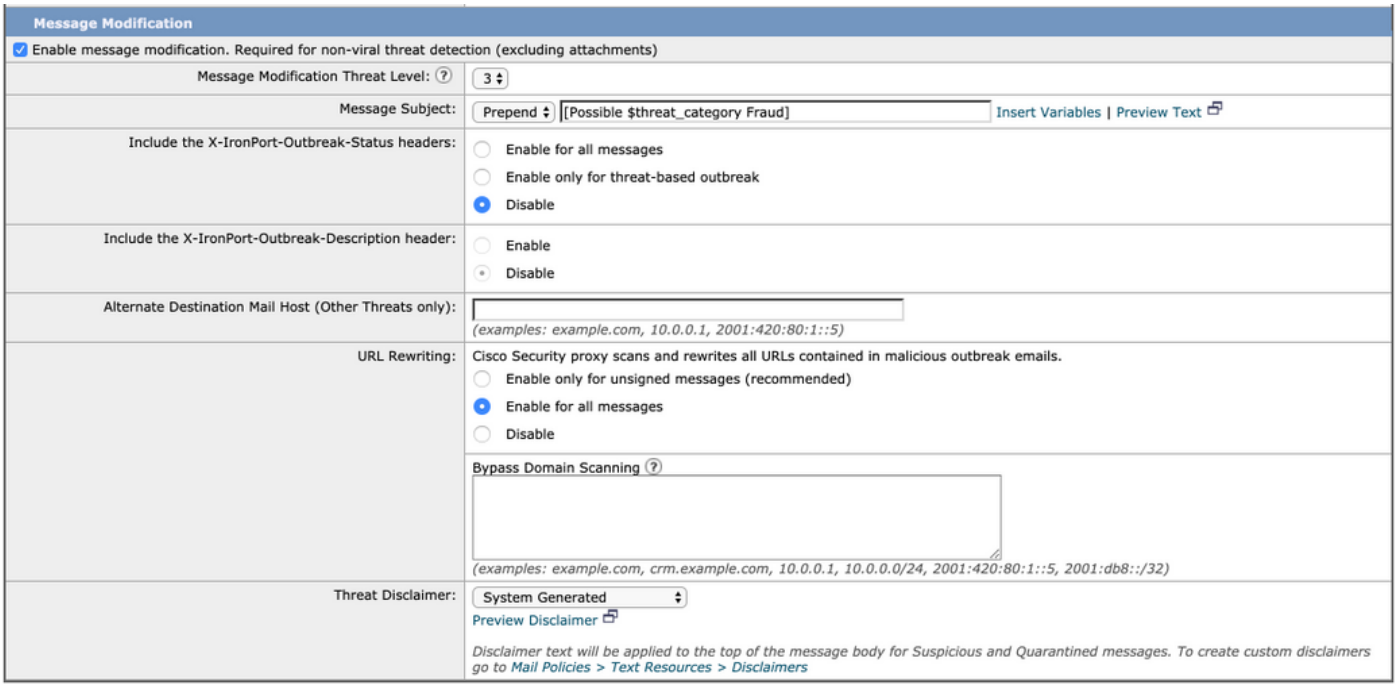
在策略中配置爆發過濾器

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：



- 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：



- 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。