傳入和傳出內容過濾器的最佳實踐指南

目錄

簡介

內容過濾器允許您檢查電子郵件的複雜詳細資訊並對電子郵件執行操作（或無操作）。建立傳入或傳出內容過濾器後，將其應用於傳入或傳出郵件策略。當任何電子郵件與內容過濾器匹配時，思科郵件安全裝置(ESA)和安全管理裝置(SMA)上的「內容過濾器」報告可以顯示與任何內容過濾器匹配的所有電子郵件。因此，即使不採取任何措施，它也是獲得有關進入和離開您組織的電子郵件型別的有用資訊的極好方法 — 使您可以「模式」您的電子郵件流。

由於內容過濾器「條件」和「操作」有很多不同，本文檔將指導您完成一些非常常見且推薦的傳入和傳出內容過濾器。

步驟概述

第1步：匯入所需的詞典

本文檔將提供實施一些最佳實踐傳入和傳出內容過濾器所需的步驟。我們要建立的內容篩選器將引用一些詞典 — 因此我們需要先匯入這些詞典。ESA隨附詞典，您只需將其匯入配置中，以便在我們將建立的內容過濾器中引用它們。

第2步：建立集中隔離區

對於大多數內容過濾器，我們將建立，並將「操作」設定為將電子郵件（或電子郵件的副本）隔離到指定的自定義（新）隔離區，因此，我們需要首先在SMA上建立這些隔離區，因為本文檔假定您已在ESA和SMA之間啟用集中式PVO（策略、病毒和爆發）隔離區。

步驟3:建立傳入和傳出內容過濾器並應用於策略

匯入字典並建立隔離區後，我們將建立入站內容過濾器並將其應用於傳入郵件策略，然後建立傳出內容過濾器並將其應用於傳出郵件策略。

第1步：匯入所需的詞典

匯入將在內容過濾器中引用的詞典：

- 在ESA裝置上，導航至**「郵件策略>字典」**
- 按一下頁面右側的「Import Dictionary」按鈕。

髒話：

- 選擇**「從IronPort裝置上的配置目錄匯入」**
- 選擇「profanity.txt」，然後按一下「Next」。
- 姓名：Profanity
- 按一下「Match whole words」(**匹配整個字**詞)（非常重要）
- 修改條款（新增新條款或刪除不需要的條款）
- 按一下**「提交」**

性內容：

- 選擇**「從IronPort裝置上的配置目錄匯入」**
- 選擇「sexual_content.txt」，然後按一下「Next」。
- 名稱：性**內容**
- 按一下「Match whole words」(**匹配整個字**詞)（非常重要）
- 修改條款（新增新條款或刪除不需要的條款）
- 按一下**「提交」**

專有：

- 選擇**「從IronPort裝置上的配置目錄匯入」**
- 選擇「proprietary_content.txt」，然後按一下「Next」。
- 名稱：**專有**
- 按一下「Match whole words」(**匹配整個字**詞)（非常重要）
- 修改條款（新增新條款或刪除不需要的條款）
- 按一下**「提交」**

第2步：建立集中隔離區

- 在SMA上，導航到**「Email Tab > Message Quarantine > PVO Quarantines」**
- 開始之前，隔離區表應如下所示。所有隔離區均為預設值。

Quarantines

Add Policy Quarantine... | Search Across Quarantines

Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	--	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	--	0	
Policy	Centralized Policy	0	Retain 10 days then Delete	--	0	
Unclassified	Unclassified	0	Retain 30 days then Release	--	0	
Virus	Antivirus	0	Retain 30 days then Delete	--	0	

Available space for Policy, Virus & Outbreak quarantines is 33G.

- 按一下 **"新增策略隔離....."** 按鈕
- 建立下面的隔離區。
- 某些內容將由傳入內容過濾器使用，某些內容將由傳出內容過濾器使用。以相同的方式建立它們。

PVO隔離區 — 由傳入內容過濾器使用

URL惡意入站：
名稱:URL惡意入站

SPF硬故障：
名稱:SPF硬故障

保留期：14天
預設操作：刪除
釋放空間：啟用

URL類別入站：
名稱:URL類別傳入
保留期：14天
預設操作：刪除
釋放空間：啟用

銀行資料傳入：
名稱:銀行資料傳入
保留期：14天
預設操作：刪除
釋放空間：啟用

SSN入站：
名稱:SSN傳入
保留期：14天
預設操作：刪除
釋放空間：啟用

不適當的入站：
名稱:不適當的入站
保留期：14天
預設操作：刪除
釋放空間：啟用

保留期：14天
預設操作：刪除
釋放空間：啟用

SPF軟故障：
名稱:SPF軟故障
保留期：14天
預設操作：刪除
釋放空間：啟用

欺騙郵件：
名稱:SpoofMail
保留期：14天
預設操作：刪除
釋放空間：啟用

DKIM硬失敗：
名稱:DKIM硬失敗
保留期：14天
預設操作：刪除
釋放空間：啟用

受密碼保護的入站：
名稱:Pwd受保護傳入
保留期：14天
預設操作：刪除
釋放空間：啟用

PVO隔離區 — 由傳出內容過濾器使用

銀行資料出站：
名稱:銀行資料出站
保留期：14天
預設操作：刪除
釋放空間：啟用

SSN出站：
名稱:SSN傳出
保留期：14天
預設操作：刪除
釋放空間：啟用

出站不當：
名稱:出站不當
保留期：14天
預設操作：刪除
釋放空間：啟用

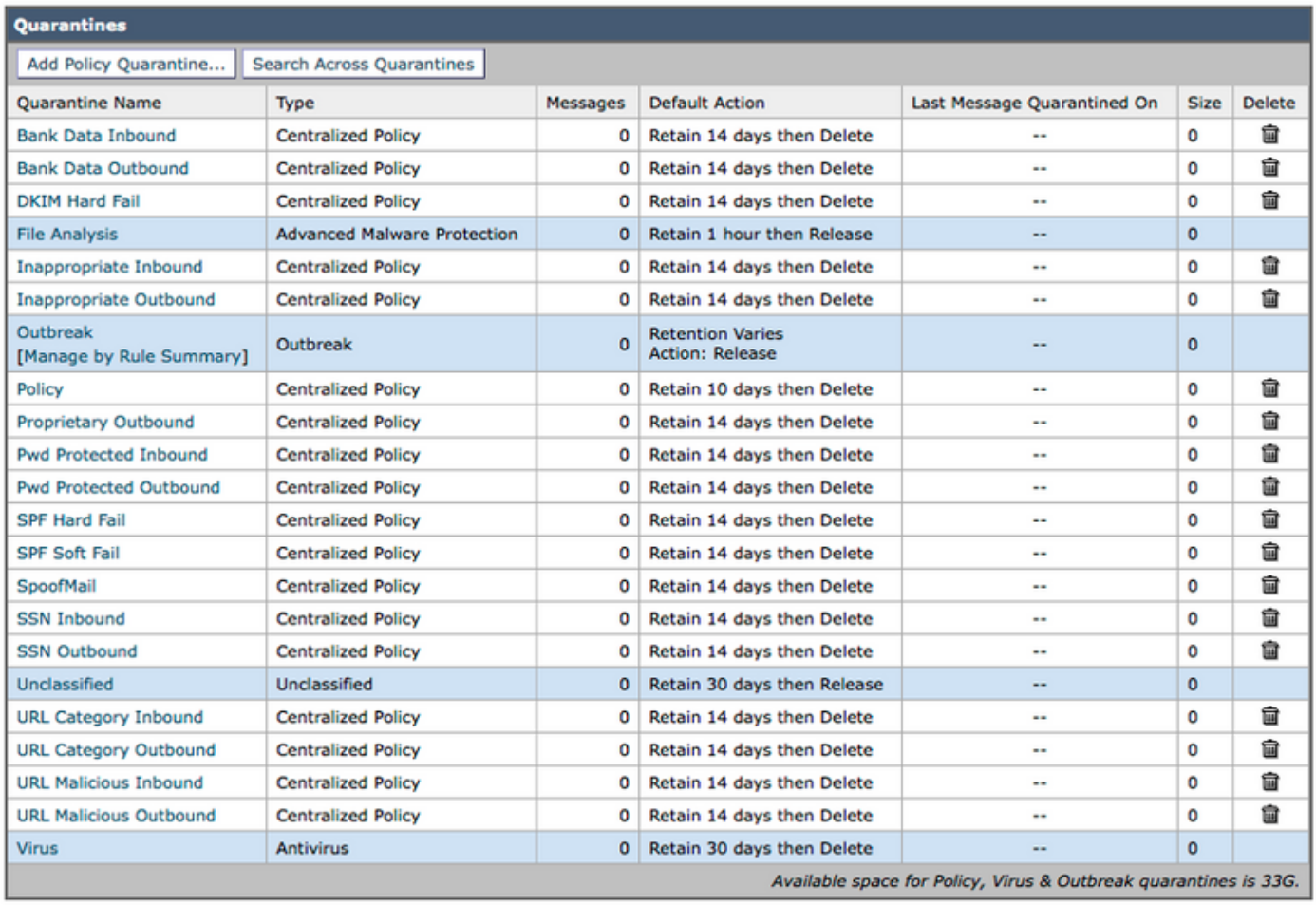
專有出站：
名稱:專有出站
保留期：14天
預設操作：刪除
釋放空間：啟用

URL惡意出站：
名稱:URL惡意出站
保留期：14天
預設操作：刪除
釋放空間：啟用

出站URL類別：
名稱:URL類別出站
保留期：14天
預設操作：刪除
釋放空間：啟用

受密碼保護的出站：
名稱:Pwd Protected Outbound
保留期：14天
預設操作：刪除
釋放空間：啟用

- 以下是建立所有PVO隔離區後PVO表應遵循的注意事項。



Quarantines

Add Policy Quarantine... | Search Across Quarantines

Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
Bank Data Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Bank Data Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
DKIM Hard Fail	Centralized Policy	0	Retain 14 days then Delete	--	0	
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	--	0	
Inappropriate Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Inappropriate Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	--	0	
Policy	Centralized Policy	0	Retain 10 days then Delete	--	0	
Proprietary Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Pwd Protected Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Pwd Protected Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
SPF Hard Fail	Centralized Policy	0	Retain 14 days then Delete	--	0	
SPF Soft Fail	Centralized Policy	0	Retain 14 days then Delete	--	0	
SpoofMail	Centralized Policy	0	Retain 14 days then Delete	--	0	
SSN Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
SSN Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Unclassified	Unclassified	0	Retain 30 days then Release	--	0	
URL Category Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
URL Category Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
URL Malicious Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
URL Malicious Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Virus	Antivirus	0	Retain 30 days then Delete	--	0	

Available space for Policy, Virus & Outbreak quarantines is 33G.

步驟3:建立傳入內容過濾器

匯入字典並建立PVO隔離區後，您現在可以開始建立傳入內容過濾器：

- 導航至：**「郵件策略>傳入內容過濾器」**
- 這是您應該建立的傳入內容過濾器表。例如，該表下面是一個螢幕截圖，說明如何建立第一個截圖。

建立這些傳入內容過濾器

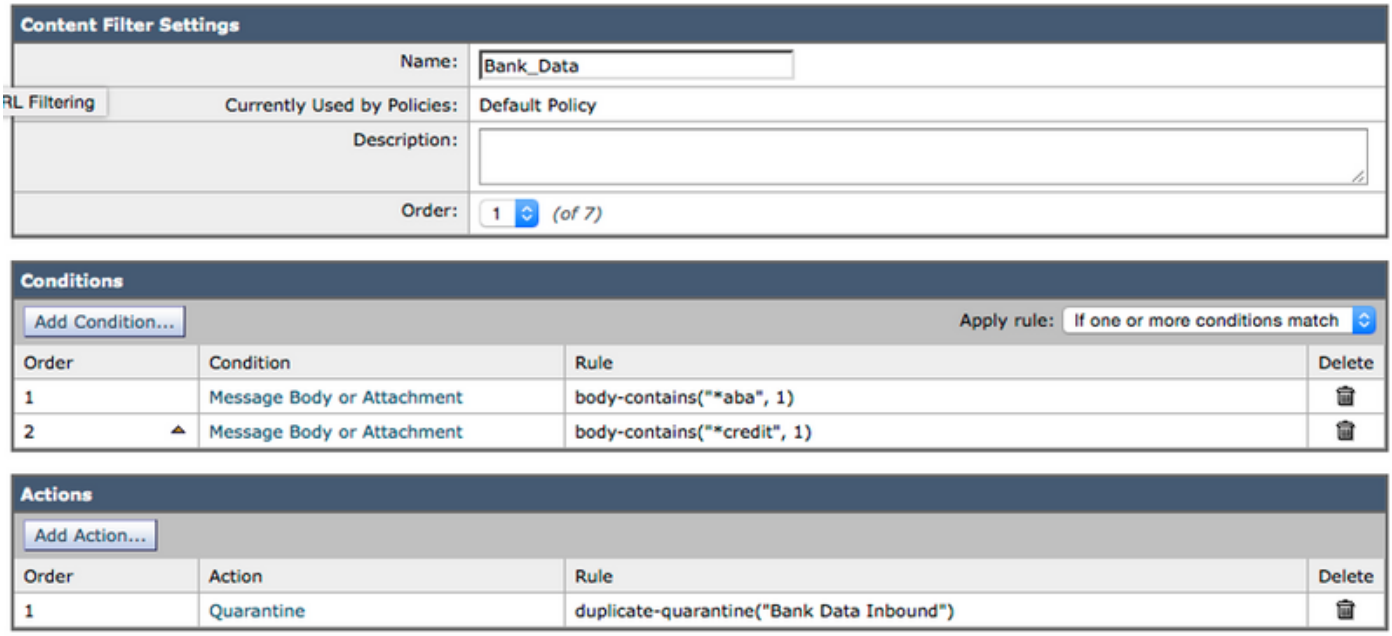
名稱:Bank_Data
新增兩個條件：
  郵件正文或附件：
    包含智慧識別符號：ABA路由編號
    包含智慧識別符號：信用卡號
新增一個操作：
  隔離：
    將郵件傳送到隔離區："銀行資料入站（集中）"
    重複消息：已啟用
（請注意，應用規則應為「如果一個或多個條件匹配」）
名稱:SSN
新增一個條件：
  郵件正文或附件：
    包含智慧識別符號：社會保險號碼(SSN)
新增一個操作：
  隔離：
    將郵件傳送到隔離區："SSN入站（集中）"
    重複消息：已啟用

名稱:**不合適**
新增兩個條件：
  郵件正文或附件：
    包含詞典中的術語：髒話
    包含詞典中的術語：性內容
新增一個操作：
  隔離：
    將郵件傳送到隔離區："不適當的入站（集中）"
    重複消息：已啟用
名稱:**URL_Category**
新增一個條件：
  URL類別：
    選擇類別：
      成人、約會、過濾規避、免費軟體和共用軟體、賭博、
      遊戲，駭客，內衣和泳衣，非性裸體，
      暫留的域、對等檔案傳輸、色情
新增一個操作：
  隔離：
    將郵件傳送到隔離區："URL類別入站（集中）"
    重複消息：已啟用
(附註：此內容過濾器要求您啟用「安全服務」—>「URL過濾」)
名稱:**URL_惡意**
新增一個條件：
  URL信譽：
    URL信譽為：惡意（–10.0到–6.0）
新增一個操作：
  隔離：
    將郵件傳送到隔離區："URL惡意入站（集中）"
    重複消息：已禁用****隔離原始****)
名稱:**Password_Protected**
新增一個條件：
  附件保護：一個或多個附件受到保護
新增一個操作：
  隔離：
    將郵件傳送到隔離區："Pwd Protected Inbound（集中）"
    重複消息：已啟用
名稱:**大小_10M**
新增一個條件：
  郵件大小為：
    大於或等於：1000萬
新增一個操作：
  新增消息標籤：
    輸入術語：NOOP
(附註：必須執行某些操作，因此，我們在此標籤郵件以表示未執行任何操作。內容篩選器為「已匹配」這一事實將允許它在報告中顯示。無需執行任何「操作」即可將其顯示在「報告」中。)
名稱:**SPF_Hard_Fail**
新增一個條件：
  SPF驗證：「is」失敗
新增一個操作：
  隔離：
    將郵件傳送到隔離區："SPF硬故障（集中）"
    重複消息：已啟用

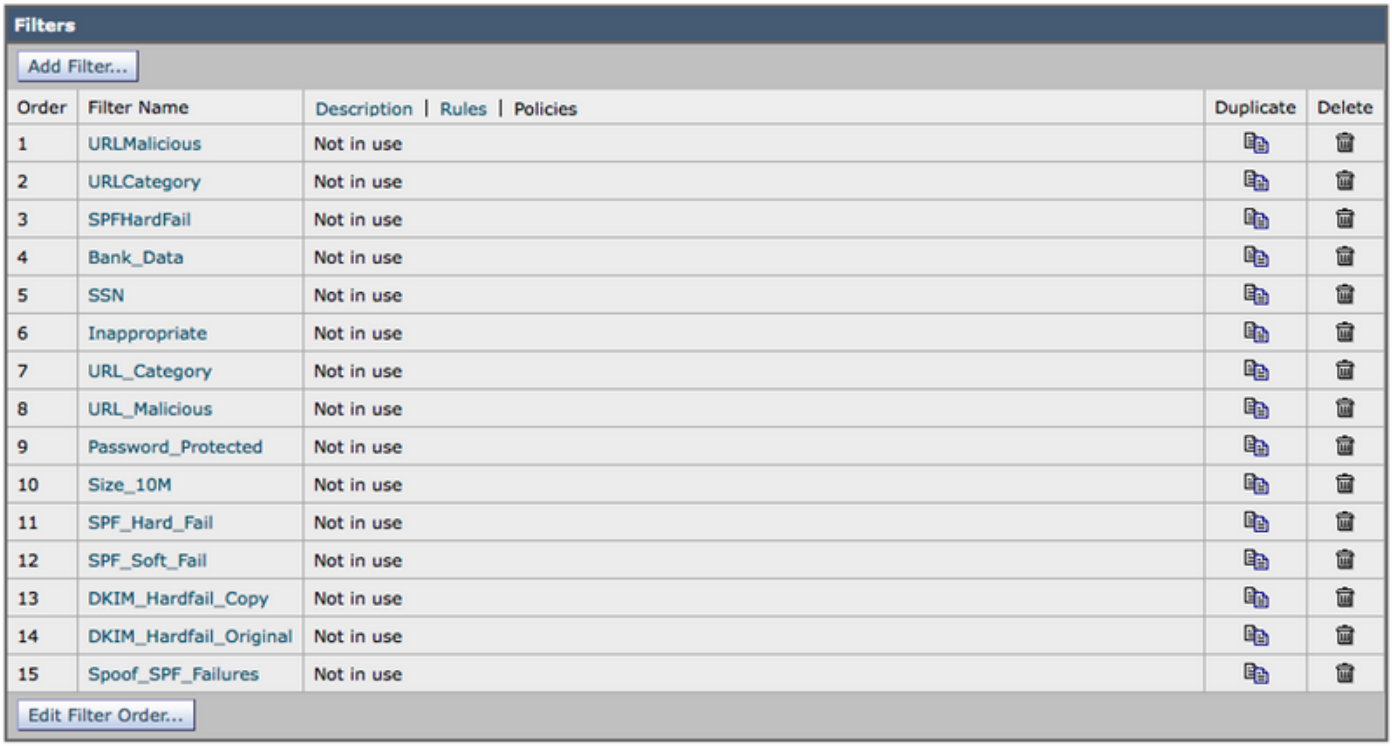
(附註：「Is Fail」是硬SPF故障，它表示域的所有者將告訴您丟棄從發件人處收到的未在其SPF記錄中列出的所有電子郵件。最初，最好是使用「重複郵件」，並在隔離原始郵件之前（即關閉重複郵件）檢查失敗的一兩週。

名稱:**SPF_Soft_Fail**
新增一個條件：
  SPF驗證："is"軟故障
新增一個操作：
  隔離：
    將郵件傳送到隔離區："SPF軟故障（集中）"
    重複消息：已啟用
名稱:**DKIM_Hardfail_Copy**
新增一個條件：
  DKIM身份驗證："is" Hardfail
新增兩個操作：
  新增/編輯標題：
    標題名稱：主題
    點選「Prepend to the Value of Existing Header」（附加到現有題頭的值）並輸入：[複製 — 不發佈]"
  隔離：
    將郵件傳送到隔離區："DKIM硬故障（集中）"
    重複消息：已啟用
(附註：最初隔離郵件的副本。)
名稱:**DKIM_Hardfail_Original**
新增一個條件：
  DKIM身份驗證："is" Hardfail
新增一個操作：
  隔離：
    將郵件傳送到隔離區："DKIM硬故障（集中）"
    重複消息：已禁用
(附註：我們將為PayPal和eBay域建立另一個傳入郵件策略行，並將此內容過濾器用於我們知道應通過DKIM驗證的域。)
名稱:**Spoof_SPF_Failures**
新增一個條件，但已選中Softfail和Hardfail:
  SPF驗證："is" Softfail，同時點選"Fail"
 (因此您按一下了「Softfail」和「Fail」兩個覈取方塊
新增一個操作：
  隔離：
    將郵件傳送到隔離區："SpoofMail（集中）"
    重複消息：啟用
(附註：我們將使用此內容過濾器對來自您自己的域的偽裝傳送的傳入電子郵件執行操作 — 欺騙。從設定為隔離副本的操作開始，在檢視SpoofMail隔離區幾週後，您可以修改SPF TXT DNS記錄以新增所有合法發件人，並且在某些時候，可以通過禁用重複郵件覈取方塊來更改此內容過濾器以隔離原始郵件。)

例如，在提交之前，Bank_Data內容過濾器應具有如下外觀。



建立所有傳入內容過濾器後，該表現在應如下所示：



由於選擇了「Policies」函數（您將看到頂部中間的Policies超文本），因此中間列顯示內容過濾器應用到的傳入郵件策略。由於我們尚未將其應用於任何傳入郵件策略，因此將顯示「未使用」。

將傳入內容過濾器應用於傳入郵件策略

- 導覽至："Mail Policies > Incoming Mail Policies"
- 按一下「默認策略」的內容過濾器單元格中的「禁用」文本。
- 下拉選單按鈕被設定為「禁用內容過濾器」。
- 按一下該按鈕並設定為「啟用內容過濾器」，您將立即看到已建立的所有傳入內容過濾器。
- 啟用除DKIM_Hardfail_Original和Spoof_SPF_Failures之外的所有篩選器。
- 「Submit」和「Commit」。

適用於您的域的eBay & Paypal和Spoof電子郵件保護的DKIM驗證

這兩個主題將涉及利用DKIM驗證和SPF驗證的內容過濾器。因此，我們必須首先確保啟用DKIM和SPF驗證。

1.在郵件流策略內啟用DKIM和SPF驗證

- 導覽至：**"郵件策略>郵件流策略"**
- 在具有「Accept」的「Connection Behavior」的所有郵件流策略內啟用DKIM和SPF驗證。
- 按一下底部超文本「Default Policy Parameters」，將「**DKIM Verification**」設定為「**On**」，並將「SFP/SIDF Verification」設定為「**On**」。
- 按一下「**提交**」和「**提交**」。
- 現在可檢視「郵件流策略」(Mail Flow Policies)表。檢視名為「**Behavior**」的**列，並編**輯行為設定為「**Relay**」的任何郵件流**策略**
- 對這些郵件流策略的DKIM和SPF驗證均關閉「**關閉**」。
- 按一下「**提交**」和「**提交**」。

我們不希望ESA對從您的Exchange郵件伺服器出站標題接收到ESA的電子郵件執行DKIM或SPF驗證。在大多數配置中，「RELAYED」郵件流策略是中繼行為的唯一一行。

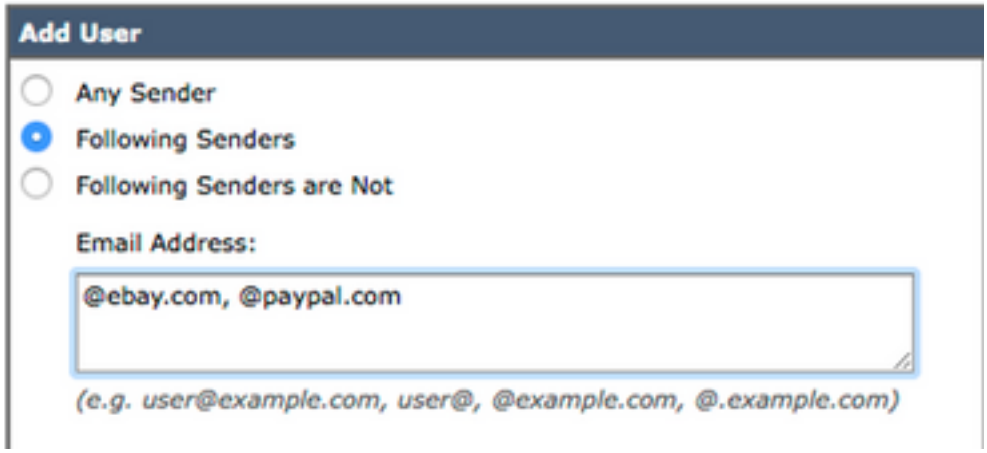
2.為eBay和Paypal建立新的傳入郵件流策略

從eBay和Paypal收到的入站電子郵件應始終通過DKIM驗證。因此，我們將建立另一個傳入郵件策略，以對這些域中的電子郵件使用DKIM_Hardfail_Original Incoming Content Filter。

- 導覽至：**"Mail Policies > Incoming Mail Policies"**
- 按一下「**Add Policy**」**按**鈕。
- 輸入名稱：**"DKIM硬體故障原始"**
- 按一下 **"新增使用者……"** 按鈕。

在下一個配置面板中，您可以定義哪些郵件將與此新的傳入郵件策略匹配。我們只想定義「發件人」（配置面板的左側部分）的條件。

- 按一下 **"關注發件人"** 單選按鈕並在「電子郵件地址」表中輸入**"@ebay.com, @paypal.com」**



- 按一下 **"確定"** 按鈕。
- 按一下」**提交**」.

3.為您的域建立新的傳入郵件流策略（欺騙保護）

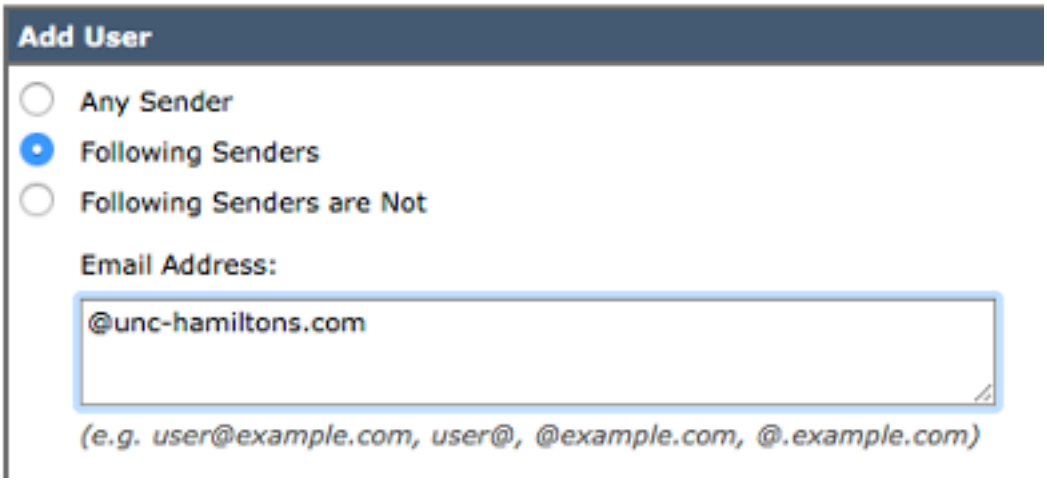
本節中的步驟將允許您對包含您自己的域的「發件人」電子郵件地址且SPF驗證失敗的傳入電子郵

件執行操作。當然，這取決於您已在DNS中發佈了SPF文本記錄。如果尚未建立/發佈域的SPF文本資源記錄，請跳過這些步驟。

- 導覽至："Mail Policies > Incoming Mail Policies"
- 按一下「Add Policy」按鈕。
- 輸入名稱："欺騙保護"
- 按一下 "新增使用者....." 按鈕。

在下一個配置面板中，您可以定義哪些郵件將與此新的「傳入郵件策略」行匹配。您只需要定義「發件人」(Sender)的條件（配置面板的左側部分）。

- 按一下 "關注發件人" 單選按鈕，然後在「電子郵件地址：」文本框中輸入域。對我來說，我的域是「@unc-hamiltons.com」



- 按一下」提交」.

系統再次顯示「傳入郵件策略」(Incoming Mail Policies)表格，但現在，在「預設策略」(Default Policy)的上方又顯示了一個新的「郵件策略」(Mail Policy)行。

- 在新行的「內容過濾器」單元格中按一下（使用預設值）超文本。
- 將下拉選單反向「Enable Content Filters(Customized Settings)」。
- 選中Spoof_SPF_Failures，同時確保未選中「DKIM_Hardfail_Copy」和「DKIM_Hardfail_Original」。
- 按一下「提交」和「提交更改」。

Incoming Mail Policies表現在應如下所示：

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	DKIM Hardfail Original	(use default)	(use default)	(use default)	(use default)	URLMalicious URLCategory SPFHardFail Bank_Data ...	(use default)	
2	Spoof_Protection	(use default)	(use default)	(use default)	(use default)	URLMalicious URLCategory SPFHardFail Bank_Data ...	(use default)	
	Default Policy	IronPort Intelligent Multi-Scan Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Deliver	Disabled	URLMalicious URLCategory SPFHardFail Bank_Data ...	Retention Time: Virus: 1 day	

第4步：建立傳出內容過濾器

- 導航至：**「郵件策略>傳出內容過濾器」**
- 以下是您應建立的傳出內容過濾器表。

建立這些傳出內容過濾器

名稱:**Bank_Data**
新增兩個條件：
　郵件正文或附件：
　　包含智慧識別符號：ABA路由編號
　　包含智慧識別符號：信用卡號
新增一個操作：
　隔離：
　　將郵件傳送到隔離區："銀行資料出站（集中）"
　　重複消息：已啟用
（請注意，應用規則應為「如果一個或多個條件匹配」）
名稱:**SSN**
新增一個條件：
　郵件正文或附件：
　　包含智慧識別符號：社會保險號碼(SSN)
新增一個操作：
　隔離：
　　將郵件傳送到隔離區："SSN出站（集中）"
　　重複消息：　已啟用
名稱:**不合適**
新增兩個條件：
　郵件正文或附件：
　　包含詞典中的術語：髒話
　　包含詞典中的術語：性內容
新增一個操作：
　隔離：
　　將郵件傳送到隔離區："不適當的出站（集中）"
　　重複消息：已啟用
名稱:**URL_Category**
新增一個條件：
　URL類別：
　　選擇類別：
　　成人、約會、過濾規避、免費軟體和共用軟體、賭博、
　　遊戲，駭客，內衣和泳衣，非性裸體，
　　暫留的域、對等檔案傳輸、色情
新增一個操作：
　隔離：
　　將郵件傳送到隔離區："URL類別出站（集中）"
　　重複消息：已啟用
名稱:**URL_惡意**
新增一個條件：
　URL信譽：
　　URL信譽為：惡意（–10.0到–6.0）
新增一個操作：
　隔離：
　　將郵件傳送到隔離區："URL惡意出站（集中）"
　　重複消息：已禁用****隔離原始****)
名稱:**Password_Protected**
新增一個條件：
　附件保護：一個或多個附件受到保護
新增一個操作：

隔離：
將郵件傳送到隔離區："Pwd Protected Outbound（集中）"
重複消息：已啟用
名稱:**大小_10M**
新增一個條件：
郵件大小為：
大於或等於：1000萬
新增一個操作：
新增消息標籤：
輸入術語：NOOP
(附註：必須執行某些操作，因此，我們在此標籤郵件以表示未執行任何操作。內容篩選器為「已匹配」這一事實將允許它在報告中顯示。無需執行任何「操作」即可將其顯示在「報告」中。)
名稱:**專有**
新增一個條件：
郵件正文或附件：
包含詞典中的術語：專有
新增一個操作：
隔離：
將郵件傳送到隔離區："專有（集中）"
重複消息：已啟用

由於選擇了「Policies」函式（您將看到頂部中間的Policies超文本），因此中間列顯示內容過濾器應用到的傳出郵件策略。由於我們尚未將其應用於任何外發郵件策略，因此將顯示「未使用」。

- 導覽至："Mail Policies > Outgoing Mail Policies"
- 點選預設策**略的內容篩**選器單元格中的「禁用」文本。
- 下拉選單按鈕設定為「Disable Content Filters」。
- 按一下該按鈕並設定為**「啟用內容過濾器」**，您將立即看到已建立的所有傳出內容過濾器。
- **「啟用」所有**篩選器。
- 「Submit」和「Commit」。

摘要

現在，您已為傳入和傳出內容過濾器實施了初始最佳實踐。大多數（不是全部）內容過濾器使用隔離操作，並選擇選中(啟用)「重複郵件」選項 — 該選項僅放置原始郵件的副本，並不阻止郵件的傳送。這些內容過濾器的用途是允許您收集有關流向您公司的入站和出站電子郵件型別的資訊。

話雖如此，在運行內容過濾器報告並檢視儲存在隔離區中的電子郵件副本後，取消選中「重複郵件」覈取方塊選項，從而開始將原始電子郵件放入隔離區而不是副本/重複郵件，可能比較謹慎。