传入和传出内容过滤器最佳实践指南

目录

简介

内容过滤器允许您检查电子邮件的复杂详细信息并对电子邮件采取操作（或不采取操作）。创建传入或传出内容过滤器后，即可将其应用于传入或传出邮件策略。当任何邮件与内容过滤器匹配时，思科邮件安全设备(ESA)和安全管理设备(SMA)上的“内容过滤器”报告将能够显示与任何内容过滤器匹配的所有邮件。因此，即使不采取任何措施，也是获取有关进出贵组织的电子邮件类型的宝贵信息的绝佳方法，使您能够“模式化”您的电子邮件流。

由于内容过滤器“条件”和“操作”有许多不同，因此本文档将指导您完成一些非常常见且推荐的传入和传出内容过滤器。

步骤概述

步骤 1：导入所需的词典

本文档将提供实施一些最佳实践传入和传出内容过滤器所需的步骤。我们要创建的内容过滤器将引用一些字典，因此我们需要先导入这些字典。ESA随字典一起提供，您只需将其导入配置，以便在我们将创建的内容过滤器中引用它们。

第2步：创建集中隔离区

对于大多数内容过滤器，我们将创建“操作”，将隔离邮件（或邮件副本）到指定的指定自定义（新）隔离区，因此，我们需要首先在SMA上创建这些隔离区，因为本文档假定您已在ESA和隔离区之间启用集中PVO（策略、病毒和爆发）隔离区SMA。

步骤 3：创建传入和传出内容过滤器并应用于策略

导入词典并创建隔离区后，我们将创建入站内容过滤器并将其应用于传入邮件策略，然后创建传出内容过滤器并将其应用于传出邮件策略。

步骤 1：导入所需的词典

导入我们将在内容过滤器中引用的词典：

- 在ESA设备上，导航至“邮件策略>字典”
- 单击页面右侧的Import Dictionary按钮。

脏话：

- 选择“从IronPort设备上的配置目录导入”
- 选择“profanity.txt”并单击“下一步”。
- 名称：粗俗
- 单击“匹配整个单词”(非常重要)
- 修改术语（添加新术语或删除不需要的术语）
- 单击“提交”

性内容：

- 选择“从IronPort设备上的配置目录导入”
- 选择“semor_content.txt”，然后单击“下一步”。
- 名称：性内容
- 单击“匹配整个单词”(非常重要)
- 修改术语（添加新术语或删除不需要的术语）
- 单击“提交”

专有：

- 选择“从IronPort设备上的配置目录导入”
- 选择“propritary_content.txt”并单击“下一步”。
- 名称：专有
- 单击“匹配整个单词”(非常重要)
- 修改术语（添加新术语或删除不需要的术语）
- 单击“提交”

步骤2：创建集中隔离区

- 在SMA上，导航至“Email Tab > Message Quarantine > PVO Quarantines”
- 这是“隔离区”(Quarantines)表在我们开始之前应显示的内容。所有隔离区都为默认隔离区。

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.

- 单击 "添加策略隔离区……" 按钮
- 创建以下隔离区。
- 有些将被传入内容过滤器使用，有些将被传出内容过滤器使用。您以相同的方式创建它们。

PVO隔离区 — 由传入内容过滤器使用

URL恶意入站：
名称：URL恶意入站
保留期：14 天
默认操作:DELETE

SPF硬故障：
名称：SPF硬故障
保留期：14 天
默认操作:DELETE

释放空间：enable
入站URL类别：
名称：入站URL类别
保留期：14 天
默认操作:DELETE
释放空间：enable
银行数据入站：
名称：银行数据入站
保留期：14 天
默认操作:DELETE
释放空间：enable
SSN入站：
名称：SSN入站
保留期：14 天
默认操作:DELETE
释放空间：enable
入站不当：
名称：不适当的入站
保留期：14 天
默认操作:DELETE
释放空间：enable

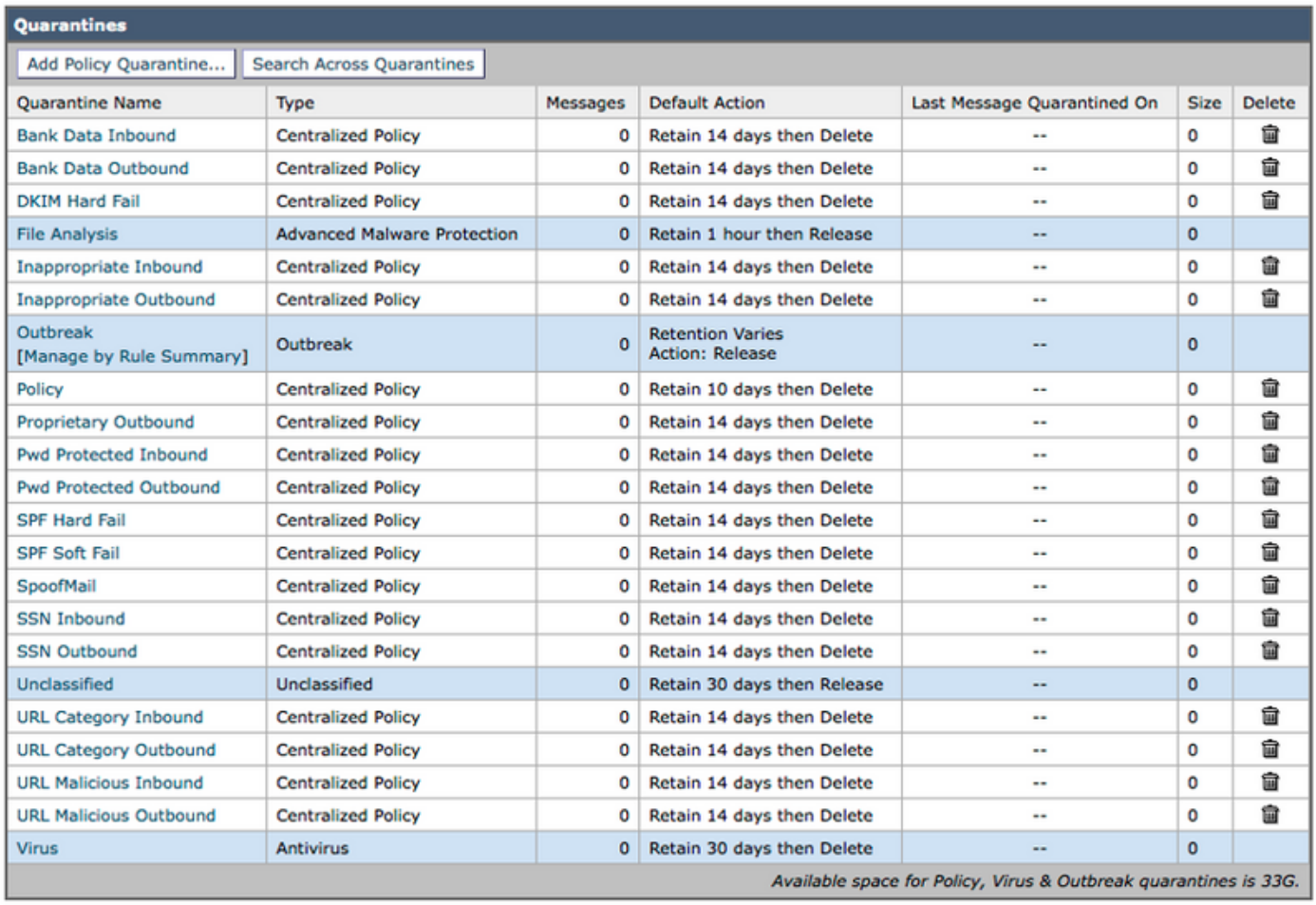
释放空间：enable
SPF软故障：
名称：SPF软故障
保留期：14 天
默认操作:DELETE
释放空间：enable
SpoofMail:
名称：SpoofMail
保留期：14 天
默认操作:DELETE
释放空间：enable
DKIM硬失败：
名称：DKIM硬故障
保留期：14 天
默认操作:DELETE
释放空间：enable
入站密码保护：
名称：Pwd保护入站
保留期：14 天
默认操作:DELETE
释放空间：enable

PVO隔离区 — 外发内容过滤器使用

银行数据出站：
名称：银行数据出站
保留期：14 天
默认操作:DELETE
释放空间：enable
SSN出站：
名称：SSN出站
保留期：14 天
默认操作:DELETE
释放空间：enable
出站不当：
名称：不适当的出站
保留期：14 天
默认操作:DELETE
释放空间：enable
专有出站：
名称：专有出站
保留期：14 天
默认操作:DELETE
释放空间：enable

URL恶意出站：
名称：URL恶意出站
保留期：14 天
默认操作:DELETE
释放空间：enable
出站URL类别：
名称：出站URL类别
保留期：14 天
默认操作:DELETE
释放空间：enable
受密码保护的出站：
名称：Pwd保护出站
保留期：14 天
默认操作:DELETE
释放空间：enable

- 以下是创建所有PVO隔离区后PVO表应如何处理。



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.

步骤 3：创建传入内容过滤器

导入词典并创建PVO隔离区后，您现在可以开始创建传入内容过滤器：

- 导航至："**邮件策略>传入内容过滤器**"
- 这是您应创建的传入内容过滤器表。例如，下表下方是一个屏幕截图，说明如何创建第一个屏幕截图。

创建这些传入内容过滤器

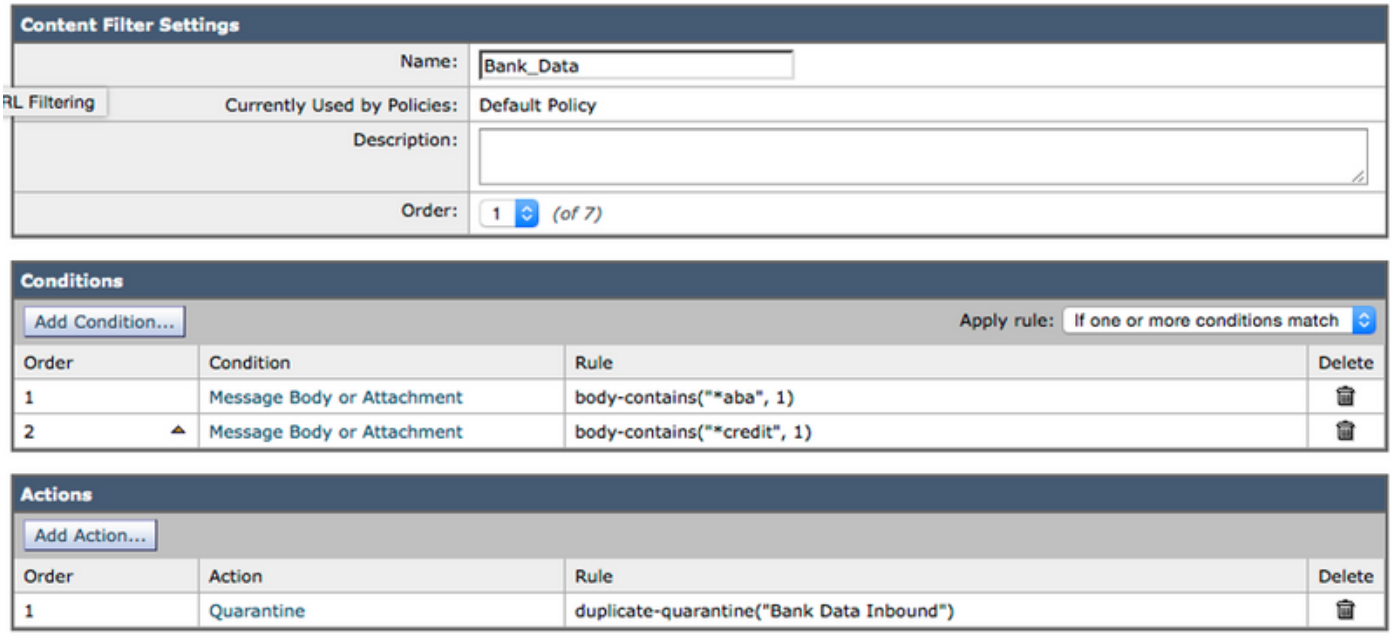
名称：**银行数据**
添加两个条件：
  邮件正文或附件：
    包含智能标识符：ABA路由号
    包含智能标识符：信用卡号
添加一个操作：
  隔离：
    将邮件发送到隔离区："银行数据入站（集中）"
    重复消息：启用
（请注意，应用规则应为"如果一个或多个条件匹配"）
名称：**SSN**
添加一个条件：
  邮件正文或附件：
    包含智能标识符：社会保障号(SSN)
添加一个操作：
  隔离：
    将邮件发送到隔离区："SSN入站（集中）"
    重复消息：启用

名称：**不适当**
添加两个条件：
  邮件正文或附件：
    包含词典中的术语：脏话
    包含词典中的术语：性内容
添加一个操作：
  隔离：
    将邮件发送到隔离区："不适当的入站（集中）"
    重复消息：启用
名称：**URL_Category**
添加一个条件：
  URL类别：
    选择职业类别：
      成人、约会、过滤规避、免费软件和共享软件、赌博、
      游戏，黑客，内衣和泳装，非性裸体，
      暂留的域、对等文件传输、色情
添加一个操作：
  隔离：
    将邮件发送到隔离区："入站URL类别（集中）"
    重复消息：启用
(注：此内容过滤器要求您启用“安全服务” — >“URL过滤”)
名称：**URL_恶意**
添加一个条件：
  URL信誉：
    URL信誉为：恶意（–10.0到–6.0）
添加一个操作：
  隔离：
    将邮件发送到隔离区："URL恶意入站（集中）"
    重复消息：已禁用（****隔离原始****）
名称：**Password_Protected**
添加一个条件：
  附件保护：一个或多个附件受保护
添加一个操作：
  隔离：
    将邮件发送到隔离区："Pwd Protected Inbound（集中）"
    重复消息：启用
名称：**大小_10M**
添加一个条件：
  邮件大小为：
    大于或等于：1000万
添加一个操作：
  添加邮件标记：
    输入术语：NOOP
(注：必须执行某些操作，因此我们在此处“标记”消息以表示未执行任何操作。内容过滤器为“匹配”的事实将允许其显示在报告中。无需执行任何“操作”即可在报告中显示。)
名称：**SPF_Hard_Fail**
添加一个条件：
  SPF验证：“是”失败
添加一个操作：
  隔离：
    将邮件发送到隔离区："SPF硬故障（集中）"
    重复消息：启用
(注：“is fail”是硬SPF故障，这意味着域的所有者会告诉您删除从发件人处收到的所有未在其

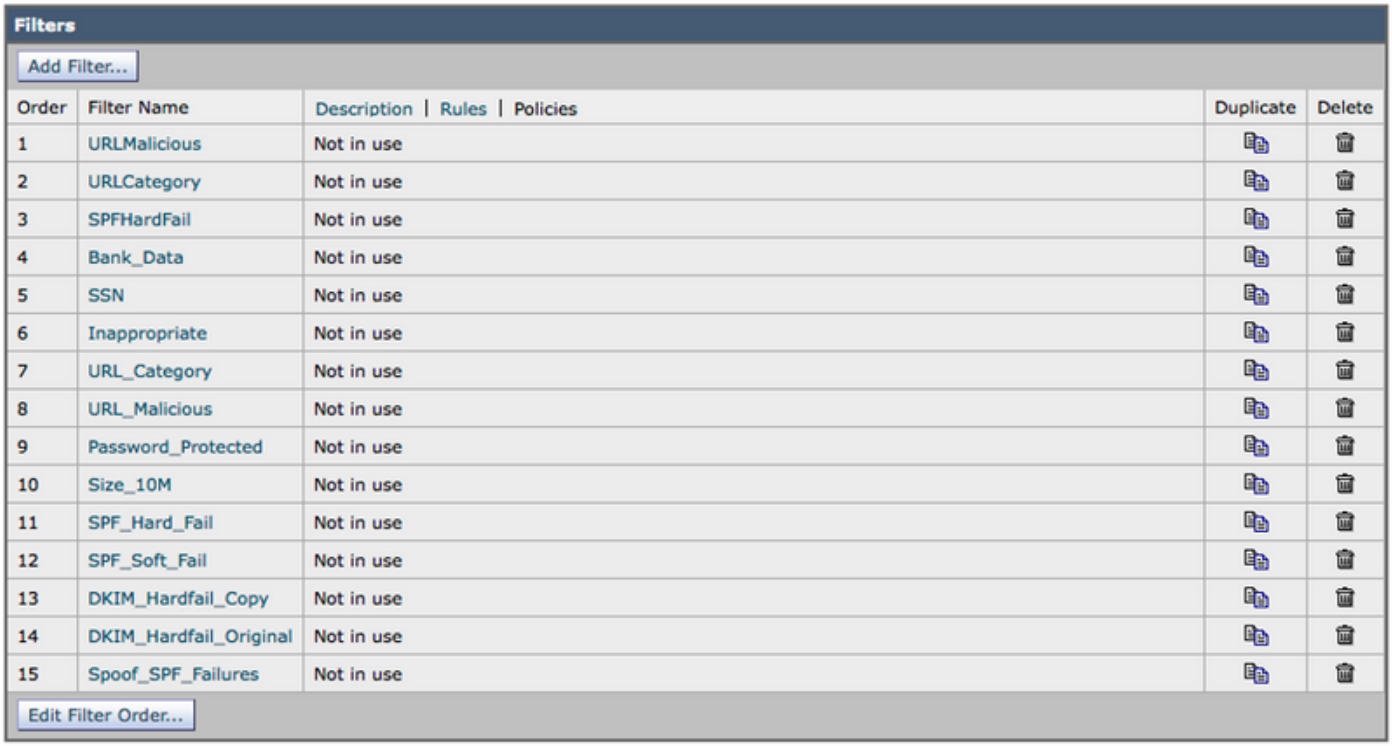
SPF记录中列出的邮件。最初，最好使用“重复邮件”，在隔离原始邮件（即关闭重复邮件）之前检查一两周的故障。

名称：**SPF_Soft_Fail**
添加一个条件：
  SPF验证：“is”软失败
添加一个操作：
  隔离：
    将邮件发送到隔离区："SPF软故障（集中）"
    重复消息：启用
名称：**DKIM_Hardfail_Copy**
添加一个条件：
  DKIM身份验证：“是”硬故障
添加两个操作：
  添加/编辑标题：
    标题名称：主题
    点击“Prepend to the Value of Existing Header”，然后输入：[副本 — 不发布]”
  隔离：
    将邮件发送到隔离区："DKIM硬故障（集中）"
    重复消息：启用
(注：最初隔离邮件的副本。)
名称：**DKIM_Hardfail_Original**
添加一个条件：
  DKIM身份验证：“是”硬故障
添加一个操作：
  隔离：
    将邮件发送到隔离区："DKIM硬故障（集中）"
    重复消息：禁用
(注：我们将为PayPal和eBay域创建另一个传入邮件策略行，并将对我们知道应通过DKIM验证的域使用此内容过滤器。)
名称：**Spoof_SPF_Failures**
添加一个条件，但同时选中了“软故障”和“硬故障”：
  SPF验证：“is”Softfail，然后点击“Fail”
 (因此，您有两个复选框已单击“Softfail”和“Fail”
添加一个操作：
  隔离：
    将邮件发送到隔离区："SpoofMail（集中）"
    重复消息：enable
(注：我们将使用此内容过滤器对伪装从您自己的域发送的传入电子邮件采取操作 — 欺骗。从设置为隔离副本的操作开始，在查看SpoofMail隔离区几周后，您可以修改SPF TXT DNS记录以添加所有合法发件人，并且在某个时候，您可以通过禁用重复邮件复选框来更改此内容过滤器以隔离原始邮件。)

例如，在提交之前，Bank_Data内容过滤器应该这样。



创建所有传入内容过滤器后，表现在应如下所示：



由于选择了“策略”功能（您将在顶部中间看到“策略”超文本），因此中间列显示内容过滤器已应用的传入邮件策略。由于我们尚未将它们应用到任何传入邮件策略，因此会显示“未使用”。

将传入内容过滤器应用于传入邮件策略

- 导航至：**"邮件策略>传入邮件策略"**
- 单击“默**认策略"**的“内容过滤器”单元格中**的“禁用”文本**。
- 下拉菜单按钮设置为“禁**用内容过滤器"**。
- 单击该按钮并设置为“**启用内容过滤器"**，系统会立即显示已创建的所有传入内容过滤器。
- 启用除DKIM_Hardfail_Original和Spoof_SPF_Failures之外的所有过滤器。
- **“提交”**和“提**交"**。

eBay & Paypal的DKIM验证和您域的Spoof电子邮件保护

这两个主题将涉及使用DKIM验证和SPF验证的内容过滤器。因此，我们必须首先确保DKIM和SPF验证都已启用。

1.在邮件流策略中启用DKIM和SPF验证

- 导航至："**邮件策略>邮件流策略**"
- 在"连接行为"为"接受"的所有邮件流策略中启用DKIM和SPF验证。
- 单击底部超文本"默认策略参数"，将**"DKIM验**证"设**置为**"On"，**将"SFP/SIDF验证"设置为"On**"。
- 单击**"提交"**和"**提交"**。
- 现在您将看到"邮件流策略"(Mail Flow Policies)表。查看名为"Behavior"**的列**，并编辑任何将Behavior设置为"Relay"的邮件**流策略**
- 为这**些邮件流**策略关闭DKIM和SPF验证。
- 单击**"提交"**和"**提交"**。

我们不希望ESA对从Exchange邮件服务器标题出站的ESA中收到的电子邮件执行DKIM或SPF验证。在大多数配置中，"RELAYED"邮件流策略是中继行为的唯一行。

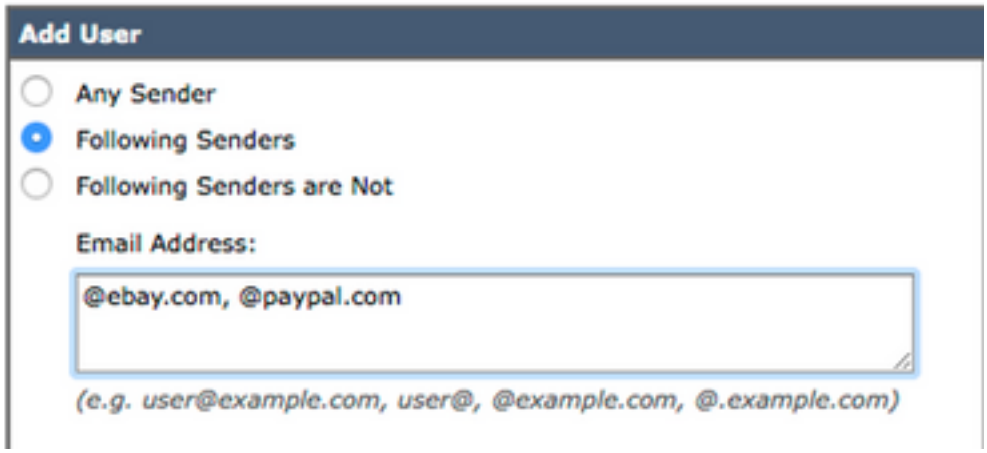
2.为eBay和Paypal创建新的传入邮件流策略

从eBay和Paypal收到的入站电子邮件应始终通过DKIM验证。因此，我们将创建另一个传入邮件策略，以对来自这些域的邮件使用DKIM_Hardfail_Original传入内容过滤器。

- 导航至："**邮件策略>传入邮件策略"**
- 单击"**Add Policy"(添加策**略)按钮。
- 输入名称："**DKIM Hardfail原始"**
- 单击 **"添加用户……"** 按钮。

下一个配置面板允许您定义哪些邮件将匹配此新传入邮件策略。我们只想定义发件人（配置面板的左部分）的条件。

- 单击 **"以下发件人"** 单选按钮，在"电子邮件地址"表中**输入"@**ebay.com,@paypal.com"



- 单击 **"确定"** 按钮。
- 单击**"提交"**。

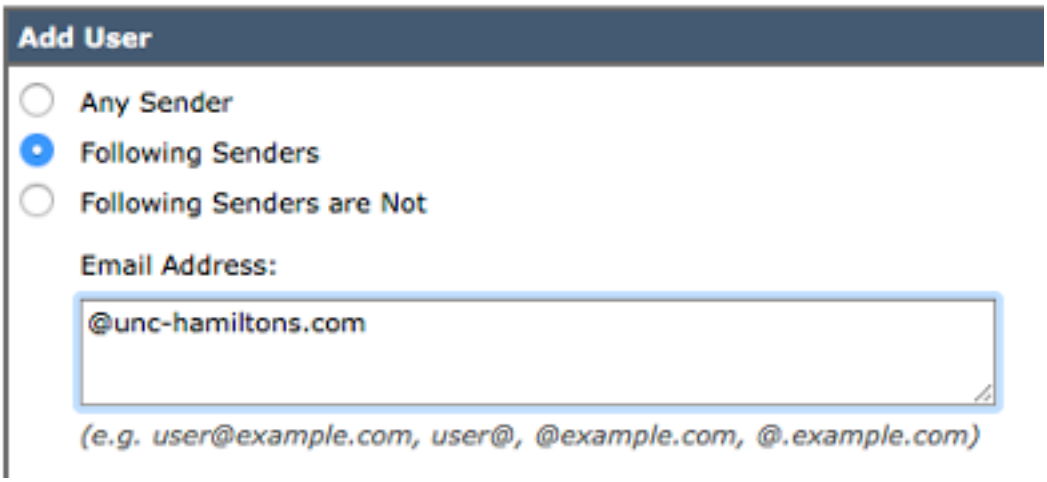
3.为域创建新的传入邮件流策略（欺骗保护）

本节中的步骤将允许您对具有您自己的域的发件人电子邮件地址且未通过SPF验证的传入邮件采取操作。当然，这取决于您已在DNS中发布SPF文本记录。如果尚未为域创建/发布SPF文本资源记录，请跳过这些步骤。

- 导航至："**邮件策略>传入邮件策略**"
- 单击"Add Policy"(**添加策**略)按钮。
- 输入名称："**欺骗保护**"
- 单击 "**添加用户……**" 按钮。

下一个配置面板允许您定义哪些邮件将匹配此新传入邮件策略行。您只想定义发件人的条件（即配置面板的左部分）。

- 单击 "**以下发件人**" 单选按钮，然后在"Email Address:"**文本框中输**入域。对我来说，我的领**域是**"@unc-hamiltons.com"



- 单击"**提交**"。

系统再次显示"传入邮件策略"(Incoming Mail Policies)表，但现在您在"默认策略"(Default Policy)上方又有一个新邮件策略(Mail Policy)行。

- 单击新**行的"内**容过滤器"单元格中的超文本（使用默认）。
- 将下拉菜单翻转到"**启用内容过滤器（自定义设置）**"。
- 检查"**Spoof_SPF_Failures"还**确保"DKIM_**Hardfail_Copy"**和"**DKIM_Hardfail_Original"都未**被检查。
- 单击"**提交**"和"**提交更改**"。

"传入邮件策略"(Incoming Mail Policies)表现在应如下所示：

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	

步骤 4：创建传出内容过滤器

- 导航至："**邮件策略>传出内容过滤器**"
- 这是您应创建的传出内容过滤器表。

创建这些传出内容过滤器

名称：**银行数据**
添加两个条件：
　邮件正文或附件：
　　包含智能标识符：ABA路由号
　　包含智能标识符：信用卡号
添加一个操作：
　隔离：
　　将邮件发送到隔离区："银行数据出站（集中）"
　　重复消息：启用
（请注意，应用规则应为“如果一个或多个条件匹配”）
名称：**SSN**
添加一个条件：
　邮件正文或附件：
　　包含智能标识符：社会保障号(SSN)
添加一个操作：
　隔离：
　　将邮件发送到隔离区："SSN出站（集中）"
　　重复消息：　启用
名称：**不适当**
添加两个条件：
　邮件正文或附件：
　　包含词典中的术语：脏话
　　包含词典中的术语：性内容
添加一个操作：
　隔离：
　　将邮件发送到隔离区："不适当的出站（集中）"
　　重复消息：启用
名称：**URL_Category**
添加一个条件：
　URL类别：
　　选择职业类别：
　　成人、约会、过滤规避、免费软件和共享软件、赌博、
　　游戏，黑客，内衣和泳装，非性裸体，
　　暂留的域、对等文件传输、色情
添加一个操作：
　隔离：
　　将邮件发送到隔离区："出站URL类别（集中）"
　　重复消息：启用
名称：**URL_恶意**
添加一个条件：
　URL信誉：
　　URL信誉为：恶意（–10.0到–6.0）
添加一个操作：
　隔离：
　　将邮件发送到隔离区："URL恶意出站（集中）"
　　重复消息：禁用（****隔离原始****）
名称：**Password_Protected**
添加一个条件：
　附件保护：一个或多个附件受保护
添加一个操作：
　隔离：
　　将邮件发送到隔离区："Pwd Protected Outbound（集中）"
　　重复消息：启用

名称：**大小_10M**
添加一个条件：
　邮件大小为：
　　大于或等于：1000万
添加一个操作：
　添加邮件标记：
　　输入术语：NOOP
(注：必须执行某些操作，因此我们在此处“标记”消息以表示未执行任何操作。内容过滤器为“匹配”的事实将允许其显示在报告中。无需执行任何“操作”即可在报告中显示。)
名称：**专有**
添加一个条件：
　邮件正文或附件：
　　包含词典中的术语：专有
添加一个操作：
　隔离：
　　将邮件发送到隔离区："专有（集中）"
　　重复消息：启用

由于选择了“策略”功能（您将在顶部中间看到“超文本”策略），因此中间列显示内容过滤器已应用的传出邮件策略。由于我们尚未将它们应用于任何外发邮件策略，因此显示“未使用”。

- 导航至：**"邮件策略>传出邮件策略”**
- 单击默认策**略的“内**容过滤器”(Content Filters)单元格中的“禁用”(Disabled)文本。
- 下拉菜单按钮设置为“禁用内**容过滤器**”。
- 单击该按钮并设置为“**启用内容过滤器”**，系统会立即显示已创建的所有传出内容过滤器。
- **“启用”所**有过滤器。
- **“提交”**和“**提交”**。

摘要

您现在已实施传入和传出内容过滤器的初始最佳实践。大多数（并非全部）内容过滤器使用隔离操作并选择选中（启用）“重复邮件”选项 — 该选项仅放置原始邮件的副本，并且不会阻止邮件送达。这些内容过滤器的目的是让您收集有关流向公司的入站和出站电子邮件类型的信息。

话虽如此，在运行内容过滤器报告并查看隔离区中保存的电子邮件副本后，可以谨慎地取消选中“重复邮件”复选框，从而开始将原始邮件放入隔离区，而不是复制/复制。