检测ESA上的欺骗性电子邮件并创建例外

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 什么是邮件欺骗
- 如何检测欺骗性邮件
- 如何允许特定发件人的欺骗

配置

- 创建发件人组
- 创建字典
- 创建邮件过滤器
- 向MY_TRUSTED_SPOOF_HOSTS添加欺骗异常

验证

- 验证伪装邮件是否已隔离
- 验证是否正在传送欺骗异常消息

相关信息

简介

本文档介绍如何控制思科ESA上的邮件欺骗，以及如何为允许发送欺骗邮件的用户创建例外。

先决条件

要求

邮件安全设备(ESA)必须处理传入和传出邮件，并使用RELAYLIST的标准配置将邮件标记为传出。

使用的组件

使用的具体组件包括：

- 词典：用于存储所有内部域。

- 邮件过滤器：用于处理逻辑以检测伪装邮件并插入内容过滤器可以操作的信头。
- 策略隔离区：用于临时存储伪造的电子邮件副本。考虑将已放行邮件的IP地址添加到MY_TRUSTED_SPOOF_HOSTS，以防止此发件人以后的邮件进入策略隔离区。
- MY_TRUSTED_SPOOF_HOSTS:列表以引用您信任的发送IP地址。将发件人的IP地址添加到此列表会跳过隔离区并允许发件人欺骗。您可以将受信任的发件人放置在MY_TRUSTED_SPOOF_HOSTS发件人组中，以便不会隔离来自这些发件人的欺骗邮件。
- 中继列表：列表验证允许中继的IP地址或发送出站电子邮件。如果通过此发件人组发送电子邮件，则假设该邮件不是伪装邮件。

注意：如果调用任一发件人组时调用了不同于MY_TRUSTED_SPOOF_HOSTS或RELAYLIST的内容，则必须使用相应的发件人组名称修改过滤器。此外，如果您有多个侦听程序，则您还有多个MY_TRUSTED_SPOOF_HOSTS。

本文档中的信息基于任何AsyncOS版本的ESA。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

默认情况下，思科ESA上启用欺骗。允许其他域代表您发送邮件有几个正当的理由。 一个常见示例是，ESA管理员想要通过在发送欺骗邮件之前隔离这些邮件来控制欺骗邮件。

要采取特定操作，如隔离伪造的邮件，必须先检测伪造的邮件。

什么是邮件欺骗

邮件欺骗是指伪造邮件信头，使邮件看似来自某人或实际来源以外的其他地方。电子邮件欺骗是网络钓鱼和垃圾邮件活动中使用的一项策略，因为人们更倾向于在认为电子邮件是由合法来源发送时打开该电子邮件。

如何检测欺骗性邮件

您想要过滤信封发件人(Mail-From)和友好发件人(From)信头的邮件，这些邮件在邮件地址中包含您自己的某个传入域。

如何允许特定发件人的欺骗

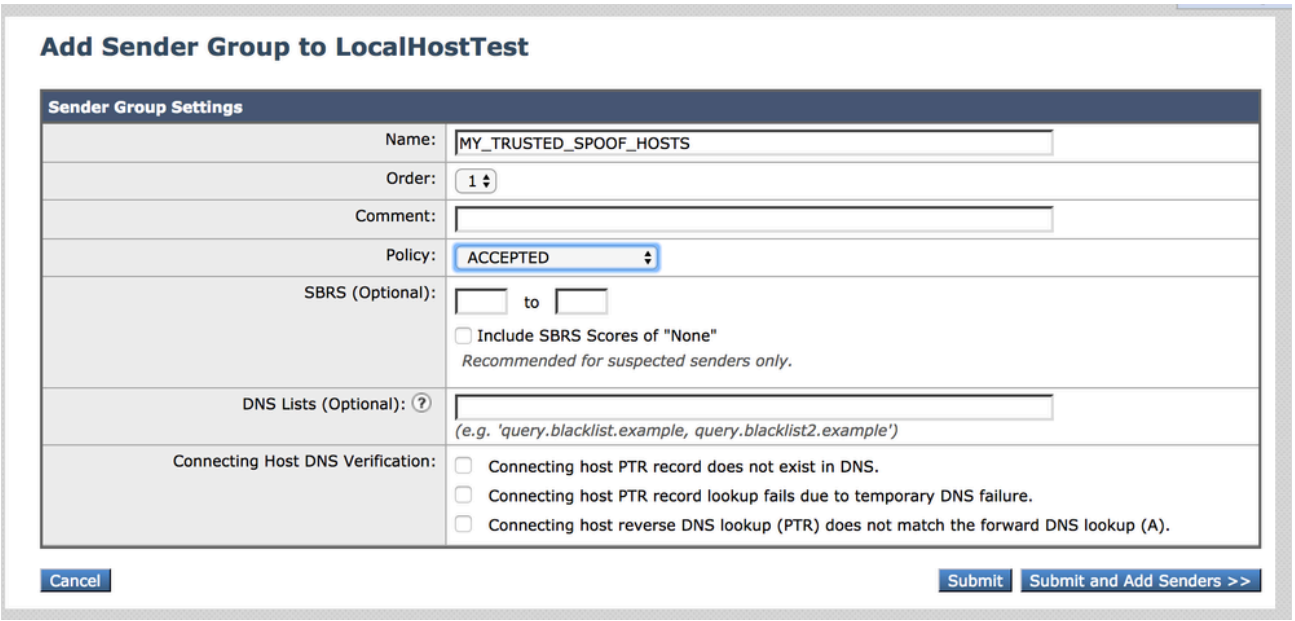
当您实施本文中提供的邮件过滤器时，伪造的邮件会使用信头进行标记，而内容过滤器则用于对信头执行操作。要添加例外，只需将发件人IP添加到MY_TRUSTED_SPOOF_HOSTS。

配置

创建发件人组

1. 从ESA GUI导航到邮件策略> HAT概述
2. 单击 Add。
3. 在Name字段中，指定MY_TRUSTED_SPOOF_HOSTS。
4. 在“订单”字段中指定1。
5. 对于Policy字段，指定ACCEPTED。
6. 单击Submit保存更改。
7. 最后，单击Commit Changes以保存配置

示例：



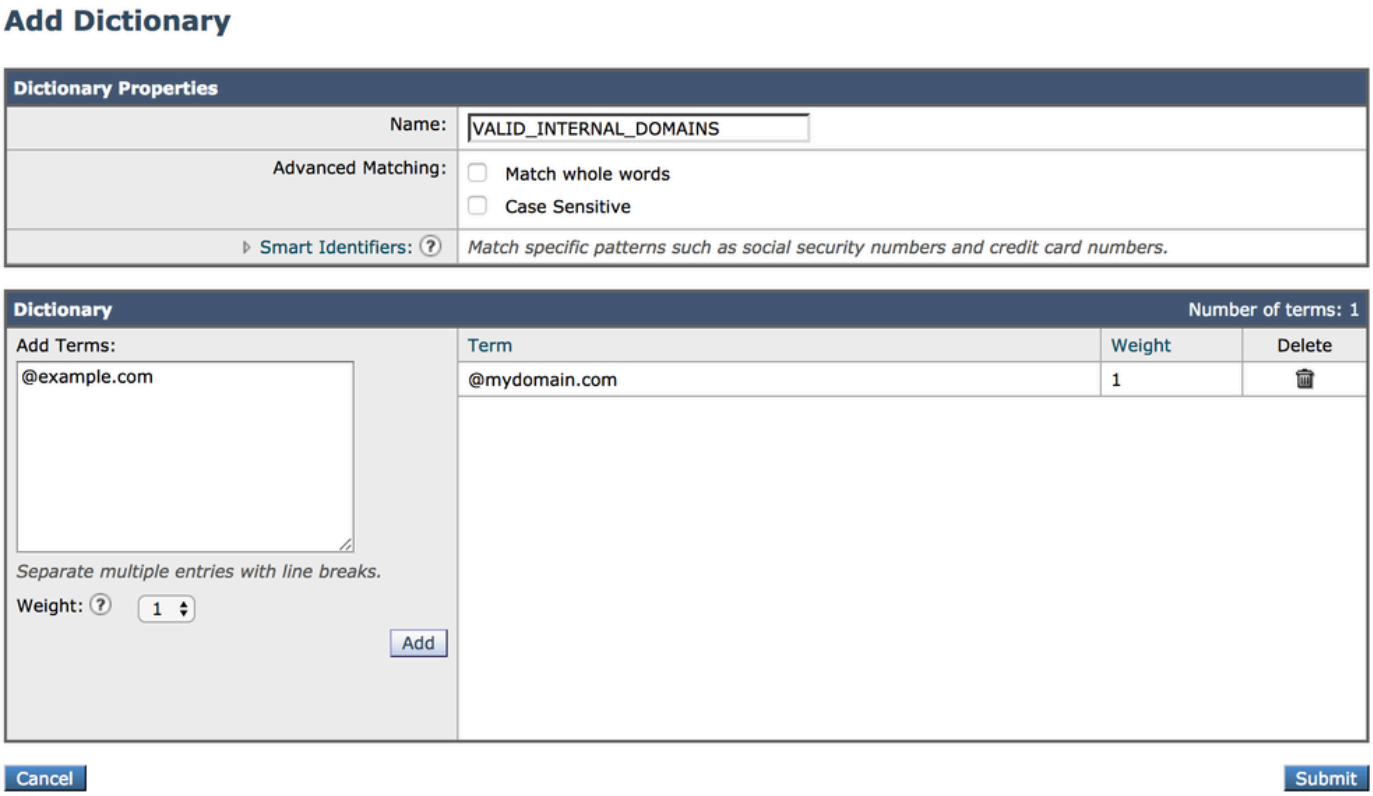
创建字典

为要在ESA上为其禁用欺骗的所有域创建词典：

1. 从ESA GUI导航到邮件策略>字典。
2. 单击Add Dictionary。
3. 在Name字段中，指定“VALID_INTERNAL_DOMAINS”，以使复制和粘贴邮件过滤器不会出错。
4. 在add terms下，添加要检测欺骗的所有域。 在域前面输入带有@符号的域，然后单击add。
5. 确保match whole words复选框未选中。

6. 单击Submit保存字典更改。
7. 最后，单击Commit Changes以保存配置。

示例：



创建邮件过滤器

接下来，您需要创建邮件过滤器以利用刚创建的词典“VALID_INTERNAL_DOMAINS”:

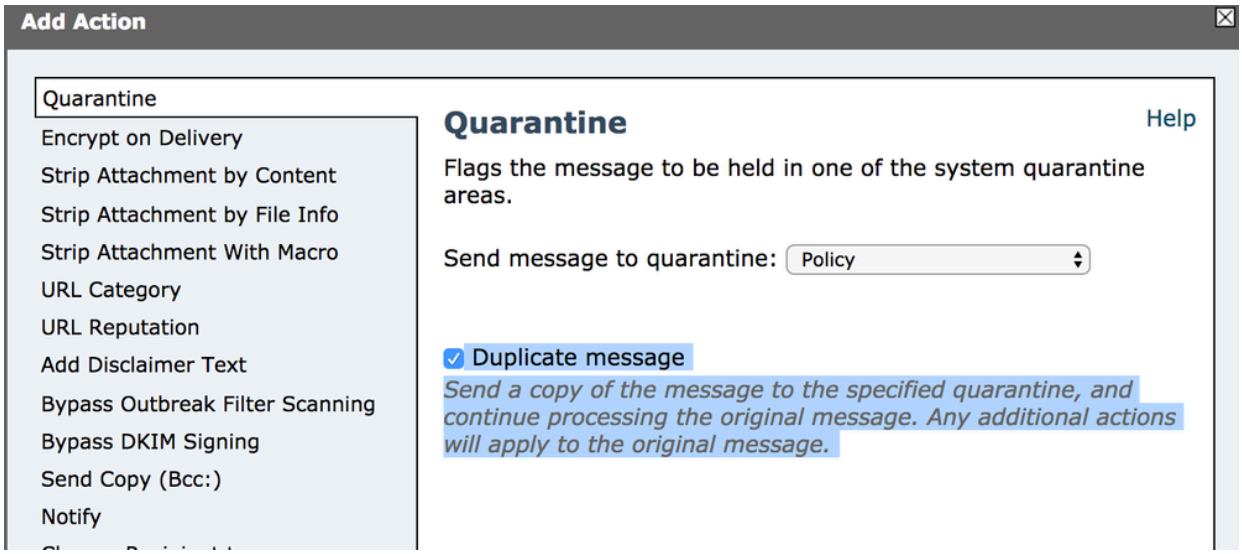
1. 连接到ESA的命令行界面(CLI)。
2. 运行命令Filters。
3. 运行命令New创建新的邮件过滤器。
4. 复制并粘贴此过滤器示例，根据需要编辑实际的发件人组名称：

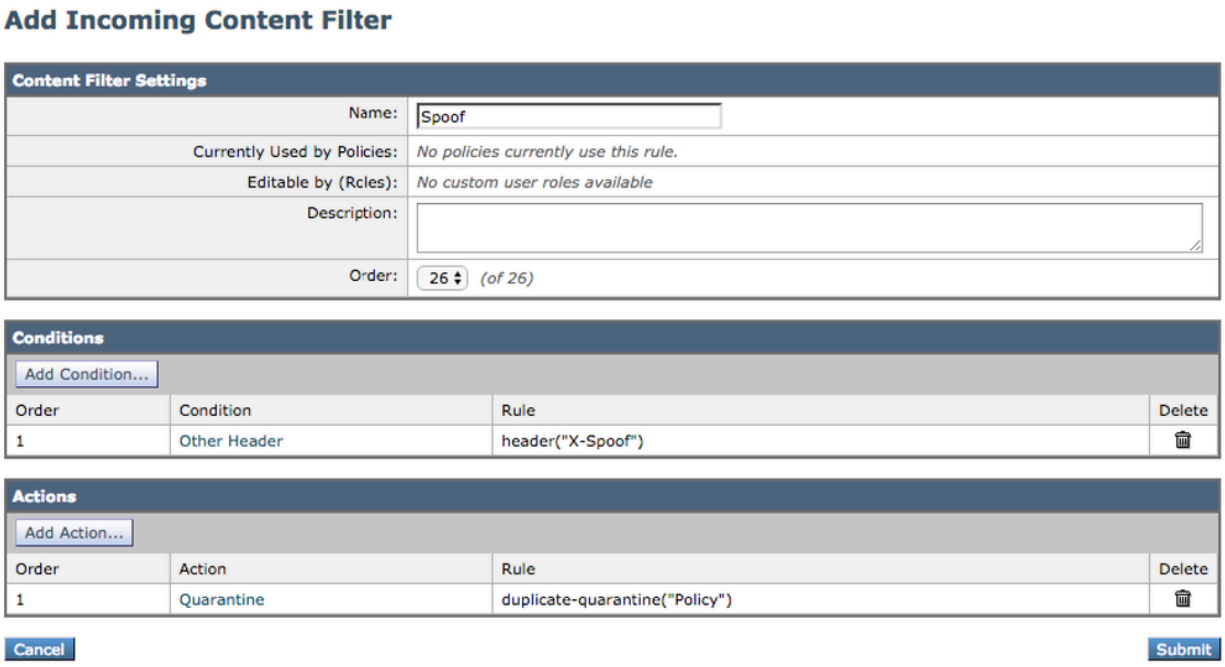
```
mark_spoofed_messages:
if(
     (mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
 OR  (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
 AND ((sendergroup != "RELAYLIST")
 AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
  )
{
insert-header("X-Spoof", "");
}
```

5. 返回主CLI提示符并运行Commit以保存配置。
6. 导航到GUI > Mail Policies > Incoming Content Filters
7. 创建对欺骗报头X-Spoof执行操作的传入内容过滤器：

    1. 添加其他信头
    2. 报头名称：X欺骗
    3. 报头存在单选按钮
    4. 添加操作：duplicate-quarantine（策略）。

> 注意：此处显示的“复制邮件”功能保留邮件的副本，并继续向收件人发送原始邮件。





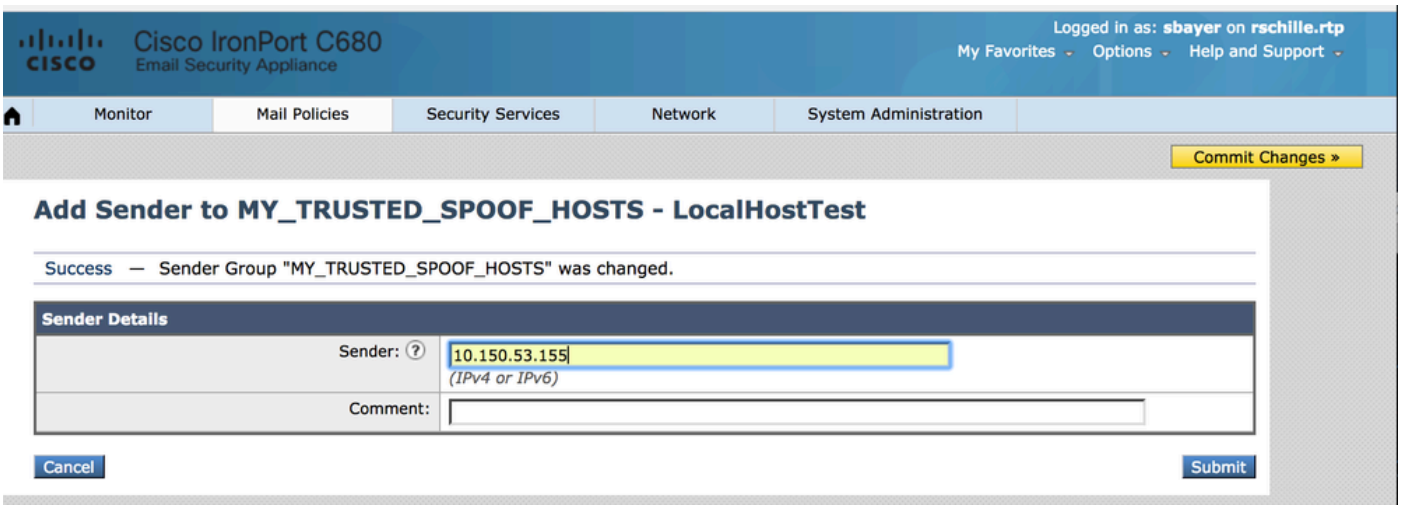
8. 通过GUI > Mail Policies > Incoming Mail Policies将内容过滤器链接到传入邮件策略。
9. 提交并确认更改。

向MY_TRUSTED_SPOOF_HOSTS添加欺骗异常

最后，您需要将欺骗异常（IP地址或主机名）添加到MY_TRUSTED_SPOOF_HOSTS发件人组。

1. 通过Web GUI导航：邮件策略> HAT概述
2. 单击并打开MY_TRUSTED_SPOOF_HOSTS发件人组。
3. 单击Add Sender... 添加IP地址、范围、主机名或部分主机名。
4. 单击Submit保存发件人更改。
5. 最后，单击Commit Changes以保存配置。

示例：



验证

验证伪装邮件是否已隔离

发送测试消息，指定其中一个域作为信封发件人。通过对邮件执行邮件跟踪，验证过滤器是否按预期工作。预期的结果是邮件被隔离，因为您尚未为允许假冒的发件人创建任何例外。

<#root>

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <xxxx_xxxx@domain.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 Subject 'test1'
Thu Apr 23 07:10:07 2015 Info: MID 102 ready 177 bytes from <user_1@example.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 matched all recipients for per-recipient policy DEFAULT in the i
Thu Apr 23 07:10:11 2015 Info: MID 102 interim verdict using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:10:11 2015 Info: MID 102 antivirus negative
```

Thu Apr 23 07:10:12 2015 Info: MID 102 quarantined to "Policy" (message filter:quarantine_spoofed_messag

```
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

验证是否正在传送欺骗异常消息

欺骗例外发件人是上面过滤器中引用的发件人组中的IP地址。

引用RELAYLIST的原因是ESA用它来发送出站邮件。由RELAYLIST发送的邮件通常是出站邮件，若不包含，则会产生误报，或以上过滤器隔离出站邮件。

添加到MY_TRUSTED_SPOOF_HOSTS的欺骗异常IP地址的邮件跟踪示例。预期操作为deliver而不是quarantine。（此IP允许伪装）。

<#root>

```
Thu Apr 23 07:25:57 2015 Info: Start MID 108 ICID 11
Thu Apr 23 07:25:57 2015 Info: MID 108 ICID 11 From: <user_1@example.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <user_xxxx@domain.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 Subject 'test2'
Thu Apr 23 07:26:10 2015 Info: MID 108 ready 163 bytes from <user_1@example.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 matched all recipients for per-recipient policy DEFAULT in the i
Thu Apr 23 07:26:10 2015 Info: MID 108 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:26:10 2015 Info: MID 108 antivirus negative
Thu Apr 23 07:26:10 2015 Info: MID 108 queued for delivery
Thu Apr 23 07:26:10 2015 Info: Delivery start DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: Message done DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: MID 108 RID [0] Response '2.0.0 t58EVG9N031598
```

Message accepted for delivery'

```
Thu Apr 23 07:26:11 2015 Info: Message finished MID 108 done
```

相关信息

- ESA欺骗邮件过滤
- 使用发件人验证进行欺骗保护

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。