目录

问题：

如何配置ESA跳过反垃圾邮件和抗病毒扫描委托发送方的？

AsyncOS提供您能使用跳过反垃圾邮件或抗病毒检查您的多数委托发送方的三个主要工具。请注意: ESA不建议跳过的抗病毒在任何时间检查，您的多数委托发送方，由于在因疏忽所致的传染的可能性与病毒。下列是能跳过反垃圾邮件检查您的消息流的某子集的您三个方式的讨论。

对您的第一工具联机是主机访问表(帽子)邮件流量策略。使用邮件流量策略，您能鉴别发送方由IP地址(使用数字IP地址或PTR DNS名)，由SenderBase分数，或者通过本地DNS whitelist或黑名单。一旦在一发送方组内识别发送方作为委托帽子的，您能然后标记跳过反垃圾邮件扫描的发送方组。

例如，请假设您要识别一个特定业务伙伴， EXAMPLE.COM，不应该有检查他们的邮件的反垃圾邮件。您会必须发现SCU.COM邮件服务器IP地址(或DNS命名指针记录)。在这种情况下，假设，EXAMPLE.COM有将有与DNS PTR记录的IP地址"smtp1.mail.scu.com"至"smtp4.mail.scu.com."在这种情况下记住的邮件服务器我们查看PTR记录(有时呼叫反向DNS)为邮件服务器;这与居于在SCU.COM将使用流出的邮件的域名无关。

您可能创建一新的发送方组(或使用一现有发送方组，例如WHITELIST)与邮件Policies>Overview>Add发送方组。请创建呼叫“NotSpammers的”一。在您提交了此页后，您将返回对邮件Policies>Overview屏幕，您将有机会添加此发送方组的一项新的策略。如果点击“请添加策略”，您将给机会创建一项新的策略。在这种情况下，我们在一个区域中要只改写默认策略：垃圾邮件检测。给予策略名称并且设置连接行为是“接受”，然后请移下来对垃圾邮件检测部分和设置此策略跳过垃圾邮件检查。提交新的策略，和不忘记“确认更改”。

备选方法将使用流入的邮件策略跳过反垃圾邮件扫描。在帽子和流入的邮件策略之间的区别是帽子根据在发送方的IP信息完全地：真的IP地址、IP地址如在DNS反射，根据IP地址)的SenderBase分数(或根据IP地址的DNS whitelist或黑名单条目。流入的邮件策略根据消息信封信息：谁消息是给或谁消息是从。 这意味着他们是易受被唬弄由扮演消息发送方的某人。然而，如果要跳过所有反垃圾邮件检查流入的邮件的来自有电子邮件地址在“@example.com结束的人”，您可能执行那。

要创建这样策略，请去邮寄Policies>Incoming邮件Policies>Add策略。这将让您添加定义了一套发送方的策略(或收件人)。一旦定义了流入的邮件策略，在概述屏幕(邮件Policies>Incoming邮件策略)将看起来。 您能然后点击“反垃圾邮件”列和编辑反垃圾邮件的特定设置此特定用户的。

一项特定的策略的反垃圾邮件设置有大量选项，但是在这种情况下，我们要跳过反垃圾邮件检查。注意此处在基于帽子的策略和流入的邮件策略之间的另一个区别：而流入的邮件策略有更加巨大的控制，帽子能只让您跳过或不跳过反垃圾邮件扫描。例如，您可能选择检疫从某些发送方的垃圾邮件和从其他发送方的删除垃圾邮件。

跳过的反垃圾邮件扫描第三个选项在消息过滤器。(请注意内容过滤器不可能用于此，因为内容过滤器发生，在反垃圾邮件扫描已经发生)后。其中一在消息过滤器的操作是“跳过spamcheck”。下面消息过滤器将跳过检查有一个特定IP地址或来自一个特定的域名的发送方的反垃圾邮件：

```
SkipSpamcheckFilter
```

```
((IP == '192.168.195.101')
     (== ‘@example \ \ .com$’))
{
    spamcheck();
}
```