如何将ESA配置为跳过对受信任发件人的反垃圾邮件和/或防病毒扫描？

目录

[问题](#)
[答案](#)
[相关信息](#)

问题

如何将ESA配置为跳过对受信任发件人的反垃圾邮件和/或防病毒扫描？

答案

AsyncOS提供三种主要工具，可用于跳过对最受信任的发件人进行反垃圾邮件或防病毒检查。请注意，ESA不建议随时跳过防病毒检查，即使对您最信任的发件人也是如此，因为可能会无意中感染病毒。以下是有关如何跳过针对邮件流部分的反垃圾邮件检查的三种方法的讨论。

第一个可用工具是主机访问表(HAT)邮件流策略。使用邮件流策略，可以按IP地址（使用数字IP地址或PTR DNS名称）、SenderBase分数或本地DNS允许列表或阻止列表识别发件人。在HAT中将发件人标识为发件人组内的受信任发件人后，可以将该发件人组标记为跳过反垃圾邮件扫描。

例如，假设您想要确定某个特定的业务合作伙伴EXAMPLE.COM，该合作伙伴的邮件不应进行反垃圾邮件检查。您必须找到SCU.COM的邮件服务器IP地址（或DNS指针记录）。 在本例中，我们假设EXAMPLE.COM的邮件服务器具有IP地址，其DNS PTR记录为“smtp1.mail.scu.com”，通过“smtp4.mail.scu.com”。 请记住，在本例中，我们查看的是邮件服务器的PTR记录（有时称为反向DNS）；这与SCU.COM的人员用于外发邮件的域名无关。

您可以使用Mail Policies>Overview>Add Sender Group创建新的发件人组（或使用现有发件人组，如ALLOWLIST）。我们创建一个名为“NotSpammers”的邮件。 提交此页后，您将返回到Mail Policies>Overview屏幕，在该屏幕中，您将有机会为此发件人组添加新策略。如果点击“添加策略”(Add Policy)，您将有机会创建新策略。在这种情况下，我们只希望覆盖一个区域中的默认策略：垃圾邮件检测。为策略指定名称并将连接行为设置为“接受”，然后向下滚动到“垃圾邮件检测”部分，并将此策略设置为跳过垃圾邮件检查。提交新策略，不要忘记“提交更改”。

另一种方法是使用传入邮件策略跳过反垃圾邮件扫描。HAT和传入邮件策略的区别在于HAT完全基于发件人的IP信息：真实IP地址、反映在DNS中的IP地址、SenderBase得分（基于IP地址）或基于IP地址的DNS允许列表或阻止列表条目。传入邮件策略基于邮件信封信息：邮件来自谁或来自谁。这意味着他们很容易被冒充邮件发件人的人欺骗。但是，如果您只想跳过所有反垃圾邮件检查，以检查来自具有“@example.com”结尾的电子邮件地址的人的传入邮件，您也可以这样做。

要创建此类策略，请转到**Mail Policies > Incoming Mail Policies > Add Policy**。这将允许您添加定义一组发件人（或收件人）的策略。 定义传入邮件策略后，该策略将显示在概述屏幕（邮件策略>传入邮件策略）中。 然后，您可以点击“反垃圾邮件”列，并编辑此特定用户的反垃圾邮件的特定设置。

特定策略的反垃圾邮件设置有许多选项，但在这种情况下，我们只是想跳过反垃圾邮件检查。请注

意，基于HAT的策略和传入邮件策略之间的另一个区别：HAT只能让您跳过或不跳过反垃圾邮件扫描，而传入邮件策略的控制要大得多。例如，您可以选择隔离来自某些发件人的垃圾邮件，并删除来自其他发件人的垃圾邮件。

跳过反垃圾邮件扫描的第三个选项是配置和使用邮件过滤器。

> **注意：**无法将内容过滤器用于此，因为内容过滤器在反垃圾邮件扫描已进行后发生

邮件过滤器中的一个操作是“skip-spamcheck”。 以下邮件过滤器将跳过对具有特定IP地址或来自特定域名的发件人的反垃圾邮件检查：

```
SkipSpamcheckFilter:
   if ( (remote-ip == '192.168.195.101') or
        (mail-from == '@example\\.com$')      )
   {
       skip-spamcheck();
   }
```

有关如何使用邮件过滤器的详细信息，请查看已部署的AsyncOS版本的用户指南。

相关信息

- 技术支持和文档 - Cisco Systems