如何配置ESA以跳過對受信任的發件人的反垃圾郵件和/或防病毒掃描？

目錄

問題

如何配置ESA以跳過對受信任的發件人的反垃圾郵件和/或防病毒掃描？

答案

AsyncOS提供三種主要工具，您可以使用這些工具來跳過對最受信任的發件人的反垃圾郵件或防病毒檢查。請注意，ESA不建議隨時跳過防病毒檢查，即使對您最信任的發件人也是如此，因為可能會在無意中感染病毒。下面討論三種方法，您可以針對郵件流的某些子集跳過反垃圾郵件檢查。

第一個可用的工具是主機訪問表(HAT)郵件流策略。使用郵件流策略，您可以通過IP地址（使用數字IP地址或PTR DNS名稱）、SenderBase得分或本地DNS允許清單或阻止清單來識別發件人。在HAT中的發件人組中識別出受信任的發件人後，即可將該發件人組標籤為跳過反垃圾郵件掃描。

例如，假設您要確定一個特定的業務合作夥伴EXAMPLE.COM，該合作夥伴不應對其郵件進行反垃圾郵件檢查。您必須查詢SCU.COM的郵件伺服器IP地址（或DNS指標記錄）。 在本例中，我們假設EXAMPLE.COM具有郵件伺服器，這些郵件伺服器的IP地址的DNS PTR記錄為「smtp1.mail.scu.com」至「smtp4.mail.scu.com」。 請記住，在此案例中，我們正在檢視郵件伺服器的PTR記錄（有時稱為反向DNS）；這與SCU.COM上的使用者用於傳出郵件的域名無關。

您可以使用Mail Policies>Overview>Add Sender Group建立新的發件人組（或使用現有的發件人組，如ALLOWLIST）。讓我們建立一個名為「非垃圾郵件傳送者」的郵件。 提交此頁面後，您將返回到「郵件策略>概述」螢幕，您可以在此為該發件人組新增新策略。如果按一下「新增策略」，您將有機會建立新策略。在這種情況下，我們只希望在一個區域中覆蓋預設策略：垃圾郵件檢測。為該策略指定一個名稱，並將連線行為設定為「接受」，然後向下滾動到「垃圾郵件檢測」部分，並將此策略設定為跳過垃圾郵件檢查。提交新策略，並且不要忘記「提交更改」。

另一種方法是使用傳入郵件策略來跳過反垃圾郵件掃描。HAT和傳入郵件策略之間的區別在於HAT完全基於發件人的IP資訊：真實IP地址、反映在DNS中的IP地址、SenderBase得分（基於IP地址）或基於IP地址的DNS允許清單或阻止清單條目。傳入郵件策略基於郵件信封資訊：郵件發件人或發件人。這意味著他們很容易被假冒郵件發件人的人員所愚弄。但是，如果您只想跳過對來自電子郵件地址以「@example.com」結尾的人員的傳入郵件的所有反垃圾郵件檢查，也可以這樣做。

要建立此類策略，請轉到**郵件策略>傳入郵件策略>新增策略**。這將允許您新增定義一組發件人（或收件人）的策略。 定義傳入郵件策略後，該策略將顯示在概述螢幕（郵件策略>傳入郵件策略）中。 然後，您可以按一下「反垃圾郵件」列並編輯此特定使用者的反垃圾郵件特定設定。

特定策略的反垃圾郵件設定有很多選項，但在本例中，我們只是想跳過反垃圾郵件檢查。請注意基於HAT的策略和傳入郵件策略之間的另一個區別：hat只能讓您跳過或不跳過反垃圾郵件掃描，而「

傳入郵件策略」具有更大的控制能力。例如，您可以選擇隔離來自某些發件人的垃圾郵件，並刪除來自其他發件人的垃圾郵件。

跳過反垃圾郵件掃描的第三個選項是配置和使用郵件過濾器。

附註：內容篩選器無法用於此功能，因為內容篩選器是在進行反垃圾郵件掃描之後發生的

郵件過濾器中的一個操作是「skip-spamcheck」。 以下郵件過濾器將跳過對具有特定IP地址或來自特定域名的發件人的反垃圾郵件檢查：

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

有關如何使用郵件過濾器的詳細資訊，請檢視使用手冊，瞭解所部署的AsyncOS版本。

相關資訊

- 技術支援與文件 - Cisco Systems