防止欺骗的ESA SMTP身份验证条件

目录

[简介](#)
[先决条件](#)
[背景信息](#)
[创建过滤器](#)
[示例规则](#)
[相关信息](#)

简介

本文档介绍如何根据经过简单邮件传输协议(SMTP)身份验证的用户创建过滤器并将用户名记录到X报头中。

先决条件

思科建议您了解AsyncOS 6.5版及更高版本。

背景信息

SMTP身份验证功能允许客户对其客户端使用SMTP身份验证，以便连接到邮件安全设备(ESA)并从其发送邮件。 由于此功能允许经过身份验证的用户进行中继，因此用户可以在通过思科ESA发送的电子邮件中伪造“发件人：”字段。为防止用户伪造，ESA AsyncOS 6.5版及更高版本现在包含允许与经过身份验证的SMTP用户用户名和邮件发件人电子邮件地址进行比较的邮**件过**滤条件。

创建过滤器

邮件过滤器条件允许管理员编写类似于下一节示例规则的过滤器，该示例规则比较通过SMTP身份验证会话出站中继的邮件。如果SMTP凭据受损，发送电子邮件的计算机通常会生成多个地址，用作邮件发**件人：**标题。邮件过滤条件仅允许在用户名和邮件发件人为以下状态时离开**邮件：**信头匹配。否则，该邮件将被视为伪造邮件**“发件人**：”，并激活邮件过滤器操作。邮件过滤器操作可以是任何最终操作；示例规则显示隔离操作。过滤器条件具有以下语法：

```
smtp-auth-id-matches("<target>" [, "<sieve-char>"])
```

过滤器允许与以下目标之一进行比较：

- **信封发件人：**比较在“发件人：”中**指定的地址**的子网页。

- **发件人地址：**比较从“发件人：”(From:)**解析的地址**标题。因为允许在“发件人：”中**使用多个地址**报头，只有一个必须匹配。
- **发件人：**比较发件人中指定的**地址：**标题。
- **Any:**匹配在经过身份验证的SMTP会话期间创建的邮件（无论身份如何）。
- **无:**匹配在经过身份验证的SMTP会话期间未创建的邮件(例如，当首选SMTP身份验**证时**)。

SMTP身份验证ID	筛炭	比较地址	匹配？
某用户		otheruser@example.com	无
某用户		someuser@example.com	Yes
某用户		someuser@face.localhost	Yes
部分用户		someuser@example.com	Yes
某用户		someuser+folder@example.com	无
某用户	+	someuser+folder@example.com	Yes
someUser@example.com		someuser@forged.com	无
someUser@example.com		someuser@example.com	Yes
someUser@example.com		someuser@example.com	Yes

创建此变量替**代$SMTPAuthID**，以允许在用于中继的原始身份验证凭据的报头中包含。

示例规则

```
Msg_Authentication: if (smtp-auth-id-matches("*Any"))
{
   # Always include the original authentication credentials in a
   # special header.
   insert-header("X-SMTPAUTH", "$SMTPAuthID");

   if (smtp-auth-id-matches("*FromAddress", "+") and
       smtp-auth-id-matches("*EnvelopeFrom", "+"))
   {
       # Username matches.  Verify the domain
       if (header('from') != "(?i)@(?:example\.com|example\.com)" or mail-from !=
"(?i)@(?:example\.com|\.com)"
       {
           # User has specified a domain which cannot be authenticated
           quarantine("forged");
       }
   } else {
       # User claims to be an completely different user
       quarantine("forged");
   }
}
```

注意：此过滤器假设您有一个称为“伪造**的隔离**区。

相关信息

- IronPort AsyncOS Advanced User Guide for IronPort邮件安全设备
- 技术支持和文档 - Cisco Systems