ESA SMTP防止的验证情况伪装

目录

简介

本文描述如何创建根据简单邮件传输协议(SMTP)已认证的用户的过滤器和记录用户名到X报头。

先决条件

Cisco建议您有AsyncOS版本6.5和以上知识。

背景信息

SMTP验证功能允许客户使用SMTP验证他们的客户端为了连接对和发送从电子邮件安全工具(ESAs)的邮件。因为功能允许已认证的用户中继，伪造“从用户是可能的：”他们通过思科ESA发送的电子邮件的字段。为了防止用户锻件， ESA AsyncOS版本6.5和以上当前包含允许比较已验证SMTP用户名和**从**电子邮件地址的**邮件的**消息过滤器情况。

创建过滤器

消息过滤器情况允许管理员写入过滤器类似于比较电子邮件中继的出站通过SMTP验证会话在下一部分的示例规则。如果SMTP凭证折衷，发送电子邮件的计算机通常生成作为邮件将使用的几个地址**从**：报头。消息过滤器情况只允许电子邮件离开，如果用户名和邮件**从**：报头匹配。否则，电子邮件认为伪造的邮件**从**：和消息过滤器操作激活。消息过滤器操作可以是所有最后的行动;示例规则显示检疫操作。过滤器情况有此语法：

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

过滤器允许比较这些目标之一：

- **EnvelopeFrom** ：比较**邮件**指定的地址**从**：在SMTP会话。
- **FromAddress** ：比较地址解析在外面**从**：报头。因为多个地址在允许**从**：报头，仅一个必须配

比。

- **发送方**：比较在**发送方**指定的地址：报头。
- **其中任一**：匹配创建在一已验证SMTP会话期间的消息(不管标识)。
- **无**：匹配例如未创建在一已验证SMTP会话期间的消息(，当SMTP验证**被偏好**)时。

SMTP验证ID	筛子字符	比较地址	匹配？
someuser		otheruser@example.com	无
someuser		someuser@example.com	是
someuser		someuser@face.localhost	是
SomeUser		someuser@example.com	是
someuser		someuser+folder@example.com	无
someuser	+	someuser+folder@example.com	是
someUser@example.com		someuser@forged.com	无
someUser@example.com		someuser@example.com	是
someUser@example.com		someuser@example.com	是

此可变替换法，**$SMTPAuthID**，创建为了允许在用于的原始认证证书的报头的包括中继。

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");
   }
}
```

Note:此过滤器假设您安排一检疫呼叫**被伪造**。

相关信息

- IronPort AsyncOS IronPort电子邮件的安全工具高级用户指南
- 技术支持和文档 - Cisco Systems