配置ESA SMTP身份验证匹配以防止地址欺骗

目录

简介

本文档介绍如何创建邮件过滤器，将SMTP身份验证的用户名与信头From:地址 .

先决条件

思科建议您了解适用于邮件版本15.0及更高版本的Cisco AsyncOS。

背景信息

SMTP身份验证功能允许客户对其邮件客户端使用SMTP身份验证，以通过思科邮件安全设备(ESA)连接和发送邮件。 由于此功能允许经过身份验证的会话中继出站邮件，因此客户端可以假冒信头From:地址 .为帮助防止欺骗，Cisco AsyncOS for Email 6.5版及更高版本包含邮件过滤条件，将经过身份验证的SMTP用户名与信头From:地址并将用户名记录在X报头中。

创建过滤器

邮件过滤器条件允许管理员编写过滤器（例如，下一节中的规则），比较在SMTP身份验证会话期间出站中继的邮件。如果SMTP凭证受损，发送客户端通常会生成多个信头From:地址。此条件允许仅在经过身份验证的用户名与信头From:地址 ;否则，该邮件将被视为伪装信头From:并应用配置的邮件过滤器操作。邮件过滤器操作可以是任何最终操作；示例规则使用隔离操作。过滤条件的语法如下：

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

可选的sieve-char参数指定用于忽略比较地址中该字符之后的部分的分隔符字符（例如+）。如表所示，这通常用于加编址。

过滤器允许与以下目标之一进行比较：

- 信封发件人：比较Mail From:在SMTP会话中。
- 发件人地址：比较从From解析的地址：报头。由于From:报头，只能匹配一个。
- 发件人：比较发件人中指定的地址：报头。
- 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	筛过炭	比较地址	匹配？
某些用户		otheruser@example.com	无
某些用户		someuser@example.com	Yes
某些用户		someuser@face.localhost	Yes
SomeUser		someuser@example.com	Yes
某些用户		someuser+folder@example.com	无
某些用户	+	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

此变量替换$SMTPAuthID允许将经过身份验证的用户名包括在经过身份验证的SMTP会话期间中继的消息的消息标头中。

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" or mail-from != "(?i)@example\.com")
        {
            # User has specified a domain which cannot be authenticated.
            quarantine("forged");
        }
    }
    else
    {
        # User claims to be a completely different user.
        quarantine("forged");
    }
}
```

注意：此过滤器假定存在名为forged的隔离区。

相关信息

- 思科邮件安全设备的Cisco AsyncOS高级用户指南
- 技术支持和文档

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。