防止欺騙的ESA SMTP身份驗證條件

目錄

簡介

本文說明如何根據通過簡單郵件傳輸協定(SMTP)身份驗證的使用者建立過濾器，並將使用者名稱記錄到X報頭中。

必要條件

思科建議您瞭解AsyncOS版本6.5及更高版本。

背景資訊

SMTP身份驗證功能允許客戶對其客戶端使用SMTP身份驗證，以便連線到郵件安全裝置(ESA)並從其傳送郵件。 由於該功能允許經過身份驗證的使用者中繼，因此使用者可以偽造通過思科ESA傳送的電子郵件中的「From：」欄位。為了防止使用者偽造，ESA AsyncOS版本6.5及更高版本現在包含允許與經過身份驗證的SMTP使用者使用者名稱和郵件發件人電子郵件地址進行比較的消息過濾條件。

建立篩選器

郵件過濾器條件允許管理員編寫類似於下一部分中的示例規則的過濾器，該示例規則比較通過SMTP身份驗證會話中繼出站的電郵。如果SMTP憑證受到危害，則傳送電子郵件的電腦通常會生成多個地址用作郵件**源：**標題。郵件篩選條件僅允許使用者名稱和郵件發件人(**From:**標頭匹配。否則，該電子郵件被視為偽造的**郵件發件人**:，郵件過濾器操作將啟用。郵件過濾器動作可以是任何最終動作；示例規則顯示隔離操作。篩選條件的語法如下：

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

過濾器允許與以下目標之一進行比較：

- **信封發件人**：比較**Mail From**：中指定的**地址**：在SMTP會話中。
- **發件人地址**：比較從From解析的**地址**：標題。由於**From**:標頭，只能匹配一個。
- **發件人**：比較發件人中指定的地**址**：標題。
- **任何**：匹配在經過身份驗證的SMTP會話期間建立的郵件（無論其身份如何）。
- **無**:匹配在經過身份驗證的SMTP會話期間未建立的郵件(例如，當首選SMTP身份驗證時)。

SMTP身份驗證ID	篩焦	比較地址	配對？
某些使用者		otheruser@example.com	否
某些使用者		someuser@example.com	是
某些使用者		someuser@face.localhost	是
SomeUser		someuser@example.com	是
某些使用者		someuser+folder@example.com	否
某些使用者	+	someuser+folder@example.com	是
someUser@example.com		someuser@forged.com	否
someUser@example.com		someuser@example.com	是
someUser@example.com		someuser@example.com	是

建立此變數替代**$SMTPAuthID**的目的是允許在用於中繼的原始身份驗證憑據的標頭中包含該變數。

示例規則

```
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");
   }
}
```

附註：此過濾器假定您有一個名為**forged**的隔離。

相關資訊

- 適用於IronPort郵件安全裝置的IronPort AsyncOS高級使用手冊
- 技術支援與文件 - Cisco Systems