スプーフィングを防止する ESA SMTP 認証の条件

内容

概要

このドキュメントでは、シンプルメール転送プロトコル(SMTP)認証ユーザに基づいてフィルタを作成し、ユーザ名をXヘッダーに記録する方法について説明します。

前提条件

AsyncOSバージョン6.5以降に関する知識があることが推奨されます。

背景説明

SMTP認証機能を使用すると、Eメールセキュリティアプライアンス(ESA)に接続してメールを送信するために、クライアントにSMTP認証を使用できます。 この機能により、認証されたユーザはリレーできるので、ユーザはCisco ESAを介して送信する電子メールの「From:」フィールドを偽造できます。ユーザの偽造を防ぐために、ESA AsyncOSバージョン6.5以降には、認証済みのSMTPユーザ名およびメールのFrom電子メールアドレスとの比較を許可するメッセージフィルタ条件が含まれます。

フィルタの作成

メッセージフィルタ条件を使用すると、管理者は、SMTP認証セッションを介して送信される電子メールを比較する次のセクションのルール例のようなフィルタを作成できます。SMTPクレデンシャルが侵害された場合、電子メールを送信するマシンは通常、メールの送信元として使用する複数のアドレスを生成します。ヘッダーが含まれています。メッセージフィルタ条件では、ユーザ名とメールがFrom:ヘッダーが一致します。それ以外の場合、電子メールは偽造メール From：と見なされ、メッセージフィルタのアクションがアクティブになります。メッセージフィルタアクションは、任意の最終アクションにすることができます。このルールの例は、検疫アクションを示しています。フィルタ条件の構文は次のとおりです。

```
smtp-auth-id-matches("<target>" [, "<sieve-char>"])
```
このフィルタでは、次のいずれかのターゲットとの比較が可能です。

- **エンベロープ送信者**：[Mail From:]で指定されたアドレ**スを比較します。**設定します
- **FromAddress:**From:ヘッダーが含まれています。From:ヘッダーに一致する必要があるのは1つだけです。
- **送信者:**送信者で指定されたアドレスを比較**します。**ヘッダーが含まれています。
- **すべて:**認証されたSMTPセッション中に作成されたメッセージに一致します（IDに関係なく）。
- **[なし（None）]**： 認証されたSMTPセッション中に作成されなかったメッセージに一致します(たとえば、SMTP認証が優先される**場合**)。

SMTP AUTH ID	シーブチャー	比較アドレス	MATCHES?
誰か		otheruser@example.com	No
誰か		someuser@example.com	Yes
誰か		someuser@face.localhost	Yes
SomeUser		someuser@example.com	Yes
誰か		someuser+folder@example.com	No
誰か	+	someuser+folder@example.com	Yes
someUser@example.com		someuser@forged.com	No
someUser@example.com		someuser@example.com	Yes
someUser@example.com		someuser@example.com	Yes

この変数の置換**$SMTPAuthID**は、リレーに使用される元の認証資格情報のヘッダーに含めることができるように作成されました。

ルールの例

```
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：このフィルタは、**forged**という隔離があることを前提**としています。**

関連情報

- IronPort AsyncOS Advanced User Guide for IronPort Email Security Appliances
- テクニカル サポートとドキュメント – Cisco Systems