スプーフィングを防止する ESA SMTP 認証の条件

目次

概要

この資料に Simple Mail Transfer Protocol (SMTP) 認証済みユーザに基づいてフィルタを作成し X ヘッダにユーザ名を記録する方法を記述されています。

前提条件

Cisco は AsyncOS バージョン 6.5 および それ 以降の知識があることを推奨します。

背景説明

SMTP 認証 機能はに接続するために顧客がクライアントのために SMTP 認証および E メール セキュリティ アプライアンス (ESA) からのメール送信を使用することを可能にします。 機能は認証済みユーザが中継で送ることを可能にするのでユーザが「からの造ることは可能性のあるです: 」彼らが Cisco ESA を通して送信 する メールのフィールド。 ユーザを鍛造材から防ぐために、ESA AsyncOS バージョン 6.5 および それ 以降は今 e メールアドレス**からの**認証された SMTP ユーザ ユーザ名および**メール**に対して比較を可能にするメッセージ フィルタ状態が含まれています。

フィルタの作成

メッセージ フィルター状態は管理者がルール例と同じような SMTP 認証セッションによって中継で送られた送信であるメールを比較する次の セクションにフィルタを書くことを可能にします。 SMTP 信任状が妥協される場合、メールを送信 する マシンは通常メールとして**からの**使用されるべき複数のアドレスを生成します: メッセージフィルタを次に示します。 メッセージ フィルター状態はユーザ名およびメール**からのだけ**メールが去るようにします: ヘッダー致。 さもなければ、メールは造られたメールと**からの**みなされます: およびメッセージ フィルター操作アクティブ化。 メッセージ フィルター操作はどの最終措置である場合もあります; ルール例は検疫操作

を示します。 フィルター条件にこの構文があります:

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

フィルタ割り当てこれらのターゲットの 1 つに対する比較:

- **EnvelopeFrom: メール**で**からの**規定 されるアドレスを比較します: SMTP メッセージ交換。
- **FromAddress:** から**からの**解析されるアドレスを比較します: メッセージフィルタを次に示します。 複数のアドレスがで**からの**許可されるので: ヘッダは、1 だけ一致する必要があります。
- **送信側: 送信側**で規定 されるアドレスを比較します: メッセージフィルタを次に示します。
- **:** 認証された SMTP セッションの間に作成されたメッセージと一致します (識別に関係なく)。
- **None**： SMTP 認証が**優先される**とき) 認証された SMTP セッションの間に作成されなかったメッセージと一致します (たとえば。

SMTP AUTH ID	ふるい文字	比較アドレス	一致か。
someuser		otheruser@example.com	なし
someuser		someuser@example.com	○
someuser		someuser@face.localhost	○
SomeUser		someuser@example.com	○
someuser		someuser+folder@example.com	なし
someuser	+	someuser+folder@example.com	○
someUser@example.com		someuser@forged.com	なし
someUser@example.com		someuser@example.com	○
someUser@example.com		someuser@example.com	○

この可変代替は、**$SMTPAuthID**、中継で送るのに使用されたオリジナル認証クレデンシャルのヘッダの包含を可能にするために作成されました。

ルール例

```
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: このフィルタは呼出される検疫を**造って**もらうことを仮定します。

関連情報

- IronPort E メール セキュリティ アプライアンスのための IronPort AsyncOS アドバンスド ユーザー ユーザーズ ガイド
- テクニカル サポートとドキュメント – Cisco Systems