Condition d'authentification SMTP ESA pour empêcher l'usurpation

Contenu

Introduction

Ce document explique comment créer un filtre basé sur l'utilisateur authentifié SMTP (Simple Mail Transfer Protocol) et enregistrer le nom d'utilisateur dans un en-tête X.

Conditions préalables

Cisco vous recommande de connaître AsyncOS version 6.5 et ultérieure.

Informations générales

La fonction d'authentification SMTP permet aux clients d'utiliser l'authentification SMTP pour leurs clients afin de se connecter aux appliances de sécurité de la messagerie et d'envoyer des messages à partir de ces appliances. Puisque la fonctionnalité permet à l'utilisateur authentifié de relayer, il est possible pour les utilisateurs de créer le champ « De : » dans les e-mails qu'ils envoient via le Cisco ESA. Afin d'empêcher les utilisateurs de falsifier, ESA AsyncOS version 6.5 et ultérieure contient désormais une condition de filtre de messages qui permet des comparaisons avec le nom d'utilisateur SMTP authentifié et l'adresse e-mail **de** courrier **de** départ.

Créer un filtre

La condition de filtre de message permet à un administrateur d'écrire un filtre similaire à la règle d'exemple de la section suivante qui compare les e-mails qui sont relayés en sortie via une session d'authentification SMTP. Si les informations d'identification SMTP sont compromises, la machine qui envoie les e-mails génère généralement plusieurs adresses à utiliser comme courrier **De :** Header (En-tête) . La condition de filtre de message permet uniquement aux e-mails de quitter si le nom d'utilisateur et le message **De :** les en-têtes correspondent. Sinon, l'e-mail est considéré comme un courrier falsifié **De :** et l'action de filtre de message est activée. L'action de

filtre de message peut être n'importe quelle action finale ; la règle d'exemple montre une action de quarantaine. La condition de filtre a la syntaxe suivante :

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

Le filtre permet une comparaison avec l'une de ces cibles :

- **EnveloppeDe :** Compare l'adresse spécifiée dans **Mail From :** dans la conversation SMTP.
- **FromAddress :** Compare les adresses analysées à partir de **From :** Header (En-tête) . Étant donné que plusieurs adresses sont autorisées dans le **champ De :** , seul un doit correspondre.
- **Expéditeur :** Compare l'adresse spécifiée dans l'**expéditeur :** Header (En-tête) .
- **Tous les modèles:** Correspond aux messages créés au cours d'une session SMTP authentifiée (quelle que soit l'identité).
- **Aucune:** Correspond aux messages qui n'ont pas été créés lors d'une session SMTP authentifiée (par exemple, lorsque l'authentification SMTP est **préférée**).

ID AUTH SMTP	CHAR DE SIÈGE	ADRESSE DE COMPARAISON	CORRESPONDANCES ?
someuser		otheruser@example.com	Non
someuser		someuser@example.com	Oui
someuser		someuser@face.localhost	Oui
CertainsUtilisateurs		someuser@example.com	Oui
someuser		someuser+folder@example.com	Non
someuser	+	someuser+folder@example.com	Oui
someUser@example.com		someuser@forged.com	Non
someUser@example.com		someuser@example.com	Oui
someUser@example.com		someuser@example.com	Oui

Cette substitution de variable, **$SMTPAuthID**, a été créée afin de permettre l'inclusion dans les en-têtes des informations d'identification d'authentification d'origine utilisées pour le relais.

Exemple de règle

```
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: Ce filtre suppose que vous avez une quarantaine appelée **forgée**.

Informations connexes

- Guide de l'utilisateur avancé IronPort AsyncOS pour les appareils de sécurité de la messagerie IronPort
- Support et documentation techniques - Cisco Systems