État d'authentification de SMTP ESA pour empêcher charrier

Contenu

Introduction

Ce document décrit comment créer un filtre basé sur l'utilisateur authentifié par Protocole SMTP (Simple Mail Transfer Protocol) et se connecter le nom d'utilisateur dans une X-en-tête.

Conditions préalables

Cisco recommande que vous ayez la connaissance de la version 6.5 et ultérieures d'AsyncOS.

Informations générales

La fonction d'authentification de SMTP permet à des clients pour employer l'authentification de SMTP pour leurs clients afin de se connecter à et envoyer la messagerie des appliances de sécurité du courrier électronique (ESAs). Puisque la caractéristique permet à l'utilisateur authentifié pour transmettre par relais, il est possible que les utilisateurs modifient « de : » mettez en place dans les emails qu'ils envoient par Cisco ESA. Afin d'empêcher des utilisateurs de la pièce forgéee, la version 6.5 et ultérieures ESA AsyncOS contiennent maintenant un état de filtre de message qui permet des comparaisons contre l'username authentifié d'utilisateur de SMTP et la **messagerie de l'**email address.

Créez un filtre

L'état de filtre de message permet à un administrateur pour écrire un filtre semblable à l'exemple de règle dans la section suivante qui compare les emails qui sont sortants transmis par relais par l'intermédiaire d'une session d'authentification de SMTP. Si les qualifications de SMTP sont compromises, l'ordinateur qui envoie les emails génère habituellement plusieurs adresses à utiliser comme messagerie **de :** en-tête. L'état de filtre de message permet seulement à des emails pour partir si le nom d'utilisateur et la messagerie **de :** correspondance d'en-têtes.

Autrement, l'email est considéré une messagerie modifiée **de :** , et l'action de filtre de message lance. L'action de filtre de message peut être n'importe quelle mesure finale ; l'exemple de règle affiche une action de quarantaine. L'état de filtre a cette syntaxe :

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

Le filtre permet une comparaison contre une de ces cibles :

- **EnvelopeFrom :** Compare l'adresse spécifiée dans la **messagerie de :** dans la conversation de SMTP.
- **FromAddress :** Compare des adresses analysées hors du **de :** en-tête. Puisqu'on permet des plusieurs adresses dans **de :** l'en-tête, seulement une doit s'assortir.
- **Expéditeur :** Compare l'adresse spécifiée dans l'**expéditeur :** en-tête.
- **Quels :** Apparie les messages qui ont été créés pendant une session authentifiée de SMTP (indépendamment de l'identité).
- **Aucun :** Apparie les messages qui n'ont pas été créés pendant une session authentifiée de SMTP (par exemple, quand l'authentification de SMTP **est préférée**).

ID AUTHENTIQUE DE SMTP	CAR DE TAMIS	ADRESSE DE COMPARAISON	CORRESPONDANCES
someuser		otheruser@example.com	Non
someuser		someuser@example.com	Oui
someuser		someuser@face.localhost	Oui
SomeUser		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 variable, **$SMTPAuthID**, a été créée afin de permettre l'intégration dans les en-têtes des qualifications d'origine d'authentification utilisées pour transmettre par 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 faites **modifier une** quarantaine appelée.

Informations connexes

- Guide d'utilisateur avancé d'IronPort AsyncOS pour des appliances de sécurité du courrier électronique d'IronPort
- Support et documentation techniques - Cisco Systems