Configurer la correspondance d'authentification SMTP ESA pour empêcher l'usurpation d'adresse

Table des matières

Introduction

Ce document décrit comment créer un filtre de message qui compare le nom d'utilisateur authentifié SMTP à l'en-tête From : adresse.

Conditions préalables

Cisco vous recommande de connaître Cisco AsyncOS pour la version 15.0 et ultérieure de la messagerie électronique.

Informations générales

La fonction d'authentification SMTP permet aux clients d'utiliser l'authentification SMTP pour leurs clients de messagerie afin de se connecter et d'envoyer des e-mails via l'appliance de sécurisation de la messagerie Cisco (ESA). Comme la fonctionnalité permet à une session authentifiée de relayer le courrier sortant, un client peut usurper l'en-tête From : adresse. Pour empêcher l'usurpation, Cisco AsyncOS for Email version 6.5 et ultérieures inclut une condition de filtre de message qui compare le nom d'utilisateur SMTP authentifié à l'en-tête From : et enregistre le nom d'utilisateur dans un en-tête X.

Créer un filtre

La condition de filtre de message permet à un administrateur d'écrire un filtre (par exemple, la règle de la section suivante) qui compare les messages relayés en sortie au cours d'une session authentifiée SMTP. Si les informations d'identification SMTP sont compromises, le client émetteur génère souvent plusieurs en-têtes From : adresses IP. Cette condition permet aux messages d'être remis uniquement lorsque le nom d'utilisateur authentifié correspond à l'en-tête De : adresse ; sinon, le message est traité comme un en-tête usurpé De : et l'action de filtrage des messages

configurée est appliquée. L'action de filtrage du message peut être n'importe quelle action finale ; la règle exemple utilise une action de quarantaine. La condition de filtre a la syntaxe suivante :

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

Le paramètre facultatif sieve-char spécifie un caractère de séparation (par exemple, +) utilisé pour ignorer la partie de l'adresse de comparaison après ce caractère. Il est généralement utilisé pour l'adressage en plus, comme indiqué dans le tableau.

Le filtre permet une comparaison avec l'une des cibles suivantes :

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

ID AUTH SMTP	CAROTTE TAMISÉE	ADRESSE DE COMPARAISON	DES ALLUMETTES ?
utilisateur occasionnel		otheruser@example.com	Non
utilisateur occasionnel		someuser@example.com	Oui
utilisateur occasionnel		someuser@face.localhost	Oui
CertainsUtilisateurs		someuser@example.com	Oui
utilisateur occasionnel		someuser+folder@example.com	Non
utilisateur occasionnel	+	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, permet l'inclusion du nom d'utilisateur authentifié dans les en-têtes de message pour les messages relayés au cours d'une session SMTP authentifiée.

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" or mail-from != "(?i)@example\.com")
        {
            # User has specified a domain which cannot be authenticated.
            quarantine("forged");
        }
    }
    else
    {
        # User claims to be a completely different user.
        quarantine("forged");
    }
}
```

Remarque : Ce filtre suppose qu'une quarantaine nommée forgé existe.

Informations connexes

- Guide de l'utilisateur avancé de Cisco AsyncOS pour les appareils de sécurité de la messagerie Cisco
- Documentation et assistance techniques

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.