Identifiez et permettez les pauvres serveurs de messagerie du score de réputation de SenderBase (SBRS)

Contenu

Introduction

Cet article décrit comment identifier et permettre temporairement des serveurs de messagerie avec le score pauvre de réputation de SenderBase (SBRS) par l'appliance de sécurité du courrier électronique (ESA).

Informations générales

Le filtrage de réputation d'expéditeur est la première couche de protection de Spam, te permettant pour contrôler les messages qui sont livré par la passerelle d'email basée sur la fiabilité de l'expéditeur comme déterminée par SBRS. Les serveurs de mail avec SBRS pauvre peuvent avoir leurs connexions rejetées, ou leurs messages rebondis, basé sur vos préférences.

Problème

Un serveur de messagerie se connecte à l'ESA et est signalé car SBRS pauvres et emails sont dus retardé à une réponse du SMTP 554 reçue par le serveur se connectant.

Réponse de l'échantillon 554 :

```
-----Original Message-----
From: Mail Delivery System [mailto:Mailer-Daemon@example.domain.com]
Sent: 25 April 2013 23:23
To: user@companyx.com
Subject: Mail delivery failed: returning message to sender

This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its
recipients. This is a permanent error. The following address(es) failed:

person@example.domain.com
SMTP error from remote mail server after initial connection:
```

```
host gatekeeper.companyx.com [195.195.195.1]: 554-gatekeeper1.companyx.com
554 Your access to this mail system has been rejected due to the sending
MTA's poor reputation. If you believe that this failure is in error, please
contact the intended recipient via alternate means.
```

Solution

Identifiez le pauvre serveur de messagerie SBRS

Utilisez l'interface de ligne de commande (CLI) car le cheminement du message de l'interface utilisateur graphique (GUI) n'enregistre pas les connexions rejetées par défaut.

> Remarque: Le cheminement des connexions rejetées peut être activé à **GUI > Services de sécurité > message dépistant > enable « manipulation rejetée de connexion »**

Employez le **grep** contre le domaine afin de tirer toutes les données se connectantes relatives contre ce domaine. Pour cette sortie, le domaine d'exemple utilisé est *test.com* :

```
myesa.local> grep "test.com" mail_logs

Info: New ICID 1512 to Management (10.0.0.1) from 198.51.100.1 connecting host reverse DNS
hostname: smtp1. test.com
Info: MID 6531 ICID 1512 From: test@test.com
```

Puis **grep l'**ID de connexion entrante (ICID) pour extraire les informations d'hôte de messagerie. L'ICID se connecte est utilisé afin d'indiquer toutes les informations comme : l'adresse IP d'hôte expéditeur, les DN a vérifié l'adresse Internet (si disponible), apparier de sendergroup et le score associé SBRS :

```
myesa.local> grep "ICID 1512" mail_logs


Tue Mar 10 12:04:29 2015 Info: New SMTP ICID 1512 interface Management (10.0.0.1) address
198.51.100.1 reverse dns host unknown verified smtp1.test.com
Tue Mar 10 12:04:29 2015 Info: ICID 1512 REJECT SG BLACKLIST match sbrs[-10:-3] SBRS -4.0
```

Permettez le pauvre serveur de messagerie SBRS par l'ESA

1. Du GUI, naviguez **pour envoyer par mail des stratégies > l'aperçu de CHAPEAU**.
2. Cliquez sur Add le **groupe d'expéditeur…**
3. Nommez le groupe d'expéditeur avec un nom signicatif.
4. Sélectionnez la commande de sorte qu'elle soit au-dessus du groupe d'expéditeur de LISTE NOIRE.
5. Sélectionnez la stratégie de messagerie, **REÇUE** ou **ÉTRANGLÉE**.
6. Quittez tous autres champs vides.
7. Cliquez sur Submit **et ajoutez les expéditeurs**
8. Ajoutez l'adresse IP ou l'adresse Internet de DN des hôtes affectés comme localisé de la commande de grep.
9. Cliquez sur Submit
10. Passez en revue l'aperçu de CHAPEAU et assurez-vous que le nouveau groupe d'expéditeur est commandé correctement.
11. En conclusion, **validation de** clic pour sauvegarder toutes les modifications de configuration.

Pour l'adresse d'expéditeur, on permet les formats suivants :

- Adresses d'IPv6 telles que 2001:420:80:1::5
- Adresses d'ipv4 telles que 10.1.1.0

- Sous-réseaux d'ipv4 ou d'IPv6 tels que 10.1.1.0/24, 2001:db8::/32
- L'ipv4 ou l'ipv6 addres s'étend comme 10.1.1.10-20, 10.1.1-5, ou 2001:db8::1-2001:db8::10
- Adresses Internet telles qu'example.com
- Adresses Internet partielles telles que .example.com.

Dans l'exemple comme affiché ci-dessus, afin de permettre n'importe quelle autre fin de l'information de serveur de messagerie avec *test.com*, ceci aurait été configuré en tant que :

```
198.51.100.1
smtp1.test.com
.test.com
```

Informations connexes

Au sujet de Cisco SenderBase