L'ESA subit une tempête de rebond (NDR)

Contenu

Introduction

Ce document décrit un problème rencontré lorsque votre appliance de sécurité de la messagerie (ESA) connaît une tempête de rebond et offre une solution au problème.

Informations générales

Une tempête de renvoi est un effet secondaire d'un travail joe ou d'une rétrodiffusion de spam par e-mail.

Joe Job

Une tâche joe est une attaque de spam qui utilise des données d'expéditeur usurpées et vise à ternir la réputation de l'expéditeur apparent et/ou à inciter les destinataires à agir contre l'expéditeur apparent.

Rétrodiffusion

Un antidiffusion est un effet secondaire du courrier indésirable, des virus et des vers dans lesquels les serveurs de messagerie qui reçoivent du courrier indésirable et d'autres messages envoient des messages de renvoi à une partie innocente. Cela se produit car l'expéditeur de l'enveloppe de message d'origine est falsifié afin de contenir l'adresse e-mail de la victime. Comme ces messages n'ont pas été sollicités par les destinataires, sont sensiblement similaires les uns aux autres et sont livrés en grande quantité, ils sont considérés comme des courriers électroniques ou des courriers indésirables non sollicités. En tant que tels, les systèmes qui génèrent la diffusion différée des e-mails peuvent être répertoriés sur différentes listes de blocage des systèmes de noms de domaine (DNSBL) et enfreindre les conditions d'utilisation des fournisseurs de services

Internet.

Problème

Votre ESA subit une tempête de rebond où un déluge de messages sont injectés dans l'ESA. Le nombre de connexions entrantes pique au cours d'une telle attaque. L'appliance peut développer une sauvegarde de file d'attente de travail. Afin de vérifier si l'appliance est soumise à une telle attaque, récupérez les journaux de messagerie de l'adresse **De**. Les rebondissements (rapports de non-remise - NDR) ont une adresse d'enveloppe vide **De**.

```
ironport.com> grep -e "From:" mail_logs
Mon Oct 20 14:40:55 2008 Info: MID 10 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 11 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 12 ICID 19 From: <>
```

Une appliance soumise à une tempête de renvoi aura la majorité des messages avec l'adresse **De** l'enveloppe de '**<>**'.

Solution

Il existe plusieurs options pour gérer une tempête de renvoi.

Vérification du renvoi

Afin de lutter contre ces attaques de renvoi mal dirigées, AsyncOS inclut la vérification de renvoi de Cisco. Lorsqu'elle est activée, cette fonction étiquette l'adresse de l'expéditeur du message pour les messages envoyés via l'ESA. Le destinataire de l'enveloppe pour tout message de renvoi reçu par l'ESA est ensuite vérifié pour vérifier la présence de cette balise. Lorsque des messages de renvoi légitimes sont reçus, la balise qui a été ajoutée à l'adresse de l'expéditeur du message est supprimée et le renvoi est remis au destinataire. Les messages de renvoi qui ne contiennent pas la balise peuvent être traités séparément.

AsyncOS considère les rebondissements comme des courriers avec une adresse **De** courrier nulle (**<>**). Les messages provenant d'adresses telles que mailer-daemon@example.com ou postmaster@example.com ne sont pas considérés comme des rebondissements par le système et ne sont pas soumis à la vérification du renvoi.

Configurer les clés de marquage d'adresse de vérification de renvoi

La liste Clés de marquage d'adresse de vérification de renvoi affiche votre clé actuelle et les clés non purgées que vous avez utilisées dans le passé. Pour ajouter une nouvelle clé, procédez comme suit :

1. Sur le **Stratégies de messagerie > Vérification du renvoi** , cliquez sur **Nouvelle clé**.
2. Entrez une chaîne de texte et cliquez sur **Envoyer**.
3. Validez vos modifications.

Touches de purge

Vous pouvez purger vos anciennes clés de marquage d'adresse si vous sélectionnez une règle à purger dans le menu déroulant et cliquez sur **Purger.**

Configurer les paramètres de vérification du renvoi Cisco

Les paramètres de vérification du renvoi déterminent l'action à entreprendre lorsqu'un renvoi non valide est reçu.

- Choisir **Stratégies de messagerie > Vérification du renvoi**.
- Cliquez sur **Modifier les paramètres**.
- Indiquez si vous voulez rejeter les rebondissements non valides ou ajouter un en-tête personnalisé au message. Si vous souhaitez ajouter un en-tête, saisissez le nom et la valeur de l'en-tête.
- Activez éventuellement les exceptions intelligentes. Ce paramètre permet aux messages entrants et aux messages de renvoi générés par les serveurs de messagerie internes d'être automatiquement exemptés du traitement de vérification de renvoi (même lorsqu'un seul écouteur est utilisé pour les messages entrants et sortants).
- Envoyez et confirmez vos modifications.

Configurer la vérification de renvoi Cisco avec l'interface de ligne de commande

Vous pouvez utiliser les commandes **bvconfig** et **destconfig** dans l'interface de ligne de commande afin de configurer la vérification du renvoi. Ces commandes sont décrites dans le Guide de référence CLI de Cisco AsyncOS.

Vérification du renvoi Cisco et configuration du cluster

La vérification du renvoi fonctionne dans une configuration de cluster tant que les deux appliances Cisco utilisent la même clé de renvoi. Lorsque vous utilisez la même clé, l'un ou l'autre système doit pouvoir accepter un retour arrière légitime. La balise/clé d'en-tête modifiée n'est pas spécifique à chaque appliance Cisco.

Filtre courrier

Si vous ne pouvez pas utiliser la vérification de renvoi parce que vous utilisez des appliances distinctes pour la réception et la remise, vous pouvez configurer un filtre de messages afin de bloquer les messages dont l'adresse **De** courrier est vide.

Bloc de messagerie

Puisque ces messages de renvoi auront probablement une adresse de destinataire d'enveloppe inexistante, vous pouvez bloquer des adresses non valides via la validation de destinataire LDAP (Lightweight Directory Access Protocol) de conversation afin de réduire l'impact de ces messages.