

Noms du fichier de log ESA d'exemple de configuration de connexions

Contenu

[Introduction](#)

[Conditions préalables](#)

[Configurez](#)

Introduction

Ce document décrit comment se connecter les noms du fichier des connexions qui traversent l'appliance de sécurité du courrier électronique de Cisco (ESA).

Conditions préalables

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ESA
- Toutes les versions d'AsyncOS

Configurez

Remarque: Dans la version 7.x et ultérieures d'AsyncOS, les connexions sont enregistré automatiquement si vous faites installer au moins un filtre qui vérifie les informations de fichier (nom du fichier, extension, type de fichier, lecture satisfaite). Référez-vous au guide utilisateur ou à l'aide en ligne dans le pour en savoir plus d'AsyncOS.

Cette solution peut être utilisée pour des versions plus tôt d'AsyncOS.

1. Créez une nouvelle en-tête qui contient les noms du fichier de toutes les connexions.
2. Utilisez le **logconfig > les logheaders** pour enregistrer la valeur de cette en-tête au **mail_log**.

Voici un filtre qui enregistre les noms du fichier pour les messages qui ont des connexions :

```
add_filenames_header:
if (attachment-filename == "^.+$.") {
insert-header ("X-fn", "$filenames");
```

L'expression régulière « **^.+\$.** » s'assure qu'il y a une connexion avec au moins un caractère dans

le nom du fichier. C'est faux pour des messages sans des connexions, ainsi seulement des connexions sont enregistré.

Remarque: La définition de la « connexion » à un message électronique est discutable. Typiquement, le premiers texte/brute et pièces text/HTML sont considérés le « corps ». Voyez le guide de l'utilisateur pour plus de détail sur ce qui est considéré une connexion.

Voici un échantillon de ce qu'apparaît il dans dans les mail_logs :

```
Fri Sep 15 13:49:39 2006 Info: Start MID 98 ICID 146
Fri Sep 15 13:49:39 2006 Info: MID 98 ICID 146 From: <joe@example.com>
Fri Sep 15 13:49:39 2006 Info: MID 98 ICID 146 RID 0 To: <carl@example.com>
Fri Sep 15 13:49:39 2006 Info: MID 98 Message-ID '<9151349.VSREACRQ@example.com>'
Fri Sep 15 13:49:39 2006 Info: MID 98 Subject '1:49 pm'
Fri Sep 15 13:49:39 2006 Info: MID 98 ready 20670 bytes from <joe@example.com>
Fri Sep 15 13:49:39 2006 Info: MID 98 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Fri Sep 15 13:49:39 2006 Info: MID 98 antivirus negative
Fri Sep 15 13:49:39 2006 Info: MID 98 queued for delivery
Fri Sep 15 13:49:39 2006 Info: Delivery start DCID 64 MID 98 to RID [0]
Fri Sep 15 13:49:41 2006 Info: Message done DCID 64 MID 98 to RID [0] [('X-fn',
'Encoding.txt')]
Fri Sep 15 13:49:41 2006 Info: MID 98 RID [0] Response '2.0.0 OK 1158353381
r66si9145992pye'
Fri Sep 15 13:49:41 2006 Info: Message finished MID 98 done
```