Descriptions des actions du filtre de messages ESA

Contenu

Introduction

Ce document décrit les différences entre les actions de filtre de messages drop-pièces-by-name, -type, -filetype et -mimetype sur le dispositif de sécurité de la messagerie Cisco (ESA).

Présentation de l'action de filtre de messages

Les messages envoyés à l'aide de MIME peuvent avoir des étiquettes attribuées à différentes parties du corps, souvent appelées pièces jointes. Ces étiquettes peuvent (et peuvent) entrer en conflit dans les informations qu'elles fournissent. En outre, une partie du corps peut avoir ses propres caractéristiques. Par exemple, un utilisateur peut prendre une image JPEG, la joindre à un message électronique, lui donner un type MIME de **texte/html**, et la marquer avec un nom de fichier MIME de **jan.mp3**. Toutes ces étiquettes sont en conflit avec la réalité de l'attachement.

Par exemple, considérez cet en-tête de message :

```
Boundary_(ID_n6BU1raweF+4UwCeweFmVQ)
Content-type: application/msword; name="eval form.doc"
Content-transfer-encoding: BASE64
Content-disposition: attachment; filename="eval form.doc"
Content-description: eval form.doc
```

Dans ce cas, les noms de fichiers MIME et les types MIME sont tous cohérents et peuvent correspondre ou non au format réel de la partie du corps (pièce jointe). Cependant, dans cet en-tête, il y a des incohérences :

```
Boundary_(ID_n6BU1raweF+4UwCeweFmVQ)
Content-type: image/jpeg; name="eval form.doc"
Content-transfer-encoding: BASE64
Content-disposition: attachment; filename="evaluation.zip"
Content-description:  These are the latest warez, d00d.
```

Pour les messages bien formés, la mise en oeuvre de la politique est assez facile. Mais dans le cas d'une personne qui tente, intentionnellement ou non, de contourner la politique, une flexibilité supplémentaire est nécessaire.

Les administrateurs réseau souhaitent souvent supprimer des pièces jointes d'un type particulier, telles que tous les fichiers MP3. Cependant, la mise en oeuvre de cette stratégie signifie que vous devez choisir les étiquettes auxquelles vous voulez prêter attention (le cas échéant). AsyncOS vous donne la flexibilité de regarder le type MIME (tel que *text/html*), le nom de fichier MIME (tel que *jan.mp3*), et d'*empreinte* de *fait* la pièce jointe afin d'essayer de déterminer quel est le format réel. Lors de la mise en oeuvre de votre stratégie à l'aide de filtres de messages ou de filtres de contenu, vous pouvez utiliser une ou plusieurs de ces étiquettes.

Description des actions de filtre de message

Voici les descriptions des actions de filtrage des messages :

- **drop-pièces jointes-by-name** - Vérifie les noms de fichiers de chaque pièce jointe dans un message pour voir si elle correspond à l'expression régulière donnée. Le nom du fichier provient des en-têtes MIME. Cette comparaison est sensible à la casse. Si l'une des pièces jointes du message correspond au nom de fichier, cette règle renvoie **true**. Si une pièce jointe est une archive, l'appareil IronPort série C récupère les noms de fichiers à l'intérieur de l'archive et applique les règles **scanconfig** (par défaut, les types MIME de vidéo/*, audio/* et image/* ne sont pas analysés et rien de plus de 5 Mo n'est analysé) en conséquence.

- **drop-pièces jointes-by-type** - Supprime toutes les pièces jointes des messages ayant un type MIME, déterminé par le type MIME donné ou par l'extension du fichier. Les pièces jointes des fichiers d'archive (zip, tar) seront supprimées si elles contiennent un fichier correspondant.

- **drop-pièces jointes-by-filetype** - Examine les pièces jointes en fonction de l'empreinte digitale du fichier, et pas seulement de l'extension de nom de fichier à trois lettres. Ceci est similaire à la commande de fichier UNIX. Outre les types de fichiers individuels qui peuvent être spécifiés, les expressions de groupe Comprimées, Document, Exécutable, Image et Support incluent tous les types de fichiers du type général. Par exemple, le groupe *exécutable* inclut les fichiers .exe, .java .msi .pif, .dll, .scr et.com. Reportez-vous au Guide de l'utilisateur AsyncOS pour obtenir une liste complète des types de fichiers qui peuvent être spécifiés.

- **drop-pièces jointes-by-mimetype** - Supprime toutes les pièces jointes des messages ayant un type MIME donné. Cette action ne tente pas de déterminer le type MIME par extension de fichier, elle n'examine donc pas non plus le contenu des archives.