Descriptions d'action de filtre de message ESA

Contenu

Introduction

Ce document décrit les différences entre le baisse-connexion-par-nom, de type, - filetype, et - des actions de filtre de message de mimetype sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Aperçu d'action de filtre de message

Les messages qui sont envoyés utilisant le MIME peuvent avoir des étiquettes assignées aux diverses parties du corps, qui s'appellent souvent les connexions. Ces étiquettes mettent en boîte (et faites) le conflit les uns avec les autres dans les informations elles pour fournir. En outre, une partie du corps pourrait avoir ses propres caractéristiques. Par exemple, un utilisateur pourrait prendre une image JPEG, la relier à un message, lui donner un type MIME du **texte/HTML**, et l'identifier par un nom du fichier MIME de **jan.mp3**. Toutes ces étiquettes sont en conflit avec la réalité de ce qu'est la connexion.

Par exemple, considérez cette 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 du fichier et les types MIME sont tous MIME cohérents et pourraient ou ne pourraient pas apparier le format réel de la partie du corps (connexion). Cependant, dans cette 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 stratégie est assez facile. Mais dans le cas de quelqu'un intentionnellement ou involontairement essayant de sauter la stratégie, la flexibilité supplémentaire est exigée.

Les gestionnaires de réseau veulent souvent relâcher des connexions d'un type particulier, telles que tous les fichiers MP3. Cependant, la mise en oeuvre de cette stratégie signifie que vous devez décider aux lesquelles des étiquettes vous voulez pour prêter l'attention (si l'un d'entre eux). AsyncOS te donne la flexibilité de regarder le type MIME (tel que *texte/HTML*), le nom du fichier MIME (tel que *jan.mp3*), et *de relever les empreintes digitales* réellement de la connexion afin d'essayer et déterminer ce qu'est le format vrai. Quand la mise en oeuvre de votre stratégie utilisant le message filtre ou les filtres satisfaits, vous pourriez vouloir utiliser un ou plusieurs de ces étiquettes.

Descriptions d'action de filtre de message

Voici les descriptions d'action de filtre de message :

- **baisse-connexion-par-nom** - Vérifie les noms du fichier de chaque connexion dans un message pour voir s'il apparie l'expression régulière donnée. Le nom du fichier est pris des en-têtes MIME. Cette comparaison distingue les majuscules et minuscules. Si une des connexions de message apparie le nom du fichier, des retours de cette règle **vrais**. Si une connexion est des archives, l'appliance de série C d'IronPort moissonnera les noms de fichier de l'intérieur des archives et appliquera des règles de **scanconfig** (par défaut, des types MIME de video/*, les audio/* et les image/* ne sont pas balayés, et rien plus de 5 Mo n'est balayé) en conséquence.

- **baisse-connexion-par-type** - Relâche toutes les connexions sur les messages qui ont un type MIME, déterminés par le type MIME donné ou l'extension de fichier. Des connexions de fichier d'archivage (zip, goudron) seront abandonnées si elles contiennent un fichier qui s'assortit.

- **baisse-connexion-par-filetype** - Examine des connexions basées sur l'empreinte digital du fichier, et pas simplement de l'extension de nom du fichier de trois-lettre. C'est semblable à la commande de fichier UNIX. En plus des types de fichier individuel qui peuvent être spécifiés, les expressions de groupe compressées, le document, exécutables, image, et medias incluent tous les types de fichier du type général. Par exemple, le groupe *exécutable* inclut .exe, .java .msi .pif, .dll, .scr, des fichiers d'and.com. Veuillez se référer au guide utilisateur d'AsyncOS pour une liste complète de types de fichier qui peuvent être spécifiés.

- **baisse-connexion-par-mimetype** - Relâche toutes les connexions sur les messages qui ont un type MIME donné. Cette action ne tente pas d'établir le type MIME par l'extension de fichier, ainsi elle également n'examine pas le contenu des archives.