Fonctionner avec des filtres de message

Contenu

Introduction

Cet article va au-dessus des pratiques recommandées et de l'implémentation concernant des filtres de message sur l'appliance de sécurité du courrier électronique (ESA). Les filtres de message permettent la création des règles particulières décrivant comment manipuler les messages qui remplissent des conditions spécifiques pendant qu'elles sont reçues et traitées par l'ESA.

Conditions préalables

- Compréhension de base d'exécution de filtre ESA
- Connaissance de l'interface de ligne de commande (CLI) sur l'ESA

Avantages d'utiliser des filtres de message

Il y a deux principaux avantages d'utiliser des filtres de message au-dessus des filtres satisfaits :

1. Ils sont appliqués aux messages vers le début du workqueue traitant le pipeline. En raison de ceci, nous pouvons potentiellement économiser un grand nombre de ressources par le filtrage des messages avant que toutes les engines importantes de lecture soient utilisées (IE : Anti-Spam, antivirus, AMP, etc.).
2. Ils agiront sur entrant et le trafic sortant, tandis que pour satisfait vous filtre devrait créer un pour entrant et un pour sortant.

En outre, il y a peu de conditions qui ne sont pas disponibles pour être configurées utilisant les filtres satisfaits qui peuvent être faits seulement par l'intermédiaire des filtres de message.

Exemple : S'il y a une condition requise de définir des conditions basées sur Sendergroup de l'ESA, cette option est disponible seulement dans des filtres de message.

> Remarque: les actions de filtre de message de Non-finale sont cumulatives. Si un message apparie de plusieurs filtres où chaque filtre spécifie une action différente, alors toutes les actions sont accumulées et imposées. Cependant, si un message apparie de plusieurs filtres spécifiant la même action, les actions antérieures sont ignorées et l'action de filtre final est imposée.

Fonctionnements des filtres de message

Quand AsyncOS traite des filtres de message, le contenu qu'AsyncOS balaye, la commande du traitement, et les mesures prises est basé sur plusieurs facteurs :

- Des filtres de message sont traités dans la commande qu'ils sont configurés (de haut en bas aKa d'abord pour durer)
- Un filtre de message sera traité sur le contenu du message au moment où il atteint le filtre.
- Quand vous appariez une expression régulière, vous configurez un « score » pour compter vers le haut du nombre de fois où une correspondance doit se produire avant qu'une mesure de filtre soit prise. Ceci vous permet « pèsent » les réponses à différents termes.
- Les principaux remplaçants en joignant des états d'un filtre de message sont : (ET/OU/SI/AUTREMENT)

Création des filtres de message

```
partha.cisco.com> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]>
```

D'abord, nous émettons les **filtres de** commande du CLI pour écrire le mode de configuration de filtres de message. Alors les options sont :

- NOUVEAU : Cette option est de commencer la création d'un nouveau filtre. Cette sélection d'option est suivie par le nom du filtre et puis la syntaxe.
- EFFACEMENT : Cette option est de supprimer un filtre existant selon le besoin. Après avoir émis cette commande, vous pouvez écrire le nom du filtre du numéro de séquence pour supprimer
- IMPORTATION : Vous pouvez importer un fichier associé des filtres enregistré dans le répertoire d'appareils.
- EXPORTATION : Cette option laisse exporter le fichier associé des filtres, pour être importée à une autre destination
- MOUVEMENT : Cette option laisse modifier la commande d'un filtre selon la préférence
- POSITIONNEMENT : Cette option nous permet pour changer l'état d'un filtre d'actif à inactif et

vice-versa

- **LISTE** : Cette option affichera tous les filtres créés actuels dans l'ESA
- **DÉTAIL** : Cette option nous permet pour voir les composants du filtre créé, comme les conditions et les actions définies.
- **LOGCONFIG** : Cette option affiche les noms de fichier journal créés pour les filtres de message qui ont eu des actions définies comme archives (nom du dossier de `")
- **ROLLOVERNOW** : Cette option laisse rouler plus de tous les logs actuels dans les répertoires qui sont dus créé à l'action d'archives définie dans des filtres de message

Les filtres peuvent être créés dans tous les modes d'ESA tels que la **batterie**, **grouper** ou **usiner le** mode.

Les critères de la préférence de config dans lesquels l'ESA appliquera les filtres aux emails seront comme sous :

1er Préférence : Mode d'ordinateur

2ème Préférence : Mode de groupe

3ème Préférence : Mode de batterie

Pour la création des filtres de message, nous avons besoin d'une combinaison de syntaxe pour définir des conditions et des actions :

Exemple :

```
if (recv-listener == 'InboundMail' or recv-int == 'notmain')

{

skip-filters();

}

else

{

quarantine(“Policy”);

}
```

.
Le filtre ci-dessus dépeint que si l'auditeur de réception est « InboundMail » OU l'interface de réception est « notmain » alors que l'action sera d'ignorer tous filtres restants de message.

Si les conditions ne s'assortissent pas, alors mettez en quarantaine à la stratégie. Ceci est défini après autrement.

Conseils utiles

Parfois, la syntaxe à utiliser dans des filtres de message peut obtenir confondre, mais un point de référence facile pour la même chose pourrait être les filtres satisfaits.

Nous pouvons créer un filtre satisfait dans les conditions et les actions que nous voulons dans le filtre de message. Après que nous soumettions le filtre, dans la page suivante nous verrons 3 onglets en haut des filtres sectionner à savoir :

- Description
- Règles
- Stratégies

Quand nous cliquons sur en fonction les **règles d'**onglet, cela nous affichera la syntaxe que les utilisations de filtre et les mêmes peuvent être utilisées pour créer des filtres de message. C'est la manière la plus simple de rétrécir vers le bas la syntaxe pour des états de filtre selon notre condition requise.

Expression régulière utilisée dans des filtres de message

- **Carat (^)** : les règles contenant l'accent circonflexe (^) apparient seulement le début de la chaîne.

Exemple : **le ^I AM** m'appariera suis un ingénieur

- **Symbole dollar ($) :** Les règles contenant le caractère de symbole dollar ($) apparient seulement l'extrémité de la chaîne

Exemple : **.com $** appariera google.com aussi bien que yahoo.com

- **Caractère de période (.) :** Règles contenant un caractère de match any de caractère de période (.) (excepté une nouvelle ligne).

Exemple : Le ^… admin$ d'expression régulière apparie le macadmin de chaîne aussi bien que le sunadmin de chaîne mais pas win32admin.

- **Directive d'astérisque (*) :** Les règles contenant un astérisque (*) apparient « zéro correspondances ou plus de la directive précédente. » En particulier, l'ordre d'une période et un astérisque (. *) apparie n'importe quel ordre des caractères (ne contenant pas une nouvelle ligne).

Exemple : L'expression régulière **^P.*Piper$** apparie toutes ces chaînes : PPiper, joueur de pipeau de Peter, P.Piper

- **Caractères particuliers de barre oblique inverse (\)** : Le caractère de barre oblique inverse

échappe à des caractères particuliers. Ainsi l'ordre \. apparie seulement une période littérale, les correspondances de l'ordre \ $ seulement un symbole dollar littéral, et l'ordre \ ^ apparie seulement un accent circonflexe littéral.

Exemple : **\ \ De ^ik d'**expression régulière **\ .ac \ .uk$** apparie seulement la chaîne ik.ac.uk

- **Dossier-insensibilité ((? i))** : Le jeton (? i) qui indique le reste de l'expression régulière devrait être traité en mode ne distinguant pas majuscules et minuscules.

Exemple : L'expression régulière **(? i) Cisco** concurrence Cisco, CISCO aussi bien que Cisco

- **Ou (|) :** « Ou » opérateur. Si A et B sont des expressions régulières, l'expression « A|B » la chaîne de match any qui apparie « A » ou « le B. »

Exemple : **Foo de l'**expression **« |la barre »** appariera le **foo ou la barre**, mais non foobar.

Informations connexes

Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur