Comment est-ce que je garde des copies des messages appariés par mon filtre de message ?

Contenu

Question :

Comment est-ce que je garde des copies des messages appariés par mon filtre de message ?

Réponse :

Il y a plusieurs manières de garder des copies des messages appariés par un filtre de message.

L'action de filtre de message d'archives archivera une copie du message à un fichier journal sur l'ESA dans le format de fichier de mbox UNIX (qui est un format texte très simple). Une fois que créé, le fichier journal peut être contrôlé avec la commande CLI de `filters->logconfig`. Des fichiers journal peuvent être coupés sur des bornes régulières, et être régulièrement poussés hors fonction à un serveur de fichiers d'archives. Voici un exemple d'un filtre de message pour se connecter toute la messagerie d'arrivée au destinataire alan@exchange.example.com :

```
Log-Alan-Tout-messagerie :
si (== « InboundMail » de recv-auditeur)
et (rcpt-à == « \ \ d'alan@exchange \ .example \ .com ») {
  archives (« Alan-tout-messagerie ») ;
}
```

Dans le message archivé, supplémentaire X-IronPort-RCPT-À : des en-têtes sont ajoutées pour chaque destinataire d'enveloppe (au lequel pourrait différer du contenu : ligne d'en-tête.) Veuillez noter que cette liste de destinataires d'enveloppe n'inclut pas nécessairement tous les destinataires que l'expéditeur a indiqués. Si un expéditeur spécifie une adresse de bcc, par exemple, le MTA de envoi pourrait choisir de l'envoyer comme message indépendant entièrement. Inclus dans le log d'archives sont les destinataires d'enveloppe de la transaction de SMTP qui a créé le message.

Remarque: L'action de filtre de message d'archives remplace l'action de log. Les filtres de message qui utilisent les noms précédents seront automatiquement mis à jour quand le système est mis à jour.

Une autre manière de garder des copies d'un message est de générer une copie avec l'action de filtre de bcc. L'action de bcc tire une copie exacte du message et l'envoie au destinataire indiqué,

qui pourrait être une boîte aux lettres de collecte sur un serveur d'archives. Ce sera une copie exacte du contenu du message, mais n'inclut pas les destinataires d'enveloppe (aux lesquels pourrait différer du contenu : ligne d'en-tête.)

```
Copie-Alan-Tout-messagerie :
si (== « InboundMail » de recv-auditeur)
et (rcpt-à == « \ \ d'alan@exchange \ .example \ .com ») {
  bcc (« sam@exchange.example.com ") ;
}
```

Dans des les deux cas ci-dessus, la copie de message est créée par l'action de filtre et est fournie sans transformation plus ultérieure, qui inclut les filtres supplémentaires de filtres, d'anti-Spam, d'antivirus ou de contenu de message. Ainsi une copie de message pourrait contenir un virus.

Il y a une nouvelle action de filtre appelée le bcc-balayage. Ceci peut être utilisé inseated du bcc pour avoir la nouvelle copie balayée par le pipeline normal d'email. Ceci devrait être fait pour aider à réduire les possibilités des virus ou du Spam d'écrire votre réseau. Voici un exemple :

```
Copie-Alan-Tout-messagerie :
si (== « InboundMail » de recv-auditeur)
et (rcpt-à == « \ \ d'alan@exchange \ .example \ .com ») {
  bcc-balayage (« sam@exchange.example.com ") ;
}
```

Notez que dans les filtres ci-dessus de message, l'argument pour rcpt-à la règle est une expression régulière, tels que laquelle exige les opérateurs de évasion d'expression régulière « . ». Dans les actions d'archives ou de bcc, l'argument est simplement une chaîne de texte.

Une manière à très court terme d'examiner des messages appariés par un filtre implique utilisant des quarantaines de système.

Pour plus d'informations, reportez-vous à:

ID 87 de réponse : Comment est-ce que je teste et débogue un filtre de message ou un filtre satisfait avant que je le mette dans la production ?

Pour plus d'informations sur des actions de filtre de message, voyez l'AsyncOS pour le guide de configuration avancée d'email :

Guides d'utilisateur d'appareils de sécurité du courrier électronique de Cisco