ESA - Verwenden eines Nachrichtenfilters, um auf große Nachrichten ohne Anlagen zu reagieren

Inhalt

Einführung

Bestimmte Spammer senden sehr große Nachrichten ohne Anhänge, um die Antispam-Prüfung zu überwinden. Wenn eine Nachricht gesendet werden kann, die größer ist als die maximale Antispam-Scangröße der ESA-Antispam-Engine, wird der Antispam-Scan für diese Nachricht übersprungen. Zum Zeitpunkt der Erstellung dieses Artikels wird nicht empfohlen, die maximale Größe des Antispam-Scanners auf über 2 MB zu erhöhen, es sei denn, es wird anderweitig empfohlen. Daher können Nachrichten mit einer Größe von mehr als 2 MB in den meisten Fällen problemlos Antispam umgehen.

In diesem Artikel wird ein Konzept erläutert, mit dem Sie mithilfe eines Nachrichtenfilters Maßnahmen für diese Arten von Nachrichten ergreifen können.

Anforderungen

1. Befehlszeilenzugriff auf die E-Mail Security Appliance (ESA).
2. Grundkenntnisse zum Schreiben von Nachrichtenfiltern.
3. Grundkenntnisse von Regular Expression (RegEx).

Erstellen des Nachrichtenfilters

In diesem Abschnitt erstellen wir den Nachrichtenfilter. Dieser Nachrichtenfilter entspricht allen Nachrichten, die größer als 2 MB sind und keine Anlage enthalten:

1. Öffnen Sie einen Texteditor, und kopieren Sie den folgenden Nachrichtenfilter/fügen Sie ihn ein:

```
large_spam_no_attachment:
if ((body-size > 2097152) AND NOT (attachment-size > 0)) {
   quarantine("large_spam");
   log-entry("*****This is a large message with no attachments*****");
}
```

Hinweis: *Sie müssen eine Quarantäne für Policy, Virus and Outbreak (PVO) erstellen, die mit*

dem Namen der Quarantäne übereinstimmt, die in der Quarantäneaktion des Nachrichtenfilters verwendet wird, damit der Nachrichtenfilter wie vorgesehen funktioniert. Andernfalls müssen Sie einen anderen Aktionstyp verwenden. Sobald diese PVO-Quarantäne erstellt und der Nachrichtenfilter auf die ESA angewendet wurde, empfehlen wir dringend, die PVO-Quarantäne zu überwachen und gegebenenfalls Quarantänenachrichten freizugeben oder zu löschen.

2. Von hier aus können Sie diesen Nachrichtenfilter an Ihre spezifischen Anforderungen anpassen. Wenn beispielsweise die maximale Scangröße für den Antispam-Scan auf 1 MB festgelegt ist, können Sie die Körpergröße auf 1 MB reduzieren.
3. Sie können auch festlegen, dass dieser Nachrichtenfilter nur auf Nachrichten einer bestimmten Sendergruppe oder eines bestimmten Listeners angewendet werden soll. Im Folgenden sind zwei weitere Beispiele aufgeführt, die für Ihre Zwecke verwendet werden können:

```
large_spam_no_attachment:
if (recv-listener == "IncomingMail") AND ((body-size > 2097152) AND NOT (attachment-size >
0)) {
   quarantine("large_spam");
   log-entry("*****This is a large message with no attachments*****");
}

large_spam_no_attachment:
if (sendergroup != "RELAYLIST") AND ((body-size > 2097152) AND NOT (attachment-size > 0)) {
   quarantine("large_spam");
   log-entry("*****This is a large message with no attachments*****");
}
```

4. Wenn Sie weitere Änderungen vornehmen möchten, empfehle ich, den Abschnitt zum Nachrichtenfilter im ESA-Benutzerhandbuch zu überprüfen. Im Leitfaden finden Sie Abschnitte mit einer Liste der Bedingungen und Aktionen, die verwendet werden können.

Wenden Sie den Nachrichtenfilter auf die ESA an.

In diesem Abschnitt wenden wir den im vorherigen Abschnitt erstellten Nachrichtenfilter auf die ESA an. Nachrichtenfilter können nur über die Befehlszeile auf die ESA angewendet werden. Sie benötigen also Zugriff auf die ESA über die Befehlszeile.

1. Melden Sie sich über die Befehlszeile bei der ESA an.
2. Führen Sie die folgenden hervorgehobenen Befehle aus, um den Nachrichtenfilter auf die ESA anzuwenden:

```
ironport.example.com> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> NEW

Enter filter script.  Enter '.' on its own line to end.
large_spam_no_attachment:
if ((body-size > 2097152) AND NOT (attachment-size > 0)) {
   quarantine("large_spam");
   log-entry("*****This is a large message with no attachments*****");
} .
```

```
1 filters added.
```

3. Von hier aus können Sie den Nachrichtenfilter anzeigen und sicherstellen, dass er aktiv und gültig ist. Führen Sie dazu die folgenden Befehle aus:

```
ironport.example.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.
[]> LIST

Num Active Valid Name
  1   Y      Y   large_spam_no_attachment


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.
[]> DETAIL

Enter the filter name, number, or range:
[]> 1

Num Active Valid Name
  1   Y      Y   large_spam_no_attachment
large_spam_no_attachment: if (body-size > 2097152) AND NOT (attachment-size > 0)) {
                              quarantine("large_spam");
                              log-entry("*****This is a large message with no
attachments*****");
                          }
```

4. Führen Sie den Commit-Befehl aus, und fügen Sie alle relevanten Commit-Kommentare hinzu:

```
ironport.example.com> commit

Please enter some comments describing your changes:
[]> Applied large_spam_no_attachment message filter
```

Zusätzliche Ressourcen

[ESA-Endbenutzeranleitung]