ESA — 使用郵件過濾器對沒有附件的大郵件執行操作

目錄

簡介

您可能會發現某些垃圾郵件傳送者會傳送沒有附件的超大郵件，以便通過反垃圾郵件掃描。如果他們可以傳送大於ESA反垃圾郵件引擎最大掃描大小的郵件，則會跳過該郵件的反垃圾郵件掃描。在撰寫本文時，除非另有建議，否則我們建議不要將反垃圾郵件最大掃描大小增加至2MB以上。因此，在多數情況下，2MB以上的郵件可以輕鬆繞過反垃圾郵件。

本文將解釋利用消息過濾器對這些型別的消息採取行動的一個概念。

需求

1. 對郵件安全裝置(ESA)的命令列訪問。
2. 有關如何編寫郵件過濾器的基本知識。
3. 正規表示式(RegEx)基礎知識。

建立郵件篩選器

在本節中，我們將建立郵件過濾器。此郵件過濾器將匹配大小超過2MB且不包含附件的所有郵件：

1. 開啟文本編輯器並複製/貼上以下郵件過濾器：

```
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*****");
}
```

   附註： *您需要建立與郵件過濾器的隔離操作中使用的隔離區名稱相匹配的策略、病毒和爆發(PVO)隔離區，郵件過濾器才能按原樣工作。否則，必須使用不同的操作型別。建立此PVO隔離區並將郵件過濾器應用於ESA後，強烈建議您監視PVO隔離區，並根據需要釋放或刪除隔離的郵件。*
2. 在此處，您可能希望修改此郵件過濾器以適應您的特定要求。例如，如果最大反垃圾郵件掃描大小設定為1MB，則可以將正文大小減小到1MB。
3. 您可能還希望此消息過濾器僅應用於來自特定發件人組或監聽程式的消息。以下兩個額外的示例可能適用於您的用途：

```
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. 如果您想進行任何其他更改，我建議您檢視《ESA最終使用指南》中的郵件過濾器部分。指南中有一些部分提供了可使用條件和操作的清單。

將郵件過濾器應用於ESA

在本節中，我們將將在上一節中建立的郵件過濾器應用於ESA。消息過濾器只能通過命令列應用於ESA。因此，您需要命令列訪問ESA。

1. 通過命令列登入到ESA。
2. 運行以下突出顯示的命令，將郵件過濾器應用於ESA:

```
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. 在此處，您可能需要檢視郵件篩選器並確保其處於活動狀態且有效。您可以通過運行以下命令來做到這一點：

```
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. 運行commit命令並新增任何相關的提交註釋：

```
ironport.example.com> commit

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

其他資源

[ESA最終使用手冊]