ESA消息過濾器操作說明

目錄

簡介

本檔案介紹思科電子郵件安全裝置(ESA)上按名稱、-type、-filetype和 — mimetype郵件過濾器操作之間的差異。

郵件過濾器操作概述

使用MIME傳送的郵件可以將標籤分配給各個正文部分，這些部分通常稱為附件。 這些標籤可能在其提供的資訊中相互衝突（並且確實存在衝突）。此外，身體部位可能有其自己的特徵。 例如，使用者可能獲取JPEG影象，將其附加到郵件郵件，為其提供**text/html**的MIME型別，並用MIME檔名**jan.mp3**對其進行標籤。所有這些標籤都與附件內容的實際情況相衝突。

例如，請考慮以下消息標題：

```
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
```

在這種情況下，MIME檔名和MIME型別都是一致的，並且可能與正文部分（附件）的實際格式不匹配。但是，在此標頭中存在不一致：

```
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.
```

對於格式完好的消息，實施策略相當容易。但如果有人有意或無意地試圖繞過策略，則需要更大的靈活性。

網路管理員通常希望丟棄特定型別的附件，例如所有MP3檔案。但是，實施該策略意味著您必須決定您要關注哪些標籤（如果有）。 AsyncOS使您可以靈活地檢視MIME型別(如*text/html*)、MIME檔名(如*jan.mp3*)，並實際對附件進行*指紋*，以嘗試確定真正的格式。在使用郵件過濾器或內容過濾器實施策略時，您可能希望使用這些標籤中的一個或多個標籤。

郵件過濾器操作說明

以下是郵件過濾器操作說明：

- **drop-attachments-by-name** — 檢查郵件中每個附件的檔名，以檢視它是否與給定的正規表示式匹配。檔名取自MIME報頭。比較區分大小寫。如果其中一個郵件附件與檔名匹配，則此規則返回**true**。如果附件是歸檔檔案，則IronPort C系列裝置將從歸檔檔案內部收集檔名並應用**scanconfig規**則（預設情況下，不會掃描video/*、audio/*和image/*的MIME型別，並且不會掃描超過5 MB的檔案）。

- **drop-attachments-by-type** — 丟棄郵件中具有MIME型別的所有附件，該型別由給定的MIME型別或副檔名確定。 如果存檔檔案附件(zip、tar)包含符合的檔案，則會將其捨棄。

- **drop-attachments-by-filetype** — 根據檔案的指紋（而不僅僅是三字母的副檔名）檢查附件。這類似於UNIX file命令。除了可以指定的個別檔案型別外，組表達式Compressed、Document、Executable、Image和Media還包括一般型別的所有檔案型別。例如，*Executable*組包括.exe、.java .msi .pif、.dll、.scr和and.com檔案。有關可以指定的檔案型別的完整清單，請參閱《AsyncOS使用手冊》。

- **drop-attachments-by-mimetype -**丟棄具有給定MIME型別的郵件上的所有附件。此操作不會嘗試通過副檔名確定MIME型別，因此也不會檢查存檔的內容。