使用郵件過濾器

目錄

簡介

本文介紹有關郵件安全裝置(ESA)上的郵件過濾器的最佳實踐和實施。 報文過濾器允許建立特殊規則，描述如何處理在ESA接收和處理符合特定條件的報文。

必要條件

- 對ESA過濾器操作的基本瞭解
- 熟悉ESA上的命令列介面(CLI)

使用郵件過濾器的優點

使用郵件過濾器比內容過濾器主要有兩個優點：

1. 它們將應用於接近工作隊列處理管道開始處的消息。因此，我們可能會在使用任何主要掃描引擎之前過濾消息，從而節省大量資源(即：反垃圾郵件、防病毒、AMP等)。
2. 它們將對傳入和傳出流量執行操作，而對於內容過濾器，您需要為傳入和傳出建立一個過濾器。

此外，還有少數條件無法使用只能通過郵件過濾器的內容過濾器進行配置。

範例：如果要求根據ESA的Sendergroup定義條件，則該選項僅在Message Filters中可用。

> **附註**：非最終郵件過濾器操作是累積的。如果消息與多個過濾器匹配，其中每個過濾器指定了不同的操作，則所有操作都將累加並實施。但是，如果消息與指定相同操作的多個過濾器匹配，則覆蓋先前的操作並執行最終過濾器操作。

郵件過濾器的操作

當AsyncOS處理郵件過濾器時，AsyncOS掃描的內容、處理順序和所採取的操作基於以下幾個因素：

- 郵件過濾器按配置順序處理（從上到下Ka從首到末）
- 當郵件內容到達過濾器時，將對郵件內容處理郵件過濾器。
- 當匹配正規表示式時，可以配置「分數」以計算在執行篩選操作之前必須發生匹配的次數。這允許您根據不同的術語「權衡」回答。
- 消息過濾器的連結條件的主要替代項為：**（和/或/如果/其他）**

建立郵件過濾器

```
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.
[]>
```

首先，從CLI發出**filters**命令以進入消息過濾器的配置模式。然後選項為：

- **新**:此選項將開始建立新過濾器。此選項選擇後跟篩選器名稱，然後是語法。
- **刪除**:此選項根據需要刪除現有篩選器。發出此命令後，您可以輸入要刪除的序列號過濾器名稱
- **匯入**:您可以匯入儲存在裝置目錄中的過濾器相關檔案。
- **匯出**:此選項允許匯出篩選器的相關檔案，以匯入到另一個目標
- **移動**:此選項允許根據首選項修改篩選器的順序
- **SET**:此選項允許我們將過濾器的狀態從「活動」更改為「非活動」，反之亦然
- **清單**:此選項將顯示在ESA中存在的所有已建立的過濾器
- **詳細資訊**:此選項允許我們檢視所建立過濾器的元件，例如定義的條件和操作。
- **LOGCONFIG**:此選項顯示為郵件過濾器建立的日誌檔名稱，這些過濾器具有定義為存檔的操作（「資料夾名稱」）
- **ROLLOVERNOW**:使用此選項可以滾動因郵件過濾器中定義的存檔操作而建立的資料夾中存在的所有日誌

可以在ESA的所有模式(例如**集群**、**組**或**電腦**)中建立過濾器。

ESA將對電子郵件應用過濾器的配置首選項標準如下所示：

1st Preference:機器模式

第2個首選項：組模式

第三個首選項：群集模式

要建立消息過濾器，我們需要結合使用語法來定義條件和操作：

範例：

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

{

skip-filters();

}

else

{

quarantine(“Policy”);

}
```

.
上面的過濾器說明，如果接收監聽程式為「InboundMail」或接收介面為「notmain」，則操作將是跳過任何剩餘郵件過濾器。

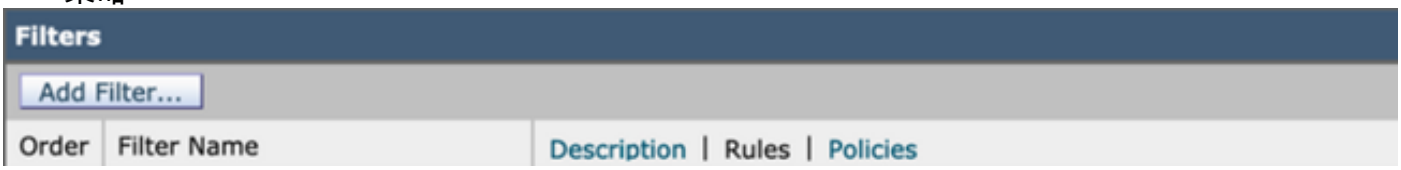
如果條件不匹配，則隔離到策略。這是用其它名稱定義的。

實用提示

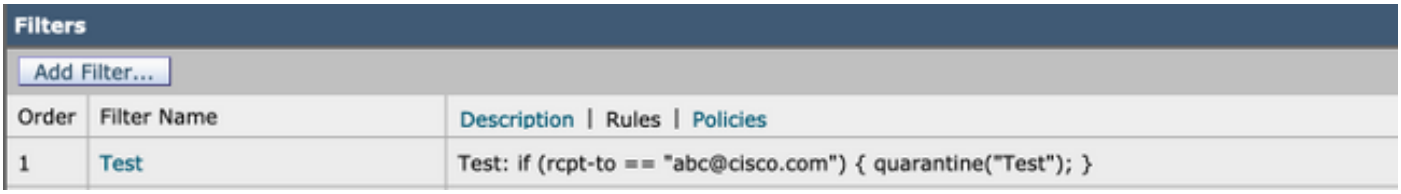
有時，在郵件過濾器中使用的語法可能會令人困惑，但內容過濾器卻是一個簡單的參考點。

我們可以建立內容過濾器，該過濾器包含我們希望在郵件過濾器中使用的條件和操作。提交過濾器後，在下一頁中，我們將看到過濾器部分頂部的3個頁籤，即：

- 說明
- 規則
- 策略



按一下**Rules**頁籤後，該頁籤將顯示過濾器使用的語法，可用於建立郵件過濾器。這是根據我們的要求縮小過濾條件語法範圍的最簡單方法。



消息過濾器中使用的正規表示式

- **卡拉(^)**:包含脫字元號(^)的規則只與字串的開頭匹配。

範例：^我會配得上工程師

- **美元符號($):**包含美元符號字元($)的規則僅與字串的結尾匹配

範例：.com$將匹配google.com和yahoo.com

- **句點字元(.):**包含句點字元(.)的規則與任何字元（新行除外）匹配。

範例：正則表達**式^...admin$**匹配字串macadmin和字串sunadmin，但不匹配win32admin。

- **星號(*)指令：**包含星號(*)的規則與「上一個指令的零個或多個匹配項」匹配。 特別是句點和星號(.*)的序列與任意字元序列（不包含新行）匹配。

範例：正則表達**式^P.*Piper$匹配**以下所有字串：派珀，彼得·派珀，P.派珀

- **反斜線特殊字元(\):**反斜線字元*轉義*特殊字元。因此，序列\.只匹配文本句點，序列\$只匹配文本美元符號，序列\^只匹配文本脫字元號。

範例：正則表達**式^ik\\.ac\\.uk$僅**匹配字串ik.ac.uk

- **不區分大小寫(?i)):**指示正規表示式的其餘部分的令牌(?i)應在不區分大小寫的模式下處理。

範例：正則表**達式(?i)cisco**匹配Cisco、CISCO以及cisco

- **或(|):**「或」運算子。如果A和B是正規表示式，則表達式「A|B」將與匹配「A」或「B」的任何字串匹配。

範例： 表達式**「foo|bar」將匹配**foo或**bar，但不**匹配foobar。

相關資訊

Cisco Email Security Appliance — 最終使用手冊