ESA のメッセージ フィルタ動作の説明

目次

[はじめに](#)
[メッセージ フィルタ アクションの概要](#)
[メッセージ フィルタ アクションの説明](#)

概要

このドキュメントでは、Cisco Email Security Appliance（ESA）上の drop-attachments-by-name、-type、-filetype、および -mimetype のメッセージ フィルタ アクションの違いについて説明します。

メッセージ フィルタ アクションの概要

MIME を使用して送信されるメッセージでは、添付ファイルと呼ばれる本文パートにラベルを割り当てることができます。 これらのラベルは提供する情報が相互に矛盾する可能性があります（現にそうなっています）。 加えて、本文パートには独自の特性を持たせることができます。 たとえば、ユーザは JPEG 画像を取って、それをメール メッセージに添付し、それに **text/html** の MIME タイプを割り当て、それを **jan.mp3** の MIME ファイル名でマーキングすることができます。 これらのラベルのすべてが、添付ファイルの実体と矛盾します。

たとえば、次のメッセージ ヘッダーについて考えましょう。

```
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
```

このケースでは、MIME ファイル名と MIME タイプのすべてが一貫しており、本文パート（添付ファイル）の実際の形式と一致する場合としない場合があります。 ただし、このヘッダーには、矛盾があります。

```
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.
```

正しく定義されたメッセージの場合は、ポリシーの実装が比較的簡単です。 しかし、何者かが意図的か無意識かに関係なくポリシーをバイパスしようとする場合は、さらなる柔軟性が必要になります。

ネットワーク マネージャは、MP3 ファイルなどの特定のタイプの添付ファイルをドロップしたい場合があります。 ただし、このポリシーを実装するには、注意すべきラベル（もしあれば）を決定する必要があります。 AsyncOS は、MIME タイプ（*text/html* など）や MIME ファイル名（*jan.mp3* など）を検査したり、実際に添付ファイルの*フィンガープリント*を採取して本当の形式を特定したりする柔軟性を備えています。 メッセージ フィルタまたはコンテンツ フィルタを使用してポリシーを実装すれば、これらのラベルを 1 つ以上使用することができます。

メッセージ フィルタ アクションの説明

メッセージ フィルタ アクションの説明を以下に示します。

- **drop-attachments-by-name**：メッセージ内の各添付ファイルのファイル名をチェックして、指定された正規表現と一致するかどうかを確認します。 ファイル名は、MIME ヘッダーから取得されます。 この比較では大文字と小文字は区別されます。 メッセージの添付ファイルのいずれかがファイル名と一致すると、このルールは **true** を返します。 添付ファイルがアーカイブの場合は、IronPort C シリーズ アプライアンスがアーカイブ内からファイル名を取得し、それに応じて **scanconfig** ルールを適用します（デフォルトで、video/*、audio/*、および image/* の MIME タイプはスキャンされず、5 MB を超えるファイルもスキャンされません）。

- **drop-attachments-by-type**：メッセージの添付ファイルのうち、指定された MIME タイプまたはファイル拡張子で識別される MIME タイプのファイルをすべてドロップします。 アーカイブ ファイルの添付ファイル（zip、tar）は、それらに含まれるファイルが一致した場合にドロップされます。

- **drop-attachments-by-filetype**：3 文字のファイル拡張子だけではなく、ファイルのフィンガープリントに基づいて添付ファイルを検査します。 これは、UNIX の file コマンドに似ています。 指定可能な個別のファイル タイプに加えて、グループとしての Compressed、Document、Executable、Image、および Media には、その一般タイプのすべてのファイル タイプが含まれます。 たとえば、*Executable* グループには、.exe、.java、.msi、.pif、.dll、.scr、および.com ファイルが含まれます。 指定可能なファイル タイプの完全なリストについては、AsyncOS ユーザ ガイドを参照してください。

- **drop-attachments-by-mimetype**：特定の MIME タイプを持つメッセージのすべての添付ファイルをドロップします。 このアクションは、ファイル拡張子による MIME タイプの判別を行わないため、アーカイブの内容の検査も行いません。