Beschreibung der ESA-Nachrichtenfilter-Aktion

Inhalt

Einführung

In diesem Dokument werden die Unterschiede zwischen den Aktionen für die Drop-Attachments nach Name, -Typ, -Dateityp und -mimetype-Nachrichtenfilter auf der Cisco E-Mail Security Appliance (ESA) beschrieben.

Übersicht über die Nachrichtenfilteraktion

Bei Nachrichten, die mit MIME gesendet werden, können Labels verschiedenen Körperteilen zugeordnet werden, die häufig als Anhänge bezeichnet werden. Diese Labels können in den von ihnen bereitgestellten Informationen miteinander in Konflikt stehen (und dies auch tun). Zusätzlich kann ein Körperteil seine eigenen Eigenschaften haben. Beispielsweise kann ein Benutzer ein JPEG-Bild nehmen, es an eine E-Mail-Nachricht anhängen, ihm einen MIME-Typ von **Text/HTML** geben und es mit einem MIME-Dateinamen von **jan.mp3** markieren. All diese Etiketten widersprechen der Realität der Anlage.

Betrachten Sie zum Beispiel diesen Nachrichtenheader:

```
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
```

In diesem Fall sind die MIME-Dateinamen und die MIME-Typen konsistent und stimmen möglicherweise nicht mit dem tatsächlichen Format des Textteils (Anlage) überein. In dieser Überschrift treten jedoch Inkonsistenzen auf:

```
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.
```

Bei wohlformulierten Botschaften ist die Umsetzung von Richtlinien ziemlich einfach. Im Falle einer Person, die entweder absichtlich oder unabsichtlich versucht, eine Richtlinie zu umgehen, ist jedoch zusätzliche Flexibilität erforderlich.

Netzwerkmanager möchten häufig Anhänge eines bestimmten Typs löschen, z. B. alle MP3-Dateien. Die Umsetzung dieser Richtlinie bedeutet jedoch, dass Sie entscheiden müssen, auf welche der Labels Sie achten möchten (wenn überhaupt). AsyncOS bietet Ihnen die Flexibilität, den MIME-Typ (z. B. *text/html*), den MIME-Dateinamen (z. B. *jan.mp3*) und *Fingerabdrücke* der Anlage zu *erstellen*, um das tatsächliche Format zu bestimmen. Wenn Sie Ihre Richtlinie mithilfe von Nachrichtenfiltern oder Content-Filtern implementieren, können Sie eine oder mehrere dieser Bezeichnungen verwenden.

Beschreibung der Nachrichtenfilteraktion

Nachfolgend finden Sie die Beschreibungen der Nachrichtenfilteraktion:

- **drop-Attachments-by-name**: Überprüft die Dateinamen jeder Anlage in einer Nachricht, um festzustellen, ob sie mit dem angegebenen regulären Ausdruck übereinstimmt. Der Dateiname stammt aus den MIME-Headern. Beim Vergleich wird die Groß- und Kleinschreibung beachtet. Wenn einer der Nachrichtenanhänge mit dem Dateinamen übereinstimmt, gibt diese Regel **true** zurück. Wenn es sich bei einer Anlage um ein Archiv handelt, erfasst die Appliance der IronPort C-Serie die Dateinamen aus dem Archiv und wendet **scanconfig-**Regeln an (standardmäßig werden die MIME-Typen Video/*, Audio/* und Bild/* nicht gescannt, und es werden nicht mehr als 5 MB gescannt).

- **Dropdownanhänge nach Typ** - Legt alle Anhänge von Nachrichten mit einem MIME-Typ ab, der entweder durch den angegebenen MIME-Typ oder die Dateierweiterung bestimmt wird. Anlagen mit Archivdateien (zip, tar) werden gelöscht, wenn sie eine übereinstimmende Datei enthalten.

- **drop-anhänge-by-filetype** - Analysiert Anhänge basierend auf dem Fingerabdruck der Datei und nicht nur auf der Dateierweiterung mit drei Buchstaben. Dies ähnelt dem UNIX-Dateibefehl. Neben den einzelnen Dateitypen, die angegeben werden können, enthalten die Gruppenausdrücke Komprimiert, Dokument, ausführbare Datei, Bild und Medien alle Dateitypen des allgemeinen Typs. Beispielsweise enthält die Gruppe *Ausführbare* Dateien .exe, .java.msi.pif, .dll, .scr und.com. Eine vollständige Liste der Dateitypen, die angegeben werden können, finden Sie im AsyncOS-Benutzerhandbuch.

- **drop-anhänge-by-mimetype** - Legt alle Anhänge von Nachrichten mit einem bestimmten MIME-Typ ab. Bei dieser Aktion wird nicht versucht, den MIME-Typ nach Dateierweiterung zu ermitteln, daher wird auch der Inhalt der Archive nicht geprüft.