ESA-Content-Filter für E-Mail-Nachrichten mit mehreren Anhängen

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Filterbedingungen für negative Inhalte für E-Mail-Nachrichten funktionieren, die mehrere Anhänge der Cisco E-Mail Security Appliance (ESA) enthalten.

Problem

Sie verwenden einen Content-Filter, der bestimmte Arten von E-Mail-Anhängen zulässt, während andere Arten von Anhängen für die Quarantäne markiert werden sollten. Wenn eine E-Mail-Nachricht eingeht, die mehrere Anhänge enthält, von denen eine zugelassen und eine andere für die Quarantäne markiert werden soll, identifiziert der Filter die gesamte Nachricht als *zulässig*.

Hier ist der verwendete Content-Filter:

```
if attachment filename != (list of attachments), then quarantine
```

Diese Bedingung und Aktion funktioniert wie vorgesehen, wenn die E-Mail-Nachricht nur einen Anhang enthält, sie funktioniert jedoch nicht ordnungsgemäß für Nachrichten, die mehrere, unterschiedliche Anhänge enthalten.

Beispielszenario

Folgende Arten von Anhängen sind zulässig:

- rar
- PDF
- jpg

Alle anderen Anhänge sollten gemäß der Filterbedingung und -aktion in Quarantäne gesendet

werden.

Filterbedingung

Die Filterbedingung lautet wie folgt:

```
if attachment filename != (rar|pdf|jpg)
```

Aktion filtern

Hier ist die Filteraktion, die verwendet wird:

```
quarantine
```

In der Regel wird erwartet, dass die E-Mail-Nachricht, die einen **PDF-**Anhang und einen **Text-**Anhang enthält, aufgrund des **TXT-**Anhangs unter Quarantäne gestellt wird, da sie nicht in der Liste der zulässigen Anhänge enthalten ist. Dieser Content-Filter funktioniert jedoch nicht wie vorgesehen, da er mit dem **PDF-**Anhang in der Nachricht übereinstimmt und ihn direkt zulässt, obwohl er über einen **Text-**Anhang verfügt.

Lösung

Aus folgenden Gründen ist es nicht möglich, die E-Mail mit dem **Text-**Anhang zu isolieren:

- Die Anhangsbedingungen gelten für **alle** Anlagen, die in einer Nachricht enthalten sind.
- Der negative **!=** Vergleich überprüft, ob die Anhänge übereinstimmen.

Wenn **eine** der Anhänge zulässig ist (z. B. bei Übereinstimmung mit dem **!=**), wird die gesamte Nachricht als *zulässig* behandelt. Es gibt keinen Weg, das zu umgehen; Es ist einfach die Art und Weise, wie diese Bedingungen funktionieren.

Die einzige andere Lösung besteht darin, die Logik umzukehren und bestimmte Anhänge zu blockieren. Dies gilt nicht nur für Anlagen, die nicht in der weißen Liste aufgeführt sind.