Arbeiten mit Nachrichtenfiltern

Inhalt

Einführung

In diesem Artikel werden Best Practices und die Implementierung von Nachrichtenfiltern auf der E-Mail Security Appliance (ESA) vorgestellt. Nachrichtenfilter ermöglichen die Erstellung spezieller Regeln, in denen beschrieben wird, wie Nachrichten behandelt werden, die bestimmte Bedingungen erfüllen, wenn sie von der ESA empfangen und verarbeitet werden.

Voraussetzungen

- Grundlegendes Verständnis des ESA-Filterbetriebs
- Vertrautheit mit der CLI (Command Line Interface) der ESA

Vorteile der Verwendung von Nachrichtenfiltern

Die Verwendung von Nachrichtenfiltern gegenüber Content-Filtern bietet zwei wesentliche Vorteile:

1. Sie werden auf Nachrichten am Anfang der Workqueue Processing Pipeline angewendet. Daher können wir möglicherweise eine große Anzahl von Ressourcen durch Filtern von Nachrichten speichern, bevor größere Scan-Engines genutzt werden (d. h.: Anti-Spam, Anti-Virus, AMP usw.).
2. Sie ergreifen Aktionen für eingehenden und ausgehenden Datenverkehr, während Sie für Content-Filter einen für eingehenden und einen für ausgehenden Datenverkehr erstellen müssen.

Außerdem gibt es nur wenige Bedingungen, die nicht mit Content-Filtern konfiguriert werden können, die nur über Nachrichtenfilter konfiguriert werden können.

Beispiel: Wenn Bedingungen auf Basis der Sendergruppe der ESA definiert werden müssen, ist diese Option nur in Nachrichtenfiltern verfügbar.

> **Hinweis**: Nicht-finale Nachrichtenfilteraktionen sind kumulativ. Wenn eine Nachricht mit mehreren Filtern übereinstimmt, bei denen jeder Filter eine andere Aktion angibt, werden alle Aktionen akkumuliert und durchgesetzt. Wenn jedoch eine Nachricht mehreren Filtern entspricht, die dieselbe Aktion angeben, werden die vorherigen Aktionen überschrieben und die letzte Filteraktion erzwungen.

Betrieb der Nachrichtenfilter

Wenn AsyncOS Nachrichtenfilter verarbeitet, basieren der von AsyncOS gescannte Inhalt, die Reihenfolge der Verarbeitung und die durchgeführten Aktionen auf mehreren Faktoren:

- Nachrichtenfilter werden in der Reihenfolge verarbeitet, in der sie konfiguriert wurden (Top to Bottom Ka First to Last)
- Beim Erreichen des Filters wird ein Nachrichtenfilter für den Nachrichteninhalt verarbeitet.
- Wenn Sie einen regulären Ausdruck zuordnen, konfigurieren Sie eine "Punktzahl", um die Anzahl festzulegen, die eine Übereinstimmung vor einer Filteraktion auftreten muss. Dadurch können Sie die Antworten auf unterschiedliche Begriffe "abwägen".
- Die wichtigsten Alternativen bei den Verknüpfungsbedingungen eines Nachrichtenfilters sind: (UND/ODER/IF/ELSE)

Erstellen von Nachrichtenfiltern

```
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.
[]>
```

Zunächst geben wir die **Befehlsfilter** aus der CLI aus, um in den Konfigurationsmodus von Nachrichtenfilter zu wechseln. Anschließend sind folgende Optionen verfügbar:

- **NEU**: Mit dieser Option wird die Erstellung eines neuen Filters gestartet. Auf diese Optionsauswahl folgen der Name Filter und anschließend die Syntax.
- **LÖSCHEN**: Diese Option besteht darin, einen vorhandenen Filter je nach Bedarf zu löschen. Nachdem Sie diesen Befehl ausgegeben haben, können Sie den Filternamen der zu löschenden Sequenznummer eingeben.
- **IMPORTIEREN**: Sie können eine Filterdatei importieren, die im Appliance-Verzeichnis gespeichert ist.
- **EXPORTIEREN**: Mit dieser Option können die zugehörigen Dateien der Filter exportiert und in ein anderes Ziel importiert werden.
- **BEWEGEN**: Mit dieser Option können Sie die Reihenfolge eines Filters je nach Präferenz ändern.

- **SET**: Mit dieser Option können wir den Status eines Filters von Active (Aktiv) in Inactive (Inaktiv) und umgekehrt ändern.
- **LISTE**: Diese Option zeigt alle erstellten Filter an, die in der ESA vorhanden sind.
- **DETAILS**: Diese Option ermöglicht es uns, die Komponenten des erstellten Filters zu sehen, wie die Bedingungen und die Aktionen definiert.
- **LOGCONFIG**: Diese Option zeigt die Protokolldateinamen an, die für Nachrichtenfilter erstellt wurden, deren Aktionen als Archiv definiert waren ("Ordnername").
- **ROLLOVERNOW**: Mit dieser Option können alle Protokolle in den Ordnern, die aufgrund der in Nachrichtenfiltern definierten Archivaktion erstellt wurden, umgeleitet werden.

Filter können in allen ESA-Modi erstellt werden, z. B. **Cluster**, **Gruppe** oder **Computer**-Modus.

Die Konfigurationsvoreinstellungen, nach denen die ESA die Filter auf die E-Mails anwendet, sind wie folgt:

1. **Präferenz:** Maschinenmodus

2. **Präferenz:** Gruppenmodus

3. **Präferenz:** Clustermodus

Zum Erstellen von Nachrichtenfiltern ist eine Kombination aus Syntax erforderlich, um Bedingungen und Aktionen zu definieren:

Beispiel:

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

{

skip-filters();

}

else

{

quarantine(“Policy”);

}
```

.

Der obige Filter zeigt an, dass, wenn der empfangende Listener 'InboundMail' ist ODER die empfangende Schnittstelle 'not main' ist, alle verbleibenden Nachrichtenfilter übersprungen werden.

Stimmen die Bedingungen nicht überein, wird die Quarantäne auf Policy gesetzt. Dies wird später definiert.

Hilfreiche Tipps

Manchmal ist die in Nachrichtenfiltern zu verwendende Syntax verwirrend, aber ein einfacher Bezugspunkt für dasselbe kann Content-Filter sein.

Wir können einen Content-Filter mit Bedingungen und Aktionen erstellen, die wir im Nachrichtenfilter wünschen. Nach dem Einsenden des Filters werden auf der nächsten Seite drei Registerkarten oben im Filterbereich angezeigt:

- Beschreibung
- Regeln
- Richtlinien

Wenn wir auf die Registerkarte **Regeln** klicken, wird uns die Syntax angezeigt, die der Filter verwendet, und das gleiche kann zum Erstellen von Nachrichtenfiltern verwendet werden. Dies ist die einfachste Methode, um die Syntax für Filterbedingungen gemäß unserer Anforderung einzugrenzen.

Regulärer Ausdruck in Nachrichtenfiltern verwendet

- **Carat (^)**: Regeln, die das Caret-Symbol (^) enthalten, entsprechen nur dem Anfang der Zeichenfolge.

Beispiel: **Ich** bin Ingenieur.

- **Dollarzeichen ($):** Regeln, die das Dollarzeichen ($) enthalten, entsprechen nur dem Ende der Zeichenfolge

Beispiel: **.com$** werden sowohl auf google.com als auch auf yahoo.com abgleichen.

- **Periodenzeichen (.):** Regeln, die ein Punkt-Zeichen (.) enthalten, entsprechen jedem beliebigen Zeichen (mit Ausnahme einer neuen Zeile).

Beispiel: Der reguläre Ausdruck **^..admin$** stimmt mit dem String macadmin sowie der String sunadmin überein, aber win32admin ist nicht zulässig.

- **Asterisk-Richtlinie (*):** Regeln, die ein Sternchen (*) enthalten, stimmen mit "0 oder mehr Übereinstimmungen der vorherigen Direktive" überein. Insbesondere entspricht die Sequenz eines Zeitraums und eines Sternchens (.*) einer beliebigen Zeichensequenz (die keine neue Zeile enthält).

Beispiel: Der reguläre Ausdruck **^P.*Piper$** stimmt mit allen folgenden Zeichenfolgen überein: Piper, Peter Piper, P.Piper

- **Sonderzeichen (\)**: Der umgekehrte Schrägstrich *Escapt* Sonderzeichen. So die Sequenz \. nur einem literalen Zeitraum entspricht, entspricht die Sequenz \$ nur einem literalen Dollarzeichen, und die Sequenz \^ entspricht nur einem literalen Caretsymbol.

Beispiel: Der reguläre Ausdruck **^ik\\.ac\\.uk$** stimmt nur mit der Zeichenfolge ik.ac.uk überein.

- **Groß- und Kleinschreibung (i)**: Das Token (?i), das den Rest des regulären Ausdrucks angibt, sollte im Modus ohne Berücksichtigung der Groß-/Kleinschreibung behandelt werden.

Beispiel: Der reguläre Ausdruck **(?i)cisco** stimmt mit Cisco, CISCO und Cisco überein.

- **oder (|):** Der Operator "oder". Wenn A und B reguläre Ausdrücke sind, entspricht der Ausdruck "A|B" jeder Zeichenfolge, die entweder "A" oder "B" entspricht.

Beispiel: Der Ausdruck **"foo|bar"** entspricht entweder **foo oder bar**, aber nicht foobar.

Zugehörige Informationen

Cisco Email Security Appliance - Benutzerhandbücher