ASA HTTP-URL-Filterfunktionen mit Regex

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration von URL-Filtern auf einer Adaptive Security Appliance (ASA) mit der HTTP Inspection Engine. Dies ist abgeschlossen, wenn Teile der HTTP-Anforderung mit der Verwendung einer Liste von Regex-Mustern abgeglichen werden. Sie können entweder bestimmte URLs blockieren oder alle URLs mit Ausnahme einiger ausgewählter URLs blockieren.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Konfigurationsschritte

Dies sind die allgemeinen Konfigurationsschritte:

1. Identifizieren Sie eine kurze Liste von Domänen, die blockiert oder zugelassen werden sollen.
2. Erstellen Sie eine regex-Klassenzuordnung, die mit allen in Frage stehenden Domänen übereinstimmt.
3. Erstellen einer HTTP Inspection Policy Map, die Datenverkehr, der diesen Domänen entspricht, verwirft oder zulässt
4. Anwenden dieser HTTP-Inspektionsrichtlinienzuordnung auf eine HTTP-Überprüfung in modularem Richtlinien-Framework

Unabhängig davon, ob Sie versuchen, einige Domänen zu blockieren und alle anderen zu erlauben oder alle Domänen zu blockieren und nur einige wenige zu erlauben, sind die Schritte bis auf die Erstellung der HTTP Inspection Policy Map identisch.

Identifizieren Sie eine kurze Liste von Domänen, die blockiert oder zugelassen werden sollen.

In diesem Konfigurationsbeispiel werden diese Domänen entweder blockiert oder zugelassen:

- cisco1.com
- Cisco2.com
- Cisco3.com

Konfigurieren Sie die regulären Muster für diese Domänen:

```
regex cisco1.com "cisco1.com"regex cisco2.com "cisco2.com"regex cisco3.com "cisco3.com"
```

Erstellen Sie eine regex-Klassenzuordnung, die mit allen in Frage stehenden Domänen übereinstimmt.

Konfigurieren Sie eine regex-Klasse, die mit den regulären Mustern übereinstimmt:

```
class-map type regex match-any domain-regex-classmatch regex cisco1.commatch regex
cisco2.commatch regex cisco3.com
```

Erstellen einer HTTP Inspection Policy Map, die Datenverkehr, der diesen Domänen entspricht,

verwirft oder zulässt

Um zu verstehen, wie diese Konfiguration aussehen soll, wählen Sie die Beschreibung aus, die am besten zum Ziel dieses URL-Filters passt. Die oben erstellte regex-Klasse ist entweder eine Liste der Domänen, die zugelassen werden sollen, oder eine Liste der Domänen, die blockiert werden sollen.

- **Zulassen aller Domänen mit Ausnahme der aufgeführten**Der Schlüssel zu dieser Konfiguration besteht darin, dass eine Klassenzuordnung erstellt wird, bei der eine HTTP-Transaktion, die mit den aufgeführten Domänen übereinstimmt, als "blockierte Domänenklasse" klassifiziert wird. Die HTTP-Transaktion, die dieser Klasse entspricht, wird zurückgesetzt und geschlossen. Im Wesentlichen wird nur die HTTP-Transaktion zurückgesetzt, die diesen Domänen entspricht.
```
class-map type inspect http match-all blocked-domain-class match request header host regex
class domain-regex-class!policy-map type inspect http regex-filtering-policy parameters
class blocked-domain-class  reset log
```
- **Alle Domänen mit Ausnahme der aufgeführten blockieren**Der Schlüssel zu dieser Konfiguration besteht darin, dass eine Klassenzuordnung mit dem Schlüsselwort "match not" erstellt wird. Dies weist die Firewall darauf hin, dass alle Domänen, die nicht mit der Domänenliste übereinstimmen, der Klasse mit dem Namen "allowed-domain-class" entsprechen sollten. HTTP-Transaktionen, die dieser Klasse entsprechen, werden zurückgesetzt und geschlossen. Im Wesentlichen werden alle HTTP-Transaktionen zurückgesetzt, es sei denn, sie stimmen mit den aufgeführten Domänen überein.
```
class-map type inspect http match-all allowed-domain-class match not request header host
regex class domain-regex-class!policy-map type inspect http regex-filtering-policy
parameters class allowed-domain-class  reset log
```

Anwenden dieser HTTP-Inspektionsrichtlinienzuordnung auf eine HTTP-Überprüfung in modularem Richtlinien-Framework

Nachdem die HTTP Inspection Policy Map als "regex-filter-policy" konfiguriert ist, wenden Sie diese Richtlinienzuordnung auf eine vorhandene HTTP-Inspektion oder eine neue Überprüfung in Modular Policy Framework an. Damit wird die Prüfung beispielsweise der in der globalen Richtlinie konfigurierten Klasse "Inspection_default" hinzugefügt.

```
policy-map global_policy class inspection_default  inspect http regex-filtering-policy
```

Häufige Probleme

Wenn die HTTP Inspection Policy Map und die HTTP-Klassenzuordnung konfiguriert sind, stellen Sie sicher, dass Übereinstimmung oder Übereinstimmung nicht so konfiguriert ist, wie es für das gewünschte Ziel sein sollte. Dies ist ein einfaches Schlüsselwort zum Überspringen und führt zu unbeabsichtigtem Verhalten. Diese Form der Regex-Verarbeitung kann ebenso wie jede erweiterte Paketverarbeitung dazu führen, dass die ASA-CPU-Auslastung steigt und der Durchsatz sinkt. Seien Sie vorsichtig, wenn immer mehr Regex-Muster hinzugefügt werden.