Konfiguration der SNORT_BPF-Variablen in einem Defense Center

Inhalt

Einleitung

Sie können Berkeley Packet Filter (BPF) verwenden, um einen Host oder ein Netzwerk von der Überprüfung durch ein Defense Center auszuschließen. Snort verwendet die Variable **Snort_BPF**, um Datenverkehr aus einer Richtlinie für Sicherheitsrisiken auszuschließen. Dieses Dokument enthält Anweisungen zur Verwendung der Variable **Snort_BPF** in verschiedenen Szenarien.

> **Tipp**: Es wird dringend empfohlen, eine Vertrauensregel in einer Zugriffskontrollrichtlinie zu verwenden, um zu bestimmen, welcher Datenverkehr überprüft wird und nicht, und nicht eine BPF in der Richtlinie für Sicherheitsrisiken. Die Variable **`Snort_BPF`** steht für die Softwareversion 5.2 zur Verfügung und ist für die Softwareversion 5.3 oder höher veraltet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den Bereichen Defense Center, Intrusion Policy, Berkeley Packet Filter und Snort-Regeln verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Hardware- und Software-Versionen:

- Verteidigungszentrum
- Softwareversion 5.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurationsschritte

Um die Variable **Snort_BPF** zu konfigurieren, gehen Sie wie folgt vor:

1. Greifen Sie auf die Web-Benutzeroberfläche Ihres Defense Center zu.
2. Navigieren Sie zu **Policies > Intrusion > Intrusion Policy**.
3. Klicken Sie auf das *Bleistiftsymbol*, um Ihre Richtlinie für Sicherheitsrisiken zu bearbeiten.
4. Klicken Sie **Variablen** aus dem Menü auf der linken Seite.
5. Nach der Konfiguration der Variablen müssen Sie die Änderungen speichern und die Richtlinie für Sicherheitsrisiken erneut anwenden, damit sie wirksam wird.

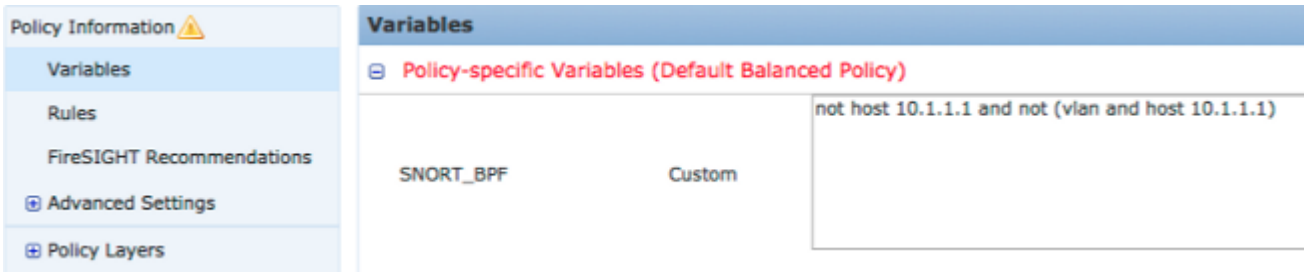

Abbildung: Screenshot der Konfigurationsseite der Variablen Snort_BPF

Konfigurationsbeispiele

Nachstehend finden Sie einige grundlegende Beispiele für Referenzzwecke:

Szenario 1: Ignorieren des gesamten Datenverkehrs, VON und AN einem Scanner mit Sicherheitslücken

1. Wir haben einen Scanner für Sicherheitslücken an der IP-Adresse 10.1.1.1
2. Wir möchten den gesamten Datenverkehr VOM und ZUM Scanner ignorieren.
3. Datenverkehr darf kein 802.1q (VLAN)-Tag haben

Der **SNORT_BPF** ist:

```
not host 10.1.1.1 and not (vlan and host 10.1.1.1)
```

VERGLEICH: Datenverkehr *ist nicht* VLAN-markiert, aber Punkt 1 und 2 bleiben wahr wäre:

```
not host 10.1.1.1
```
In einfachem Englisch würde dies den Datenverkehr ignorieren, bei dem einer der Endpunkte 10.1.1.1 (der Scanner) ist.

Szenario 2: Ignorieren des gesamten Datenverkehrs, VON und AUF zwei Schwachstellen-Scannern

1. Wir haben einen Scanner für Sicherheitslücken an der IP-Adresse 10.1.1.1
2. Wir haben einen zweiten Scanner für Sicherheitslücken an der IP-Adresse 10.2.1.1
3. Wir möchten den gesamten Datenverkehr VOM und ZUM Scanner ignorieren.
4. Datenverkehr darf kein 802.11 (VLAN)-Tag haben

Der **SNORT_BPF** ist:

```
not (host 10.1.1.1 or host 10.2.1.1) and not (vlan and (host 10.1.1.1 or host 10.2.1.1))
```
Vergleich: Datenverkehr *ist nicht* VLAN-markiert, aber Punkt 1 und 2 bleiben wahr wäre:
```
not (host 10.1.1.1 or host 10.2.1.1)
```
Zusammenfassend lässt sich sagen, dass dabei der Datenverkehr ignoriert wird, wenn einer der Endpunkte 10.1.1.1 ODER 10.2.1.1 ist.

> **Hinweis**: Das VLAN-Tag sollte in fast allen Fällen nur einmal in einer bestimmten BPF vorkommen. Sie sollten es nur mehrmals sehen, wenn Ihr Netzwerk geschachteltes VLAN Tagging verwendet (manchmal auch als "QinQ" bezeichnet).

Szenario 3: Ignorieren von VLAN-markiertem Datenverkehr, ZU und AUS zwei Schwachstellen-Scannern

1. Wir haben einen Scanner für Sicherheitslücken an der IP-Adresse 10.1.1.1
2. Wir haben einen zweiten Scanner für Sicherheitslücken an der IP-Adresse 10.2.1.1
3. Wir möchten den gesamten Datenverkehr VOM und ZUM Scanner ignorieren.
4. Der Datenverkehr ist mit 802.11 (VLAN) markiert, und Sie möchten ein bestimmtes (VLAN)-Tag verwenden, wie in VLAN 101.

Der **SNORT_BPF** ist:

```
not (host 10.1.1.1 or host 10.2.1.1) and not (vlan 101 and (10.1.1.1 or host 10.2.1.1))
```

Szenario 4: Datenverkehr von einem Backup-Server ignorieren

1. Wir haben einen Netzwerk-Backup-Server mit der IP-Adresse 10.1.1.1
2. Computer im Netzwerk werden mit diesem Server an Port 8080 verbunden, um das nächtliche Backup auszuführen.
3. Wir möchten diesen Backup-Datenverkehr ignorieren, da er verschlüsselt ist und hohe Datenvolumen aufweist.

Der SNORT_BPF ist:

```
not (dst host 10.1.1.1 and dst port 8080) and not (vlan and (dst host 10.1.1.1
and dst port 8080))
```

Vergleich: Datenverkehr *ist nicht* VLAN-markiert, aber Punkt 1 und 2 bleiben wahr wäre:

```
not (dst host 10.1.1.1 and dst port 8080)
```

Übersetzt bedeutet dies, dass der Datenverkehr zu 10.1.1.1 (unserem hypothetischen Backup-Server) an Port 8080 (Überwachungsport) nicht von der IPS-Erkennungs-Engine überprüft werden sollte.

Es ist auch möglich, net anstelle von host zu verwenden, um einen Netzwerkblock anstelle eines einzelnen Hosts anzugeben. Beispiele:

```
not net 10.1.1.0/24
```

Im Allgemeinen empfiehlt es sich, die BPF so spezifisch wie möglich zu gestalten, wobei der auszuschließende Datenverkehr von der Überprüfung ausgenommen wird, jedoch nicht der unzusammenhängende Datenverkehr, der Exploit-Versuche enthalten könnte.

Szenario 5: Zur Verwendung von Netzwerkbereichen anstelle von einzelnen Hosts

Sie können Netzwerkbereiche in der BPF-Variablen und nicht in Hosts angeben, um die Länge der Variablen zu verkürzen. Dazu verwenden Sie das net-Schlüsselwort anstelle von host und geben einen CIDR-Bereich an. Hier ein Beispiel:

```
not (dst net 10.8.0.0/16 and dst port 8080) and not (vlan and (dst net 10.8.0.0/16
and dst port 8080))
```

> Hinweis: Stellen Sie sicher, dass Sie die Netzwerkadresse in der CIDR-Schreibweise und mit einer verwendbaren Adresse innerhalb des CIDR-Blockadressbereichs eingeben. Verwenden Sie beispielsweise net 10.8.0.0/16 anstelle von net 10.8.2.16/16.

Die Fehlermeldung **SNORT_BPF** -Variable verwendet wird, um zu verhindern, dass bestimmter Datenverkehr von einer IPS-Erkennungs-Engine überprüft wird, häufig aus Leistungsgründen. Diese Variable verwendet das Berkeley Pack Filters (BPF)-Standardformat. Datenverkehr entspricht dem **SNORT_BPF** -Variable überprüft werden; während der Verkehr NICHT mit der **SNORT_BPF** -Variable wird NICHT von der IPS-Erkennungs-Engine überprüft.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.