在防禦中心上配置SNORT_BPF變數

目錄

簡介

您可以使用Berkeley資料包過濾器(BPF)排除由防禦中心檢查的主機或網路。Snort使用Snort_BPF變數從入侵策略中排除流量。本文提供如何在各種方案中使用Snort_BPF變數的說明。

> **提示**：強烈建議在訪問控制策略中使用信任規則來確定哪些流量是經過檢查的和不被檢查的，而不是入侵策略中的BPF。`Snort_BPF`變數在軟體版本5.2中可用，而在軟體版本5.3或更高版本中不再使用。

必要條件

需求

思科建議您瞭解防禦中心、入侵策略、Berkeley Packet Filter和Snort規則。

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

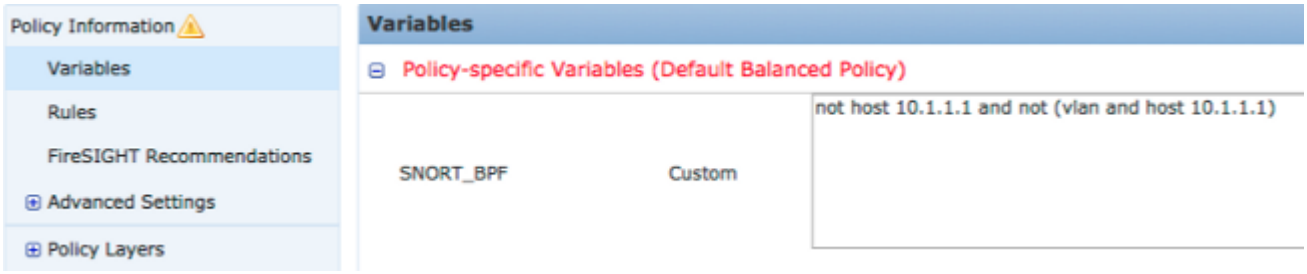
- 防禦中心
- 軟體版本5.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

配置步驟

要配置 Snort_BPF變數，請執行以下步驟：

1. 訪問您的防禦中心的Web使用者介面。
2. 導航到**Policies > Intrusion > Intrusion Policy**。
3. 按一下*pencil*圖示編輯入侵策略。
4. 按一下 **變數** 從左邊的選單。
5. 配置變數後，您需要儲存更改並重新應用入侵策略，以使更改生效。



圖：Snort_BPF變數配置頁的螢幕快照

組態範例

下面提供一些基本示例供參考：

場景1：忽略所有流量，包括傳入和傳出漏洞掃描器

1. IP地址為10.1.1.1的漏洞掃描程式
2. 我們要忽略所有進出掃描器的流量
3. 流量可能具有802.1q(vlan)標籤，也可能沒有

SNORT_BPF為：

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

比較：流量*不是* VLAN標籤，但點1和點2保持為真將是：

```
not host 10.1.1.1
```

簡單地說，這將忽略其中一個端點為10.1.1.1（掃描器）的流量。

案例 2: 忽略所有流量，即兩個漏洞掃描器的TO和FROM

1. IP地址為10.1.1.1的漏洞掃描程式
2. IP地址為10.2.1.1的第二個漏洞掃描程式

3. 我們要忽略所有進出掃描器的流量
4. 流量可能具有802.11(vlan)標籤，也可能沒有

SNORT_BPF為：

```
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))
```

比較：流量*不是* VLAN標籤，但點1和點2保持為真將是：

```
not (host 10.1.1.1 or host 10.2.1.1)
```

總而言之，這會忽略其中有一個端點為10.1.1.1或10.2.1.1的流量。

> **注意**:必須注意的是，幾乎在所有情況下，VLAN標籤都應在給定BPF中僅出現一次。您只能多次看到它，即您的網路使用巢狀的VLAN標籤（有時稱為「QinQ」）。

案例 3: 忽略VLAN標籤的流量、往返兩個漏洞掃描器

1. IP地址為10.1.1.1的漏洞掃描程式
2. IP地址為10.2.1.1的第二個漏洞掃描程式
3. 我們要忽略所有進出掃描器的流量
4. 流量已標籤802.11(vlan)，並且您希望使用特定(vlan)標籤，如vlan 101

SNORT_BPF為：

```
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))
```

場景4：忽略來自備份伺服器的流量

1. IP地址為10.1.1.1的網路備份伺服器
2. 網路上的電腦連線到埠8080上的此伺服器以運行其夜間備份
3. 由於此備份流量是加密且高容量的，因此我們希望將其忽略

SNORT_BPF為：

```
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))
```

比較：流量*不是* VLAN標籤，但點1和點2保持為真將是：

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

換句話說，這意味著IPS檢測引擎不應檢查埠8080（偵聽埠）上到10.1.1.1（我們假設的備份伺服器）的流量。

也可以使用net代替主機來指定網路塊，而不是單個主機。 例如：

```
not net 10.1.1.0/24
```

一般來說，最好使BPF儘可能具體；將需要排除的流量從檢測中排除，但不排除可能包含利用漏洞企圖的任何不相關流量。

案例5：用於使用網路範圍而不是單個主機

您可以在BPF變數中指定網路範圍而不是主機，以縮短變數的長度。為此，您將使用net關鍵字代替主機並指定CIDR範圍。以下是範例：

```
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))
```

> **註**:請確保使用CIDR標籤輸入網路地址，並在CIDR塊地址空間中輸入可用地址。例如，使用net 10.8.0.0/16 而不是net 10.8.2.16/16。

其 **SNORT_BPF** 變數用於防止IPS檢測引擎檢查某些流量；通常是出於效能原因。此變數使用標準的Berkeley Pack Filters(BPF)格式。與 **SNORT_BPF** 將檢查變數；當流量與 **SNORT_BPF** ips檢測引擎不會檢查變數。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。