SNORT_BPF变量的配置在防御中心的

Contents

Introduction

您能使用伯克利信息包过滤器(BPF)从检查屏蔽主机或网络由防御中心。喷鼻息使用**Snort_BPF**变量从闯入策略排除数据流。本文提供指令关于怎样在各种情况下使用**Snort_BPF**变量。

> **提示**：在访问控制策略强烈建议使用信任规则确定什么数据流是和没有检查，而不是在闯入策略的BPF。**Snort_BPF**变量是可用的在软件版本5.2和贬抑在软件版本5.3或更高。

Prerequisites

Requirements

Cisco建议您有在防御中心、闯入策略，伯克利信息包过滤器和喷鼻息规则的知识。

Components Used

本文档中的信息基于下列硬件和软件版本：

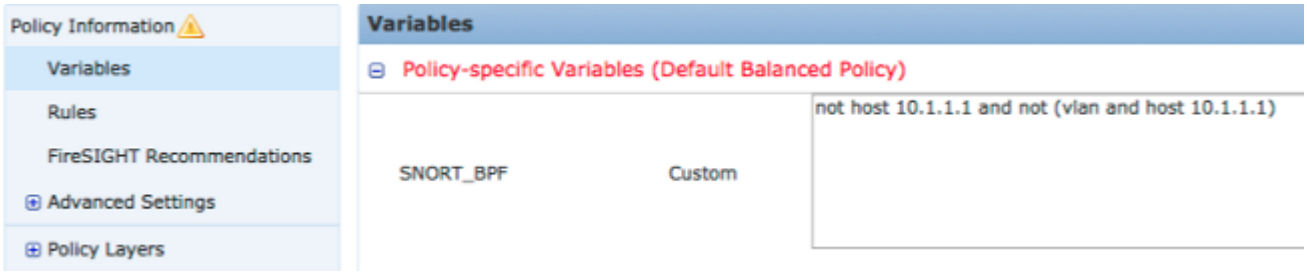
- 防御中心
- 软件版本5.2

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Configuration Steps

为了配置 **Snort_BPF**变量，请遵从下面步骤：

1. 访问您的防御中心网页用户界面。
2. 连接对**策略>闯入>闯入策略**。
3. 点击*铅笔*图标编辑您的闯入策略。
4. 点击从菜单的**变量**在左边。
5. 一旦配置变量，您将需要保存更改，并且重新应用您的它的闯入策略能生效。



图：Snort_BPF可变的配置页的屏幕画面

配置示例

一些基本示例下面提供供参考：

情形 1：到/从弱点扫描程序忽略所有数据流，

1. 我们有弱点扫描程序在IP地址10.1.1.1
2. 我们要到/从扫描程序忽略所有数据流
3. 数据流可能或可能没有802.1q (VLAN)标记

SNORT_BPF是：

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

比较：数据流VLAN标记的*is的not*，但是点1和2依然是真是：

```
not host 10.1.1.1
```

用浅显的英语，这将忽略其中一个终端是10.1.1.1的数据流(扫描程序)。

方案 2：到/从两个弱点扫描程序忽略所有数据流，

1. 我们有弱点扫描程序在IP地址10.1.1.1
2. 我们有第二个漏洞扫描程序在IP地址10.2.1.1

3. 我们要到/从扫描程序忽略所有数据流
4. 数据流可能或可能没有802.11 (VLAN)标记

SNORT_BPF是：

```
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))
```

比较：数据流VLAN标记的*is的not*，但是点1和2依然是真是：

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

总之，这将忽略其中一个终端是10.1.1.1或10.2.1.1的数据流。

> Note:请注意VLAN标记在特定BPF应该只一次，在任何情况下，发生。唯一的时代您应该不止一次看到它，是，如果您的网络使用使VLAN标记套入(有时指'QinQ')。

情形 3：到/从两个弱点扫描程序忽略VLAN标记的数据流，

1. 我们有弱点扫描程序在IP地址10.1.1.1
2. 我们有第二个漏洞扫描程序在IP地址10.2.1.1
3. 我们要到/从扫描程序忽略所有数据流
4. 数据流是标记为的802.11 (VLAN)，并且您在VLAN 101希望使用特定(VLAN)标记，正如

SNORT_BPF是：

```
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))
```

场景 4：从备份服务器的忽略数据流

1. 我们有网络备份服务器在IP地址10.1.1.1
2. 在网络的机器连接到在端口8080的此服务器运行他们每夜的备份
3. 因为是被加密和大容积的，我们希望忽略此备份的数据流

SNORT_BPF是：

```
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))
```

比较：数据流VLAN标记的*is的not*，但是点1和2依然是真是：

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

转换，这意味着不应该由IPS检测引擎检查对10.1.1.1 (我们的假定备份服务器)的数据流在端口8080 (监听端口)。

在使用指定网络地址块，而不是单个主机也是可能的。 例如：

```
not net 10.1.1.0/24
```

一般来说，它是尽可能具体地做BPF的好习惯;除了需要被排除从检查的数据流，当不除了也许包含检测安全漏洞代码尝试的任何无关的数据流时。

场景 5：为使用网络范围而不是单个主机

您在BPF变量能指定网络范围而不是主机缩短变量的长度。如此要执行您在主机位置将使用关键字并且指定CIDR范围。下面示例：

```
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))
```

> Note:请保证您输入网络地址使用CIDR表示和在CIDR块地址空间内的可用的地址。例如请使用净10.8.0.0/16而不是网10.8.2.16/16。

SNORT_BPF变量用于为了防止某一数据流检查由IPS检测引擎;经常由于性能上的原因。此变量使用标准的伯克利装箱过滤器(BPF)格式。匹配**SNORT_BPF**变量的数据流将被检查;当不匹配的数据流**SNORT_BPF**变量不会由IPS检测引擎时检查。