在防御中心上配置SNORT_BPF变量

目录

简介

您可以使用Berkeley数据包过滤器(BPF)将主机或网络排除在防御中心检查范围之外。Snort使用Snort_BPF变量从入侵策略中排除流量。本文档提供有关如何在各种场景中使用Snort_BPF变量的说明。

> **提示**：强烈建议在访问控制策略中使用信任规则来确定要检查和不检查的流量，而不是入侵策略中的BPF。`Snort_BPF`变量在软件版本5.2上可用，在软件版本5.3或更高版本上已弃用。

先决条件

要求

Cisco建议您了解防御中心、入侵策略、Berkeley数据包过滤器和Snort规则。

使用的组件

本文档中的信息基于下列硬件和软件版本：

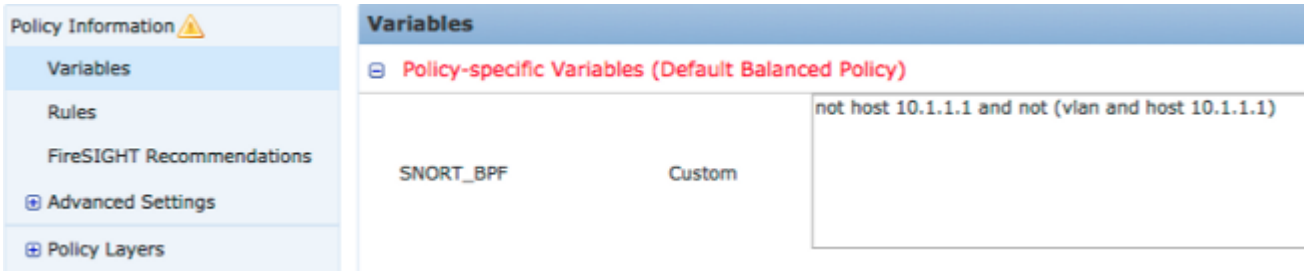
- 防御中心
- 软件版本 5.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置步骤

要配置 Snort_BPF变量，请执行以下步骤：

1. 访问防御中心的网络用户界面。
2. 导航到**Policies > Intrusion > Intrusion Policy**。
3. 单击*铅笔*图标编辑入侵策略。
4. 点击 **变量** 从左边的菜单打开。
5. 配置变量后，您需要保存更改并重新应用入侵策略以使其生效。



图：Snort_BPF变量配置页面的截图

配置示例

下面提供了一些基本示例以供参考：

场景1：忽略所有流量、流向和来自漏洞扫描器

1. IP地址为10.1.1.1的漏洞扫描程序
2. 我们要忽略所有进出扫描仪的流量
3. 流量可能有，也可能没有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：流量*不是* VLAN标记，但点1和点2保持正确将是：

```
not host 10.1.1.1
```

用简明语言，这将忽略其中一个终端为10.1.1.1（扫描仪）的流量。

方案 2： 忽略所有流量、流向和来自两个漏洞扫描器

1. IP地址为10.1.1.1的漏洞扫描程序
2. IP地址为10.2.1.1的第二个漏洞扫描程序

3. 我们要忽略所有进出扫描仪的流量
4. 流量可能有，也可能没有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：流量*不是* VLAN标记，但点1和点2保持为真的情况将是：

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

总之，这将忽略其中一个终端为10.1.1.1或10.2.1.1的流量。

注意:必须注意，几乎在所有情况下，vlan标记都应在给定BPF中仅出现一次。您唯一应该多次看到它的情况是，您的网络使用嵌套的VLAN标记（有时称为“QinQ”）。

情形 3： 忽略VLAN标记流量、TO和FROM两个漏洞扫描器

1. IP地址为10.1.1.1的漏洞扫描程序
2. IP地址为10.2.1.1的第二个漏洞扫描程序
3. 我们要忽略所有进出扫描仪的流量
4. 流量标记为802.11(vlan)，您希望使用特定(vlan)标记，如vlan 101

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：忽略来自备份服务器的流量

1. IP地址为10.1.1.1的网络备份服务器
2. 网络上的计算机通过端口8080连接到此服务器以运行其夜间备份
3. 我们希望忽略此备份流量，因为它已加密且流量大

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：流量*不是* VLAN标记，但点1和点2保持为真的情况将是：

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

转换后，这意味着端口8080（侦听端口）上到10.1.1.1（我们假设的备份服务器）的流量不应由IPS检测引擎进行检测。

也可以使用net代替主机来指定网络块，而不是单个主机。 例如：

```
not net 10.1.1.0/24
```

一般而言，最好使BPF尽可能具体；将流量从需要排除的检查中排除，但不排除任何可能包含漏洞攻击尝试的不相关流量。

场景5：用于使用网络范围而不是单个主机

您可以在BPF变量中指定网络范围而不是主机，以缩短变量的长度。为此，您将使用net关键字代替主机并指定CIDR范围。下面是一个示例：

```
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))
```

> **注**:请确保使用CIDR表示法输入网络地址，并在CIDR块地址空间中输入可用地址。例如，使用net 10.8.0.0/16 而不是net 10.8.2.16/16。

此 **SNORT_BPF** 使用变量是为了防止IPS检测引擎检查某些流量；通常是为了性能原因。此变量使用标准的Berkeley Pack Filters(BPF)格式。匹配的 **SNORT_BPF** 将检查变量；而流量与流量不匹配 **SNORT_BPF** ips检测引擎不会检查变量。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。