Configuration of SNORT_BPF variable on a Defense Center

Document ID: 118090

Contributed by Nazmul Rajib, Jeremy Weiss, Cisco TAC Engineers.

Jul 25, 2014

Contents

Introduction

You can use Berkeley Packet Filter (BPF) to exclude a host or network from being inspected by a Defense Center. Snort uses ***Snort_BPF*** variable to exclude traffic from an intrusion policy. This document provides instructions on how to use ***Snort_BPF*** variable in various scenarios.

Tip: It is strongly recommended to use a trust rule in an Access Control policy to determine what traffic is and is not inspected, rather than a BPF in the intrusion policy. The ***Snort_BPF*** variable is available on software version 5.2, and is deprecated on software version 5.3 or higher.

Prerequisites

Requirements

Cisco recommends that you have knowledge on Defense Center, Intrusion Policy, Berkeley Packet Filter, and Snort rules.

Components Used

The information in this document is based on these hardware and software versions:

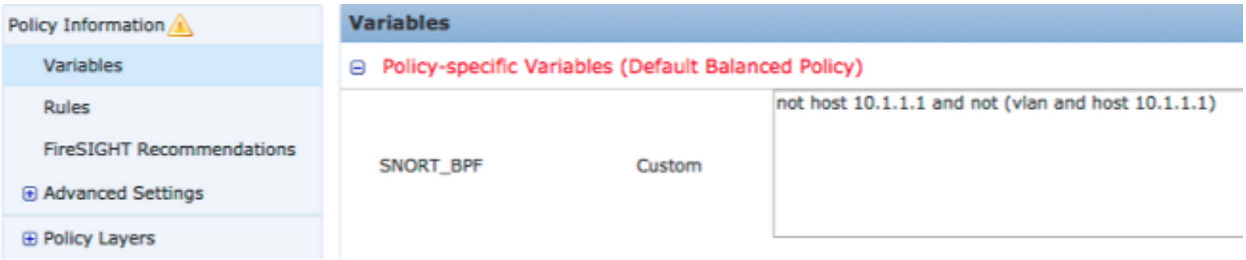
- Defense Center
- Software Version 5.2

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

In order to configure ***Snort_BPF*** variable, follow the steps below:

1. Access the web user interface of your Defense Center.
2. Navigate to ***Policies*** > ***Intrusion*** > ***Intrusion Policy***.
3. Click the *pencil* icon to edit your intrusion policy.
4. Click on ***Variables*** from the menu on the left.
5. Once the variables are configured, you will need to save changes, and reapply your intrusion policy for it to take effect.


Policy Information
Variables
Rules
FireSIGHT Recommendations
Advanced Settings
Policy Layers
Variables
Policy-specific Variables (Default Balanced Policy)

SNORT_BPF Custom not host 10.1.1.1 and not (vlan and host 10.1.1.1)

Figure: Screenshot of the Snort_BPF variable configuration page

Configuration Examples

Some basic examples are provided below for reference:

Scenario 1: Ignore all traffic, TO and FROM a vulnerability scanner

1. We have a vulnerability scanner at IP address 10.1.1.1
2. We want to ignore all traffic TO and FROM the scanner
3. Traffic may or may not have an 802.1q (vlan) tag

The ***SNORT_BPF*** is:

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

COMPARISON: traffic *is not* VLAN−tagged, but points 1 and 2 remain true would be:

```
not host 10.1.1.1
```

In plain english, this would ignore traffic where one of the endpoints is 10.1.1.1 (the scanner).

Scenario 2: Ignore all traffic, TO and FROM two vulnerability scanners

1. We have a vulnerability scanner at IP address 10.1.1.1
2. We have a second vulnerability scanner at IP address 10.2.1.1
3. We want to ignore all traffic TO and FROM the scanner
4. Traffic may or may not have an 802.11 (vlan) tag

The ***SNORT_BPF*** is:

```
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))
```

Comparison: Traffic *is not* VLAN−tagged, but points 1 and 2 remain true would be:

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

In summary, this would ignore traffic where one of the endpoints is 10.1.1.1 OR 10.2.1.1.

Note: It is important to note that the vlan tag should, in almost all cases, occur only once in a given BPF. The only times you should see it more than once, is if your network uses nested VLAN tagging (sometimes referred to as 'QinQ').

Scenario 3: Ignore VLAN tagged traffic, TO and FROM two vulnerability scanners

1. We have a vulnerability scanner at IP address 10.1.1.1
2. We have a second vulnerability scanner at IP address 10.2.1.1
3. We want to ignore all traffic TO and FROM the scanner
4. Traffic is 802.11 (vlan) tagged, and you wish to use a specific (vlan) tag, as in vlan 101

The ***SNORT_BPF*** is:

```
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))
```

Scenario 4: Ignore traffic from a backup server

1. We have a network backup server at IP address 10.1.1.1
2. Machines on the network connect to this server on port 8080 to run their nightly backup
3. We wish to ignore this backup traffic, as it is encrypted and high−volume

The ***SNORT_BPF*** is:

```
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))
```

Comparison: Traffic *is not* VLAN−tagged, but points 1 and 2 remain true would be:

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

Translated, this means that traffic to 10.1.1.1 (our hypothetical backup server) on port 8080 (listening port) should not be inspected by the IPS detection engine.

It is also possible to use net in the place of host to specify a network block, rather than a single host. For example:

```
not net 10.1.1.0/24
```

In general, it is a good practice to make the BPF as specific as possible; excluding the traffic from inspection that needs to be excluded, while not excluding any unrelated traffic which might contain exploit attempts.

Scenario 5: For using network ranges rather than individual hosts

You can specify network ranges in the BPF variable rather than hosts to shorten the length of the variable. To do so you will use the net keyword in place of host and specify a CIDR range. Below is an example:

```
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: Please ensure that you enter the network address using CIDR notation and a usable address within the CIDR block address space. For example use net 10.8.0.0/16 rather than net 10.8.2.16/16.

The ***SNORT_BPF*** variable is used in order to prevent certain traffic from being inspected by an IPS detection engine; often for performance reasons. This variable uses the standard Berkeley Pack Filters (BPF) format. Traffic matching the ***SNORT_BPF*** variable will be inspected; while traffic NOT matching the ***SNORT_BPF*** variable will NOT be inspected by the IPS detection engine.

Updated: Jul 25, 2014 Document ID: 118090