Configuration de la variable SNORT_BPF sur un centre de défense

Table des matières

Introduction

Vous pouvez utiliser le filtre de paquets Berkeley (BPF) pour empêcher un hôte ou un réseau d'être inspecté par un centre de défense. Snort utilise la variable **Snort_BPF** pour exclure le trafic d'une politique d'intrusion. Ce document fournit des instructions sur la façon d'utiliser la variable **Snort_BPF** dans divers scénarios.

> **Conseil** : il est fortement recommandé d'utiliser une règle d'approbation dans une politique de contrôle d'accès pour déterminer quel trafic est et n'est pas inspecté, plutôt qu'un BPF dans la politique d'intrusion. La variable **`Snort_BPF`** est disponible sur le logiciel version 5.2, et est déconseillée sur le logiciel version 5.3 ou ultérieure.

Conditions préalables

Exigences

Cisco recommande que vous ayez des connaissances sur Defense Center, Intrusion Policy, Berkeley Packet Filter et les règles Snort.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Centre De Défense
- Logiciel 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

Afin de configurer la variable **Snort_BPF**, suivez les étapes ci-dessous :

1. Accédez à l'interface utilisateur Web de votre Centre de défense.
2. Accédez à **Politiques > Intrusion > Politique d'intrusion**.
3. Cliquez sur l'icône *crayon* pour modifier votre stratégie d'intrusion.
4. Cliquez sur **Variables** dans le menu de gauche.
5. Une fois les variables configurées, vous devrez enregistrer les modifications et réappliquer votre stratégie d'intrusion pour qu'elle prenne effet.

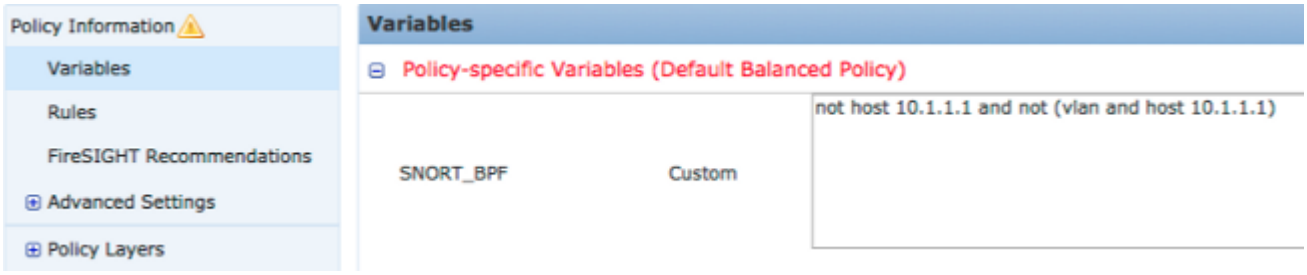

Figure : Capture d'écran de la page de configuration de la variable Snort_BPF

Exemples de configuration

Voici quelques exemples de base à titre de référence :

Scénario 1 : Ignorer tout le trafic, à destination et en provenance d'un analyseur de vulnérabilité

1. Nous avons un analyseur de vulnérabilité à l'adresse IP 10.1.1.1
2. Nous voulons ignorer tout le trafic en provenance et à destination du scanner
3. Le trafic peut avoir ou non une étiquette 802.1q (vlan)

Le **SNORT_BPF** est :

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

COMPARAISON : le trafic *n'est pas* étiqueté VLAN, mais les points 1 et 2 restent vrais :

```
not host 10.1.1.1
```

En anglais courant, cela ignorerait le trafic où l'un des points d'extrémité est 10.1.1.1 (l'analyseur).

Scénario 2 : Ignorez tout le trafic, à destination et en provenance de deux scanners de vulnérabilité

1. Nous avons un analyseur de vulnérabilité à l'adresse IP 10.1.1.1
2. Nous avons un deuxième analyseur de vulnérabilité à l'adresse IP 10.2.1.1
3. Nous voulons ignorer tout le trafic en provenance et à destination du scanner
4. Le trafic peut avoir ou non une balise 802.11 (vlan)

Le **SNORT_BPF** est :

```
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))
```

Comparaison : le trafic *n'est pas* étiqueté VLAN, mais les points 1 et 2 restent vrais :

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

En résumé, ceci ignorerait le trafic où l'un des points d'extrémité est 10.1.1.1 OU 10.2.1.1.

> **Remarque** : il est important de noter que la balise vlan ne doit, dans presque tous les cas, se produire qu'une seule fois dans un BPF donné. Les seules fois où vous devriez le voir plus d'une fois, c'est si votre réseau utilise l'étiquetage VLAN imbriqué (parfois appelé 'QinQ').

Scénario 3 : Ignorer le trafic étiqueté VLAN, À et DE deux analyseurs de vulnérabilité

1. Nous avons un analyseur de vulnérabilité à l'adresse IP 10.1.1.1
2. Nous avons un deuxième analyseur de vulnérabilité à l'adresse IP 10.2.1.1
3. Nous voulons ignorer tout le trafic en provenance et à destination du scanner
4. Le trafic est étiqueté 802.11 (vlan) et vous souhaitez utiliser une étiquette spécifique (vlan), comme dans le vlan 101

Le **SNORT_BPF** est :

```
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))
```

Scénario 4 : ignorer le trafic provenant d'un serveur de sauvegarde

1. Nous avons un serveur de sauvegarde réseau à l'adresse IP 10.1.1.1
2. Les ordinateurs du réseau se connectent à ce serveur sur le port 8080 pour exécuter leur sauvegarde de nuit

3. Nous souhaitons ignorer ce trafic de sauvegarde, car il est chiffré et volumineux

Le SNORT_BPF est :

```
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))
```

Comparaison : le trafic *n'est pas* étiqueté VLAN, mais les points 1 et 2 restent vrais :

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

Traduit, cela signifie que le trafic vers 10.1.1.1 (notre hypothétique serveur de sauvegarde) sur le port 8080 (port d'écoute) ne doit pas être inspecté par le moteur de détection IPS.

Il est également possible d'utiliser net à la place de host pour spécifier un bloc réseau, plutôt qu'un hôte unique. Exemple :

```
not net 10.1.1.0/24
```

En règle générale, il est recommandé de rendre le protocole BPF aussi spécifique que possible, en excluant le trafic de l'inspection qui doit être exclue, sans exclure tout trafic non lié susceptible de contenir des tentatives d'exploitation.

Scénario 5 : utilisation de plages réseau plutôt que d'hôtes individuels

Vous pouvez spécifier des plages réseau dans la variable BPF plutôt que des hôtes pour réduire la longueur de la variable. Pour ce faire, vous utiliserez le mot clé net à la place de host et spécifierez une plage CIDR. En voici un exemple :

```
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))
```

> Remarque : assurez-vous que vous entrez l'adresse réseau en utilisant la notation CIDR et une adresse utilisable dans l'espace d'adressage de bloc CIDR. Par exemple, utilisez net 10.8.0.0/16 plutôt que net 10.8.2.16/16.

Les **SNORT_BPF** est utilisée afin d'empêcher que certains trafics soient inspectés par un moteur de détection IPS ; souvent pour des raisons de performances. Cette variable utilise le format standard BPF (Berkeley Pack Filters). Trafic correspondant à la **SNORT_BPF** sera inspectée ; tandis que le trafic NE correspond PAS à la **SNORT_BPF** ne sera PAS inspectée par le moteur de détection IPS.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.