Configuration de variable SNORT_BPF à un centre de la défense

Contenu

Introduction

Vous pouvez utiliser le filtre de paquet de Berkeley (BPF) pour exclure un hôte ou un réseau d'être examiné par un centre de la défense. Reniflez la variable de **`Snort_BPF d'`** utilisations pour exclure le trafic d'une stratégie d'intrusion. Ce document fournit des instructions sur la façon dont utiliser la variable de **`Snort_BPF`** dans divers scénarios.

> **Conseil** : Il est fortement recommandé pour utiliser une règle de confiance dans une stratégie de contrôle d'accès de déterminer quel trafic est et n'est pas examiné, plutôt qu'un BPF dans la stratégie d'intrusion. La variable de **`Snort_BPF`** est disponible sur la version de logiciel 5.2, et est désapprouvée sur la version de logiciel 5.3 ou plus élevé.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance au centre de la défense, stratégie d'intrusion, filtre de paquet de Berkeley, et renifliez des règles.

Composants utilisés

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

logiciel suivantes :

- Centre de la défense
- Version de logiciel 5.2

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Étapes de configuration

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

1. Accédez à l'interface utilisateur d'utilisateur web de votre centre de la défense.
2. Naviguez vers des **stratégies > l'intrusion > la stratégie d'intrusion**.
3. Cliquez sur l'icône de *crayon* pour éditer votre stratégie d'intrusion.
4. Cliquez sur en fonction les **variables du** menu du côté gauche.
5. Une fois que les variables sont configurées, vous devrez sauvegarder des modifications, et réappliquez votre stratégie d'intrusion pour elle pour prendre effet.

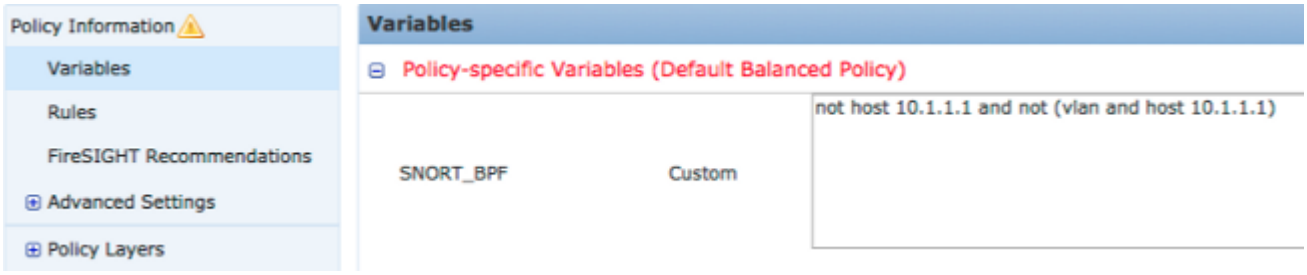

Figure : Tir d'écran de la page variable de configuration de Snort_BPF

Exemples de configuration

Quelques exemples de base sont donnés ci-dessous pour la référence :

Scénario 1 : Ignorez tout le trafic, à et d'un scanner de vulnérabilité

1. Nous avons un scanner de vulnérabilité à l'adresse IP 10.1.1.1
2. Nous voulons ignorer tout le trafic à et du scanner
3. Le trafic peut ou peut ne pas avoir une balise de 802.1Q (VLAN)

`Le SNORT_BPF` est :
`not host 10.1.1.1 and not (vlan and host 10.1.1.1)`COMPARAISON : trafiquez le not* de *is VLAN-étiqueté, mais les points 1 et 2 demeurent vrais seraient : **`not host 10.1.1.1`**En termes clairs, ceci ignorerait le trafic où un des points finaux est 10.1.1.1 (le scanner).

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

1. Nous avons un scanner de vulnérabilité à l'adresse IP 10.1.1.1
2. Nous avons un deuxième scanner de vulnérabilité à l'adresse IP 10.2.1.1
3. Nous voulons ignorer tout le trafic à et du scanner
4. Le trafic peut ou peut ne pas avoir une balise de 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 :** Trafiquez le not* de *is VLAN-étiqueté, mais les points 1 et 2 demeurent vrais seraient : `not (host 10.1.1.1 or host 10.2.1.1)`En résumé, ceci ignorerait le trafic où un des points finaux est 10.1.1.1 OU 10.2.1.1.

> Remarque: Il est important de noter que la balise de VLAN devrait, dans des presque tous les cas, se produire seulement une fois dans un BPF donné. Les seuls temps vous devriez le voir plus d'une fois, est si votre réseau utilise l'étiquetage imbriqué VLAN (parfois désigné sous le nom de « QinQ ").

Scénario 3 : Ignorez le trafic étiqueté par VLAN, à et de deux scanners de vulnérabilité

1. Nous avons un scanner de vulnérabilité à l'adresse IP 10.1.1.1
2. Nous avons un deuxième scanner de vulnérabilité à l'adresse IP 10.2.1.1
3. Nous voulons ignorer tout le trafic à et du scanner
4. Le trafic est 802.11 (VLAN) étiqueté, et vous souhaitez utiliser une balise spécifique (de 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 : Ignorez le trafic d'un serveur de sauvegarde

1. Nous avons un serveur de sauvegarde de réseau à l'adresse IP 10.1.1.1
2. Les ordinateurs sur le réseau se connectent à ce serveur sur le port 8080 pour exécuter leur sauvegarde nocturne
3. Nous souhaitons ignorer ce trafic de sauvegarde, car il est chiffré et à fort débit

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 : Trafiquez le not* de *is VLAN-étiqueté, mais les points 1 et 2 demeurent vrais seraient : **not (dst host 10.1.1.1 and dst port 8080)**
Traduit, ceci signifie que ce trafic à 10.1.1.1 (notre serveur de sauvegarde hypothétique) sur le port 8080 (port en mode écoute) ne devrait pas être examiné par l'engine de détection IPS.

Il est également possible d'employer le `net` au lieu de l'`hôte` pour spécifier un bloc de réseau, plutôt qu'un seul hôte. Exemple :

not net 10.1.1.0/24
Généralement l'il est conseillé de font le BPF aussi précis que possible ; à l'exclusion du trafic de l'inspection qui doit être exclue, tandis que pas à l'exclusion de tout trafic indépendant qui pourrait contenir des tentatives d'exploit.

Scénario 5 : Pour l'usage le réseau s'étend plutôt que différents hôtes

Vous pouvez spécifier des plages de réseau dans la variable BPF plutôt que des hôtes pour raccourcir la longueur de la variable. Pour vous faire ainsi utilisera le mot clé `net` au lieu de l'hôte et spécifiera une plage CIDR. Est ci-dessous 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: Veuillez s'assurer que vous introduisez l'adresse réseau utilisant la notation CIDR et une adresse utilisable dans l'espace d'adressage de bloc CIDR. Par exemple net 10.8.0.0/16 d'utilisation plutôt que le net 10.8.2.16/16.

La variable **SNORT_BPF** est utilisée afin d'empêcher certain trafic d'être examiné par une engine de détection IPS ; souvent pour des raisons de performances. Cette variable utilise le format standard des filtres de paquet de Berkeley (BPF). Le trafic appariant la variable **SNORT_BPF** sera examiné ; tandis que le trafic n'appariant pas la variable **SNORT_BPF** ne sera pas examiné par l'engine de détection IPS.