Configuración de la variable SNORT_BPF en un centro de defensa

Contenido

Introducción

Puede utilizar el filtro de paquetes de Berkeley (BPF) para excluir un host o una red de la inspección de un centro de defensa. Snort utiliza la variable **Snort_BPF** para excluir el tráfico de una política de intrusiones. Este documento proporciona instrucciones sobre cómo utilizar la variable **Snort_BPF** en varios escenarios.

> **Sugerencia**: se recomienda encarecidamente utilizar una regla de confianza en una directiva de control de acceso para determinar qué tráfico se inspecciona y qué tráfico no, en lugar de un BPF en la directiva de intrusiones. La variable **`Snort_BPF`** está disponible en la versión 5.2 del software y ha quedado obsoleta en la versión 5.3 o superior del software.

Prerequisites

Requirements

Cisco recomienda tener conocimientos sobre el Centro de defensa, la política de intrusiones, el filtro de paquetes de Berkeley y las reglas de Snort.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Centro de defensa
- Versión de software 5.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Configuration Steps

Para configurar la variable **Snort_BPF**, siga los pasos a continuación:

1. Acceda a la interfaz de usuario web de su centro de defensa.
2. Vaya a **Políticas > Intrusión > Política de intrusión**.
3. Haga clic en el icono *del lápiz* para editar su política de intrusiones.
4. Haga clic en **Variables** en el menú de la izquierda.
5. Una vez configuradas las variables, deberá guardar los cambios y volver a aplicar la directiva de intrusiones para que surta efecto.

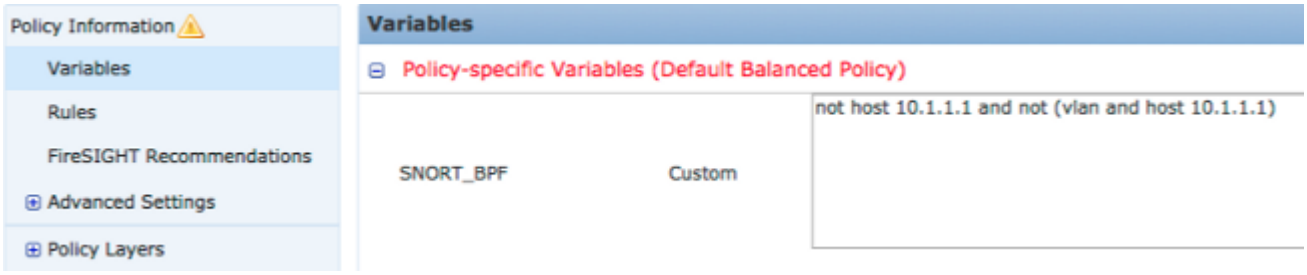

Figura: Captura de pantalla de la página de configuración de la variable Snort_BPF

Ejemplos de Configuración

A continuación se proporcionan algunos ejemplos básicos como referencia:

Situación 1: Ignorar todo el tráfico, PARA y DESDE un escáner de vulnerabilidades

1. Tenemos un analizador de vulnerabilidades en la dirección IP 10.1.1.1
2. Queremos ignorar todo el tráfico HACIA y DESDE el escáner
3. El tráfico puede o no tener una etiqueta 802.1q (vlan)

SNORT_BPF es:

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

COMPARACIÓN: el tráfico *no está* etiquetado en VLAN, pero los puntos 1 y 2 siguen siendo ciertos sería:

```
not host 10.1.1.1
```

En lenguaje sencillo, esto ignoraría el tráfico donde uno de los puntos finales es 10.1.1.1 (el escáner).

Escenario 2: Ignorar todo el tráfico, TO y FROM de dos analizadores de vulnerabilidades

1. Tenemos un analizador de vulnerabilidades en la dirección IP 10.1.1.1
2. Tenemos un segundo escáner de vulnerabilidades en la dirección IP 10.2.1.1
3. Queremos ignorar todo el tráfico HACIA y DESDE el escáner
4. El tráfico puede o no tener una etiqueta 802.11 (vlan)

SNORT_BPF es:

```
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))
```

Comparación: el tráfico *no* está etiquetado con VLAN, pero los puntos 1 y 2 siguen siendo ciertos sería:

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

En resumen, esto ignoraría el tráfico donde uno de los extremos es 10.1.1.1 O 10.2.1.1.

> **Nota**: Es importante tener en cuenta que la etiqueta vlan debería, en casi todos los casos, ocurrir sólo una vez en un BPF determinado. Las únicas veces que debería verlo más de una vez, es si su red utiliza etiquetado de VLAN anidado (a veces conocido como 'QinQ').

Escenario 3: Ignorar el tráfico etiquetado VLAN, TO y FROM de dos analizadores de vulnerabilidades

1. Tenemos un analizador de vulnerabilidades en la dirección IP 10.1.1.1
2. Tenemos un segundo escáner de vulnerabilidades en la dirección IP 10.2.1.1
3. Queremos ignorar todo el tráfico HACIA y DESDE el escáner
4. El tráfico está etiquetado como 802.11 (vlan) y desea utilizar una etiqueta específica (vlan), como en vlan 101

SNORT_BPF es:

```
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))
```

Situación 4: ignorar el tráfico de un servidor de respaldo

1. Tenemos un servidor de respaldo de red en la dirección IP 10.1.1.1

2. Las máquinas de la red se conectan a este servidor en el puerto 8080 para ejecutar su copia de seguridad nocturna
3. Deseamos ignorar este tráfico de respaldo, ya que está cifrado y es de gran volumen

SNORT_BPF es:

```
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))
```

Comparación: el tráfico *no* está etiquetado con VLAN, pero los puntos 1 y 2 siguen siendo ciertos sería:

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

Traducido, esto significa que el tráfico a 10.1.1.1 (nuestro hipotético servidor de respaldo) en el puerto 8080 (puerto de escucha) no debe ser inspeccionado por el motor de detección IPS.

También es posible utilizar net en lugar de host para especificar un bloque de red, en lugar de un solo host. Por ejemplo:

```
not net 10.1.1.0/24
```

En general, es una buena práctica hacer que el BPF sea lo más específico posible; excluir el tráfico de la inspección que debe excluirse, sin excluir ningún tráfico no relacionado que pueda contener intentos de aprovechamiento.

Situación 5: para utilizar rangos de red en lugar de hosts individuales

Puede especificar rangos de red en la variable BPF en lugar de hosts para acortar la longitud de la variable. Para ello, utilizará la palabra clave net en lugar de host y especificará un rango CIDR. Debajo tiene un ejemplo:

```
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))
```

> Nota: Asegúrese de introducir la dirección de red utilizando la notación CIDR y una dirección utilizable dentro del espacio de direcciones de bloque CIDR. Por ejemplo, utilice net 10.8.0.0/16 en lugar de net 10.8.2.16/16.

SNORT_BPF se utiliza para evitar que cierto tráfico sea inspeccionado por un motor de detección IPS; a menudo por razones de rendimiento. Esta variable utiliza el formato estándar de los filtros de paquetes de Berkeley (BPF). Tráfico que coincide con el **SNORT_BPF** se inspeccionará; mientras que el tráfico NO coincide con el **SNORT_BPF** El motor de detección IPS NO inspeccionará la variable.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).