Configuração da variável SNORT_BPF em um centro da defesa

Índice

Introdução

Você pode usar o filtro de pacote de Berkeley (BPF) para excluir um host ou uma rede da inspeção por um centro da defesa. O Snort usa a variável de **`Snort_BPF`** para excluir o tráfego de uma política da intrusão. Este documento fornece instruções em como usar a variável de **`Snort_BPF em`** várias encenações.

> **Tip**: Recomenda-se fortemente usar uma regra da confiança em uma política do controle de acesso para determinar o que o tráfego seja e não seja inspecionado, um pouco do que um BPF na política da intrusão. A variável de **`Snort_BPF`** está disponível na versão de software 5.2, e é suplicada na versão de software 5.3 ou mais alto.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento em regras do centro da defesa, da política da intrusão, do filtro de pacote de Berkeley, e do Snort.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- Centro da defesa
- Versão de software 5.2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Passos de configuração

A fim configurar a variável de **`Snort_BPF`**, siga as etapas abaixo:

1. Alcance a relação de usuário de web de seu centro da defesa.
2. Navegue às **políticas > à intrusão > à política da intrusão**.
3. Clique o ícone do *lápis* para editar sua política da intrusão.
4. Clique sobre **variáveis do** menu à esquerda.
5. Uma vez que as variáveis são configuradas, você precisará de salvar mudanças, e reaplica sua política da intrusão para que tome o efeito.

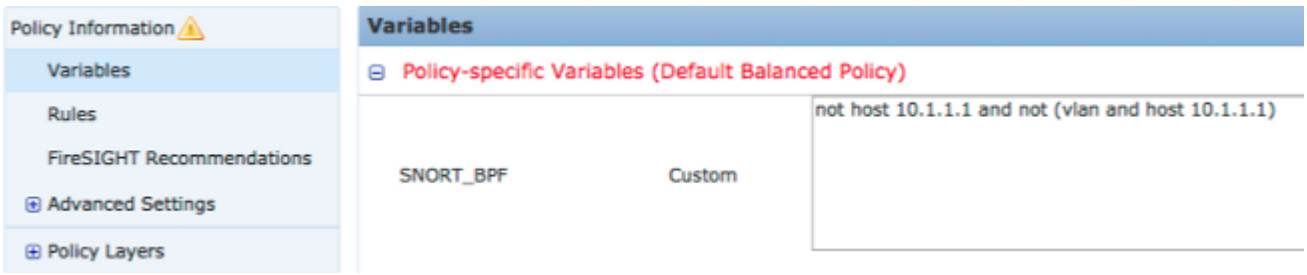

Figura: Tiro de tela da página da configuração variável de Snort_BPF

Exemplos de configuração

Alguns exemplos básicos são fornecidos abaixo para a referência:

Cenário 1: Ignore todo o tráfego, a e de um scanner de vulnerabilidade

1. Nós temos um scanner de vulnerabilidade no endereço IP 10.1.1.1
2. Nós queremos ignorar todo o tráfego a e do varredor
3. O tráfego pode ou não pode ter uma etiqueta 802.1q (vlan)

O **`SNORT_BPF`** é:

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

COMPARAÇÃO: o not* dos *is do tráfego VLAN-etiquetado, mas os pontos 1 e 2 permanece verdadeiros seria:

```
not host 10.1.1.1
```

No inglês liso, isto ignoraria o tráfego onde um dos valores-limite é 10.1.1.1 (o varredor).

Cenário 2: Ignore todo o tráfego, a e de dois scanner de vulnerabilidade

1. Nós temos um scanner de vulnerabilidade no endereço IP 10.1.1.1
2. Nós temos um segundo scanner de vulnerabilidade no endereço IP 10.2.1.1
3. Nós queremos ignorar todo o tráfego a e do varredor
4. O tráfego pode ou não pode ter uma etiqueta (vlan) do 802.11

- **SNORT_BPF** é:

```
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))
```

Comparação: O not* dos *is do tráfego VLAN-etiquetado, mas os pontos 1 e 2 permanece verdadeiros seria:

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

Em resumo, isto ignoraria o tráfego onde um dos valores-limite é 10.1.1.1 OU 10.2.1.1.

> Note: É importante notar que a etiqueta vlan deve, em quase todos os casos, ocorrer somente uma vez em um BPF dado. Os únicos tempos você deve vê-lo mais de uma vez, é se seus usos da rede aninharam a colocação de etiquetas VLAN (referida às vezes como “QinQ ").

Cenário 3: Ignore o tráfego rotulado VLAN, a e de dois scanner de vulnerabilidade

1. Nós temos um scanner de vulnerabilidade no endereço IP 10.1.1.1
2. Nós temos um segundo scanner de vulnerabilidade no endereço IP de Um ou Mais Servidores Cisco ICM NT 10.2.1.1
3. Nós queremos ignorar todo o tráfego a e do varredor
4. O tráfego é 802.11 (vlan) etiquetado, e você deseja usar uma etiqueta (vlan) específica, como no VLAN 101

- **SNORT_BPF** é:

```
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))
```

Encenação 4: Ignore o tráfego de um servidor de backup

1. Nós temos um server do backup de rede no endereço IP de Um ou Mais Servidores Cisco ICM NT 10.1.1.1
2. As máquinas na rede conectam a este server na porta 8080 para executar seu backup noturno

3. Nós desejamos ignorar este tráfego alternativo, porque é cifrado e volume alto

O SNORT_BPF é:

```
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))
```

Comparação: O not* dos *is do tráfego VLAN-etiquetado, mas os pontos 1 e 2 permanece verdadeiros seria:

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

Traduzido, isto significa que o tráfego a 10.1.1.1 (nosso servidor de backup hipotético) na porta 8080 (porta de escuta) não deve ser inspecionado pelo motor da detecção IPS.

É igualmente possível usar a `rede` no lugar do `host` para especificar um bloco da rede, um pouco do que um host único. Por exemplo:

```
not net 10.1.1.0/24
```

Geralmente, é uma boa prática fazer o mais específico possível o BPF; com exclusão do tráfego da inspeção que precisa de ser excluída, quando não com exclusão de algum tráfego não relacionado que pudesse conter tentativas da façanha.

Encenação 5: Para usar intervalos de rede um pouco do que host individuais

Você pode especificar intervalos de rede na variável BPF um pouco do que anfitriões para encurtar o comprimento da variável. Para fazê-lo assim usará a palavra-chave `líquida` no lugar do host e especificará uma escala CIDR. A seguir, está um exemplo:

```
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**: Assegure-se de por favor que você incorpore o endereço de rede usando a notação CIDR e um endereço útil dentro do espaço de endereços do bloco CIDR. Por exemplo use a rede 10.8.0.0/16 um pouco do que a rede 10.8.2.16/16.

A variável **SNORT_BPF** é usada a fim impedir que determinado tráfego esteja inspecionado por um motor da detecção IPS; frequentemente para razões de desempenho. Esta variável usa o formato padrão dos filtros do bloco de Berkeley (BPF). O tráfego que combina a variável **SNORT_BPF** será inspecionado; quando o tráfego que não combina a variável **SNORT_BPF** não será inspecionado pelo motor da detecção IPS.