Configuração da variável SNORT_BPF em um Centro de Defesa

Contents

Introduction

Você pode usar o Berkeley Packet Filter (BPF) para impedir que um host ou uma rede seja inspecionada por um Defense Center. O Snort usa a variável **Snort_BPF** para excluir o tráfego de uma política de intrusão. Este documento fornece instruções sobre como usar a variável **Snort_BPF** em vários cenários.

> **Dica**: é altamente recomendável usar uma regra de confiança em uma política de Controle de acesso para determinar qual tráfego é ou não inspecionado, em vez de um BPF na política de intrusão. A variável **`Snort_BPF`** está disponível na versão de software 5.2 e foi preterida na versão de software 5.3 ou superior.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento sobre as regras Defense Center, Intrusion Policy, Berkeley Packet Filter e Snort.

Componentes Utilizados

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

- Centro de Defesa
- Software versão 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

Para configurar a variável **Snort_BPF**, siga as etapas abaixo:

1. Acesse a interface de usuário da Web do seu Defense Center.
2. Navegue até **Policies > Intrusion > Intrusion Policy**.
3. Clique no ícone do *lápis* para editar sua política de intrusão.
4. Clique em **Variáveis** no menu à esquerda.
5. Depois que as variáveis forem configuradas, você precisará salvar as alterações e reaplicar a política de invasão para que ela entre em vigor.

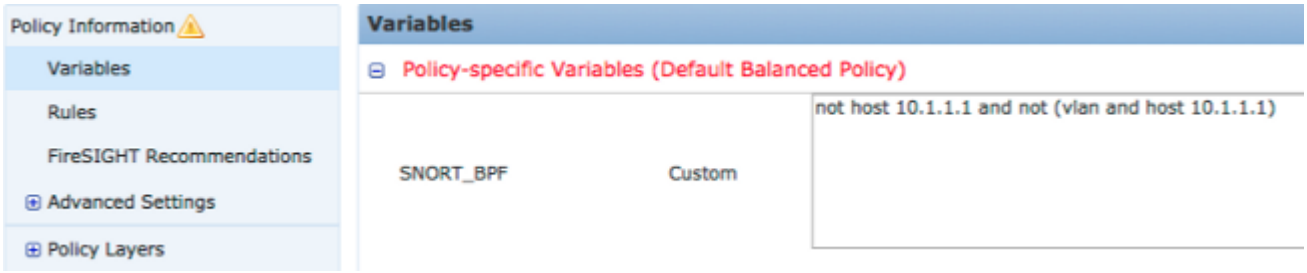

Figura: Captura de tela da página de configuração da variável Snort_BPF

Exemplos de configuração

Alguns exemplos básicos são fornecidos abaixo para referência:

Cenário 1: Ignorar todo o tráfego, PARA e DE um scanner de vulnerabilidade

1. Temos um verificador de vulnerabilidade no endereço IP 10.1.1.1
2. Desejamos ignorar todo o tráfego DE E PARA o scanner
3. O tráfego pode ou não ter uma marca 802.1q (vlan)

O **SNORT_BPF** é:

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

COMPARAÇÃO: o tráfego *não* está marcado como VLAN, mas os pontos 1 e 2 permanecem verdadeiros:

```
not host 10.1.1.1
```

Em inglês simples, isso ignoraria o tráfego onde um dos pontos finais é 10.1.1.1 (o scanner).

Cenário 2: Ignorar todo o tráfego, PARA e DE dois verificadores de vulnerabilidade.

1. Temos um verificador de vulnerabilidade no endereço IP 10.1.1.1
2. Temos um segundo verificador de vulnerabilidade no endereço IP 10.2.1.1
3. Desejamos ignorar todo o tráfego DE E PARA o scanner
4. O tráfego pode ou não ter uma marca 802.11 (vlan)

O **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 tráfego *não* está marcado como VLAN, mas os pontos 1 e 2 permanecem verdadeiros:

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

Em resumo, isso ignoraria o tráfego onde um dos pontos finais é 10.1.1.1 OU 10.2.1.1.

> **Observação**: é importante observar que a marca de vlan deve, em quase todos os casos, ocorrer apenas uma vez em um determinado BPF. A única vez que você deve vê-lo mais de uma vez é se a rede usar a marcação de VLAN aninhada (às vezes chamada de 'QinQ').

Cenário 3: Ignorar tráfego marcado de VLAN, PARA e DE dois verificadores de vulnerabilidade.

1. Temos um verificador de vulnerabilidade no endereço IP 10.1.1.1
2. Temos um segundo verificador de vulnerabilidade no endereço IP 10.2.1.1
3. Desejamos ignorar todo o tráfego DE E PARA o scanner
4. O tráfego é 802.11 (vlan) marcado e você deseja usar uma marca (vlan) específica, como na vlan 101

O **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))
```

Cenário 4: Ignorar o tráfego de um servidor de backup

1. Temos um servidor de backup de rede no endereço IP 10.1.1.1
2. Os computadores na rede se conectam a este servidor na porta 8080 para executar o backup noturno
3. Desejamos ignorar esse tráfego de backup, pois ele é criptografado e de alto volume

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 tráfego *não* está marcado como VLAN, mas os pontos 1 e 2 permanecem verdadeiros:

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

Traduzido, isso significa que o tráfego para 10.1.1.1 (nosso servidor de backup hipotético) na porta 8080 (porta de escuta) não deve ser inspecionado pelo mecanismo de detecção IPS.

Também é possível usar net no lugar de host para especificar um bloco de rede, em vez de um único host. Por exemplo:

```
not net 10.1.1.0/24
```

Em geral, é uma boa prática tornar o BPF o mais específico possível, excluindo o tráfego da inspeção que precisa ser excluído, sem excluir qualquer tráfego não relacionado que possa conter tentativas de exploração.

Cenário 5: Para usar intervalos de rede em vez de hosts individuais

Você pode especificar intervalos de rede na variável BPF em vez de hosts para encurtar o comprimento da variável. Para fazer isso, você usará a palavra-chave net no lugar do host e especificará um intervalo 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))
```

> Observação: certifique-se de inserir o endereço de rede usando a notação CIDR e um endereço utilizável dentro do espaço de endereço do bloco CIDR. Por exemplo, use net 10.8.0.0/16 em vez de net 10.8.2.16/16.

O **SNORT_BPF** A variável é usada para impedir que determinado tráfego seja inspecionado por um mecanismo de detecção de IPS, frequentemente por motivos de desempenho. Esta variável usa o formato padrão BPF (Berkeley Pack Filters). Tráfego correspondente ao **SNORT_BPF** variável será inspecionada; embora o tráfego NÃO corresponda ao **SNORT_BPF** A variável NÃO será inspecionada pelo mecanismo de detecção de IPS.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.