Procedimentos da captura de pacote de informação em dispositivos da potência de fogo de Sourcefire, e dispositivos virtuais NGIPS

Índice

Introdução

Este documento descreve como usar o **comando tcpdump** capturar os pacotes que são vistos por uma interface de rede de seu dispositivo de Sourcefire. Usa a sintaxe do filtro de pacote de Berkeley (BPF).

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento no dispositivo da potência de fogo de Sourcefire e nos modelos do dispositivo virtual.

Componentes Utilizados

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

- Dispositivos do 7000 Series da potência de fogo de Sourcefire, dispositivos do 8000 Series, e dispositivos virtuais NGIPS
- Versão de software 5.0 de Sourcefire ou mais atrasado

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.

> **aviso:** Se você executa o **comando tcpdump em um** sistema da produção, pode impactar o desempenho da rede.

Requisitos de hardware

Esta instrução é aplicável em dispositivos do 7000 Series da potência de fogo de Sourcefire, em dispositivos do 8000 Series, e em dispositivos virtuais NGIPS.

Requisitos de software

Esta instrução é aplicável nas versões de software 5.0 ou maior.

Etapas para capturar pacotes

No CLI, incorpore o captação-**tráfego do suporte de sistema**. Por exemplo:

```
> system support capture-traffic

Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set (Interfaces s2p1, s2p2)
```

Após ter feito uma seleção, você será alertado para opções:

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

A fim capturar suficientes dados dos pacotes, é necessário usar - a opção s para ajustar corretamente o snaplength. O snaplength deve ser ajustado a um valor que combine o valor configurado da unidade de transmissão máxima (MTU) da configuração ajustada da relação, que opta 1518.

> **aviso:** Desde que capturar o tráfego à tela pode degradar o desempenho do sistema e da rede, Cisco recomenda-o usar - a opção do <filename> w com comando tcpdump. Captura os pacotes a um arquivo. Se você executa o comando sem - a opção w, pressiona **CTRL +** combinação chave **c** a retirar.

Exemplo - da opção do <filename> w:

```
-w capture.pcap -s 1518
```

> Cuidado: Não use nenhuns elementos do trajeto ao especificar o nome de arquivo do pcap. Você deve especificar somente o nome de arquivo do pcap a ser criado no dispositivo.

Se é desejável capturar um número limitado de pacotes, você pode usar - a bandeira do <packets> c para especificar o número de pacotes para capturar. Por exemplo, para capturar exatamente 5000 pacotes:

```
-w capture.pcap -s 1518 -c 5000
```

Adicionalmente, um filtro BPF pode ser adicionado no fim do comando limitar que pacotes são capturados. Por exemplo, para limitar a captura de pacote de informação a 5000 pacotes com uma fonte ou um endereço IP de destino de 192.0.2.1, você poderia usar as seguintes opções:

```
-w capture.pcap -s 1518 -c 5000 host 192.0.2.1
```

Quando você está capturando o tráfego que é LAN virtual (VLAN) etiquetado, você deve especificar o VLAN usando a sintaxe BPF. Se não, o pcap não contém alguns dos pacotes rotulados VLAN. Por exemplo, o seguinte limitaria a captação ao tráfego que é VLAN etiquetado de 192.0.2.1:

```
-w capture.pcap -s 1518 -c 5000 vlan and host 192.0.2.1
```

Se você é incerto se o tráfego é VLAN etiquetado, a seguinte sintaxe poderia ser usada para capturar o tráfego de 192.0.2.1 que é e não é VLAN etiquetado:

```
-w capture.pcap -s 1518 -c 5000 'host 192.0.2.1 or (vlan and host 192.0.2.1)'
```

> Nota: No exemplo precedente, o parêntese é precisado de modo que "ou" se aplique não somente a "vlan". As quotas únicas são precisadas então de impedir toda a interpretação errônea possível do parêntese pelo shell.

Especificar uma etiqueta VLAN captura todo o tráfego de VLAN que combina o resto de seu BPF. Contudo, se você quer capturar uma etiqueta específica VLAN, você pode especificar que etiqueta VLAN você gostaria de capturar como assim:

```
-w capture.pcap -s 1518 -c 5000 vlan 1 and host 192.0.2.1
```

Após ter especificado as opções desejadas e a pressão entre, tcpdump começa a capturar o tráfego.

> Dica: Se - a opção c não foi usada, pressiona **CTRL +** combinação chave **c** para parar a captação.

Uma vez que você para a captação, você receberá a confirmação. Por exemplo:

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -w capture.pcap -s 1518 -c 5000 host 192.0.2.1
Cleaning up.
Done.
```

Copie um arquivo de Pcap

A fim copiar um pcap arquive de um dispositivo da potência de fogo a um outro sistema que aceite conexões de SSH de entrada, usam o comando seguinte:

```
> system file secure-copy hostname username destination_directory pcap_file
```

Depois que você pressiona entre, você estará alertado para a senha ao sistema remoto. O arquivo será copiado através da rede.

Nota: Neste exemplo, o **hostname** refere o nome ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do host remoto do alvo, o **username** especifica o nome do usuário no host remoto, o **destination_directory** especifica o caminho de destino no host remoto, e o **pcap_file** especifica o arquivo local do pcap para transferência.