Procedimentos da captura de pacote de informação no dispositivo de Cisco FirePOWER

Índice

Introdução

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

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do dispositivo de Cisco FirePOWER e dos modelos do dispositivo virtual.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Etapas para capturar pacotes

Entre ao CLI de seu dispositivo de FirePOWER.

Nas versões 6.1 e mais recente, incorpore o captação-**tráfego**. Por exemplo,

```
> capture-traffic

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

Nas versões 6.0.x.x e anterior, 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)
```

Depois que você faz uma seleção, você estará alertado para opções:

```
> system support capture-traffic

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

A fim capturar suficientes dados dos pacotes, é necessário usar - `a` opção `s` a fim 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 que você usa - `a` opção do `<filename> w` com `comando tcpdump`. Captura os pacotes a um arquivo. Se você executa o comando sem - `a` opção `w`, pressiona a combinação chave do **Ctrl-c** a fim retirar.

Exemplo - `da` opção do `<filename> w`:

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

> **Caution**: Não use nenhuns elementos do trajeto quando você especifica o nome de arquivo da captura de pacote de informação (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` a fim especificar o número de pacotes para capturar. Por exemplo, a fim capturar exatamente 5000 pacotes:

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

Adicionalmente, um filtro BPF pode ser adicionado no fim do comando a fim limitar que pacotes são capturados. Por exemplo, a fim 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 estas opções:

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

Quando você captura o tráfego que é LAN virtual (VLAN) etiquetado, você deve especificar o VLAN com a sintaxe BPF. Se não, o pcap não contém alguns dos pacotes rotulados VLAN. Por

exemplo, este exemplo limita 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, esta sintaxe poderia ser usada a fim 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)'
```

> **Note**: No exemplo anterior, os parênteses são precisados de modo que "`ou`" se aplique não somente a "`vlan`". As quotas únicas são precisadas então a fim impedir toda a interpretação errônea possível dos parênteses pelo shell.

A especificação de 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
```

Depois que você especifica as opções desejadas e as pressiona **entra**, o tcpdump começa a capturar o tráfego.

> **Tip**: Se `-a` opção `c` não foi usada, pressiona a combinação chave do **Ctrl-c** a fim 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 de FirePOWER a um outro sistema que aceite conexões de SSH de entrada, usam este comando:

```
> 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.

> **Note**: 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.