Usar procedimentos de captura de pacotes no dispositivo Firepower

Contents

Introdução

Este documento descreve como usar o comando **tcpdump** para capturar pacotes que são vistos por uma interface de rede do seu dispositivo Firepower.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento do dispositivo Cisco Firepower e dos modelos de dispositivo virtual.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas. Usa a sintaxe do Filtro de Pacotes Berkeley (BPF).

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

> **Aviso**: se você executar o comando **tcpdump** em um sistema de produção, ele poderá afetar o desempenho da rede.

Etapas para capturar pacotes

Faça login na CLI do seu dispositivo Firepower.

Nas versões 6.1 e posteriores, insira **capture-traffic**. Por exemplo,

<#root>

```
> 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 anteriores, insira **system support capture-traffic**. Por exemplo,

<#root>

```
> system support capture-traffic
```

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

Depois de fazer uma seleção, você é solicitado a fornecer opções:

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

Para capturar dados suficientes dos pacotes, é necessário usar a opção -s para definir o comprimento do instantâneo corretamente. O snaplength pode ser definido para um valor que corresponda ao valor configurado da unidade de transmissão máxima (MTU) da configuração do conjunto de interfaces, que assume o padrão 1518.

> **Aviso**: quando você captura o tráfego para a tela, isso pode degradar o desempenho do sistema e da rede. A Cisco recomenda que você use a opção -w <nome do arquivo> com o comando tcpdump. Ele captura os pacotes em um arquivo. Se você executar o comando sem a opção -w, pressione a combinação de teclas **Ctrl-C** para sair.

Exemplo da opção -w <nome do arquivo>:

<#root>

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

> **Cuidado**: não use nenhum elemento de caminho ao especificar o nome de arquivo de captura de pacote (pcap). Você deve especificar somente o nome de arquivo pcap a ser criado no equipamento.

Se for desejável capturar um número limitado de pacotes, você pode usar o flag -c <packets> para especificar o número de pacotes a serem capturados. Por exemplo, para capturar exatamente 5000 pacotes:

<#root>

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

Além disso, um filtro BPF pode ser adicionado ao final do comando para limitar quais pacotes são capturados. Por exemplo, para limitar a captura de pacotes a 5000 pacotes com um endereço IP de origem ou destino 192.0.2.1, você pode usar estas opções:

<#root>

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

Ao capturar o tráfego que é LAN virtual (VLAN) marcado, você deve especificar a VLAN com a sintaxe BPF. Caso contrário, o pcap não contém nenhum dos pacotes marcados com VLAN. Por exemplo, este exemplo limita a captura ao tráfego que é marcado como VLAN de 192.0.2.1:

<#root>

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

Se você não tiver certeza de que o tráfego está marcado como VLAN, esta sintaxe poderá ser usada para capturar o tráfego de 192.0.2.1, que está e não está marcado como VLAN:

<#root>

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

> **Observação**: no exemplo anterior, os parênteses são necessários para que 'or' não se aplique apenas a 'vlan'. As aspas simples são então necessárias para evitar qualquer possível interpretação incorreta dos parênteses pelo shell.

A especificação de uma marca de VLAN captura todo o tráfego de VLAN que corresponde ao restante do seu BPF. No entanto, se você quiser capturar uma tag de VLAN específica, poderá especificar a tag de VLAN que gostaria de capturar da seguinte forma:

<#root>

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

Depois de especificar as opções desejadas e pressionar **Enter**, tcpdump começa a capturar o tráfego.

> **Dica**: se a opção -c não tiver sido usada, pressione a combinação de teclas **Ctrl-C** para interromper a captura.

Depois de parar a captura, você receberá uma confirmação. Por exemplo:

<#root>

```
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.
```

Copiar um arquivo Pcap

Para copiar um arquivo pcap de um dispositivo FirePOWER para outro sistema que aceita conexões SSH de entrada, use este comando:

<#root>

> system file secure-copy hostname username destination_directory pcap_file

Depois de pressionar **Enter**, você será solicitado a fornecer a senha para o sistema remoto. O arquivo pode ser copiado através da rede.

> **Observação**: Neste exemplo, o nome do host se refere ao nome ou ao endereço IP do host remoto de destino, o nome do usuário especifica o nome do usuário no host remoto, o destination_diretory especifica o caminho de destino no host remoto e o pcap_file especifica o arquivo pcap local para transferência.

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.