Utilizar procedimientos de captura de paquetes en un dispositivo Firepower

Contenido

Introducción

Este documento describe cómo utilizar el comando **tcpdump** para capturar los paquetes que son vistos por una interfaz de red de su dispositivo Firepower.

Prerequisites

Requirements

Cisco recomienda que conozca los modelos de dispositivos Cisco Firepower y de dispositivos virtuales.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware. Utiliza la sintaxis del filtro de paquetes de Berkeley (BPF).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

> **Advertencia**: Si ejecuta el comando **tcpdump** en un sistema de producción, puede afectar el rendimiento de la red.

Pasos para capturar paquetes

Inicie sesión en la CLI del dispositivo Firepower.

En las versiones 6.1 y posteriores, ingrese **capture-traffic**. Por ejemplo,

<#root>

```
> capture-traffic
```

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

En las versiones 6.0.x.x y anteriores, ingrese **system support capture-traffic**. Por ejemplo,

<#root>

> system support capture-traffic

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

Después de realizar una selección, se le solicitarán las siguientes opciones:

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

Para capturar suficientes datos de los paquetes, es necesario utilizar la opción -s para establecer la longitud de onda correctamente. La longitud de ajuste se puede establecer en un valor que coincida con el valor de la unidad de transmisión máxima (MTU) configurada en la configuración del conjunto de interfaces, cuyo valor predeterminado es 1518.

> **Advertencia**: Cuando captura tráfico en la pantalla, puede degradar el rendimiento del sistema y de la red. Cisco recomienda que utilice la opción -w <filename> con el comando tcpdump. Captura los paquetes en un archivo. Si ejecuta el comando sin la opción -w, presione la combinación de teclas **Ctrl-C** para salir.

Ejemplo de la opción -w <filename>:

<#root>

-w capture.pcap -s 1518

> **Precaución**: no utilice ningún elemento de ruta cuando especifique el nombre de archivo de captura de paquetes (pcap). Debe especificar solamente el nombre de archivo pcap que se creará en el dispositivo.

Si es deseable capturar un número limitado de paquetes, puede utilizar el indicador -c <packets> para especificar el número de paquetes que se van a capturar. Por ejemplo, para capturar exactamente 5000 paquetes:

<#root>

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

Además, se puede agregar un filtro BPF al final del comando para limitar los paquetes que se capturan. Por ejemplo, para limitar la captura de paquetes a 5000 paquetes con una dirección IP de origen o destino de 192.0.2.1, podría utilizar estas opciones:

<#root>

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

Al capturar tráfico etiquetado como LAN virtual (VLAN), debe especificar la VLAN con la sintaxis BPF. De lo contrario, el pcap no contiene ninguno de los paquetes etiquetados de VLAN. Por ejemplo, este ejemplo limita la captura al tráfico que es VLAN etiquetado desde 192.0.2.1:

<#root>

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

Si no está seguro de si el tráfico está etiquetado como VLAN, esta sintaxis se podría utilizar para capturar el tráfico de 192.0.2.1 que está etiquetado como VLAN y no lo está:

<#root>

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

> **Nota**: En el ejemplo anterior, se necesitan los paréntesis para que 'or' no se aplique solamente a 'vlan'. Las comillas simples son entonces necesarias para evitar cualquier posible mala interpretación de los paréntesis por el shell.

La especificación de una etiqueta VLAN captura todo el tráfico VLAN que coincide con el resto de su BPF. Sin embargo, si desea capturar una etiqueta VLAN específica, puede especificar qué etiqueta VLAN desea capturar de esta manera:

<#root>

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

Después de especificar las opciones deseadas y presionar **Enter**, tcpdump comienza a capturar el tráfico.

> **Sugerencia**: Si la opción -c no se utilizó, presione la combinación de teclas **Ctrl-C** para detener la captura.

Una vez detenida la captura, recibirá una confirmación. Por ejemplo:

<#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 un archivo Pcap

Para copiar un archivo pcap de un dispositivo FirePOWER a otro sistema que acepte conexiones SSH entrantes, utilice este comando:

<#root>

> system file secure-copy hostname username destination_directory pcap_file

Después de presionar **Enter**, se le pedirá la contraseña para el sistema remoto. El archivo se puede copiar en la red.

> **Nota**: En este ejemplo, el nombre de host hace referencia al nombre o la dirección IP del host remoto de destino, el nombre de usuario especifica el nombre del usuario en el host remoto, destination_directory especifica la ruta de acceso de destino en el host remoto y pcap_file especifica el archivo pcap local para la transferencia.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).