Procedimientos de la captura de paquetes en el dispositivo de Cisco FirePOWER

Contenido

Introducción

Este documento describe cómo utilizar el **comando tcpdump** para capturar los paquetes que son vistos por una interfaz de la red de su dispositivo de FirePOWER. Utiliza el sintaxis del filtro de paquete de Berkeley (BPF).

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento del dispositivo de Cisco FirePOWER y de los modelos del dispositivo virtual.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

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

Pasos para capturar los paquetes

Inicie sesión al CLI de su dispositivo de FirePOWER.

En las versiones 6.1 y posterior, ingrese el captura-**tráfico**. Por ejemplo,

```
> 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 anterior, ingrese el captura-**tráfico del soporte de sistema**. Por ejemplo,

```
> system support capture-traffic

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

Después de que usted haga una selección, le indicarán para las opciones:

```
> system support capture-traffic

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

Para capturar los datos suficientes de los paquetes, es necesario utilizar `- la` opción `s` para fijar el snaplength correctamente. El snaplength se debe fijar a un valor que haga juego el valor configurado de la Unidad máxima de transmisión (MTU) (MTU) de la configuración determinada de la interfaz, que omite 1518.

> Advertencia: Puesto que la captura del tráfico a la pantalla puede degradar el funcionamiento del sistema y de la red, Cisco recomienda que usted utiliza `- la` opción del `<filename> w` con el `comando tcpdump`. Captura los paquetes a un archivo. Si usted funciona con el comando sin `- la` opción `w`, presiona la combinación de claves del **Ctrl-c** para salir.

Ejemplo `- de la` opción del `<filename> w`:

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

> **Caution**: No utilice ninguna elementos de la trayectoria cuando usted especifica el nombre de fichero de la captura de paquetes (pcap). Usted debe especificar solamente el nombre de fichero del pcap que se creará en el dispositivo.

Si es deseable capturar un número limitado de paquetes, usted puede utilizar `- el` indicador del `<packets> c` para especificar el número de paquetes para capturar. Por ejemplo, para capturar exactamente 5000 paquetes:

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

Además, un filtro BPF se puede agregar en el final del comando para limitar se capturan qué paquetes. Por ejemplo, para limitar a la captura de paquetes a 5000 paquetes con una fuente o un IP Address de destino de 192.0.2.1, usted podría utilizar estas opciones:

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

Cuando usted captura el tráfico que es Virtual LAN (VLAN) marcado con etiqueta, usted debe especificar el VLA N con el sintaxis BPF. Si no, el pcap no contiene los paquetes con Tag uces de los del VLA N. Por ejemplo, este ejemplo limita la captura al tráfico que es VLA N marcado con etiqueta de 192.0.2.1:

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

Si usted es inseguro si el tráfico es VLA N marcado con etiqueta, este sintaxis se podría utilizar para capturar el tráfico de 192.0.2.1 que es y no es VLA N marcado con etiqueta:

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

> **Note**: En el ejemplo anterior, paréntesis son necesarios de modo que "`o`" no sólo se aplique a "`vlan`". Las únicas cuotas entonces son necesitadas para prevenir cualquier interpretación posible de paréntesis por el shell.

La especificación de una etiqueta del VLA N captura todo el tráfico VLAN que haga juego el resto de su BPF. Sin embargo, si usted quiere capturar una etiqueta específica del VLA N, usted puede especificar qué etiqueta del VLA N usted quisiera capturar como tan:

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

Después de que usted especifique las opciones y el Presione ENTER deseados, el tcpdump comienza a capturar el tráfico.

> **Tip**: Si - `la` opción `c` no fue utilizada, presiona la combinación de claves del **Ctrl-c** para parar la captura.

Una vez que usted para la captura, usted recibirá la confirmación. Por ejemplo:

```
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 un archivo de Pcap

Para copiar un pcap clasifíe de un dispositivo de FirePOWER a otro sistema que valide las conexiones SSH entrantes, utilizan este comando:

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

Después de que le Presione ENTER, usted indiquen para la contraseña al sistema remoto. El archivo será copiado a través de la red.

> **Note**: En este ejemplo, el **nombre de host** refiere al nombre o a la dirección IP del host remoto de la blanco, el **nombre de usuario** especifica el nombre del usuario en el host remoto, el **destination_directory** especifica el trayecto de destino en el host remoto, y el **pcap_file** especifica el archivo local del pcap para la transferencia.