Captura de paquetes integrada para el Cisco IOS y el ejemplo de configuración IOS-XE

Contenido

Introducción

Este documento describe la característica integrada de la captura de paquetes (EPC) en el software del ® del Cisco IOS.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IOS Release 12.4(20)T o Posterior
- Versión 15.2(4)S del Cisco IOS XE - 3.7.0 o más adelante

La información en este documento fue creada de los dispositivos en un ambiente de laboratorio. 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.

Antecedentes

Cuando está habilitado, el router captura los paquetes enviados y recibidos. Los paquetes se salvan dentro de un buffer en el DRAM y no son así persistentes a través de una recarga. Una vez que se capturan los datos, pueden ser examinados en un resumen o una vista detallada en el router. Además, los datos se pueden exportar como archivo de la captura de paquetes (PCAP) para tener en cuenta el examen adicional. La herramienta se configura en el modo EXEC y se considera una herramienta temporal de la ayuda. Como consecuencia, no seguirá habiendo la configuración de la herramienta no se salva dentro de la configuración del router y en el lugar después de una recarga del sistema.

La herramienta del generador y del analizador de los Config de la captura de paquetes está disponible para que los clientes de Cisco ayuden en la configuración, la captura, y la extracción de las capturas de paquetes.

Ejemplo de la configuración del Cisco IOS

Configuración básica del EPC

1. Defina un “buffer de la captura”, que es un buffer temporal que los paquetes capturados están salvados dentro. Hay las diversas opciones que pueden ser seleccionadas cuando se define el buffer; por ejemplo el tamaño, el tamaño de paquetes del maxium, y circular/Lineal:

   ```
   monitor capture buffer BUF size 2048 max-size 1518 linear
   ```
2. Un filtro se puede también aplicar para limitar la captura al tráfico deseado. Defina una lista de control de acceso (ACL) dentro del modo de configuración y aplique el filtro al buffer:

   ```
   ip access-list extended BUF-FILTER
   permit ip host 192.168.1.1 host 172.16.1.1
   permit ip host 172.16.1.1 host 192.168.1.1monitor capture buffer BUF filter access-list
   BUF-FILTER
   ```
3. Defina una “punta de la captura”, que define la ubicación en donde ocurre la captura. La punta de la captura también define si la captura ocurre para el IPv4 o el IPv6 y en qué trayecto de Switching (proceso contra el cef):

   ```
   monitor capture point ip cef POINT fastEthernet 0 both
   ```
4. Asocie el buffer a la punta de la captura:

   ```
   monitor capture point associate POINT BUF
   ```
5. Comience la captura:

   ```
   monitor capture point start POINT
   ```
6. La captura es activa ahora. Permita la colección de los datos necesarios.

7. Pare la captura:

   ```
   monitor capture point stop POINT
   ```
8. Examine el buffer en la unidad:

   `show monitor capture buffer BUF dump`Nota: Esta salida muestra solamente el vaciado Hex de las capturas de los paquetes. Para ver en legible allí son dos maneras.Exporte el buffer del router para el análisis adicional:

`monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap`Consejo: El pedido de mejora CSCuw77601 se ha clasifiado para agregar a correo-a la opción bajo exportación así que usted puede enviar por correo electrónico el buffer diretly a una correo electrónico-identificación.Sin embargo el método anterior no es siempre práctico como él requirió el acceso T/FTP al router. En tales situaciones, usted puede tomar una copia del vaciado Hex y utilizar cualquier convertidor en línea del hex.-pcap para ver los archivos.

9. Una vez que se han recogido los datos necesarios, borre la "punta de la captura" y "capture el buffer": `no monitor capture point ip cef POINT fastEthernet 0 both`
`no monitor capture buffer BUF`

Notas:

- En las versiones anterior que el Cisco IOS Release 15.0(1)M, el tamaño de almacén intermedio fue limitado a 512K.
- En las versiones anterior que el Cisco IOS Release 15.0(1)M, el tamaño de paquetes capturado fue limitado a 1024 bytes.
- El almacén intermedio del paquete se salva en el DRAM y no persistirá a través de las recargas.
- La configuración de la captura no se salva en el NVRAM y no persistirá a través de las recargas.
- La punta de la captura se puede definir para capturar en el cef o los trayectos del process switching.
- La punta de la captura se puede definir para capturar solamente en una interfaz o global.
- Cuando el buffer de la captura se exporta en el formato PCAP, la información L2 (tal como encapsulado Ethernet) no se preserva.
- SeeBest practica para buscar los comandos para obtener más información sobre los comandos usados en esta sección.

Ejemplo de configuración del Cisco IOS XE

La característica integrada de la captura de paquetes fue introducida en la versión 3.7 del Cisco IOS XE - 15.2(4)S. La configuración de la captura es diferente que el Cisco IOS pues agrega más características.

Configuración básica del EPC

1. Defina la ubicación en donde ocurrirá la captura:

```
monitor capture CAP interface GigabitEthernet0/0/1 both
```

2. Asocie un filtro. El filtro se puede especificar en línea, o un ACL o un clase-mapa puede ser referido:

```
monitor capture CAP match ipv4 protocol tcp any any
```

3. Comience la captura:

```
monitor capture CAP start
```

4. La captura es activa ahora. Permita que recoja los datos necesarios.

5. Pare la captura:

```
monitor capture CAP stop
```

6. Examine la captura en una visión sumaria:

```
show monitor capture CAP buffer brief
```

7. Examine la captura en una vista detallada:

```
show monitor capture CAP buffer detailed
```

8. Además, exporte la captura en el formato PCAP para el análisis adicional:

```
monitor capture CAP export ftp://10.0.0.1/CAP.pcap
```

9. Una vez que se han recogido los datos necesarios, quite la captura:

```
no monitor capture CAP
```

Notas:

- La captura se puede realizar en las interfaces físicas, los subinterfaces, y las interfaces del túnel.
- El Reconocimiento de aplicaciones basadas en la red (NBAR) basó los filtros, ese uso el **comando match protocol** bajo el clase-mapa, no se soporta actualmente.
- Vea las mejores prácticas para buscar los comandos para obtener más información sobre los comandos usados en esta sección.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Para el EPC que se ejecuta en el Cisco IOS XE, este comando debug puede ser utilizado para asegurarse que el EPC está configurado correctamente:

```
no monitor capture CAP
```

Información Relacionada

- Captura de paquetes integrada - Cisco IOS XE
- Captura de paquetes integrada - Cisco IOS
- Soporte Técnico y Documentación - Cisco Systems