Usando el comando tcpdump en software del ACNS

Contenido

Introducción

El cisco application and content networking software (acns) 4.2.1 presentó al **comando tcpdump**. Este comando le permite para recolectar una traza de sniffer en el Content Engine, el router de contenido, o el administrador de distribución de contenido con el fin del troubleshooting, cuando es pedido recopilar los datos por el Soporte técnico de Cisco. Esta utilidad es muy similar al **comando tcpdump de** Linux/de Unix.

prerrequisitos

Requisitos

Quienes lean este documento deben tener conocimiento de los siguientes temas:

- FTP
- ACNS
- Comando line interface(cli) del ACNS

Componentes Utilizados

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

- Software ACNS 4.2.1 y posterior
- Todas las Plataformas que ejecutan ACNS 4.2.X y arriba

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.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Captura de los paquetes

El CLI en el ACNS ahora permite que el administrador (debe ser el administrador de usuario) capture los paquetes de los Ethernetes. En el Content Engine 500 Series, los nombres de la interfaz son eth0 y eth1. En todas las plataformas ACN, se recomienda que usted especifica una trayectoria/un nombre de fichero en el directorio del local1.

Usted puede hacer un volcado recto del encabezado de paquete a la pantalla si usted publica el **comando tcpdump** en el CLI. Presione el **Ctrl-c** para parar el volcado.

Opciones

El comando tcpdump tiene estas opciones:

- **- *nombre de fichero* w** — Escribe la salida sin procesar de la captura de paquetes a un archivo.
- **- *cuenta* s** — Captura los primeros bytes del <count> de cada paquete.
- **- *interconecto*** — Permite que usted especifique una interfaz específica para utilizar para capturar los paquetes.
- **- *límites de recuento* c la** captura *para contar los* paquetes.

Esto es un ejemplo de comando:

tcpdump - w /local1/dump.pcap - eth0 i - s 1500 - c 10000

Este comando captura los primeros 1500 bytes de los 10,000 paquetes siguientes del interface ethernet 0, y pone la salida en un archivo nombrado **dump.pcap en el** directorio del local1 en el Content Engine.

Note: Asegúrese de que usted especifique la opción **– s** para fijar la extensión snap del paquete. El valor predeterminado captura solamente 64 bytes, y éste guarda solamente los encabezados de paquete en el capturar archivo. Para resolver problemas de los paquetes reorientados o del tráfico de alto nivel (HTTP, autenticación, y así sucesivamente), una copia de los paquetes completos es necesaria.

Usted puede también funcionar con el **tcpdump** y el filtro en un IP Address particular:

- Agregue el **host 10.255.1.34** al final de la línea del **tcpdump**. **Note**: Substituya **10.255.1.34** por la dirección IP que el cliente está utilizando.
- También, utilice 1600 como el tamaño para coger los malos paquetes que pueden ser más grandes de 1500 bytes.

Aquí tiene un ejemplo:

```
tcpdump -w /local/mydump -s 1600 -c10000 host 10.255.2.34
```

FTP

Después de que se haya recogido el volcado TCP, usted necesita mover el archivo desde el Content Engine a un PC para poderlo ver por un decodificador sabueso.

```
ftp <ip address of the CE>
 !--- Log in with the admin username and password. cd local1 bin hash get <name of the file> !--
- Using the previous example, it is dump.pcap.

     bye
```

Etéreo

Etérea es la aplicación de software recomendada para leer el volcado TCP, debido al fragmento de sus características y de su uso con las Redes de contenido, incluyendo la capacidad de decodificar los paquetes que se encapsulan en un túnel GRE, usados por el redireccionamiento de WCCP. Refiera al sitio web de Wireshark para más información.

Note: En la mayoría de los casos, los paquetes reorientados capturados por el **recurso tcpdump** disponible con el ACNS CLI diferencian de los datos recibidos en la interfaz. Debido a la implementación y a la dirección internas de los paquetes reorientados, del IP Address de destino y del número del puerto TCP se modifican para reflejar la dirección IP y el número del puerto 8999 del dispositivo.

Información Relacionada

- Software support del cisco application and content networking software (acns)
- Soporte Técnico y Documentación - Cisco Systems