Procedimientos de la captura de paquetes ESA

Contenido

Introducción

Este documento describe cómo realizar a las capturas de paquetes en el dispositivo de seguridad del correo electrónico de Cisco (ESA).

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de Cisco ESA.

Componentes Utilizados

La información en este documento se basa en Cisco ESA que funciona con cualquier versión de AsyncOS.

Antecedentes

Cuando usted entra en contacto el soporte de cliente de IronPort con un problema, usted puede ser que sea pedido proporcionar la penetración en la actividad de la red saliente y entrante del ESA. El dispositivo proporciona la capacidad de interceptar y de visualizar el TCP, el IP, y otros paquetes que se transmiten o se reciben sobre la red a la cual se asocia el dispositivo. Usted

puede ser que quiera funcionar con a una captura de paquetes para hacer el debug de la configuración de la red y para verificar el tráfico de la red que alcanza o sale del dispositivo.

> **Note**: Este documento se refiere al software que no es mantenido ni es soportado por IronPort. La información se proporciona como cortesía para su conveniencia. Para la asistencia adicional, entre en contacto por favor al proveedor de software.

Es importante observar que substituyen al comando CLI previamente usado del **tcpdump** por el nuevo comando del **packetcapture** en las versiones 7.0 de AsyncOS y posterior. Este comando ofrece las funciones similares al **comando tcpdump**, y está también disponible para el uso en el GUI.

Si usted funciona con la versión 6.x o anterior de AsyncOS, refiera a las instrucciones en cómo utilizar el **comando tcpdump** en las **capturas de paquetes en las versiones 6.x de AsyncOS y la** sección **anterior de** este documento. También, las opciones de filtro que se describen en los **filtros de la captura de paquetes** seccionan son válidas para el nuevo comando del **packetcapture** también.

Capturas de paquetes en las versiones 7.x de AsyncOS y posterior

Esta sección describe el proceso de la captura de paquetes en las versiones 7.x de AsyncOS y posterior.

Comience o pare a una captura de paquetes

Para comenzar a una captura de paquetes con el GUI, navegue al soporte y al menú de ayuda, **captura de paquetes** selecta, y después haga clic la **captura del comienzo**. Para parar el proceso de la captura de paquetes, haga clic la **captura de la parada**.

> **Note**: Una captura que comienza en el GUI se preserva entre las sesiones.

Para comenzar a una captura de paquetes con el CLI, ingrese el **packetcapture > el comando start**. Para parar el proceso de la captura de paquetes, ingrese el **packetcapture > el comando stop**, y el ESA para a la captura de paquetes cuando la sesión termina.

Funciones de la captura de paquetes

Aquí está una lista de información útil que usted puede utilizar para manipular a las capturas de paquetes:

- El ESA guarda la actividad capturada del paquete a un archivo y salva el archivo localmente. Usted puede configurar el tamaño del capturar archivo del PAQUETE MÁXIMO, la longitud del tiempo para la cual la captura de paquetes se ejecuta, y en qué interfaz de la red funciona con la captura. Usted puede también utilizar un filtro para limitar a la captura de paquetes

para traficar con un puerto o un tráfico específico de un cliente o de un dirección IP del servidor específico.

- Navegue **para soportar y ayuda > captura de paquetes del** GUI para ver una lista completa de los archivos de la captura de paquetes que se salvan en la unidad de disco duro. Cuando una captura de paquetes se ejecuta, las páginas muestra de la captura de paquetes el estatus de la captura en curso con las estadísticas actuales, tales como tamaño del archivo y el tiempo transcurrieron.

- Haga clic el **botón File Button de la descarga** para descargar un archivo de la captura de paquetes. Usted puede remitirlo en un correo electrónico al soporte de cliente de IronPort para hacer el debug de y resolver problemas cualquier problema.

- Para borrar un archivo de la captura de paquetes, seleccionar uno o más archivos y hacer clic la **cancelación seleccionó los archivos**.

- Para editar las configuraciones de la captura de paquetes con el GUI, la **captura de paquetes** selecta del soporte y el menú de ayuda y el tecleo **editan las configuraciones**.

- Para editar las configuraciones de la captura de paquetes con el CLI, ingrese el **packetcapture > el comando setup**.

Note: El GUI visualiza solamente a las capturas de paquetes que comienzan en el GUI, no los que comiencen con el CLI. Semejantemente, el CLI visualiza solamente el estatus de una captura del paquete actual que comenzó en el CLI. Solamente una captura puede ejecutar el en un momento.

Tip: Para más información sobre las opciones de la captura de paquetes y las configuraciones del filtro, refiera a la sección de los **filtros de la captura de paquetes de** este documento. Para acceder la Ayuda en Línea de AsyncOS el GUI, navegar **para ayudar y apoyar la ayuda del >Online > el índice > P > a la captura de paquetes**.

Capturas de paquetes en las versiones 6.x de AsyncOS y anterior

Esta sección describe el proceso de la captura de paquetes en las versiones 6.x de AsyncOS y anterior.

Comience o pare a una captura de paquetes

Usted puede utilizar el **comando tcpdump** para capturar el TCP/IP y otros paquetes que se transmiten o se reciben sobre una red a la cual se asocie el ESA.

Complete estos pasos para comenzar o parar a una captura de paquetes:

1. Ingrese el **de diagnóstico > red > comando tcpdump** en el CLI del ESA. A continuación se presenta un ejemplo de salida:

```
example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
[]> network

Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> tcpdump

- START - Start packet capture
- STOP - Stop packet capture
- STATUS - Status capture
- FILTER - Set packet capture filter
- INTERFACE - Set packet capture interface
- CLEAR - Remove previous packet captures
[]>
```

2. Fije la interfaz (datos 1, datos 2, o Administración) y el filtro.

   Note: El filtro utiliza el mismo formato que el **comando tcpdump de** Unix.
3. Seleccione el **COMIENZO** para comenzar la captura y **PARAR** para terminarla.

   Note: No salga el menú del tcpdump mientras que la captura está en curso. Usted debe utilizar una segunda ventana CLI para funcionar con cualquier otro comando. El proceso de la captura es una vez completo, usted debe utilizar el Secure Copy (SCP) o el File Transfer Protocol (FTP) de su escritorio local para descargar los archivos del directorio nombrado Diagnostic (refiera a la sección de los **filtros de la captura de paquetes** para los detalles). Los archivos utilizan el formato de la captura de paquetes (PCAP) y se pueden revisar con un programa tal como etéreo o Wireshark.

Filtros de la captura de paquetes

El de diagnóstico > comando CLI de la **RED** utiliza el sintaxis estándar del filtro del tcpdump. Esta sección proporciona la información con respecto a la captura del tcpdump filtra y proporciona algunos ejemplos.

Éstos son los filtros estándar se utilizan que:

- **IP -** Filtros para todos protocolo IP tráfico
- **tcp -** Filtros para todo el tráfico del protocolo TCP
- **filtros del host del IP** para una fuente o un destino específica de la dirección IP

Aquí están algunos ejemplos de los filtros funcionando:

- **host 10.1.1.1 del IP** - Este filtro captura cualquier tráfico que incluya 10.1.1.1 como una fuente o destino.
- **host 10.1.1.1 del IP o host 10.1.1.2 del IP** - este filtro captura el tráfico que contiene 10.1.1.1 o 10.1.1.2 como fuente o el destino.

Para la extracción del archivo capturado, navegue a **var > registro > diagnóstico** o los **datos > pub > diagnóstico** para alcanzar el directorio de diagnóstico.

> **Note**: Cuando se utiliza este comando, puede hacer su espacio en disco ESA llenarse, y puede también causar la degradación del rendimiento. Cisco recomienda que usted utiliza solamente este comando con la ayuda de un ingeniero de asistencia técnica al cliente de Cisco IronPort.