Dispositivos de seguridad contentos FAQ: ¿Cómo usted realiza a una captura de paquetes en un dispositivo de seguridad del contenido de Cisco?

Contenido

Introducción

Este documento describe cómo realizar a las capturas de paquetes en los dispositivos de seguridad del contenido de Cisco.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo de seguridad del correo electrónico de Cisco (ESA)
- Dispositivo de seguridad de la red de Cisco (WSA)
- Dispositivo de la Administración del Cisco Security (S A)
- AsyncOS

Componentes Utilizados

La información en este documento es baja en todas las versiones de AsyncOS.

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.

¿Cómo usted realiza a una captura de paquetes en un dispositivo de seguridad del contenido de Cisco?

Complete estos pasos para realizar a una captura de paquetes (**comando tcpdump**) con el GUI:

1. Navegue **para ayudar y soporte > captura de paquetes** en el GUI.
2. Edite las configuraciones de la captura de paquetes como sea necesario, por ejemplo la interfaz de la red en la cual la captura de paquetes se ejecuta. Usted puede utilizar uno de los filtros predefinidos, o usted puede crear un filtro de encargo con el uso de cualquier sintaxis que sea soportado por el **comando tcpdump de** Unix.
3. **Captura del comienzo del** tecleo para comenzar la captura.
4. **Captura de la parada del** tecleo para terminar la captura.
5. Descargue a la captura de paquetes.

Complete estos pasos para realizar a una captura de paquetes (**comando tcpdump**) con el CLI:

1. Ingrese este comando en el CLI:

```
wsa.run> packetcapture

Status: No capture running


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     (tcp port 80 or tcp port 3128)
```

2. Elija la operación que usted quiere realizar:

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> setup
```

3. Ingrese el tamaño máximo permitido para el capturar archivo (en el MB):

```
[200]> 200
```

```
Do you want to stop the capture when the file size is reached? (If not, a new
 file will be started and the older capture data will be discarded.)

[N]> n

The following interfaces are configured:

1. Management

2. T1

3. T2
```

4. Ingrese el nombre o el número de una o más interfaces de las cuales capturar los paquetes, separados por las comas:

```
[1]> 1
```

5. Ingrese el filtro que usted quiere utilizar para la captura. Ingrese la palabra CLARO para borrar el filtro y capturar todos los paquetes en las interfaces seleccionadas.

```
[(tcp port 80 or tcp port 3128)]> host 10.10.10.10 && port 80


Status: No capture running


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     host 10.10.10.10 && port 80
```

6. Elija la operación del comienzo para comenzar la captura:

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> start


Status: Capture in progress (Duration: 0s)

File Name: S650-00137262569A-8RVFDB1-20080919-174302.cap (Size: 0K)


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management
```

```
 Capture Filter:     host 10.10.10.10 && port 80
```

7. Elija la operación de la **parada** para terminar la captura:

```
- STOP - Stop packet capture.

- STATUS - Display current capture status.

- SETUP - Change packet capture settings.

[]> stop


Status: No capture running (Capture stopped by user)


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     host 10.10.10.10 && port 80
```