Uso del Sniffer del fortigate

El fortigate tiene un comando que permite hacer sniffer del trafico de red como si fuera un tcpdump. La sintaxis es esta:

```
diagnose sniffer packet <interface|any>  '<filtros-tcpdump>' <verbose>
<count> <time-format>
```

Filtros

Los filtros son expresiones iguales a las que se usan en el tcpdump

Ejemplos

```
diagnose sniffer packet any 'host 8.8.8.8' 4 4 l
diagnose sniffer packet any 'host 8.8.8.8 and dst port 53' 4 10 a
diagnose sniffer packet wan1 'dst port (80 or 443)' 2 50 l
```

verbose

- 1→ Muestra la cabecera de los paquetes
- 2→ Muestra la cabecera y los datos de los paquetes por ip
- 3→ Muestra la cabecera y los datos de los paquetes ethernet
- 4→ Muestra la cabecera de los pquetes con su nombre de interfaz
- 5→ Muestra la cabecera, los datos desde la ip con el nombre de la interfaz
- 6→ Muestra la cabecera y los datos de los paquetes ethernet con el nombre de la interfaz

count

número de paquetes a capturar

time-format

- a → hora UTC
- l → hora local

Referencias

- https://kb.fortinet.com/kb/viewContent.do?externalId=11186&sliceId=1
- https://kb.fortinet.com/kb/documentLink.do?externalID=11186
- https://fortixpert.blogspot.com/2016/07/comandos-basicos-de-troubleshooting.html

From:
https://wiki.intrusos.info/ - **LCWIKI**

Permanent link:
https://wiki.intrusos.info/doku.php?id=hardware:fortigate:sniffer

Last update: **182023/01/ 13:36**