Debug

Con debug podemos analizar el flujo del tráfico de red de una conexión.

| debug flow filter ? |
|--------------------------|
| Clear filter. |
| Index of virtual domain. |
| Protocol number. |
| IP address. |
| Source IP address. |
| Destination IP address. |
| port |
| Source port. |
| Destination port. |
| Inverse filter. |
| |

Números de protocolos más usados (https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml)

- Protocol number 1: ICMP
- Protocol number 6: TCP
- Protocol number 17: UDP

Para saber si estamos ejecutando algún filtro

diagnose debug info

Es muy importante después de ejecutar alguno de los comandos de debug, el borrar la traza y deshabilitar el debug

diag debug flow trace stop diag debug reset diag debug flow filter clear diag debug disable

Como ejemplo vamos a analizar el tráfico desde una dirección ip hacia el servidor de google 8.8.8.8

```
diagnose debug reset
diagnose debug flow filter saddr 192.168.1.1
diagnose debug flow filter daddr 8.8.8.8
diagnose debug flow show console enable
diagnose debug enable
diagnose debug flow trace start 10
diagnose debug disable
```

1/3

hardware:fortigate:debug https://intrusos.info/doku.php?id=hardware:fortigate:debug&rev=1563875548

Debug de un puerto

```
diag debug flow filter dport 25
diag debug enable
diag debug flow trace start 100
```

debug de una dirección ip

diag debug flow filter addr 192.168.0.100 diag debug enable diag debug flow trace start 100

DNS

```
diag debug reset
diag debug flow filter clear
diag debug flow filter port 53
```

a la hora de poner filtros podemos poner varios. Por ejemplo



OSPF

diagnose ip router ospf level info diagnose ip router ospf all enable diag debug enable

Significado de los flags de la traza

- [.] = Ack set
- [S] = Syn set
- [S.] = Syn set, Ack Set
- [F] = Fin set
- [F.] = Fin set, Ack Set

- [R] = Reset set
- [R.] = Reset set , Ack Set

Referencias

- https://iserghini.com/2018/07/24/fortinet-fortigate-troubleshooting-traffic-flows/
- https://www.schalley.eu/2016/11/10/troubleshooting-fortigate-command-line-check-debugging-t race-sniffer/
- https://kb.fortinet.com/kb/documentLink.do?externalID=FD31702
- https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD30 038

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

Permanent link: https://intrusos.info/doku.php?id=hardware:fortigate:debug&rev=1563875548



Last update: 2023/01/18 14:15