fortigate, debug, troubleshooting

Debug

Con debug podemos analizar el flujo del tráfico de red de una conexión. Para ver las opciones del comando

```
diag debug flow ?
```

```
 diagnose debug flow filter ?
clear     Clear filter.
vd        Index of virtual domain.
proto     Protocol number.
addr      IP address.
saddr     Source IP address.
daddr     Destination IP address.
port      port
sport     Source port.
dport     Destination port.
negate    Inverse filter.
```

Algunos ejemplos:

- diagnose debug flow filter addr x.x.x.x
- diagnose debug flow filter saddr x.x.x.x (ip origen)
- diagnose debug flow filter daddr x.x.x.x (ip destino)

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

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
```



a partir de la versión 5.6 ya no hace falta poner el la opción **diagnose debug flow show console enable**

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

```
diag debug flow filter port 53
diag debug flow filter addr 192.168.0.100
diag debug enable
diag debug flow trace start 100
```

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-trace-sniffer/
- https://kb.fortinet.com/kb/documentLink.do?externalID=FD31702
- https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD30038

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

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

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