

[fortigate](#), [debug](#), [troubleshooting](#)

Comandos de Debug

```
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.
```

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
```

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
```

Referencias

- <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=FD30038>

From:
<http://wiki.intrusos.info/> - LCWIKI

Permanent link:
<http://wiki.intrusos.info/doku.php?id=hardware:fortigate:debug&rev=1560516624>

Last update: **2023/01/18 14:15**

