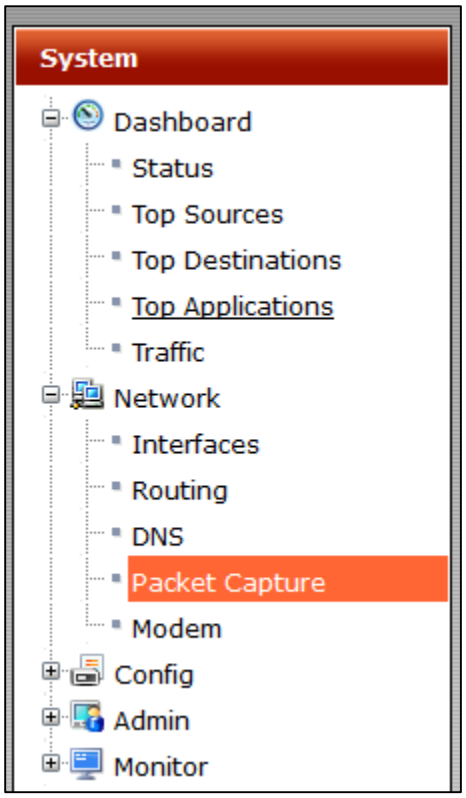
**Make a packet capture using the built-in tool on Graphic User Interface and import it to Wireshark**

FortiOS offers a simple and fast way to make a packet capture through the CLI and got a PCAP file that we can import to Wireshark for further analysis.

Please, follow the following steps:

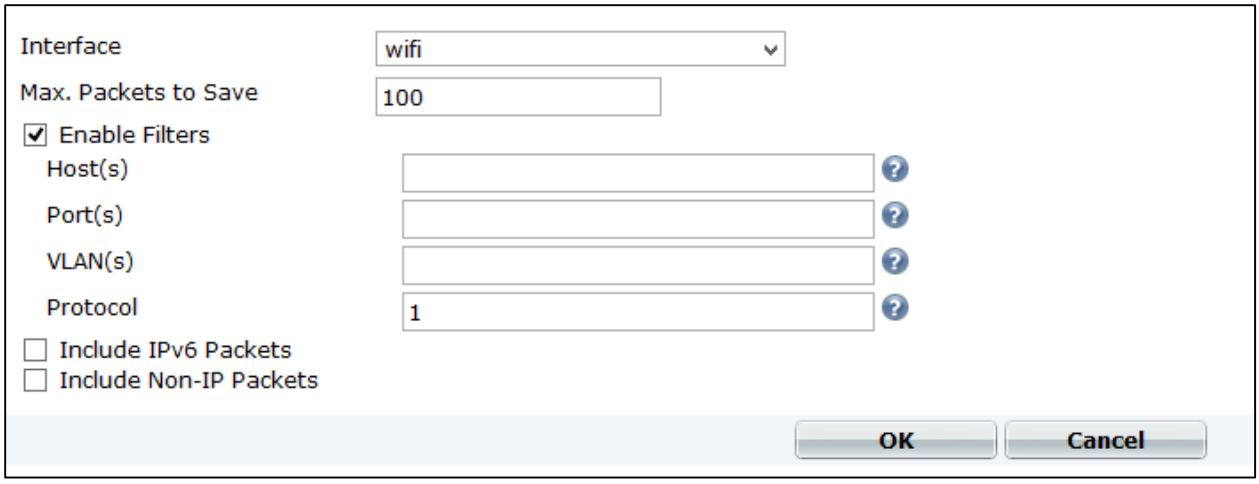
a) On FortiGate GUI,

Click **System -> Network -> Packet Capture** (for reference, see the image below)



b) Click on ‘Create New’


c) Select the Interface which you want to monitor, and select the Max. quantity of packets that you want to capture, in case you want to capture traffic only of one protocol, port, vlan or host, you can mark the box ‘Enable Filters’ too. In this case, I’ll capture only ICMP packets (protocol = 1) passing through WIFI interface. (for reference, see the image below)




d) Click OK and then click on Start button.


e) FortiOS will capture the traffic until reach the Max. numbers of packets you configured or you can also stop it by clicking in the stop button.

f) When it finished, click on Download button to download the PCAP file.


g) Open Wireshark, click on ‘File’ menu and then Click on ‘Open’, select the PCAP file you downloaded and click open.

h) Now, you can see all the packet capture on Wireshark and make further revision to this.