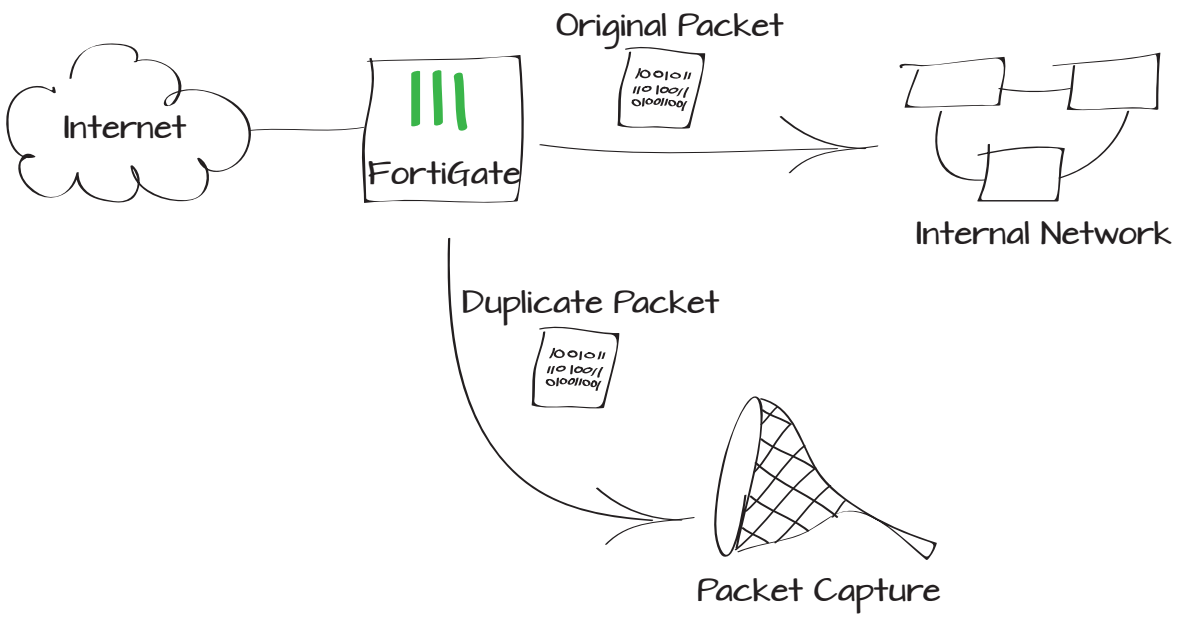
Adding packet capture to help troubleshooting

Packet capture is a means of logging traffic and its details to troubleshoot any issues you might encounter with traffic flow or connectivity. This example shows the basics of setting up packet capture on the FortiGate unit and analyzing the results.

1. Creating a packet capture filter
2. Starting the packet capture
3. Stopping the packet capture
4. Results

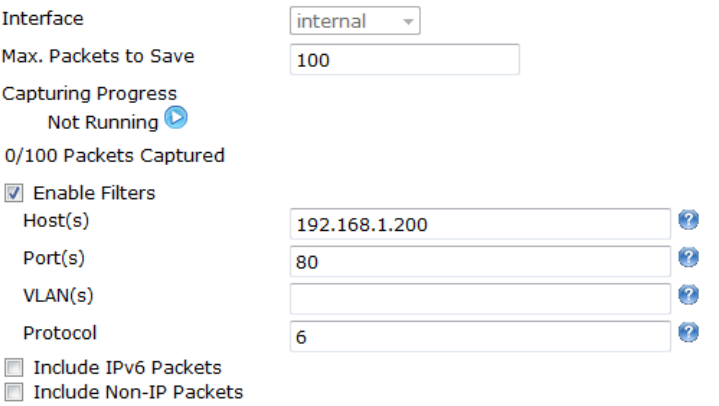


Creating a packet capture filter

Go to **System > Network > Packet Capture.**

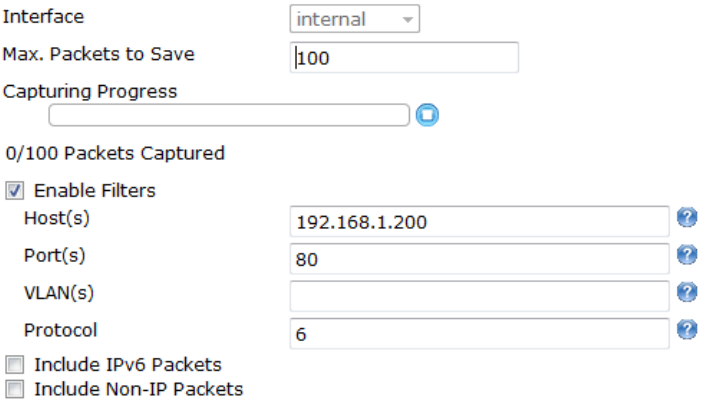
Create a new filter. In this example, the FortiGate unit will capture 100 HTTP packets on the internal interface from/to host 192.168.1.200.

- Host(s) can be a single IP or multiple IPs separated by comma, IP range, or subnet.
- Port(s) can be single or multiple separated by comma or range.
- Protocol can be single or multiple separated by comma or range. Use 6 for TCP, 17 for UDP, and 1 for ICMP.



Starting the packet capture

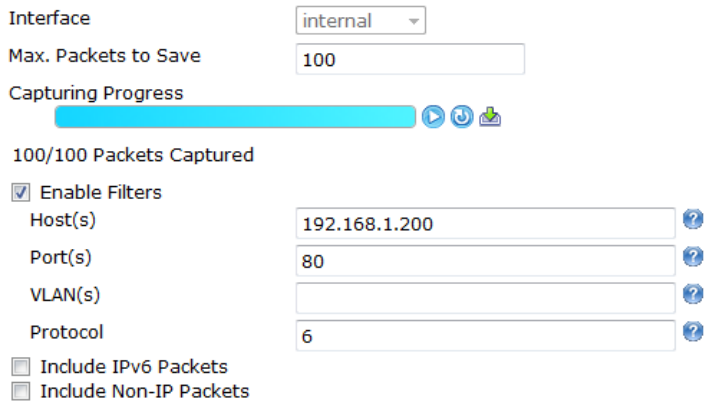
Select **Start** to begin the packet capture. Using an internal computer, or a device set to IP address 192.168.1.200, surf the Internet to generate traffic.



Stopping the packet capture

Once the FortiGate reaches the maximum number of packets to save (in this case 100), the capturing progress stops and you can download the saved pcap file.

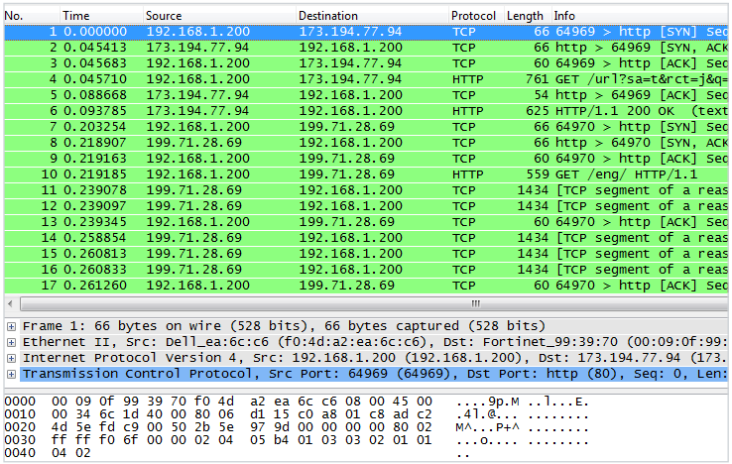
You can also stop the capturing at any time before reaching the maximum number of packets.



Results

Open the pcap file with a pcap file viewer, such as tcpdump or Wireshark.

Adjust the settings in the filter depending on the kind of traffic you wish to capture.



Go to **Log & Report > Event Log > System** to verify that the packet capture file downloaded successfully.