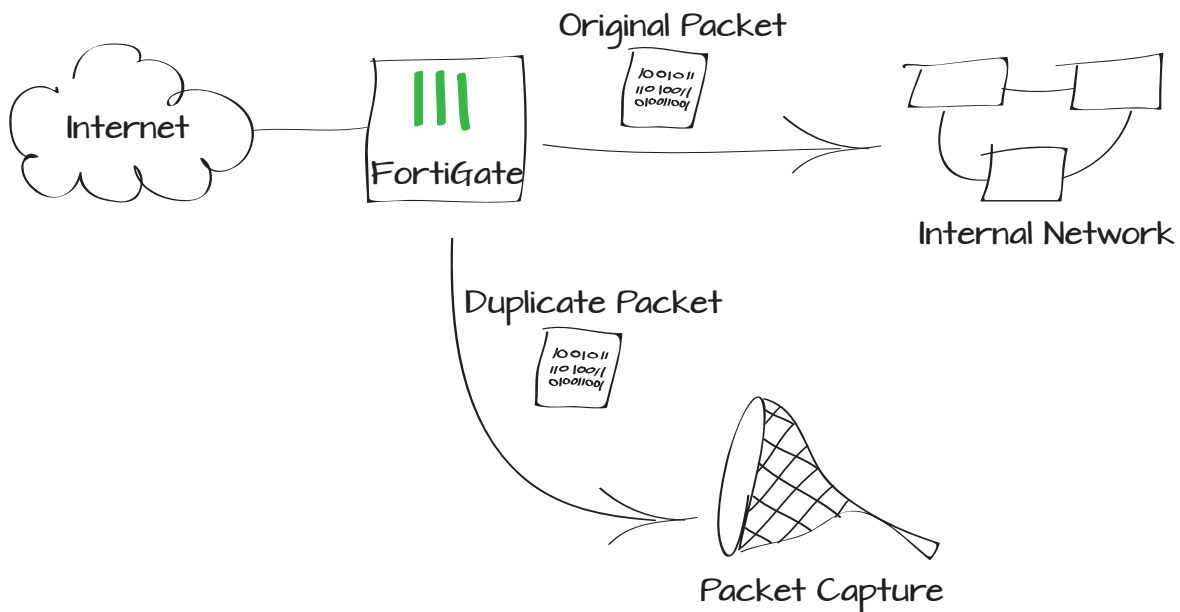


# Adding packet capture to help troubleshooting

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.

Interface	internal
Max. Packets to Save	100
Capturing Progress	Not Running
0/100 Packets Captured	
<input checked="" type="checkbox"/> Enable Filters	
Host(s)	192.168.1.200
Port(s)	80
VLAN(s)	
Protocol	6
<input type="checkbox"/> Include IPv6 Packets	
<input type="checkbox"/> Include Non-IP Packets	

Interface	internal
Max. Packets to Save	100
Capturing Progress	
0/100 Packets Captured	
<input checked="" type="checkbox"/> Enable Filters	
Host(s)	192.168.1.200
Port(s)	80
VLAN(s)	
Protocol	6
<input type="checkbox"/> Include IPv6 Packets	
<input type="checkbox"/> Include Non-IP Packets	

# 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.

Interface:

Max. Packets to Save:

Capturing Progress:

100/100 Packets Captured

Enable Filters

Host(s):

Port(s):

VLAN(s):

Protocol:

Include IPv6 Packets

Include Non-IP Packets

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.200	173.194.77.94	TCP	66	64969 > http [SYN] Seq
2	0.045413	173.194.77.94	192.168.1.200	TCP	66	http > 64969 [SYN, ACK
3	0.045683	192.168.1.200	173.194.77.94	TCP	60	64969 > http [ACK] Seq
4	0.045710	192.168.1.200	173.194.77.94	HTTP	761	GET /url?sa=t&rc=t=j&q=
5	0.088668	173.194.77.94	192.168.1.200	TCP	54	http > 64969 [ACK] Seq
6	0.093785	173.194.77.94	192.168.1.200	HTTP	625	HTTP/1.1 200 OK (text
7	0.203254	192.168.1.200	199.71.28.69	TCP	66	64970 > http [SYN] Seq
8	0.218907	199.71.28.69	192.168.1.200	TCP	66	http > 64970 [SYN, ACK
9	0.219163	192.168.1.200	199.71.28.69	TCP	60	64970 > http [ACK] Seq
10	0.219185	192.168.1.200	199.71.28.69	HTTP	559	GET /eng/ HTTP/1.1
11	0.239078	199.71.28.69	192.168.1.200	TCP	1434	[TCP segment of a reas
12	0.239097	199.71.28.69	192.168.1.200	TCP	1434	[TCP segment of a reas
13	0.239345	192.168.1.200	199.71.28.69	TCP	60	64970 > http [ACK] Seq
14	0.258854	199.71.28.69	192.168.1.200	TCP	1434	[TCP segment of a reas
15	0.260813	199.71.28.69	192.168.1.200	TCP	1434	[TCP segment of a reas
16	0.260833	199.71.28.69	192.168.1.200	TCP	1434	[TCP segment of a reas
17	0.261260	192.168.1.200	199.71.28.69	TCP	60	64970 > http [ACK] Seq

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Ethernet II, Src: Dell\_ea:6c:c6 (f0:4d:a2:ea:6c:c6), Dst: Fortinet\_99:39:70 (00:09:0f:99:39:70)

Internet Protocol Version 4, Src: 192.168.1.200 (192.168.1.200), Dst: 173.194.77.94 (173.194.77.94)

Transmission Control Protocol, Src Port: 64969 (64969), Dst Port: http (80), Seq: 0, Len: 66

```
0000  00 09 0f 99 39 70 f0 4d a2 ea 6c c6 08 00 45 00  ...9p.M ...E.
0010  00 34 6c 1d 40 00 80 06 d1 15 c0 a8 01 c8 ad c2  .4l.@...
0020  4d 5e fd c9 00 50 2b 5e 97 9d 00 00 00 80 02  M...P+A .....
0030  ff ff f0 6f 00 00 02 04 05 b4 01 03 03 02 01 01  ...o....
0040  04 02
```

Status	success	Virtual Domain	root
Level	warning	Timestamp	Thu Mar 21 11:55:20 2013
Log ID	32095	Sub Type	system
User Interface	GUI(172.20.120.21)	User	admin
Action	download	Date/Time	11:55:20 (Thu Mar 21 11:55:20 2013)
roll	65535	Message	Packet Capture File file has been downloaded b