
Subject: iptables NFQUEUE - dumpcap (wireshark) connection doesn't work

Posted by [ttas](#) on Mon, 12 May 2014 18:53:42 GMT

[View Forum Message](#) <> [Reply to Message](#)

Dear professionals! I have an issue. The terms consist of capturing all outgoing TCP-packets of the specified user. But it seems that connection between NFQUEUE target of iptables and dumpcap doesn't work. I decided to check this up with the next example.

```
# iptables -A OUTPUT -m tcp -p tcp --dport=80 -j NFQUEUE --queue-num=2
```

```
# dumpcap -i nfqueue:2 &
```

```
[1] 20424
```

```
# Capturing on nfqueue:2
```

```
File: /tmp/wireshark_nfqueue-2_20140512211225_1QWcTP
```

```
# telnet google.com 80
```

```
Trying 74.125.136.138...
```

```
telnet: connect to address 74.125.136.138: Connection timed out
```

```
Trying 74.125.136.113...
```

```
^C
```

```
# fg
```

```
dumpcap -i nfqueue:2
```

```
Packets captured: 0
```

```
Packets received/dropped on interface nfqueue:2: 0/0 (0.0%)
```

```
# iptables -D OUTPUT -m tcp -p tcp --dport=80 -j NFQUEUE --queue-num=2
```

```
# telnet google.com 80
```

```
Trying 74.125.136.113...
```

```
Connected to google.com.
```

```
Escape character is '^['.
```

```
^]
```

```
telnet> Connection closed.
```

```
# uname -r
```

```
2.6.32-042stab085.17
```

```
# dumpcap -v
```

```
Dumpcap 1.8.10 (SVN Rev Unknown from unknown)
```

Copyright 1998-2013 Gerald Combs <gerald@wireshark.org> and contributors.

This is free software; see the source for copying conditions. There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (64-bit) with GLib 2.26.1, with libpcap, with libz 1.2.3, without POSIX capabilities.

Running on Linux 2.6.32-042stab085.17, with locale en_US.UTF-8, with libpcap version 1.4.0, with libz 1.2.3.

Built using gcc 4.4.7 20120313 (Red Hat 4.4.7-4).

See www.wireshark.org for more information.

```
# iptables
iptables v1.4.7: no command specified
Try `iptables -h' or 'iptables --help' for more information.
```

As you can see the packets get lost. What is the reason of this behavior? How can I fix it? Thanks in advance.
