

# Re: natd port forward times out, tcpdump yields nothing

---

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2008-03/msg00326.html>

---

- *From:* Henri Hennebert <hlh@xxxxxxxxxxx>
  - *Date:* Sat, 22 Mar 2008 14:27:18 +0100
- 

Kage wrote:

Hey guys,

This is a fun one that's stumped people in Freenode ##freebsd.  
Basically, I have this layout:

irc.domain.com -> DNS A -> IRC Jail

When someone connects to irc.domain.com on IRC ports (6667, 8067, etc.), it round-robins them using natd, otherwise it sends all other port requests to the IRC jail as per normal (such as port 80, which is my primary concern). As for having it setup to have ipfw divert to natd, that's done and works, as shown by natd verbose mode:

```
In {default}[TCP] [TCP] 72.65.73.23:2980 -> 207.210.114.45:6667 aliased to  
[TCP] 72.65.73.23:2980 -> 207.210.114.45:6667
```

(For reference)

207.210.114.45 = jail IP

72.20.28.202 = example target IP in the round-robin

72.65.73.23 = my IP

Right now, my ipfw.rules file is as follows:

```
[root@nub /etc]# cat ipfw.rules
```

```
IPF="ipfw -q add"
```

```
ipfw -f -q flush
```

```
#loopback
```

```
$IPF 10 allow all from any to any via lo0
```

```
$IPF 20 deny all from any to 127.0.0.0/8
```

```
$IPF 30 deny all from 127.0.0.0/8 to any
```

```
$IPF 40 deny tcp from any to any frag
```

```
# statefull
```

```
$IPF 50 check-state
```

```
$IPF 60 allow tcp from any to any established
```

Re: natd port forward times out, tcpdump yields nothing

```
$IPF 70 allow all from any to any out keep-state  
$IPF 54999 allow icmp from any to any
```

```
# Include the deny file  
./etc/ipfw.deny
```

```
[snip -- some allowed ports]  
# IRC (natd divert for IRC port-forwarding)  
$IPF 50220 divert natd all from any to 207.210.114.45 6667 via r10  
$IPF 50230 divert natd all from any to 207.210.114.45 8067 via r10  
$IPF 50240 divert natd all from any to 207.210.114.45 8068 via r10  
$IPF 50250 divert natd all from any to 207.210.114.45 6697 via r10  
$IPF 50260 divert natd all from any to 207.210.114.45 7000 via r10
```

You must also divert the response traffic AFAIK eg:

```
$IPF 50220 divert natd all from 72.20.28.202 6667 to 207.210.114.45 via r10
```

```
# keep these two IRC ports normally open for BNC  
$IPF 50270 allow all from any to any 31337 in  
$IPF 50380 allow all from any to any 31337 out  
[snip -- more allowed ports]  
# deny and log everything  
$IPF 55000 deny log all from any to any
```

-----

Here's a dump of ipfw show, with some stuff cut out for space purposes  
(they're just denied DDoS IPs)

```
[root@nub /etc]# ipfw show  
00010 61124 16056802 allow ip from any to any via lo0  
00020 0 0 deny ip from any to 127.0.0.0/8  
00030 0 0 deny ip from 127.0.0.0/8 to any  
00040 0 0 deny tcp from any to any frag  
00050 0 0 check-state  
00060 670616 455926379 allow tcp from any to any established  
00070 16213 14071853 allow ip from any to any out keep-state  
[snip]  
50220 468 22464 divert 8668 ip from any to 207.210.114.45  
dst-port 6667 via r10  
50230 0 0 divert 8668 ip from any to 207.210.114.45  
dst-port 8067 via r10  
50240 0 0 divert 8668 ip from any to 207.210.114.45  
dst-port 8068 via r10  
50250 0 0 divert 8668 ip from any to 207.210.114.45  
dst-port 6697 via r10  
50260 0 0 divert 8668 ip from any to 207.210.114.45  
dst-port 7000 via r10
```

Re: natd port forward times out, tcpdump yields nothing

Re: natd port forward times out, tcpdump yields nothing

```
50270 1 60 allow ip from any to any dst-port 31337 in
54999 66 3991 allow icmp from any to any
55000 4364 343609 deny log logamount 100 ip from any to any
65535 29 4176 allow ip from any to any
```

My natd.conf is as follows:

```
[root@nub /etc]# cat natd.conf
# Nub.Core NATd
verbose
alias_address 207.210.114.45
log
log_denied
log_ipfw_denied
pid_file /var/run/natd.pid
```

```
### IRC Redirect Ports
# 6667
```

If I understand man natd

```
redirect_port tcp 72.20.28.202:6667 207.210.114.45:6667 207.210.114.45:6667
```

^^^^^^^^^^^^^^

Traffic is coming from 72.65.73.23 – so the rule don't apply

```
[root@nub /etc]#
```

And, as stated above, I am showing connection diverts to natd. When I run the following three tcpdumps:

```
tcpdump -s 0 -w me_to_nat.pcap -vvv -i rl0 src host 72.65.73.23 and
dst host 207.210.114.45 and dst port 6667
tcpdump -s 0 -w nat_to_jail.pcap -vvv -i rl0 src host 72.20.28.202 and
dst host 207.210.114.45 and dst port 6667
tcpdump -s 0 -w jail_to_nat.pcap -vvv -i rl0 src host 207.210.114.45
and dst host 72.20.28.202 and src port 6667
```

Only the "me\_to\_nat.pcap" gets any data. The rest are 0 bytes. Example:

```
-rw-r--r-- 1 root wheel 0 Mar 21 14:57 jail_to_nat.pcap
-rw-r--r-- 1 root wheel 16384 Mar 21 15:24 me_to_nat.pcap
-rw-r--r-- 1 root wheel 0 Mar 21 14:57 nat_to_jail.pcap
```

So, can anyone diagnose and fix this? Thanks.

(P.S.: I'm aware of the DNS methods of doing round-robin, but please

Re: natd port forward times out, tcpdump yields nothing

keep that from this discussion. I need to port-forward round-robin,  
not whole DNS)

---

freebsd-net@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-net>

To unsubscribe, send any mail to "freebsd-net-unsubscribe@xxxxxxxxxxx"