

Re[2]: Bad loopback traffic not stopped by ipfw.

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2004-02/0290.html>

From: Andrew Riabtsev (*resident_at_b-o.ru*)

Date: 02/25/04

Date: Wed, 25 Feb 2004 16:47:03 +0300

To: Iasen Kostov <tbyte@OTEL.net>

Иәәәәә Iasen,

Wednesday, February 25, 2004, 3:37:25 PM, you wrote:

IK> netstat -s -p ip

IK> .

IK> .

IK> .

IK> 3575124 datagrams with bad address in header

IK> Could it be this that drops "bad" packets before they enter the IPFW ?

To me it would be also interesting to know where this traffic comes from. I have same on my local net:

```
# tcpdump -neifxp0 src or dst 127.0.0.1
```

```
tcpdump: listening on fxp0
```

```
16:26:23.280737 0:50:fc:ed:d4:4 0:02:55:b0:90:e4 0800 60: 127.0.0.1.80 > 192.168.141.148.1928: R 0:0(0)  
ack 1986723841 win 0
```

```
16:26:23.285831 0:d:61:e:3f:c3 0:02:55:b0:90:e4 0800 60: 127.0.0.1.80 > 192.168.213.167.1571: R 0:0(0)  
ack 812253185 win 0
```

```
16:26:23.287642 0:1:2:9c:cf:e2 0:02:55:b0:90:e4 0800 60: 127.0.0.1.80 > 192.168.118.205.1046: R 0:0(0)  
ack 1959723009 win 0
```

```
16:26:23.297289 0:4:79:68:14:9c 0:02:55:b0:90:e4 0800 60: 127.0.0.1.80 > 192.168.214.208.1997: R 0:0(0)  
ack 1905917953 win 0
```

```
16:26:23.297555 0:c0:df:13:87:c4 0:02:55:b0:90:e4 0800 60: 127.0.0.1.80 > 192.168.53.212.1836: R 0:0(0)  
ack 1137442817 win 0
```

dst mac-address is mac of fxp0 and src addresses is macs from local net not just nonexistent macs. It could be some kind of attack or it is flood from broken device in local net or maybe something else, i'll try to find it out. Let me know if You find out something new.

Andrew <mailto:resident@b-o.ru>

freebsd-net: Re[2]: Bad loopback traffic not stopped by ipfw.

freebsd-net@freebsd.org mailing list

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

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