

## Re: Localhost traffic and ipfw rules

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-02/0082.html>

---

**From:** Flemming Jacobsen (*fj\_at\_batmule.dk*)

**Date:** 02/15/04

Date: Sun, 15 Feb 2004 07:57:24 +0100

To: erschulz@comcast.net

erschulz@comcast.net wrote:

> *I seem to be stumped on this one. I have TCP packets*  
> *destined to my external interface from 127.0.0.1 (Ack+Reset*  
> *zero data) with source MAC of my default gateway and I*  
> *can't seem to block this traffic.*  
>  
> *Snort picked up the traffic and I have confirmed with*  
> *tcpdump. So I decided I needed to examine my anti-spoof*  
> *rules. I already had this one*  
>  
> *deny ip from any to 127.0.0.0/8 in recv \${oif}*

You probably want this as your first 3 rules:

```
allow ip from any to any via lo0
deny ip from any to 127.0.0.0/8
deny ip from 127.0.0.0/8 to any
```

Some say that the TCP stack already takes care of this, but I like these rules in my set – just to be 100% sure.

About the rest of your question, you probably are blocking the traffic with your rules.

Bpf which tcpdump and snort uses to snoop packets, picks up packets before your ipfw rules are applied, thus you see the full packet feed.

Regards  
Flemming

PS: Please insert linebreaks so your lines are no longer than 70–75 characters.

--

Flemming Jacobsen

Email: [fj@batmule.dk](mailto:fj@batmule.dk)

----- If speed kills, Windows users may live forever. -----

---

freebsd-security@freebsd.org mailing list

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

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