

## Re: Linux firewall/IDS/NAT suggestions

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2003-06/0022.html>

---

**From:** J Norfleet ([jnorfleet\\_at\\_picusnet.com](mailto:jnorfleet_at_picusnet.com))

**Date:** 05/31/03

To: "Petty, Robert" <[rpetty@DenverNewspaperAgency.com](mailto:rpetty@DenverNewspaperAgency.com)>, [focus-linux@securityfocus.com](mailto:focus-linux@securityfocus.com)

Date: Sat, 31 May 2003 02:18:05 -0400

On Friday 30 May 2003 11:54 am, Petty, Robert wrote:

–snip–

Just to add a few things.

> Which kernel would be best? 2.0.x, 2.2.x, or 2.4.x?

MHO. Go with 2.4 and iptables (Stateless firewall), for reasons mentioned before

- > Should snort be running on the firewall machine or another machine? If on
- > another machine, should I put the firewall and IDS box on a hub as the
- > first hop so they both see the same traffic? The customer's router is not
- > manageable (linksys) and they have no budget for a Cisco Router or PIX.
- >
- > The Linux box will serve as a secondary NAT layer, any pitfalls with this?

iptables handles NAT'ing between interfaces, controlling of DMZ's, etc. If I understood the question right?

- > Should SSH go to the firewall machine or be passed through to an internal
- > Linux box?

Through iptables, you can specify traffic on a certain interface (eth0), for a set port (22), from a certain host (1.2.3.4). Then there's tcp wrappers.

- > Should the NAT and Firewall rules be written and maintained on CD-R media
- > so a malicious attacker cannot hide rule changes? Should the firewall be
- > re-initialized on a schedule to ensure the live rules are those from the
- > read-only media?

I've heard of the whole linux OS and firewall running off a CD. (Trinux has a few ISO's :)

- > Last, but not least, what's a good HowTo that can be used as a basis? I
- > would prefer one that starts off a little more strict so I can simplify
- > rather than have to bone up on all of the current vulnerabilities.

SecurityFocus Linux: Re: Linux firewall/IDS/NAT suggestions

<http://www.linuxguruz.com/iptables/howto/iptables-HOWTO.html>

<http://www.netfilter.org/documentation/tutorials/blueflux/iptables-tutorial.html>

>

> *Thanks for any replies!*

>

> *Robert*

np,

jnorfleet