

## Re: firewalling off the world?

**Source:** <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2001-12/0718.html>

---

**From:** ALiaS ([alias@work.com](mailto:alias@work.com))

**Date:** 12/27/01

From: "ALiaS" <[alias@work.com](mailto:alias@work.com)>  
Date: Thu, 27 Dec 2001 07:40:50 GMT

Greets,

Never really bother to post, but I've still got \$0.02 available balance on my credit card after Xmas, so what the hey! ;)

> *The question still remains, why should discrimination against country by IP# be either (a) on-topic for cols or (b) tolerated?*

- a) Its on-topic in the sense that it asks if what he was proposing is a security advantage. (Which we know its not, but dont shoot the guy for asking)
- b) Tolerance is a 2 edged sword. Even those you disagree with should be tolerated. I really dont think that its racially slanted anyway, I mean we all know that its punk US teenagers hacking those boxes in Asia anyway! ;)

Walter was spot on with his analysis, except for one thing. In the case of the guy who copped the dictionary attack, blocking at his core firewall would only stop traffic within his network. He would still be charged by his ISP as they still deliver all the connection attempts to his core router. Try option i) below to achieve the desired result.

- If you are fed up with massive scans on your network, either;
  - i) Get your provider to provide upstream acls, restricting access, for instance, to a set range of ip addresses for port 80 access etc etc. (At the peak of Nimda season, the 5 class Cs that I administer were copping 250+ connects per minute at the core firewall. I got in touch with my provider and now of the 1250 odd addresses, only 8 per netblock are permitted. More than required, but now only 4% of the connects get to my core. If you are systematic with your ip addressing, you can setup similar acls for pretty much all of your vital servers and say goodbye to huge quantities of scan traffic.
  - ii) Run snort or similar ids. Ensure that you keep your rulesets up to date and configure it only to inform you of threat levels that you give a shit about. Provided that you keep your servers patched, all those scans for Nimda, portmap, SSH etc will fail. Who gives a shit if your logs are big?
  - iii) Ok, so you give a shit that your logs are big. Then run a firewall with limit matching like iptables. Set it up to log only a proportion of the

attempts.

The lessons are;

- You cant secure your system by blocking any netblocks other than 0.0.0.0/0.0.0.0
- You CAN reduce traffic by setting up acls at you upstream provider
- It generally isnt the people in China or Korea who are scanning your network, its people who have hacked their boxes. If all network providers in the US setup decent egress filtering, maybe those Chinese boxes wouldnt be compromised in the first place.

Its all about egress filtering people. Prevention is better than cure.

ALiaS

"Tim Haynes" <[usenet@stirfried.vegetable.org.uk](mailto:usenet@stirfried.vegetable.org.uk)> wrote in message news:86zo46rlzd.fsf@potato.vegetable.org.uk...

> *Walter Dnes* <[waltdnes@waltdnes.org](mailto:waltdnes@waltdnes.org)> writes:

>

>> *On Sat, 22 Dec 2001 19:00:48 -0500, John Doe, <[expires2002@hotmail.com](mailto:expires2002@hotmail.com)>*

>> *wrote:*

>>

>> *Ian reacted a bit emotionally. Let's try a more cold calculated*

>> *response...*

>

> *Hmmmm.*

>

>> *This does \*NOT\* increase your security by a factor of 3. If your system*

>> *is insecure to begin with, it'll get cracked by a "domestic" machine. If*

>> *you have vulnerability X, the first attempt will compromise your machine.*

>> *Having 100 attempts rather than 400 attempts won't really make any*

>> *difference. If it's secure, it won't get cracked, regardless of the*

>> *number of attempts.*

>

> *Quite so. Only 1 probe is needed, 100 or 400 makes stuff-all difference.*

>

> *The question still remains, why should discrimination against country by*

> *IP# be either (a) on-topic for cols or (b) tolerated?*

>

> *~Tim*

> --

> *Bagpuss gave a big yawn,*

> [piglet@stirfried.vegetable.org.uk](mailto:piglet@stirfried.vegetable.org.uk)

> *and settled down to sleep. /<http://spodzone.org.uk/>*

- 
- **Next message:** [Cam Haughton: "Re: small linux firewall/router advice"](#)
  - **Previous message:** [baho-utot: "Re: password Generator"](#)
  - **In reply to:** [Tim Haynes: "Re: firewalling off the world?"](#)

comp.os.linux.security: Re: firewalling off the world?

- *Next in thread:* JimM: "Re: firewalling off the world?"
- *Messages sorted by:* [ date ] [ thread ] [ subject ] [ author ] [ attachment ]