

Re: Use iptables to block all non-US ssh traffic

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2005-09/0217.html>

From: Moe Trin (*ibuprofin_at_painkiller.example.tld*)

Date: 09/18/05

Date: Sat, 17 Sep 2005 22:32:42 -0500

In the Usenet newsgroup comp.os.linux.security, in article
<Ym%We.30621\$ua.299227@twister.southeast.rr.com>, base60 wrote:

>Moe Trin wrote:

>> China has no "Class As".

>

>Sorry, I use China interchangeably with APNIC.

There's one heck of a large difference, as shown in my reply to
"matt_left_coast". But to answer that...

```
[compton ~]$ cut -d' ' -f3 < IP.ADDR/stats/APNIC | sort | uniq -c | sort -n
+1 | column
  1 255.0.0.0 240 255.254.0.0 1095 255.255.0.0
  4 255.192.0.0 301 255.255.128.0 1118 255.255.240.0
  8 255.224.0.0 427 255.255.192.0 1177 255.255.254.0
 25 255.240.0.0 661 255.255.248.0 4190 255.255.255.0
 81 255.248.0.0 961 255.255.252.0
138 255.252.0.0 1060 255.255.224.0
[compton ~]$ grep -E '255.(0|192).0.0' IP.ADDR/stats/APNIC
CN 59.192.0.0 255.192.0.0 allocated
JP 60.64.0.0 255.192.0.0 allocated
JP 126.0.0.0 255.0.0.0 allocated
JP 219.0.0.0 255.192.0.0 allocated
JP 220.0.0.0 255.192.0.0 allocated
[compton ~]$
```

The "allocated" means that it has been assigned to a smaller IR (in this case nic.ad.jp – the national registry for Japan and cnic.net.cn – the national registry for China) and that organization has allocated/assigned chunks to ISPs and local IRs. Gone are the days when you could get a /8, and APNIC is rather stingy handing out /9s and /10s it would seem.

>> Just how, exactly? I've just shown that IP blocks are assigned on what

>> amounts to be a random basis. Are you going to block on TLDs?

>

>Yes.

Both "matt_left_coast" and I have shown that to be impractical.

*>Agreed, but please note that I said non-US based and, as you've
>noted, .com etc. do not fit that description. I'm referring to .jp etc.*

So, whois Sony? Matsushita? NEC? Mazda? Toyota? I know it varies a lot, but checks of my spam traps on the home firewall show Japan not even in the top 10. Actually, I see ABOUT 38 percent of the stupid stuff comes from the US (mainly zombies on cable nets), followed by China 11%, Korea Canada and Brazil each with 6%, France with 3%, and so on. Even Taiwan and Hong Kong have been pushed out of the top ten. And yes, I am in the USA. I don't run (or even have access) to the corporate firewall, but the last time I asked, their results were broadly similar – main stuff from cable zombies.

*>Our default posture is to deny unless explicitly allowed. Using the
>TLDs etc. as filters is mostly to reduce the volume of IDS alerts.*

WTF are they getting so far as to hit IDS??? Sounds like your firewall isn't set well, and/or your "available services" needs work.

*>If we do wrap someone out, they receive contact info and I find that
>legitimate people aren't shy about complaining.*

If you are referring to mail, I don't handle the company stuff (that's a corporate problem), but because we're multi-national, a lot of our regional mail goes to regional offices direct. I know they are running spam-assassin, but know little how it's configured.

If you are referring to web services, those are in DMZs within the regions, and mainly run from read-only media. FTP downloads are similar. We don't accept uploads. PERIOD.

Old guy