

# Re: IPTables rules and hosts that use DHCP

---

*Source:* <http://linux.derkeiler.com/Newsgroups/comp.os.linux.misc/2007-12/msg01694.html>

---

- *From:* "K. Jennings" <kjennings@xxxxxxxxxxxxxxxx>
  - *Date:* Thu, 27 Dec 2007 20:35:43 -0000
- 

On Thu, 27 Dec 2007 14:03:59 -0600, Moe Trin wrote:

On Thu, 27 Dec 2007, in the Usenet newsgroup comp.os.linux.misc, in article <pan.2007.12.27.13.58.10@xxxxxxxxxxxxxxxx>, K. Jennings wrote:

I have a set of IPTables rules to keep SSH attacks at bay – you know, to prevent script kiddies from hammering my servers with oodles of password authentication requests with all sorts of passwords and/or usernames. Essentially, the rules blacklist hosts that attempt to connect more than three times within a 30 second time interval. I also have an IPTables rule that exempts some hosts from such constraints – that is, SSH connections from such hosts are accepted at any connection rate.

Do you really need to allow access to the entire world?

I have to allow a priori potential access from anywhere.

The proble that I have is that one of those hosts uses DHCP, and its IP address changes with time. I use DynDNS services so that I can use the same name (let's call it A) for that host, with the guarantee that it will always resolve to the right IP address. However, I notice that when I use the name A in my IPTables rule, when checking out the rule with iptables -L the name actually used is the one assigned to the particular IP address in use at the time the rule was defined – which is fine until the host I am interested in changes its IP address.

I'm assuming that "A" is some remote host you want to allow. There really isn't a dynamic way out of things. What I've been doing is to allow access to the pool of addresses that the allowed host may get assigned. For example, my sister and I act as backup servers for each other (nightly backup diffs get sent to the "remote" server), and I know

## Re: IPTables rules and hosts that use DHCP

she will get an address out of a /20 range (lets say 198.18.32.0 – 198.18.47.255), so I allow access from that range to the port where the backup service is listening. I allow other access to a different service to a /24 for a similar reason. This doesn't prevent the zombie problem, but it sure knocks back the number of attempts that I see.

The problem that I have is that A seems to be able to take up a wide variety of IP addresses. They don't seem to be constrained to a specific network, as far as I can tell. Indeed, not even the first components of the IP addresses used are always the same.

Is there a way around this? Unfortunately, reconfiguring my SSH servers so that password authentication is not accepted is not an option.

Do you HAVE to have your SSH server on port 22,

Yes. See below one of the reasons why.

or can you move it to a port less frequented by zombies/skript\_kiddiez? Your clients do have to be aware of the "non-standard" port, but (depending on the tool they are using to access) this is USUALLY trivial.

That is true. The problem is that some people who would like to connect to my boxes work with ISPs that do traffic management, and connections to non-standard ports are severely limited, performance-wise, in such cases.

.