

Re: Blocking incoming IP address immediately

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2004-11/0449.html>

From: Tim Haynes (usenet-20041129_at_stirfried.vegetable.org.uk)

Date: 11/29/04

Date: Mon, 29 Nov 2004 15:56:43 +0000

"Jeff Franks" <jfranks1970@charter.net> writes:

> *I have a gaming server and am trying to create an IPTABLES firewall that
> will allow me to "ban" an IP. I have been able to do this, but the ban only
> takes place if I reboot the firewall pc.*

Yuck? WTF?

> *I need this to be something that can take effect immediately. If I have a
> cheater/abuser in the game, I need to be able to script something so that
> I can block all traffic from that person's IP or IP Range. From what I've
> dug up, this should be doable with a simple :
>
> iptables -A INPUT -s 123.45.67.89 -j DROP*

Well yeah, that should work. Does what it says on the tin – appends a rule taking packets from that ip and drops them, to the end of the INPUT chain.

Now.

You might've wanted to REJECT them instead, for speed – up to you in this case.

Depending on how many concurrent packets hitting your server are destined for the game rather than other services, it might make sense to peel off a chain and call it `abusers', so you check incoming packets first whether they're for the game service (by port#), then you push them through the game-specific abusers chain where naughty people are REJECTed/DROPped, or otherwise if it's not for the game, it bypasses all that processing and gets handled normally.

Second thought: depending on what else happens in your iptables `INPUT' chain, you might find that appending or prepending the rule after everything else is daft. This is where having a separate chain for abusers makes sense because you can firmly stick the rule on either end of that chain in the knowledge that it's not messing-up your firewall order any further (e.g. the abuser should be able to send you a mail (25/tcp) saying

sorry).

I'm thinking in terms of my firewall script at
<<http://spodzone.org.uk/packages/secure/iptables.sh>> here, but with a few
extra lines:

```
iptables -N abusers # somewhere near the other -N lines

iptables -p tcp --dport 1234 -j abusers # deflect them through chain
iptables -p tcp --dport 1234 -j ACCEPT # otherwise let them past
...
iptables -j DROP
```

then a paragraph of lines like:

```
iptables -A abusers -s 123.45.67.89 -j REJECT
...etc.
```

> *I've also seen where the -SYN option should be used and I've played with
> the ESTABLISHED and RELATED options. ANY ideas on this will be greatly
> appreciated.*

I don't think you want to distinguish at all. It's enough that the
originator of the packet has been a Bad Boy, not whether it's a new one or
not. Reject them mid-connection, why not :)

[snip entire current script]

~Tim

```
--
Famous moments vanish without trace      |piglet@stirfried.vegetable.org.uk
Trees grow tall, fields grow wheat       |http://pig.sty.nu/
```