

# [fw-wiz] Best way to drop forged TCP packets with RST flag set from comcast traffic shaping devices with iptables

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2008-04/msg00014.html>

---

- *From:* "Chris Smith" <[chris.smith@xxxxxxxxxxx](mailto:chris.smith@xxxxxxxxxxx)>
  - *Date:* Mon, 7 Apr 2008 19:58:33 -0700
- 

Hi all,

I found this while reading Slashdot today, and decided to ask about it.

[http://systems.cs.colorado.edu/mediawiki/index.php/Broadband\\_Network\\_Management](http://systems.cs.colorado.edu/mediawiki/index.php/Broadband_Network_Management)

I don't really want to wait for the results of any FCC investigation that may or may not find that Comcast is violating fair use policy, network neutrality, etc.

I would like to use IP tables to start blocking these forged TCP packets as they hit the external interface of a Linux firewall.

I've noticed a lot of different functionality that can be enabled or modularized in the 2.6 kernel for netfilter. I.E. Rate limiting, Flag matching support, state match etc.

What is the best way to configure the netfilter options in the kernel config to identify and drop these invalid TCP RST packets? What Iptables rules can be used to implement and filter these forged packets?

[fw-wiz] Best way to drop forged TCP packets with RST flag set from comcast traffic shaping devices with iptables

It seems that using the old method that I'm aware of, (Filtering these packets because they are not part of an already related or established connection) is no longer adequate. This seems to be a very transparent man in the middle centric approach that Comcast is using.

One method that they seem to be using which is particularly interesting is that the TTL value set in the incoming forged TCP packets, often has a specific static value. I.E. 30

Another netfilter option that can be enabled is TTL match support. Can this functionality be used to find these packets? Could TTL match support be used in combination with rate match support to detect if more than X TCP packets with RST flag set and with a TTL value of 30 arrived in a given time frame? I.E. more than 1 every five seconds, and if so drop them? Would the packets have to be queued in order for this to work?

Would this be a reliable way to find and block forged packets?

Please share your thoughts. I'm just entertaining a few ideas here.

---

firewall-wizards mailing list  
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>

[fw-wiz] Best way to drop forged TCP packets with RST flag set from comcast traffic shaping devices with iptables