
Subject: Re: Iptables in HN or VE?

Posted by [marcel.chastain](#) on Tue, 17 Jun 2008 15:50:24 GMT

[View Forum Message](#) <> [Reply to Message](#)

For any troublesome ports, I throttle inbound and outbound connections, and log any problems. Now, anywhere in your iptables rules for the FORWARD chain you can throttle it, esp for inbound ssh attacks, spam, outbound scans, MSSQL worms, etc

Inbound

-A throttle_15 -m state --state NEW -m recent --set

-A throttle_15 -m state --state NEW -m recent --update --seconds 60 --hitcount 15 -j log_throttle

Logging to go with it

-A log_throttle -m limit --limit 5/s -j LOG --log-prefix "THROTTLE: "

-A log_throttle -j DROP

Note the traffic direction

FROM venet TO the outside world

This is outbound/egress throttling to port 80

-A FORWARD -i venet0 -o eth0 -m state --state NEW -p tcp -m tcp --dport 80 -j throttle_15

FROM outside world TO venet

This is inbound/ingress throttling to port 22

-A FORWARD -o venet0 -i eth0 -m state --state NEW -p tcp -m tcp --dport 22 -j throttle_15

Note: you can omit the '-i' inbound interface specification in the above rules, and it's just as effective, if not more so. Sometimes packets show up that don't have an inbound interface, which I don't understand.

Hope this helps.
