Subject: Re: Cant block DDoS to a VPS? How to do it?
Posted by grep on Sun, 17 Nov 2013 02:16:32 GMT
View Forum Message <> Reply to Message

When you block IPs on HN Node it will not affect openvz containers.
You need to block bad IPs on container. Maybe you can block on HN when drop IPs to forward chain and not to input.

If
212.185.56.58 - - [16/Nov/2013:21:32:49 +0000] "-" 408 0 "-" "-"Is an attacking IP it seems to be very simple HTTP flood which you can block it easy. Just write a script which parse the http log and check the num of connections which call /. If greater than x then drop. Or use mod security, but this will use more cpu.
Or just block all traffic which has no referrer.

And it seems that bad IPs just come from one subnet - block it & write abuse with tcpdump file as proof.

If you delete the IP from your Hostsystem the traffic should be nullrouted. If not then ask your dc, maybe they 'hard-route' the IP to your server.

If you want to try migrating the DDoS check out litespeed and nginx. But your HN must have enough network speed and if ddos goes to hard then you may get in trouble with your dc.

Quote:
::1 - - [16/Nov/2013:21:32:59 +0000] "OPTIONS * HTTP/1.0" 200 152 "-" "Apache/2.2.14 (Ubuntu) (internal dummy connection)"
FULLL of thisnormal.