## Subject: Any way to limit SSH bruteforce scanning of VPS's on the node?
Posted by mustardman on Wed, 21 Dec 2011 01:44:32 GMT

View Forum Message <> Reply to Message

Hi,

My VPS's are getting a lot of SSH bruteforce scanning. It's getting to the point where it's adding a significant amount of load to the nodes. Besides using something other than port 22 on each VPS and doing things with iptables on each VPS, is there anything I can do on the node?

I was thinking maybe rate limit port 22 in iptables at the node before the VPS forward statements.

I don't want to do this on a production system though so I was wondering if anyone has successfully done something like this.

The iptables statements I have tried in individual VPS's are:

```
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set --name SSH
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 60
--hitcount 6 --rttl --name SSH -j DROP
```

It would be easier to do it globally on the node and perhaps there are other benefits to dropping the packets before they get forwarded.

I have a bunch of existing VPS's so I don't want to have to go through all of them and make changes. I'll probably use a different port on new VPS's but I still gotta deal with the existing ones.