Subject: iptables on VE0 to prevent SSH Attacks?
Posted by phpfreak on Wed, 01 Feb 2006 15:18:34 GMT
View Forum Message <> Reply to Message

Had an interesting scenario this morning. We had a brute force scan network wide and it was hitting all of the VE's on a single server. When this happened, we had about 250 sshd processes running and visible in TOP on the host machine. Of course this spiked the load considerably.

I tried to drop the offending host's IP address on venet0 on the host machine (VE0) but it had no effect.

Is there any simple way to have a firewall rule on the host machine that can affect all of the VE's in a case like this?

Please let us know.

Thanks,