Subject: Protecting your node/containers from attacks and spam
Posted by DaneV on Thu, 11 Nov 2010 19:35:07 GMT
View Forum Message <> Reply to Message

We currently have 6 servers running 130 OpenVZ containers in total.
Now that the amount of VZ servers are growing, so do the occasional problems we get with attacks and/or spam being send from one of the containers. The reason for this is that we offer unmanaged services, and unfortunately not everyone knows how to secure their server well (only 40% of the clients actually have a firewall).

Allthough we actively try to push our clients into securing their server, our "education" is not enough to counter all the problems. And our "fix" right now is to block the container (iptables forward drop) after we get the message at our abuse email adress.

I am looking for ways to limit the damage done by a container that is abusing the hardware/network by sending spam, or doing a portscan (which our network provider is not happy about when this happens).

I Would like to be able to drop traffic from and to a container that is behaving strange.

Like opening an insane amount of connections, or sending big amounts of traffic trough port 25. Because we use venet, and all the traffic goes trough the HW node i`m sure i could set some iptables rules on the hardwarenode to block certain attacks (incoming and outgoing), portscans and possibly even large amounts of traffic on port 25.

Has anyone done this kind of thing, and is able to put me in the right direction. Maybe some essential iptable rules i`m missing?