Subject: Re: CSF xt_connlimit on vm failed
Posted by lelik67 on Fri, 10 Feb 2012 15:06:36 GMT
View Forum Message <> Reply to Message

The issue is that, due to the way RH builds iptables, there have been longstanding disparities between the iptables userspace tool and the kernel. For example, in Fedora 6/RHEL 5/CentOS 5, although there is an iptables module in /lib/iptables/libipt_connlimit.so which supports the connlimit match in iptables, there is no corresponding netfilter module in
/lib/modules/(version)/kernel/net/ipv4/netfilter/
to handle it in the kernel.

Since there is no stock kernel support for connlimit, the iptables module included in these distros is rather useless.

To have connlimit working there are three options:

1. Upgrade your node kernel to a newer version (Co-operation of your VPS provider is required).

The connlimit module finally went into mainline at kernel v2.6.23.
xxx://xxx.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.23

Latest stable kernel for RHEL5 2.6.18 does not have it.
xxx://wiki.openvz.org/Download/kernel/rhel5/028stab095.1

But latest stable kernel for RHEL6 2.6.32 does:
xxx://wiki.openvz.org/Download/kernel/rhel6/042stab044.17

2. Patch it and maintain your own build (Super co-operation of your VPS provider is required as they have to compile a custom kernel for you).

See xxx://xxx.netfilter.org/projects/patch-o-matic/pom-external.html#pom-external-connlimit

3. Find a pre-built module maintained elsewhere.

Hope this helpful.