Subject: Bridging problems with el5 kernel
Posted by strakar on Sun, 14 Oct 2007 18:53:37 GMT
View Forum Message <> Reply to Message

I have an x86_64 host node loaded with CentOS5 running ovzkernel-2.6.18-8.1.14.el5.028stab045.1.x86_64 with 2 ve's created using the Centos5 x86_64 default template from the contributors section of the download area. The first VE (VE101) is set up to be a firewall while the second VE (VE102) is set up to be DMZ server. The host node is meant to be on my internal network and the whole setup is behind a commercial firewall appliance which performs the firewall/nat function to the internet. The network is setup as follows

Host Node Interfaces
eth1 - internal lan
eth0 - DMZ lan to the firewall appliance
veth101.0 <-> eth0 on VE101 (firewall ve)
veth101.1 <-> eth1 on VE101 (firewall ve)
veth102.0 <-> eth0 on VE102 (dmz server ve)

Bridges on Host Node
br0 - bridges eth0, veth101.0, and veth102.0
br1 - bridges eth1, and veth101.1

IP Assignments
eth0 on VE101 and eth0 on VE102 both have DMZ subnet IPs
eth1 on VE101 and br1 on the HN both have internal subnet IPs.
No other IPs are assigned to any other inerfaces.

Route Assignments
HN default route points to eth1 IP on VE101
VE101 default route points to firewall appliance IP
VE102 default route points to firewall appliance IP
VE102 route to internal subnet points to VE101 eth0 IP

VE101 currently has no firewall rules (all chain have default policy of ACCEPT) and has ip_forwading enabled.

I can successfully ping the HN, VE102, and the firewall appliance from VE101. I can also successfully ping VE101 from the HN.
I cannot ping the HN from VE102 nor can I ping VE102 or the firewall appliance from the HN.

When I try to ping the HN from VE102 and run tcpdump on veth101.0 and br1 on the HN, I can see ping request packets coming in (they are making it through br0 veth102.0->veth101.0->eth0 on ve101, being forwarded by ve101 eth0->eth1->veth101.0) but they are not being bridged over to the br1 interface.
When I ping the HN from the firewall, tcpdump on veth101.0 and br1 shows that the packets are being bridged properly. The main difference seems to be that the packets when pinging from the VE101 are coming from the same subnet as the destination whereas when I ping from VE102 the packets are coming from a different subnet from the destination. It kind of looks like there is some

filtering going on in the bridge code. I disabled all of the bridge filtering flags on the HN in /proc/sys/net/bridge directory and still no success. I also installed ebtables to axamine any potential default filtering rules and all chains are set to a policy of ACCEPT.

When I install the non el5 kernel (kernel-2.6.18-ovz028stab045.1.x86_64.rpm), I can successfully ping the HN from VE102 and VE102 from the HN. Does the el5 kernel have some other default setting which I have to alter to have it bridge properly? I noticed that the non el5 kernel does not have bridge firewalling configued by default. Could this be making a difference?

Any help would be greatly appreciated.