Subject: Re: VPN server inside a CT?
Posted by ceegeebee on Fri, 22 Jan 2010 14:35:15 GMT
View Forum Message <> Reply to Message

tcpdump is your friend.

If your VPN tunnel is up, and you can ping the tunnel interface's remote IP address, then the rest should just be routing.

Your remote server is most likely generating packets with a source IP of the tunnel interface. That will be received by your VZ containers VPN software on the tun interface, and then put out on the venet network with the same source IP. You should see with with 'tcpdump -ni venet0 icmp' on the VPN container, and then send a ping from the remote site, to a node on the container nodes network.

If this looks good so far, the issue might be that your receiving node on the VPN server side, doesn't have a route for this VPN tunnel range. It will hand it off to it's default gateway, and if that gateway doesn't have a route for your VPN range, the packets go in the wrong direction. tcpdump or wireshark on the ICMP receiving node will allow you to confirm the packet is being received.

NAT on the VZ VPN node can help to rewrite the source IP of the remote server, to be that of the LAN IP of the VPN server. That allows you to ensure packtes come back to the VPN server, without getting the routing fixed up. On the VPN server,

iptables -t nat -A POSTROUTING -o venet0 -s vpn.ip.of.remote.server -j SNAT --to-source lan.ip.of.vz.vpn.server

Let me know how that goes.

Chris Bennett
cgb