Subject: VPN server inside a CT?
Posted by althalus on Fri, 22 Jan 2010 11:14:26 GMT
View Forum Message <> Reply to Message

Hi,

I'm trying to set up a VPN server inside a container using vtund. Following http://wiki.openvz.org/VPN_via_the_TUN/TAP_device I managed to get the tun device working, and I also managed to get a basic vtund setup working, with the CT as the server, and a machine in a different network connecting. The problem is, the IP addresses used for the tunnel are a different network, and I can't work out how to allow communication between the client and the rest of the network the server exists in.

Any pointers or suggestions? Is there a better/easier way than using vtund?

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

Subject: Re: VPN server inside a CT?
Posted by althalus on Fri, 22 Jan 2010 20:40:49 GMT
View Forum Message <> Reply to Message

Thanks Chris, tcdump is a wonderful tool.

If I run 'tcpdump -ni venet0 icmp' in the container, I can see the packets flowing from the VPN client to the CT.

But if I run tcpdump on the node I'm trying to ping, nothing. It's not even receiving the request, let alone how it'll try and route it back. It seems like packets aren't being forwarded from the VPN CT to the other nodes? I thought net.ipv4.ip_forward=1 should have enabled that? Or am I off base here?

Subject: Re: VPN server inside a CT?
Posted by ceegeebee on Sat, 23 Jan 2010 06:44:38 GMT
View Forum Message <> Reply to Message

You're on track, we just need to hone in on what is wrong.

net.ipv4.ip_forward is the setting you'd enable in sysctl.conf, but is that the current setting for /proc/sys/net/ipv4/ip_forward, both inside the CT, and the host node?

vpnclient <-> (tunX) CT (venet0)<-> (physical int on host node) LAN

You've confirmed the packet is exiting venet0 inside the CT - does it exit the physical interface on the VZ host node? (eth0 perhaps)

Chris Bennett
cgb

Subject: Re: VPN server inside a CT?
Posted by althalus on Sat, 23 Jan 2010 07:46:48 GMT
View Forum Message <> Reply to Message

cat /proc/sys/net/ipv4/ip_forward
1

This is in both CT node and the host node. I can't see any evidence of the packet passing through any of the host's interfaces using tcpdump.

Subject: Re: VPN server inside a CT?
Posted by ceegeebee on Sun, 24 Jan 2010 00:44:43 GMT
View Forum Message <> Reply to Message

Do you see any packets on venet0 on the host node, for the VPN client? IP Forwarding is enabled the host node as well?

Is there any firewall on the host node that might be blocking the packets?

Subject: Re: VPN server inside a CT?
Posted by althalus on Sun, 24 Jan 2010 01:41:39 GMT
View Forum Message <> Reply to Message

After rebooting the client and re-establishing the tunnel and the routes, everything is working as expected. Only thing I can presume is that I made a typo in the routing? Either way, thanks for your help!

Subject: Re: VPN server inside a CT?
Posted by ceegeebee on Sun, 24 Jan 2010 08:24:34 GMT
View Forum Message <> Reply to Message

I'm glad to hear your problem is fixed - I was running out of ideas as it all seemed to be configured right except you're tests were failing ..

I havn't used vtun before, but OpenVPN is a really flexible VPN solution for LAN to LANs and hub/spoke client VPN access. If you continue to experience problems, and suspect it's vtun related, give OpenVPN a go.