Subject: Re: Unable to run OpenVPN - "openvpn --mktun --dev tap0" fails
Posted by tomfra on Thu, 25 Oct 2007 21:31:01 GMT
View Forum Message <> Reply to Message

bwoo wrote on Thu, 25 October 2007 21:19So is there a way of running OpenVPN as a server inside a VE?

Yes, it is! I've just finished installing & testing it, with some help from the Experts Exchange and a lot of Googling...

I installed it in the routing mode as the "road warrior" setup plus with routing all Internet traffic through the VPN tunnel. It works great, but the config is a bit tricky.

"openvpn --mktun --dev tap0" is not needed to make it work, also the "dummy0" trick is not needed for the routing setup, it is needed for the bridging setup which I have not tested but I am sure that it would work too.

Sometime I will hopefully write the "Howto install OpenVPN on an OpenVZ VPS" but it would be something like this (on CentOS 5):

1 ) Add rpmforge to your list of yum repos - simply install the correct rpm for your distro from http://dag.wieers.com/rpm/packages/rpmforge-release/

2 ) yum -y install openvpn

3 ) Install the openvpn webmin module, it is great for creating the certificates, monitoring the VPN connections etc. It's a bit tricky for configuring so you will have to play with it for a while.

4 ) You will need the /dev/tun device in your VPS. The how-to is at http://wiki.openvz.org/VPN_via_the_TUN/TAP_device. If you haven't done so already, do "modprobe tun" on the hardware node, I believe it should be added into /etc/init.d as well.

5 ) server.conf file could roughly look something like this:

```
port 1194
tls-server
mode server
proto udp
dev tun0
ca keys/myserver/ca.crt
cert keys/myserver/defaultserverkey.crt
key keys/myserver/defaultserverkey.key
dh keys/myserver/dh2048.pem
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1"
push "dhcp-option DNS 10.8.0.1"
crl-verify keys/myserver/crl.pem
cipher AES-256-CBC
```

```
user nobody
group nobody
status servers/myserver/logs/openvpn-status.log
log-append servers/myserver/logs/openvpn.log
verb 2
mute 20
max-clients 500
management 127.0.0.1 4444
keepalive 10 120
client-config-dir /etc/openvpn/servers/myserver/ccd
comp-lzo
persist-key
persist-tun
ccd-exclusive
```

The 2 occurences of "push" are needed if you want to route all Internet traffic, including web etc., through the VPN tunnel, otherwise comment them out. Make sure the certificate & other paths correspond with those valid for your server.

If you set the push "dhcp-option DNS 10.8.0.1", you will need to install Bind or other DNS server on the VPS (listening on the main VPS IP). Or you can specify any public IP of DNS servers accepting queries from the VPS IP.

6 ) Client side:

I installed openvpn on my Win XP Home PC as a part of the OpenVPN GUI you can get at http://openvpn.se . Rename the Virtual TAP Network Adapter to "OpenVPN" (or something else but you will need to specify the name in the dev-node switch).

client.conf example:

```
client
dev tun
pull
dev-node OpenVPN
proto udp
remote PUBLIC_IP_OF_YOUR_VPN_SERVER 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert defaultclientkey.crt
key defaultclientkey.key
ns-cert-type server
cipher AES-256-CBC
```

keysize 256
comp-lzo
verb 3
mute 20

The "dev", "proto" & "cipher" switches must be the same as on the server. My chosen cipher - "AES-256" is somewhat extreme so you may comment it out (together with the "keysize" switch and OpenVPN will then default to Blowfish).

7 ) On the server:

service openvpn start

This should create the tun0 device I believe. Then do:

/sbin/iptables -A FORWARD -j ACCEPT -p all -s 0/0 -i tun0
/sbin/iptables -A FORWARD -j ACCEPT -p all -s 0/0 -o tun0
/sbin/iptables -t nat --flush
/sbin/iptables -t nat -A POSTROUTING -s ! x.x.x.x -o venet0 -j SNAT --to-source x.x.x.x

Replace x.x.x.x with your VPS public IP address. You should probably include those lines in the openvpn init file in /etc/init.d . Technically, only the last line may be necessary. There are probably better ways but this should work. I use CSF firewall and I added those lines to csfpre.sh instead.

8 ) Now you should be able to create the VPN tunnel from the client side.

It's not a perfect how-to but at least it could give you a few hints.

Tomas