Problem on SecureNAT

SecureNAT is a fairly simple way to setup Softether. You don't need a lot of sysadmin skill and network understanding in order to get Softether up and running.

The problem is SecureNAT is a bit **SLOW**. I will show a comparison at the end of this article.

We can boost the performance using a local bridge.

Softether using local bridge

To start with you need Softether installed and setup. You can follow the guide on Softether on VPS

Just skip the last step "Enable the Virtual NAT"

Local bridge Setup

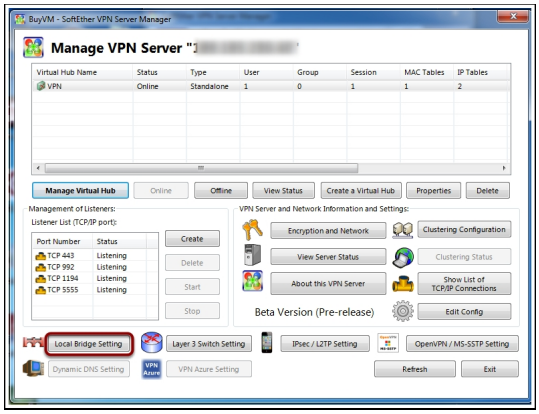
Network setup

VPN Server IP: 192.168.7.1

VPN Client IP Range: 192.168.7.50-192.168.7.60

Tap Device name: tap_soft

From here we go to the “Local Bridge Setting”

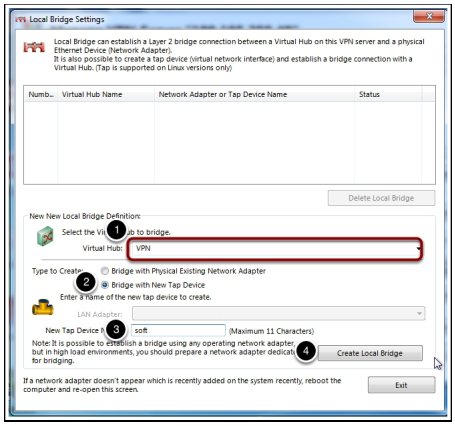


Local Bridge Setting

First we choose the Virtual Hub. It should be only one for normal setup.

Then we check the tap device box.

After that we type in the name of the tap device(I use soft here for simplicity).

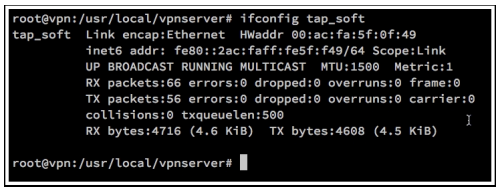


Create Local Bridge

After the creation of the local bridge we jump back to our server. And run

```
1                    # ifconfig tap_soft
```

It should show you something similar to this



Check on the server

Because we are not going to use SecureNAT and SecureDHCP. We need to install a DHCP server on our VPS. We are going to use dnsmasq as our DHCP server.

```
1                    # apt-get install dnsmasq
```

Now edit the /etc/dnsmasq.conf file. Add these 3 lines at the end.

```
1                    2                    3                    interface=tap_soft    d
```

The above 3 lines are used to enable the dhcp server on interface tap_soft.

Next step we need a new set of init script which will config tap interface for us when Softether start up.

/etc/init.d/vpnserver

```
1                    2                    3                    4                    5
```

Then we need to enable NAT on linux server.

Add this file to /etc/sysctl.d/ to enable ipv4 forwarding.

/etc/sysctl.d/ipv4_forwarding.conf

```
1 net.ipv4.ip_forward = 1
```

Apply the sysctl run

```
1 # sysctl --system
```

Then we add a POSTROUTING rule to iptables

```
1 # iptables -t nat -A POSTROUTING -s 192.168.7.0/24 -j SNAT --to-sourc
```

To make our iptables rule survive after reboot install iptables-persistent

```
1 # apt-get install iptables-persistent
```

After all the above setting, restart the vpnserver then we are good to go.

```
1 2 # /etc/init.d/vpnserver re#t/etc/init.d/dnsmasq rest
```

Comparison on SecureNAT and local bridge method.



Speed test on local bridge 

Speed test on SecureNAT

Conclusion

Local bridge use far less CPU resources than SecureNAT. It is a bit trouble to setup but I think it is worth to use local bridge.