I - OPENVPN on IPFIRE Setup

(using remote SSH)

Credits: https://nordvpn.com/tutorials/ipfire/openvpn/

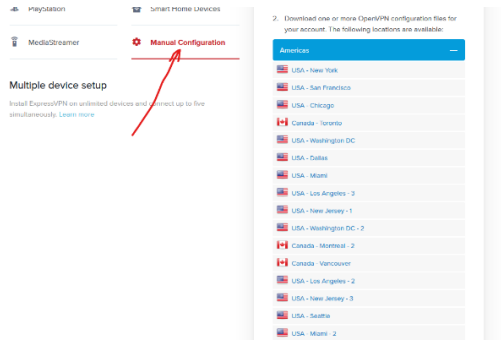
Ref: https://www.frozentux.net/iptables-tutorial/chunkyhtml/c962.html
https://www.tecmint.com/linux-iptables-firewall-rules-examples-commands/
https://help.skysilk.com/support/solutions/articles/9000136471-how-to-enable-tun-tap-on-linux-vps-with-skysilk

open an SSH session to your ipfire machine or login on the ipfire machine as root

1 **==>cd /var/ipfire/ovpn** ***(create that **dir** if doesn't exist)

2 download the **openvpn** config files from ExpressVPN website that you'll need, to that directory. e.g. "**my_expressvpn_usa_-_new_york_udp.ovpn**" etc.

https://www.expressvpn.com/setup#manual
(select Linux → Manual configuration)



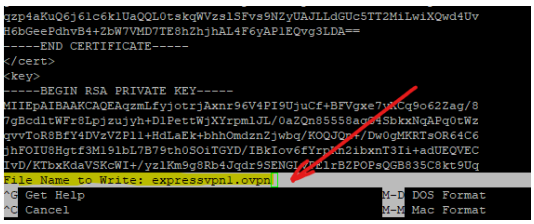
3 edit your preferred .ovpn file

3.1 **==>nano my_expressvpn_usa_-_new_york_udp.ovpn**

3.2 go to the line starting with "**auth-user-pass**" and change it to: "**auth-user-pass /var/ipfire/ovpn/user_pass**"

(this file – **user_pass** - will hold your secret username and password)

3.3 save the .ovpn file and rename it: "**expressvpn1.ovpn**"



4 edit a new file named "**user_pass**" (where your secret username and password will be saved)

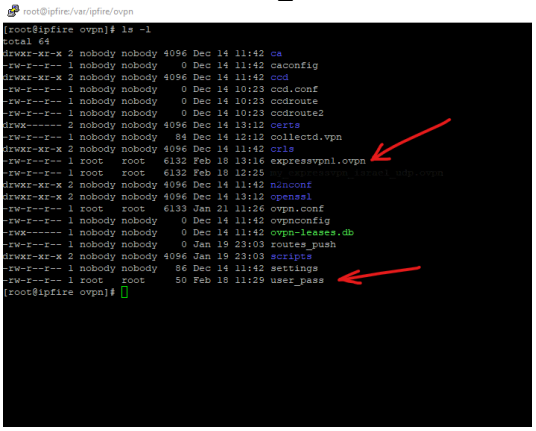
4.1 **==>nano user_pass**

4.2 the first line is your username (from your ExpressVPN account/website)

4.3 the second line is the password (ditto)

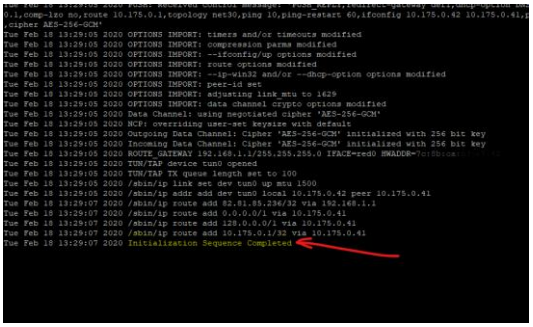
4.4 save the file

5 so you should have (at least) 2 files: the ExpressVPN config file renamed "**expressvpn1.ovpn**" and the secret file "**user_pass**" (we are still in that directory: **/var/ipfire/ovpn**)

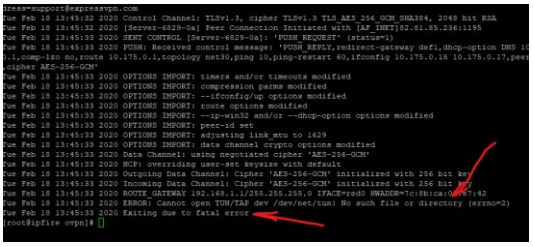


6 you need now to add a rule to the routing table. Type:
==>iptables -t nat -A POSTROUTING -s **YOUR_GREEN_NETWORK_IP/24** -o tun0 -j MASQUERADE
for example: "**==>iptables -t nat -A POSTROUTING -s 192.168.3.0/24 -o tun0 -j MASQUERADE**"

7 start the ExpressVPN service. type: "**==>openvpn expressvpn1.ovpn**"
if you are lucky you should get: "**Initialization Sequence Completed**" (no more prompt) and you are connected and your life is good



otherwise, the VPN cannot start and you are getting this output:
"**ERROR: Cannot open TUN/TAP dev /dev/net/tun: No such file or directory (errno=2)**"



then do the following :

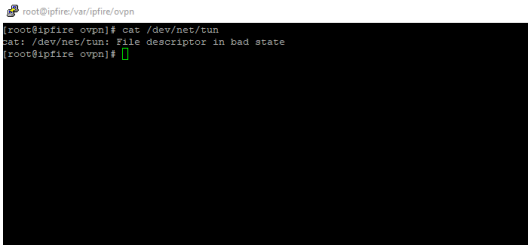
7.1 **==>mkdir -p /dev/net**

7.2 **==>mknod /dev/net/tun c 10 200**

7.3 **==>chmod 600 /dev/net/tun**

7.4 **==>cat /dev/net/tun**

you should read back: "**cat: /dev/net/tun: File descriptor in bad state**"



which means that you are OK (TUN/TAP is ready)

8 start again the ExpressVPN service. retype: "**==>openvpn expressvpn1.ovpn**"
this time you will get: "**Initialization Sequence Completed**" (no more prompt)
you are connected to the VPN server and all is **OK**

if not recheck the process and find the error

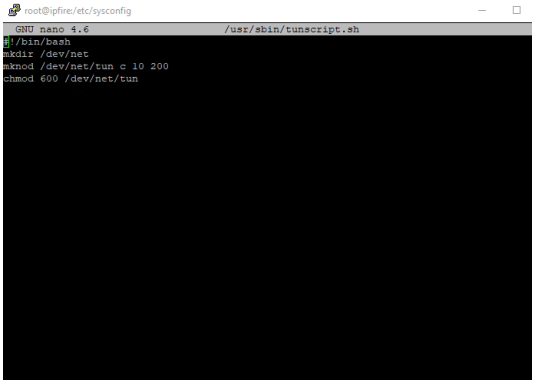
II - OPENVPN on IPFIRE bash scripts

If everything went fine and you have access to ExpressVPN server with a new masked IP address, you must create the following scripts to make everything automatic at boot. Otherwise you'll need to repeat all this stuff after each reboot.

1 **==>nano /usr/sbin/tunscript.sh**
I guess the file doesn't exist. Write (add) these 4 lines:

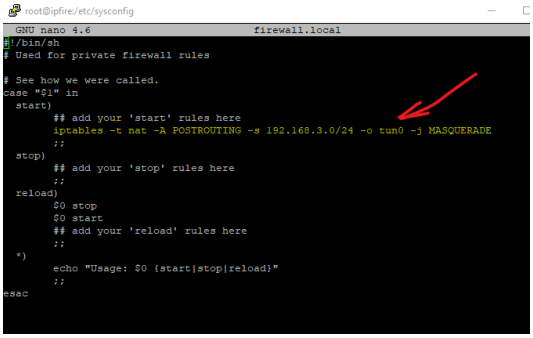
```
#!/bin/bash
mkdir /dev/net
mknod /dev/net/tun c 10 200
chmod 600 /dev/net/tun
```

1.2 Save the file

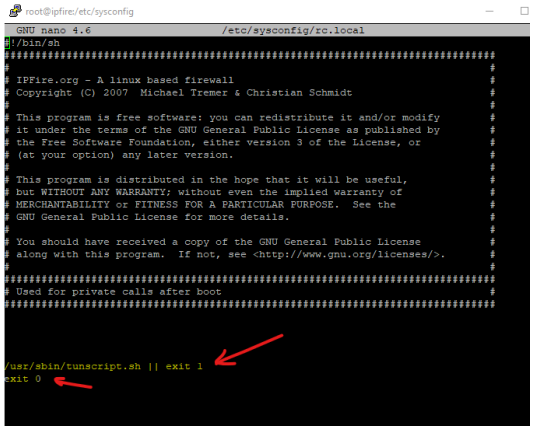


1.3 **chmod +x /usr/sbin/tunscript.sh**
(make it executable)

2 ==>**nano /etc/sysconfig/firewall.local**
After "**start**" add the iptable rule:
iptables -t nat -A POSTROUTING -s 192.168.3.0/24 -o tun0 -j MASQUERADE



3. and finally update the rc.local script:
nano /etc/sysconfig/rc.local
usr/sbin/tunscript.sh || exit 1
exit 0



peace