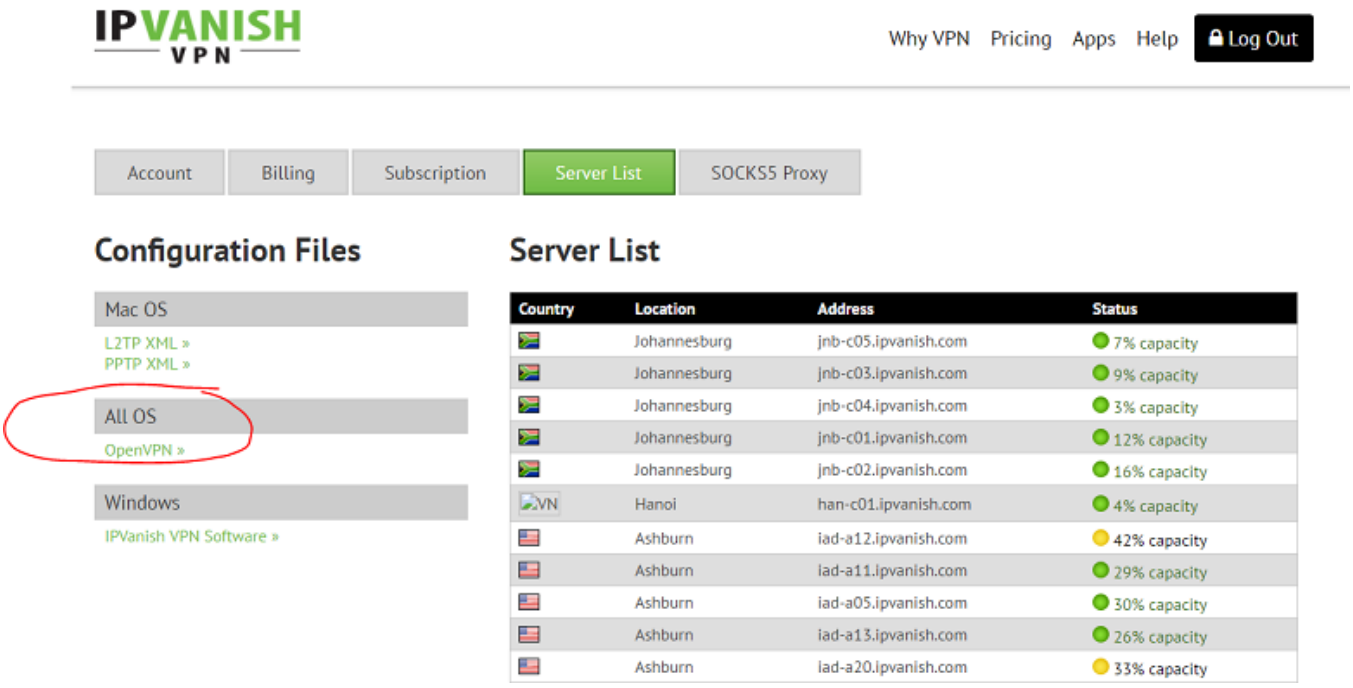
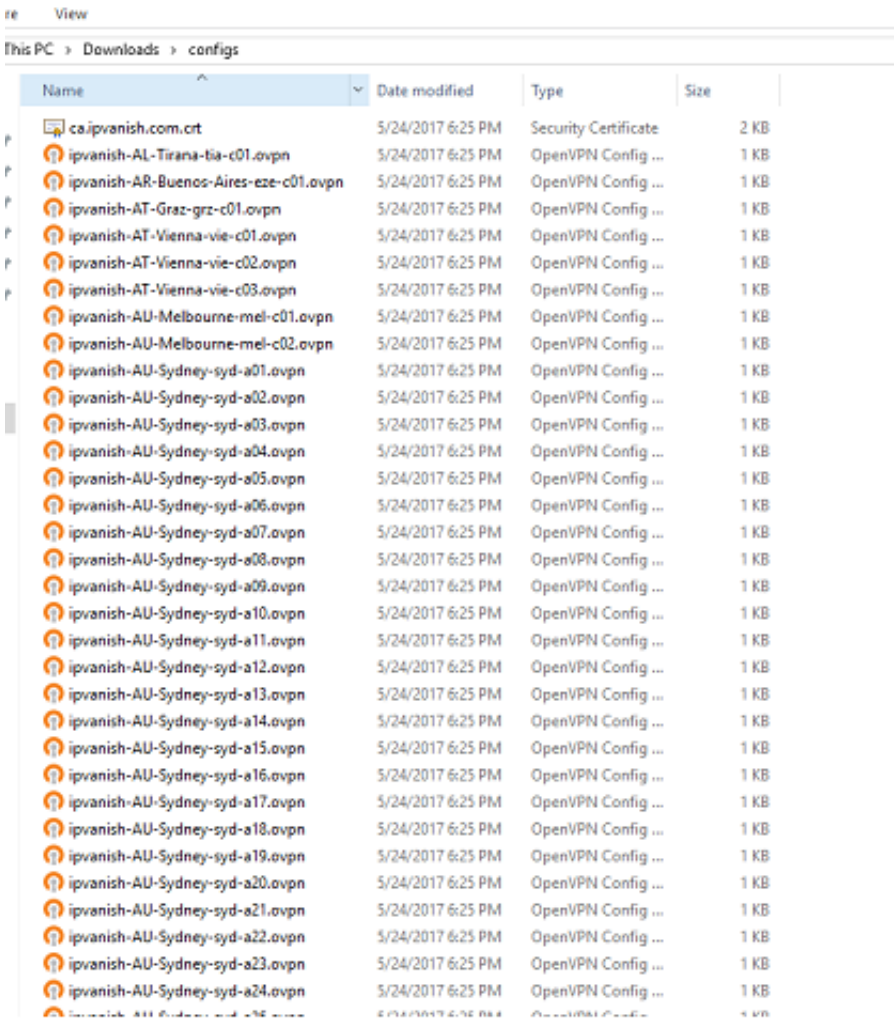
# Guide - How to connect pfSense OpenVPN client to IPVanish

*Disclaimer: This guide is based on pfSense version 2.3.4 and IPVanish as of 5/27/2017. While I don't expect this guide to change much in the meantime, there is always the chance that something can change that can break things. That said, the basic principles should still apply and could even work with other VPN providers who utilize OpenVPN. Your mileage may vary.*

Login to IPVanish and under the server list, all OS section, click the download link for OpenVPN.



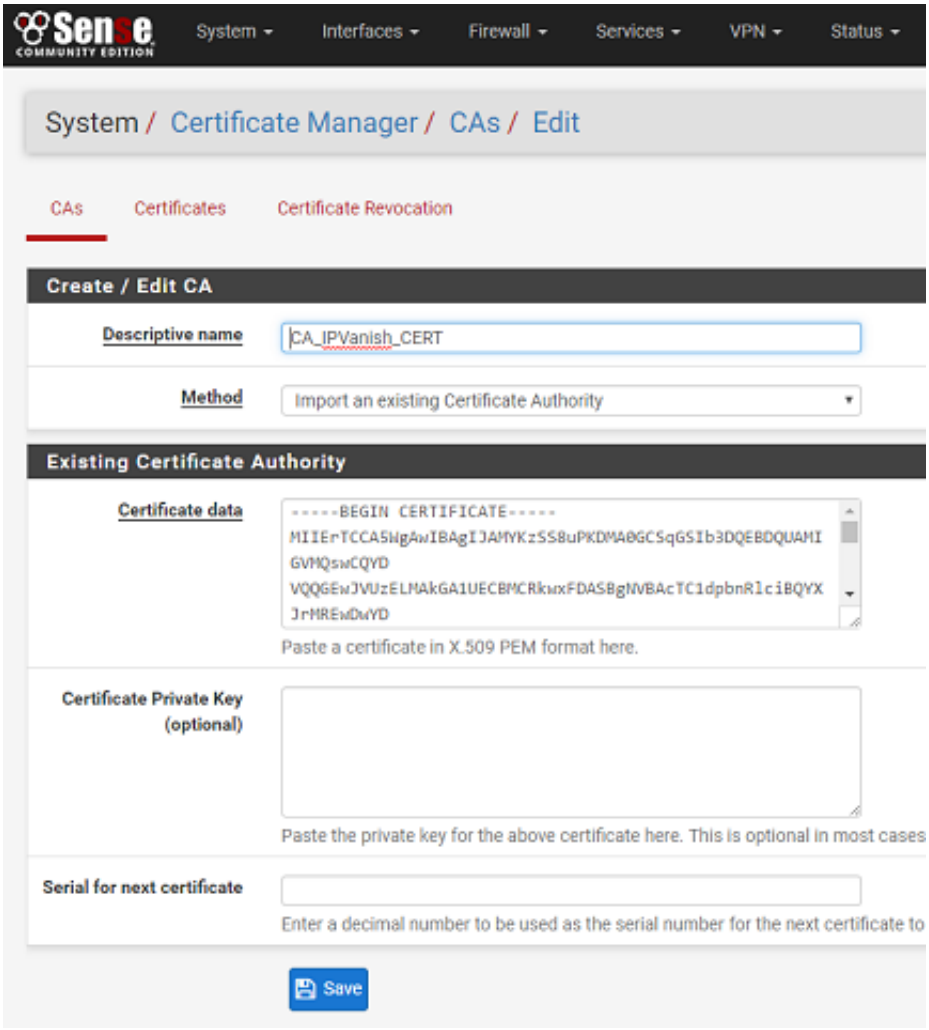

This will give you a zip file which contains the OpenVPN profiles as well as the CA that you will need to create.




Login to your pfSense web interface and go to System/Certificate Manager

Click Add to start to create a new certificate authority

Give the CA a name (it can be whatever you want). Chose to Import an existing Certificate Authority. Copy and paste the info from the file you downloaded called: ca.ipvanish.com.crt into the Certificate data field. You can open it with notepad to do this.




Now go to VPN, OpenVPN, and click on the Client tab. Click Add.

This is where things can get a bit tricky. In order to fill out the information in this screenshot, you need to open up one of the OpenVPN profiles that you downloaded. I recommend looking at the first place where you downloaded the list to find a server close to you that has very little load. Once you've identified that server, go back to your OpenVPN files and open the one that corresponds to the name of the server you want to connect to. The URL you want is what comes after "udp remote." Copy and paste this into pfSense under server host or address. After that, copy the rest of the information I have in my screen shots including your IPVanish username and password. In the custom options field, you can actually leave this blank. The settings that I have in there are redundant and not needed.

## General Information

**Disabled**
☐ Disable this client
Set this option to disable this client without removing it from the list.

**Server mode**: Peer to Peer ( SSL/TLS )

**Protocol**: UDP

**Device mode**: tun

**Interface**: WAN

**Local port**:
Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.

**Server host or address**: p[redacted]

**Server port**: 1194

**Proxy host or address**:

**Proxy port**:

**Proxy Auth. - Extra options**: none

**Server hostname resolution**
☑ Infinitely resolve server
Continuously attempt to resolve the server host name. Useful when communicating with a server that is not permanently connected to the Internet.

**Description**: p[redacted]
A description may be entered here for administrative reference (not parsed).

## User Authentication Settings

**Username**: [redacted]com
Leave empty when no user name is needed

**Password**: ••••••••
Leave empty when no password is needed

••••••••
Confirm

## Cryptographic Settings

**TLS authentication**
☐ Enable authentication of TLS packets.

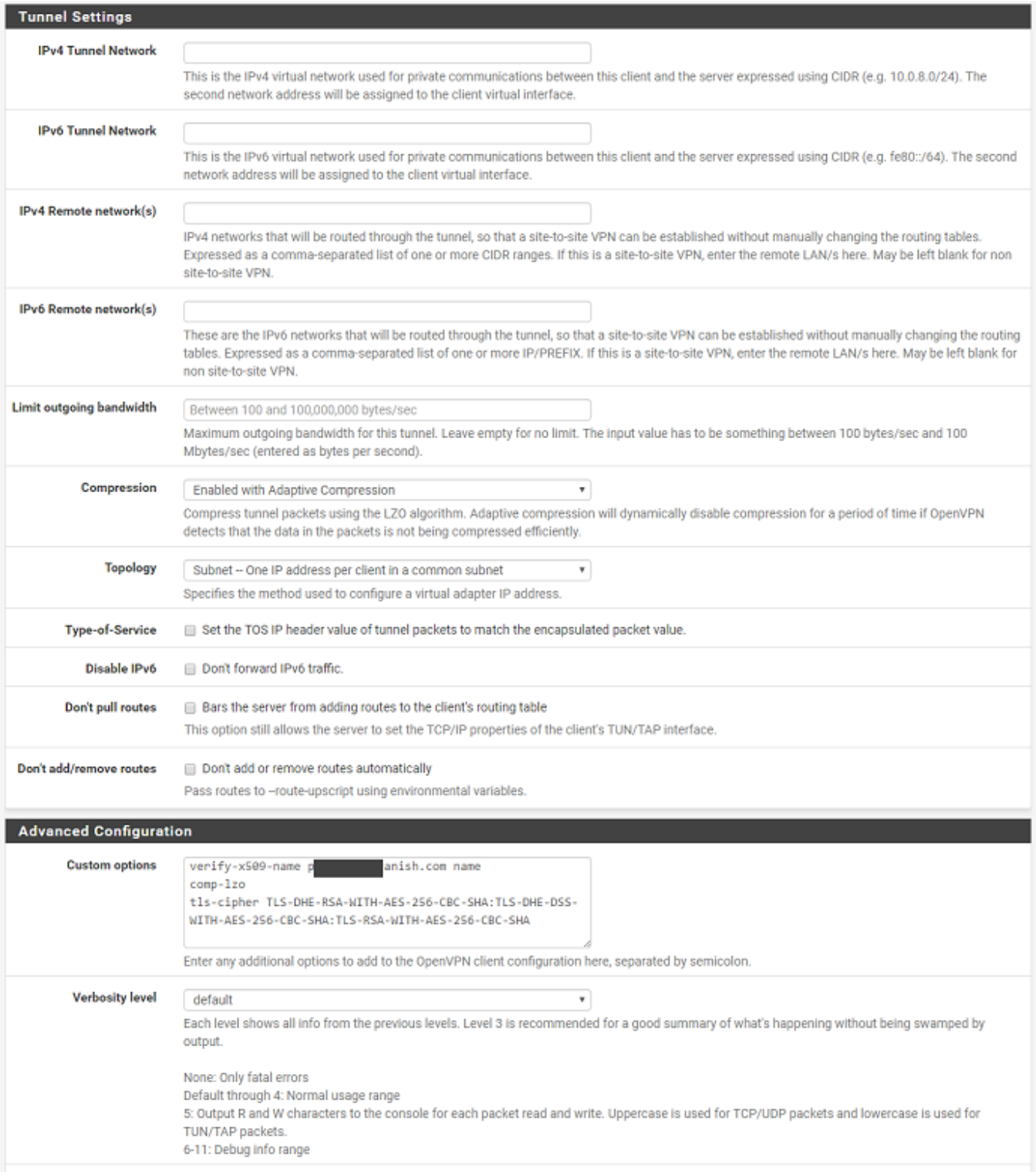
**Peer Certificate Authority**: CA_IPVanish_CERT

**Client Certificate**: None (Username and/or Password required)

**Encryption Algorithm**: AES-256-CBC (256 bit key, 128 bit block)

**Auth digest algorithm**: SHA256 (256-bit)
Leave this set to SHA1 unless all clients are set to match. SHA1 is the default for OpenVPN.

**Hardware Crypto**: No Hardware Crypto Acceleration




At this point, hit save, and like magic if you did your job right you should be connected and browsing using the OpenVPN client. You can check the status under Status/OpenVPN. If it says UP and has a green check mark you should be good to go! Check to see if your new IP is working by going to a site like [www.ipchicken.com](http://www.ipchicken.com).

### *Optional*

This section is optional, but I'm including it because quite frankly it took

me a long time to figure out and I could never find any up to date guides that actually worked. This section will cover how to only pass certain traffic over the VPN client. In my case, I only really wanted one computer to use the VPN instead of the whole house. I don't need other things being slower going over a VPN such as my Roku or Media Center PC. While IPVanish is actually quite fast, it still is slower than my normal internet connection.

There may be other (perhaps even better ways) of doing this, but again this is what worked for me.

Start by going to interfaces and assign.

Select opvpnc (it might be called something else similar) under the list of available interfaces and click Add.

Click on the interface you just created and check the box that says Enable Interface. Save and apply.

Now go to Firewall/Rules and click on the LAN tab. Edit your current Default LAN to any rule. Scroll to the bottom and show advanced options. Change the Gateway from default to your ISPs gateway. Click save and apply.

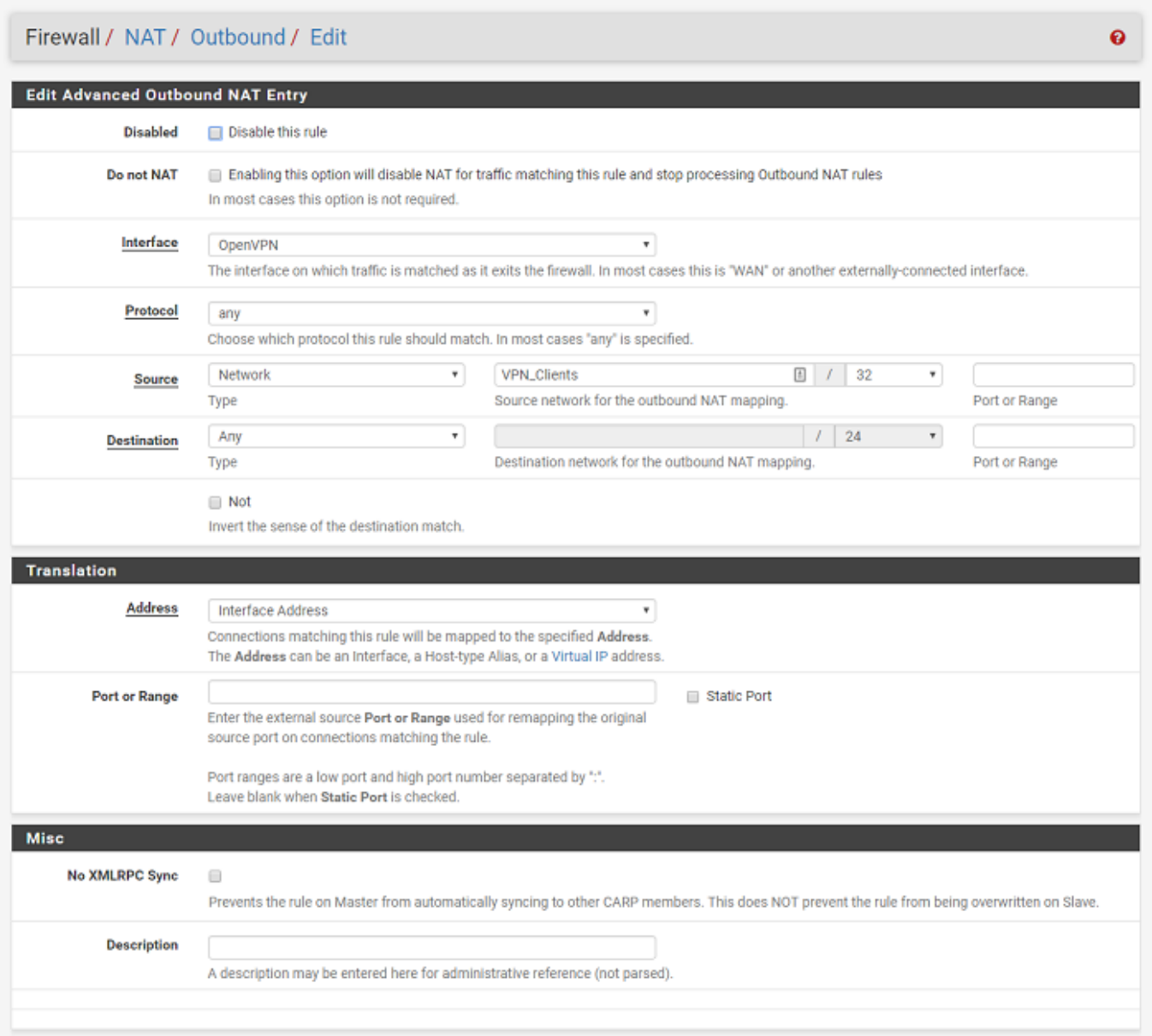
Now create a new rule under the LAN tab. Change protocol from TCP to any. Change your source to either a single host, network range, or an alias (in my case I used an alias list that I can update whenever I want). Go to advanced and this time change the Gateway from default to your OpenVPN gateway. Click save and apply.

IMPORTNAT: Make sure that you move the OpenVPN rule above the other rule or this won't work as intended.

Finally go to Firewall/NAT and click on outbound. Change your setting from Automatic to Hybrid or Manual. Personally, I prefer Hybrid so I don't have to maintain anything and can just make changes as needed, but this is really just up to you.

Click on Add.

Set your rule to something similarly to this. Remember I'm using an alias here but you can put in a single IP if that's all you need.




Click save and apply.

Now check your clients. Everything except the client you specified should be using the normal WAN and that client or clients should be getting a different IP over the VPN.