MUFFIN'S LAB

Just a boy and his toys;

Tunneling Specific Traffic over a VPN with pfSense

8 min read

March 14, 2016 by MonsterMuffin

Recently I stumbled on a post in /r/sysadmin by /u/ThatOnePrivacyGuy that had a spreadsheet he had created comparing a load of VPN services, you can find it here.

This got me thinking, my automated downloads crunch through *terabytes* of data every month on a home connection, and if my ISP were to look into this it would not show me in a good light due to a lot of p2p I have going on in my household; with my flat mate *constantly* having torrent connections open and Sonarr + Couchpotato downloading via torrents and NZBs there is a lot of data I would like to mask from my ISP. Thanks to that awesome spreadsheet I managed to find a service that looked perfect for me, vpn.ac.

So this post has gotten a bit of attention after almost a year and I'm super grateful for that, if you end up signing up for VPN.ac (who are still kicking ass btw) my affiliate link is here. No pressure, *just helps me out if I helped you out.*
Cheers, MM~~

They offer a weeks trial for 2$ which I went for test it out and if it worked well I was going to purchase a year, here's what I did to tunnel only select traffic over the tunnel.
This is very achievable for most services if you just install the client inside the OS but this will tunnel *all* that hosts traffic over the VPN, this is no good for me as I wanted only my downloads to go over this link and the rest of the traffic still going over my WAN, turns out this is very easy to accomplish in pfSense if the provider allows OpenVPN connections.

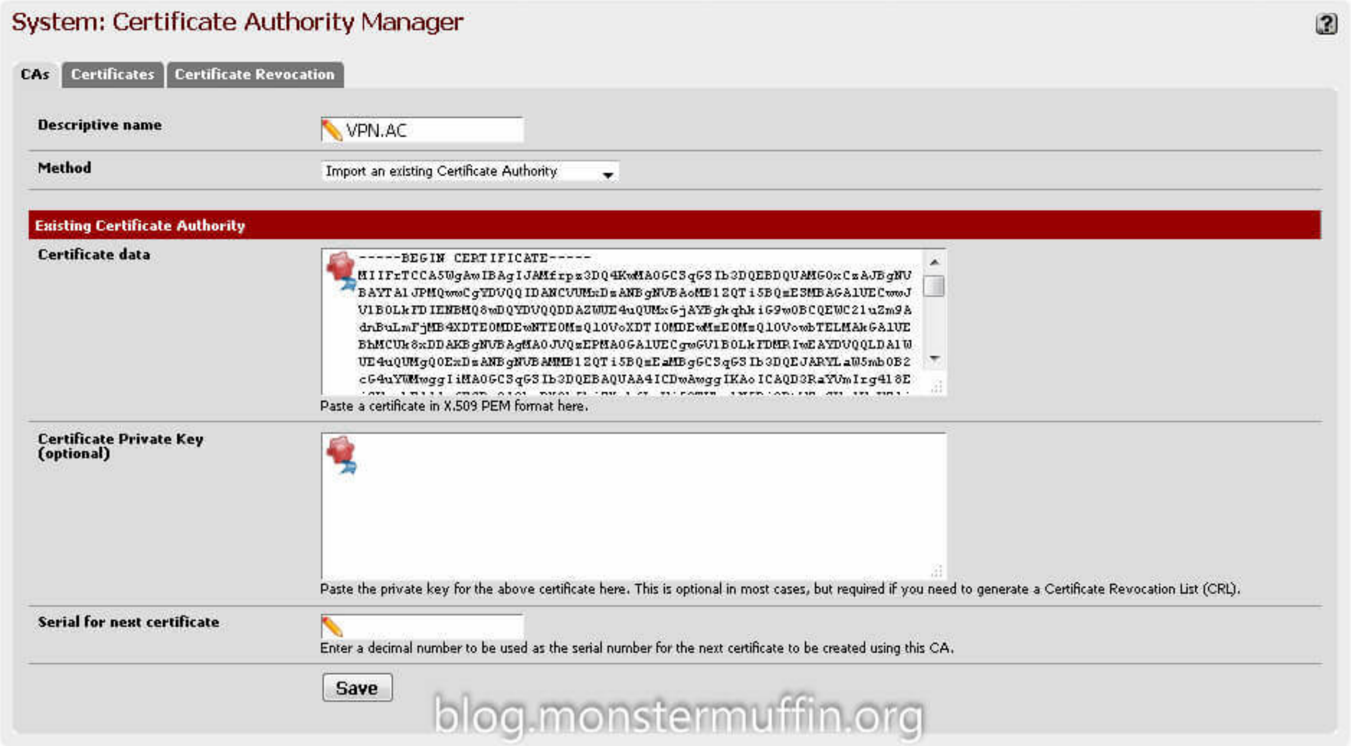
The setup will follow the following steps:

- Setup VPN connection inside pfSense
- Setup interface with that VPN connection
- Setup gateway with that interface
- Add NAT rules to allow whatever VLANs out to the VPN
- Add firewall rules to tunnel the traffic
- Test the tunnel

So let's get stuck in.

VPN Setup:

I won't cover the VPN setup in pfSense because the methods for this will vary across different providers but there should be a tutorial showing you how to do this. For me it was easy enough, all I had to do was add a CA with my providers certificate as follows:



System: Certificate Authority Manager

Descriptive name	VPN.AC
Method	Import an existing Certificate Authority

Existing Certificate Authority

Certificate data

```
-----BEGIN CERTIFICATE-----
MIIFrTCCA5WgAwIBAgIJAMfrpz3DQ4KwMA0GCSqGSIb3DQEBDQUAMG0xCzAJBgNV
BAYTAlJPMQwwCgYDVQQIDANCVUMxDzANBgNVBAoMBlZQTi5BQzESMBAGA1UECwwJ
VlB0LkFDIENBMQ8wDQYDVQQDDAZWUE4uQUMxGjAYBgkqhkiG9w0BCQEWC2luZm9A
dnBuLmFjMB4XDTE0MDEwNTE0MzQ10VoXDTI0MDEwMzE0MzQ10VowbTELMAkGA1UE
BhMCUk8xDDAKBgNVBAgMA0JVQzEPMA0GA1UECgwGVlB0LkFDMRIwEAYDVQQLDAlW
UE4uQUMgQ0ExDzANBgNVBAMMBlZQTi5BQzEaMBgGCSqGSIb3DQEJARYLaW5mb0B2
cG4uYWMwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQD3RaYUmIrg418E
```

Paste a certificate in X.509 PEM format here.

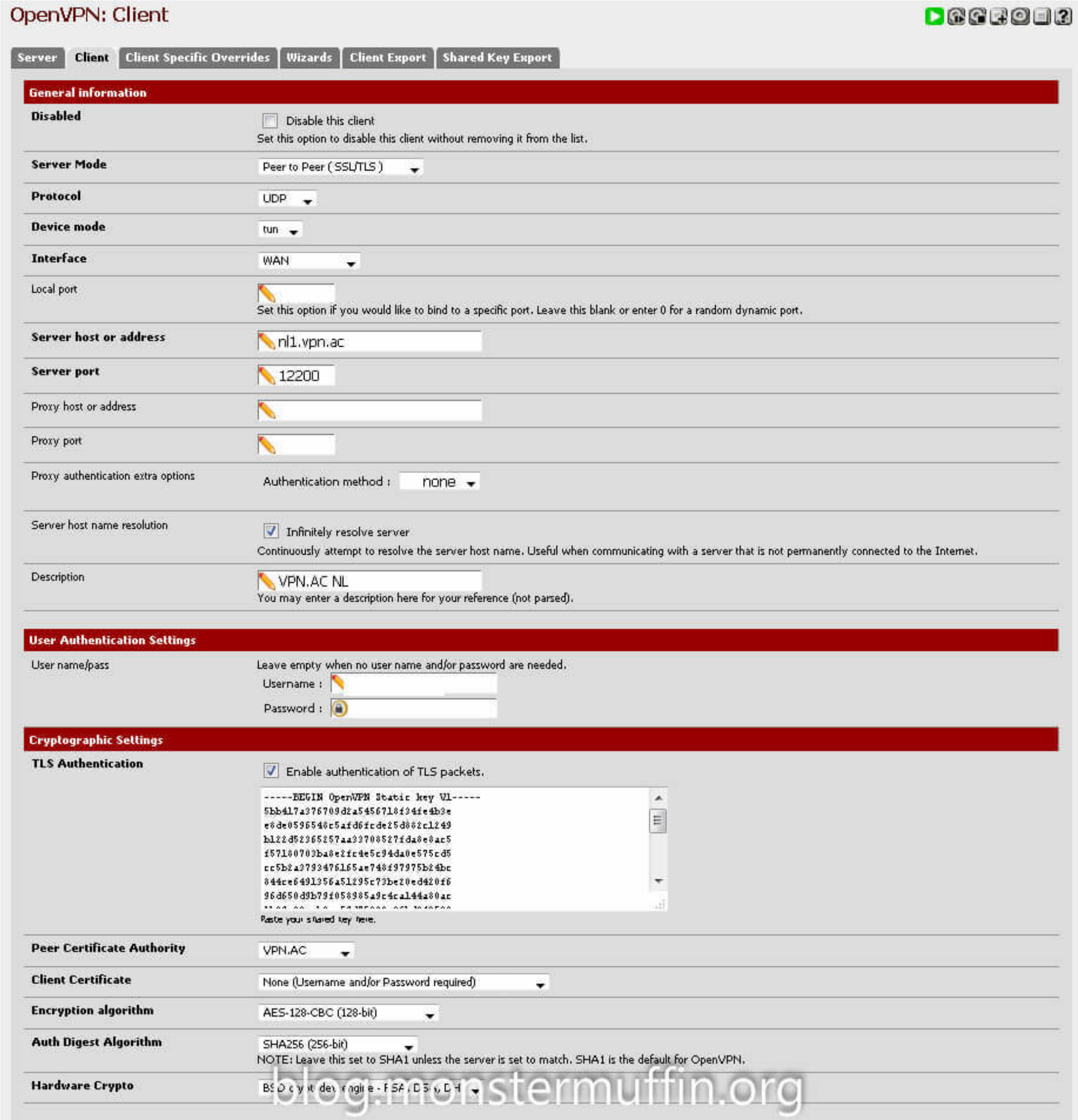
Certificate Private Key (optional)

Paste the private key for the above certificate here. This is optional in most cases, but required if you need to generate a Certificate Revocation List (CRL).

Serial for next certificate

Enter a decimal number to be used as the serial number for the next certificate to be created using this CA.

After that, under VPN > OpenVPN > Client create a new connection with the provided details from your provider, here you can choose which server to connect to. My provider has ‘p2p optimized nodes’ so I setup my connection to one of those servers, the closest of which to me was the Netherlands.



OpenVPN: Client

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 if you would like to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.
Server host or address	nl1.vpn.ac
Server port	12200
Proxy host or address	
Proxy port	
Proxy authentication extra options	Authentication method : none
Server host name 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	VPN.AC NL You may enter a description here for your reference (not parsed).

User Authentication Settings

User name/pass	Leave empty when no user name and/or password are needed. Username : Password :

Cryptographic Settings

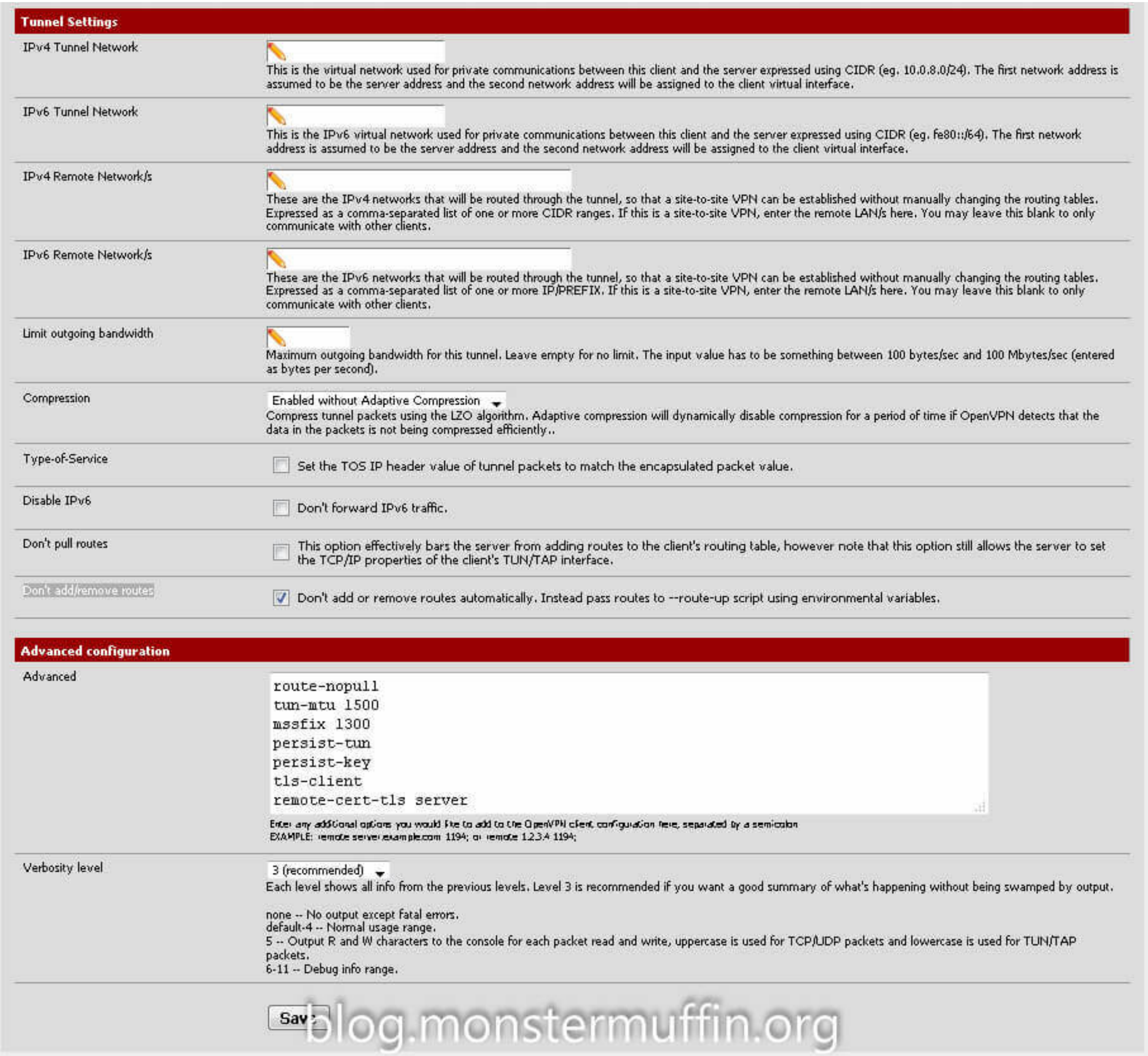
TLS Authentication	☑ Enable authentication of TLS packets.

```
-----BEGIN OpenVPN Static key V1-----
5bb417a376709d2a5456718f34fe4b3e
e8de0596548c5afd6fcde25d882c1249
b122d52365257aa33708527fda8e8ac5
f5718070 3ba8e2fc4e5c94da0e575cd5
cc5b2a3793476165ae748f97975b24bc
844ce6491356a51295c73be20ed420f6
96d650d9b79f058985a9c4ca144a80ac
```

Paste your shared key here.

Peer Certificate Authority	VPN.AC
Client Certificate	None (Username and/or Password required)
Encryption algorithm	AES-128-CBC (128-bit)
Auth Digest Algorithm	SHA256 (256-bit) NOTE: Leave this set to SHA1 unless the server is set to match. SHA1 is the default for OpenVPN.
Hardware Crypto	BSD cryptodev engine - RSA, DSA, DH

The tunnel settings were also provided by my provider with one addition made my me, the “route-nopull” setting. Checking “Don’t add/remove routes” should do the trick aswell but I added this in the advanced settings as well. The first time I did this I did not add this option and **all** my traffic started going over the pipe regardless of firewall rules, so ensure you add this option or you’ll end up with a mess.



Tunnel Settings

IPv4 Tunnel Network	This is the virtual network used for private communications between this client and the server expressed using CIDR (eg. 10.0.8.0/24). The first network address is assumed to be the server address and the second network address will be assigned to the client virtual interface.
IPv6 Tunnel Network	This is the IPv6 virtual network used for private communications between this client and the server expressed using CIDR (eg. fe80::/64). The first network address is assumed to be the server address and the second network address will be assigned to the client virtual interface.
IPv4 Remote Network/s	These are the IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. You may leave this blank to only communicate with other clients.
IPv6 Remote Network/s	These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP/PREFIX. If this is a site-to-site VPN, enter the remote LAN/s here. You may leave this blank to only communicate with other clients.
Limit outgoing bandwidth	Maximum outgoing bandwidth for this tunnel. Leave empty for no limit. The input value has to be something between 100 bytes/sec and 100 Mbytes/sec (entered as bytes per second).
Compression	Enabled without Adaptive Compression Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently..
Type-of-Service	□ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Disable IPv6	□ Don't forward IPv6 traffic.
Don't pull routes	□ This option effectively bars the server from adding routes to the client's routing table, however note that this option still allows the server to set the TCP/IP properties of the client's TUN/TAP interface.
Don't add/remove routes	☑ Don't add or remove routes automatically. Instead pass routes to --route-up script using environmental variables.

Advanced configuration

Advanced

```
route-nopull
tun-mtu 1500
mssfix 1300
persist-tun
persist-key
tls-client
remote-cert-tls server
```

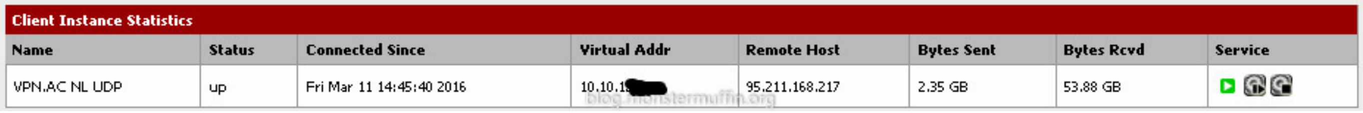
Enter any additional options you would like to add to the OpenVPN client configuration here, separated by a semicolon
EXAMPLE: remote server.example.com 1194; or remote 1.2.3.4 1194;

Verbosity level

3 (recommended)
Each level shows all info from the previous levels. Level 3 is recommended if you want a good summary of what's happening without being swamped by output.

none -- No output except fatal errors.
default-4 -- Normal usage range.
5 -- Output R and W characters to the console for each packet read and write, uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11 -- Debug info range.

Once this is done and completed going to Status > OpenVPN should list your connection and it should have the status “up”. This means we are connected to the provider.



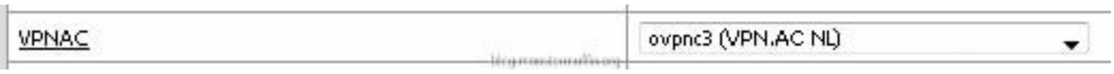
Client Instance Statistics

Name	Status	Connected Since	Virtual Addr	Remote Host	Bytes Sent	Bytes Rcvd	Service
VPN.AC NL UDP	up	Fri Mar 11 14:45:40 2016	10.10.1[redacted]	95.211.168.217	2.35 GB	53.88 GB	

Interface and Gateway Setup:

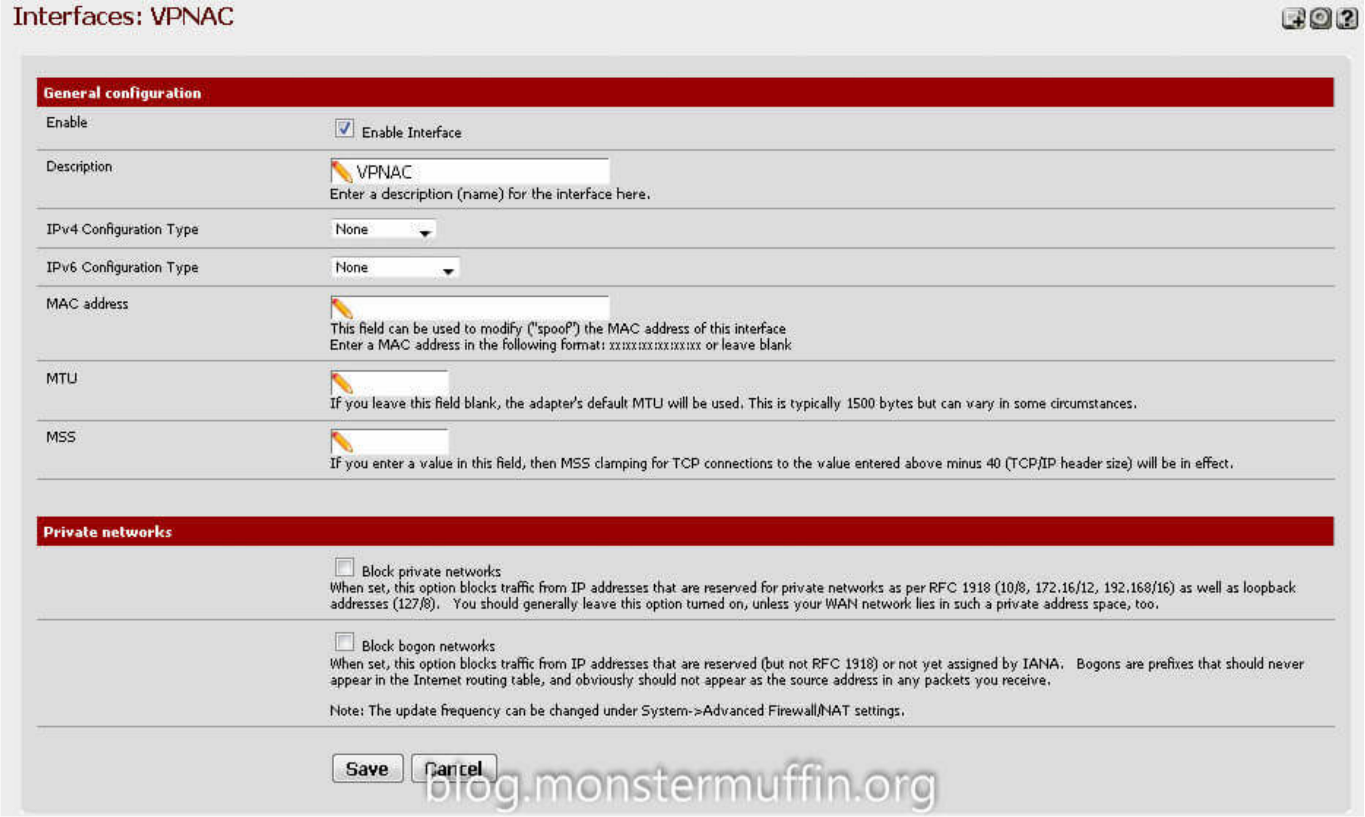
Next we need to add an interface for the connection and then a gateway for that interface, this is simple.

Head over to Interfaces > Assign, click on the ‘+’ icon and set the network port to your OpenVPN connection. (Yours won’t have a name yet like in mine, this is next.)



VPNAC | ovpnc3 (VPN.AC NL)

Click on the newly created interface and enable it, you can give it whatever name you want here. Once this is done, click save.



Interfaces: VPNAC

General configuration

Enable: ☑ Enable Interface

Description: VPNAC
Enter a description (name) for the interface here.

IPv4 Configuration Type: None

IPv6 Configuration Type: None

MAC address:
This field can be used to modify ("spoof") the MAC address of this interface
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU:
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

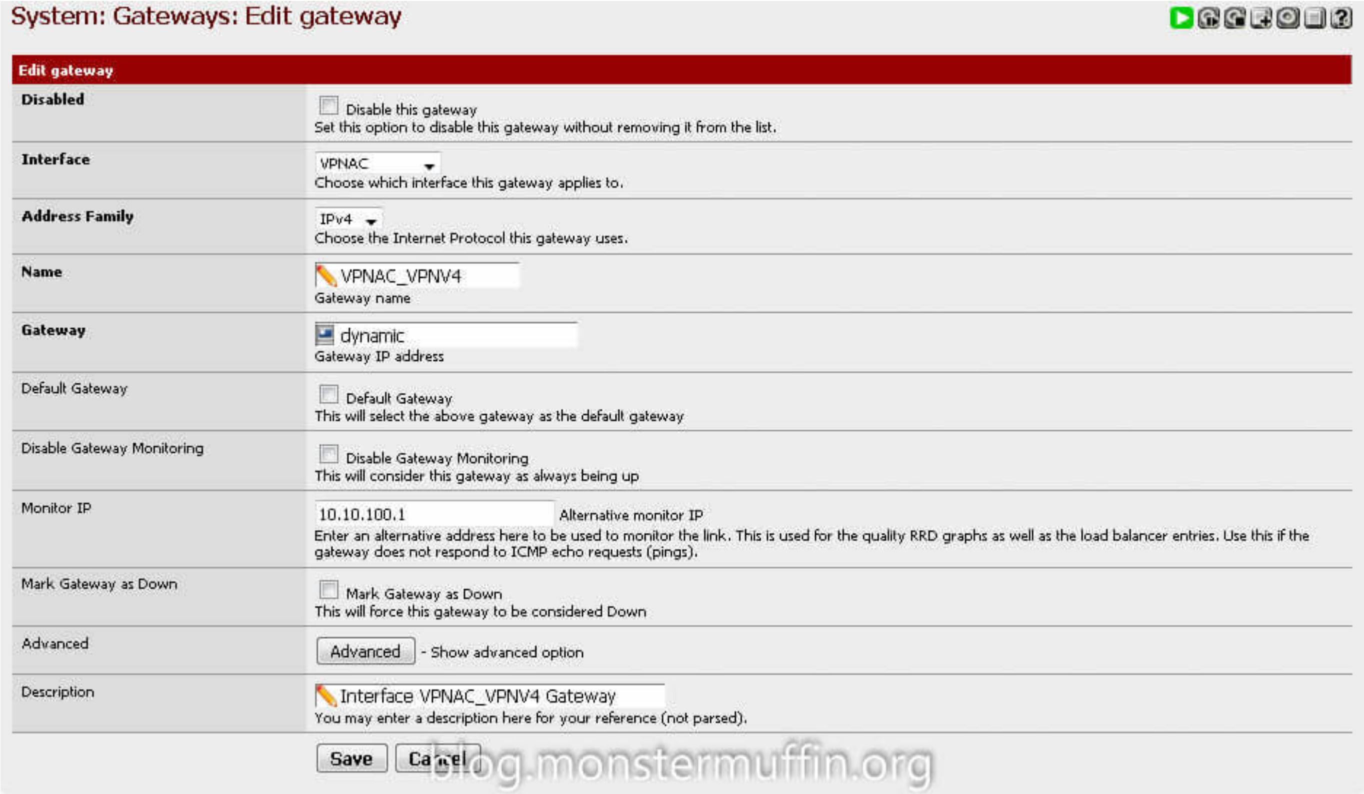
Private networks

□ Block private networks
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

□ Block bogon networks
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.

Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.

Now we have an interface for our new VPN connection head over to System > Routing and again, click the ‘+’ to add an gateway and go ahead and edit that gateway.
You want to name the gateway anything you like, and set the interface to the interface we just created. The gateway settings and monitor IP will be given by your provider.



System: Gateways: Edit gateway

Edit gateway

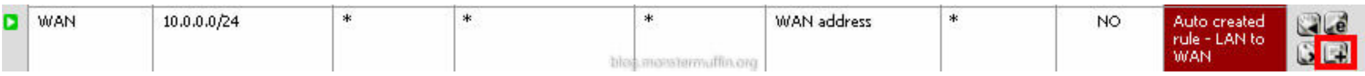
Disabled	□ Disable this gateway Set this option to disable this gateway without removing it from the list.
Interface	VPNAC Choose which interface this gateway applies to.
Address Family	IPv4 Choose the Internet Protocol this gateway uses.
Name	VPNAC_VPNV4 Gateway name
Gateway	dynamic Gateway IP address
Default Gateway	□ Default Gateway This will select the above gateway as the default gateway
Disable Gateway Monitoring	□ Disable Gateway Monitoring This will consider this gateway as always being up
Monitor IP	10.10.100.1 Alternative monitor IP Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).
Mark Gateway as Down	□ Mark Gateway as Down This will force this gateway to be considered Down
Advanced	Advanced - Show advanced option
Description	Interface VPNAC_VPNV4 Gateway You may enter a description here for your reference (not parsed).
	Save Cancel

Go ahead and save that. At this point you are ready to create the firewall rules. Now, the issue I had here is that I was unable to get anything working and it was really getting on my tits, turns out pfSense was not configuring this gateway with a valid IP/correct routes straight off the bat, or even after FW state resets. I would highly recommend a reboot here as this was the only thing that made the next few steps work.

Adding NAT Rules:

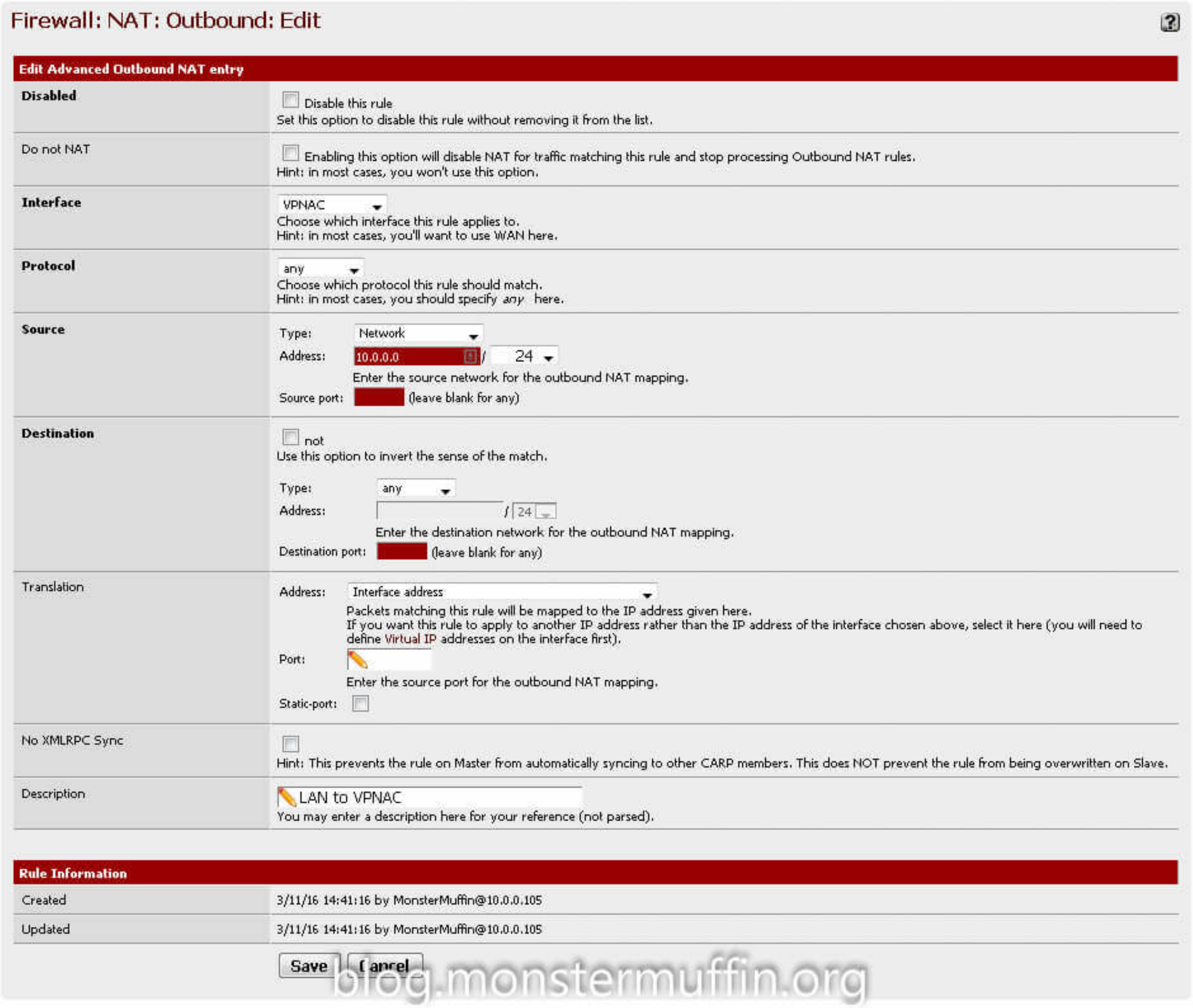
The next thing we need to do is add the NAT rules to allow for traffic to go out of the gateway, this is done from Firewall > NAT > Outbound

If you have Automatic NAT enabled you want to enable Manual Outbound NAT or Hybrid, I like hybrid NAT personally. Find the rule that allows the devices you wish to tunnel to the VPN to the internet. This is most likely “Auto created rule - LAN to WAN”



WAN	10.0.0.0/24	*	*	*	WAN address	*	NO	Auto created rule - LAN to WAN

You want to click the highlighted ‘+’ button which will create a new rule based on that one. Change the interface to your VPN interface, change the description and save.



Firewall: NAT: Outbound: Edit

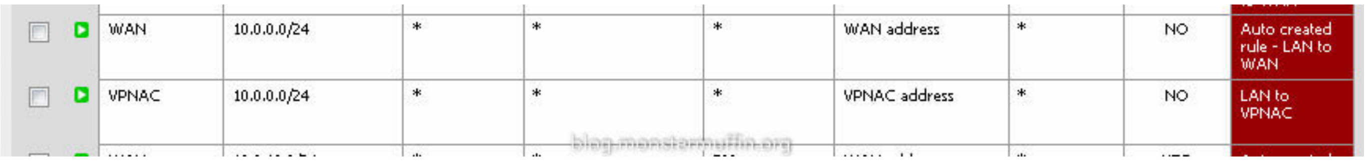
Edit Advanced Outbound NAT entry

Disabled	□ Disable this rule Set this option to disable this rule without removing it from the list.
Do not NAT	□ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules. Hint: in most cases, you won't use this option.
Interface	VPNAC Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Protocol	any Choose which protocol this rule should match. Hint: in most cases, you should specify *any* here.
Source	Type: Network Address: 10.0.0.0 / 24 Enter the source network for the outbound NAT mapping. Source port: (leave blank for any)
Destination	□ not Use this option to invert the sense of the match. Type: any Address: / 24 Enter the destination network for the outbound NAT mapping. Destination port: (leave blank for any)
Translation	Address: Interface address Packets matching this rule will be mapped to the IP address given here. If you want this rule to apply to another IP address rather than the IP address of the interface chosen above, select it here (you will need to define Virtual IP addresses on the interface first). Port: Enter the source port for the outbound NAT mapping. Static-port: □
No XMLRPC Sync	□ Hint: This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
Description	LAN to VPNAC You may enter a description here for your reference (not parsed).

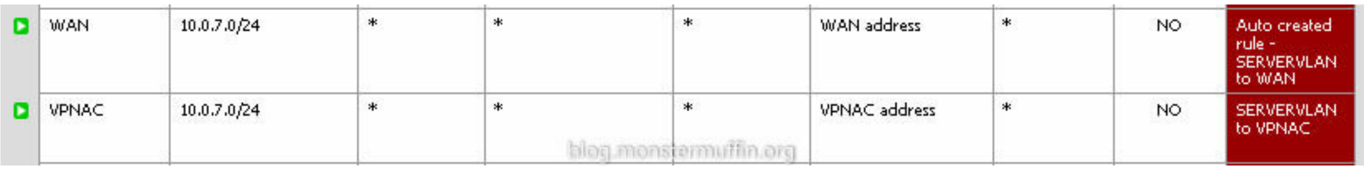
Rule Information

Created	3/11/16 14:41:16 by MonsterMuffin@10.0.0.105
Updated	3/11/16 14:41:16 by MonsterMuffin@10.0.0.105

Do this for every subnet that needs to go out to the VPN. At the end of this you should have something like this for your subnets:



□	▶	WAN	10.0.0.0/24	*	*	*	WAN address	*	NO	Auto created rule - LAN to WAN
□	▶	VPNAC	10.0.0.0/24	*	*	*	VPNAC address	*	NO	LAN to VPNAC

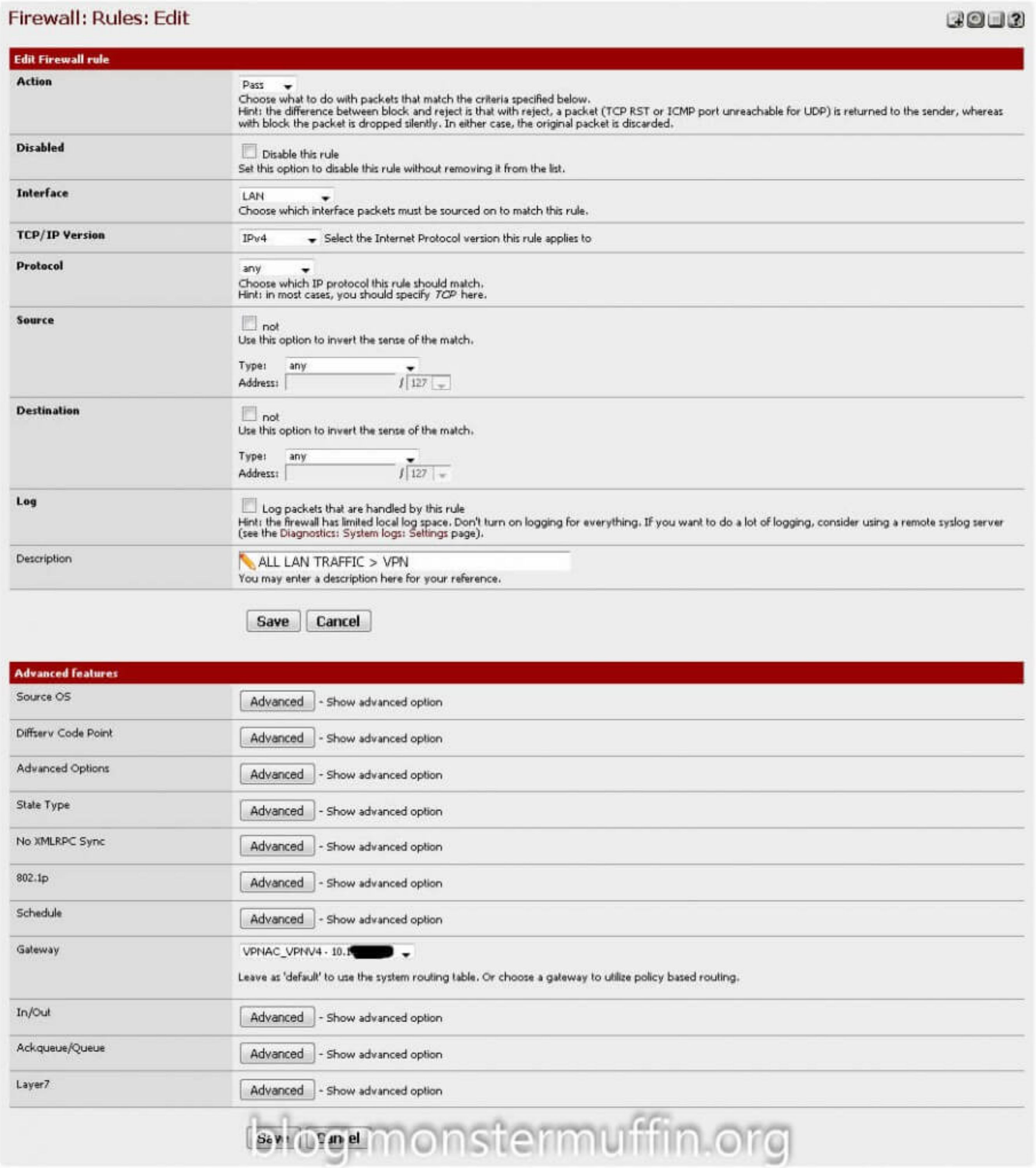


▶	WAN	10.0.7.0/24	*	*	*	WAN address	*	NO	Auto created rule - SERVERVLAN to WAN
▶	VPNAC	10.0.7.0/24	*	*	*	VPNAC address	*	NO	SERVERVLAN to VPNAC

Adding the Firewall rules:

For me, this had to be very fine grain as I only wanted download traffic on specific hosts to go out of the VPN and not all the traffic on the hosts, this was done using source and destination addresses and ports.

If you wish to send all the traffic in a subnet through the tunnel you must do the following, go to Firewall > Rules > The interface you want to tunnel > Add a new rule



Firewall: Rules: Edit

Edit Firewall rule

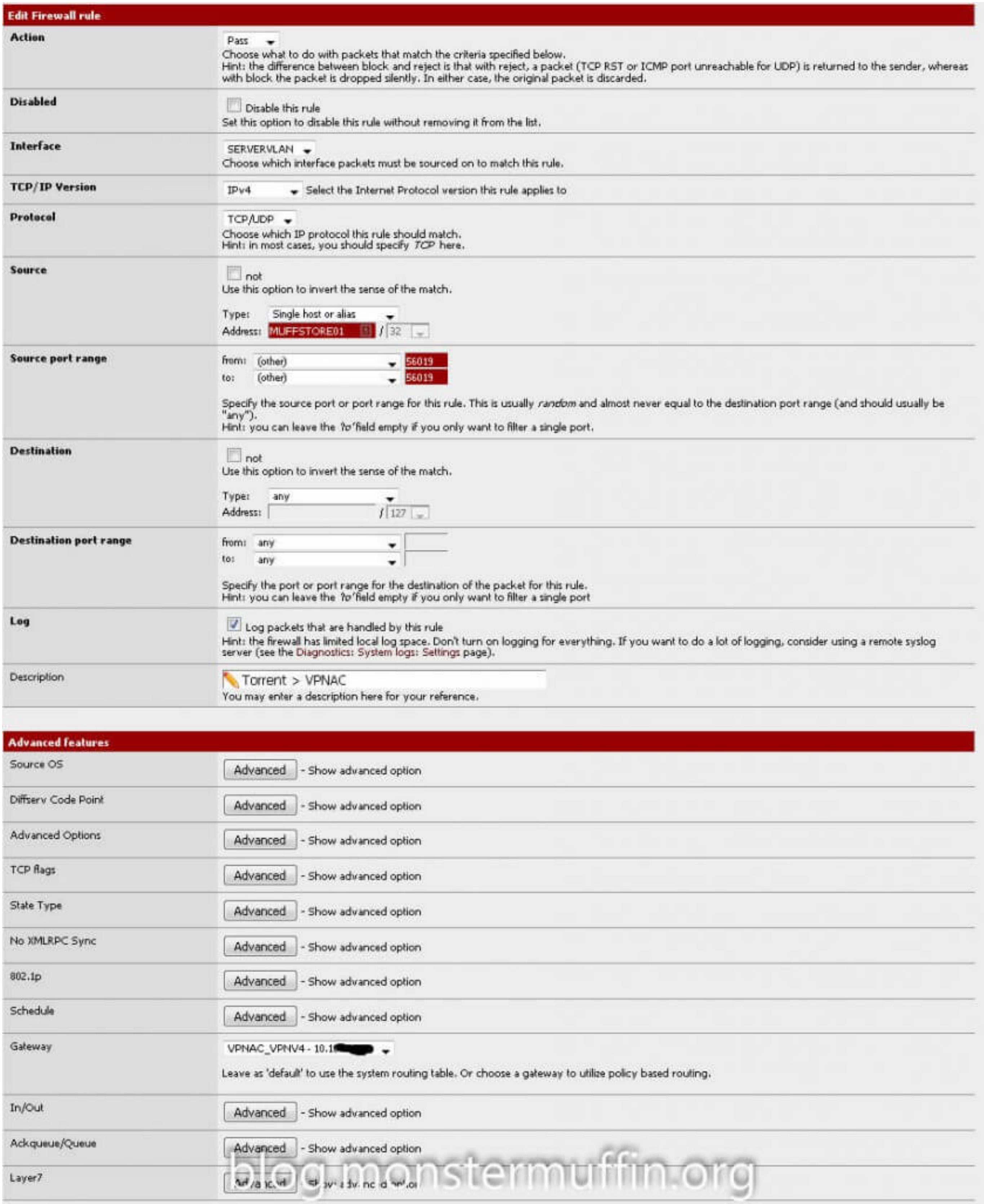
Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	□ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	LAN Choose which interface packets must be sourced on to match this rule.
TCP/IP Version	IPv4 Select the Internet Protocol version this rule applies to
Protocol	any Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	□ not Use this option to invert the sense of the match. Type: any Address: / 127
Destination	□ not Use this option to invert the sense of the match. Type: any Address: / 127
Log	□ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	ALL LAN TRAFFIC > VPN You may enter a description here for your reference.

Advanced features

Source OS	Advanced - Show advanced option
Diffserv Code Point	Advanced - Show advanced option
Advanced Options	Advanced - Show advanced option
State Type	Advanced - Show advanced option
No XMLRPC Sync	Advanced - Show advanced option
802.1p	Advanced - Show advanced option
Schedule	Advanced - Show advanced option
Gateway	VPNAC_VPNV4 - 10.1[redacted] Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.
In/Out	Advanced - Show advanced option
Ackqueue/Queue	Advanced - Show advanced option
Layer7	Advanced - Show advanced option

The above rule will send **all** the traffic on that interface into the VPN tunnel, you **must** ensure that the ‘gateway’ option is set to your VPN gateway and that this rule is **above any other rule that allows hosts to go out to the internet.** pfSense needs to be able to catch this rule before any others.

If you **don't** wish to send all the traffic, like me, you can do what I did. To start with, I tackled my torrent clients. I know my torrent client uses port 56019, manually set by me, so I created the following rule under the interface where that host lives:



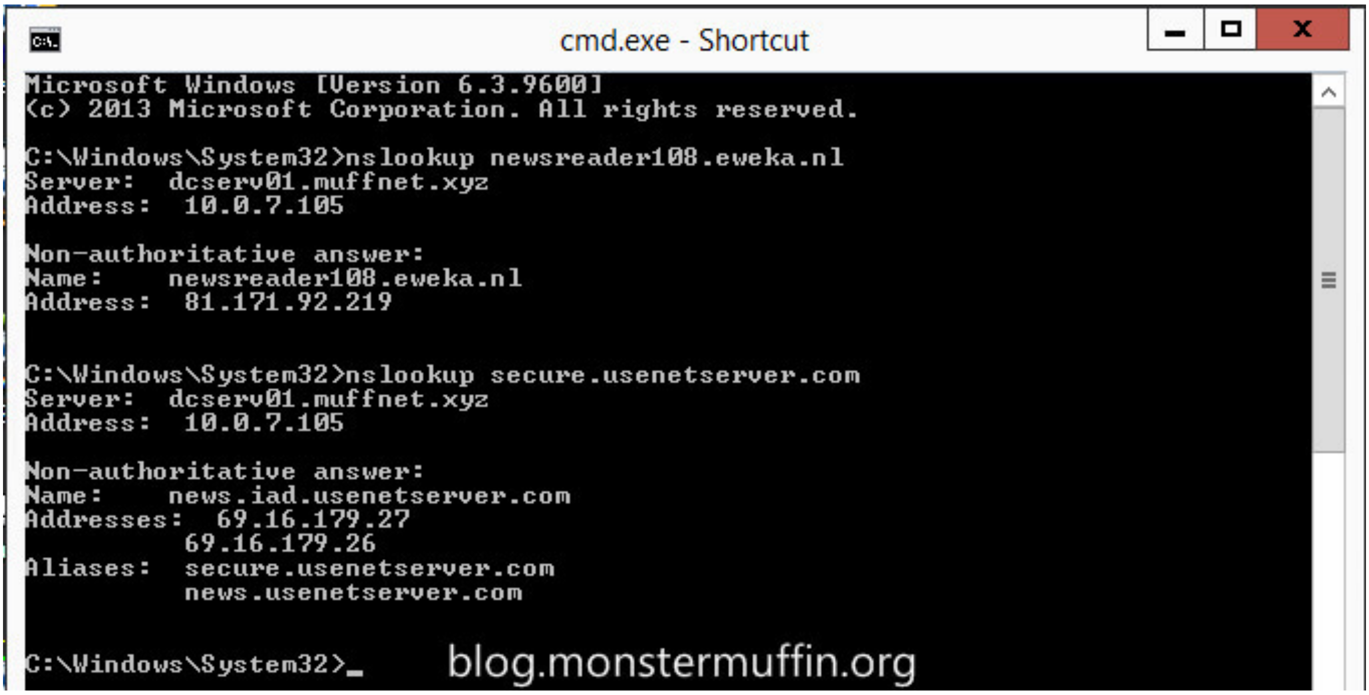
Edit Firewall rule	
Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	□ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	SERVERVLAN Choose which interface packets must be sourced on to match this rule.
TCP/IP Version	IPv4 Select the Internet Protocol version this rule applies to
Protocol	TCP/UDP Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	□ not Use this option to invert the sense of the match. Type: Single host or alias Address: MUFFSTORE01 / 32
Source port range	from: (other) 56019 to: (other) 56019 Specify the source port or port range for this rule. This is usually *random* and almost never equal to the destination port range (and should usually be "any"). Hint: you can leave the *'to'* field empty if you only want to filter a single port.
Destination	□ not Use this option to invert the sense of the match. Type: any Address: / 127
Destination port range	from: any to: any Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the *'to'* field empty if you only want to filter a single port
Log	☑ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	Torrent > VPNAC You may enter a description here for your reference.
Advanced features	
Source OS	Advanced - Show advanced option
Diffserv Code Point	Advanced - Show advanced option
Advanced Options	Advanced - Show advanced option
TCP flags	Advanced - Show advanced option
State Type	Advanced - Show advanced option
No XMLRPC Sync	Advanced - Show advanced option
802.1p	Advanced - Show advanced option
Schedule	Advanced - Show advanced option
Gateway	VPNAC_VPNV4 - 10.1[redacted] Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.
In/Out	Advanced - Show advanced option
Ackqueue/Queue	Advanced - Show advanced option
Layer7	Advanced - Show advanced option

This rule works because my torrent client is going **out** from port 56019 from the host MUFFSTORE01. I placed this rule above my default allow all rule.

Next was Usenet, Usenet downloads via HTTP/HTTPS so catching the ports wasn't going to work as all the HTTP(S) traffic would be tunneled, so instead I looked at the providers themselves. I use 2 Usenet providers, Eweka and UsenetServer. In my NZB client I looked at the hosts I was connecting to and they were the following:

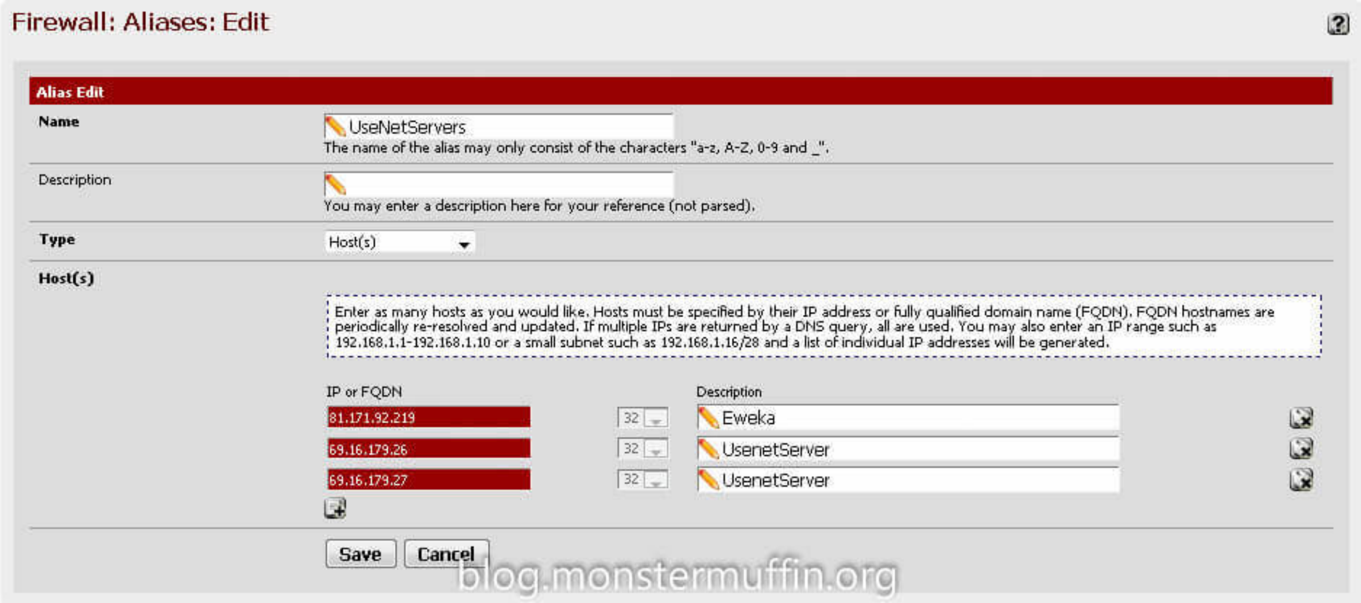
- newsreader108.eweka.nl
- secure.usenetserver.com

A quick nslookup shows me the IPs of these servers:



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\System32>nslookup newsreader108.eweka.nl
Server:  dcserv01.muffnet.xyz
Address:  10.0.7.105

Non-authoritative answer:
Name:    newsreader108.eweka.nl
Address:  81.171.92.219


C:\Windows\System32>nslookup secure.usenetserver.com
Server:  dcserv01.muffnet.xyz
Address:  10.0.7.105

Non-authoritative answer:
Name:    news.iad.usenetserver.com
Addresses:  69.16.179.27
          69.16.179.26
Aliases:  secure.usenetserver.com
          news.usenetserver.com


C:\Windows\System32>_
```

Create an Alias in pfSense under Firewall > Aliases with any name you like and the IPs of your Usenet providers.


Firewall: Aliases: Edit

Alias Edit

Name: UseNetServers
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description:
You may enter a description here for your reference (not parsed).

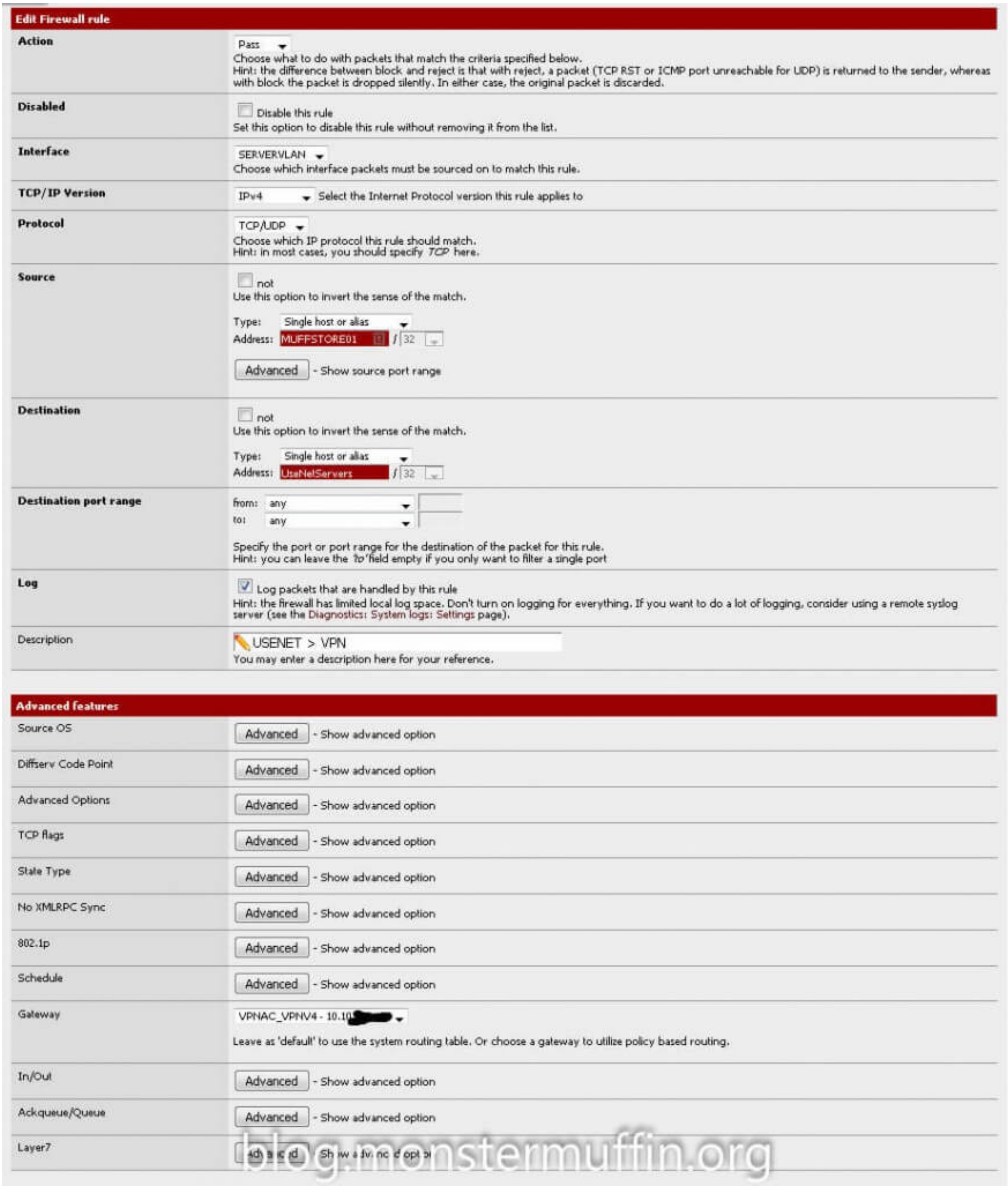
Type: Host(s)

Host(s)

Enter as many hosts as you would like. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. You may also enter an IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 and a list of individual IP addresses will be generated.

IP or FQDN		Description
81.171.92.219	32	Eweka
69.16.179.26	32	UsenetServer
69.16.179.27	32	UsenetServer

After that it's as simple as creating a rule up top in the required interface with the source as the host and the destination as your Usenet server aliases. The ports can be ANY for both source and destination, and once again you must place this rule above any other rule that will catch internet traffic for this host.



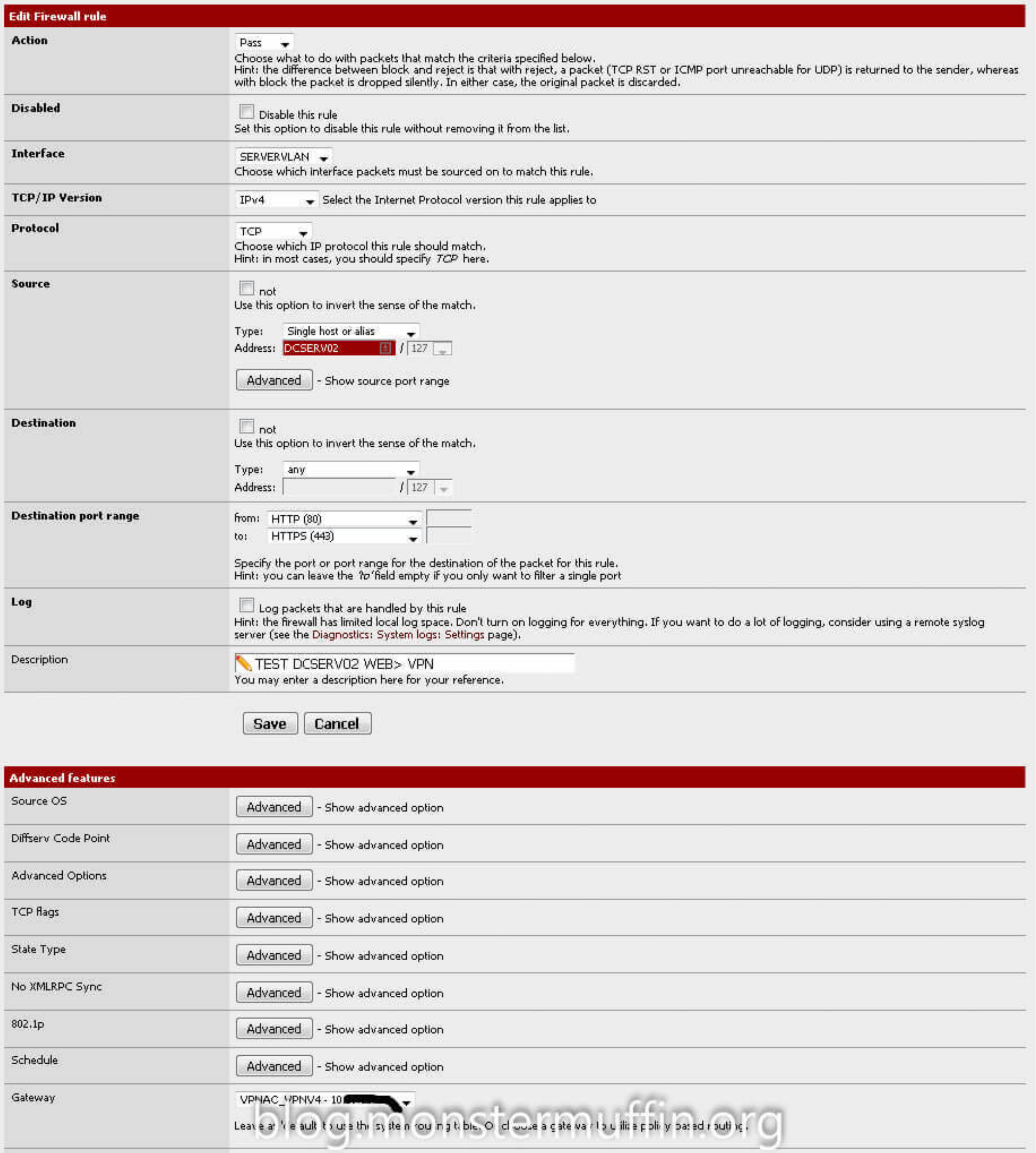
Edit Firewall rule

Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	□ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	SERVERVLAN Choose which interface packets must be sourced on to match this rule.
TCP/IP Version	IPv4 Select the Internet Protocol version this rule applies to
Protocol	TCP/UDP Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	□ not Use this option to invert the sense of the match. Type: Single host or alias Address: MUFFSTORE01 / 32 Advanced - Show source port range
Destination	□ not Use this option to invert the sense of the match. Type: Single host or alias Address: UseNetServers / 32
Destination port range	from: any to: any Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the *'to'* field empty if you only want to filter a single port
Log	☑ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	USENET > VPN You may enter a description here for your reference.

Advanced features

Source OS	Advanced - Show advanced option
Diffserv Code Point	Advanced - Show advanced option
Advanced Options	Advanced - Show advanced option
TCP flags	Advanced - Show advanced option
State Type	Advanced - Show advanced option
No XMLRPC Sync	Advanced - Show advanced option
802.1p	Advanced - Show advanced option
Schedule	Advanced - Show advanced option
Gateway	VPNAC_VPNV4 - 10.1[redacted] Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.
In/Out	Advanced - Show advanced option
Ackqueue/Queue	Advanced - Show advanced option
Layer7	Advanced - Show advanced option

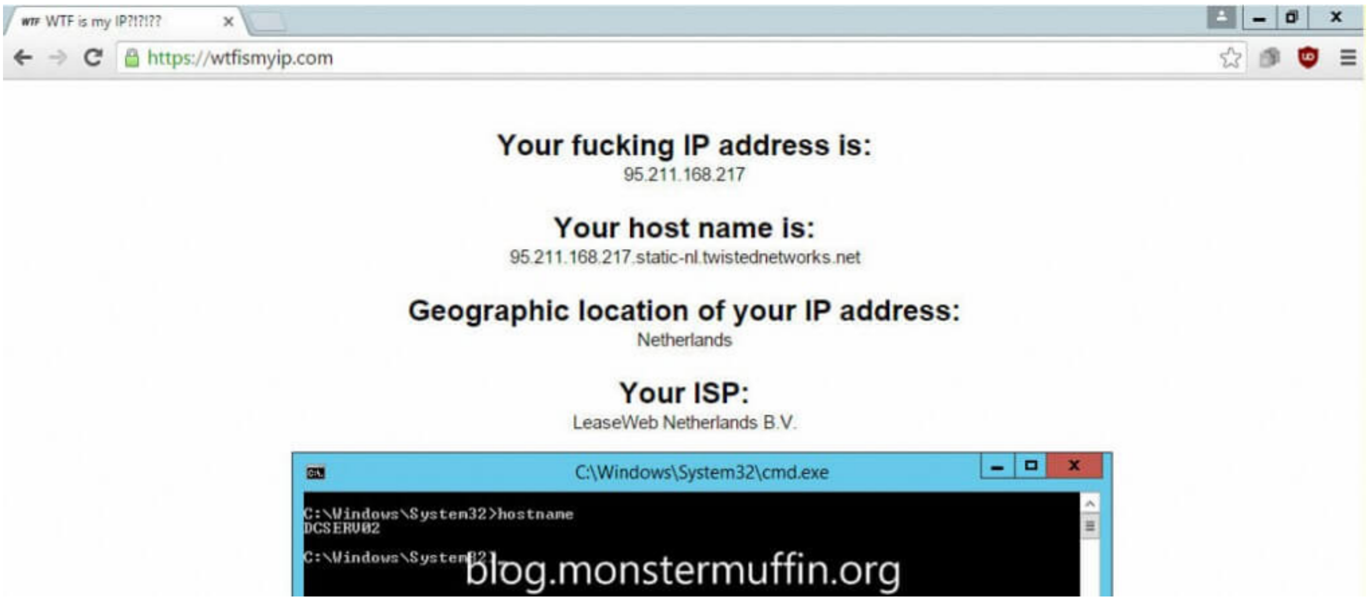
One thing you can do if you want to see this working straight away is to create a rule to send HTTP(S) for all traffic from one of your hosts to the VPN gateway and place it on top, I did this:



Edit Firewall rule	
Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	□ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	SERVERVLAN Choose which interface packets must be sourced on to match this rule.
TCP/IP Version	IPv4 Select the Internet Protocol version this rule applies to
Protocol	TCP Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	□ not Use this option to invert the sense of the match. Type: Single host or alias Address: DCSERV02 / 127 Advanced - Show source port range
Destination	□ not Use this option to invert the sense of the match. Type: any Address: / 127
Destination port range	from: HTTP (80) to: HTTPS (443) Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the *'to'* field empty if you only want to filter a single port
Log	□ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	TEST DCSERV02 WEB> VPN You may enter a description here for your reference.
	Save Cancel
Advanced features	
Source OS	Advanced - Show advanced option
Diffserv Code Point	Advanced - Show advanced option
Advanced Options	Advanced - Show advanced option
TCP flags	Advanced - Show advanced option
State Type	Advanced - Show advanced option
No XMLRPC Sync	Advanced - Show advanced option
802.1p	Advanced - Show advanced option
Schedule	Advanced - Show advanced option
Gateway	VPNAC_VPNV4 - 10[redacted] Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.

After all your desired rules are in place head over to Diagnostics > States > Reset States and click on **reset states.** After doing **any** firewall changed that involve a gateway change I would do this before checking if anything has worked as in my experience it will not. PfSense WebGUI may hang once you do this and it will take a few seconds for routing to come back and up to a minute for the GUI to come back, don't panic.

Once you're done head over to any host you configured and start downloading something, for me I went over the host I was tunneling HTTP(S) and used my favourite IP checker to see what the result was, and:



Your fucking IP address is:
95.211.168.217

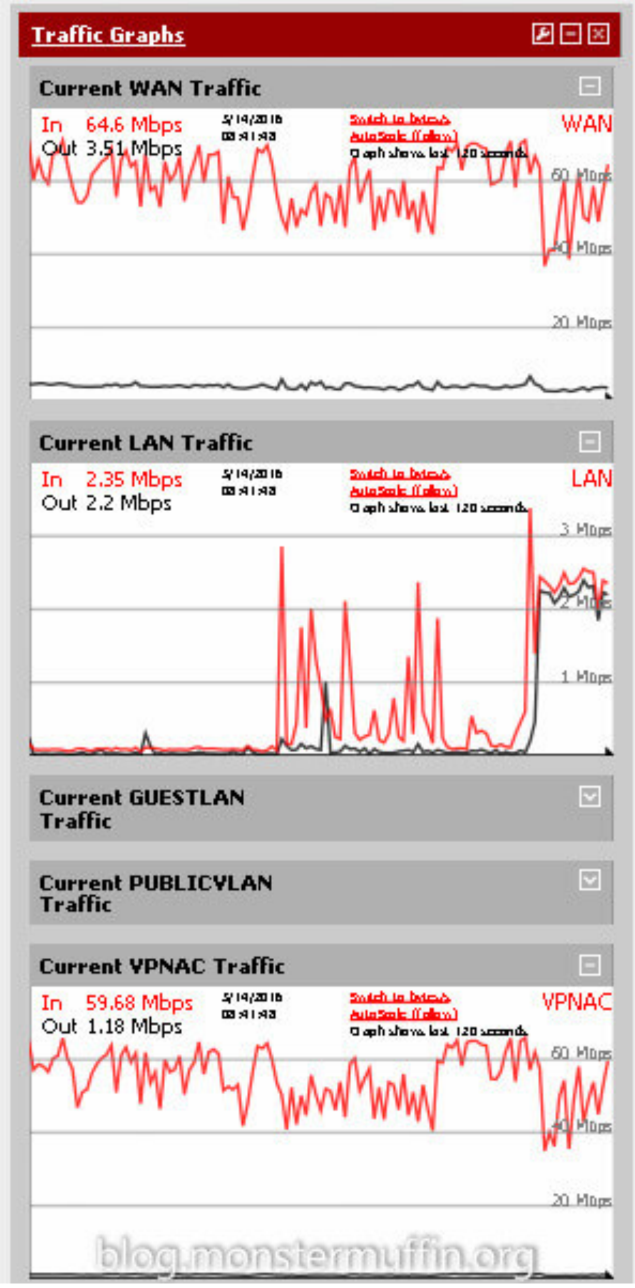
Your host name is:
95.211.168.217.static-nl.twistednetworks.net

Geographic location of your IP address:
Netherlands

Your ISP:
LeaseWeb Netherlands B.V.

```
C:\Windows\System32>hostname
DCSERV02

C:\Windows\System32>
```

Success! Testing the torrents and NZBs was pretty simple. Add the VPN interface to your dashboard under traffic graphs and start downloading something separately. If you see traffic going out of the interface you know it’s working, here you can see I started downloading an NZB and the VPN interface matched the traffic that the application was using, as well as this it is *only* the Usenet traffic and torrent traffic, browsing the web still gives me my WAN IP, which is what I want.


Traffic Graphs

Current WAN Traffic

In 64.6 Mbps
Out 3.51 Mbps

Current LAN Traffic

In 2.35 Mbps
Out 2.2 Mbps

Current GUESTLAN Traffic

Current PUBLICVLAN Traffic

Current VPNAC Traffic

In 59.68 Mbps
Out 1.18 Mbps

And there you have it, using fine grain firewall rules you can tunnel as little or as much of your internet traffic over a VPN using pfSense. I live in London and downloading through the Netherlands servers that VPN.AC provides I was able to saturate my download speed which is a huge win, obviously your milage may vary depending on a number of factors but with so many providers offering free trials it’s worth a try.

I hope this was helpful and good luck! MM~~

Tutorial, Networking

vpn, tunnel traffic, privacy, hide traffic, p2p, PfSense, TUTORIAL

‹ Building a Rackmount Storage Server

› Getting Started with VMware’s ESXi

45 thoughts on “Tunneling Specific Traffic over a VPN with pfSense

8 min read

”

rehman

March 2, 2021 at 9:09 am | Reply

It’s working out pretty great actually! Not noticed any slowdowns in my downloading and the piece of mind is nice. The VPN is also great to use on the go when I’m abroad far away from my lab as they have servers in many places.CDDS

Like

billy

February 8, 2021 at 7:00 am | Reply

Thank you. This was really helpful. Maybe you should leave a donation address? This and your networking article has got me up and running.

Like

Nathan

February 3, 2021 at 8:42 pm | Reply

This works for all incoming traffic, however outgoing traffic gets assigned a (semi) random source port by the Operating System. In the case of P2P traffic, this would mean downloads are not tunneled through the VPN, only uploaded content. Any idea on how to solve this issue without restricting an entire device to use the VPN?

Like

Dick

December 12, 2020 at 9:48 pm | Reply

Usenet is SSL encrypted so you are just wasting your time with the Vpn to be honest.

Like

Emma

October 28, 2020 at 8:37 am | Reply

i just noticed that the incoming packets do not go through the tunnel but through the wan. Because of this my client, transmission, thinks that my port is closed.

Like

Pingback: pfSense – syspiloz

andrew
June 17, 2020 at 2:33 pm | Reply

Thanks for the write up! I tested this and it looks like all traffic is going via the VPN interface. Did you think to block the port on wan then only allow this port on VPN instead? Reason being to a) if the vpn interface is down is blocked anyways on the WAN interface. and b) to try and apply QoS (I have FQ_CODEL applied but I don't think it's actually shaping the openvpn traffic yet)

Loading...

Robb
October 6, 2019 at 8:28 am | Reply

Great post. I would have used the FQDN instead of IP for your usenet. Should they change IP, or have a pool of addresses, this will ensure your rule will continue to work.

Loading...

chris
June 24, 2019 at 9:43 pm | Reply

On the client PC do I need to specify PFsense as the gateway and DNS ?

Loading...

chris
June 24, 2019 at 9:44 pm | Reply

I have my router at 192.168.0.1 and pfsense on 192.168.0.70. router runs dns and gateway.

Loading...

rafiks
December 4, 2018 at 3:24 pm | Reply

how do i port forward using the VPN, i just noticed that the incoming packets do not go through the tunnel but through the wan. Because of this my client, transmission, thinks that my port is closed.

Loading...

rafiks
November 5, 2018 at 1:44 am | Reply

hi!
thank you for this tutorial. i got it working on my usenetexpress account.

Loading...

rafiks
November 11, 2018 at 1:24 pm | Reply

i have a couple questions.
1. on the traffic graph. it seems my traffic is going outbound. is this correct?
2. how do i verify in pfsense that my traffic is going to through the VPN. i do not run a gui i only have CLI on my server.

thanks.

Loading...

MonsterMuffin
November 13, 2018 at 4:37 pm | Reply

Yes, this is correct.

And you can just curl something like the following: https://wtfismyip.com/text

Loading...

Loading...

rafiks
November 14, 2018 at 12:16 am | Reply

Curl. Thanks. I forgot about that awesome tool.

Loading...

Sal
July 10, 2018 at 9:43 am | Reply

Thanks for this. I’m looking to switch VPN’s so that I can accomplish this. I tried creating a P2P only tunnel with AirVPN’s Eddie, but it relies on launching .bat files in conjunction with the client, and the overall operation is problematic and inconsistent for several reasons – AirVPN’s standard recommendation is “run a VM”

Do you have a link to a good pfsense tutorial to get started running it in Win 10? Then I’d move to VPN.ca and use this tutorial.

Loading...

shetu
April 29, 2018 at 7:25 pm | Reply

Hi
I want forward 5060 port to my pfsense via vps openvpn server. I add vpn client to pfsense and able to forward tcp port but no udp sip port. Here is my iptables commadn at centos openvz vps.

```
iptables -t nat -A PREROUTING -p udp -dport 5004:5082 -j DNAT -to-destination 10.8.0.2
iptables -t nat -A PREROUTING -p udp -dport 10000:65000 -j DNAT -to-destination 10.8.0.2
iptables -t nat -I POSTROUTING -d vps ip -j SNAT -to 10.8.0.2
```

Loading...

Nicki Patrzalek
January 29, 2018 at 9:59 pm | Reply

I looked up vpn.ac and they dont seem to support port forwarding. How did you resolve this?

I have PIA at the moment. And if I just port forward without using their prober way of doing it, it will not work.

So I am guessing your torrent client would say the port is not open?

Loading...

John Jacobs
December 31, 2017 at 11:56 pm | Reply

I was able to take your guide and modify it a bit to send traffic based on LAN IPs rather than ports. It seems to work except for some reason when I want to have a port open, I can’t seem to get it to work. When I check to see if my ports are forwarded correctly on the clients that are set to use the VPN, it appears as though I’m behind a firewall. Is this normal? The only setting I couldn’t set was the “Monitor IP” for the gateway because my VPN provider doesn’t specify what this should be. Could this be why no clients can connect directly to my PC in the LAN?

Loading...

Kevin Burke
December 19, 2017 at 9:55 pm | Reply

This is easier to follow, more clear and concise than the vast majority of pfSense guides I’ve encountered. Kudos.

Loading...

Ben Dixon
December 4, 2017 at 4:33 pm | Reply

This blog post is awesome, but it doesn’t seem to work for ipsec. Any tips on an equivalent goal with ipsec?

I have a site-to-site ipsec VPN where I want to send everything but the local subnet over the VPN. If I follow along, I don’t have a way to add an interface on the interface assignments tab with ipsec..there isn't an add or plus icon with pfsense 2.4. So I'm unable to create the VPN gateway that would eventually allow me to create firewall rules customized for the proper gateway (VPN or not).

Currently, my site to site works great, but all my local private traffic "breaks" once I connect to site B. After connection, I have no connectivity to site A.

Loading...

Pingback: Set up OpenVPN tunnel on pfSense – Chris Tech Blog

Zombiekiller
April 15, 2017 at 4:47 am | Reply

Having a strange issue when i try to add the firewall rule. When trying to select the "VPN" gateway from the drop down menu, I don't have the option to select my VPN gateway. The only one in the list is my "default" gateway.

Loading...

zombiekiller
April 16, 2017 at 3:18 am | Reply

Nm – total noon mistake.

Loading...

MonsterMuffin

April 16, 2017 at 12:14 pm | Reply

Glad to see you got it working!

Loading...

Cal

April 10, 2017 at 4:14 pm | Reply

Great article and site. Kudo's

Question I was researching is along this same topic (and split tunnel) for VPN.

OpenVPN (PIA) is working sweet on my pfsense box. I am having a problem with our new Toy (Amazon Fire TV), and Playstation Vue, which is zip code specific.

Do you suggest I put a static IP on the AFT, Roku, etc. and route them through my pfSense OpenVPN with exceptions? Examples?

Loading...

MonsterMuffin

April 11, 2017 at 6:27 am | Reply

Pretty much. I'll be making a new post soon detailing this process in light of recent security clusterfucks that governments are bringing down.

You can either route the static IPs via your main connection, or set the destination IPs in an alias and set those IPs to go via the normal gateway.

I do this for iPlayer so any device in the house can still access iPlayer whilst all other traffic is tunneled via Amsterdam.

Loading...

n99
April 12, 2017 at 5:07 am | Reply

If you could, please post details regarding this. My desire would be to have certain destination IP's go around the VPN Tunnel. Any help with that would be very much appreciated.

Loading...

Tyler
April 26, 2017 at 5:38 am | Reply

Not entirely sure how possible this would be, but what about doing this at layer 7 and allowing a particular application to bypass the VPN rule?

Loading...

SirChoice
September 27, 2017 at 6:40 pm | Reply

Did you get to write this up yet? It’s exactly what I want to setup but keep hitting issues!

Loading...

Steveo
April 6, 2017 at 9:34 pm | Reply

Wow – you know your stuff when it comes to PFsense. Well done.

Loading...

Darren David
April 5, 2017 at 3:28 pm | Reply

THANK YOU for the amazing writeup. I’ve seen similar writeups elsewhere, but this is quite thorough and detailed. All that said, I’m hitting a wall here. I’m also a VPN.ac user and I’ve followed this all exactly, VPN link is up, but as soon as I add the LAN rule, network connectivity fails from the specific host. I can see the logged requests getting a PASS in the firewall system log, but there’s no response. It’s as if there’s something funky with NAT. Any ideas where/how to troubleshoot?

Loading...

MonsterMuffin

April 6, 2017 at 12:17 pm | Reply

Hi Darren, have you ensured you added a NAT rule for the subnet to use the VPNAC gateway?

If you need some help feel free to PM me on discord at MonsterMuffin#3820

Loading...

Darren David

April 7, 2017 at 4:34 am | Reply

I solved it. Turns out if I enable compression traffic doesn’t flow. Set compression to “none specified” and everything works like a charm. Also notable that “Encryption Algorithm” for me is AES-256-CBC and “Auth digest algorithm” is SHA512. Thanks again for the instructions!

Loading...

MonsterMuffin

April 7, 2017 at 8:37 am | Reply

Huh, I’ve never seen that before, good to know.

Glad to see you got it fixed though, enjoy!

Loading...

dd

April 18, 2017 at 4:45 am

OK, so now I’m trying to get tricky and things aren’t playing nicely. My goal is to run 2 VPN connections to VPN.ac: 1 to some far flung part of the world for the kind of traffic described in your sample here, and a second connection to a local server for all regular traffic, just for privacy’s sake. The good news: I can get them both working successfully! However, as soon as I flip on the LAN pass rule to redirect the traffic for all DHCP clients to run through the 2nd VPN, all of my inbound NAT port forwarding rules to my server (not in the DHCP block) stop working completely. Basically, as soon as I enable the pass rule for the 2nd VPN, I can no longer access my server remotely. If I disable that rule and flush the states, they start working again. Thoughts?

Loading...

Zachary Grimshaw
March 30, 2017 at 1:38 am | Reply

I can set a rule that sends all traffic from one static IP out through my VPN successfully, but when I specify a port (my torrent client) it seems to just ignore the rule. Any ideas why this happens?

Loading...

Aki
September 16, 2017 at 1:42 am | Reply

I am having the same problem. Copied your setting with vpn.ac, it works if I set to pass all traffic through the VPN, but not with specific ports. I noticed the difference in the screenshots, one has LAN and other has SERVERBVLAN as interface. Is this significant? Or any suggestions?

Loading...

Mark Warren
October 8, 2018 at 8:03 pm | Reply

I'm getting the same results, works fine when all traffic goes through it, but if I set it to use ports then it just ignores the rule. Did you ever find a solution?

Loading...

Mark Epps
August 22, 2016 at 12:37 pm | Reply

Thank you, This helped me figure everything out.

Loading...

Tom
August 11, 2016 at 10:46 am | Reply

How is the VPN.ac working for you? I am considering switching after looking at the charts.

Loading...

MonsterMuffin
September 6, 2016 at 7:20 am | Reply

It’s working out pretty great actually! Not noticed any slowdowns in my downloading and the piece of mind is nice. The VPN is also great to use on the go when I’m abroad far away from my lab as they have servers in many places.

Loading...

Mat Miller
August 9, 2016 at 6:22 pm | Reply

Great, thanks for sharing! One other way you could test if the rules are working is by doing a traceroute from a host the rules apply to.

Loading...

MonsterMuffin
September 6, 2016 at 7:22 am | Reply

Well, this would only be a valid test if you were forwarding the entire machine, else you would need to add ICMP to the forwarding rule.

Loading...

Jeffrey Hardy
July 30, 2016 at 5:51 pm | Reply

Awesome article.Thanks for sharing

Loading...

Leave a Reply

Enter your comment here...

This site uses Akismet to reduce spam. Learn how your comment data is processed.