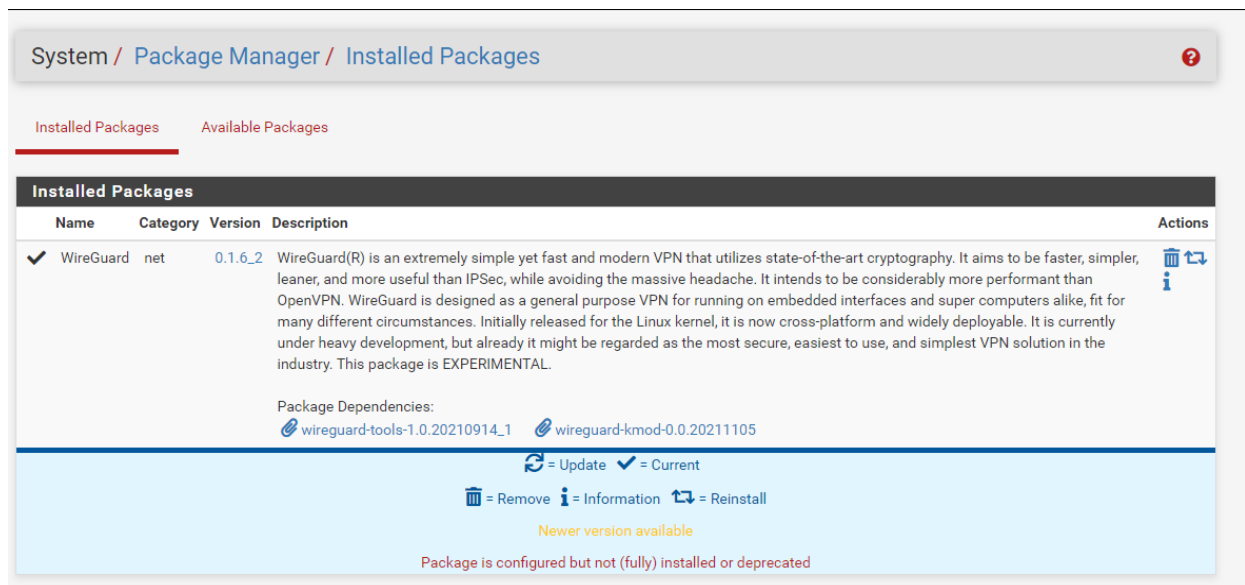


Setting up a Surfshark WireGuard connection on **pfSense 2.6.0**.

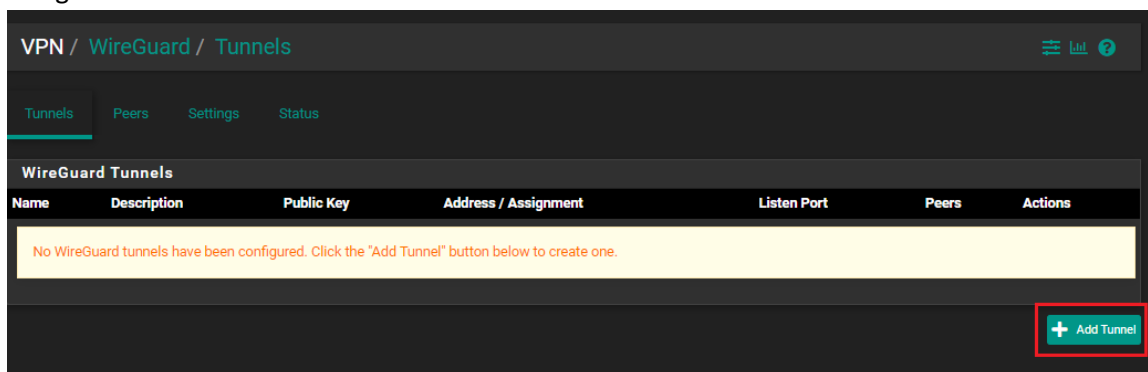
Firstly, we're going to have to install the WireGuard connection package.  
To do so, follow these steps.

1. Click **System > Package Manager** and go to **Available Packages**.
2. Search for *wireguard* and install the **WireGuard** package.



Next, we're going to have to set up the WireGuard VPN tunnel.

1. Navigate to **VPN > WireGuard** and click on **+ Add Tunnel**.



2. Check **Enabled**.
3. Enter a **Description** - in our example, we used *Surf\_BR*. This field can be filled in however you like.
4. **Listen Port**, by default, should be 51820. Leave it so.
5. Enter your **Public key** and **Private key** from [https://my.surfshark.com/vpn/manual-setup/main/wireguard\\_credentials](https://my.surfshark.com/vpn/manual-setup/main/wireguard_credentials) tab.

The configuration should end up looking like so:

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

VPN / WireGuard / Tunnels / Edit

Tunnels Peers Settings Status

### Tunnel Configuration (tun\_wg0)

**Enable** ☒ **Enable Tunnel**  
Note: Tunnel cannot be disabled when assigned to a pfSense interface.

**Description**   
Description for administrative reference (not parsed).

**Listen Port**   
Port used by this tunnel to communicate with peers.

**Interface Keys**  
Private key for this tunnel. (Required)  Public key for this tunnel. (Copy)   New Keys

### Interface Configuration (tun\_wg0)

Enter your Public and Private keys here.

**Assignment** ☒ SURF\_01 (opt1)

**Interface** ☒ Interface Configuration

**Firewall Rules** ☒ Firewall Configuration

### Peer Configuration

| Description | Public key          | Tunnel  | Allowed IPs | Endpoint : Port                 | Actions   |
|-------------|---------------------|---------|-------------|---------------------------------|---|
| SurfShark   | IFTVXxhLEqVgZI/J... | tun_wg0 | 0.0.0.0/0   | br-sao.prod.surfshark.com:51820 | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

After, we need to configure the **Peer Configuration**.

You can do so by entering the **Peers** tab or by pressing **Add Peer** at the bottom of the window.

1. **Description** - describe the VPN server name.
2. **Dynamic Endpoint** needs to be unchecked!
3. In the **Endpoint** field, enter the hostname of the server. In our example, it is *br-sao.prod.surfshark.com* also, make sure to configure the port to **51820**.
4. We can set **Keep Alive** to 25.
5. **Public Key** field needs to be filled with the server's public key address. You can find it in the server's configuration file, or in <https://my.surfshark.com/vpn/manual-setup/main/wireguard> after selecting a server.

## Download configuration files

Location

**Brazil • Sao Paulo**



Server address

br-sao.prod.surfshark.com



Server IP

138.199.58.57



Server public key

IFTVXxhLEqVgZI/JGOPRtmrNUQW1DN...



Download

WireGuard configuration files



Close

6. Leave the **Pre-shared Key** section blank.
7. **Allowed IPs** - enter **0.0.0.0/0**.  
When done, click **Save Peer** and **Apply Changes** buttons.  
The finished configuration should look as follows:

VPN / WireGuard / Peers / Edit

Tunnels Peers Settings Status

### Peer Configuration

**Enable** ☒ **Enable Peer**  
Note: Uncheck this option to disable this peer without removing it from the list.

**Tunnel** tun\_wg0 (Surf\_BR)  
WireGuard tunnel for this peer. (Create a New Tunnel)

**Description** SurfShark  
Peer description for administrative reference (not parsed).

**Dynamic Endpoint** ☐ **Dynamic**  
Note: Uncheck this option to assign an endpoint address and port for this peer.

**Endpoint** br-sao.prod.surfshark.com 51820  
Hostname, IPv4, or IPv6 address of this peer. Leave endpoint and port blank if unknown (dynamic endpoints). Port used by this peer. Leave blank for default (51820).

**Keep Alive** 25  
Interval (in seconds) for Keep Alive packets sent to this peer. Default is empty (disabled).

**Public Key**   
WireGuard public key for this peer.

**Pre-shared Key** Pre-shared key   
Optional pre-shared key for this tunnel. (Copy) New Pre-shared Key

### Address Configuration

Hint: Allowed IP entries here will be transformed into proper subnet start boundaries prior to validating and saving.

**Allowed IPs** 0.0.0.0 / 0   
IPv4 or IPv6 subnet or host reachable via this peer. Description for administrative reference (not parsed).

**Add Allowed IP**

Next up, we're going to have to configure the **Interfaces**.

1. Navigate to **Interfaces > Assignments** and click the **+ Add** button besides **Available network ports: tun\_wg0**. The interface becomes **OPT1** (or another OPT\*).
2. Click the **Save** button.
3. Click on **OPT1** interface name link and put a check mark beside **Enable**.
4. Change the description from **OPT1** to what you like. In our example, we chose *Surf\_01*.
5. Change the **IPv4 Configuration Type** to **Static IPv4**. On **IPv6 Configuration Type**, select **None**.
6. Enter **1420** in the **MTU** field and leave **MAC Address** and **MSS** fields blank.
7. Into **IPv4 Address**, enter **10.14.0.2**.  
 Beside **IPv4 Upstream gateway**, click on **+ Add a new gateway**.

In **Gateway name**, enter whatever you like. In our example, we are using *Surf\_01* once again.  
 In **Gateway IPv4**, enter **10.14.0.2**.

## New IPv4 Gateway

Default ☒ Default gateway

Gateway name

Gateway IPv4

Description

Lastly, click the **Save** button and click the **Apply Changes** button.  
The finished setup should look like so:

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Interfaces / Surf\_01 (tun\_wg0)

### General Configuration

Enable ☒ Enable interface

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

IPv4 Configuration Type

IPv6 Configuration Type

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

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

MSS   
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

### Static IPv4 Configuration

Add new gateway IPv4 10.14.0.2

IPv4 Address  / 32

IPv4 Upstream gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be "none".  
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).  
Gateways can be managed by [clicking here](#).

### Reserved Networks

Block private networks ☐

- If you have no devices connected to your pfSense device via LAN, you can skip this step.

Go to **Interfaces > LAN** and set the **MSS** to 1412.

Other settings should be left untouched and this only applies if you are using a LAN connection from your pfSense device. The settings should look like so:

Interfaces / LAN (hn1)

**General Configuration**

**Enable** ☒ Enable interface

**Description** LAN  
Enter a description (name) for the interface here.

**IPv4 Configuration Type** Static IPv4

**IPv6 Configuration Type** None

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

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

**MSS** 1412  
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

**Speed and Duplex** Default (no preference, typically autoselect)  
Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

**Static IPv4 Configuration**

**IPv4 Address** 192.1 / 24

**IPv4 Upstream gateway** None [+ Add a new gateway](#)  
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be "none".  
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).  
Gateways can be managed by [clicking here](#).

Next up, we need to configure pfSense **Firewall** settings.

1. Navigate got **Firewall > NAT > Outbound** and change the mode to **Manual**.

Firewall / NAT / Outbound

Port Forward 1:1 **Outbound** NAT

**Outbound NAT Mode**

**Mode**

Automatic outbound NAT rule generation. (IPsec passthrough included)

Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)

**Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)**

Disable Outbound NAT rule generation. (No Outbound NAT rules)

[Save](#)

2. Click on the **Save** button and click the **Apply Changes** button.
3. Now look for the entry that contains your local network subnet (**the one that does not contain port "500" or IP address "127.0.0.0" entries, this might be 192.168.1.0/24 for example**) and click on the **Pen icon (Edit mapping)**.
4. Change **Interface** to *Surf\_01* and change the **Description** to mention the VPN, like **LAN to SURF\_01** for easier navigation and understanding of the settings.
5. Click the **Save** button and click the **Apply Changes** button.
6. Delete the other rule(s) containing your local network subnet that exists via WAN, (keep the

127.0.0.0). This will ensure that traffic does not leak if the VPN tunnel accidentally goes down.  
*You can choose to skip this step.*

7. Finally, click the **Apply Changes** button once again.

In our case, the **Outbound** settings ended up looking like so:

Firewall / NAT / Outbound

Port Forward 1:1 Outbound NAT

Outbound NAT Mode

Mode

- Automatic outbound NAT rule generation. (IPsec passthrough included)
- Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
- Disable Outbound NAT rule generation. (No Outbound NAT rules)

Save

Mappings

|                                     | Interface | Source         | Source Port | Destination | Destination Port | NAT Address     | NAT Port | Static Port | Description   | Actions |
|-------------------------------------|-----------|----------------|-------------|-------------|------------------|-----------------|----------|-------------|---|---------|
| <input checked="" type="checkbox"/> | WAN       | 127.0.0.0/8    | *           | *           | 500 (ISAKMP)     | WAN address     | *        | ✓           | Auto created rule for ISAKMP - localhost to WAN     |         |
| <input checked="" type="checkbox"/> | WAN       | 127.0.0.0/8    | *           | *           | *                | WAN address     | *        | ✗           | Auto created rule - localhost to WAN                |         |
| <input checked="" type="checkbox"/> | SURF_01   | 127.0.0.0/8    | *           | *           | 500 (ISAKMP)     | SURF_01 address | *        | ✓           | Auto created rule for ISAKMP - localhost to SURF_01 |         |
| <input checked="" type="checkbox"/> | SURF_01   | 127.0.0.0/8    | *           | *           | *                | SURF_01 address | *        | ✗           | Auto created rule - localhost to SURF_01            |         |
| <input checked="" type="checkbox"/> | WAN       | ::1/128        | *           | *           | 500 (ISAKMP)     | WAN address     | *        | ✓           | Auto created rule for ISAKMP - localhost to WAN     |         |
| <input checked="" type="checkbox"/> | WAN       | ::1/128        | *           | *           | *                | WAN address     | *        | ✗           | Auto created rule - localhost to WAN                |         |
| <input checked="" type="checkbox"/> | SURF_01   | ::1/128        | *           | *           | 500 (ISAKMP)     | SURF_01 address | *        | ✓           | Auto created rule for ISAKMP - localhost to SURF_01 |         |
| <input checked="" type="checkbox"/> | SURF_01   | ::1/128        | *           | *           | *                | SURF_01 address | *        | ✗           | Auto created rule - localhost to SURF_01            |         |
| <input checked="" type="checkbox"/> | SURF_01   | 192.168.1.0/24 | *           | *           | 500 (ISAKMP)     | SURF_01 address | *        | ✓           | Auto created rule for ISAKMP - LAN to SURF_01       |         |
| <input checked="" type="checkbox"/> | SURF_01   | 192.168.1.0/24 | *           | *           | *                | SURF_01 address | *        | ✗           | Auto created rule - LAN to Surf_01                  |         |

Next up, we must configure the Rules.

1. Navigate to **Firewall > Rules > LAN**, click the **Add (top)** button and set the following:  
**Action: Pass**  
**Interface: LAN**  
**Address Family: IPv4**  
**Protocol: Any**  
**Source: LAN net**  
Add an optional **Description**  
Click **Extra Options > Display Advanced** and scroll down to **Gateway** and set it to the our WireGuard gateway, in our case, **Surf\_01**.
2. Click the **Save** button and make sure to also click on **Apply Changes**.
3. Disable the default **WAN** access firewall rules on the **Firewall > Rules > LAN** page:  
Click the **green check marks** beside the **Default allow** rules for IPv4.  
Click **Apply Changes** button.

The complete settings should look like so:

pfSense  
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

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 the interface from which packets must come to match this rule.

**Address Family** IPv4 ▾  
Select the Internet Protocol version this rule applies to.

**Protocol** Any ▾  
Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match LAN net ▾ Source Address ▾ / ▾ ▾

**Destination**

**Destination** ☐ Invert match any ▾ Destination Address ▾ / ▾ ▾

**Extra Options**

**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 doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**   
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.



**No pfSync** ☐ Prevent states created by this rule to be sync'd over pfsync.

**State type** Keep  
Keep works with all IP protocols

**No XMLRPC Sync** ☒ Prevent the rule on Master from automatically syncing to other CARP members  
This does NOT prevent the rule from being overwritten on Slave.

**VLAN Prio** none  
Choose 802.1p priority to match on.

**VLAN Prio Set** none  
Choose 802.1p priority to apply.

**Schedule** none  
Leave as 'none' to leave the rule enabled all the time.

**Gateway** Surf\_01 - 10.14.0.2  
Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.  
Gateway selection is not valid for "IPv4+IPv6" address family.

**In / Out pipe** none none  
Choose the Out queue/Virtual interface only if In is also selected. The Out selection is applied to traffic leaving the interface where the rule is created, the In selection is applied to traffic coming into the chosen interface.  
If creating a floating rule, if the direction is In then the same rules apply, if the direction is Out the selections are reversed, Out is for incoming and In is for outgoing.

**Ackqueue / Queue** none none  
Choose the Acknowledge Queue only if there is a selected Queue.

**Rule Information**

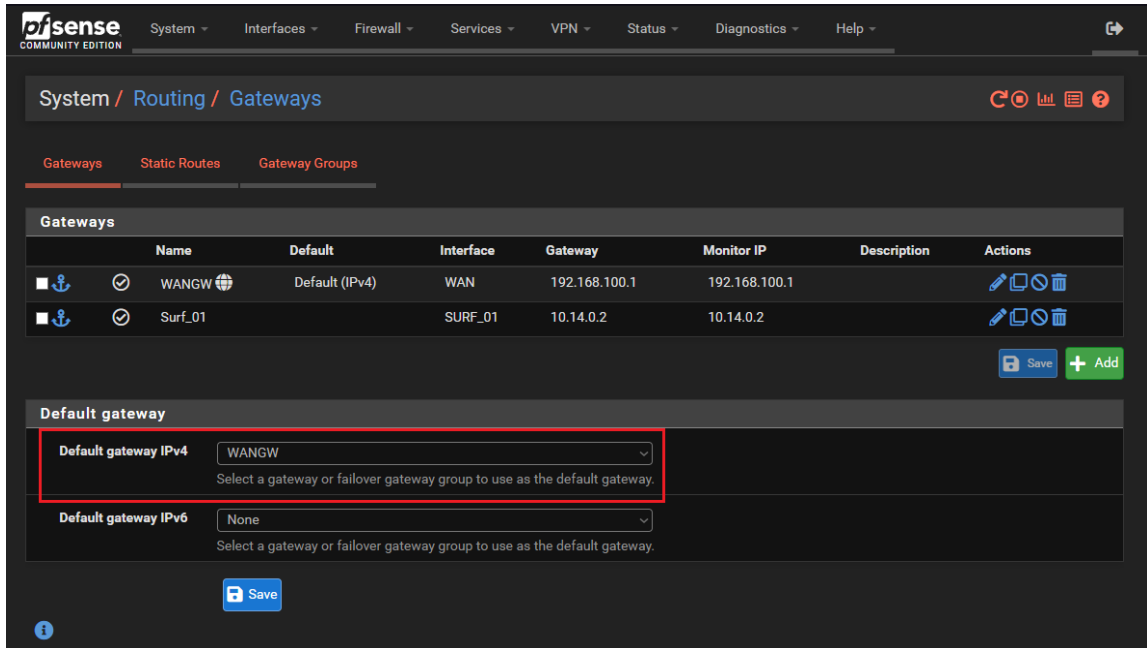
|             |   |
|-------------|---|
| Tracking ID | 1673118606  |
| Created     | 1/7/23 22:10:06 by admin@192.168.100.9 (Local Database) |
| Updated     | 1/7/23 22:10:06 by admin@192.168.100.9 (Local Database) |

**Save**

## Static routing configuration.

1. Navigate to **System > Routing > Static routes** tab.
2. Click the **Add** button and configure the routes as follows:  
**Destination network:** The IP address of the **WireGuard** server - **10.14.0.2**
3. **Gateway:** your router's **WAN** gateway.
4. **Description** (not necessary) - **WAN to VPN**, for example. In our case, we left it blank.
5. Navigate to **System > Routing > Gateways** tab and set **Default gateway IPv4** to the one we configured previously (you should be able to see it in the dropdown menu).
6. Click **Save** and **Apply changes**.

The finished configuration on our end ended up looking like so:



Now it is time to configure the **DNS** on your pfSense device.

1. Navigate to **System > General Setup > DNS** and set the **DNS Servers > Address** to Surfshark's DNS addresses (162.252.172.57 and 149.154.159.92), although you can also use Google DNS (8.8.8.8 and 8.8.4.4).
2. Make sure to also uncheck the **DNS Server Override** option and click **Save**. Set the **Gateway** to our WireGuard gateway, in our case - *Surf\_01*.

**pfSense** COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

System / General Setup

**System**

**Hostname** pfWireguard  
Name of the firewall host, without domain part

**Domain** home.arpa  
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternative TLDs such as 'local.lan' or 'mylocal' are safe.

**DNS Server Settings**

| DNS Servers | DNS Hostname | Gateway                    |        |
|-------------|--------------|----------------------------|--------|
| 8.8.8.8     |              | Surf_01 - opt1 - 10.14.0.2 | Delete |
| 8.8.4.4     |              | Surf_01 - opt1 - 10.14.0.2 | Delete |

**Address**  
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.

**Hostname**  
Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).

**Gateway**  
Optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.

**Add DNS Server** + Add DNS Server

**DNS Server Override** ☐ Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server  
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.

**DNS Resolution Behavior** Use local DNS (127.0.0.1), fall back to remote DNS Servers (Default)   
By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.

**Localization**

- Now, navigate to **Service > DHCP Server** and set the **DNS Servers > DNS Server 1** to the one we just chose above - in this case, that would be 8.8.8.8.

*Not tested:*

It should also work just fine by adding two DNS servers and entering both of the DNS addresses specified above, for example Surfshark's.

- Finally, click **Save** once again.

The last step would be to configure the **DNS Resolver**.

- Navigate to **Services > DNS Resolver** and have the **Enable DNSSEC** checked.
- Check **Enable Forwarding Mode** beside **DNS Query Forwarding**.
- Click **Save** and **Apply Changes** buttons afterwards.

|   |  |
|---|--|
| Network Interfaces                        | <div> <div> WAN<br/>LAN<br/>SURF_01<br/>WAN.ID6.Link.Local </div> </div> <p>Interface IPs used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected below are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.</p>   |
| Outgoing Network Interfaces               | <div> <div> All<br/>WAN<br/>LAN<br/>SURF_01<br/>WAN.ID6.Link.Local </div> </div> <p>Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.</p>  |
| Strict Outgoing Network Interface Binding | <input type="checkbox"/> Do not send recursive queries if none of the selected Outgoing Network Interfaces are available.<br>By default the DNS Resolver sends recursive DNS requests over any available interfaces if none of the selected Outgoing Network Interfaces are available. This option makes the DNS Resolver refuse recursive queries.  |
| System Domain Local Zone Type             | <div>Transparent</div> <p>The local-zone type used for the pfSense system domain (System   General Setup   Domain). Transparent is the default. Local-Zone type descriptions are available in the <a href="#">unbound.conf(5)</a> manual pages.</p>  |
| DNSSEC                                    | <input checked="" type="checkbox"/> Enable DNSSEC Support  |
| Python Module                             | <input type="checkbox"/> Enable Python Module<br>Enable the Python Module.   |
| DNS Query Forwarding                      | <input checked="" type="checkbox"/> Enable Forwarding Mode<br>If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under <a href="#">System &gt; General Setup</a> or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).   |
|   | <input type="checkbox"/> Use SSL/TLS for outgoing DNS Queries to Forwarding Servers<br>When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.  |
| DHCP Registration                         | <input type="checkbox"/> Register DHCP leases in the DNS Resolver<br>If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in <a href="#">System &gt; General Setup</a> should also be set to the proper value. |
| Static DHCP                               | <input type="checkbox"/> Register DHCP static mappings in the DNS Resolver<br>If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in <a href="#">System &gt; General Setup</a> should also be set to the proper value.   |

That is it - what is left, is to test out the connection!  
You can do so by going to <https://surfshark.com/check>