

# Setup WireGuard Site to Site VPN Tunnel on pfsense 2.7.2

This guide was inspired by [Marcus Rath](#)

## Introduction

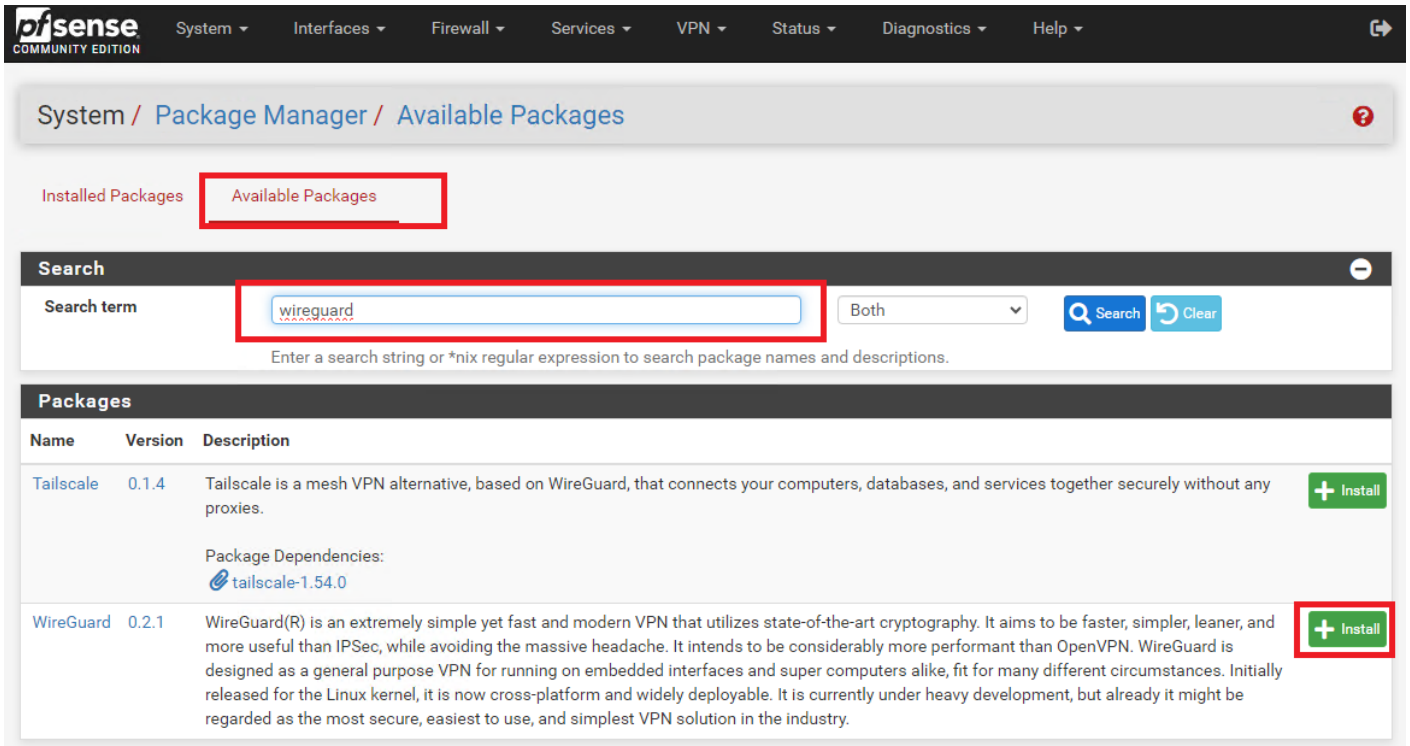
This guide will walk you through setting up a WireGuard site to site VPN tunnel on pfsense 2.7.2. For this guide we assume **Site A** with a **network subnet of 192.168.1.0/24**, **Site B with a network subnet of 192.168.24.0/24** and a **Tunnel Subnet of 10.10.12.0/30**. Obviously adjust these settings to your specific needs.

Ensure that the **Tunnel Subnet** you choose does NOT overlap with any other network subnets currently in use in your network environment.

## Install WireGuard Package on Both Sites

On **BOTH** site pfsense installations, install the **WireGuard package from System ---> Package Manager ---> Available Packages**. Enter **Wireguard** in the **Search term** field, click search and then click on the **Install** button next to WireGuard package (**Figure 1**).

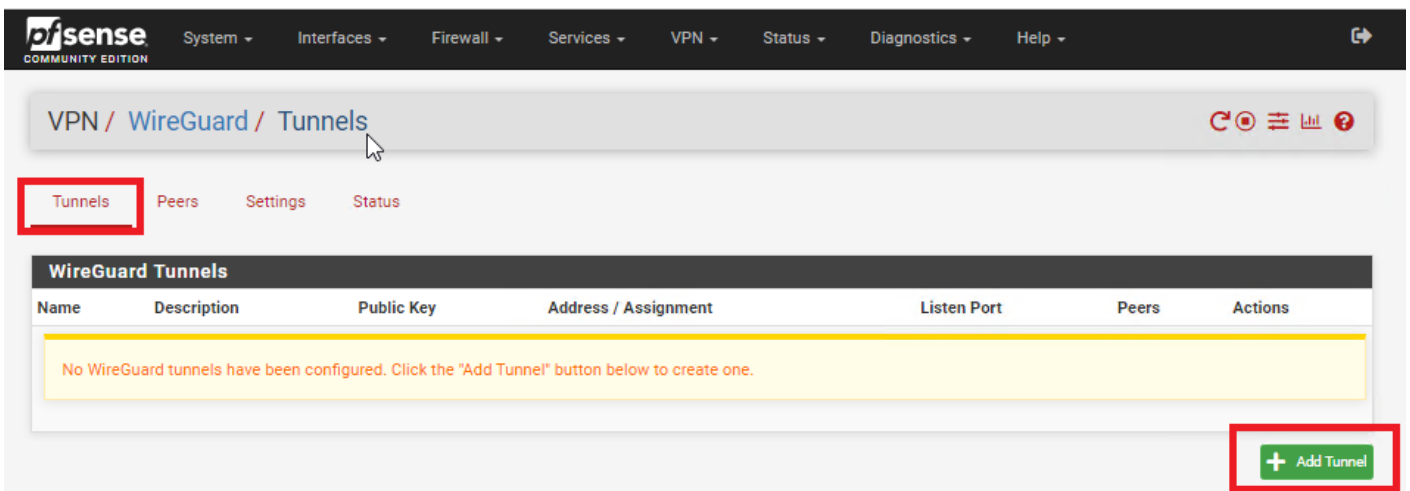
**Figure 1**



## Create Tunnel on Site A

On **Site A**, refresh the pfSense web GUI and navigate to **VPN ---> Wireguard**, click on the **Tunnels** tab and then click on **Add Tunnel** button (**Figure 2**).

**Figure 2**

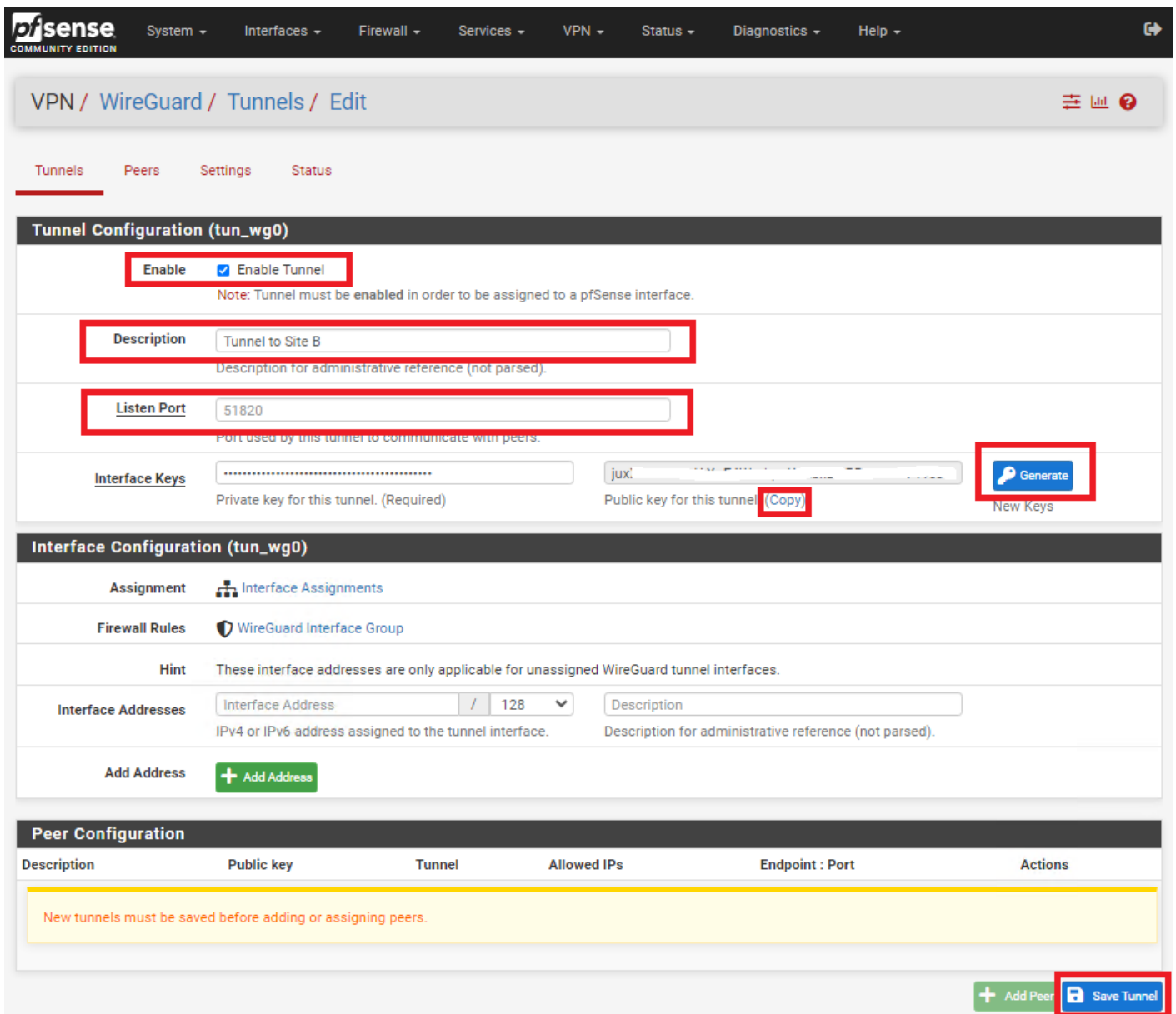


In the **Tunnel Configuration** fill/set in the following fields (**Figure 3**):

- **Enable:** Checked
- **Description:** Optionally, describe the purpose of this tunnel (Ex: Tunnel to Site B)
- **Listen Port:** Leave blank to use port UDP/51820 or enter a specific port number you wish to use

- **Interface Keys:** click the **Generate** button to create a new Private/Public key pair and copy the **Public Key** that's generated in order to enter it in the Public Key field on Site B.
- Click the **Save Tunnel** button

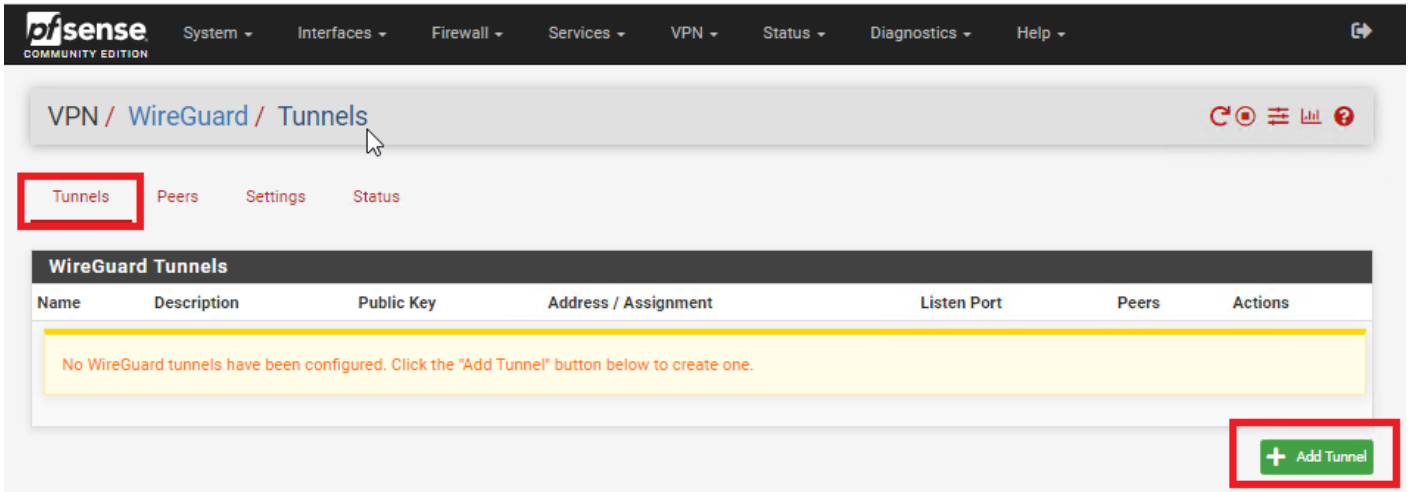
Figure 3



## Create Tunnel on Site B

On **Site B**, refresh the pfSense web GUI and navigate to **VPN ---> Wireguard**, click on the **Tunnels** tab and then click on **Add Tunnel** button (**Figure 4**).

Figure 4



In the **Tunnel Configuration** fill/set in the following fields (**Figure 5**):

- **Enable:** Checked
- **Description:** Optionally, describe the purpose of this tunnel(Ex: Tunnel to Site A)
- **Listen Port:** Leave blank to use port UDP/51820 or enter a specific port number you wish to use
- **Interface Keys:** click the **Generate** button to create a new Private/Public key pair and copy the **Public Key** that's generated in order to enter it in the Public Key field on Site B.
- Click the **Save Tunnel** button

**Figure 5**

## Enable WireGuard on Both Sites

On **BOTH** sites, navigate to **VPN ---> WireGuard**, click on the **Settings** tab and click on the **Enable WireGuard** checkbox, select **Only Unassigned Tunnels** on the **Interface Group Membership** drop-down and then click on the **Save** button (**Figure 6**).

**Figure 6**

VPN / WireGuard / Settings

The WireGuard service is not running.

Tunnels Peers **Settings** Status

### General Settings

**Enable**  Enable WireGuard  
Note: WireGuard cannot be disabled when one or more tunnels is assigned to a pfSense interface.

**Keep Configuration**  Enable  
Note: With 'Keep Configurations' enabled (default), all tunnel configurations and package settings will persist on install/de-install.

**Endpoint Hostname**   Track System Resolve Interval  
Interval (in seconds) for re-resolving endpoint host/domain names. Tracks the system 'Aliases Hostnames Resolve Interval' setting.  
Note: The default is 300 seconds (0 to disable). Note: See System > Advanced > Firewall & NAT

**Interface Group Membership**   
Configures which WireGuard tunnels are members of the WireGuard interface group.  
Note: Group firewall rules are evaluated before interface firewall rules. Default is 'All Tunnels.'

### User Interface Settings

**Hide Secrets**  Enable  
Note: With 'Hide Secrets' enabled, all secrets (private and pre-shared keys) are hidden in the user interface.

**Hide Peers**  Enable  
Note: With 'Hide Peers' enabled (default), all peers for all tunnels will initially be hidden on the status page.

**Save**

# Add Peer on Site A

On **Site A**, navigate to **VPN ---> WireGuard**, click on the **Peers** tab and then click on the **Add Peer** button (**Figure 7**).

**Figure 7**

VPN / WireGuard / Peers

Tunnels **Peers** Settings Status

### WireGuard Peers

Description	Public key	Tunnel	Allowed IPs	Endpoint : Port	Actions
No WireGuard peers have been configured. Click the "Add Peer" button below to create one.					

**+ Add Peer**

In the **Peer Configuration** fill/set in the following fields (**Figure 8**):

- **Enable:** Checked
- **Tunnel:** Select the Tunnel previously configured from the drop-down list
- **Description:** Optionally, describe the purpose of this Peer (Ex: Peer to Site B)
- **Dynamic Endpoint:** Unchecked
- **Endpoint:** Fill in the Internet IP or Hostname as well as the port number for **Site B**
- **Public Key:** Paste the previously copied **Public Key** from the **Tunnel** on **Site B**
- **Pre-shared Key:** Click the Generate button to generate a new pre-shared key and copy it in order to paste in the Peer configuration of **Site B**
- **Allowed IPs:** Enter an **UNUSED** Network address (Example: 10.10.12.0) with a CIDR of **30** (For a total of two IPs) in the first field, click the **Add Allowed IP** and then enter the Network Address and corresponding CIDR of the subnet for **Site B**
- Click the **Save Peer** button

**Figure 8**

The screenshot shows the 'Peer Configuration' page with the following fields highlighted by red boxes:

- Enable:** The 'Enable Peer' checkbox is checked.
- Tunnel:** A dropdown menu is set to 'tun\_wg0 (Tunnel to Site B)'. Below it is a link: 'WireGuard tunnel for this peer. (Create a New Tunnel)'.
- Description:** A text input field containing 'Peer to Site B'. Below it is a note: 'Peer description for administrative reference (not parsed)'.
- Dynamic Endpoint:** The 'Dynamic' checkbox is unchecked. Below it is a note: 'Note: Uncheck this option to assign an endpoint address and port for this peer.'
- Endpoint:** Two input fields: 'siteB.domain.tld' (Hostname, IPv4, or IPv6 address of this peer. Leave endpoint and port blank if unknown (dynamic endpoints).) and '51820' (Port used by this peer. Leave blank for default (51820)).
- Keep Alive:** An input field containing 'Keep Alive'. Below it is a note: 'Interval (in seconds) for Keep Alive packets sent to this peer. Default is empty (disabled)'.
- Public Key:** A text input field containing a long alphanumeric string. Below it is a note: 'WireGuard public key for this peer.'
- Pre-shared Key:** A text input field with a masked key. To its right is a 'Generate' button. Below the key is a '(Copy)' button and the text 'New Pre-shared Key'.

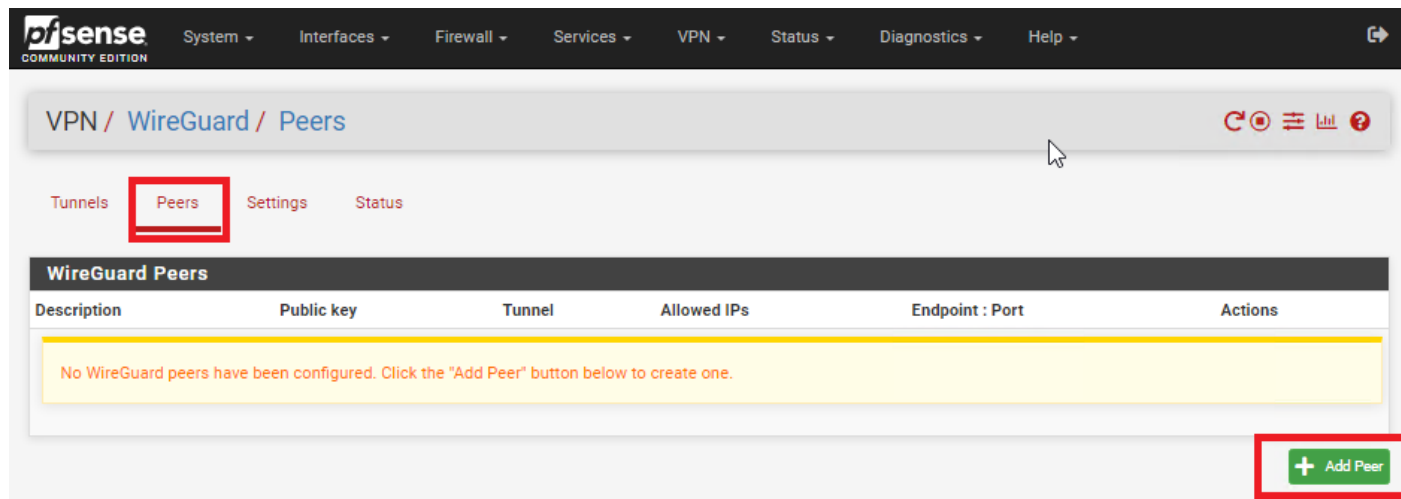
Below the Peer Configuration section is the 'Address Configuration' section:

- Hint:** Allowed IP entries here will be transformed into proper subnet start boundaries prior to validating and saving. These entries must be unique between multiple peers on the same tunnel. Otherwise, traffic to the conflicting networks will only be routed to the last peer in the list.
- Allowed IPs:** A table with two rows:
  - Row 1: '10.10.12.0' / '30' (Tunnel Subnet) with a 'Delete' button.
  - Row 2: '192.168.24.0' / '24' (Site B Subnet) with a 'Delete' button.
- Add Allowed IP:** A green button with a plus sign and the text 'Add Allowed IP'.
- Save Peer:** A blue button at the bottom right.

# Add Peer on Site B

On **Site B**, navigate to **VPN** ---> **WireGuard**, click on the **Peers** tab and then click on the **Add Peer** button (**Figure 9**).

**Figure 9**



In the **Peer Configuration** fill/set in the following fields (**Figure 10**):

- **Enable:** Checked
- **Tunnel:** Select the Tunnel previously configured from the drop-down list
- **Description:** Optionally, describe the purpose of this Peer (Ex: Peer to Site A)
- **Dynamic Endpoint:** Unchecked
- **Endpoint:** Fill in the Internet IP or Hostname as well as the port number for **Site A**
- **Public Key:** Paste the previously copied **Public Key** from the **Tunnel** on **Site A**
- **Pre-shared Key:** Paste the previously copied **Pre-Shared key** from the **Peer** on **Site A**
- **Allowed IPs:** Enter the **SAME Tunnel Subnet Network address and CIDR** you set on the **Peer** on **Site A**, click the **Add Allowed IP** and then enter the Network Address and corresponding CIDR of the subnet for **Site A**
- Click the **Save Peer** button

**Figure 10**

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 (Tunnel to Site B)  
 WireGuard tunnel for this peer. (Create a New Tunnel)

**Description** Peer to Site B  
 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** siteB.domain.tld 51820  
 Hostname, IPv4, or IPv6 address of this peer. Port used by this peer.  
 Leave endpoint and port blank if unknown (dynamic endpoints). Leave blank for default (51820).

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

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

**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. These entries must be unique between multiple peers on the same tunnel. Otherwise, traffic to the conflicting networks will only be routed to the last peer in the list.

<b>Allowed IPs</b>	10.10.12.0 / 30	Tunnel Subnet	<input type="button" value="Delete"/>
	192.168.24.0 / 24	Site B Subnet	<input type="button" value="Delete"/>

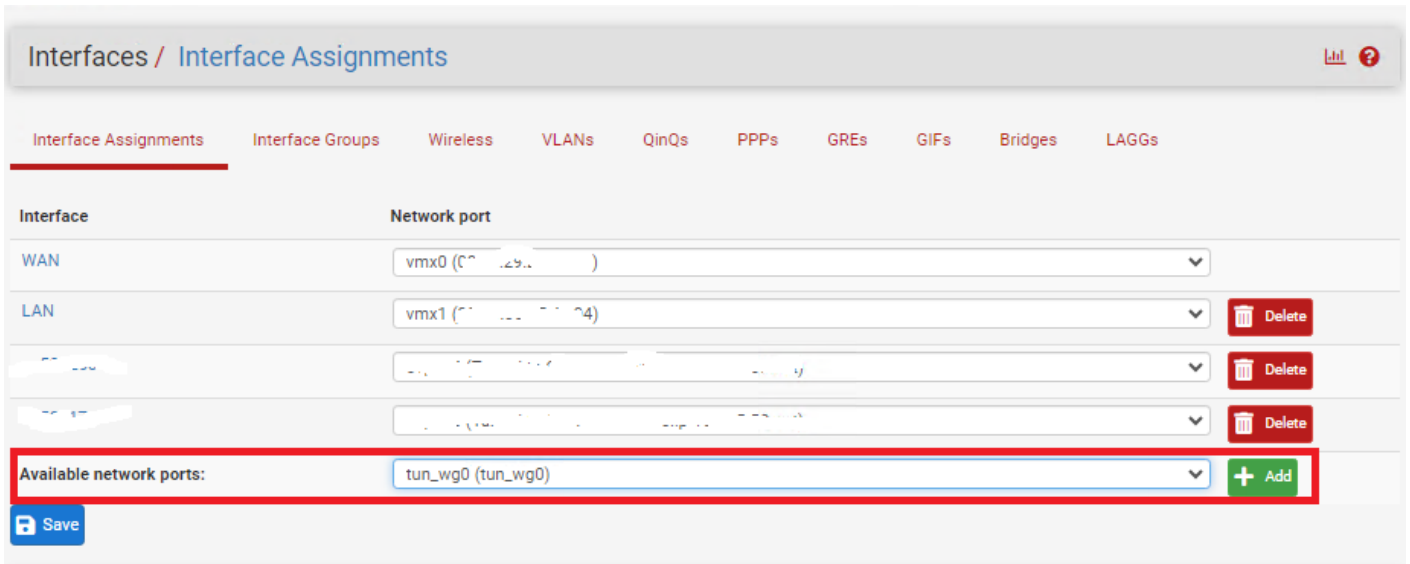
IPv4 or IPv6 subnet or host reachable via this peer. Description for administrative reference (not parsed).

**Add Allowed IP**

## Configure Interface for Site A

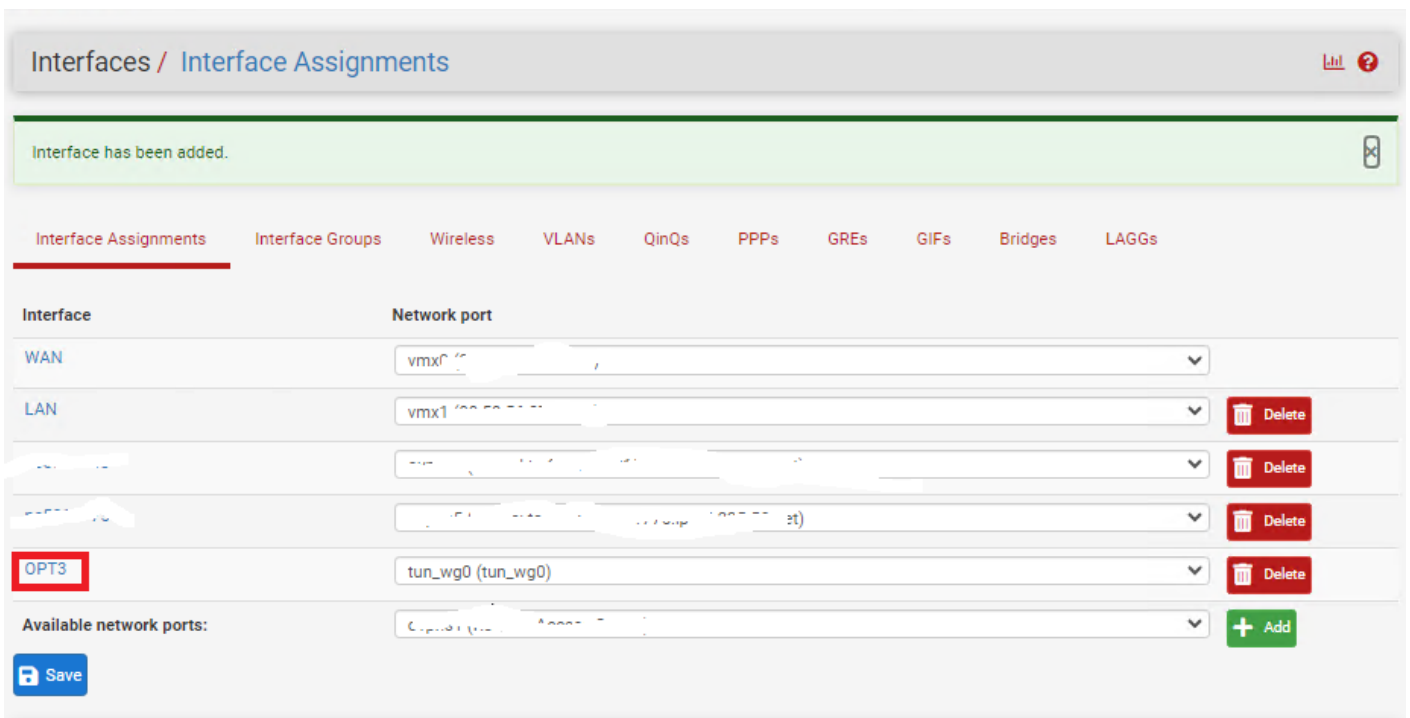
On **Site A**, navigate to **Interfaces** ---> **Assignments** and under **Available network ports** drop-down select the WireGuard tunnel you previously created and click the **Add** button (**Figure 11**).

**Figure 11**



Click on the new **OPT(X)** interface that was just created (**Figure 12**).

**Figure 12**



In the **General Configuration** page fill/set the following fields (**Figure 13**):

- **Enable:** Checked
- **Description:** Optionally, describe the purpose of this Interface (Ex: Tunnel to Site B)
- **IPv4 Configuration Type:** Static IPv4
- **IPv4 Address:** Enter an IP address for **Site A**. The IP address you enter here will be one of two possible IP addresses you can use from the /30 Tunnel Subnet you chose earlier. For this example, we used the Subnet Tunnel of **10.10.12.0/30** which gives us **10.10.12.1** and **10.10.12.2** as the only two usable IPs for this subnet. So, for this example we will use **10.10.12.1 for Site A**.
- Click the **Save** button and then click the **Apply Changes** button.

Figure 13

**General Configuration**

Enable  Enable interface

Description: Tunnel to Site B  
Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

MAC Address: xxxxxxxxxx  
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**

IPv4 Address: 10.10.12.1 / 30

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](#).

**Reserved Networks**

Block private networks and loopback addresses   
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

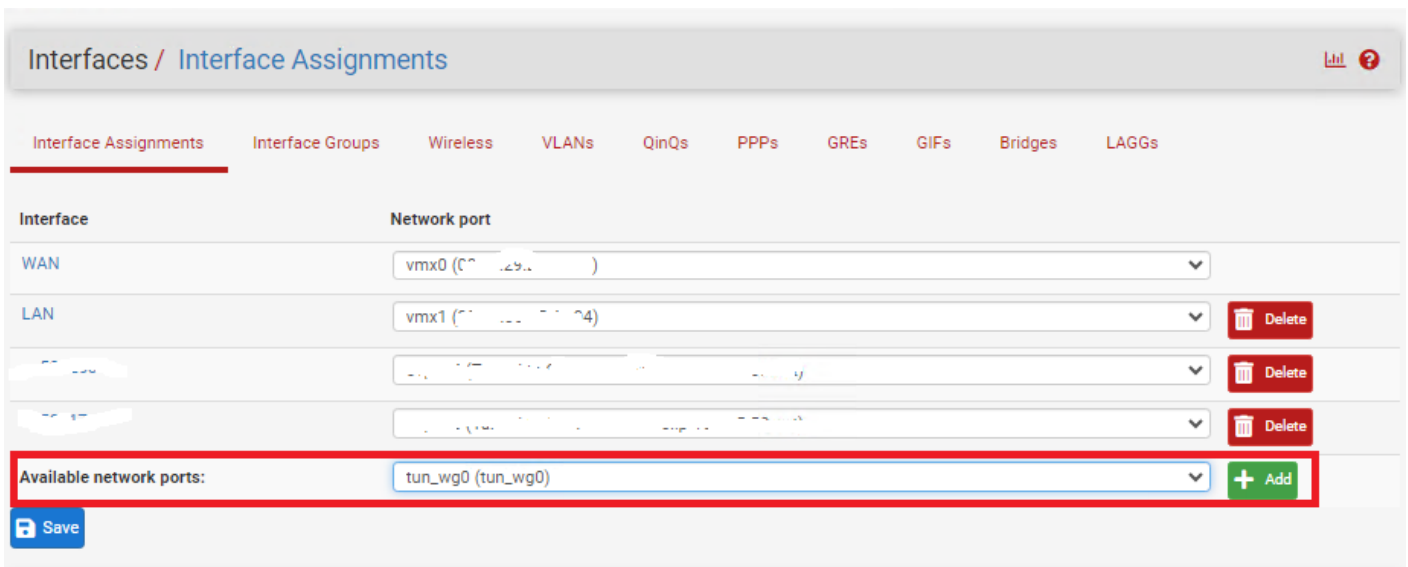
Block bogon networks   
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

[Save](#)

## Configure Interface for Site B

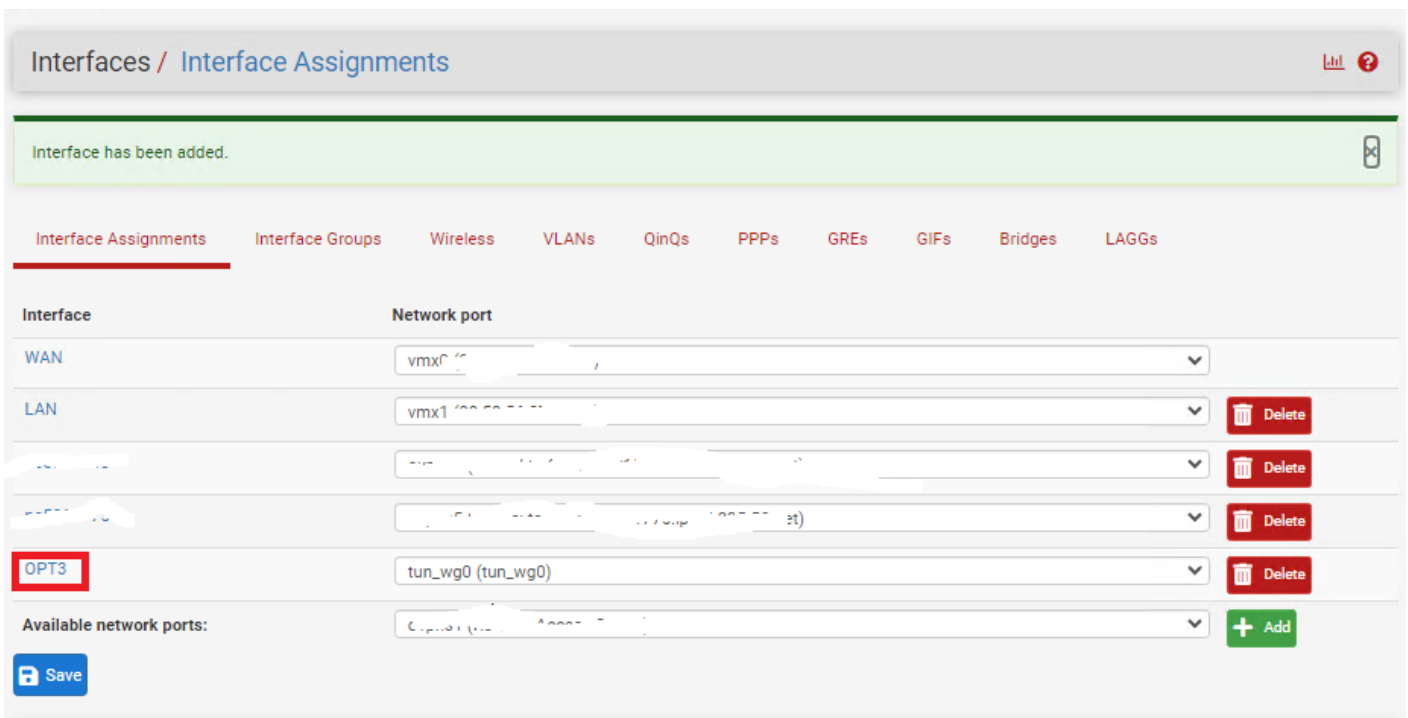
On **Site B**, navigate to **Interfaces** ---> **Assignments** and under **Available network ports** drop-down select the WireGuard tunnel you previously created and click the **Add** button (**Figure 14**).

Figure 14



Click on the new **OPT(X)** interface that was just created (**Figure 15**).

**Figure 15**



In the **General Configuration** page fill/set the following fields (**Figure 16**):

- **Enable:** Checked
- **Description:** Optionally, describe the purpose of this Interface (Ex: Tunnel to Site A)
- **IPv4 Configuration Type:** Static IPv4
- **IPv4 Address:** Enter an IP address for **Site B**. The IP address you enter here will be one of two possible IP addresses you can use from the /30 Tunnel Subnet you chose earlier. For this example, we used the Subnet Tunnel of **10.10.12.0/30** which gives us **10.10.12.1** and **10.10.12.2** as the only two usable IPs for this subnet. So, for this example we will use **10.10.12.2 for Site B**.
- Click the **Save** button and then click the **Apply Changes** button.

Figure 16

**General Configuration**

Enable  Enable interface

Description Tunnel to Site A

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xxxxxxxx

MTU

MSS

**Static IPv4 Configuration**

IPv4 Address 10.10.12.2 / 30

IPv4 Upstream gateway None + Add a new gateway

**Reserved Networks**

Block private networks and loopback addresses

Block bogon networks

Save

## Create Gateway and Route on Site A

On **Site A** navigate to **System** ---> **Routing** and under the **Gateways** tab click the **Add** button ( **Figure 17**).

Figure 17

System / Routing / Gateways

Gateways Static Routes Gateway Groups

### Gateways

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
<input checked="" type="checkbox"/> GW_WAN	Default (IPv4)	WAN			Interface wan Gateway	
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						

### Default gateway

Default gateway IPv4:   
 Select a gateway or failover gateway group to use as the default gateway.

Default gateway IPv6:   
 Select a gateway or failover gateway group to use as the default gateway.

In the **Edit Gateway** page fill/set the following fields (**Figure 18**):

- **Disabled:** Unchecked
- **Interface:** Select the interface for **Site A** you created earlier
- **Name:** Enter a name for this gateway (Ex: WG\_GW\_Site\_B)
- **Gateway:** Enter the **Tunnel Subnet IP** address for **Site B**. For this example we used **10.10.12.2** for **Site B**.
- **Description:** Optionally, enter a description (Ex: Wireguard Gateway to Site B)
- Click the **Save** button and then click the **Apply Changes** button.

**Figure 18**

**Edit Gateway**

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

**Interface** TUNNELTOSITEB  
Choose which interface this gateway applies to.

**Address Family** IPv4  
Choose the Internet Protocol this gateway uses.

**Name** WG\_GW\_Site\_B  
Gateway name

**Gateway** 10.10.12.2  
Gateway IP address

**Gateway Monitoring**  Disable Gateway Monitoring  
This will consider this gateway as always being up.

**Gateway Action**  Disable Gateway Monitoring Action  
No action will be taken on gateway events. The gateway is always considered up.

**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).

**Static route**  Do not add static route for gateway monitor IP address via the chosen interface  
By default the firewall adds static routes for gateway monitor IP addresses to ensure traffic to the monitor IP address leaves via the correct interface. Enabling this checkbox overrides that behavior.

**Force state**  Mark Gateway as Down  
This will force this gateway to be considered down.

**State Killing on Gateway Failure** Use global behavior (default)  
Controls the state killing behavior when this specific gateway goes down. Killing states for specific down gateways only affects states created by policy routing rules and reply-to. Has no effect if gateway monitoring or its action are disabled or if the gateway is forced down. May not have any effect on dynamic gateways during a link loss event.

**Description** Wireguard Gateway to Site B  
A description may be entered here for reference (not parsed).

Display Advanced

Save

Next, on **Site A** navigate to **System ---> Routing** and under the **Static Routes** tab click the **Add** button (**Figure 19**).

**Figure 19**



In the **Edit Route Entry** page, fill/set the following fields (**Figure 20**):

- **Destination network:** Enter the network subnet for **Site B (NOT the tunnel subnet)**. In this example, the network subnet we used for Site B was **192.168.24.0/24**.
- **Gateway:** Select the Gateway to **Site B** you created earlier
- **Description:** Optionally, enter a description (Ex: Route to Site B)
- Click the **Save** button and then click the **Apply Changes** button.

Figure 20

**Edit Route Entry**

**Destination network** 192.168.24.0 / 24

Destination network for this static route

**Gateway** WG\_GW\_Site\_B - 10.10.12.2

Choose which gateway this route applies to or add a new one first.

**Disabled**  Disable this static route  
Set this option to disable this static route without removing it from the list.

**Description** Route to Site B

A description may be entered here for administrative reference (not parsed).

**Save**

## Create Gateway and Route on Site B

On **Site B** navigate to **System** ---> **Routing** and under the **Gateways** tab click the **Add** button ( **Figure 21**).

Figure 21

System / Routing / Gateways

Gateways Static Routes Gateway Groups

**Gateways**

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
GW_WAN	Default (IPv4)	WAN			Interface wan Gateway	[Edit] [Copy] [Delete]
				192.168.24.2		[Edit] [Copy]
				192.168.24.2		[Edit] [Copy]
						[Edit] [Copy]

**Default gateway**

**Default gateway IPv4** GW\_WAN  
Select a gateway or failover gateway group to use as the default gateway.

**Default gateway IPv6** Automatic  
Select a gateway or failover gateway group to use as the default gateway.

**Save** **+ Add**

**Save**

In the **Edit Gateway** page fill/set the following fields (**Figure 22**):

- **Disabled:** Unchecked
- **Interface:** Select the interface for **Site A** you created earlier
- **Name:** Enter a name for this gateway (Ex: WG\_GW\_Site\_A)
- **Gateway:** Enter the **Tunnel Subnet IP** address for **Site A**. For this example we used **10.10.12.1** for **Site A**.
- **Description:** Optionally, enter a description (Ex: Wireguard Gateway to Site A)
- Click the **Save** button and then click the **Apply Changes** button.

**Figure 22**

The screenshot shows the 'Edit Gateway' configuration page. The following fields are highlighted with red boxes:

- Disabled:** A checkbox labeled 'Disable this gateway' is unchecked.
- Interface:** A dropdown menu is set to 'TUNNELTOSITEA'.
- Name:** A text input field contains 'WG\_GW\_Site\_A'.
- Gateway:** A text input field contains '10.10.12.1'.
- Description:** A text input field contains 'Wireguard Gateway to Site A'.
- Save:** A blue button with a floppy disk icon and the text 'Save' is highlighted.

Other visible fields include 'Address Family' (IPv4), 'Gateway Monitoring' (unchecked), 'Gateway Action' (unchecked), 'Monitor IP' (empty), 'Static route' (unchecked), 'Force state' (unchecked), and 'State Killing on Gateway Failure' (Use global behavior (default)).

Next, on **Site B** navigate to **System ---> Routing** and under the **Static Routes** tab click the **Add** button (**Figure 23**).

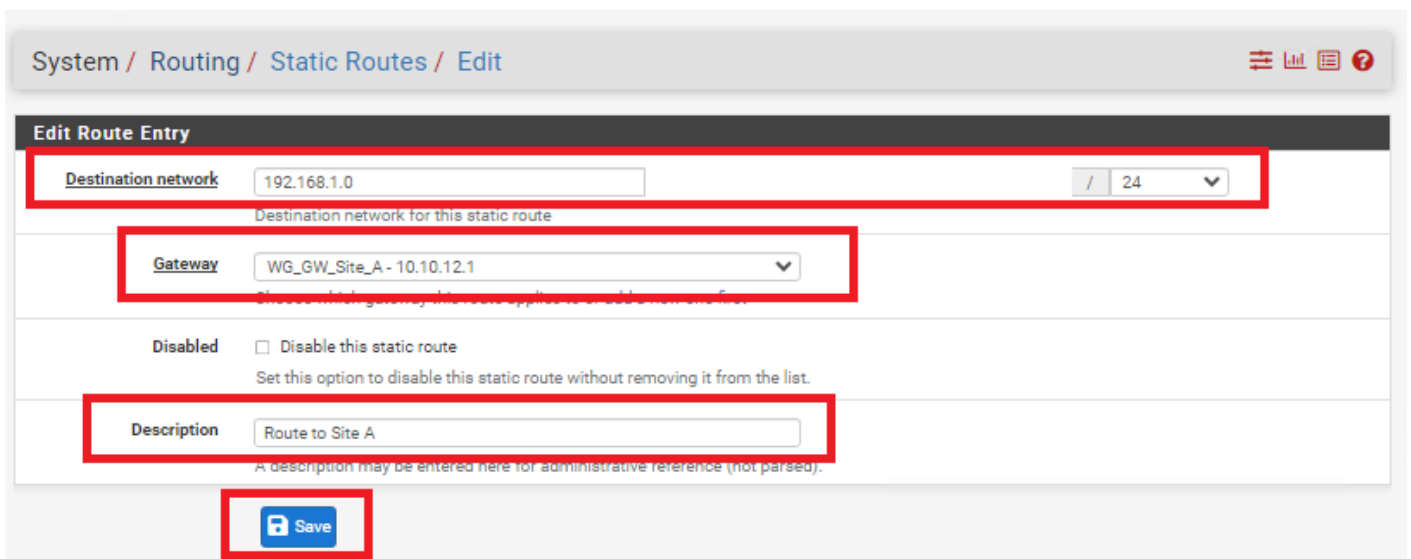
Figure 23



In the **Edit Route Entry** page, fill/set the following fields (**Figure 24**):

- **Destination network:** Enter the network subnet for **Site A (NOT the tunnel subnet)**. In this example, the network subnet we used for **Site A** was **192.168.1.0/24**.
- **Gateway:** Select the Gateway to **Site A** you created earlier
- **Description:** Optionally, enter a description (Ex: Route to Site A)
- Click the **Save** button and then click the **Apply Changes** button.

Figure 24



## Add Firewall Rules on BOTH Firewalls

On **BOTH** firewalls, navigate to **Firewall ---> Rules** and under the **WAN** tab, click the **Add** button. In the **Edit Firewall Rule** page, fill/set the following fields (**Figure 25**).

- **Action:** Pass
- **Interface:** WAN
- **Address Family:** IPv4
- **Protocol:** UDP
- **Source:** Any
- **Destination:** WAN address

- **Destination Port Range:** (other) 51820 to (other) 51820
- **Log:** Optionally, check to Log packets that are handled by this rule
- **Description:** Optionally, enter a description (Ex: Wireguard Site A and Site B)
- Click the **Save** button and then click the **Apply Changes** button.

Figure 25

**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** WAN

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** UDP

Choose which IP protocol this rule should match.

**Source**

**Source**  Invert match Any Source Address /

[Display Advanced](#)

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

**Destination**

**Destination**  Invert match WAN address Destination Address /

**Destination Port Range** (other) 51820 (other) 51820

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**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** Wireguard Site A and Site B

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.

**Advanced Options** [Display Advanced](#)

On **BOTH** firewalls, navigate to **Firewall ---> Rules** and under the **TUNNELTOSITE(X)** tab, click the **Add** button. In the **Edit Firewall Rule** page, fill/set the following fields (**Figure 25**).

- **Action:** Pass
- **Interface:** Ensure the interface you created earlier for each site is already selected
- **Address Family:** IPv4
- **Protocol:** Any (Start with **Any** and then you can tighten the rules further after you ensure tunnel is working properly)

- **Source:** Any (Start with **Any** and then you can tighten the rules further after you ensure tunnel is working properly)
- **Destination:** Any (Start with **Any** and then you can tighten the rules further after you ensure tunnel is working properly)
- **Destination Port Range:** Any (Start with **Any** and then you can tighten the rules further after you ensure tunnel is working properly)
- **Log:** Optionally, check to Log packets that are handled by this rule
- **Description:** Optionally, enter a description (Ex: Wireguard Traffic Site A and Site B)
- Click the **Save** button and then click the **Apply Changes** button.

Figure 25

The screenshot shows the 'Edit Firewall Rule' configuration page. Several fields are highlighted with red boxes:

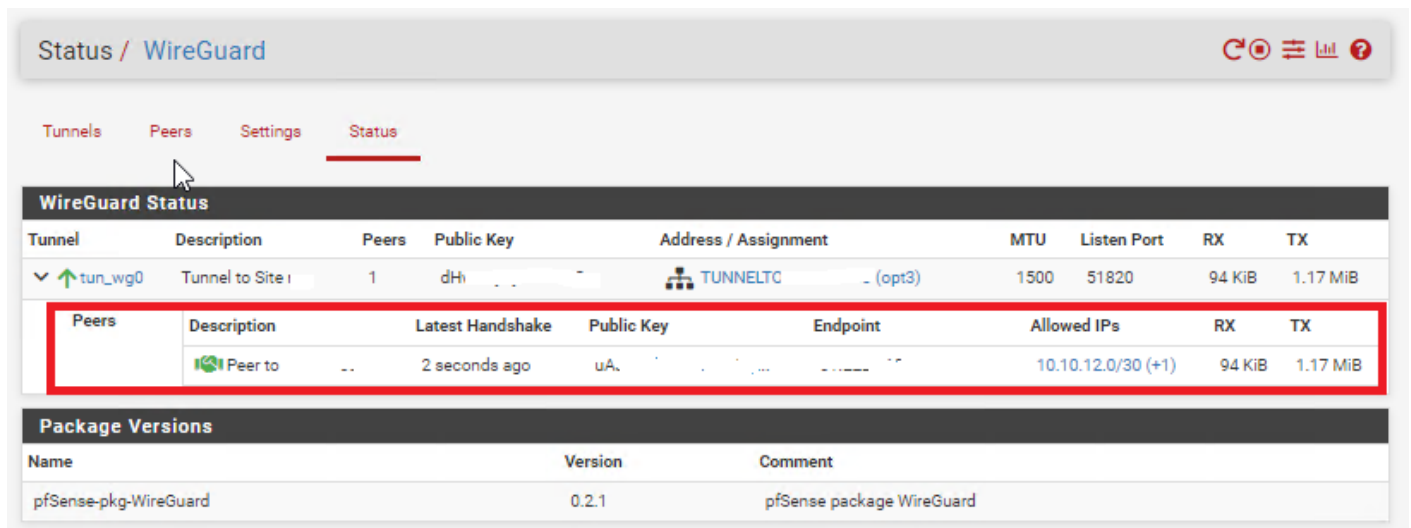
- Action:** Set to 'Pass'.
- Interface:** Set to 'WAN'.
- Address Family:** Set to 'IPv4'.
- Protocol:** Set to 'UDP'.
- Source:** 'Source' is set to 'Any'.
- Destination:** 'Destination' is set to 'WAN address'.
- Destination Port Range:** Both 'From' and 'To' are set to '51820'.
- Log:** The checkbox 'Log packets that are handled by this rule' is checked.
- Description:** Set to 'Wireguard Site A and Site B'.

Other visible elements include 'Disabled' (unchecked), 'Source Address' (empty), 'Destination Address' (empty), and 'Advanced Options' (displayed).

## Check the Wireguard Status

On **BOTH** firewalls navigate to **Status** ---> **Wireguard**, locate the WireGuard tunnel you created, expand it and ensure the Peers are connected on BOTH firewalls (**Figure 26**).

**Figure 26**



The screenshot shows the pfSense interface for WireGuard status. The breadcrumb is 'Status / WireGuard'. There are tabs for 'Tunnels', 'Peers', 'Settings', and 'Status'. The 'WireGuard Status' section contains a table with the following data:

Tunnel	Description	Peers	Public Key	Address / Assignment	MTU	Listen Port	RX	TX
▼ ↑ tun_wg0	Tunnel to Site 1	1	dH...	TUNNELTC (opt3)	1500	51820	94 KiB	1.17 MiB

Below the tunnel table, the 'Peers' section is expanded, showing a table with the following data:

Peers	Description	Latest Handshake	Public Key	Endpoint	Allowed IPs	RX	TX
🟢	Peer to ...	2 seconds ago	uA...	...	10.10.12.0/30 (+1)	94 KiB	1.17 MiB

The 'Package Versions' section shows:

Name	Version	Comment
pfSense-pkg-WireGuard	0.2.1	pfSense package WireGuard

Additionally, ensure you can ping and access resources on each remote network from the corresponding site.

Revision #16

Created 2024-01-18 18:26:24 UTC by Dino Edwards

Updated 2024-01-20 14:50:10 UTC by Dino Edwards