

# [pfSense] Wireguard

## Introduction

Wireguard supporte depuis récemment l'installation d'un VPN wiregard qui est le plus rapide et performant du marché des VPNs open source.



## Installation

Tout d'abord, installez le paquet **WireGuard** depuis le menu **System > Package Manager > Available Packages** :

The screenshot shows the pfSense Package Manager interface. The breadcrumb navigation is "System / Package Manager / Available Packages". There are two tabs: "Installed Packages" and "Available Packages", with the latter being selected. A search bar contains the text "WireGuard". Below the search bar, a table lists the search results. The first result is "WireGuard" with version "0.2.1". The description for WireGuard is: "WireGuard(R) is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPSec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN. WireGuard is designed as a general purpose VPN for running on embedded interfaces and super computers alike, fit for many different circumstances. Initially released for the Linux kernel, it is now cross-platform and widely deployable. It is currently under heavy development, but already it might be regarded as the most secure, easiest to use, and simplest VPN solution in the industry." To the right of the description is a green button with a plus sign and the text "Install".

Name	Version	Description	
WireGuard	0.2.1	WireGuard(R) is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPSec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN. WireGuard is designed as a general purpose VPN for running on embedded interfaces and super computers alike, fit for many different circumstances. Initially released for the Linux kernel, it is now cross-platform and widely deployable. It is currently under heavy development, but already it might be regarded as the most secure, easiest to use, and simplest VPN solution in the industry.	<a href="#">+ Install</a>

Cliquez sur **Install** puis **Confirm** et attendez que le message suivant apparaisse :

System / Package Manager / Package Installer

pfSense-pkg-WireGuard installation successfully completed.

Installed Packages Available Packages **Package Installer**

### Package Installation

```
Custom commands...
Executing custom_php_install_command()...done.
  Installing WireGuard early shell commands...done.
  Creating WireGuard interface group...done.
  Creating WireGuard Unbound access list...done.
  Installing WireGuard service...done.
  Applying WireGuard default settings as necessary...done.
done.
Executing custom_php_resync_config_command()...done.
Menu items... done.
Services... done.
Writing configuration... done.
>>> Cleaning up cache... done.
Success
```

Ensuite, rendez vous dans l'onglet **VPN > Wireguard** et cliquez sur **Add tunnel** :

VPN / WireGuard / Tunnels

Tunnels Peers Settings Status

### WireGuard Tunnels

Name	Description	Public Key	Address / Assignment	Listen Port	Peers	Actions
No WireGuard tunnels have been configured. Click the "Add Tunnel" button below to create one.						

+ Add Tunnel

Pour la configuration du tunnel, saisissez en **description** le nom de votre VPN puis générez une paire de clés en cliquant sur **Generate** :

### Tunnel Configuration (tun\_wg0)

**Enable**  Enable Tunnel  
**Note:** Tunnel must be **enabled** in order to be 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**   **Generate**  
Private key for this tunnel. (Required) Public key for this tunnel. (Copy) New Keys

Dans la configuration de l'interface, saisissez l'adresse IP privée du routeur associée à l'interface du tunnel :

**Interface Configuration (tun\_wg0)**

**Assignment** [Interface Assignments](#)

**Firewall Rules** [WireGuard Interface Group](#)

**Hint** These interface addresses are only applicable for unassigned WireGuard tunnel interfaces.

**Interface Addresses**  /    
IPv4 or IPv6 address assigned to the tunnel interface. Description for administrative reference (not parsed).

**Add Address** [+ Add Address](#)

Cliquez sur **Save** et rendez vous dans l'onglet **Peer** puis cliquez sur **Add Peer** :

VPN / [WireGuard](#) / [Peers](#)

The WireGuard service is not running.

[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](#)

Sélectionnez votre **Tunnel** dans le menu déroulant et mettez le nom de votre client en **Description** :

**Peer Configuration**

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

**Tunnel**   
WireGuard tunnel for this peer. (Create a New Tunnel)

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

Depuis votre client Wireguard, générez une paire de clés publique/privée :

```
[~/tmp]$ wg genkey | tee wg-private.key
EJUzxJoaNo3SfxjF0iyrxcT3kRcR0aPBzoKBG6NKEm4=
```

```
[~/tmp]$ cat wg-private.key | wg pubkey | tee wg-public.key
QNQJsUuG9SfsMCR4cYj90/fr5uSL+qM1kgjLah+MZmc=
```

```
wg genkey | tee wg-private.key
```

```
cat wg-private.key | wg pubkey | tee wg-public.key
```

Et renseignez la clé publique dans la configuration du peer sur pfsense :

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

Et n'oubliez pas de décocher **Dynamic Endpoint** :

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

Saisissez ensuite l'adresse IP de l'**Endpoint** (IP publique de votre routeur qui sera atteinte pour se connecter au VPN) :

**Endpoint**   
Hostname, IPv4, or IPv6 address of this peer.  
Leave endpoint and port blank if unknown (dynamic endpoints).

Dans la configuration d'adressage, vous pouvez choisir les réseaux accessibles via le VPN.

Vous devez saisir l'IP du peer ainsi que les sous-réseaux de destination que vous souhaitez autoriser :

**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>	<input type="text" value="192.168.5.0"/> / <input type="text" value="24"/> <input type="button" value="v"/>	<input type="text" value="Description"/>	<input type="button" value="Delete"/>
	<input type="text" value="10.1.0.2"/> / <input type="text" value="32"/> <input type="button" value="v"/>	<input type="text" value="Description"/>	<input type="button" value="Delete"/>

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

**Add Allowed IP**

Cliquez sur **Save** puis rendez vous dans l'onglet **Settings** pour activer le service Wireguard et cliquez sur **Save** :

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  
Resolve Interval**

Interval (in seconds) for re-resolving endpoint host/domain names.  
**Note:** The default is 300 seconds (0 to disable).

Track System Resolve Interval

Tracks the system 'Aliases Hostnames Resolve Interval' setting.  
**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

Cliquez sur **Apply Changes** :

The WireGuard configuration has been changed.  
The changes must be applied for them to take effect.  
**Notice:** This action may momentarily suspend active WireGuard peer connections on any changed tunnels.

 Apply Changes

Après, allez sur **Interfaces > Assignements**, sélectionnez l'interface du tunnel et cliquez sur **Add** :

Interfaces / Interface Assignments [List] [?] [?]

Interface Assignments   Interface Groups   Wireless   VLANs   QinQs   PPPs   GREs   GIFs   Bridges   LAGGs

Interface	Network port	
LAN100	vtnet0 (a2:7f:98:ef:db:f6)	
NAS400	vtnet1 (e2:9e:7a:96:27:21)	Delete
CONT200	vtnet2 (c6:29:f3:fb:ab:10)	Delete
ADMIN300	vtnet3 (be:bb:f0:65:99:e0)	Delete
LAB500	vtnet4 (1a:0c:7d:5b:cd:e6)	Delete
DMZ600	vtnet5 (0e:11:79:fa:0f:7f)	Delete
Available network ports:	tun_wg0 (tun_wg0)	+ Add

[Save](#)

Interfaces that are configured as members of a lagg(4) interface will not be shown.  
Wireless interfaces must be created on the Wireless tab before they can be assigned.

Cliquez sur le nom de la nouvelle interface créée pour accéder à sa configuration puis activez l'interface et modifiez son nom :

Interfaces / OPT5 (tun\_wg0) [List] [?] [?]

**General Configuration**

**Enable**  Enable interface

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

En **IPv4 Configuration Type** sélectionnez **Static IPv4** puis dans Static IPv4 Configuration renseignez l'adresse du routeur sur le réseau VPN (définie précédemment) :

**IPv4 Configuration Type**

**Static IPv4 Configuration**

**IPv4 Address**  / 32

**IPv4 Upstream gateway**  [+ 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](#).

Cliquez sur **Add a new gateway** puis renseignez les informations et cliquez sur **Add** :

## New IPv4 Gateway ×

Default  Default gateway

Gateway name

Gateway IPv4

Description

Cliquez ensuite sur **Save** et **Apply Changes**.

On doit ensuite configurer le pare-feu pour autoriser les connexions en allant dans le menu **Firewall > Rules > WG** puis **Add** :

The screenshot shows the Firewall configuration interface. The breadcrumb path is "Firewall / Rules / WG". A tabbed interface at the top shows various interfaces: Floating, WireGuard, LAN100, NAS400, CONT200, ADMIN300, LAB500, DMZ600, **WG** (selected), and OpenVPN. Below this is a table header for "Rules (Drag to Change Order)" with columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. A yellow warning box states: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule." At the bottom right, there is a row of action buttons: "Add" (up arrow), "Add" (down arrow), "Delete" (trash), "Toggle" (power), "Copy", "Save", and "Separator" (plus).

Faites une règle pour autoriser tout le trafic ou seulement ce que vous souhaitez si vous souhaitez affiner vos règles et cliquez sur **Save** et **Apply Changes** :

## Edit Firewall Rule

**Action**

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**

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

**Address Family**

Select the Internet Protocol version this rule applies to.

**Protocol**

Choose which IP protocol this rule should match.

## Source

**Source**  Invert match   /

## Destination

**Destination**  Invert match   /

## 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.

Vous devez aussi créer une règle sur votre **WAN** pour autoriser le flux **UDP/51820** vers votre pare-feu.

La dernière étape consiste à créer le fichier de configuration du client VPN :

```
[Interface]
```

```
PrivateKey = <PEER_PRIV_KEY>
```

```
Address = 10.1.0.2/24
```

```
[Peer]
```

```
PublicKey = <SRV_PUB_KEY>
```

```
AllowedIPs = 10.1.0.0/24, 192.168.5.0/24
```

```
Endpoint = <SRV_PUBLIC_IP>:51820
```

Revision #6

Created 28 May 2024 07:25:42 by Elieroc

Updated 28 May 2024 09:05:58 by Elieroc