

[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** :

System / Package Manager / Available Packages

Installed Packages

Available Packages

Search

Search term

WireGuard

Name

Search

Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

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.	+ Install

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

neopipe

Description for administrative reference (not parsed).

Listen Port

51820

Port used by this tunnel to communicate with peers.

Interface Keys

.....

Private key for this tunnel. (Required)

pUgAwL3urq1JB+TKpwDNsXWmS7q4wzW8UFQqV5EjI

Public key for this tunnel. (Copy)

Generate

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

10.1.0.1 / 24

Description

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

tun_wg0 (neopipe)

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

Description

first-client

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.

Allowed IPs	<input type="text" value="192.168.5.0"/> / <input type="text" value="24"/>	<input type="text" value="Description"/>	 Delete
	<input type="text" value="10.1.0.2"/> / <input type="text" value="32"/>	<input type="text" value="Description"/>	 Delete

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

Add Allowed IP

 **Save Peer**

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

☐ Track System Resolve Interval

Resolve Interval

Interval (in seconds) for re-resolving endpoint host/domain names.

Note: The default is 300 seconds (0 to disable).

Tracks the system 'Aliases Hostnames Resolve Interval' setting.

Note: See System > Advanced > [Firewall & NAT](#)

Interface Group

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.'

Membership

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 🔍 ?

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) 🔍 ?

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 /

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** :

Firewall / Rules / WG 📊 📋 ?

Floating WireGuard LAN100 NAS400 CONT200 ADMIN300 LAB500 DMZ600 WG OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
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.										

ℹ

Faite 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** :

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

WG

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

Any

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

PASS

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
```