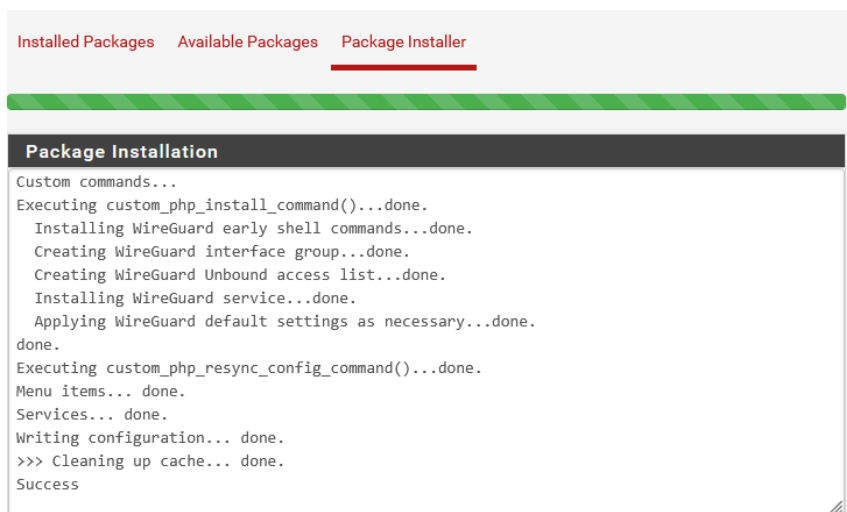


1. Installer le package WireGuard

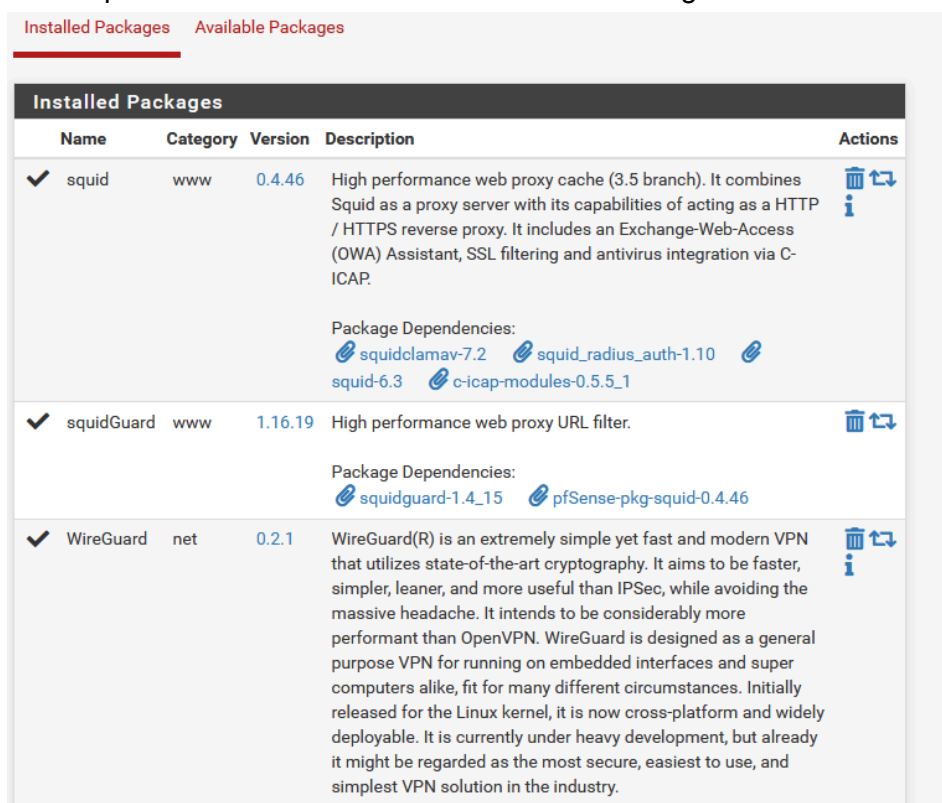
- Connecte-toi à pfSense.
- Va dans : **System > Package Manager > Available Packages**
- Cherche **WireGuard**
- Clique sur **Install** puis confirme.











```
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
```

- Vérifie qu'il se soit bien installé dans Installed Package



Installed Packages				
Name	Category	Version	Description	Actions
✓ squid	www	0.4.46	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package Dependencies: squidclamav-7.2 squid_radius_auth-1.10 squid-6.3 c-icap-modules-0.5.5_1	  
✓ squidGuard	www	1.16.19	High performance web proxy URL filter. Package Dependencies: squidguard-1.4.15 pfSense-pkg-squid-0.4.46	 
✓ WireGuard	net	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.	  

2. Créer l'interface WireGuard

- Va dans : **VPN > WireGuard**
- Clique sur **+ Add Tunnel**

Remplis :

Champ	Exemple
Name	WG_Admin
Listen Port	51820 (par défaut)
Interface Keys	Clique sur Generate (clé publique/privée auto-générées)
Tunnel Address	10.10.10.1/24 (adresse IP interne du tunnel VPN) ip différentes des deux interfaces déjà utilisé

Sauvegarde.

3. Ajouter un client (peer)

- Sous le tunnel créé, clique sur **+ Add Peer**

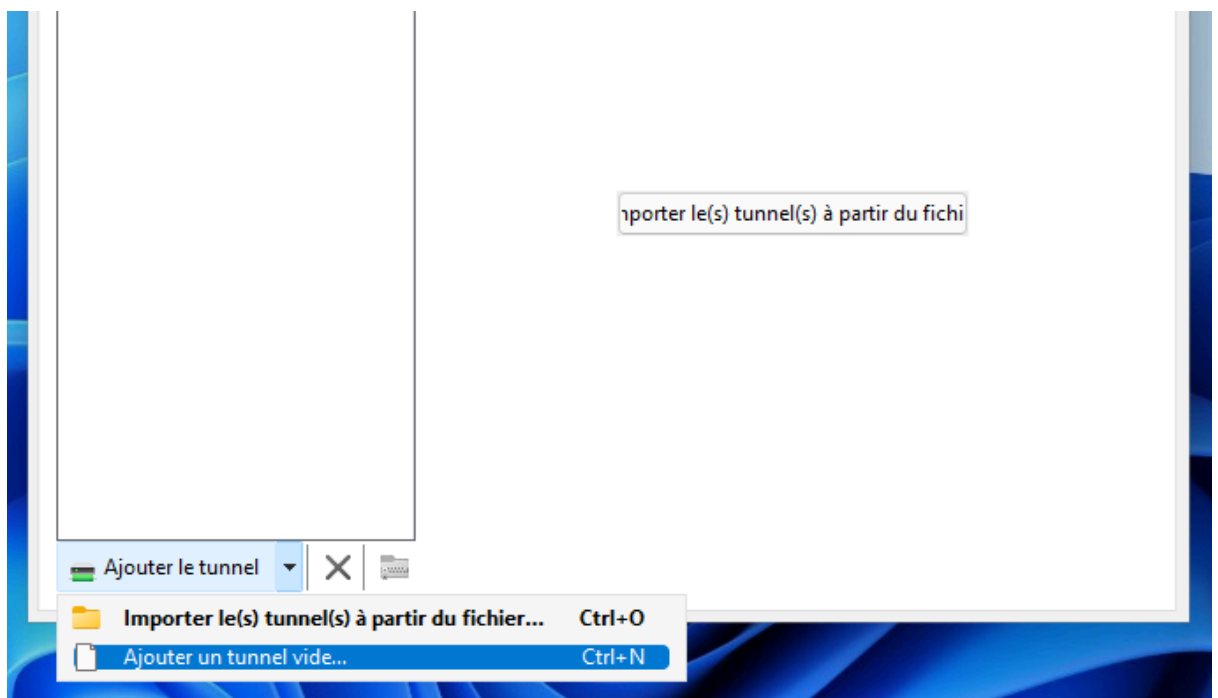
Remplis :

Champ	Exemple
Name	AdminClient
Public Key	(clé publique générée côté client)
Allowed IPs	10.10.10.2/32
Endpoint	(laisser vide si client se connecte depuis internet)

4. Configurer le client WireGuard

Sur ta machine admin (PC), installe WireGuard :

- WireGuard pour Windows
- Ou Linux/macOS depuis leur gestionnaire de paquets
- Clique sur la petite flèche à cotér de ajouter le tunnel puis ensuite ajouter un tunnel vide



[Interface]

PrivateKey = (laisse celle générée automatiquement)

Address = 10.10.10.2/32

DNS = 192.168.100.100

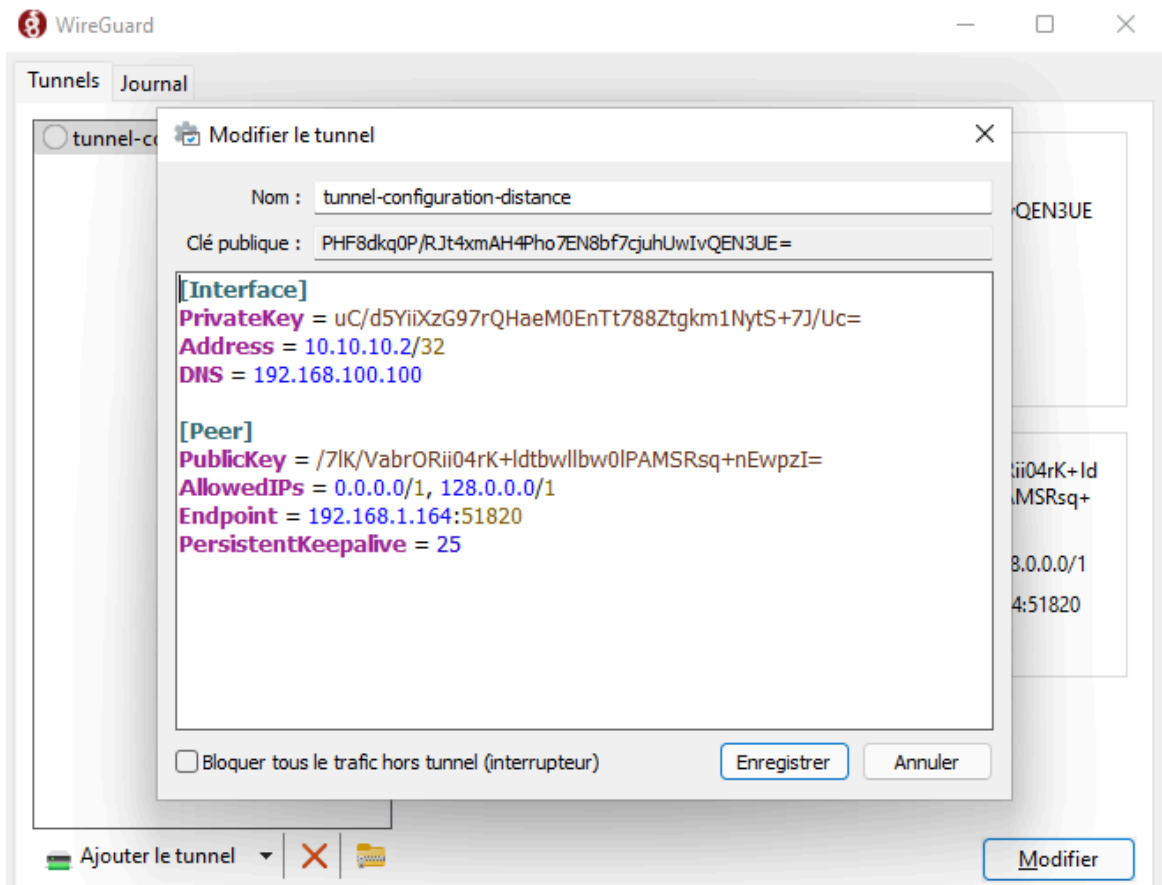
[Peer]

PublicKey = (clé publique de ton serveur pfSense tu la trouves dans le tunnel créé plus tôt)

Endpoint = IP_PUBLIQUE_PFSense:51820 (L'adresse IP en WAN)

AllowedIPs = IP de tes interfaces du serveur (WAN & LAN) ip du client et ip du serveur WireGuard et Client WireGuard

PersistentKeepalive = 25



ATTENTION: NE JAMAIS PARTAGEZ LES CLEF PRIVÉE

1. Autoriser le port WireGuard côté WAN


Menu : Firewall > Rules > WAN

Clique sur **Add** (↑) en haut

- **Action** : Pass
- **Interface** : WAN
- **Protocol** : UDP
- **Source** : any
- **Destination** : WAN address
- **Destination Port Range** : 51820 (ou celui que tu utilises)
- **Description** : Autoriser WireGuard

✓ Clique **Save** puis **Apply Changes**

Le règle doit ressembler à celle ci-dessous

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 UDP	*	*	WAN address	51820	*	none	Autoriser Wireguard	
--------------------------	-------------------------------------	-------	-------------	---	---	----------------	-------	---	------	------------------------	---

- Va dans **Firewall > Rules > WireGuard**
(ou `tun_wg0` si c'est sous ce nom)
- Clique sur **"Add"** (bouton flèche ↑ en haut)
- Configure la règle comme ceci :

Champ	Valeur
Action	Pass
Interface	WireGuard (ou <code>tun_wg0</code>)
Protocol	Any
Source	<code>10.10.10.0/24</code>
Destination	<code>any</code> (ou <code>192.168.100.0/24</code> pour limiter au LAN)
Description	Autoriser trafic VPN vers LAN/Internet

Clique **Save**, puis **Apply Changes**

Le règle doit ressembler à celle ci-dessous

Floating WireGuard WAN LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	10.10.10.0/24	*	*	*	*	none	autoriser trafic VPN vers LAN/ Internet	

Vérifiez ensuite dans Vpn / Wireguard / Settings soit bien coché

VPN / WireGuard / Settings

The changes have been applied successfully.

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.

Ensuite Menu : Interfaces / interface Assignments

Interface	Network port
WAN	em0 (08:00:27:e7:53:f3)
LAN	em1 (08:00:27:b7:bf:ea) Delete
Available network ports:	tun_wg0 (tun_wg0) Add

Save

Cliquez sur Add





Ensuite allez dans Firewall / Rules / WireGuard

- Cliquez sur **Add** (en haut)
- Remplis :

Champ	Valeur
Action	Pass
Interface	WireGuard
Protocol	Any
Source	Any
Destination	LAN net ou Any
Description	Allow WireGuard Traffic

- Cliquez sur **Save**, puis **Apply Changes**

Le résultat doit être similaire à celui ci

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	*	*	*	*	none		Allow Wireguard traffic	   

8. Tester la connexion

- Lance WireGuard sur ton client.
- Active le tunnel.
- Ping les bornes du réseau local.(Toute tes interfaces) si tout fonctionne c'est que la configuration est bonne

9. Sécuriser

- Garde ta clé privée confidentielle.
- Ajoute un utilisateur pfSense avec mot de passe fort.

Menu : System / User manager

Cliquez sur Add

User Properties	
Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	<input type="text" value="remipourtierrechargeplus"/>
Password	<input type="password" value="....."/> <input type="password" value="....."/>
Full name	<input type="text" value="Administrateur recharge+"/> <small>User's full name, for administrative information only</small>
Expiration date	<input type="text" value="03/05/2036"/> <small>Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY</small>
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	<input type="text" value="Not member of"/> <input type="text" value="admins"/> <small>Member of</small>
<input type="button" value="» Move to 'Member of' list"/> <input type="button" value="« Move to 'Not member of' list"/>	
<small>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</small>	

Certificate Click to create a user certificate

Create Certificate for User

Descriptive name

Certificate authority

Key type

The length to use when generating a new RSA key, in bits.

The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm

The digest method used when the certificate is signed.

The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime

Keys

Authorized SSH Keys


Enter authorized SSH keys for this user

IPsec Pre-Shared Key

Shell Behavior

Keep Command History Keep shell command history between login sessions

If this user has shell access, this option preserves the last 1000 unique commands entered at a shell prompt between login sessions. The user can access history using the up and down arrows at an SSH or console shell prompt and search the history by typing a partial command and then using the up or down arrows.

 Save

SAVE

La configuration principale de Wireguard est fini