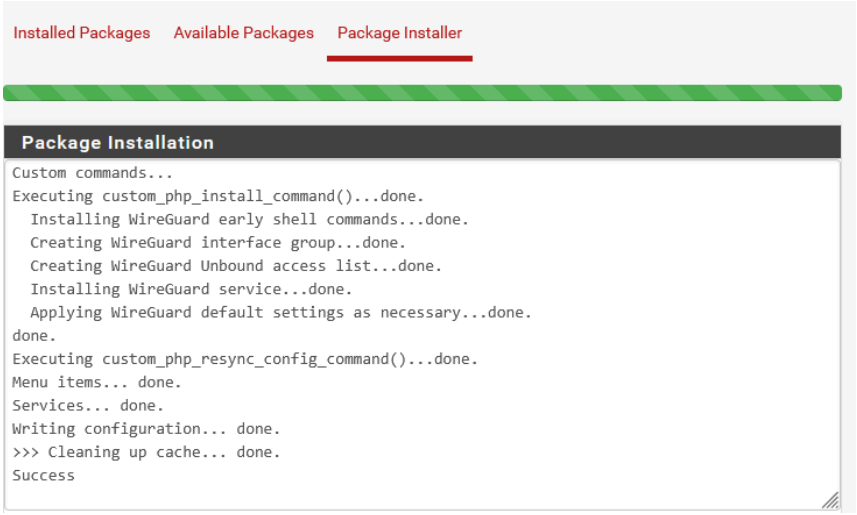
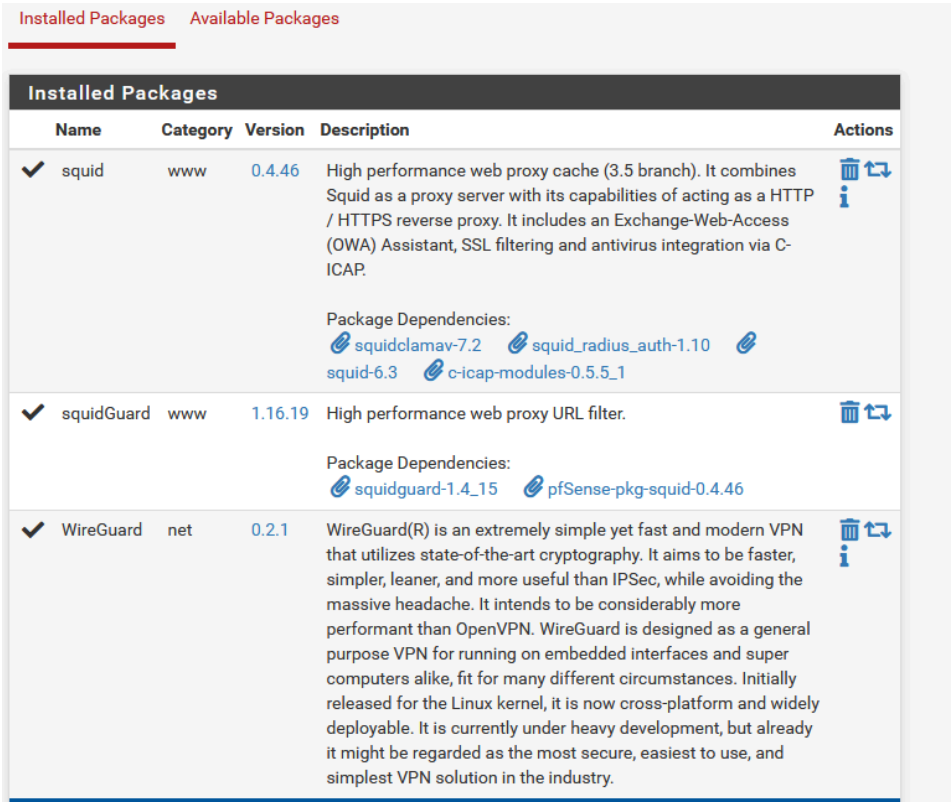
1. Installer le package WireGuard

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



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



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 déja 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)

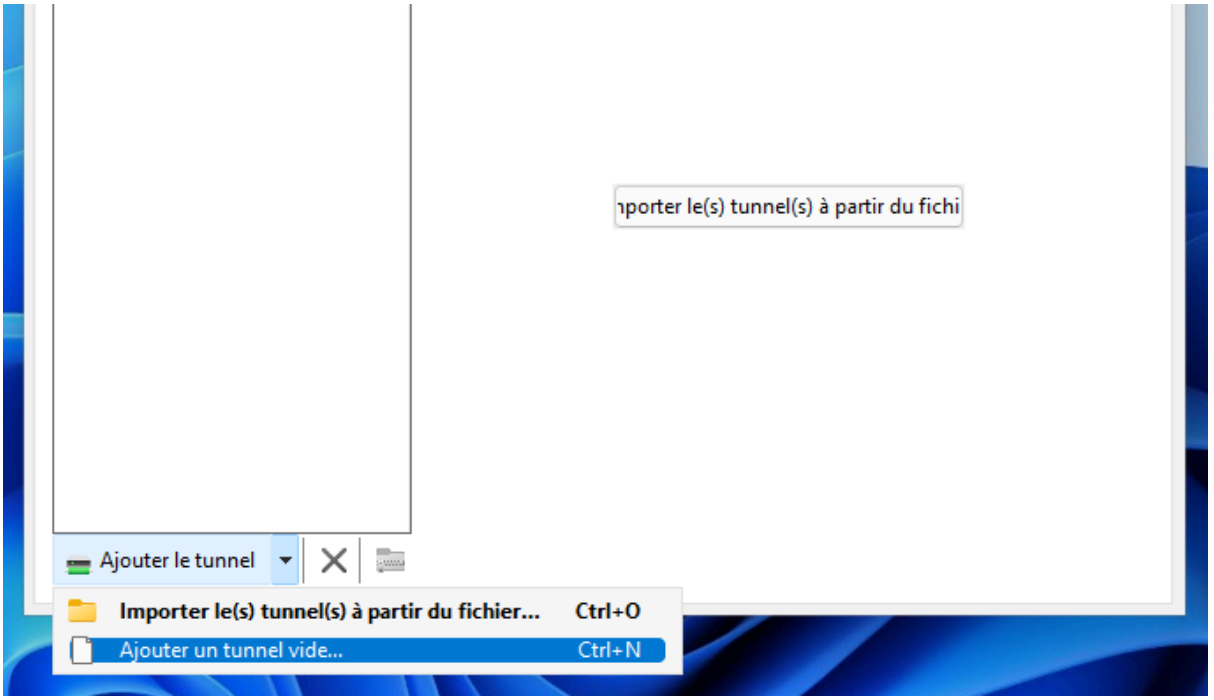
---

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

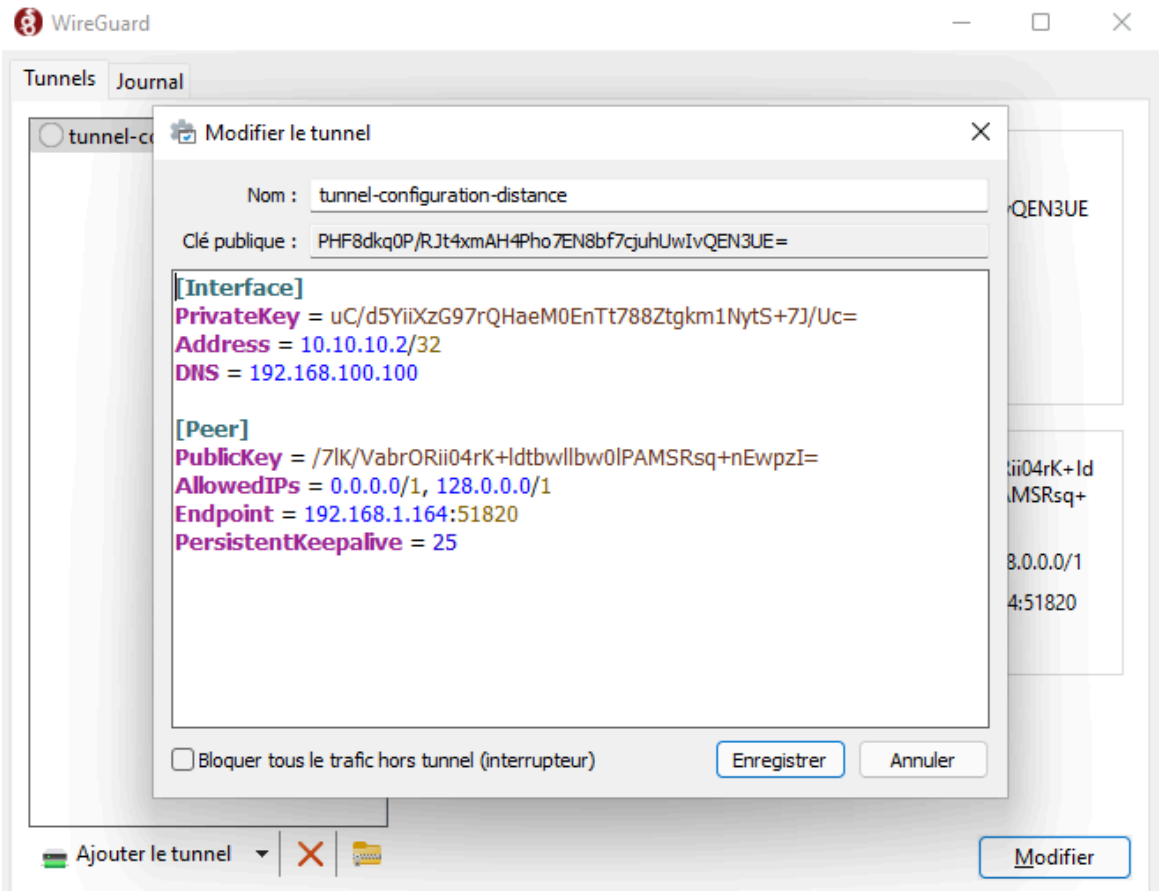
[Peer]

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

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

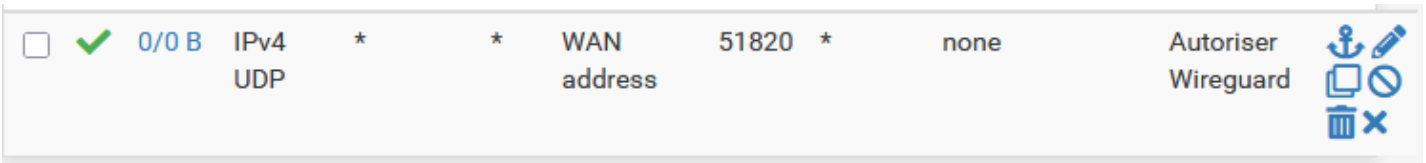
1. Autoriser le port WireGuard côté WAN

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

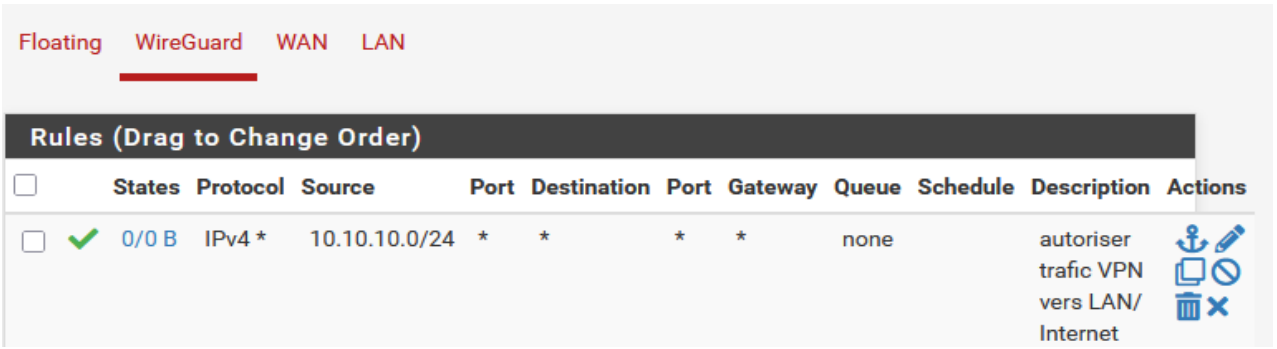


- Va dans **`Firewall > Rules > WireGuard`**
  (ou `tun_wg0` si c'est sous ce nom)
- Clique sur **"Add"** (bouton flèche ↑ en haut)
- Configure la règle comme ceci :

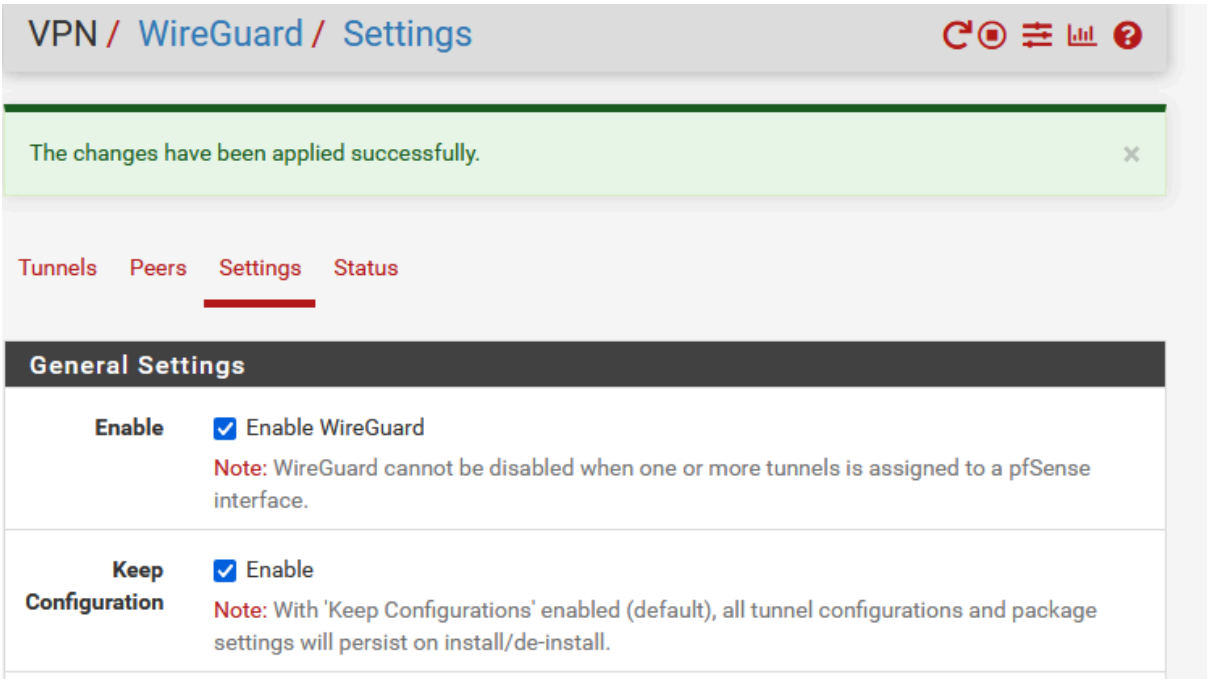
Champ	Valeur
Action	Pass
Interface	`WireGuard` (ou `tun_wg0`)
Protocol	Any
Source	`10.10.10.0/24`
Destination	`any` (ou `192.168.100.0/24` pour limiter au LAN)
Description	Autoriser trafic VPN vers LAN/Internet

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

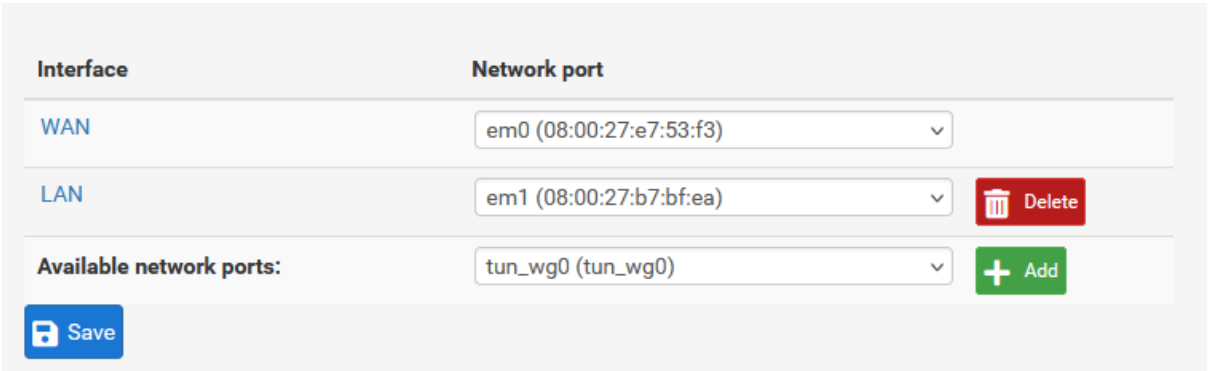
Le règle doit ressembler à celle ci-dessous



Vérifez ensuite dans Vpn / Wireguard / Settings soit bien coché



Ensuite Menu : Interfaces / interface Assigments



Cliquez sur Add

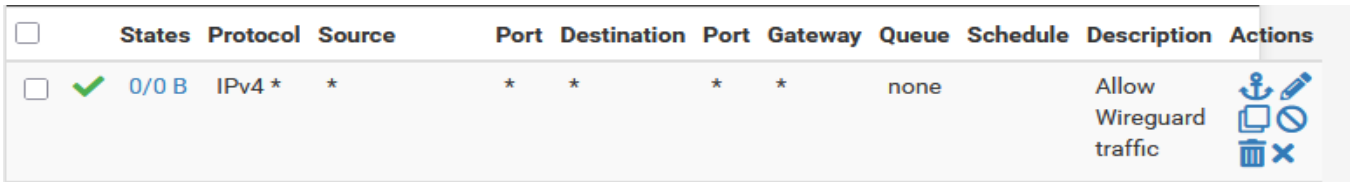
Ensuite allez dans Firewall / Rules / WireGuard

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

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

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

Le résultat doit être similaire à celui ci



---

8. Tester la connexion

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

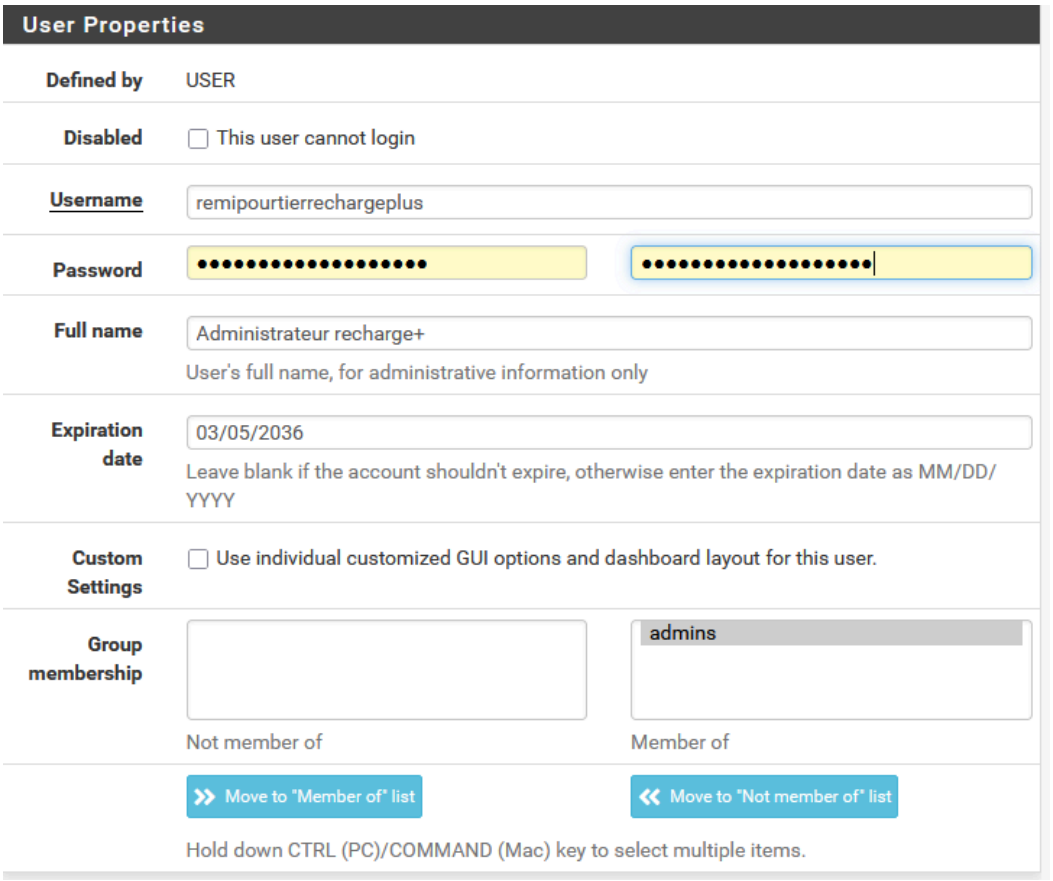
---

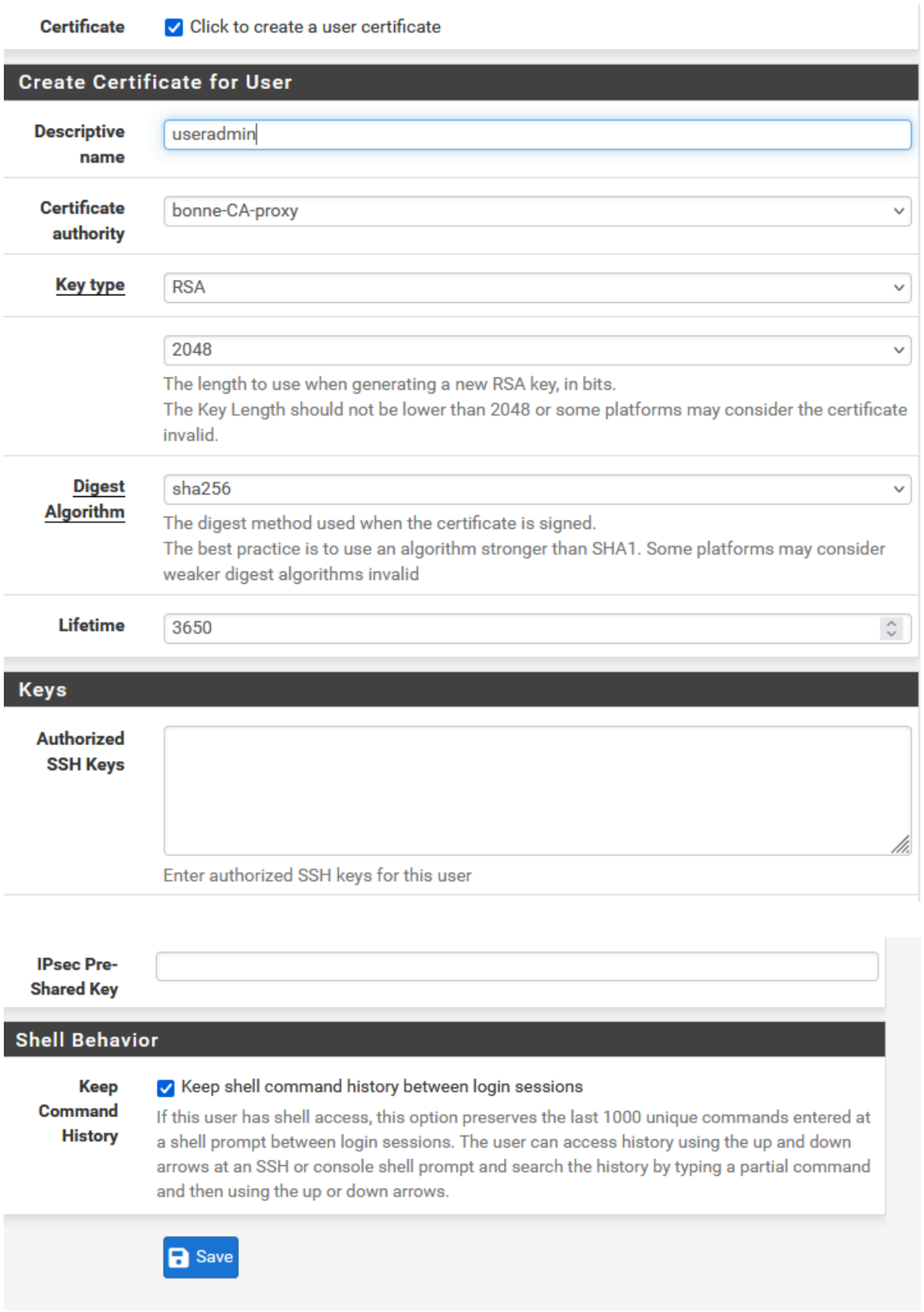
9. Sécuriser

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

Menu : System / User manager

Cliquez sur Add




Certificate
Click to create a user certificate
Create Certificate for User
Descriptive name
useradmin
Certificate authority
bonne-CA-proxy
Key type
RSA
2048
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
sha256
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
3650
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