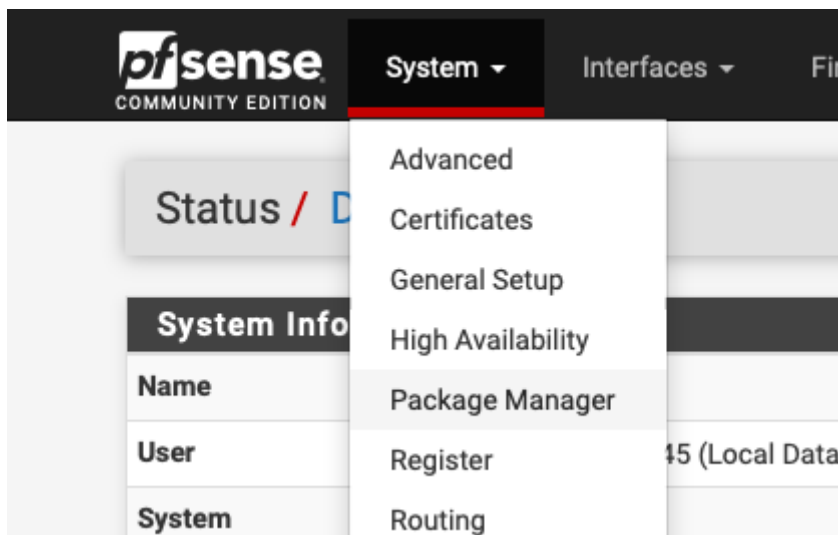


VPN (remote access)

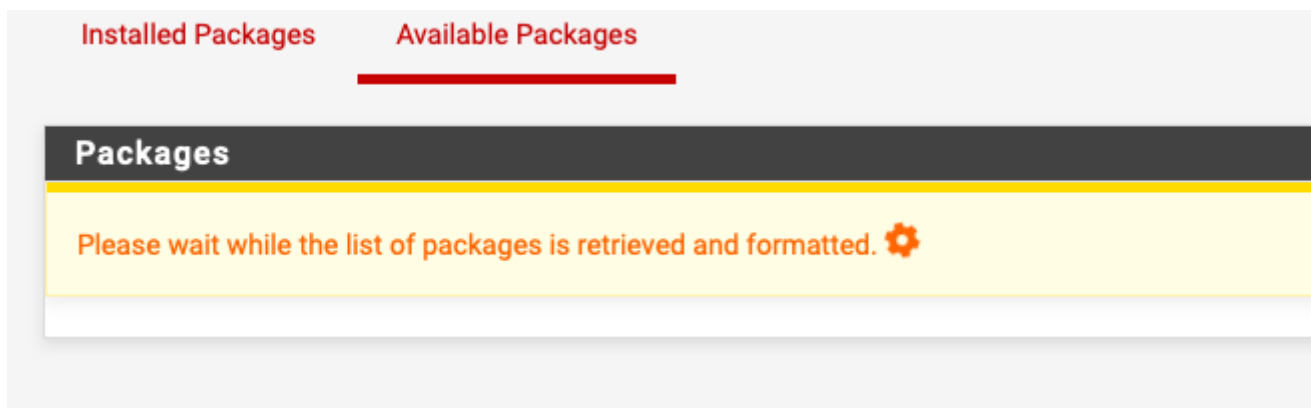
Wireguard sur Pfsense

Installation

Rendez vous sur votre page web pfsense, dans l'onglet système pour accéder au package manager.



Sur l'onglet Available Packages, attendez le chargement et recherchez le packet wireguard pour l'installer.



Cliquer et confirmer pour installer le paquet. L'installation peut prendre quelques minutes.

Please wait while the installation of **pfSense-pkg-WireGuard** completes.
This may take several minutes. Do not leave or refresh the page!

Installed Packages

Available Packages

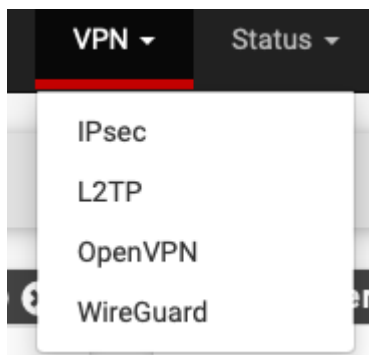
Package Installer

Package Installation

```
>>> Installing pfSense-pkg-WireGuard...  
Updating pfSense-core repository catalogue...
```

Configuration

Une fois l'installation terminée, sur l'onglet VPN vous trouverez wireguard.



Cliquer sur add tunnel. Mettez le port d'écoute que souhaitez, sinon il utilise celui par défaut (51820).

Appuyer sur **Generate** pour générer un couple de clé. Copiez la clé **publique** et converser là.

Laissez le reste par défaut et assigner une adresse ip pour votre réseau vpn avec un masque 255.255.255.0 (/24)

Cette adresse doit être la première du réseau, par exemple 192.168.63.1/24.

Enregistrez vos paramètres.

Retournez sur l'onglet Wireguard, dans l'onglet setting, cliquez sur enable pour activer le service. Vous pouvez laissez les autres paramètres par défaut ou les changer selon vos attentes.

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. 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](#)

Cliquez sur Save, ensuite cliquez sur apply changes.

Rendez vous sur l'onglet peer pour rajouter un utilisateur. Mais à l'avance ouvre votre application wireguard sur votre pc et cliquer sur ajouter un utilisateur, l'application va vous générer une paire de clé, copier la clé publique.

Sur l'onglet "peer" sur pfsense, sur la partie tunnel sélectionner le tunnel créer juste avant. Laissez cocher la partie dynamique endpoint, on mettra le endpoint sur la configuration wireguard au niveau de votre PC en local.

Vous pouvez choisir de mettre le endpoint sur la config pfsense selon vos spécificités.

Mettez une valeur sur la partie "keep alive" 300 par exemple ou laisser la par défaut. Coller la clé publique créer par l'application wireguard de l'utilisateur créer sur votre PC sur la partie **public key**.

Vous pouvez configurer une pre-shared key si voulue (ce tuto ne contient pas de pre-shared key dans la configuration).

Au niveau de **allowed ip**, mettez l'adresse ip de votre peer avec /32, par exemple 192.168.63.2/31. Enregistrez vos paramètres et cliquez sur apply changes.

Sur le fichier wireguard sur votre PC mettez votre configuration, par exemple :

“ [Interface]

PrivateKey = clé privé (générer par défaut par l'application wireguard)

Address = 192.168.63.2/24

DNS = 8.8.8.8, 8.8.4.4

MTU = 1420

[Peer]

PublicKey = clé publique du tunnel wireguard pfsense

AllowedIPs = 192.168.63.0/24, 192.168.2.0/24

Endpoint = 10.10.10.10:51820

La clé privé est automatiquement généré par l'application. Sur la partie **Address** mettez l'adresse de votre peer en /24.

Pour le DNS mettez ceux de google. Le MTU peut être modifié selon vos attentes.

Au niveau de public key, rendez vous sur l'onglet tunnel et copier la clé publique et placez là sur la partie **PublicKey**.

Au niveau **AllowedIPs** mettez l'adresse réseau du réseau **VPN** et idéalement l'adresse réseau du **LAN** pfsense.

Sur la partie **Endpoint**, mettez l'ip public de votre box internet suivi du même port que vous saisi sur le tunnel VPN wireguard lors de la configuration si vous l'avez changé.

Sur la partie firewall sur pfsense, vous trouverez un onglet WireGuard automatiquement créer, acceptez le trafic entrant et sortant sur n'importe quelle port,

Attention, si vous n'accepter que le trafic UDP les communications ne fonctionneront pas.

La règle ressemblera à ça :

FloatingWireGuardWANLAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	2/78.10 MiB	IPv4 *	*	*	*	*	none		Allow trafic for wireguard	

↑ Add

↓ Add

Delete

Toggle

Copy

Save

Separator

Sur la partie WAN, mettez une règle acceptant le trafic entrant vers le WAN en UDP sur le port 51820 (changez le port si vous l'avez changer lors de la création du tunnel).

Ne pas oublier que le port doit être le même sur le tunnel, sur la config VPN du peer (pfsense comme fichier application wireguard, et également le même sur les règles de firewall).

La règle du WAN ressemble à ça.

FloatingWireGuardWANLAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✗	0/752 KiB	*		RFC 1918 networks	*	*	*		Block private networks	
☐	✗	0/98 KiB	*		Reserved Not assigned by IANA	*	*	*		Block bogon networks	
☐	✓	0/0 B	IPv4 UDP	*			WAN address	52820	*	none	Allow trafic for wireguard

↑ Add

↓ Add

Delete

Toggle

Copy

Save

Separator

Si Pfsense n'est pas votre routeur principale (s'il se trouve derrière une box internet active) ne pas oublier la redirection de port vers votre box à l'adresse WAN pfsense en UDP sur le port du tunnel. Ajouter aussi une règle qui laisse passer le trafic si le firewall de votre box est activé.