


| | | |
|---|---|---------------|
|  | ASSUR MER | Version : 1.0 |
| | Configuration du serveur VPN WireGuard | Page 1 sur 7 |



Configuration du serveur VPN WireGuard


| Rédaction | Validation | État | Confidentialité | Création | Révision |
|-------------------------------------|------------------|----------------|-----------------|------------|----------|
| B RUELLO- BABALONI S BARDAZZI | DSI ASSUR MER | Document final | Interne | 17/02/2023 | |



Sommaire

| | |
|--|---|
| Avant-propos..... | 3 |
| Prérequis..... | 3 |
| I. Installation de WireGuard..... | 3 |
| II. Configuration du tunnel WireGuard..... | 5 |

| Rédaction | Validation | État | Confidentialité | Création | Révision |
|-------------------------------------|------------------|----------------|-----------------|------------|----------|
| B RUELLO- BABALONI S BARDAZZI | DSI ASSUR MER | Document final | Interne | 17/02/2023 | |

| | | |
|---|---|----------------------------|
|  | ASSUR MER | Version : 1.0 |
| | Configuration du serveur VPN WireGuard | Page 3 sur 7 |

Avant-propos

Le but de cette documentation est de vous guider dans la configuration d'un tunnel WireGuard sur votre pfSense. WireGuard est un protocole de réseau privé virtuel (VPN) moderne et sécurisé, qui offre une connexion sécurisée et rapide entre deux points. Cette documentation suppose que vous avez déjà installé et configuré pfSense sur votre système.

Prérequis

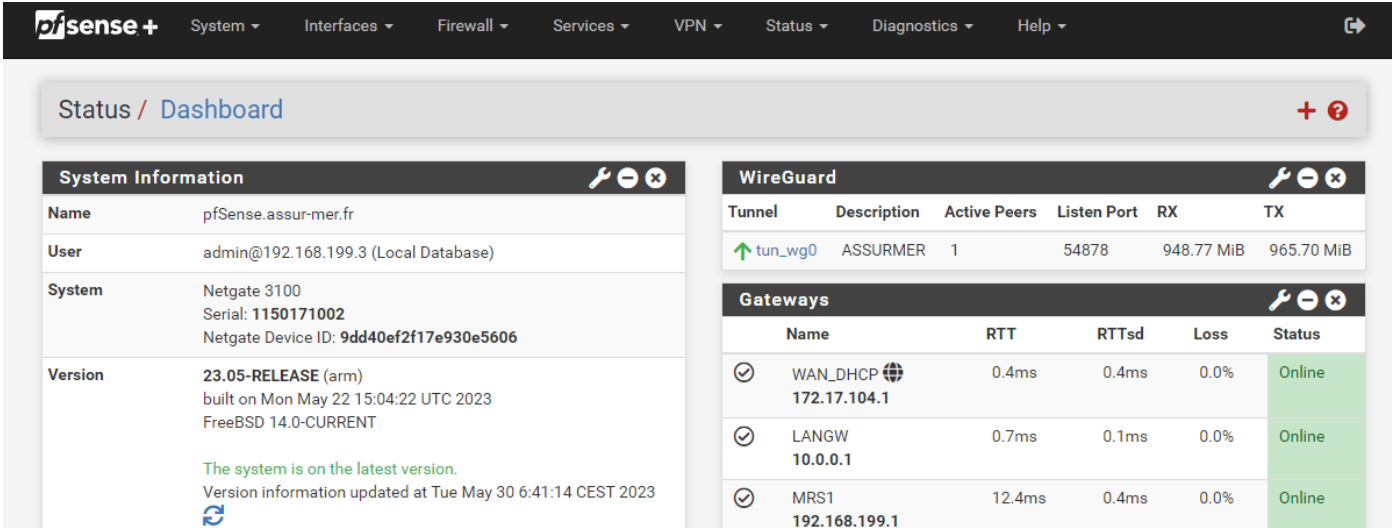
Avant de commencer la configuration du tunnel WireGuard, assurez-vous que vous disposez des éléments suivants :

- Un pare-feu/routeur pfSense configuré et en cours d'exécution.
- Une connexion Internet fonctionnelle sur votre pfSense.
- Les privilèges administratifs pour accéder à l'interface de configuration de pfSense.

I. Installation de WireGuard

Pour installer le module WireGuard sur votre pfSense, suivez ces étapes :

- Connectez-vous à l'interface web de pfSense en utilisant un navigateur.




The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into two panels. The left panel, titled 'System Information', displays details about the pfSense instance, including the name (pfSense.assur-mer.fr), user (admin@192.168.199.3), system (Netgate 3100), serial (1150171002), netgate device ID (9dd40ef2f17e930e5606), and version (23.05-RELEASE (arm)). The right panel, titled 'WireGuard', shows a table of active tunnels and gateways. The 'WireGuard' table has columns for Tunnel, Description, Active Peers, Listen Port, RX, and TX. The 'Gateways' table has columns for Name, RTT, RTTsd, Loss, and Status.

| System Information | |
|--------------------|---|
| Name | pfSense.assur-mer.fr |
| User | admin@192.168.199.3 (Local Database) |
| System | Netgate 3100 Serial: 1150171002 Netgate Device ID: 9dd40ef2f17e930e5606 |
| Version | 23.05-RELEASE (arm) built on Mon May 22 15:04:22 UTC 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Tue May 30 6:41:14 CEST 2023 |

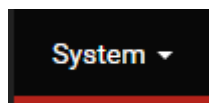
| WireGuard | | | | | |
|-----------|-------------|--------------|-------------|------------|------------|
| Tunnel | Description | Active Peers | Listen Port | RX | TX |
| ↑ tun_wg0 | ASSURMER | 1 | 54878 | 948.77 MiB | 965.70 MiB |

| Gateways | | | | |
|-----------------------|--------|-------|------|--------|
| Name | RTT | RTTsd | Loss | Status |
| WAN_DHCP 172.17.104.1 | 0.4ms | 0.4ms | 0.0% | Online |
| LANGW 10.0.0.1 | 0.7ms | 0.1ms | 0.0% | Online |
| MRS1 192.168.199.1 | 12.4ms | 0.4ms | 0.0% | Online |

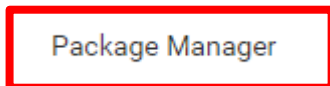
| | | | | | |
|-------------------------------------|------------------|----------------|-----------------|------------|----------|
| Rédaction | Validation | État | Confidentialité | Création | Révision |
| B RUELLO- BABALONI S BARDAZZI | DSI ASSUR MER | Document final | Interne | 17/02/2023 | |

| | | |
|---|---|---------------|
|  | ASSUR MER | Version : 1.0 |
| | Configuration du serveur VPN WireGuard | Page 4 sur 7 |

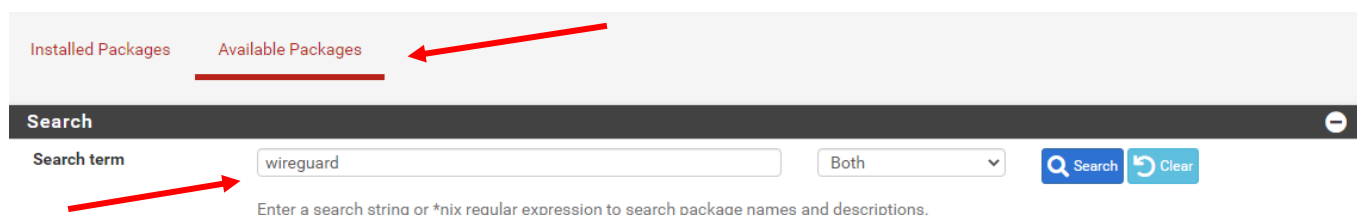
b) Accédez à l'onglet "System" (Système) dans la barre de navigation supérieure.



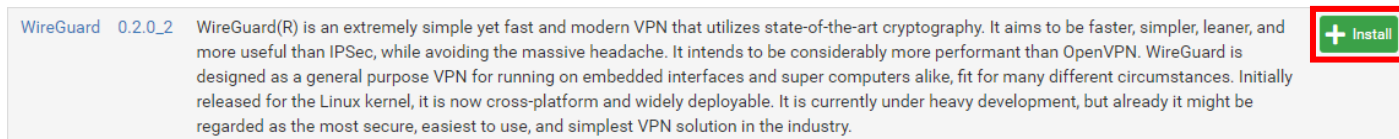
c) Sélectionnez "Package Manager" (Gestionnaire de paquets) dans le menu déroulant.



d) Recherchez "WireGuard" dans la liste des packages disponibles.



e) Cliquez sur le bouton "Install" (Installer) à côté du package WireGuard pour l'installer sur votre système.



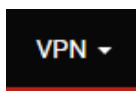
f) Attendez que l'installation soit terminée.

| Rédaction | Validation | État | Confidentialité | Création | Révision |
|-------------------------------------|------------------|----------------|-----------------|------------|----------|
| B RUELLO- BABALONI S BARDAZZI | DSI ASSUR MER | Document final | Interne | 17/02/2023 | |

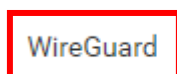
II. Configuration du tunnel WireGuard

Maintenant que WireGuard est installé sur votre pfSense, voici comment configurer un tunnel WireGuard :

- a) Accédez à l'onglet **VPN** dans la barre de navigation supérieure.



- b) Cliquez sur **WireGuard** dans le menu déroulant.



- c) Cliquez sur le bouton **Add Tunnel** pour créer une nouvelle configuration de tunnel.



- d) Configurez les paramètres suivants pour votre tunnel WireGuard :

Tunnel Configuration (tun_wg1)

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

Private key for this tunnel. (Required) Public key for this tunnel. (Copy) New Keys

Interface Configuration (tun_wg1)

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

| Rédaction | Validation | État | Confidentialité | Création | Révision |
|-------------------------------------|------------------|----------------|-----------------|------------|----------|
| B RUELLO- BABALONI S BARDAZZI | DSI ASSUR MER | Document final | Interne | 17/02/2023 | |

| | | |
|---|---|----------------------------|
|  | ASSUR MER | Version : 1.0 |
| | Configuration du serveur VPN WireGuard | Page 6 sur 7 |

- Interface name (Nom de l'interface) : Entrez un nom pour votre interface WireGuard.
- Private key (Clé privée) : Générez ou collez votre clé privée pour le serveur pfSense.
- Listen port (Port d'écoute) : Spécifiez le port sur lequel votre serveur WireGuard écoutera les connexions entrantes.
- Address (Adresse) : Configurez l'adresse IP et le masque réseau pour votre serveur WireGuard.
- Peer configuration (Configuration de pair) : Cliquez sur **Add Peer** pour ajouter une configuration de pair.
 - Public key (Clé publique) : Entrez la clé publique du client distant.
 - Allowed IPs (IP autorisées) : Spécifiez les adresses IP autorisées pour le client distant.


e) Cliquez sur le bouton **Save** pour sauvegarder votre configuration.

III. Réglages des règles de pare-feu

Pour permettre le trafic à travers le tunnel WireGuard, vous devez configurer les règles du pare-feu de pfSense. Voici comment le faire :

- a) Accédez à l'onglet **Firewall** dans la barre de navigation supérieure.
- b) Cliquez sur **Rules** dans le menu déroulant.
- c) Créez une nouvelle règle de pare-feu dans le WAN pour autoriser le trafic WireGuard en utilisant les paramètres suivants :
 - Action : Pass (Autoriser)
 - Interface : Sélectionnez votre interface WireGuard.
 - Address family : IPv4 ou IPv6 en fonction de votre configuration.
 - Protocol : Tout ou sélectionnez un protocole spécifique si nécessaire.
 - Source : Sélectionnez "Any" (Tout) ou spécifiez l'adresse source souhaitée.
 - Destination : Sélectionnez "Any" (Tout) ou spécifiez l'adresse de destination souhaitée.

| Rédaction | Validation | État | Confidentialité | Création | Révision |
|-------------------------------------|------------------|----------------|-----------------|------------|----------|
| B RUELLO- BABALONI S BARDAZZI | DSI ASSUR MER | Document final | Interne | 17/02/2023 | |

| | | |
|---|---|---------------|
|  | ASSUR MER | Version : 1.0 |
| | Configuration du serveur VPN WireGuard | Page 7 sur 7 |

- Description : Ajoutez une description pour la règle.
- d) Cliquez sur le bouton **Save** pour sauvegarder la règle.

IV. Activation du tunnel WireGuard

Une fois la configuration du tunnel et des règles du pare-feu terminée, vous pouvez activer le tunnel WireGuard en suivant ces étapes :


- a) Revenez à l'onglet "VPN" dans la barre de navigation supérieure.
- b) Cliquez sur "WireGuard" dans le menu déroulant.
- c) Cochez la case à côté de votre interface WireGuard nouvellement créée.
- d) Cliquez sur le bouton "Apply Changes" (Appliquer les modifications) pour activer le tunnel WireGuard.

V. Conclusion

Félicitations ! Vous avez maintenant configuré avec succès un tunnel WireGuard sur votre pfSense. Assurez-vous de bien configurer les clés privées et publiques pour chaque pair afin d'assurer une communication sécurisée. N'oubliez pas de configurer également les clients distants avec leurs clés correspondantes pour établir la connexion.

NB : Veuillez noter que cette documentation fournit une vue d'ensemble générale de la configuration d'un tunnel WireGuard sur pfSense et qu'il peut y avoir des variations en fonction des spécificités de votre environnement.


| Rédaction | Validation | État | Confidentialité | Création | Révision |
|-------------------------------------|------------------|----------------|-----------------|------------|----------|
| B RUELLO- BABALONI S BARDAZZI | DSI ASSUR MER | Document final | Interne | 17/02/2023 | |

| | | |
|---|--|----------------------------|
|  | ASSUR MER | Version : 1.0 |
| | Documentation utilisateur Wireguard | Page 1 sur 4 |



Documentation utilisateur Wireguard


| Rédaction | Validation | État | Confidentialité | Création | Révision |
|-------------------------------------|------------------|----------------|-----------------|------------|----------|
| B RUELLO- BABALONI S BARDAZZI | DSI ASSUR MER | Document final | Interne | 17/02/2023 | |

| | | |
|---|--|----------------------------|
|  | ASSUR MER | Version : 1.0 |
| | Documentation utilisateur Wireguard | Page 2 sur 4 |

Sommaire

| | | |
|-----|---|---|
| I. | Ajout d'un tunnel VPN au client Wireguard | 3 |
| A. | Par import depuis un fichier de configuration | 3 |
| B. | Par saisie dans un tunnel vide | 3 |
| II. | Tests de fonctionnement..... | 4 |

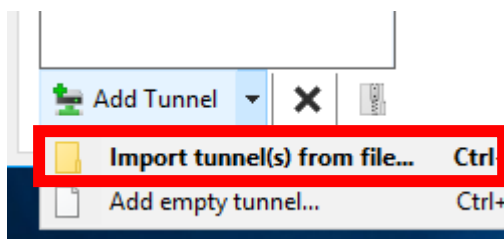
| Rédaction | Validation | État | Confidentialité | Création | Révision |
|-------------------------------------|------------------|----------------|-----------------|------------|----------|
| B RUELLO- BABALONI S BARDAZZI | DSI ASSUR MER | Document final | Interne | 17/02/2023 | |

| | | |
|---|--|----------------------------|
|  | ASSUR MER | Version : 1.0 |
| | Documentation utilisateur Wireguard | Page 3 sur 4 |

I. Ajout d'un tunnel VPN au client Wireguard

A. Par import depuis un fichier de configuration

Il existe une méthode simple d'ajout de la configuration VPN, si vous disposez d'un fichier de configuration pré-généré, il est possible de l'importer directement sur Wireguard.



Cliquer sur **Add Tunnel** puis **Import tunnel(s) from file** et sélectionner dans l'explorateur de fichier la configuration (.conf)

La configuration s'ajoute dans la liste à gauche. La configuration est maintenant terminée, il ne reste plus qu'à activer le tunnel et à procéder aux tests de fonctionnement.


B. Par saisie dans un tunnel vide

Une fenêtre de configuration va s'ouvrir. À chaque fois que l'on crée une nouvelle configuration de tunnel, WireGuard génère un couple de clés privé/public propre à cette configuration. Dans cette configuration, nous devons déclarer le "peer", c'est-à-dire le serveur distant. Pour le moment, nous avons seulement ceci :

```
[Interface]
PrivateKey = <clé privée>
```

La première étape consiste à nommer le tunnel VPN -> **ASSURMER**

| Rédaction | Validation | État | Confidentialité | Création | Révision |
|-------------------------------------|------------------|----------------|-----------------|------------|----------|
| B RUELLO- BABALONI S BARDAZZI | DSI ASSUR MER | Document final | Interne | 17/02/2023 | |

| | | |
|---|--|---------------|
|  | ASSUR MER | Version : 1.0 |
| | Documentation utilisateur Wireguard | Page 4 sur 4 |

Puis, il faut ajouter l'adresse IP de l'interface VPN, renseigner la clé **Address** = l'IP fourni avec le masque de sous-réseau noté en /

```
[Interface]
PrivateKey = <clé privé>
Address = 192.168.199.3/24
```

Ensuite, nous devons déclarer le bloc "Peer" avec trois propriétés.

```
[Peer]
PublicKey = 1D/Gf5yd3hUDoFyYQ3P1zayBHUJhJZq+k6Sv03HnJCQ=
AllowedIPs = 192.168.199.0/24
Endpoint = <ip-passerelle-vpn>:51820
```

La propriété **PublicKey** est l'empreinte du serveur avec lequel notre client est autorisé à dialoguer.

La propriété **AllowedIPs** est la liste des segments réseaux à transiter par le tunnel.

La propriété **Endpoint** est le point de terminaison de la connexion VPN, il se compose d'un nom FQDN ou d'une adresse IP avec un port ici 51820.

II. Tests de fonctionnement

Pour s'assurer du bon fonctionnement de la connexion VPN, il est possible de le vérifier sur Wireguard, dans la section **Homologue**, si les valeurs de transfert reçu et envoyé s'incrémentent la connexion est fonctionnelle.

Il est également possible de ping la passerelle :

```
PS C:\Users\Bapti> ping 192.168.199.2

Envoi d'une requête 'Ping' 192.168.199.2 avec 32 octets de données :
Réponse de 192.168.199.2 : octets=32 temps=9 ms TTL=64
Réponse de 192.168.199.2 : octets=32 temps=11 ms TTL=64
Réponse de 192.168.199.2 : octets=32 temps=7 ms TTL=64
Réponse de 192.168.199.2 : octets=32 temps=9 ms TTL=64

Statistiques Ping pour 192.168.199.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 7ms, Maximum = 11ms, Moyenne = 9ms
```

| Rédaction | Validation | État | Confidentialité | Création | Révision |
|-------------------------------------|------------------|----------------|-----------------|------------|----------|
| B RUELLO- BABALONI S BARDAZZI | DSI ASSUR MER | Document final | Interne | 17/02/2023 | |