
	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

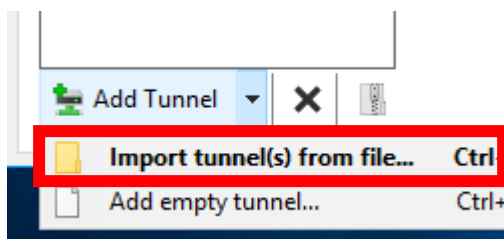
Rédaction	Validation	État	Confidentialité	Création	Révision
B RUELLO- BABALONI S BARDAZZI	DSI ASSUR MER	Document final	Interne	17/02/2023	

	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	