
	ASSUR MER	Version : 1.0
	Configuration du serveur VPN WireGuard	Page 1 sur 5



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	

	ASSUR MER	Version : 1.0
	Configuration du serveur VPN WireGuard	Page 2 sur 5

Sommaire

Avant-propos.....	3
Prérequis.....	3
I. Installation de WireGuard.....	3
II. Configuration du tunnel WireGuard.....	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
	Configuration du serveur VPN WireGuard	Page 3 sur 5

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.
- Accédez à l'onglet "System" (Système) dans la barre de navigation supérieure.
- Sélectionnez "Package Manager" (Gestionnaire de paquets) dans le menu déroulant.
- Recherchez "WireGuard" dans la liste des packages disponibles.
- Cliquez sur le bouton "Install" (Installer) à côté du package WireGuard pour l'installer sur votre système.
- 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	

	ASSUR MER	Version : 1.0
	Configuration du serveur VPN WireGuard	Page 4 sur 5

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** pour créer une nouvelle configuration de tunnel.
- d) Configurez les paramètres suivants pour votre tunnel WireGuard :
 - 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** 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.

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 5 sur 5

c) Créez une nouvelle règle de pare-feu 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.
- 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	