PortailSIO

NOUVELLE FORMULE

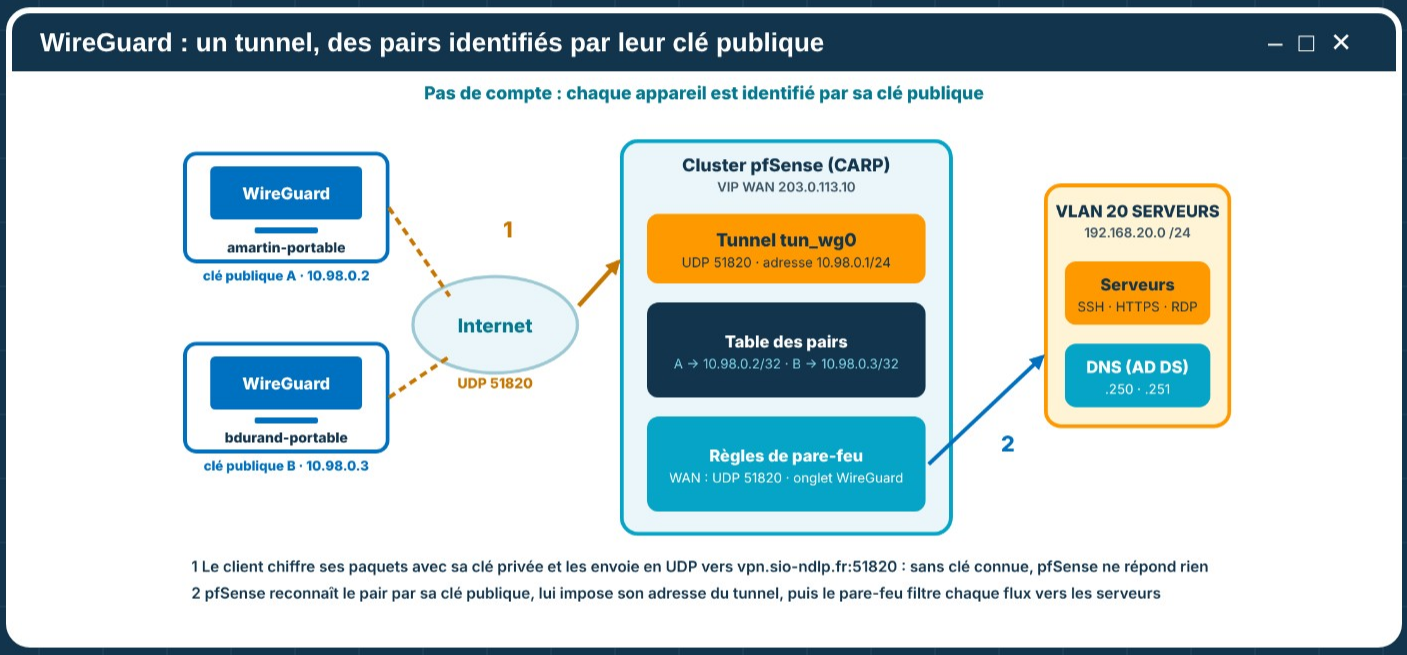
TUTORIEL

PFSENSE · WIREGUARD · UDP 51820

Accès distant rapide avec WIREGUARD



NIVEAU
Intermédiaire



1 Comprendre WireGuard et préparer le plan d'adressage

2 Installer le paquet et créer le tunnel

3 Préparer le client et déclarer le pair

4 Ouvrir le pare-feu

5 Configurer le client et tester

6 Exploiter : pairs, tunnel complet et haute disponibilité

CC BY-NC
Utilisation commerciale interdite
© PortailSIO – 11/2026

Ce tutoriel en ligne
Scannez le QR code. Tous les tutoriels :
portail.sio-ndlp.fr/tutoriels.php

Ce tutoriel a été réalisé avec l'hyperviseur © Proxmox VE. Il peut être réalisé dans un environnement de virtualisation personnel à l'aide des logiciels © VirtualBox ou © VMware Player. Il **suppose que vous disposez du cluster pfSense en haute disponibilité** (nœuds **PFS-1** et **PFS-2**, adresses virtuelles CARP) et des contrôleurs de domaine **SRV-DC1** et **SRV-DC2** sous Windows Server 2025 (leurs adresses servent de serveurs DNS aux clients). Il faut aussi un **poste Windows 11 situé hors du réseau du lycée** (un partage de connexion de téléphone convient très bien) pour jouer le rôle de l'utilisateur nomade. Le tutoriel précédent (OpenVPN) n'est pas indispensable, mais **les deux VPN peuvent cohabiter** sur le même pare-feu.

WireGuard est un VPN récent, **très léger** (quelques milliers de lignes de code, contre plusieurs centaines de milliers pour OpenVPN) et **très rapide**, car il s'exécute dans le noyau du système. Sa configuration tient en quelques lignes et son fonctionnement est radicalement différent de celui d'OpenVPN : **il n'y a ni certificat, ni compte, ni mot de passe**. Chaque appareil possède une paire de clés ; le pare-feu connaît la **clé publique** de chaque appareil autorisé et ignore toute autre personne. Ce tutoriel vous apprend à le déployer pour des utilisateurs nomades, à régler **ce que chaque appareil peut atteindre**, et à mesurer ce que cette simplicité implique pour la sécurité.

Les écrans de pfSense correspondent à la version **CE 2.9** ; ils sont très proches en 2.8 et sur pfSense Plus. L'interface est en anglais : les noms des menus et des champs sont donnés tels qu'ils s'affichent. WireGuard est fourni sous forme de **paquet** : son installation fait l'objet de l'étape 2. Nous utilisons les paramètres suivants (valeurs données à titre d'exemple : adaptez-les à votre réseau) :

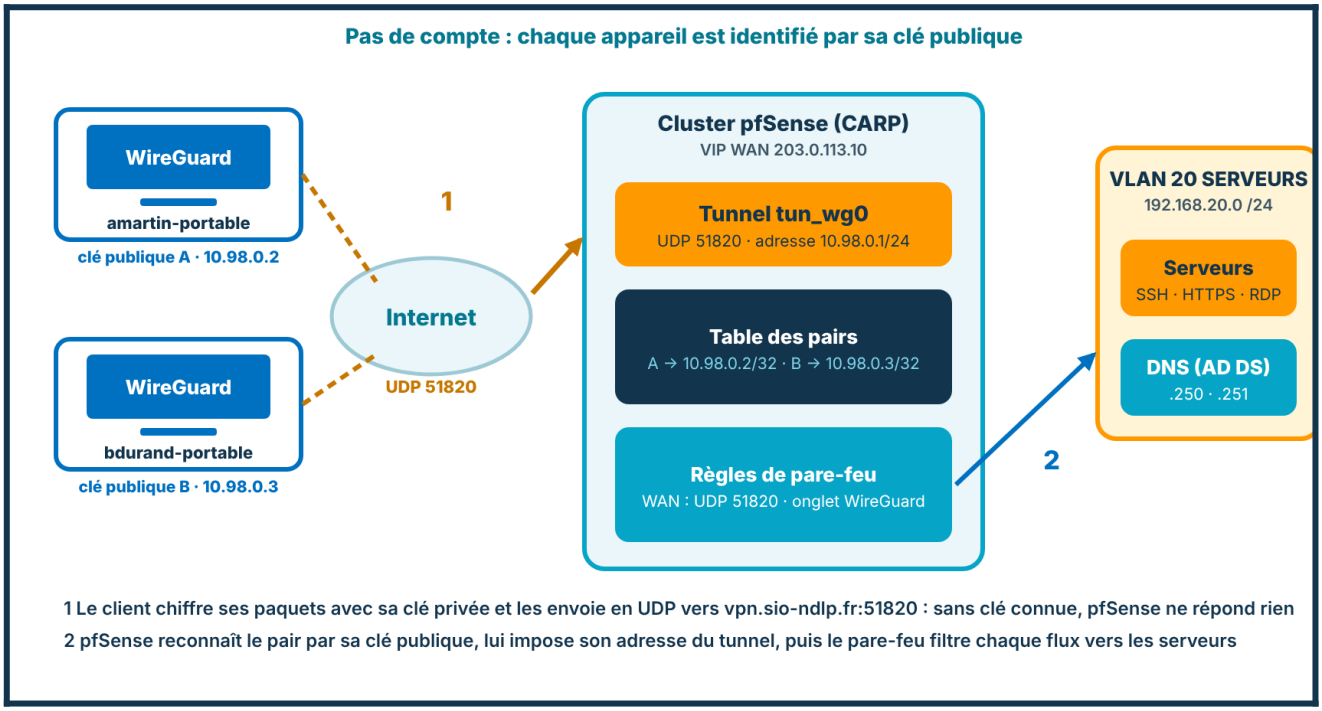
Élément	Valeur	Remarque
Nom et adresse publics du VPN	vpn.sio-ndlp.fr → 203.0.113.10	Adresse virtuelle CARP du WAN (203.0.113.0 /24 est une plage réservée à la documentation : remplacez-la)
Port du tunnel	UDP 51820	Le port habituel de WireGuard ; WireGuard n'utilise jamais TCP
Réseau du tunnel	10.98.0.0 /24	Distinct de celui d'OpenVPN (10.99.0.0 /24) ; ne doit chevaucher aucun réseau du lycée
Adresse de pfSense dans le tunnel	10.98.0.1	L'adresse du tunnel, jamais celle d'un VLAN
Appareils des utilisateurs	amartin-portable → 10.98.0.2 ; bdurand-portable → 10.98.0.3	Une adresse fixe par appareil : elle sert à le reconnaître et à lui appliquer des règles
Réseau accessible par le VPN	192.168.20.0 /24 (VLAN 20 SERVEURS)	Les autres VLAN restent inaccessibles
Serveurs DNS donnés aux clients	192.168.20.250 et 192.168.20.251	Les contrôleurs de domaine : les noms en sio.local fonctionnent à distance
Nom du tunnel sous Windows	SIO-WG	Nom local au poste, libre

ÉTAPE 1 SUR 6

01 Comprendre WireGuard et préparer le plan d'adressage

A – Comment fonctionne WireGuard ?

WireGuard ne distingue pas un « serveur » et des « clients » : tous les participants sont des **pairs** (*peers*). Chacun possède une **clé privée**, qui ne quitte jamais son appareil, et la **clé publique** qui en est déduite, que l'on peut communiquer sans risque. Pour qu'un pair accepte de dialoguer avec un autre, il doit **connaître sa clé publique**. C'est tout : pas d'annuaire, pas de négociation de certificats, pas de session à ouvrir. Le schéma suivant montre la situation de notre laboratoire :



Deux conséquences découlent de ce fonctionnement. D'abord, **pfSense ne répond à rien** tant qu'un paquet n'est pas chiffré avec la clé d'un pair connu : un scanneur de ports ne voit pas le service, car WireGuard reste silencieux. Ensuite, le tunnel est **identifié par l'appareil, pas par la personne** : si le portable d'amartin est volé, son voleur dispose du tunnel, sans autre barrière que la session Windows.

B – Pas d'authentification Active Directory

C'est la **différence majeure avec OpenVPN** : WireGuard ne sait pas interroger un annuaire. Il est impossible de lui faire vérifier un mot de passe du domaine ou l'appartenance à un groupe. La sécurité repose donc sur quatre mesures, que ce tutoriel met en œuvre :

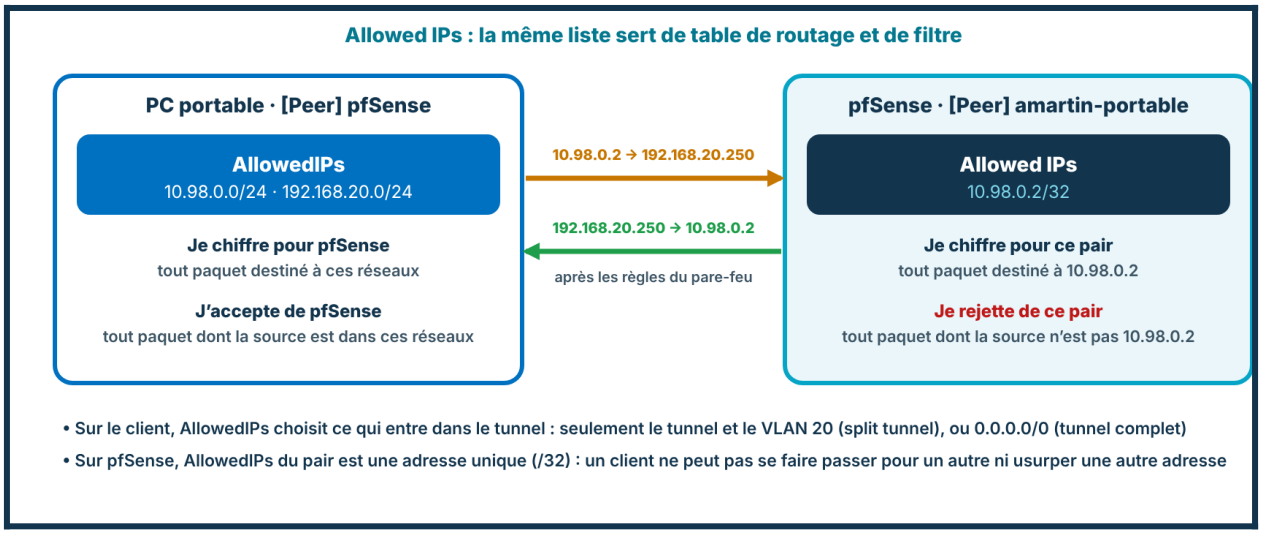
1. **Une paire de clés par appareil**, générée **sur l'appareil** : la clé privée n'est jamais transmise
2. **Une adresse fixe par appareil** dans le tunnel, vérifiée par pfSense : un appareil ne peut pas usurper l'adresse d'un autre
3. **Des règles de pare-feu écrites par adresse** : chaque appareil ne peut joindre que ce qu'on lui autorise
4. **Une clé pré-partagée** (*pre-shared key*) par appareil, qui ajoute une couche de chiffrement symétrique et se révoque avec lui

REMARQUE IMPORTANTE

Comme aucun mot de passe n'intervient, **un appareil perdu ou volé doit être retiré du pare-feu sans délai** : il suffit de **désactiver son pair** dans pfSense (étape 6). Imposez aussi **BitLocker** et un **verrouillage de session** sur les postes qui possèdent un tunnel. Si vous devez vérifier l'identité d'une personne avec son compte du domaine, ou imposer un second facteur, préférez OpenVPN (tutoriel précédent).

C – Allowed IPs : la notion à comprendre

Dans WireGuard, chaque pair déclare une liste d'**Allowed IPs**. Cette liste joue **deux rôles à la fois**, dans les deux sens : elle sert de **table de routage** (« pour joindre ces adresses, j'envoie les paquets à ce pair ») et de **filtre à l'entrée** (« je n'accepte de ce pair que des paquets dont la source est dans cette liste »). C'est ce qu'on appelle le *cryptokey routing*.



Les deux extrémités n'ont pas la même liste. Sur **pfSense**, le pair « amartin-portable » est limité à **sa propre adresse** (10.98.0.2/32) : un paquet venant de ce pair avec une autre adresse est rejeté. Sur le **poste**, les Allowed IPs du pair « pfSense » décident de ce qui entre dans le tunnel : avec **10.98.0.0/24 et 192.168.20.0/24**, seul le trafic destiné au tunnel et au VLAN 20 est chiffré, le reste d'Internet sort normalement (*split tunnel*) ; avec **0.0.0.0/0**, tout passe par pfSense (*tunnel complet*, étape 6).

D – WireGuard ou OpenVPN ?

Critère	WireGuard	OpenVPN (tutoriel précédent)
Authentification	Une **clé publique** par appareil	Certificat **et** mot de passe du domaine
Annuaire Active Directory	**Non** : pas de groupe, pas de mot de passe	**Oui**, en LDAPS, avec filtre de groupe
Mise en place et performances	Très simple (quelques lignes par appareil) et très rapide (noyau)	Plus longue (autorité, certificats, export) et plus modeste en débit
Protocole et port	UDP uniquement, port au choix	UDP ou TCP, 1194 par défaut
Adresse du client	**Fixe**, déclarée par pair	Prise dans un pool, par connexion
Changement de réseau (Wi-Fi vers 4G)	Le tunnel **reprend seul**	Reconnexion nécessaire
Retirer un utilisateur	Désactiver ou supprimer le **pair**	Retirer du groupe AD, révoquer le certificat
Journalisation	Très peu d'informations (dernière poignée de main)	Détaillée : connexion, utilisateur, échecs

En pratique, **WireGuard convient aux appareils connus et maîtrisés** (postes de l'établissement, portables des techniciens, liaison entre deux sites) ; **OpenVPN convient quand on doit authentifier des personnes** avec leur compte du domaine. Les deux peuvent tourner sur le même pare-feu, avec deux réseaux de tunnel distincts.

✔ POINT DE CONTRÔLE

- Vous savez qu'**aucun mot de passe du domaine** n'intervient avec WireGuard
- Vous pouvez expliquer à quoi servent les **Allowed IPs** sur pfSense et sur le client
- Le réseau du tunnel (**10.98.0.0/24**) ne chevauche aucun réseau existant

02 ÉTAPE 2 SUR 6 Installer le paquet et créer le tunnel

A – Installer le paquet WireGuard

Connectez-vous à l'interface web du nœud maître **PFS-1** (`https://pfs-1.sio.local`) puis effectuez les manipulations suivantes :

1. Cliquez le menu « **System** » puis « **Package Manager** » et choisissez l'onglet « **Available Packages** »
2. Dans « **Search term** », saisissez `wireguard` et cliquez « **Search** » ; dans la ligne « **WireGuard** », cliquez « **+ Install** » puis « **Confirm** » :

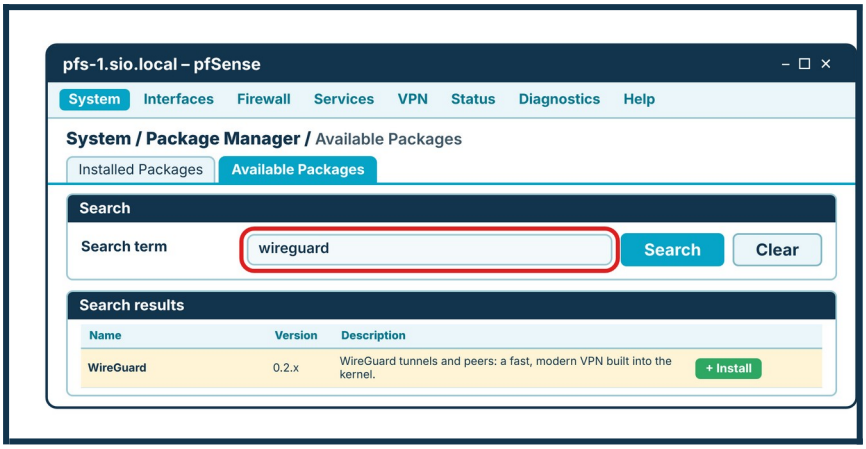


Figure 1 – System > Package Manager : installer le paquet WireGuard

À SAVOIR

Le paquet ajoute le menu « **VPN > WireGuard** ». Les paquets ne sont **pas copiés automatiquement** vers le second nœud : il faudra répéter l'installation sur PFS-2 (étape 6).

B – Activer le service WireGuard

1. Cliquez « **VPN** » puis « **WireGuard** » et choisissez l'onglet « **Settings** »
2. Cochez « **Enable WireGuard** » et « **Keep Configuration** » (les tunnels et pairs sont conservés si le paquet est désinstallé ou mis à jour) ; laissez « **Hide Secrets** » coché

3 Cliquez « **Save** » puis, si pfSense le propose, « **Apply Changes** » :

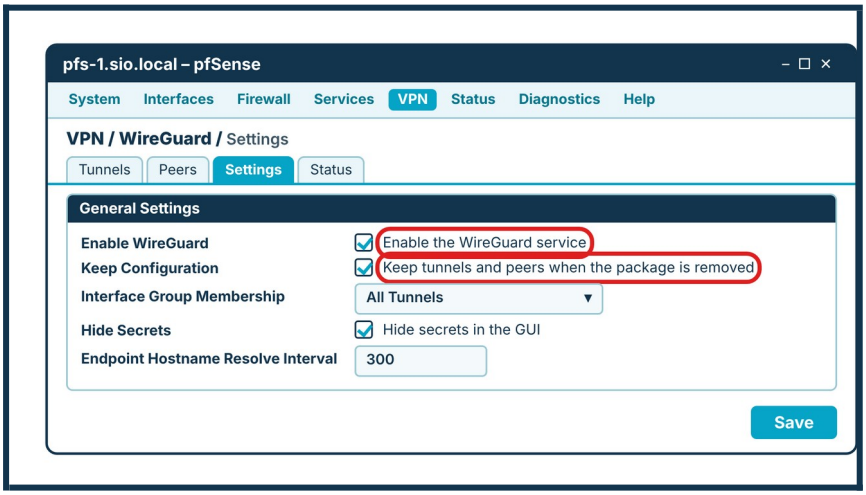


Figure 2 – VPN > WireGuard > Settings : activer le service

À SAVOIR

« **Hide Secrets** » masque les clés privées et pré-partagées dans les pages de pfSense : une capture d'écran ou un regard par-dessus l'épaule n'exposent plus la clé. « **Interface Group Membership** » rattache les tunnels au groupe d'interfaces « WireGuard » utilisé à l'étape 4.

C – Créer le tunnel de pfSense

Le **tunnel** représente l'**extrémité pfSense** : sa clé, son port d'écoute et son adresse dans le réseau du VPN. Cliquez l'onglet « **Tunnels** » puis « **+ Add Tunnel** » :

1 Cochez « **Enable tunnel** » ; « **Description** » : `Accès distant SIO` ; « **Listen Port** » : `51820`

2 Dans « **Interface Keys** », cliquez « **Generate** » : pfSense crée la **clé privée** et affiche la **clé publique** qui en découle (celle que les clients devront connaître)

3 Dans « **Interface Configuration (Optional)** », « **Interface Addresses** » : `10.98.0.1` avec le masque `24`

4 Cliquez « **Save Tunnel** » puis « **Apply Changes** » :

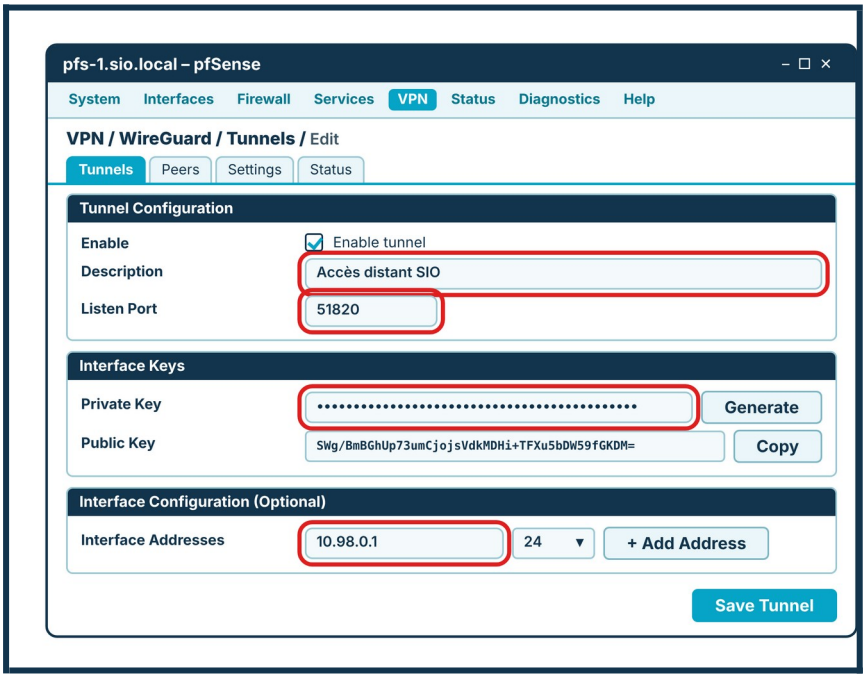


Figure 3 – VPN > WireGuard > Tunnels : création du tunnel tun_wg0

À SAVOIR

Le port d'écoute est celui de la règle de pare-feu de l'étape 4. L'adresse **10.98.0.1/24** est celle de pfSense **dans le tunnel** : elle définit aussi le réseau 10.98.0.0/24, où chaque pair aura une adresse.

Le tunnel apparaît dans la liste, nommé **tun_wg0** par pfSense. Relevez sa **clé publique** : copiez-la dans un fichier texte, elle sera collée dans le client à l'étape 5.



Figure 4 – VPN > WireGuard > Tunnels : le tunnel tun_wg0 est créé

À SAVOIR

La colonne « Peers » indique **0** : aucun appareil n'est encore autorisé. L'adresse est suivie de « (unassigned) » : le tunnel n'est pas encore associé à une interface pfSense, ce qui convient pour un accès à un réseau interne (étape 6 pour l'autre cas).

REMARQUE IMPORTANTE

La **clé privée** du tunnel reste dans pfSense et n'est jamais communiquée aux clients : seule la clé **publique** circule. Si vous la perdez, régénérez-la, mais **tous les clients devront alors recevoir la nouvelle clé publique**.

✔ **POINT DE CONTRÔLE**

- Le paquet **WireGuard** est installé et « **Enable WireGuard** » est coché
- Le tunnel **tun_wg0** existe, écoute sur **51820** et porte l'adresse **10.98.0.1/24**
- La **clé publique** du tunnel est copiée dans un fichier texte

03 ÉTAPE 3 SUR 6 — Préparer le client et déclarer le pair

A – Installer WireGuard sur le poste nomade

Sur le **poste Windows 11 situé hors du réseau du lycée**, installez **WireGuard pour Windows**, téléchargé sur le site officiel (wireguard.com, rubrique « Install »). Vous pouvez aussi l'installer en ligne de commande, depuis PowerShell en tant qu'administrateur :

POWERSHELL (POSTE NOMADE)

```
winget install --id WireGuard.WireGuard -e
```

B – Générer la paire de clés sur le poste

La clé privée doit être **créée sur l'appareil** qui la porte, afin de ne **jamais circuler**. Lancez l'application « **WireGuard** » puis cliquez la flèche de « **Add Tunnel** » (en bas à gauche) et « **Add empty tunnel…** » :

1. « **Name** » : `SIO-WG` ; l'application génère aussitôt la paire de clés et affiche la **clé publique** (« **Public key** »)
2. Sélectionnez la clé publique, copiez-la (Ctrl+C) et conservez-la : elle sera déclarée dans pfSense (C)

3 Laissez la case « **Block untunneled traffic (kill-switch)** » décochée (elle ne sert qu'avec un tunnel complet, étape 6) puis cliquez « **Save** » :



Figure 5 – WireGuard pour Windows : créer un tunnel vide

À SAVOIR

La zone de texte contient déjà la ligne « **PrivateKey** » : c'est la clé privée générée par l'application. **Ne la supprimez pas** à l'étape 5 : sans elle, la clé publique affichée changerait et ne correspondrait plus à celle déclarée dans pfSense.

C – Déclarer l'appareil comme pair dans pfSense

Revenez sur **PFS-1**, menu « **VPN > WireGuard** », onglet « **Peers** » puis « **+ Add Peer** » :

1 Cochez « **Enable peer** » ; « **Tunnel** » : « **tun_wg0 (Accès distant SIO)** » ; « **Description** » : `amartin-portable`

2 Cochez « **Dynamic Endpoint** » : le portable change d'adresse selon le réseau utilisé, donc pfSense ne peut pas le contacter le premier ; laissez « **Keep Alive** » vide (c'est le client qui enverra les paquets de maintien)

3 « **Public Key** » : collez la clé publique générée par le poste ; « **Pre-shared Key** » : cliquez « **Generate** » et copiez la clé obtenue

4 « **Allowed IPs** » : `10.98.0.2` avec le masque `32` (l'adresse de cet appareil, et elle seule) ; cliquez « **Save Peer** » puis « **Apply Changes** » :

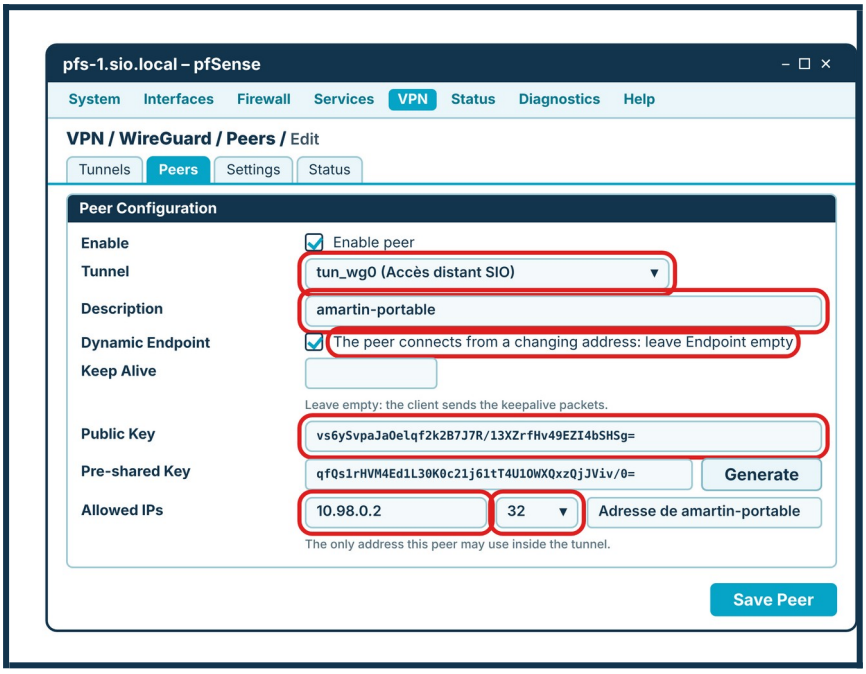


Figure 6 – VPN > WireGuard > Peers : déclarer amartin-portable

À SAVOIR

Le masque **/32** désigne **une seule adresse** : pfSense n'acceptera de ce pair que des paquets dont la source est 10.98.0.2. Chaque appareil reçoit sa propre adresse, **jamais la même qu'un autre** : sinon pfSense ne saurait pas auquel remettre les réponses.

Répétez l'opération pour le portable de bdurand (`bdurand-portable`, adresse `10.98.0.3`, sa propre clé publique et sa propre clé pré-partagée). La liste des pairs doit alors ressembler à ceci :

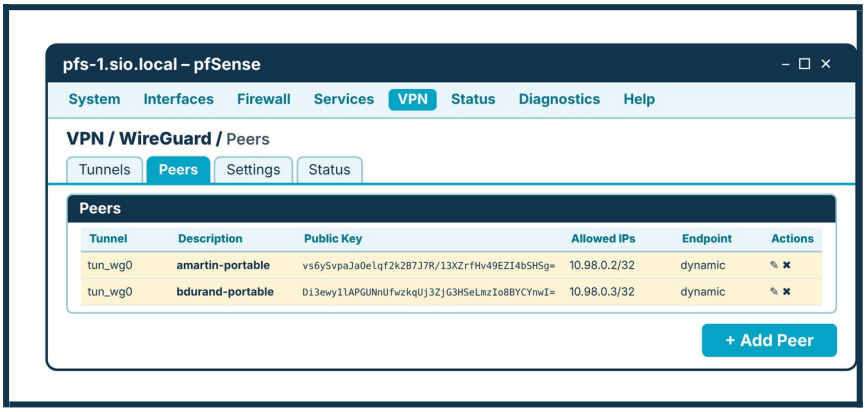


Figure 7 – VPN > WireGuard > Peers : les deux appareils autorisés

À SAVOIR

Les clés publiques sont différentes : c'est ce qui identifie chaque appareil. La colonne « Endpoint » affiche **dynamic** : pfSense apprend l'adresse du poste dès le premier paquet reçu.

À SAVOIR

La **clé pré-partagée** est facultative, mais utile : elle ajoute un secret symétrique, propre à chaque appareil, au chiffrement. Elle doit être **identique des deux côtés** (pfSense et client) ; si l'une des deux est absente ou différente, la poignée de main échoue sans message d'erreur. Transmettez-la par un canal sûr (coffre de mots de passe, remise en main propre), jamais par courriel ordinaire.

✔ **POINT DE CONTRÔLE**

- Le poste possède le tunnel **SIO-WG** et sa **clé publique** a été copiée
- Les pairs **amartin-portable** et **bdurand-portable** existent dans pfSense, chacun avec une **adresse /32 différente**
- Chaque pair a sa **clé pré-partagée**, notée pour être collée dans le client

04 ÉTAPE 4 SUR 6 Ouvrir le pare-feu

A – Autoriser le port UDP 51820 sur le WAN

Il faut **deux séries de règles** : l'une laisse les clients **atteindre** pfSense, l'autre décide de ce qu'ils **peuvent faire** une fois dans le tunnel. Commencez par le WAN : cliquez « **Firewall > Rules** », l'onglet « **WAN** » puis « **↑ Add** » :

1. « **Action** » : « **Pass** » ; « **Protocol** » : « **UDP** » ; « **Source** » : « **Any** »
2. « **Destination** » : « **Address or Alias** » et `203.0.113.10` ; « **Destination Port Range** » : « **(other)** » et `51820` (champs « From » et « To »)
3. « **Description** » : `WireGuard : accès distant SIO` puis cliquez « **Save** » :

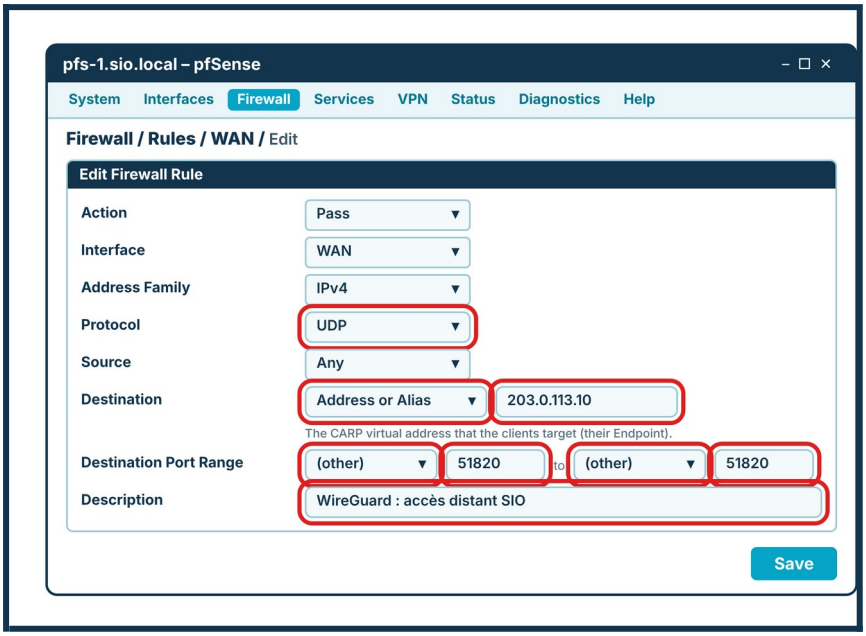


Figure 8 – Firewall > Rules > WAN : autoriser UDP 51820 vers le VPN

À SAVOIR

La destination est l'**adresse virtuelle CARP** et non « WAN address » : cette dernière désigne l'adresse propre du nœud, et la règle ne fonctionnerait plus après une bascule. La source est « Any » : les clients nomades ont une adresse inconnue à l'avance.

B – Créer les alias de ports et de serveurs

Les règles suivantes utilisent deux alias. **Si vous avez réalisé le tutoriel OpenVPN, ils existent déjà** et vous pouvez passer à C. Sinon, cliquez « **Firewall > Aliases** » :

1. Onglet « **IP** » puis « **+ Add** » : « **Name** » `DC_SIO`, « **Type** » « **Host(s)** », deux entrées `192.168.20.250` et `192.168.20.251`, « **Description** » `Contrôleurs de domaine` ; cliquez « **Save** »
2. Onglet « **Ports** » puis « **+ Add** » : « **Name** » `PORTS_ADMIN`, « **Type** » « **Port(s)** », trois entrées `22`, `443` et `3389`, « **Description** » `SSH, HTTPS et RDP` ; cliquez « **Save** » puis « **Apply Changes** »

C – Filtrer ce que les clients peuvent faire dans le tunnel

Une fois le tunnel créé, pfSense affiche un onglet « **WireGuard** » dans « **Firewall > Rules** » : c'est le **groupe d'interfaces** auquel appartiennent tous les tunnels WireGuard. Ses règles s'appliquent à **tout paquet entrant par un tunnel**, sans qu'il soit nécessaire d'assigner une interface au tunnel. Sans règle, **tout est refusé**. Créez les trois règles suivantes, de la plus précise à la plus large, avec « **Action** » « **Pass** » et « **Source** » « **Network** » `10.98.0.0/24` :

Protocole	Destination	Port	Description
ICMP (« any »)	Network 192.168.20.0/24	—	WG : ping vers les serveurs
TCP/UDP	Address or Alias **DC_SIO**	DNS (53)	WG : DNS vers les contrôleurs
TCP	Network 192.168.20.0/24	Alias **PORTS_ADMIN**	WG : SSH, HTTPS, RDP vers les serveurs

Cliquez « **Save** » après chaque règle, puis « **Apply Changes** » :

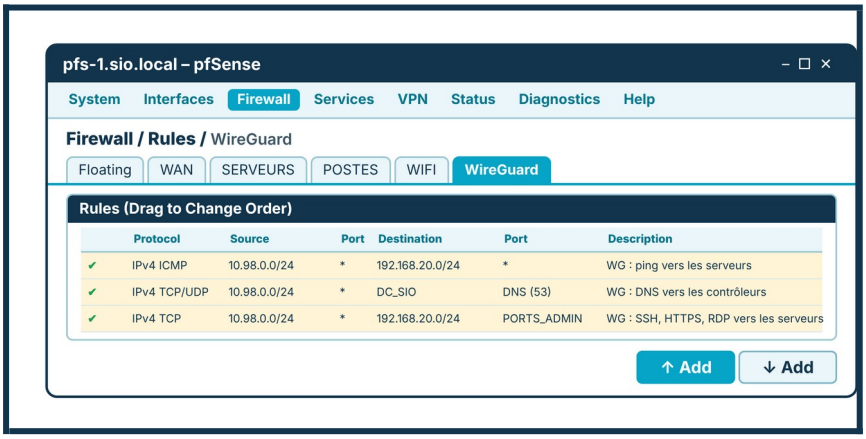


Figure 9 – Firewall > Rules > WireGuard : ce que les clients peuvent faire

À SAVOIR

Les règles suivent le **moindre privilège** : le client atteint les serveurs sur trois ports seulement, plus le DNS. Tout le reste, y compris le partage de fichiers (445), est refusé par la règle implicite de pfSense.

REMARQUE IMPORTANTE

Aucune règle de **NAT** n'est nécessaire ici : les serveurs du VLAN 20 ont pour passerelle l'adresse virtuelle de pfSense (192.168.20.254), donc leurs **réponses reviennent par le tunnel**. Si un serveur de ce VLAN utilise une autre passerelle, les réponses partent ailleurs et la connexion échoue : c'est la première chose à vérifier en cas de blocage.

✔ POINT DE CONTRÔLE

- La règle **WAN UDP 51820** cible l'**adresse virtuelle** 203.0.113.10
- Les alias **DC_SIO** et **PORTS_ADMIN** existent
- L'onglet **WireGuard** contient les **trois règles** de filtrage

05 ÉTAPE 5 SUR 6 Configurer le client et tester

A – Compléter la configuration du poste

Sur le poste nomade, sélectionnez le tunnel **SIO-WG** puis cliquez « **Edit** » (en bas à droite). La zone de texte contient la section « **[Interface]** » avec la clé privée : **conservez cette ligne** et complétez la configuration comme suit :

1. Ajoutez, sous « **PrivateKey** », les lignes « **Address** » et « **DNS** » ; puis la section « **[Peer]** » qui décrit pfSense
2. Collez la clé publique du **tunnel** (étape 2, C) dans « **PublicKey** » et la clé pré-partagée du **pair** (étape 3, C) dans « **PresharedKey** »
3. Cliquez « **Save** » :

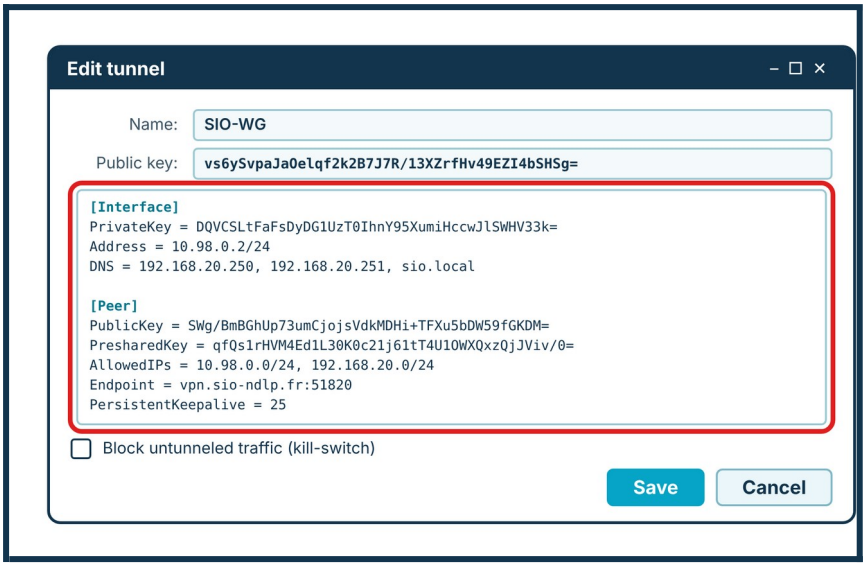


Figure 10 – WireGuard pour Windows : la configuration complète du tunnel SIO-WG

À SAVOIR

La clé publique affichée en haut (celle du **poste**) n'a pas changé : c'est la preuve que la clé privée est intacte. Les clés de ce document sont des exemples : ne les réutilisez jamais.

Chaque ligne a un rôle précis ; les repérer facilite le dépannage :

Directive	Rôle	Valeur ici
PrivateKey	Clé privée du poste (générée par l'application)	Ne se transmet à personne
Address	Adresse du poste dans le tunnel	10.98.0.2/24 : l'adresse déclarée dans pfSense, avec le masque du réseau du tunnel
DNS	Serveurs DNS (et suffixe de recherche) utilisés **tant que le tunnel est actif**	192.168.20.250, 192.168.20.251, sio.local
PublicKey	Clé publique de **pfSense** (celle du tunnel)	Collée depuis pfSense
PresharedKey	Clé pré-partagée de ce pair	Identique à celle de pfSense
AllowedIPs	Ce qui entre dans le tunnel (et ce qui est accepté en retour)	10.98.0.0/24, 192.168.20.0/24 : le tunnel et le VLAN 20
Endpoint	Adresse et port où joindre pfSense	vpn.sio-ndlp.fr:51820 (adresse virtuelle du WAN)
PersistentKeepalive	Envoie un paquet de maintien toutes les N secondes	25 : garde ouverte la correspondance du NAT de la box et permet à pfSense de répondre

B – Activer le tunnel

Dans la fenêtre principale, sélectionnez **SIO-WG** puis cliquez « **Activate** ». Le voyant passe au vert et l'état devient « **Active** ». Le champ « **Latest handshake** » indique la dernière **poignée de main** cryptographique : elle prouve que pfSense a reconnu le poste.

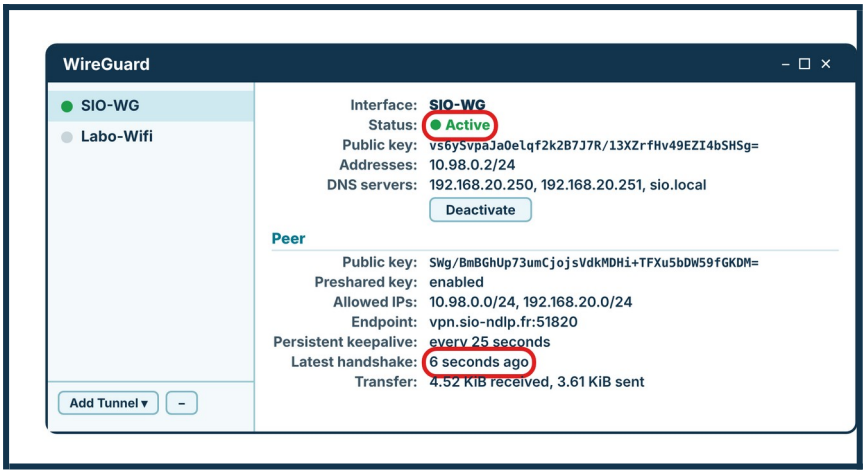


Figure 11 – WireGuard pour Windows : le tunnel SIO-WG est actif

À SAVOIR

« Latest handshake » doit afficher quelques secondes à quelques minutes : WireGuard renouvelle la clé de session environ toutes les deux minutes tant que du trafic circule. « Transfer » montre les octets échangés : un tunnel actif sans poignée de main n'est pas connecté.

C – Vérifier l'accès aux serveurs

Depuis PowerShell, sur le poste nomade, contrôlez que le trafic **passe par le tunnel** pour les ports autorisés et qu'il est **bloqué** pour les autres :

POWERSHELL (POSTE NOMADE)

```
Test-NetConnection 192.168.20.250 -Port 3389
Resolve-DnsName srv-dc1.sio.local -Type A
Test-NetConnection 192.168.20.250 -Port 445
```

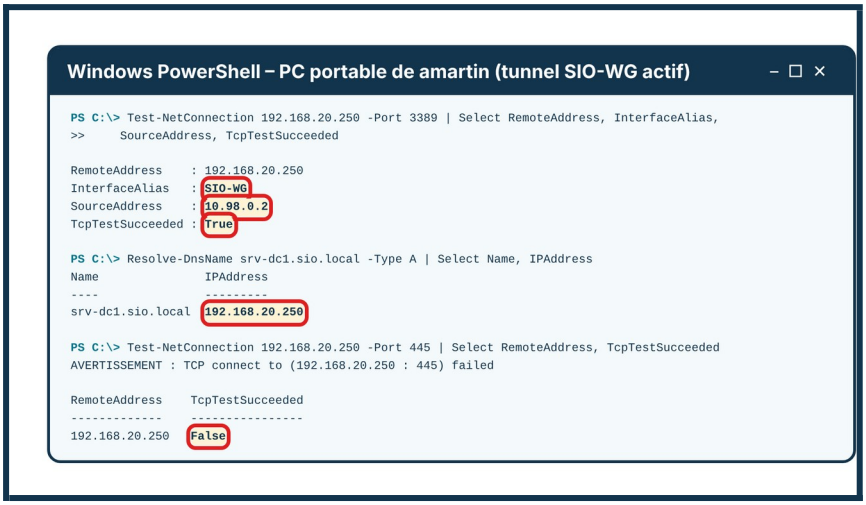


Figure 12 – PowerShell : accès autorisé (3389), nom résolu et accès refusé (445)

À SAVOIR

« InterfaceAlias » = SIO-WG et « SourceAddress » = 10.98.0.2 prouvent que le trafic part du tunnel. Le port 3389 (RDP) passe, le port 445 (partage de fichiers) est refusé : les règles de l'onglet WireGuard s'appliquent bien.

D – Contrôler côté pfSense

Cliquez « **Status** » puis « **WireGuard** » (ou l'onglet « **Status** » du menu WireGuard). Le pair d'amartin est connecté ; celui de bdurand n'a encore jamais reçu de paquet :

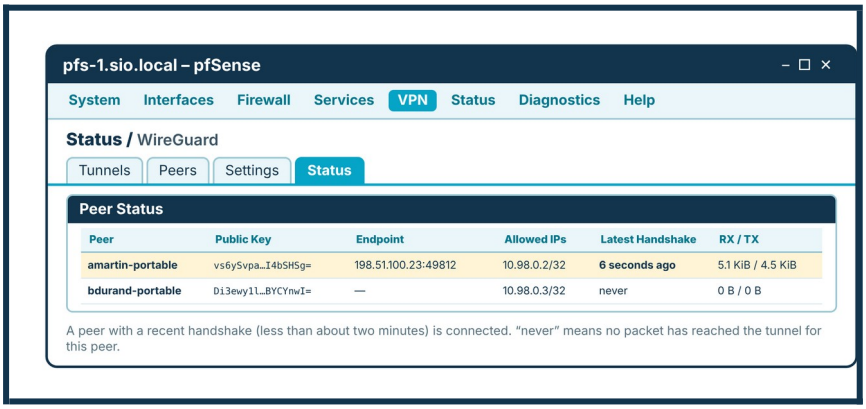


Figure 13 – Status > WireGuard : état des pairs

À SAVOIR

Une poignée de main **de moins de deux ou trois minutes** signifie que le pair est connecté. L'adresse affichée dans « Endpoint » est celle que pfSense a apprise : c'est l'adresse **publique** actuelle du poste (ici, le partage de connexion du téléphone).

À SAVOIR

Sur le poste, l'application WireGuard installe le tunnel comme un **service Windows** : tant que vous ne cliquez pas « Deactivate », il redémarre avec la machine. Par défaut, **seuls les administrateurs** peuvent l'activer ou le désactiver ; pour permettre à un utilisateur standard de le faire, la documentation de WireGuard décrit une valeur de registre (`LimitedOperatorUI`) et l'appartenance au groupe « **Network Configuration Operators** ». Pour un déploiement par script, la commande `wireguard.exe /installtunnelservice <fichier.conf>` installe un tunnel depuis un fichier de configuration.

✔ POINT DE CONTRÔLE

- Le client est **Active** et « **Latest handshake** » indique quelques secondes
- Le **port 3389** de SRV-DC1 répond par le tunnel (**SourceAddress 10.98.0.2**), le **port 445** est refusé
- Le nom **srv-dc1.sio.local** est résolu (DNS de l'annuaire)
- **Status > WireGuard** montre une poignée de main récente pour amartin-portable

ÉTAPE 6 SUR 6

06 Exploiter : pairs, tunnel complet et haute disponibilité

A – Les opérations courantes

Je veux…	Je fais…
Autoriser un nouvel appareil	Générer la paire de clés **sur l'appareil** ; créer un pair dans pfSense (clé publique, **nouvelle adresse /32**, clé pré-partagée) ; compléter le client ; ajouter l'appareil à vos tableaux de suivi
Retirer un appareil perdu ou volé	Dans « **VPN > WireGuard > Peers** », **décocher « Enable peer »** (ou supprimer le pair) puis « **Apply Changes** » : sa poignée de main échoue immédiatement
Retirer une personne qui quitte l'établissement	Désactiver tous ses pairs ; **ce n'est pas automatique**, car rien ne relie l'appareil à son compte AD : tenez un registre des appareils par utilisateur
Renouveler les clés d'un appareil	Générer une nouvelle paire sur le poste, mettre à jour la clé publique du pair dans pfSense, éventuellement la clé pré-partagée : les deux extrémités doivent changer ensemble
Changer de port ou d'adresse publique	Modifier « Listen Port » du tunnel, la règle WAN **et** la ligne « Endpoint » de tous les clients
Surveiller les connexions	« **Status > WireGuard** » (poignées de main, volumes) ; en SSH ou « **Diagnostics > Command Prompt** » : `wg show`

B – Différencier les droits selon l'appareil

Chaque appareil a une adresse fixe : on peut donc lui appliquer des règles **qui lui sont propres**. Supposons que **bdurand** (technicienne) puisse administrer les serveurs, alors qu'**amartin** (direction) n'ait besoin que du web interne. Dans l'onglet « **WireGuard** », remplacez la règle SSH, HTTPS et RDP par ces deux règles (la plus précise en premier) :

Source	Destination	Port	Description
Single host 10.98.0.3	Network 192.168.20.0/24	Alias **PORTS_ADMIN**	WG : bdurand administre les serveurs
Network 10.98.0.0/24	Network 192.168.20.0/24	HTTPS (443)	WG : les autres appareils : web interne uniquement

Pour plus de lisibilité, regroupez les adresses dans un alias (par exemple `WG_TECH`) plutôt que d'écrire des adresses isolées. C'est la contrepartie de l'absence d'annuaire : **les droits se rattachent aux appareils**, pas aux personnes.

C – Variante : un tunnel complet

Pour envoyer **tout** le trafic d'un poste dans le tunnel (navigation web comprise), trois changements sont nécessaires.

1. **Côté client** : dans « **AllowedIPs** », remplacez la liste par `0.0.0.0/0, ::/0` (le second réseau évite les fuites par IPv6) ; la case « **Block untunneled traffic (kill-switch)** » devient alors utile : elle coupe tout trafic hors du tunnel

2 **Côté pfSense, assignez l'interface** du tunnel : « **Interfaces > Assignments** », ajoutez « **tun_wg0** » puis cliquez sur son nom (OPT1). Cochez « **Enable interface** », décrivez-la `WG_SIO`, choisissez « **Static IPv4** » avec **10.98.0.1/24** et un **MTU** de `1440`, puis « **Save** » et « **Apply Changes** » :

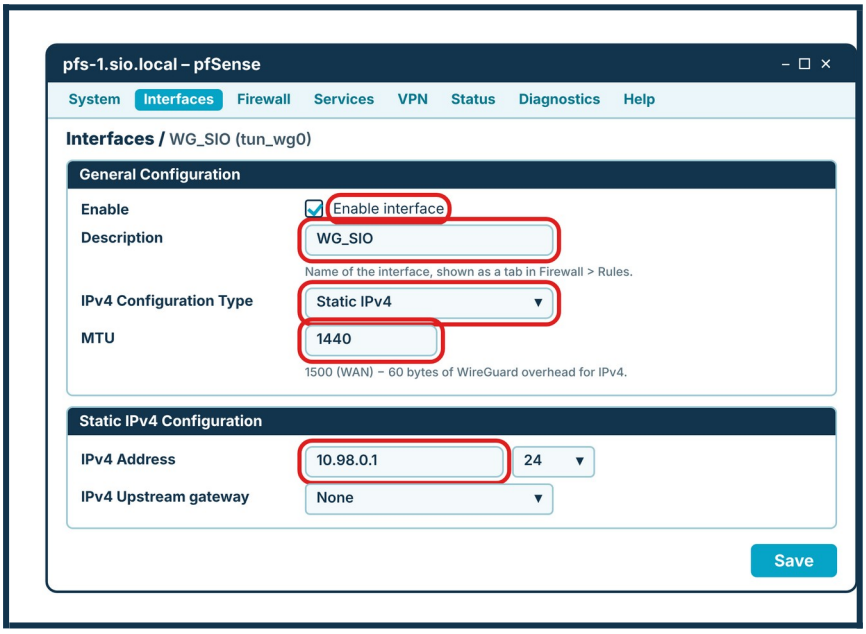


Figure 14 – Interfaces > WG_SIO : assigner le tunnel à une interface

À SAVOIR

L'assignation fait apparaître le tunnel comme une interface pfSense : elle permet au NAT sortant automatique de traduire les adresses du tunnel vers le WAN. Le **MTU 1440** correspond à un WAN de 1500 octets moins les 60 octets d'en-têtes de WireGuard (IPv4).

3 Ajoutez dans l'onglet « **WireGuard** » une règle qui autorise `10.98.0.0/24` vers « **Any** » sur les ports web (TCP 80 et 443) ; si le NAT sortant n'est pas en mode « **Automatic** » (« **Firewall > NAT > Outbound** »), ajoutez une règle pour la source `10.98.0.0/24` sur le WAN

Contrôlez le chemin des paquets depuis le poste : le premier saut doit être **l'adresse de pfSense dans le tunnel** :

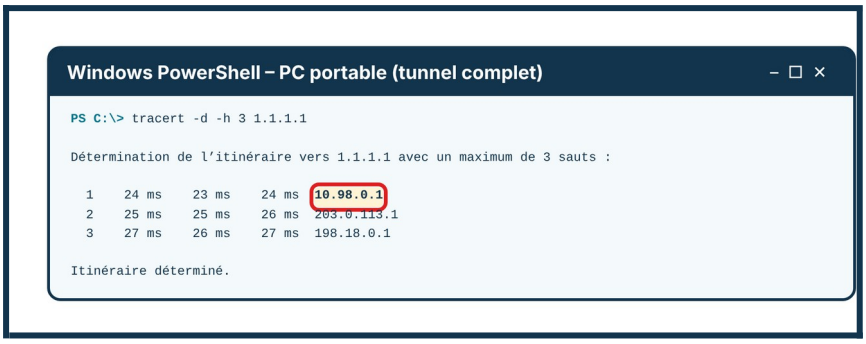


Figure 15 – PowerShell : tracert montre que le trafic passe par pfSense

À SAVOIR

Les adresses du deuxième et du troisième saut sont celles du fournisseur d'accès, données ici à titre d'exemple. Sans le premier saut en 10.98.0.1, le trafic ne passe pas par le tunnel : vérifiez « AllowedIPs ».

REMARQUE IMPORTANTE

Un tunnel complet transforme le **débit du WAN du lycée en goulot d'étranglement** pour tous les utilisateurs nomades, et le trafic web est vu par vos pare-feux. Dans « **System > Routing > Gateways** », veillez à ce que la passerelle par défaut soit bien celle du WAN : choisissez-la explicitement plutôt que « Automatic » dès qu'une interface WireGuard possède une passerelle.

D – Haute disponibilité : ce que la synchronisation ne copie pas

Avec le cluster, WireGuard demande une attention particulière : **la configuration du paquet n'est pas synchronisée automatiquement** vers le second nœud (contrairement aux règles de pare-feu et aux alias). Pour que le VPN survive à la panne de PFS-1, reproduisez la configuration sur **PFS-2** :

1. Installez le paquet **WireGuard** sur PFS-2 (étape 2, A) et activez-le (étape 2, B)
2. Sur PFS-1, dans « **Settings** », décochez momentanément « **Hide Secrets** », ouvrez le tunnel et copiez la **clé privée** ; sur PFS-2, créez un tunnel identique (même port, même adresse) en y **collant cette clé privée** : la clé publique obtenue doit être **la même** que sur PFS-1
3. Recréez **les mêmes pairs** (mêmes clés publiques, mêmes clés pré-partagées, mêmes adresses /32) puis recochez « **Hide Secrets** » sur les deux nœuds
4. Contrôlez que les règles du WAN et de l'onglet WireGuard sont bien présentes sur PFS-2 (elles, sont synchronisées)

À SAVOIR

Testez la bascule en **redémarrant ou en éteignant PFS-1**, pas seulement avec le mode maintenance CARP : dans ce mode, les réponses de WireGuard peuvent partir d'une autre adresse que l'adresse virtuelle, et le client les ignore. Après la bascule, le client reprend de lui-même (paquets de maintien) en quelques secondes à une minute ; si ce n'est pas le cas, comparez les clés publiques des deux nœuds.

✔ **POINT DE CONTRÔLE**

- Un appareil peut être **ajouté** et **retiré** (désactivation du pair) sans toucher aux autres
- Les droits d'**amartin** et de **bdurand** sont différenciés par **leur adresse** dans le tunnel
- PFS-2 possède **la même clé privée de tunnel** et les **mêmes pairs** que PFS-1
- Le VPN reprend après un **redémarrage de PFS-1**

Notre accès distant WireGuard est maintenant en service : chaque appareil est identifié par sa clé, ses droits sont réduits au strict nécessaire et la panne d'un pare-feu n'interrompt le service que quelques secondes. Gardez en tête sa limite principale : **la sécurité de l'accès repose sur la sécurité de l'appareil**, puisque aucun mot de passe n'est demandé.

Dépannage : les symptômes les plus fréquents

Symptôme	Cause probable	Solution
« Latest handshake » absent (aucune poignée de main), le client reste sans réponse	Les paquets UDP 51820 n'atteignent pas pfSense	Vérifier la règle WAN (adresse virtuelle, port 51820), le DNS de vpn.sio-ndlp.fr, la redirection du port derrière une box ; Diagnostics > Packet Capture sur le WAN (UDP 51820)
Les paquets arrivent sur le WAN mais aucune poignée de main	Clé publique du client ou du tunnel erronée (copie incomplète, tunnel recréé)	Comparer la clé publique affichée par le client avec celle du pair dans pfSense, et celle du tunnel avec le « PublicKey » du client
Aucune poignée de main alors que les clés sont identiques	Clés pré-partagées différentes (ou présente d'un seul côté)	Régénérer la clé pré-partagée dans pfSense et la recopier dans le client, ou la supprimer des deux côtés
Poignée de main correcte, mais aucun serveur ne répond	Règle de l'onglet WireGuard manquante, « AllowedIPs » du client sans 192.168.20.0/24, ou passerelle du serveur différente de pfSense	Contrôler les règles ; « AllowedIPs » ; `route print` sur le client ; la passerelle du serveur (192.168.20.254)
Le ping vers 10.98.0.1 répond, pas vers les serveurs	Règle ICMP manquante ou route du VLAN 20 absente du client	Ajouter la règle ICMP ; ajouter 192.168.20.0/24 dans « AllowedIPs »
Deux appareils qui s'excluent mutuellement	Même adresse /32 dans deux pairs, ou deux postes qui partagent la même clé	Une adresse /32 et une paire de clés **par appareil**
Les adresses IP répondent mais pas les noms	Ligne « DNS » absente ou règle DNS manquante	Ajouter « DNS = 192.168.20.250, 192.168.20.251, sio.local » ; vérifier la règle vers DC_SIO ; ipconfig /all
Certaines pages web ou transferts bloquent, d'autres fonctionnent	MTU trop élevé (paquets fragmentés)	Fixer le MTU de l'interface à 1440 (1420 si le WAN est en IPv6) et celui du client à 1420
Plus d'accès après une bascule CARP	Configuration absente de PFS-2, clé privée différente, mode maintenance CARP	Contrôler PFS-2 (tunnel, clé publique, pairs) ; tester avec un redémarrage de PFS-1

Pense-bête : où regarder

Où / commande	Utilité
Status > WireGuard (pfSense)	Poignée de main, adresse apprise et volumes pour chaque pair
wg show (SSH ou Diagnostics > Command Prompt)	Même information en ligne de commande, avec le port d'écoute et les clés publiques
VPN > WireGuard > Peers (pfSense)	Ajouter, désactiver ou supprimer un appareil
Firewall > Rules et Status > System Logs > Firewall	Règles WAN et WireGuard ; paquets bloqués
Diagnostics > Packet Capture (pfSense)	Capture sur le WAN (UDP 51820) ou sur le VLAN SERVEURS
Fenêtre du client : Latest handshake, Transfer	Dernière poignée de main et octets échangés, côté poste
Menu de l'icône WireGuard > View log	Journal du client : tentatives de poignée de main, erreurs de configuration
Test-NetConnection <serveur> -Port <port>	Teste un flux à travers le tunnel (client)
route print et ipconfig /all (client)	Routes ajoutées par le tunnel, serveurs DNS reçus