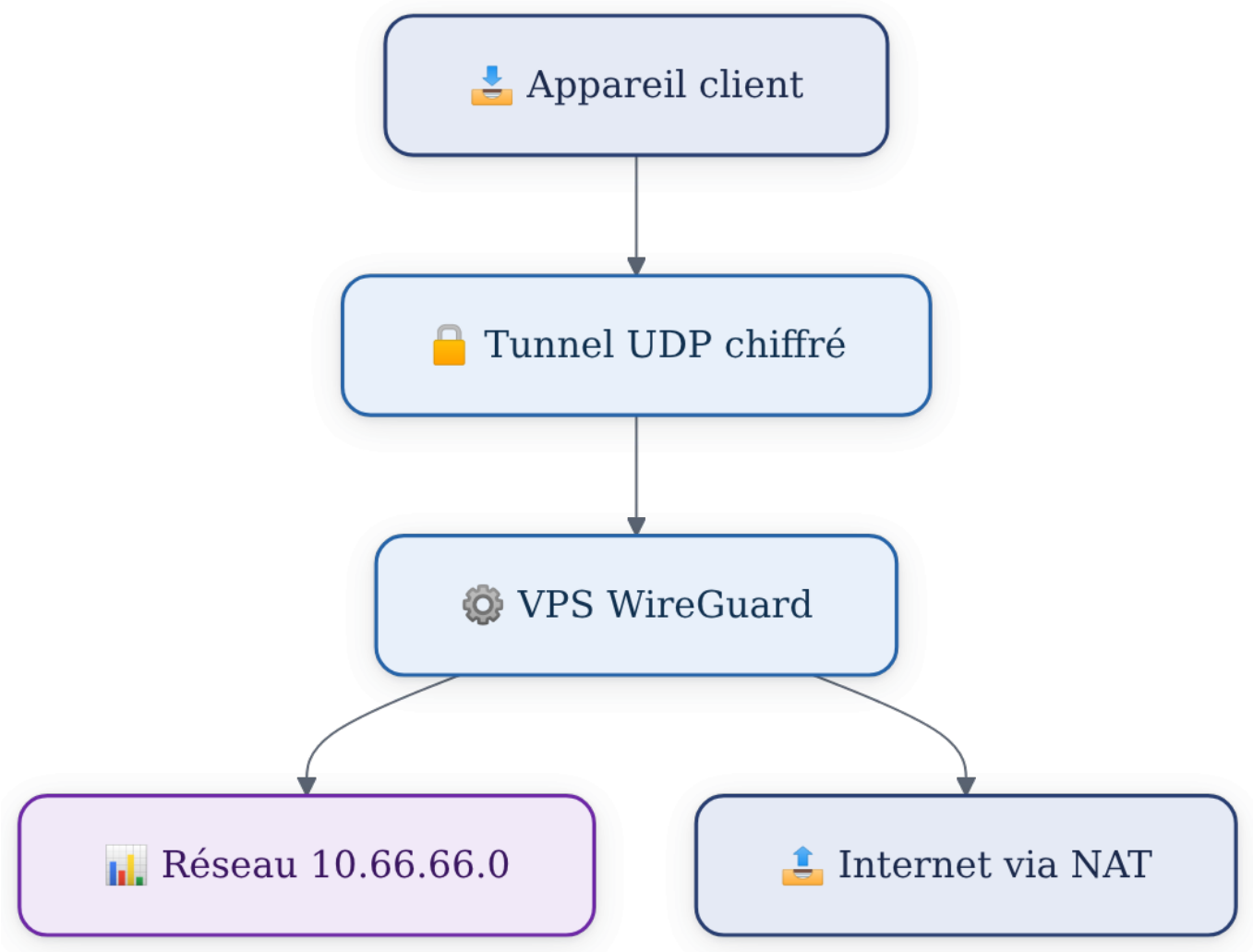
Votre checklist WireGuard sur VPS : du serveur au client vérifié

Préparez, configurez et contrôlez votre VPN personnel WireGuard sans oublier les points qui bloquent le plus souvent : clés, pare-feu, routage, NAT et DNS. Cochez chaque étape avant de considérer votre tunnel comme opérationnel.

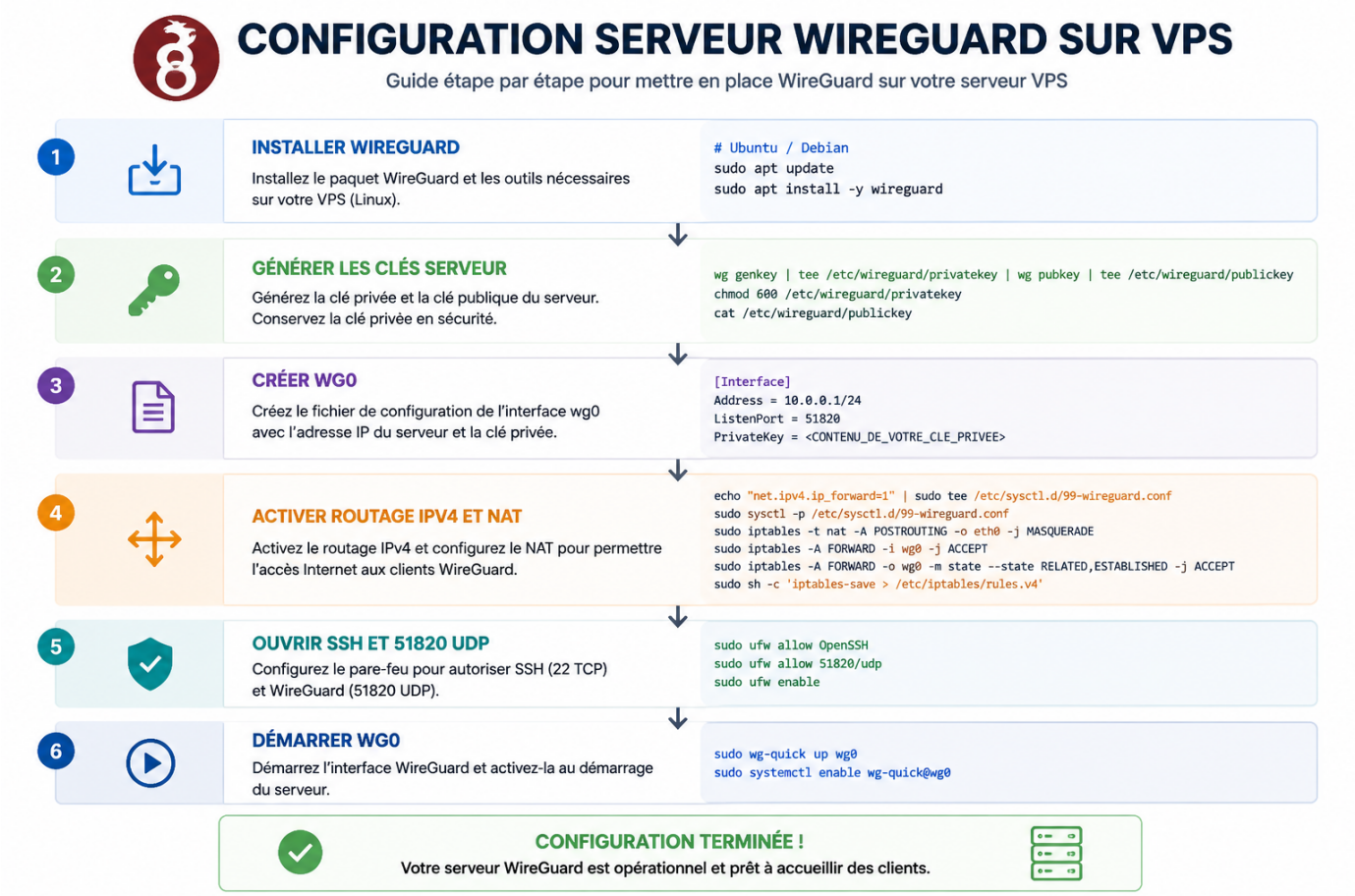
Au sommaire

1. Préparer le VPS sans vous couper l'accès

- [ ] **Mettre à jour le VPS Ubuntu ou Debian.**
  Prévoyez un redémarrage si les mises à jour installées le nécessitent.
- [ ] **Vérifier l'accès SSH administrateur ou sudo.**
- [ ] **Conserver une session SSH ouverte avant toute modification réseau.**
  Gardez aussi un accès de secours via la console du fournisseur de VPS.
- [ ] **Identifier l'interface Internet du VPS.**
  Relevez la route par défaut avec « ip route show default » et notez le nom après « dev ».
- [ ] **Choisir un sous-réseau VPN qui ne chevauche ni le réseau domestique ni un réseau professionnel.**
- [ ] **Installer le client WireGuard officiel sur chaque appareil à connecter.**



INFOGRAPHIE *Schéma WireGuard sur VPS montrant le tunnel VPN chiffré entre client et serveur*

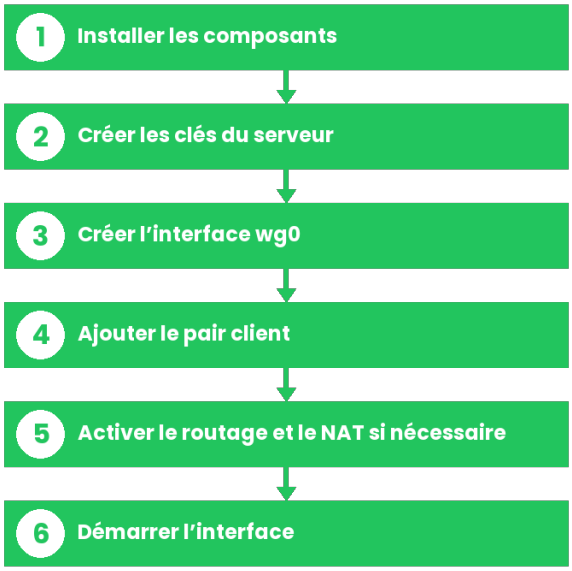


INFOGRAPHIE *Schéma de configuration WireGuard sur VPS, de l'installation au démarrage de l'interface wg0.*

2. Plan d'adressage à compléter

Élément	Valeur de référence	Contrôle à effectuer
Adresse VPN du serveur	10.66.66.1/24	Elle sert de passerelle au réseau WireGuard.
Adresse VPN du premier client	10.66.66.2/32	Elle doit être unique ; une adresse différente par appareil.
Port d'écoute	51820/UDP	Il doit être autorisé par tous les pare-feux concernés.
Interface de sortie Internet	eth0, ens3 ou autre	Utiliser le nom réellement trouvé sur le VPS, jamais une valeur supposée.

3. Configurer le serveur WireGuard



1 **Installer les composants**
Installez WireGuard et, si vous l'utilisez, UFW. Vérifiez ensuite que la commande « wg » est disponible avec « wg --version ».

2 **Créer les clés du serveur**
Générez une paire de clés dans /etc/wireguard. Protégez la clé privée avec des permissions restrictives et ne la copiez jamais hors du serveur.

3 **Créer l'interface wg0**
Renseignez l'adresse VPN du serveur, le port d'écoute et la clé privée réelle du serveur dans /etc/wireguard/wg0.conf.

4 **Ajouter le pair client**
Associez la clé publique du client à son adresse VPN autorisée. N'attribuez jamais la même adresse VPN à deux clients.

5 **Activer le routage et le NAT si nécessaire**
Le NAT est requis seulement si le client doit sortir sur Internet avec l'adresse IP publique du VPS. Utilisez l'interface Internet réellement identifiée.

6 **Démarrer l'interface**
Activez wg0 puis contrôlez son état avant de passer aux tests côté client.

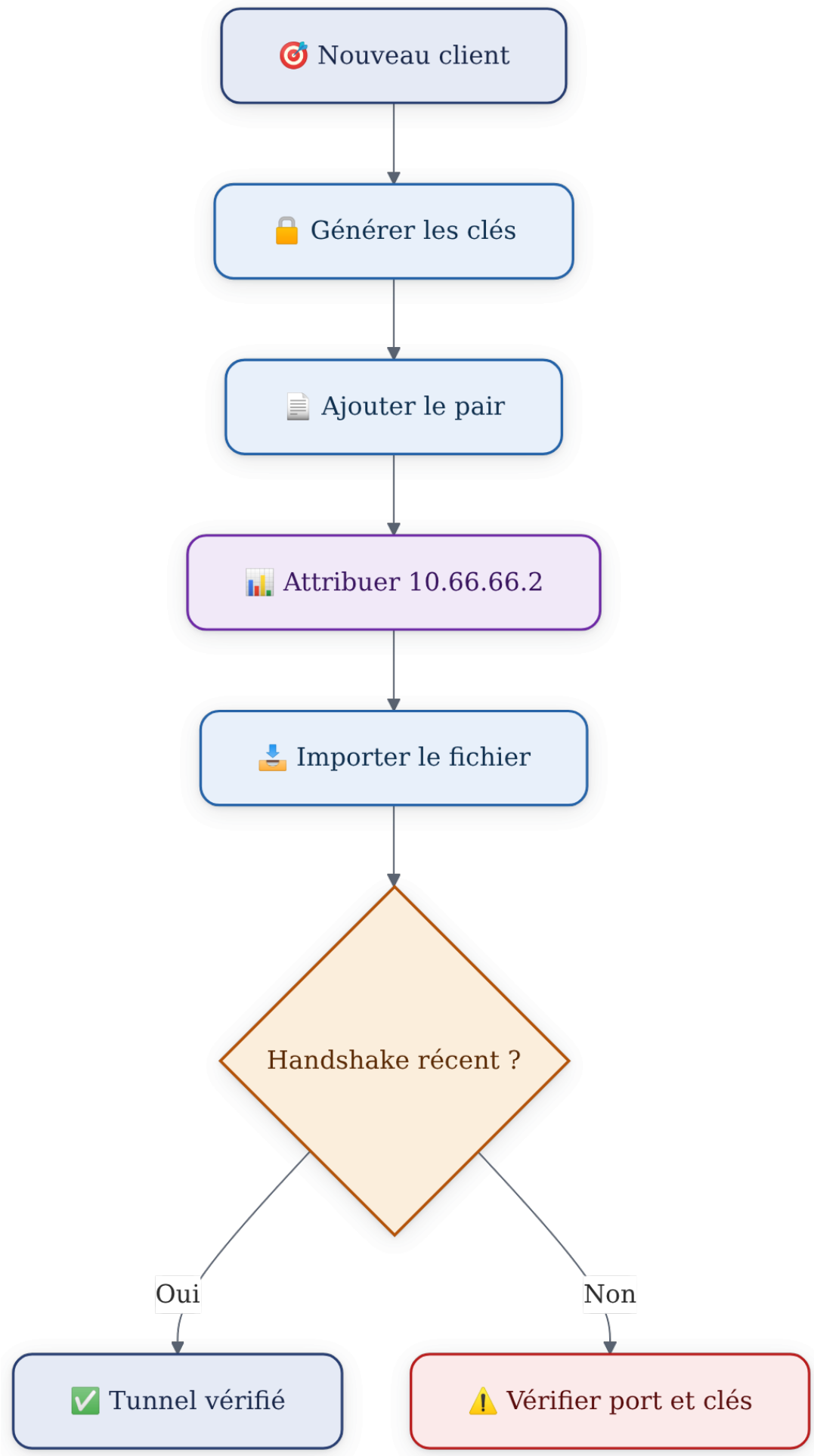

🎯 Nouveau client
🔒 Générer les clés
📄 Ajouter le pair
📊 Attribuer 10.66.66.2
📥 Importer le fichier
Handshake récent ?
Oui
Non
✅ Tunnel vérifié
⚠️ Vérifier port et clés

SCHÉMA *Repère visuel pour l'ajout et la vérification d'un client WireGuard.*

4. Ouvrir uniquement ce qui est nécessaire

- [ ] **Autoriser le port WireGuard en UDP sur le pare-feu du VPS.**
  Le port habituel indiqué dans cette configuration est 51820/UDP.
- [ ] **Autoriser le même port UDP dans le panneau réseau ou pare-feu cloud de l'hébergeur, s'il existe.**
- [ ] **Activer le transfert IPv4 si le trafic doit être routé via le VPS.**
- [ ] **Vérifier que les règles NAT utilisent la bonne interface de sortie Internet.**
- [ ] **Conserver un pare-feu restrictif et un accès SSH sécurisé par clé.**

5. Valider le tunnel, le trafic et la sortie DNS

- [ ] **Activer le tunnel depuis le client WireGuard.**
- [ ] **Contrôler qu'un handshake récent apparaît côté serveur.**
  Un tunnel affiché comme actif ne suffit pas à prouver que le trafic circule.
- [ ] **Vérifier que le client utilise bien son adresse VPN prévue.**
- [ ] **Tester le routage entre le client et l'adresse VPN du serveur.**
- [ ] **Vérifier l'accès Internet à travers le tunnel si tout le trafic doit passer par le VPS.**
- [ ] **Contrôler séparément la résolution DNS.**
  Un routage fonctionnel ne garantit pas à lui seul une sortie DNS correcte.
- [ ] **Confirmer que l'adresse IP de sortie correspond au VPS lorsque le trafic Internet est routé dans le tunnel.**

> ! **Les règles de sécurité à ne pas contourner**
> La clé privée ne quitte jamais l'appareil qui l'a générée ; seule la clé publique est partagée avec le pair distant. Un VPN personnel chiffre le trajet entre votre appareil et le VPS, mais ne vous rend pas anonyme et ne remplace ni les mises à jour ni la sécurisation du serveur.

Conservez les clés privées hors des captures d'écran, dépôts Git et échanges non sécurisés.