PROCÉDURE TECHNIQUE

Installation et Configuration du serveur VPN

Wireguard Client à site

Tables des matières

1. Objet et contexte

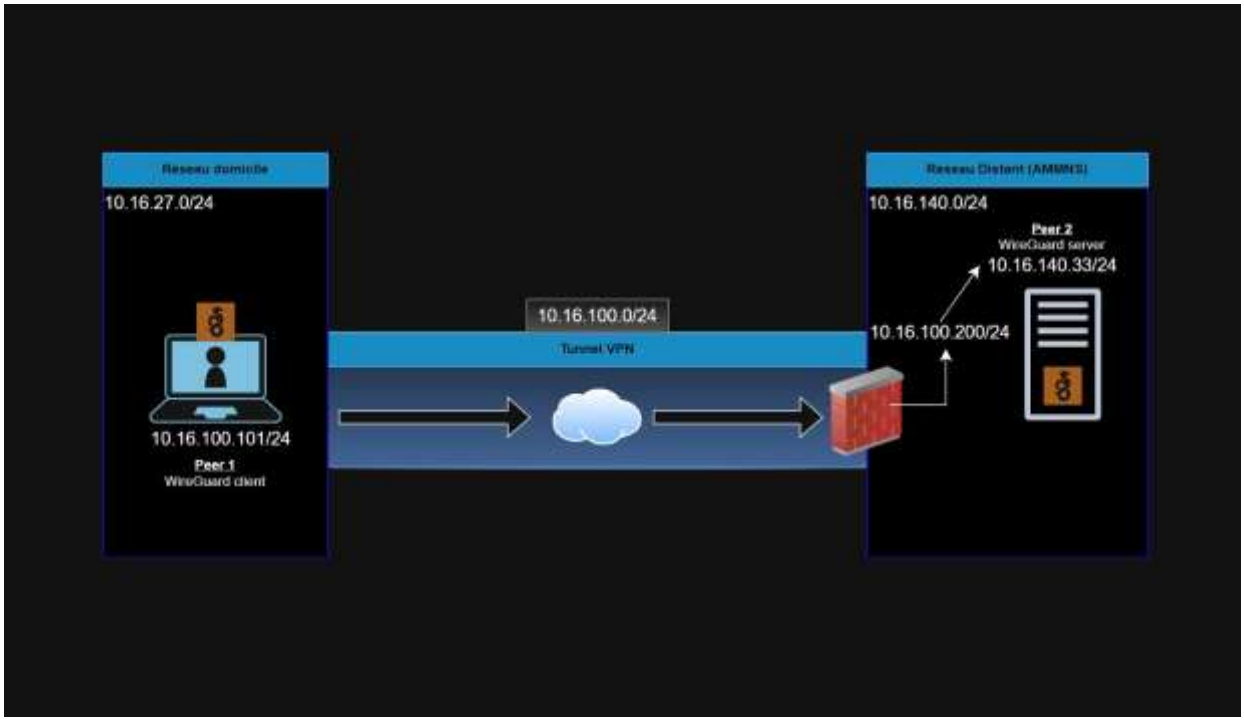
Un VPN (Virtual Private Network) permet de créer un tunnel sécurisé entre un poste distant et le réseau d'une entreprise à travers Internet. Dans cette réalisation professionnelle, la solution WireGuard a été utilisée afin de mettre en place un accès VPN client à site. Le serveur WireGuard est installé sur une machine Debian présente dans le réseau de l'entreprise, tandis que le client WireGuard est configuré sur un poste Windows distant. L'objectif est de permettre à l'utilisateur distant d'accéder aux ressources internes de manière sécurisée, sans exposer directement les services de l'entreprise sur Internet.

2. Principe d'un VPN client à site

Un VPN client à site relie un seul poste distant à un réseau d'entreprise. Le client établit une connexion vers un serveur VPN situé sur le site principal. Une fois le tunnel actif, le poste distant peut accéder aux ressources internes autorisées.

Élément	Rôle
Client WireGuard	Poste Windows distant qui initie la connexion VPN.
Serveur WireGuard	Serveur Debian qui écoute sur UDP 51820 et accepte le trafic autorisé.
Tunnel WireGuard	Lien chiffré entre le client Windows et le serveur Debian.
Réseau d'entreprise	Réseau interne contenant les serveurs, postes et services à protéger.

3. Architecture réseau utilisée



Élément	Adresse / réseau

Réseau domicile	10.16.27.0/24
Réseau entreprise	10.16.140.0/24
Réseau tunnel WireGuard	10.16.100.0/24
Client Windows dans le tunnel	10.16.100.101/24
Serveur Debian dans le tunnel	10.16.100.200/24
Interface LAN du serveur Debian	ens18
Adresse LAN du serveur Debian	10.16.140. 33
Port WireGuard	UDP 51820

4. Prérequis

Prérequis	Détail
Serveur Debian	Debian 13.1.0 avec accès administrateur (root)
Client Windows	Client WireGuard installé et configuré.
Accès réseau	Le serveur Debian doit être joignable depuis le pare-feu principal.
Pare-feu principal	Possibilité de rediriger le port UDP 51820 vers le serveur Debian.
Informations nécessaires	Clé publique du serveur, clé publique du client, adresse IP publique du site.

5. Installation de WireGuard sur Debian

Se connecter au serveur Debian avec un compte administrateur, puis mettre à jour les dépôts et installer les paquets nécessaires.

```
apt update
apt install -y wireguard wireguard-tools ufw tcpdump
```

Limiter les permissions du dossier crée.

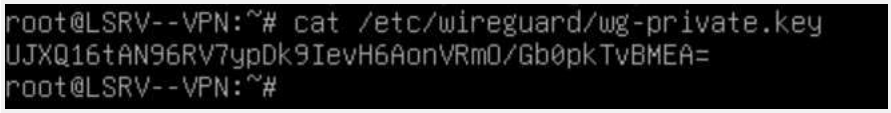
```
chmod 700 /etc/wireguard
```

Le paquet tcpdump est installé afin de faciliter le diagnostic si le tunnel ne s'établit pas.

6. Génération des clés WireGuard

WireGuard utilise une clé privée et une clé publique pour chaque pair. La clé privée reste toujours sur la machine qui l'a générée. La clé publique est échangée avec l'autre pair. wg genkey | tee /etc/wireguard/wg-private.key | wg pubkey | tee /etc/wireguard/wg-public.key

Afficher la clé publique du serveur Debian :



cat /etc/wireguard/wg-public.key

Sécuriser les fichiers de clés :

```
chmod 600 /etc/wireguard/wg-private.key chmod
644 /etc/wireguard/wg-public.key
```

7. Configuration du serveur WireGuard

Créer ou modifier le fichier de configuration du tunnel WireGuard.

```
nano /etc/wireguard/wg0.conf
```

Exemple de configuration côté serveur Debian :

```
[Interface]
Address = 10.16.100.200/24
ListenPort = 51820
PrivateKey = <clé_privée_serveur>
SaveConfig = true

[Peer]
PublicKey = <clé_publique_client_windows> AllowedIPs = 10.16.100.101/32
```

Démarrer le tunnel WireGuard :

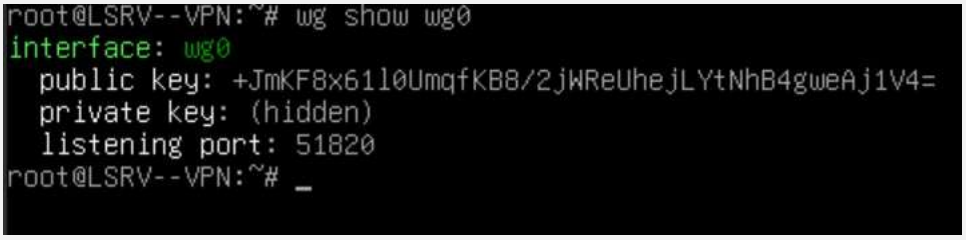
```
wg-quick up wg0
```

Activer le démarrage automatique au boot :

```
systemctl enable wg-quick@wg0
```

Vérifier l'état du tunnel :

```
wg show
```



8. Activation du routage IP

Pour que le serveur Debian puisse transférer les paquets entre le réseau VPN et le réseau LAN, l'IP forwarding doit être activé.

```
tee /etc/sysctl.d/99-wireguard-forward.conf >/dev/null <<'EOF' net.ipv4.ip_forward=1
net.ipv6.conf.all.forwarding=1 EOF
```

Appliquer la configuration :

```
sysctl --system
```

Contrôler que le routage IPv4 est actif :

```
sysctl net.ipv4.ip_forward
```

Résultat attendu :

```
net.ipv4.ip_forward = 1
```

9. Configuration du pare-feu UFW

9.1 Autoriser les ports nécessaires

Autoriser SSH afin de conserver l'accès d'administration au serveur, puis autoriser WireGuard sur le port UDP 51820.

```
ufw allow 22/tcp ufw
allow 51820/udp
```

9.2 Autoriser le forwarding dans UFW

Modifier la politique de forwarding par défaut d'UFW.

```
nano /etc/default/ufw
```

Remplacer la ligne suivante :

```
DEFAULT_FORWARD_POLICY="DROP"
```

par :

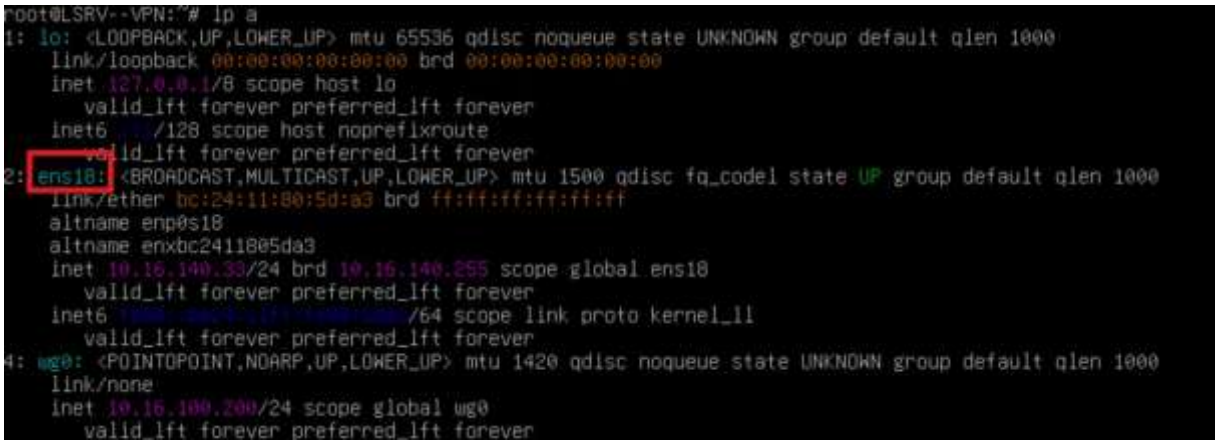
```
DEFAULT_FORWARD_POLICY="ACCEPT"
```

9.3 Ajouter le NAT dans UFW

Modifier le fichier before.rules afin de masquer les adresses du réseau VPN lors de l'accès au LAN de l'entreprise.

```
nano /etc/ufw/before.rules
```

Ajouter les lignes suivantes au début du fichier, avant la section *filter :




```
*nat
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 10.16.100.0/24 -o ens18 -j MASQUERADE COMMIT
```

9.4 Autoriser les flux entre le VPN et le LAN

Dans le même fichier /etc/ufw/before.rules, ajouter les règles de forwarding suivantes dans la section filter, avant les règles de rejet :

```
-A ufw-before-forward -i wg0 -o ens18 -s 10.16.100.0/24 -d 10.16.140.0/24 -j ACCEPT
-A ufw-before-forward -i ens18 -o wg0 -s 10.16.140.0/24 -d 10.16.100.0/24 -j ACCEPT
```

Activer ou recharger UFW :

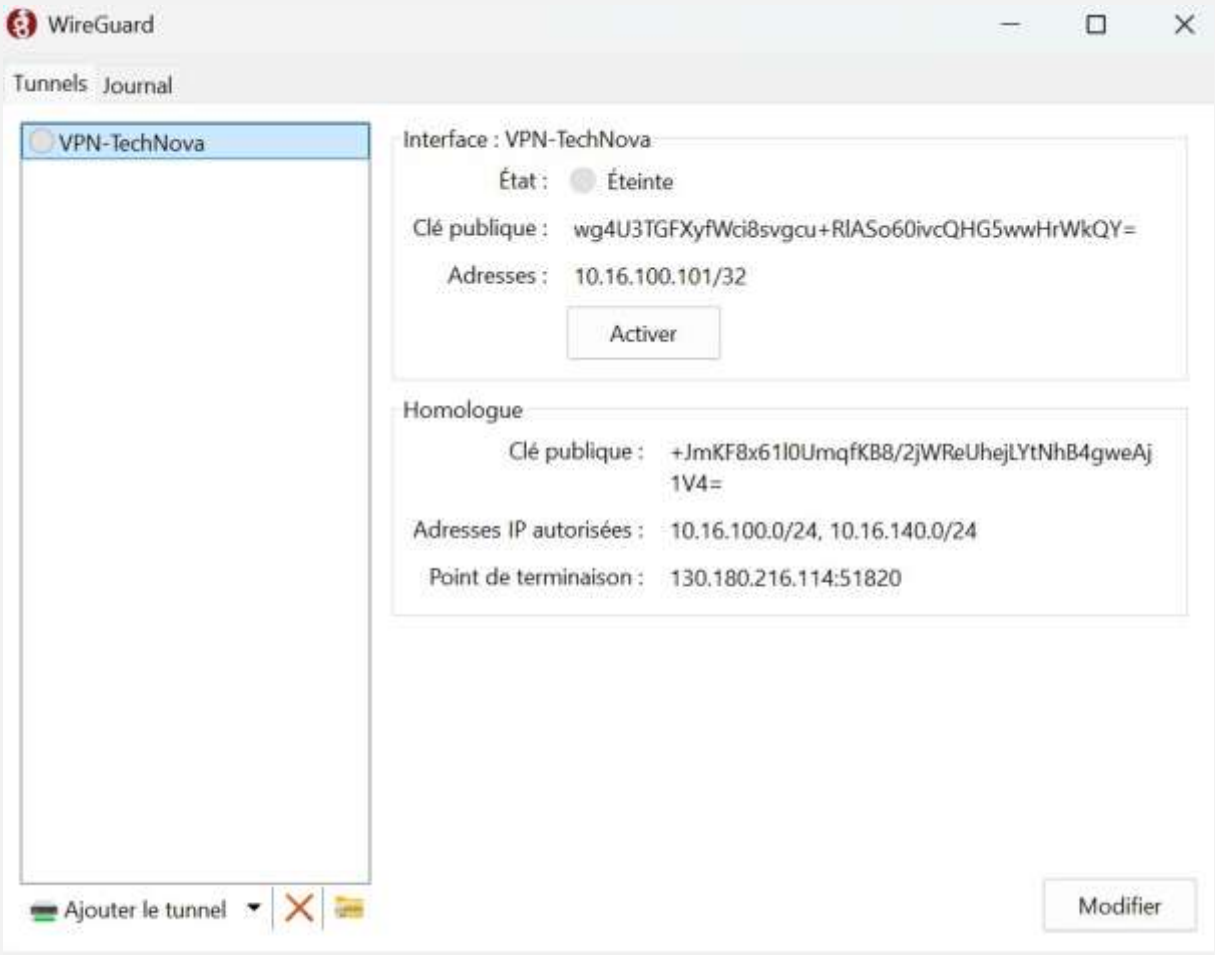
```
ufw enable ufw
reload ufw status
verbose
```

10. Configuration du client WireGuard Windows

Sur le poste Windows, installer le client WireGuard, puis créer un nouveau tunnel. Le client génère automatiquement sa clé privée et sa clé publique. La clé publique du client doit être copiée dans la configuration du serveur Debian.

```
[Interface]
PrivateKey = <clé_privée_client_windows>
Address = 10.16.100.101/24
DNS = 10.16.140.10

[Peer]
PublicKey = <clé_publique_serveur_debian>
AllowedIPs = 10.16.100.0/24, 10.16.140.0/24
Endpoint = <IP_publique_firewall>:51820
PersistentKeepalive = 25
```



Paramètre	Explication
PrivateKey	Clé privée du client Windows. Elle ne doit pas être partagée.
Address	Adresse IP du client dans le tunnel VPN.
DNS	Serveur DNS interne à utiliser si la résolution de noms de l'entreprise est nécessaire. À adapter.
PublicKey	Clé publique du serveur Debian WireGuard.
AllowedIPs	Réseaux qui doivent passer dans le tunnel VPN.
Endpoint	Adresse IP publique du site principal et port UDP 51820.
PersistentKeepalive	Maintient la session active si le client est derrière un NAT.

NB : Le port d'écoute affiché sur le client Windows peut être différent de 51820. C'est normal : WireGuard Windows utilise souvent un port local aléatoire. Le port important est le port serveur UDP 51820.

11. Configuration du pare-feu principal

Le pare-feu principal doit autoriser le trafic entrant UDP 51820 depuis Internet et le rediriger vers l'adresse LAN du serveur Debian.

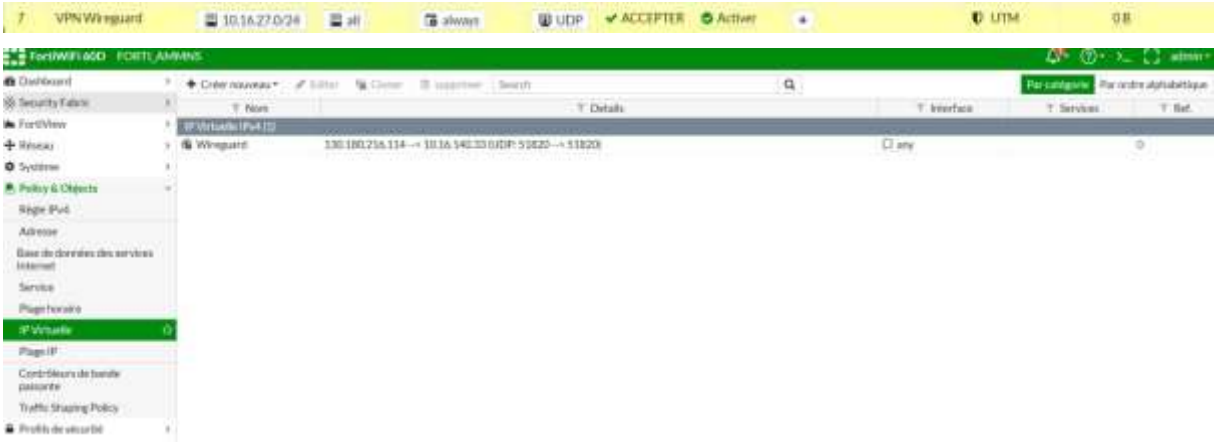
Paramètre	Valeur
Protocole	UDP
Port WAN	51820
Destination LAN	10.16.140.33:51820
Interface concernée	WAN vers LAN

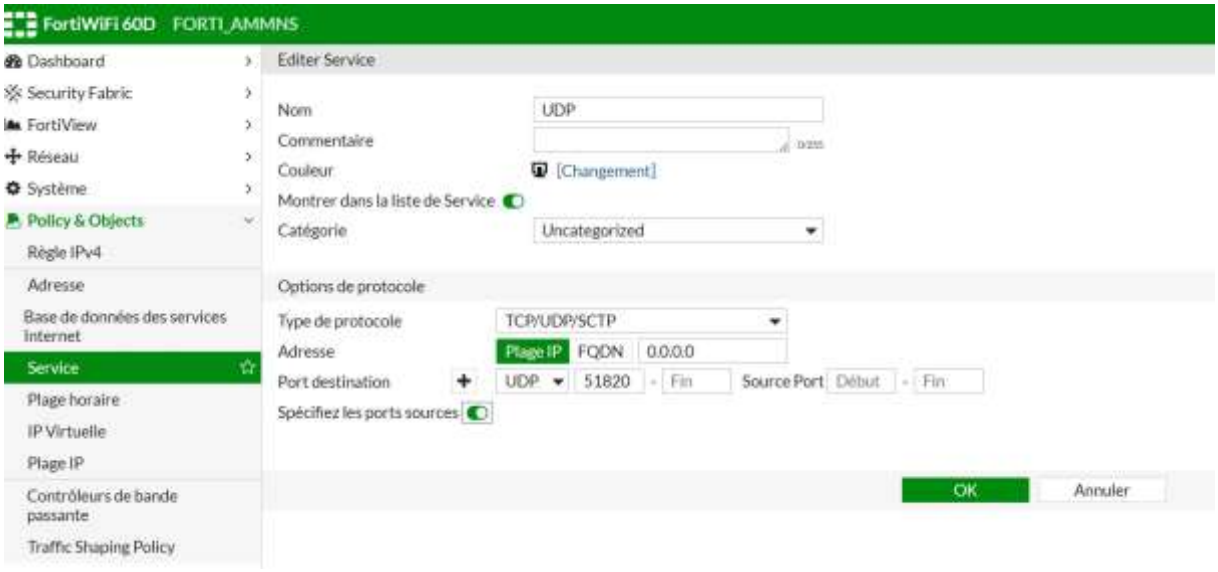
```
WAN UDP 51820  ->  10.16.140.60:51820
```

11.1 Route statique de retour

Deux modes sont possibles pour le retour des paquets depuis le réseau LAN vers le réseau VPN :

Mode	Principe	Route statique nécessaire ?
Mode NAT / MASQUERADE	Le serveur Debian masque les clients VPN derrière son adresse LAN.	non.
Mode routé sans NAT	Les serveurs du LAN voient directement les IP VPN 10.16.100.x.	Oui, vers le serveur Debian.





Si le mode routé sans NAT est retenu, ajouter sur le routeur ou le pare-feu principal :

```
Destination : 10.16.100.0/24
Passerelle : 10.16.140.60
```

12. Tests de validation

12.1 Vérifier que WireGuard écoute sur Debian

```
ss -ulnp | grep 51820
```

Résultat attendu : une ligne doit indiquer que le serveur écoute sur le port UDP 51820.

12.2 Vérifier l'état du tunnel

```
wg show
```

Lorsque le client Windows est connecté, un latest handshake doit apparaître. Cette ligne confirme que le tunnel s'est établi.

12.3 Tester depuis le client Windows

```
ping 10.16.100.200 ping
10.16.140.60 ping
10.16.140.X
```

Le premier ping teste l'interface WireGuard du serveur. Les pings suivants testent l'accès au réseau d'entreprise.

13. Dépannage du tunnel VPN

Si le tunnel ne s'établit pas, il faut procéder par étapes afin d'identifier si le problème vient du client Windows, de WireGuard, d'UFW ou du pare-feu principal.

Symptôme	Cause probable	Vérification	Correction

Aucun handshake	Le client n'atteint pas le serveur ou les clés sont incorrectes.	wg show et tcpdump sur ens18.	Vérifier NAT, endpoint, clés publiques et port UDP 51820.
Le client envoie mais ne reçoit rien	Le serveur ne reçoit pas les paquets ou ne répond pas.	Compteurs WireGuard et tcpdump.	Vérifier redirection NAT et règles du pare-feu principal.
Handshake OK mais LAN inaccessible	Forwarding, NAT UFW ou AllowedIPs incorrects.	sysctl, before.rules, config Windows.	Corriger IP forwarding, MASQUERADE et AllowedIPs.
Ping VPN OK mais pas LAN	Retour des paquets impossible.	Tester depuis plusieurs hôtes LAN.	Vérifier NAT ou route statique de retour.

13.1 Vérifier le service et le port d'écoute

```
systemctl status wg-quick@wg0 ss -
ulnp | grep 51820
```

Si aucune ligne n'apparaît avec 51820, redémarrer le tunnel :

```
systemctl restart wg-quick@wg0
```

13.2 Vérifier la configuration WireGuard

```
cat /etc/wireguard/wg0.conf
```

Les points à contrôler sont :

la clé publique du client Windows dans la section [Peer] du serveur ; la clé publique du serveur dans la section [Peer] du client Windows ; l'adresse VPN du client 10.16.100.101/24 ; les AllowedIPs côté client : 10.16.100.0/24 et 10.16.140.0/24 ; l'Endpoint : <IP_publique_firewall>:51820.

13.3 Vérifier si les paquets arrivent sur Debian

L'interface LAN du serveur Debian est ens18. Il faut donc écouter le trafic WireGuard sur cette interface.

```
tcpdump -i ens18 udp port 51820
```

Activer ensuite le tunnel WireGuard depuis Windows.

Résultat tcpdump	Interprétation
Des paquets apparaissent	Le client atteint bien le serveur Debian. Le problème se situe alors dans WireGuard, les clés, UFW ou AllowedIPs.
0 packets captured	Les paquets n'arrivent pas au serveur Debian. Le problème se situe avant Debian : NAT, ACL, routeur ou pare-feu principal.

13.4 Vérifier le NAT du pare-feu principal

Sur un équipement Cisco, les commandes suivantes permettent de vérifier les translations NAT et la configuration associée :

```
show ip nat translations show
running-config | include nat
```

Si aucune translation liée au port 51820 n'apparaît lorsque le client tente de se connecter, la redirection NAT ne fonctionne pas ou le flux est bloqué avant d'atteindre le serveur Debian.

13.5 Vérifier UFW

```
ufw status verbose ufw
reload
```

Vérifier que le port UDP 51820 est autorisé, que le forwarding est accepté et que la règle MASQUERADE utilise bien l'interface ens18.

14. Sécurisation et bonnes pratiques

- Ne jamais publier les clés privées dans une documentation ou une capture d'écran.
- Limiter les ports ouverts sur le serveur Debian au strict nécessaire.
- Mettre à jour régulièrement Debian et WireGuard.
- Créer une paire de clés différente pour chaque client VPN.
- Supprimer la clé publique d'un client qui n'est plus autorisé à se connecter.
- Documenter l'adresse IP, les AllowedIPs et le nom de chaque client déclaré.
- Vérifier régulièrement les journaux système et l'état du service WireGuard.
- Appliquer des permissions restrictives au fichier de configuration :

```
chmod 600 /etc/wireguard/wg0.conf chmod
700 /etc/wireguard
```

Conclusion : La configuration WireGuard est validée lorsque le client Windows obtient un handshake, peut joindre 10.16.100.200 et accède aux ressources autorisées du réseau 10.16.140.0/24. En cas d'échec, tcpdump permet de savoir rapidement si les paquets atteignent le serveur Debian ou si le problème se situe sur le pare-feu principal.