Configuration Serveurs

Serveur OVH

```
# ================================================================================
# WireGuard — VPS OVH (Hub du mesh)
# IP WireGuard : 10.0.0.1/24
# Rôle : hub + exit node OVH + Portainer UI + entrée private-only (10.0.0.40)
# ================================================================================
#
#   - Les LAN (192.168.1.0/24 et 192.168.2.0/24) ne font pas parti des AllowedIPs
#     des peers serveurs. OVH ne "connaît" plus les LAN des sites physiques.
#   - La politique FORWARD passe à DROP par défaut : seul le trafic
#     explicitement autorisé est routé. Tout le reste est silencieusement jeté.
#   - Conséquence : un client connecté à OVH ne peut PAS atteindre
#     192.168.1.x ou 192.168.2.x, même s'il connaît l'adresse.
#
# PRÉREQUIS :
#   - Port UDP 51820 ouvert dans le firewall OVH ET dans UFW
#   - Vérifier le nom de l'interface réseau : ip link show
#     (peut être eth0, ens3, ens4, enp1s0 selon le VPS)
#   - ip_forward activé au niveau hôte (fait par le script UFW)
#
# ================================================================================

[Interface]
Address    = 10.0.0.1/24
ListenPort = 51820
PrivateKey = <CLE_PRIVEE_OVH>

# ================================================================================
# PEER : Serveur Marseille
# ================================================================================
[Peer]
PublicKey = <CLE_PUBLIQUE_MRS>
Endpoint  = <IP_PUBLIQUE_MRS>:51820
```

```
#   10.0.0.2/32   → IP WireGuard de MRS (mesh)
#   10.0.0.20/32  → client mrs-exitnode : son trafic retour repasse par MRS
#   10.0.0.41/32  → client private-only entré via MRS : retour via MRS
# Pas de 192.168.1.0/24 : OVH ne route jamais vers le LAN de Marseille.
AllowedIPs          = 10.0.0.2/32, 10.0.0.20/32, 10.0.0.41/32
PersistentKeepalive = 25


# ================================================================================
# PEER : Serveur Albi
# ================================================================================
[Peer]
PublicKey = <CLE_PUBLIQUE_ALBI>
Endpoint  = <IP_PUBLIQUE_ALBI>:51820

#   10.0.0.3/32   → IP WireGuard d'Albi (mesh)
#   10.0.0.30/32  → client albi-exitnode : retour via Albi
#   10.0.0.42/32  → client private-only entré via Albi : retour via Albi
AllowedIPs          = 10.0.0.3/32, 10.0.0.30/32, 10.0.0.42/32
PersistentKeepalive = 25


# ================================================================================
# PEER : Client ovh-exitnode
# Tout le trafic internet sort par OVH. IP publique = VPS OVH.
# ================================================================================
[Peer]
PublicKey  = <CLE_PUBLIQUE_CLIENT_OVH_1>
AllowedIPs = 10.0.0.10/32


# ================================================================================
# PEER : Client private-only entré via OVH
# ================================================================================
[Peer]
PublicKey  = <CLE_PUBLIQUE_CLIENT_PRIVATE_OVH>
AllowedIPs = 10.0.0.40/32
```

Serveur Marseille

```
# ================================================================================
# WireGuard — Serveur physique Marseille (Spoke)
# IP WireGuard : 10.0.0.2/24
# LAN local    : 192.168.1.0/24
# Rôle         : exit node MRS (+ accès LAN MRS) + Portainer Agent
#                + entrée private-only (10.0.0.41) + sauvegardes P2P avec Albi
# ================================================================================
#
# ACCÈS AU LAN 192.168.1.0/24 :
#   Autorisé UNIQUEMENT au client mrs-exitnode (10.0.0.20) via UFW.
#   Voir ufw/marseille-ufw-setup.sh pour les règles de filtrage.
#
#   Tout autre peer (OVH, Marseille, clients exit-MRS, private-only…)
#   est bloqué par le Pare-feu.
#
# PRÉREQUIS SUR LA BOX :
#   1. Port forwarding UDP 51820 → 192.168.1.100 (IP locale du serveur)
#
# ================================================================================

[Interface]
Address    = 10.0.0.2/24
ListenPort = 51820
PrivateKey = <CLE_PRIVEE_ALBI>



# ================================================================================
# PEER : VPS OVH
# ================================================================================
[Peer]
PublicKey = <CLE_PUBLIQUE_OVH>
Endpoint  = <IP_PUBLIQUE_OVH>:51820

# Destinations routées VERS OVH depuis Marseille :
#   10.0.0.1/32   → IP WireGuard d'OVH (mesh, Portainer UI)
#   10.0.0.10/32  → client ovh-exitnode : retour via OVH
#   10.0.0.40/32  → client private-only entré via OVH : retour via OVH
AllowedIPs          = 10.0.0.1/32, 10.0.0.10/32, 10.0.0.40/32
PersistentKeepalive = 25
```

```
# ================================================================================
# PEER : Serveur Albi (tunnel P2P direct — sauvegardes sans passer par OVH)
# ================================================================================
[Peer]
PublicKey = <CLE_PUBLIQUE_ALBI>
Endpoint  = <IP_PUBLIQUE_ALBI>:51820

# Destinations routées VERS Albi :
#   10.0.0.3/32   → IP WireGuard d'Albi (sauvegardes rsync/SSH)
#   10.0.0.30/32  → client albi-exitnode (symétrie mesh)
#   10.0.0.42/32  → client private-only entré via Albi
# Pas de 192.168.2.0/24 : MRS ne route jamais vers le LAN d'Albi.
AllowedIPs          = 10.0.0.3/32, 10.0.0.30/32, 10.0.0.42/32
PersistentKeepalive = 25



# ================================================================================
# PEER : Client mrs-exitnode (IP publique = MRS, accès LAN MRS)
# ================================================================================
[Peer]
PublicKey  = <CLE_PUBLIQUE_CLIENT_MRS>
AllowedIPs = 10.0.0.20/32



# ================================================================================
# PEER : Client private-only entré via MRS
# ================================================================================
[Peer]
PublicKey  = <CLE_PUBLIQUE_CLIENT_PRIVATE_MRS>
AllowedIPs = 10.0.0.41/32
```

Serveur Albi

```
# ================================================================================
# WireGuard — Serveur physique Albi (Spoke)
# IP WireGuard : 10.0.0.3/24
# Interface physique : enp2s0
# LAN local : 192.168.2.0/24
# Rôle : exit node Albi (+ accès LAN Albi) + Portainer Agent
```

```
#        + entrée private-only (10.0.0.42) + sauvegardes P2P avec MRS
# ================================================================================
#
# COHABITATION AVEC HOME ASSISTANT / FRIGATE :
#   WireGuard tourne en network_mode: host, comme Home Assistant.
#   Aucun conflit : plusieurs conteneurs peuvent partager la pile réseau
#   de l'hôte. Le filtrage FORWARD posé par UFW n'affecte pas la
#   communication HA <-> Frigate (trafic local ou géré par Docker),
#   il ne filtre que le trafic VPN routé.
#
# ACCÈS AU LAN 192.168.2.0/24 :
#   Autorisé UNIQUEMENT au client albi-exitnode (10.0.0.30) via UFW.
#
# PRÉREQUIS BOX ALBI :
#   - Port forwarding UDP 51820 → 192.168.2.100 (IP locale du serveur)
#
# ================================================================================

[Interface]
Address    = 10.0.0.3/24
ListenPort = 51820
PrivateKey = <CLE_PRIVEE_ALBI>



# ================================================================================
# PEER : VPS OVH
# ================================================================================
[Peer]
PublicKey = <CLE_PUBLIQUE_OVH>
Endpoint  = <IP_PUBLIQUE_OVH>:51820

#   10.0.0.1/32   → IP WireGuard d'OVH
#   10.0.0.10/32  → client ovh-exitnode : retour via OVH
#   10.0.0.40/32  → client private-only entré via OVH
AllowedIPs          = 10.0.0.1/32, 10.0.0.10/32, 10.0.0.40/32
PersistentKeepalive = 25



# ================================================================================
# PEER : Serveur Marseille (tunnel P2P direct)
```

```
# ================================================================================
[Peer]
PublicKey = <CLE_PUBLIQUE_MRS>
Endpoint  = <IP_PUBLIQUE_MRS>:51820

#   10.0.0.2/32   → IP WireGuard de MRS (sauvegardes)
#   10.0.0.20/32  → client mrs-exitnode (symétrie mesh)
#   10.0.0.41/32  → client private-only entré via MRS
# Pas de 192.168.1.0/24 : Albi ne route jamais vers le LAN de Marseille.
AllowedIPs          = 10.0.0.2/32, 10.0.0.20/32, 10.0.0.41/32
PersistentKeepalive = 25



# ================================================================================
# PEER : Client albi-exitnode (IP publique = Albi, accès LAN Albi)
# ================================================================================
[Peer]
PublicKey  = <CLE_PUBLIQUE_CLIENT_ALBI>
AllowedIPs = 10.0.0.30/32



# ================================================================================
# PEER : Client private-only entré via Albi
# ================================================================================
[Peer]
PublicKey  = <CLE_PUBLIQUE_CLIENT_PRIVATE_ALBI>
AllowedIPs = 10.0.0.42/32
```

Revision #3
Created 29 May 2026 13:46:30 by gpatruno
Updated 5 June 2026 09:11:20 by gpatruno