FR

SÉRIE STACK OPNSENSE — BILLET 3

WireGuard VPN et failover LTE avec OPNsense

Accès distant et résilience réseau

Mars 2026

Table des matières

Article complet : blog.botum.ca/opnsense-wireguard-vpn-sdwan-lte

1. Pourquoi WireGuard plutôt qu'OpenVPN en 2026 ?

J'utilise WireGuard depuis qu'OPNsense l'a intégré nativement au kernel en version 21.7. Sur mon infra BOTUM, la comparaison avec OpenVPN est sans appel :

• **Performance :** WireGuard tourne dans le kernel Linux/BSD — 3 à 5× plus rapide qu'OpenVPN user-space.

• **Latence :** Handshake en ~100ms contre 1-2 secondes pour TLS OpenVPN.

• **Code :** 4 000 lignes vs 70 000+ pour OpenVPN — surface d'attaque minimale.

• **Cryptographie moderne :** ChaCha20, Poly1305, Curve25519 — pas de négociation fragile.

• **Roaming :** Changement d'IP transparent (parfait pour les remote workers sur mobile).

• **Config simplifiée :** Un fichier plat, une clé publique/privée, c'est tout.

2. Prérequis

Ce billet est la suite directe des billets 1 et 2 de la série :

• **Billet 1** : OPNsense installé dans Proxmox — voir le guide

• **Billet 2** : VLANs et Zero Trust configurés — voir le guide

• OPNsense 24.x fonctionnel avec accès WebUI

• VLANs configurés (Work, IoT, Guest, DMZ)

• Adresse IP publique ou DNS dynamique (pour le serveur WireGuard)

• Port UDP 51820 ouvert en entrée sur le WAN

• Pour LTE failover : clé USB 4G/5G reconnue par OPNsense (ex: Huawei E3372)

3. Installer le plugin WireGuard dans OPNsense

```
# WebUI : System > Firmware > Plugins
# Chercher : os-wireguard
# Cliquer [+] pour installer

# Après installation, reboot OPNsense :
# Power > Reboot

# Vérification post-reboot :
# VPN > WireGuard doit apparaître dans le menu
```

■ *Sur mon infra BOTUM, le plugin est inclus par défaut depuis OPNsense 24.1.*

4. Tunnel WireGuard site-à-site (bureau ↔ datacenter)

4.1 Générer les clés sur les deux nœuds

```
# Sur NOEUD A (bureau) :
wg genkey | tee /tmp/nodeA.private | wg pubkey > /tmp/nodeA.public
cat /tmp/nodeA.private   # → noter la clé privée
cat /tmp/nodeA.public    # → partager avec le nœud B

# Sur NOEUD B (datacenter) :
wg genkey | tee /tmp/nodeB.private | wg pubkey > /tmp/nodeB.public
```

```
cat /tmp/nodeB.private
cat /tmp/nodeB.public    # → partager avec le nœud A
```

4.2 Configurer le serveur WireGuard (Nœud A)

```
# VPN > WireGuard > Local > Add
# Name: wg-site-a-site
# Public key: (auto-générée ou coller la clé publique du nœud A)
# Private key: (clé privée nœud A)
# Listen port: 51820
# Tunnel address: 10.10.0.1/24
# DNS server: 10.10.0.1
# Save

# VPN > WireGuard > Peers > Add
# Name: datacenter-nodeB
# Public key: (clé publique du nœud B)
# Endpoint: IP_PUBLIQUE_NODEB:51820
# Allowed IPs: 10.10.0.0/24, 192.168.20.0/24
# Save
```

4.3 Activer l'interface WireGuard

```
# Interfaces > Assignments > Add
# Network port: wg0 (WireGuard)
# Description: WG_SITE2SITE
# Save & Apply

# Interfaces > WG_SITE2SITE
# Enable: ✓
# IPv4: 10.10.0.1/24
# Save & Apply

# Firewall > Rules > WG_SITE2SITE
# Action: Pass | Source: WG_SITE2SITE net | Destination: any
# Save & Apply Changes
```

5. Accès remote worker (client mobile)

Pour les télétravailleurs sur mon infra BOTUM, chaque device a sa propre paire de clés. Pas de clé partagée — chaque révocation est granulaire.

```
# VPN > WireGuard > Peers > Add
# Name: remote-worker-alice
# Public key: (clé publique du device d'Alice)
# Allowed IPs: 10.10.1.2/32  ← IP dédiée à Alice
# Keep alive: 25

# Sur le mobile Alice (app WireGuard iOS/Android) :
# Interface :
#   Private key: (clé privée générée sur le mobile)
#   Address: 10.10.1.2/32
#   DNS: 10.10.0.1

# Peer (serveur OPNsense) :
#   Public key: (clé publique du nœud OPNsense)
#   Endpoint: MON_IP_PUBLIQUE:51820
#   Allowed IPs: 0.0.0.0/0  ← full tunnel (tout le trafic via VPN)
```

```
#   Persistent keepalive: 25
```

■ *Générer un QR code depuis l'interface OPNsense : VPN > WireGuard > Peers > icône QR. Alice scanne avec l'app mobile.*

6. SD-WAN : configurer le failover LTE automatique

Sur mon infra BOTUM, la clé 4G/5G est branchée en USB sur le nœud Proxmox hébergeant OPNsense. OPNsense la voit comme une interface WAN secondaire.

6.1 Vérifier la reconnaissance de la clé USB

```
# Dans OPNsense WebUI :
# System > Diagnostics > Shell
ifconfig -a | grep -i usb
# ou
dmesg | grep -i "ue0\|umb\|cdce\|urndis"
# La clé apparaît généralement comme ue0 (RNDIS) ou umb0 (CDC-NCM)
```

6.2 Configurer WAN2 (LTE)

```
# Interfaces > Assignments
# Ajouter ue0 (ou l'interface LTE détectée)
# Description: WAN2_LTE
# Save

# Interfaces > WAN2_LTE
# Enable: ✓
# IPv4 Configuration: DHCP  (la clé fournit son propre IP via le réseau opérateur)
# Block private networks: ✓
# Save & Apply
```

6.3 Créer le Gateway Group pour failover

```
# System > Gateways > Configuration
# Vérifier que WAN_DHCP (tier 1) et WAN2_LTE_DHCP (tier 2) sont présents

# System > Gateways > Groups > Add
# Group Name: WAN_FAILOVER
# Gateway Priority:
#   WAN_DHCP → Tier 1 (prioritaire)
#   WAN2_LTE_DHCP → Tier 2 (backup)
# Trigger level: Packet Loss or High Latency
# Description: Failover LTE automatique
# Save

# Firewall > Rules > LAN
# Modifier la règle "Default LAN to any"
# Gateway: WAN_FAILOVER  ← changer de Default à WAN_FAILOVER
# Save & Apply Changes
```

■ *Le monitoring de gateway est automatique. OPNsense envoie des pings vers 8.8.8.8 et 8.8.4.4 par gateway. Si WAN1 échoue, le trafic bascule sur WAN2_LTE en ~30 secondes.*

7. Tester le basculement WAN → LTE

```
# Terminal (depuis un client sur le LAN) :
# Lancer un ping continu avant de couper le WAN :
ping -t 8.8.8.8   # (Windows) ou ping 8.8.8.8 (Linux/Mac)
```

```
# Simuler la coupure WAN :
# Interfaces > WAN > Edit > Uncheck "Enable"
# Save & Apply Changes

# Observer :
# - Quelques paquets perdus (~30s de basculement)
# - Le ping reprend via WAN2_LTE
# - System > Gateways : WAN_DHCP = offline, WAN2_LTE_DHCP = online

# Vérifier l'IP publique :
curl -s ifconfig.me  # Doit retourner l'IP de votre opérateur LTE

# Restaurer WAN :
# Interfaces > WAN > Edit > Re-enable
# Le trafic revient sur WAN1 automatiquement
```

8. Prochaines étapes

WireGuard est en place et le failover LTE protège votre connectivité. La suite de la série :

• **Billet 4 :** WiFi par VLAN — APs, SSIDs segmentés, 802.1Q trunking

• **Billet 5 :** CrowdSec + fail2ban — IDS/IPS collaboratif, protection SSH

• **Billet 6 :** Monitoring & alertes — Uptime Kuma, Grafana, métriques réseau

---

Article complet : blog.botum.ca/opnsense-wireguard-vpn-sdwan-lte

Site : www.botum.ca • contact@botum.ca