EN

OPNSENSE ENTERPRISE STACK — POST 3

WireGuard VPN and LTE Failover with OPNsense

Remote Access and Network Resilience

March 2026

Table of Contents

Full article: blog.botum.ca/opnsense-wireguard-vpn-sdwan-lte-failover

1. Why WireGuard Over OpenVPN in 2026?

I've been using WireGuard since OPNsense integrated it natively into the kernel in version 21.7. On my BOTUM infrastructure, the comparison with OpenVPN is clear:

- **Performance:** WireGuard runs in the Linux/BSD kernel — 3 to 5× faster than OpenVPN user-space.
- **Latency:** Handshake in ~100ms vs 1-2 seconds for OpenVPN TLS.
- **Code:** 4,000 lines vs 70,000+ for OpenVPN — minimal attack surface.
- **Modern cryptography:** ChaCha20, Poly1305, Curve25519 — no fragile negotiation.
- **Roaming:** Transparent IP change (perfect for remote workers on mobile).
- **Simple config:** One flat file, one public/private key pair — that's it.

2. Prerequisites

This post is the direct continuation of Posts 1 and 2 in the series:

- **Post 1:** OPNsense installed in Proxmox — see the guide
- **Post 2:** VLANs and Zero Trust configured — see the guide

- OPNsense 24.x running with WebUI access
- VLANs configured (Work, IoT, Guest, DMZ)
- Public IP or dynamic DNS (for the WireGuard server)
- UDP port 51820 open inbound on WAN
- For LTE failover: 4G/5G USB dongle recognized by OPNsense (e.g. Huawei E3372)

3. Install the WireGuard Plugin in OPNsense

```
# WebUI: System > Firmware > Plugins
# Search: os-wireguard
# Click [+] to install

# After installation, reboot OPNsense:
# Power > Reboot

# Post-reboot verification:
# VPN > WireGuard should appear in the menu
```

■ *On my BOTUM infrastructure, the plugin is included by default since OPNsense 24.1.*

4. WireGuard Site-to-Site Tunnel (Office ↔ Datacenter)

4.1 Generate Keys on Both Nodes

```
# On NODE A (office):
wg genkey | tee /tmp/nodeA.private | wg pubkey > /tmp/nodeA.public
cat /tmp/nodeA.private   # → note the private key
cat /tmp/nodeA.public    # → share with node B

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

```
cat /tmp/nodeB.private
cat /tmp/nodeB.public    # → share with node A
```

4.2 Configure the WireGuard Server (Node A)

```
# VPN > WireGuard > Local > Add
# Name: wg-site-a-site
# Public key: (auto-generated or paste Node A public key)
# Private key: (Node A private key)
# 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: (Node B public key)
# Endpoint: NODE_B_PUBLIC_IP:51820
# Allowed IPs: 10.10.0.0/24, 192.168.20.0/24
# Save
```

4.3 Activate the WireGuard Interface

```
# 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. Remote Worker Access (Mobile Client)

For remote workers on my BOTUM infrastructure, each device has its own key pair. No shared keys — each revocation is granular.

```
# VPN > WireGuard > Peers > Add
# Name: remote-worker-alice
# Public key: (Alice's device public key)
# Allowed IPs: 10.10.1.2/32  ← dedicated IP for Alice
# Keep alive: 25

# On Alice's mobile (WireGuard iOS/Android app):
# Interface:
#   Private key: (private key generated on mobile)
#   Address: 10.10.1.2/32
#   DNS: 10.10.0.1

# Peer (OPNsense server):
#   Public key: (OPNsense node public key)
#   Endpoint: MY_PUBLIC_IP:51820
#   Allowed IPs: 0.0.0.0/0  ← full tunnel (all traffic via VPN)
```

```
#   Persistent keepalive: 25
```

■ *Generate a QR code from the OPNsense interface: VPN > WireGuard > Peers > QR icon. Alice scans with the mobile app.*

6. SD-WAN: Configure Automatic LTE Failover

On my BOTUM infrastructure, the 4G/5G dongle is plugged into USB on the Proxmox node hosting OPNsense. OPNsense sees it as a secondary WAN interface.

6.1 Verify USB Dongle Recognition

```
# In OPNsense WebUI:
# System > Diagnostics > Shell
ifconfig -a | grep -i usb
# or
dmesg | grep -i "ue0\|umb\|cdce\|urndis"
# Dongle typically appears as ue0 (RNDIS) or umb0 (CDC-NCM)
```

6.2 Configure WAN2 (LTE)

```
# Interfaces > Assignments
# Add ue0 (or detected LTE interface)
# Description: WAN2_LTE
# Save

# Interfaces > WAN2_LTE
# Enable: ✓
# IPv4 Configuration: DHCP  (dongle provides IP via carrier network)
# Block private networks: ✓
# Save & Apply
```

6.3 Create Gateway Group for Failover

```
# System > Gateways > Configuration
# Verify WAN_DHCP (tier 1) and WAN2_LTE_DHCP (tier 2) are present

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

# Firewall > Rules > LAN
# Edit "Default LAN to any" rule
# Gateway: WAN_FAILOVER  ← change from Default to WAN_FAILOVER
# Save & Apply Changes
```

■ *Gateway monitoring is automatic. OPNsense sends pings to 8.8.8.8 and 8.8.4.4 per gateway. If WAN1 fails, traffic switches to WAN2_LTE in ~30 seconds.*

7. Test WAN → LTE Failover

```
# Terminal (from a LAN client):
# Start continuous ping before cutting WAN:
ping -t 8.8.8.8   # (Windows) or ping 8.8.8.8 (Linux/Mac)
```

```
# Simulate WAN outage:
# Interfaces > WAN > Edit > Uncheck "Enable"
# Save & Apply Changes

# Observe:
# - A few dropped packets (~30s switchover)
# - Ping resumes via WAN2_LTE
# - System > Gateways: WAN_DHCP = offline, WAN2_LTE_DHCP = online

# Verify public IP:
curl -s ifconfig.me  # Should return your LTE carrier IP

# Restore WAN:
# Interfaces > WAN > Edit > Re-enable
# Traffic automatically returns to WAN1
```

8. Next Steps

WireGuard is in place and LTE failover protects your connectivity. The rest of the series:

- **Post 4:** WiFi by VLAN — APs, segmented SSIDs, 802.1Q trunking
- **Post 5:** CrowdSec + fail2ban — collaborative IDS/IPS, SSH protection
- **Post 6:** Monitoring & alerts — Uptime Kuma, Grafana, network metrics

---

Full article: blog.botum.ca/opnsense-wireguard-vpn-sdwan-lte-failover

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