FR

Guide Pratique

Stack Securite Enterprise

OPNsense + WireGuard + WiFi + LTE

dans Proxmox

Firewall enterprise self-hosted complet -- zero trust + VPN + IDS/IPS

Mars 2026

Sommaire

Introduction : Pourquoi cette stack en 2026 ?

Sur mon infra BOTUM, j'ai centralise toute la securite reseau dans une seule VM OPNsense tournant sur Proxmox. Le resultat : un firewall enterprise-grade qui gere simultanement les VLANs, le VPN WireGuard, le failover LTE, la gestion WiFi par VLAN, et la protection collaborative CrowdSec -- le tout pour moins de $300 en materiel.

Ce guide documente l'architecture complete que j'utilise pour isoler les reseaux IoT, Work, Guest et DMZ, avec des regles Zero Trust inter-VLAN et un IDS/IPS collaboratif.

---

1. Pourquoi OPNsense plutot que pfSense en 2026 ?

La question revient souvent dans les forums homelab. Voici pourquoi j'ai choisi OPNsense :

- Interface moderne : OPNsense utilise Bootstrap/Vue.js, pfSense reste sur une UI vieillissante.

- WireGuard natif : integre dans le kernel depuis OPNsense 21.7, zero plugin tiers.

- Mises a jour transparentes : updates hebdomadaires, pfSense CE est beaucoup plus lent.

- CrowdSec plugin officiel : IDS/IPS collaboratif disponible directement dans les plugins.

- Open Source complet : BSD 2-Clause, sans version Community degradee.

2. Prerequis : Proxmox, ressources VM

Architecture cible

```
Proxmox (hyperviseur bare-metal)
+-- VM OPNsense (firewall + router)
    +-- WireGuard  -> VPN site-a-site + remote workers
    +-- WiFi       -> gestion APs + SSID par VLAN (IoT/Work/Guest)
    +-- SD-WAN     -> failover LTE automatique (cle 4G/5G backup WAN)
    +-- VLANs      -> IoT / Management / Production / DMZ
    +-- Zero Trust -> regles inter-VLAN "never trust, always verify"
    +-- CrowdSec   -> IDS/IPS collaboratif + bouncer
    +-- fail2ban   -> protection SSH + services exposes
```

Ressources VM recommandees

- CPU : 2-4 vCPUs (4 recommandes pour CrowdSec + IDS actif)

- RAM : 4 Go minimum, 8 Go ideal

- Stockage : 32 Go SSD systeme + logs separes

- NICs : 2 interfaces min (WAN + LAN), 3 ideal (WAN + LAN + DMZ)

- Proxmox 8.x recommande (kernel 6.x pour perfs WireGuard)

Astuce : Utilisez VirtIO pour les NICs VM. Les perfs sont 3x superieures aux interfaces emulees.

3. Installer OPNsense dans une VM Proxmox

Etape 1 : Telecharger l'ISO

```
wget https://mirror.dns-root.de/opnsense/releases/24.7/OPNsense-24.7-dvd-amd64.iso.bz2
bzip2 -d OPNsense-24.7-dvd-amd64.iso.bz2
sha256sum OPNsense-24.7-dvd-amd64.iso
```

Etape 2 : Creer la VM

```
qm create 100 \
  --name opnsense-fw \
  --memory 4096 --cores 2 \
  --net0 virtio,bridge=vmbr0 \
  --net1 virtio,bridge=vmbr1 \
  --ide2 local:iso/OPNsense-24.7-dvd-amd64.iso,media=cdrom \
  --scsi0 local-lvm:32 \
  --boot order=ide2 \
  --ostype other
```

Etape 3 : Installation

1. Booter sur l'ISO, login : installer / opnsense
2. Choisir Install (UFS)
3. Selectionner le disque vtbd0
4. Finaliser et rebooter, retirer l'ISO
5. Assigner les interfaces : WAN = vtnet0, LAN = vtnet1

4. Configuration des VLANs

VLAN 10 - IoT : Cameras, thermostats. Acces Internet uniquement, zero acces aux autres VLANs

VLAN 20 - Work : Postes et serveurs. Acces complet aux services internes

VLAN 30 - Guest : WiFi invites. Internet uniquement, DNS filtre, debit limite

VLAN 40 - DMZ : Services exposes. Acces entrant uniquement

```
# Interfaces > Other Types > VLAN
# VLAN IoT : Tag 10 sur LAN (em1)
# VLAN Work : Tag 20 sur LAN (em1)
# VLAN Guest : Tag 30 sur LAN (em1)
# VLAN DMZ : Tag 40 sur LAN (em1)

# DHCP par VLAN
# IoT  : 10.10.10.100-200, GW 10.10.10.1
# Work : 10.20.20.100-200, GW 10.20.20.1
# Guest: 10.30.30.100-200, GW 10.30.30.1, DNS 1.1.1.3
# DMZ  : 10.40.40.10-50,  GW 10.40.40.1
```

5. Regles Zero Trust inter-VLAN

```
# IoT : bloquer tout acces au LAN interne
Action : Block | Source : VLAN_IoT | Destination : RFC1918
Description : ZT - IoT isole

# IoT : autoriser Internet
Action : Pass | Source : VLAN_IoT | Destination : any

# Work -> DMZ (services)
Action : Pass | Source : VLAN_Work | Destination : VLAN_DMZ | Ports : 443, 8080

# Work ne voit pas IoT
Action : Block | Source : VLAN_Work | Destination : VLAN_IoT
```

Regle d'or : bloquer RFC1918 entier en priorite, puis ouvrir les exceptions specifiques.

6. WireGuard : VPN site-a-site + acces remote

```
# VPN > WireGuard > Instances > Add (Serveur)
Name         : wg0-remote-access
Listen Port  : 51820
Tunnel Addr  : 10.100.0.1/24
DNS          : 10.20.20.1

# Pair site-a-site
Name       : site-b
Public Key : <cle-publique-site-B>
AllowedIPs : 10.200.0.0/24
Endpoint   : vpn.site-b.exemple.com:51820
Keepalive  : 25

# Client Linux (remote worker) : /etc/wireguard/wg0.conf
[Interface]
PrivateKey = <cle-privee-client>
Address    = 10.100.0.10/32
DNS        = 10.20.20.1

[Peer]
PublicKey           = <cle-publique-serveur>
Endpoint            = vpn.votre-domaine.com:51820
AllowedIPs          = 10.0.0.0/8
PersistentKeepalive = 25

sudo wg-quick up wg0
```

7. Gestion WiFi : APs + SSIDs par VLAN

```
# SSID Work : VLAN 20, WPA3/WPA2, 5 GHz
# SSID IoT  : VLAN 10, WPA2-PSK, 2.4 GHz
# SSID Guest: VLAN 30, WPA2-PSK, 2.4/5 GHz, limite 20 Mbps

# Trunk VLAN switch : port OPNsense + port APs
# Mode trunk (VLANs 10, 20, 30 tagges)
```

8. SD-WAN avec failover LTE automatique

```
# Interfaces > Assignments : ajouter interface LTE (ue0)
# Name : LTE_BACKUP | Type : DHCP | MTU : 1500

# System > Gateways > Gateway Groups
Name          : WAN_FAILOVER_GROUP
Gateway WAN   : WAN_DHCP     (tier 1)
Gateway LTE   : LTE_BACKUP   (tier 2)
Trigger Level : Packet Loss or High Latency

# Route par defaut vers le groupe
Network : 0.0.0.0/0 | Gateway : WAN_FAILOVER_GROUP
```

Certains FAI LTE bloquent les connexions entrantes. Le failover LTE est ideal pour le trafic sortant.

9. CrowdSec bouncer OPNsense

```
# System > Firmware > Plugins > os-crowdsec
cscli bouncers add opnsense-bouncer
cscli decisions list
cscli alerts list --limit 20

# Collections recommandees
cscli collections install crowdsecurity/linux
cscli collections install crowdsecurity/sshd
cscli collections install crowdsecurity/nginx
service crowdsec restart
```

CrowdSec bloque en moyenne 5 000 a 50 000 IPs malveillantes selon votre exposition.

10. fail2ban sur les services derriere OPNsense

```
sudo apt install -y fail2ban
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

# jail.local - [DEFAULT]
bantime  = 3600   # 1 heure
findtime = 600    # 10 min
maxretry = 5

# [sshd]
enabled = true | port = 22 | maxretry = 3

# [nginx-http-auth]
enabled = true | logpath = /var/log/nginx/error.log

sudo systemctl restart fail2ban
sudo fail2ban-client status
```

11. Tests et validation

```
# Test isolation VLAN (depuis IoT vers Work)
ping -c 3 10.20.20.1   # Attendu : timeout

# Test failover LTE : deconnecter WAN -> basculement < 30s
ping -i 0.5 8.8.8.8

# Test WireGuard
wg show
ping -c 3 10.20.20.1   # depuis client VPN

# Test CrowdSec
cscli decisions list --type ban
```

12. Prochaines etapes

- Suricata (IDS inline) en complement de CrowdSec pour l'inspection DPI
- HAProxy pour le load balancing des services DMZ
- RADIUS server (FreeRADIUS) pour l'auth WiFi 802.1X
- Supervision Prometheus + Grafana (metriques OPNsense via SNMP)
- Backups config OPNsense vers S3/Minio automatises
- OPNsense HA avec CARP pour zero downtime

Article complet : https://blog.botum.ca/opnsense-stack-securite-enterprise-proxmox/

Ce guide PDF : Guide PDF OPNsense Stack Securite