FR

Guide Pratique

VLANs et Zero Trust avec OPNsense

Configuration complete : 4 VLANs, regles firewall, DHCP

Mars 2026

Sommaire

1. Pourquoi les VLANs ? Securite par segmentation

Un reseau plat (flat network) ou tous les appareils coexistent sur le meme segment est une bombe a retardement securitaire. Un seul appareil compromise (camera IoT, TV connectee, PC invite) peut potentiellement atteindre tous les autres.

Les VLANs (Virtual Local Area Networks) permettent de segmenter logiquement votre reseau physique en plusieurs zones isolees, chacune avec ses propres regles d'acces.

• Isolation des appareils IoT — une camera hackee ne peut pas atteindre vos serveurs

• Protection des invites — le reseau Guest ne voit pas votre reseau interne

• DMZ pour les services publics — les serveurs exposes sont isoles du LAN

• Zero Trust inter-VLAN — tout trafic entre zones est refuse par defaut

• Audit simplifie — vous savez exactement quel trafic circule ou

i Prerequis : avoir suivi Billet 1 — OPNsense installe et operationnel dans Proxmox.

2. Prerequis : OPNsense installe + switch manageable

Avant de configurer les VLANs, verifiez que vous disposez de :

• OPNsense installe et operationnel (voir Billet 1 de la serie)

• Un switch manageable supportant le 802.1Q (VLAN tagging)

• Recommande : TP-Link TL-SG108E (~$30) — parfait pour un homelab

• Alternatif : Netgear GS308E, UniFi USW-Flex-Mini

• Acces administrateur a l'interface web OPNsense (http://192.168.1.1)

• Au moins 2 interfaces reseau sur la VM OPNsense (WAN + LAN)

• Interface LAN sur un bridge Proxmox avec "VLAN aware" active

```
# Verifier que vmbr1 est VLAN aware dans Proxmox
# System > Network > vmbr1 > VLAN aware : Yes

# Ou via CLI :
cat /etc/network/interfaces | grep -A5 'vmbr1'
# Doit contenir : bridge-vlan-aware yes
```

3. Creer les VLANs dans OPNsense

3.1 Creer les interfaces VLAN

Dans OPNsense, les VLANs sont crees comme des sous-interfaces sur l'interface LAN existante.

```
# Interface > Other Types > VLAN
# Cliquer "+" pour ajouter chaque VLAN

VLAN 10 — IoT :
  Parent Interface : vtnet1 (votre LAN)
  VLAN Tag         : 10
  Description      : VLAN_IoT

VLAN 20 — Work :
  Parent Interface : vtnet1
  VLAN Tag         : 20
  Description      : VLAN_Work

VLAN 30 — Guest :
  Parent Interface : vtnet1
  VLAN Tag         : 30
  Description      : VLAN_Guest

VLAN 40 — DMZ :
  Parent Interface : vtnet1
  VLAN Tag         : 40
  Description      : VLAN_DMZ
```

3.2 Assigner les interfaces

Apres creation des VLANs, il faut les assigner comme interfaces OPNsense :

```
# Interfaces > Assignments
# Cliquer "+" pour chaque VLAN cree :

OPT1 → vtnet1.10  (IoT)   → renommer : "IoT"
OPT2 → vtnet1.20  (Work)  → renommer : "Work"
OPT3 → vtnet1.30  (Guest) → renommer : "Guest"
OPT4 → vtnet1.40  (DMZ)   → renommer : "DMZ"

# Pour chaque interface assignee :
# Interfaces > [Nom] > Enable Interface : Yes
# IPv4 Configuration Type : Static
# IPv4 Address : voir section 4
```

4. Configurer les 4 VLANs

VLAN 10 — IoT (192.168.10.0/24)

```
# Interfaces > IoT
Enable    : Yes
IPv4 Addr : 192.168.10.1/24
Description : IoT — Appareils connectes (cameras, TV, thermostats)

# Usage :
# Internet uniquement — acces au LAN et aux autres VLANs REFUSE
# DNS filtre (bloquer domaines de tracking IoT recommande)
```

VLAN 20 — Work (192.168.20.0/24)

```
# Interfaces > Work
Enable    : Yes
IPv4 Addr : 192.168.20.1/24
Description : Work — Postes de travail et serveurs internes

# Usage :
# Acces complet aux services internes
# Acces Internet complet
# Acces LAN (optionnel, selon votre politique)
```

VLAN 30 — Guest (192.168.30.0/24)

```
# Interfaces > Guest
Enable    : Yes
IPv4 Addr : 192.168.30.1/24
Description : Guest — Visiteurs et appareils temporaires

# Usage :
# Internet uniquement — debit limite (10 Mbps recommande)
# DNS filtre (bloquer publicites et tracking)
# Isolation totale des autres VLANs
```

VLAN 40 — DMZ (192.168.40.0/24)

```
# Interfaces > DMZ
Enable    : Yes
IPv4 Addr : 192.168.40.1/24
Description : DMZ — Serveurs exposes (web, mail, API)

# Usage :
# Trafic entrant depuis Internet autorise (ports specifiques)
# Trafic vers LAN/Work REFUSE
# Monitoring renforce recommande
```

5. Regles firewall inter-VLAN (Zero Trust)

Le Zero Trust signifie : tout est refuse par defaut, on autorise explicitement ce qui est necessaire. Voici les regles pour chaque VLAN :

Regles VLAN IoT (deny-all inter-VLAN, allow Internet)

```
# Firewall > Rules > IoT

# Regle 1 : BLOQUER acces a tous les RFC1918 (LAN prive)
Action   : Block
Interface: IoT
Protocol : any
Source   : IoT net
Dest     : 192.168.0.0/16  (et 10.0.0.0/8, 172.16.0.0/12)
Desc     : Block RFC1918 - Zero Trust inter-VLAN

# Regle 2 : AUTORISER Internet
Action   : Pass
Interface: IoT
Protocol : any
Source   : IoT net
Dest     : any
Desc     : Allow Internet access
```

Regles VLAN Work (acces interne autorise)

```
# Firewall > Rules > Work

# Regle 1 : AUTORISER acces aux services internes specifiques
Action   : Pass
Interface: Work
Protocol : TCP
Source   : Work net
Dest     : 192.168.1.0/24  (LAN principal)
Dest Port: 443, 80, 22  (web, SSH)
Desc     : Allow Work to internal services

# Regle 2 : BLOQUER acces IoT et Guest depuis Work
Action   : Block
Interface: Work
Source   : Work net
Dest     : 192.168.10.0/24, 192.168.30.0/24
Desc     : Block Work to IoT/Guest

# Regle 3 : AUTORISER Internet
Action   : Pass
Source   : Work net
Dest     : any
```

Regles VLAN Guest (Internet only, debit limite)

```
# Firewall > Rules > Guest

# Regle 1 : BLOQUER acces a tout RFC1918
Action   : Block
Interface: Guest
Source   : Guest net
Dest     : 192.168.0.0/16
Desc     : Block all private subnets

# Regle 2 : AUTORISER DNS (vers OPNsense uniquement)
Action   : Pass
Interface: Guest
Protocol : UDP/TCP
Source   : Guest net
Dest     : 192.168.30.1  (gateway Guest)
Dest Port: 53
Desc     : Allow DNS to gateway only

# Regle 3 : AUTORISER Internet avec limiteur de debit
Action   : Pass
Source   : Guest net
Dest     : any
Advanced : Traffic shaper — 10 Mbps download / 5 Mbps upload
```

6. Serveur DHCP par VLAN

Chaque VLAN a son propre serveur DHCP pour distribuer les adresses IP automatiquement :

```
# Services > DHCPv4 > [Interface]

# IoT DHCP :
Enable   : Yes
Range    : 192.168.10.100 - 192.168.10.200
Gateway  : 192.168.10.1
DNS      : 1.1.1.1, 9.9.9.9  (ou Pi-hole si configure)

# Work DHCP :
Enable   : Yes
Range    : 192.168.20.100 - 192.168.20.200
Gateway  : 192.168.20.1
DNS      : 192.168.20.1  (OPNsense DNS interne)

# Guest DHCP :
Enable   : Yes
Range    : 192.168.30.100 - 192.168.30.200
Gateway  : 192.168.30.1
DNS      : 1.1.1.3  (Cloudflare Family — filtrage)
Lease    : 2h  (courts, renouvellement frequent)

# DMZ DHCP :
Enable   : Yes
Range    : 192.168.40.100 - 192.168.40.150
Gateway  : 192.168.40.1
DNS      : 192.168.40.1
```

i Pour des serveurs en DMZ, preferez des adresses IP statiques hors du range DHCP (ex: 192.168.40.10-50).

7. Tester la segmentation

Tests de connectivite de base

```
# Depuis un client sur VLAN IoT (192.168.10.x) :

# Test 1 : Gateway accessible (doit repondre)
ping 192.168.10.1    → OK

# Test 2 : Isolation inter-VLAN (doit ECHOUER)
ping 192.168.20.1    → Request timeout  ✓
ping 192.168.1.1     → Request timeout  ✓

# Test 3 : Internet accessible (doit repondre)
ping 1.1.1.1         → OK
curl ifconfig.me     → votre IP publique  ✓

# Depuis un client Work (192.168.20.x) :
ping 192.168.1.1     → OK  (acces LAN autorise)
ping 192.168.10.1    → timeout  ✓ (IoT bloque)
ping 192.168.30.1    → timeout  ✓ (Guest bloque)
```

Verification dans les logs OPNsense

```
# Firewall > Log Files > Live View
# Filtrer par interface IoT
# Vous devez voir les "block" inter-VLAN en temps reel

# Exemple de log attendu :
Mar 12 20:00:01  block  IoT → 192.168.1.1  (regle Zero Trust)
Mar 12 20:00:02  pass   IoT → 1.1.1.1  (Internet OK)
```

8. Prochaines etapes

Votre infrastructure VLANs + Zero Trust est en place. Voici la suite de la serie :

• Billet 3 : WireGuard VPN — tunnel site-a-site + acces remote workers

• Billet 4 : WiFi par VLAN — APs multi-SSID segmentes

• Billet 5 : CrowdSec + fail2ban — IDS/IPS actif

• Billet 6 : SD-WAN failover LTE automatique

Article complet : blog.botum.ca/opnsense-vlans-zero-trust-configuration

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