FR

Guide Pratique

WiFi & APs avec OPNsense

SSIDs par VLAN, trunking 802.1Q, isolation reseau

Mars 2026

Sommaire

1. Pourquoi segmenter le WiFi par VLAN ?

Sur mon infra BOTUM, chaque SSID WiFi est isole dans son propre VLAN. Un thermostat IoT compromis ne peut pas atteindre mon poste de travail. Un invite qui scanne votre reseau ne voit que son subnet. La segmentation WiFi par VLAN est l'extension logique de la strategie Zero Trust au sans-fil.

+ Securite : un appareil IoT compromis reste confine a son VLAN

+ Performance : trafic IoT n'impacte pas le WiFi Work

+ Conformite : Guest et IoT sans acces aux ressources internes

+ Visibilite : logs OPNsense distincts par SSID/VLAN

+ Flexibilite : politiques QoS differentes par type de trafic

i Prerequis : avoir lu Billet 2 (VLANs Zero Trust) avant de commencer.

2. Prerequis

+ OPNsense operationnel (voir Billet 1 : installer-opnsense-proxmox)

+ VLANs configures dans OPNsense (voir Billet 2 : opnsense-vlans-zero-trust)

+ Switch manageable supportant 802.1Q (Cisco, Netgear, TP-Link, Ubiquiti)

+ AP WiFi compatible multi-SSID et VLAN tagging (UniFi, TP-Link Omada, Meraki)

+ Acces admin au switch et a l'AP

Schema type sur mon infra BOTUM :

```
OPNsense (routeur/firewall)
    |
    | Trunk (VLANs 10,20,30,99)
    |
Switch Manageable
    |
    | Trunk (VLANs 10,20,30)
    |
Access Point (UniFi/Omada)
    |-- SSID "BOTUM-IoT"    -> VLAN 30
    |-- SSID "BOTUM-Work"   -> VLAN 10
    +-- SSID "BOTUM-Guest"  -> VLAN 99
```

3. Concepts : SSID par VLAN

Le principe est simple : chaque SSID WiFi est "tague" avec un VLAN ID. Le trafic de chaque SSID arrive sur OPNsense dans son VLAN propre, avec ses propres regles firewall.

SSID | VLAN VLAN | Usage | Internet: Acces Internet | LAN: Acces LAN

BOTUM-Work | VLAN 10 | Postes pro | Internet: Oui | LAN: Oui (restreint)

BOTUM-IoT | VLAN 30 | Objets connectes | Internet: Oui | LAN: NON

BOTUM-Guest | VLAN 99 | Visiteurs | Internet: Oui | LAN: NON

4. Configuration du switch

Port trunk vers OPNsense

```
# Cisco IOS / IOS-XE :
interface GigabitEthernet0/1  ! Port vers OPNsense
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,99
  switchport trunk native vlan 1
  no shutdown

# TP-Link TL-SG108E (GUI) :
# VLAN -> 802.1Q -> Add VLAN
# VLAN 10 : Port 1 (Tagged), Port 8 (Untagged)
# VLAN 30 : Port 1 (Tagged), Port 8 (Untagged)
# VLAN 99 : Port 1 (Tagged), Port 8 (Untagged)
# Port 1 = uplink OPNsense | Port 8 = downlink AP
```

Port trunk vers l'AP

```
# Le port connecte a l'AP doit etre en TRUNK
# avec tous les VLANs des SSIDs

# Cisco :
interface GigabitEthernet0/8  ! Port vers AP
  switchport mode trunk
  switchport trunk allowed vlan 10,30,99
  no shutdown

# Netgear ProSafe (GUI) :
# Switching -> VLAN -> 802.1Q
# Ajouter VLAN 10 : port AP = Tagged
# Ajouter VLAN 30 : port AP = Tagged
# Ajouter VLAN 99 : port AP = Tagged
```

5. Configuration AP : UniFi et TP-Link Omada

UniFi Controller

```
# 1. Creer les reseaux WiFi dans UniFi Controller
# Settings -> WiFi -> Create New WiFi

# SSID BOTUM-Work :
# Name: BOTUM-Work | Password: ***
# Network: VLAN 10 (selectionner le reseau VLAN cree)
# Security: WPA2/WPA3

# SSID BOTUM-IoT :
# Name: BOTUM-IoT | Password: ***
# Network: VLAN 30
# Client Device Isolation: ON (devices IoT isoles entre eux)

# SSID BOTUM-Guest :
# Name: BOTUM-Guest | Password: ***
# Network: VLAN 99
# Guest Policy: ON | Client Isolation: ON
```

TP-Link Omada Controller

```
# Settings -> Wireless Networks -> Add

# SSID IoT-WiFi :
# SSID: BOTUM-IoT | VLAN: 30
# Security: WPA2-PSK

# SSID Work-WiFi :
# SSID: BOTUM-Work | VLAN: 10
# Security: WPA3

# SSID Guest-WiFi :
# SSID: BOTUM-Guest | VLAN: 99
# Guest Network: Enable | Portal: optionnel
```

6. Configuration OPNsense : bridge WiFi -> VLANs

OPNsense recoit les trames taguees sur le port trunk. Les sous-interfaces VLAN doivent deja exister (Billet 2). Il suffit de verifier que le DHCP est actif sur chaque VLAN.

```
# Verifier les interfaces VLAN dans OPNsense :
# Interfaces -> Assignments
# vlan10 -> WORK (192.168.10.1/24)
# vlan30 -> IOT  (192.168.30.1/24)
# vlan99 -> GUEST (192.168.99.1/24)

# Services -> DHCP Server
# WORK : 192.168.10.100-200
# IOT  : 192.168.30.100-200
# GUEST: 192.168.99.100-200

# Verifier qu'un client WiFi VLAN 30 recoive bien :
# IP: 192.168.30.x | GW: 192.168.30.1 | DNS: 192.168.30.1
```

7. Regles firewall : isolation des SSIDs

Les regles firewall OPNsense controlent ce que chaque VLAN WiFi peut atteindre. Principe : blocage inter-VLAN par defaut, internet autorise pour tous.

```
# Firewall -> Rules -> IOT (VLAN 30)

# Regle 1 : BLOQUER acces au LAN Work
# Action: Block | Interface: IOT
# Source: IOT net | Dest: 192.168.10.0/24
# Description: Block IoT -> Work VLAN

# Regle 2 : BLOQUER acces au LAN Management
# Action: Block | Interface: IOT
# Source: IOT net | Dest: 192.168.1.0/24
# Description: Block IoT -> Management

# Regle 3 : AUTORISER Internet
# Action: Pass | Interface: IOT
# Source: IOT net | Dest: !RFC1918
# Description: IoT Internet access

# Firewall -> Rules -> GUEST (VLAN 99)
# Meme pattern : bloquer tout RFC1918, autoriser Internet
```

i Ordre des regles CRITIQUE : les regles Block doivent preceder les regles Pass.

8. Test : IoT ne peut pas acceder au reseau Work

Connecter un device au SSID BOTUM-IoT et valider l'isolation :

```
# Depuis un device connecte sur BOTUM-IoT (VLAN 30) :

# 1. Verifier l'IP recue (doit etre 192.168.30.x)
ip addr show  # ou : ifconfig

# 2. Ping vers la passerelle IoT (doit repondre)
ping 192.168.30.1

# 3. Ping vers un host Work (doit etre BLOQUE)
ping 192.168.10.100
# Expected: Request timeout / 100% packet loss

# 4. Test Internet (doit fonctionner)
curl -s ifconfig.me
ping 8.8.8.8

# 5. Verifier les logs firewall OPNsense :
# Firewall -> Log Files -> Live View
# Filtrer sur : interface=IOT, dest=192.168.10.0/24
# Les tentatives doivent apparaitre comme BLOCKED
```

i Si IoT peut pinguer Work : verifier l'ordre des regles firewall et que le SSID est bien associe au bon VLAN.

9. Prochaines etapes

Votre infrastructure WiFi est maintenant segmentee et securisee par VLAN. La suite de la serie Stack OPNsense Enterprise :

+ Billet 5 : CrowdSec + fail2ban -- IDS/IPS collaboratif sur OPNsense

+ Billet 6 : Monitoring & alertes -- Uptime Kuma, Grafana, Prometheus

+ Billet 7 : HAProxy et reverse proxy SSL -- exposer des services en toute securite

---

Article complet : blog.botum.ca/opnsense-wifi-ap-management-unifi

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