EN

Quick Reference Guide

WiFi & APs with OPNsense

SSIDs per VLAN, 802.1Q trunking, network isolation

Mars 2026

Table of Contents

1. Why Segment WiFi by VLAN?

On my BOTUM infrastructure, each WiFi SSID is isolated in its own VLAN. A compromised IoT thermostat cannot reach my workstation. A guest scanning your network only sees their own subnet. WiFi VLAN segmentation is the logical extension of the Zero Trust strategy to wireless.

+ Security: a compromised IoT device stays confined to its VLAN

+ Performance: IoT traffic does not impact Work WiFi

+ Compliance: Guest and IoT without access to internal resources

+ Visibility: separate OPNsense logs per SSID/VLAN

+ Flexibility: different QoS policies per traffic type

i Prerequisites: read Post 2 (VLANs Zero Trust) before starting.

2. Prerequisites

+ OPNsense operational (see Post 1: installer-opnsense-proxmox)

+ VLANs configured in OPNsense (see Post 2: opnsense-vlans-zero-trust)

+ Managed switch supporting 802.1Q (Cisco, Netgear, TP-Link, Ubiquiti)

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

+ Admin access to switch and AP

Typical layout on my BOTUM infrastructure:

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

3. Concepts: SSID per VLAN

The principle is simple: each WiFi SSID is "tagged" with a VLAN ID. Traffic from each SSID arrives at OPNsense in its own VLAN, with its own firewall rules.

SSID BOTUM-Work | VLAN 10 | Pro workstations | Internet: Yes | LAN: Yes (restricted)

SSID BOTUM-IoT | VLAN 30 | Connected devices | Internet: Yes | LAN: NO

SSID BOTUM-Guest | VLAN 99 | Visitors | Internet: Yes | LAN: NO

4. Switch Configuration

Trunk Port to OPNsense

```
# Cisco IOS / IOS-XE:
interface GigabitEthernet0/1  ! Port to 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 = OPNsense uplink | Port 8 = AP downlink
```

Trunk Port to AP

```
# The port connected to the AP must be in TRUNK mode
# with all SSID VLANs

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

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

5. AP Configuration: UniFi and TP-Link Omada

UniFi Controller

```
# 1. Create WiFi networks in UniFi Controller
# Settings -> WiFi -> Create New WiFi

# SSID BOTUM-Work:
# Name: BOTUM-Work | Password: ***
# Network: VLAN 10 (select the VLAN network created)
# Security: WPA2/WPA3

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

# 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: optional
```

6. OPNsense Configuration: Bridge WiFi -> VLANs

OPNsense receives tagged frames on the trunk port. The VLAN sub-interfaces must already exist (Post 2). Just verify that DHCP is active on each VLAN.

```
# Verify VLAN interfaces in 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

# Verify a WiFi client on VLAN 30 receives:
# IP: 192.168.30.x | GW: 192.168.30.1 | DNS: 192.168.30.1
```

7. Firewall Rules: SSID Isolation

OPNsense firewall rules control what each WiFi VLAN can reach. Principle: inter-VLAN blocked by default, internet allowed for all.

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

# Rule 1: BLOCK access to Work LAN
# Action: Block | Interface: IOT
# Source: IOT net | Dest: 192.168.10.0/24
# Description: Block IoT -> Work VLAN

# Rule 2: BLOCK access to Management LAN
# Action: Block | Interface: IOT
# Source: IOT net | Dest: 192.168.1.0/24
# Description: Block IoT -> Management

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

# Firewall -> Rules -> GUEST (VLAN 99)
# Same pattern: block all RFC1918, allow Internet
```

i Rule order is CRITICAL: Block rules must precede Pass rules.

8. Test: IoT Cannot Access Work Network

Connect a device to SSID BOTUM-IoT and validate isolation:

```
# From a device connected to BOTUM-IoT (VLAN 30):

# 1. Verify received IP (must be 192.168.30.x)
ip addr show  # or: ifconfig

# 2. Ping to IoT gateway (should respond)
ping 192.168.30.1

# 3. Ping to Work host (must be BLOCKED)
ping 192.168.10.100
# Expected: Request timeout / 100% packet loss

# 4. Internet test (should work)
curl -s ifconfig.me
ping 8.8.8.8

# 5. Check OPNsense firewall logs:
# Firewall -> Log Files -> Live View
# Filter: interface=IOT, dest=192.168.10.0/24
# Attempts should appear as BLOCKED
```

i If IoT can ping Work: check firewall rule order and that the SSID is correctly mapped to the right VLAN.

9. Next Steps

Your WiFi infrastructure is now segmented and secured by VLAN. The rest of the OPNsense Enterprise Stack series:

+ Post 5: CrowdSec + fail2ban -- collaborative IDS/IPS on OPNsense

+ Post 6: Monitoring & alerts -- Uptime Kuma, Grafana, Prometheus

+ Post 7: HAProxy and SSL reverse proxy -- exposing services securely

---

Full article: blog.botum.ca/opnsense-wifi-ap-management-vlans

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