EN

Quick Reference Guide

OPNsense VLANs and Zero Trust

Complete setup: 4 VLANs, firewall rules, DHCP

Mars 2026

Table of Contents

1. Why VLANs? Security Through Segmentation

A flat network where all devices share the same segment is a security time bomb. A single compromised device (IoT camera, smart TV, guest laptop) can potentially reach everything else on your network.

VLANs (Virtual Local Area Networks) let you logically segment your physical network into isolated zones, each with its own access rules and policies.

- IoT device isolation — a hacked camera cannot reach your servers
- Guest protection — the Guest network cannot see your internal LAN
- DMZ for public services — exposed servers isolated from the main LAN
- Zero Trust inter-VLAN — all cross-zone traffic denied by default
- Simplified auditing — know exactly which traffic flows where

i Prerequisite: Follow Part 1 — OPNsense installed and running in Proxmox.

2. Prerequisites: OPNsense + Managed Switch

Before configuring VLANs, make sure you have:

- OPNsense installed and operational (see Part 1 of this series)
- A managed switch supporting 802.1Q VLAN tagging
- Recommended: TP-Link TL-SG108E (~$30) — great for homelab
- Alternative: Netgear GS308E, UniFi USW-Flex-Mini
- Admin access to OPNsense web interface (http://192.168.1.1)
- At least 2 network interfaces on the OPNsense VM (WAN + LAN)
- LAN interface on a Proxmox bridge with "VLAN aware" enabled

```
# Verify vmbr1 is VLAN aware in Proxmox
# System > Network > vmbr1 > VLAN aware: Yes

# Or via CLI:
cat /etc/network/interfaces | grep -A5 'vmbr1'
# Should contain: bridge-vlan-aware yes
```

3. Creating VLANs in OPNsense

3.1 Create VLAN Interfaces

In OPNsense, VLANs are created as sub-interfaces on your existing LAN interface.

```
# Interfaces > Other Types > VLAN
# Click "+" to add each VLAN

VLAN 10 — IoT:
  Parent Interface: vtnet1 (your 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 Assign the Interfaces

```
# Interfaces > Assignments
# Click "+" for each created VLAN:

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

# For each assigned interface:
# Interfaces > [Name] > Enable Interface: Yes
# IPv4 Configuration Type: Static
# IPv4 Address: see section 4
```

4. Configuring the 4 VLANs

VLAN 10 — IoT (192.168.10.0/24)

```
# Interfaces > IoT
Enable     : Yes
IPv4 Addr  : 192.168.10.1/24
Description: IoT — Connected devices (cameras, TVs, thermostats)

# Policy: Internet only
# Access to LAN and other VLANs: DENIED
```

VLAN 20 — Work (192.168.20.0/24)

```
# Interfaces > Work
Enable     : Yes
IPv4 Addr : 192.168.20.1/24
Description: Work — Workstations and internal servers

# Policy: Full internal access
# Internet: allowed
# LAN access: allowed (per policy)
```

VLAN 30 — Guest (192.168.30.0/24)

```
# Interfaces > Guest
Enable     : Yes
IPv4 Addr : 192.168.30.1/24
Description: Guest — Visitors and temporary devices

# Policy: Internet only — throttled (10 Mbps)
# DNS: filtered (Cloudflare Family 1.1.1.3)
# All other VLANs: isolated
```

VLAN 40 — DMZ (192.168.40.0/24)

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

# Policy: Inbound from Internet on specific ports
# Access to LAN/Work: DENIED
# Enhanced monitoring recommended
```

5. Inter-VLAN Firewall Rules (Zero Trust)

Zero Trust means: deny everything by default, explicitly allow only what is needed. Here are the rules for each VLAN:

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

```
# Firewall > Rules > IoT

# Rule 1: BLOCK all RFC1918 private ranges
Action   : Block
Interface: IoT
Protocol : any
Source   : IoT net
Dest     : 192.168.0.0/16  (also 10.0.0.0/8, 172.16.0.0/12)
Desc     : Block RFC1918 - Zero Trust inter-VLAN

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

Work Rules (internal access allowed)

```
# Firewall > Rules > Work

# Rule 1: ALLOW access to specific internal services
Action   : Pass
Interface: Work
Protocol : TCP
Source   : Work net
Dest     : 192.168.1.0/24  (main LAN)
Dest Port: 443, 80, 22  (web, SSH)
Desc     : Allow Work to internal services

# Rule 2: BLOCK access to IoT and Guest
Action   : Block
Interface: Work
Source   : Work net
Dest     : 192.168.10.0/24, 192.168.30.0/24
Desc     : Block Work to IoT/Guest

# Rule 3: ALLOW Internet
Action   : Pass
Source   : Work net
Dest     : any
```

6. DHCP Server Per VLAN

```
# 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

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

# 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 filtering)
Lease   : 2h  (short lease, frequent renewal)

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

7. Testing Segmentation

```
# From a client on IoT VLAN (192.168.10.x):

# Test 1: Gateway reachable (should respond)
ping 192.168.10.1     → OK

# Test 2: Inter-VLAN isolation (should FAIL)
ping 192.168.20.1     → Request timeout  ✓
ping 192.168.1.1      → Request timeout  ✓

# Test 3: Internet accessible (should respond)
ping 1.1.1.1          → OK
curl ifconfig.me      → your public IP  ✓

# From Work client (192.168.20.x):
ping 192.168.1.1      → OK  (LAN access allowed)
ping 192.168.10.1     → timeout  ✓ (IoT blocked)
ping 192.168.30.1     → timeout  ✓ (Guest blocked)
```

i Check OPNsense Firewall > Log Files > Live View to see blocked inter-VLAN traffic in real-time.

8. Next Steps

Your VLANs + Zero Trust infrastructure is in place. Here is what comes next in the series:

- Part 3: WireGuard VPN — site-to-site tunnel + remote workers
- Part 4: WiFi per VLAN — multi-SSID APs with segmentation
- Part 5: CrowdSec + fail2ban — active IDS/IPS protection
- Part 6: SD-WAN with automatic LTE failover

Full article: blog.botum.ca/opnsense-vlans-zero-trust-guide

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