📘 Network Segmentation & VLAN Implementation Summary

Date: 2025-11-18

Engineer: Bruce Thornton

Environment: pfSense + TP-Link TL-SG108E + Multi-VLAN Red Team/SOC Lab

---

1. Objective

To rebuild and properly segment a multi-device cybersecurity lab environment using pfSense and a TP-Link Easy Smart Switch (TL-SG108E), ensuring:

- Logical network segmentation
- Isolated VLANs for SOC, Attacker, C2 Server, Victim, and Honeypot
- Centralized routing and DHCP via pfSense
- SOC monitoring visibility while preserving realistic red-team style network boundaries
- Reliable switch configuration using the TP-Link safe VLAN method to prevent service disruption
- Stable baseline network for future Security Onion / Elastic Stack integration

---

2. Baseline Recovery

After several failed attempts with previous VLAN configurations, the environment was reset to a clean, known-good state.

pfSense Recovery

- Reset admin password from physical console (Option 3)
- Restored access to webConfigurator
- Verified LAN interface IP: **10.0.1.1/24**
- Confirmed LAN DHCP server operational (10.0.1.100–200)

Switch Recovery

- Factory reset TL-SG108E
- Switch reachable at **192.168.0.1**
- All ports defaulted to VLAN1 untagged, PVID=1
- Clean environment for safe VLAN reconstruction

This provided a stable starting point for the segmentation project.

---

3. VLAN Architecture (Target Design)

VLAN	Purpose	Gateway	Subnet	Switch Port
10	SOC (Kali Purple)	10.0.10.1	10.0.10.0/24	2
20	DefenderBox (Victim)	10.0.20.1	10.0.20.0/24	3
30	Attacker Pi	10.0.30.1	10.0.30.0/24	4
31	C2 Server Pi	10.0.31.1	10.0.31.0/24	5
50	Honeypot (OpenCanary)	10.0.50.1	10.0.50.0/24	6
1	pfSense LAN (mgmt/safety net)	10.0.1.1	10.0.1.0/24	1 (and optionally 7–8)

---

4. pfSense VLAN Configuration

4.1 VLAN Definitions Created

Under **Interfaces → Assignments → VLANs**, the following were created:

- VLAN 10 on parent interface ue0
- VLAN 20 on ue0
- VLAN 30 on ue0
- VLAN 31 on ue0
- VLAN 50 on ue0

4.2 VLAN Interfaces Assigned & Configured

Each VLAN assigned an OPT interface and configured:

Interface	Static IP	Mask
VLAN10_SOC	10.0.10.1	/24
VLAN20_DefenderBox	10.0.20.1	/24
VLAN30_Attacker	10.0.30.1	/24
VLAN31_C2	10.0.31.1	/24
VLAN50_HoneyPot	10.0.50.1	/24

LAN (ue0) remained unchanged at **10.0.1.1/24** for management continuity, preventing lockout.

4.3 DHCP Services Enabled per VLAN

Each VLAN received its own DHCP pool (100–200 range).
LAN DHCP was intentionally left enabled during setup to maintain stability.

5. Switch Configuration (TP-Link Safe VLAN Method)

Because TL-SG108E is an “Easy Smart” device with strict VLAN behavior, the safe configuration method was used to ensure:

- No lockouts
- No loss of GUI access
- No accidental removal of VLAN1 during setup

5.1 VLAN Membership

Port 1 (pfSense) tagged on all VLANs:

VLAN	Tagged	Untagged
10	1	2
20	1	3
30	1	4
31	1	5
50	1	6

Ports 2–6 untagged in their respective VLANs.

VLAN 1 was left unchanged on all ports (TP-Link best practice until final verification).

5.2 PVID Assignment

Port	PVID	Purpose
1	1	pfSense trunk (untagged VLAN1)
2	10	SOC
3	20	Victim
4	30	Attacker

5	31	C2
6	50	Honeypot
7–8	1	Spare/Management

This combination of PVID and VLAN membership **forces untagged devices into the correct VLAN** while maintaining switch accessibility.

---

6. Validation Results

After finalizing switch PVIDs and VLAN assignments:

- SOC (port 2) obtained **10.0.10.x**
- DefenderBox (port 3) obtained **10.0.20.x**
- Attacker Pi (port 4) obtained **10.0.30.x**
- C2 Pi (port 5) obtained **10.0.31.x**
- OpenCanary (port 6) obtained **10.0.50.x**

All VLANs pulled the correct DHCP leases, confirming correct tagging, PVID behavior, and routing through pfSense.

The SOC VLAN was intentionally configured to have “allow any” outbound access to reach the Elastic/Kibana web interface for log and alert monitoring.

---

7. Final Network State

✔ pfSense successfully manages routing for all VLANs

✔ Switch correctly enforces VLAN separation

✔ DHCP functional across all isolated networks

✔ SOC VLAN fully operational with Elastic/Kibana access

✔ All devices in the lab segmented and operating within their assigned security zones

✔ Baseline ready for firewall tuning, IDS/IPS monitoring, and red-team exercises

---

✅ Summary

Today’s work successfully transformed a previously unstable, repeatedly-breaking network setup into a fully structured, professionally segmented lab environment using industry-aligned VLAN practices.

The final result is a reliable, multi-VLAN environment suited for:

- SOC analysis
- Elastic/Kibana centralized monitoring
- Red team C2 operations
- Attacker-Victim simulation
- Honeypot telemetry (OpenCanary)
- Realistic cyber range behavior

All built on low-cost hardware with enterprise-style isolation and routing.
