

TheDen Home Network Runbook

- [1. Introduction](#)
- [2. Security Principles](#)
- [3. Network Architecture](#)
- [4. Firewall and Routing](#)
- [5. DNS](#)
- [6. Wireless Network Configuration](#)
- [7. Threat Detection and Response](#)
- [8. Incident Response - WIP](#)
- [9. Operations and Maintenance](#)
- [10. Appendix](#)

1. Introduction

This runbook defines the network topology, architecture, security configuration, and operational procedures for TheDen Home Network. It documents how the household network is segmented, protected, monitored, and maintained to ensure privacy, integrity, and availability of local systems and connected devices.

Date	Version	Author	Description
2025-11-01	0.1	Chris Landis	Initial draft
2025-11-04	0.2	Chris Landis	Added appendix
2026-05-23	1.0	Chris Landis	Full update and review

2. Security Principles

2.1 Defense in Depth Overview

TheDen Home Network follows a layered defense model, with multiple safeguards that provide independent protection. Layers include OPNsense, VLAN segmentation, encrypted DNS (DoT), and Suricata IPS.

2.2 Zero Trust and Least Privilege

All devices are treated as untrusted by default. Access is restricted to essential communications only, using a default-deny policy between VLANs.

Administrative access requires authenticated HTTPS and IoT devices are limited to U.S.-based connections only.

3. Network Architecture

3.1 Overview

TheDen Home Network is designed for segmentation, performance, and manageability using VLANs to isolate traffic and prevent lateral movement between device classes. A router (Protectli FW6D running OPNSense) handles routing/NAT, VLAN termination, and DNS. A WiFi AP (UniFi 6+) connects directly to the FW6D via an 802.1Q trunk, broadcasting eight SSIDs across isolated VLANs.

3.2 Design Goals

- Isolation: Each VLAN has a clear and limited purpose.
- Visibility: All inter-VLAN and WAN traffic passes through OPNsense for inspection and logging.
- Control: Only authorized management systems can alter network configuration.
- Scalability: VLAN framework supports future expansion and additional IoT segmentation.

3.3 Physical Topology

[AT&T BGW320-500]

| (Fiber handoff)

|

[Protectli FW6D Firewall (OPNsense)]

├─ igb0 -> WAN (DHCP from ISP)

├─ igb1 -> 802.1Q Trunk to UniFi U6+ AP (VLANs 10,20,30,40,50,60,70,80,99)

└─ igb2 -> Admin (192.168.100.0/24)

|

[UniFi U6+ AP]

├─ SSID "thedenhome" -> VLAN 10

├─ SSID "thedenmobile" -> VLAN 20

├─ SSID "thedeniot" -> VLAN 30

├─ SSID "thedenguest" -> VLAN 40

└─ SSID "thedenprinter" -> VLAN 50

- └─ SSID “thedenwork1” -> VLAN 60
- └─ SSID “thedenwork2” -> VLAN 70
- └─ SSID “thedenwork3” -> VLAN 80

3.4 Interface Summary

Interface	Description	VLAN	IP/Subnet	Notes
igb0	WAN	—	DHCP (public)	Connection to modem
igb1	LAN Trunk	10-99	—	VLAN trunk from AP
igb2	ADMIN	—	192.168.100.1/24	Ethernet mgmt port
vlan0.10	VLAN10_HOME	10	192.168.10.1/24	Personal computers
vlan0.20	VLAN20_MOBILE	20	192.168.20.1/24	Cellphones and tablets
vlan0.30	VLAN30_IOT	30	192.168.30.1/24	Smart devices
vlan0.40	VLAN40_GUEST	40	192.168.40.1/24	Guest WiFi
vlan0.50	VLAN50_PRINT	50	192.168.50.1/24	Printer VLAN
vlan0.60	VLAN60_WORK1	60	192.168.60.1/24	Work VLAN #1
vlan0.70	VLAN70_WORK2	70	192.168.70.1/24	Work VLAN #2
vlan0.80	VLAN80_WORK3	80	192.168.80.1/24	Work VLAN #3
vlan0.99	VLAN99_MGMT	99	192.168.99.1/24	WiFi AP VLAN

3.5 Subnet IP Addressing

VLAN	Subnet	Gateway	DHCP Range
VLAN10_HOME	192.168.10.0/24	192.168.10.1	100-200
VLAN20_MOBILE	192.168.20.0/24	192.168.20.1	100-200
VLAN30_IOT	192.168.30.0/24	192.168.30.1	100-200
VLAN40_GUEST	192.168.40.0/24	192.168.40.1	100-200
VLAN50_PRINT	192.168.50.0/24	192.168.50.1	100-200
VLAN60_WORK1	192.168.60.0/24	192.168.60.1	100-200
VLAN70_WORK2	192.168.70.0/24	192.168.70.1	100-200
VLAN80_WORK3	192.168.80.0/24	192.168.80.1	100-200

VLAN99_MGMT	192.168.99.0/24	192.168.99.1	100-200
ADMIN	192.168.100.0/24	192.168.100.1	100-200

4. Firewall and Routing

4.1 Overview

The OPNsense firewall on the FW6D serves as the central routing, filtering, and NAT layer. It enforces a stateful inspection model with a default-deny policy between VLANs. Explicit rules are defined to permit minimal, functional inter-VLAN communication where necessary.

4.2 Default Policy

All inbound and inter-VLAN traffic is denied by default, and required services are explicitly permitted. Outbound internet access is restricted to trusted VLANs, and the IoT and Print VLANs have limited access through GeoIP. All DNS traffic is encrypted through Unbound using DNS-over-TLS (DoT).

4.3 Inter-VLAN Access Matrix

From->To	HOME	MOBILE	IOT	GUEST	PRINT	WORK1	WORK2	WORK3	MGMT
HOME	✓	X	X	X	✓	X	X	X	✓
MOBILE	X	✓	X	X	✓	X	X	X	X
IOT	X	X	✓	X	X	X	X	X	X
GUEST	X	X	X	✓	✓	X	X	X	X
PRINT	X	X	X	X	✓	X	X	X	X
WORK1	X	X	X	X	✓	✓	X	X	X
WORK2	X	X	X	X	✓	X	✓	X	X
WORK3	X	X	X	X	✓	X	X	✓	X
MGMT	✓	X	X	X	X	X	X	X	✓

✓ Access allowed

X Access denied

✓ Access allowed for management of the UniFi U6+

4.4 NAT and Port Forwarding Rules

NAT is applied only on the WAN interface (igb0). A Port Forward on each VLAN interface transparently redirects outbound UDP/TCP 53 to this firewall (Unbound), and a block rule drops attempts to use external DNS over 53. No inbound port forwarding is configured from WAN.

4.5 GeoIP and Traffic Control

The IoT VLAN (30) and Print VLAN (60) are restricted to U.S. destinations only using GeoIP aliases. Rules permit traffic only if the destination is within the U.S.; all other destinations are blocked and logged. This minimizes risk from untrusted devices phoning home to non-U.S. regions.

4.6 Logging and Alerting

Firewall logging is enabled for all default-deny and GeoIP rules. Suricata inline IPS is active on the WAN and IoT VLANs. Alert summaries are reviewed weekly, with log rotation every 30 days.

4.7 Management Access

The OPNsense firewall web UI is accessible only from the Home (VLAN10) network through firewall rules. Home VLAN devices can reach the UniFi AP management interface via firewall rules permitting HOME <-> MGMT traffic.

5. DNS

5.1 Overview

TheDen Home Network uses the Unbound recursive DNS resolver integrated within OPNsense for all local name resolution. All VLANs resolve queries through Unbound, ensuring encrypted DNS using DoT and preventing external DNS leakage. The resolver validates DNSSEC and caches responses locally.

5.2 DNS-over-TLS Configuration

DNS Resolver (Unbound) is configured for DoT to Cloudflare and Quad9 with DNSSEC validation. The configuration enforces strict authentication of upstream certificates and disallows fallback to plain DNS.

Primary DoT servers include Cloudflare (1.1.1.1#cloudflare-dns.com) and Quad9 (9.9.9.9#dns.quad9.net). Both providers are validated for TLS certificate integrity and DNSSEC compliance.

To prevent DNS hijacking or leakage, all DNS requests (TCP/UDP port 53) are blocked unless directed to the firewall itself. A NAT redirect rule ensures that any direct DNS queries are transparently routed to Unbound on 192.168.x.1.

5.3 Logging and Validation

DNS query logging is enabled for Unbound. Queries from each VLAN are tagged with source IP for audit visibility. DNSSEC failures and DoT handshake failures are logged and reviewed monthly. All cache data is purged automatically on Unbound service restart.

6. Wireless Network Configuration

6.1 Overview

Wireless connectivity is provided by an UniFi U6+ access point running eight WiFi networks. Each SSID is mapped to a corresponding VLAN and carried through a 802.1Q trunk line to the router to provide isolation between wireless networks.

6.2 SSID to VLAN Mapping

SSID	Network Protocol	Mapped VLAN	Purpose
thedenhome	WPA2/WPA3-Personal	VLAN10	Trusted household devices
thedenmobile	WPA2/WPA3-Personal	VLAN20	Family phones and tablets
thedeniot	WPA2-Personal	VLAN30	Untrusted smart devices
thedenguest	WPA2/WPA3-Personal	VLAN40	Guest network
thedenprinter	WPA2-Personal	VLAN50	Printer network
thedenwork1	WPA3-Personal	VLAN60	Primary work devices
thedenwork2	WPA3-Personal	VLAN70	Secondary work devices
thedenwork3	WPA3-Personal	VLAN80	Tertiary work devices

6.3 Security Configuration

Wireless networks use the strongest security protocol available based on the types of devices connecting. For IoT and print networks, only WPA2-Personal is possible due to the capabilities of those devices. Home, mobile and guest networks use WPA3 transition mode (WPA2/WPA3) to ensure legacy devices are able to connect. The remaining work networks use strict WPA3. Each SSID is bound to its VLAN and carried to the router via a tagged trunk to the LAN port.

6.4 Isolation and Access Control

Client isolation is enabled on all SSIDs, except Home, to prevent peer-to-peer communication.

6.5 Management Access

The UniFi Controller resides on the Management VLAN (192.168.99.0/24). Home devices running the controller software can reach the AP based on firewall configuration allowing communication between Home and Management VLANs on ports 443, 8080, and 8443. Access through the UI is HTTPS-only and restricted to the admin account, the credentials for which are stored in Bitwarden.

6.6 Optimization and Maintenance

Wireless channels are statically assigned to minimize overlap, and transmit power is tuned for even coverage. Band steering is enabled to prefer 5 GHz clients. AP firmware updates are applied quarterly through the UniFi Controller.

7. Threat Detection and Response

7.1 Overview

TheDen Home Network employs a layered approach to threat detection, focusing on visibility, containment, and recovery. While advanced monitoring is not yet implemented, the foundation is established through OPNsense's Suricata intrusion detection system (IDS) and detailed firewall logging. This section describes the configuration, IoT isolation policy, and future plans for active monitoring and response.

7.2 Intrusion Detection System (Suricata)

Suricata is enabled to detect suspicious inbound or outbound traffic patterns. It operates in inline IPS mode, allowing OPNsense to block packets matching known exploit signatures. Default rulesets include Emerging Threats Open and Abuse.ch for malware and command-and-control traffic detection.

Suricata is configured to:

- Inspect all WAN traffic (inbound and outbound)
- Log alerts to the OPNsense dashboard
- Automatically block high-confidence signatures
- Rotate logs every 7 days

7.3 IoT Device Policy and Containment

IoT devices operate on VLAN 30 (192.168.30.0/24) and are considered untrusted. They are allowed outbound internet access only to U.S. destinations and are blocked from communicating with any

internal VLANs to limit potential compromise impact.

IoT devices follow a strict isolation and containment workflow:

1. All new IoT devices are connected to the IoT SSID and automatically assigned to VLAN 30.
2. If unusual network behavior is detected (e.g., non-U.S. connection attempts), Suricata logs are reviewed.
3. Devices exhibiting repeated anomalies are manually quarantined by disabling their MAC address or moving them to the quarantine VLAN.
4. Quarantined devices are isolated until re-imaged, factory reset, or replaced.

7.4 Quarantine VLAN (Future Implementation)

A dedicated quarantine VLAN will be implemented for compromised or suspicious devices. This VLAN will have no routing to other subnets and will be limited to basic management tools for inspection. Firewall automation or manual rule adjustments will allow rapid device isolation directly from the OPNsense interface.

7.5 Logging and Review

OPNsense maintains logs for all blocked traffic, DNS enforcement events, and GeoIP rejections. Logs are retained for 30 days and reviewed during monthly maintenance sessions. High-signal alerts (Suricata severity = 1 and GeoIP blocks from VLAN30 and VLAN50) trigger email alerts to landisfam.org@gmail.com. These entries are reviewed ASAP.

8. Incident Response - WIP

8.1 Purpose

Defines how to identify, contain, and recover from potential network or device security incidents within TheDen Home Network. Focuses on practical response steps using OPNsense, UniFi, and Suricata without centralized monitoring.

8.2 Incident Categories

Category	Description	Example Indicators
Network Intrusion	Unauthorized access attempt or unexpected inbound traffic	Suricata alerts, new device detected
Device Compromise	IoT or personal device showing unusual behavior	Non-U.S. connections, bandwidth spike
Policy Violation	Device bypassing VLAN or DNS restrictions	Traffic logs showing cross-VLAN attempts
Malware/Phishing	Infected endpoint or malicious download	Antivirus alert, suspicious domain
Configuration Error	Change causing unexpected access or outage	Device unreachable, DNS failure

8.3 Incident Response Workflow

In the event of a detected or suspected security incident, the following steps are taken:

- **Detection**** – Alert triggered by Suricata or firewall logs.
- **Containment**** – Immediately block or quarantine the affected device using VLAN assignment or MAC filtering.
- **Investigation**** – Review logs to determine traffic patterns, destinations, and scope of exposure.
- **Eradication**** – Reset, re-image, or replace affected devices as needed.
- **Recovery**** – Verify restored connectivity and confirm normal traffic.
- **Review**** – Document findings in the Incident Log and update rules as necessary.

IPS rule created to update and reload IDS rules (system->settings->cron)

8.4 Detection Methods

- Suricata alerts (Services → Intrusion Detection → Alerts)
- Firewall logs (Firewall → Log Files → Normal View)
- UniFi client list for new or unexpected devices
- ISP or modem logs for bandwidth anomalies

8.5 Immediate Containment

1. Identify the device by hostname, MAC address, or IP.
2. Block traffic:
 - In OPNsense: disable DHCP lease or create a temporary block rule.
 - In UniFi: block or disconnect the device.
3. Move the device to a quarantine VLAN if available.
4. Record timestamps, IPs, and rule triggers for later review.

8.6 Investigation

Review logs in Suricata and OPNsense to determine the event source, direction, and potential cause. Assess recent firmware or configuration changes for correlation.

8.7 Eradication and Recovery

- **IoT:** Factory reset and reconnect under VLAN 30.
- **Personal Devices:** Perform antivirus scans or OS reinstall.
- **Network Devices:** Restore configuration from backup if misconfiguration suspected.

8.8 Documentation

Maintain an incident log for trend tracking.

Date	Device	Issue	Action Taken	Resolution
2025-10-29	Smart Plug (IoT)	Attempted non-US connection	Blocked and reset	Device re-added successfully

8.8 Post-Incident Review

- Verify firewall and IDS rules are correct.
- Identify configuration gaps.
- Update runbook if process improvements are made.
- Add new rules or VLAN restrictions to prevent recurrence.

8.10 Notification

External notification is not required for home-only incidents. If a work or shared account is involved, contact the appropriate administrator immediately.

9. Operations and Maintenance

9.1 Overview

This section defines the operational procedures for keeping TheDen Home network current, stable, and secure.

9.2 Software and Firmware Updates

- OPNsense: Check for updates monthly (System -> Firmware -> Updates)
 - Apply security updates immediately; feature updates at least quarterly
 - Take a snapshot and configuration backup immediately before any updates are made
- System Packages (Suricata, GeoIP, etc.): Verify automatic updates under Services -> Intrusion Detection -> Download. Update manually if stale
- UniFi Network Controller and Access Points: Check for firmware updates quarterly through the controller dashboard

9.3 Log Review

Review Firewall, Suricata, and DNS logs monthly, focusing on:

- Repeated GeoIP blocks on the IoT VLAN
- Unusual outbound destinations
- Suricata “severity 1” events

Make sure logs older than 30 days are archived, delete after 90 days.

9.4 Backup Validation

Automated backups are planned; once configured, validate quarterly.

- Confirm existence and timestamp of:
 - OPNsense configuration backup
 - UniFi Controller backup
- Delete backups over 90 days old

9.5 Credential Management

All administrative credentials are stored in my Bitwarden vault in the TheDen Admin folder. The vault is protected by MFA, and shared within the Landisfam family.

9.6 Maintenance Checklists

Monthly Tasks:

Quarterly Tasks:

10. Appendix

Appendix A - Hardware

Device	Description	Link
Protectli FW6D	OPNsense firewall/router appliance	https://protectli.com/product/fw6d/
UniFi U6+ Access Point	Dual-band WiFi 6 AP (managed by UniFi Controller)	https://techspecs.ui.com/unifi/wifi/u6-plus

Appendix B - Software

Software	Purpose	Link
OPNsense	Firewall, router, DNS resolver, IDS/IPS	https://opnsense.org/
UniFi Network Server (Controller)	WiFi AP management and firmware control	https://ui.com/download/releases/netw-ork-server

Appendix C - Firewall Rule Sets

Aliases:

Alias	Type	Content	Description
RFC1918	Network	192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12	All private IP ranges
Geo_US	GeoIP	United States	U.S. IP address ranges
print_ports	Port	515, 631, 9100	Printing — LPD, IPP, RAW
scan_ports	Port	139, 445	SMB scan-to-folder (Windows only)
scanback	Port	137, 161, 54925	Brother iPrint&Scan scanning (UDP only)
unifi_ports	Port	443, 8080, 8443	UniFi AP management

Rules:

VLAN	Action	Dir	TCP/IP	Protocol	Source	Destinati on	Ports	Descripti on
All	Pass	in	IPv4	TCP/UDP	(VLAN) net	(VLAN) address	53	DNS to Unbound
HOME	Pass	in	IPv4	TCP	HOME net	Home address	443	OPNsense WebGUI
Admin	Pass	in	IPv4	TCP	Admin net	Admin address	443	OPNsense WebGUI — emergency access
HOME	Pass	in	IPv4	TCP	HOME net	VLAN99_MGMT net	unifi_ports	UniFi controller management
MGMT	Pass	in	IPv4	TCP	MGMT net	192.168.9.100	unifi_ports	Controller reach to AP
MGMT	Pass	in	IPv4	TCP	192.168.9.100	VLAN10_HOME net	8080	AP inform back to controller
HOME, MOBILE, GUEST, WORK1, WORK2, WORK3	Pass	in	IPv4	TCP	(VLAN) net	VLAN50_PRINT net	print_ports	Printing
HOME	Pass	in	IPv4	UDP	HOME net	VLAN50_PRINT net	scanback	Mac scanning to printer
PRINT	Pass	in	IPv4	UDP	VLAN50_PRINT net	VLAN10_HOME net	scanback	Printer scan response to Mac
PRINT	Pass	in	IPv4	TCP	VLAN50_PRINT net	RFC1918	scan_ports	SMB scan-to-folder — Windows; enable when needed
All	Block	in	IPv4	*	(VLAN) net	RFC1918	*	Block inter-VLAN lateral movement

IoT, PRINT	Block	in	IPv4	UDP	(VLAN) net	Any	443	Block QUIC
IoT, PRINT	Pass	in	IPv4	*	(VLAN) net	Geo_US	*	Internet — U.S. destinations only
IoT, PRINT	Block	in	IPv4	*	(VLAN) net	! Geo_US	*	Block non- U.S. destinations (logged)
HOME, MOBILE, GUEST, WORK1, WORK2, WORK3	Pass	in	IPv4	*	(VLAN) net	any	*	Internet access
MGMT, Admin	Block	in	IPv4	*	(VLAN) net	any	*	Block all remaining traffic

Notes:

- “In” = traffic entering the interface from that VLAN toward others or WAN
- The DNS pass rule appears at the top of every interface's rule set. The explicit pass is necessary because the VLAN gateway address (where Unbound listens) falls within RFC1918 space and would otherwise be caught by the RFC1918 block rule.
- For IoT and PRINT, the RFC1918 block is evaluated before the GeoIP rules, so the Geo_US pass and non-U.S. block only ever act on public internet traffic.
- Logging is enabled for all “block” and geoIP rules
- The SMB scan-to-folder rule (PRINT, disabled) is disabled by default. Enable temporarily for Windows scan-to-folder, then disable when finished.
- For MGMT and Admin, the final block-all rule ensures no internet access regardless.
- The static AP IP 192.168.99.100 used in the MGMT rules is maintained via a DHCP static reservation on VLAN99_MGMT.