

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.

Revision #3

Created 2026-07-12 20:39:24 UTC by Chris Landis

Updated 2026-08-30 18:44:01 UTC by Chris Landis