

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:

1. ****Detection**** – Alert triggered by Suricata or firewall logs.
2. ****Containment**** – Immediately block or quarantine the affected device using VLAN assignment or MAC filtering.
3. ****Investigation**** – Review logs to determine traffic patterns, destinations, and scope of exposure.
4. ****Eradication**** – Reset, re-image, or replace affected devices as needed.
5. ****Recovery**** – Verify restored connectivity and confirm normal traffic.
6. ****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.

Revision #1

Created 2026-07-12 20:40:03 UTC by Chris Landis

Updated 2026-07-12 20:41:31 UTC by Chris Landis