

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

✗ 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.

Revision #2

Created 2026-07-12 20:36:26 UTC by Chris Landis

Updated 2026-08-30 18:38:01 UTC by Chris Landis