

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.

Revision #1

Created 2026-07-12 20:38:11 UTC by Chris Landis

Updated 2026-07-12 20:38:30 UTC by Chris Landis