EN

Quick Reference Guide

AdGuard Home + DNS over HTTPS

DNS Filtering and Privacy with OPNsense

Mars 2026

Table of Contents

1. Why DNS Is the Weakest Link

Every time you visit a website, your device sends a DNS query to translate a domain name into an IP address. By default, these queries travel in plaintext over port 53, visible to your ISP, intermediate routers, and any attacker on the same network.

Three major risks:

• **Tracking:** Your ISP logs all DNS queries and may sell that data to third parties.

• **Ads and malware:** Without filtering, tracking pixels and malware-distribution domains resolve normally.

• **DNS hijacking:** An attacker can redirect your DNS queries to malicious servers (man-in-the-middle).

i References: RFC 7858 (DNS over TLS), RFC 8484 (DNS over HTTPS)

2. AdGuard Home vs Pi-hole — Comparison

Both are local DNS resolvers with blocklist filtering. Key differences:

Web UI: AdGuard Home — Modern, responsive | Pi-hole — Classic, functional

DNS over HTTPS: AdGuard Home — Native, built-in | Pi-hole — Requires dnscrypt-proxy

DNS over TLS: AdGuard Home — Native, built-in | Pi-hole — Manual configuration

Per-client stats: AdGuard Home — Detailed per device | Pi-hole — Basic

DNS rewrites: AdGuard Home — GUI-based | Pi-hole — Via config files

REST API: AdGuard Home — Full API | Pi-hole — Partial

Community: AdGuard Home — Active (AdGuard team) | Pi-hole — Very large

i BOTUM recommendation: AdGuard Home for new deployments — native DoH/DoT support out of the box.

3. Install AdGuard Home (Docker on Proxmox)

Option A — Docker Compose

```
mkdir -p /opt/adguardhome/{work,conf}

cat > /opt/adguardhome/docker-compose.yml << 'EOF'
version: '3.8'
services:
  adguardhome:
    image: adguard/adguardhome:latest
    container_name: adguardhome
    restart: unless-stopped
    network_mode: host
    volumes:
      - ./work:/opt/adguardhome/work
      - ./conf:/opt/adguardhome/conf
EOF

cd /opt/adguardhome
docker compose up -d

# Access the setup wizard at:
# http://VM-IP:3000
```

Option B — LXC Container on Proxmox

```
# Inside a Debian/Ubuntu LXC container
curl -fsSL https://static.adguard.com/adguardhome/release/AdGuardHome_linux_amd64.tar.gz \
  | tar -xz -C /opt/

cd /opt/AdGuardHome
./AdGuardHome -s install

systemctl status AdGuardHome
# Web interface: http://LXC-IP:3000
```

i Assign a static IP to your AdGuard Home VM/LXC in OPNsense DHCP leases.

4. Configure OPNsense to Redirect DNS

4.1 Default DNS in OPNsense

```
# Services > Unbound DNS > General
# Uncheck "Enable" to disable Unbound
# OR: point Unbound to AdGuard Home as upstream

# System > Settings > General
DNS servers: 192.168.1.x  (AdGuard Home IP)
```

4.2 Forced NAT Redirect (DNS Bypass Prevention)

```
# Firewall > NAT > Port Forward
# Create a rule for each VLAN:

Interface     : VLAN_LAN (repeat for each VLAN)
Protocol      : TCP/UDP
Destination   : ! 192.168.1.x (inverted — all except AdGuard)
Dest. port    : 53
Redirect IP   : 192.168.1.x  (AdGuard Home IP)
Redirect port : 53
Description   : Force DNS to AdGuard Home
```

i This rule silently intercepts devices trying to use external DNS (8.8.8.8, 1.1.1.1, etc.) and redirects them to AdGuard Home.

5. Enable DNS over HTTPS (DoH)

In the AdGuard Home web interface:

1. Settings > DNS Settings > Upstream DNS servers

2. Replace default servers with DoH servers:

```
# Cloudflare DoH (recommended)
https://cloudflare-dns.com/dns-query

# NextDNS (customizable)
https://dns.nextdns.io/YOUR-ID

# Quad9 DoH (security-focused)
https://dns.quad9.net/dns-query

# Mullvad (no-log)
https://base.dns.mullvad.net/dns-query
```

5.1 Parallel Mode (Fastest IP)

```
# Settings > DNS Settings
# Load-balancing strategy: Parallel requests
# AdGuard Home queries all upstreams simultaneously
# and returns the first response received
```

i Enable "DNSSEC" in Settings > DNS Settings to validate DNS signatures.

6. Recommended Blocklists

In Filters > DNS blocklists > Add blocklist:

AdGuard DNS filter: Ads + malware — AdGuard's main list

OISD Big: Ads, tracking, malware — 150k+ domains

Hagezi Pro: Aggressive tracking — recommended

Steven Black Hosts: Ads + malware — very stable

Malware Domain List: Active malicious domains

IoT Blocklist: IoT telemetry and C2 traffic

i Start with 2-3 lists and adjust based on false positive rate observed in your stats.

7. Force DNS on All VLANs

Apply DNS redirect NAT rules on each VLAN interface defined in OPNsense:

```
# For each VLAN (LAN, IoT, Guest, DMZ):
# Firewall > NAT > Port Forward > Add

# Rule 1: Block direct outbound DNS (except AdGuard)
Action       : Block
Interface    : VLAN_IOT
Protocol     : TCP/UDP
Source       : VLAN_IOT net
Destination  : ! 192.168.1.x
Dest. port   : 53

# Rule 2: Allow to AdGuard only
Action       : Pass
Interface    : VLAN_IOT
Protocol     : TCP/UDP
Source       : VLAN_IOT net
Destination  : 192.168.1.x
Dest. port   : 53
```

Block Direct DoH (Port 443 to 1.1.1.1)

```
# Firewall > Rules > VLAN_IOT
# Block direct access to known DoH IP addresses
# Create alias "DNS_Public" with: 1.1.1.1, 8.8.8.8, 9.9.9.9

# Then add rule: Block port 443 to alias DNS_Public
```

i Warning: blocking port 443 to DoH IPs may break some apps. Test in log-only mode first.

8. Monitoring and Dashboard

8.1 AdGuard Home Dashboard

- DNS Queries today: total request count for the day
- Blocked by filters: percentage blocked (target: 15-30%)
- Blocked by SafeBrowsing: malicious domains intercepted
- Top clients: most active devices on your network
- Top blocked domains: most frequently blocked domains

8.2 Export to Grafana (Part 9 Preview)

```
# AdGuard Home exposes stats via REST API
curl http://192.168.1.x:3000/control/stats \
  -u admin:password | python3 -m json.tool

# Prometheus integration (prometheus-exporter)
docker run -d --name adguard-exporter \
  -e ADGUARD_HOSTNAME=192.168.1.x \
  -e ADGUARD_USERNAME=admin \
  -e ADGUARD_PASSWORD=password \
  -p 9617:9617 \
  ebrianne/adguard-exporter
```

i Part 9 will cover full Grafana + Prometheus integration for visualizing network metrics.

Full article: blog.botum.ca/opnsense-adguard-home-dns-https-guide

OPNsense Series: blog.botum.ca/opnsense-stack-securite-enterprise-proxmox

Website: www.botum.ca • contact@botum.ca