FR

Guide Pratique

AdGuard Home + DNS over HTTPS

Filtrage DNS et vie privee avec OPNsense

Mars 2026

Sommaire

1. Pourquoi le DNS est le maillon faible

Chaque fois que vous visitez un site web, votre appareil effectue une requete DNS pour traduire le nom de domaine en adresse IP. Par defaut, ces requetes sont envoyees en clair sur le port 53, visibles par votre FAI, les routeurs intermediaires et tout acteur malveillant sur le meme reseau.

Trois risques majeurs :

• **Tracking :** Votre FAI journalise toutes vos requetes DNS et peut revendre ces donnees a des tiers.

• **Publicites et malware :** Sans filtrage, tous les domaines de tracking et de distribution de malware sont resolus normalement.

• **DNS hijacking :** Un attaquant peut rediriger vos requetes DNS vers des serveurs malveillants (man-in-the-middle).

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

2. AdGuard Home vs Pi-hole — comparatif

Les deux solutions sont des resolvers DNS locaux avec filtrage par listes de blocage. Voici les differences cles :

Interface web : AdGuard Home — Moderne, responsive | Pi-hole — Classique, fonctionnelle

DNS over HTTPS : AdGuard Home — Natif integre | Pi-hole — Necessite dnscrypt-proxy

DNS over TLS : AdGuard Home — Natif integre | Pi-hole — Configuration manuelle

Stats par client : AdGuard Home — Detaillees par appareil | Pi-hole — Basiques

Réécriture DNS : AdGuard Home — Interface graphique | Pi-hole — Via fichiers

API REST : AdGuard Home — Oui, complete | Pi-hole — Oui, partielle

Communaute : AdGuard Home — Active (Adguard) | Pi-hole — Tres grande

i Recommandation BOTUM : AdGuard Home pour les nouveaux deploiements grace au support DoH natif.

3. Installation AdGuard Home (Docker sur Proxmox)

Option A — Docker Compose

```
# Sur votre hote Proxmox ou VM Ubuntu
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

# Acceder au wizard d'installation
# http://IP-VM:3000
```

Option B — VM LXC Proxmox

```
# Dans un conteneur LXC Debian/Ubuntu
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
# Interface web : http://IP-LXC:3000
```

i Attribuez une IP fixe a votre VM/LXC AdGuard Home dans les baux DHCP OPNsense.

4. Configurer OPNsense pour rediriger le DNS

4.1 DNS par defaut dans OPNsense

```
# Services > Unbound DNS > General
# Decocher "Enable" pour desactiver Unbound
# OU : pointer Unbound vers AdGuard Home

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

4.2 Redirection NAT forcee (DNS bypass prevention)

```
# Firewall > NAT > Port Forward
# Creer une regle pour chaque VLAN :

Interface     : VLAN_LAN (repeter pour chaque VLAN)
Protocol      : TCP/UDP
Destination   : ! 192.168.1.x (inverse — tout sauf AdGuard)
Dest. port    : 53
Redirect IP   : 192.168.1.x  (IP AdGuard Home)
Redirect port : 53
Description   : Force DNS vers AdGuard Home
```

i Cette regle intercepte les appareils qui tentent d'utiliser un DNS externe (8.8.8.8, 1.1.1.1, etc.) et les redirige silencieusement vers AdGuard Home.

5. Activer DNS over HTTPS (DoH)

Dans l'interface AdGuard Home :

1. Settings > DNS Settings > Upstream DNS servers

2. Remplacer les serveurs par defaut par des serveurs DoH :

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

# NextDNS (personnalisable)
https://dns.nextdns.io/VOTRE-ID

# Quad9 DoH (focus securite)
https://dns.quad9.net/dns-query

# Mullvad (sans log)
https://base.dns.mullvad.net/dns-query
```

5.1 Mode parallele (Fastest IP)

```
# Settings > DNS Settings
# Load-balancing strategy : Parallel requests
# AdGuard Home envoie la requete a tous les upstreams
# et retourne la premiere reponse recue
```

i Activez "DNSSEC" dans Settings > DNS Settings pour valider les signatures DNS.

6. Listes de blocage recommandees

Dans Filters > DNS blocklists > Add blocklist :

AdGuard DNS filter : Publicites + malware — liste principale AdGuard

URL : https://adguardteam.github.io/AdGuardSDNSFilter/Filters/filter.txt

OISD Big : Publicites, tracking, malware — 150k+ domaines

URL : https://big.oisd.nl

Hagezi Pro : Tracking agressif — recommande

URL : https://raw.githubusercontent.com/hagezi/dns-blocklists/main/adblock/pro.txt

Steven Black Hosts : Publicites + malware — tres stable

URL : https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts

Malware Domain List : Domaines malveillants actifs

URL : https://www.malwaredomainlist.com/hostslist/hosts.txt

IoT Blocklist : IoT telemetrie et C2

URL : https://raw.githubusercontent.com/nicehash/nice-hash-blocklist/main/blocklist.txt

i Commencez avec 2-3 listes et ajustez selon le taux de faux positifs observe dans vos stats.

7. Forcer le DNS sur tous les VLANs

Appliquez les regles NAT de redirection DNS sur chaque interface VLAN definie dans OPNsense :

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

# Regle 1 : Bloquer DNS direct sortant (sauf AdGuard)
Action        : Block
Interface     : VLAN_IOT
Protocol      : TCP/UDP
Source        : VLAN_IOT net
Destination   : ! 192.168.1.x
Dest. port    : 53

# Regle 2 : Autoriser vers AdGuard uniquement
Action        : Pass
Interface     : VLAN_IOT
Protocol      : TCP/UDP
Source        : VLAN_IOT net
Destination   : 192.168.1.x
Dest. port    : 53
```

Bloquer aussi DoH direct (port 443 vers 1.1.1.1)

```
# Firewall > Rules > VLAN_IOT
# Bloquer acces direct aux IP DoH connues
# Liste : 1.1.1.1, 8.8.8.8, 9.9.9.9 (alias OPNsense)

# Creer un alias "DNS_Publics" avec ces IPs
# Puis regle Block sur port 443 vers cet alias
```

i Attention : bloquer le port 443 vers les IP DoH peut casser des applications. Testez d'abord en mode log-only.

8. Monitoring et dashboard

8.1 Dashboard AdGuard Home

• DNS Queries today : nombre total de requetes du jour

• Blocked by filters : pourcentage bloque (objectif : 15-30%)

• Blocked by SafeBrowsing : domaines malveillants interceptes

• Top clients : appareils les plus actifs

• Top blocked domains : domaines les plus souvent bloques

8.2 Export vers Grafana (apercu Billet 9)

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

# Integration Prometheus (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 Le Billet 9 couvrira l'integration complete Grafana + Prometheus pour visualiser les metriques reseau.

Article complet : blog.botum.ca/opnsense-adguard-home-dns-over-https

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

Site web : www.botum.ca • contact@botum.ca