Guide de Déploiement Souverain : AdGuard Home & Unbound

Auteur : Communautaire / Technique
Objectif : Créer un résolveur DNS récursif local, sécurisé et immunisé contre la censure et les blocages des ayants droit.

1. Architecture Théorique du Flux DNS

Ce guide documente la mise en place d'une architecture DNS locale indépendante. Au lieu de s'appuyer sur des résolveurs tiers (soumis aux censures géographiques et aux législations locales), cette solution combine le filtrage chirurgical des menaces à une résolution récursive à la racine de l'Internet.

Le cheminement d'une requête réseau s'effectue comme suit :

Appareil Client → **AdGuard Home (Port 53)** *[Filtrage des Malwares & Pubs]* → **Unbound (Port 5335 via 127.0.0.1)** *[Résolution récursive autonome + Validation DNSSEC]* → **Serveurs Racines Mondiaux (Root Servers)** → **Résolution finale sans intermédiaire.**

2. Étape A : Installation et Configuration d'Unbound

Unbound agit comme le moteur de résolution récursif. Il interroge directement les serveurs racines de l'Internet sans passer par les serveurs menteurs des intermédiaires.

Exécutez la commande suivante pour installer le paquet sur un système basé sur Debian ou Ubuntu :

```
sudo apt update && sudo apt install unbound dnsutils -y
```

Créez ensuite un fichier de configuration durci dédié à l'interconnexion locale :

```
sudo nano /etc/unbound/unbound.conf.d/adguard.conf
```

```
server:
    # Écouter exclusivement sur la boucle locale (IPv4 et IPv6)
    interface: 127.0.0.1
    interface: ::1
    port: 5335
    do-ip4: yes
    do-ip6: yes
    do-udp: yes
    do-tcp: yes

    # Durcissement de la sécurité et validation DNSSEC
    harden-glue: yes
    harden-dnssec-stripped: yes
    use-caps-for-id: no
    edns-buffer-size: 1232
    prefetch: yes
    num-threads: 1
```

```
    # Respect de la vie privée (Masquage de l'identité)
    hide-identity: yes
    hide-version: yes

    # Optimisation du cache pour architectures légères
    msg-cache-size: 4m
    rrset-cache-size: 8m
    infra-cache-numhosts: 10000
```

Redémarrez le service pour appliquer les paramètres et testez la résolution récursive directe :

```
sudo systemctl restart unbound
dig deb.debian.org @127.0.0.1 -p 5335
```

3. Étape B : Installation et Configuration d'AdGuard Home

AdGuard Home intercepte les requêtes de vos équipements locaux pour filtrer les cybermenaces, publicités et traceurs.

Option 1 : Installation native (Méthode officielle automatisée)

Exécutez le script officiel pour télécharger et installer AdGuard Home en tant que service système :

```
curl -sSL
https://raw.githubusercontent.com/AdguardTeam/AdGuardHome/master/scripts/install.sh | sh
```

Option 2 : Installation via Docker / Docker Compose

Si vous préférez l'isolation par conteneur, utilisez ce bloc de déploiement compose :

```
version: '3'
services:
  adguardhome:
    image: adguard/adguardhome
    container_name: adguardhome
    ports:
      - "53:53/tcp"
      - "53:53/udp"
      - "3000:3000/tcp"
    volumes:
      - ./workdir:/opt/adguardhome/work
      - ./confdir:/opt/adguardhome/conf
    restart: unless-stopped
```

4. Étape C : Alignement Fin des Paramètres de l'Interface Web

Accédez à l'interface d'initialisation sur le port 3000 (ex: http://IP_SERVEUR:3000). Suivez l'assistant pour configurer l'interface d'écoute DNS sur le port 53. Une fois dans le tableau de bord, rendez-vous dans **Paramètres** → **Paramètres DNS** pour appliquer l'alignement suivant :

1. Serveurs DNS amont (Upstream DNS) : Effacez les lignes existantes et saisissez les boucles locales pointant vers le port d'Unbound (une adresse par ligne) :

```
127.0.0.1:5335
[::1]:5335
```

Sélectionnez le mode d'équilibrage de charge en **Configuration personnalisée**.

2. Serveurs DNS de secours & d'amorçage (Bootstrap/Fallback) : Laissez ces cases totalement **vides**. Unbound étant ciblé via des adresses IP numériques locales brutes, AdGuard Home n'a besoin d'aucune traduction de domaine externe pour amorcer son trafic. Cela empêche également toute fuite DNS vers des serveurs tiers.

3. Optimisations et Sécurité globale (Plus bas sur la même page) :

• **Activer le sous-réseau du client EDNS (ECS) :** Décocher. Garantit l'anonymat en interdisant la fuite de votre IP locale sur le web.
• **Activer DNSSEC :** Décocher. Évite les doublons de calculs et les conflits. C'est Unbound qui valide déjà la cryptographie à la racine.
• **Intervalle de mise à jour des filtres :** Ajuster à **24 heures** dans les paramètres généraux pour soulager le processeur de la machine hôte.

4. Listes de Menaces Recommandées (Remplacement Quad9) :
Allez dans **Filtres** → **Listes de blocage DNS** → **Ajouter une liste**, puis activez la liste essentielle suivante pour blinder la protection contre les cybermenaces :
• **HaGeZi's Threat Intelligence Feeds** (Mise à jour continue contre les malwares, ransomwares et serveurs C&C;).

5. Déploiement au sein du Réseau Local (LAN)

Pour protéger vos équipements, deux méthodes s'offrent à vous :

• **Méthode Globale (Routeur/Box) :** Accédez à l'interface de votre routeur local, accédez aux paramètres du serveur **DHCP**, et remplacez le **Serveur DNS principal (DNS 1)** par l'adresse IP fixe de votre serveur AdGuard Home. *Note : Attention aux boîtiers TV opérateurs qui intègrent parfois des DNS en dur. Si un dysfonctionnement TV apparaît, utilisez la méthode ciblée.*
• **Méthode Ciblé par Appareil :** Laissez la Box internet inchangée. Allez dans les configurations de la carte réseau de vos machines critiques (PC, Serveurs) et modifiez manuellement le DNS principal pour y injecter l'adresse IP fixe de votre instance AdGuard Home.

6. Synthèse Matricielle de l'Infrastructure

Service / Composant	Interface d'écoute	Port Externe	Rôle & Avantage Technique
AdGuard Home	IP Privée LAN (0.0.0.0)	**53** (UDP/TCP)	Point d'entrée unique du LAN. Nettoyage chirurgical des malwares, traqueurs et publicités avant traitement.
Unbound	Boucle locale (127.0.0.1 / ::1)	**5335** (UDP/TCP)	Résolveur récursive souverain. Interrogation directe de la racine de l'Internet. Immunité totale contre la censure géolocalisée.
Interface Admin Web	IP Privée LAN	**3000 / 80**	Gestion des listes de filtrage, consultation du journal des requêtes et statistiques de sécurité en temps réel.
Équipements LAN Clients	Interface Physique (Eth/Wi-Fi)	Dynamique	Consomment de manière transparente une navigation accélérée par le cache local et totalement sécurisée.

Ce document technique est fourni à titre informatif et d'entraide communautaire pour l'auto-hébergement et la sécurité des systèmes d'information.
AI responses may include mistakes.