

Adguard settings on OPNsense with Unbound

Under **Settings** > **DNS Settings**:



Dashboard **Instellingen** Filters Query log Installatie gids Afmelden

DNS instellingen

Upstream DNS-servers

Een server-adres per regel invoeren. [Meer weten](#) over het configureren van upstream DNS-servers. hier is een [lijst of gekende DNS providers](#) waarvan je kan kiezen.

```
# In geval Unbound wordt gebruikt dan de cache in /home/AdGuardHome.yaml op 0. Anders cache_size: 4194304
127.0.0.1:5335
[/lan/]127.0.0.1:5335
[/]/127.0.0.1:5335
[/168.192.in-addr.arpa/]127.0.0.1:5335
```

☐ Volume balanceren
Eén server per keer bevragen. AdGuard Home gebruikt hiervoor een gewogen willekeurig algoritme om de server te kiezen zodat de snelste server meer zal gebruikt worden.

☒ Parallele verzoeken
Parallele verzoeken gebruiken om te versnellen door gelijktijdig verzoeken te sturen naar alle upstream servers.

Bootstrap DNS-servers

IP-adressen van DNS-servers die worden gebruikt om IP-adressen om te zetten van de DoH/DoT-resolvers die je opgeeft als upstreams. Opmerkingen zijn niet toegestaan.

9.9.9.10
149.112.112.10

Private omgekeerde DNS-servers

DNS-servers die door AdGuard Home worden gebruikt voor privé PTR-, SOA- en NS-verzoeken. Een verzoek wordt als privé beschouwd als het vraagt om een ARPA-domein dat een subnet binnen privé-IP-bereiken bevat (zoals "192.168.12.34") en afkomstig is van een client met een privé-IP-adres. Indien niet ingesteld, zullen de standaard DNS-resolvers van je besturingssysteem worden gebruikt, behalve de AdGuard Home IP-adressen.

AdGuard Home kon voor dit systeem geen geschikte private omgekeerde DNS-resolvers bepalen.

127.0.0.1:5353

☒ Private omgekeerde DNS-resolvers gebruiken

PTR-, SOA- en NS-verzoeken voor ARPA-domeinen die privé-IP-adressen bevatten oplossen via privé-upstreamservers, DHCP, /etc/hosts, enz. Indien uitgeschakeld, zal AdGuard Home op al dergelijke verzoeken reageren met NXDOMAIN.

☒ Omzetten van hostnamen van clients inschakelen

Indien ingeschakeld, zal AdGuard Home proberen om IP-adressen van apparaten te converteren in hun hostnamen door PTR-verzoeken te sturen naar overeenkomstige resolvers (privé-DNS-servers voor lokale apparaten, upstream-server voor apparaten met een openbaar IP-adres).

Test upstream

Toepassen

DNS-server configuratie

Ratio limiet

Het aantal verzoeken per seconde toegelaten per toestel. 0 betekent onbeperkt.

20

Lengte subnetvoorvoegsel voor IPv4-adressen

Lengte subnetvoorvoegsel voor IPv4-adressen die worden gebruikt voor snelheidsbeperking. De standaardwaarde is 24

24

Lengte subnetvoorvoegsel voor IPv6-adressen

Lengte subnetvoorvoegsel voor IPv6-adressen die worden gebruikt voor snelheidsbeperking. De

Blocking modus

- Standaard: Reageer met een nul IP adres (0.0.0.0 for A; :: voor AAAA) wanneer geblokkeerd door een Adblock-type regel; reageer met het IP-adres dat is opgegeven in de regel wanneer geblokkeerd door een /etc/hosts type regel
- REFUSED: Antwoorden met REFUSED code
- NXDOMAIN: Reageer met NXDOMAIN code
- Nul IP: Reageer met een nul IP address (0.0.0.0 voor A; :: voor AAAA)
- Aangepast IP: Reageer met een handmatige ingesteld IP adres

- ☒ Standaard
- ☐ REFUSED
- ☐ NXDOMAIN
- ☐ Nul IP
- ☐ Aangepast IP

Geblokkeerde reactie TTL

Hiermee geef je op hoeveel seconden de clients een gefilterd antwoord in de cache moeten opslaan

Opslaan

DNS cache configuratie

Hier kan de DNS cache geconfigureerd worden

Cache grootte

DNS-cachegrootte (in bytes). Leeg laten om caching uit te schakelen.

Minimale TTL overschrijven

Uitbreiden van korte Time-To-Live waarden (seconden) ontvangen van de upstream server bij het cacheren van DNS antwoorden.

Maximale TTL overschrijven

Instellen van maximum time-to-live waarde (seconden) voor opslag in de DNS cache.

☐ Optimistisch cacheren

Laat AdGuard Home reageren vanuit de cache, zelfs als de vermeldingen zijn verlopen en probeer deze ook te vernieuwen.

Opslaan

Cache wissen

Toegangs instellingen

Hier kan je toegangsregels voor de AdGuard Home DNS-server instellen

Toegangs gebruikers

OPNsense - Settings / General:

- **Prefer IPv4 over IPv6:** Checked
- **DNS Servers:** all empty

OPNsense - Services

- DHCPv4 / LAN / **DNS Servers:** All empty for all Interfaces

Unbound

- **Listen Port:** 5353
- **DNSSEC:** Checked
- **DHCP Registration:** Checked
- **DHCP Static Mappings:** Checked
- **DNS Cache:** Checked, Flush cache
- **Overrides** - non set

AdGuard Home

- **Enabled:** Checked
- **Primary DNS:** Checked
- **Upstream DNS server:**

```
127.0.0.1:5353  
[/lan/]127.0.0.1:5353  
[/]/127.0.0.1:5353  
[/168.192.in-addr.arpa/]127.0.0.1:5353
```

- When using Unbound **set cache to 0** (leave empty). In other cases use a cache_size: 4194304

Firewall (each interface, below for LAN)

- **TCP/IP:** IPv4+6
- **Protocol:** TCP/UDP
- **Source:** LAN net
- **Destination:** LAN address
- **Dest Port Range:** DNS

The screenshot shows the OPNsense web interface. The left sidebar contains navigation links: Lobby, Reporting, System, Interfaces, Firewall, Aliases, Automation, Categories, Groups, NAT, Rules, Floating, LAN (selected), Loopback, WAN, WAN_IPTV, Shaper, Settings, Log Files, and Diagnostics. The main content area is titled "Firewall: Rules: LAN". A success message states: "The changes have been applied successfully." Below this is a table of firewall rules. The table has columns: Protocol, Source, Port, Destination, Port, Gateway, Schedule, and Description. The rules listed are: 1. "LAN INBOUND IGMP, incl. allow options" (IPv4 IGMP, LAN net to 224.0.0.0/8). 2. "IPTV" (IPv4 *, LAN net to 213.75.112.0/21). 3. "Redirect all DNS traffic to This Firewall" (IPv4 TCP/UDP, LAN net port 53 (DNS) to LAN address port 53 (DNS)). 4. "Default allow LAN to any rule" (IPv4 *, LAN net to *). Below the table, there are sections for "Active/Inactive Schedule" and "Alias". A note at the bottom explains: "LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default."

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
Automatically generated rules								
<input type="checkbox"/>	IPv4 IGMP	LAN net	*	224.0.0.0/8	*	*	*	LAN INBOUND IGMP, incl. allow options
<input type="checkbox"/>	IPv4 *	LAN net	*	213.75.112.0/21	*	*	*	IPTV
<input type="checkbox"/>	IPv4 TCP/UDP	LAN net	53 (DNS)	LAN address	53 (DNS)	*	*	Redirect all DNS traffic to This Firewall
<input type="checkbox"/>	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
<input type="checkbox"/>	pass	<input checked="" type="checkbox"/> block		<input checked="" type="checkbox"/> reject		<input checked="" type="checkbox"/> log		<input checked="" type="checkbox"/> in
<input type="checkbox"/>	pass (disabled)	<input checked="" type="checkbox"/> block (disabled)		<input checked="" type="checkbox"/> reject (disabled)		<input checked="" type="checkbox"/> log (disabled)		<input checked="" type="checkbox"/> out

OPNsense

<

root@OPNsense.lan

Lobby

Reporting

System

Access

Configuration

Firmware

Gateways

High Availability

Routes

Settings

Administration

Cron

General

Logging

Miscellaneous

Tunables

Snapshots

Trust

Wizard

Log Files

Diagnostics

Interfaces

Firewall

VPN

Services

Zenarmor

Power

Help

Hostname

OPNsense

Domain

lan

Time zone

Europe/Amsterdam

Language

English

Theme

opnsense

Picture

Bladeren...

Geen bestand geselecteerd.

Networking

Prefer IPv4 over IPv6

☒ Prefer to use IPv4 even if IPv6 is available

DNS servers

DNS Server	Use gateway
	none
	none
	none
	none
	none
	none
	none
	none

DNS search domain

DNS server options

☐ Allow DNS server list to be overridden by DHCP/PPP on WAN

☐ Do not use the local DNS service as a nameserver for this system

Gateway switching

☐ Allow default gateway switching

Save

OPNsense (c) 2014-2025 Deciso B.V.

Revisie #3

Gemaakt: 24 januari 2025 17:45:41 door Gert

Bijgewerkt: 29 januari 2025 06:34:48 door Gert