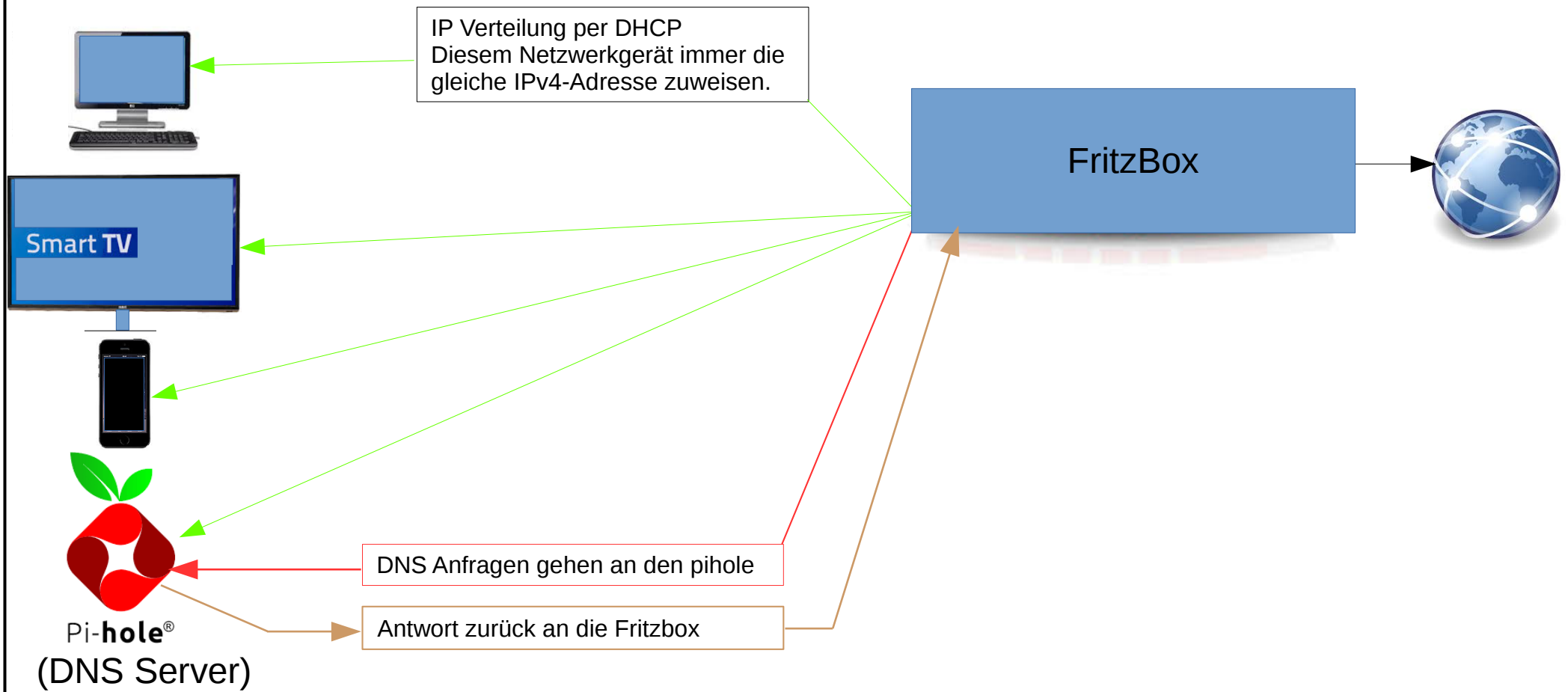


Aufbau



Einstellungen DNS Server – Bild 1

FRITZ!Box 7490

Internet > Zugangsdaten

InternetzugangIPv6LISPAnbieter-DiensteAVM-Dienste**DNS-Server**

Hier können Sie auswählen, ob für die Namensauflösung von Internet-Adressen die vom Internetanbieter zugewiesenen oder an

DNSv4-Server

☒ Vom Internetanbieter zugewiesene DNSv4-Server verwenden (empfohlen)

☐ Andere DNSv4-Server verwenden

Bevorzugter DNSv4-Server: . . .

Alternativer DNSv4-Server: . . .

DNSv6-Server

☒ Vom Internetanbieter zugewiesene DNSv6-Server verwenden (empfohlen)

☐ Andere DNSv6-Server verwenden

Bevorzugter DNSv6-Server

Alternativer DNSv6-Server

Einstellungen DNS Server – Bild 2

FRITZ!Box 7490

FRITZ!NAS

IPv4-Adressen

Geben Sie die IPv4-Adresse an, unter der die FRITZ!Box im lokalen Netzwerk erreichbar ist.

Achtung!

Änderungen auf dieser Seite können dazu führen, dass die FRITZ!Box nicht mehr erreichbar ist. Beachten Sie unbedingt die Hilfe, bevor Sie Änderungen vornehmen.

Heimnetz

IPv4-Adresse . . .

Subnetzmaske . . .

☒ DHCP-Server aktivieren

DHCP-Server vergibt IPv4-Adressen

von . . .

bis . . .

Gültigkeit Tage

Die vergebenen IP-Adressen werden nach Ablauf der Gültigkeit wieder freigegeben.

Wenn Sie einen anderen DNS-Server in Ihrem Heimnetz verwenden möchten, tragen Sie hier dessen IP-Adresse ein, damit die FRITZ!Box diese den Geräten im Heimnetz bekannt gibt.

Lokaler DNS-Server: . . .

Gastnetz

Das Gastnetz der FRITZ!Box hat einen eigenen IP-Adressbereich, aus dem die FRITZ!Box den Gastgeräten die IP-Adressen vergibt. Der Adressbereich wird von der FRITZ!Box festgelegt und ist nicht veränderbar.

IPv4-Adresse . . .

Subnetzmaske . . .

Einstellungen IPv6 Einstellungen – Bild 1

FRITZ!Box 7490

IPv6-Adressen

Wenn keine IPv6-Internetverbindung hergestellt ist, kann die FRITZ!Box Geräten im Heimnetz Unique Local Addresses (ULA) zuweisen, damit diese untereinander kommunizieren können.

Unique Local Addresses

Wählen Sie aus, wie den Geräten im Heimnetz die Unique Local Addresses (ULA) zugewiesen werden sollen.

- ☐ Unique Local Addresses (ULA) zuweisen, solange keine IPv6-Internetverbindung besteht (empfohlen)
- ☐ keine Unique Local Addresses (ULA) zuweisen (nicht empfohlen)
- ☒ Unique Local Addresses (ULA) immer zuweisen

Unique Local Address Ihrer FRITZ!Box: fd00::c225:6ff:fef1:c74c/64

☐ ULA-Präfix manuell festlegen

fd : : : /64

Weitere IPv6-Router im Heimnetz

☐ Auch IPv6-Präfixe zulassen, die andere IPv6-Router im Heimnetz bekanntgeben

☒ Diese FRITZ!Box stellt den Standard-Internetzugang zur Verfügung

Präferenz des Router Advertisement setzen. Höhere Präferenzen werden von Klienten bevorzugt.

- ☐ Niedrig
- ☒ Mittel
- ☐ Hoch

Einstellungen IPv6 Einstellungen – Bild 2

FRITZ!Box 7490

FRITZ!NAS

IPv6-Adressen

☐ Hoch

DNSv6-Server im Heimnetz

☒ DNSv6-Server auch über Router Advertisement bekanntgeben (RFC 5006)

Wenn Sie einen anderen DNSv6-Server in Ihrem Heimnetz verwenden möchten, tragen Sie hier dessen IPv6-Adresse ein, damit die FRITZ!Box diese den Geräten im Heimnetz bekannt gibt.

Lokaler DNSv6-Server:

fd00 : 0 : 0 : 0 : aaaa : bbbb : cccc : dddd

Zurücksetzen

DHCPv6-Server im Heimnetz

☒ DHCPv6-Server in der FRITZ!Box für das Heimnetz aktivieren:

Wählen Sie aus, welche Informationen der DHCPv6-Server im Heimnetz bereit stellen soll.

☒ Nur DNS-Server zuweisen

FRITZ!Box als DNS-Server via DHCPv6 bekannt geben.

☐ DNS-Server und IPv6-Präfix (IA_PD) zuweisen

FRITZ!Box als DNS-Server via DHCPv6 bekannt geben. Teile des vom Internetanbieter zugewiesenen IPv6-Netzes an nachgelagerte Router weitergeben.

☐ DNS-Server, Präfix (IA_PD) und IPv6-Adresse (IA_NA) zuweisen

FRITZ!Box wird als DNS-Server via DHCPv6 bekannt gegeben. Teile des vom Internetanbieter zugewiesenen IPv6-Netzes werden an nachgelagerte Router weitergegeben. Geräte im Heimnetz bekommen zugewiesen.

Falls mehrere DHCPv6-Server im Heimnetz aktiv sind, wird der DHCPv6-Server mit dem höheren Präferenzwert von den Heimnetzgeräten priorisiert.

Präferenz des FRITZ!Box (Wertebereich 0..255)

DHCPv6-Servers:

☐ DHCPv6-Server in der FRITZ!Box deaktivieren:

Einstellungen DNS-Rebind-Schutz

DNS-Rebind-Schutz

FRITZ!Box unterdrückt DNS-Antworten, die auf IP-Adressen im eigenen Heimnetz verweisen (DNS-Rebind-Schutz). Hier können Sie eine Liste von Domainnamen eingeben.

Domainnamen-Ausnahmen:

192.168.178.11




IP vom pi-hole

Einstellungen der Datei /etc/pihole/setupVars.conf

```
GNU nano 2.7.4                                     Datei: setupVars.conf
WEBPASSWORD=
PIHOLE_INTERFACE=eth0
IPV4_ADDRESS=192.168.178.11/24
IPV6_ADDRESS=fd00::aaaa:bbbb:cccc:dddd
QUERY_LOGGING=true
INSTALL_WEB=true
LIGHTTPD_ENABLED=1
DNSMASQ_LISTENING=single
PIHOLE_DNS_1=84.200.69.80
PIHOLE_DNS_2=2001:1608:10:25:0:0:1c04:b12f
PIHOLE_DNS_3=194.150.168.168
DNS_FQDN_REQUIRED=false
DNS_BOGUS_PRIV=false
DNSSEC=false
CONDITIONAL_FORWARDING=false
```

Einstellungen im pi-hole

Pi-hole

**Status**

- Active Temp: 44.9°C
- Load: 0.06 0.11 0.07
- Memory usage: 13.8%

MAIN NAVIGATION

- Dashboard
- Query Log
- Long term data
- Whitelist
- Blacklist
- Disable
- Tools
- Settings
- Donate
- Help

pihole Pi-hole

System Block Lists DNS DHCP API / Web interface Teleporter

Upstream DNS Servers

IPv4	IPv6	Name
<input type="checkbox"/>	<input type="checkbox"/>	Google
<input type="checkbox"/>	<input type="checkbox"/>	OpenDNS
<input type="checkbox"/>	<input type="checkbox"/>	Level3
<input type="checkbox"/>	<input type="checkbox"/>	Norton
<input type="checkbox"/>	<input type="checkbox"/>	Comodo
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	DNS.WATCH
<input type="checkbox"/>	<input type="checkbox"/>	Quad9

Custom 1 (IPv4)☒ 194.150.168.168

Custom 2 (IPv4)☐

Custom 3 (IPv6)☐

Custom 4 (IPv6)☐

Interface listening behavior

- ☐ Listen on all interfaces
Allows only queries from devices that are at most one hop away (local devices)
- ☒ Listen only on interface eth0
- ☐ Listen on all interfaces, permit all origins

Note that the last option should not be used on devices which are directly connected to the Internet. This option is safe if your Pi-hole is located within your local network, i.e. protected behind your router, and you have not forwarded port 53 to this device. In virtually all other cases you have to make sure that your Pi-hole is properly firewalled.

Advanced DNS settings

- ☐ Never forward non-FQDNs
- ☐ Never forward reverse lookups for private IP ranges

Note that enabling these two options may increase your privacy slightly, but may also prevent you from being able to access local hostnames if the Pi-hole is not used as DHCP server

- ☐ Use DNSSEC