OPNsense

Handbuch zur OPNsense

- IPv6
  - IPv6 mit festen Adressen (z.B. Rechenzentrum)
  - IPv6 mit dynamischen Adressen (z.B. Heimnetz)

- Allgemein
  - Passwort zurücksetzen

IPv6

Anleitungen zur Aktivierung von IPv6.

IPv6 mit festen Adressen (z.B. Rechenzentrum)

IPv6 mit dynamischen Adressen (z.B. Heimnetz)

Vorwort

IPv6 unterscheidet sich in einigen Dingen zu IPv4. Eine der Verbesserungen ist der Verzicht auf NAT. Dies bringt jedoch einige Änderungen mit sich. So hat man nun nicht mehr nur eine öffentliche Adresse, sondern bekommt auf die Öffentliche Adresse ein ganzes Netz geroutet. Dies wird nun vom Router bzw. der Firewall weitergegeben - dies nennt man **delegate Präfix.** Aus diesem Präfix und dem Hostanteil des entsprechenden Geräte setzt sich die IP Adresse zusammen. Da die Präfixe jedoch dynamisch sind ändern sich die Adressen der Gerät permanent, deshalb benötigt man einige Dienste wie DNSv6, DHCPv6 und Router Advertisement.

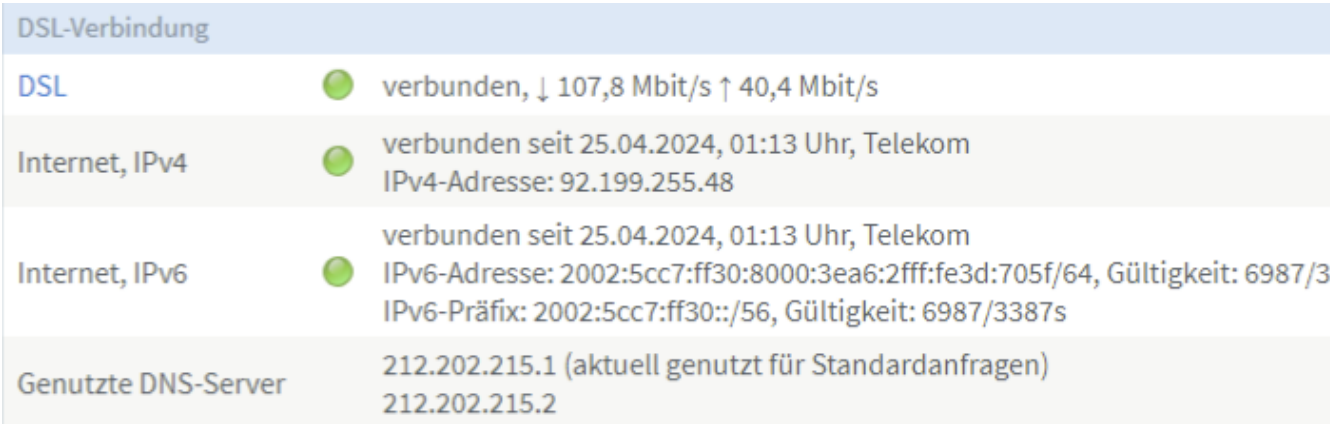
Einstellungen Fritzbox

- Melden sie sich auf ihrer Fritzbox an.
- Navigieren sie zu *Internet > Zugangsdaten > IPv6.*
- Aktivieren Sie den Punkt *IPv6-Unterstützung aktiv*.

> Ich verwende einen Anbieter, der kein natives IPv6 anbietet (Telekom Region Anschluss, angebunden über PlusNet an NetCologne). Ggf. müssen Sie in dem folgenden Punkt etwas anderes einstellen, wenn z.B. ihr Anbieter natives IPv6 anbietet.

- Wählen Sie nun bei IPv6-Anbindung den Punkt *IPv6-Anbieter mit Tunnelprotokoll verwenden*.
- Nun wählen sie bei *Verbindungseinstellungen* den Punkt *6to4*.
- Navigieren Sie nun zu *Heimnetz > Netzwerk > Netzwerkeinstellungen* > unten bei *WAN-Einstellungen* auf *weitere Einstellungen > IPv6-Einstelliungen* > und aktivieren sie die folgenden Punkte in dem öffnenden Fenster:
  - *Router Advertisement im LAN aktiv*, sowie die Option *Unique Local Addresses (ULA) zuweisen, solange keine IPv6 Internetverbindung besteht (empfohlen).*
  - *Auch IPv6-Präfixe zulassen, die andere IPv6 Router im Heimnetz bekanntgeben*.
  - *Diese Fritzbox stellt den Standard-Internetzugang zur Verfügung* mit der Option *Mittel*.
  - *DNSv6 Server auch über Routeradvertisement bekanntgeben (RFC 5006)* - lassen sie den Wert bei Lokaler DNSv6 Server stehen.

    - *DHCPv6-Server in der Fritzbox für das Heimnetz aktivieren* und dann die Option *DNS-Server und IPv6-Präfix (IA_PD) zuweisen* aktivieren.
- Gehen Sie nun zum Punkt *Internet > Freigaben > Portfreigaben*.
- Wählen sie nun das entsprechende Gerät und klicken auf das *Stiftsymbol*.
- Gehen Sie nun zu IPv6-Einstellungen und aktivieren die folgenden Punkte und speichern sie diese:
    - PING6 freigeben
    - Firewall für delegierte Pv6-Präfixe dieses Gerätes öffnen
    - Dieses Gerät komplett für den Internetzugriff über IPv6 freigeben (Exposed Host)
- Kontrollieren sie nun, ob IPv4 und IPv6 Adressen sowie weitere Präfixe (Subnetze) zugewiesen wurde - dies sollte so aussehen:



Einstellungen OPNsense

Aktivieren IPv6 in der Firewall

- Gehen Sie zu *Firewall > Settings > Advanced*.
- Aktivieren Sie die folgenden Punkte:
    - Bei *IPv6 Options* den Punkt *Allow IPv6*.
    - Bei *Network Address Translation* die Punkte *Reflect for port forwards* und *Automatic outbound NAT for reflections*.

Aktivieren IPv6 auf dem WAN Interface

- Navigieren Sie zu *Interfaces* und wählen das entsprechende *WAN* Interface auf.
- Gehen Sie zu *Generic configuration* und wählen sie bei *IPv6 Configuration Type* den Typ *DHCPv6* aus.
- Aktivieren Sie bei dem Punkt DHCPv6 client configuration die folgenden Optionen:
    - *Request only an IPv6 Präfix*
    - *Send IPv6 prefix hint*
    - Stellen Sie bei *Prefix delegation size* den Wert auf *60*.

> Hier müssen Sie ggf. ein wenig testen, ich habe von 63 runter bis 60 getestet, damit ich die entsprechende Anzahl Subnetze verwenden konnte.

>

> Sollte Sie hier jedoch einen Wert einsetzen, welcher nicht unterstützt wird - so werden den LAN Interface keine Präfixe delegiert und es sind nur die local link Adressen (fe80...) zugeordnet.

> Bei diversen testen, hatte ich das Problem das nach den Einstellungen der DHCPv6 Server nicht mehr lief bzw. sogar nicht mehr gestartet werden konnte. Ich habe dann alle IPv6 Einstellungen zurückgenommen und Stück für Stück wieder aktiviert.

Aktivieren IPv6 auf den LAN Interfaces

- Gehen Sie nach *Interfaces* und wählen das *entsprechende Interface.*
- Wählen sie bei *IPv6 configuration Type* den Typ *Track interface*.
- Wählen Sie unten bei *Track IPv6 Interface* die folgenden Punkte:
  - *IPv6 Interface* das entsprechende *WAN* Interface auswählen.
  - Bei IPv6 Prefix ID bitte 0x0 (die letzte Stelle fortlaufend)

> Sollte die Prefix ID nicht eingestellt werden können, schauen sie bitte nach, ob der oben genannte Punkt Prefix delegation Size angepasst werden muss.

  - Aktivieren Sie unter den Punkt *Manual configuration* den Punkt *Allow manual adjustment of DHCPv6 and Router Advertisements*.
- Gehen sie nun nach *Services* und dann nach *Router Advertisement*.

> Dieser Punkt ist erst verfügbar, wenn beim ersten Interface die Option *Allow manual adjustment of DHCPv6 and Router Advertisements* aktiviert wurde, vorher nicht.

- Gehen Sie nun auf das *entsprechende Interface* und wählen die folgenden Optionen:
  - *Router Advertisement* auf *Assisted* stellen.

> Sollten Sie nicht per DHCPv6 Adressen vergeben und kontrollieren wollen, so können sie auch nur SLAAC verwenden mit der Option *Router only*.

  - *Router Priority* auf *Normal* stellen.
  - *Source Address* auf *Automatic* stellen.
  - *Aktivieren* der Option *Advertise Default Gateway*.
  - *Aktivieren* der Option *Use the DNS configuration of the DHCPv6 server.*
- Prüfen Sie nach de Speichern nun die Einstellungen unter *Interfaces > Overview:*

	LAN (lan)	igb8		static	192.168.1.254/24	2002:5cc7:ff30:f2:21a:8cff:fe58:259e/64 fe80::21a:8cff:fe58:259e/64	10.1.1.1
	WAN (wan)	igb9		dhcp	192.168.177.62/24	2002:5cc7:ff30:0:20c:29ff:fec1:effd/64 fe80::20c:29ff:fec1:effd/64	192.168.177.1 fe80::3ea6:2fff:fe3d:7062
	Loopback (lo0)	lo0		static	127.0.0.1/8	::1/128 fe80::1/64	
	INTERNAL (opt7)	vlan0.2	2	static	192.168.2.254/24	2002:5cc7:ff30:f1:21a:8cff:fe58:259e/64 fe80::21a:8cff:fe58:259e/64	

In diesem Beispiel sehen Sie, das eigene Präfixe zugewiesen wurden (siehe rote Markierung) - z.B. 2002:5CC7:ff30:**f2**:21a:8cff:fe58:259e**/64** und 2002:5Cc7:ff30**:f1:**21a:8cff:fe58:259e**/64**, das WAN hat dabei die öffentliche Adresse (siehe Bild oben von der Fritzbox) 2002:5cc7:ff30:8000:3ea6:2fff:fe3d:705f/64 - die Präfixe hingegen sind geteilte Netze aus dem delegierten Prefix 2002:5cc7:ff30::**/56** (das Hauptnetz ist ein /56, die einzelne Netze haben verschiedene Präfixe und Endungen z.B. /64 - siehe grüne Markierungen).

Passen sie die Firewallregeln an

> Beachten sie auch unbedingt die Floating Rules.

Eingehend

> Erstellen sie unbedingt als erstes eine Regel auf dem WAN Interface, die den IPv6 Verkehr eingehend blockt - da bei IPv6 kein NAT angewendet wird, wäre sonst jedes System aus dem Interner erreichbar welches IPv6 aktiviert hat und keine lokale Firewall aktiv hat!

Gehen Sie nach *Firewall* > *Rules* > *WAN* > klicken Sie oben rechts auf das *Plus* und erstellen sie die folgende Regel:

- *Action: Block*
- *Quick: Apply the Action immediately on match*
- *Direction: in*
- *TCP/IP Version: IPv6*
- *Procol: any*
- *Source: any*
- *Destination: any*
- *Destination port range: any*
- *Log: aktivieren*
- *Description: IPv6 Blockregeln WAN*

Speichern und aktivieren Sie die Regel - achten sie beim positionieren der Regeln, das diese auch angewendet wird und keine andere beeinflusst. Kontrollieren Sie, ob diese greift - verwenden Sie

dafür das Live View.

Ausgehend

Erstellen Sie nun die ausgehende Regeln für IPv6, gehen Sie dazu nach Firewall > Rules > LAN (oder wie das Interface auch heißt) und klicken auf das Plus oben rechts, erstellen Sie nun die Regel mit den folgenden Einstellungen:

- *Action: Pass*
- *Quick: Apply the Action immediately on match*
- *Interface: LAN (oder wie das Interface heißt)*
- *Direction: in*
- *TCP/IP Version: IPv6*
- *Procol: any*
- *Source: LAN (oder wie das Interface heißt)*
- *Destination: any*
- *Destination port range: any*
- *Log: aktivieren*
- *Description: IPv6 Internet erlauben*

Speichern und aktivieren Sie die Regel - achten sie beim positionieren der Regeln, das diese auch angewendet wird und keine andere beeinflusst. Kontrollieren Sie, ob diese greift - verwenden Sie dafür das Live View.

Testen der Verbindung

Die Verbindung könnt ihr nun mit dem Ping Befehl testen, wenn ihr einen Namen anpingt, habt ihr den Vorteil das ihr auch direkt die Namensauflösung prüft:

```
# Ping unter Linux:
ping6 -c3 heise.de
# Ping unter Windows:
ping -6 heise.de
```

Mit dem folgenden Onlinedienst könnt ihr die IPv6 Adressen testen, ob diese von extern erreichbar sind und ob eure Firewallregeln greifen: http://www.ipv6scanner.com/cgi-bin/main.py

Weitere Informationen

- https://teqqy.de/ipv6-mit-fritzbox-und-opnsense-bei-vodafone/
- https://blog.veloc1ty.de/2019/05/26/pfsense-opnsense-ipv6-delegation-fritzbox/
- https://www.kuerbis.org/2023/03/ipv6-im-heimnetz-mit-pfsense-und-dynamischer-prefix-delegation-teil-1/

Allgemein

Passwort zurücksetzen

> Während des Vorgangs haben sie vermutlich nur die US Tastatur - achten sie besonders bei Vergabe des neuen Passwort darauf.

Melden Sie sich lokal an, sollte die OPNsense in einem Rechenzentrum stehen, so können sie sich auch mit iLO oder aber über die Console des Hypervisors anmelden.

- Starten sie die VM neu, sollten die Hypervisor Tools nicht installiert sein - so müssen sie die VM hart reseten.
- Bei der Auswahl bitte 2 wählen für *Single User Mode*.
- Sollte eine Rückfrage nach der Shell kommen (z.B. /sbin/sh) einfach auf *Enter* drücken.
- Geben Sie nun den folgenden Befehl ein:

```
/sbin/mount -o rw /
```

- Sollte eine Fehlermeldung erscheinen, dann verwenden sie wahrscheinlich ZFS als Dateisystem - geben sie dann folgendes ein:

```
/sbin/mount -u /
/sbin/zfs mount -a
```

- Wenn Sie nun das Dateisystem schreibend eingebunden ist, dann können sie das Passwort mit den folgenden Befehl ändern:

```
opnsense-shell password
```

- Stellen Sie wieder auf "local" die Anmeldung und setzen sie das Passwort zurück und starten sie das System mit dem folgenden Befehl neu:

```
reboot
```

Weitere Informationen: https://docs.opnsense.org/troubleshooting/password_reset.html