#Sonstiges | Externer Zugriff über IPv6 aufs Netzwerk

Inhaltsverzeichnis

1 Was wollen wir?

Wir wollen Zugriff auf unser Netzwerk aus dem Internet über das IPv6 Protokoll erreichen.

1.1 Erklärung Unterschied IP4 und IPv6:

1.1.1 Aufbau der IPv6 Adresse:

Die 128-Bit IPv6-Adresse besteht aus acht Kommata getrennte 16-Bit Hexadezimal-Blöcke. Die Trennung erfolgt durch einen Doppelpunkt. Zum Beispiel 2dfc:0:0:0:0217:cbff:fe8c:0

1.1.2 Unterschied IP4 & IPv6

Die 32-Bit IPv4-nutzt weltweit eindeutige öffentliche Adressen für Datenverkehrs- und „private“ Adressen.

IPv6 nutzt weltweit einzigartige Unicast- und lokale Adressen.

Beide Protokolle sind nicht kompatibel zueinander und können nicht direkt miteinander kommunizieren. Eine IPv6 ist auch aus einem reinem IP4 Netzwerk nicht aufrufbar, umgekehrt aus einem IPv6 Netzwerk sind IP4 Adressen nicht direkt ansprechbar.

Während man die IP4 Adresse im Browser direkt mit z.b. http://192.168.0.1 eingeben kann, muss man die IPv6 in eckige Klammer packen z.b. http://[2dfc:0:0:0:0217:cbff:fe8c:0]

Es empfiehlt sich aber immer bei einem Domain Anbieter seiner Wahl eine Internet Adresse zu mieten und die Auflösung der IP über einen DNS-Eintrag zu erledigen. Eine Internetadresse ist immer einfacher zu merken als eine IP.

2 Warum wollen wir das?

2.1 Hintergrund:

Bei jedem Internet Anbieter bekommt man eine IP4 Adresse vom Provider zugewiesen, über die wir im Internet surfen können.

2.2 Funktionsweise Zugriff bei IP4:

Man bekommt entweder eine feste oder eine wechselnde IP4 vom Provider zugewiesen. Die feste IP4 bleibt dauerhaft bestehen und erleichtert den Zugriff auf das Netzwerk.

Die wechselnde IP hält nur für die Dauer der Verbindung an und wechselt in unterschiedlichen Zeitabständen. Für diesen Fall bieten sich DynDNS Provider an, denen man mit Hilfe des Routers oder eines Servers in bestimmten Intervallen seine aktuelle IP4 mitteilt. Der Provider der dynamischen IP wandelt dann eine Euch zugewiesenen DNS Namen in die IP4 um.

Mit dieser IP4 oder dynamischen DNS kann man von außerhalb auf seinen Router zugreifen. Im Router richtet man nun eine Portweiterleitung an die gewünschte Zieladresse innerhalb des eigenen Netzwerkes ein. Für jeden Port kann es hierbei nur ein Zielgerät geben.

2.3 Provider ohne öffentliche IP4

Es gibt nun Provider, die einem keine öffentliche IP4 geben, sondern deren IP4 nur innerhalb des Provider Netzwerkes gültig ist, außerhalb des Provider Netzes ist diese Adresse unbekannt und somit nicht ansprechbar aus dem Internet. Gerade viele Glasfaser Anbieter bieten hier nur DS-Lite (Dual-Stack Lite). DS-Lite wird von Internetanbietern eingesetzt, die nicht über genügend öffentliche IPv4-Adressen für ihre Kunden verfügen und für diese daher IPv6-Internetzugänge mit DS-Lite einrichten.Der Vorteil bei diesen Anbietern ist allerdings das man oftmals eine festen IPv6 Adressbereich zugewiesen bekommt.

2.4 Funktionsweise Zugriff bei IPv6:

Der Provider weist einem einen IPv6 Präfix zu. Standard ist hier eigentlich /56, aber auch /64 wird häufig verwendet.

2.4.1 Beispiel:

Die Adresse von oben 2dfc:0:0:0:0217:cbff:fe8c:0 wird ungekürzt so geschrieben:

2dfc:0000:0000:0000:0217:cbff:fe8c:0000

Mit einem /56 Präfix kann man nun innerhalb seines Netzwerkes die Adressen von

2dfc:0000:0000:0000:0000:0000:0000:0000 bis

2dfc:0000:0000:00ff:ffff:ffff:ffff:ffff vergeben

Der Bereich

2dfc:0000:0000:00

führt also automatisch zu Eurem Router, der Bereich dahinter wird vom Router vergeben und weist jedem Gerät, wenn gewünscht, eine IPv6 Adresse zu.

Wichtig hierbei, die Adressen sind von überall auf der Welt aus dem IPv6 Netzwerk direkt ansprechbar, es erfolgt hier keine Portweiterleitung durch den Router wie bei IP4. Freigaben werden bei IPv6 mit einer Firewall Regel erstellt, wo nur die Ports und Adressen durchgelassen werden welche man zwingend benötigt.

3 Und wie genau geht das?

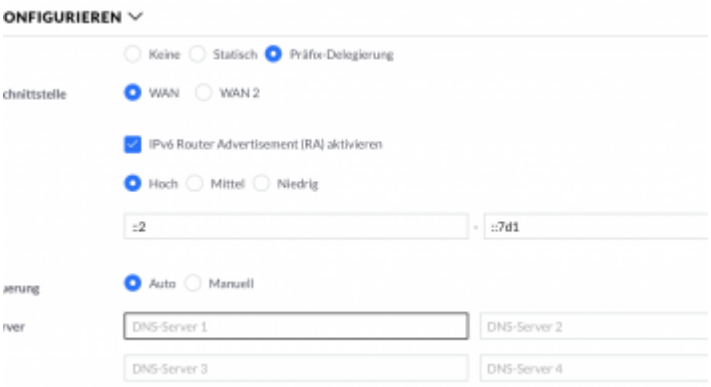
3.1 IPv6 aktivieren

Geht im Controller -> Netzwerk zu Eurem WAN Port und aktiviert DHCPv6 aktivieren, gebt die Präfix-Delegierungsgröße Eures Providers ein.

3.2 IPv6 weiter verteilen

Für jedes VLAN kann man nun die Vergabe von IPv6 Adressen aktivieren oder deaktivieren.

Hier muss nur bei IPv6 Schnittstellentyp die Präfix-Delegierung aktiviert werden, das IPv6RA wird auch aktiviert und mit Priorität Hoch versehen. Den Bereich kann man so lassen wie vorgegeben.



3.2.1 Beispiel:

An dem Bereich von oben 2dfc:0000:0000:00 hängt der Controller nun für das erste VLAN eine 01 an und nummeriert alle VLAN die aktiviert weiter durch -> 2dfc:0000:0000:0001:

Hinter diesem Bereich werden die Adressen den Geräten nun fix vorgegeben.

Aus dem Beispiel oben

2dfc:0000:0000:0000:0217:cbff:fe8c:0000 wird also

2dfc:0000:0001:0000:0217:cbff:fe8c:0000 im erstem VLAN

2dfc:0000:0002:0000:0217:cbff:fe8c:0000 im zweiten VLAN, usw.

Hinweis: Hierbei ist zu beachten, wenn man am Anfang nur in einzelnen VLAN das IPv6 aktiviert und später weitere hinzufügt, kann es sein das Unifi die VLAN Nummer verschiebt, dies ist sehr unangenehm, weil sich dadurch die kompletten Adressen eines VLAN verändern können.

3.3 IPv6 des Gerätes herausfinden:

Man kann bei IPv6 nicht einfach das Netzwerk scannen und sich die IP-Adressen anzeigen lassen, deshalb müssen diese aus dem Gerät selber ausgelesen werden. Falls diese nach der Aktivierung im Controller noch nicht zugewiesen wurde, muss das Gerät erst neu gestartet werden.

Bei Betriebssystemen wie Windows oder MacOS geht man in die Netzwerkeinstellungen und kann dort neben der IP4 auch die IPv6 auslesen.

Auf einer NAS wie eine Synology findet man diese auch in der Oberfläche unter Netzwerkeinstellungen.

Bei Geräten mit Linux System kann man sich per ssh einloggen und mittels <IP addr> die Adresse anzeigen lassen, falls das nicht funktioniert kann man auch den Befehl <ifconfig> versuchen.

Oftmals werden hier sehr viele Adressen angegeben, einige sind nur lokal im Netzwerk verfügbar, andere sind dann wirklich global verfügbar. Wichtig bei der Auswahl der korrekten Adresse ist, dass diese mit dem zugewiesenem IPv6 Präfix übereinstimmt, also im Beispiel oben mit 2dfc:0000:00 beginnt. Dies wird auch mit dem sogenannten Score hinter der Adresse angezeigt.

Die beiden wichtigsten Scopes sind der Link-Local-Scope und Global-Scope. Nur IPv6-Pakete mit einer globalen Absender-Adresse werden außerhalb des lokalen Netzwerks geroutet.

In der Unifi UDM Pro kann man sich auch per ssh einloggen und mit

Code

```
ip neighbour
```

alle IP Adressen der verbundenen Geräte anzeigen lassen. Hierbei werden auch dem Gerät bekannte IPv6 Adressen angezeigt.

3.4 Zugriff aus dem Internet:

Es gibt hierbei mehrere Lösungen, nicht alle sind kostenlos umzusetzen, aber eine feste IP4 kann bei solchen Anbietern durchaus teurerer werden, meist ist dies nur mit Business Tarifen oder der Zu Buchung einer Option möglich. Jede dieser Möglichkeiten hat Ihre eigenen Vor- und Nachteile. Dabei muss man selber entscheiden welche der Möglichkeiten zu einem passt. Es gibt durchaus auch weitere Möglichkeiten und Anbieter solcher Funktionen, die hier angegebenen Beispiel sind exemplarisch zu sehen.

3.5 Möglichkeit 1 DynDNS:

Es gibt Anbieter von dynamischen Adressen, welche auch die IPv6 unterstützen.

Leider unterstützt Unifi nicht die Benutzung des IPv6 Protokolls zur Synchronisation der eigenen IP mit einem externen Anbieter. Man kann dies aber z.b. mit einer Synology umsetzen.

Um Zugriff auf seine Synology zu bekommen installiert man das Tool „DDNS Updater 2“ und richtet es entsprechend mit seiner dynamischen DNS ein.

3.5.1 Nachteil:

Die Geräte sind über die dynamische Adresse nur aus einem IPv6 Netzwerk heraus zu benutzen. Befindet man sich in einem Netzwerk, welches kein IPv6 beherrscht, bekommt man keinen Zugriff. Dies kommt durchaus noch in einigen Handy Netzen und insbesondere aus dem Ausland heraus noch vor. Wer aber vorab prüft von woher er Zugriff benötigt kann mit dieser Lösung bereits seinen Server erreichen.

3.6 Möglichkeit 2 Portmapper:

Man benötigt im Internet einen Anbieter einer festen IP4 der über einen zugewiesenen Port die Verbindung zu seiner IPv6 weiter leitet.

Ein bekannter Anbieter ist z.b.

www.feste-IP.net

Die Preise sind durchaus attraktiv, man kauft sich Kredits und kann sich nach seinen Wünschen die Umleitung einrichten. Je nach Anzahl benutzter Ports ist es günstiger oder teurer. Eine günstige Variante ist dabei die Verwendung vom Provider generierter Ports, hier bekommt man keinen Wunsch Port, sondern z.b. den Port 69024 und leitet diesen auf den benötigten Port z.b. 80 um.

3.6.1 Nachteil:

Der komplette Traffic wird nun über diesen Provider geleitet, es empfiehlt sich also alle Verbindungen zu verschlüsseln.

Weiterhin funktioniert die Verbindung nur über das TCP Protokoll, wer UDP benötigt um z.b. eine VPN Verbindung aufzubauen, dem bleibt nur das VPN über IPSec zu nutzen und dort die Verbindung auf TCP umzustellen.

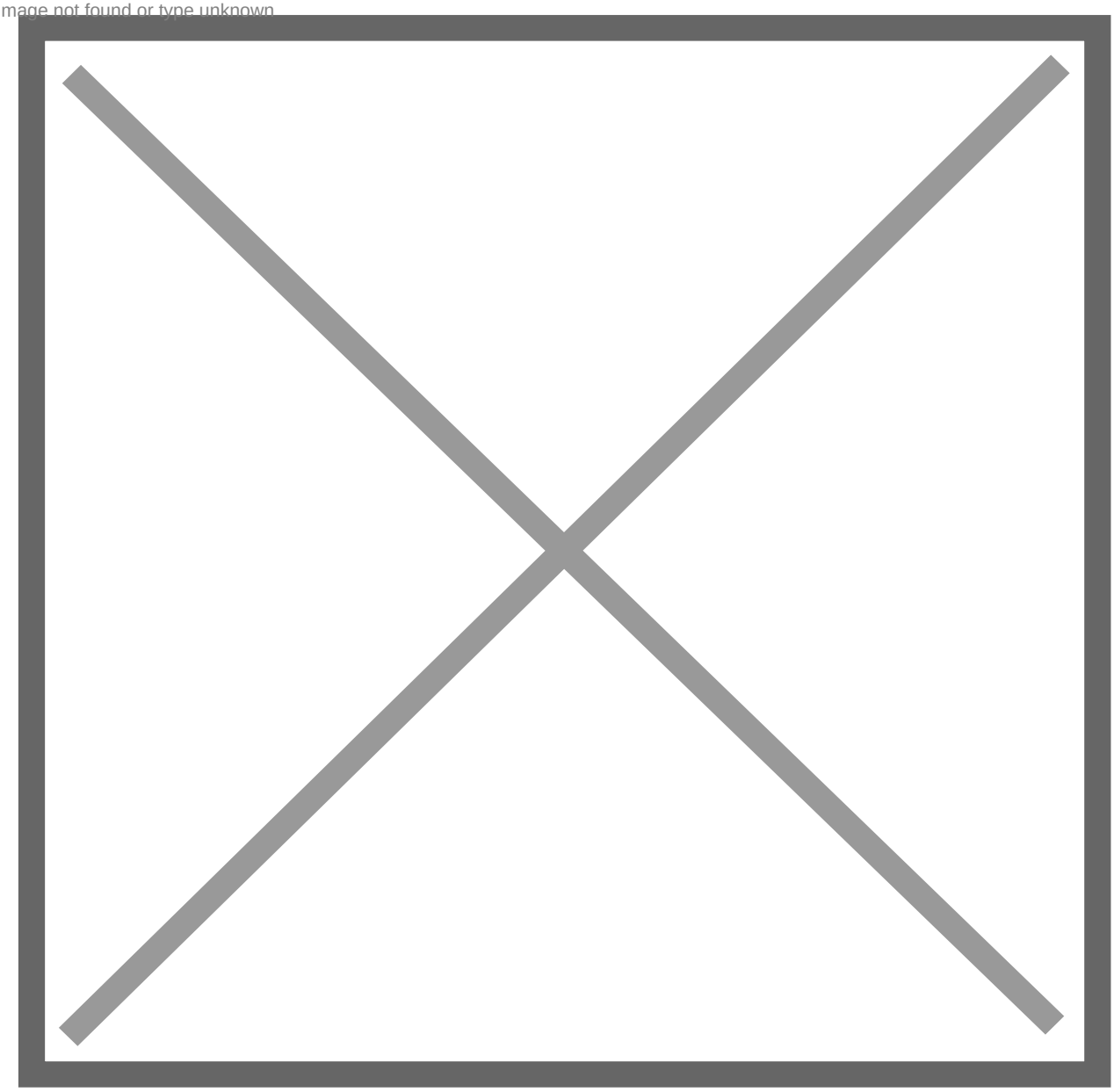
Der Zugriff auf sein Gerät funktioniert nur auf den gekauften Port und in der günstigen Variante nur mit per Zufall generierten Ports. Dies kann man umgehen indem man z.b. bei einem Domainanbieter eine Domainumleitung auf diese IP:Port durchführt, aber spätestens wenn man Server Dienste nutzen möchte, welche nur auf bestimmten Ports möglich sind, kommt man hier schnell an seine Grenzen. Für das Hosting seiner eigenen Webseite reicht dies vollkommen aus.

3.7 Möglichkeit 3 eigener VServer:

Die Königsklasse ist ein eigener Server im Internet mit einer festen IP4 Adresse. Dabei gibt es bereits für wenig Geld virtuelle Server. Wichtig bei der Auswahl ist nur, dass er eine feste IP4 beinhaltet und dass es keine Limitierung des Traffic gibt, da auch hier der Traffic über den VServer geleitet wird. Allerdings mit dem Vorteil, dass er einem selber gehört.

Als Beispiel hier die Erklärung mit dem VServer von Ionos, dieser ist in der kleinsten Variante bereits für 1€ im Monat erhältlich und reicht vollkommen aus für den Zugriff.

Image not found or type unknown



vServer Günstig Mieten » VPS ab 1€ / M. | Windows o. Linux
Virtuelle Server (VPS Hosting) » Schnell und einfach günstig mieten ? Mit Windows oder Linux ? Starke V-Server für Ihre individuellen Anwendungen
www.ionos.de

Bei der Bestellung kann man nun bereits ein Betriebssystem wählen, im Beispiel wählen wir das Ubuntu 20.04, man kann dieses aber später auch noch ändern.

Dann loggt man sich mit den Zugangsdaten ein und wählt Server&Cloud. Dort findet man auch Zugangsdaten, Root Passwort und die IP4 zum neuen Server. Hier muss evtl. beim Server auch noch die Unterstützung für IPv6 aktiviert werden.

Update (10/2022): Es gibt auch die Möglichkeit einen kostenlosen VServer zu bekommen, zb einen Oracle Cloud Server. Für weitere Anleitung schaut hier: My Blog

Der Zugang erfolgt dann über ssh, entweder über das Windows Programm Putty oder vom Mac über das Terminal. Eingeloggt wird sich über

Code

```
ssh root@IP4
```

Das Passwort sollte hier maximal kompliziert sein, um unberechtigten Zugriff auszuschließen.

Als erstes mach man ein Update des Servers, dies sollte man auch dringend immer wieder durchführen, um das System aktuell zu halten und Sicherheitslücken zu schließen.

3.7.1 Update Server

Code

```
sudo apt update && sudo apt dist-upgrade -y
reboot
```

Nach dem Neustart muss man sich erneut einloggen

3.7.2 6Tunnel

Nun wird das Programm 6Tunnel installiert mit

Code

```
apt-get install 6tunnel
```

Nun erstellt man sich ein Skript welches den Tunnel erstellt, dazu wird das Programm nano verwendet. Falls es nicht vorhanden ist, installiert man sich dieses mit <apt-get install nano> nach.

Code

```
nano /home/tunnels.sh
```

Nun öffnet sich ein Editor in dem man folgenden Text eingibt:

Bash

```
#!/bin/sh
#    Da    das    Skript    direkt    nach    dem    (Re)Boot    ausgefuehrt    wird,
#               erst               einen               Moment               warten
sleep                                                                          20s
#          Ggf.          vorhandene          6tunnel-Instanzen          beenden
killall                                                                    6tunnel
#                                                                            Pause
sleep                                                                          10s
#                                  6tunnel                                 starten
# Dies ist ein Beispiel für den Tunnel von Port 80 zu einer IPv6 mit dem Zielport 80
6tunnel 80 2dfc:0000:0001:0000:0217:cbff:fe8c:0000  80
```

Alles anzeigen

Den Editor verlässt man mit Control&X, dann einem „Y“ zum Speichern und Bestätigung mit Enter

Die IPv6 ist dabei an die Adresse des Gerätes anzupassen, welches man erreichen möchte. Die Zeilen die mit einer # beginnen sind nur Kommentare und werden nicht ausgeführt.

Die Funktionsweise von 6Tunnel ist dabei: „6tunnel IPv4-Port IPv6-Adresse IPv6-Port“

Weitere Zeilen können unter dieser Zeile einfach hinzugefügt werden um weitere Adressen oder Ports umzuleiten.

Wichtig hierbei: Auf einem virtuellen Server muss man die Ports, welche man weiterleiten möchte, auch in der Firewall frei schalten.

Das Script muss noch ausführbar gemacht werden mit

Code

```
chmod +x /home/tunnels.sh
```

Damit das Skript auch nach jedem Neustart ausgeführt wird, fügt Ihr dieses in den Crontab ein

Code

```
sudo crontab -e
```

(Bei der ersten Verwendung wird man gefragt welchen Editor man verwenden möchte, den Nano kennen wir ja schon und wählen diesen)

Nun fügt man folgende Zeile hinzu und speichert die Datei wieder ab.

Code

```
@reboot /home/tunnels.sh
```

Manuell kann man das Skript mit der Eingabe von „/home/tunnels.sh“ starten.

Mit dem Befehl „ps -ef | grep 6tunnel“ kann man sich eine Liste der aktiven Tunnel anzeigen lassen.

3.7.3 Firewall

Im Controller nicht vergessen die Firewall Regeln für den Zugriff aus dem Internet anzupassen.

Hierzu bei „IPv6 WAN eingehend“ erst entsprechende Regeln für jedes Zielgerät und den entsprechenden Ports erstellen. Falls es mehrere sind, können auch Portgruppen oder Adressgruppen erstellt werden.

3.7.4 Nachteil:

Auch hier ist die Weiterleitung auf das TCP Protokoll begrenzt, es gibt aber auch Lösungen mit einem Sockel Tunnel der auch UDP erlaubt.

3.8 Tipp zur Anwendung:

Die Anzahl Offener Ports und die Anzahl der IPv6 Adressen sollten, der Sicherheit wegen, so gering wie möglich genutzt werden. Es ist oftmals wesentlich effektiver den Zugang über einen Reverse Proxy Server zu gewähren. Hierzu kann man eigene Domains oder Subdomain auf die IP4 des VServers umleiten, diese werden über den Tunnel an einen Reverse Proxy Server geleitet und von dort an die entsprechenden Server verteilt.

Update (28.10.22: Schaut auch zu diesem Thema das WIKI #Sonstiges | Wireguard Reverse VPN Tunnel erstellen auf.

3.9 Disclaimer:

Alle Anleitungen/Tutorials sind nach bestem Wissen und Gewissen verfasst, gehen immer von den definierten Software/Firmware-Versionen aus und sind auf das englische GUI ausgelegt.

Es gibt keine Garantien auf Erfolg. Im Falle eines Misserfolges hilft aber sicherlich die Community hier immer weiter.

Keiner der Autoren oder der Betreiber des Forums ist für die aus der Nutzung resultierenden Probleme/Herausforderungen verantwortlich.

Jegliche hier beschriebenen Schritte erfolgen ausnahmslos in eigener Verantwortung des Durchführenden. Eltern haften für ihre Kinder.

Auswählen:

Gültige Software-Version Keine Firmware-Relevanz!