Zugriff auf Server oder eingehendes VPN mit DS-Lite-Anschlüssen

Wer z.B. bei einem günstigen DSL-Anbieter oder meist bei den Kabel-Anbietern (um diese geht es nachfolgend) mit einem DS-Lite-Anschluss bedient wird, hat zwar in der Regel beim durchschnittlichen Surfen keine Probleme, bekommt aber beim Betrieb eigener öffentlich zugänglicher Server oder wenn eingehendes VPN verwendet werden soll Schwierigkeiten, da zwar ein IPv6-Subnetz zur Verfügung steht oder keine öffentlich zugängliche IPv4-Adresse.

Mal abgesehen von den Gegebenheiten des Kabelanschlusses, da es ein shared medium ist (je mehr dran hängen, desto bescheidener wird’s) und meist die Upload-Rate eher mäßig ausfällt, macht einem das Fehlen einer öffentlichen IPv4-Adresse das Leben schwer, da IPv6 nicht unbedingt überall funktioniert.

Bei (Business-)DSL und Standleitungen sieht die Welt in der Regel anders aus. Je nach Region kann die Lage allerdings eine ganz andere sein wie Gespräche mit Kollegen neulich auf einer Schulung zeigten. Mitunter ist DSL keine Lösung, da nicht verfügbar oder grottenschlecht, so das dann eigentlich nur Kabel übrig bleibt (teurere Standleitungen, sofern sie überhaupt angeboten oder gebaut werden und SkyDSL lassen wir mal außen vor). Da es ja nach Anbieter oder sogar mit dem gleichen Anbieter und unterschiedlichen Ansprechpartner durchaus kuriose Geschichten geben kann, kommt erschwerend hinzu.

Eine öffentliche IPv4-Adresse gibt es im Regelfall nur mit Geschäftskundentarif, sofern verfügbar. Ein Gewerbenachweis kann dafür nötig sein, so mancher Kollege berichtete dabei, das mal danach gefragt wird, mal nicht, also irgendwie nicht einheitlich. Richtig witzig wurde dieses Thema bereits bei freien Berufen, da dort i.d.R. kein Gewerbe angemeldet ist. Ob der Anbieter das dann akzeptiert ist wiederum so eine (weitere) Sache.

Lange Vorrede. Jetzt hat es uns dieses Thema erwischt bei einer Kundin (freier Beruf) und nur ein Vodafone- (vormals Kabel Deutschland) Anschluss vorhanden. Es soll ein VPN verwendet werden, die Daten bleiben im Haus, also eingehend. Vorhanden ist eine AVM FRITZ!BOX 6490 Cable vom Anbieter. Der Anruf bei der Hotline war einigermaßen ernüchternd: Ja, Business-Tarif mit IPv4 wäre möglich, aber erst nach Ablauf der restlichen Vertragslaufzeit (ca. ein Jahr) und andere aktuell genutztes Tarif-Vorteile (TV/Handy/…-Komplettpaket) würden verloren gehen. Man kann sagen: “Doppelautsch” und meiner Meinung nach nicht im Sinne des Kunden, genau genommen auch nicht im Sinne des Anbieters. So lange und mit so vielen Nachteilen konnte und wollte man nicht warten, also musste ein Plan B her.

Dieser sieht so aus, das mit von IPv4 auf IPv6 tunnelt oder wenn man so will umleitet. Das Ganze geht relativ einfach und schnell mit wenig Aufwand von statten. An dieser Stelle kommt ein wenig Linux und das Paket 6tunnel ins Spiel, mit dessen Hilfe das Vorhaben schnell und gut umgesetzt werden kann. Auf diese Weise können recht bequem TCP-Verbindungen von IPv4 auf IPv6 umgeleitet werden. UDP- oder IPsec geht (leider) nicht.

Nebenbei bemerkt: Wem das Einrichten und betreiben eines Root- oder vServer zu aufwendig ist, der kann auf Dienste wie z.B. Feste-IP.Net – Portmapper (kostenpflichtig) zurückgreifen.

Voraussetzungen

Ein Root- oder vServer mit einer öffentlichen IPv4- und IPv6-Adresse und einem beliebigen Linux oder BSD. Nachfolgend wird Debian verwendet.

Zugang zum Provider-/Kabel-Router. In diesem Fall die zuvor erwähnte FRITZ!BOX, die Daten waren der Kundin bekannt, von daher kein Problem.

Die IPv6-Adresse des Routers/der FRITZ!BOX und des dahinter liegenden OpenVPN-Servers müssen bekannt sein. Beides lässt sich am Beispiel der FRITZ!BOX auf der Status-Seite und in der Heimnetzübersicht auslesen:

Ein OpenVPN-Server hinter dem Provider-/Kabel-Router. Das IPsec-basierte VPN der FRITZ!BOX kann aufgrund der Gegebenheiten nicht verwendet werden. Da die Kundin ein Synology-NAS einsetzt, war OpenVPN kein Problem. Alternativ kann z.B. ein Raspberry Pi, pfSense, OPNsense, usw. verwendet werden. Wichtig ist, das man den OpenVPN-Server von “udp” (Voreinstellung/Standard) auf “tcp” umstellen kann.

Schritt 1: Root- oder vServer vorbereiten

Wer (noch) keinen solchen Server hat kann günstig z.B. bei active-servers einen Mieten oder das kostenlose DHP Minipaket von KAMP nutzen. Letztgenanntes wurde für dieses Szenario herangezogen.

Wofür man sich entscheidet ist vom persönlichen Anspruch als auch ggf. den Datenmengen abhängig. KAMP beschränkt auf 10GB mit Gigabitgeschwindigkeit pro Tag (danach wird auf 10Mbit reduziert, kann erweitert werden). Damit kann man imho schonmal was anfangen. Wichtig ist, das man sich alle paar Wochen mal am ControlCenter anmeldet, da man sonst wegen Inaktivität bzw. Nicht-Nutzung rausfliegt.

Da nur ein wenig Netzwerkverkehr durchgeleitet wird, werden keine großartigen Ressourcen benötigt. Von daher Reichen die eine vCPU, der 1GB RAM und die 25GB Storage dicke aus. Als Betriebssystem wird schlicht das aktuelle Debian mit den Vorgaben installiert.

Bei KAMP wird “ab Werk” zunächst keine Verbindung zum vServer zugelassen. Dies verhindert die Firewall des DHP. Das installierte Linux lässt sich über die Konsole des DHP ControlCenter konfigurieren, alternativ kann man “ssh” (Port 22/tcp) freischalten. Für OpenVPN wird der Port “1194/tcp” (Nicht udp!) benötigt. Möchte man auch auf die FRITZ!BOX von extern zugreifen, so ist der entsprechende Port freizuschalten.

Hinweis: Der Port, den die FRITZ!BOX verwendet, wird einmalig dynamisch bei der Einrichtung von z.B. MyFRITZ festgelegt, dieser kann unter “Internet – Freigaben” eingesehen bzw. geändert werden.

Schritt 2: 6tunnel installieren, konfigurieren und automatischen Start einrichten

Läuft der Root- bzw. vServer soweit, kann 6tunnel installiert werden:

```
apt install 6tunnel
```

Die Syntax des Tools ist simple:

```
sudo 6tunnel 1194 <Ziel-IPv6-Adresse_oder_Hostname> 1194
```

So würde z.B. die Weiterleitung von OpenVPN schon funktionieren. Für jeden Port muss eine eigene 6tunnel-Instanz gestartet werden. Damit das automatisch z.B. nach einem Reboot funktioniert, kann man das Ganze als Shell-Skript verpacken und mittels cron ausführen lassen:

```
#!/bin/sh

# Da das Skript direkt nach dem (Re)Boot ausgefuehrt wird,
# erst einen Moment warten

sleep 10s

# Ggf. vorhandene 6tunnel-Instanzen beenden

killall 6tunnel

# Pause

sleep 10s

# 6tunnel starten

# FritzBox
6tunnel 49073 <Ziel-IPv6-Adresse_der_FRITZ!BOX> 49073

# OpenVPN
```

```
6tunnel 1194 <Ziel-IPv6-Adresse_des_Synology-NAS> 1194
```

Beim Test gab es direkt nach dem Neustart erstmal Schwierigkeiten, das nicht alle Tunnel aufgebaut wurden, daher die Pause von 10 Sekunden.

Nicht vergessen: Das Skript mittels “chmod +x tunnels.sh” ausführbar machen!

Dieses Shell-Skript muss zwingend mit root-Rechten ausgeführt werden. Daher es im crontab des root-Benutzers eintragen:

```
sudo crontab -e
```

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

Ab nun werden die Tunnel direkt nach dem Neustart, genau genommen nach der Pause, aufgebaut.

Schritt 3: Die FRITZ!BOX-Freigabe(n) einrichten

Die FRITZ!BOX-Firewall muss die Anfragen zu sich selbst bzw. zum OpenVPN-Server durchlassen. Dazu die entsprechenden Freigaben unter “Internet – Freigaben – Portfreigaben” erstellen:

Wichtig: Nur den “Internetzugriff über IPv6” aktivieren, andernfalls klappt es in dieser Konstellation nicht!

Bemerkung: Für die FRITZ!BOX selbst muss keine gesonderte Freigabe erstellt werden, dies geschieht z.B. bei der Einrichtung von MyFRITZ automatisch und wird an dieser Stelle auch nicht angezeigt.

Schritt 4: OpenVPN-Server einrichten

Je nachdem was man für einen OpenVPN-Server betreibt, fällt die Einrichtung unterschiedlich komplex aus. Wie bereits erwähnt kommt hier ein Synology-NAS zum Einsatz, daher ist die Einrichtung sehr einfach:

- Über das “Paket-Zentrum” den “VPN Server” installieren.
- Aus dem Hauptmenü dann “VPN Server” starten.
- Unter “VPN Server einrichten” auf “OpenVPN” klicken.

Wenn man möchte, kann man die Voreinstellungen belassen. Wichtig ist nur das Protokoll von “udp” auf “tcp” zu ändern:

Hinweis: Unter “Privileg” können die VPN-Benutzer eingeschränkt werden. Es sollten nur die Benutzer das Recht haben sich per VPN einzuwählen, für die es relevant ist.

- Abschließend auf “Konfigurationsdatei exportieren” klicken.

Schritt 5: OpenVPN-Client installieren und Einstellungen importieren

Je nach Betriebssystem stehen verschiedene OpenVPN-Clients zur Verfügung. Für Windows z.B. das Original oder die Variante von Securepoint, für MacOS z.B. Tunnelblick, usw. Unter Windows verwende ich gerne den Client von Securepoint, da dieser durch das “versteckte” Protokoll und die bessere farbliche Statusmeldung für den gemeinen Anwender leichter zu verstehen bzw. zu handhaben ist.

Bevor man nun die zuvor exportierte Konfigurationsdatei importiert, muss man das ZIP-Archiv entpacken und die darin enthaltene “VPNConfig.ovpn”-Datei editieren. Bei “YOUR_SERVER_IP” muss die IPv4-Adresse des vServers eingetragen werden. Nun kann die Datei in den jeweiligen OpenVPN-Client importiert werden. Beim (ersten) Verbindungsaufbau wird man nach Benutzername und Kennwort gefragt. Es gelten die gleichen Angaben, wie wenn man z.B. ein Netzaufwerk verbindet.

(Abschluss-)Bemerkung

Die hier vorgestellte Lösung ist nicht der einzige Weg, neben 6tunnel gibt es weitere Optionen, auch ließe sich mittels VPN noch was drehen. Mir erschien dieser Weg neben der Nutzung externer Portmapper-Dienste soweit als möglichst einfachster und kostengünstigster.

Quellen

Björn’s Techblog – Server hinter Unitymedia DS-Lite Anschluss betreiben

bjoerns1983/6tunnel_command.sh

wojtekka/6tunnel

ubuntu manuals – 6tunnel

askubuntu – How to set up a root cron job properly

nixCraft – Linux Execute Cron Job After System Reboot

Update 26.06.2018

Zur Info:

Feste-IP.net – Supportforum – Anleitung OpenVpn Unitymedia/DS-Lite Iphone

Neben 6tunnel soll das Ganze, gemeint das Weiterleiten von IPv4 zu IPv6, zudem mittels socat oder xinetd gehen:

serverfault – Use iptables to forward ipv6 to ipv4?

Quelle: https://www.andysblog.de/zugriff-auf-server-oder-eingehendes-vpn-mit-ds-lite-anschluessen

Eindeutige ID: #1192
Verfasser: n/a
Letzte Änderung: 2026-03-06 12:09