VPN-Zugriff über IPv6 für kleine Unternehmen

von Thomas Kestler, 10.07.2017

Inhaltsverzeichnis

Einleitung

Kaum ein kleines Unternehmen kommt heute ohne Internet aus. Meist nutzen die Firmen einen kostengünstigen ADSL- oder VDSL-Anschluss, der eigentlich eher für Privatkunden ausgelegt ist. Auch die verwendeten Router sind in der Regel sehr einfach gestrickt und bieten Zugriffe von außen auf das Firmennetz nicht oder nur bedingt. Gerade ein solcher Fernzugriff für Mitarbeiter und Inhaber ist aber oft gewünscht und hilfreich. Es existieren verschiedene Lösungsansätze, welche sich in der Praxis auch bewährt haben. Mit der zunehmenden Umstellung der Provider von IPv4 auf IPv6 kann der Fernzugriff zur Herausforderung werden.

Dieses Dokument gibt einen Überblick und zeigt Lösungswege anhand der OpenSource-Lösung OpenVPN auf. Selbstverständlich gibt es auch weitere Lösungen, z. B. Business-Router.

Technische Grundlagen

Im Folgenden beschreibe ich die technischen Grundlagen und Unterschiede bei IPv4 und IPv6.

IPv6 – warum?

Das Internet-Protocol (IP) hat sich über viele Jahre bewährt und das Internet erst möglich gemacht. Da aber nur 32 Bit für IP-Adressen vorgesehen waren, ließen sich nur maximal 4 Mrd. Geräte adressieren. Bei mehr als 7 Mrd. Menschen auf der Welt (und oft mehreren Geräten pro Person in entwickelten Ländern) war klar, dass dies nicht ausreichen wird. Erschwerend kommt hinzu, dass die Vergabe von Adressbereichen an Provider und Firmen die real verfügbaren Adressen deutlich weiter einschränkte, so dass es tatsächlich zu einer Knappheit kam. Deshalb wurde über Jahre das erweiterte IPv6-Protokoll erarbeitet und schrittweise eingeführt. IPv6 nutzt 64-Bit für die Adressierung und ermöglicht damit sehr viel mehr Adressen (mehr als genug). Die großen Backbone-Netze des Internet sind längst auf IPv6 migriert und auch große Firmen nutzen IPv6 schon länger.

Die meisten kleinen Firmen nutzten intern und extern IPv4. Intern nutzten die Geräte meist einen Adressbereich 192.168.x.y und extern wurde dem Router eine temporäre IPv4-Adresse wie z. B. 83.115.116.87 zugewiesen, die sich von Zeit zu Zeit änderte (Zwangstrennung[1]).

Schrittweise Migration

Die Provider bereiteten die schrittweise Migration der Endkundenanschlüsse vor. Wer noch alte Router hatte, der blieb zunächst intern und extern auf IPv4. Wer einen neuen Router bestellte, der bekam je nach Provider intern IPv6 oder IPv4 und extern je nach Anschlusstechnik in der Vermittlungsstelle. Anfangs konnte es also sein, dass intern bereits IPv6 genutzt wurde, extern aber IPv4. Die Migration erfolgte aber so schnell, dass meist schon IPv6 in den Vermittlungsstellen (DSLAM) verfügbar war und der Router intern IPv6 nutzte und extern entweder IPv6 und IPv4 parallel oder nur IPv6 nutzte.

1 Der Provider will stabile IP-Adressen vermeiden, damit er diese flexibel nutzen kann. Außerdem könnte man das Feature ja auch kostenpflichtig anbieten.

Dies bringt uns zu zwei unterschiedlichen Anschlusstechniken, welche zur Herausforderung werden können:

- DualStack (DS) – extern IPv4 und IPv6 verfügbar
- DualStack Lite (DS-Lite) – extern nur IPv6 verfügbar

Bei DS kann der Router selbst über eine IPv4-Adresse angesprochen werden und bestehende Anwendungen wie VPN's laufen einfach weiter wie bisher.

Bei DS-Lite ist das nicht so einfach möglich, da der Router keine IPv4-Adresse mehr bekommt, auch wenn nach außen eine IPv4-Adresse simuliert[2] wird. Bestehende Anwendungen müssen migriert werden!

Der Screenshot zeigt einen DSL-Router an DS-Lite, es ist nur IPv6 verfügbar.

Welche Technik zum Einsatz kommt hängt vom Provider ab. Die Telekom bietet DS, andere wie M-Net bieten DS-Lite (da günstiger). Insbesondere beim Provider-Wechsel sollte man sich also gut informieren. Auf lange Sicht wir IPv4 aber aussterben. Die Telekom plant angeblich ab 2018 einen Abbau der IPv4-Anschlusstechnik[3].

NAT und Port-Forwarding

In der guten alten IPv4-Welt waren die Dinge überschaubar. Der Router verwaltete die Geräte im Firmennetz im Adressbereich 192.168.x.y. Griff ein Computer auf `spiegel.de` zu, so merkte sich das der Router, setzte seine externe IPv4-Adresse als Absender ein und nahm die Antwort von `spiegel.de` entgegen, um sie dem Computer im internen Netz dann weiterzuleiten. Man spricht von NAT (Network Address Translation)[4].

Diese Weiterleitung erfolgte immer nur dann, wenn vorher ein Computer aus dem internen Netzwerk auf eine externe Adresse zugegriffen hatte. Selbst wenn ein interner Computer z. B. auf Port 80 selbst für Anfragen bereit stand, war er von außen nicht erreichbar. Die war aus Sicherheitsgründen durchaus wünschenswert, aber wenn man eben doch von außen erreichbar sein wollte, musste man den Router so konfigurieren, dass er auf seiner externen IPv4-Adresse und einem vorgegebenen Port (hier 80) Anfragen entgegen nahm

2 Lesenswerter Artikel zum Thema: Elektronik Kompendium - IPv6-Tunneling mit 6in4 / 6to4 / 6over4 / 4in6 https://www.elektronik-kompendium.de/sites/net/1904031.htm

3 Eine endgültige Bestätigung dafür lies sich bislang aber im Netz nicht finden. Aus Kostengründen scheint es aber naheliegend, dass die Telekom IPv4 zurückbaut, bzw. abschaltet.

4 https://de.wikipedia.org/wiki/Netzwerkadress%C3%BCbersetzung

und an den internen Computer weiterleitete. Man spricht vom Port-Forwarding[5]. Für die Einrichtung eines VPN (Virtual Private Network) z. B. mit OpenVPN musste man ein Port-Forwarding für den Port 1194 einrichten.

Bei IPv6 findet (prinzipiell) kein NAT statt, da jedes Gerät seine eigene externe IPv6-Adresse erhält.

Dynamisches DNS

Das Domain Name System verwaltet Domainnamen wie spiegel.de und die zugehörigen IP-Adressen. Will ein Benutzer die Seite `spiegel.de` aufrufen, erfragt der Browser beim DNS die zugehörige IP-Adresse und zwar entweder die IPv4-Adresse oder die IPv6-Adresse, je nachdem, in welchem Netzwerk er sich befindet. Für die IPv4-Adresse steht deshalb im DNS ein sogenannter A-Record, für die IPv6-Adresse ein AAAA-Record. Bei Servern wie `spiegel.de` bleibt die IP-Adresse stabil, daher ändert sich der Eintrag im DNS nur sehr selten.

Bei den DSL-Routern ändert sich die IP-Adresse (egal, ob IPv4 oder IPv6) öfters, das bestehende DNS kommt da also nicht hinterher. Daher hatten findige Entwickler vor Jahre ein dynamisches System entwickelt, bei dem der Router oder ein Computer hinter dem Router regelmäßig seine externe IP-Adresse mitteilt, so dass das DynDNS stets auf die aktuelle IP zeigt. Mittlerweile gibt es zahlreiche Anbieter, manche kostenlos, manche gegen Gebühr. Die meisten unterstützten IPv4 und IPv6, bei einigen muss man IPv6 erst extra konfigurieren.

Viele Router unterstützen einige der etablierten DynDNS-Dienste in ihrem Konfigurationsmenu. Allerdings scheinen die Router-Entwickler dazu das Thema IPv6 nicht bis zum Ende durchdacht zu haben.

IPv6 interne und externe Adressen

Während bei älteren Router und IPv4-Technik der Router eine einzige externe IPv4-Adresse erhielt und jeder Computer im Netzwerk eine einzige interne, verhält es sich bei IPv6-fähigen Routern durchaus anders.

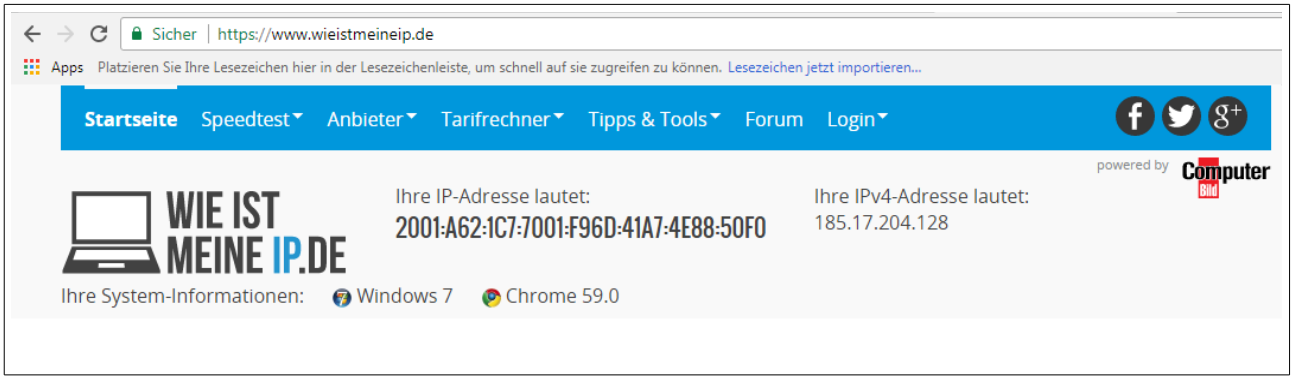
IPv6 enthält zahlreiche Erweiterung im Adressschema, so dass man auch Gruppen von Geräten bilden und per Unicast oder Multicast ansprechen kann. Dies führt dazu, dass ein Computer in einem IPv6-Netzwerk gleich mehrere IP-Adresse erhalten kann:

5 https://de.wikipedia.org/wiki/Portweiterleitung

```
C:\Users\test>ipconfig

Windows-IP-Konfiguration

Drahtlos-LAN-Adapter Drahtlosnetzwerkverbindung:

   Verbindungsspezifisches DNS-Suffix: fritz.box
   IPv6-Adresse. . . . . . . . . . . : 2001:a62:1cc:f701:51b2:75c8:5cc8:1c75
   IPv6-Adresse. . . . . . . . . . . : fd00::51b2:75c8:5cc8:1c75
   Temporäre IPv6-Adresse. . . . . . : 2001:a62:1cc:f701:2940:bb95:ac1c:e4fc
   Temporäre IPv6-Adresse. . . . . . : fd00::2940:bb95:ac1c:e4fc
   Verbindungslokale IPv6-Adresse  . : fe80::51b2:75c8:5cc8:1c75%14
   IPv4-Adresse  . . . . . . . . . . : 192.168.178.20
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . : fe80::cece:1eff:fe69:9403%14
                                       192.168.178.1
```

Der Computer im Beispiel hat also vier IPv6-Adressen und eine IPv4-Adresse vom Router erhalten. Einige Adressen davon sind rein intern, aber andere haben globale Gültigkeit (die 2001-er)! Von außen beliebig ansprechbar ist der Computer deshalb noch nicht, da die Firewall des Routers darüber wacht, dass zunächst nur Antworten auf ausgehende Anfragen beantwortet werden dürfen. Es ist aber wichtig zu wissen, dass jetzt jedes (!) Endgerät eine globale IPv6-Adresse erhält. Die Temporäre IPv6-Adresse soll eine Nachverfolgung eines Benutzers erschweren, da die Primäre IPv6-Adresse aus festen Bestandteilen immer gleich gebildet wird[6]. Daher ändert sich die Temporäre Adresse von Zeit zu Zeit.

Hier ein Beispiel zur Abfrage dieser (temporären) IPv6-Adresse:



Die IPv4-Adresse ist eine simulierte Adresse.

Soll ein interner Computer von außen erreichbar sein, hängt es stark vom Router und der verfügbaren Anschlusstechnik ab (DS / DS-Lite). Bei DS hat der Router eine IPv4-Adresse und kann über Port-Forwarding den Computer „freigeben“. Bestehende VPN-Anwendungen (z. B. OpenVPN) laufen ohne Änderung weiter.

Bei DS-Lite hat der Router nur eine externe IPv6-Adresse (also keine IPv4-Adresse mehr). Der VPN-Zugriff (mit OpenVPN) oder ein Zugriff auf den Web-Server auf dem Computer erfolgt über dessen externe IPv6-Adresse und dafür muss die Firewall des Routers dies zulassen. Achtung: Der Zugriff von außen erfolgt jetzt über die externe IPv6-Adresse des

6 Elektronik Kompendium: Privacy Extensions (IPv6) - https://www.elektronik-kompendium.de/sites/net/1601271.htm

Computers (und nicht die des Routers)! Und genau deshalb muss der DynDNS-Eintrag eben auf diesen Computer zeigen und nicht auf den Router!!! D. h. dass der Computer selbst über einen Update-Client seine externe IPv6-Adresse an den DynDNS-Dienst melden muss! Eine Konfiguration des DynDNS-Dienstes im Router selbst macht nur dann Sinn, wenn der Router gleichzeitig auch ein Port-Forwarding vornimmt.

Zusammenfassung

Die Einleitung zeigte also dass mit der schrittweisen Einführung von IPv6 Änderungen durchaus neue Herausforderungen entstehen. Prinzipiell ist IPv6 als Fortschritt zu begrüßen, die Umsetzung mit unterschiedlichen Anschlusstechniken und sehr unterschiedlichen Implementierungen in Routern und Betriebssystemen machen es aber teilweise schwierig.

Eine konsequente Umsetzung (im Router) wäre es z. B. gewesen, DynDNS-Aktualisierungen je nach internem Gerät vorzunehmen plus Firewall-Freischaltung für einzelne Ports auf diesen Geräten und dafür das Port-Forwarding ganz zu entfernen. Aber ein Mischmasch aus allem wie z. B. in der Fritz!Box 7430 SE ist nicht wirklich hilfreich.

Umsetzung eines VPN mit OpenVPN

Das grundsätzliche Aufsetzen eines VPN mit OpenVPN ist im Internet hinreichend beschrieben. Die Crux liegt einfach darin, welche Anschlusstechnik bei der Firma und den Mitarbeitern vorliegt.

Am einfachsten ist es, wenn die Firma IPv4 nutzen kann, dann geht die Einrichtung wie in den Wikis beschrieben leicht von der Hand. Mitarbeiter können zuhause noch beliebige Technik haben und der Zugriff über IPv4 wird klappen. Auch wenn ein Mitarbeiter schon eine DS-Lite-Anschluss bekommen hat, sind Zugriffe auf IPv4-VPN's möglich (sofern nicht der Provider oder eine Firewall) reinfunken.

Hat die Firma einen DS-Lite-Anschluss und folglich nur IPv6 am Router, so wird die Konfiguration etwas sportlicher. Zum einen müssen alle Mitarbeiter jetzt über UDP6 zugreifen, zum anderen muss DynDNS für IPv6-Adressen konfiguriert werden. Außerdem muss im Firmen-Router die Portfreigabe/weiterleitung konfiguriert werden.

Auch möglich ist ein Zugriff von einer reinen IPv4-Umgebung (z. B. Mobile Hotspot) zuhause auf ein IPv6-basiertes Firmennetz. Die meisten aktuellen Betriebssysteme bieten Protokolle wie 6in4, 6to4 oder Teredo dafür an.

UDP6 in OpenVPN nutzen

Die Konfigurationsänderung ist einfach, in der server.client und in der client.ovpn muss nur der Eintrag für das Protokoll geändert werden:

```
proto udp6
```

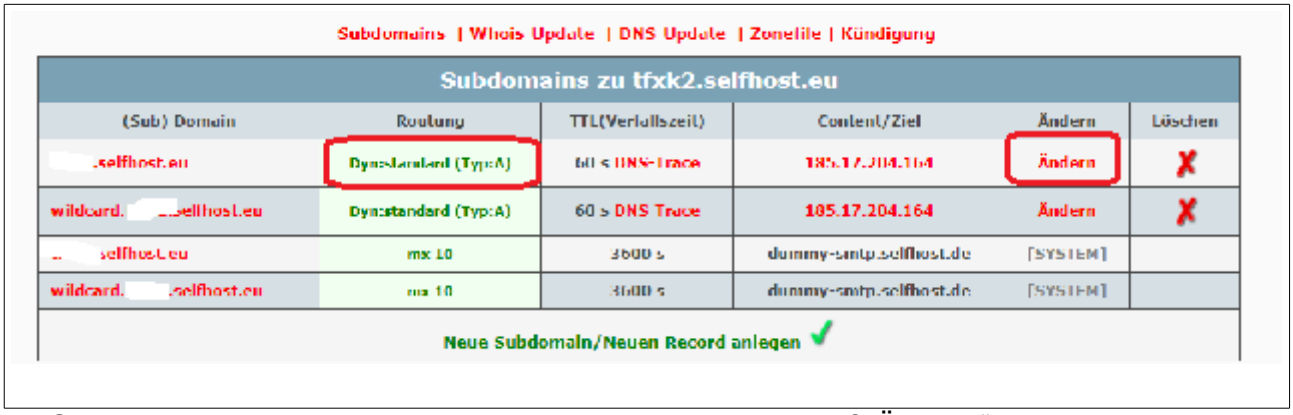
Der Hostname des DynDNS wird in client.ovpn eingetragen (nicht anders als bei IPv4):

```
remote meinefirma.selfhost.eu 1194
```

Aufgrund des Protokolls UDP6 fordert OpenVPN die IPv6-Adresse zu dem Hostnamen an (AAAA-Record), deshalb muss das DynDNS auch eine solche liefern.

DynDNS für IPv6 konfigurieren

Je nach DynDNS-Dienst kann die Konfiguration anders aussehen, wichtig ist, dass das DynDNS anschließend in der DNS-Abfrage (mit nslookup) einen Typ AAAA-Record liefert. Hier die Konfiguration bei selfhost.de:



Im Screenshot ist noch Typ-A (IPv4) eingestellt, mit Klick auf „Ändern“ kann dies umgestellt werden.

In den meisten Fällen müssen Sie einen DynDNS-Client auf dem Computer, der von außen erreicht werden soll, installieren, da die DynDNS-Konfiguration des Routers wohl die IPv6-Adresse des Routers senden würde, was aber nicht das ist, was erreicht werden soll.

Nur wenn der Router wirklich ein Port-Forwarding vornimmt, was bei IPv6 eigentlich nicht angesagt ist, wäre die IPv6-Adresse des Routers beim DynDNS-Dienst zu melden.

Schlussbemerkung

Die Umstellung auf IPv6 wird kommen. Wer noch DualStack, also IPv4 und IPv6 nutzen kann, der freue sich darüber und kann solange auf IPv4 bleiben. Bis zum endgültigen Wegfall von IPv4 haben hoffentlich die Beteiligten (Provider, Router-Hersteller) dazugelernt und die heutigen Probleme sind gelöst (z. B. per SW-Update).

Die obigen Ausführungen gelten natürlich nicht nur für VPN-Anwendungen. Auch ein im Firmennetz betriebener Webserver (oder Webcam) wären nach Umstellung auf DS-Lite nur noch per IPv6-Adresse (und IPv6-DynDNS) erreichbar.