UDM-PRO Wireguard Service

Was wollen wir?

Sicheren Zugriff auf das (private) Netz hinter einer UDM

Warum wollen wir das?

Private Geräte allerart sind mittlerweile Ziel von Angreifern mit mehr oder weniger boshaften Interessen. Gemeinnützige Institutionen scannen kontinuierlich IP Adressen nach geöffneten Ports um Ihr Wissen zu ergänzen. Heimgeräte werden oft vom Hersteller nicht ausreichend mit Sicherheitsupdates versorgt oder sind nicht auf dem aktuellen Stand. Um Risiken zu vermeiden ist es Hilfreich Geräte nicht direkt frei zu geben. Um trotzdem einen direkten Zugriff ohne Verwendung von Cloud Lösungen zu ermöglichen VPN Lösungen eine direkte gesicherte Verbindung zum Heimnetzwerk.

Wireguard ist eine moderne und performante VPN technology. Sie verwendet moderne Verschlüsselungstechnologien und versucht durch den OpenSource Ansatz und schlanke Programmierung Angriffsflächen zu vermeiden.

Und wie geht das genau?

In meinem Beispiel möchte ich das Einrichten auf einer UDM-PRO hinter einer Fritzbox für jeweils Dual Stack und Lite(IPv6) beschreiben.

Hinweise

Voraussetzung dazu ist eine öffentliche erreichbare IP (kein Providcer NAT IP).

Bei einem Lite Anschluß müssen Clints entweder eine IvP6 Adresse haben. Im Mobilfunkbereich werden diese zwar oft aber nicht immer zugeteilt. Oder eine externer IP4 zu IP6 tunnel verwendet werden. (Dies ist nicht Teil dieser Anleitung)

Schritte

- Einrichtung des WireguardServers auf der UDM-PRO
- Einrichtung der Portweiterleitung auf der FritzBox
- Einrichtung des Clients

Einrichtung des WireguardServers auf der UDM-PRO

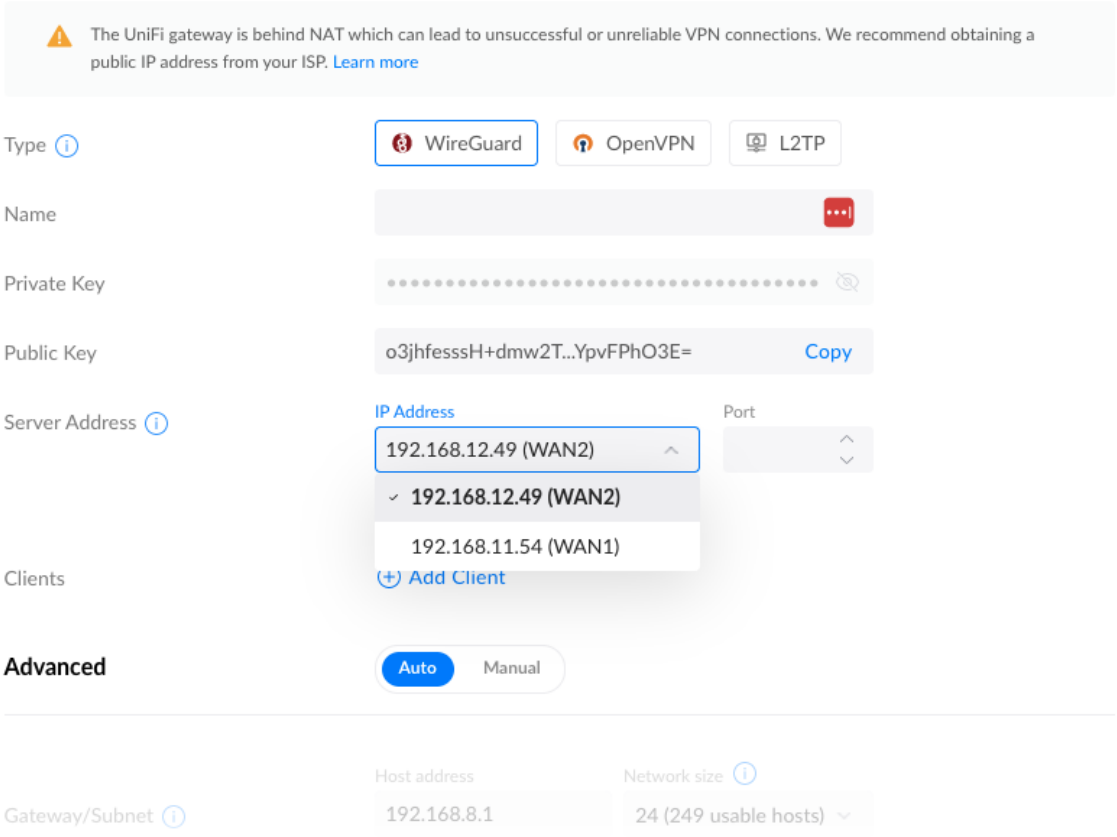
Im Bereich Network->Teleport&VPN->VPN Server Create Server auswählen.

Dort WireGuard auswählen

Bei mir befindet sich die DMP hinter einer Fritz mit einem NAT (IPv4). (doppeltem NAT beim IPv4. Da bei IPv6 NAT abgeschafft wurde spielt dies hier keine Rolle) Daher wird ein Warnhinweis angezeigt. Dies hat mir aber bisher keine Probleme bereitet.

Bei Server Adresse kann die oder eine der IP Adressen vom WAN Inferface ausgewählt werden. Im idealfall einer öffentlichen IP zum Beispiel bei einer Fritz im Bridegmode ist diese dann auch erreichbar. In meinem Fall mit internen IP's wähle ich einfach eine beliebige aus da es für den Server selbst nicht wichtig ist. Allerdings passe ich später die Konfiguration auf dem Client manuell an. Dazu später. Optional kann die IP der VPN Gateways hier 192.168.8.1 angepasst werden.

Mit add Client können nun Clients, die sie sich später mit dem Server verbinden dürfen, hinzugefügt werden. Dies ist auch nachträglich möglich. Unter VPN Server den angelegten Server anklicken und u.A. wir dann die Liste der eingerichteten Client angezeigt. Auch gibt es hier die Möglichkeit Clients zu löschen oder neue Clients anzulegen.



Die Datei mit den Einstellungen des Clients muß bei der Anlage per OCR eingescannt, was bei mir nicht klappen wollte oder per Download heruntergeladen werden.

Einrichten der Weiterleitung auf einer Fritzbox.

dort unter Internet-> Freigaben den UDP Port (Wireguard Standardport ist UDP 51820 an die DMP freigeben) Ping6 ist hilfreich bei Verbindungstests. Die Freigabe der IPv6-Präfixe ist für die IP6 Vergabe im lokalen Lan wird aber für Wireguard nicht benötigt.

Dort unter neue Freigabe die UDM-PRO als Gerät wählen. Auch wenn bei IPv6 das NAT abgeschafft wurde muß dort eine Freigabe eingerichtet werden.

Bei eine Fritzbox mit IPv4 sollt es es dann etwas so aus sehen.

Bei IPv6 zum Beispiel so.

Gerät / Name	IP-Adresse	Freigaben	Port extern vergeben IPv4	Port extern vergeben IPv6	Selbstständige Portfreigabe
Dream-Machiene-Pro	192.168.12.49 ::7a45:58ff:fef9:564a	Wireguard		51820	0 aktiv

(In meinem Fall ist der eine WG Server über beide Leitungen unabhängig erreichbar)

Einrichtung auf dem Client

Zu Verwendung den Wireguard Client aus dem google Store, APP store, ..store oder der Downloadseite herunterladen. Dort die Konfiguration importieren.

Die sieht dann in meinem Beispiel so aus. (Nur ein Beispiel)

Code

```
[Interface]
PrivateKey = 8AW+SRXJRhvIQT0j36qGeJyD8u9Tp8MM0[illegible] # [illegible] Authentifizierung und Verschlüsselung
Address = 192.168.8.2/32 # Wireguard IP des Clients mit dem dieser dann im Netz sichtbar ist
DNS = 192.168.8.1

[Peer]
PublicKey = [illegible]sH+dmw2TAe5knfMq/sq[illegible]Jf[illegible]= # [illegible] Authentifizierung und Verschlüsselung
AllowedIPs = 192.168.8.1/32, 192.168.8.0/[illegible] # [illegible] Daten [illegible] geschickt.
Endpoint = 192.168.11.54:undefined                          # Hier steht die "öffentlich" I
```

Da ich natürlich meinem Wireguardserver nicht über die private IP erreichen kann passe ich diese nun manuell auf dem Client an.

Hier kann eine feste IPv4 oder auch IPv6 eingetragen werden, zum Beispiel [1111:1111:1111:1111:21a:8cff:fe6c:330d]:51820 aber auch ein DNS oder DynDNS Eintrag stehen dmp.meindyndnsp.de:51820

Allowed IP's regelt welcher Datenverkehr an den Server geschickt werden soll. Es können hier einzelne Server (192.168.8.1/32, 192.168.8.2/32, 192.168.76.12/32), die Lokalen Netzwerke oder auch nur bestimmte (192.168.8.1/32, 192.168.8.2/32, , 192.168.16.0/22) aber auch der komplette Datenverkehr ins Internet (192.168.8.1/32, 192.168.8.2/32, 0.0.0.0/0, ::/0) ausgewählt werden.

Den Wireguard server kann ich aus meinem lokalen Netz mit ca. 150 MBit erreichen. Da mein Upload begrenzt hab ich extern nur 150/50 aus einem externem Festnetz und 20/50 bei Verwendung vom Mobilfunk hinbekommen (4G)

Ich hoffe es ist alles seit korrekt und über Hinweise zu Fehlern oder Anregungen freue ich mich.

Auswählen:

Gültige Software-Version Keine Firmware-Relevanz!