WireGuard-Installation auf dem USG

Was wollen wir?

Sicheren Zugriff auf das (private) Netz hinter einem USG-Pro-4 (UGW4) oder USG-3P (UGW3).

Warum wollen wir das?

Wie die Vergangenheit deutlich gezeigt hat haben wenigstens einige private Geräte wie z.B. NAS oder Controller zur Heimautomatisierung oder ähnliches immer wieder Sicherheitslücken, welche auch schon erfolgreich ausgenutzt wurden. So etwas passiert häufig, wenn diese Geräte für alle und jeden über eine simple Portfreigabe im Internet erreichbar und nur mit den "internen Sicherheitsmechanismen" geschützt sind, welche oft nicht ausreichen. Vielleicht möchte man auch einen Dienst aus dem (heimischen) LAN verwenden, welchen man nicht veröffentlichen möchte oder sollte, wie z.B. ein pi-hole.

Daher sollten solche Services nicht direkt von außen erreicht werden können oder man möchte das einfach nicht.

Leider werden wohl weder das USG-Pro-4 noch das USG-3P das dafür nötige Update von Ubiquiti erhalten, was ich sehr schade finde. ☹

Aber auch dafür gibt es eine Lösung, welche ich schon länger im Einsatz habe. 🥰 *Und jetzt übersteht sie sogar einen Reboot und auch ein Provisioning - und vielleicht auch ein Update. Das konnte ich aber nicht testen, da ich dafür nicht genug Hardware habe.* 😉

Und wie geht das genau?

Hinweis: Ich gehe davon aus, dass

1. *rudimentäre Linux-Kenntnisse vorhanden sind, um sich auf dem USG "fortzubewegen" (`cd`, `ls` u.ä.).*
2. *das USG selbst Zugriff auf das Internet hat.*
3. *klar / bekannt ist, wie man eine ssh-Verbindung zum USG aufbauen kann.*
4. *der Editor `vi` benutzt werden kann.*
5. *klar / bekannt ist, wie man per (Win)`scp` Dateien auf das USG übertragen kann (Alternative zu 3. & 4.).*
6. *es keine Überschneidungen bei den (V)LANs aller beteiligten Parteien gibt.*
7. *nur Site-2-Site-Verbindungen hergestellt werden sollen (Road-Worrior-Szenario folgt).*
8. *alle Netze mit allen Netzen kommunizieren können sollen.*

Folgende Netzwerk-Konfigurationen nehme ich für meine Konfiguration an:

- *Alice*
  - *Netze*
    - *10.10.101.0/24*
    - *10.10.105.0/24*
  - *WireGuard Gateway-IPs*

        - *192.168.179.5/32 (Alice <-> Bob)*
        - *192.168.179.9/32 (Alice <-> Charlie)*
    - *private key: alice_private_key (Datei: `/config/auth/wireguard/wg_private.key`)*
    - *public key: alice_public_key (Datei: `/config/auth/wireguard/wg_public.key`)*
    - *DNS: alice.ubiquiti-networks-forum.de*
- *Bob*
    - *Netz*
        - *192.168.2.0/24*
    - *WireGuard Gateway-IPs*
        - *192.168.179.6/32 (Bob <-> Alice)*
        - *192.168.179.13/32 (Bob <-> Charlie)*
    - *private key: bob_private_key (Datei: `/config/auth/wireguard/wg_private.key`)*
    - *public key: bob_public_key (Datei: `/config/auth/wireguard/wg_public.key`)*
    - *DNS: bob.ubiquiti-networks-forum.de*
- *Charlie*
    - *Netze*
        - *10.10.191.0/24*
        - *10.10.192.0/24*
    - *WireGuard Gateway-IPs*
        - *192.168.179.10/32 (Charlie <-> Alice)*
        - *192.168.179.14/32 (Charlie <-> Bob)*
    - *private key: charlie_private_key (Datei: `/config/auth/wireguard/wg_private.key`)*
    - *public key: charlie_public_key (Datei: `/config/auth/wireguard/wg_public.key`)*
    - *DNS: charlie.ubiquiti-networks-forum.de*
- *Transfer-Netze*
    - *Alice <-> Bob: 192.168.179.4/30*
    - *Alice <-> Charlie: 192.168.179.8/30*
    - *Bob <-> Charlie: 192.168.179.12/30*

Ich werde hier nicht auf die Konfiguration der Firewall eingehen, um z.B. VLANs gegeneinander abzusichern o.ä.

Freundlicherweise hat WireGuard selbst auf GitHub schon mehr oder weniger alles bereitgestellt, um das umzusetzen.

Bevor wir aber "ins Eingemachte" gehen sollten wir uns im GitHub-Repository umsehen, unter welchem Link das aktuelle WireGuard-Debian-Paket zu bekommen ist. Dabei hilft ein Blick auf DIESE Seite. Hier sind alle Releases für die unterstützten Geräte gelistet. Das aktuelle Release ist vom 02. Juli 2022 - ja: auch schon 'was älter. Hier die aktuellen Links:

- *USG-3P (UGW3): https://github.com/WireGuard/w…0220627-v1.0.20210914.deb*
- *USG-Pro-4 (UGW4): https://github.com/WireGuard/w…0220627-v1.0.20210914.deb*

Und los geht's auf den Reitern oben:

1. Server vorbereiten
2. Server konfigurieren

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 Garantie auf Erfolg. Im Falle eines Misserfolges hilft aber die Community hier sicherlich 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!