HowTo – WireGuard Konfiguration

In dieser HowTo wird zuerst die schrittweise Konfiguration behandelt. Nachfolgend werden ein paar Beispielkonfigurationen wiedergegeben, um den Einstig in die Konfiguration von WireGuard zu erleichtern.

1 Schlüssel generieren

WireGuard benötigt base64-codierte öffentliche und private Schlüssel. Diese können auf der Kommandozeile mit dem Dienstprogramm **wg** erzeugt werden.

Hinweis
- Der private Schlüssel oder Private Key wird in der lokalen Konfiguration der eigenen Seite verwendet.
- Den öffentlichen Schlüssel (Public Key) benötigt die gegenüberliegende Seite, der Verbindungspartner.
- Für die Konfiguration ist ein Erstellen von Dateien nicht notwendig.

1.1 Private Key

Um einen privaten Schlüssel zu erzeugen verwendet man die im Beispiel genannten Befehlszeile. Der Schüssel lässt sich auch mit dem Namen **private.key** speichern, für die Konfiguration ist das aber nicht zwingend nötig.

Beispiel
Ausgabe auf der Kommandozeile:
```
wg genkey
```

In Datei speichern:
```
wg genkey > private.key
```

1.2 Public Key

Aus dem eben erzeugten **private.key** wird der öffentliche Schlüssel – der für die Konfiguration eines Verbindungspartners benötigt wird – mit dem folgenden Befehl errechnet. Der Public Key wird auch auf der 4 WireGuard Status Seite im Webinterface angezeigt.

Beispiel
Ausgabe auf der Kommandozeile:
```
wg pubkey < private.key
```

In Datei speichern:
```
wg pubkey < private.key > public.key
```

1.3 Alternative in einem Schritt

Die beiden Schlüssel lassen sich auch mit einem Einzeiler erzeugen.

Beispiel
```
wg genkey | tee private.key | wg pubkey > public.key
```

2 Schnittstellenkonfiguration

Eine `Neue Schnittstelle Hinzufügen...`.

In der Dialogseite den **`Name der neuen Schnittstelle`** festlegen und im Dropdown das **`Protokoll für die neue Schnittstelle`** auf ***`WireGuard VPN`*** stellen.

2.1 Allgemeine Konfiguration

Hier werden die Einstellungen der eigenen Seite durchgeführt.

- Unter **`Privater Schlüssel`** wird der für die Authentifizierung benötigte Key eingetragen. Dieser wird nach *1.1 Private Key* erstellt, dabei reicht es den Schlüssel auf der Kommandozeile auszugeben und von dort zu kopieren.
- Soll der Router als Gegenstelle zum Aufbauen von Client-Verbindungen dienen kann hier ein eigener Port eingetragen werden, auf den der Server hört. (Default **`51820`**)
- Idealerweise sollte unter **`IP-Adressen`** die IP angegeben werden, die der WireGuard-Schnittstelle zugewiesen werden soll. Zudem muss auch ein Subnetz als CDIR-Index mit angegeben.
  (z.B. **`192.168.100.254/24`** als VPN-Netz-IP)

> **Hinweis**
> ➢ Wird keine IP-Adresse mit Subnetzdeklaration vergeben müssen entsprechende Routen für die Kommunikation erstellt werden.
> ➢ Für ein Debugging ist es hilfreich, wenn eine IP vergeben wird.

2.2 Verbindungspartner

Die Verbindungspartner stellen jeweils eine Gegenstelle oder einen Einwahlaccount dar. Das Anlegen eines neuen Verbindungspartners ist einfach umsetzbar.

- Für die Authentifizierung wird der **`Öffentlicher Schlüssel`** des Verbindungspartners eingetragen.
- Erlaubte IPs spezifiziert die IP-Adressen und Subnetze, von denen aus der Verbindungspartner Daten senden darf. Sprich hier werden die erlaubten Absender-IPs konfiguriert. Hier muss auch ein Subnetz als CDIR-Index angegeben werden.
- Um eventuell vorhandene, vom VPN-Netz abweichende IPs zu Routen wird die Option **`Erlaubte IP-Adressen routen`** aktiviert.
- Baut der Router die Verbindung zu seiner Gegenstelle auf, wird entsprechend **`Entfernter Server`** und **`Entfernter Port`** konfiguriert.
- Wird die Verbindung auf der Strecke genattet (z.B. Client hinter Gateway, oder Mobilfunk) empfiehlt es sich zudem **`Persistentes Keep-Alive`** zu aktivieren.
- Zudem kann man eine **`Beschreibung`** angeben, um die Gegenstelle einfacher identifizieren zu können. Dazu das Feld ***`Beschreibung`*** bei **`-- Zusätzliches Feld --`** `Hinzufügen`.

2.2.1 Zusätzliche Absicherung (PSK)

Als weitere Sicherheitsstufe kann für jeden Verbindungspartner ein Gemeinsamer Schlüssel (PSK) verwendet werden.

- Dazu das Feld ***Gemeinsamer Schlüssel*** als `-- Zusätzliches Feld --` `Hinzufügen`.
- Mit dem Kommando ***wg genpsk*** auf der Kommandozeile einen Schlüssel erstellen und in dem neuen Feld **Gemeinsamer Schlüssel** hinterlegen. Der PSK muss auch beim Verbindungspartner hinterlegt werden.

2.3 Firewall Einstellungen

Um den Zugriff auf den Router und das Netzwerk zu Steuern ist in der Firewall schon eine Zone **VPN** vordefiniert.

- Die Zone ***VPN*** wird in den Schnittstelleneinstellungen unter **Firewall Einstellungen** bei **Firewallzone anlegen / zuweisen** ausgewählt.

2.4 Schnittstellenkonfiguration abschließen und WireGuard starten

Nach dem die Schnittstelle vollständig konfiguriert wurde werden noch folgende Schritte durchgeführt.

- Zuerst wird die Konfiguration mit `Speichern & Anwenden` übernommen.
- Danach wird die Schnittstelle mit `Neustarten` einmal neu initialisiert.

3 Firewall: Verbindungsaufbau zulassen

Damit ein Tunnel von außen aufgebaut werden kann, muss der WireGuard Port in der Firewall freigegeben werden.

- In der Firewall auf den Tab **Traffic-Regeln** wechseln.
- Bei **Ports auf dem Router öffnen** wird die neue Regel hinzugefügt.
- Dazu wird als **Name** zum Beispiel ***Allow-WireGuard-Input*** verwendet.
- Als **Protokoll** wird ***UDP*** ausgewählt.
- Bei **Externer Port** wird der Port aus den Schnittstellen Einstellungen eingetragen. (Default ***51820***)

> **Hinweis**
> ➢ Der verwendete Port ist bei WireGuard frei wählbar.
> ➢ Daher ist bei der Konfiguration der Firewall darauf zu achten, dass der bei der Schnittstelle eingestellte **Port (lauschen)** in der Firewall freigegeben wird.

- Nach `Hinzufügen` wird die Firewall-Änderung mit `Speichern & Anwenden` übernommen.

4 WireGuard Status

Im Menü des Webinterface ist unter **Status** auch der **WireGuard** Status zu finden. Hier werden die öffentlichen Schlüssel und Statusinformationen zu den konfigurierten Verbindungspartner angezeigt.

5 Beispielkonfigurationen

Um die Parametrierung in den Beispielen übersichtlich zu gestalten werden die Werte für die Verbindungspartner farbig gekennzeichnet und in einer Tabelle gegenübergestellt.

5.1 Site-2-Site

Dieses Beispiel zeigt, wie zwei Netze via WireGuard miteinander verbunden werden, um beispielsweise eine **Außenstelle** an eine Firmenzentrale (**Zentrale**) anzubinden.

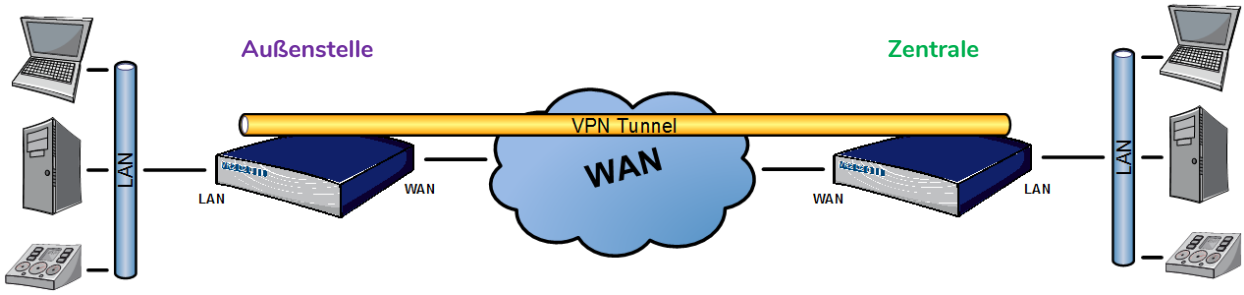

Abbildung 1: Netzplan-Beispiel

Hinweis

- Hier werden zwei TDT-Router mittels **WAN**-Schnittstelle direkt miteinander verbunden. Die Verbindung kann natürlich auch über jeden anderen WAN-Weg etabliert werden, so sich die Geräte erreichen.
- Außenstelle mit ***wechselnder IP*** an Schnittstelle **WAN** und ***192.168.1.50/24*** an **LAN**.
- Zentrale hat die IP ***10.99.99.1*** an Schnittstelle **WAN** und ***192.168.0.50/24*** an **LAN**.
- Als Transfernetz wird ***192.168.100.0/24*** verwendet.
- Die IPs sind Außenstelle ***192.168.100.1*** und Zentrale ***192.168.100.254***.

Parameter	Außenstelle	Zentrale
Allgemeine Konfiguration		
Privater Schlüssel	*<Private Key>*	*<Private Key>*
Port (lauschen)		*51820*
IP-Adressen	*192.168.100.1/24*	*192.168.100.254/24*
Verbindungspartner		
Beschreibung	*Zentrale*	*Aussenstelle*
Öffentlicher Schlüssel	*<Public Key>*	*<Public Key>*
Erlaubte IPs	*192.168.100.254/32* (Transfer-IP) *192.168.0.0/24* (LAN-Netzwerk)	*192.168.100.1/32* (Transfer-IP) *192.168.1.0/24* (LAN-Netzwerk)
Erlaubte IP-Adressen routen	☑	☑
Entfernter Server	*10.99.99.1*	
Entfernter Port	*51820*	
Persistentes Keep-Alive	***25***	

5.2 Mobile Road Warrior (Smartphone)

Dieses Beispiel zeigt, wie ein Smartphone (z.B. Android, iOS) mittels WireGuard App zu einem VPN Server verbunden wird, um beispielsweise dem Benutzer **max0815** Zugriff auf die Firmenzentrale (**Zentrale**) zu gewähren.

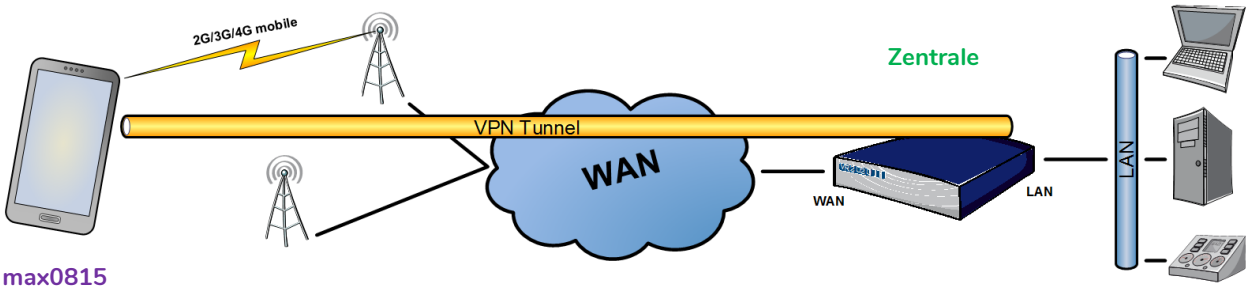

Abbildung 2: Netzplan-Beispiel

Hinweis

- Hier wird ein Smartphone an einen TDT-Router mittels **WAN**-Schnittstelle verbunden. Die Verbindung kann natürlich auch über jeden anderen WAN-Weg etabliert werden, so sich die Geräte erreichen.
- max0815 mit ***wechselnder WAN IP*** via **LAN**.
- Zentrale hat die IP ***10.99.99.1*** an Schnittstelle **WAN** und ***192.168.0.50/24*** an **LAN**.
- Als Transfernetz wird ***192.168.100.0/24*** verwendet.
- Die IPs sind Außenstelle ***192.168.100.1*** und Zentrale ***192.168.100.254***.

Parameter	max0815	Zentrale
	Interface	Allgemeine Konfiguration
Private Key / Privater Schlüssel	*<Private Key>*	*<Private Key>*
Listen Port / Port (lauschen)		*51820*
Addresses / IP-Adressen	*192.168.100.1/24*	*192.168.100.254/24*
	Peer	Verbindungspartner
Beschreibung		*max0815*
Public Key / Öffentlicher Schlüssel	*<Public Key>*	*<Public Key>*
Endpoint / Entfernter Server	*10.99.99.1:51820*	
Entfernter Port		
Allowed IPs / Erlaubte IPs	*192.168.0.0/24* (LAN-Netzwerk)	*192.168.100.1/32* (Transfer-IP)
Persistant keepalive	*25*	

5.3 Unterwegs sicher surfen

Mit Hilfe eines WireGuard Tunnel ist es einfach möglich sich geschützt in potenziell unsicheren Umgebungen, wie zum Beispiel in offenen WLAN-Hotspots zu bewegen. Dazu wird einfach ein Tunnel vom Endgerät bis zum eigenen Gateway aufgebaut und jeglicher Traffic darüber gesendet.

Um das zu realisieren werden nur wenige zusätzliche Änderungen am Client und an der Firewall des TDT-Gerätes gegenüber der Konfiguration 5.2 Mobile Road Warrior (Smartphone) nötig.

5.3.1 Client Konfiguration

Nachfolgend werden nur die zusätzlichen/abweichenden Einstellungen wiedergegeben.

Parameter	max0815	Zentrale
	Interface	**Allgemeine Konfiguration**
`DNS Servers`	***192.168.100.254*** (Router VPN-IP)	
	Peer	**Verbindungspartner**
`Allowed IPs / Erlaubte IPs`	***0.0.0.0/0*** (entspricht einer Default-Route)	

> **Achtung**
> ➢ Da die providereigenen DNS Server nach dem Tunnelaufbau eventuell nicht mehr erreichbar sind, ist es häufig nötig unter **`DNS Servers`** entweder den Router oder öffentlich erreichbare Server einzutragen.

5.3.2 Erweiterung der Router Firewall

Damit die Daten des Clients nun auch über den Router ins Internet dürfen muss die Firewall angepasst werden.

- Dazu wird die Zone VPN mit dem Button `Bearbeiten` geöffnet.
- Dort wird bei **`Erlaube Weiterleitung zu Zielzone:`** zusätzlich zur Zone **`LAN`** die Zone ***WAN*** ausgewählt und die Änderung mit `Speichern & Anwenden` übernommen.

5.4 Windows Client Konfiguration

Unter Windows ist der WireGuard Client noch textbasiert, daher wird hier die Konfiguration 5.2 Mobile Road Warrior (Smartphone) zusammen mit 5.3 Unterwegs sicher surfen abgebildet.

```
[Interface]
PrivateKey = <Private Key>
Address = 192.168.100.1/24
DNS = 192.168.100.254

[Peer]
PublicKey = <Public Key>
AllowedIPs = 0.0.0.0/0
Endpoint = 10.99.99.1:51820
PersistentKeepalive = 25
```