Netzwerk

VPN Wireguard an Lancom/R&S Firewall

Diese Anleitung ist noch in Bau! Ich bin dankbar für jede Hilfe, Ergänzung oder Korrektur.

Allgemeines
Seit Firmware FX 10.12 RU1 (07/2023) unterstützen die Rohe&Schwarz UF-xxx Firewalls Wireguard.
Die UF-Firewall als Verbindungs-Empfänger muß eine feste IP haben und der verwendete UDP-Port muss beim Router ankommen.
Wird die Firewall als WG-Router nach dem Standardgateway installiert, sind im Gateway-Router folgende Einstellungen erforderlich:

- Portforwarding: UDP-Port (Bsp: 51820) zum WG-Router (LAN-IP)
- Routing-Tabelle: WG-Transfernetz (Bsp: 192.168.200.0/24) zum WG-Router (LAN-IP), Maskierung aus
- Firewall: UDP-Zielport (51820) frei geben
- Firewall: Verbindungsquelle Wireguard-Router (LAN-IP) Internet erlauben
- Firewall: Verbindungsziel WG-Transfernetz (192.168.200.0/24) erlauben

Wireguard ist OpenSource und für jedes gängige Betriebssystem kostenfrei verfügbar.

Wireguard (WG) Server
(Bsp. Transfer-LAN: 192.168.200.1)

- Voraussetzung (siehe oben): Internetverbindung (ausgehend) und offener UDP-Port (eingehend)
- Netzwerk -> Interfaces -> WireGuard-Interfaces: "+" Interface wg0 (ff.) erstellen, MTU (1420), Interface AKTIVIEREN
- VPN -> WireGuard: "+" WG-Verbindung erstellen, Interface AKTIVIEREN
  - Name: Verbindungsname
  - Interface: wg0 (Bsp) Interface von oben auswählen
  - Adresse: WG Transfernetz Adresse des Servers (bisher nicht verwendetes Netz, Bsp: 192.168.200.1/32)
  - Port: UDP-Port (51820) der WG-Verbindung -frei festlegbar (UDP 49152-65535)
  * pro UDP-Port kann nur ein Wireguard-Interface angelegt werden
  * pro Router genügt ein Wireguard-Server, wenn man nicht verschiedene Ports nutzen möchte

- Desktop -> Dienste -> Benutzerdef.Dienste: "+" Dienst "WireGuard" anlegen
  - Port: 51820
  - Protocol: UDP
- Netzwerk -> Netzwerk-Verbindungen: "+" Verbindung hinzufügen

- Name: WireGuard
- Interface: WG-Interface (wg01)
- Netzwerk Adressen: In Feld klicken und oben konfigurierte erlaubte IP-Adressen auswählen. (192.168.200.0/24)

- Firewallobjekt: Host hinzu fügen (keinen VPN-Host), WireGuard-Server
  - Host: Wireguard-Server (192.168.200.1)
- Firewall Verbindung (WireGuard-Server <-> WAN) erstellen
  - benutzerdef. Dienst "Wireguard" (von oben) zufügen
  - Verbindungsrichtung drehen (von außen nach innen), Serverspezif.Einstellung, NAT =aus, DMZ/Port-Weiterleitung aktivieren (Portforwarding UDP-Port zum WG-Server)

Wireguard Peers im LF-Router
(Bsp Client: 192.168.200.10)
Für jede Gegenstelle muß ein Peer angelegt werden, dass dem Client eine eigene IP (Allowed IPs) zuweist und den Public-Key der Verbindung enthält.

- VPN -> WireGuard: WG-Verbindung von oben auswählen
- Authentifizierung: Schlüsselpaar erzeugen, kann auch importiert werden (Private-Key bleibt im Router, Public-Key bekommt die Gegenseite)
- Peers: "+" neuen Peer erzeugen
  - Name: Peer-Name
  - Remote Adresse: Optionale öffentl. erreichbare Adresse oder DNS-Name der Gegenstelle. Nur nütig für Initiator der Verbindung. Die Angabe wird benötigt, wenn ein Remote-Port angegeben ist.
  - Remote Port: Port wie Gegenseite (Bsp: 51820)
  - Public-Key: Key des Peers (WG-Tool (unten) oder Wireguard-Peer erzeugt Schlüsselpaar)
  - Keep-Alive: Haltezeit (25s). Wert ist nur verfügbar, wenn eine Remote Adresse eingegeben wurde
  - Routen erstellen: Wenn aktiviert, werden alle IP-Adressen unter Erlaubte IP-Adressen automatisch in die Routing-Tabelle 201 eingetragen. Sonst müssen die Routen manuell erstellt werden.
  - Erlaubte IP-Adressen: IP-Adressen oder Netze mit Subnetzmaske (CIDR-Schreibweise), die über die WG-Verbindung erreichbar sein sollen
    Bei LAN-LAN müssen hier alle erlaubten Netze rein, die über den Tunnel erreichbar sein sollen, kann auch 0.0.0.0/0 (alle) sein.
    ACHTUNG, Bug!? Trägt man hier das eigene LAN ein, ist der Router über LAN nicht mehr erreichbar.

Wireguard Endgerät (Handy oder beliebiges anderes Gerät mit dem offiziellen Wireguard-Client)
(Bsp: 192.168.200.10)

- Wireguard-Client laden
- neue Verbindung - manuell erstellen
- beliebiger Verbindungsname

- Privater Schlüssel (wird automatisch erstellt)
- Öffentl. Schlüssel: Key in Router -> Wireguard Peer -> Public Key kopieren
- Adressen: Client Adresse (192.168.200.10/32) (wie Allowed Address vom Wireguard Peer)
- Nameserver: ggf. Wireguard-Server/Router (192.168.200.1)
- Öffentl. Schlüssel: PK des Routers aus Wireguard -> Wireguard
- Erlaubte IPs: 0.0.0.0/0 schicke gesamten Traffic (auch Internet!) in den Tunnel
  sinnvoller ist konkrete Angabe (Transfernet + Zielnetz(e), siehe .conf unten)
- Endpunkt: Einwahlpunkt IP oder Domain der Gegenseite **+Doppelpunkt:Port**! 1.2.3.4:51820 (wie oben)

Beispiel der .conf -Datei des Clients (IP: 3):

```
[Interface]
Address = 192.168.200.3/32
PrivateKey = OMjSCv6e/iXECZwq0ZVL5Ywf/KzZvdsGpYKv1512345=
# DNS = 172.16.7.254

[Peer]
# Name = VPN-zu-Oma
PublicKey = cA+mynt84tVH1gPaUN66E8K0nfzvpsQMohrEbz54321=
Endpoint = router.myfritz.de:51820
AllowedIPs = 192.168.200.0/24, 192.168.40.0/24
# PersistentkeepAlive = 25
```

- Address: VPN-Adresse des Clients
- PrivateKey: Privat-Key des jeweiligen Clients (im Client sieht man dann den Public-Key)
- DNS falls gewünscht
- PublicKey: Public-Key des WG-Servers
- Endpoint: öffentliche Adresse des VPN-Servers **mit Port**
- AllowedIPs: alle Adressen, die der Wireguard Server in den Tunnel routet. (also zumindest Wireguard-Server und Serverside-LAN)
  Dieses "Cryptokey Routing" bewirkt, dass Wireguard Server und Client das Routing für die jeweils remoten IP Netze automatisch in die Routing Tabelle übernehmen.
  AllowedIPs = 0.0.0.0/0 bewirkt, dass der gesamte Traffic durch den Tunnel geht.

Wireguard **Online Config Generator:**

- Tool erstellt komplette .conf-Datei: https://www.wireguardconfig.com/
- Tool erstellt Schlüsselpaare: https://wg.orz.tools/

Quellen und Links:

- https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=141459491

Netzwerk

Verwendete Abkürzungen:
- WG - Wireguard
- GW - Gateway

Eindeutige ID: #1435
Verfasser: Uwe Kernchen
Letzte Änderung: 2023-07-14 22:40