



KB 70196: WGIP

Feste, öffentliche IPv4-Adresse mit
WireGuard® einrichten auf Teltonika
RUT951 / RUT955

Stand 10.09.2024, 14:18:21
Version 66e0390d
Referenz-URL <https://internet-xs.de/kb/70196>
PDF-URL https://internet-xs.de/kb/Internet-XS_KB-70196-66e0390d.pdf

Inhalt

- Einleitung** 3
- Voraussetzungen** 4
- 4
- Sicherheitsvorkehrungen** 4
- Neue Client-Konfiguration erstellen** 4
- Port-Weiterleitungen konfigurieren** 5
- Auto Reboot (optional, empfohlen)** 6
- Fehlerdiagnose** 6

Einleitung

Mittels WireGuard® kann auf einfachste Art und Weise eine feste, öffentliche IPv4-Adresse auf einem Teltonika RUT950 / RUT951 / RUT955 und ggf. weiteren RUT-Modellen bereitgestellt werden.

Wir betreiben verschiedene Einwahl-Server zur Bereitstellung von IP-Tunnel-Verbindungen / festen, öffentlichen IPv4-Adressen. Die Anleitungen in dieser Kategorie sind speziell abgestimmt auf diesen Server:

- Name: WGIP
- Hostname: wgip.internet-xs.de
- IP-Adresse: 212.58.69.15
- Protokoll: Wireguard (Beta)
- Client IP-Adress-Bereich: 212.58.85.0/24 (212.58.85.1 - 212.58.85.254)

Bitte prüfen Sie, ob Ihr IP-Tunnel-Zugang auch auf dem o.g. Server registriert ist.

Alle Arbeiten geschehen auf eigene Gefahr. Für Schäden an Soft- und Hardware sowie für Ausfälle Ihrer Infrastruktur sind Sie selbst verantwortlich. Wir können keine Unterstützung für nicht von uns getestete Szenarien, Hardware, Software und Betriebssysteme anbieten. Alle Anleitungen setzen ein Blanko- bzw. minimal konfiguriertes System voraus und sind als eine mögliche Konfigurationsvariante zu verstehen, die ggf. an Ihr lokales Umfeld und Ihre Anforderungen angepasst werden muss. Bitte beachten Sie immer die Sicherheitshinweise in der Bedienungsanleitung des Herstellers, besonders zum Betrieb von Hardware, dem Aufstellungsort und Betriebstemperaturen. Führen Sie Tests nicht in Produktivumgebungen durch. Testen Sie die Lösung ausgiebig, bevor Sie sie produktiv einsetzen. IT-Systeme sollten nur von qualifiziertem Personal konfiguriert werden. Als Administrator müssen Sie selbst abwägen, ob unsere Produkte und Dienstleistungen für Ihren Anwendungszweck und die gewünschte Verfügbarkeit geeignet sind, oder nicht. Führen Sie Änderungen nicht über eine entfernte Verbindung (Remote-Verbindung) durch. **Verwenden Sie stets sichere Passwörter, ändern Sie Standard-Passwörter umgehend ab.**

In einer PDF-Datei können Zeilenumbrüche innerhalb von Code-Blöcken vorhanden sein, da die Seitenbreite begrenzt ist. Bitte verwenden Sie für Copy & Paste im Zweifelsfall ein Editor-Programm als Zwischenritt und entfernen Sie unerwünschte Zeilenumbrüche.

Voraussetzungen

Um die Schritte, die in dieser Anleitung beschrieben sind durchführen zu können, müssen folgende Voraussetzungen erfüllt sein:

1. Teltonika RUT951 / RUT955 (ggf. auch RUT240, RUTX011 usw.) (der Setup-Wizard sollte abgeschlossen sein) (z.B. RUT95100XXXX)
2. Ein aktivierter Test- oder bezaltes IP-Tunnel-Zugang auf dem Server wgip.internet-xs.de bzw. 212.58.69.12
3. Eine funktionsfähige SIM-Karte mit mind 1 GiByte Datenvolumen eines beliebigen Netzbetreibers / Anbieters / Tarif
4. Firmware-Version: Mind. RUT9M_R_00.07.07.1
5. Unter **Status > Overview** im Bereich **INTERNAL MODEM** muss im Feld **DATA CONNECTION** der Wert **Connected** stehen. Falls dies nicht der Fall ist, prüfen Sie bitte Ihre Mobilfunkeinstellungen.

Einschränkungen

- Die zu erwartende maximale Upload-/Download-Bandbreite beträgt **bis zu 30 MBit/s** (Beschränkt durch Prozessor-Leistung des Routers, <https://www.speedtest.net/result/16343415759>)

Sicherheitsvorkehrungen

1. **Vergeben Sie vor der Konfiguration ein sicheres Geräte-Passwort.** Ihr Teltonika RUT951 ist nach Abschluss dieser Anleitung über eine öffentliche IP-Adresse aus dem weltweiten Internet erreichbar. Falls Sie ein unsicheres Geräte-Passwort verwenden, wird das Gerät innerhalb von Minuten von automatischen Angreifern übernommen.
2. Betreiben Sie keine Dienste (z.B. Zugriff auf IP-Kamera / Webcam / Datenlogger) über unverschlüsselte Verbindungen. **Der IP-Tunnel kann keine zusätzliche Verschlüsselung bereitstellen, da er nur ein Stück der Gesamtstrecke zwischen Ihrem Client (z.B. Smartphone) und dem anzubindenden Gerät (z.B. Smart-Home-Zentrale) abdeckt.** Eine richtige Ende-zu-Ende-Verschlüsselung muss immer vom Client bis zum Server erfolgen, z.B. von dem Gerät, von dem Sie auf IP-Kameras / Datenlogger / Smart-Home-Zentrale zugreifen (z.B. Smartphone) bis zum angebotenen Gerät (z.B. Smart-Home-Zentrale) (z.B. mit HTTPS).
3. Leiten Sie keine Port-Bereiche weiter sondern immer nur einzelne Ports (wenn möglich) und immer so spezifisch wie möglich (z.B. nur Port 80/TCP, nicht Port 80/TCP+UDP)
4. **Beachten Sie die Hinweise des Geräte-Herstellers zur Anbindung von IP-Kameras / Webcams / Datenloggern / Smart-Home-Zentralen an das Internet.** Manche Hersteller (z.B. Homematic) weisen ausdrücklich darauf hin, dass die Web-Oberflächen ihrer Geräte nicht aus dem Internet erreichbar sein sollten.

Neue Client-Konfiguration erstellen

1. Loggen Sie sich auf der Web-Oberfläche Ihres Teltonika RUT951 ein.
2. Navigieren Sie zu **Services > VPN**
3. Klicken Sie auf den Reiter **WireGuard®**
4. Erstellen Sie eine neue WireGuard®-Konfiguration: **New configuration name:** ixswgip
5. Klicken Sie auf **Add**

Daraufhin sollte sich eine Eingabemaske zur weiteren Konfiguration öffnen.

Bereich **WireGuard® Interface: ixswgip**

1. Enable: **on**
2. Private key: **Kopieren Sie in dieses Feld den Private-Key, den wir Ihnen per E-Mail mitgeteilt haben** (überschreiben Sie den vom Router generierten Schlüssel)
3. Public key: **Kopieren Sie in dieses Feld den Public-Key, den wir Ihnen per E-Mail mitgeteilt haben** (überschreiben Sie den vom Router generierten Schlüssel)
4. IP addresses: Tragen Sie hier das Ihrem Zugang zugeteilte IP-Netz ein, z.B. **212.58.85.265/32**
5. Wechseln Sie zum Reiter **Advanced settings**
6. Metric: *leer*
7. Listen port: *Wird nicht verwendet, Sie können hier einen beliebigen Port einsetzen*
8. MTU: **1420**
9. DNS servers: Tragen Sie hier einen öffentlichen DNS-Server ein, z.B. **9.9.9.9** oder **1.1.1.1** oder **8.8.8.8**

Bereich **Peers**

1. Erstellen Sie eine neue WireGuard®-Peer-Konfiguration: **Add new instance: wgipixs**
2. Klicken Sie auf **Add**
3. Public key: **Kopieren Sie in dieses Feld den Public-Key des WireGuard®-Servers (tdVDRs . . .)**
4. Endpoint host: **212.58.69.12** (setzen Sie hier **nicht** die Ihrem Zugang zugeteilte feste, öffentliche IPv4-Adresse ein!)
5. Allowed IPs: 0.0.0.0/0
6. Description: *leer*
7. Route allowed IPs: **on**
8. Wechseln Sie zum Reiter **Advanced settings**
9. Tunnel source: Any
10. Preshared key: *leer*
11. Endpoint port: **51820**
12. Persistent keep alive: **30**
13. Routing table: *leer*

Klicken Sie auf **Save & Apply** um die Konfiguration zu speichern.

Ihr Teltonika RUT951 / RUT955 sollte nach wenigen Minuten über die Ihrem WireGuard® IP-Tunnel-Zugang zugeteilte feste, öffentliche IPv4-Adresse erreichbar sein:

z.B. **http://212.58.85.XXX**

!! Bei der ersten Verbindung mit dem Dienst kann es bis zu 20 Minuten dauern, bis Traffic in beide Richtungen möglich ist.

Port-Weiterleitungen konfigurieren

Falls Sie im LAN des RUT951 / RUT955 Geräte wie z.B. Datenlogger, IP-Kameras, Smart-Home-Zentralen usw. erreichbar machen möchten, müssen Sie für jeden Dienst jedes Geräts eine Port-Weiterleitung einrichten.

1. Navigieren Sie zu **Network > Firewall**

2. Klicken Sie auf den Reiter **Port Forwarding**
3. Im Bereich **Add new instance** (ganz unten)
4. **Name**: z.B. IP_CAM_80
5. **Protocol**: Vorgegeben durch Ihr Gerät (z.B. TCP+UDP)
6. **External port**: z.B. 8080 (kann vom "Internal Port" abweichen, sofern Ihr anzubindendes Gerät dies unterstützt)
7. **Internal IP address**: Wählen Sie die LAN-IP-Adresse des Geräts aus, das Sie mittels der Port-Weiterleitung erreichbar machen möchten (diese LAN-IP sollte auf dem erreichbar zu machenden Gerät fest eingetragen sein, d.h. als "statische LAN-IP", z.B. 192.168.1.50)
8. **Internal port**: Vorgegeben durch Ihr Gerät (z.B. 80)
9. Klicken Sie auf **Add**
10. Daraufhin öffnet sich eine Eingabemaske zum festlegen von erweiterten Einstellungen
11. Enable: **on**
12. Source zone: **wireguard@: ixswgip**
13. Klicken Sie auf **Save & Apply**

Ihr Anzubindendes Gerät (IP-Kamera, Datenlogger usw.) sollte anschließend über die Ihrem IP-Tunnel-Zugang zugeteilte feste, öffentliche IPv4-Adresse unter Angabe des External port (s) erreichbar sein:

z.B. `http://212.58.85.XXX:8080`

Auto Reboot (optional, empfohlen)

Falls die Verbindung zum mobilen Datennetz oder dem IP-Tunnel-Server verloren geht, kann mittels einem konfigurierten Auto-Reboot das Gerät automatisch neu gestartet werden. Vor allem bei Geräten, die sich an entlegenen Standorten befinden, hat sich der Auto Reboot schon vielfach bewährt.

1. Navigieren Sie zu **System > Maintenance > Auto Reboot**
2. Klicken Sie in der vorhandenen Zeile auf **Edit**
3. Enable: **Aktiviert**
4. No action on data limit: **wenn möglich, deaktiviert**
5. Action if no echo is received: **Reboot**
6. Interval between pings: **5 mins**
7. Ping timeout (sec): **5**
8. Packet size: **56**
9. Retry count: **3**
10. Interface: **Automatically selected**
11. Host to ping: **212.58.85.1**
12. Klicken Sie auf **Save**

Fehlerdiagnose

1. Bitte prüfen Sie alle Schritte der Konfigurationsanleitung. Anleitungen werden von uns getestet, bevor sie veröffentlicht werden. Wir verwenden diese Anleitungen selbst für die Konfiguration von Geräten, die wir an Kunden versenden.
2. Ist das Gerät mit dem Mobilfunknetz verbunden?
3. Stimmt die Uhrzeit auf dem Gerät?

4. Speichern Sie die VPN-Konfiguration (Services > VPN) erneut ab, damit wird der Dienst neu gestartet.
5. **Starten Sie das Gerät neu, damit der Protokollringpuffer neu initialisiert wird. Falls Sie das Gerät vor Generierung der Protokolldaten nicht neu starten, können wir keinen Support leisten da die benötigten Startprotokolle fehlen.**
6. Navigieren Sie zu System > Administration > Reiter "Troubleshoot"
7. Schicken Sie uns unter Angabe Ihres Benutzernamens und der zugeteilten IPv4-Adresse sowie einer genauen Fehlerbeschreibung folgende Daten an info@internet-xs.de
8. System log: Show (Ausgabe per E-Mail zuschicken)
9. Kernel log: Show (Ausgabe per E-Mail zuschicken)
10. Include GSMD information: Aktivieren
11. Include PPPD information: Aktivieren
12. Include chat script information: Aktivieren
13. Include network topology information": Aktivieren
14. Troubleshoot file: Download (Ausgabe per E-Mail zuschicken)

Impressum

Verantwortlich für die Inhalte in diesem Dokument:

Internet XS Service GmbH
Internetagentur
Heißbrühlstr. 15
70565 Stuttgart

Telefon: 07 11/78 19 41 - 0
Telefax: 07 11/78 19 41 -79
E-Mail: info@internet-xs.de
Internet: www.internet-xs.de

Geschäftsführer: Helmut Drodofsky
Registergericht: Amtsgericht Stuttgart
Registernummer: HRB 21091
UST.IdNr.: DE 190582774

Alle Preise, sofern nicht ausdrücklich anders gekennzeichnet, inkl. gesetzlich geltender deutscher MwSt.

Angebote, sofern nicht ausdrücklich anders gekennzeichnet, gültig bis 4 Wochen nach Zusendung / Abruf.

Die Weiterverbreitung dieses Dokuments, der darin befindlichen Inhalte, auch nur Auszugsweise, ist nur mit ausdrücklicher Genehmigung der Internet XS Service GmbH gestattet.