



KB 24695: OVPNIP5

IP-Tunnel mit OpenVPN einrichten auf Teltonika RUT950 / RUT955 (Firmware- Version bis 6.xx)

Stand	12.08.2022, 12:05:35
Version	62f625ef
Referenz-URL	https://www.internet-xs.de/kb/24695
PDF-URL	https://www.internet-xs.de/kb/Internet-XS_KB-24695-62f625ef.pdf

Vorwort	4
Vorbereitung	4
Grundkonfiguration	4
VPN-Client zum Bezug der festen IP einrichten	5
DNS-Einstellungen	6
Ping-Reboot einrichten	6
Neustart	7
Verbindung testen	7
Port-Weiterleitungen definieren	7
Angebundenes Gerät konfigurieren	8
Fehlerdiagnose	8
Protokolle und Referenzen	9
iperf3	9
Ping 2048 Byte	9
Ping 1472 Facebook	10
Check-IP Amazon AWS	10

Zielgruppe:

Besitzer von Teltonika RUT950 / RUT955-Geräten mit Firmware-Version 4.xx bis 6.xx

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: OVPNIP5
- Hostname: ovpnip5.internet-xs.de
- IP-Adresse: 212.58.69.9
- Protokoll: OpenVPN / TUN / UDP oder TCP
- Client IP-Adress-Bereich: 212.58.84.0/24 (212.58.84.1 - 212.58.84.254)
- Benutzername / Zugangskennung Format: ix009-....-.....

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.

Vorwort

Ziel dieser Anleitung ist die Konfiguration eines Teltonika RUT955 oder RUT950 für die Nutzung unseres Produkts "Feste, öffentliche IPv4 Adresse". Nach der Konfiguration kommuniziert der RUT950 / RUT955 über eine feste, öffentliche IPv4-Adresse mit dem Internet und ist über diese IP-Adresse aus dem Internet erreichbar. Grundvoraussetzung ist eine funktionierende Internet-Verbindung am Teltonika RUT950 / RUT955 sowie ein aktiver Zugang auf unserem Einwahlserver. Der verwendete LTE-Provider sowie der Tarif spielen keine Rolle, da unser Dienst UDP (oder TCP) Port 1194 verwendet, der auch für HTTPS-Verbindungen verwendet wird und daher bei allen uns bekannten Providern nutzbar ist.

Wir gehen davon aus, dass das Gerät im Großen und Ganzen nach Standardeinstellungen konfiguriert ist.

Die Anleitung basiert auf diesem Modell:

Router Modell : Teltonika RUT950 (z.B. RUT950 U022C0) Firmware Version : RUT9XX_R_00.06.06.1

Die Anleitung ist ebenfalls geeignet für diese Modelle:

- RUT955
- RUT230 (nicht empfohlen)
- RUT240 (aufgrund der begrenzten Prozessorleistung langsam)

Falls die Konfiguration nicht gelingen sollte, aktualisieren Sie Ihr Gerät bitte zunächst auf die o.g. Firmware-Version, da wir Sie sonst nicht bei der Konfiguration unterstützen können.

Für Konfigurationen, die sich außerhalb der Anleitung bewegen (insbesondere Verwendung zusätzlicher Tunnel zu anderen Providern), können wir keinen Support leisten. Bitte konfigurieren Sie zunächst unseren Dienst und prüfen Sie die volle Funktionsfähigkeit.

Vorbereitung

Bitte laden Sie diese Datei herunter, sie wird im Laufe der weiteren Konfiguration benötigt:

[Download "ovpnip5.internet-xs.de.ca.crt.txt"](https://ovpnip5.internet-xs.de/ca.crt.txt)

Grundkonfiguration

Nehmen Sie die Konfiguration des Geräts zunächst gemäß Ihren Anforderungen vor. Es muss sichergestellt sein, dass das Gerät vor Beginn der Konfiguration über eine funktionsfähige Internet-Verbindung verfügt.

1. Starten Sie das Gerät neu (System > Reboot)
2. Prüfen Sie, ob der APN für Ihren Mobilfunkanbieter korrekt konfiguriert ist (Network > Mobile > SIM1 > Einstellung "APN"). Falls Sie die APN-Einstellungen korrigieren müssen: Speichern Sie die Einstellung ("Save") und starten Sie das Gerät erneut neu und führen Sie Schritt 1. nochmals aus.
3. Prüfen Sie, ob die Uhrzeit auf dem Gerät stimmt (Status > System > "Local Device Time")
4. Prüfen Sie, ob Ihr Gerät mit dem Mobilfunknetz verbunden ist (Status > Network > Mobile > "Data connection state" muss "Connected" sein. Außerdem sollte die Signalstärke nicht weniger als 50 dBm betragen (verwenden Sie ggf. externe Antennen).
5. Prüfen Sie, ob der Internet XS Einwahlserver erreichbar ist:
6. System > Administration > Tab "Diagnostics"

7. Feld "Host": Geben sie ovnpip5.internet-xs.de ein
8. Klicken Sie auf "Ping"

Eine Ausgabe wie diese sollte erscheinen:

```
PING ovnpip5.internet-xs.de (212.58.69.9): 56 data bytes
64 bytes from 212.58.69.9: seq=0 ttl=53 time=50.245 ms
64 bytes from 212.58.69.9: seq=1 ttl=53 time=87.647 ms
64 bytes from 212.58.69.9: seq=2 ttl=53 time=78.950 ms
64 bytes from 212.58.69.9: seq=3 ttl=53 time=86.542 ms
64 bytes from 212.58.69.9: seq=4 ttl=53 time=91.697 ms
--- ovnpip5.internet-xs.de ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 50.245/79.016/91.697 ms
```

So lange kein erfolgreicher Ping zustande kommt, ist das Gerät nicht korrekt konfiguriert. Die Einrichtung der festen IP ist dann noch nicht möglich. Bitte prüfen Sie Ihre SIM-Karte und Netzwerk / APN-Konfiguration. Wenden Sie sich ggf. an Ihren Mobilfunkprovider.

Wichtig: Vergeben Sie ein sicheres Zugriffspasswort. Nach der Konfiguration ist das Gerät öffentlich, weltweit mit einer festen IP-Adresse über das Internet erreichbar. Standardpasswörter / schwache Passwörter führen binnen wenigen Minuten zu einem gehackten Gerät.

VPN-Client zum Bezug der festen IP einrichten

Wenn eine funktionierende Internet-Verbindung vorhanden ist, können Sie mit der Einrichtung des VPN-Clients beginnen.

1. Services > VPN
2. Tab "OpenVPN"
3. Role: Client
4. New configuration name: **ixsvpnip** (der Name muss exakt so lauten)
5. Auf "Add new" klicken
6. In der Zeile mit der neuen Client-Definition auf "Edit" klicken
7. Enable OpenVPN config from file: **deaktiviert**
8. Enable: Aktivieren
9. TUN/TAP: TUN (tunnel)
10. Protocol: UDP
11. Port: 1194
12. LZO: Deaktiviert
13. Authentication: Password
14. Encryption: none
15. TLS cipher: All
16. Remote host/IP address: **212.58.69.9** (nicht "Ihre" feste IP-Adresse)
17. Resolve retry: infinite
18. Keep alive: 20 120
19. Remote network IP address: *leer*
20. Remote network IP netmask: *leer*
21. HMAC authentication algorithm: SHA1 (default)
22. Additional HMAC authentication: None

23. User name: ix009-xxxx-yyyyyyyyyy (setzen Sie hier den Benutzernamen / Zugangskennung ein, den Sie von uns erhalten haben)
24. Passwort: YYYYYYYYYY (setzen Sie hier das Zugangspasswort ein, das Sie von uns erhalten haben)
25. Extra options (Klick auf grünes "+", um ein weiteres Feld für "Extra options" zu erzeugen):
 - sndbuf 0
 - rcvbuf 0
 - tun-mtu 1500
 - explicit-exit-notify
 - persist-key
 - persist-tun
 - reneg-sec 0
 - reneg-bytes 0
 - setenv CLIENT_CERT 0
 - remote-cert-tls server
 - fast-io
26. Use PKCS #12 format: deaktiviert
27. Certificate authority: Laden Sie die zuvor heruntergeladene Datei "ovpnip5.internet-xs.de.ca.crt.txt" hoch
28. Client certificate: *leer* (die Authentifizierung erfolgt mittels Benutzername + Passwort)
29. Client key: *leer* (die Authentifizierung erfolgt mittels Benutzername + Passwort)
30. Klicken Sie auf "Save".

DNS-Einstellungen

Ihr Mobilfunkprovider beantwortet DNS-Anfragen wahrscheinlich nur wenn diese von einer IP aus seinem Netz gestellt wurden. Da Ihr Gerät nun mit einer öffentlichen IP aus unserem Netz kommuniziert, wird Ihr Provider die DNS-Anfragen wahrscheinlich nicht mehr beantworten. Daher ist die Eingabe eines benutzerdefinierten DNS-Servers notwendig. Für Tests eignet sich z.B. 8.8.8.8 (Google DNS). Liste öffentlicher DNS-Server in Deutschland: <http://www.ungefiltert-surfen.de/nameserver/de.html>

1. Network > WAN > Zeile "Mobile (WAN)" > Edit
2. Tab: "Advanced Settings"
3. Use DNS servers advertised by peer: Deaktivieren
4. Use custom DNS servers: z.B. 1.1.1.1
5. Durch klicken auf das "+" Symbol können Sie weitere DNS-Server eintragen, z.B. 8.8.8.8 oder 9.9.9.9 (jeder öffentliche DNS-Server ist nutzbar)

Ping-Reboot einrichten

Falls das Gerät an einem schwer erreichbaren Ort aufgestellt wird oder das angeschlossene Netzwerk sehr ruhig ist, empfehlen wir, einen sog. "Ping-Reboot" einzurichten. Dabei versucht der RUT 950 / RUT 955 alle X Minuten ein bestimmtes Ziel zu erreichen. Ist das Ziel für Y versuche nicht erreichbar, wird der Router automatisch neu gestartet.

1. Services > Auto reboot
2. Add
3. Edit
4. Enable: aktivieren

5. Action if no echo is received: reboot
6. Interval between pings: 5 mins
7. Ping timeout: 10 sec
8. Packet size: 56
9. Retry count: 2
10. Interface: Automatically selected
11. Host to ping: **212.58.84.1**

****Außerdem sollte ein "Periodic Reboot" eingestellt werden. ****

1. Services > Auto reboot
2. Reiter "Periodic Reboot"
3. Enable: Aktiviert
4. Days: Sunday: Aktiviert
5. Days: Monday: Aktiviert
6. Days: Tuesday: Aktiviert
7. Days: Wednesday: Aktiviert
8. Days: Thursday: Aktiviert
9. Days: Friday: Aktiviert
10. Days: Saturday: Aktiviert
11. Hours: z.B. 5
12. Minutes: z.B. 7

Damit startet das Gerät jeden Tag um 05:07 neu.

Neustart

Starten Sie das Gerät jetzt neu.

1. System > Reboot > Reboot

Verbindung testen

Nach dem Neustart des Geräts sollte die feste IP-Adresse am Gerät anliegen. Zum testen geben Sie die öffentliche IPv4-Adresse die Sie von uns erhalten haben in die Adresszeile Ihres Browsers ein, also z.B. 212.58.84.ZZZ. Daraufhin sollte das Login-Formular des RUT950 / RUT955 erscheinen.

Falls ein PC / Smartphone im (W)LAN des RUT950 / RUT955 verfügbar ist: Rufen Sie die Adresse <http://internet-xs.eu/tools/ip/> mit einem Browser auf. Dort sollte die Ihnen zugewiesene feste IP angezeigt werden.

Port-Weiterleitungen definieren

Jetzt landen alle eingehenden Pakete an 212.58.84.ZZZ direkt auf dem Teltonika RUT950 / RUT955. Falls Sie z.B. Überwachungstechnik etc. anbinden möchten, die eine interne LAN-IP vom Teltonika RUT950 / RUT955 bezieht, müssen dafür je Endgerät / Dienst Port-Weiterleitungen (DNAT) auf dem RUT950 / RUT955 eingerichtet werden.

1. Network > Firewall

2. Reiter "Port Forwarding"
3. Bereich "New port forward":
4. Name: Beliebiger Name für die Regel
5. Protocol: TCP, UDP (falls unbekannt "TCP+UDP")
6. External port: z.B. 80 für Webserver, 443 für HTTPS, 3398 für RDP usw. (entspricht IhreFestelIP:External port, z.B. 212.58.84.XXX:3389)
7. Internal IP address: LAN-IP-Adresse des Geräts, auf das weitergeleitet werden soll
8. Internal port: Port für den zu erreichbar machenden Dienst (dieser Port wird i.d.R. durch die Software vorgegeben, z.B. Webinterface einer IP-Kamera etc.)
9. Klicken Sie auf "Save"
10. **Klicken Sie neben der neu erstellten Regel auf "Edit"**
11. **Source zone:** Von **"wan: wan: ppp"** auf **"vpn: openvpn:"** umstellen.
12. Weitere Einstellungen nach bedarf vornehmen
13. Speichern mit "Save"

Diese Schritte sind für alle gewünschten Port-Weiterleitungen zu wiederholen.

Angebundenes Gerät konfigurieren

Für das angebundene Gerät ist keine spezielle Konfiguration erforderlich. Es muss lediglich als Standard-Gateway die LAN-IP-Adresse des Teltonika RUT950 / RUT955 eingestellt sein, also z.B. 192.168.1.1.

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 > OpenVPN) 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)

Protokolle und Referenzen

iperf3

Upload:

```
C:\Users\user>iperf3 -c 212.58.84.1
Connecting to host 212.58.84.1, port 5201
[ 4] local 192.168.1.60 port 8799 connected to 212.58.84.1 port 5201
[ ID] Interval           Transfer     Bandwidth
[ 4]  0.00-1.00    sec   1.25 MBytes  10.5 Mbits/sec
[ 4]  1.00-2.00    sec   1.50 MBytes  12.6 Mbits/sec
[ 4]  2.00-3.00    sec   1.50 MBytes  12.6 Mbits/sec
[ 4]  3.00-4.00    sec   1.50 MBytes  12.6 Mbits/sec
[ 4]  4.00-5.00    sec   1.38 MBytes  11.5 Mbits/sec
[ 4]  5.00-6.00    sec   1.50 MBytes  12.6 Mbits/sec
[ 4]  6.00-7.00    sec   1.50 MBytes  12.6 Mbits/sec
[ 4]  7.00-8.00    sec   1.50 MBytes  12.6 Mbits/sec
[ 4]  8.00-9.00    sec   1.50 MBytes  12.6 Mbits/sec
[ 4]  9.00-10.00   sec   1.50 MBytes  12.6 Mbits/sec
- - - - -
[ ID] Interval           Transfer     Bandwidth
[ 4]  0.00-10.00   sec   14.6 MBytes  12.3 Mbits/sec      sender
[ 4]  0.00-10.00   sec   14.6 MBytes  12.3 Mbits/sec
receiver
iperf Done.
```

Download:

```
C:\Users\user>iperf3 -c 212.58.84.1 -R
Connecting to host 212.58.84.1, port 5201
Reverse mode, remote host 212.58.84.1 is sending
[ 4] local 192.168.1.60 port 8802 connected to 212.58.84.1 port 5201
[ ID] Interval           Transfer     Bandwidth
[ 4]  0.00-1.00    sec   1.03 MBytes  8.60 Mbits/sec
[ 4]  1.00-2.00    sec   1.18 MBytes  9.88 Mbits/sec
[ 4]  2.00-3.00    sec   1.10 MBytes  9.24 Mbits/sec
[ 4]  3.00-4.00    sec   1.18 MBytes  9.93 Mbits/sec
[ 4]  4.00-5.00    sec   1.27 MBytes  10.6 Mbits/sec
[ 4]  5.00-6.00    sec   1.26 MBytes  10.6 Mbits/sec
[ 4]  6.00-7.00    sec   1.32 MBytes  11.1 Mbits/sec
[ 4]  7.00-8.00    sec   1.29 MBytes  10.8 Mbits/sec
[ 4]  8.00-9.00    sec   1.11 MBytes  9.30 Mbits/sec
[ 4]  9.00-10.00   sec   1.26 MBytes  10.5 Mbits/sec
- - - - -
[ ID] Interval           Transfer     Bandwidth      Retr
[ 4]  0.00-10.00   sec   12.3 MBytes  10.4 Mbits/sec    21      sender
[ 4]  0.00-10.00   sec   12.2 MBytes  10.3 Mbits/sec
receiver
iperf Done.
```

Ping 2048 Byte

Dieser Test stellt fest, ob die IP-Fragmentierung korrekt funktioniert.

```
C:\Users\user>ping -l 2048 heise.de
```

```
Ping wird ausgeführt für heise.de [193.99.144.80] mit 2048 Bytes Daten:
```

```
Antwort von 193.99.144.80: Bytes=2048 Zeit=76ms TTL=241
```

```
Antwort von 193.99.144.80: Bytes=2048 Zeit=56ms TTL=241
```

```
Antwort von 193.99.144.80: Bytes=2048 Zeit=57ms TTL=241
```

```
Antwort von 193.99.144.80: Bytes=2048 Zeit=58ms TTL=241
```

```
Ping-Statistik für 193.99.144.80:
```

```
  Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0  
  (0% Verlust),
```

```
Ca. Zeitangaben in Millisek.:
```

```
  Minimum = 56ms, Maximum = 76ms, Mittelwert = 61ms
```

Ping 1472 Facebook

Dieser Test stellt fest, ob die maximale Paketgröße an Facebook-Server gesendet werden kann (IP-Fragmentierung)

```
C:\Users\user>ping -l 1472 facebook.com
```

```
Ping wird ausgeführt für facebook.com [69.171.250.35] mit 1472 Bytes Daten:
```

```
Antwort von 69.171.250.35: Bytes=1472 Zeit=46ms TTL=51
```

```
Antwort von 69.171.250.35: Bytes=1472 Zeit=75ms TTL=51
```

```
Antwort von 69.171.250.35: Bytes=1472 Zeit=50ms TTL=51
```

```
Antwort von 69.171.250.35: Bytes=1472 Zeit=53ms TTL=51
```

```
Ping-Statistik für 69.171.250.35:
```

```
  Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0  
  (0% Verlust),
```

```
Ca. Zeitangaben in Millisek.:
```

```
  Minimum = 46ms, Maximum = 75ms, Mittelwert = 56ms
```

Check-IP Amazon AWS

```
C:\Users\user>curl http://checkip.amazonaws.com  
212.58.84.XXX
```

Impressum

Verantwortlich für die Inhalte in diesem Dokument:

Internet XS Service GmbH
Internetagentur
Heßbrühlstr. 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 geldender 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.