KB 34213: OpenVPN allgemein

OpenVPN-Server konfigurieren auf Teltonika RUT950

Stand	24.02.2022, 12:51:26
Version	6217713e
Referenz-URL	https://www.internet-xs.de/kb/34213
PDF-URL	https://www.internet-xs.de/kb/Internet-XS_KB-34213-6217713e.pdf

Inhalt

Einleitung

Für den sicheren Zugriff auf ein LAN aus dem Internet wird ein OpenVPN-Server benötigt. Dieser kann zusätzlich zu einer IP-Tunnel-Verbindung, die die feste, öffentliche IPv4-Adresse bereitstellt die dafür notwendig ist, konfiguriert werden. Port-Weiterleitungen zu einzelnen Geräten im LAN wie z.B. IP-Kameras / Webcams, Datenloggern etc. werden dann nicht mehr benötigt. Die Gesamtlösung ist vergleichbar mit anderen VPN-Lösungen wie z.B. FRITZ!Fernzugang.

Zielgruppe:
Besitzer eines Teltonika RUT950 mit fester, öffentlicher IPv4-Adresse, die über eine verschlüsselte Verbindung auf das LAN des Teltonika RUT950 zugreifen möchten.

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.**

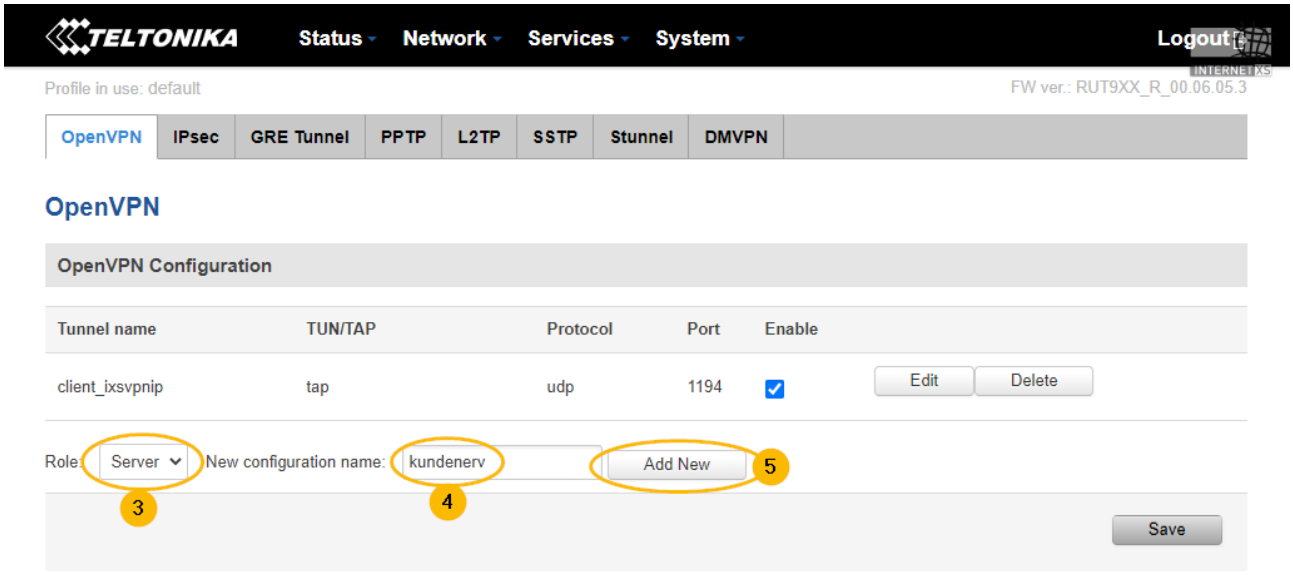
In einer PDF-Datei können Zeilenumbrüche innerhalb von Code-Blöcken vorhanden sein, da die Seitenbreite begrenzt ist. Bitte verwenden Sie für Copy & Paste im Zweifelsfall ein Editor-Programm als Zwischenritt und entfernen Sie unerwünschte Zeilenumbrüche.

Voraussetzungen

1. Teltonika RUT950 (möglicherweise auch geeignet für RUT955 / RUT240)
2. Bereits konfigurierte IP-Tunnel-Verbindung zur Bereitstellung einer festen, öffentlichen IPv4-Adresse auf dem Teltonika RUT950
3. CA-Zertifikat (“ca.crt”), Server-Zertifikat (“server.crt”), Server-Schlüssel (“server.key”), DH-Parameter (“dhparam.pem”) EasyRSA Anleitung

OpenVPN-Server-Profil erstellen

1. Loggen Sie sich auf die Web-Oberfläche des RUT950 ein.
2. Navigieren Sie zu **Services > VPN > OpenVPN**
3. Wählen Sie in der Auswahlliste **Role** den Wert **Server**
4. Vergeben Sie einen Namen für den Server, z.B. **kundenserv**
5. Klicken Sie auf **Add New**

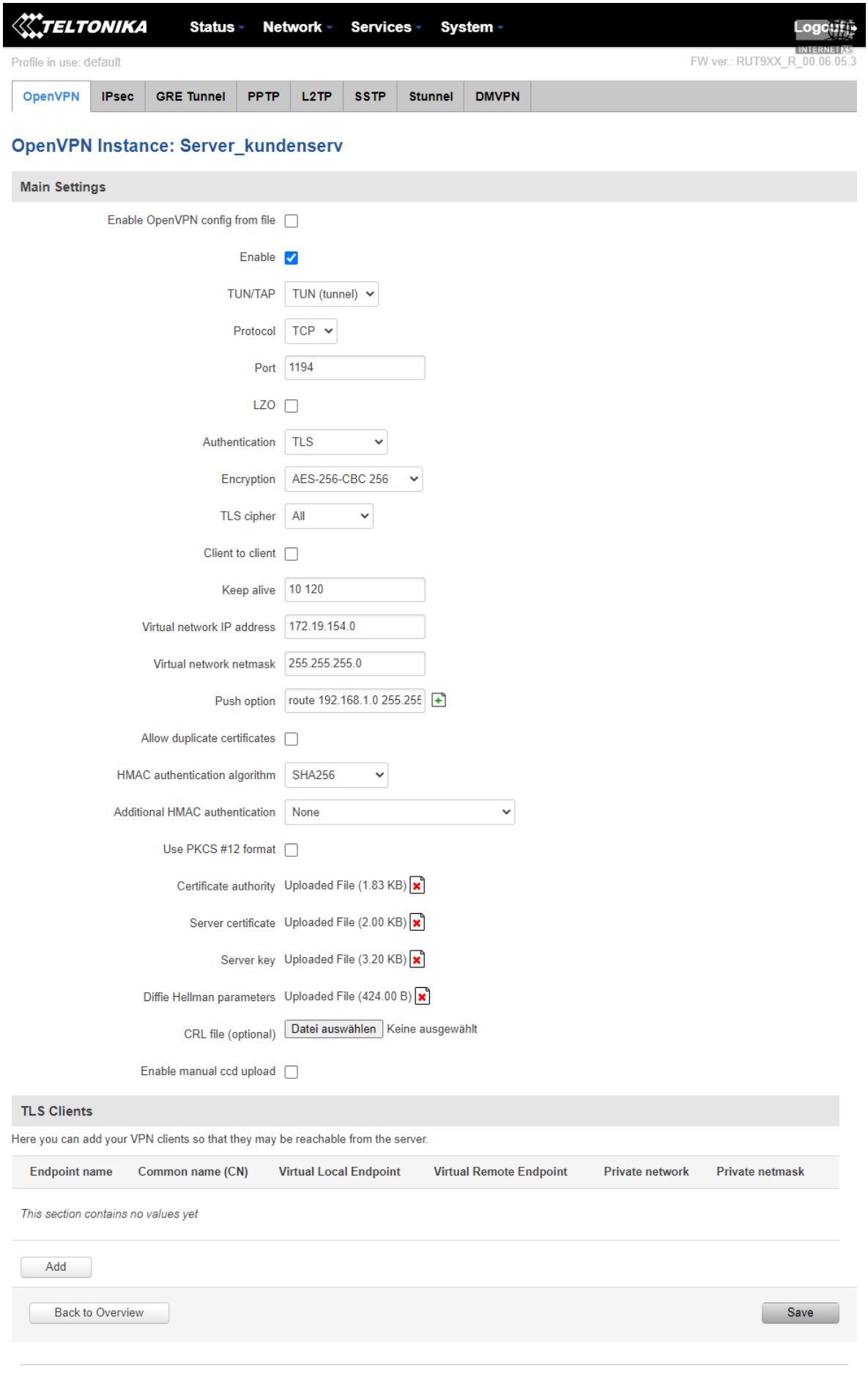


OpenVPN-Server konfigurieren

Hinweis: Die genauen Feld-Bezeichnungen und Anordnungen können je nach Firmware-Version variieren. Die vorgeschlagenen Einstellungen sind als Beispiel zu verstehen. Die Abwägung, ob diese Einstellungen zeitgemäß und für Ihre individuelle Anwendung und deren Sicherheitsanforderungen geeignet sind, nehmen Sie als Administrator selbst vor.

1. Enable OpenVPN config from file: **Deaktiviert**
2. Enable: **Aktiviert**
3. Protocol: **TCP** (UDP ist möglich, jedoch sind dann u.U. weitere Einstellungen über die Kommandozeile notwendig)
4. Port: z.B. 1194
5. LZO: Deaktiviert
6. Authentication: TLS
7. Encryption: z.B. **AES-256-CBC 256**
8. TLS cipher: All

9. Client to client: Falls Sie die Kommunikation zwischen verschiedenen Clients ermöglichen möchten, aktivieren. (Standard: Deaktiviert)
10. Keep alive: z.B. 10 120
11. Virtual network IP address: z.B. 172.19.154.0 (frei wählbar, darf weder auf Client noch Server existieren. Geben Sie hier auf keinen Fall das LAN des RUT950 an.)
12. Virtual network netmask: z.B. 255.255.255.0
13. Push option: z.B. route 192.168.1.0 255.255.255.0 (setzen Sie hier das LAN Ihres Teltonika RUT950 ein. Standard: 192.168.1.0. Weitere Beispiele: 192.168.2.0, 192.168.3.0
14. Allow duplicate certificates: Deaktiviert
15. HMAC authentication algorithm: z.B. **SHA256**
16. Additional HMAC authentication: None
17. Use PKCS #12 format: Deaktiviert
18. Certificate authority: CA-Zertifikat (falls Sie die Zertifikate mittels unserer EasyRSA-Anleitung erstellt haben: **ca.crt**)
19. Server certificate: Server-Zertifikat (falls Sie die Zertifikate mittels unserer EasyRSA-Anleitung erstellt haben: openvpn-server01**.crt**)
20. Server certificate: Server-Zertifikat (falls Sie die Zertifikate mittels unserer EasyRSA-Anleitung erstellt haben: openvpn-server01.unencrypted**.key**)
21. Diffie Hellman parameters: “dh.pem” (falls Sie die Zertifikate mittels unserer EasyRSA-Anleitung erstellt haben: dh**.pem**)
22. Klicken Sie auf **Save**



Beispiel OpenVPN-Client-Konfigurationsdatei

Jeder Client, der sich mit dem OpenVPN-Server verbinden können soll, benötigt eine Konfigurationsdatei. Bitte passen Sie die Konfigurationsdatei auf Ihre Einstellungen an und platzieren Sie die Konfigurationsdatei auf dem Gerät, das sich per VPN mit dem Teltonika RUT950 verbinden soll wie bspw. einem Smartphone (mit OpenVPN Connect App), Windows-PC (mit OpenVPN GUI), Mac OS X (mit Tunnelblick).

Der Dateiname sollte mit “.ovpn” enden, da manche OpenVPN-Clients nur Dateien mit dieser Dateiendung zur Auswahl erlauben.

```
remote 123.456.789.0
```

Setzen Sie hier die feste, öffentliche IPv4-Adresse des Teltonika RUT950 als Verbindungsziel ein.

```
port 1194
```

Falls Sie den OpenVPN-Server nicht auf dem Standard-Port 1194 betreiben, ändern Sie hier den Port entsprechend ab.

```
<ca>...</ca>
```

Setzen Sie hier das CA-Zertifikat ein (falls Sie die Zertifikate mittels unserer EasyRSA-Anleitung erstellt haben: Inhalt der Datei ca.crt)

```
<cert>...</cert>
```

Setzen Sie hier ein Client-Zertifikat ein (falls Sie die Zertifikate mittels unserer EasyRSA-Anleitung erstellt haben: Inhalt der Datei openvpn-client01.crt)

```
<key>...</key>
```

Setzen Sie hier den zum Client-Zertifikat zugehörigen Key ein (falls Sie die Zertifikate mittels unserer EasyRSA-Anleitung erstellt haben: Inhalt der Datei openvpn-client01.key)

```
remote 123.456.789.0
proto tcp-client
port 1194
dev tun
client
verb 5
keepalive 10 60
float
persist-tun
persist-key
auth SHA256
cipher AES-256-CBC
pull

<ca>
-----BEGIN CERTIFICATE-----
MIIDZTCCAk2gAwIBAgIJAPOaLpL5w2mRMA0GCSqGSIb3DQEBCwUAMCYxJDAiBgNV
BAMMGyhJaHIgRmlybWVubmFtZSkgT3BlblZQTiBDQTAeFw0yMDA1MDcwOTM3NDBa
...
bV9W4kTc5S4WSbGPnULqng7CfMn2j+ehrxGHHaFocrji3vmZwvcWYOAfrJK+pzw1
Yn5kdWU0cEVn
-----END CERTIFICATE-----
</ca>

<cert>
-----BEGIN CERTIFICATE-----
MIIDczCCAlugAwIBAgIQM7Z7bF8/cbYhbcDRNRrMczANBgkqhkiG9w0BAQsFADAm
MSQwIgYDVQQDDBsoSWhyIEZpcm1lbm5hbWUpIE9wZW5WUE4gQ0EwHhcNMjAwNTA3
...
1iWo1NUK4x84DW01LxdeIaI4ypFSGZqvOqpcoPqCf2gZVMKETVdPFRbpZ8644ZXd
Xm6AQOc5PuAKaTermRztaZ2M4SxMDnU=
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQINM+s0rj+K7ECAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECFmzle30sgypBIIEyEPMC+TZe6wY
...
cO6yon3c/7byRdhzkj4V+SXat7Jw+JoXeX5qmQwuRHIhFW2WyAmm8Eq/mgY7rs0R
34wgdPL7TwG3HoBZ4/X7Gg==
-----END ENCRYPTED PRIVATE KEY-----
</key>
```

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.

