KB 37864: OVPNIP8

IP-Tunnel mit OpenVPN einrichten auf Lucom LR77 v2

Stand	24.09.2024, 16:47:46
Version	66f2d112
Referenz-URL	https://www.internet-xs.de/kb/37864
PDF-URL	https://www.internet-xs.de/kb/Internet-XS_KB-37864-66f2d112.pdf

Voraussetzungen 4
Testumgebung 4
Grundkonfiguration 4
Passwort ändern 4
SIM-Einstellungen vornehmen 4
Mobilfunkverbindung testen 5
Firewall vorbereiten 6
OpenVPN Client konfigurieren 7
Verbindung prüfen 9
Port-Weiterleitungen / DNAT konfigurieren 11
Optional: Zugriff auf lokale Dienste erlauben 11
Optional: Exposed Host 11
Neustart 12
Port-Weiterleitungen / DNAT testen 12
Automatischer Verbindungs-Neustart bei Verbindungsabbruch (optional) 13
Tipps 13
Fehlerdiagnose 13

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: OVPNIP8
- Hostname: ovpnip8.internet-xs.de
- IP-Adresse: 212.58.69.24
- Protokoll: OpenVPN / TUN / UDP oder TCP
- Client IP-Adress-Bereich: 212.58.88.0/24 (212.58.88.1 - 212.58.88.254)
- Benutzername / Zugangskennung Format: ixs024-....-.....

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

1. Lucom LR77 v2 (LTE router LR77 v2 Libratum) (B+B SmartWorx / Advantech)
2. Firmware-Version: mind. 6.2.8 (2021-02-19)
3. SIM-Karte mit Datenverbindung
4. Test-Zugang oder bezahlter Zugang auf dem IP-Tunnel-Server OVPNIP8
5. Stabile LTE-Verbindung

Testumgebung

- Router: Lucom LR77 v2 (LTE router LR77 v2 Libratum) (B+B SmartWorx / Advantech)
- Firmware: 6.2.8 (2021-02-19)
- SIM-Karte: Vodafone

Die zu erwartende Bandbreite liegt bei ca. 5,5 Mbit/s (Download) bzw. 6,5 Mbit/s (Upload) (der Durchsatz wird durch die Prozessorleistung des Geräts begrenzt, nicht durch den IP-Tunnel-Dienst).

Grundkonfiguration

Damit der IP-Tunnel-Zugang konfiguriert werden kann, muss der Router über eine funktionierende Internet-Verbindung verfügen. Konfigurieren Sie den Router gemäß der Anleitung des Herstellers so, dass eine Internet-Verbindung zustande kommt.

Öffnen Sie die Konfigurationsoberfläche mit einem Internet-Browser.

1. Adresse: http://192.168.1.1/ (in neueren Firmware-Versionen wird Ihr Browser auf HTTPS weitergeleitet, weshalb eine Zertifikatswarnung erscheint)
2. Benutzername: root
3. Passwort: root

Passwort ändern

Nach Abschluss der Konfiguration ist der Router über eine feste, öffentliche IPv4-Adresse aus dem Internet erreichbar. Deshalb sollte das Standard-Passwort umgehend durch ein sicheres Passwort ersetzt werden.

1. Navigieren Sie zu **Administration** > **Change Password**
2. New Password: *ein neues, sicheres Passwort*
3. Confirm Password: *“New Password” wiederholen*
4. Klicken Sie auf **Apply**.

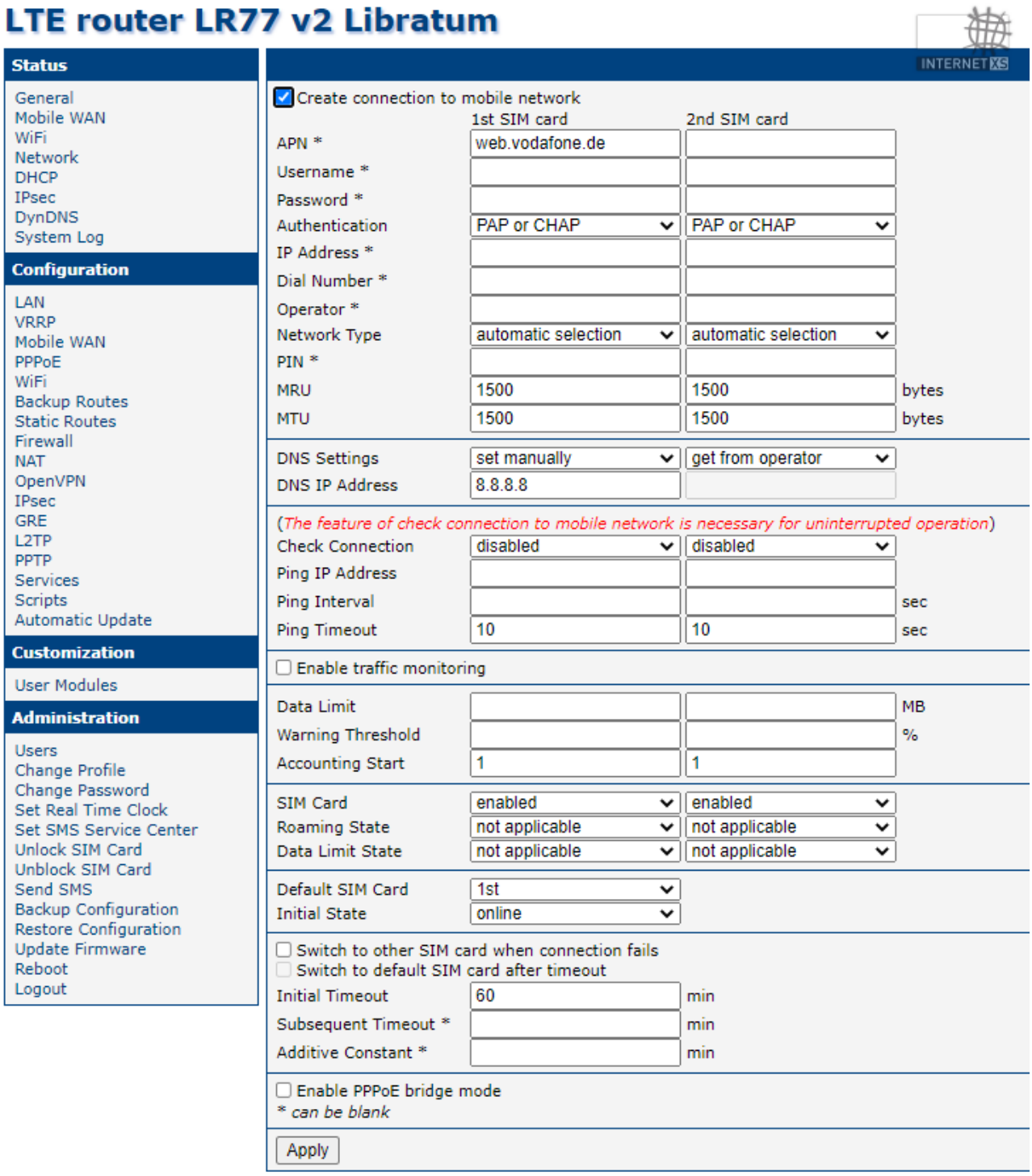
SIM-Einstellungen vornehmen

1. Navigieren Sie zu **Configuration** > **Mobile WAN**
2. Create connection to mobile network: Aktiviert (falls das Kontrollkästchen sichtbar ist)
3. Nehmen Sie die folgenden Einstellungen für den genutzten SIM-Slot vor.
4. APN: Wie von Ihrem Mobilfunkprovider vorgegeben (z.B. `web.vodafone.de` (Vodafone), `internet.telekom` (Telekom / T-Mobile) oder `internet` (o2))
5. Username: Wie von Ihrem Mobilfunkprovider vorgegeben (z.B. *leer* (Vodafone), `t-mobile` (Telekom / T-Mobile)

6. Password: Wie von Ihrem Mobilfunkprovider vorgegeben (z.B. *leer* (Vodafone), `tm` (Telekom / T-Mobile)
7. DNS Settings: **set manually**
8. DNS IP Address: Setzen Sie hier einen DNS-Server wie z.B. `8.8.8.8` (Google), `1.1.1.1` (Cloudflare) oder `9.9.9.9` (IBM Quad9) ein, da Ihr Mobilfunkanbieter DNS-Anfragen, die von einer IP-Adresse außerhalb seines Netzes stammen, nicht beantworten wird, sobald der Router über eine feste, öffentliche IPv4-Adresse verfügt.
9. Klicken Sie auf **Apply**

Mobilfunkverbindung testen

Prüfen Sie, ob Sie mit dem Konfigurationscomputer Webseiten im Internet über den LR77 v2 Router erreichen können. Es sollte außerdem ein `ping` auf `ovpnip8.internet-xs.de` möglich sein. Falls Sie keine Webseiten im Internet erreichen oder ein Ping auf `ovpnip8.internet-xs.de` nicht möglich ist, prüfen Sie bitte die Mobile WAN-Einstellungen.



Firewall vorbereiten

Damit die an die per IP-Tunnel-Verbindung bereitgestellte feste, öffentliche IPv4-Adresse gesendeten Pakete von den über die Web-Oberfläche konfigurierten Firewall-Regeln erfasst werden, muss die virtuelle Netzwerkschnittstelle in die entsprechende Firewall-Zone gesetzt werden.

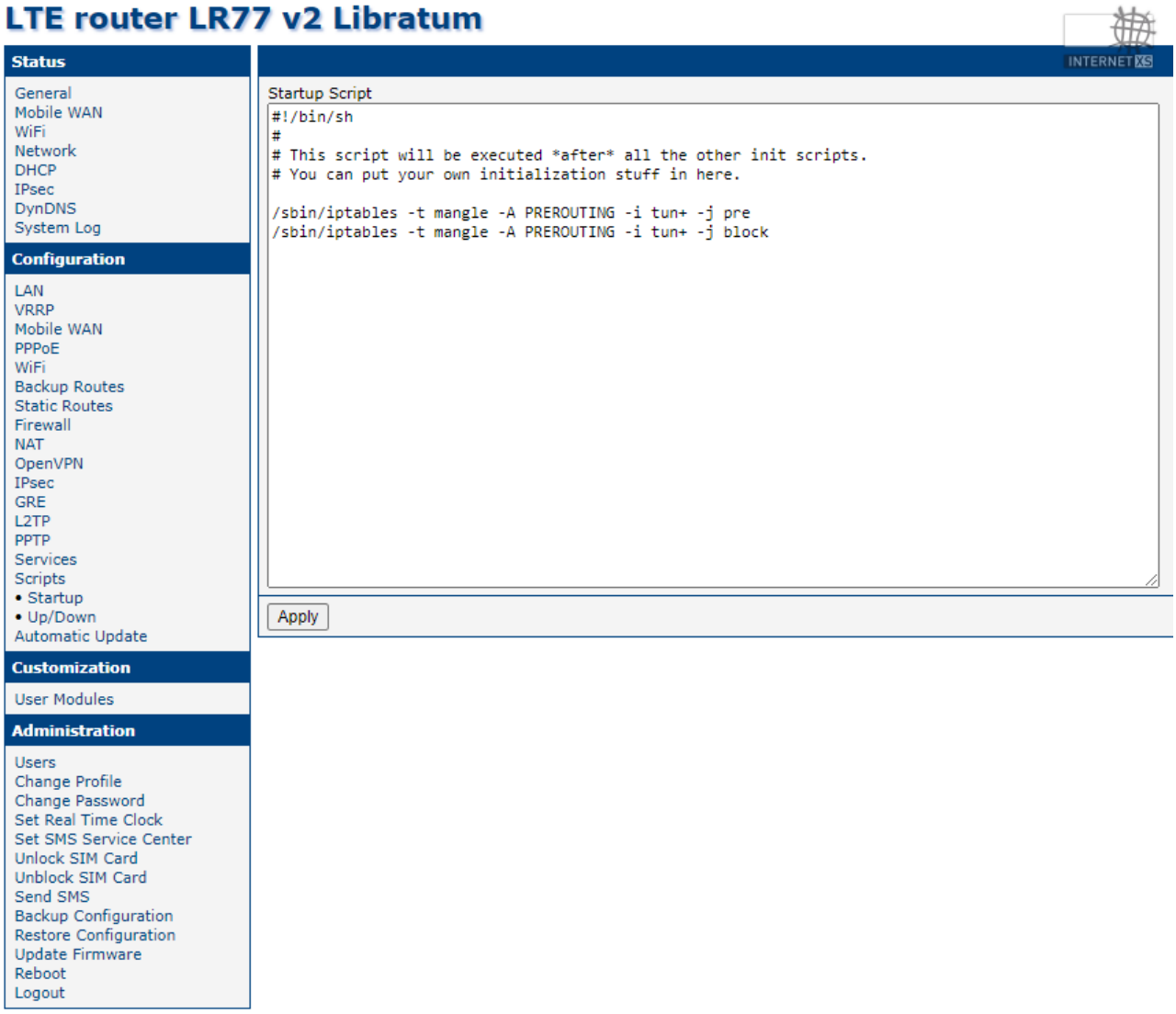
1. Navigieren Sie zu **Configuration** > **Scripts** > **Startup**
2. Fügen Sie dem Startup-Script diese Zeilen an:

```
/sbin/iptables -t mangle -A PREROUTING -i tun+ -j pre
/sbin/iptables -t mangle -A PREROUTING -i tun+ -j block
```

Das Feld `Startup Script` sollte anschließend so aussehen:

```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here.

/sbin/iptables -t mangle -A PREROUTING -i tun+ -j pre
/sbin/iptables -t mangle -A PREROUTING -i tun+ -j block
```



OpenVPN Client konfigurieren

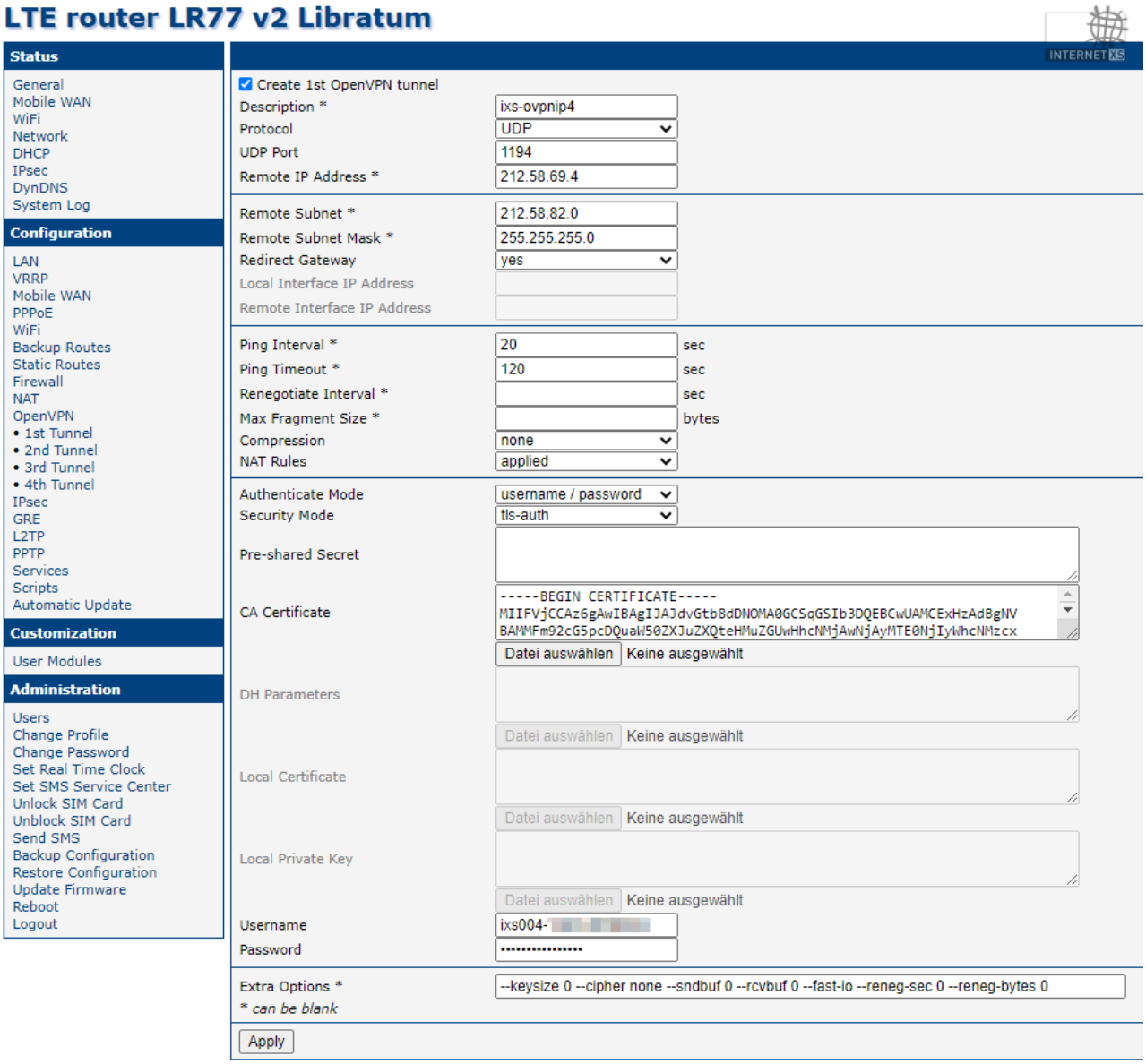
1. Navigieren Sie zu **Configuration** > **OpenVPN** > **1st Tunnel**
2. Create 1st OpenVPN tunnel: Aktiviert
3. Description: ixs-ovpnip8
4. Protocol: UDP
5. UDP Port: 1194

6. Remote IP Address: 212.58.69.24 (setzen Sie hier **nicht** die Ihrem IP-Tunnel Zugang zugeteilte feste, öffentliche IPv4-Adresse ein!)
7. Remote Subnet: 212.58.88.0 (setzen Sie hier **nicht** die Ihrem IP-Tunnel Zugang zugeteilte feste, öffentliche IPv4-Adresse ein!)
8. Remote Subnet Mask: 255.255.255.0
9. Redirect Gateway: yes (falls Sie Port-Weiterleitungen / DNAT konfigurieren möchten) oder no (falls Sie nur auf die Web-Oberfläche des Routers zugreifen möchten)
10. Local Interface IP Address: *leer*
11. Remote Interface IP Address: *leer*
12. Ping Interval: 20
13. Ping Timeout: 120
14. Renegotiate Interval: *leer*
15. Max Fragment Size: *leer*
16. Compression: none
17. Nat Rules: applied
18. Authenticate Mode: username / password
19. Security Mode: tls-auth
20. Pre-shared Secret: Leer
21. CA Certificate: Bitte kopieren Sie den Text-Block unten **inklusive** "`-----BEGIN CERTIFICATE-----`" und "`-----END CERTIFICATE-----`" in das Textfeld:

```
-----BEGIN CERTIFICATE-----
MIIFWDCCA0CgAwIBAgIJAM6lHqecPPDWMA0GCSqGSIb3DQEBCwUAMCExHzAdBgNV
BAMMFm92cG5pcDguaW50ZXJuZXQteHMuZGUwIBcNMjQwOTI0MTEzMzIxWhgPMjEw
MTA1MjQxMTMzMjFaMCExHzAdBgNVBAMMFm92cG5pcDguaW50ZXJuZXQteHMuZGUw
ggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDEQ+LMHtB7BtX1tXB66r9b
+wD93ZSy2Grquv4xweCkeF8ttSJq7pS7Vt+goGFqAS4fOtqofs6iDgliEs/luWQW
lzmW+HgDzni8DZkWFdnSbGc8pMCp1HrQSlJm3NXPc+jUVIOeWy8gPed2WP92aJs2
x1oWFgSD7FvFkDgWMCXsVYZOMCzSc0+55zY8cB/BYYATlSCG4CZ9NJtw/JVecIFa
CaYyMPN8bpbdYW+OrBApbsfDJqICX6iIoC7owyKMOy6/LSluSrUYzVLoHV0JG7kP
5VGhEEA4F926z7shJSNzVSZWUE7CRueKRm+QlSAiloiASSI02jCwy4tmSRaEriEL
pA/kWTnJF+61bsKorkGinkWqksiYokZo0diXqThDV/0C3P0eKgX1AtR2WhoQr9ke
A7IvLdDtAxYKDr9DBNgfL5f/MdJcD17TBj8PzDNdh1W5kSLuYMwzxW/bScBpgfro
KIn2jKtMEbFl+qBmzu3cWttMkCIoKPKO+Pr9ZGsvYzcOvxsCxWEG5/PgZjL3Sf/B
4Pa7bQSyTbQOdocxjRs8qmrt58DFBoCOc3db3OD6BqQ35e9AMUgx0R7CxbsNrGXf
qSnyg9HvI7bSWxDVm4bzpw29lTk6dshDHtwXrDUlOzgmho0S6yWljykV9kJLRTT/
O9AZvYs6rB5fSWVfOSvzUwIDAQABo4GQMIGNMB0GA1UdDgQWBBQ/aVQtQzAloOGh
6DGWPgwG7hqBCTBRBgNVHSMESjBIgBQ/aVQtQzAloOGh6DGWPgwG7hqBCaElpCMw
ITEfMB0GA1UEAwwWb3ZwbmlwOC5pbnRlcm5ldC14cy5kZYIJAM6lHqecPPDWMAwG
A1UdEwQFMAMBAf8wCwYDVR0PBAQDAgEGMA0GCSqGSIb3DQEBCwUAA4ICAQCGa+jS
Vj3Zgmtqvdb5K+ufAPU00ude2BlgA2v3waNB1uXsvA5d7O21HfaBrtYobVewQ1FH
00Xm8skxrV3fwdeTs1GBQ7Sy95TuKER1FOMnRGLiJJQOmsvkyQkuopQW2q4Aon5h
rdhQIim4hmutiNK/LtLcePe/D8pVSn8CxZ0h8M7WYfp2yqEOOwcXAEk2VIW03YcE
z4pVEuwEkJT1Pha6KVXcVmYsvknACqm6hneaexZXHIrSNbDtm0Ap2GSzG/nLlKr6
E30UlZB7hsAjBmM0TxF8HS6g6npzhxeANqy3Zst+vBomfbJI6AmWQn3kvWkZS8V/
ZxhDptR7Cp14OtIN0VNvBR7DZzNbgNUs23wDGEqLUqlHVFciiIzipSOXxICJGfbr
bwABBi5KSQWokluMR4kyhWJb7e3Kv88HPGhaIDyQkemF4qKx4T0RN9vYxwDoErXp
AI7gqXSmJ8v/5PgRvZ2Hm+bN2HYB369JsF2TcngctIQGv91SIaPTOSveeVmDLoan
4MpgTa0NVwcoO/qzXFH4kMskcmAKJ9ZZIDAKiZ1VTprUz/2ua56cAo1a9HCwTeoD
1yA3uuKtGQS7hqfCW00ZoKAWG7xl8a1Sk460GcN5trABc7d817nbHr3dn+WcGlW
g4yUi2HNRaZt2VMGp3FJpPLdxxhLCJXh+RQCxg==
-----END CERTIFICATE-----
```

22. Username: Setzen Sie hier den Benutzernamen / die Zugangskennung Ihres IP-Tunnel-Zugangs ein (z.B. ixs024-1234-a1b2c3d4)

23. Password: Setzen Sie hier das Passwort zu Ihrem IP-Tunnel-Zugang ein
24. Extra Options: `--keysize 0 --cipher none --sndbuf 0 --rcvbuf 0 --fast-io --reneg-sec 0 --reneg-bytes 0` (falls Sie keine Port-Weiterleitungen vornehmen möchten, sondern nur die Konfigurationsoberfläche per fester, öffentlicher IPv4-Adresse erreichbar machen möchten, verwenden Sie diese Optionen: `--keysize 0 --cipher none --pull-filter ignore redirect-gateway`
25. Klicken Sie auf **Apply**



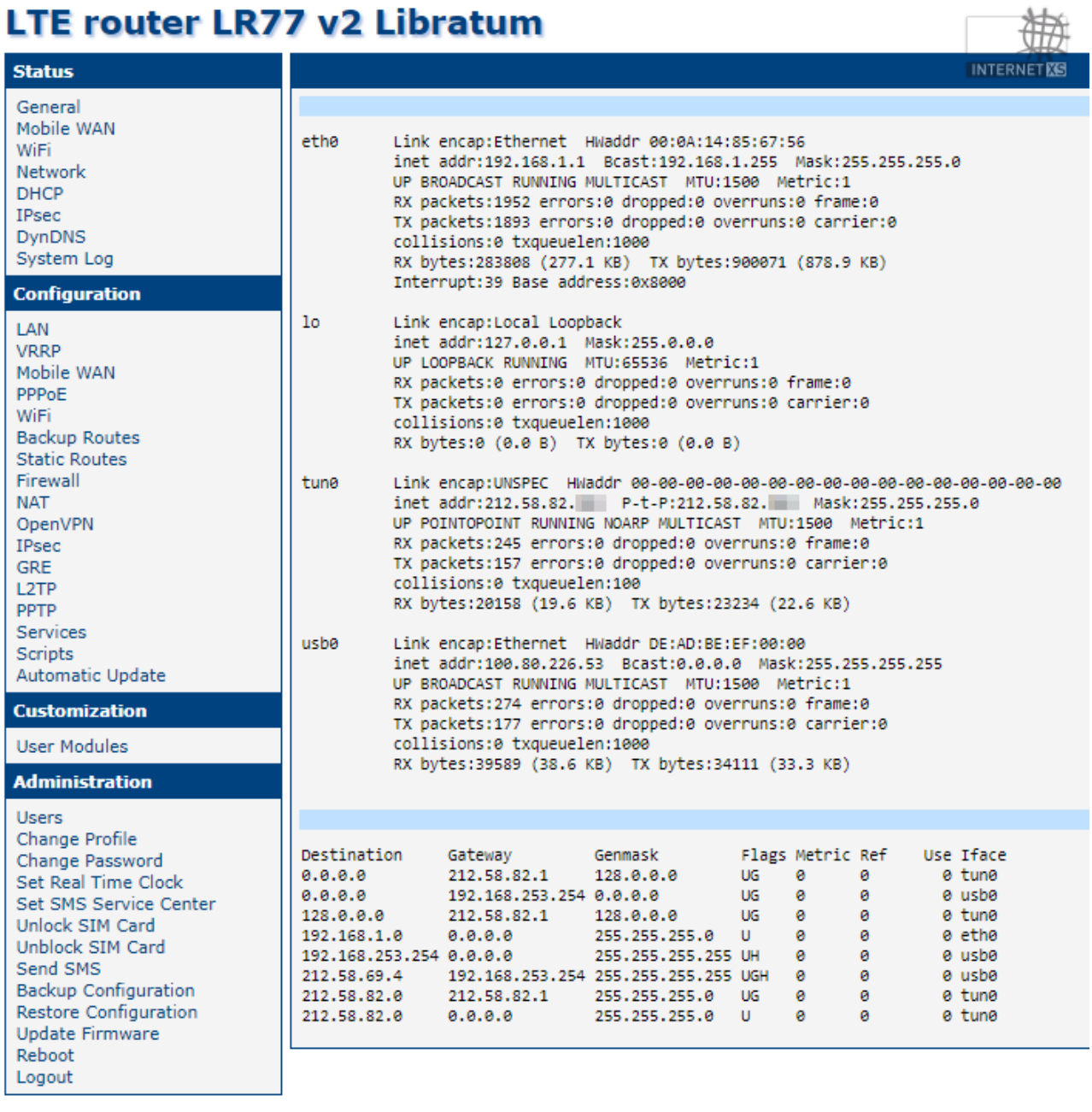
Verbindung prüfen

1. Navigieren Sie zu **Status** > **System Log**
2. Eine Zeile wie diese sollte im Protokoll auftauchen: `2021-03-24 17:02:34 openvpn[1380]: Initialization Sequence Completed`.
3. Navigieren Sie zu **Status** > **Network**
4. Im Bereich **Interfaces** sollte ein Eintrag ähnlich diesem erscheinen:

```
tun0      Link encap:UNSPEC  HWaddr
00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:212.58.88.XXX  P-t-P:212.58.88.XXX  Mask:255.255.255.0
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:82 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:11757 (11.4 KB)  TX bytes:20324 (19.8 KB)
```

5. Im Bereich **Routing Table** sollten folgende Zeilen vorhanden sein, falls Sie die Option **Redirect Gateway** auf **yes** gesetzt haben:

```
0.0.0.0         212.58.88.1     128.0.0.0       UG    0      0        0 tun0
128.0.0.0       212.58.88.1     128.0.0.0       UG    0      0        0 tun0
212.58.69.24     192.168.253.254 255.255.255.255 UGH   0      0        0 usb0
212.58.88.0     212.58.88.1     255.255.255.0   UG    0      0        0 tun0
212.58.88.0     0.0.0.0         255.255.255.0   U     0      0        0 tun0
```



Port-Weiterleitungen / DNAT konfigurieren

Um Dienste von Geräten im Netzwerk des LR77 v2 Libratum per fester, öffentlicher IPv4-Adresse aus dem Internet zu erreichen, müssen entsprechende Port-Weiterleitungen / DNAT konfiguriert werden.

Die folgenden Schritte sind für alle Ports zu wiederholen, die per IP-Tunnel-IP-Adresse erreicht werden sollen.

1. Navigieren Sie zu **Configuration** > **NAT**
2. Public Port(s): Geben Sie hier eine Port-Nummer zwischen 1 und 65535 als **externen** Port ein, z.B. `8080`
3. Private Port(s): Geben Sie hier die Ziel-Port-Nummer der Port-Weiterleitung ein. Dieser Port wird i.d.R. durch das anzubindende Gerät vorgegeben, bspw. `80` oder `554` oder `443` oder `3389`.
4. Type: Das Protokoll wird durch das anzubindende Gerät vorgegeben (`80`, `443`, `3389` i.d.R. TCP, `554` i.d.R. UDP)
5. Server IP Address: Geben Sie hier die LAN-IP-Adresse des anzubindenden Geräts / Webcam / NVR / Datenlogger etc. ein (z.B. `192.168.0.10`)
6. Masquerade outgoing packets: Aktiviert
7. Klicken Sie auf **Apply**.

Optional: Zugriff auf lokale Dienste erlauben

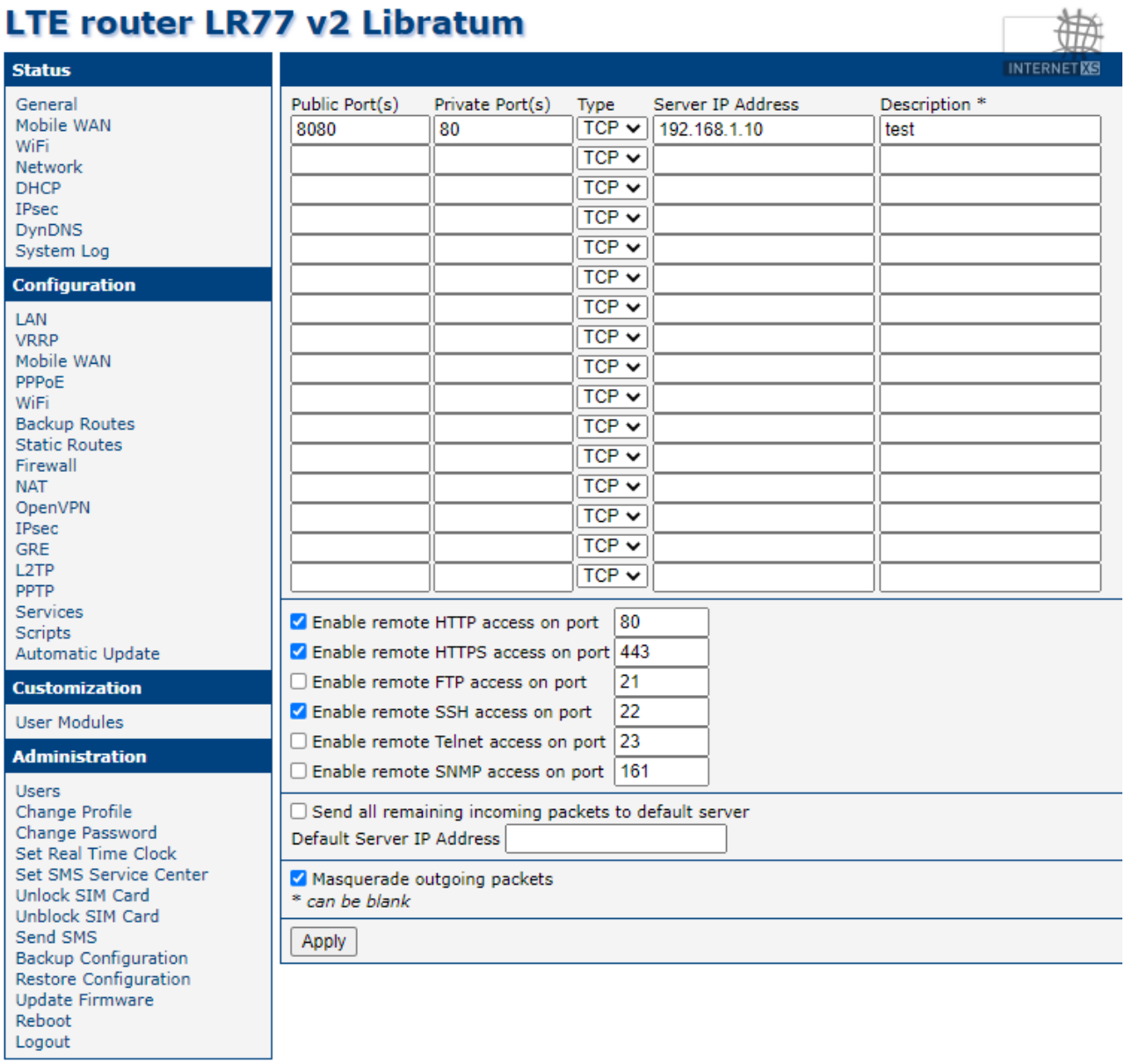
1. Enable remote HTTP access on port: Aktiviert den Zugriff auf die Web-Oberfläche des Routers aus dem Internet.
2. Enable remote HTTPS access on port: Aktiviert den Zugriff auf die Web-Oberfläche des Routers aus dem Internet mittels HTTPS (verschlüsselte Verbindung).
3. Enable remote FTP access on port: Aktiviert den Zugriff auf den FTP-Server des Routers aus dem Internet.
4. Enable remote SSH access on port: Aktiviert den Zugriff auf die Kommandozeile des Routers aus dem Internet (verschlüsselte Verbindung).
5. Enable remote Telnet access on port: Aktiviert den Zugriff auf die Kommandozeile des Routers aus dem Internet (unverschlüsselt, **sollte immer deaktiviert sein**).
6. Enable remote SNMP access on port: Aktiviert den Zugriff auf den SNMP-Server zum auslesen des Status aus dem Internet (unverschlüsselt, **sollte immer deaktiviert sein**).

Aktivieren Sie diese Optionen nur, wenn Sie sie wirklich benötigen. Ändern Sie ggf. die Ports ab, damit das Gerät von automatischen Scannern nicht so leicht gefunden werden kann. Verwenden Sie stets sichere Passworte und verschlüsselte Verbindungen für den Zugriff.

Sie können diese Einstellungen unter **Configuration** > **Firewall** weiter einschränken und bspw. den Zugriff auf die Web-Oberfläche des Routers nur aus bestimmten IP-Netzen erlauben.

Optional: Exposed Host

Mithilfe dem Kontrollkästchen *Send all remaining incoming packets to default server* kann jeglicher eingehender Traffic, der nicht von einer anderen Port-Weiterleitung erfasst wird, an eine bestimmte Ziel-LAN-IP-Adresse (*Default Server IP Address*) gesendet werden. Dies eignet sich immer dann, wenn Sie einen Firewall-Router im Netzwerk betreiben und den LR77 v2 Libratum z.B. als Backup-WAN-Zugang einsetzen möchten.



Neustart

Damit das zuvor eingerichtete Startup-Script erstmalig ausgeführt wird, muss der Router neu gestartet werden.

1. Navigieren Sie zu **Administration** > **Reboot**
2. Klicken Sie auf **Reboot**

Port-Weiterleitungen / DNAT testen

Verbinden Sie sich nun mit einem Gerät, das sich außerhalb des Netzwerks des LR77 v2 Libratum befindet (bspw. mit einem Smartphone, das ins LTE-Netz eingebucht ist), mit einem Port-Weiterleitungsziel. Beispiel:

http://212.58.88.X:8080

- 212.58.88.X: Die Ihrem IP-Tunnel-Zugang zugeteilte feste, öffentliche IPv4-Adresse
- 8080: Im Bereich *Public Port(s)* angegebene Port-Nummer

Die Anfrage wird vom Router dann an bspw. 192.168.0.10:80 weitergeleitet, wobei

- 192.168.0.10: Im Feld *Server IP Address* angegebene Ziel-LAN-IP-Adresse
- 80: Im Bereich *Private Port(s)* angegebener Ziel-Port

entspricht.

Automatischer Verbindungs-Neustart bei Verbindungsabbruch (optional)

Falls das Gerät an einem schwer erreichbaren Ort aufgestellt wird empfehlen wir, einen sog. “Ping-Reboot” einzurichten. Dabei versucht der Router, alle X Minuten ein bestimmtes Ziel zu erreichen. Ist das Ziel nicht erreichbar, wird die Mobilfunkverbindung neu gestartet. Das Ping-Ziel ist dabei der IP-Tunnel-Einwahlserver, auf dem der konfigurierte Zugang beheimatet ist.

1. Navigieren Sie zu **Configuration** > **Mobile WAN**
2. Check Connection: enabled
3. Ping IP Address: 212.58.88.1
4. Ping Interval: 120
5. Ping Timeout: 10
6. Apply

Der Router verfügt leider über keine Möglichkeit, sich automatisch vollständig neu zu starten. Es wird nur die Mobilfunkverbindung neu gestartet.

Tipps

1. Nach erfolgreicher Konfiguration sollte ein Konfigurations-Backup über **Administration** > **Backup Configuration** erstellt werden.
2. Ein Reset kann nur über den Reset-Taster am Gerät durchgeführt werden.

Fehlerdiagnose

1. Bitte prüfen Sie im **Status** > **System Log**, ob das Gerät über ein aktuelles Datum / Uhrzeit verfügt.
2. Die Ihrem IP-Tunnel-Zugang zugeteilte feste, öffentliche IPv4-Adresse muss **nirgends** eingesetzt werden, sie wird automatisch vom IP-Tunnel-Server bezogen.

Falls trotz minutiöser Befolgung dieser Anleitung keine Verbindung mit dem IP-Tunnel-Dienst zustande kommt, senden Sie uns bitte das Systemprotokoll (**Status** > **System Log**) unter Angabe der IP-Tunnel-Zugangskennung (Benutzername) und der zugeteilten IP-Adresse an info@internet-xs.de.

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.

