



KB 64264: OVPNIP4

IP-Tunnel mit OpenVPN einrichten auf Lucom LR77 v2

Stand 24.02.2022, 12:51:26
Version 6217713e
Referenz-URL <https://www.internet-xs.de/kb/64264>
PDF-URL https://www.internet-xs.de/kb/Internet-XS_KB-64264-6217713e.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: OVPNIP4
- Hostname: ovpnip4.internet-xs.de
- IP-Adresse: 212.58.69.4
- Protokoll: OpenVPN / TUN / UDP oder TCP
- Client IP-Adress-Bereich: 212.58.82.0/24 (212.58.82.1 - 212.58.82.254)
- Benutzername / Zugangskennung Format: ixS004-....-.....

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 OVPNIP4
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),  (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 **ovpnip4.internet-xs.de** möglich sein. Falls Sie keine Webseiten im Internet erreichen oder ein Ping auf **ovpnip4.internet-xs.de** nicht möglich ist, prüfen Sie bitte die Mobile WAN-Einstellungen.

Status		INTERNET XS	
General	<input checked="" type="checkbox"/> Create connection to mobile network		
Mobile WAN	1st SIM card	2nd SIM card	
WiFi	APN *	web.vodafone.de	
Network	Username *		
DHCP	Password *		
IPsec	Authentication	PAP or CHAP ▼	PAP or CHAP ▼
DynDNS	IP Address *		
System Log	Dial Number *		
Configuration			
LAN	Operator *		
VRRP	Network Type	automatic selection ▼	automatic selection ▼
Mobile WAN	PIN *		
PPPoE	MRU	1500	1500 bytes
WiFi	MTU	1500	1500 bytes
Backup Routes	DNS Settings	set manually ▼	get from operator ▼
Static Routes	DNS IP Address	8.8.8.8	
Firewall	<i>(The feature of check connection to mobile network is necessary for uninterrupted operation)</i>		
NAT	Check Connection	disabled ▼	disabled ▼
OpenVPN	Ping IP Address		
IPsec	Ping Interval		sec
GRE	Ping Timeout	10	sec
L2TP	<input type="checkbox"/> Enable traffic monitoring		
PPTP	Data Limit		MB
Services	Warning Threshold		%
Scripts	Accounting Start	1	1
Automatic Update	Customization		
User Modules			
Administration			
Users	SIM Card	enabled ▼	enabled ▼
Change Profile	Roaming State	not applicable ▼	not applicable ▼
Change Password	Data Limit State	not applicable ▼	not applicable ▼
Set Real Time Clock	Default SIM Card	1st ▼	
Set SMS Service Center	Initial State	online ▼	
Unlock SIM Card	<input type="checkbox"/> Switch to other SIM card when connection fails		
Unblock SIM Card	<input type="checkbox"/> Switch to default SIM card after timeout		
Send SMS	Initial Timeout	60	min
Backup Configuration	Subsequent Timeout *		min
Restore Configuration	Additive Constant *		min
Update Firmware	<input type="checkbox"/> Enable PPPoE bridge mode		
Reboot	* can be blank		
Logout	<input type="button" value="Apply"/>		

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
```

LTE router LR77 v2 Libratum

The screenshot shows the web interface of the Libratum LTE router LR77 v2. The left sidebar contains a navigation menu with sections: Status, Configuration, Customization, and Administration. The main content area is titled 'Startup Script' and contains a text area with the following script:

```
#!/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
```

Below the text area is an 'Apply' button. The top right corner of the interface shows the 'INTERNET XS' logo.

OpenVPN Client konfigurieren

1. Navigieren Sie zu **Configuration > OpenVPN > 1st Tunnel**
2. Create 1st OpenVPN tunnel: Aktiviert
3. Description: ix-s-ovnpip4
4. Protocol: UDP
5. UDP Port: 1194

6. Remote IP Address: 212.58.69.4 (setzen Sie hier **nicht** die Ihrem IP-Tunnel Zugang zugeteilte feste, öffentliche IPv4-Adresse ein!)
7. Remote Subnet: 212.58.82.0 (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-----
MIIFVjCCAz6gAwIBAgIJAJdvGtb8dNOMA0GCSqGSIb3DQEBCwUAMCEXHzAdBgNV
BAMMFm92cG5pcDQuaW50ZXJ1ZXQteHMuZGUwHhcNMjAwNjAyMTE0NjIyWhcNMzcw
MTI0MTE0NjIyWjAhMR8wHQYDVQDDbZvdnBuaXA0Lm1udGVybmV0LXhzLmRlMIIC
IjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA2egYDqkOxsV+tkuz8eUzG9ek
uRs5TJp/GZlW6MERHFL8nrBXI0Ookg1E7HXkozIN6ucmT1NzODOXTuhrVnY4/ol
7KdsfUjcx55Vf9x/t3LfaA0ZSBU/o1LVpFBDC9BQ7mssfqueRhGI1CmbPLkw9Sry
oLGLAcfV9xb+hWiYQ2SliDaRl1K/osLe/g9neo07ihjBsbvFRa/cm4vVrgS46Yi
FW1gDcSAqpMfarJUhfAeiMs0GP2fmAvsELW992g+JtXmh/5iQXhtix4cI1kIga29
6cyMgdpD2OGQzkXSfiz0Rvb1HI46I1lLojhxBxYHP8RIfUU6r1m/Upz+lONrFpV
q/D03talgMpdK4RpxBwFwkcZ/6dwYcmTgRFQxAKn4Pdx3h4V2GjTf01x7f5zen
Jg4UVWDWdGjFvOpaUGgMIRLgybK9+fYzXOj22vz5cBdrbmrpRz5vhNQbDv7jIttW
8X46mH6GoJrzEHjR2RWL0nXGxxdt2tSwHlqz6t4Lk8p5tck28icmX/ZmXezxa8uz
po+9uBsJ8wZJ+zIQoTtthF3oeKmNnV6X9HYhlq+7XhD/jWaq15wNjPy7ZXWEvb4
mfdBz68kgf4bvQKYKgBLLU2BgX/v384RESd6nZ3EIZUBQlugiDI5nJ5bBfzATMek
umvtSkiK6ohiRWNPzBsCAwEAAaOBkDCBjTAdBgNVHQ4EFgQUbMdu9IRFwgppwNGjc
hs1aqk5I7NYuYQYDVR0jBEowSIAUbmdu9IRFwgppwNGjchslaqk5I7NahJaQjMCEX
HzAdBgNVBAMMFm92cG5pcDQuaW50ZXJ1ZXQteHMuZGUwZGwCCQCXbXrW/HQzTjAMBgNV
HRMEBTADAQH/MASGA1UdDwQEAwIBBjANBgkqhkiG9w0BAQsFAAOCAgEAKU9FW53K
pRjXbsCv+xCnlzMdLyDuBWg0Kgi6N5Rxi471Phz+QVB1/QyivfHANHTpLs891ir
2UXzSQtao+7vZGNShqM6bam41yDiYASGCT/rSh5p0yVrx7Z+9TYsfR16zIwn9E63
R3RCnzPKfjAgBnBeu7/5bL1o0d/v2VxnzE/9rQiY5vZ1DfXzFWtuvwogpADI4B4
vC1+9n2dxeTCAzoy7g4HH+Ct7K78M/S51auQmvAIYOfSagIn8Bvy/haAkURT9aF/
TPZSBRWH2UEvj8UpndC8siROjs398+CMmae+rNnQ9HZZFeF5qDtsdHfvg5VLI5OC
lnNOeqPSFRKxxuDcKaRvfbErN01RyT1AzbuRry3UluU8DMspCO7W0kxErFJxP+2L
kxJrQVqv+4xJgY5LNghX+SdF4XRvSHaN65BnshQ9tUnGRwcUMQcQftUzOyQJslm
EStgKoWyl8MvOIGPE72PNAJ1P2Tb3mTfDiJe2UJpen4OMGi45h4l+F8tKMA/jIeU
S4kYvx0hp9trQ1wbdoK17u9VeB4qBk3SBPAag/ZZV61SxYdRdWmrEiyC0jSQ8JT+
99CULCLvW19BKFjEXRSd6c3LFjXfDKzHlnCxfPzFVXjkQZe5FtihtZOOXprEUb2Q
kTH6y4k8Iyw8DtLAJOT6u0ayzMSNgBohho4=
-----END CERTIFICATE-----
```

22. Username: Setzen Sie hier den Benutzernamen / die Zugangskennung Ihres IP-Tunnel-Zugangs ein (z.B. ixS004-1234-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**

LTE router LR77 v2 Libratum



Status	INTERNET XS
General Mobile WAN WiFi Network DHCP IPsec DynDNS System Log	<input checked="" type="checkbox"/> Create 1st OpenVPN tunnel
	Description * <input type="text" value="ixs-ovpnip4"/>
	Protocol <input type="text" value="UDP"/>
	UDP Port <input type="text" value="1194"/>
	Remote IP Address * <input type="text" value="212.58.69.4"/>
	Remote Subnet * <input type="text" value="212.58.82.0"/>
	Remote Subnet Mask * <input type="text" value="255.255.255.0"/>
	Redirect Gateway <input type="text" value="yes"/>
	Local Interface IP Address <input type="text"/>
	Remote Interface IP Address <input type="text"/>
	Ping Interval * <input type="text" value="20"/> sec
	Ping Timeout * <input type="text" value="120"/> sec
	Renegotiate Interval * <input type="text"/> sec
	Max Fragment Size * <input type="text"/> bytes
	Compression <input type="text" value="none"/>
	NAT Rules <input type="text" value="applied"/>
	Authenticate Mode <input type="text" value="username / password"/>
	Security Mode <input type="text" value="tls-auth"/>
	Pre-shared Secret <input type="text"/>
	CA Certificate <pre>-----BEGIN CERTIFICATE----- MIIFVjCCAz6gAwIBAgIJA7dvGtb8dDNOMA0GCSqGSIb3DQEBCwUAMCExHzAdBgNV BAUMFm92cG5pcDQuaw50ZXJ1ZXQteHMuZGUwHhcNMjAwNjAyMTE0NjIyWWhcNMzc Datei auswählen Keine ausgewählt</pre>
	DH Parameters <input type="text"/>
	Local Certificate <input type="text"/>
	Local Private Key <input type="text"/>
	Username <input type="text" value="ixs004-"/>
	Password <input type="password" value="....."/>
	Extra Options * <input type="text" value="--keysize 0 --cipher none --sndbuf 0 --rcvbuf 0 --fast-io --reneg-sec 0 --reneg-bytes 0"/>
	<small>* can be blank</small>
	<input type="button" value="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:212.58.82.XXX  P-t-P:212.58.82.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      212.58.82.1      128.0.0.0      UG      0      0      0 tun0
128.0.0.0    212.58.82.1      128.0.0.0      UG      0      0      0 tun0
212.58.69.4  192.168.253.254  255.255.255.255 UGH     0      0      0 usb0
212.58.82.0  212.58.82.1      255.255.255.0  UG      0      0      0 tun0
212.58.82.0  0.0.0.0           255.255.255.0  U       0      0      0 tun0
```

LTE router LR77 v2 Libratum



Status	INTERNET XS																																																																								
<ul style="list-style-type: none"> General Mobile WAN WiFi Network DHCP IPsec DynDNS System Log 	<pre>eth0 Link encap:Ethernet HWaddr 00:0A:14:85:67:56 inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:1952 errors:0 dropped:0 overruns:0 frame:0 TX packets:1893 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:283808 (277.1 KB) TX bytes:900071 (878.9 KB) Interrupt:39 Base address:0x8000 lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 UP LOOPBACK RUNNING MTU:65536 Metric:1 RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B) tun0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 inet addr:212.58.82. P-t-P:212.58.82. Mask:255.255.255.0 UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1 RX packets:245 errors:0 dropped:0 overruns:0 frame:0 TX packets:157 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:100 RX bytes:20158 (19.6 KB) TX bytes:23234 (22.6 KB) usb0 Link encap:Ethernet HWaddr DE:AD:BE:EF:00:00 inet addr:100.80.226.53 Bcast:0.0.0.0 Mask:255.255.255.255 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:274 errors:0 dropped:0 overruns:0 frame:0 TX packets:177 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:39589 (38.6 KB) TX bytes:34111 (33.3 KB)</pre>																																																																								
<ul style="list-style-type: none"> Configuration LAN VRRP Mobile WAN PPPoE WiFi Backup Routes Static Routes Firewall NAT OpenVPN IPsec GRE L2TP PPTP Services Scripts Automatic Update 	<table border="1"> <thead> <tr> <th>Destination</th> <th>Gateway</th> <th>Genmask</th> <th>Flags</th> <th>Metric</th> <th>Ref</th> <th>Use</th> <th>Iface</th> </tr> </thead> <tbody> <tr> <td>0.0.0.0</td> <td>212.58.82.1</td> <td>128.0.0.0</td> <td>UG</td> <td>0</td> <td>0</td> <td>0</td> <td>tun0</td> </tr> <tr> <td>0.0.0.0</td> <td>192.168.253.254</td> <td>0.0.0.0</td> <td>UG</td> <td>0</td> <td>0</td> <td>0</td> <td>usb0</td> </tr> <tr> <td>128.0.0.0</td> <td>212.58.82.1</td> <td>128.0.0.0</td> <td>UG</td> <td>0</td> <td>0</td> <td>0</td> <td>tun0</td> </tr> <tr> <td>192.168.1.0</td> <td>0.0.0.0</td> <td>255.255.255.0</td> <td>U</td> <td>0</td> <td>0</td> <td>0</td> <td>eth0</td> </tr> <tr> <td>192.168.253.254</td> <td>0.0.0.0</td> <td>255.255.255.255</td> <td>UH</td> <td>0</td> <td>0</td> <td>0</td> <td>usb0</td> </tr> <tr> <td>212.58.69.4</td> <td>192.168.253.254</td> <td>255.255.255.255</td> <td>UGH</td> <td>0</td> <td>0</td> <td>0</td> <td>usb0</td> </tr> <tr> <td>212.58.82.0</td> <td>212.58.82.1</td> <td>255.255.255.0</td> <td>UG</td> <td>0</td> <td>0</td> <td>0</td> <td>tun0</td> </tr> <tr> <td>212.58.82.0</td> <td>0.0.0.0</td> <td>255.255.255.0</td> <td>U</td> <td>0</td> <td>0</td> <td>0</td> <td>tun0</td> </tr> </tbody> </table>	Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface	0.0.0.0	212.58.82.1	128.0.0.0	UG	0	0	0	tun0	0.0.0.0	192.168.253.254	0.0.0.0	UG	0	0	0	usb0	128.0.0.0	212.58.82.1	128.0.0.0	UG	0	0	0	tun0	192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0	192.168.253.254	0.0.0.0	255.255.255.255	UH	0	0	0	usb0	212.58.69.4	192.168.253.254	255.255.255.255	UGH	0	0	0	usb0	212.58.82.0	212.58.82.1	255.255.255.0	UG	0	0	0	tun0	212.58.82.0	0.0.0.0	255.255.255.0	U	0	0	0	tun0
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface																																																																		
0.0.0.0	212.58.82.1	128.0.0.0	UG	0	0	0	tun0																																																																		
0.0.0.0	192.168.253.254	0.0.0.0	UG	0	0	0	usb0																																																																		
128.0.0.0	212.58.82.1	128.0.0.0	UG	0	0	0	tun0																																																																		
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0																																																																		
192.168.253.254	0.0.0.0	255.255.255.255	UH	0	0	0	usb0																																																																		
212.58.69.4	192.168.253.254	255.255.255.255	UGH	0	0	0	usb0																																																																		
212.58.82.0	212.58.82.1	255.255.255.0	UG	0	0	0	tun0																																																																		
212.58.82.0	0.0.0.0	255.255.255.0	U	0	0	0	tun0																																																																		
<ul style="list-style-type: none"> Customization User Modules 																																																																									
<ul style="list-style-type: none"> Administration Users Change Profile Change Password Set Real Time Clock Set SMS Service Center Unlock SIM Card Unblock SIM Card Send SMS Backup Configuration Restore Configuration Update Firmware Reboot Logout 																																																																									

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 Passwörter 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.

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: 212.58.82.1
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
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.