

# Hardware

## Lucom Router

- VPN Preshared Key darf keine Sonderzeichen enthalten
- während der Konfiguration: Debug-Mode der IPSec-Verbindung auf "control-more" stellen
- Mobilfunk verbunden: in "Mobile WAN" steht unter Connection Log: "(1st SIM card) Connection successfully established."
- NTP-Server eintragen, Zeit muß für VPN stimmen
- VPN verbunden: im System-Log steht "establishing CHILD\_SA ipsec2-1"
- VPN IPSec verbunden: in IPSec-Status steht "ipsec1-1: #1, ESTABLISHED"

```
ipsec1-1: #27, ESTABLISHED, IKEv2, 5625fc8e5cd2d1d8_i* 61f636a1d4dcf7b4_r
  local 'C=de, O=XXXXXXXXXX, CN=halle01-client2' @ XXXXXXXX[4500]
  remote 'C=de, O=XXXXXXXXXX, CN=halle01-server' @ XXXXXXXX[4500]
  AES_GCM_16-256/PRF_HMAC_SHA2_256/MODP_1024
  established 259s ago, reauth in 85147s
ipsec1-1: #28, reqid 1, INSTALLED, TUNNEL-in-UDP, ESP:AES_GCM_16-256
  installed 255s ago, expires in 3345s
  in c71e61cc, 165900 bytes, 1161 packets, 0s ago
  out d4676a8e, 314515 bytes, 5024 packets, 0s ago
  local 10.12.43.0/24
  remote 192.168.250.0/24
```

- Network -> tun0: OpenVPN -Tunnel Schnittstelle
- Network -> usb0: Mobile Netzwerk-Verbindung
- Zertifikate und private Schlüssel müssen im Format PEM sein. Zertifikate müssen Start- und Stop-Tags besitzen.
- Lucom unterstützt für die local und remote ID:
  - IP-Adresse (z. B.: 192.168.1.1)
  - &#15; DN (z. B.: C=CZ,O=CompanyName,OU=TP,CN=A)
  - &#15; FQDN (z. B.: @director.companyname.cz) - Das Symbol @ symbol geht der FQDN voran.
  - User FQDN (z. B.: director@companyname.cz)

### E2M / IEC104 Energy-Steuerung Pholtaikanlagen

- Open VPN
- Port 2404 muß vom VPN-Router zum IEC-Server erreichbar sein
- VPN-Server: m2m.e2m.energy
- Encryption algorithm: AES-256-CBC (256 bit)
- DH Parameter Leght: 2048 bit
- Auth Digest Algorithm: SHA1 (160bit)
- E2M Network: 192.168.210.0 / 24

### Lucom Router Konfiguration:

- Interface-Typ: TUN
- USER-PASS.TXT in Lucom Startup-Script kopieren
- OpenVPN Eintrag erstellen:
- Protocol: UDP
- UDP Port: • 1194 für VPN010009xxxxxx, • 1195 für VPN010008xxxxxx

Seite 1 / 4

(c) 2024 Uwe Kernchen <news@uwe-kernchen.de> | 2024-04-27 02:19

URL: <https://uwe-kernchen.de/phpmyfaq/index.php?action=faq&cat=3&id=395&artlang=de>  
(C) <https://uwe-kernchen.de>

# Hardware

- Remote IP: m2m.e2m.energy (80.64.177.239)
- Remote Subnet: 192.168.210.0
- Remote Subnet Mask: 255.255.255.0
- Redirect GW: no
- Ping Interval: 120 sek
- Ping Timeout: 30 sek
- Compression: LZO
- NAT Rules: applied
- Auth Mode: X.509 cert (multicert)
- Preshares Secret: TLSAuth.KEY hinein kopieren (2048 bit OpenVPN static key)
- CA Certificate: ca.cert
- Local Certificate: VPNxxxx.crt
- Local Private Key: VPNxxx.key
- Extra Options: " o --cipher AES-256-CBC --auth SHA1 --lport 0 --verify-x509-name hlurvkb02.energy2market.de name --auth-user-pass /tmp/user-pass.txt "
- speichern, Privat Key-PW eingeben

Der Router baut nun automatisch den VPN Kanal auf. Wenn der Kanal aufgebaut ist wird unter „Status – Network“ ein „tunX“ Netzwerk (x= Nummer der VPN Konfiguration) angezeigt. Sollte dieses nicht erfolgen sollte über „Status – System LOG“ geprüft werden, welcher Fehler vorliegt.

- Test mit PING auf Tunnel Client IP

Vor der nachfolgenden Erstellung der VPN-Verbindung [müssen die » Zertifikate erstellt werden «.](#)

## VPN (Lan <-> LAN) IPSec IKEv2 zertifikatsbasiert

### Router Lancom

Grundkonfiguration [siehe hier](#).

(Zertifikat mit X509v3 Subject Alternative Name: IP-Adresse)

- Verschlüsselung: DH14, DH2, kein PFS, AES-CBC-256, AES-CGM-256, SHA-256, SHA1, MD5
- Authentifizierung: lokal/entfernte Identität: RSA-Signatur, ASN.1-Distinguished-Name, VPN1, CRL-Check: Ja
- Verbindungsparameter: Default (30 sek, keine)
- Gültigkeitsdauer: 85.860 sek, 0 kB, 14.400 sek, 2.000.000 kB)
- Regelerzeugung: Manuell
- IKE-CFG: Server
- IPv4-Adress-Pool eintragen
- IPv4-Routing-Tabelle: Eintrag erstellen

Seite 2 / 4

# Hardware

- Firewall IPv4-Regel: VPN übertragen (je nach Firmware)

## Router Lucom

LTE router LR77 v2 Libratum

- Type: policy-based
- Remote IP Address: Router-IP
- Remote ID: Identität aus Server-Zertifikat -> Inhaber -> RFC-2253 (Reihenfolge gedreht!!)
- Local ID: Identität aus Client-Zertifikat -> Inhaber -> RFC-2253 (Reihenfolge gedreht!!)
- Remote Subnet + Mask: Remote Subnet + Mask
- Local Subnet + Mask: Local Subnet + Mask
- Encapsulation Mode: tunnel
- Force NAT Traversal: yes
- IKE: IKE v2
- IKE Algorithm: manual
- IKE Encryption: AES256CGM128
- IKE Hash: SHA256
- IKE DH Group: 2
- IKE Reauthentication: yes
- ESP Algorithm: manual
- ESP Encryption: AES256GCM128
- PFS: disabled
- Key Lifetime: 3600 sek
- IKE Lifetime: 86400
- Rekey Margin: 540 sec
- Rekey Fuzz: 100%
- Authenticate Mode: X.509 certificate
- CA.crt / Remote Cert Pubkey.crt / Local Cert PubKey.crt / Local Zert PrivKey.pem, am Besten in Klartext rein kopieren
- Revocation Check: if possible

## LR77 v.2 Libratum

LTE/4G/3G/Edge Modem

2x LAN (10/100), 2x SIM-Card

\* max. 4x OpenVPN

\* max. 4x IPsec IP v4 / v6 / DualStack

Default IP: 192.168.1.1

User: root

PW: P + letzten 8 Stellen der SnNr. + h

\* Mobile WAN: APN: internet, Dial: \*99#, PAP

\* Service -> HTTP: Zertifikat muß ggf. erneuert werden

\* LED Power: green blinking = ready, on = starting Router, fast blinking = Updating

\* LED DAT: rot blinking = Communication

\* LED WAN: gelb 1x flash per Sec = Signal good, 2x flash per Sec = Signal

Seite 3 / 4

(c) 2024 Uwe Kernchen <news@uwe-kernchen.de> | 2024-04-27 02:19

URL: <https://uwe-kernchen.de/phpmyfaq/index.php?action=faq&cat=3&id=395&artlang=de>  
(C) <https://uwe-kernchen.de>

# Hardware

angemessen, 3x flash per Sec = Signal schlecht

\* LED SIM: gelb on: SIM Card aktiv

Handbücher:

<https://www.lucom.de/files/inhalte/downloads/router/lr77v2-libratum/lr77v2-libratum-user-guide.pdf>

<https://www.lucom.de/industrierouter/lr77-v2libratum-sl-lte-vpn-4g-mobilfunkrouter-ohne-zubeh-r-25704z-bb-lr2l710020.html#downloads>

Hersteller: <https://advantech-bb.com/>

## Quellen und Links:

- IPSec PSK Lan-Lan: <https://help.lucom.de/doku.php?id=lucom:router:vpn-lcm-fortinet-ipsec>
- IPSec PSK zu Lancom: [https://help.lucom.de/doku.php?id=lucom:router:lancom\\_router\\_als\\_ipsec\\_server](https://help.lucom.de/doku.php?id=lucom:router:lancom_router_als_ipsec_server)
- Konfigurationshandbuch: <https://www.lucom.de/industrierouter/xr5i-v2e-lan-to-lan-vpn-router-25602-bb-xr2l000011.html?file=files/inhalte/downloads/router/config-v2-router-de.pdf>

Eindeutige ID: #1394

Verfasser: Uwe Kernchen

Letzte Änderung: 2023-01-21 19:25