

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."
- VPN verbunden: im System-Log steht "establishing CHILD_SA ipsec2-1"
- VPN IPsec verbunden: in IPsec-Status steht "ipsec1-1: #1, ESTABLISHED"
- 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)
 - DN (z. B.: C=CZ,O=CompanyName,OU=TP,CN=A)
 - 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
- 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)

Hardware

- CA Certificate: ca.cert
- Local Certifikate: VPNxxxx.crt
- Local Private Key: VPNxxx.key
- Extra Options: " o --cipher AES-256-CBC --auth SHA1 --lport 0 --verify-x509-name hluvkw02.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

Router Lucom

LTE router LR77 v2 Libratum

- Type: policy-based
- Remote IP Adress: Router-IP
- Remote ID: Identität aus Server-Zertifikat -> Inhaber -> RFC-2253
- Local ID: Identität aus Client-Zertifikat -> Inhaber -> RFC-2253
- Remote Subnet + Mask: Remote Subnet + Mask
- Local Subnet + Mask: Local Subnet + Mask
- Encapsulation Mode: tunnel
- Force NAT Traversal: yes

Seite 2 / 3

(c) 2022 Uwe Kernchen <news@uwe-kernchen.de> | 2022-08-11 09:53

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

Hardware

- 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 / Remote Cert Pubkey / Local Cert PubKey / Local Zert PrivKey - am Besten in Klartext rein kopieren
- Revocation Check: if possible

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
- Konfigurationshandbuch: <https://www.lucom.de/industrieroeuter/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: 2022-07-24 10:53