

# TW-EAV510AC-LTE OpenVPN -ohjeistus


## OpenVPN Remote Access Android -puhelimien ja TW-EAV510 välillä.

OpenVPN Remote Access-yhteydellä voidaan luoda VPN-yhteys, jossa liikenne on sallittu toiseen suuntaan eli etälaitte pääsee OpenVPN-palvelimen verkkoon mutta OpenVPN-palvelimen laitteet eivät pääse etälaitteen verkkoon.

**HUOM!** Jos yhteyttä käytetään 3G/4G/LTE-verkon yli, pitää käytössä olla operaattorilta julkiset IP-osoitteet eli **ei tupla-NAT:ia** (esimerkiksi **Soneran opengate**-palvelu). Riippumatta ulkoisen yhteydenkäytännöstä on suotavaa käyttää omaa kiinteää IP-osoitetta **tai mieluiten dynaamista nimipalvelua** esim. ilmaista FreeDNS:ää, jotta etälaitteella löydetään aina VPN-palvelin myös julkisen IP:n muuttuessa.

## Palvelinpuolen (TW-EAV510AC-LTE) asetukset(Ohjelmisto 2.50a.d55)

### 1. VPN → VPN-asetukset:



**TW-EAV510 AC / LTE-reititin ADSL/VDSL-modeemi WLAN-tukiasema Palomuuuri**

Tietoa laitteesta

Pika-asetukset

Asetukset

VPN

IPSec

VPN-asetukset

Erikoissääntöjen ryhmä

PPTP

L2TP

OpenVPN

GRE

Lisäasetukset

Kieli/Language

VPN

VPN-asetukset

VPN-tili jaettu PPTP/L2TP/OpenVPN-palvelimelle.

Asetukset

Nimi

HomeVPN

Tunneli

☒ Päälle ☐ Pois päältä

Käyttäjä

test

Salasana

.....

Yhteystapa

☒ Etäyhteys ☐ LAN --> LAN

Kohde verkon IP-osoite

Asiakkaan aliverkonpeite

Lisää

Muuta / Poista

Muuta	Nimi	Tunneli	Yhteystapa	Kohde verkon IP-osoite	Asiakkaan aliverkonpeite	Poista
<input checked="" type="radio"/>	HomeVPN	Päälle	Etäyhteys			<input type="checkbox"/>

#### ○ Esimerkissä:

- VPN-palvelimen nimi: HomeVPN
- Käyttäjä: test
- Salasanaksi joku yleinen hyvien salasanavaatimusten täyttävä salasana.
- Yhteystapa: Etäyhteys
- Tunneli: Päälle

## 2. VPN → OpenVPN → OpenVPN-palvelin:

**VPN**

**OpenVPN-palvelin**

Asetukset

OpenVPN-palvelin	<input checked="" type="radio"/> Päälle <input type="radio"/> Pois päältä
Ulkoverkon ohjelmistorajapinta	3G/4G/LTE
Protokolla	TCP
Portin numero	1194
Tunnelin ohjelmallinen aliverkonpeite	192.168.1.0
Tunnelin aliverkonpeite	255.255.255.0
Cipher salaus	AES-192-CBC
HMAC-käyttö	SHA1
LZO-pakkaus	<input checked="" type="checkbox"/> Päälle

Tallenna Keskeytytys

### ○ Esimerkissä:

- OpenVPN palvelin: Päälle
- Käytetään ulkoverkon yhteyslinkkinä mobiiliverkkoa: 3G/4G/LTE. **Jos käytössä useampia WAN-linkkejä, tässä voidaan määritellä mitä käytetään OpenVPN-yhteyksille.**
- Protokollaksi: TCP
- Portin numero oletus: 1194
- Tunnelin ohjelmallinen aliverkonpeite pitää olla eri kuin reitittimen normaali aliverkko. Esimerkin tapauksessa reitittimen kotiverkko on 192.168.0.xxx ja valitaan VPN:lle seuraava aliverkko eli 192.168.1.0.
- Tunnelin aliverkonpeite annetaan olla oletuksena 255.255.255.0. Tällä voitaisiin rajoittaa samanaikaisesti yhteyttä ottavien VPN-asiakkaitten lukumäärää rajoittamalla tarjottavien IP-osoitteiden määrää.
- **Huom! Cipher-salaukseen älä käytä oletuksena olevaa BF-CDC:tä.** Vaikka se onkin nopeampi kuin muut vaihtoehdot, sen turvataso ei ole nykypäivän mittapuulla riittävä. **Esimerkissä on valittu sen sijaan 192bit AES: AES-192-CBC**
- **Vaikka tunneli onkin salattu em. Cipher-salauksella, niin periaatteessa dataa voidaan silti muuttaa matkalla, jota varten käytetään HMAC-tarkistusta SHA-hajautusalgoritmeilla.** SHA2 on vahvempi, mutta huomattavasti resurssi-intensiivisempi kuin SHA1. Käytännössä hajautusalgoritmin murtaminen tässä käytössä eli millisekuntiajassa ei ole nykytekniikalla mahdollista minkä takia SHA1 on täysin riittävä HMAC:lle.
- LZO-pakkaus: päälle. Tämä voi nopeuttaa joidenkin VPN-tunnelin läpi käytettyjen palvelujen käyttöä esim. pakkaamattomien tiedostojen tiedostosiirtoja.

### 3. Kopioidaan reitittimestä sertifikaatti talteen etälaitetta varten:


The screenshot shows the TelWell router's web interface. The top header displays the TelWell logo and the device model: "TW-EAV510 AC / LTE-reititin ADSL/VDSL-modeemi WLAN-tukiasema Palomuri". On the left, a sidebar menu lists various configuration options, with "VPN" expanded to show "OpenVPN". The main content area is titled "VPN" and contains a section for "OpenVPN CA".

Under "OpenVPN CA", there is a "Sertifikaatti" (Certificate) section. It features a text area containing a certificate in PEM format, starting with "-----BEGIN CERTIFICATE-----" and ending with "-----END CERTIFICATE-----". Below the text area is a "Vastaanottajan sähköpostiosoite" (Recipient email address) field, which is currently empty. To the right of this field is a button labeled "Tallenna" (Save). A note next to the field says "(Tulee olla muotoa xxx@yyy.zzz)".

Below the "Sertifikaatti" section, there is a section for "OpenVPN Static Key (tls-auth)".

- Valitaan koko tekstikentän tiedosto (Ctrl+A) ja tallennetaan sertifikaatti tekstitiedostoon. Huomaa, että myös Begin ja End certificate-rivit tulee sisällyttää tiedostoon. Tässä tapauksessa tallennettu nimellä HomeVPN.ca ja siirretty puhelimen Downloads-kansioon USB-kaapelilla.

#### 4. Tarkistetaan reitittimen nykyinen ulkoverkon IP-osoite valitsemalla Tietoa laitteesta:



**TW-EAV510 AC / LTE-reititin ADSL/VDSL-modeemi WLAN-tukiasema**  
**Palomuuuri**

Tietoa laitteesta

Yhteenveto

Ulkoverkko(WAN)

Tilastot

Kaistan käyttö

3G/4G/LTE-tila

Reititys

ARP

DHCP

VPN

Loki

Kaistanjaon tila

Pika-asetukset

Asetukset

VPN

Lisäasetukset

Kieli/Language

Tietoa laitteesta

Laitteen tiedot

Malli	TW-EAV510 AC / LTE		
Palvelimen nimi	TeleWell		
Järjestelmäaika	1D 0H 44M 57S		
Pvm/alka	Thu Nov 2 16:53:06 2017	Tahdista	
Ohjelmistoversio	2.50a.d55		
Lähiverkon IPv4 IP-osoite	192.168.0.1		
MAC-osoite	00:1e:ab:0b:26:6b		
DSL PHY ja Driver -Versiot	A2pv6F039v.d26p		
Langattoman verkon ohjelmisto	7.10.274.18		

Internet(WAN)

Linjanopeus - Lähetys (Kbps)	0
Linjanopeus - Vastaanotto (Kbps)	0
Oletusyhdykskäytävä / IPv4 IP-osoite	3G/4G/LTE / 193.210.227.146
Yhteysaika	11:54:03
Ensisijainen nimipalvelin	192.89.123.230
Toissijainen nimipalvelin	192.89.123.231

- Esimerkissä ulkoverkon IP: 193.210.227.146. Huomaa että jos käytössä dynaaminen nimipalvelin: Lisäasetukset → Nimipalvelut (DNS) → Dynaaminen nimipalvelin (DynDNS), niin voidaan käyttää siellä määriteltyä DNS-nimeä suoran ulkoverkon IP:n sijaan. Tällöin ei ulkoista IP:tä tarvitse etälaitteessa tietää joka yhteyskerralla vaan sama domain-nimi osoittaa aina kulloinkin käytössä olevaan julkiseen IP-osoitteeseen.

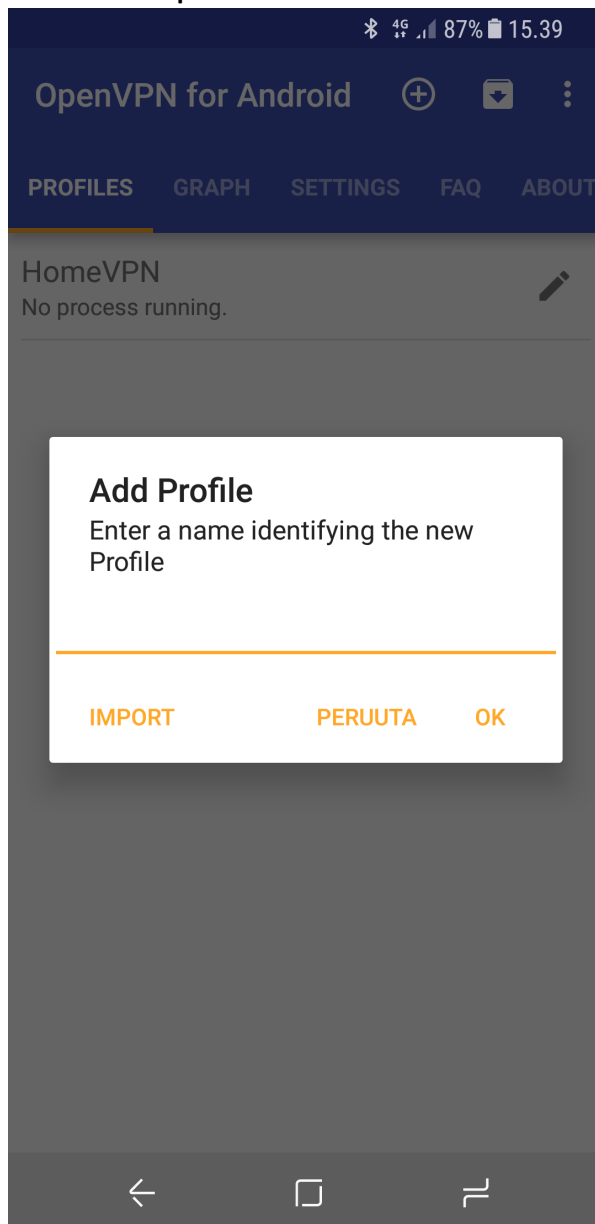
**Tältä osin reititin/palvelinpuolen asetukset on valmiiksi konfiguroitu. Etälaitteita varten siis tarvitaan kolme tietoa:**

- Käyttäjätunnus ja salasana
- Sertifikaattitiedosto, joka kopioidaan etälaitteeseen
- Telewell-reitittimen julkinen IP tai dynaamisen palvelimen välittämä julkinen IP-osoite

## Etälaitteen asetuksien määrittäminen

Android-laitteille on olemassa useampia ilmaisia OpenVPN:ää tukevia appeja. Moni niistä vaatii kuitenkin valmiiksi määritellyn ovpn-määrittelytiedoston, jota ei nyt tässä esimerkissä tehdä. **Tämän tiedoston voi kuitenkin määritellä graafisesti ”OpenVPN for Android” nimisessä appissa. Seuraavaksi käydään tarvittavat askeleet etälaitteessa käyttäen kyseistä appia.**

### 1. Luodaan uusi profiili:



Annetaan haluttu nimi. Esimerkissä HomeVPN.

## 2. Muokataan profiilin basic-välilehden asetuksia:

Editing "HomeVPN"

BASIC SERVER LIST IP AND DNS ROUTING

Profile Name

HomeVPN

☒ LZO Compression

Type

Username/Password

CA Certificate

[Imported from: HomeVPN.ca]  
87 months leftE=www.te  
lewell.fi,CN=TeleWell Oy  
CA,OU=TeleWell Oy,O=TeleWell  
Oy,L=Helsinki,ST=Finland,C=FI

Select...

Username

test

Password

.....

Behaviour on AUTH\_FAILED

Disconnect, forget password

Certificate Revoke List (optional)

No Data

Select...

- Valitaan LZO-pakkaus.
- Autentikointityypiksi Username/Password ja syötetään Username- ja Password-kenttiin reitittimen päässä annettu käyttäjätunnus ja salasana.
- CA Certificate-kohdassa valitaan Select ja haetaan puhelimen Download-kansioon reitittimestä kopioitu HomeVPN.ca-sertifikaattitiedosto.

3. Server List-välilehdelle täytetään reitittimen asennuksen neljännessä kohdassa talteen otettu julkinen IP-osoite tai vaihtoehtoisesti dynaamisen nimipalvelimen osoite:

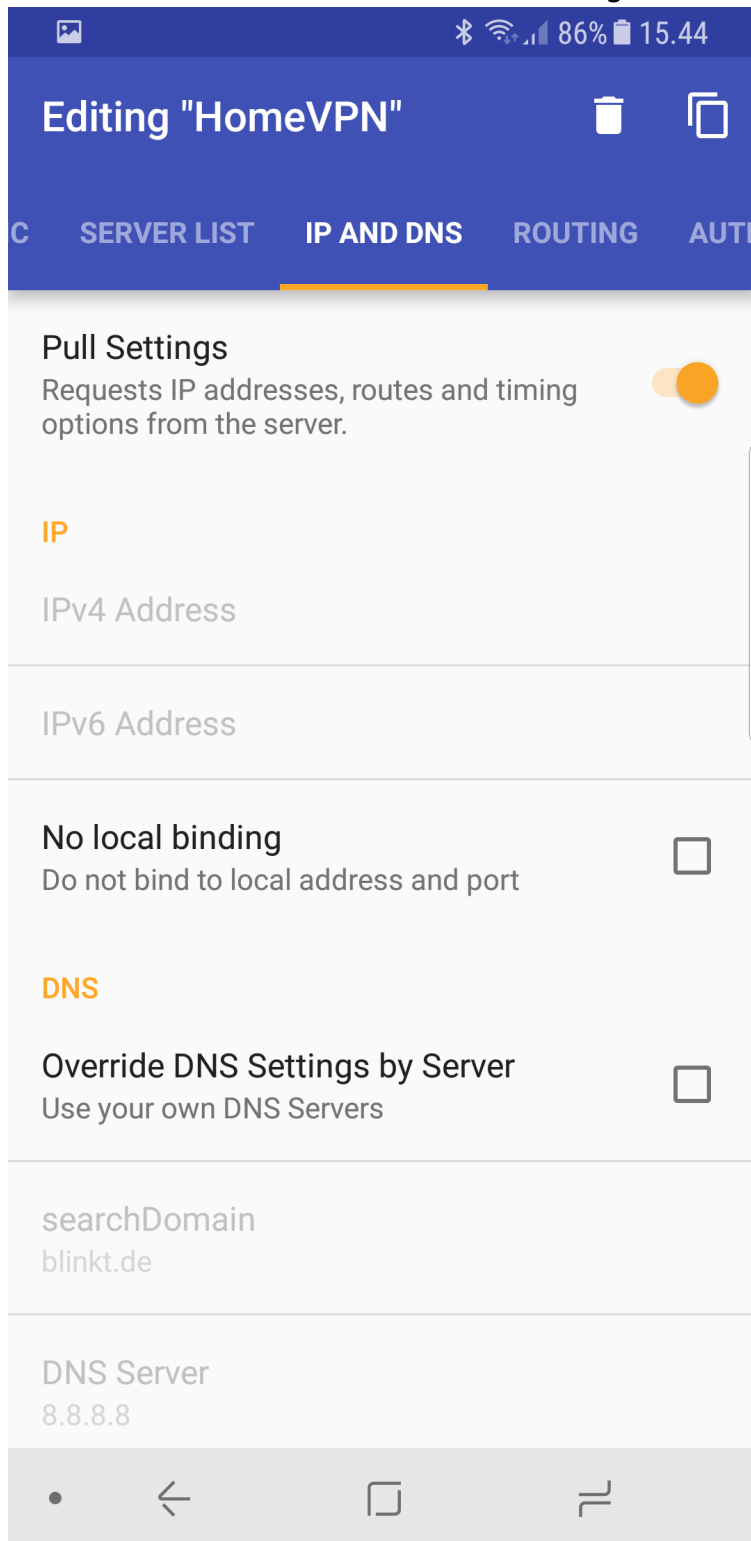
The screenshot shows the 'Editing "HomeVPN"' interface with the 'SERVER LIST' tab selected. The interface includes a toggle for 'Use connection entries in random order on connect'. Two server entries are listed:

Server Address	Server Port	Protocol	Enabled
193.210.227.146	1194	TCP	Yes
openvpn.example.com	1194	UDP	No

A plus button (+) is located at the bottom right of the server list, indicating an option to add more servers.

- Portti: 1194
- Protokolla: TCP
- Enabled-täppä päälle ja jos alla on lista muita palvelimia, niin kaikkiin "Enabled" pois päältä.

4. IP and DNS-kohtaan varmistetaan että Pull Settings on valittuna:



Editing "HomeVPN"

C SERVER LIST **IP AND DNS** ROUTING AUTH

**Pull Settings**  
Requests IP addresses, routes and timing options from the server. ☒

**IP**

IPv4 Address

IPv6 Address

**No local binding** ☐  
Do not bind to local address and port

**DNS**

**Override DNS Settings by Server** ☐  
Use your own DNS Servers

searchDomain  
blinkt.de

DNS Server  
8.8.8.8

• < □ ≡



5. Annetaan olla oletukset muissa välilehdissä, mutta Authentication/Encryption-välilehdellä käydään kirjoittamassa Encryption cipher-kohtaan: AES-192-CBC. Samalla otetaan täppä pois kohdasta Certificate Hostname Check.

Editing "HomeVPN"

ROUTING AUTHENTICATION/ENCRYPTION ADVANC

**TLS Settings**

**Expect TLS server certificate**  
Checks whether the server uses a certificate with TLS Server extensions (--remote-cert-tls server) ☐

**Certificate Hostname Check**  
Checks the Remote Server Certificate Subject DN ☐

Remote certificate subject  
CN (default)

X509 Username Field  
CN (default)

**TLS Authentication/Encryption**

**Use TLS Authentication**  
Enables the TLS Key Authentication ☐

TLS Auth File  
You must select a certificate

TLS Direction

**Encryption**

**Encryption cipher**  
AES-192-CBC

Packet authentication

- 6. Generated config-välilehdeltä voi tarkastella generoitua ovpn-konfiguraatitiedostoa. Tämän tiedoston voi halutessaan tallentaa/lähetellä toisaalle ja käyttää muiden ovpn:ää tukevien client-ohjelmien kanssa.**

Tullaan asetuksista pois, näpätetään HomeVPN-profiilia ja yhteyden tulisi muodostua. Niin kauan kuin VPN-putki on päällä, pystyy mobiililaitteella ottamaan yhteyttä Telewell-reitittimen takana oleviin laitteisiin kuten valvontakameroihin, kotiautomaatiolaitteisiin yms jos niihin pääsyä eri erikseen ole estetty. Näillä asetuksilla mobiililaitteella ulkomaailmaan otetut yhteydet esim. Google, Iltasanomat jne, ohjautuvat kuitenkin normaalisti suoraan puhelimesta kyseisiin osoitteisiin käyttämättä VPN-putkea.