

# VPN-yhteys

Tämän lisäselvityksen aiheena on VPN-palvelimen pystyttäminen Ubuntun virtuaaliselle koneelle, yhteyden luominen palvelimeen Windows koneelta, sekä yhteyden reititys VPN-palvelimelta internettiin. Yhteys toteutetaan OpenVPN-ohjelmiston avulla. OpenVPN käyttää SSL:ää suojatun yhteyden luomiseen. Toisin, kuin useimmat SSL VPN -järjestelmät siihen ei oteta yhteyttä selaimella, vaan asiakaskoneeseen on asennettava OpenVPN-ohjelmisto. Tässä tapauksessa Linuxiin asennettava palvelinohjelmisto ja Windowsiin asennettava asiakasohjelmisto.

## Mikä on VPN?

VPN (Virtual Private Network) tarkoittaa virtuaalista erillisverkkoa, jonka avulla kaksi tai useampia koneita voidaan liittää toisiinsa julkisen verkon yli ilman että liikennettä on mahdollista seurata. VPN:llä on useita eri käyttötarkoituksia. VPN luotiin alun perin mahdollistamaan etätyöntekijöiden turvallinen pääsy työpaikkojensa verkkoihin. Nykyään termillä VPN tarkoitetaan useimmiten kaupallisia VPN-palveluja, joiden palvelimien kautta asiakkaat voivat yhdistää laitteensa internetiin yksityisesti.

## Kuinka VPN toimii?

VPN yhteydessä asiakkaan ja palvelimen välillä kulkeva data liikkuu salatun yhteyden kautta (VPN-tunneli). Tiedon salaukseen VPN käyttää jotakin tunnelointiprotokollaa. Julkisesti standardoidut vaihtoehdot ovat:

- IPsec-protokolla, ESP-tunnelointimoodissa. Sitä voi sinällään käyttää niin lähiverkkojen yhdistämiseen kuin etäkäyttöönkin.
- L2TP-tunnelointiprotokolla, jota voi käyttää ainoastaan etäkäyttöön. Siinä ei tosin ole omaa salaustaan, vaan sen kanssa käytetään IPsec-protokollaa salaukseen.
- L2F-tunnelointiprotokollaa voi käyttää vain lähiverkkojen yhdistämiseen. Se on Ciscon protokolla, jonka päälle L2TP:kin paljolti perustuu. Se käyttää PPP:n Point-to-point Encryption Protocol (ECP) -protokollaa salaukseen.
- PPTP on Microsoftin oma etäkäyttöprotokolla, joka käyttää Microsoft Point-to-Point Encryption (MPPE) -protokollaa salaukseen.

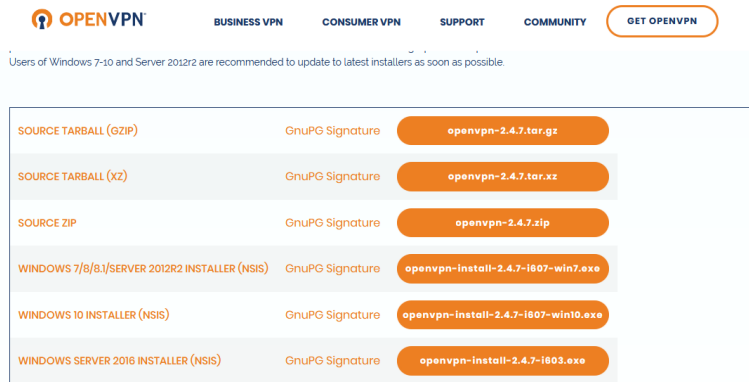
Näiden lisäksi on myös SSL VPN, joka eroaa aiemmista siinä, että se on toteutettu OSI mallin kerroksilla 4-7, toisin kuin esimerkiksi IPsec, joka toimii verkkokerroksella. SSL VPN:ssä asiakas ottaa yhteyden palvelimeen ennalta määrättyyn porttiin ja muodostaa SSL-tunnelin laitteiden välille, varaa itselleen suljetusta verkosta IP-osoitteen ja muodostaa virtuaaliverkon näiden välille.

## OpenVPN käyttöönotto

OpenVPN:n käyttöönotto sisältää useita vaiheita, jotka on lueteltu alla. Raportissa ei ole kerrottu yksityiskohtaisia tietoja OpenVPN:n asennuksesta vain kerrottu pääpiirteittäin asennuksen vaiheet.

### OpenVPN asennus

OpenVPN on avoimen lähdekoodin ohjelma ja se on saatavana ilmaiseksi OpenVPN:n nettisivuilla.



Kun asennustiedoston on ladannut koneelle voi asennuksen aloittaa avaamalla tiedoston. GUI (Graphic User Interface) asentuu helposti seuraamalla näytön ohjeita.

Palvelinohjelmiston ja easy-RSA paketin asennus, jota tarvitaan varmenteiden luomiseen, onnistuu Ubuntuille komennolla:

```
sudo apt-get install openvpn easy-rsa
```

Kun ohjelma on asennettu, luodaan palvelimelle ja käyttäjälle sertifikaatit ja avaimet. Tätä kutsutaan PKI:ksi (Public Key Infrastructure). PKI koostuu julkisesta ja yksityisestä avaimesta palvelimelle ja jokaiselle käyttäjälle. Siihen kuuluu myös pääavain, jolla palvelimen ja käyttäjien sertifikaatit allekirjoitetaan. Näiden tekemiseen OpenVPN:ssä käytetään easy-RSA-ohjelmaa.

### Palvelimen parametrit

Seuraavaksi muokataan palvelimen parametrit esimerkiksi palvelimen nimi, sekä kansio johon avaimet luodaan.

### Diffie Hellman avaimenvaihtoprotokolla

Diffie Hellman on salausprotokolla, jota käytetään avaintenvaihtoon. DH avulla luodaan kaksi salaista avainta, joiden avulla kummankin avaimen haltija pystyy avaamaan salauksen.

### Pääavaimen luonti

Pääavain (Certificate Authority CA) sisältää sertifikaatin ja avaimen, joita käytetään allekirjoittamaan palvelimen ja asiakkaan sertifikaatit.

### Palvelimen ja asiakkaan avainten luonti

Tässä kohdassa luodaan salausavaimet ja sertifikaatit palvelimelle sekä asiakkaalle. Molempien sertifikaatit allekirjoitetaan edellisessä kohdassa luoduilla pääavaimella.

## Avainten siirto asiakkaan koneelle

Kun avaimet on luotu, asiakkaan avaimet täytyy siirtää asiakkaan koneelle. Tässä tapauksessa avainten siirtoon käytettiin SCP-ohjelmalla, jotta salausavaimet eivät joutuisi siirtovaiheessa väriin käsiin.

## Palvelimen konfigurointi

Palvelimen konfigurointitiedostosta asetetaan palvelin käyttämään UDP-protokollaa ja porttia 1194, joka on varattu OpenVPN sovellukselle. VPN verkolle asetetaan IP-osoite. Tässä tapauksessa käytettiin osoitetta 10.8.0.0/24.

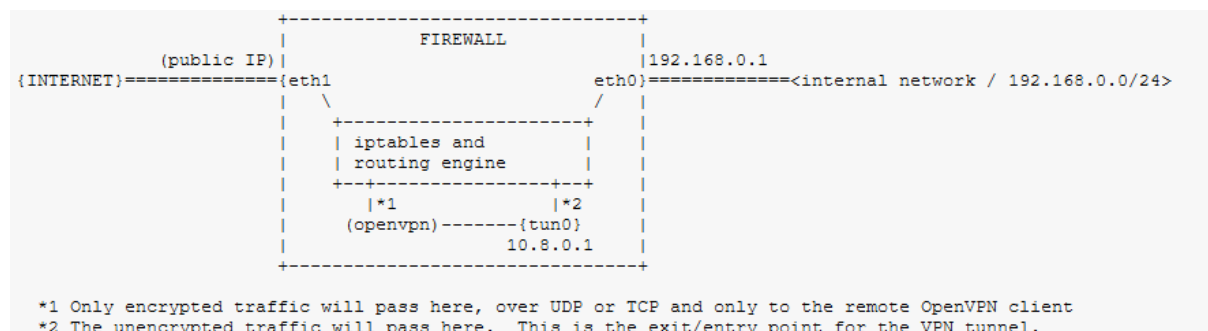
## Asiakkaan konfigurointi

Windowsissa asiakkaan konfigurointitiedosto tallennetaan uudestaan tiedostopäätteellä .ovpn, Linuxin .conf tiedostopäätteen asemesta. Tiedosto asetetaan vastaamaan palvelimen konfigurointia. Lisäksi asetetaan IP-osoite ja portti, jossa palvelin sijaitsee. Tiedoston loppuun lisätään html muodossa CA-sertifikaatti, asiakkaan sertifikaatti ja avain.

## Reititys ja palomuuuri asetukset

Jotta yhteys toimisi on reititystauluun ja palomuuriin tehtävä joitain muutoksia. Ensin sallitaan palomuurisäännöistä ssh-yhteydet, sekä UDP-yhteys porttiin 1194.

OpenVPN käyttää datan tunnelointiin virtuaalista TUN adapteria. Siksi palomuuuri täytyy asettaa sallimaan tuleva liikenne TUN adapterilta. TUN adapteri toimii OSI mallin verkkokerroksella.



Tässä näkyy kuinka TUN-adapteri tun0 on konfiguroitu VPN palvelimen IP-osoitteeksi 10.8.0.1 ja VPN verkon osoite on 10.8.0.0/24. OpenVPN siis hyväksyy asiakkaan eth1:stä tulevan datan, jonka jälkeen OpenVPN purkaa salauksen ja lähettää sen tun0:n, josta se reititetään eth0 aliverkkoon. Kun reititin lähettää dataa tun0 verkkoon OpenVPN poimii sen ja salaa tiedot ja lähettää ne eth1:n kautta oikealle asiakkaalle.

## Yhteyden muodostus

Kun palvelimen ja asiakkaan konfiguroinnit on tehty ja asiakkaan konfigurointitiedosto on tallennettu ohjelman config kansioon, yhteyden voi muodostaa helposti GUI:n kautta klikkaamalla connect.

```
GNU nano 2.9.3 openvpn-status.log

OpenVPN CLIENT LIST
Updated,Sun Nov 17 11:02:10 2019
Common Name,Real Address,Bytes Received,Bytes Sent,Connected Since
arttu,192.168.10.48:58805,698416,6166206,Sun Nov 17 10:38:03 2019
ROUTING TABLE
Virtual Address,Common Name,Real Address,Last Ref
10.8.0.4,arttu,192.168.10.48:58805,Sun Nov 17 11:01:49 2019
GLOBAL STATS
Max bcst/mcast queue length,1
END
```

Kuva: OpenVPN:n status log

```
OpenVPN Connection (client)
Current State: Connected
Sun Nov 17 10:38:06 2019 TAP-Windows Driver Version 9.24
Sun Nov 17 10:38:06 2019 Set TAP-Windows TUN subnet mode network/local/netmask = 10.8.0.0/10.8.0.4/255.255.255.0 [SUCCEEDED]
Sun Nov 17 10:38:06 2019 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.8.0.4/255.255.255.0 on interface {F2BC07A8-01E2-4ADC-8C54-3ED4D574E806} [DHCP-serv: 10.8.0.254, lease-time: 31536000]
Sun Nov 17 10:38:06 2019 Successful ARP Flush on interface [20] {F2BC07A8-01E2-4ADC-8C54-3ED4D574E806}
Sun Nov 17 10:38:06 2019 MANAGEMENT: >STATE:1573979886,ASSIGN_IP,,10.8.0.4,...
Sun Nov 17 10:38:06 2019 Blocking outside dns using service succeeded.
Sun Nov 17 10:38:11 2019 TEST ROUTES: 1/1 succeeded len=0 ret=1 a=0 u/d=up
Sun Nov 17 10:38:11 2019 C:\Windows\system32\route.exe ADD 192.168.10.120 MASK 255.255.255.255 192.168.10.1 IF 19
Sun Nov 17 10:38:11 2019 Route addition via service succeeded
Sun Nov 17 10:38:11 2019 C:\Windows\system32\route.exe ADD 0.0.0.0 MASK 128.0.0.0 10.8.0.1
Sun Nov 17 10:38:11 2019 Route addition via service succeeded
Sun Nov 17 10:38:11 2019 C:\Windows\system32\route.exe ADD 128.0.0.0 MASK 128.0.0.0 10.8.0.1
Sun Nov 17 10:38:11 2019 Route addition via service succeeded
Sun Nov 17 10:38:11 2019 Initialization Sequence Completed
Sun Nov 17 10:38:11 2019 MANAGEMENT: >STATE:1573979891,CONNECTED,SUCCESS,10.8.0.4,192.168.10.120,1194,...
```

Kuva: GUI:n connection status

## Reititys internettiin

Nyt asiakkaan ja palvelimen välille on saatu yhteys. Jotta VPN:ää voisi käyttää nettisivujen selailuun täytyy palvelimelle tehdä vielä muutamia reitityksiä. Jotta asiakaslaitteiden paketit menevät myös Internetiin eivätkä pysähdy palvelimelle täytyy IP-pakettien reititys sallia. Tämä tapahtuu Ubuntun käyttöjärjestelmän kansiossa `/etc/sysctl` komennolla `net.ipv4.ip_forward=1`.

Myös palomuurin reititys täytyy sallia ja se tapahtuu palomuurin asetuksissa muuttamalla

```
DEFAULT_FORWARD_POLICY="DROP" muotoon
```

```
DEFAULT_FORWARD_POLICY="ACCEPT".
```

Näiden lisäksi täytyy NAT sallia lähettämään paketit VPN:ltä verkkokortille komennolla

```
iptables -t nat -I POSTROUTING -o eth1 -s 10.8.0.0/24 -j MASQUERADE.
```

Tämän jälkeen kaikki verkkoliikenne asiakkaan koneelta ohjautuu VPN:n kautta verkkoon.

## DNS leak test







Nyt kun liikenne on saatu ohjattua VPN palvelimen kautta internettiin, käydään vielä tarkistamassa, ettei DNS vuoda VPN:n DNS palvelimen sijaan internetpalveluntarjoajan palvelimelle. Testi tehtiin osoitteessa <https://www.dnsleaktest.com/> ja kävi ilmi, että osa DNS hauista todella meni internetpalveluntarjoajan palvelimelle, joten VPN palvelimen konfigurointitiedostoon lisättiin kohta `block-outside-dns`.

Tämän jälkeen vuotoja ei enää havaittu.

## Test complete

Query round	Progress...	Servers found
1	.....	3
2	.....	4
3	.....	3
4	.....	5
5	.....	4
6	.....	4

Sponsored by  
**IVPN**  
Ultimate IP leak Protection

IP	Hostname	ISP	Country
146.112.135.64	r1.compute.cph1.edc.strln.net.	Cisco OpenDNS, LLC	Copenhagen, Denmark 
146.112.135.65	r2.compute.cph1.edc.strln.net.	Cisco OpenDNS, LLC	Copenhagen, Denmark 
146.112.135.66	r3.compute.cph1.edc.strln.net.	Cisco OpenDNS, LLC	Copenhagen, Denmark 
146.112.135.67	r4.compute.cph1.edc.strln.net.	Cisco OpenDNS, LLC	Copenhagen, Denmark 
146.112.135.68	r5.compute.cph1.edc.strln.net.	Cisco OpenDNS, LLC	Copenhagen, Denmark 
146.112.135.69	r6.compute.cph1.edc.strln.net.	Cisco OpenDNS, LLC	Copenhagen, Denmark 

Kuva: DNS leak test