**VPN konto – loomine, üles seadmine ja testimine**   
  
Kõigil VPN süsteemidel, on üks arvuti, mis on loodud serveriks (piiranguteta asukohas), millele üks või enama klienti ühendab. Serveri loomine on käesolevas juhendist välja jäetud ja sellise süsteemi loomine on üldiselt hõlmatud teie VPN teenusepakkuja poolt. See server on üks kahest otsast teie krüpteeritud tunnelis. Oluline on, et seda ettevõtet, kus see server töötab saab usaldada ja asub piirkonnas, mida te usaldate. Nii, et jooksutada on vaja sellises usaldusväärses serveris VPN kontot.

Palun pidage meeles, et kontot võib sageli kasutada ainult ühel seadmel korraga. Kui soovite kasutada VPNi nii mobiiltelefonil ja sülearvutil üheaegselt, siis on väga hästi võimalik peate looma kaks kontot.  
  
**Kaubanduslik VPN teenusepakkuja konto**

Olemas on palju VPN-i pakkujad. Mõned annavad teile tasuta prooviperiood aja , teised alustavad koheselt raha küsimist, seda ligikaudu € 5 kuus. Otsi VPN pakkujat, kes pakub OpenVPN kontosid - see on avatud lähtekoodiga, usaldusväärne lahendus, mis on olemas Linux-il, OS X-i- ja Windows-il, samuti Android-il ja iOS-il.  
Valides VPN teenusepakkuja peate arvestama järgmiste punktidega:  
  
    Teavet mida on vaja sinult, et registreerida konto – mida vähem on tarvis seda parem. Tõeliselt privaatsusest muretsev VPN teenusepakkuja küsiks sinult ainult e-posti aadressi (loo endale üks ajutine!), Kasutajanime ja parooli. Rohkem ei nõuta, kui pakkuja loob kasutaja andmebaasi, millest te ilmselt ei taha osa olla.  
    Makseviisi, mida kasutatakse, et maksta oma tellimuse eest. Sularaha ülekanne on ilmselt kõige privaatsem meetod, kuna see ei lingiteie pangakontot ja te VPN-võrgu ID-d. Paypal võib olla ka vastuvõetav variant, eeldades, et sa saad registreerida ja kasutada ajutiselt moodustatud kontot, igaks makseks. Maksmine pangaülekande kaudu või krediitkaardi võib tõsiselt kahjustada teie anonüümsust nii VPN-is kui ka VPN-ist kaugemale.  
    Vältida VPN pakkujad, mis küsivad teil paigaldada oma sobivaid klienditarkvarasid. On olemas suurepäraseid avatud lähtekoodiga lahendusi igale platvormile ja kuna peate jooksutama "erilise" kliendi tarkvara, on see selge märk võltsteenusest.  
    Vältige PPTP- põhinevat VPN-i, kuna mitmeid turvahaavatavusi eksisteerib selles protokollis.  
    Vaata VPN teenusepakkujat, kes kasutab OpenVPN-i - avatud lähtekoodiga, multi-platvormne VPN lahendus.  
    Exit väravaid riikides, mis on teie huvides. Võime valida mitmete riikide seas võimaldab teil muuta oma geopoliitilist konteksti ja tundub tulevat erinevate osast maailmas. Sa pead olema teadlik õigusaktide üksikasjadest ja eraelu puutumatust käsitlevatest seadustest selles riigis.  
    Anonüümsus poliisi, mis puudutab teie liiklust - ohutu VPN teenusepakkujal on mitte-avalikustamise poliis. Isiklik info, nagu kasutajanimi ja kellaajad teie ühendustega seoses, ei tohiks logisse üldse sattuda.  
    Lubatud protokollid, mis on lubatud kasutada VPN piires ja protokolle, mis suunatakse internetti. Sa ilmselt tahad, et kõik enamus protokolle oleks kättesaadavad.  
    Hind vs teenuse kvaliteet ja selle usaldusväärsus.  
    Kõik teadaolevad küsimused, mis tulevad anonüümsusega seoses arvesse võtta, mis võisid VPN teenusepakkujal kasutajatega minevikus olla. Vaata internetis ringi, lugege foorumeid ja ringi küsida. Ärge sattuke kiusatusse tundmatu, uue, odava või kahtlaste pakkumiste ees.  
  
On mitmeid VPN läbivaatamisele orienteeritud kohti internetis, mis aitavad teil teha õige valiku:  
  
http://www.bestvpnservice.com/vpn-providers.php  
http://vpncreative.com/complete-list-of-vpn-providers  
http://en.cship.org/wiki/VPN  
  
   
**Seadistame VPN klient-i**  
    "OpenVPN [..] on kõigi võimalustega SSL VPN tarkvara lahendus, mis ühendab OpenVPN serveri võimeid, ettevõtte juhtimise oskused, lihtsustatud OpenVPN Connect UI ja OpenVPN Client tarkvara pakette, mis mahutavad GNU / Linux-i, OSX-i, Window-si keskkondi. OpenVPN Access Server toetab laialt erinevaid konfiguratsioone, sealhulgas turvalise ja granuleeritud kaugjuurdepääsu sisevõrgule ja / või erapilve võrgu ressursse ja rakendusi peeneteralise juurdepääsu kontrolliga. " (Http://openvpn.net/index.php/access-server/overview.html)  
  
On mitmeid erinevaid standardeid, et luua VPN, sealhulgas PPTP, LL2P/IPSec ja OpenVPN. Nad on erineva keerukusega, turvalisuse taseme poolest, ja millisele operatsioonisüsteemile nad on kättesaadavad. **Ärge kasutage PPTP kuna tal on mitmeid turvahaavatavusi**. Selles tekstis keskendume OpenVPN-ile. See toimib enamuse GNU / Linux, OSX, Windowsi versioonidel. OpenVPN on TLS / SSL-põhine - see kasutab sama tüüpi krüpteerimist, mida kasutatakse HTTPS-s (Secure HTTP) ja hulgaliselt muid krüpteeritud protokolle. OpenVPN krüpteerimine põhineb RSA võtme vahetamise algoritmil. Et see toimiks ja, et toimuks kommunikatsioon, peab nii serveril ja kliendil olema avaliku ja erasektori RSA võtmed.  
  
Kui sa saad juurdepääsu oma VPN kontole, siis server genereerib need võtmed ja sa pead lihtsalt need allalaadima teie VPN-i teenusepakkuja veebisaidilt või lasta need saata oma e-posti aadressile. Koos oma võtmedega saate juursertifikaadi (\*. Ca) ja peamise konfiguratsiooni faili (\*. Conf või \*. Ovpn). Enamasti on ainult järgmised failid vajalikud, et seadistada ja käivitada OpenVPN klient:  
  
    client.conf (või client.ovpn) - konfiguratsioonifail, mis sisaldab kõiki vajalikke parameetreid ja seadeid. MÄRKUS: Mõnel juhul võivad sertifikaadid ja võtmed tulla varjatuna peamise konfiguratsioonifaili sees. Sellisel juhul ei ole allpool mainitud failid vajalikud.  
    ca.crt (juhul, kui ei ole konfiguratsioonifailis) –teie virtuaalse privaatvõrgu serveri juursertifikaat, et alla kirjutada ja kontrollida teisi võtmeid    client.crt (kui see ei ole konfiguratsioonifailis) – sinu kliendi sertifikaat, mis võimaldab teil suhelda VPN-i serveriga.  
  
Tuginedes iseäralikule konfiguratsioonile, teie VPN teenusepakkuja võib nõuda kasutajanime / parooli, et autentida oma ühendus. Sageli mugavuse pärast, kasutajanime ja parooli saab salvestada eraldi faili või lisada peamissee konfiguratsioonifaili. Muudel juhtudel võtmepõhist autentimist kasutatakse, ja võti on salvestatud eraldi faili:  
  
    client.key (kui see ei ole konfiguratsioonifaili) - kliendi autentimise võti, mida kasutatakse autentimiseks VPN serverisse ja krüpteeritud andmekanali loomiseks.  
  
Enamikul juhtudel, kui see ei ole just vajalik, siis ei pea te midagi konfiguratsioonifailis muutma ja (kindlalt!) **ärge muutke võtme või sertifikaadifaili**! Kõigil VPN pakkujatel on põhjalikud juhised üles seadmisest. Lugege ja järgige neid juhiseid, et veenduda, et teie VPN klient on õigesti konfigureeritud.  
  
MÄRKUS: Tavaliselt on lubatud kasutada ainult ühte võtit ühe andmesideühenduse kohta, nii et sa ilmselt ei tohiks samu võtmeid samal ajal erinevatel seadmetel kasutada. Saa uus võti iga seadme jaoks mida te kavatsete kasutada VPN-is –või, kui üritate luua oma kohaliku VPN-i (edasijõudnutele, siin ei käsitleta).  
  
Lae alla oma OpenVPN konfiguratsiooni ja kopeeri võtmefailid kindlasse kohta ja jätkake järgmises peatükis.  
  
   
Seadistamine OpenVPN kliendi  
  
Järgmistes peatükkides on mõned näited loomise OpenVPN kliendi tarkvara. Igal maitse GNU / Linux kasutada oma lemmik paketi manager ja paigaldada OpenVPN või OpenVPN-kliendi paketiga.  
  
Kui soovite kasutada OpenVPN Windows-il või OSX-il:  
  
<http://openvpn.se> (Windows kasutajaliides)  
<http://code.google.com/p/tunnelblick> (OSX pesaga)