**VPN**  
  
Viis kuidas teie andmeid jõuavad teie sülearvutist või mobiiltelefonist soovitud serverini ja tagasi pole nii lihtne, kui see võib tunduda. Oletame, et te olete kodus ühendatud traadita võrku ja avate wikipedia.org lehe. Teie taotluse teekond (andmed) koosneb mitmest kesk punktist, või "hüppest" võrgu-arhitekti terminoloogias. Igas selles hüppes (tõenäoliselt siis 5) saab teie andmeid ammutada, kopeerida ja potentsiaalselt muuta. Näiteks:  
  
    Teie traadita võrg (teie andmeid saab õhust nuuskida)  
    Teie ISP (enamikus riikides on nad kohustatud pidama üksikasjalikku logi teie, kui kasutaja tegevusest)  
    Internet Exchange Point (IXP) kuskil teisel mandril (tavaliselt turvalisem, kui mõni muu hüpe)  
    ISP hosting ettevõte, mis korraldab kohapeal (hoiab ilmselt logisid )  
    Sisevõrgus, millega server on ühendatud  
    Ja mitu hüpet vahepeal ...  
  
Iga isik, kellel on füüsiline ligipääs arvutitele või võrkudele, mis jäävad teist kuni serverini teepeale, tahtlikult või mitte, saab koguda ja paljastada andmeid, mis möödub teist serverini ja tagasi. See kehtib eriti mõne viimase hüppe kohta, kus internetiühendus proovib jõuda kasutajani - nn „viimase miili“ olukordades. See sisaldab sise-ja avaliku traadita või traadiga võrke, telefoni-ja mobiilsidevõrke, võrke raamatukogudes, kodudes, koolides, hotellides. Teie ISP-d ei saa pidada ohutuks, ega"andmete neutraalseks". Paljudes riikides ei nõua riigiasutused juurdepääsu teie andmetele, ja seal on alati suur oht sissetungile, makstud ründajatelt, kes töötavad vastastele, kellel on sügavad taskud.  
  
**VPN - Virtual Private Network** - on lahendus sellele "viimase miili“ lekkele. VPN on tehnoloogia, mis võimaldab luua virtuaalse võrgu olemasoleva infrastruktuuri peale. Selline VPN võrk kasutab töötamiseks samu protokolle ja standardeid, kui fundamentaalne füüsikaline võrk. Programmid ja operatsioonisüsteemid kasutavad seda läbipaistvalt, nagu oleks see eraldi võrguühendus. Aga tema topoloogia - kuidas võrgu sõlmed (kuidas te, VPN server ja potentsiaalselt, teised liikmed või teenused, mis on kättesaadavad VPN-il) on omavahel seotud füüsilisele ruumile - on täielikult uuesti defineeritud.

Kujutage ette, et selle asemel, et usaldada oma andmeid terves ridades vahemeestele (su kohalik võrk, ISP, riik) sul on valida selle asemel see läbi serveri lasta kasutades selleks usaldusväärset VPN-i (soovitus või uurimustöö tuleb siin kasuks). Teie andmeid alustavad oma teekonda siit kõrvalisse kohta. VPN võimaldab teil taastada oma kohalik ja geopoliitiline kontekst kõik koos - alates hetkest, mil teie andmed lahkuvad arvutist ja satub VPN-i võrku, siis see on täielikult tagatud TLS / SSL tüüpi krüpteeringuga. Nõnda ilmub see juhusliku mürana igas sõlmes, kus võidakse teie järele luurata. See on sama, kui teie andmed reisiksid sõltumatus Titaanisulamist torus, purunematu kuni see on jõudnud te sülearvutist VPN serverini. Muidugi võib väita, et lõpuks, kui teie andmed on väljaspool VPN-i ohutut sadamat , siis see muutub uuesti haavatavaks, kuid see on ainult osaliselt tõsi. Kui teie andmed väljuvad VPN serverist on need teist väga kaugel- piisavalt kaugel sulidest, kes ei saa kohaliku traadita võrgus teie järgi nuuskida, teie äraostetavast ISP-st või valitsusest, kes on kinnisideeks võtnud terrorismivastased seadused. Tõsine VPN-i teenusepakkuja on oma servereid paigaldanud kõrge turvalisusega Interneti vahetus asukohta, peatades igasuguse füüsilise juurdepääsu inimestele, koputamise või raske ülesande logimise.

*"Kõike mida sa tänapäval internetis teed jälgitakse ja me tahame seda muuta. Tänu meie kiirele VPN teenusele saate te internetis jääda täiesti anonüümseks. Samuti on võimalik surfata tsenseeritud veebisaitidel, mida teie kool, ISP, töö või riik võivad takistada . [DarkVPN] mitte ainult ei aita inimestel surfata anonüümselt, see aitab ka inimestel sellistes riikides nagu Hiina,surfata tsenseeritud veebilehtedel. Milline on iga inimese demokraatlik õigus. DarknetVPN annab kõigile VPN-i kasutajatele anonüümse IP-aadressi. Kõik elektroonilised read lõppevad koos meiega. Me ​​ei salvesta logifaile kuna soovime saavutada maksimaalset anonüümsust. Meiega surfate alati anonüümselt, turvaliselt ja krüpteeritult. "*  
(Http://www.darknetvpn.com/about.php)  
  
Teine huvitav ja sageli alahinnatud omadusi VPN-il on kodeeritud tema nimesse - peale selle,et ta on **V**irtuaalne ja **P**rivaatne ning oma **V**õrgustik. VPN ei võimalda mitte ainult ühendada VPN serveri kaudu mujalw maailmas, vaid ka suhtlemist teiste liikmetega samas VPN võrgus, ilma, et peaksid kunagi lahkuma ohutust krüpteeritud ruumist. Läbi selle funktsionaalsuse Virtuaalne Privaatne Võrk muutub *DarkNet.-i* sarnaseks (laiemas tähenduses mõiste) – võrk, mis on eraldatud Internetist ja kättesaamatu kutsumata külalistele. Ühendus VPN serveriga, ja seega eravõrku mida see hõlbustab, nõuab võtit või sertifikaati ja seega ainult "kutsutud" kasutajad on lubatud. Ei ole võimalik, et Internetis keegi võõras pääseb ligi sellele, mis on selle VPN-i peal, ilma, et näides registreeritud kasutajana või varastades kelleltki selleks võtmed. Kuigi tavaliselt ei nimetada neid sellistena, siis ükskõik, millist tüüpi ühendatud Intranet võrguga on tegemist on see tehniliselt DarkNet.   
"*Virtuaalne PrivaatVõrk (VPN) on tehnoloogia, mis võimaldab Interneti või muu vahelise võrgu kaudu ühendada arvuteid isoleeritud kaugarvuti võrkutesse, mis muidu oleksid kättesaamatud .."* (http://en.wikipedia.org/wiki/Virtual\_private\_network)  
  
Paljud kaubanduslikud VPN pakkujad rõhutavad anonüümsust mida nende teenused pakuvad. Tsiteerides Ipredator.org lehte (VPN teenus, mis alustati Pirate Bay projekti taga olevate inimeste poolt): "Sa vahetad oma IP aadressi, mille sa saad oma ISP-lt anonüümse IP-aadressi vastu. Sa saad ohutu / krüpteeritud ühenduse teie arvuti ja Interneti vahel ". Tõepoolest, kui ühendate Internetti VPN-i kaudu, siis nähakse, et nagu ühenduse IP-aadress oleks pärit IPredator serveritest.   
  
*" Sa vahetad oma IP aadressi, mille sa saad oma ISP-lt anonüümse IP-aadressi vastu. Sa saad ohutu / krüpteeritud ühenduse teie arvuti ja Interneti vahel."*  
    (Https://www.ipredator.se)

**Oluline märkus VPN turvalisuse** **kohta**  
Lihtsalt seetõttu, et sa kasutad VPN-i ei tähenda, et sinu krüpteerimismeetod on täiesti turvaline. Oluline on olla teadlik riskidest registreerides end VPN teenuse pakkujaga, kuna nad võivad pakkuda ühendust, mis on purunev. **Kui teil on tõesti tarvis kõrge turvalisuse taset** siis ärge kasutage ühenduse tüübiks **PPTP**. **PPTP** on üks vanematest VPN tehnoloogiatest. Kuigi on teada, et **PPTP** kasutab nõrgemaid krüpteerimise viise kui mõlemad L2TP/IPSec või OpenVPN, siis see võib ikka olla kasulik, et pääseda mööda Interneti blokeeringutest ja pakkuda mõnel tasemel krüpteeringut. Klienditarkvara on mugavalt sisse ehitatud enamustele Microsoft Windows versioonidele, Apple-ile, Linux-i arvutitele ja isegi mobiiltelefonidele. Seda on väga lihtne üles seada. PPTP VPN sessiooni on võimalik murda kasutades *Cloud Cracker* teenust ja seda väga vähese raha eest.