# Virtuelne privatne mreže (VPN)

Virtuelne privatne mreže su nastale usled potrebe da se biznisi, organizacije, vlade i slični subjekti koji poseduju osetljive informacije zaštite od hakovanja i gubitka podataka u slučajevima kada je potrebno da im udaljeni korisnici ili satelitske kancelarije pristupe kao i radi smanjenja telekomunikacionih troškova efikasnijim korišćenjem infrastrukture[3]. Virtuelne privatne mreže su privatne mreže koje rade preko deljene javne infrastrukture kao što je internet[1] . Virtuelna je zato što ne postoji odvojena fizička infrastruktura za datu mrežu već koristi već postojeću javnu infrastrukturu. Privatna je zato što omogućava bezbednu upotrebu uz garanciju da će samo članovi mreže moći da vide poslate informacije [5]. VPN omogućavaju privatnost podataka korišćenjem sigurnosnih procedura(enkripcija) i protokola tuneliranja(IPsec, PPTP, L2TP). VPN napravi „tunel“ izmedju korsinika pri čemu se podaci enkriptuju na strani pošiljaoca, šalju kroz tunel i zatim dekriptuju na strani primaoca. Pored podataka mogu se kriptovati i polazna i završna adresa radi veće sigurnosti [4]. Dva osnovna tipa ovih mreža su: **VPN „od lokacije do lokacije“**(site-to-site) koja omogućava da se uspostavi bezbedna konekcija između više poslovnica na različitim lokacijama preko javne infrastrukture i time podaci sa jedne lokacije stavljaju na korišćenje zaposlenima na drugoj i **VPN za udaljen pristup** koja omogućava pojedincima da uspostave bezbednu vezu sa udaljenom mrežom i pristupe njenim resursima kao da su direktno povezani na dati server[4].

Iako su prvobitno nisu bile namenjene za to, usled skorašnjih otkrića o velikim projektima za nadzor i ograničenja koje određene vlade nameću svojim građanima sve više i više raste upotreba VPN usluga za zaštitu privatnosti pojedinaca, zaštitu od cenzorisanja kao i za pristup sadržaju koji je geografski ograničen [2,6]. Još jedan od razloga za povećano korišćene je porast upotrebe javnih mreža koje je prouzrokovano širenjem mobilne industrije. Ovo je dovelo do stvaranja uslova za napade kao što su krađa akreditiva, presretanje paketa i krađa sesija što vodi do toga da neki korisnici koriste VPN za zaštitu svojih interakcija. Mnoge VPN usluge nude mogućnost izbora izlaznih tačaka tako da korisnici mogu da dobiju IP adrese u različitim državama. Iako do nekog stepena VPN provajderi pružaju navedene usluge dovodi se u pitanje njihova sposobnost da očuvaju anonimnost i privatnost se dovodi u pitanje pošto to nije njihova prvobitna namena. Privatnost se kod ovih mreža ne odnosi na privatnost krajnjih korisnika već na povezivanje više privatnih mreža. Usled lakoće korišćenja, velikih performansi i jakog marketinga postoji velika privlačnost prema ovim mrežama iako slepa vera neinformisanih korisnika dovodi do problema[6].

## Rizici za korisnike virtuelnih privatnih mreža

-Dosta prevedeno samo-Iako veliki broj pružalaca VPN usluga tvrde da pružaju robusne i sigurne infrastrukture uz obezbeđivanje bezbedonsti korisnike tako što ne loguju podatke(ne vode dnevnike) ne postoje alati i istraživanja koji te tvrdnje proveravaju. Pored toga neki provajderi su poznati po tome što prodaju podatke korisnika i manipulišu saobraćajem. Takmičenje izmedju provajdera zajedno sa nedostatkom objektivnih mera kvaliteta dovode do zavarivanja klijenata kako bi ih privukli. Usled nedostatka nezavisnih ocena VPN usluga korisnici su primorani da se o tome informišu sa blogova ili websajtova koji su većinom podržani od strane VPN partnerskog marketinga i usluga pa se od njihovih ocena ne može očekivati nepristrasnost. To se odnosi na neke od najbolje rankiranih sajtova za ocenjivanje VPN usluga. Pored curenja saobraćaja usled loše bezbednosti oko 10% VPN servisa presreću i/ili manipulišu saobraćajem stim što su mogući načini za nadziranje saobraćaja koji su teški da se otkriju. Takođe, VPN servisi obično obećavaju veliki broj različitih geografskih lokacija koje korisnici mogu da izaberu kao izlazne čvorove ali oko 10% njih je pogrešno predstavio lokacije tako što se 5%-30% nalazi na lokaicijama koje su različite od reklamiranih. Čak postoje provajderi koji tvrde da imaju lokacije u preko 190 država ali u stvarnosti se server nalaze u ne više od 10 centara podataka. [6 uz 2.1 2.2 poglavlja]

1 - [http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.5.2253&rep=rep1&type=pdf - 1. poglavlje]

2 - [http://eprints.networks.imdea.org/1886/1/imc18-final198.pdf – abstract + 1. poglavlje]

3 - [https://www.le-vpn.com/history-of-vpn/ - What is the purpose of VPN poglavlje]

4 -[http://ijarcsse.com/Before\_August\_2017/docs/papers/10\_October2012/Volume\_2\_issue\_10\_October2012/V2I900209.pdf - 1. poglavlje]

5 - [https://singipedia.singidunum.ac.rs/preuzmi/41767-virtuelne-privatne-mreze/1846 3. poglavlje]

6 - [https://petsymposium.org/2015/papers/02\_Perta.pdf – 1. poglavlje]