CARNET

# VPN usluge – što su, kako funkcioniraju i kada su korisne

CERT.hr-PUBDOC-2019-6-382

CERT.hr

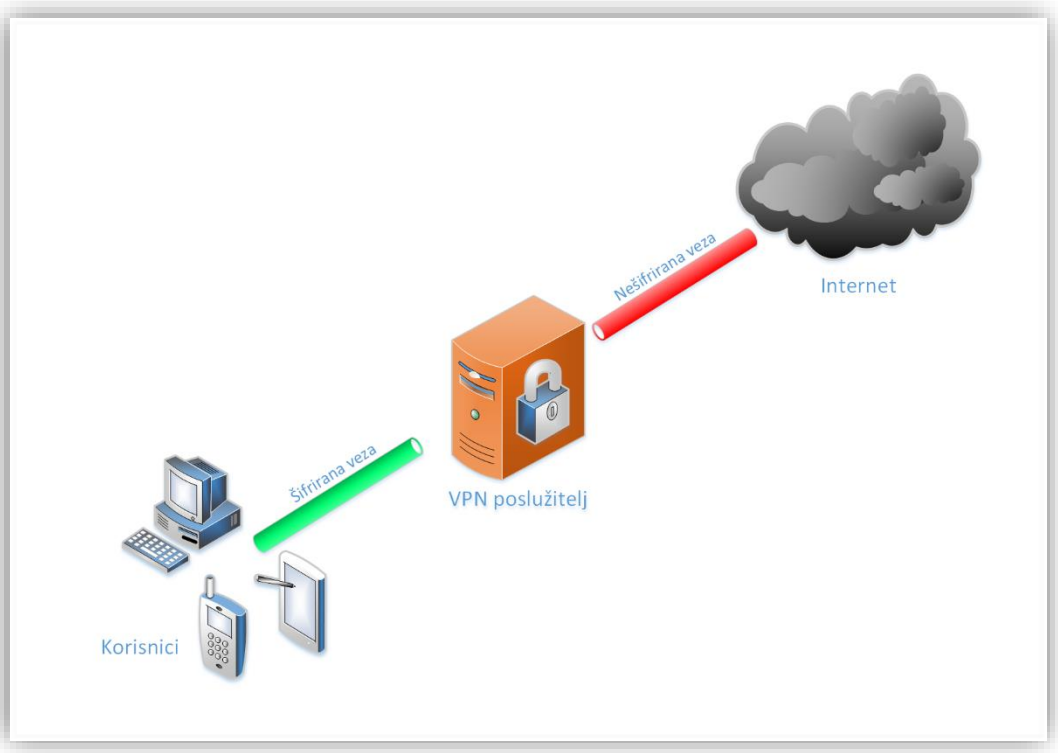
# Sadržaj



Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

# 1 Uvod

VPN ili Virtualna privatna mreža (engl. *Virtual Private Network*) omogućava ostvarivanje sigurne, zaštićene (šifrirane) veze prema drugoj računalnoj mreži, najčešće preko interneta, no u poslovnoj primjeni i preko dijeljene mrežne infrastrukture (Slika 1).




**Slika 1 – Prikaz rada VPN veze**

Najčešće potrebe za korištenje VPN rješenja su:

- Sigurno povezivanje poslovnih korisnika koji nisu na istoj (geografskoj) lokaciji
- Sakrivanje identiteta i lokacije korisnika na internetu od pružatelja informacijske usluge
- Pristup zaštićenim/komercijalnim sadržajima na internetu
- Zaštita od prisluškivanja u nesigurnim bežičnim (WiFi) i žičanim lokalnim mrežama
- Cjelokupno šifriranje prometa kojim se povećava anonimnost na internetu

Dva su načina implementacije VPN servisa:

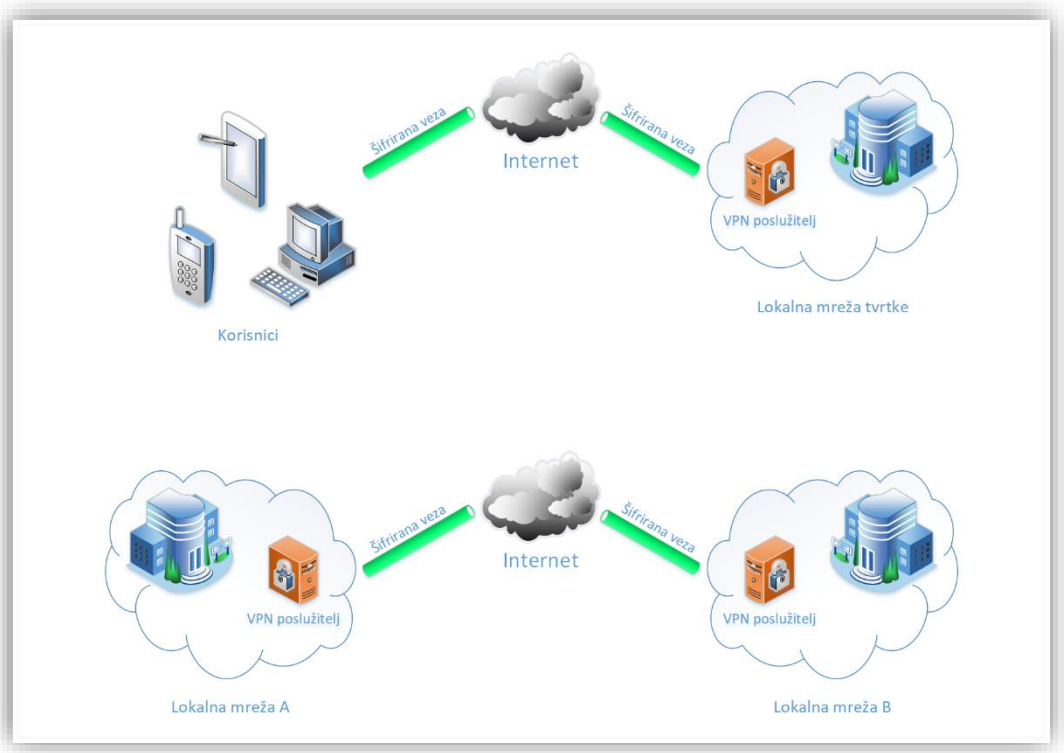
1. VPN usluga koja se može „kupiti“ i praktički odmah koristiti bez puno tehničkog znanja
2. I servis koji se mora implementirati na privatni ili poslovni poslužitelj i koji traži puno više tehničkog ICT znanja

Prvi spadaju isključivo u domenu privatnih korisnika i kupuju se kao usluga u oblaku (engl. *cloud service*), dok je drugi tip programski alat koji se instalira u korporativne mreže

i na vlastite poslužitelje ili postoji kao dio hardverske komponente vatrozida (engl. *firewall*) ili usmjerivača (engl. *router*).

Osim prema načinu implementacije, VPN-ovi se razlikuju i po funkcionalnosti (Slika 2):

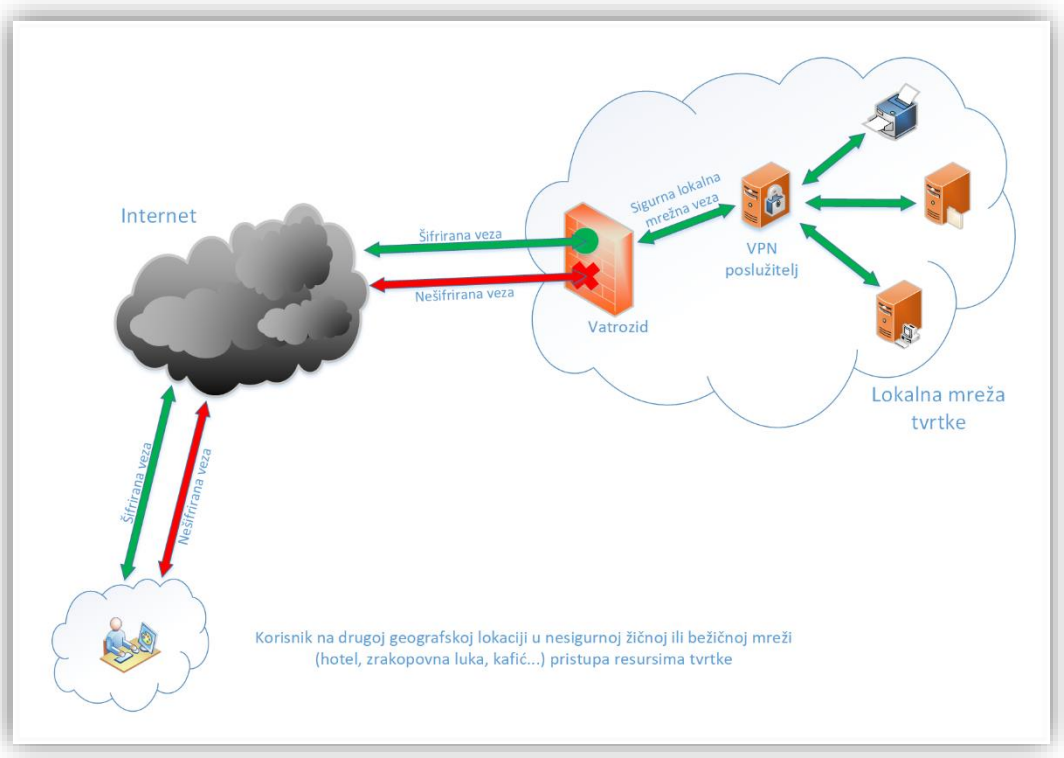
1. Oni koji se koriste da se pojedinac (klijent) spoji na poslužitelj, odnosno u određenu lokalnu mrežu (engl. *Remote access VPN*)
2. I oni koji omogućavaju spajanje dviju udaljenih lokalnih mreža, te se time ostvaruje siguran i transparentan rad svih korisnika i poslužitelja obiju mreža, odnosno da dvije nezavisne mreže rade kao jedna jedinstvena mreža (engl. *site-to-site*)




**Slika 2 – Prikaz rada klijent-poslužitelj / poslužitelj-poslužitelj**

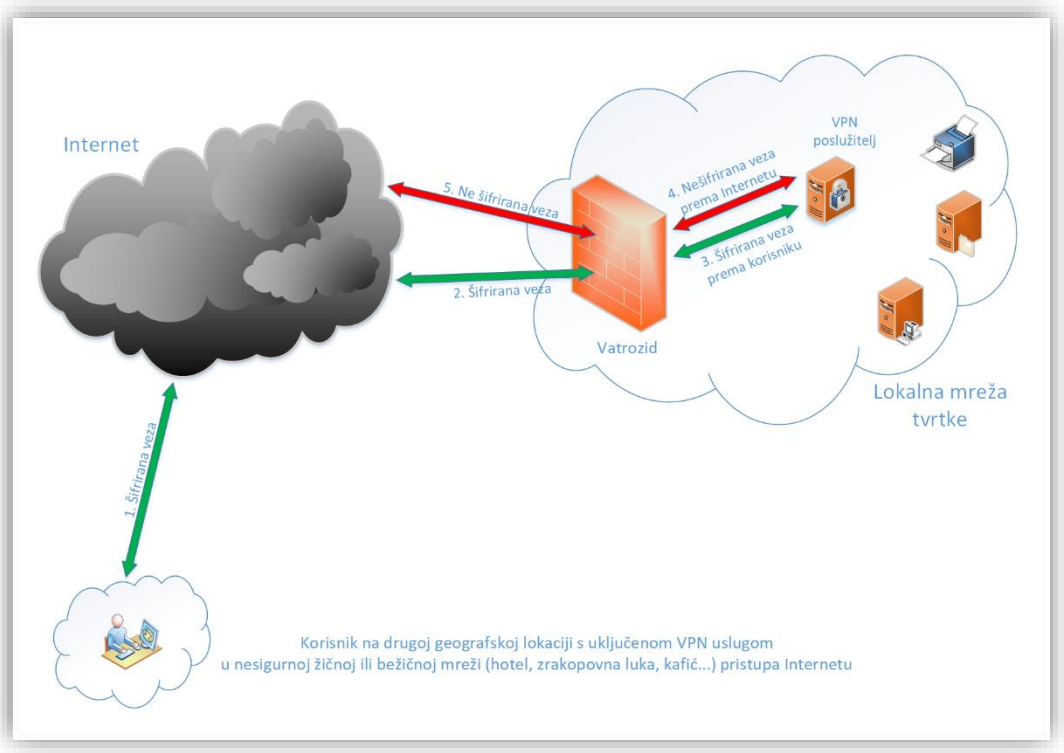
# 2 Kako radi VPN?

Kada se računalo (ili tablet, ili mobitel) koje se nalazi bilo gdje u svijetu spoji u VPN mrežu, interna (zaštićena) mreža tretira sav njegov mrežni promet kao da se to računalo nalazi u istoj toj lokalnoj mreži kao i VPN poslužitelj. Tada se sav mrežni promet šalje preko sigurne veze do VPN poslužitelja, a računalu se omogućava sigurno korištenje lokalnih mrežnih resursa (Slika 3).



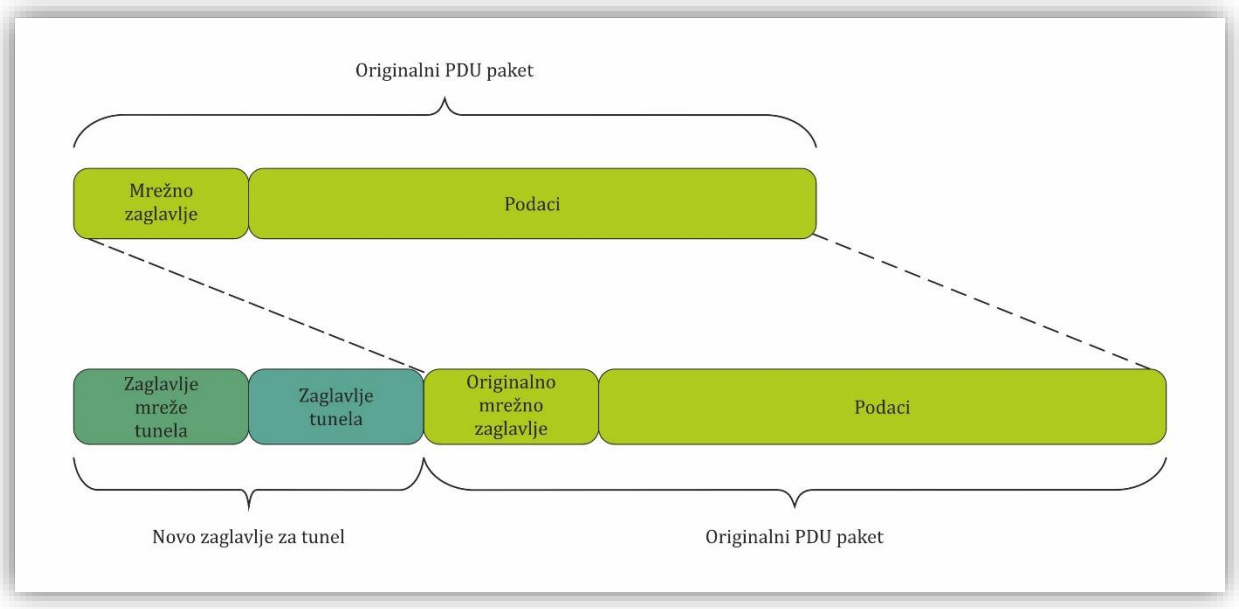

**Slika 3 – Prikaz pristupa zaštićenoj lokalnoj računalnoj mreži s i bez aktivne VPN veze**

Također, pristup internetu s tog računala je moguć kao da se to računalo nalazi na VPN lokaciji, što može biti korisno ako se korisnik nalazi na nekoj nesigurnoj lokaciji, kao što su zrakoplovne luke, kafići, besplatne javne WiFi pristupne točke i sl. (Slika 4).



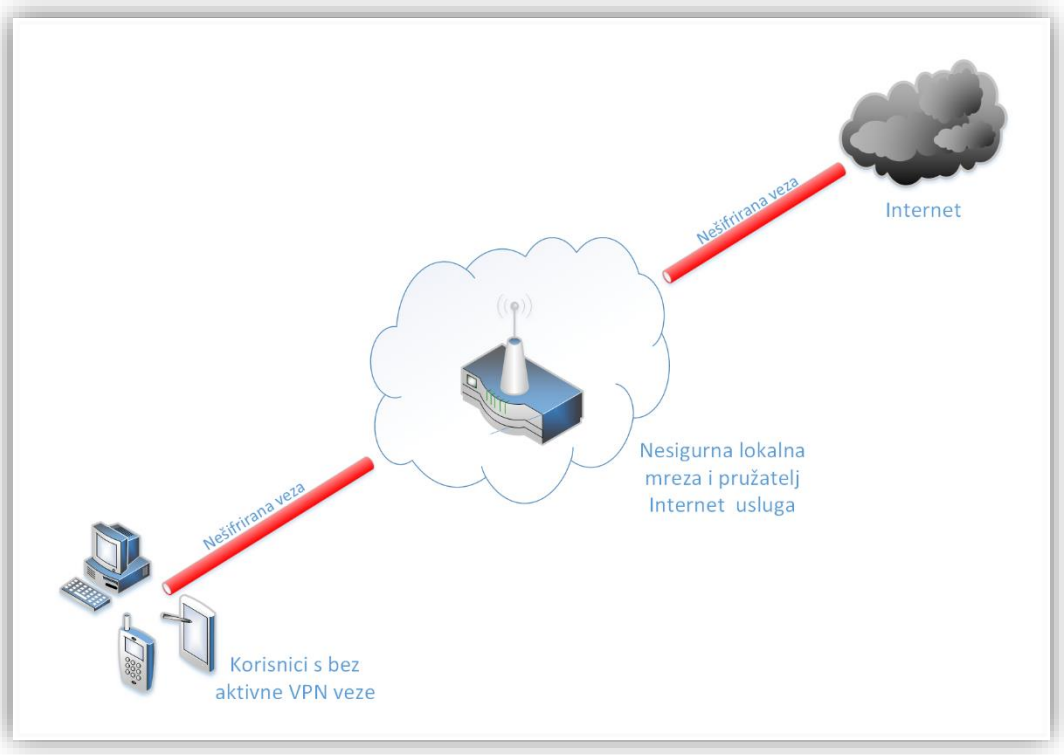

**Slika 4 – Prikaz korištenja VPN veze i pristupanje internet sadržajima**

Tuneliranje (engl. *tunneling*) je tehnika prijenosa podataka iz jedne privatne mreže u drugu tako da ih se „zamota“ u VPN paket. Podaci koji se šalju iz jedne u drugu mrežu mogu biti paketi (engl. PDU – *protocol data unit*) bilo kojeg protokola. Protokoli kojima se implementira tuneliranje enkapsuliraju (engl. *encapsulate*) originalne PDU pakete u novi oblik PDU paketa s novim posebno oblikovanim zaglavljem. Takvo zaglavlje uz originalne PDU pakete sadrži i dodatne „prijenosne“ podatke, koji služe da bi enkapsulirani podaci bili usmjereni kroz VPN mrežu do njihovog odredišta, a to je druga strana VPN tunela. Nakon što takav paket stigne na odredište, on se ekstrahira, te se podaci koji su bili enkapsulirani šalju dalje na ciljano odredište u privatnoj mreži i dalje ako je potrebno na internet. Tuneliranje označava cijeli navedeni proces prijenosa podataka kroz VPN vezu, a to je enkapsulacija, prijenos i ekstrakcija podataka (Slika 5).

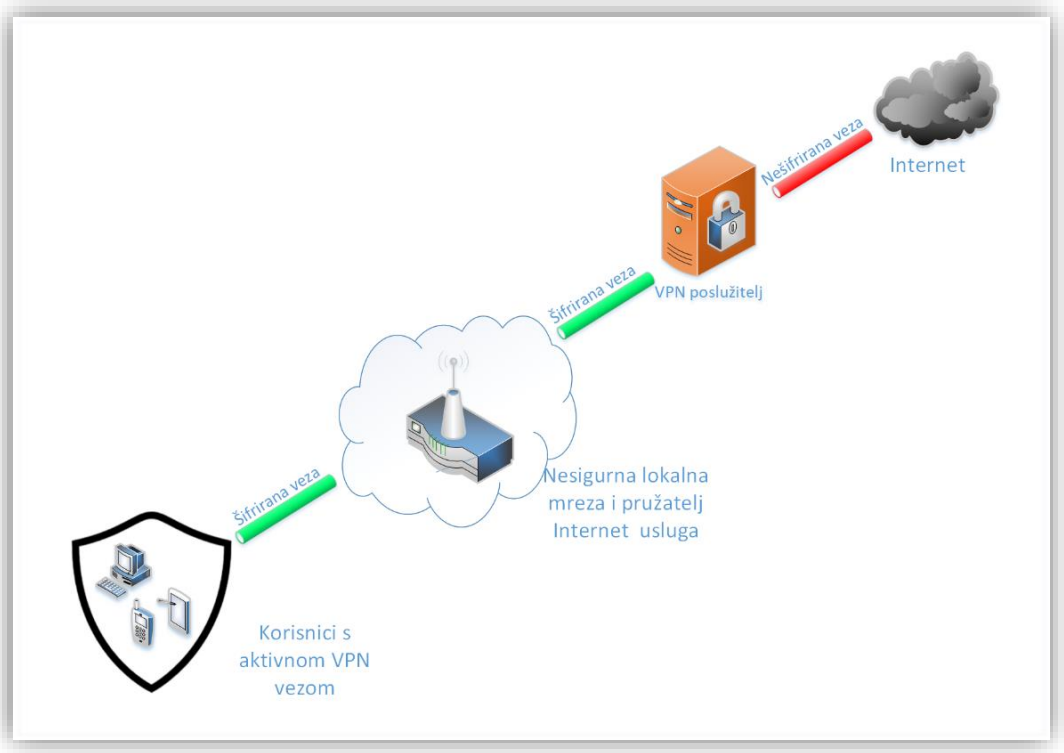



**Slika 5 – Princip enkapsuliranja podataka VPN prometa**

Pregledavanjem weba dok je VPN veza aktivna, korisnikovo računalo pristupa web stranicama preko sigurne VPN veze. VPN prosljeđuje inicijalni zahtjev računala, te tako korisnikov upit izgleda web poslužitelju kao da je došao s adrese VPN poslužitelja. Istim putem putuje odgovor web poslužitelja nazad do korisnikovog računala, koji je također u povratku šifriran.




**Slika 6 – Prikaz nesigurne komunikacije unutar lokalne mreže (npr. javne bežične mreže)**




**Slika 7 - Prikaz sigurne komunikacije unutar lokalne mreže (npr. javne bežične mreže)**

Malo drugačiji način primjene VPN-a je kada više korisnika, poslužitelja i raznih drugih mrežnih uređaja koji se nalaze na različitim udaljenim fizičkim lokacijama, odnosno lokalnim mrežama, moraju raditi kao jedna jedinstvene lokalna mreža. Tada se na svakoj lokaciji postavlja VPN poslužitelj/usmjerivač, koji usmjerava pakete između te dvije mreže. Sav promet koji putuje iz jedne u drugu mrežu je također šifriran.

# 3 Zašto DA i zašto NE koristiti VPN u svakodnevnom radu

U poslovnom okruženju je jasno zašto bi se trebale i morale koristiti sigurne VPN veze, no u svakodnevnom privatnom životu postoje brojni razlozi za i protiv korištenja VPN veza.

Neki primjeri zašto je dobro i korisno koristiti VPN veze su:

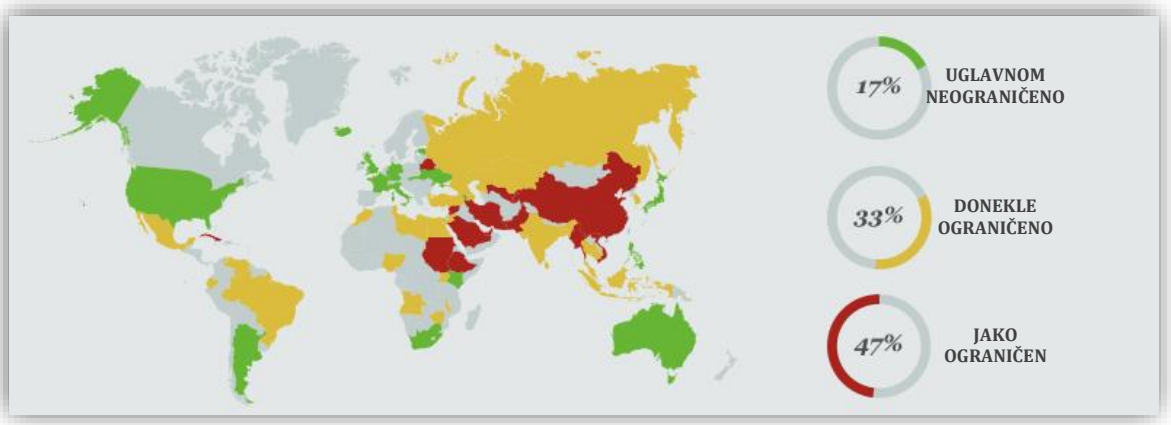
- **Pregledavanje weba preko nesigurnih javnih bežičnih, ali i žičanih mreža** – Kava u kafiću, odsjedanje u hotelu, kupovina u dućanu – gotovo svugdje se može dobiti besplatan pristup internetu. Nakon što se korisnik spoji na besplatni WiFi ili utakne žicu u „zid" može jednostavno i brzo krenuti na internet i na svoje društvene mreže, provjeriti poštu, obaviti video razgovore itd. Problem je u tome što je takav rad u nepoznatoj i javnoj mreži vrlo riskantan i opasan jer se pregledava web i općenito koristi internet na nesiguran način. Nešifriran promet koji putuje radio valovima ili žicom se izuzetno lako i jednostavno može prisluškivati, te ako se pristupa stranicama koje traže korisničke podatke zlonamjerna osoba može vrlo lako saznati i kasnije ih upotrijebiti protiv korisnika ili ih iskoristiti na neki ilegalan način, tj. na štetu korisnika. Također mogu postojati i lažne WiFi pristupne točke, koje nisu legitimne pristupne točke, nego su stvorene i osmišljene da se lažno predstavljaju kao npr. WiFi od hotela, a osoba koja ih je postavila može jednostavno prisluškivati nešifrirani promet spojenih korisnika, tj. žrtva. U slučaju da korisnik pristupa zaštićenim stranicama putem protokola HTTPS ili pak korisnik čita elektroničku poštu putem sigurnih protokola (POP3S, IMAPS, SMTPS, Exchange i dr.) tada VPN nije nužno potreban i tu je korisnik većinom siguran No sav drugi sadržaj koji nije dio navedenog, je vrlo ranjiv po pitanju prisluškivanja prometa i tada je VPN nužan za sigurnu komunikaciju.

- **Zaobilaženje ograničenja koja su vezana za različite geografske lokacije web sadržaja** – danas su vrlo česta i popularna ograničenja video sadržaja. Recimo, pristup određenim komercijalnim video uslugama (IP televizija, plaćeni TV programi) je često ograničen na razini raspona IP adresa, tako da ako korisnik nije korisnik nekog pružatelja internet usluga ili IP adresa korisnika nije unutar države u kojoj se nalazi poslužitelj za te usluge, neće se moći koristiti dotični sadržaj. No to nije vezano samo za video sadržaj, nego to vrijedi za sav tip sadržaja na internetu.
  Korištenjem VPN-a, poslužitelj vidi IP adresu VPN poslužitelja, a ne stvarnu IP adresu korisnika. Dakle, dovoljno je da VPN poslužitelj bude u dijelu interneta kojeg poslužitelj prihvaća kao legitimnog korisnika.

- **Sigurne VoIP i chat usluge popularnih aplikacija za razgovor** – dobar dio današnjih aplikacija koje omogućavaju razmjenu poruka i razgovora (glasovni pozivi) na računalima, pametnim telefonima i tabletima još uvijek ne koriste šifriranje prometa, te se poruke i razgovor izlaže lakom prisluškivanju. VPN-om se to može spriječiti kada se uređaj nalazi u nekom nesigurnom okruženju. Ipak, najpopularnije aplikacije (WhatsApp, Viber, Skype…) nedavno su prešle na šifriranje takvog tipa prometa, te kod korištenja takvih sigurnih aplikacija potreba za VPN-om za taj tip zaštite više nije nužan (Slika 8).


**Slika 8 – Današnji popularni servisi za razmjenu poruka i VoIP razgovora**

- **Cenzura interneta** – u mnogim zemljama u svijetu vlada blokira određeni tip sadržaja kojemu korisnici interneta mogu pristupiti, te ih time ograničava da koriste svu slobodu medija i trenutno dostupne tehnologije (Slika 9). Korištenjem VPN poslužitelja skrivaju se stvarni promet i sudionici u komunikaciji, što omogućava zaobilaženje raznih cenzura i ograničenja.




**Slika 9 – Prikaz cenzure interneta u svijetu (izvor)**

- **Štedi prilikom online kupnje** – neki *online* dućani koriste tehniku detekcije IP adresa korisnika i ovisno s koje IP adrese dolaze, tj. iz kojih država dolaze mogu korisnicima tih *online* dućana prikazati drugačije cijene. To je primjerice rašireno kod kupovine avionskih karata.

- **Praćenje rada na računalu** – danas je primjerice Google postao sveprisutna tvrtka na internetu, koja nudi brojne korisne usluge koje koriste milijarde ljudi širom svijeta. No za uzvrat Google na brojne načine prikuplja podatke o korisnicima koji koriste Chrome web preglednik, Google servise, Google Analytics koji se nalaze gotovo na svakoj web stranici. Sve to da bi kasnije mogao te iste

podatke o korisnicima i njihovom načinu ponašanja na internetu iskoristiti u svrhe profiliranja i ciljanog oglašavanja.

- **Šifriranje svega** – ako se želi šifrirati sve što izlazi i dolazi u korisničko računalo, VPN je pravi alat za to. S njime je moguće zaobići sva ograničenja cenzura, vatrozidova (engl. *firewall*) i prisluškivanja zlonamjernih ljudi, organizacija, pružatelja internetskih usluga i relativno sigurno stići do potrebnog web sadržaja, jer sav promet koji putuje VPN vezom je šifriran i jedino što ostaje upitno prilikom korištenja VPN-a su dvije stvari:
    - Koristiti VPN koji koristi pouzdan i siguran protokol, odnosno šifriranje podataka
    - Svako korištenje VPN-a podrazumijeva da korisnik VPN-a vjeruje svom odabranom VPN servisu/poslužitelju. Razlog tome je što šifrirani podaci nakon što ih VPN poslužitelj primi, moraju biti dešifrirani i kao takvi poslani dalje u svijet interneta. Što znači da VPN servis može znati sve što je korisnik radio na internetu i zna s koje IP adrese je pristupao. Dakle, kada podaci izađu iz VPN poslužitelja, te ako taj promet nije bio upućen prema nekom sigurnom *online* servisu npr. putem protokola HTTPS, nego nesigurnim protokolom kao što je protokol HTTP za web ili protokoli POP3, IMAP, SMTP za elektroničku poštu, podaci će biti nezaštićeni i podložni prisluškivanju na putu do tog *online* servisa.

Kako postoje brojne pozitivne strane VPN-a, tako postoje i neke negativne strane:

- **VPN usluge/poslužitelji** – prilikom dešifriranja prometa koji je bio šifriran od korisnika do VPN poslužitelja, VPN poslužitelj u svojim dnevnicima (engl. *logs*) može spremati svu statistiku o prometu korisnika na internetu. Ovo je problem iz perspektive privatnosti, kako za VPN servis, tako i za korisnika ako podaci dospiju u „krive“ ruke. Iako gotovo sve VPN usluge u oblaku tvrde da su korisnički podaci i statistike prometa sigurni, odnosno da se ne spremaju na poslužitelju, to svakako treba uzeti s dozom rezerve po pitanju istinitosti ove tvrdnje. Jer ako to nije istina, zbog mogućeg hakerskog napada na VPN poslužitelj i krađe takvih osjetljivih podataka ili pak jednostavno zbog predaje svih zapisa VPN poslužitelja nekoj vanjskoj organizaciji, ti zapisi mogu postati javni ili pak na neki način iskorišteni za određene legalne ili ilegalne radnje, te tim činom korisnik gubi anonimnost na internetu.

- **Brzina VPN veze** – iako su današnje širokopojasne (engl. *broadband*) veze postale jako brze za uobičajeno korištenje interneta (surfanje, igranje, gledanje video sadržaja), može doći do usporavanja prometa kada se koristi VPN veza. Usporavanje bi trebalo biti minimalno, tako da ga korisnik vjerojatno neće ni primijetiti. No vjerojatnije je da će doći do usporenja prometa kroz VPN vezu ako VPN poslužitelj zaprimi previše korisnika na sebe, tj. usluga dotičnog VPN poslužitelja bude preopterećena, te poslužitelj, odnosno njegovi računalni i mrežni resursi postanu usko grlo VPN veze. Kada se koriste besplatne VPN usluge ili besplatne inačice komercijalnih VPN usluga, tada je moguće da se dogodi značajno usporavanje prometa kroz VPN vezu. No to je ili marketinški razlog kako bi se korisnika navelo da kupi „punu“ inačicu VPN usluge ili je to stvarno usporenje prometa kod korištenja besplatne VPN usluge jer je usluga besplatna i njezini

resursi ne mogu podnijeti toliku količinu korisnika koji bi htjeli besplatno koristiti VPN usluge.

# 4 VPN protokoli

Protokoli definiraju kako VPN servis upravlja prijenosom podataka koji idu kroz njega. Danas najčešće korišteni protokoli su OpenVPN, SSTP, L2TP, PPTP i IPSec.

## 4.1 PPTP (Point-To-Point Tunneling Protocol)

Ovo je jedan od najstarijih protokola koji se još uvijek koristi. Izvorno ga je dizajnirala skupina tvrtki: Microsoft, US Robotics, Ascend Communications, 3Com i ECI Telematics. Danas se uglavnom može pronaći kod korisnika Microsoft Windows poslužitelja, no i to je danas rijetkost jer protokol slovi kao poprilično nesiguran i ranjiv na nekoliko načina, pa bi trebalo izbjegavati njegovo korištenje. Protokol je smješten u mrežni sloj i temelji se na poznatom PPP (engl. *Point-to-Point Protocol*) protokolu.

## 4.2 L2TP (Layer 2 Tunneling Protocol)

L2TP protokol je rezultat fuzije protokola PPTP i L2F (Layer 2 Forwarding) tvrtki Cisco i Microsoft. Cilj je bio da se kombiniranjem najboljih značajki oba protokola stvori sigurniji protokol.

## 4.3 IPSec (Internet Protocol security)

IPSec protokol je jedan od najstarijih protokola, koji je nastao krajem 80-tih godina 20. stoljeća pod sponzorstvom američke agencije NSA. Za razliku od prethodno opisanih protokola IPSec pripada trećem sloju OSI modela. IPSec protokol osigurava ispunjenje traženih sigurnosnih zahtjeva: tajnost (engl. *confidentiality*), autentičnost (engl. *authentication*), cjelovitost (engl. *integrity*) i raspoloživost (engl. *availability*). Nažalost, kroz godine korištenja sama fleksibilnost i velika konfigurabilnost protokola je stvorila pad zainteresiranosti u komercijalnoj primjeni, a ista ta fleksibilnost je ukazala i na brojne probleme s protokolom zbog svoje kompleksnosti. Kako s raznim sigurnosnim sustavima, tako i loše održavanje sustava koji iziskuje jako veliko tehničko znanje, posebno kod velikih razgranatih sustava, lako može dovesti do kritičnih kvarova i problema u radu cjelokupnog sustavu.

## 4.4 SSTP (Secure Socket Tunneling Protocol)

Još jedan Microsoftov protokol, kod kojeg se sigurna veza ostvaruje putem SSL/TLS šifriranja, što je između ostaloga i standardni način za sigurno pregledavanje web stranica (protokol HTTPS). Uglavnom se ne koristi za povezivanje lokacija, nego mu je glavna namjena za vezu klijenta i poslužitelja.

## 4.5 OpenVPN

Jedan od najpopularnijih protokola danas je svakako OpenVPN. Razlog tome je to što je jedan od najsvestranijih i sigurnijih protokola, a osim toga je projekt otvorenog koda, što znači da ga na stotine programera širom svijeta stalno poboljšavaju i razvijaju. To je i jedan od razloga zašto je podržan na gotovo svim današnjim platformama. OpenVPN koristi SSL/TLS (engl. *Secure Sockets Layer* / *Transport Layer Security*) za uspostavu

sigurne veze i razmjenu kriptografskih ključeva između krajnjih točaka VPN veze. Za autentifikaciju korisnika mogu se koristiti unaprijed podijeljeni ključevi (engl. *pre-shared keys*), certifikati i klasično korisničko ime sa zaporkom.

## 4.6 WireGuard

WireGuard je sasvim novo razvijeni protokol projekta otvorenog koda koji ima tendenciju da u bliskoj budućnosti pretekne i zamijeni OpenVPN. Cilja na bolje performanse od protokola IPSec i OpenVPN, a ujedno i na jednostavnost, jer po nekim testovima i povratnim informacijama drugi protokoli su često kompliciranizaimplementaciju, a isto tako i zastarjeli po pitanju algoritama za šifriranje i bazirani na velikoj količini koda kojega je teško održavati i učiniti sigurnim. Ovim projektom WireGuard želi postići:

- Veće brzine
- Dulje trajanje baterije na telefonima / tabletima
- Bolju podršku za *roaming* (mobilni uređaji)
- Više pouzdanosti
- Brže uspostavljanje veze / ponovno spajanje (engl. *faster handshake*)

# 5 Zaključak

VPN (virtualna privatna mreža) je nužnost u dobu internet cenzure i *online* praćenja, pogotovo ako se žele zaštititi podaci dok putuju mrežom.

VPN stvara privatni „tunel“, zatvorenu vezu koju ne može dekriptirati napadač ili neka druga strana, kao što su npr. pružatelji internet usluga. To znači da se odaslani podaci više ne mogu presresti i/ili ukrasti sve dok se nalaze u VPN tunelu.

VPN je važan za internetsku sigurnost, osobito za korisnike koji često putuju i koriste javne Wi-Fi mreže. Također, omogućuje da se izbjegnu cenzure vlade i koriste *online* usluge koje su ograničene na određene geografske lokacije. Veliki su koraci napravljeni prema stvaranju vrlo sigurnih VPN-ova koji pružaju privatnu i sigurnu internetsku vezu.

Neke organizacije poput velikih tvrtki, posebno tvrtke/lokacije s visokim zahtjevima sigurnosti, državne institucije, te hoteli, pa i najobičniji uređaji za kućni širokopojasni internet imaju tako podešene vatrozide da oni propuštaju samo najpoznatiji i najčešći promet poput elektroničke pošte (SMTP) i web (HTTP) te poneki tehnički protokol (DNS). Ostale protokole ne propuštaju. To znači da korisnik s takve lokacije ne može uspostaviti VPN tunel prema nekom VPN poslužitelju izvan te lokalne mreže. U takvim slučajevima je dobro da korisnik zna koji tip protokola koristi njegova VPN veza. OpenVPN i SSTP protokoli su jedni od rijetkih koji koriste SSL/TLS šifriranje, a mogu koristi i priključak (engl. *port*) 443 koji uobičajeno služi za sigurno pregledavanje weba protokolom HTTPS, te koji zato gotovo nikada nije blokiran.

Što se tiče privatnih korisnika koji se žele maksimalno zaštiti i osigurati svoju anonimnost na internetu, postoje na stotine raznih VPN usluga. Besplatna rješenja mogu biti spora, imati mali broj VPN poslužitelja koji se mogu odabrati, puna su reklama, a najvažnije, upitna im je sigurnost korisničkih podataka koje im se praktički daje na korištenje. U svakom slučaju, preporuka je da se koriste renomirane usluge, kojih danas već ima jako mnogo. Od najpoznatiji i najkorištenijih su: NordVPN, ExpressVPN i Private Internet Access, TunnerBear, Surfshark, PerfectPrivacy, PureVPN itd.

Kod poslovnih korisnika odabir VPN rješenja je malo kompleksniji zadatak, zbog individualnih potreba svake tvrtke. VPN-ovi predstavljaju izvrsno rješenje za tvrtke u smislu sigurnosti, povjerljivosti i integriteta podataka te su važna komponenta sigurnosti u organizacijama. Prilikom odabira potrebno je odlučiti hoće li to biti neki dedicirani ili ne dedicirani poslužitelj s određenim implementiranim programskim VPN rješenjem ili će to biti odvojeni hardverski uređaj. Što se tiče sigurnosti VPN sustava, brzine rada, autentifikacije korisnika, integracije u postojeću korporativnu mrežu i sl., oduku o odabiru mora donijeti svaka tvrtka za svoje potrebe i preferencije. No u svakom slučaju, smjernice odabira bi trebale biti u praćenju razvoja postojećih i novih tehnologija na području sigurnosti i efikasnosti VPN programskih rješenja i sukladno s time bi se trebala donijeti konačna odluka o izboru ili zamijeni postojećeg VPN rješenja.

# 6 Literatura

1. **Hoffman, Chris.** What Is a VPN, and Why Would I Need One? *How-To Geek.* [Mrežno] 18. lipnja 2019. [Citirano: 1. srpnja 2019.] https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/.

2. **Thomas, John i Elbirt, Adam J.** How IPsec works, why we need it, and its biggest drawbacks. *CSO Online.* [Mrežno] 6. siječnja 2004. [Citirano: 1. srpnja 2019.] https://www.csoonline.com/article/2117067/data-protection-ipsec.html.

3. **Mardisalu, Rob.** VPN Beginner's Guide. *TheBestVPN.com.* [Mrežno] 26. veljače 2019. [Citirano: 1. srpnja 2019.] https://thebestvpn.com/what-is-vpn-beginners-guide/.

4. **Golden Frog.** The Global Struggle for Internet Freedom. [Mrežno] 14. siječnja 2014. [Citirano: 1. srpnja 2019.] https://www.goldenfrog.com/blog/the-worldwide-struggle-for-internet-freedom.

5. **Chung, Jackson.** 5 Common VPN Myths and Why You Shouldn't Believe Them. [Mrežno] 27. rujna 2017. [Citirano: 1. srpnja 2019.] https://www.makeuseof.com/tag/5-common-vpn-myths-shouldnt-believe/.

6. **Cawley, Christian.** 11 Reasons Why You Should Be Using a VPN. *MakeUseOf.* [Mrežno] 19. studenog 2018. [Citirano: 1. srpnja 2019.] https://www.makeuseof.com/tag/reasons-to-use-vpn/.

7. **Nacionalni CERT.** Osnovni koncepti VPN tehnologije. [Mrežno] 2003. [Citirano: 1. srpnja 2019.] https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf.

8. —. OpenVPN. [Mrežno] 2010. [Citirano: 1. srpnja 2019.] https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-04-298.pdf.