SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Vukelićeva 4, Zagreb

Sandra Posavac

RAZVITAK I TEHNOLOŠKE ZNAČAJKE VIRTUALNIH PRIVATNIH MREŽA

ZAVRŠNI RAD

Zagreb, 2018.

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, Zagreb

ZAVRŠNI RAD

RAZVITAK I TEHNOLOŠKE ZNAČAJKE VIRTUALNIH PRIVATNIH MREŽA

DEVELOPMENT AND TECHNOLOGICAL FEATURES OF VIRTUAL PRIVATE NETWORKS

Mentor: doc. dr. sc. Ivan Grgurević

Student: Sandra Posavac
JMBAG: 0135203303

Zagreb, veljača 2018.

SAŽETAK

Virtualna privatna mreža (VPN) je tehnologija kod koje se podaci između korisnika putem Interneta prenose do lokalne mreže, a u tu svrhu koriste se posebni programi i protokoli. Situacije u kojima podaci koji putuju mrežom nisu adekvatno zaštićeni može doći do neželjenih posljedica, poput neovlaštenog pristupa podacima. Upravo iz tog razloga nastale su virtualne privatne mreže kao način da se osigura prijenos osjetljivih podataka preko javne mreže. U ovom radu detaljnije će biti analiziran razvoj i tehnološke značajke virtualnih privatnih mreža uključujući i tehnologije za prijenos podataka unutar spomenutih mreža, protokoli za tuneliranje te dvije vrste VPN-a, Remote-access VPN i Site-to-site VPN. Također, prikazan će biti i osvrt na budući razvoj virtualnih privatnih mreža.

Ključne riječi: *tehnologija, virtualne privatne mreže, prijenos podataka, tuneliranje, protokoli*

SUMMERY

The Virtual Private Network (VPN) is a tehnology where data is transmitted to the local area network by user over the Internet, and special programs and protocols are used for this purpose. Situations in which network data are not adequately protected can lead to unwanted consequences such as unauthorized access to data. For this reason, virtual private networks, were created as a way to ensure the transmission of sensitive data over the public network. In this thesis, the development and technological features of virtual private networks, including data transfer technologies within said networks, tunneling protocols, and two VPN's, Remote-access VPN's and Site-to-site VPN's, will be further analyzed. Also, an overview of the future development of virtual private networks will be presented.

Keywords: *technology, virtual private networks, data transfer, tunneling, protocols*

SADRŽAJ

1. UVOD

Danas je nezamislivo funkcionirati bez modernih tehnologija koje okružuju svakog pojedinca. Informacijska i telekomunikacijska tehnologija obuhvaća danas gotovo sva područja ljudskog života i čovjekovih aktivnosti. Zaista je nužna njihova uporaba, budući da virtualni svijet postaje okruženje u kojem se danas svaki čovjek nalazi.

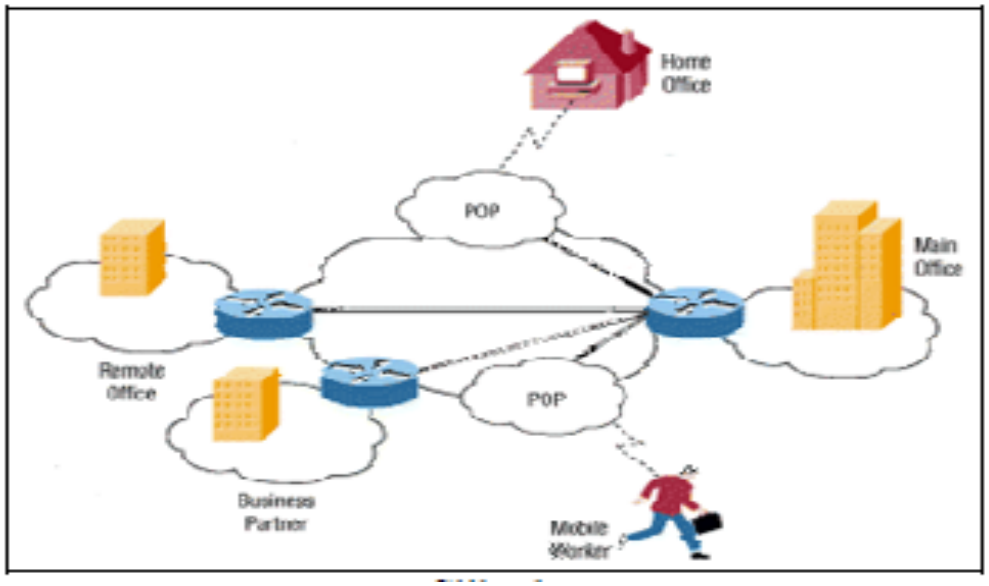
Potreba za razvojem virtualnih privatnih mreža (engl. *Virtual Private Network*, kratica: VPN) javila se zbog toga što u današnje vrijeme mnoga poduzeća dijele svoje informacije s drugim poduzećima. Radi se o tome da potreba za umrežavanjem s udaljenim lokacijama istog poduzeća i poslovnim partnerima postoji odavno, međutim, tek je od nedavno Internet postao dovoljno siguran za povezivanje putem spomenutih mreža.

Kada se govori o virtualnoj privatnoj mreži odnosno VPN-u može se reći kako predstavlja tehnologiju koja je nezaobilazna pri međusobnom spajanju udaljenih lokacija određenog poduzeća, dva različita poduzeća ili pak spajanju njegovih zaposlenika sa svoje osobne mreže na mrežu svog poduzeća. Iako većina ljudi poznaje ovaj termin, mnogi ne znaju njegovu pravu vrijednost. Stoga će kroz ovaj završni rad biti objašnjeno što je to VPN, kako funkcionira i za što se može koristiti. Dakle, cilj rada bio je prikazati razvitak i tehnološke značajke VNP-a u privatnom i poslovnom okruženju, dok je svrha rada objasniti pojam i princip na kojem djeluje spomenuta tehnologija te prikazati njezinu praktičnost primjene.

Završni rad se sastoji od osam poglavlja/teza. Uvodno poglavlje daje osnovnu sliku o radu te definira cilj i strukturu rada. U drugom poglavlju završnog rada detaljno je objašnjen pojam virtualnih privatnih mreža, a treće i četvrto poglavlje rada odnosi se na njihove podjele i vrste. Peto poglavlje je cjelina koja se dotiče teme sigurnosnih zahtjeva, dok se u šestoj objašnjavaju vrste VPN rješenja. Posljednje, sedmo poglavlje, dio je završnog rada koji se bavi analizom budućeg razvoja virtualnih privatnih mreža. U osmom poglavlju, Zaključku, sintetizirane su sve informacije prikupljene i obrađene tijekom izrade završnog rada. Na kraju rada, nalazi se Literatura koja daje uvid u sve knjige i stručne članke različitih domaćih i stranih autora, kao i internetske stranice koje se bave zadanom problematikom, a korištene su pri izradi ovog završnog rada.

2. OPĆENITO O VIRTUALNIM PRIVATNIM MREŽAMA (VPN)

Rješenje za zaštitu podatka od neovlaštenog pristupa predstavlja virtualna privatna mreža (engl. *Virtual Private Network*, kratica VPN) tehnologija. Unutar privatne i poslovne okoline moguće je svakodnevno susresti korištenje virtualne privatne mreže. One se koriste u razmjeni podataka i komunikaciji između dvije ili više točaka koje imaju potrebu za pristup privatnim podacima[4].



Slika 1. Struktura VPN-a [11]

Prilikom spomenute komunikacije dolazi i do potrebe za zaštitom, pod kojom se podrazumijeva zabrana pristupa neautoriziranim korisnicima te potvrda o tome da preneseni podaci nisu mijenjani ili poslani sa neovlaštenog izvora [4]. Dakle, njima se ostvaruje sigurna komunikacija putem internetske mreže, što znači da je njihovim korisnicima omogućeno slanje i primanje povjerljivih podataka putem javne mreže, kao u slučaju kada su njihova računala izravno povezana na istu privatnu lokalnu mrežu, iako se fizički ne nalaze u istoj mreži [7].

Ukratko rečeno, VPN se definira kao interkonekcija lokalne mreže koja koristi sigurne odnosno kriptirane načine međusobne komunikacije, najčešće putem Interneta. Drugim riječima, VPN produžuje privatnu mrežu preko javne mreže, što omogućuje korisnicima

slanje i primanje osjetljivih podataka, na način da su njihova računala izravno spojena na isti privatni LAN (lokalnu mrežu)[1], iako fizički, oni nisu u istoj mreži.

Na slici 1 prikazana je standardna struktura virtualne privatne mreže koja najčešće ima glavni LAN u sjedištu poduzeća, a ostale mreže u udaljenim podružnicama i pojedinačne korisnike. Virtualna privatna mreža u biti predstavlja privatnu mrežu koja koristi javnu mrežu za spajanje udaljenih mjesta i korisnika.

Nadalje, to je proširenje privatne mreže u kojem se korisnici mogu promatrati kao da su spojeni na istu lokalnu ili privatnu mrežu. Jednostavnije rečeno, postoji slična razina sigurnosti i povjerenja među uključenim stranama. Uloga VPN je stvaranje sigurne veze između strana koje razmjenjuju podatke, koristeći enkripciju i metode provjere korisnika kako bi osigurao zaštićenost podataka koji se prenose komunikacijskim kanalom, a to se osigurava korištenjem posebnih protokola za tuneliranje i enkripciju.

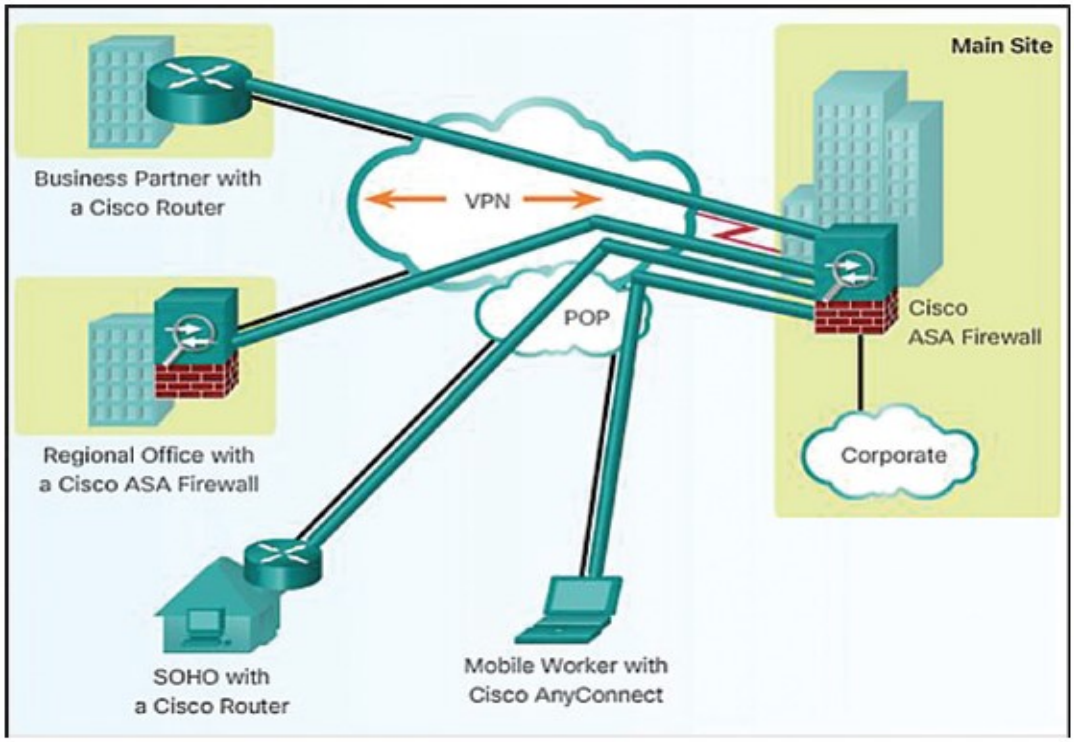
Može se reći kako je VPN jedno vrlo popularno rješenje za problem sigurne komunikacije budući da su alternativna rješenja često neusporedivo skuplja, kao npr. izgradnja vlastite fizičke komunikacijske infrastrukture (WAN)[2], a uz to je i puno fleksibilniji zbog mobilnosti korisnika [11].

Stvaranje virtualne mreže predstavlja presložen proces. Ova procedura stvaranja može se razdvojiti na tri dijela i to na:

- konfiguriranje routera, kada je potrebno konfigurirati router mreže na koji se korisnik namjerava spojiti, a iza kojeg se nalazi server. Nije potrebno konfigurirati router, ukoliko postoji s kojeg se spajamo na virtualnu privatnu mrežu, osim ako to računalo treba biti dostupno i s druge strane.
- konfiguriranje poslužitelja odnosno servera - potrebno je konfigurirati server te
- konfiguriranje klijenata - konfiguriranje udaljenih računala s kojih se želimo spajati u ured.

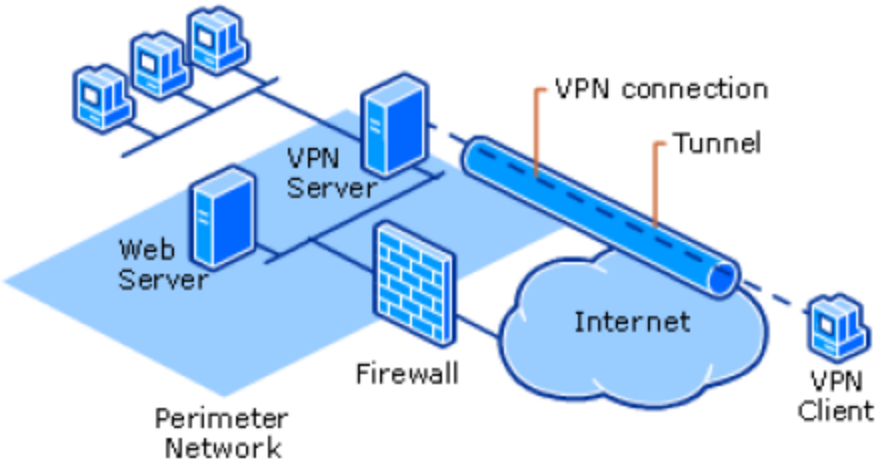
[1] Računalna mreža u kojoj su računala smještena na manjim udaljenostima. Najčešće su u cijelosti u vlasništvu i pod upravljanjem onih koji ih koriste tako da je prijenos podataka putem njih za korisnike besplatan. Značajno je i da su moguće jako velike brzine prijenosa podataka

[2] Mreža koja se proteže preko granica grada, regije ili države. Za povezivanje se koriste usmjerivači (routeri) i javne komunikacijske veze. Nisu u vlasništvu osoba ili organizacija koje ih koriste i prijenos podataka preko njih je ograničen prema brzini, količini i cijeni. Potrebno je platiti za korištenje komunikacijskih veza. U odnosu na lokalne mreže brzine su dosta ograničene.



Slika 2. VPN tuneli preko Interneta [2]

Na slici 2 može se vidjeti kako poduzeća koriste virtualne privatne mreže kako bi stvorile privatne mrežne veze odnosno tunele na način da koriste mrežu pružatelja Internet usluga. Naime, tunelom se može eliminira negativnost koju stvara udaljenost između lokacija i omogućiti korisnicima na udaljenim lokacijama spajanje na iste, a sve kako bi pristupili resursima poduzeća. Postojanje VPN tunela nije garancija da će informacije koje kroz njega prolaze ostati sigurne, pa se iz tog razloga konfiguraciji virtualnih privatnih mreža dodaju različite kriptografske metode kako bi se omogućilo sigurno povezivanje.



Slika 3. VPN sastavnice [11]

Nadalje, za konfiguriranje sigurnih VPN tunela koriste se IP Security ili IPsec radna okruženja koja preko Interneta omogućuju udaljenim lokacijama i poslovnim partnerima sigurno spajanje na centralnu lokaciju.

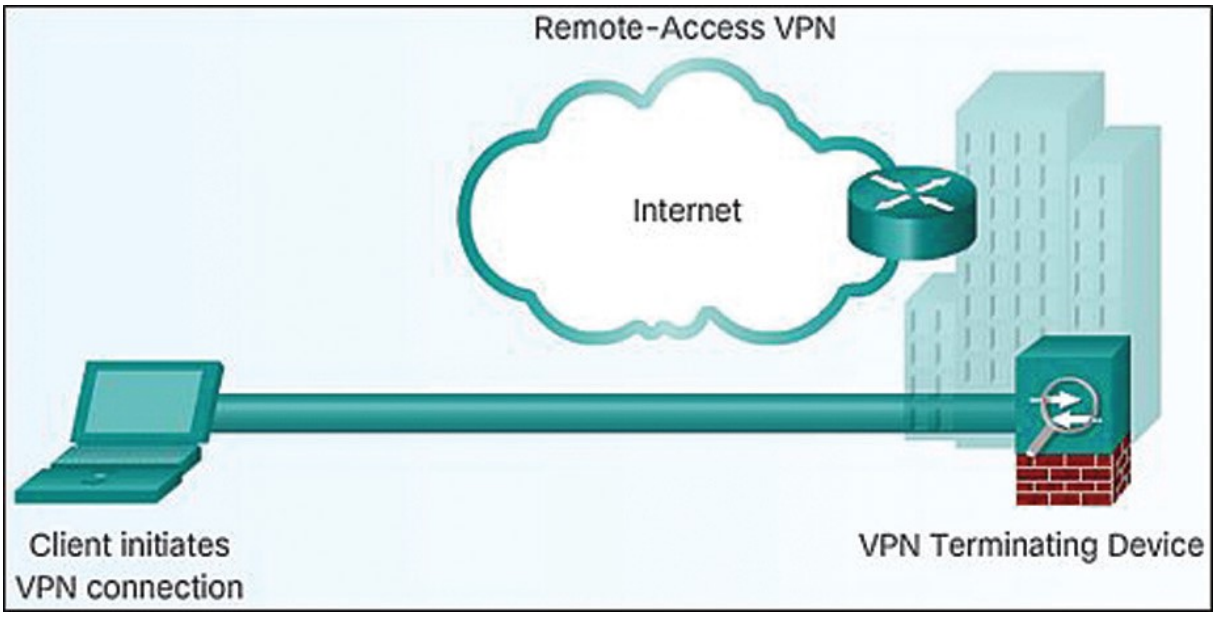
Kada se govori o spajanju djelatnika na centralnu lokaciju, može se reći kako se sve češće koristi SSL VPN koji je gotovo potpuno istisnuo IPsec jer je sa SSL VPN-om puno lakše proći kroz vatrozide[2]. Na slici 3 jasno se mogu vidjeti i osnovne sastavnice virtualnih privatnih mreža, a to su:

- privatna računalna mreža;
- veza prema Internetu;
- VPN pristupnik (engl. Gateway);
- uređaji (usmjernik, vatrozid, VPN koncentrator i drugi) te
- Programska podrška za kreiranje i upravljanje tunelima.

Jasno je kako se upravo zahvaljujući ovim navedenim sastavnicama omogućuje komunikacija preko virtualnih privatnih mreža. U situaciji kada neka od tih sastavnica nedostaje ne može biti moguć prijenos podataka i očuvanje integriteta podataka.

3. VRSTE VIRTUALNIH PRIVATNIH MREŽA

Virtualne privatne mreže predstavljaju skup zaštićenih veza između udaljenih korisničkih lokacija realiziranih unutar neke javne ili privatne mreže. Takve mreže zovemo privatnim jer resurse ovih mreža mogu koristiti samo organizacije odnosno kompanije koje su njihov vlasnik. VPN mreže su privatne s pozicije usmjeravanja i plana adresiranja. Primjenom *ATM (*engl. *Asynchronous Transfer Mode)*[3] tehnologije, koja je ponuđena za izgradnju okosnice Interneta omogućen je prijenos podataka preko jedne mreže poštujući pri tome sve potrebne protokole.



Slika 4. Remote-access VPN [2]

Ipak problem preslikavanja IP protokola u ATM je kompleksan, te uslijed svoje složenosti i problema skalabilnosti ne predstavlja pravo rješenje. Unutar Interneta, organizacije zapravo kreiraju svoju virtualnu infrastrukturu koja povezuje različite udaljene lokacije. Umjesto da organizacija za spajanje udaljenih lokacija koristi unajmljenu liniju, pomoću VPN veze kreira se virtualna veza koja Internetom usmjerava podatke od ishodišta do odredišta.

[3] *Paketska tehnika komutiranja, multipleksiranja i prijenosa koja se koristi paketima (tzv. ćelije) male i konstantne duljine da bi se prenijela informacija u B-ISDN mreži. Kratke ćelije koje putuju vrlo velikim brzinama nude mreži fleksibilnost i čine je dobro iskorištenom.*

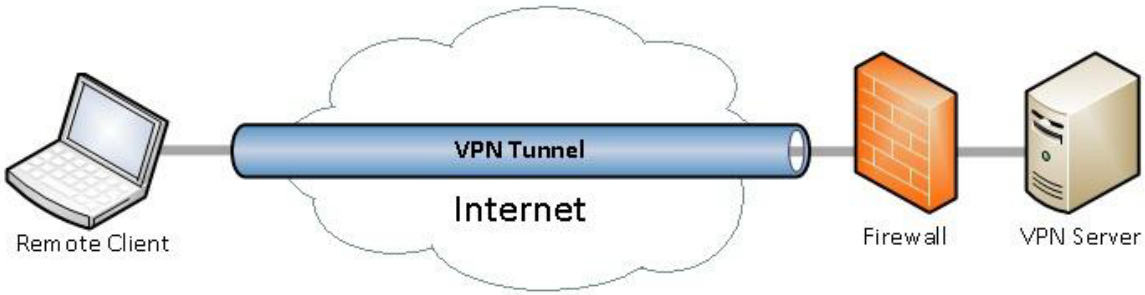
Postoje dvije vrste VPN-a, a to su *Site-to-site VPN* i *Remote-access VPN. Site-to site VPN* spaja dvije ili više mreža u jednu mrežu. Te mreže koriste sofisticirane načine kriptiranja kako bi zaštitile promet od hakera. Veza između nekog ureda odvojenog od glavne lokacije je jedan od primjera *Site-to-site VPN-a.* Korisnici na tim lokacijama nisu svjesni njihovog pristupanja resursima na tim lokacijama [2].

S druge strane, *Remote-access VPN* dopušta korisniku s računalom spajanje na privatnu mrežu. Na primjer, korisnik ima službeno prijenosno računalo s kojim se spaja putem VPN softvera na mrežu svoje kompanije. Tada korisnik može pristupiti file serverima, e-mailovima ili spojiti se na svoje računalo [12].

4. PODJELA VPN TEHNOLOGIJE

Za razliku od privatnih mreža koje koriste iznajmljene linije za slanje podataka, virtualna privatna mreža preko javne mreže stvara sigurni kanal između dviju krajnjih točki. Bilo da se radi o uvezivanju samo jednog računala na udaljenu mrežu ili da se putem VPN-a povezuju dvije mreže na udaljenim lokacijama, komunikacija između subjekata ove strukture zaštićena je enkripcijom čije parametre dogovaraju obje strane. Izbor enkripcijskog algoritma i dužine ključa je od suštinskog značaja za sigurnost uspostavljene komunikacije, i tek u slučaju treće primjene, gdje komunikacija između mreža nije javna, enkripcija igra nešto manju ulogu.

Tuneliranje je tehnika prijenosa podataka namijenjenih određenoj mreži preko druge mreže. Implementira se pomoću protokola koji enkapsulira okvir u posebno oblikovano zaglavlje. Enkapsulirani podaci se šalju između krajnjih točaka tunela kroz koji isti prolaze pomoću mreže koja predstavlja medij za prijenos. U situaciji kada okvir dođe do svog odredišta, iz njega izlaze korisni podaci koji se ponovno šalju na ciljno odredište [11].



Slika 5. Prikaz VPN tunela [11]

Uspostava veze sa slike 5 može se objasniti kroz tri koraka, a to su da se najprije udaljeni korisnik spaja na Internet preko svog pružatelja Internet usluga, nakon toga korisnik pokreće zahtjev za spajanjem na VPN poslužitelj tvrtke, dok VPN poslužitelj provjerava korisničko ime i lozinku te mu dozvoljava daljnji rad. Posljednji korak je kada se veza uspostavi udaljeni korisnik može komunicirati ili preuzimati podatke s lokalnom mrežom kao da je svojim računalom izravno spojen na istu.

Ova tehnika omogućuje enkapsulaciju paketa jedne vrste protokola unutar jednog bloka podataka različitog protokola. Na primjer, VPN koristi PPTP protokol za enkapsulaciju IP paketa preko javne mreže kao što je Internet. Neki od protokola za tuneliranje su: PPTP, L2F, L2TP i GRE, a zbog niske razine sigurnosti često se koriste zajedno sa IPsecom [12].

Na tržištu je danas dostupan velik broj komercijanih rješenja koja omogućuju VPN pristup, a najpoznatija su ona velikih proizvođača kao što su Cisco, CheckPoint, NetScreen, i dr. Postoji i nekoliko open-source projekata u ovome smjeru, ali su ona daleko manje popularna u odnosu na komercijalne proizvode. Osnovni razlog tome je činjenica što komercijalne tvrtke uz svoje proizvode nude kompletnu uslugu instalacije, održavanja i administracije sustava, što je posebno važno kod velikih tvrtki gdje uređaji moraju biti raspoloživi u svakom trenutku.

Besplatna rješenja za sada ovakvu podršku ne nude, što im je osnovno ograničenje za širu primjenu. Jedan od najvećih nedostataka komercijalnih VPN proizvoda je njihova prilično visoka cijena (do nekoliko tisuća američkih dolara), što predstavlja ozbiljan problem za manje tvrtke, koje si tako velike troškove ne mogu priuštiti.

4.1. IPSec

IPsec protokol (engl. *Internet Protocol Security*) je standard i skup protokola koji obuhvaćaju mehanizme za zaštitu prometa na razini trećeg sloja OSI mrežnog modela. Kako bi osigurao autentikaciju, integritet i pouzdanost komunikacije IPsec koristi tri različita protokola, AH, ESP i IKEv2 [3]. *Authentification Header* (AH) osigurava integritet, autentifikaciju i neporecivost. Opcionalno može poslužiti za zaštitu od napada ponavljanja poruke. Definiran je u RFC 2402. Protokol ima vlastito zaglavlje koje se umeće između IP zaglavlja i IP podataka. U nastavku slijedi obrazloženje polja u zaglavlju.

Kroz rad IPSec koristi sljedeće protokole i standarde:

- Diffie-Hellman metodu za razmjenu ključeva - glavni ključ koji se koristi za generiranje regularnih ključeva se ne prenosi istim medijem kao i ostali podaci za spajanje
- DES ili 3DES standard za šifriranje podataka - enkripcijski podatkovni standard
- HMAC - kombinirano orijentirana autentifikacija koda
- Digitalna uvjerenja izdana od strane odgovarajućeg autoriteta

IPSec protokol podržava dva načina rada i to prijenos podataka i IPSec tuneliranje podataka. Kod prijenosa podataka šifriraju se samo aplikacijska zaglavlja dok su IP zaglavlja dostupna za pregled routerima na mreži koji su zaslužni za usmjerivanje prometa što predstavlja potencijalni rizik gdje napadač može pratiti izvor i destinaciju paketa.

IPSec tuneliranje je poseban način tuneliranja prometa koji implementira dodatnu zaštitu na način da obje strane (klijent i poslužitelj) konfiguriraju IPSec mod kod tuneliranja prometa. Kod prijenosa prometa koriste se dogovoreni mehanizmi za enkapsulaciju i šifriranje gdje se za razliku od metode prijenosa podataka enkriptiraju kompletni IP paketi što omogućava siguran prijenos neovisno da li se koristi javna ili privatna mreža.

4.1.1. Authentification Header (AH)

Next header je vrsta dodatnog zaglavlja, pokazuje koji je protokol višeg sloja zaštićen. Vrijednost se uzima iz popisa brojeva IP protokola. *Payload lenght* označava duljinu AH zaglavlja u 32-bitnim riječima, umanjenu za vrijednost dva. Iako se veličina mjeri u jedinicama od 4 okteta17, duljina ovog zaglavlja mora biti višekratnik od 8 okteta ako se nosi u IPv6 paketu. *Reserved* je polje rezervirano za buduću upotrebu. Do tad mora biti ispunjeno nulama.

Security parameter index je proizvoljna vrijednost koja se koristi zajedno sa odredišnom IP adresom za identifikaciju sigurnosnih parametara *Security Association* (SA). Najjednostavnije se definira kao skup parametara i ključeva za kriptiranje i autentifikaciju toka podataka. Potrebna su dva SA za dvosmjerni prijenos. *Sequence number* je broj koji se monotono i striktno povećava za jedan (inkrementira za 1 za svaki poslani paket). Služi za prevenciju replay napada.

Kada je uključena detekcija replay napada, jednom iskorišten sekvencijski broj ne smije se ponoviti tj. prvo se mora ugovoriti nova SA kada se sekvencijalni broj inkrementira do svoje maksimalne vrijednosti. Tada se vrijednost ponovno vraća na 1.

Authentification data polje se koristi za autentifikaciju paketa. Varijabilne je duljine. Polje sadrži vrijednost provjere autentičnosti i integriteta poruke (engl. *Integrity Check Value*, kratica: ICV). Može sadržavati padding za popunjavanje polja na 8-oktetnu granicu za IPv6 ili granicu od četiri okteta za IPv4 [20].

4.1.2. *Encapsulated Security Payload* (ESP)

Encapsulated Security Payload uz integritet, autentifikaciju i neporecivost osigurava i povjerljivost podataka (engl. payload) koji se prenose. Definiran je u RFC 2406. Protokol ima vlastito zaglavlje koje se umeće iza IP zaglavlja. Enkapsulira sve podatke višeg sloja te dodaje završni slog u kojem mogu biti sadržani autentifikacijski podaci.

U ESP datagramu nalaze se Security parameter index odnosno polje isto kao i kod AH. Proizvoljne je vrijednosti i služi za identifikaciju SA. *Sequence number* je isto polje kao i kod AH. Služi za zaštitu od replay napada. *Payload data* je zaštićeni sadržaj originalnog IP paketa, uključuje i podatke koje se koriste za zaštitu. *Next header* polje pokazuje vrste podataka koji se štite. *Padding* je ispuna za enkripciju. Proširuje payload na duljinu koju zahtjeva kriptografski algoritam za šifriranje odnosno blokovi fiksne duljine koje koristi algoritam. Također, služi za poravnavanje sa sljedećim poljem odnosno omogućava da se dobije zahtijevana duljina zaglavlja. *Pad lenght* je duljina ispune u oktetima. *Next header* je polje isto kao i kod AH. Vrijednost se uzima iz liste brojeva IP protokola. *Authetification data* je isto polje kao i u AH. Sadrži ICV.

ESP funkcionira na dva načina, a može biti određen potrebnom funkcionalnošću i sposobnošću metode IPSec u cilju prepoznavanja računala ili usmjerivača. Transportni modalitet u kojem se podaci u paketu korisničkih podataka enkriptiraju, ali zaglavlje ostaje nepromijenjeno. Namijenjen je enkriptiranju podataka između dva računala koji poznaju IPSec i sposobni su dekriptirati paket korisničkih podataka direktno kao kod Microsoft Windows sustava [9].

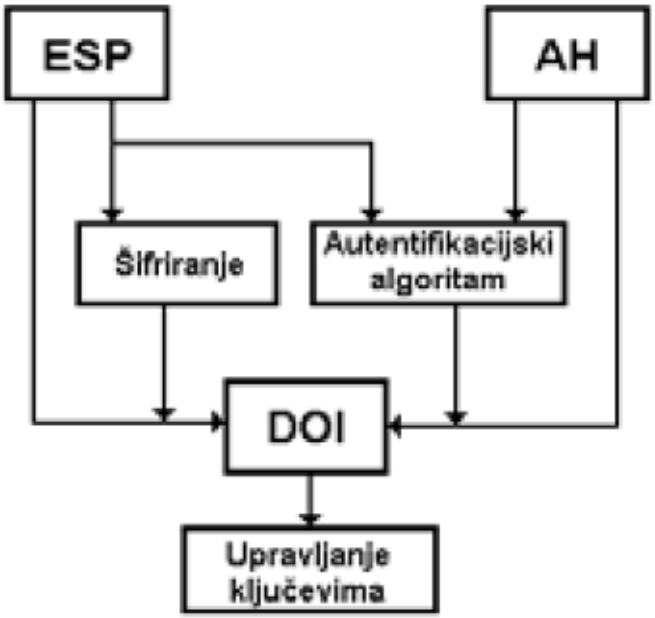
Nadalje, tunelski modalitet u kojem je cijeli originalni paket enkriptiran i postaje paket korisničkih podataka novog paketa koji se onda prenosi između usmjerivača koji poznaju IPSec. Tunelski modalitet omogućuje ruterima, koji poznaju IPSec, enkapsulaciju i enkriptiranje mrežnog prometa od računala koja ne poznaju IPSec, preko neosigurane mreže i onda ga dekriptiraju za upotrebu na ciljanoj mreži drugih računala koje ne poznaju IPSec. U Windowsu se nalazi isključivo zbog interoperativnosti s trećom stranom kada se Windows programi upotrebljavaju kao usmjerivači [9].

4.1.3. *Internal Key Exchange* (IKE)

Još jedan protokol iz seta IPsec protokola je *Internal Key Exchange,* odnosno IKE protokol koji obavlja obostranu autentifikaciju korisnika te uspostavlja *Security Association* (SA) vezu. Uspostava SA veze podrazumijeva izračunavanje keying materijala te dogovaranje oko skupa algoritama i drugih parametara koji će štititi SA. Protokol radi tako da inicijator veze nudi prihvatljive parametre za zaštitu SA. Ako ih druga strana prihvati ostvaruje se SA veza [9].

Osim što proširuje IPv4 koji se trenutno koristi, dolazi i kao integralni dio IPv6 protokola. S obzirom na to da se integrira s IP protokolom, IPSec implementira sigurnu mrežnu komunikaciju na trećem, odnosno mrežnom internet sloju, ukoliko se promatra TCP/IP. Isto tako, sigurnost je moguće implementirati i u drugim slojevima, od fizičkog do aplikacijskog sloja, a svaka od implementacija ima svoje prednosti i nedostatke [11].

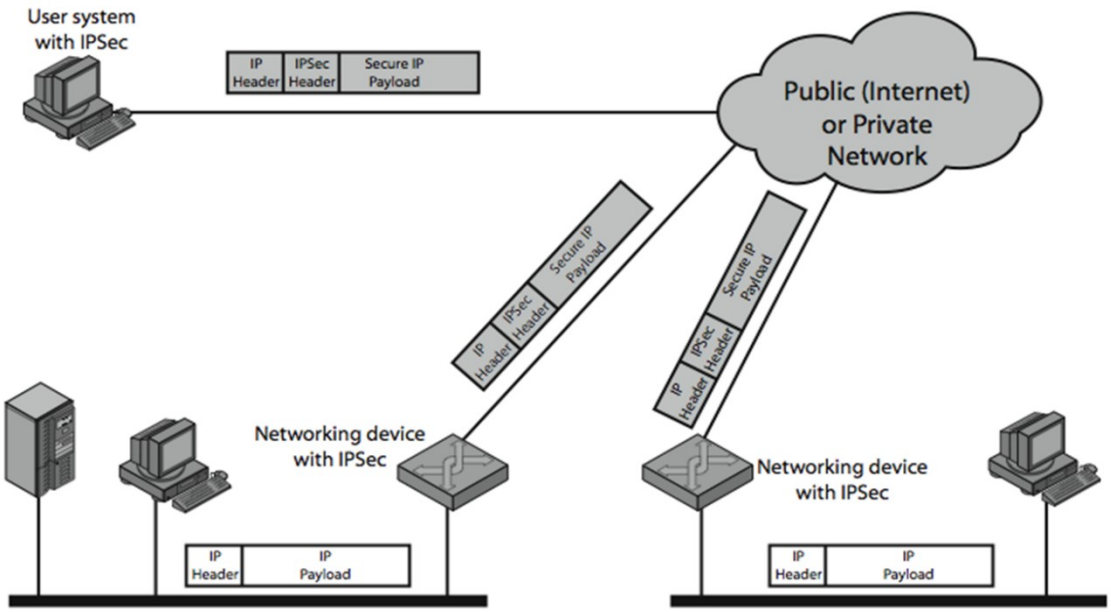
Komponente IPSec-a prikazane su na slici 7. IPSec definira metode kako specificirati promet koji će se zaštiti, način na koji će biti zaštićeni i kome je namijenjen. Ranije su pristupi bili na nivou aplikacija modela komunikacije. Za IPsec se kaže kako je posebno koristan za implementaciju virtualne privatne mreže i za daljinski pristup korisnika preko internet veze na privatnim mrežama.



Slika 6. Komponente IPSec-a [1]

Iz slike je vidljivo kako se IPSec struktura sastoji od tri glavne komponente. To su AH (Authentication Header) i ESP (Encapsulated) protokoli te upravljanje ključevima. Autentifikacijska zaglavlja se koristi za autentifikaciju i integritet, bez mogućnosti šifriranja. Drugim riječima, netko treći može pročitati, ali ne može mijenjati poslane podatke. Nadalje, ESP osigurava iste mogućnosti, ali dodaje i mehanizam za šifriranje. Sigurni ključ poznaju isključivo pošiljatelj i primatelj tako da ukoliko su autentifikacijski podaci valjani, primatelj može biti siguran da je podatak stigao od strane pošiljatelja te da se tijekom prijenosa nije promijenio.

U IPSec-u se mogu koristiti razni algoritmi šifriranja, ključevi različite duljine i drugo, stoga je potreban dogovor između pošiljatelja i primatelja o standardima koje će koristiti. Za to je zadužen DOI (Domain of Interpretation), čija je velika prednost to što mjere sigurnosti ne zahtijevaju promijene u određenim računalima korisnika. DOI se koristi u tuneliranju i u transportnom modu koji osigurava sigurnu vezu između dvije krajnje točke, budući da smanjuje teret IP-a, dok u sustavu tunela smanjuje cijeli IP paket kako bi se realizirala sigurna virtualna veza.



Slika 7. Primjer IPsec-a [17]

Pomoću mehanizma tzv. klizećih prozora, IPsec pruža zaštitu od napada, što znači da se svakom paketu pridružuje određeni redni broj i paket se dostavlja samo u slučaju da se njegov redni broj nalazi u promatranom prozoru ili je noviji. Svi stariji paketi se automatski odbacuju.

Navedeni postupak štiti od napada snimanjem i ponavljanjem u kojima napadač snimljene originalne pakete pokušava ponovno poslati. Krećući se slijeva na desno, prozor „klizi“ kako se pojedini bajt pošalje i potvrdi njegov prijem.

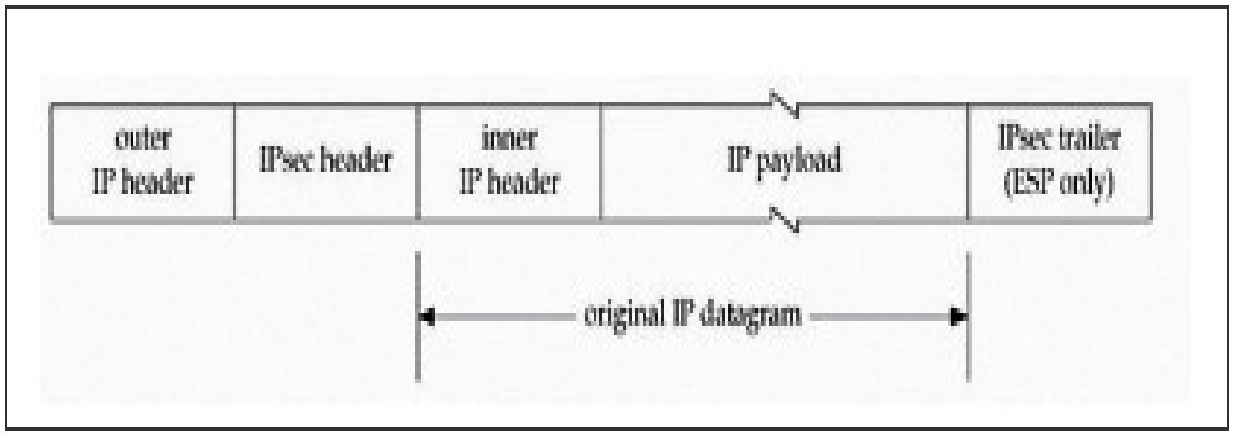
IPsec omogućuje sigurnu komunikaciju preko LAN mreža, privatnih i javnih WAN mreža, i preko Interneta. Isto uključuje:

- sigurno povezivanje ureda nekog poduzeća matičnim uredom preko Interneta

spajanje korisnik na siguran način na lokalnu mrežu poduzeća i to preko javnog Interneta;

- sigurno povezivanje partnerskih organizacija i poduzeća putem Interneta;
- povećavanje sigurnosti postojećih klijent-server aplikacija i usluga koje već imaju ugrađene određene sigurnosne mehanizme (Slika 7).

Prednost ovog načina rada jest što se ne moraju definirati nove mreže na mrežnoj opremi i osigurati komunikacija s drugim IP adresama. Ovaj način rada pruža zaštitu podataka do krajnjih točaka komunikacijskog kanala. Zaštita odnosno kriptiranje se obavlja na podacima koji se prenose. Nadalje, u tunelnom načinu rada originalni IP paket je zaštićen unutar drugog paketa sa IPSec zaglavljem koje sadrži IP adrese graničnih uređaja mreža koje se povezuju (Slika 8).

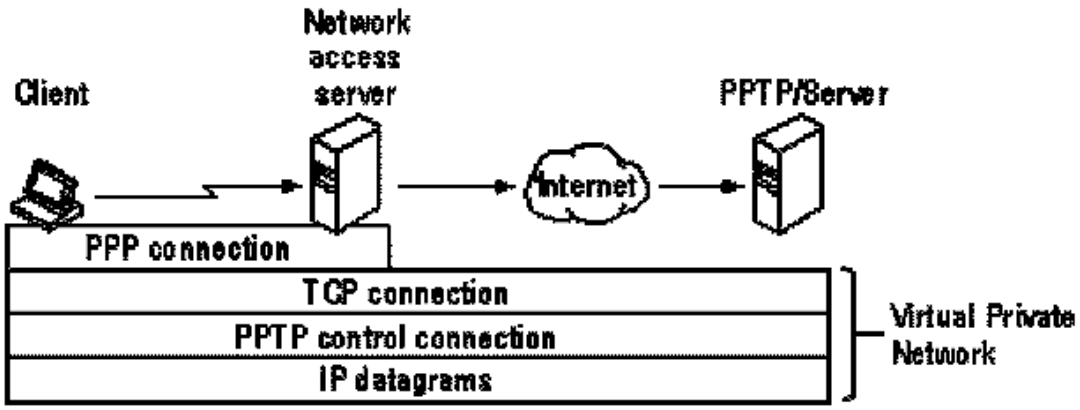


Slika 8. Enkapsulacija paketa u tunel načinu prijenosa [16]

Kroz privremeni tunel koristeći javnu ili privatnu mrežu, putuje originalan paket. Tunelni način rada koristi se u situacijama kada se želi kroz javno dostupnu mrežu spojiti dvije odvojene privatne mreže. Prednost ovog načina rada jest što neautorizirana osoba ne može vidjeti stvarne IP adrese, te se može udaljeni ured prikazat kao da je spojen lokalno u centralu (kao da je na istom LAN-u).

4.2. PPTP (*Point-to-Point Tunneling Protocol*)

Mrežni protokol koji omogućava siguran prijenos podataka s udaljenog klijenta na privatnu mrežu preko Interneta ili neke druge mreže koja se temelji na TCP/IP protokolu (engl. *Transmission Control Protocol/Internet protocol*) naziva se PPTP protokol. TCP protokol koristi se za stvaranje i održavanje tunela, dok se za tuneliranje PPP paketa koristi GRE enkapsulacija (engl. *Generic Routing Encapsulation*). Ovaj je protokol proširenje mrežnog protokola PPP (engl. *Point-to-Point Protocol*) čime se omogućuje uspostava VPN veze.



Slika 9. Point-to-Point Tunneling Protocol [16]

Također, PPTP osigurava autentifikaciju i kompresiju, međutim, slabija strana mu je upravo sigurnost, što se manifestira kroz sigurnosne propuste koje napadači vrlo često koriste za otkrivanje pristupnih lozinki i tako pristup privatnoj mreži.

Autentifikacija se ostvaruje korištenjem protokola MSCHAP[4], MS-CHAPv2, a enkripcija preko RC-4 ili MPPE algoritma. Kada PPTP poslužitelj primi paket s javne mreže, on ga dalje šalje privatnom mrežom do odredišnog računala. To obavlja obradom enkapsuliranog paketa u kojem je definirana adresa odredišta [12].

Na slici 9 prikazan je VPN s PPTP poslužiteljem na privatnom LAN-u. Radi se o tome da tuneliranje predstavlja proces slanja paketa na računalo u privatnoj mreži usmjeravajući ih preko neke druge mreže, kao npr. Interneta. Drugi mrežni usmjerivači ne mogu pristupiti računalu koje je u privatnoj mreži. Međutim, tuneliranje omogućuje mreži za usmjeravanje prijenos paketa na intermedijalno računalo, kao što je PPTP poslužitelj, koji je povezan s mrežom usmjeravanja i privatnom mrežom. PPTP klijent i PPTP poslužitelj koriste tuneliranje za sigurno usmjeravanje paketa na računalo u privatnoj mreži korištenjem usmjerivača koji znaju samo adresu posredničkog poslužitelja privatne mreže.

[4] Upotrebljava se pri autentikaciji korisnika koji se VPN-om spajaju izvana preko Microsoftova PPTP protokola (Point to Point Tunneling Protocol). Koristi se i pri bežičnoj WPA2 autentikaciji.

U situaciji kada PPTP poslužitelj primi paket iz mreže za usmjeravanje, šalje ga preko privatne mreže na odredišno računalo. PPTP poslužitelj to čini na način da obrađuje PPTP paket kako bi dobio ime ili adresu računala privatne mreže u enkapsuliranom PPP paketu. Inkapsulirani PPP paket može sadržavati podatke s više protokola kao što su TCP / IP, IPX[5] ili NetBEUI protokoli.[6] Budući da je PPTP poslužitelj konfiguriran da komunicira preko privatne mreže pomoću privatnih mrežnih protokola, on može čitati pakete s više protokola.

4.3. L2F (*Layer 2 Forwarding*)

Layer 2 Forwarding (L2F) predstavlja protokol za tuneliranje razvijen od tvrtke *Cisco*, a vrlo je sličan PPTP protokolu. Naime, ovaj protokol djeluje na mrežnom sloju, pri čemu je neovisan o prijenosnom mediju. Također, njime je omogućen i dial-up pristup poslužiteljima. Njegova osnovna funkcija je osigurati mehanizam tuneliranja za okvire prijenosnog sloja ili protokole viših slojeva.

Preko WAN spojeva do L2F poslužitelja se prenose enkapsulirani paketi gdje se obavlja inverzna enkapsulacija te prosljeđivanje u mrežu. Ovaj protokol ne definira klijente i funkcionira samo u definiranim tunelima. Nakon toga, Cisco i Microsoft odlučili su spojiti svoja dva protokola u jedan, pod nazivom *Layer 2 Tunneling Protocol* (L2TP), a o kojem će više biti rečeno u narednoj podcjelini [10].

4.4. L2TP (*Layer 2 Tunneling Protocol*)

L2TP (Layer 2 Tunneling Protocol) je standard organizacije posvećene razvoju i promoviranju internetskih standarda i protokola IETF (engl. *Internet Engineer Task Force*) koji je nastao kombinacijom funkcionalnosti PPTP i L2F protokola, karakterističnog za Cisco uređaje. Ovaj protokol radi na drugom sloju OSI modela i koristi se kao protokol tuneliranja za IP, X.25, FrameRelay ili ATM mreže.

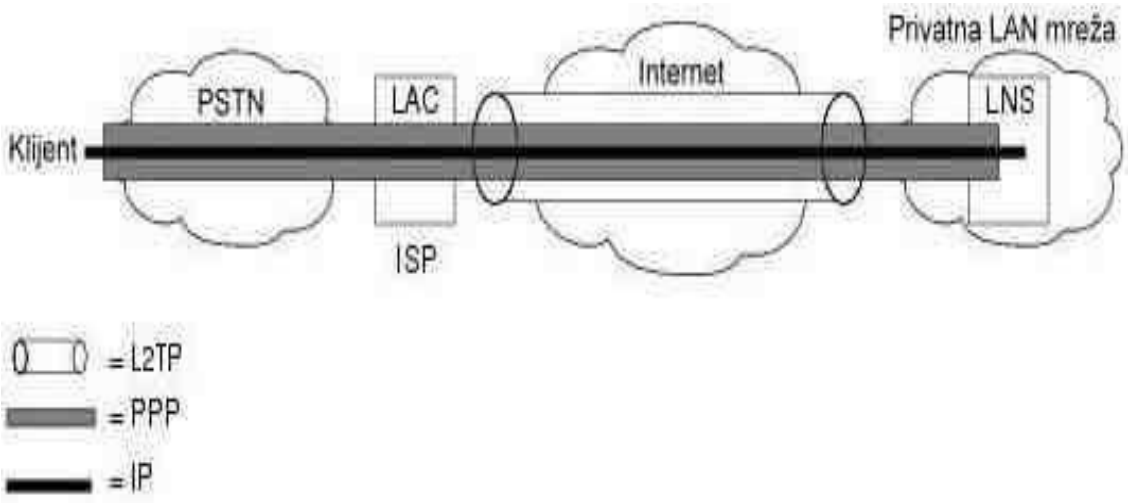
[5] Danas se rijetko koristi zbog brzog širenja interneta i predstavljanja univerzalnog TCP/IP protokola. Računala i mreže mogu izvršavati više mrežnih protokola tako da sve IPX stranice se mogu izvršavati i u TCP/IP-u.
[6] Protokol koji je napravio IBM 1985. godine namijenjen za komuniciranje u lokalnoj mreži

Funkcionira na principu rada na način da se osnovnom paketu koji se šalje mrežom dodaje L2TP zaglavlje te se na njega dodaje UDP[7] zaglavlje. Na kraju, paket se enkapsulira dodavanjem IP zaglavlja koje sadrži IP adrese klijenta i poslužitelja [10].

Protokol L2TP koristi slabu autentikaciju i ne omogućuje enkripciju te se mora koristi u kombinaciji s IPsec protokolom. Kombinacija L2TP-a i IPsec protokola prikazuje se kao L2TP/Ipsec standard koji je definiran dokumentom RFC 3193.

Uspostava veze odvija se na sljedeći način:

- pregovaranje o *Ipsec Security Association* (SA), komunikaciji preko UDP priključka. Autentikacija se odvija korištenjem certifikata ili zajedničkog ključa. Pritom obje strane koriste zajedničku lozinku, javni ključ ili X.509 certifikat;
- uspostava *Encapsulating Security Payload* (ESP) komunikacije čime se uspostavlja siguran kanal koji koristi IPsec enkripciju;
  pregovaranje i uspostava L2TP veze između klijenta i poslužitelja;
  razmjena informacija i podataka [10].



Slika 10. Način prijenosa podataka korištenjem L2TP protokola [10]

[7] *Protokol koji se nalazi u dijelu transportne razine OSI modela, te je uz TCP jedan od temeljnih Internet protokola. UDP omogućuje slanje kratkih poruka između aplikacija na umreženim računalima. U odnosu na mrežnu razinu OSI modela, ovaj dodaje samo funkcije multipleksiranja i provjeravanja pogreške prilikom prenošenja podataka, a nema mogućnost provjere primitka poruke jer ne čuva informaciju o stanju veze*

Princip rada je takav da se osnovnom paketu (koji se šalje mrežom) dodaje L2TP zaglavlje te se na njega dodaje UDP zaglavlje. Na kraju, paket se enkapsulira dodavanjem IP zaglavlja koje sadrži IP adrese klijenta i poslužitelja [10]. Na slici 10 prikazan je način prijenosa podataka korištenjem L2TP protokola.

4.5. SSL (*Secure Sockets Layer*) protokol

Transportni protokol koji je razvijen kako bi se omogućila sigurna i zaštićena komunikacija sugovornika preko javne mreže naziva se SSL protokol. Njegova prednosti je ta što nije potrebna instalacija posebnih programa za spajanje na poslužitelj već se komunikacija odvija preko web preglednika na način da je pogodan za povremene korisnike (udaljeni djelatnici, poslovni partneri, itd.).

Ovo je najšire korišteni kriptografski protokol kojeg je 1999. naslijedio TLS. Osnova protokola je ostala ista. Osigurava privatnost podataka i njihovu cjelovitost. Enkripcija se provodi pomoću algoritama simetričnog ključa pri čemu obje strane moraju posjedovati isti tajni ključ. To onemogućuje interpretaciju podataka trećim stranama koje nemaju ključ, čak niti u slučajevima kada oni te podatke mogu čitati. TLS se sastoji od dva sloja - sloja rukovanja i sloja zapisa. Sloj rukovanja je zadužen za međusobnu autentikaciju servera i klijenta, te dogovor o ključu i enkripciji koja će biti korištena. Ta interakcija se odvija prije izmjene bilo kakvih podataka [20].

Sloj zapisa se bavi sigurnošću podataka koristeći poznate podatke iz sloja rukovanja. On enkriptira i dekriptira podatke, osigurava cjelovitost (integritet) podataka, te ih štiti od neovlaštenog čitanja. Danas ovi protokoli, a pretežito TLS, imaju široku primjenu u području sigurnog prijenosa podataka, sigurnom pristupu web stranicama i sl. Tako je protokol HTTPS, koji je poznatiji kao sigurna verzija HTTP protokola, zapravo kombinacija protokola HTTP i SSL/TLS.

Za uspostavu zaštićenog prijenosa podataka ovaj protokol zahtijeva minimalno identifikaciju poslužitelja. Nakon što je identifikacija obavljena, klijent i poslužitelj mogu krenuti sa razmjenom kriptiranih poruka štiteći tako podatke od prisluškivanja i neovlaštenih izmjena. Za svoj rad SSL koristi dva protokola. Jedan je *SSL Handsake* koji omogućuje klijentu i poslužitelju međusobnu identifikaciju.

Identitet strana koje sudjeluju u komunikaciji osigurava se primjenom digitalnog potpisa i javnih ključeva. Koriste se algoritmi RSA i DSS. Kada SSL klijent i SSL poslužitelj prvi puta započnu komunikaciju, dogovaraju se o inačici protokola, algoritmu za kompresiju i odabiru algoritama za simetrično kriptiranje nakon čega mogu započeti s razmjenom podataka. Još jedna prednost korištenja SSL algoritma leži u činjenici kako je veza pouzdana jer se provjerava integritet datoteka ili poruke prilikom prijenosa između pošiljatelja i primatelja. U tu se svrhu koriste algoritmi SHA i MD5 [20].

Nadalje, drugi protokol je *SSL Record*, a zadužen je za kriptiranje i prijenos poruka. Radi na principu da primanja podataka od aplikacijskog sloja u blokovima proizvoljnih duljina. Same podatke ne interpretira, već ih fragmentira u blokove fiksne dužine (veličine 214 bajtova ili manje), koje zaštiti i šalje sugovorniku, gdje se odvija obrnuti proces. Na taj način više klijentskih poruka može biti spojeno u jedan fragment ili jedna poruka podijeljena u više fragmenata.

Isti se podaci zatim komprimiraju i zaštićuju korištenjem algoritama za simetrično kriptiranje – DES i RC4. Tako se, u odnosu na asimetrične ključeve, postiže veća brzina rada, iako ona nije toliko bitna kada se poslužuje jedan korisnički zahtjev, međutim, ukoliko se radi o velikom broju zahtjeva koji se poslužuju paralelno, bolje je koristiti simetrični sustav [20].

4.6. *Secure Socket Tunneling Protocol* (SSTP)

Secure Socket Tunneling Protocol (SSTP) je tunelski protokol koji omogućuje prijenos PPP ili L2TP prometa kroz SSL/TLS kanal. Ovaj se protokol smatra jako sigurnim zbog jake enkripcije (zaštitna sekvenca duljine 2048 bita). Korištenjem SSL/TLS protokola na TCP portu 443, uspijeva zaobići gotovo sve vatrozide i proxy servere.

Uz to, koristi se HTTPS protokolom[8] koji je danas u širokoj upotrebi, pa ga zbog toga većina vatrozida i proxy servera ne blokira. Vlasništvo je Microsoft-a, i kao takav nije dostupan na konkurentskim operativnim sustavima, no ima ugrađenu podršku na Windows operacijskim sustavima pa je samim time poprilično zastupljen u praksi.

HTTP je protokol s ugrađenom zaštitom u obliku kriptografskih protokola TLS/SSL koji osiguravaju kriptiranje podataka i sigurnu komunikaciju između pretraživača i servera. Kako bi ga stranica mogla koristiti mora imati SSL certifikat koji potvrđuje da su podaci na stranici sigurni. Za prelazak na HTTPS nužno je kupiti SSL certifikat i instalirati ga na poslužitelju

4.7. *Secure Sockets Layer/Transport Layer Security* (SSL/TLS)

Secure Sockets Layer je najšire korišteni kriptografski protokol kojeg je 1999. naslijedio TLS. Osnova protokola je ostala ista. Ovi protokoli osiguravaju privatnost podataka i njihovu cjelovitost. Enkripcija se provodi pomoću algoritama simetričnog ključa pri čemu obje strane moraju posjedovati isti tajni ključ. To onemogućuje interpretaciju podataka trećim stranama koje nemaju ključ, čak niti u slučajevima kada oni te podatke mogu čitati. TLS se sastoji od dva sloja - sloja rukovanja i sloja zapisa.

Sloj rukovanja je zadužen za međusobnu autentikaciju servera i klijenta, te dogovor o ključu i enkripciji koja će biti korištena. Ta interakcija se odvija prije izmjene bilo kakvih podataka [20]. Sloj zapisa se bavi sigurnošću podataka koristeći poznate podatke iz sloja rukovanja. On enkriptira i dekriptira podatke, osigurava cjelovitost (integritet) podataka, te ih štiti od neovlaštenog čitanja.

Danas ovi protokoli, a pretežito TLS, imaju široku primjenu u području sigurnog prijenosa podataka, sigurnom pristupu web stranicama i slično. Tako je protokol HTTPS, koji je poznatiji kao sigurna verzija HTTP protokola, zapravo kombinacija protokola HTTP i SSL/TLS.

5. SIGURNOSNI ZAHTJEVI VIRTUALNIH PRIVATNIH MREŽA

U tehnološkom smislu, na temelju proučavanja zaštitne funkcije sigurnosti umreženih računala, istraživanja su pokazala da razvojem tehničkih mogućnosti računala postoji ujedno i potreba da se ta ista istovremeno i zaštite na najbolji, najsigurniji i najsuvremeniji tehnički način. Kao najveći i najčešći oblik rizika kod umreženih računala pod operativnim sustavom Windows predstavljaju hakeri koji ne prezaju ni pred čim i za koje ne postoje nikakve granice da bi ostvarili svoje zamišljene ili slučajne i često sulude ideje samo da bi poremetili normalno funkcioniranje računala, ne razmišljajući pri tome koju i kakvu materijalnu i nematerijalnu štetu su spremni učiniti [6].

Govoreći sa psihološkog aspekta, programeri su predvidjeli mogućnost rizika za sigurnost rada umreženih računala. Stoga su programirali i razvili poseban sustav sigurnosti usmjeravanja i daljinskog pristupa (engl. *Routing and Remote Access*, kratica: RRAS), te nekoliko vrsta i metoda napada kako bi korisnici umreženih računala bili što sigurniji pri njihovoj uporabi.

RRAS ne samo da omogućuje pristup mreži s udaljenih lokacija nego služi i kao krajnja točka VPN (virtualna privatna mreža) koneksija koje primjenjuju enkripciju da bi sigurno spojile privatne mreže preko svjetske mreže kao što je internet. Budući da je svaka udaljena pristupna točka potencijalno mrežno rizična, potreban je poseban oprez kako bi se RRAS učinio što sigurnijim [6].

Alati koji mogu pomoći u konfiguriranju sigurnosnog RRAS sustava u sklopu Windowsa su:

- *Remote Access Policies* odnosno pravila udaljenog pristupa dopuštaju ili ne dopuštaju pristup svim korisnicima na server u skladu s točno određenim uvjetima.
- *Internet Authentication Service* odnosno internetska provjera valjanosti omogućuje centralno upravljanje sigurnošću udaljenog pristupa. Pravila pristupa ove provjere omogućuju zaštitu i sigurnost za svaki broj RRAS servera.

Isto tako, za korisnika su dostupni sljedeći alati:

- daljinski pristup svojstvima korisničkog računa (Remote Access Properties of User Accounts) dopuštaju ili ne dopuštaju pristup individualnim korisnicima. Ova dozvola odnosi se na sve oblike pristupa uključujući spajanje na mrežu, te VPN.

- *Connection Manager Administration Kit* odnosno uspostava menadžerske veze dopušta kreiranje prilagođene programske podrške za pristup klijenta za dial-up ili VPN pristup mreži [9].

Već je rečeno kako je glavna prednosti VPN mreža to da svatko može s udaljenosti pristupiti lokalnoj mreži poduzeća koristeći javnu mrežu koju osigurava pružatelj Internet usluga što smanjuje troškove poslovanja [14]. VPN mreže kompatibilne su sa širokopojasnim tehnologijama što znači da djelatnici mogu iskoristiti svoju brzu Internet vezu iz svojeg doma kako bi lakše i brže pristupili svojim poduzećima.

Isto tako, osiguravaju najvišu razinu sigurnosti uz naprednu enkripciju i autentikaciju koristeći posebne protokole koji štite od neovlaštenog pristupa i hakiranja [15]. Dakle, sigurnosna zaštita VPN mreža može se podijeliti na dva sigurnosna mehanizma.

Prvi mehanizam za sigurnost je autentifikacija, a drugi je enkripcija. Autentifikacija služi za osiguravanje ograničene provjere pristupa. Ovdje se misli na dokazivanje identiteta između korisnika koji se nalaze na krajevima tunela. VPN se sastoji od unutarnjih mreža omogućava fizičku i administrativnu sigurnost te vanjska koja predstavlja Internet. Između klijenata i poslužitelja nalazi se vatrozid.

Autentifikacijskom poslužitelju u zaštićenoj mreži se prosljeđuju podaci potrebni za autentifikaciju, kada klijent želi uspostaviti komunikaciju. Ovaj je podatak bitan sa stajališta sigurnosti jer dozvoljava da klijentsko računalo klijenta bude spojeno na javnu mrežu koja nije sigurna.

Nadalje, enkripcija služi za očuvanje povjerljivosti i integriteta podataka, a označava postupak kodiranja podataka na način da ih mogu pročitati samo oni korisnici koji imaju potrebnu lozinku, dakle oni kojima su podaci i namijenjeni [10].

Naime, danas se velik dio ljudskih života odvija online, od komunikacije e-poštom i društvenim mrežama do pohrane fotografija u servisima u računalnom oblaku. Prednosti i pogodnosti koje online svijet donosi su brojne. Međutim, to je svijet koji je također pun opasnosti. Naši privatni i povjerljivi podaci, komunikacije, lokacija i drugo lako mogu postati plijenom cyberkriminalaca, vlasti i pružatelja usluga pristupa internetu. Budući da su privatnost i slobode na webu te oblici zaštite poput enkripcije sve više izloženi riziku, tako rastu i prijetnje neovlaštenog nadzora, praćenja i cenzure.

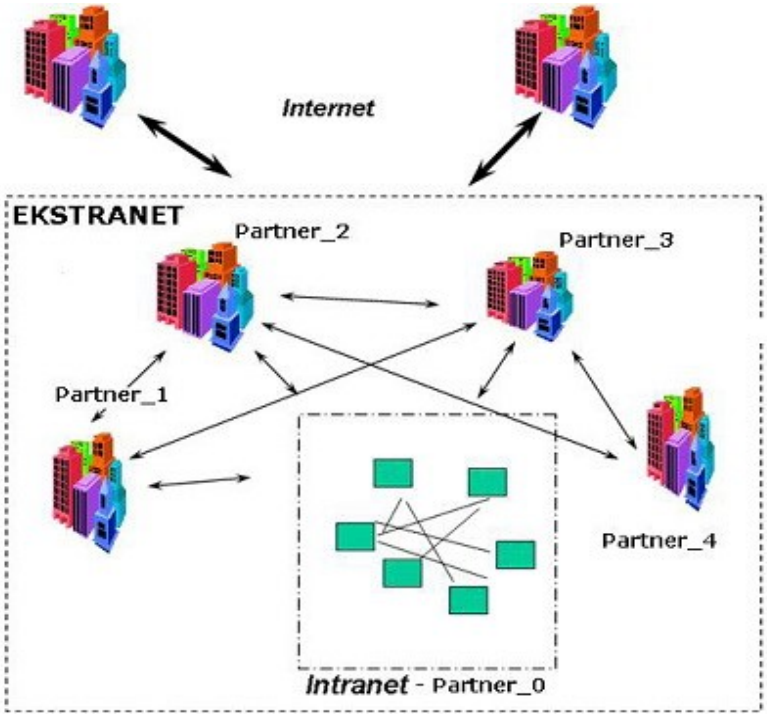
Već je rečeno kako je VPN softverski alat koji enkriptira aktivnosti online i čini ih nasumičnima, što značajno otežava njihovo praćenje i prikupljanje. Stvara barijeru između korisnika i hakera, znatiželjnika i pružatelja usluge koji želi saznati po kojim stranicama korisnici istražuju. Isto tako, VPN daje dodatni sloj sigurnosti pri korištenju Wi-Fi-a u zračnim lukama, hotelima, kafićima i kod kuće. Tako npr. u državama poput Kine koriste ga u cilju zaobilaženja blokade vlasti postavljene kako bi se onemogućio pristup nepoželjnim sadržajima.

U vrijeme kad takvi softverski alati postaju sve više nužnost VPN-ovi bi mogli razmjerno brzo postati sveprisutni, ali samo ukoliko njihovi proizvođači pronađu načine kako se nositi sa sve ozbiljnijim izazovima koji se pred njih postavljaju.

6. VRSTE VPN RJEŠENJA

Općenito govoreći, različiti VPN proizvodi mogu se svrstati u jednu od kategorija poput VPN rješenja koja se baziraju na vatrozidima te sklopovski i programski orijentirana VPN rješenja. Prva koriste postojeće sigurnosne mehanizme koji su ugrađeni u same vatrozide, a ograničavaju pristup internoj mreži.

Sklopovski orijentirana VPN rješenja omogućuju najveću propusnost između svih VPN sustava bez korištenja operativnog sustava i posebnih aplikacija. VPN rješenja koja su programski orijentirana pružaju pak najveću fleksibilnost prilikom upravljanja mrežnim prometom, što je idealno u situacijama kada svi elementi VPN sustava nisu kontrolirani od strane jedne organizacije [10].



Slika 11. Ekstranet i intranet [20]

Govoreći o vrstama VPN rješenja, prema mogućnosti primjene postoji Intranet VPN, Extranet VPN i VPN rješenja za udaljeni pristup [10]. Intranet VPN se koristi za povezivanje više lokacija unutar jedne organizacije, a za prijenos podataka se koristi Internet ili WAN. To je privatna mreža poduzeća, ustanove ili organizacije koja se sastoji od ograničenog broja računala koja su međusobno povezana i kontrolirana na definiran način. Postavlja ga organizacija kako bi se osigurala sigurna i neometana veza između svojih članova te efikasnijeg dijeljenja informacija [19].

Nadalje, Extranet VPN se koristi za povezivanje dva ili više dobavljača odnosno poslovnih partnera, dok se za prijenos podataka koristi Internet ili WAN. To je dio intraneta te se također smatra privatnom mrežom te njime upravlja ista organizacija. Cilj mu je pružiti ovlaštenim subjektima iz vanjskog svijeta siguran pristup Intranetu [19].

Tablica 1. Razlika između Intraneta i Extraneta

Intranet	Ekstranet
prvenstveno se odnosi na zaposlenike neke organizacije	dostupnost i klijentima, dobavljačima, suradnicima ili drugim ovlaštenim strankama
koristi se i za isporuku softverskih alata i aplikacija za unaprjeđenje produktivnosti	jednostavnosti korištenja sustava za sve njegove sudionike
pristup internetu se najčešće odvija kroz izlaz zaštićen vatrozidom, uz identifikaciju korisnika, kodirane poruke i kroz upotrebu VPN-a	organizacija davatelja usluge nalazi se između osoblja davatelja usluge i kontakt punktova i klijenata
omogućuje zaposlenicima brz pristup informacijama i aplikacijama	način povezivanja su iznajmljene telefonske linije, javne paketne mreže te preko Interneta
podloga za razvoj i plasiranje poslovnih aplikacija kojima se podržava poslovno djelovanje	otvoren samo prema određenim korisnicima koji mogu pristupiti podacima (npr. kupci).

VPN rješenja za udaljeni pristup povezuju udaljene korisnike ili neke manje urede sa lokalnom mrežom poduzeća. Povezivanje se obavlja putem modemske veze preko Interneta (engl. *Virtual Private Dial Network,* kratica: VPDN).

U odnosu na direktno modemsko povezivanje s poduzećem, prednosti ovog načina spajanja su niža cijena povezivanja putem Interneta, izostanak kupovine i održavanja modemskih ulaza i plaćanja telefonske pretplate te činjenica da nije moguće korištenjem ADSL tehnologije međusobno spojiti dva korisnika, već samo na Internet.

7. BUDUĆI RAZVOJ VIRTUALNIH PRIVATNIH MREŽA

Uporabom virtualnih privatnih mreža temeljnih na bežičnoj mrežnoj infrastrukturi znatno se podiže sigurnosna razina rada u mrežnom okruženju. Iako VPN tehnologija nema izravan utjecaj na procese autentikacije korisnika prilikom spajanja na bežičnu pristupnu točku, ona doprinosi unutarnjoj sigurnosti bežične mreže. Iz tog razloga tehnologija virtualnih privatnih mreža neće se detaljnije razmatrati s obzirom da se radi o unutarnjoj sigurnosnoj razini, a ne o zaštitnom mehanizmu od neovlaštenog pristupa korištenjem bežične mrežne tehnologije.

VPN je tehnologija koja omogućava sigurno povezivanje računala u virtualne privatne mreže preko distribuirane ili javne mrežne infrastrukture. Ona podrazumijeva korištenje određenih sigurnosnih i upravljačkih pravila unutar lokalnih mreža. VPN veze mogu se uspostaviti preko različitih komunikacijskih kanala kao što su internet, komunikacijske infrastrukture davatelja internetskih usluga i drugi. Vrlo je bitno kako virtualna privatna mreža preko javne mreže stvara sigurni kanal između dviju krajnjih točaka [8].

Prema konceptu virtualnih privatnih mreža, osnovna zadaća tehnologije je kreiranje sigurnog komunikacijskog kanala između privatnih mreža putem javne mreže. Uobičajena je kombinacija sklopovskog i programskog pristupa u kreiranju medija za siguran prijenos podataka. Prilikom komunikacije, podaci iz lokalne mreže prolaze kroz *gateway* uređaj koji ima ulogu zaštite komunikacijskog medija. Isti postupak se primjenjuje kada podaci dolaze u lokalnu mrežu, također prolaze kroz *gateway* uređaj. Na taj se način štite tako odaslani podaci automatskim šifriranjem prilikom slanja podataka između dviju udaljenih privatnih mreža i enkapsuliranjem u IP pakete, te automatskim dešifriranjem paketa na drugom kraju komunikacijskog kanala.

Kada se govori o korištenju, implementaciji i sigurnosti virtualnih privatnih mreža u mrežnom povezivanju, bežične mreže se u osnovi ne razlikuju od žičanih lokalnih mreža. Razlika je isključivo u pristupnom dijelu mreže (pristupni medij), dok se sa sigurnosnog aspekta u potpunosti podudaraju, odnosno ovise o upravljačkoj mrežnoj infrastrukturi. Korištenje virtualnih privatnih mreža u bežičnoj mrežnoj infrastrukturi, bežičnoj lokalnoj mreži daje proširene pristupne mogućnosti (bežični pristup) uz optimalnu sigurnosnu razinu [8].

U korištenju virtualnih privatnih mreža i njegove sigurnosti, u budućnosti se mogu očekivati samo još veća poboljšanja. Danas su se mane virtualnih privatnih mreža eliminirale korištenjem poznatih SSL i TLS enkripcijskih metoda i pojačanim procesorima vatrozida i

usmjernika. Stoga se može reći kako je najvrijednija stvar koju neko poduzeće može posjedovati upravo informacija koju je potrebno zaštititi. Iz tog razloga jasno je kako virtualne privatne mreže neće izumrijeti, budući da su privukle pozornost mnogih organizacija koje žele povećati svoje sposobnosti umrežavanja i smanjiti troškove.

Uspjeh virtualnih privatnih mreža u budućnosti ovisi uglavnom o razvoju tehnologije. Njihova najveća vrijednost krije se u potencijalnom smanjenju troškova poduzeća, a ovisi i o mogućnosti adekvatnog obavljanja svojih zadaća od strane Intraneta i Ekstraneta. Prije svega, one zahtijevaju dobro razumijevanje problema sigurnosti javih mreža i poduzimanje mjera opreza kod postavljanja. Isto tako, njihova dostupnost i performanse u određenim poduzećima ovise o faktorima koji su izvan njihove kontrole, a često su nekompatibilne zbog nepostojanja standarda VPN tehnologije različitih proizvođača.

Uslijed razvoja i pada cijena mrežne opreme koja se koristi za potrebe Interneta, virtualne privatne mreže se posljednjih godina sve više koriste kao alternativno rješenje. Ističu se svakako i kao najjeftinija metoda. Prednosti virtualnih privatnih mreža ogledaju se u:

- fleksibilnosti i skalabilnosti mreže (moguće je u kratkom roku povezati nove ili privremene adrese što nije moguće kada se koriste iznajmljene linije);
- umjesto zakupa iznajmljenih linija (ili spajanja korištenjem modema), kod VPN-a se plaćaju (samo) znatno niži troškovi za spajanje preko Interneta;
- manjem trošku za nabavu i održavanje opreme koja se koristi [10].

U odnosu na zaista velike prednosti koje se tiču fleksibilnosti i troškova same mreže, virtualne privatne mreže nisu uvijek savršeno rješenje te imaju određene nedostatke, a to su [2]:

- pouzdanost (dostupnost i brzina) – VPN ovisi o kvaliteti usluge ISP-a (pružatelja Internet usluga) koja nije uvijek zadovoljavajuća. Isto tako, ovisi i o načinu primjene VPN veze (koji protokoli se koriste, autentikacija, enkripcija, itd.);
- nekompatibilnost opreme različitih proizvođača – što ima utjecaja prilikom primjene pojedinih standarda i protokola koji u tom slučaju neće raditi kako je predviđeno;
- zahtijeva se vrhunsko poznavanje opreme koja se koristi u cilju ostvarivanja potpune zaštite privatne mreže od mogućih sigurnosnih prijetnji i napada. To uključuje poznavanje mrežnih protokola, sigurnosnih mehanizama i pažljivo konfiguriranje postavki sustava. Ljudi koji uspostavljaju, ali i održavaju VPN moraju biti visoko stručno osposobljeni i motivirani [10].

Svaki bi korisnik osobnog računala morao pratiti razvoj informacijske tehnologije. Kako se one svakodnevno usavršavaju, istodobno je potrebno da se prate i primjenjuju sve moguće sigurnosne komponente umreženih računala i podataka kojima manipulira, tako da se ne bi dogodilo da korisnik nije pripremljen na moguće upade pojedinaca i skupina u sigurnosni sustav programa, a da toga nije bio svjestan ili da nije znao primijeniti najnovija sigurnosna načela u radu s osobnim računalom [6].

Dakle, u posljednjih nekoliko godina jasno je da su prednosti koje proizlaze iz uporabe virtualnih privatnih mreža neograničene, što je vidljivo kroz razvoj novih mrežnih usluga i dostupnost novih mrežnih tehnologija. Pogodnosti za virtualnu privatnu mrežu ne treba podcjenjivati, upravo iz razloga što uključuju brzinu, fleksibilnost, privatnosti i financijske pogodnosti. Naime, one su vrlo bitne i mogu u potpunosti izmijeniti način na koji pojedinac ili poduzeća obavlja svoje poslovanje.

8. ZAKLJUČAK

Na kraju ovog završnog rada jasno je kako upravo VPN tehnologija služi za povezivanje dviju mreža koristeći enkripcijske protokole preko manje sigurne javne mreže. VPN je skraćenica za pojam virtualne privatne mreže, koje omogućuju pojedincima i poduzećima razmjenu i pristup informacijama bilo gdje i s bilo kojeg računala. Budući da im je pristup ograničen na određene korisnike te su mreže privatne. Virtualne privatne mreže funkcioniraju na način da se stvori privatni tunel kroz Internet do korisnikovog odredišta.

Virtualne privatne mreže mogu se podijeliti na *Site-to-site* VPN i *Remote-access* VPN, a glavna razlika je u *Site-to-site* VPN-u korisnik nije svjestan postojanja VPN-a, dok je kod *Remote-access* VPN-a svjestan budući da mora upisati svoje korisničko ime i lozinku kako bi se povezao s drugom mrežom. Nadalje, VPN rješenja za udaljeni pristup povezuju udaljene korisnike ili neke manje urede sa lokalnom mrežom poduzeća, a povezivanje se obavlja putem modemske veze preko Interneta.

Mehanizmi za sigurnost su autentifikacija i enkripcija. Autentifikacija osigurava ograničene provjere pristupa, odnosno dokazuje identitet između korisnika koji se nalaze na krajevima tunela. Njome se poslužitelju u zaštićenoj mreži prosljeđuju potrebni podaci kada klijent želi uspostaviti komunikaciju. Enkripcija služi za očuvanje povjerljivosti i integriteta podataka, a označava postupak kodiranja podataka na način da ih mogu pročitati samo oni korisnici koji imaju potrebnu lozinku, dakle oni kojima su podaci i namijenjeni.

Vrlo je bitno istaknuti kako virtualne privatne mreže zahtijevaju dobro razumijevanje problema sigurnosti javih mreža i poduzimanje mjera opreza kod postavljanja. Što se tiče njihovog budućeg razvoja, smatram kako ista ovisi o razvoju tehnologije. Vrijednost virtualnih privatnih mreža je u potencijalnom smanjenju troškova poduzeća. Također, dolazi se do spoznaje i zaključka kako VPN iz dana u dan privlači mnoga poduzeća kojima je cilj ojačati svoje umrežavanje te smanjiti troškove u čemu se, uz adekvatno obavljanje zadataka intraneta i ekstraneta, ujedno krije i njegova najveća vrijednost.

LITERATURA

[1] Combaj, G., Pongrac, D., Žigman, D.: *GETVPN enkripcija*, Polytechnic & Design, Tehničko veleučilište u Zagrebu, Vol. 3 (2), 2015.

[2] Ćulumović, D., Žigman, D., Mamuzić, I.: *Spajanje dviju kompanija u VPN*, Polytechnic & Design, Tehničko veleučilište u Zagrebu, Vol. 4 (8), 2016.

[3] Doraswamy, N., Harkins, D.: IPSec: *The New Security Standard for the Internet, Intranets, and Virtual Private Networks*, Second Edition, Prentice Hall, New York, 2003.

[4] Filipaj, I., Pongrac, D., Žigman, D.: *Dinamičke skalabilne virtualne privatne mreže*, Polytechnic & Design, Tehničko veleučilište u Zagrebu, Vol. 2 (1), 2014.

[5] Kosiur, D.: *Building and Managing Virtual Private Networks*, Wiley Computer Publishing, John Wiley & Sons, Inc., New York, SAD, 1998.

[6] Mrđen, I.: *Sigurnost umreženih računala pod operativnim sustavom Windows*, Sigurnost 48 (2), 2006.

[7] Pavin, S.: *Višeprotokolno komutiranje podatkovnog prometa u virtualnim privatnim mrežama temeljeno na oznakama*, Fakultet elektrotehnike, računarstva i informacijskih tehnologija, Osijek, 2018.

[8] Skendžić, A.: Sigurnost infrastrukturnog načina rada bežične mreže standarda IEEE 802.11, Zbornik Veleučilišta u Rijeci, Vol. 2 (1), 2014.

[9] Strebe, M.: *Implementing and Administering Security in a Microsoft Windows 2000 Network*, Microsoft Corporation, New York, SAD, 2003.

[10] URL: https://pcchip.hr/internet/sto-je-vpn-za-sto-se-koristi/ [11.10.2018.]

[11] URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf [11.10.2018.]

[12] URL: http://study.com/academy/lesson/what-isa-virtual-private-network-vpn-definitiontypes-quiz.html [6.10.2018.]

[13] URL: https://technet.microsoft.com/en-us/library/cc771298.aspx [6.10.2018.]

[14] URL: https://www.cactusvpn.com/beginnersguide-to-vpn/vpn-history/ [20.10.2018.]

[15] URL: https://static-course assets.s.amazonaws.com/CCNAS/index.html [20.10.2018.]

[16] URL:http://www.bug.hr/forum/topic/internet/uvod-mrezne-protokole/96549.aspx [11.10. 2018.]

[17] URL:http://www.yamaha.com/products/en/network/settings/ipv4_ipsec_vpn [11. 10. 2018.]

[18] URL: http://www.cisco2960.over-blog.com/2014/02/internet-intranet-and-

extranet.html [8. 10. 2018.]

[19] URL: https://en.wikipedia.org/wiki/Transport_Layer_Security [11. 10. 2018]

[20] URL: http://mreze.layer-x.com/s060300-0.html [16. 1. 2019]

POPIS ILUSTRACIJA

Popis slika

Popis tablica