HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Osnovni koncepti VPN tehnologije

CCERT-PUBDOC-2003-02-05

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

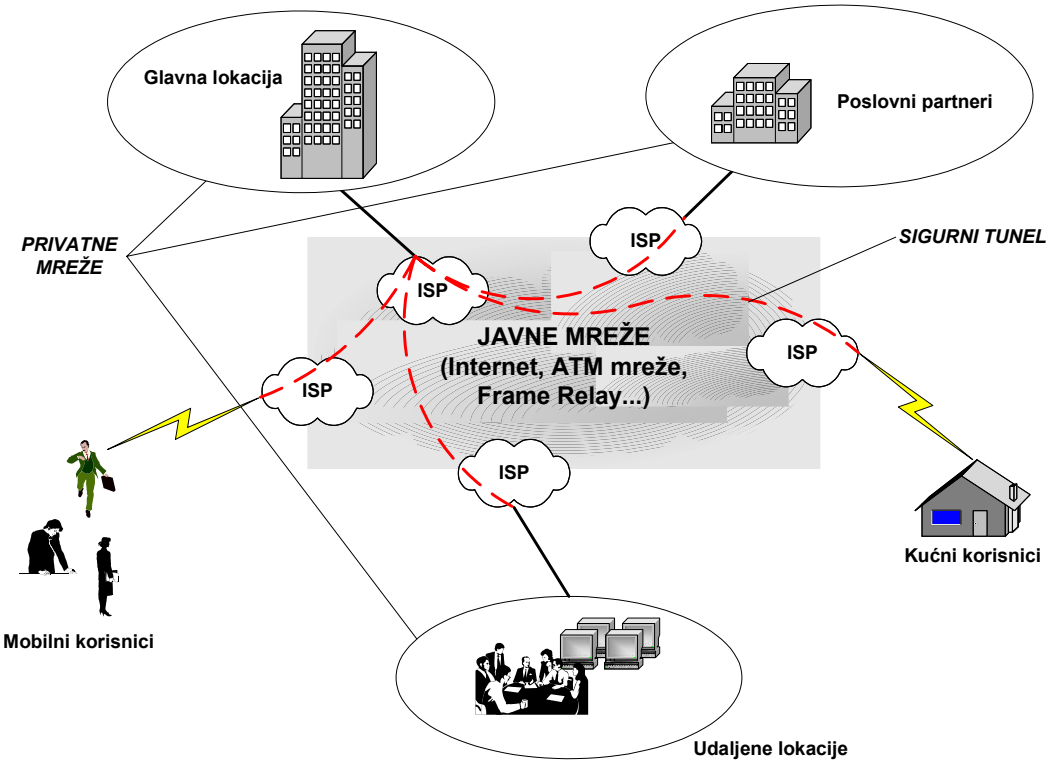
CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

VPN (*engl. Virtual Private Network*) je tehnologija koja omogućava sigurno povezivanje računala u virtualne privatne mreže preko dijeljene ili javne mrežne infrastrukture. Korištenjem VPN-a moguće je povezivanje geografski odvojenih korisnika, kupaca ili poslovnih partnera. VPN podrazumijeva korištenje istih sigurnosnih i upravljačkih pravila koja se primjenjuju unutar lokalnih mreža. Također, VPN veze mogu se uspostaviti preko različitih komunikacijskih kanala; preko Interneta, preko komunikacijske infrastrukture davatelja Internet usluga, ATM mreža itd.
Za razliku od privatnih mreža koje koriste iznajmljene linije za slanje podataka, virtualna privatna mreža preko javne mreže stvara sigurni kanal između dviju krajnjih točaka.
Slika 1 prikazuje razne mogućnosti korištenja VPN tehnologija.



Slika 1: Mogućnosti korištenja VPN tehnologija

2. Osnovni pojmovi

2.1. Koncept

Osnovni koncept VPN tehnologije je implementacija sigurnog medija između privatnih mreža, a preko javne mreže. Taj medij može biti programski ili sklopovski orijentiran, a uobičajene su i kombinacije tih pristupa.
Kada računalo šalje podatke prema drugom računalu na udaljenoj mreži, podaci koji u tom slučaju izlaze iz lokalne mreže moraju proći kroz *gateway* uređaj koji štiti tu mrežu, putovati kroz javnu mrežu, te na drugoj strani također proći kroz *gateway* uređaj koji štiti ciljno računalo na udaljenoj mreži. VPN štiti tako odaslane podatke automatskim šifriranjem prilikom slanja podataka između dviju udaljenih privatnih mreža i enkapsuliranjem u IP pakete, te automatskim dešifriranjem paketa na drugom kraju komunikacijskog kanala.
Sigurnost VPN-a temelji se na šifriranju. Cilj je ograničiti pristup podacima koji se prenose samo odgovarajućim korisnima, odnosno računalima. VPN koristi kompletnu enkripciju paketa, od jednog kraja virtualnog spoja do drugog (engl. *end-to-end*). Ova tehnika spremanja šifriranih podataka u

otvorena zaglavlja naziva se tuneliranje. Prilikom spajanja, VPN otvara sigurni tunel koji omogućava enkapsulaciju i šifriranje podataka, te autentikaciju korisnika.

2.2. Prednosti i ograničenja

Osnovna prednost korištenja VPN-a jest značajna ušteda u odnosu na cijenu korištenja privatnih iznajmljenih linija ili međugradskih/internacionalnih telefonskih poziva. Postojanje Interneta kao globalne mreže, te mogućnost sigurnog slanja povjerljivih podataka omogućavaju korištenje VPN-a kao alternative WAN mrežama i drugim načinima implementacije udaljenog pristupa, pošto u većini slučajeva VPN predstavlja manji trošak, te smanjuje potrebe za administracijom u odnosu na tradicionalne privatne mreže. Komunikacijski putovi korištenjem VPN-a mogu se uspostavljati brzo, jeftino i sigurno bilo gdje na svijetu.

Naravno, iznajmljene linije, iako skuplje, osiguravaju siguran i pouzdan medij za prijenos podataka. Nasuprot tome prijenos podataka preko Interneta može rezultirati kašnjenjima ili iznenadnim prekidima u komunikaciji.

Korištenje enkripcijskih mehanizama unosi nešto dodatnog prometa u sjednicu. No većina VPN uređaja, programskih ili sklopovskih, podržava enkripciju/dekripciju u stvarnom vremenu pri brzinama od 10Mbps i većima. Prilikom korištenja sporijih tehnologija kao npr. modemskih, ISDN ili DSL veza, obrada VPN komunikacije je mnogo brža nego kašnjenja uzrokovana ograničenom brzinom prijenosa. Pokazuje se da gubljenje paketa i latencija na lošijim Internet spojevima potencijalno više utječe na performanse nego nužnost šifriranja kod VPN-a.

Primjena VPN rješenja ima smisla u slučajevima kada korporativno okruženje ima više odvojenih lokacija, a propusnost i kvaliteta usluge nisu od kritičnog značenja. U suprotnom slučaju, kada postoji manji broj odvojenih lokacija, a propusnost i kvaliteta usluge su ključne, korištenje iznajmljenih linija je vjerojatno prihvatljivije rješenje.

2.3. Zahtjevi

VPN tehnologija mora zadovoljavati određene zahtjeve. Između ostalog, svako VPN rješenje mora osigurati sljedeće:

- Autentikaciju korisnika – VPN mora osigurati provjeru identiteta korisnika i ograničiti VPN pristup samo ovlaštenim korisnicima. Također, VPN mora osigurati praćenje i bilježenje događaja.
- Upravljanje adresama – VPN je zadužen za dodjeljivanje klijentskih adresa unutar privatnih mreža.
- Šifriranje – podaci koji se prenose preko javne mreže moraju biti šifrirani da bi njihov sadržaj bio nedostupan neovlaštenim korisnicima.
- Upravljanje ključevima – VPN mora sadržati mehanizme za generiranje i osvježavanje ključeva nužnih za šifriranje komunikacijskog kanala između klijenta i poslužitelja.;
- Podršku za razne protokole –VPN mora podržavati uobičajene protokole koji se koriste na javnim mrežama (IP, IPX itd.).

2.4. Osnovni elementi

Postoji nekoliko elemenata koje VPN rješenje mora sadržati:

- skalabilnost,
- sigurnost,
- VPN servisi,
- uređaji,
- upravljanje.

Skalabilnost podrazumijeva da svaki element mora biti izveden tako da može podržati VPN platforme od malih uredskih konfiguracija, pa do velikih korporacijskih implementacija. Mogućnost prilagodbe VPN-a prema potrebama propusnosti i načinu veze ključna je u svakom VPN rješenju.

Sigurnosni pojmovi kao što su tuneliranje, šifriranja i autentikacija paketa nužni su za sigurnost prijenosa podataka preko javnih mreža. Osim toga autentikacija korisnika i kontrola pristupa nužne su za dodjelu odgovarajućih ovlasti i prava pristupa mrežnim resursima.

Uloga VPN servisa je upravljanje propusnošću komunikacijskog kanala, te implementacija funkcija koje osiguravaju kvalitetu usluge, poput izbjegavanja zagušenja, oblikovanja prometa, klasifikacije paketa itd. Također, važni dijelovi VPN tehnologije jesu protokoli koji osiguravaju usmjerivačke servise poput EIGRP (engl. *Enhanced Interior Gateway Router Protocol*), OSPF (engl. *Open Shortest Path First*), te BGP (engl. *Border Gateway Protocol*).
Uređaji poput vatrozida, sustava za detekciju neovlaštenih aktivnosti, te aktivno praćenje sigurnosnih parametara nužni su za uspostavu odgovarajuće razine sigurnosti pri korištenju VPN-a.
Upravljanje propusnosti kanala, definicija i primjena sigurnosnih pravila, te nadgledanje mrežnog prometa također nužan element svakog VPN rješenja.

2.5. Vrste VPN rješenja

Općenito gledajući, razni VPN proizvodi mogu se svrstati u jednu od tri sljedeće kategorije:

- VPN rješenja bazirana na vatrozidima,
- sklopovski orijentirana VPN rješenja,
- programski orijentirana VPN rješenja.

VPN rješenja bazirana na vatrozidima koriste postojeće sigurnosne mehanizme ugrađene u same vatrozide, te ograničavaju pristup internoj mreži. Kroz te mehanizme implementirano je prevođenje adresa, autentikacijski zahtjevi, bilježenje događaja i uzbunjivanje u stvarnom vremenu.
Sklopovski orijentirana VPN rješenja osiguravaju najveću propusnost među svim VPN sustavima. Takva rješenja ne koriste operativni sustav niti posebne aplikacije. Većina sklopovski orijentiranih VPN-ova su usmjerivači koji šifriraju promet (engl. *encrypting routers*). Pri korištenju ovakvih rješenja sav promet, bez obzira na protokol, koristi mehanizam tuneliranja. Najbolji paketi nude i programske klijente za udaljenu instalaciju, te sadrže funkcije za kontrolu pristupa kojima se može upravljati preko vatrozida ili drugih uređaja.
Programski orijentirana VPN rješenja pružaju pak najveću fleksibilnost prilikom upravljanja mrežnim prometom. Takvi proizvodi omogućavaju selektivno tuneliranje prometa temeljeno na mrežnim adresama ili protokolima. Ovakva rješenja su idealna za slučajeve kada svi elementi VPN sustava nisu kontrolirani od strane jedne organizacije (npr. podrška korisnicima ili poslovni partneri). Ovakva rješenje također su pogodna u heterogenim mrežnim okruženjima gdje postoje različiti usmjerivači i vatrozidi.
Obzirom na mogućnost primjene, VPN tehnologije mogu se podijeliti na sljedeće:

- intranet VPN rješenja – međusobno povezuju definirane lokacije kao što su udaljeni uredi,
- ekstranet VPN rješenja – povezuju poslovne partnere,
- VPN rješenja za udaljeni pristup – povezuju udaljene korisnike ili manje udaljene urede sa računalnom infrastrukturom organizacije.

3. VPN tehnologije

3.1. Tuneliranje

Unutar infrastrukture međusobno povezanih mreža, tuneliranje predstavlja tehniku prijenosa podataka namijenjenih određenoj mreži preko druge mreže. Protokol kojim se implementira tuneliranje, umjesto da šalje originalni okvir, enkapsulira okvir u dodatno, posebno oblikovano, zaglavlje. Takvo zaglavlje osigurava informacije nužne za usmjerivanje enkapsuliranih podataka kroz mrežu koja služi za prijenos do odredišta. Enkapsulirani podaci šalju se između krajnjih točaka tunela. Tunel je logički put kroz koji enkapsulirani podaci prolaze kroz mrežu koja je medij za prijenos. Kada takav okvir dođe do svog odredišta, iz njega se ekstrahiraju korisni podaci koji se zatim šalju na ciljno odredište. Tuneliranje uključuje čitav proces enkapsulacije, prijenosa i ponovne ekstrakcije originalnih podataka.

3.2. Postojeće tehnologije

Danas postoje razne tehnologije koje implementiraju tehniku tuneliranja. Najvažnije od njih su sljedeće:

- DLSW (engl. *Data Link Switching*)

- GRE (engl. *Generic Routing Encapsulation*)
- ATMP (engl. *Ascend Tunnel Management Protocol*)
- Mobile IP – za mobilne korisnike
- IPSec (engl. *Internet Protocol Security Tunnel Mode*)
- PPTP (engl. *Point-to-Point Tunneling Protocol*)
- L2F (engl. *Layer 2 Forwarding*)
- L2TP (engl. *Layer 2 Tunneling Protocol*)

3.2.1. IPSec

IPSec je standard definiran od strane IETF-a, a cilj njegove izrade bio je siguran transport informacija preko javnih IP mreža. IPSec je protokol treće razine (engl. *Layer 3*), te u sebi sadržava nekoliko sigurnosnih tehnologija da bi osigurao tajnost, integritet i autentikaciju. IPSec implementira šifriranja i autentikaciju u mrežnom sloju, osiguravajući tako sigurnu komunikaciju od početka do kraja unutar mrežne infrastrukture.

IKE (engl. *Internet Key Exchange*) služi za određivanje sigurnosnih parametara i razmjenu ključnih informacija između entiteta koji sudjeluju u komunikaciji. Sigurnosni parametri definiraju vezu između dvaju ili više entiteta, te definiraju kako će ti entiteti koristiti sigurnosne servise u cilju uspostave međusobne sigurne komunikacije. IPSec sam po sebi ne posjeduje mehanizam se određivanje takvih sigurnosnih parametara. IETF je odabrao IKE kao standardnu metodu za definiranje sigurnosnih parametara za potrebe IPSec-a. Pri tome se također koristi IKMP (engl. *Internet Key Management Protocol*). IKE stvara autenticirani, sigurni tunel između dvaju entiteta, te zatim definira sigurnosne parametre potrebne za IPSec. Kroz taj proces dva entiteta se moraju međusobno autenticirati, te dogovoriti zajedničke ključeve.

Prilikom rada IPSec koristi sljedeće protokole i standarde :

- Diffie-Hellman-ovu metodu razmjene ključeva za određivanje ključeva između dvaju entiteta,
- kriptografiju temeljenu na javnim ključevima za digitalno potpisivanje komunikacije prilikom Diffie-Hellman-ove razmjene ključeva, da bi se osigurao identitet obiju strana u komunikaciji, te izbjegla mogućnost tzv. *Man-in-the-middle* napada,
- DES ili 3DES standard za šifriranje podataka,
- HMAC (engl. *Hashing Message Authentication*) u sprezi sa MD5 i SHA algoritmima,
- digitalna uvjerenja potpisana od strane odgovarajućeg autoriteta.

IPSec protokol definira informacije koje se moraju dodati IP paketu da bi se osigurala tajnost, integritet i autentikacija, te način šifriranja sadržaja paketa. Protokoli definirani u RFC 2406 (ESP – engl. *Encapsulated Security Payload*) i RFC 2402 (AH – engl. *Authentication Header*) dio su IPSec arhitekture. Autentikacijska zaglavlja (AH) se koriste za autentikaciju izvora i integritet bez uporabe šifriranja, dok ESP osigurava iste usluge, ali uz dodatak mehanizama za šifriranje. Sigurnosni ključ poznaju samo primatelj i pošiljatelj, a ukoliko su autentikacijski podaci valjani primatelj može biti siguran da je podatak stigao od pošiljatelja, te da nije promijenjen tijekom prijenosa.

IPSec podržava dva načina rada; prijenosni način rada (engl. *transport mode*) i tuneliranje (engl. *tunnel mode*). U prijenosnom načinu rada šifrira se samo podatkovni dio IP paketa, dok IP zaglavlja ostaju u originalnom obliku. Aplikacijska zaglavlja su šifrirana, a mogućnost pregledavanja paketa je ograničena. Prednost ovog načina rada je da se svakom paketu dodaje svega nekoliko okteta. U ovom načinu rada uređaji (usmjerivači) na javnoj mreži mogu vidjeti adrese izvora i odredišta poruka, što potencijalnom napadaču donekle omogućava određene mogućnosti analize prometa. Osim ovog načina šifriranja IP prometa, IPSec ima mogućnost IP tuneliranja što podrazumijeva posebni oblik paketa za IP promet. Taj način rada naziva se IPSec tuneliranje. Tunel se sastoji od klijenta i poslužitelja koji su oba konfigurirani da koriste IPSec tuneliranje i dogovorene mehanizme za šifriranje. IPSec tuneliranje koristi dogovorene mehanizme za enkapsulaciju i šifriranje čitavih IP paketa što osigurava potpuno siguran prijenos preko javnih ili privatnih mreža. Šifrirani podaci se spajaju sa odgovarajućim nešifriranim IP zaglavljima, formirajući tako IP pakete koji se na kraju tunela dešifriraju i oblikuju u IP pakete namijenjene krajnjem odredištu.

IPSec kao takav nalazi se ispod TCP/IP stoga protokola, tako da je za aplikacije i protokole više razine potpuno transparentan. IPSec-om se upravlja pomoću definirane sigurnosne politike, odnosno dogovorenih sigurnosnih mehanizama između primatelja i pošiljatelja. Sigurnosna politika definirana

je skupom filtara. Ukoliko IP adresa, protokol i broj porta odgovaraju filtru, paket se obrađuje na odgovarajući način.

3.2.2. PPTP (Point-to-Point Tunneling Protocol)

PPTP protokol razvio je konzorcij proizvođača koji uključuje US Robotics, Ascend Communications, 3Com, ECI Telematics i Microsoft. Nekoliko proizvođača implementiralo je PPTP sustave, ali većina PPTP korisnika koristi Microsoftovu inačicu.

Protokol je smješten u mrežnom sloju i temelji se na dobro poznatom PPP (engl. *Point-to-Point Protocol*) protokolu, odnosno na TCP/IP stogu protokola. PPP omogućava autentikaciju, te metode za šifriranje i kompresiju podataka. PPTP omogućava tuneliranje PPP sjednice kroz postojeći IP spoj, bez obzira na način na koji je on uspostavljen. Izvorno je PPTP zamišljen kao mehanizam za enkapsulaciju koji bi omogućavao prijenos protokola koji nisu temeljeni na TCP/IP stogu poput npr. IPX-a i AppleTalk-a preko Interneta korištenjem GRE (engl. *Generic Routing Encapsulation*). To je tehnologija koja omogućava siguran TCP/IP promet između Windows9x/NT/200 klijenata koji su povezani na Internet preko PPP-a, te Windows NT/2000 poslužitelja na lokalnim mrežama iza vatrozida. PPTP koristi TCP spoj za održavanje tunela, te GRE enkapsulirane PPP okvire za tuneliranje podataka. Sadržaj enkapsuliranih PPP okvira može biti šifriran i/ili komprimiran. Tuneliranje je moguće pošto PPTP osigurava enkapsulaciju omatanjem originalnih paketa (IP, IPX ili NetBEUI) u IP pakete koji se šalju preko Interneta. Nakon što paket dođe do odredišta, vanjski IP paketi se uklanjaju omogućavajući tako originalnim paketima dolazak do krajnjeg odredišta. Enkapsulacija omogućava prijenos paketa koji inače ne bi zadovoljavali standarde adresiranja na Internetu.

PPTP posjeduje i određene nedostatke od koji su najznačajniji opisani u nastavku.

Neadekvatan mehanizam za šifriranje kod PPTP-a znači da se ključevi ne generiraju na slučajan način, sjednički ključevi nisu adekvatni, a nesiguran je i prijenos *hash* vrijednosti korisničkih zaporki. Također, duljine ključeva su prekratke i nije ih moguće konfigurirati.

U heterogenim Win9x/NT/2000 okruženjima upravljanje zaporkama nije riješeno na odgovarajući način, te je statičke zaporke vrlo lako kompromitirati.

Također PPTP je ranjiv na napade lažiranjem poslužitelja pošto autentikacija paketa nije implementirana.

Microsoft RAS (engl. *Remote Access Service*) originalno je predviđen kao pristupni servis za *dial-up* korisnike. RAS je također tunelski poslužitelj za PPTP, tako da postavljanje PPTP sustava na NT/2000 poslužitelje zahtijeva konfiguraciju RAS poslužitelja, primjenu svih odgovarajućih sigurnosnih zakrpi, podešavanje PPTP specifičnih ključeva u *registry* datoteci, omogućavanje IP prosljeđivanja isto kao i kompletno osiguranje poslužitelja. RAS kao takav podržava sljedeće mehanizme:

- PAP (engl. *Password Authentication Protection*),
- CHAP (engl. *Challenge Handshake Authentication Protocol*),
- MS-CHAP (engl. *Microsoft Challenge Handshake Authentication Protocol*),
- RSA RC4 i DES mogućnosti šifriranja.

Inicijalno je PPTP koristio MS-CHAP mehanizam za autentikaciju krajnjih korisnika, no kako je u međuvremenu otkriveno da se taj mehanizam može vrlo lako kompromitirati, Microsoft je objavio MS-CHAP V2. Ovisnost PPTP autentikacije o MS-CHAP autentikaciji čini je ranjivom na napade korištenjem npr. L0phtcrack alata. PPTP koristi 40-bitnu, 56-bitnu ili 128-bitnu enkripciju, ali čitav proces šifriranja je oslabljen upotrebom korisničkih zaporki za generiranje sjedničkih ključeva te je podložan tzv. *brute-force* napadima. Jedina zaštita od takve vrste napada jesu dugački ključevi generirani na potpuno slučajan način.

PPTP je unaprjeđivan kombiniranjem sa L2F protokolom, da bi ga konačno nadgradio L2TP.

3.2.3. L2F (Layer 2 Forwarding)

L2F tehnologiju je predložio Cisco. L2F je protokol mrežnog sloja neovisan o prijenosnom mediju koji dolazi sa Cisco IOS podrškom. To je prijenosni protkol koji omogućava *dial-up* pristup poslužiteljima. Osnovna funkcija L2F protokola je osiguranje mehanizma tuneliranja za okvire prijenosnog sloja (HDLC, async PPP, SLIP ili PPP ISDN) ili protokole viših slojeva. Enkapsulirani paketi se prenose preko WAN spojeva do L2F poslužitelja (usmjerivača) gdje

se ekstrahiraju i prosljeđuju u mrežu. L2F ne definira klijente i funkcionira samo u obvezno (engl. *compulsory*) definiranim tunelima.
Kako je ranije spomenuto, L2F je unaprjeđivan kombiniranjem sa PPTP protokolom, da bi ga konačno nadgradio L2TP.

3.2.4. L2TP (Layer 2 Tunneling Protocol)

Microsoft i Cisco zajednički su razvili L2TP kombinirajući najbolje značajke PPTP i L2F protokola. L2TP je mrežni protokol koji služi za tuneliranje PPP okvira preko mreža. L2TP enkapsulira PPP okvire za slanje preko IP, X25, Frame Relay ili ATM mreža. Podaci iz enkapsuliranih PPP okvira mogu biti šifrirani i/ili komprimirani. Protokol se također može koristiti direktno preko raznih WAN medija (npr. *Frame Relay*) bez IP transportnog sloja. L2TP koristi UDP i nizove L2TP poruka za održavanje tunela preko IP mreža. Također moguće je istovremeno stvaranje više tunela između istih krajnjih točaka.
L2TP se sastoji od dva osnovna elementa; L2TP pristupnog koncentratora (engl. *L2TP Access Concentrator – LAC*) i L2TP mrežnih poslužitelja (engl. *L2TP Network Server – LNS*). Mrežni poslužitelj (LNS) predstavlja logičku krajnju točku PPP sjednice koja se tunelira kroz neki sustav korištenjem pristupnog koncentratora (LAC).
L2TP podržava obvezno definirane tunele isto kao i proizvoljne (engl. *voluntary*).
Način rada obvezno definiranog tunela opisan je sljedećim nizom koraka:

1. Udaljeni korisnik inicira PPP spoj prema svom ISP-u.
2. ISP prihvaća spoj i PPP sjednica je uspostavljena.
3. ISP zahtijeva djelomičnu autentikaciju da bi dobio korisničko ime.
4. U ISP-ovoj bazi podataka korisničko ime je povezano sa servisima i LNS krajnim točkama.
5. LAC inicira L2TP tunel prem LNS-u.
6. Ukoliko LNS prihvati spoj, LAC enkapsulira PPP u L2TP i prosljeđuje podatke preko odgovarajućeg tunela.
7. LNS prihvaća okvire, odvaja L2TP zaglavlja i obrađuje ih kao normalne PPP okvire.
8. LNS zatim koristi standardnu PPP autentikaciju da bi utvrdio identitet korisnika i dodijelio mu IP adresu.

Ukoliko se koristi proizvoljno definirani tunel način rada je drugačiji i opisan je u sljedećim koracima:

1. Udaljeni korisnik ima uspostavljenu vezu sa svojim ISP-om.
2. L2TP klijent (LAC) inicira L2TP tunel prema LNS-u.
3. Ukoliko LNS prihvati spoj LAC enkapsulira PPP u L2TP i prosljeđuje podatke kroz tunel.
4. LNS prihvaća okvire, odvaja L2TP zaglavlja i obrađuje ih kao normalne dolazne zahtjeve.
5. LNS zatim koristi PPP autentikaciju da bi utvrdio identitet korisnika i dodijelio mu IP adresu.

L2TP definira dvije vrste poruka: kontrolne poruke i podatkovne poruke. Kontrolne poruke koriste se prilikom uspostave, održavanja i čišćenja tunela. Podatkovne poruke se koriste za enkapsulaciju PPP okvira koji se prenose kroz tunel. Kontrolne poruke definiraju pouzdani kontrolni kanal unutar L2TP koji garantira dostavu. Podatkovne poruke se šalju ponovno ukoliko dođe do gubljenja paketa. PPP okviri se preko nepouzdanog podatkovnog kanala šalju enkapsulirani sa L2TP zaglavljima, a zatim i sa prijenosnim zaglavljima kao što su UDP, *Frame Relay*, ATM itd. Kontrolne poruke šalju se preko pouzdanog L2TP kontrolnog kanala. Slijedni brojevi su nužni u svim kontrolnim porukama koje služe da bi osigurale pouzdanu dostavu kroz kontrolni kanal. Podatkovne poruke mogu imati slijedne brojeve za utvrđivanje ispravnog redoslijeda i detekciju paketa koji nedostaju.
L2TP koristi NCP (engl. *Network Control Protocol*) za dodjelu IP adresa i autentikacijske sheme PPP (PAP i CHAP) za autentikaciju korisnika i kontrolu pristupa mrežnim resursima. Da bi se postigla sigurnost, L2TP zahtijeva da odgovarajući prijenosni sloj osigurava servise za šifriranje, provjeru integriteta i autentikaciju za sav L2TP promet. Taj sigurni prijenos odnosi se na cijeli L2TP paket i funkcionalno je neovisan o PPP-u i protokolu koji PPP prenosi. L2TP pažnju obraća samo sa tajnosti, integritetom i autentičnošću L2TP paketa između krajnjih točaka tunela, odnosno LAC i LNS. Kada radi preko IP-a, sigurnost daje IPSec korištenjem ESP i/ili AH.

4. Zaključak

Različitim korisnicima virtualne privatne mreže predstavljaju drugačiji pojam. Unatoč tome poveznica postoji, a to je daljnji razvoj i unaprjeđenje postojećih tehnologija u cilju postizanja sigurnosti. Među

postojećim rješenjima, funkcionalnost se razlikuje od proizvoda do proizvoda, ali većina osigurava mehanizme za šifriranje, autentikaciju udaljenih korisnika i računala, te mehanizme za prikrivanje informacija o topologiji privatnih mreža od potencijalnih napadača na javnim mrežama.
U mnogim slučajevima VPN se zajedno a IPSec i IETF standardima za sigurni TCP/IP nameće kao vrlo prihvatljivo rješenje za mnoge primjene.