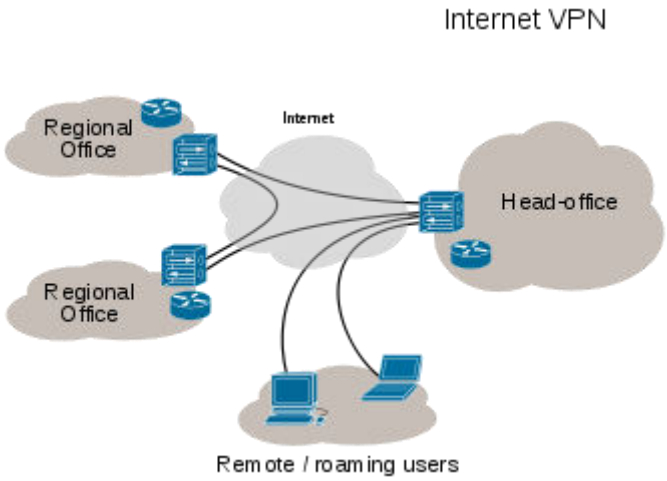
VPN - Virtuelna privatna mreža



Шема ВПН мреже

VPN (енгл. *Virtual Private Network* — Virtuelna privatna mreža) je privatna komunikaciona mreža koja se koristi za komunikaciju u okviru javne mreže. Transport VPN paketa podataka odvija se preko javne mreže (npr. Internet) korišćenjem standardnih komunikacionih protokola. VPN omogućava korisnicima na razdvojenim lokacijama da preko javne mreže jednostavno održavaju zaštićenu komunikaciju.

Arhitektura

Virtuelna privatna mreža omogućava korisnicima da razmenjuju podatke vezom koja je emulirana kao direktna veza (*point-to-point* link - PPP) između klijenta i servera. PPP emulacija dobija se enkapsulacijom podataka zaglavljem koje omogućava rutiranje kroz javnu mrežu do odredišta koje je deo privatne mreže. Podaci su šifrovani i paketi koji su presretnuti u okviru javne ili deljene mreže ne mogu se pročitati bez ključa za dešifrovanje. Infrastruktura javne mreže je nebitna jer korisnik logički vidi samo svoj privatni link, odnosno nalazi se logički u lokalnoj mreži, iako je od drugih korisnika razdvojen javnom mrežom.

Tehnologija tunelovanja

Tunelovanje je najvažnija komponenta tehnologije virtuelnih privatnih mreža i predstavlja prenos paketa podataka namenjenih privatnoj mreži preko javne mreže. Ruteri javne mreže nisu svesni da prenose pakete koji pripadaju privatnoj mreži i VPN pakete tretiraju kao deo normalnog saobraćaja.

Tunelovanje ili enkapsulacija je metod pri kome se koristi infrastruktura jednog protokola za prenos paketa podataka drugog protokola. Umesto da se šalju originalni paketi, oni su enkapsulirani dodatnim zaglavljem. Dodatno zaglavlje sadrži informacije potrebne za rutiranje, odnosno usmeravanje paketa kroz mrežu, tako da novodobijeni paket može slobodno putovati transportnom mrežom.

Tunel

Tunel predstavlja logičku putanju paketa kojom se on rutira preko mreže. Enkapsulirani podaci su rutirani transportnom mrežom sa jednog kraja tunela na drugi. Pojam tunel uvodi se jer su podaci koju putuju tunelom razumljivi samo onima koji se nalaze na njegovom izvorištu i odredištu. Ovi paketi se na mreži rutiraju kao svi ostali paketi.

Početak i kraj tunela nalaze se u VPN mrežama. Kada enkapsulirani paket stigne na odredište vrši se deenkapsulacija i prosleđivanje na konačno odredište. Ceo proces enkapsulacije, transporta i deenkapsulacije paketa naziva se tunelovanje.

Osobine tehnologije tunelovanja

Tehnologija tunelovanja ima osobine čije prednosti značajno doprinose njenoj upotrebi, od kojih su najvažnije:

- Sigurnost – bez obzira što tunel ide kroz nesigurnu javnu mrežu, pristup podacima koji su tunelovani nije dozvoljen neautorizovanim korisnicima što transport čini relativno bezbednim.
- Niska cena – pošto se koriste javne mreže troškovi su dosta niski kada se uporede sa troškovima potrebnim za iznajmljivanje privatnih linija ili implementaciju privatnih Intranet mreža.
- Lakoća implementacije – nema potrebe za promenom postojeće infrastrukture javnih mreža, pa se VPN implementira samo na strani korisnika
- Univerzalnost – zbog enkapsulacije moguće je koristiti i podatke koji pripadaju nerutabilnim protokolima. Takođe se štedi i na broju globalnih IP adresa koje kompanija mora da poseduje, što opet smanjuje cenu implementacije virtuelnih privatnih mreža.

Protokoli koji se koriste pri tunelovanju

Tehnologija tunelovanja koristi tri vrste protokola:

- Protokol nosač - ovi protokoli služe za rutiranje paketa po mreži ka njihovom odredištu. Tunelovani paketi imaju enkapsulaciju ovih protokola. Za rutiranje paketa po Internetu koristi se IP protokol.
- Protokol za enkapsulaciju – ovi protokoli služe za enkapsulaciju originalnih podataka, i koriste se za stvaranje, održavanje i zatvaranje tunela. Najčešće korišćeni su PPTP i L2TP protokoli.
- Transportni protokol – enkapsulira originalne podatke za transport kroz tunel. Najpoznatiji su PPP i SLIP protokol.

Upravljanje

Sa stanovišta upravljanja postoje dva pristupa virtuelnim privatnim mrežama. Razlikujemo VPN kojima upravljaju korisnici, i VPN kojima upravljaju provajderi mrežnih usluga (npr. *Internet Service Provider* - ISP). Virtuelne privatne mreže kojima upravljaju provajderi mrežnih usluga dele se na osnovu toga gde se nalazi oprema koja implementira VPN:

- na strani provajdera (PE - *provider edge*)
- na strani korisnika (CE - *customer edge*).

Bezbednost

Bezbednost je integralni deo VPN usluge. Postoji veliki broj pretnji VPN mrežama:

- Neovlašćeni pristup VPN saobraćaju
- Izmena sadržaja VPN saobraćaja
- Ubacivanje neovlašćenog saobraćaja u VPN (*spoofing*)
- Brisanje VPN saobraćaja
- DoS (*denial of service*) napadi
- Napadi na infrastrukturu mreže preko softvera za upravljanje mrežom
- Izmene konfiguracije VPN mreže
- Napadi na VPN protokole

Odbrana od VPN napada realizuje se i na korisničkom i na nivou provajdera VPN usluga:

- Kriptozaštita paketa
- Kriptozaštita kontrolnog saobraćaja
- Filtri
- Firewall
- Kontrola pristupa
- Izolacija

VPN mreže koje koriste Internet ili druge nebezbedne mreže obično koriste razne metode kriptozaštite. Korisnici VPN mreža sa posebnim zahtevima za bezbednost, na primer banke, obično implementiraju i dodatnu infrastrukturu za zaštitu podataka.