Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

Sustavi za praćenje i vođenje procesa

Seminarski rad
VPN (Virtual Private Network)

Mislav Brković
0036368993
INE

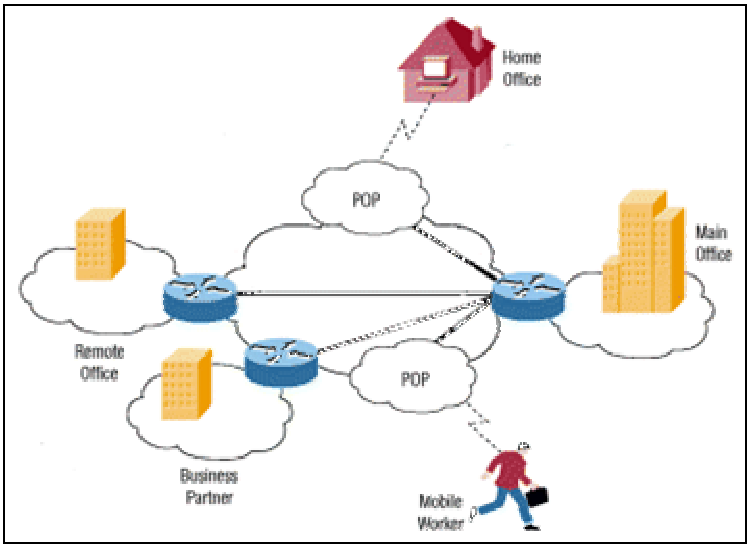
Zagreb
Lipanj, 2005.

Sadržaj

1.Uvod

Svijet se jako promijenio u posljednjih nekoliko desetlječa. Umjesto da se bave samo lokalnim i regionalnim poslovima mnogi poslovni subjekti danas moraju voditi računa o globanim tržištima i logistici. Mnoge kompanije imaju podružnice širom svijeta. Svima im je zajednička potreba za održavanem brze, sigurne i pouzdane komunikacije gdje god im se uredi nalazili. Donedavno su se za održavanje WAN-a (wide area network) koristili zakupljeni vodovi (leased lines). WAN je imao prednosti pred javnom mrežom, kao što je Internet, po pitanjima pouzdanosti, brzine i sigurnosti. Ali održavanje WAN-a, osobito kad se koriste zakupljeni vodovi, može postati prilično skupo i često troškovi rastu s udaljenošću između ureda.

Kako je rasla popularnost Interneta poslovni subjekti su se njime počeli služiti kao sredstvom širenja vlastitih mreža. Danas mnoge kompanije stvaraju vlastite VPNove, kako bi se prilagodili potrebama udaljenih zaposlenika i ureda.



Slika 1.

Na slici 1 prikazana je tipična struktura VPN mreže koja najčešće ima glavni LAN (local area network) u sjedištu kompanije, ostale mreže u udaljenim podružnicama i pojedinačne korisnike.

VPN je, u biti, privatna mreža koja koristi javnu mrežu (najčešće Internet) za spajanje udaljenih mjesta i korisnika.

2. Tipovi VPN-a

Postoje tri tipa VPN-a: Remote-Access VPN, Intranet-based VPN, Extranet-based VPN

2.1.Remote-Access VPN

Remote Access VPN također se naziva VPDN (virtual private dial-up network). Taj tip VPN-a koriste tvrtke čiji zaposlenici imaju potrebu za spajenjem na privatnu mrežu sa različitih udaljenih lokacija. Tvrtka koja želi uspostaviti Remote-Access VPN sa puno vanjskih korisnika koristi usluge ESP-a (enterprise service provider). ESP postavlja NAS (network access server), na kojeg se vanjski korisnici spajaju pomoću desktop client programa.

Dobar primjer kompanije koja treba Remote-Access VPN je velika tvrtka sa stotinama trgovačkih putnika. Remote-Access VPN omogućuje sigurnu kriptiranu vezu između privatne mreže tvrtke i udaljenih korisnika.

2.2. Intranet-based VPN

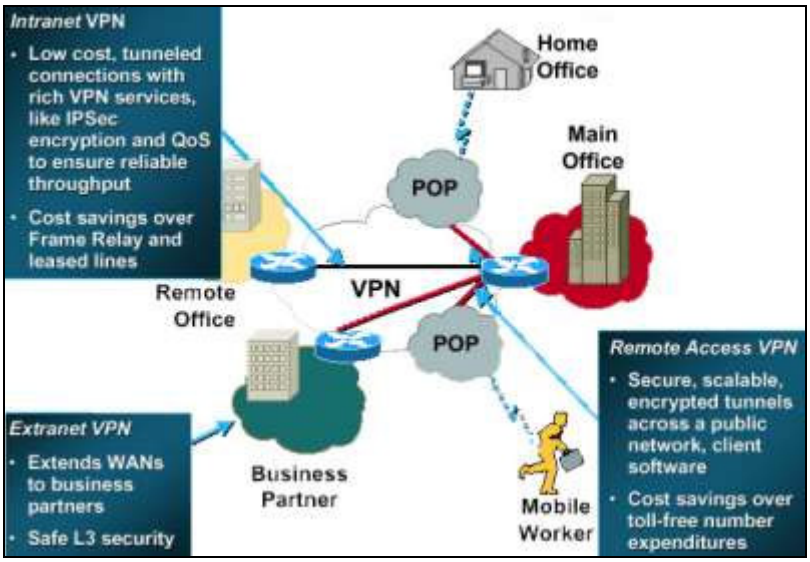
Ako kompanija ima jednu ili više udaljenih podružnica koje želi pridružiti u jednu privatnu mrežu, može stvoriti Intranet-based VPN da bi se spojili LAN-to-LAN.

Postoji nekoliko ključnih prepreka za izgradnju Intranet-based VPN-ova:

- ne postoji standardizirani pristup enkripciji
- odstupanje među proizvodima različitih proizvođača, što dovodi nekompatibilnosti
- nedostatak standarda vezanih za upravljanje javnim ključevima
- nemogućnost Interneta da osigura end-to-end QoS

2.3 Extranet-based VPN

Kad je kompanija u bliskoj vezi s drugom kompanjom (npr. kupcem, dobavljačem ili partnerom), one mogu izdraditi Extranet-based VPN koji ih povezuje LAN-to-LAN i omogućuje svim kompanijam da međusobno dijele resurse.



Slika 2. Primjeri triju tipova VPN mreže

3. Sigurnost

Budući da je Internet javna mreža putem koje se otvoreno prenosi većina podataka, dobro dizajnirani VPN koristi nekoliko metoda za očuvanje sigurnosti veze i podataka:

- Firewall
- Encryption
- IPSec
- AAA Server

3.1 Firewall

Firewall pruža jaku prepreku između privatne mreže i Interneta. Firewall se može podesiti tako da ograničava broj otvorenih portova, tip paketa koji prolaze, i koji su protokoli dozvoljeni.

3.2 Encryption

Enkripcija je proces uzimanja svih podataka koje jedan kompjuter šalje drugome i kodiranja tih podataka u oblik koji će moći dekodirati samo kompjuter kojemu su ti podatci namijenjeni.
Većina sistema za kriptiranje pripada u jedno od kategorija enkripcija:

- Symmetric-key
- Public-key

Kod symmetric key enkripcija svaki kompjuter ima tajni ključ koji može koristiti za enkripciju paketa informcija prije nego što ih putem mreže pošalje drugom kompjuteru. Symmetric-key zahtjeva da znate koji će kompjuteri komunicirati međusobno tako da možete instalirati ključ na njih. Symmetric-key enkripcija je u biti isto što i tajni kod koji svaki od dvaju kompjutera mora znati da bi mogao dekodirati informaciju. Kod pruža ključ za dekodiranje poruke.

Public-key enkripcija koristi kombinaciju privatnog i javnog ključa. Privatni ključ je poznat samo vašem kompjuteru dok javni ključ vač kompjuter daje bilo kojem kompjuteru s kojim želi sigurno komunicirati. Da bi dekodirao kodiranu poruku kompjuter mora koristiti javni ključ, koji je dobio od drugog kompjutera, i svoj privatni ključ.

3.3 IPSec

IPSec (Internet Protocol Security Protocol) pruža napredne oblike zaštite kao što su algoritmi za bolju enkripciju i opsežniju autentifikaciju.

IPSec ima dva enkripcijska načina: tunelsku (tunnel) i transportnu (transport). Tunelska enkripcija enkriptira zaglavlje i korisnu informaciju svakog paketa, dok transportna

enkriptia samo korisnu informaciju. Jedino sustavi koji su IPSec kompatibilni mogu koristiti prednosti ovog protokola. Također svi uređaji moraju imati zajednički ključ, a firewall svake mreže mora imati podešene slične sigurnosne postavke. IPSec može enkriptirati podatke između različitih uređaja kao što su:

- router na router
- firewall na router
- PC na router
- PC na server

3.4. AAA Server

AAA (authentication, authorization, accounting) serveri se koriste za sigurniji pristup u Remote-Access VPN okruženje. Kada zahtjev za uspostavu veze dolazi od dial-up korisnika, zahtjev je proslijeđen AAA serveru. AAA tada provjerava slijedeće:

- tko ste
- što vam je dozvoljeno raditi
- što zapravo radite

4. Tuneliranje

IP paketi koji se razmjenjuju između računala na krajevima VPN kanala su enkriptirani i nečitljivi ostalim korisnicima Interneta. Unutar lokalnih mreža koje se ovim putem povezuju paketi su dekriptirani i čitljivi računalima članovima mreže. Na taj način se postiže isti učinak kao u slučaju dviju mreža spojenih posebnim lokalnim ili zakupljenim vodom, uz sve prednosti takvog načina povezivanja. Ovakva veza se zbog svojih karakteristika naziva i VPN IP tunel, a sam postupak spajanja IP tuneliranje.

Tuneliranje je metoda pakiranja paketa informacija unutar IP paketa tako da može biti sigurno odaslano preko Interneta ili privatne IP mreže.

Osnovna prednost VPN tunela je što se njegovom upotrebom po cijeni pristupa javnoj mreži (Internetu) omogućuje sigurna razmjena podataka sa korisničkih računala iz dviju ili više udaljenih mreža kao da se one nalaze na istoj lokaciji, i spojene su u lokalnu mrežu. Cijene iznajmljivanja posebnog linka kojim bi se povezale udaljene mreže su u pravilu višestruko veće.

Postoje tri ključna protokola tuneliranja:

- Point to Point Tunneling Protocol (PPTP) je razvio Microsoft, 3Com i Ascend. PPTP je protokol koji radi na drugom osi sloju, koji može raditi u ne-IP okruženju, što je prednost za korisnike koji se služe različitim protokolima a ne samo IP-om. PPTP osigurava dobru kompresiju, ali mu je sigurnost slabija strana. Ne pruža enkripciju i upravljanje ključevima, te se oslanja na korisničke lozinke u stvaranju ključeva.
- Layer 2 Tunneling Protocol (L2TP) je još jedan protokol drugog sloja koji može raditi u ne-IP okruženju. Koriste ga primarno pružatelji usluga kako bi saželi i prenijeli VPN promet kroz back bone arhitekturu. Kao i PPTP ne pruža enkripciju niti upravljanje ključevima (iako preporuča IPSec za enkripciju i upravljanje ključevima).
- IPSec (IP security) je IETF protokol koji vodi brigu o cjelovitosti podataka i sigurnosti. Pokriva enkripciju autentifikaciju i razmjenu ključeva. IPSec uključuje 168-bitni enkripcijski ključ, iako veličina ključa može varirati ovisno o sposobnostima svakog kraja veze. IPSec naglašava sigurnost autentifikacijom obaju krajeva tunela, pregovarajući o enkripcijskom protokolu i ključu za enkripciju. No IPSec je ograničen na IP okruženja, svaki korisnik mora imati dobro definiranu javnu IP adresu, te ne može funkcionirati na mrežama koje koriste NAT (network address translation).

5. Zaključak

VPN je privukao pozornost mnogih organizacija koje žele povećati svoje sposobnosti umrežavanja i smanjiti njihove troškove. Uspjeh VPN-a u budućnosti ovisi uglavnom o razvoju tehnologije.

VPN zahtjeva dobro razumjevanje problema sigurnosti javih mreža i poduzimanje mjera opreza kod postavljanja. Osim toga dostupnost i performanse VPN-a neke organizacije ovise o faktorima koji su izvan njihove kontrole, a zbog ne postojanja standarda VPN tehnologije različitih proizvođača često su nekompatibilne.

Najveća vrijednost VPN-a leži u potencijalnom smanjenju troškova tvrtki. Ukoliko cijene međunarodnih poziva i zakupljenih vodova nastave padati sve će manji broj kompanija imati potrebu za prebacivanjem na VPN za udljeni pristup. U protivnom ako se VPN standardi usuglase i različiti proizvodi postanu kompatibilni povećat će se potražnja. Uspjeh VPN-a također ovisi i o mogućnosti intraneta i ekstraneta da obave adekvatno svoje zadaće.

6. Literatura

1) VPN Tutorial, An introduction to VPN software, VPN hardware and protocol solutions
   http://compnetworking.about.com/od/vpn/l/aa010701a.htm
2) How Virtual Private Networks Work by Jeff Tyson
   http://www.howstuffworks.com/vpn.htm
3) Virtual Private Networks (VPNs), International Engineering Consortium
   http://www.iec.org