



Univerzitet Singidunum

Beograd, Bulevar Zorana Đinđića br. 44

Departman za postdiplomske studije
Master studije

-Master rad-

Virtuelne privatne mreže

- Studijski program-

Savremene informacione tehnologije



Univerzitet Singidunum
Beograd, Bulevar Zorana Đinđića br.44

Mentor:

Prof. Dr Ranko Popović

Kandidat:

Marijanović Vuk
Br. Indeksa: 410280/2009

Beograd, 2011

Sadržaj

1. Uvod.....	1
2. Metodologija naučnog istraživanja.....	2
2.1. Predmet istraživanja.....	2
2.2. Ciljevi istraživanja.....	2
2.3. Metodi i tok istraživačkog procesa.....	3
2.4. Struktura rada.....	3
3. Šta predstavljaju virtuelne privatne mreže?.....	4
4. Zašto koristiti VPN?.....	5
5. Klasifikacija virtuelnih privatnih mreža.....	6
5.1. Koncept realizacije.....	6
5.1.1. VPN na nivou aplikacije.....	6
5.1.2. VPN na mrežnom sloju.....	7
5.1.3. VPN na nivou sloja veze.....	8
6. Scenario razvoja Virtuelnih privatnih mreža.....	9
6.1. Intranet.....	9
6.2. Extranet.....	9
6.3. VPN duž višestrukih autonomnih sistema.....	10
6.4. Istovremeni VPN i Internet pristup.....	11
6.5. Hijerarhijske VPN.....	13
6.6. Scenario višestrukog pristupa.....	14
7. Bezbednost.....	15
7.1. Protokoli: PPTP, L2TP, Ipsec.....	17
7.2. Analiza bezbednosti.....	20
8. Brzina i mogućnosti.....	22
9. Konfiguracija VPN konekcije.....	24
9.1. Kako radi VPN konekcija.....	24
9.1.1. Proces VPN konekcije-koraci.....	24
9.1.2. Prednosti VPN-a.....	24
9.2. Komponente VPN konekcije.....	25
9.3. Encryption protokoli za VPN konekcije.....	25
9.4. Konfiguracioni zahtevi za VPN server.....	26
9.5. Konfiguracija VPN-a za udaljene sajtove.....	27
10. Postavljanje VPN server.....	28
11. VPN zasnovane na Internet protokolu i MPLS-u.....	29
11.1. Komutacija koršćenjem labela.....	30
11.2. VPN zasnovane na MPLS-u.....	32
12. Open VPN.....	36

12.1. Ugrađena sigurnost i kriptografski algoritmi.....	37
12.2. Praktični pr. spajanja dve lokacije upotrebom stat. ključa.....	38
12.3. Praktični pr. spajanja dve lokacije upotrebom stat. sertifikata...	41
13. Primer implementacije VPN-a.....	46
14. Postupak kreiranja Virtuelne private mreže.....	48
15. Primer za implementaciju Cisco IPSec VPN servisa.....	55
16. Primer administracije VPN naloga u MUP-u Crne Gore.....	58
17. Realizacija VPN-a u preduzeću Tehpro D.O.O. Beograd.....	65
18. Zaključak.....	74
19. Literatura.....	75

1. Uvod

Lokalne mreže su svakodnevica, srećemo ih na svakom koraku u poslovnim okruženjima a sve više i u kućnim, kada je prisutno više od jednog računara. Osim toga, nemali je broj slučajeva da jedna firma ima više lokacija bilo u istom gradu ili u više gradova ili zemalja. Pretpostavimo li da na svakoj od tih lokacija postoji lokalna mreža, zahtev za njihovo povezivanje i međusobnu razmenu podataka nameće se sam od sebe. Jedan od osnovnih načina za ostvarivanje takve veze koji se do sada koristio, a i dalje se koristi, je povezivanje pomoću iznajmljene linije, sa modemima i ruterima kao hardverskom podrškom. Zakup linije na lokalnom nivou sada i nije previše skup pa tako ostaje samo izdatak za odgovarajuću opremu.

Virtuelne privatne mreže se zaista mnogo koriste i koristiće se jos više u budućnosti. Preveliko je interesovanje za njih i ako se ukuca naziv na Internetu kao rezultat dobija se mnoštvo radova i tekstova vezanih za VPN i to je ujedno i jedan od mnogo razloga zašto je ova tema odabrana. Najviše radova adekvatnih za prezentaciju i obradu ove teme može se naći na sajtu jedne od najvećih kompjuterskih organizacija- IEEE Computer Society.

Virtualna privatna mreža – VPN (Virtual Private Network) je tehnologija koja omogućava sigurno povezivanje privatnih mreža u zajedničku virtualnu privatnu mrežu kroz javnu mrežnu infrastrukturu. Virtualne privatne mreže to čine „preusmeravanjem” putem Interneta ili neke druge javne mreže na način koji pruža istu sigurnost i značaj kao i privatna mreža. Virtualne privatne mreže omogućavaju povezivanje geografski udaljenih lokacija na način koji je ekvivalentan korišćenju iznajmljenih linija.

VPN vam nudi prednosti modemske veze za telefonsko povezivanje uz jednostavnost i fleksibilnost Internet veze. Internet veza omogućava vam da se povežete s resursima širom sveta i istovremeno se, na većini mesta, povežete sa svojom kancelarijom tako da uputite lokalni poziv najbližem telefonskom broju za pristup Internetu. Ako imate brzu internet vezu kao što je kablovska ili digitalna pretplatnička linija (DSL) na računaru i u kancelariji, sa svojom firmom možete komunicirati pri punoj internet brzini. To je mnogo brže od bilo koje modemske veze koja koristi analogni modem. Virtuelne privatne mreže koriste veze čija je autentičnost proverena kako bi se samo ovlašćeni korisnici mogli povezati s vašom mrežom i koristiti šifrovanje. Na taj način ostali korisnici ne mogu presresti ni koristiti podatke koji putuju putem Interneta.

Prednosti koje dolaze iz upotrebe Virtualne privatne mreže su beskrajne. Neke od glavnih uključuju brzinu, fleksibilnost, privatnost, finansijske pogodnosti. Pogodnosti za virtualnu privatnu mrežu ne treba podceniti. One su značajne i mogu u potpunosti izmeniti način na koji radite svoj posao.

2. Metodologija naučnog istraživanja

2.1 Predmet istraživanja

Predmet ovog istraživanja predstavljaju virtuelne privatne mreže, njihov način funkcionisanja, razlozi zašto se koriste i kako se dele, kako se konfigurišu i kako se realizuju.

Rad sadrži kako teorijska objašnjenja tako i praktične prikaze VPN. Date su definicije, objašnjene su prednosti korišćenja VPN-a, data je njihova podela a obuhvaćena je i bezbednost. Pokazano je kako se vrši VPN konekcija i kako se postavlja VPN server. Postoje i dva su primera u radu gde se na slikama vidi kako se one realizuju u stvarnim uslovima.

2.2 Ciljevi i zadaci istraživanja

Cilj rada je jednostavan teorijski prikaz pojma virtuelnih privatnih mreža, podele istih i načina realizovanja njenih konekcija i postavljanja servera bez praktične primene koja je planirana za drugi pristupni rad.

Naučni cilj ovog pristupnog rada je istraživanje i sistematizacija znanja o virtuelnim privatnim mrežama.

Društveni cilj Kako živimo u informatičkom svetu u kojem raste broj korisnika kompjutera, mobilnih telefona i PDA uređaja virtuelne privatne mreže će sve više zauzimati svoje mesto jer mnoge firme već imaju a mnoge će tek koristiti i uživati u pogodnostima virtuelnih privatnih mreža pa ovde imamo nameru da objasnimo budućim korisnicima sve prednosti ove tehnologije.

Osnovni pojmovi koji su od značaja za rad su:

- Virtuelne privatne mreže,
- IP,
- MPLS.
- VPN konekcija i VPN server
- Open VPN
- VPN server

2.3 Metodi i tok istraživačkog procesa

Istraživanje je podržano saznanjima iz međunarodne naučne i stručne literature, odnosno saznanjima drugih autora koji su u svojim člancima i knjigama istraživali problematiku kojom se bavi i ovaj rad. U toku istraživanja, korišćeno je šest principa naučnog saznanja: objektivnost, pouzdanost, opštost, sistematičnost, preciznost i istoričnost ili razvojnost.

Na osnovu postavljenog cilja ovog istraživanja odabrane su metode koje će svojom kombinacijom sačinjavati metodiku rada. U izradi ovog rada korišćeno je više metoda kao što su: metoda modelovanja, metoda analize i sinteze, induktivna i deduktivna metoda i metoda klasifikacije.

2.4 Struktura rada

Rad se sastoji iz 19 poglavlja. U uvodu je data osnovna definicija i prednosti VPN-a i ukratko su dati najvažniji razlozi koji idu u prilog VPN-u.

Metodologija istraživanja je nakon uvoda i odmah posle slede dva poglavlja u kojima se jasno stavlja do znanja šta predstavljaju VPN i zašto ih trebamo koristiti. Logičan redosled podrazumevao bi klasifikaciju VPN-a i ona je u poglavlju 5. Zatim tu je scenario razvoja VPN-a koji se sastoji iz šest delova.

Poglavlje 7 tiče se bezbednosti VPN dok u poglavlju 8 date su brzine i mogućnosti u vidu testiranja VPN kanala sa SDES simetričnom enkripcijom. Poglavlje 9 detaljno objašnjava konfiguraciju VPN konekcije a postavljanje VPN servera je dato u poglavlju 10. Virtuelne privatne mreže zasnovane na Internet protokolu i MPLS-u su u poglavlju 11.

Posebno interesantan pojam u radu odnosi se na OpenVpn i on je detaljno obrađen u poglavlju 12. Sa realizacijom u radu počinje se u poglavlju 13 gde je dat prvi primer implementacije VPN-a. Odmah zatim nastavlja se sa realizacijom i vec u sledećem poglavlju 14 u najmanji korak dat je postupak kreiranja Virtuelne privatne mreže. Poglavlje 15 sadrži primer za implementaciju Cisco IPSec VPN servisa. Zatim u poglavlju 16 dat je primer administracije VPN naloga u Ministarstvu unutrašnjih poslova Crne Gore. U 17 poglavlju data je realizacija VPN-a u preduzeću TEHPRO D.O.O. Beograd koja je i vrhunac ovoga rada.

Svrha zaključka u radu je da podseti na prednosti korišćenja VPN mreža kao i da podseti na glavne elemente vezane za ovu temu.

3. Šta predstavljaju virtuelne privatne mreže?

Od vremena kada je ljudska populacija stekla mogućnost komunikacije, imamo potrebu da određeni deo te konverzacije privatizujemo, odnosno ograničimo broj onih koji učestvuju u toj komunikaciji. Bez obzira na prenosni medij, kreirane su različite tehnologije za skrivanje sadržaja komunikacije od neželjenih slušalaca: od običnog šaputanja pa sve do današnjih zaštićenih (skremblovanih) TV kanala. Privatnom konverzacijom razdvajamo pozvani auditorijum od svih ostalih. Generalno gledano, postoje dva načina za privatizovanje konverzacije: fizička separacija, gde samo odabrana publika može da pristupi komunikaciji, i šifriranje informacije, gde mnogi mogu da registruju odaslane signale, ali samo oni odabrani mogu i da razumeju taj signal. Kada se komunikacija odvija u nekom od javnih medija, skrivanje, tj. šifriranje informacije je jedina solucija.

U istorijskom smislu gledano, Internet je nova vrsta medija koja je napravila velike izmene u načinu na koji ljudi međusobno komuniciraju, a istovremeno je fundamentalno izmenio i socijalnu i komercijalnu interakciju. Pri tome, u sferi poslovanja Internet je rapidno postao komunikacioni medij izbora. Zbog toga se ovde posebno ističe problem poslovne privatne komunikacije, jer je Internet javni medij. U tehnologiji virtuelnih privatnih mreža (virtual private network - VPN), primenjene su brojne različite mrežne tehnologije radi postizanja cilja - obezbeđivanja privatnosti poslovne komunikacije unutar javne Internet infrastrukture.

Koncept virtuelnih privatnih mreža (VPN) sastavljen je iz dva dela: virtuelne mreže, koja leži na vrhu sveprisutne interkonekcije na Internetu, i privatne mreže za poverljivu komunikaciju i ekskluzivnu upotrebu. U frazi VPN ono "virtuelna" implicira da ne postoji izdvojena fizička mrežna infrastruktura. Umesto toga, imamo fizički jednu mrežnu infrastrukturu (Internet), koju deli veliki broj različitih logičkih mreža (podmreža). Na primer, možete koristiti isti mrežni pristupni tok za pristup Internetu, za konekciju na različite korporativne sajtove, i za pristup drugim poslovnim mrežama. Ovakve virtuelne mreže omogućavaju konstrukciju dodatnih logičkih mreža samo izmenom konfiguracije različitih uređaja. Ovakav pristup donosi brži razvoj i smanjenje troškova koji bi se utrošili na postavljanje fizičke infrastrukture. Možda je i bitniji aspekt virtuelnih mreža "privatnost". Osnovni cilj privatnih mreža je održavanje poverljivosti informacija (podataka), tako da oni mogu biti primljeni samo od strane onih kojima su i upućene.

4. Zašto koristiti VPN?

Nakon upoznavanja sa osnovnim konceptom virtuelnih privatnih mreža u prethodnom prilogu, pokušaćemo da vam navedemo nekoliko glavnih razloga za upotrebu Internet orijentisanih VPN-a, umesto korišćenja mreža fizički odvojenih od ostalih. Glavne prednosti koje se stižu konverzijom postojećih izdvojenih privatnih mreža u Internet virtuelne privatne mreže su :

- **Širok spektar primene** - Internet nudi mnogo veći spektar primena u odnosu na privatne mrežne infrastrukture i one koje nude lokalne telekomunikacione kompanije. Dodavanjem novih tačaka spajanja privatnim mrežama povećavamo mogućnosti poslovnih kontakata. Za razliku od Interneta, koji objedinjuje javne i privatne konekcione tačke duž čitavog sveta, kod privatnih mreža (uglavnom lokalnog tipa) servis-provajderi nude samo ograničen broj interkonekcija, a u vezi s tim i smanjene mogućnosti poslovanja. Internet predstavlja ogromnu interkonekciju heterogenih (raznorodnih) mreža. Bilo koji host (što znači i vaš server) koji je spojen na mrežu, spojen je i na Internet, što znači da ima vezu sa bilo kojim hostom koji se nalazi sa druge strane sveta. Taj drugi host može biti vaša poslovница udaljena fizički i hiljadama kilometara, što je praktično neizvodljivo spajanje u jednu privatnu fizičku mrežu.
- **Smanjenje troškova?** - Još jedna velika prednost koja se dobija uvođenjem Internet zasnovanih virtuelnih privatnih mreža jeste i redukcija troškova poslovanja. Najjednostavnije rečeno, uvođenjem VPM mreža eliminisaćete potrebu za naručivanjem i izgradnjom većeg broja specijalnih infrastrukture koje će služiti različitim tipovima komunikacionih potreba unutar kompanije. Zamislite samo koliko bi iznosilo zakupljivanje telekomunikacione linije između recimo Beograda i Moskve, za potrebe firme. Mnogo je bolje iskoristiti višestruko jeftinije Internet veze.
- **Bezbednost** - Kod VPN-a koriste se kriptografske tehnologije koje obezbeđuju poverljivost i integritet podataka koji se nalaze u tranzitu. Autentikacija i kontrola pristupa ograničavaju pristup kompanijskoj mreži, i njenim resursima i servisima. Kod tradicionalnih privatnih mreža, bezbednost tokom tranzita podataka leži na provajderu telekomunikacionih usluga (telekom), tj. njegovoj sposobnosti obezbeđenja podataka. Tako na primer, *frame relay* mreže nemaju ugrađenu mogućnost šifriranja *frame*-ova podataka. Prema tome, ukoliko podaci budu presretnuti od strane nepozvanih osoba, vrlo lako će biti dekodirani. Umesto toga, kod VPN-a, podaci su zaštićeni kriptografijom.
- **E-Commerce** - Sve više i više poslovanje biva uslovljeno upotrebom Internet servisa. Elektronsko poslovanje (*e-commerce*) nije samo novi metod za prodaju robe krajnjim kupcima ("B2C" skraćenica za business-to-consumer) već je i način za komunikaciju i poslovanje između poslovnih subjekata ("B2B" skraćenica za business-to-business). Povezivanje i interakcija poslovnih subjekata je esencijalna stvar, a Internet je logičan izbor za ostvarivanje te interkonekcije.

5. Klasifikacija Virtuelnih privatnih mreža

Klasifikacija Virtuelnih privatnih mreža se ostvaruje kroz tri kategorije:

- 4.1 Koncept realizacije
- 4.2 Način pristupa od strane korisnika
- 4.3 Bezbednost i zaštita podataka

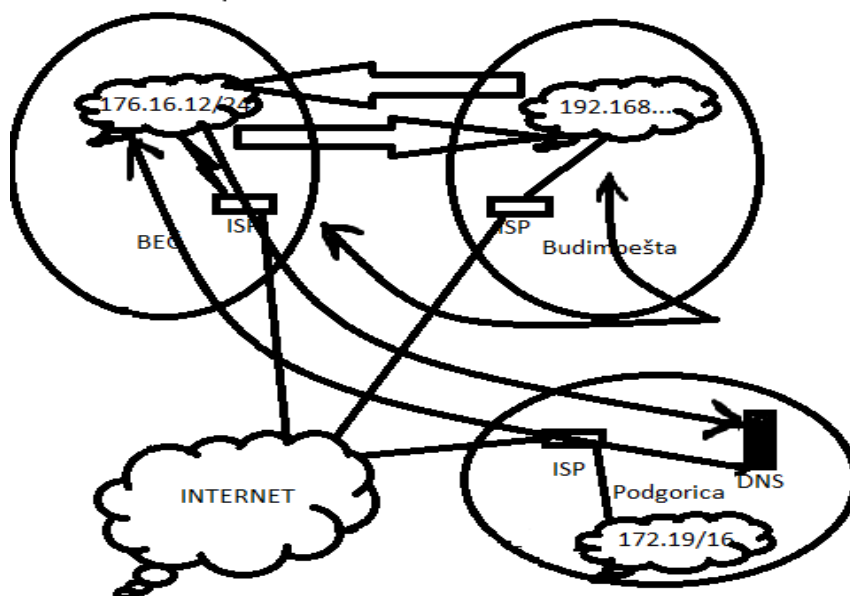
5.1. Koncept realizacije

U koncept realizacije spadaju:

- VPN na nivou aplikacije (*application-layer VPN*)
- VPN na nivou protokola mrežnog sloja (*network-layer VPN*)
- VPN na nivou protokola sloja veze (*data-link layer VPN*)

5.1.1. VPN na nivou aplikacije

Realizuje se korišćenjem DNS servera za formiranje VPN. DNS je veza između naziva i IP adresa računara. IP adrese zavise od lokacije računara i topologije mreže dok su nazivi nezavisni od fizičke topologije mreže. Svaka firma na internetu ima svoj domen (npr. **firma.cg.me**) pa računari registrovani unutar tog domena krajnjem korisniku stvaraju privid pripadnosti istoj korporacijskoj mreži. Za krajnjeg korisnika lokacija pojedinih računara nije bitna - on će uvek koristiti nazive za pristup pojedinim računarima u mreži.



Slika 1. VPN na nivou aplikacije

Prednosti ove vrste realizacije su jednostavna i jeftina implementacija-svodi se na konfigurisanje DNS servera.

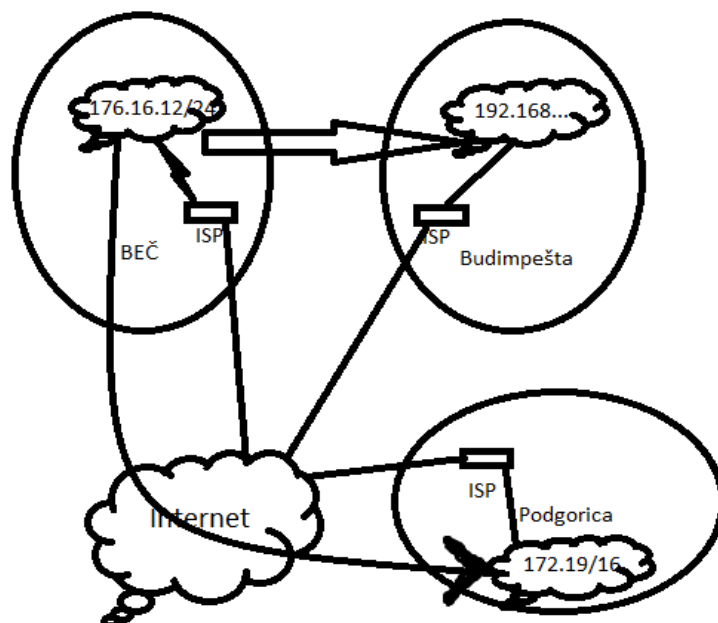
Nedostaci ove vrste realizacije su:

- Pri promeni provajdera neophodna je renumeracija kompletne mreže, kao i znatne izmene podataka u DNS-u.
- U toku renumeracije mreža uglavnom nije upotrebljiva.
- Komplikovana za konfigurisanje i održavanje i upravljanje.
- Složenost održavanja povećava se kako se povećava broj lokacija.
- DNS saobraćaj može lako da se lažira od strane zlonamernika.
- Mreža se nikakvim mehanizmima ne štiti od zlonamernika.

5.1.2. VPN na mrežnom sloju

Realizuje se kroz **metodu kontrolisanog rutiranja** koja se koristi uglavnom u okruženjima gde korisnici ne pristupaju direktno internetu i kroz **metodu logičkih tunela**. Da bi se prva ostvarila trebaju se obaviti dve radnje na ruteru i to :

- Isključiti *default* putanju (0.0.0.0).
- Ubaciti statičke putanje (*static routes*) ka mreži provajdera, za sve IP mreže koje se koriste unutar korporacijske mreže.



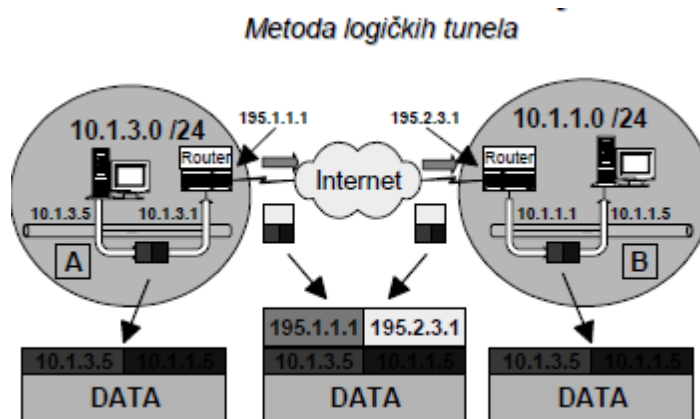
Slika 2. VPN na mrežnom sloju, rešenje sa javnim adresama

Prednost ove metode ogleda se u tome da je rešenje krajnje jednostavno jer se svodi na dodatnu konfiguraciju rutera. Dodatni nivo zaštite može da se ostvari korišćenjem *firewall* servera na pojedinim lokacijama.

Što se tiče metode logičkih tunela pre svega ćemo objasniti šta su logički tuneli. Logički tuneli su mehanizmi prenosa poruka raznih protokola unutar IP datagrama. Omogućavaju formiranje VPN koje koriste kako IP, tako i sve ostale često korišćene protokole: IPX, DECnet, SNA itd. Pakovanje poruka u IP datagrame, kao i njihovo raspakivanje se vrši na dva jasno definisana rutera u mreži (*tunnel endpoints*).

Logički tuneli mogu biti uspostavljeni:

- Između dve fiksne tačke u mreži (*point-to-point*)
- Između jedne i više fiksnih tačaka u mreži (*point-to-multipoint*).



Slika 3. VPN na mrežnom sloju, metoda logičkih tunela

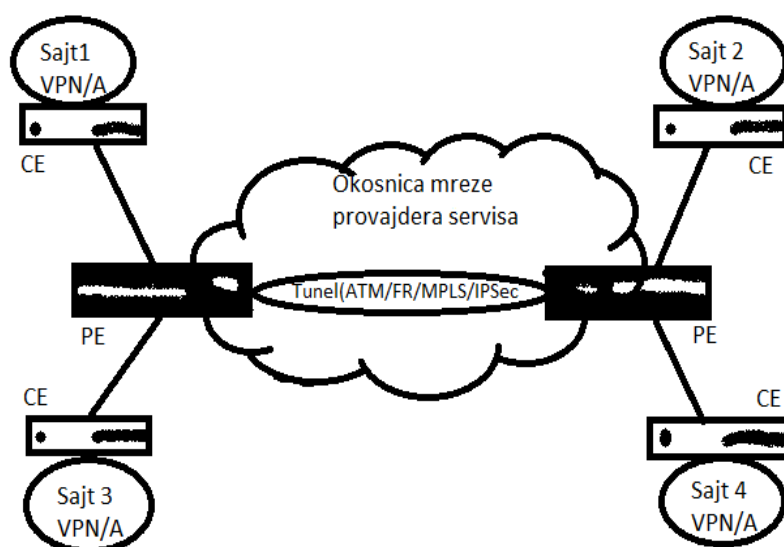
5.1.3. VPN na nivou sloja veze

Tu se takođe pominje metoda logičkih tunela-MPLS. Ta metoda je nastala iz *layer 2* tehnologija tipa Frame Relay i ATM. Svakom IP datagramu dodaje se labela koja označava kojoj VPN taj datagram pripada. MPLS VPN mreže su skalabilne jer se veoma lako proširuju dodavanjem novog čvora u mrežu što nije slučaj sa tunelima nastalim enkapsulacijom saobraćaja u IP datagram. Za sada se isključivo koriste u IP mrežama.

6. Scenario razvoja Virtuelnih privatnih mreža

6.1. Intranet (veza sajtova u istoj organizaciji)

U ovom slučaju VPN je formirana između sajtova koji pripadaju istoj organizaciji. To je slučaj kada se različite filijale međusobno povezuju ili kada se povezuju sa upravom. Na slici 4. na provajderove rutere PE (Provider Edge Device) se vezuju sajtovi korisnika preko korisnikovog krajnjeg uređaja CE rutera. Ta veza može biti ostvarena na različite načine (npr. statičkim rutiranjem, preko ATM VC)

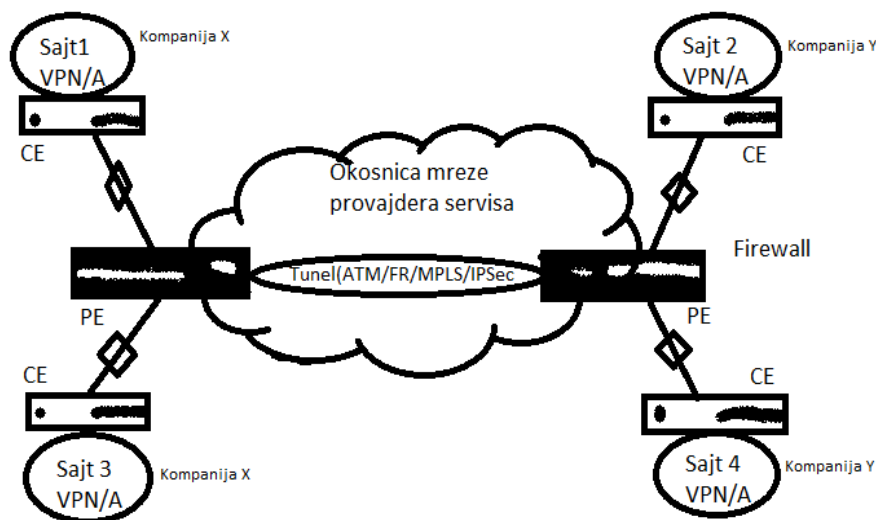


Slika 4. Primer intranet scenarija

6.2. Extranet (veza sajtova koji pripadaju različitim organizacijama)

U ovom scenariju, dve ili više oraganizacija imaju pristup ograničenom broju zajedničkih lokacija. Osnovna razlika između extraneta i interneta je da provajder mora eksplicitno da konfiguriše dostupnost između VPN i da obezbedi postojanje neke vrste kontrolnog pristupnog mehanizma pri povezivanju različitih organizacija. Ta kontrola pristupa može biti ostvarena firewall-om, listom pristupa na ruterima ili sličnim mehanizmima koji će omogućiti primenu kontrole pristupa zasnovanu na postojanju polisa tranzitnom saobraćaju. Svi ti mehanizmi kontrole pristupa mogu biti postignuti korišćenjem posebnih uređaja ili mogu biti biti integrisani u PE uređajima. Taj scenario je prikazan na slici 5. U tom primeru su formirane dve VPN koje povezuju Kompaniju X i Kompaniju Y. Za kontrolu pristupa koristi se firewall. Dodatni mehanizmi autentifikacije kao što je razmenjivanje sertifikata o autoritetu je takođe poželjno. Moguće je da sajt pripada i višestrukim VPN, koji mogu da

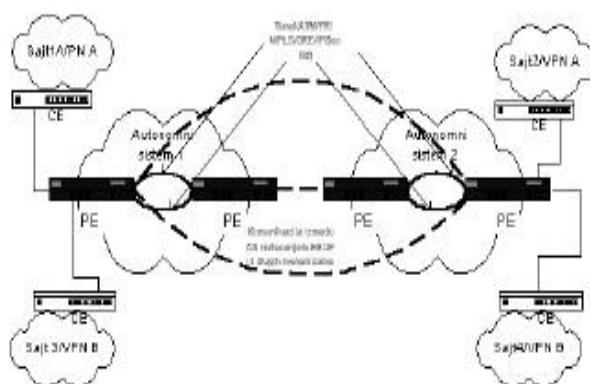
uključuju sa jedne strane intranet, a sa druge extranet. Extranet može da postoji duž backbone-a jednog provajdera ili duž više backbone-a ili autonomnih sistema.



Slika 5. Primer Extranet scenarija

6.3. VPN duž višestrukih autonomnih sistema ili provajdera servisa:

Po ovom scenariju virtuelna privatna mreža može da se širi preko mreža više provajdera servisa ili Autonomnih sistema. Osnovni predmet u tim slučajevima je pitanje komunikacije i sigurnosti između PE uređaja koji pripadaju različitim AS. Komunikacija između njih može biti ostvarena na različite načine u zavisnosti od pristupa koji je primenjen pri formiranju IP VPN. Pitanje sigurnosti između PE koji pripadaju različitim AS može biti rešeno korišćenjem PE-PE tunela (na primer IPSec tuneli mogu biti korišćeni da obezbede enkripciju duž AS). VPN ruta distribucije preko AS treba da bude ostvarena tako da izgleda kao da postoji jedan tunel od ulaznog PE u jednom AS do izlaznog PE u drugoj AS. Ovaj scenario je prikazan na slici 6. Isprekidana linija prikazuje kako se tunel "ulaz PE - izlaz PE" pojavljuje kada je komunikacija između AS ispravno ostvarena. Naravno, pri tome treba voditi računa o preduslovu da bi ta veza bila ostvarena, a to je postojanje dogovora o poverenju između uključenih provajdera servisa.



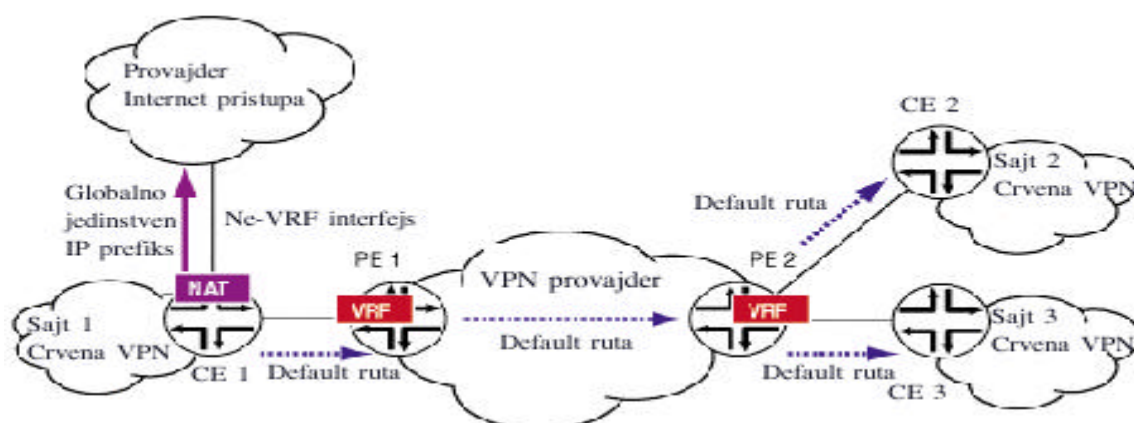
Slika 6. VPN preko više Autonomnih sistema

6.4. Istovremeni VPN i Internet pristup

Mnogim hostovima na Internetu treba istovremeno omogućiti i pristup Internetu, kao i drugim VPN sajtovima. Tu je mogao da nastane problem jer mnoga preduzeća koriste sopstveni privatni adresni prostor. Generalno postoje tri načina kako VPN mogu da koriste globalno jedinstvene adrese za komunikaciju sa drugim hostovima.

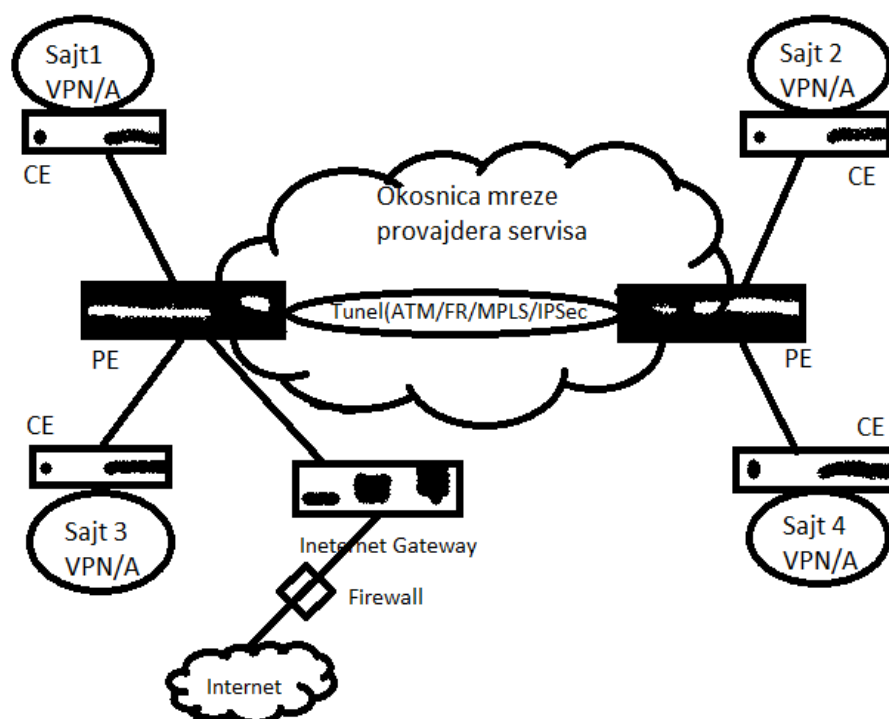
- da svi sistemi na privatnoj mreži koriste globalno jedinstvene IP adrese, što baš i nije odgovarajuće kada su adrese već dodeljene, jer ih treba menjati.
- ako samo mali broj korisnika treba da ima mogućnost pristupa Internetu onda samo njima dodeliti javne IP adrese. Uobičajeno je u mnogim firmama da neki korisnici imaju privatne IP adrese, a da istovremeno neki sistemi koriste javne.
- korišćenje Network Address Translator (NAT) servera u privatnoj mreži može da omogući korisnicima VPN kojima su dodeljene privatne IP adrese da pristupe Internetu.

Postoje i metode u okviru BGP/MPLS VPN modela koje mogu da iskoriste to. Jedan način za to je i korišćenje ne-VRF Internet pristupnog mehanizma. Korisnici VPN sajta mogu direktno da pristupe Internetu preko Internet gateway-a. On može da se ostvari na ne-VRF interfejsu ili na CE ruteru ili na nekom drugom ruteru na korisničkoj strani. Interfejs na ruteru koji omogućava Internet pristup je konfigurisan tako da ima funkciju Internet firewall-a i NAT (slika 7). Sada kako bi se omogućilo korisnicima VPN da pristupe javnom Internetu, CE1 na sajtu 1 šalje default rutu PE1, koja se postavlja u njegovu VRF, a zatim je BGP protokolom šalje PE2 ruteru, a on dalje CE2 na sajtu 2 i CE3 na sajtu 3. Kao rezultat toga svi hostovi VPN prosleđuju Internet saobraćaj CE1 ruteru na sajtu 1, koji rutira saobraćaj preko NAT interfejsa na Internet. NAT translira svaku privatnu izvorišnu adresu u javnu adresu. Kako bi se omogućilo hostovima na Intranetu da odgovore hostovima na VPN, CE1 dodaje javni IP prefiks u Internet tabelu rutiranja. Kada paket stigne na CE1 NAT interfejs, NAT servis translira javne u privatne odredišne adrese.



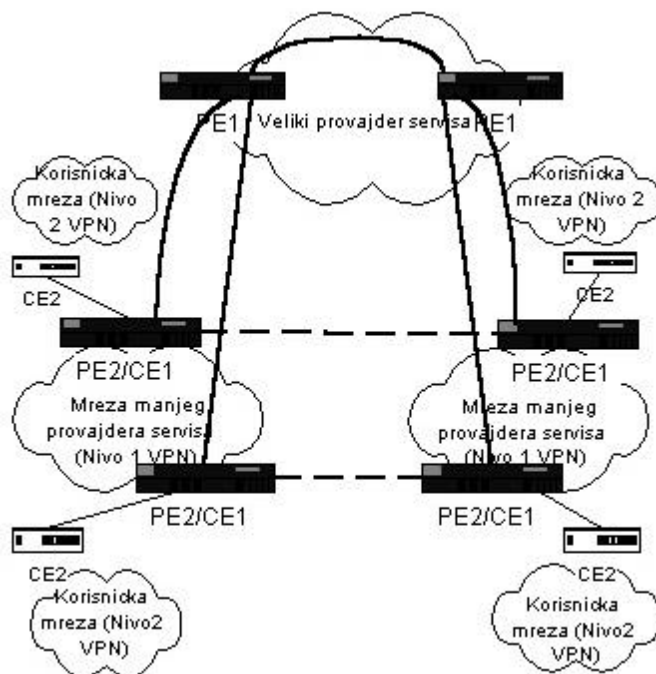
Slika 7. Primer uspostavljanja default rute za istovremeni pristup VPN i Internetu

Saobraćaj koji sa Interneta stiže na odgovarajući sajt u VPN prosleđuje se Internet rutama koji vode na sajtove u VPN. Unutrašnja struktura VPN je nevidljiva za Internet. Postojanje firewall može biti poželjno kako bi se smanjio pristup privatnim mrežama sa Interneta (slika 8).



Slika 8. Istovremeni VPN i Internet pristup

6.5. Hijerarhijske VPN (VPN unutar VPN)

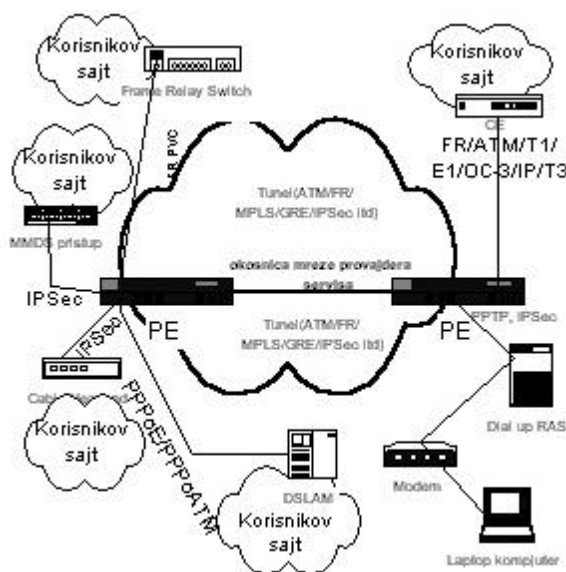


Slika 9. Hijerarhijske VPN

U ovom scenariju provajderi servisa koji obezbeđuju VPN mogu u stvari biti korisnici nekog većeg provajdera. Takav provajder može biti jedna velika VPN sa više malih VPN u okviru nje. Logički tuneli Nivoa 2 VPN su prikazani isprekidanom linijom, dok puna linija predstavlja stvarne CE1-CE1 (tj. PE2-PE2) tunele preko velike mreže provajdera servisa. Stoga, CE uređaji Nivoa 1 VPN treba da budu uključeni u mehanizme uspostavljanja VPN.

6.6. Scenario višestrukog pristupa

IP VPN treba da podržava više tipova pristupnih scenarija, na primer treba da budu podržani statičko rutiranje, ATM PVC, korišćenje različitih protokola rutiranja, xDSL modema i dial pristup. Pri tome se mogu koristiti različiti uređaji za razdvajanje različitih pristupnih mehanizama ili te funkcije mogu biti integrisane u PE uređajima. Na slici 10. je ilustrovan IP VPN sa podrškom za različite pristupne mehanizme.



Slika 10. Scenario višestrukog pristupa

7. Bezbednost

Virtuelna privatna mreža (VPN) predstavlja poseban način komunikacije računara preko Internet ili Intranet infrastrukture. Tri su osnovne primene VPN-a:

- Pristup udaljenom računaru
- Povezivanje lokalnih mreža preko Interneta
- Povezivanje lokalnih mreža preko Intraneta

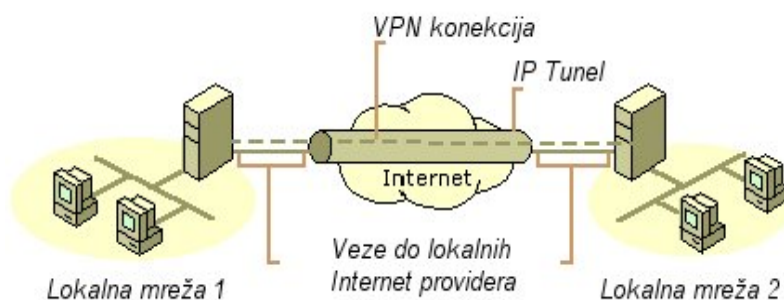
Najvažniji razlog korišćenja virtualnih privatnih mreža je ekonomski, ali virtualne privatne mreže pružaju i sledeće sigurnosne prednosti:

- Omogućena je sveukupna kriptografija podataka Virtualne privatne mreže obuhvataju celi promet koji se koristi, odnosno svi mrežni podaci koji se prenose su kriptovani. Na taj se način osigurava mrežni promet, tako da neovlašćene osobe nisu u mogućnosti doći do informacije koje unutrašnji računar koristi, koji je korišćeni protokol itd.

- Mogućnost udaljenog korišćenja protokola koje je teško osigurati na drugi način. Pojedine protokole je zbog svoje funkcionalnost vrlo teško koristiti u sigurnom okruženju koje se postiže korišćenjem paketnog filtriranja i proxy servisa. Virtualne privatne mreže omogućavaju kriptovanjem podataka siguran udaljen pristup korišćenjem ovih protokola.

Bilo da se radi o povezivanju samo jednog računara na udaljenu mrežu (kao u prvoj primeni), ili da se putem VPN-a povezuju dve mreže na udaljenim lokacijama (druga primena), komunikacija između subjekata ove strukture zaštićena je enkripcijom čije parametre dogovaraju obe strane. Izbor enkripcijskog algoritma i dužine ključa je od suštinskog značaja za sigurnost uspostavljene komunikacije, i tek u slučaju treće primene, gde komunikacija između mreža nije javna, enkripcija igra nešto manju ulogu.

Na slici je prikazan najčešći način upotrebe VPN-a. Dve lokalne mreže povezane su VPN kanalom u jedinstvenu celinu korišćenjem Internet infrastrukture.



Slika 11. Struktura VPN-a između dva LAN-a

IP paketi koji se razmenjuju između računara na krajevima VPN kanala su enkriptovani i nečitljivi ostalim korisnicima Interneta. Unutar lokalnih mreža koje se ovim putem povezuju paketi su dekriptovani, i čitljivi računarima članovima mreže. Na taj način se postiže isti efekat kao u slučaju dve mreže spojene posebnim lokalnim ili iznajmljenim linkom, uz sve prednosti takvog načina povezivanja. Ovakva veza se zbog svojih karakteristika naziva i VPN IP tunel, a sam postupak spajanja IP tunelovanje.

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

Enkripcijski protokoli VPN-a osiguravaju takođe i autentikaciju tj. dokazivanje identiteta između računara ili uređaja na krajevima tunela. Prenos komunikacionih parametara je enkriptovan, a enkripcijski ključevi se menjaju u toku same komunikacije. Pravilnom konfiguracijom operativnih sistema računara koja čine lokalne mreže, moguće je dalje sprovesti i odgovarajuću autorizacionu politiku, tj. odrediti koji će resursi biti dodeljeni kojim korisnicima u povezanim mrežama. Pri tom se korisnici iz udaljene mreže u potpunosti mogu tretirati kao lokalni korisnici, sa svim pravima i ograničenjima (npr. prilikom određivanja prava pristupa deljenim direktorijima u Microsoft mrežama).

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
- Filteri
- Firewall
- Kontrola pristupa
- Izolacija

Analize bezbednosti mreže na Internetu su ukazale da su Virtuelne privatne mreže danas najbezbednija tehnologija za komunikaciju svih vrsta podataka preko otvorene javne globalne mreže kao što je Internet. One emuliraju vezu tačka-tačka tunelovanjem podataka, sa enkapsulacijom i enkripcijom pomoću bezbedonosnih protokola, čime ostvaruju privatnost, integritet i raspoloživost, što su osnovni elementi bezbednosti svake mreže. Ipak i ove mreže pokazuju ranjivost na neke standardne napade Internet okruženja i generalno tretiranje ovih mreža kao bezbedne ne opstaje, pa su u ovom poglavlju razmatrani bezbedonosni aspekti postojećih standardnih tipova ovih mreža.

Analizirane su tri vrste Virtuelnih privatnih mreža, sa standardnim protokolima PPTP(Point-to-Point Tunneling Protocol),L2TP(Layer 2 Tunneling Protocol) i IPsec(IP Security Protocol), i ugrađenim bezbedonosnim funkcijama, i izvršena je komparacija u odnosu na kriterijum otpornosti na standardne napade na Internetu. Pored analize bezbedonosnih elemenata protokola , uvedena je i njihova ocena otpornosti na napade u Internet okruženju, koja daje odgovore na pitanja o nivoima bezbednosti Virtuelnih privatnih mreža sa ovim protokolima.

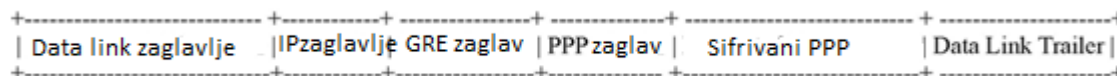
7.1. Protokoli: PPTP, L2TP, Ipsec

Tipovi Virtuelnih privatnih mreža se zasnivaju na implementaciji više različitih protokola od kojih su protokoli PPTP,L2TP i IPsec najzastupljeniji.

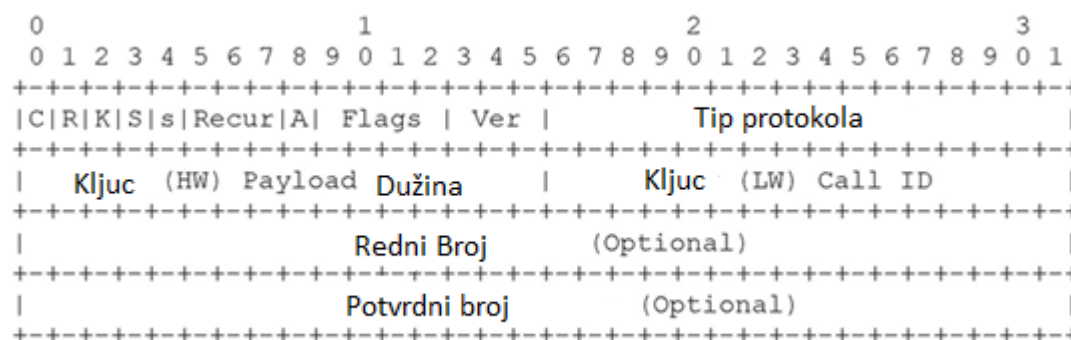
Protokol **PPTP** je najstariji protokol za realizaciju Virtuelnih privatnih mreža i bazira se na PPP(Point-to-Point) protokolu – najpoznatijem mrežnom protokolu komunikacije od tačke do tačke. PPTP protokol vrši enkapsulaciju PPP paketa od polazne tačke, preko Interneta, do odredišta. Za autentifikaciju korisnika koristi PPP protokole PAP(Password Authentication Protocol) ili CHAP(Challenge Handshake Authentication Protocol). PAP protocol predstavlja standardnu proceduru logovanja klijenta kod servera sa korisničkim imenom i lozinkom. CHAP protocol koristi periodično generisani string koji server šalje klijentu. Ovaj primenjuje Hash funkciju na taj string i otisak kao rezultat vraća serveru. Server obavlja istu Hash operaciju, i autentifikuje klijenta ako je rezultat isti sa onim dobijenim od klijenta.

Za tunelovanje PPP paketa preko Interneta PPTP protokol koristi GRE(Generic Routing Encapsulation) protokol. GRE je opšti protokol koji enkapsulira bilo koji protokol od jedne do druge tačke u mreži.

Kriptovanje tunelovanih PPP paketa u PPTP protokolu vrši MPPE (Microsoft Point-to-Point Encryption) protokol. MPPE protokol koristi za kriptovanje RSA RC4 algoritam, sa ključevima dužine 40 ili 128 bita koji se menjaju periodično. Slike 11 i 12 prikazuju izgled PPTP datagrama i GRE zaglavlja respektivno. PPTP protokol je protokol drugog nivoa OSI modela i omogućuje enkapsulaciju (GRE zaglavlje), pored IP protokola, još i drugih protokola višeg nivoa, kao što su IPX i NetBEUI. Polje Call ID u GRE zaglavlju definiše sesije kojima pripadaju PPP paketi. Paketi u okviru sesije su numerisani (polje Sequence Number) i sa potvrdom paketa (polje Acknowledgment Number) obavlja se kontrola toka paketa.



Slika 11.

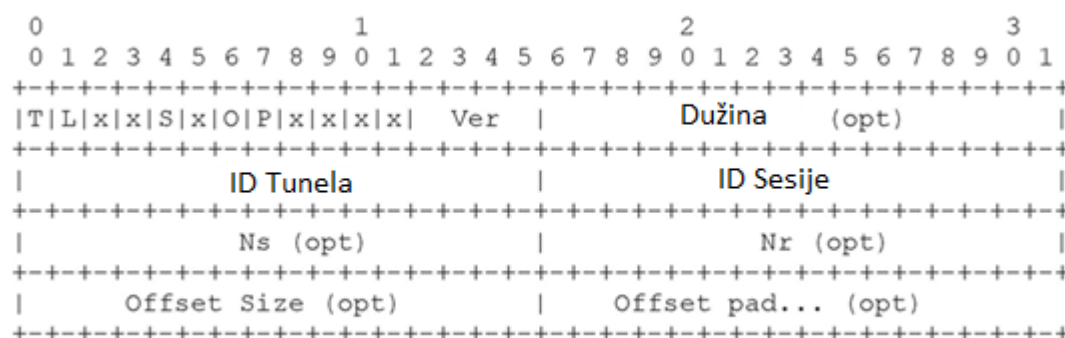


Slika 12.

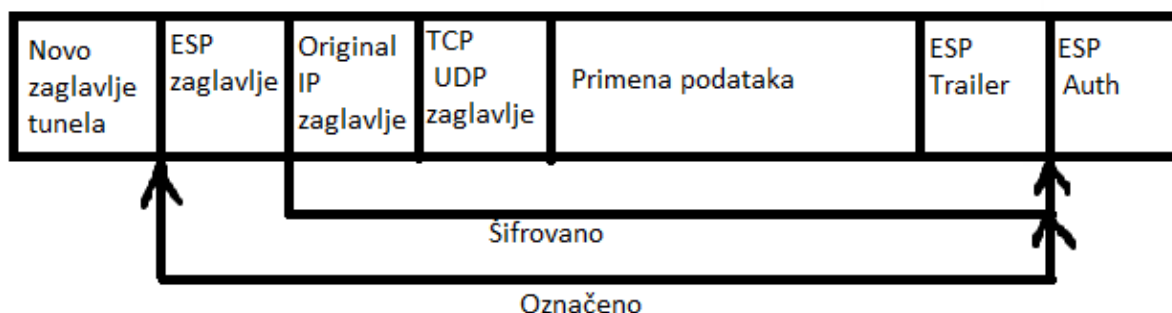
L2TP je sledeći protokol Virtuelnih Privatnih Mreža. Osim preko Interneta ovaj protokol omogućuje enkapsulaciju PPP paketa jos i preko X.25, Frame Relay i ATM mreža. Za transport preko Interneta koristi UDP(User Datagram Protocol) protokol, port 1701. L2TP protokol ima pored poruka podataka i kontrolne poruke za održavanje tunela, a i mogućnost kompresije zaglavlja čime se povećava propusna moć veze. Za autentifikaciju korisnika L2TP protokol se oslanja na PPP protokole PAP i CHAP. Format L2TP zaglavlja je prikazan na slici 13. Polje Tunnel ID služi za identifikaciju tunela, pošto protokol može da obezbedi više tunela po jednoj konekciji, a Session ID dvobajtno polje u zaglavlju definiše sesiju kojoj pripadaju paketi. Kontrolu toka obezbeđuju polja Ns i Nr iz zaglavlja. Ns definiše redosled poslate kontrolne poruke ili poruke podataka, a Nr određuje broj sledeće poruke koja se očekuje u prijemu. Bit P u zaglavlju obezbeđuje prioritetni tretman poruke u prenosu, a bit T ukazuje da li je poruka kontrolna ili je poruka podataka. Protokol L2TP nema mogućnost enkripcije i pri korišćenju preko Interneta za to koristi protokol IPsec.

Protokol **IPsec** je namenski bezbedonosni protokol koji poseduje sve attribute za formiranje Virtuelnih privatnih mreža preko Interneta. Sa enkapsulacijom IPsec protokol omogućuje autentifikaciju i enkripciju svakog IP paketa u prenosu. To je veoma složen protokol koji sadrži dva tipa – AH(Authentication Header) i ESP(Encapsulating Security Payload), a svaki taj tip ima dva moda – transport i tunel. ESP format IPsec protokola obezbeđuje autentifikaciju, integritet i privatnost podataka, dok AH format obezbeđuje samo autentifikaciju i integritet. U transportnom modu svaki od ova dva tipa bezbedno prenose postojeći IP paket od izvora do odredišta, dok u tunel modu se postojeći paket stavlja unutar

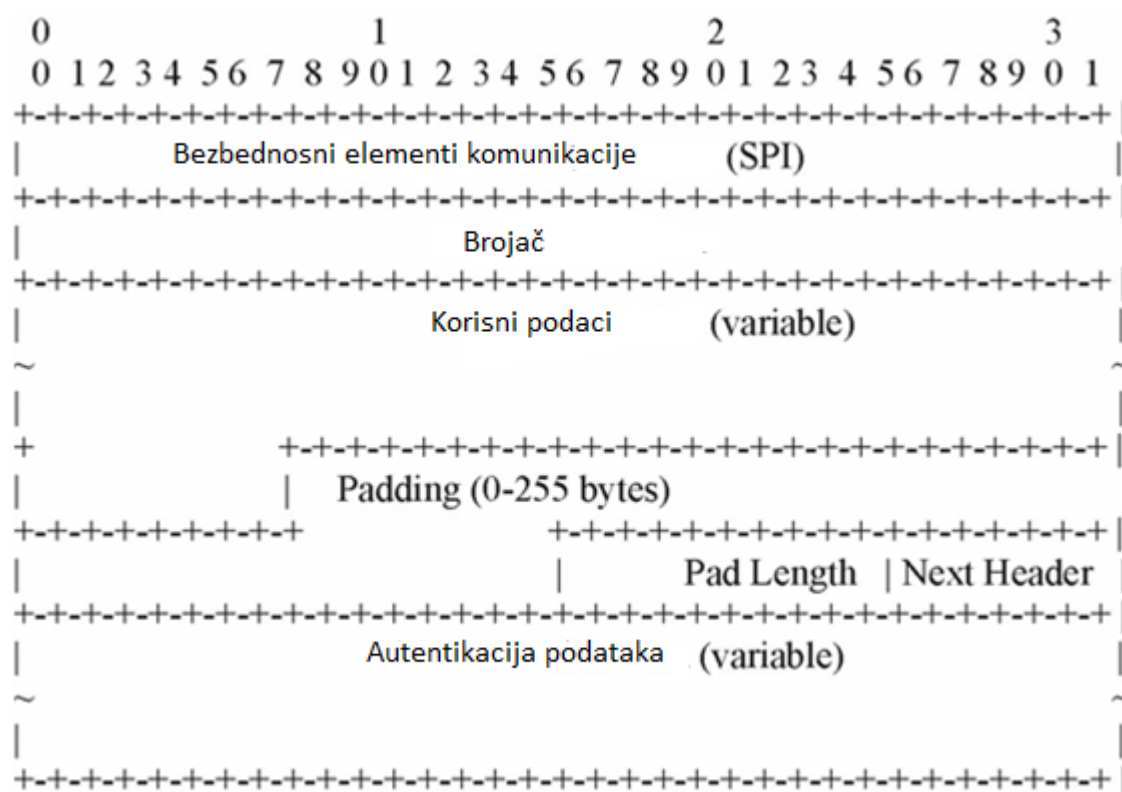
novog IP paketa sa IP adresom gejtveja virtuelne privatne mreže koji je krajnja tačka tunela. Ipsec protokol uključuje u sebe veći broj drugih protokola pomoću kojih obavlja funkcije autentifikacije, integriteta i privatnosti, kao osnovnih bezbedonosnih elemenata virtuelne privatne mreže. Za autentifikaciju IPsec protokol koristi PKI (Public Key Infrastructure) tehniku javnog i privatnog ključa sa infrastrukturom Digitalnog sertifikata preko Sertifikacionih tela (X.509 Certificate). IKE (Internet Key Exchange) protokol sa Diffie-Hellman algoritmom se koriste u procesu razmene kjučeva i pregovaranju bezbedonosnih elemenata. U okviru IPsec protokola integritet podataka obezbeđuju protokoli HMAC-MD5 i HMAC-SHA-1, a privatnost IP paketa je obezbeđena enkripcijom sa 3DES (DES) algoritmom. S obzirom da IPsec AH tip ne obuhvata enkripciju, za virtuelne privatne mreže koristi se uglavnom ESP tip, i to tunnel mod, koji obuhvata enkripciju i IP zaglavlja polaznog paketa. Na slici 14. je prikazana enkapsulacija IP paketa sa IPsec ESP protokolom u tunnel modu. Originalni IP paket je kriptovan i autentifikovan sa ESP zaglavljem i pripremkom, a novo IP zaglavlje definiše IP adresu krajnje tačke tunela. Slika 15. predstavlja IPsec ESP zaglavlje u tunnel modu. Polje SPI (Security Parameter Index) definiše bezbedonosne elemente komunikacije – autentifikacioni mehanizam, kriptografski algoritam i upravljanje ključevima. Polje Sequence Number sadrži brojač kojim otpremna strana numeriša pakete radi kontrole, za koje u prijemu može da se koristi odgovor.



Slika 13.



Slika 14.



Slika 15.

7.2. ANALIZA BEZBEDNOSTI

Bezbednost je jedan od osnovnih zahteva za Virtuelne privatne mreže. Nju ugrožava veliki broj napada, koji se mogu svrstati u veći broj grupa kao što su: napadi autentifikacije, kriptografski napadi, napadi integriteta, falsifikovanje servera, falsifikovanje paketa, napadi uskraćivanja usluga i pasivno monitorovanje. Otpornost protokola PPTP, L2TP i IPsec na ove napade, odnosno njihovih bezbedonosnih mehanizama se analizira u ovom delu i daje se jedna kvantitativna ocena stepena bezbednosti.

Analiza autentifikacionih mehanizama PAP i CHAP protokola PPTP ukazuje na veliku podložnost napadima. PAP protokol skoro da ne predstavlja zaštitu, jer postoje pristupačni alati s kojima se relativno brzo razbija lozinka (password). CHAP protokol je otporniji od PAP-a, ali je njegova slabost što se hash funkcija primenjena na string (challenge) računa na osnovu lozinke, što omogućava napad na hash funkciju sličnim alatima kao za napad na PAP. I PAP i CHAP protokol autentifikuju korisnika a ne mašinu –računar (server), niti paket. U fazi pregovaranja komunikacionih parametara PPTP protokol se oslanja na PPP konfiguracione pakete koji sadrže otvorene IP adrese, što je podložno napadima monitorovanja, preuzimanja i falsifikovanja. U PPTP protokolu korišćeni protokol za enkripciju paketa MPPE, iako se zasniva na RSA RC4 standardu sa ključem od 40 ili 125 bita, ima slabost u tome što se ključevi izvode iz lozinke, pa spada u manje bezbedne kriptografske algoritme. PPTP tunelovanje sa GRE protokolom ima istu slabost otvorene faze

pregovaranja veze, gde je moguće snimanje i modifikovanje paketa i razbijanje tunela. Sam GRE protokol ima slabost na dupliranje redoslednog broja paketa čime se postiže desinhronizacija GRE kanala. Kontrolne poruke PPTP protokola su neautentifikovane i nezaštićene, pa je PPTP protokol otvoren za napade falsifikovanja identiteta servera, falsifikovanje paketa, napade integriteta podataka i za napade uskraćivanja usluga.

S obzirom da L2TP protokol za autentifikaciju koristi PPP mehanizme PAP i CHAP, L2TP tunel je takođe ranjiv na napade. String (challenge, secret) je kod autentifikatora u otvorenom obliku, što pogoduje napadima na hash funkciju i otkrivanju identiteta. Postoji mogućnost zloupotrebe tunela u slučaju prediktivnog načina dodeljivanja broja identifikatora tunela i broja identifikatora sesije. L2TP protokol nema mehanizme za zaštitu od napada integriteta, falsifikovanje servera i paketa i od napada uskraćivanja usluga kao ni PPTP protokol, ali ima prednosti u performansama – podržava više tunela od jedne do druge krajnje tačke, prenosi direktno veći broj protokola i ima mogućnost kompresije zaglavlja. Prednost mu je i što može da se integriše sa IPsec protokolom i koristi njegove zaštitne mehanizme.

IPsec protokol pruža znatno veći broj bezbedonosnih servisa od predhodna dva protokola. PKI infrastruktura javnog ključa, verifikacija ključeva od strane Sertifikacionog tela (CA) i IKE mehanizam upravljanja ključevima obezbeđuju bezbedan kontrolni kanal u fazi pregovaranja bezbedonosnih atributa između dva računara, koji se ovim mehanizmima međusobno autentifikuju na zaštićen način. I AH i ESP format IPsec protokola autentifikuju svaki paket, a sa HMAC-MD5 ili HMAC-SHA-1 hash funkcijama obezbeđuju i integritet podataka svakog paketa. ESP tunelovanje i kriptovanje podataka paketa i originalnog IP zaglavlja sa 3DES algoritmom je potpuno otporno na kriptografske napade, s obzirom da algoritam 3DES sa ključem od 168 bita i HMAC-SHA-1 hash funkcija još uvek nisu kompromitovani. IPsec protokol ima sve mehanizme zaštite od standardnih napada na Internetu, ugrađen je u protokole IPv4 i IPv6 i otvoren je za ugradnju novih zaštitnih mehanizama za slučajeve kompromitovanja postojećih. Najteža odbrana na Internetu je od napada uskraćivanja usluga, jer ti napadi potiču uglavnom od slabosti TCP/IP protokola na koji se IPsec protokol oslanja. I IPsec protokol ima svoje slabosti. Uspostavljeni tunel ne mora uvek da je potpuno bezbedan, jer se tunel uspostavlja automatski pregovaranjem bezbedonosnih atributa računara krajnjih tačaka tunela, i ako ne postoje sa obe strane mehanizmi najvećeg stepena zaštite, koriste se oni raspoloživi sa nižim stepenom zaštite (ključ sa manjim brojem bita, slabija hash funkcija). Jedna slabost IKE protokola koji nema indikaciju predajnoj strani da je sesija prekinuta, ostavlja mogućnost napada na server ako je korišćen slabiji ključ. U tom slučaju uspostavljeni i veći period obnavljanja ključa povećava mogućnost uspešnog napada. IPsec protokol nema mogućnost direktnog prenošenja drugih protokola preko IP mreže, pa se sa aspekta funkcionalnosti, performansi i interoperabilnosti tada koristi hibridni protokol L2TP/IPsec, koji je proširenje L2TP protokola sa bezbedonosnim mehanizmima IPsec protokola.

Iako su virtualne privatne mreže važan sigurnosni alat, prisutni su sledeći nedostaci:

- Opasnost za računare spojene na javnu mrežu. Virtualna privatna mreža koristi aktuelnu mrežu koja nije privatna, odnosno sigurna mreža. Računari priključeni u virtualnim privatnim mrežama moraju biti spojeni na tu aktuelnu mrežu pa su u opasnosti od neovlašćenih upada. Na primer, ukoliko koristimo virtualne privatne mreže za spajanje unutrašnje mreže s mobilnim korisnicima koji su spojeni na Internet, njihovi računari mogu biti napadnuti s Interneta.

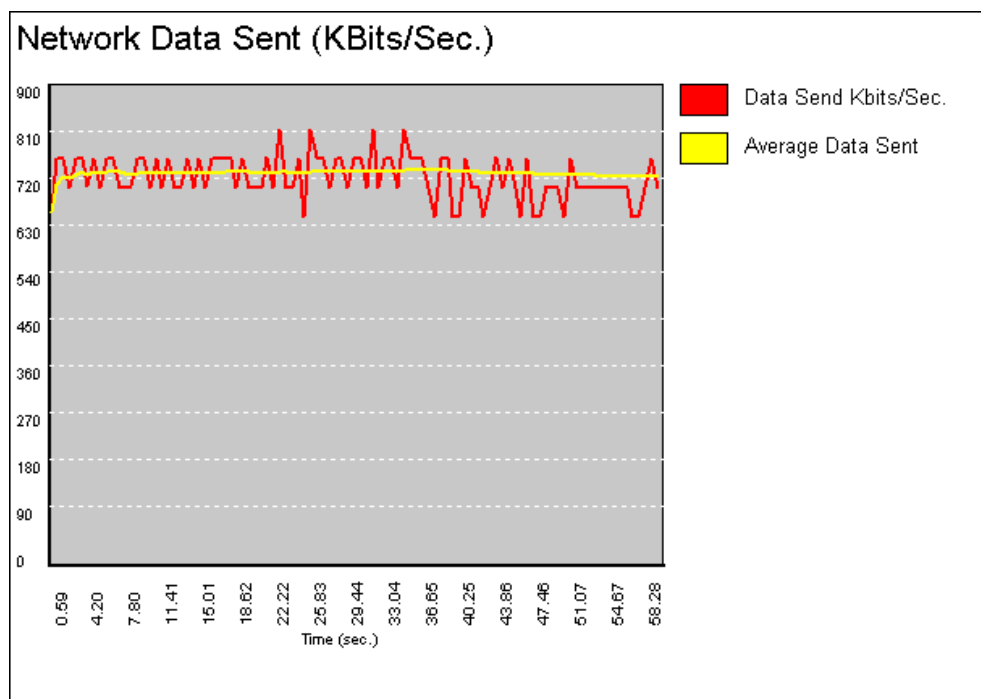
- Opasnost od neovlašćenih upada u unutrašnju mrežu. Priključenjem računara u virtualnu privatnu mrežu, taj računar postaje legitimni član unutrašnje, privatne mreže. Ukoliko je na

računaru virtualne privatne mreže napravljen neovlašćeni upad, napadač je u mogućnosti preko virtualne private mreže ugroziti sigurnost ostalih računara unutrašnje mreže. Virtualne private mreže se koriste za pružanje pristupa računarima koji su manje sigurni od računara unutrašnje mreže. Na primer, kod prenosnih računara postoji opasnost od krađe, kućnim računarima deca imaju pristup itd.

8. Brzina i mogućnosti

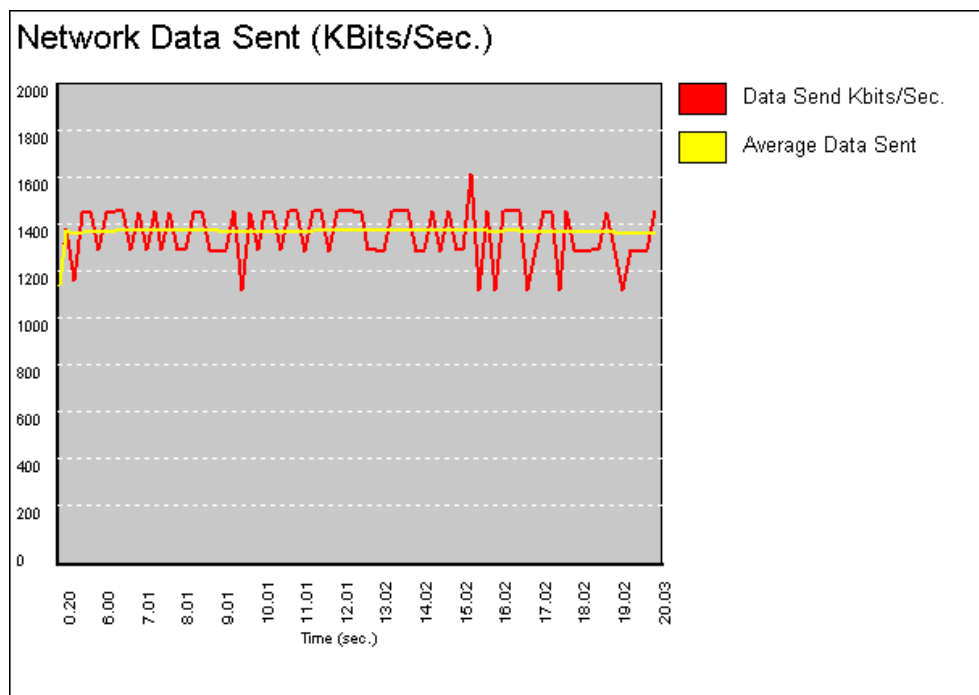
Mogućnosti VPN-a, i ovakvog načina povezivanja udaljenih mreža nisu ni izdaleka iscrpljene do sad rečenim uključujući i prvi pristupni rad. Deljenje lokalnih aplikacija između udaljenih mreža je samo jedna od mogućih dodatnih primena, a sigurnost mreža moguće je unaprediti i primenom filtera za IP pakete na određenim portovima, kao i logiranjem IP prometa u svrhu kasnije analize.

Osnovni preduslov za implementaciju distribuiranih aplikacija predstavlja i brzina komunikacije između pojedinih komponenti distribuiranog sistema, u ovom slučaju lokalnih mreža povezanih VPN-om. Testiranje brzine i propusnosti VPN komunikacijskog kanala proverili smo koristeći program *Performance Test 4.0*. Njegov mrežni test generise promet između dve tačke u mreži u proizvoljnom vremenskom intervalu, u ovom slučaju 20 s. Ako je između merenih tačaka uspostavljen VPN kanal osiguran 3DES enkripcijom, rezultati nam daju prosečnu brzinu linka od 728,1 kbit/s ili 0,711 Mbit/s (Sl. 21).



Slika 16. Testiranje VPN kanala sa 3DES simetričnom enkripcijom

U slučaju nešto slabije enkripcije DES, sigurnost sistema je za nekoliko smanjena, ali brzina dostiže i do 1600 kbit/s, dok je prosečna brzina 1381 kbit/s ili 1,35 Mbit/s (Sl. 22).



Slika 17. Testiranje VPN kanala sa DES simetričnom enkripcijom

Spremnost korisnika da žrtvuje deo sigurnosti radi brzine komunikacije određuje i izbor enkripcije. U svakom slučaju, enkripcija DES se može preporučiti samo ukoliko distribuirana aplikacija zahteva brzinu prenosa veću od 1 Mbit/s.

9. Konfiguracija VPN konekcije

9.1. Kako radi VPN konekcija

Routing and Remote Access service nudi VPN servise tako da korisnici mogu da pristupe mreži organizacije na siguran način šifrovanjem podataka između dva kompjutera kroz deljenu javnu mrežu. Paketi koji budu uhvaćeni na deljenoj ili javnoj mreži ne mogu se pročitati bez Encryption Keys (ključeva za šifrovanje). Link u kom su privatni podaci kapsulirani i šifrovani je VPN konekcija. VPN konekcija se takođe naziva i VPN tunel.

9.1.1. Proces VPN konekcije je opisan u sledećim koracima:

- VPN klijent pokušava da uspostavi VPN konekciju ka Remote Access Serveru-VPN serveru koji je konektovan na Internet. VPN server se ponaša kao Gateway i normalno je konfigurisan da nudi pristup ka celoj mreži na kojoj je VPN server povezan.
- VPN server odgovara na virtualni poziv.
- VPN server autentifikuje subjekta koji je napravio poziv i proverava njegovu autorizaciju da bi dopustio korisniku da se konektuje na mrežu.
- VPN server izvršava transfer podataka između VPN klijenta i mrežne organizacije.

9.1.2. Prednosti VPN

VPN dozvoljava korisnicima ili organizacijama da se konektuju na udaljene servere, manje kancelarije i na mreže drugih organizacija preko javne mreže (Interneta) i to sve preko veoma sigurne konekcije. U svim ovim slučajevima, sigurna konekcija se pojavljuje korisniku kao Private Network Communication – uprkos činjenici da komunikacija ide preko javne mreže (Interneta). Ostale prednosti su:

- **Prednosti u ceni:** VPN ne koristi telefonsku liniju i zahteva manje hardvera (Internet Service Provider ISP održava sav komunikacioni hardver).
- **Povećana sigurnost:** Osetljivi podaci su sakriveni od neautorizovanih korisnika, ali su pristupačni za korisnike koji su prošli proces autorizacije. VPN server prisiljava na autentifikaciju i šifrovanje.
- **Podrška za mrežne protokole:** Možemo udaljeno da startujemo bilo koju aplikaciju koja zavisi od najčešćih mrežnih protokola, kao što je TCP-IP protokol.
- **Sigurnost IP adresa:** Iz razloga što su informacije koje se šalju preko VPN šifrovane, adresa koju smo odredili je zaštićena i saobraćaj koji se šalje preko Interneta će imati vidljivu samo eksternu IP adresu.

9.2. Komponente VPN konekcije

VPN konekcija uključuje sledeće komponente:

- **VPN Server:** Kompjuter koji prihvata VPN konekcije od VPN klijenata, kao što je na primer server konfigurisan sa Routing and Remote Access servisom.
- **VPN klijent:** Kompjuter koji inicira VPN konekciju ka VPN serveru.
- **Tranzit mreža:** Deljena ili javna mreža kroz koju prolaze kapsulirani podaci.
- **VPN konekcija ili VPN tunel:** Deo konekcije u kojoj su naši podaci šifrovani i kapsulirani.
- **Tunneling protokoli:** Protokoli koji se koriste za upravljanje tunelima i za kapsuliranje privatnih podataka (na primjer, Point-to-Point Tunneling Protocol PPTP).
- **Podaci koji se šalju kroz Tunel:** Podaci koji se obično šalju kroz privatni Point-to-Point link.
- **Autentifikacija:** Identitet klijenta i servera u VPN konekciji se autentifikuju. Da bi se osiguralo da primljeni podaci predstavljaju podatke koje je stvarno poslao član konekcije (VPN klijent) i da podaci nisu prestretnuti i modifikovani, VPN takođe autentifikuje podatke koje su poslali.
- **Adrese i lociranje Name servera:** VPN server je odgovoran za dodeljivanje IP adresa koje dodeljuje preko defoltnog protokola, DHCP ili iz skupa statičkih IP adresa koji je kreirao administrator. VPN server takođe locira i daje adrese DNS i WINS servera VPN klijentima.

9.3. Encryption protokoli za VPN konekcije

Postoje dva tipa Tunneling protokola koje koristi Windows Server 2003 familija kad želi da zaštiti komunikaciju:

- **Point-to-Point Tunneling Protocol (PPTP):** Koristi User-Level PPP autentifikacione metode i Microsoft Point-to-Point Encryption (MPPE) za šifrovanje podataka.
- **Layer Two Tunneling Protocol with Internet Protocol Security (L2TP-IPSec):** Koristi User-Level PPP autentifikacione metode preko konekcije koja je šifrovana koristeći IPSec. IPSec zahteva autentifikaciju hosta koristeći Kerberos protokol, Preshared Keys ili sertifikate na nivou kompjutera (Computer-level).

Preporučuje se da koristimo L2TP-IPSec sa sertifikatima za sigurnu VPN autentifikaciju. Koristeći Internet Protocol Security (IPSec) autentifikaciju i šifrovanje, transfer podataka kroz L2TP-enabled VPN je sigurna unutar jednog LAN-a u mreži organizacije.

VPN klijent i VPN server moraju da podržavaju i L2TP i IPSec. Klijentska podrška za L2TP je ugrađena u Windows XP Remote Access Client, a VPN server podrška za L2TP je ugrađena u sve Windows Server 2003 verzije operativnog sistema.

Podrška na serveru za L2TP je instalirana kada instaliramo Routing and Remote Access servis. U zavisnosti od naših odluka, kada startujemo Routing and Remote Access Server Setup Wizard, L2TP je konfigurisan da ima 5 ili 128 L2TP portova.

9.4. Konfiguracioni zahtevi za VPN Server

Pre nego što budemo mogli da konfigurišemo VPN konekciju, moramo da omogućimo Routing and Remote Access servis. Omogućavanjem Routing and Remote Access servisa startujemo Routing and Remote Access Setup Wizard uz čiju pomoć možemo da konfigurišemo naš VPN server. Ako smo na serveru još ranije omogućili Routing and Remote Access servis, možemo da konfigurišemo VPN Network Access sa Remote Access Server Properties-a.

Sledeća tabela izlistava informacije koje je potrebno da znamo pre konfiguracije Remote Access-VPN servera.

Before Adding a VPN Server Role	Comments
Identifikovati koji mrežni interfejs konektovan na internet a koji je mrežni interfejs konektovan na privatnu mrežu	U toku konfiguracije, od nas će se tražiti da izaberemo interfejs koji je povezan na Internet. Ako odredimo pogrešan interfejs, naš Remote Access-VPN Server neće raditi kako treba.
Identifikovati da li će udaljeni klijenti dobijati IP adrese od DHCP servera na našoj privatnoj mreži ili od VPN servera koji želimo da konfigurišemo.	Ako imamo DHCP server na našoj privatnoj mreži, VPN server može da iznajmi 10 adresa odjednom sa DHCP servera i te adrese dodeli VPN klijentima. Ako nemamo DHCP server na našoj privatnoj mreži, VPN server može automatski da dodeljuje IP adrese udaljenim klijentima. Ako želimo da VPN server dodeljuje IP adrese iz skupa koji smo mi konfigurisali, moramo prethodno da konfigurišemo skup tih IP adresa (Scope).
Identifikovati da li želimo da zahtevi od VPN klijenata budu autentifikovani koristeći RADIUS server ili će taj proces odrađivati VPN server koji želimo da konfigurišemo	Dodavanje RADIUS servera je veoma korisno ako planiramo da instaliramo i konfigurišemo više VPN servera., Wireless Access Point-a ili drugih RADIUS klijenata na našoj privatnoj mreži. Dodavanje RADIUS servera će biti detaljnije objašnjeno u sledećim lekcijama u ovom modulu.

9.5. Konfiguracija VPN-a za udaljene sajtove (lokacije)

Kada konfigurišemo *Site-to-Site* VPN konekcije, potrebno je da konfigurišemo sledeće konekcije:

-Determining the tunneling protocol to use – ISA server podržava nekoliko tunneling protokola. Potrebno je da izaberemo odgovarajući protokol na osnovu zahteva naše organizaciji VPN gateway servere koje ćemo da izgradimo u svakom sajtu.

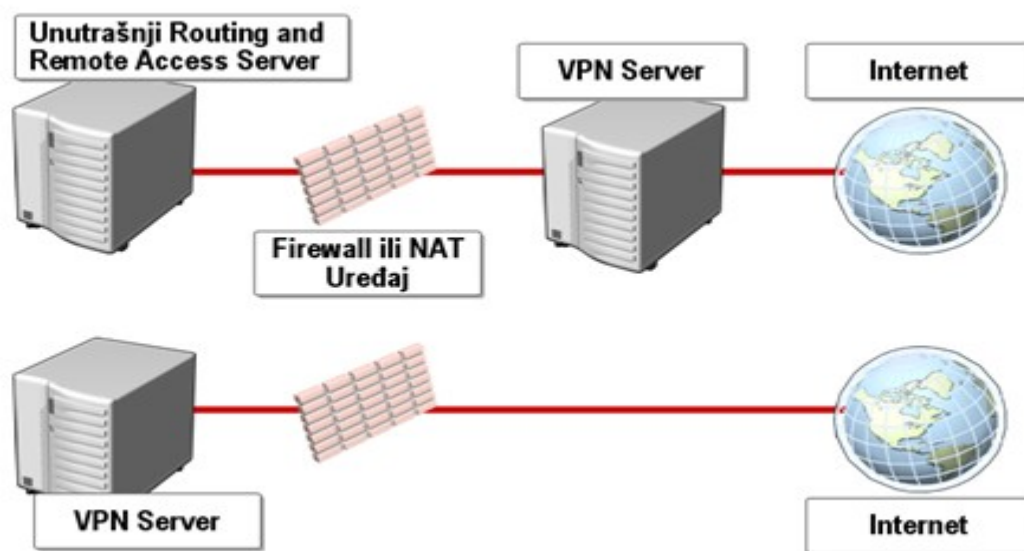
-Configure remote site network – Da bi omogućili *Site-to-Site* VPN-ove, moramo da kreiramo remote-site mrežu na ISA serveru. Svi klijentski kompjuteri u udaljenom sajtu su locirani u ovoj mreži. ISA server koristi ovu mrežu kao i bilo koju drugu mrežu.

-Configure VPN Client Access – Zbog toga što ISA server vidi Remote-site mrežu kao sto vidi bilo koju drugu mrežu, moramo da konfigurišemo postavke za VPN klijentski pristup na ISA serveru da bi omogućili pristup udaljenim klijentima, internoj mreži ili bilo kojoj drugoj mreži. Možemo da koristimo pravila pristupa ili pravila objavljivanja da bi omogućili da interni resursi budu dostupni klijentima u udaljenim kancelarijama.

-Configure the Remote-site VPN gateway – Nakon što smo jednom konfigurisali ISA server u Head (glavnoj) kancelariji, potrebno je takođe konfigurisati udaljene VPN servere. Ovaj Remote-office VPN gateway server može biti drugi kompjuter na kome radi ISA server ili na kome radi Windows server koji je konfigurisan kao RRAS ili neki drugi VPN gateway server drugog proizvođača. Tačna konfiguracija ovih gateway servera zavisi od tipa servera koji se koristi na udaljenom sajtu.

10. Postavljanje VPN servera

Postavljanje VPN servera može značajno da utiče na sigurnost mreže koja sadrži zaštitni zid ili NAT uređaj. Prikladno postavljanje VPN servera u odnosu na zaštitni zid doprinosi funkcionalnosti, dostupnosti i postizanju ciljeva infrastrukture udaljenog pristupa bez opasnosti po sigurnost mreže.



Slika18. Postavljanje VPN servera

Razmotrite upotrebu zaštitnog zida kao VPN servera ako:

- Zaštitni zid ima mogućnost da funkcioniše kao VPN server
- Zaštitni zid ima mogućnost da upravlja VPN konekcijama

Razmotrite postavljanje VPN servera sa spoljašnje strane zaštitnog zida ako:

- Izlaganje VPN servera direktno Internetu ne ugrožava bezbednosni aspekt dizajna
- Sigurnosni rizik povezan sa dozvolom pristupa celokupnom VPN IP adresnom opsegu kroz zaštitni zid nije prihvatljiv
- Svi osetljivi podaci se nalaze iza zaštitnog zida i udaljeni pristup kroz zaštitni zid je ograničen na VPN server

Postavite VPN server sa unutrašnje strane zaštitnog zida ako:

- Dodatni rizik bezbednosti izlaganjem VPN servera direktno Internetu ugrožava sigurnosni aspekt dizajna
- Sigurnosni rizik povezan sa dozvolom pristupa celokupnom VPN IP adresnom opsegu kroz zaštitni jeste prihvatljiv

U slučaju da se VPN server nalazi sa unutrašnje strane zaštitnog zida morate konfigurisati filtere zaštitnog zida da propuštaju sav PPTP i L2TP saobraćaj kroz celokupan VPN IP adresni opseg.

11. VPN zasnovane na Internet protokolu I MPLS-u

Mreže zasnovane na Internet protokolu *IP* dominiraju u oblasti telekomunikacionih mreža u prethodne dve decenije. S obzirom na svoju jednostavnost Internet servisi kao što su *www*, *e-mail*, *FTP* itd., postali su opšte prihvaćeni standardi i uneli su pravu revoluciju i u život običnog čoveka. Više se skoro i ne može zamisliti rad bez mogućnosti pristupa Internetu, a *E-biznis* i *intraneti* i *ekstraneti* su neminovnost današnjeg poslovanja. Usled toga broj korisnika sve više raste (broj hostova na Internetu se približno udvostručava svake godine), ali rastu i zahtevi korisnika u pogledu brzine, vrste i kvaliteta ponuđenih servisa. Pored toga sve je izraženija potreba za multimedijalnom primenom što zahteva mnogo više od mreže nego što je tradicionalni put saobraćaja preko Interneta kakav je *FTP (File Transfer Protocol)*.

Arhitektura Interneta je zasnovana na konceptu prosleđivanja datagrama. Svaki IP datagram se rutira korak po korak ka krajnjem odredištu u skladu sa jedinstvenom IP odredišnom adresom, koja se nalazi u IP zaglavlju. Svaki ruter na koji se naiđe će pregledati tu adresu i potražiti put u svojoj tabeli rutiranja kako bi pronašao odgovarajući izlazni interfejs za sledeći korak. Sam IP ne obezbeđuje pouzdanu isporuku podataka. Protokoli viših slojeva kakav je *TCP (Transport Control Protocol)* prate putanju datagrama i vrše ponovno slanje ako je to neophodno, u slučaju neispravnog prenosa. Ti protokoli ne obezbeđuju prenos u realnom vremenu, tako da IP sam po sebi ne nudi nikakvu mogućnost obezbeđivanja kvaliteta servisa korisnicima (nema mogućnosti *QOS (Quality of Service)* garancije). Javna i privatne IP mreže se sve više koriste za prenos aplikacija, audio i video tokova, kod kojih ne mogu da se tolerišu nepredvidljivi gubitci. Karakteristike *QoS* kao što su: minimizacija vremena kašnjenja, minimizacija varijacija kašnjenja, obezbeđivanje potrebnog propusnog opsega, moraju da se obezbede. Pored toga veliki problem za provajdere Internet servisa (*Internet Service Provider ISP*) je da ponude rešenja koja će omogućiti skalabilnost ali i ponudu ugovorenog kvaliteta usluge *SLA, (Service level agreement)*. Kako bi svi ti uslovi bili zadovoljeni vremenom su se javljali mnogi protokoli koji su svaki od problema rešavali pojedinačno. Uvođenje protokola kao što su: protokol rezervacije resursa *RSVP (Rescourse*

Reservation Protocol), diferencijalni servisi DiffServ (*Differentiated services*), sve je više komplikovalo rutiranje.

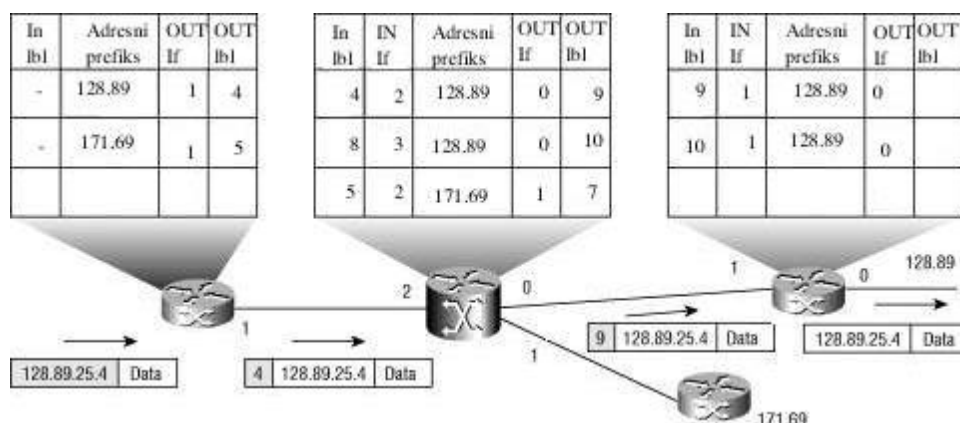
Razvojem ATM tehnologije, koja je ponuđena za izgradnju okosnicu (*backbone*) Interneta omogućen je prenos podataka i multimedijalnih informacija preko jedne mreže poštujući pri tome dogovoren kvalitet servisa. Ipak problem preslikavanja IP protokola u ATM je kompleksan i usled svoje komplikovanosti i problema skalabilnosti i za sada ne predstavlja pravo rešenje. Tako, da bi se zadovoljile potrebe za skalabilnošću, boljim performansama rutiranja, upravljanjem saobraćajem na osnovu administrativno zadatih pravila itd. započet je rad na definisanju novog protokola zasnovanog na komutaciji korišćenjem labela (*Multi Protocol label Switching*).

11.1. Komutacija korišćenjem labela

MPLS kombinuje skalabilnost i fleksibilnost komutiranja sa kontrolom saobraćaja. U stvari MPLS ne nasleđuje ATM već ga dopunjuje; zamena labela koja se koristi predstavlja isti mehanizam koji ATM komutatori koriste za prosleđivanje ATM ćelija, s tim što se informacija o labeli nalazi u ATM zaglavlju, u VPI i VCI poljima. Bez MPLS, IP transport preko ATM mreža zahteva složene protokole za mapiranje IP adresa u ATM adrese, rutiranje i za ATM komutacione tabele. U tom slučaju su neophodni protokoli za ostvarivanje sprega između mreža PNNI (*Private Network Network Interface*), protokol za razrešavanje adresa ATM ARP (*Address Resolution Protocol*) i protokol za rutiranje između podmreža NHRP (*Next Hop Resolution Protocol*). MPLS sada zadovoljava i ono najvažnije: očuvava i koristi postojeće i profitabilne tehnologije Frame Relay i ATM. Paketi koji ulaze u MPLS domen su paketi 3. sloja OSI modela, IP paketi. Ulazni ruter MPLS domena, LSR (*Label Switching Router*) analizira zaglavlje IP paketa i na osnovu dostupnih informacija dodeljuje mu odgovarajuću labelu. To LSR radi uz pomoć tabele koja mapira informaciju o klasi prosleđivanja u informaciju o labeli koja se koristi pri prosleđivanju, *FEC (Forwarding Equivalence Class) to NHLFE (Next Hop Label Forwarding Entry) Map*, koja sadrži informacije neophodne za dodeljivanje labela neoznačenim paketima koji ulaze u MPLS domen. Na slici 12. je prikazano funkcionisanje MPLS-a i metoda zamena labela koja se koristi.

Labele se definišu kao kratki identifikatori lokalnog značaja i fiksne dužine koji se nalaze u zaglavlju paketa i koji logički predstavljaju FEC kome je paket dodeljen. **FEC** je klasa ekvivalencije u prosleđivanju paketa, koja se određuje na osnovu odredišta paketa i dodatnih pravila rutiranja. U MPLS protokolu svi paketi koji pripadaju jednoj klasi ekvivalencije biće prosleđeni na isti izlaz u datom čvoru. Nakon toga **LSR** određuje sledeći skok za dati paket. Podaci o njemu se nalaze u NHLFE tabeli. Kada paket izađe iz ulaznog LSR njemu je dodeljena labela na osnovu koje će naredni LSR vršiti prosleđivanje. Iz ovoga se vidi da se analiza mrežnog sloja paketa vrši samo u ulaznom LSR pa je samim tim smanjeno i vreme potrebno da se paket obradi i prosledi, a na taj način su značajno poboljšane performanse rutiranja. Kada paket stigne do izlaznog LSR-a labela se skida i paket će opet postati običan IP paket, a dalje prosleđivanje će biti zasnovano samo na njegovom zaglavlju. Dakle u MPLS domenu prosleđivanje paketa je zasnovano samo na 32-bitnoj labeli koja se dodeljuje paketu iza zaglavlja sloja 2 i ispred IP zaglavlja. Putanja koju paket prolazi i koja je određena labelom (pripadnošću nekog paketa određenoj FEC klasi) zovemo **LSP Label Switching**

Path. Cilj MPLS protokola je da se svakom paketu koji ulazi u MPLS domen odmah pridruži LSP putanja kojom će paket prolaziti kroz domen, tj. da na samom ulazu bude poznata cela putanja paketa.



Slika19. Funkcionisanje MPLS-a

Za uspostavljanje LSP putanje odgovoran je protokol za distribuciju labela **LDP** (*Label Distribution Protocol*). To je skup procedura pomoću kojih jedan LSR ruter informiše drugi o značenju labela koje se koriste za prosleđivanje saobraćaja između LSR rutera u MPLS domenu, tj. pomoću kojih LSR uspostavljaju LSP putanje kroz mrežu, preslikavajući informacije o rutiranju sa mrežnog nivoa u direktno komutirane putanje nivoa linka podataka (*data link*) nivoa. Korišćenjem protokola za distribuiranje labela u saradnji sa protokolima rutiranja OSPF (*Open Shortest Path First*), RIP (*Routing Information Protocol*), BGP (*Border Gateway Protocol*) uspostavlja se putanja kroz MPLS mrežu i rezervišu neophodni resursi za zadovoljavanje pre-definisanih zahteva za datu putanju. Pri tome svaki LSR donosi odluku prosleđivanja jedino u skladu sa sadržajem labela. LDP ima sledeće karakteristike:

- Posедуje mehanizme za omogućavanje LSR-ima da pronađu jedni druge i uspostave komunikaciju.
- Definiše četiri klase poruka: DISCOVERY, ADJACENCY, LABEL ADVERTISEMENT I NOTIFICATION.
- Funkcioniše preko TCP kako bi se obezbedila pouzdanost poruka (kada nije potrebna potvrda prijema poruke koristi se UDP)
- Dizajniran je da bude lako proširiv
- Dva LSR koji koriste LDP da razmene preslikavanje labela i FEC nazivaju se LDP parovi i oni razmjenjuju 4 tipa LDP poruka:

- Poruke otkrivanja, za pronalaženje LSR rutera
- Poruke sesije, za uspostavljanje održavanje i zatvaranje sesija između LDP parova
- Poruke oglašavanja, za stvaranje, menjanje i brisanje labela u FEC klase
- Poruke obaveštenja, za signalizaciju grešaka

MPLS donosi i mnoge pogodnosti u odnosu na IP mreže:

- *Traffic Engineering* – sposobnost uspostavljanja putanje saobraćaja i uspostavljanje performansi karakterističnih za određenu klasu saobraćaja. *Traffic engineering* omogućava ISP da prebace saobraćaj sa najkraće putanje izračunate korišćenjem IGP (*Interior Gateway Protocol*) protokola na potencijalno manje zakrčenu putanju.
- VPN -ISP-i su ponudili korisnicima VPN MPLS kao jednostavno rešenje za obezbeđivanje privatnosti podataka i podršku za korišćenje ne-jedinstvenih privatnih IP adresa, jer se tu odluke prosleđivanja donose samo u skladu sa vrednošću labele, a ne određene IP adrese koja se nalazi u zaglavlju paketa.
- Eliminacija viših slojeva - tipicno većina koristi sveobuhvatan model gde je ATM korišćena na sloju 2 i IP na sloju 3. Korišćenjem MPLS moguće je mnoge funkcije ATM upravljačke ravni prebaciti na nivo 3, a time se pojednostavljuje upravljanje mrežom kao i složenost mreže.

11.2. VPN zasnovane na MPLS-u

Velike firme koje imaju filijale na različitim lokacijama morale su da povezuju računare radi efikasnijeg poslovanja. Njima je potrebna privatna mreža VPN (*Virtual Private Network*) koju bi mogli da administriraju u skladu sa sopstvenim potrebama sigurnosti, rutiranja i dozvola. Virtualnost se ogleda u tome što ta infrastruktura koja se koristi u toj mreži ne pripada samo njoj. Ona u stvari pripada provajderima Internet servisa, jedom ili više njih i predstavlja backbone koji mogu da koriste jedna ili više VPN. Postoje dva tipa praktične realizacije mreže preko koje mogu da se ostvare VPN.

To je:

- *Overlay* model VPN mreže:

Taj model je danas još uvek prisutniji i podrazumeva da se na svakoj korisničkoj lokaciji nalazi jedan ili više rutera, koji su sa ruterima na drugim udaljenim lokacijama povezani point-to point (tacka - tacka) vezama (iznajmljenim linijama, ATM ili Frame Relay vezama).

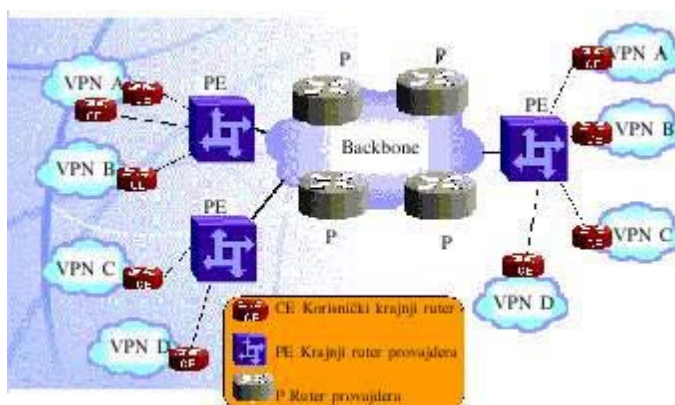
Ovaj model efikasno funkcioniše ali postoji značajan problem skalabilnosti, i zahteva koji se postavljaju korisnicima da sami upravljaju ruterima koji održavaju vezu između udaljenih lokacija, kao i problemi menjanja konfiguracije pri svakom novom dodavanju nove lokacije.

· *Peer model* VPN mreža

Ovaj model treba da omogući provajderima opsluživanje veoma velikog broja korisnika, i ujedno preuzimanje funkcije administriranja njihovih mreža tako da oni mogu da se posvete samo svom primarnom biznisu, ne upuštajući se u pravila IP rutiranja. *Peer model* se sastoji od 4 komponente:

- ograničena distribucija informacija o rutama: pošto su korisnički ruteri direktno spojeni na rutere VPN provajdera, moramo na neki način ograničiti protok, tako da samo ruteri koji pripadaju istoj VPN mreži mogu razmenjivati saobraćaj.
- upotreba višestrukih tabela rutiranja: neophodno je da PE ruter održava ne jednu, već više tabela rutiranja jer on najčešće služi za povezivanje više VPN korisnika, pa njegova tabela rutiranja sadrži u sebi sve rute dobijene od svih lokacija koje su preko njega povezane.
- korišćenje novog tipa adresa (VPN-IP adrese)
- upotreba MPLS protokola

Primer peer mreže je prikazan na slici 13. Sa CE (*Customer Edge*) su označeni ruteri na korisničkim lokacijama, a sa PE (*Provider Edge*) ruteri provajdera koji su direktno vezani na korisničke, pri čemu između njih mora biti obezbeđena direktna IP veza. Sa P su označeni *core* ruteri *backbone*-a. CE uređaj može biti vezan na PE ruter bilo kojim tipom linka podataka (na primer ATM VCC, Frame Relay, Ethernet...). Korisnička lokacija može biti vezana na provajdera preko više PE rutera, a PE ruter može obezbeđivati vezu za više od jedne korisničke lokacije. Ovaj model nosi naziv *peer* zato što korisnički ruteri direktno razmenjuju saobraćaj sa ruterima VPN provajdera, za razliku od *overlay* modela gde su korisnički ruteri na udaljenim lokacijama direktno povezani jedni sa drugima, bilo putem virtuelnih kola na data link sloju, bilo putem IP tunela.



Slika 20. Peer model VPN mreže

Svaka VPN nosi oznaku koja u implementaciji predstavlja 8-o bajtnu “oznaku rute” *Route Distinguisher RD* [1] (slika 14.). Ona se sastoji od tri polja:

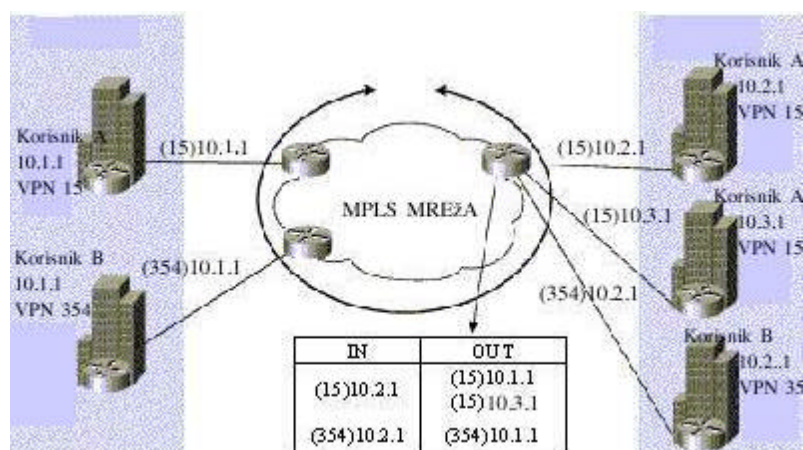
- Tip –2 okteta
- AS broj autonomnog sistema koji je dodeljen VPN provajderu -2 okteta
- VPN broj – 4 okteta

RD se koristi kao prefiks IP adresama tog sajta. Konfiguriše se na interfejsu koji je vezan za određenu lokaciju. Na primer podmreža 10.1.1.0 za VPN 15 se razlikuje od podmreže 10.1.1.0 za VPN 354. Sa gledišta MPLS VPN provajdera to su u stvari adrese 15:10.1.1.0 i 354:10.1.1.0 Dodeljivanje 8-o bajtne oznake rute ispred IP adrese dobija se VPN-IP adresa. Sa stanovišta BGP protokola, rukovanje rutama koje imaju VPN-IP adrese se ne razlikuje od standardne procedure za IP adrese, zahvaljujući osobini BGP protokola da generički rukuje adresama, bez obzira na njihov format. Na ovaj način se samo prenosi informacije o VPN drugim ruterima koji imaju interfejs sa istom vrednošću RD. Na taj način se sprečava slučajno curenje informacija korisnika A korisniku B. To takođe znači da svaki PE ruter samo prati rute korisnika koji su povezani na taj PE, a ne prefikse za sve lokacije i korisnike koji su vezani na ISP. Pri tome ostaje problem i činjenica da su to VPN-IP rute, a da je ipak mreža provajdera zasnovana na IP

protokolu, tako da je u PE ruterima neophodno da se izvrši pretvaranje IP u VPN-IP adrese. To se ostvaruje tako što ruter identifikuje VPN mrežu kojoj korisnik pripada na osnovu interfejsa po kojem stiže paket i dodeljuje VPN IP adresu koristeći oznaku rute za datu VPN mrežu. Zatim tu VPN-IP rutu prosleđuje svojim BGP susedima koristeći BGP opšti (*community*) atribut za datu mrežu. Pri tome se javljaju sledeći problemi:

- neophodno je konvertovati IP zaglavlje tako da se koriste duže adrese na ulaznim PE ruterima;
- unutrašnji ruteri treba da znaju kako da prosleđuju ovaj novi mrežni protocol;
- neophodno je na izlaznim ruterima ponovo izvršiti konverziju u IP adrese;

Zato se rešenje za taj problem našlo uvođenjem MPLS-a. Sa stanovišta MPLS-a ulazni PE ruter nije ništa drugo do ulazni LSR ruter. Kada ulazni PE ruter primi IP paket od CE rutera, on konsultuje svoju odgovarajuću FIB tabelu rutiranja (identifikovanu na osnovu porta po kom je došao IP paket). Na osnovu informacije iz tabele rutiranja, utvrđuje se sledeći hop paketa kao i labela koja će biti stavljena na njegovo IP zaglavlje. U stvari na paket se stavljaju 2 labele: prva na vrhu steka labela, govori o putanji paketa kroz mrežu VPN provajdera do izlaznog PE rutera i prosleđuje se LDP protokolom. Druga labela ispod predhodne, govori izlaznom PE ruteru kako i kom korisniku treba proslediti paket koji je primljen i prosleđuje se BGP protokolom, upotrebom VPN-IP adresa.



Slika 21. Uvođenje Route Distinguisher-a

12. Open VPN

Danas većina kompanija ima potrebu stalnog ili povremenog vanjskog povezivanja na lokalnu mrežu. Većina odustaje od sigurnog povezivanja u VPN zbog cene gotovih uređaja koji bi to omogućili, ali i zbog njihovog komplikovanog održavanja. Glavna prednost Open VPN-a je njegova jednostavnost u primeni. Koristi vrlo napredne kriptografske algoritme, ali ne opterećuje previše računara na kojem je instaliran. Generisanje sertifikata i ključeva je vrlo jednostavno i brzo, ukoliko se prati prikazana procedura opisana u nastavku poglavlja. Uz sve to je i besplatan, pa se za manje korisnike može smatrati povoljnijim rešenjem od kupovine skupih IPSEC firewall-a.

Open VPN je aplikacija koja se u osnovi koristi iz komandne linije i može se pokrenuti kao servis unutar operacionog sistema. Aplikacija se može pokretati na više načina koristeći podešavanja unutar konfiguracione datoteke, a za puni opis svih mogućih opcija preporučuje se lista na web stranicama autora: <http://openvpn.net/man.html>.

OpenVPN možemo koristiti za stalno (site-to-site) i povremeno (client) povezivanje pojedinih lokacija i uređaja. Podešavanje je u osnovi slično u oba slučaja jer uvek instaliramo istu aplikaciju na svim računarima unutar VPN mreže. Osnovno podešavanje je vrlo jednostavno, ali kompleksnost primene raste zavisno od složenosti topologije mreže. Tada su potrebna i dodatna znanja o sigurnosti računarnih mreža, naročito o infrastrukturi javnih ključeva (PKI).

OpenVPN koristi SSL/TSL (*Secure socket layer/Transport layer security*) protokol za uspostavljanje komunikacije između pojedinih tačaka VPN mreže. Na taj način se ostvaruje slična sigurnost kao i u mrežama gde se primenjuje IPsec (*IP security*) protokol. Za razliku od drugih SSL VPN-ova gde se klijenti posebno ne podešavaju, a veza se uspostavlja isključivo kroz web *browser* na strani klijenta, kod Open VPN-a se klijent posebno podešava. Ista aplikacija se instalira na serveru i klijentu pa se Open VPN može smatrati P2P (*peer-to-peer*) aplikacijom. Svi *data* paketi se usmeravaju na jedan UDP ili TCP port po izboru (po definciji se koristi UDP protokol i port 1194). Sav tako usmeren mrežni promet se enkriptuje i šalje na drugu tačku VPN mreže u odlasku ili dekriptuje ako je reč o dolaznom prometu. Aplikacija je realizovana pod Open Source GNU licencom i može se instalirati na MS Windows XP, Linux, Mac OS X, OpenBSD, FreeBSD, NetBSD operacionim sistemima.

12.1. Ugrađena sigurnost i kriptografski algoritmi

Osnovna ideja svih danas dostupnih VPN rešenja se svodi na zaštitu od pasivnih i aktivnih napada. Pasivni napadač je onaj koji prisluškuje kanal komunikacije, ali ne deluje aktivno na informacije. Enkripcija podataka može rešiti ovakav problem. Aktivni napadač može ubaciti sebe u komunikacioni kanal, dodavati, menjati ili brisati podatke u komunikacionom kanalu. Aktivni napadač se u literaturi na engleskom jeziku obično naziva “man-in-the-middle” (čovek u sredini).

Većina korisnika smatra da se VPN sigurnost uglavnom sastoji od mnoštva primenjenih enkripcijskih algoritama kojima rešavamo prisluškivanje komunikacije. Postavlja se pitanje da li je to dovoljno. Sa stanovišta sigurnosti VPN mora rešiti i puno važniji problem, a to je autentifikacija korisnika i onemogućavanje aktivnih napada. U primeni to znači potpisivanje svakog komunikacijskog paketa, tako da primalac sigurno zna da poruka dolazi iz proverenog izvora. Potpisivanje paketa izvodi se funkcijama sažimanja. OpenVPN koristi HMAC (keyed-hash message authentication code) funkciju za autentifikaciju paketa. HMAC spada u podgrupu MAC (message authentication code) funkcija i upotrebljava se uz standardne kriptografske funkcije sažimanja (MD5 ili SHA) i sigurnosni ključ.

Konstrukciju i analizu HMAC algoritma su prvi put prikazali: Mihir Bellare, Ran Canetti, i Hugo Krawczyk, 1996. godine.

HMAC autentifikacija komunikacionih paketa nije dovoljna za zaštitu od tzv. napada ponavljanjem (*replay attack*). Npr. napadač može snimiti enkriptovani, njemu zanimljivi promet (npr. Novčana transakcija) i onda ga reprodukovati. Ukoliko sistem nema zaštitu od takvog napada, moguće je imati niz takvih upitnih transakcija. Rešenje ovog problema bi bilo dodavanje jedinstvenih vremenskih oznaka na svaki paket. Primalac podataka mora tada paziti da ne primi dva puta pakete s istom vremenskom oznakom. OpenVPN koristi tzv. SWA algoritam (*Sliding Window Algorithm*) za sprečavanje aktivnog napada ponavljanjem.

Za kriptovanje podataka OpenVPN koristi gotovu OpenSSL biblioteku funkcija. Pri tome je moguće koristiti statičke ključeve koje razmenjuju učesnici u komunikaciji, u jednostavnijoj primeni. Međutim, moguće je koristiti i RSA infrastrukturu javnih ključeva za rešavanje osetljive tačke u HMAC autentifikaciji, a to je razmena ključa.

Infrastruktura javnih ključeva je prvi put predstavljena 1977. godine u časopisu *The Scientific American*, kada su autori: *Ronald L. Rivest, Adi Shamir i Leonard M. Adleman* predstavili svoju primenu RSA algoritma u kriptografiji s javnim ključevima i digitalnim potpisom. Zanimljivo je da su autori ponudili puni opis algoritma bilo kome ko pošalje poštansku omotnicu s plaćenim poštanskim odgovorom. To je rezultovalo ogromnim odzivom i frustracijom u NSA (*National security agency*) jer je prvi put na taj način masovno distribuiran kriptografski algoritam. Međutim, postupak širenja je bio u skladu s tada važećim zakonima, jer uprkos masovnosti nije bio javan.

Postupak upotrebe javnog ključa je bio inovativan upravo zbog toga jer je uveo sigurnu razmenu simetričnog ključa kriptovanja, bez upotrebe sigurnog medija. U primeni to znači da je za komunikaciju između dve tačke potrebno generisati javni i par privatnih ključeva. Svaki učesnik u komunikaciji zadržava vlastiti privatni ključ koji se nikad ne razmenjuje s drugim učesnikom. Njime dekriptuje poruke koje su kriptovane javnim ključem i koji je slobodno dostupan svima koji žele učestvovati u komunikaciji. Problem autentifikacije je rešen uvođenjem sertifikata, potpisanih u sertifikacionom centru (CA), koji utvrđuje identitet učesnika u komunikaciji.

12.2. Praktični primer spajanja dve lokacije upotrebom statičkog ključa

Nakon preuzimanja instalacionog paketa, kopiraju se instalacione datoteke na računar koje će postati VPN server. U ovom primeru će to biti računar sa MS Windows XP operacionim sistemom. Pokretanjem instalacionog postupka podešava se OpenVPN, OpenVPN GUI konfiguracioni program i alat za kreiranje sertifikata.

Može se uočiti da je na računaru instalirana nova mrežna kartica pod imenom : *Win32 Adapter v8*. Novoinstalirana mrežna kartica predstavlja virtualni uređaj preko kojeg podaci mogu prolaziti na dva načina. Ukoliko se promet preusmerava na postojeću mrežnu karticu ugrađenu u računar, tada je to tzv. “*bridge*” način rada. U protivnom se sva podešavanja na virtualnom adapteru obavljaju kao da je reč o “*pravoj*” mrežnoj kartici, s vlastitom IP adresom i tada je to tzv. “*router*” način rada.

Prvo i osnovno podešavanje na serveru obavlja se na postavkama unutar konfiguracione datoteke. Za početak se možemo poslužiti primerom takve datoteke koji se nalazi u mapi: *C:\ProgramFiles\OpenVPN\sample-config*, pod imenom: *sample.ovpn.txt.*, a koji se kopira u *C:\ProgramFiles\OpenVPN\config* pod imenom: *server.ovpn*.

Konfiguracionu datoteku otvaramo i u tekst editoru i potražimo pojam u kojem se nalazi tekst: *remote myremote*.

Ako želimo dozvoliti pristup sa tačno određene adrese npr. 213.191.134.11, tada ta linija treba glasiti: *remote 213.191.134.11*. Ukoliko želimo dozvoliti pristup sa bilo koje IP adrese, tada se jednostavno ovu liniju briše ili se komentariše sa “*;*” na početku.

Po definiciji se sva komunikacija odvija preko UDP protokola i porta 1194. Ukoliko se to menja, potrebno je promeniti linije koje počinju sa *port* (podešavanje porta) i *proto* (odabir protokola). Zatim se bira način spajanja na server. Ako želimo podesiti povezivanje dve mreže sklonimo komentare se reda sa tekstem: *dev tap*. U protivnom je reč o spajanju sa više različitih lokacija na jednu centralnu i tada se bira: *dev tun* protokol.

Za početak je prikazana jednostavnija varijanta spajanja dve mreže (u ovom primeru spajanje dva računara s Windows XP operacionim sistemom).

U tom slučaju generiše se statički ključ kojim se kriptuje komunikacija između dve lokacije. Unutar programa bira se naredba: *Generate a static OpenVPN key*, nakon čega se u mapi *C:\ProgramFiles\OpenVPN\config* stvara 2048 bitni ključ za kriptovanje komunikacije pod imenom *key.txt*. Da bi ključ postao važeći mora se u konfiguracionoj datoteci dodati linija: *secret key.txt*. Preostaje još konfigurisanje dva parametra: *verb* i *mute*. Parametar ‘verb’ određuje koliko se detaljno beleži trenutno stanje aplikacije u log datoteci. Minimalna vrednost je 0 (beleže se samo greške), a maksimalna 11. Parametar ‘mute’ definiše koliko puta se pokušava ponoviti povezivanje, ukoliko prvo povezivanje nije bilo uspešno.

Početna konfiguraciona datoteka na strani servera bi mogla biti ovako postavljena:

```
dev tap
proto udp
secret key.txt
persist-tun
ifconfig 192.168.122.1 255.255.255.0
verb 4
mute 10
```

Klijent se podešava gotovo istim parametrima kao i server, uz nekoliko odstupanja. Tako parametar ‘remote’ na strani klijenta predstavlja javnu IP adresu mreže kojoj se pristupa. Takođe je uobičajeno na strani klijenta postaviti ‘ifconfig’ parametar kojim se definiše IP adresa koju će klijent dobiti prilikom povezivanja na udaljenu mrežu.

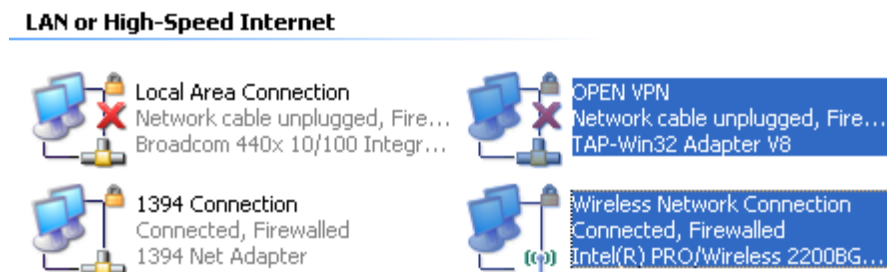
Pretpostavimo da se klijent spaja na udaljenu mrežu s javnom IP adresom: 213.191.134.11. Tada bi konfiguraciona datoteka na strani klijenta mogla biti:

```
remote 213.191.134.11
dev tap
ifconfig 192.168.122.100 255.255.255.0
secret key.txt
verb 4
mute 10
```

Na kraju treba odlučiti na koji način će se pokrenuti aplikacija na udaljenim računarima. Može se koristiti tzv. usmereni (*routing*) ili preklopljeni (*bridged*) način rada.

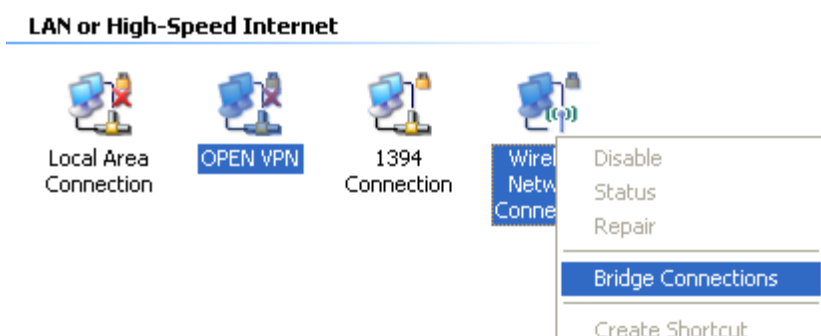
U ovom primeru spajaju se dva udaljena računara pa je moguće primeniti jednostavniju, “*bridged*” konfiguraciju kod koje se sav promet s virtualnog adaptera preusmerava na mrežnu karticu koja je fizički instalirana na računaru.

Ukoliko je operacioni sistem na računarima MS Windows XP, povezivanje mrežnih adaptera na ovaj način je vrlo jednostavno. Na popisu mrežnih adaptera odabere se s liste *TAP adapter* i postojeća mrežna kartica kombinacijom CTRL tipke i leve tipke na mišu.



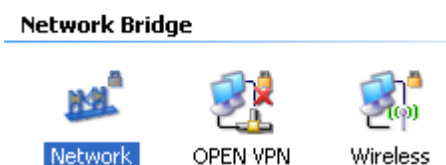
Slika 22. Odabir mrežnih kartica za povezivanje

Aktivira se desna tipka miša i odabere naredbu – Bridge Connections.



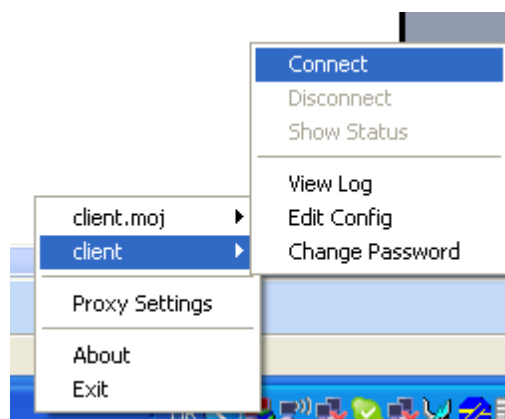
Slika 23. Povezivanje odabranih mrežnih kartica

Rezultat je nova mrežna kartica “sastavljena” od OpenVPN i “stvarne” mrežne kartice.



Slika 24. Rezultat povezivanja virtualne i stvarne mrežne kartice

Duplim klikom na GUI ikonu (*openvpn-gui-1.0.3.exe*) smeštenu na radnoj površini pokreće se OpenVPN na računarima. Rezultat pokretanja je nova sličica u *taskbar*-u. Desnom tipkom miša, otvara se mogućnost pokretanja željene konfiguracione datoteke:



Slika 25. Odabir aktivne konfiguracije

Ukoliko je sve dobro podešeno, rezultat je poruka da je spajanje uspešno i da je konfigurisana besplatna VPN veza između dve odvojene mreže spojene na zajednički subnet.

12.3. Praktični primer spajanja dve lokacije upotrebom sertifikata

Upotreba statičkog ključa je vrlo jednostavna za podešavanje, ali ima ozbiljan nedostatak. U slučaju krađe ključa, napadač može bez poteškoća upadati u kanal komunikacije. Takođe se ne mogu primeniti svi postupci autentifikacije na strani serverskog računara (npr. dodatna autorizacija lozinkom). Za uspostavljanje infrastrukture javnog ključa mora se definisati CA centar na sigurnom računaru. U ovom primeru, moguće je za tu svrhu koristiti računar koji uopšte nema nikakav mrežni pristup.

Generisanje sertifikata opisano je u nekoliko tačaka:

1. Proveri se verzija OpenSSL biblioteka na serveru i klijentu.

Poželjno je da budu iste. Pokrene se prozor s komandnom linijom i izabere mapa: `c:\Program Files\OpenVPN\bin` i pokrene se `openssl.exe` Nakon toga zadaje se naredba: `version` i na ekranu se ispiše verzija biblioteke.

2. Podešavaju se podaci o vlasniku generisanih sertifikata.

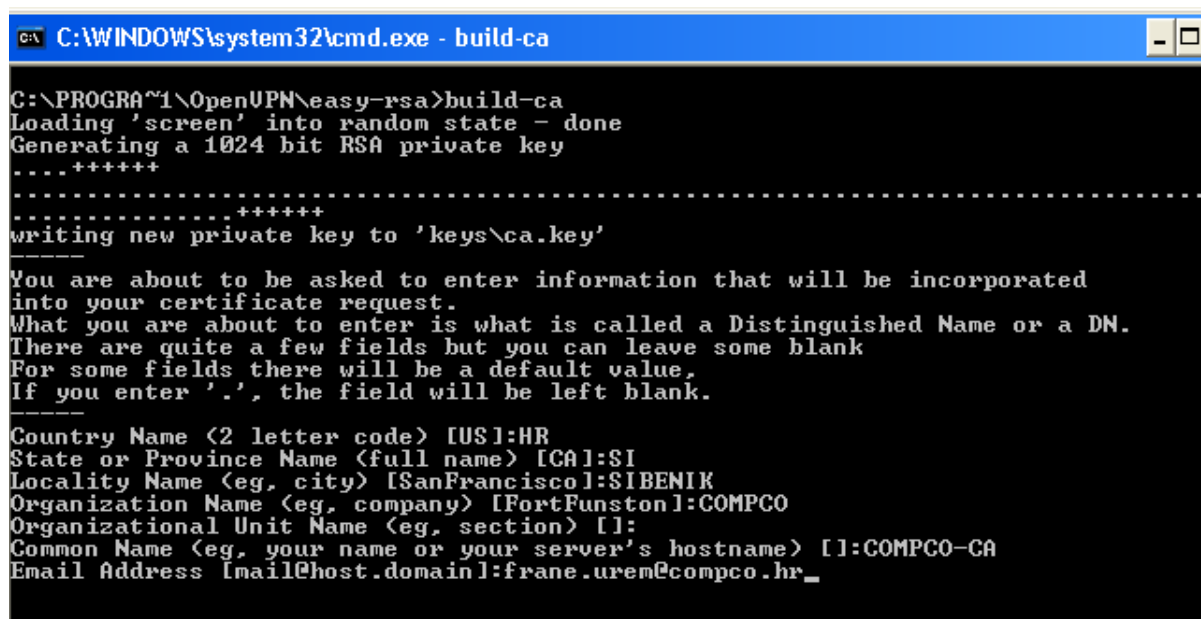
Da bi se to obavilo, potrebno je pokrenuti *init-config.bat* datoteku u mapi: *c:\Program Files\OpenVPN\easy-rsa*. Rezultat je *vars.bat* datoteka, generisana u istoj mapi. Postavlja se veličina ključa na 2048 bita, i podešavaju preostali parametri za generisanje npr.

```
set KEY_SIZE=2048
set KEY_COUNTRY=HR
set KEY_PROVINCE=SI
set KEY_CITY=SIBENIK
set KEY_ORG=COMPCO
set KEY_EMAIL=frane.urem@compco.hr
```

Pokrene se uređeni *vars.bat*, a nakon njega *clean-all.bat*, kako bi se “očistila” mapa s ključevima.

3. Stvara se CA root sertifikat pokretanjem *build-ca.bat*.

Prilikom generisanja potrebno je upisati podatke kao i u *vars.bat* datoteci. Za polje ‘Common Name’ može se upisati naziv kompanije koja izdaje sertifikat s dodatkom “-CA”, kao u primeru.



```
C:\WINDOWS\system32\cmd.exe - build-ca

C:\PROGRA~1\OpenUPN\easy-rsa>build-ca
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:HR
State or Province Name (full name) [CA]:SI
Locality Name (eg, city) [SanFrancisco]:SIBENIK
Organization Name (eg, company) [FortFunston]:COMPCO
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:COMPCO-CA
Email Address [mail@host.domain]:frane.urem@compco.hr_
```

Slika 26. Kreiranje CA root sertifikata

Konačni rezultat su: *ca.cert* i *ca.key* u mapi *c:\Program Files\OpenVPN\easy-rsa\keys*. *Ca.key* je privatni CA ključ i mora se čuvati na vrlo sigurnom računaru koji nema pristup mreži.

```
C:\Program Files\OpenUPN\easy-rsa\keys>dir
Volume in drive C has no label.
Volume Serial Number is 43E9-8090

Directory of C:\Program Files\OpenUPN\easy-rsa\keys

07.02.2007  21:26    <DIR>          .
07.02.2007  21:26    <DIR>          ..
07.02.2007  21:26             1.196 ca.crt
07.02.2007  21:26             887 ca.key
```

Slika 27. Lista generisanih CA root datoteka

4. Zatim se kreira sertifikat i privatni ključ za VPN server.

To se izvodi pokretanjem naredbe : *build-key-server.bat* server. Upisuju se traženi podaci o izdanom sertifikatu kao i kod kreiranja javnog CA sertifikata. Rezultat pokretanja su privatni ključ i sertifikat za server (*server.key*, *server.crt*), potpisani CA ključem, izdati na rok od 10 godina. Rok izdavanja možemo kontrolisati unutar *build-keyserver.bat* datoteke.

```
A challenge password []:
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'HR'
stateOrProvinceName     :PRINTABLE:'SI'
localityName            :PRINTABLE:'sibenik'
organizationName        :PRINTABLE:'COMPCO'
organizationalUnitName  :PRINTABLE:'COMPCO'
commonName              :PRINTABLE:'SERVER'
emailAddress            :IA5STRING:'frane.urem@compco.hr'
Certificate is to be certified until Feb  4 22:28:11 2017 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Slika 28. Kreiranje sertifikata i ključa za server

5. Kreiraju se sertifikati i ključevi za klijente koji će pristupati serveru.

To se izvodi pokretanjem: *build-key <ime klijenta>* , npr. ukoliko su 3 klijenta (klijent1, klijent2, klijent3), pokrene se tri puta *build-key.bat*, za svakog klijenta posebno:

```
build-key klijent1
build-key klijent2
```

build-key klijent3

Rezultat su parovi ključeva i sertifikata za svakog klijenta, u podmapu `\keys`.

6. Generiše se Diffie Hellman parametar.

To se izvodi pokretanjem *build-dh.bat*. Rezultat je veliki, slučajno generisani prim broj, koji se kopira samo na server. Ovaj postupak traje najduže, a može se ubrzati unošenjem malo entropije u sistem, npr. nasumičnim pomicanjem miša.

7. Unosi se dodatna sigurnost generisanjem tzv. *ta* ključeva.

To se izvodi pokretanjem naredbe: *openvpn --genkey --secret ta.key* Rezultat je ključ za HMAC potpisivanje paketa, u svrhu dodatne autorizacije. Ključevi se moraju sigurno razmeniti sa serverom i klijentima, i iskopirati u podmapu `\keys`.

Na kraju je potrebno iskopirati generisane ključeve, prema sledećoj tablici:

Ime datoteke:	Koristi ga:	Svrha:	Tajnost:
ca.crt	Server i svi klijenti	Root CA sertifikat	NE
ca.key	Samo sigurno računalo za generiranje ključeva	Root CA ključ	DA
dh{n}.pem	Samo server	Diffie-Hellman parametar	NE
server.crt	Samo server	Server sertifikat	NE
server.key	Samo server	Server ključ	DA
client1.crt	Klijent1	klijent1 sertifikat	NE
client1.key	Klijent1	klijent1 ključ	DA
client2.crt	Klijent2	klijent2 sertifikat	NE
client2.key	Klijent2	klijent2 ključ	DA
client3.crt	Klijent3	klijent3 sertifikat	NE
client3.key	Samo klijent3	klijent3 ključ	DA

Tablica 1: Raspodela Sertifikata, u primeru : jedan server, tri klijenta

Konfiguracione datoteke se podešavaju kao i u primeru sa statičkim ključem, ali se umesto statičkog ključa zadaju imena sertifikata i ključeva za server i klijente. Primer konfiguracijske datoteke za server:

```
dev tap
proto udp
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
persist-tun
ifconfig 192.168.122.1 255.255.255.0
verb 4
mute 10
```

Primjer konfiguracione datoteke za klijenta, koji pristupa na udaljenu IP adresu 213.191.134.11:

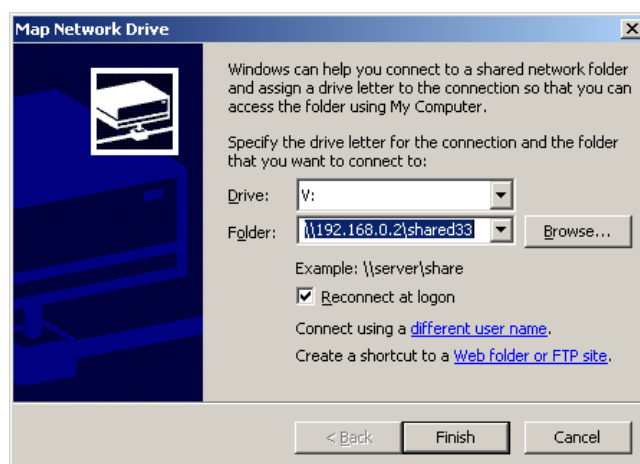
```
remote 213.191.134.11
dev tap
ifconfig 192.168.122.100 255.255.255.0
ca ca.crt
cert klijent1.crt
key klijent1.key
verb 4
mute 10
```

Sva ostala podešavanja su ista kao i u primeru sa statičkim ključem.

13. Primer implementacije VPN-a

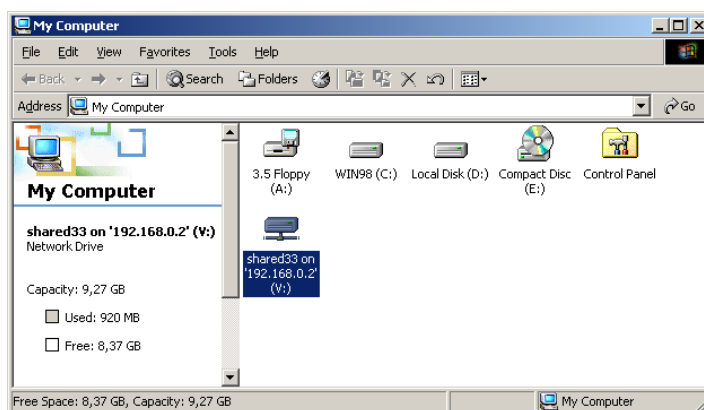
Karakterističan slučaj primene VPN-a u modernom poslovanju je dakle deljenje podataka između udaljenih lokalnih mreža. U ovom primeru date su dve lokalne mreže sa deljenim direktorijima koji moraju, uz odgovarajuću autentikaciono-autorizacijsku politiku, biti dostupni korisnicima iz dveju mreža.

VPN tunel održavaju posebni usmerivački uređaji (VPN routeri) opremljeni ethernet portovima, koji upotrebljavaju IPSec protokol. IPSec je tzv. *layer 3* protokol, koji podržava siguran prenos podataka kroz IP mreže. IPSec podaci organizovani su u posebne pakete (IPSec tunel paketi), koji u osnovi predstavljaju enkapsulirane IP pakete, enkriptovane kriptografskim algoritmom dogovorenim između dve strane IP tunela.



Slika 29. – Konfiguracija pristupa udaljenom deljenom direktorijumu

Prva lokalna mreža, sa skupom adresa 192.168.0.1/255.255.255.0 ima deljeni direktorijum na računaru sa operativnim sistemom Windows 2000 Server sa adresom 192.168.0.2. Ako je na tom računaru dozvoljen pristup korisniku *guest*, tada će računar iz druge lokalne mreže sa skupom adresa 192.168.2.1/255.255.255.0, operativnim sistemom Windows 2000 Server i adresom 192.168.2.2 primeniti sledeći postupak kako bi pristupio tom deljenom direktorijumu.



Slika 30. – Udaljeni deljeni direktorijumj u lokalnom My Computer prozoru

U meniju Windows Explorer aplikacije ići na *Tools -> Map Network Drive*, nakon čega se pojavljuje dijaloški okvir u koji treba uneti osnovne podatke o udaljenom deljenom direktorijumu (kao na Sl.29).

Nakon unošenja ovih podataka operativni sistem će tražiti *username* i *password* za korisnika koji pristupa direktorijumu, i u slučaju uspešne autorizacije napraviti novi virtualni disk - lokalnu sliku udaljenog deljenog direktorijuma (Sl. 30). Prava pisanja i čitanja na novom disku određena su autorizacionom politikom računara na kojem se deljeni direktorijum nalazi ili domena čiji je član.

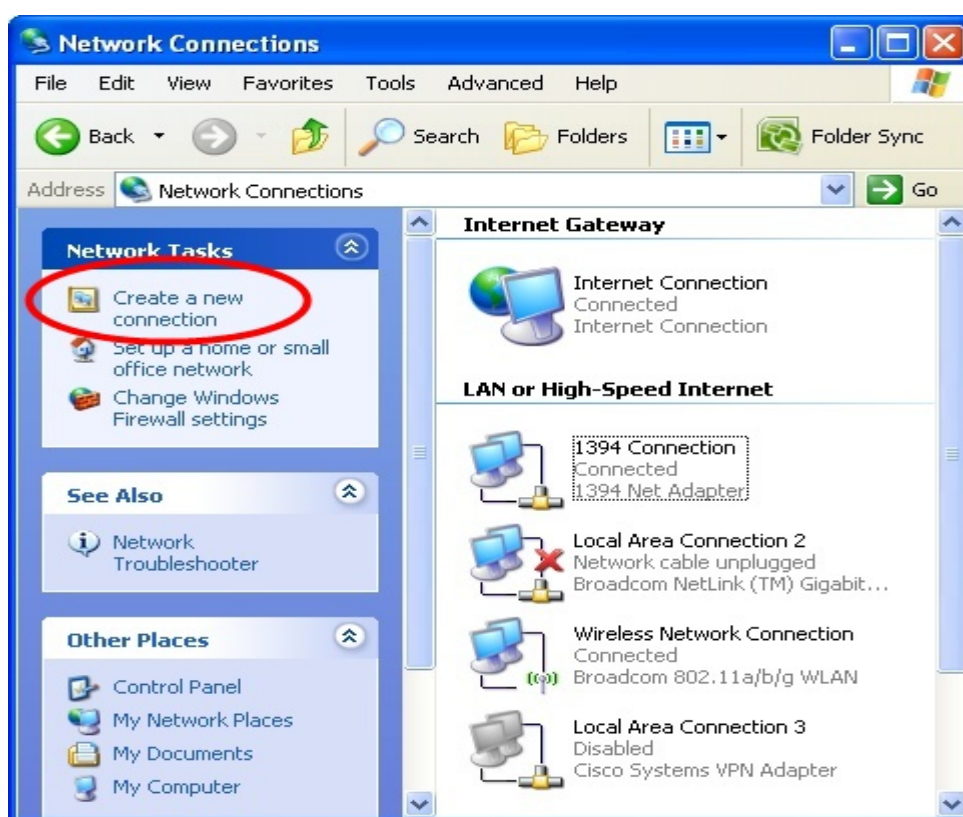
Pri svemu ovome treba još naglasiti da je su deljeni direktorijumi dobijeni ovim postupkom izolovani od Internet okruženja koje se koristi za prenos podataka koji se nalaze u njima. Njihova "nevidljivost" korisnicima Interneta proističe iz činjenice da se nalaze na računarima koji direktno nisu članovi Interneta, već su im date adrese koje pripadaju njihovim lokalnim mrežama. Sigurnost podataka koji se prenose Internetom osigurava enkripcija u IP tunelu formiranom u sklopu VPN-a. U ovom slučaju primenjuje se 3DES algoritam za simetričnu enkripciju koji koristi ključ efektivne dužine od 128 bita.

14. Postupak kreiranja Virtualne privatne mreže

U ovom poglavlju će biti prikazan postupak kreiranja Virtualne privatne mreže unutar Windows XP operacionog sistema.

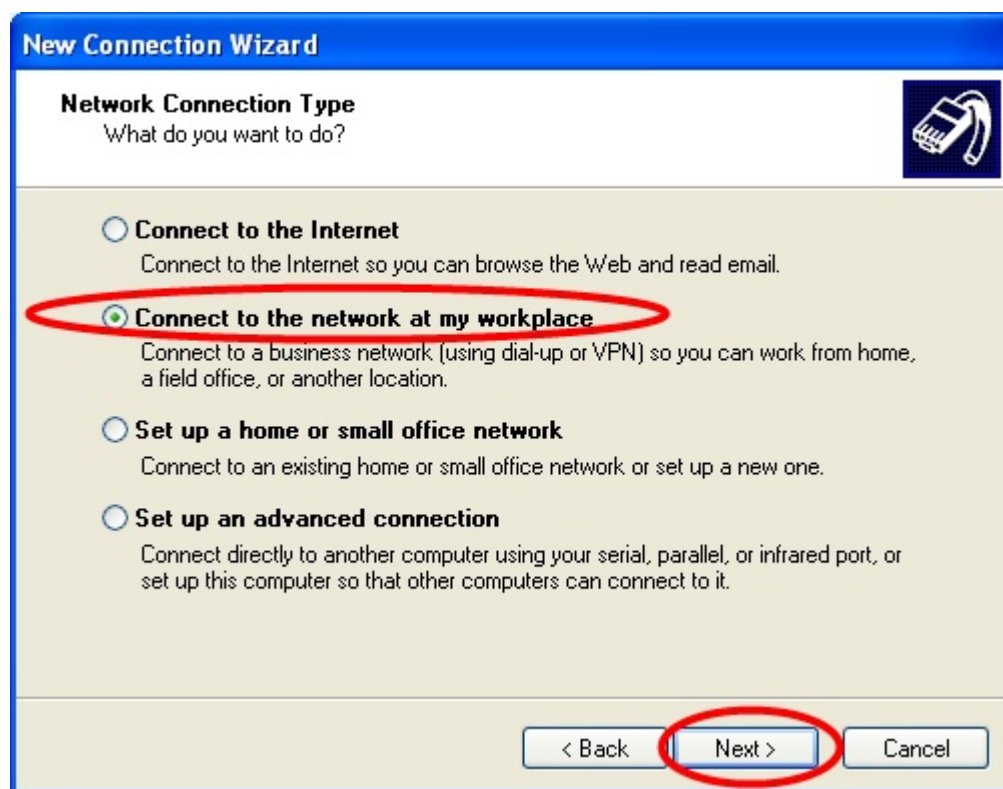
Pošto Windows XP ima sve predispozicije za kreiranje VPN konekcije bez dodatnog softvera proces se odvija na sledeći način:

1. Prvo što trebate napraviti je provera da ste uredno spojeni na Internet..
2. Kliknite „Start“ pa „Control Panel“.
3. Odaberite „Network Connections“.
4. Kliknite „Create a new connection“.



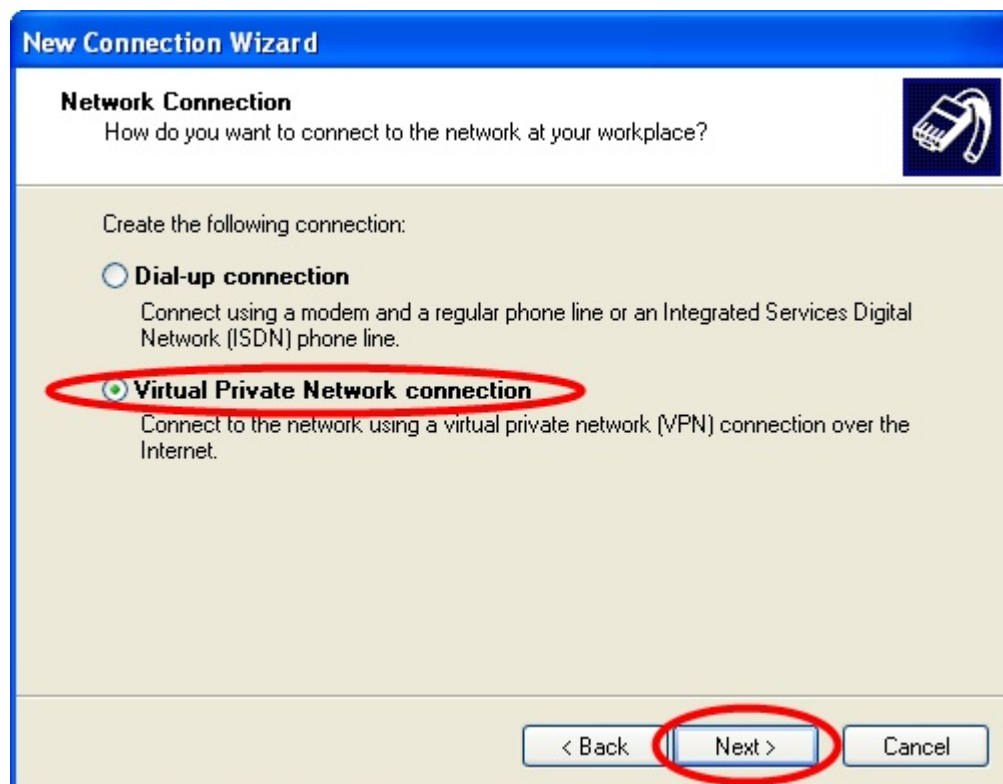
Slika 31.

5. U Network Connection Wizard –u odaberite „Next“.
6. Kliknite Connect to the network at my workplace i odaberite „Next“.



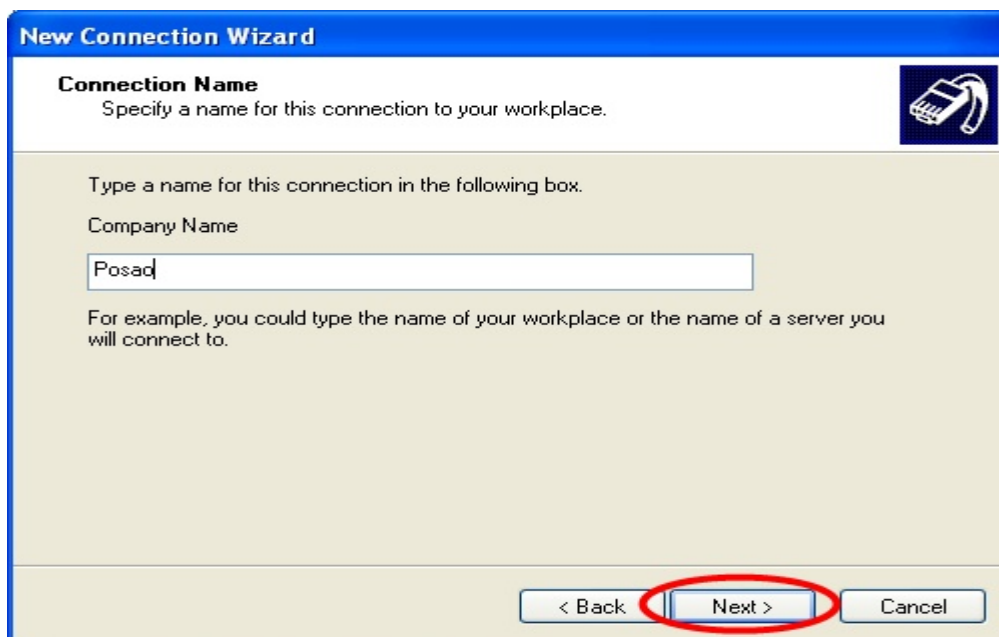
Slika 32.

7. Odaberite *Virtual Private Network* connection pa „Next“.



Slika 33.

8. Unesite proizvoljno ime vaše VPN konekcije, u ovom slučaju je to “Posao”. Odaberite “Next”.



Slika 34.

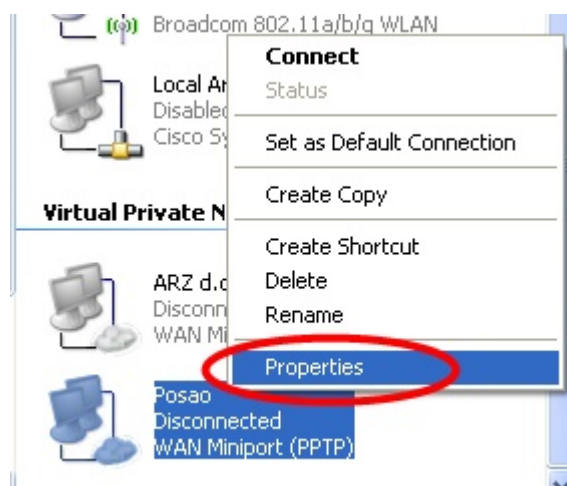
9. U slučaju da ste pitani da li ćete koristiti dial-up vezu ili već spojenu preko DSL-a (ili nečeg trećeg) odaberite: *Do not dial the initial connection* pa „Next“.

10. Unesite IP adresu ili Hostname gde ćete se spajati (te podatke obično dobijete od administratora).

11. U slučaju da ste pitani želite li koristiti Smart Card odaberite *Do not use my smart card*.

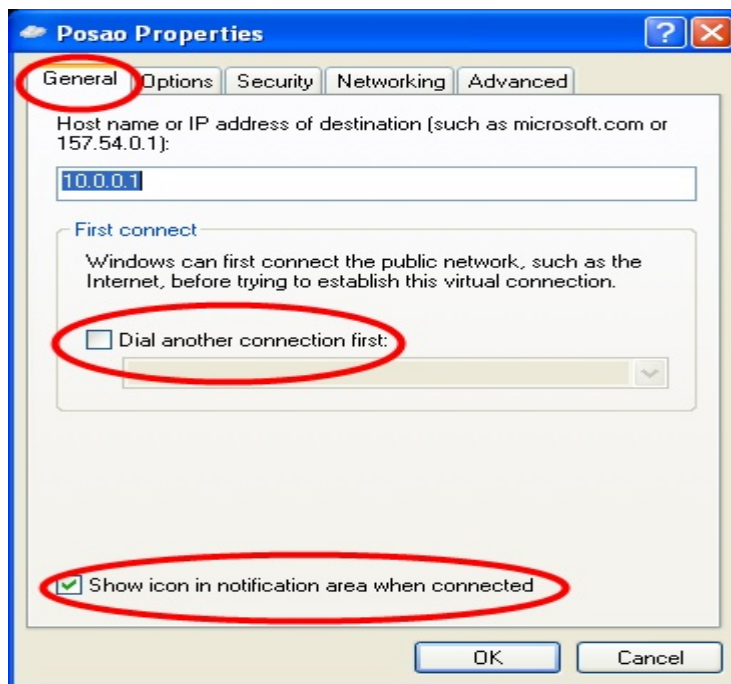
12. Sada odaberite želite li prečicu na vašoj radnoj površini ili ne i kliknite „Finish“.

13. Nakon što je konekcija napravljena možda će se automatski pokušati spojiti preko VPN –a, ako ne, odaberite *Control Panel*, pa u *Network Connections* i desnim klikom na Vašu kreiranu VPN konekciju odaberite „*Properties*“.



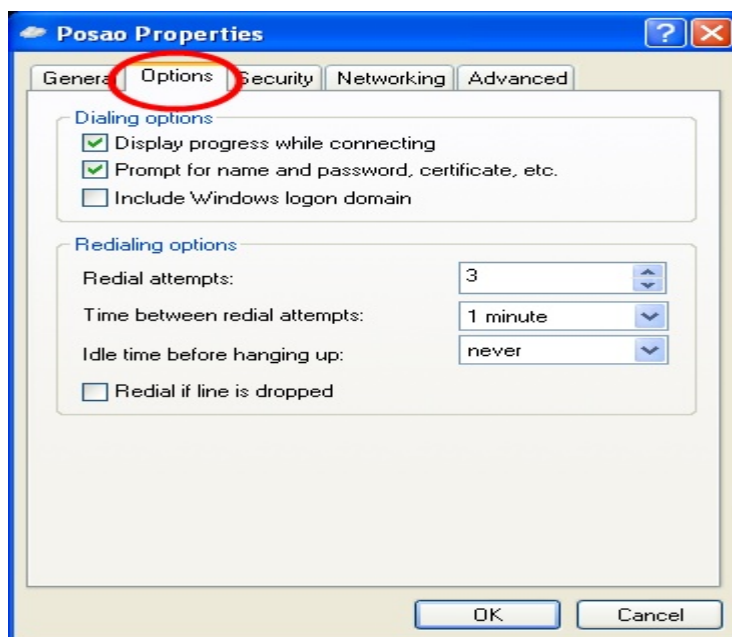
Slika 35.

14 . U prvoj opciji (tabu) General možete promeniti IP adresu ili Hostname na koji se spajate kao i automatsko spajanje na Internet prilikom pokretanja VPN konekcije (vredi samo za dial-up konekcije). Takođe imate opciju da li želite status da ste spojeni u Taskbar -u (*Show icon in notification area when connected*).



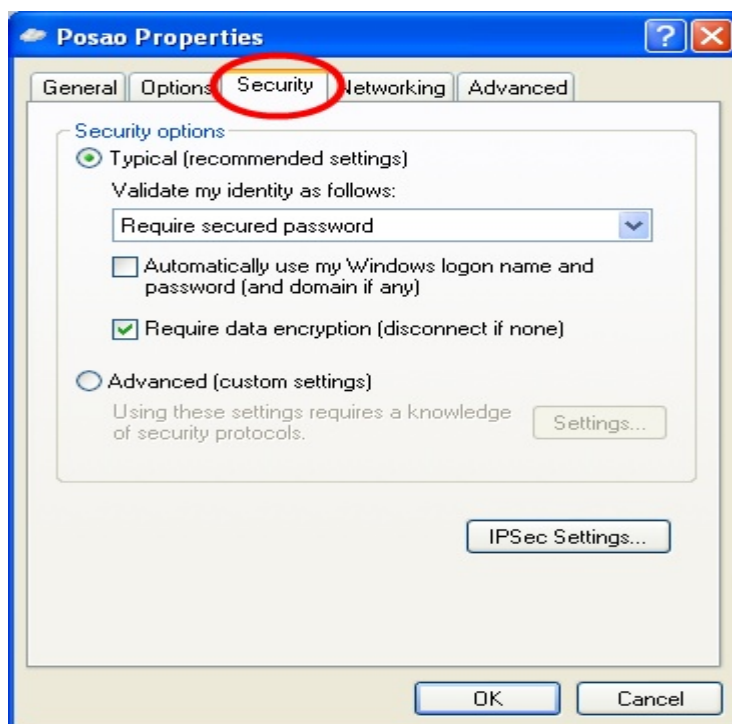
Slika 36.

15. Sljedeća opcija (tab) je „Options“ u kojoj možete puno toga podesiti. Tu su stvari kao „Include Windows logon domain“ pomoću koje će vam tražiti podatke spajanja na domenu pri pristupu VPN-u ili „Redial attempts“ što znači nakon koliko vremena da se ponovno spaja ako konekcija nije uspostavljena.



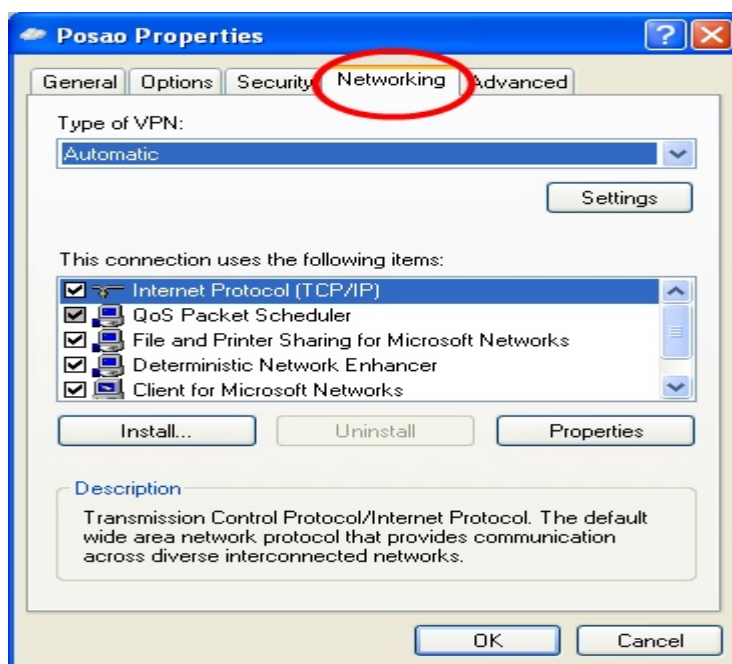
Slika 37.

16. Nakon „Options -a“ dolazi nam opcija „Security“ u kojoj u principu postavljate tip enkripcije i sigurnosti spajanja Vaše VPN konekcije. Te podatke uglavnom dobijete od administratora pošto je on odredio tip enkripcije.



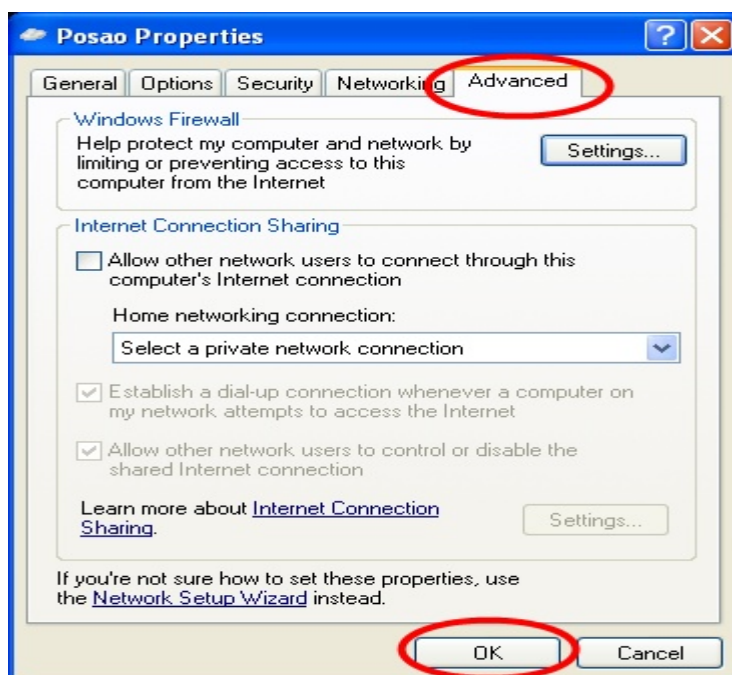
Slika 38.

17. U opciji „Networking“ možete odabrati koji protokli i servisi će biti korišteni tokom VPN konekcije.



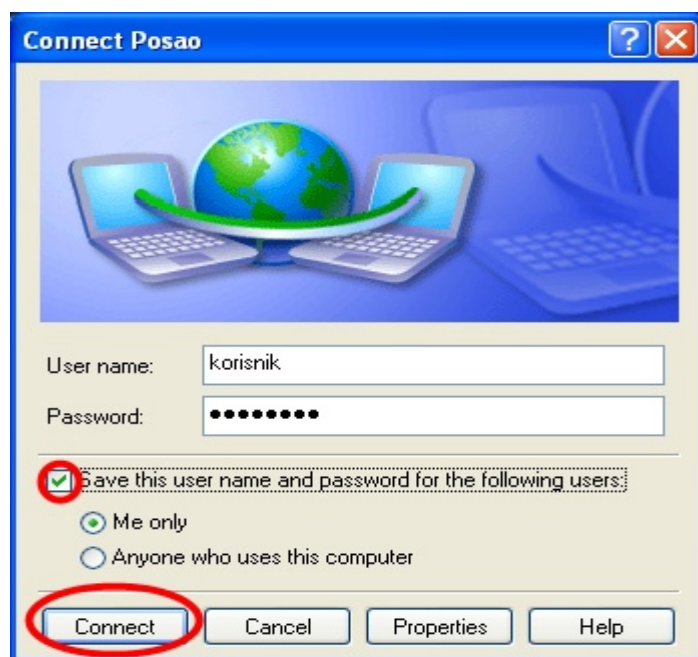
Slika 39.

18. I poslednja opcija je „Advanced“ u kojoj možete konfigurisati *Firewall* i *Sharing* (zajedničko korišćenje).



Slika 40.

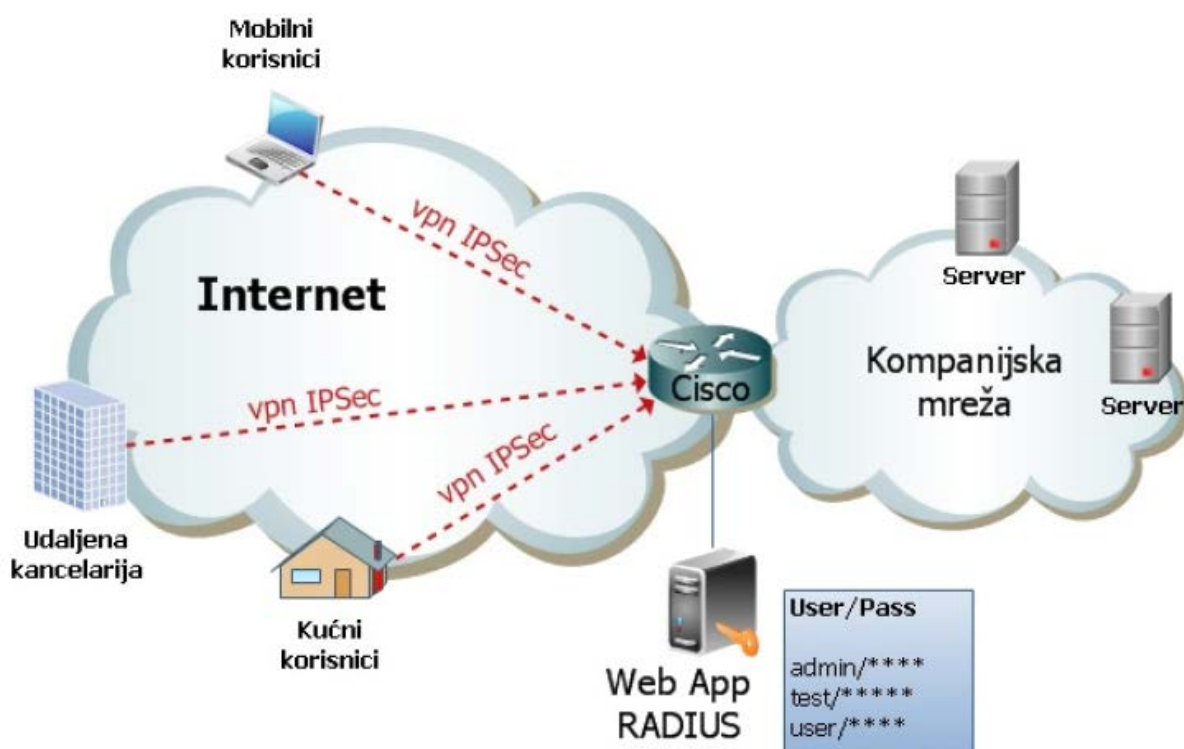
19. Nakon što ste konfigurisali VPN konekciju sve je spremno i za spajanje. Odaberite Vašu VPN konekciju i nakon unosa korisničkog imena (*User name*) i šifre (*Password*) kliknite „Connect“. Isto tako za kraj veze odaberite konekciju i kliknite „Disconnect“.



Slika 41.

15. Primer za implementaciju Cisco IPSec VPN servisa

VPN koristi javnu mrežnu infrastrukturu uz očuvanje privatnosti kroz bezbednosne procedure i protokole kao što je IPSec. Sistem funkcioniše tako što se podaci šifruju na predajnoj strani i dešifruju na prijemnoj strani. Komunikacija se odvija kroz "tunel" što obezbeđuje dodatni nivo sigurnosti, koji obuhvata šifrovanje podataka i mrežnih adresa učesnika u komunikaciji.



Slika 42 : Primer implementacije Cisco IPSec VPN servisa

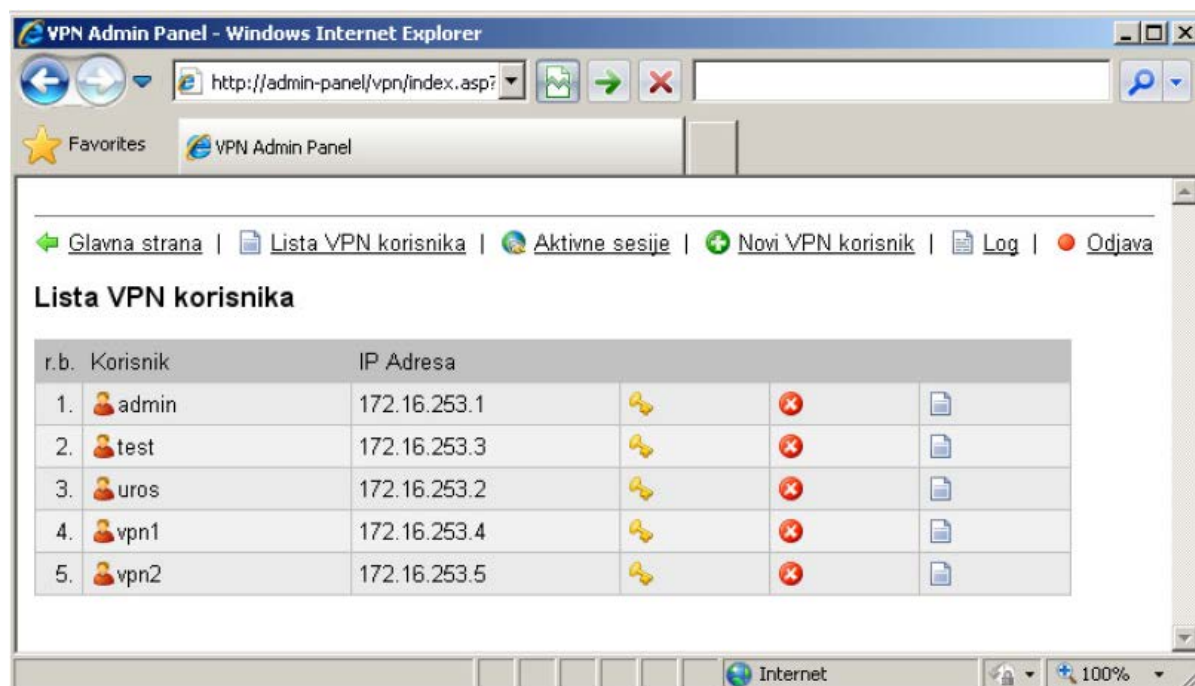
Cisco IPSec VPN omogućava:

- Povezivanje teritorijalno udaljenih kancelarija kompanije u jedinstvenu privatnu mrežu.
- Sigurnu vezu radi pristupa bazama podataka, svim dokumentima i programskim aplikacijama dostupnim zaposlenima u kompaniji.
- Pristup e-mail serveru, potrebnim adresama i brojevima telefona iz Vašeg adresara;
- Čitanje elektronske pošte i odgovaranje na hitne obaveze bez obzira na vreme i mesto na kome se trenutno nalazite.
- Pouzdanu i efikasnu komunikaciju sa mobilnim timovima kompanije uz bolju koordinaciju i organizaciju poslovanja (npr. slanje narudžbina sa terena).

Administracija korisničkih naloga omogućena je preko web aplikacije VPN Admin Panel. Web aplikacija ima sledeće karakteristike:

- Kreiranje VPN korisničkih naloga.
- Prikaz aktivnih VPN sesija na ruteru u realnom vremenu.
- Izmena podataka i brisanje korisničkih naloga.
- Pregled svih ostvarenih sesija za svaki korisnički nalog.

Za instalaciju web aplikacije VPN Admin Panel neophodno je obezbediti računar sa Windows operativnim sistemom sa instaliranom komponentom IIS (Internet Information Services).



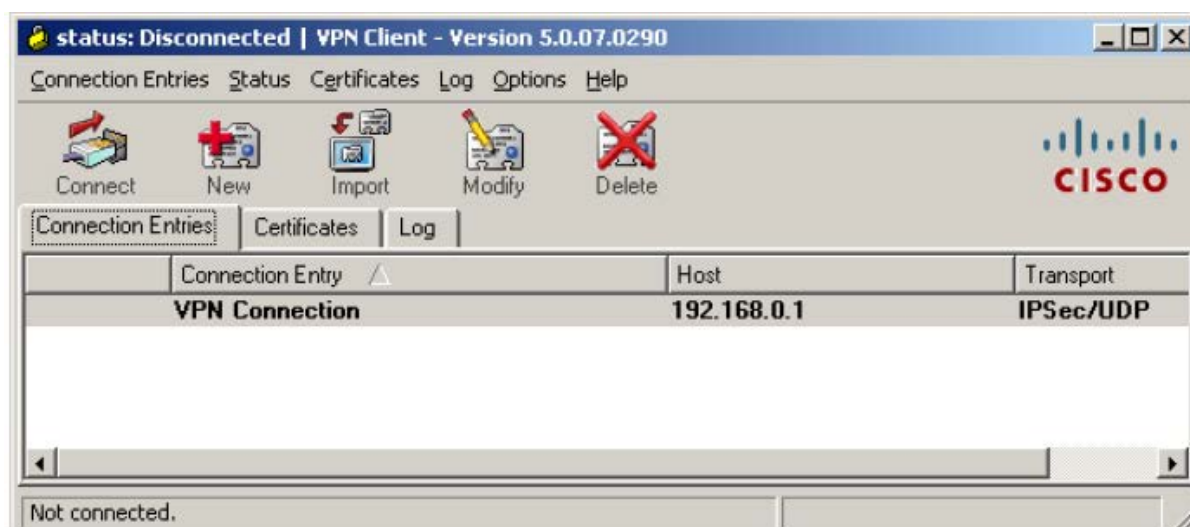
Slika 43: VPN Admin Panel – Prikaz liste VPN korisnika

Svaki kreirani VPN nalog automatski dobija fiksnu IP adresu, što omogućava veću kontrolu pristupa, koja se može ostvariti primenom pristupnih lista (eng. access list) na Cisco ruteru.



Slika 44: VPN Admin Panel – Stranica za dodavanje VPN naloga

VPN konekcija se ostvaruje preko aplikacije Cisco VPN Client. U zavisnosti od verzije operativnog sistema na računaru korisnika (32-bit ili 64-bit), neophodno je instalirati odgovarajuću verziju aplikacije.

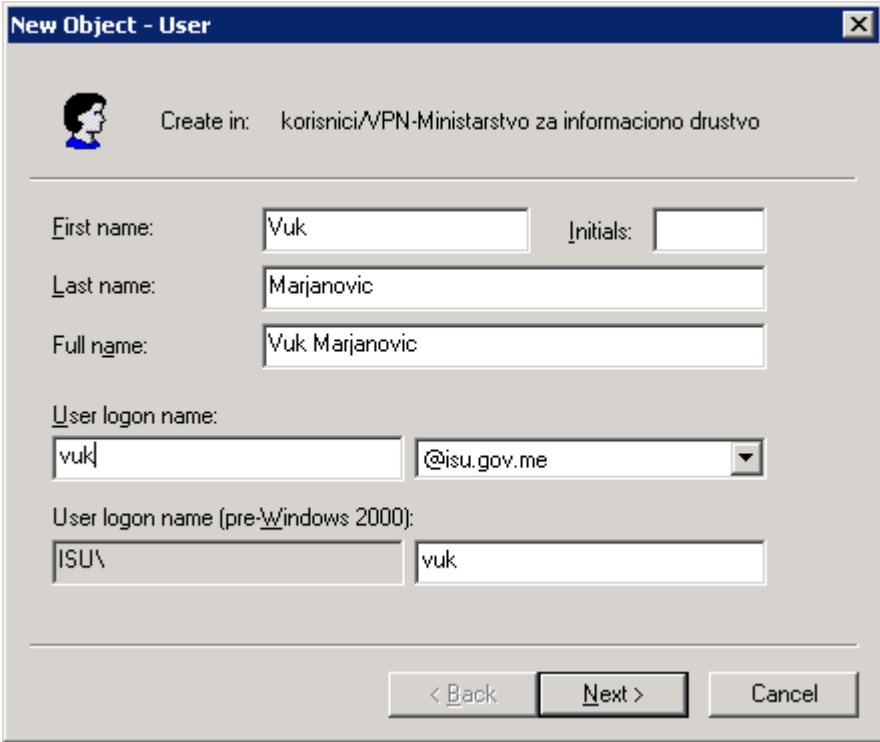


Slika 45: Cisco VPN Client – Izgled glavnog prozora

16. Primer administracije VPN naloga u MUP-u Crne Gore

Primer administracije VPN naloga na aktivnom direktorijumu koji se nalazi na Windows Serveru 2003, 64/bit.

Kreiranje VPN korisnika u AD-u. Prati se procedura:



New Object - User

Create in: korisnici/VPN-Ministarstvo za informaciono drustvo

First name: Vuk Initials:

Last name: Marjanovic

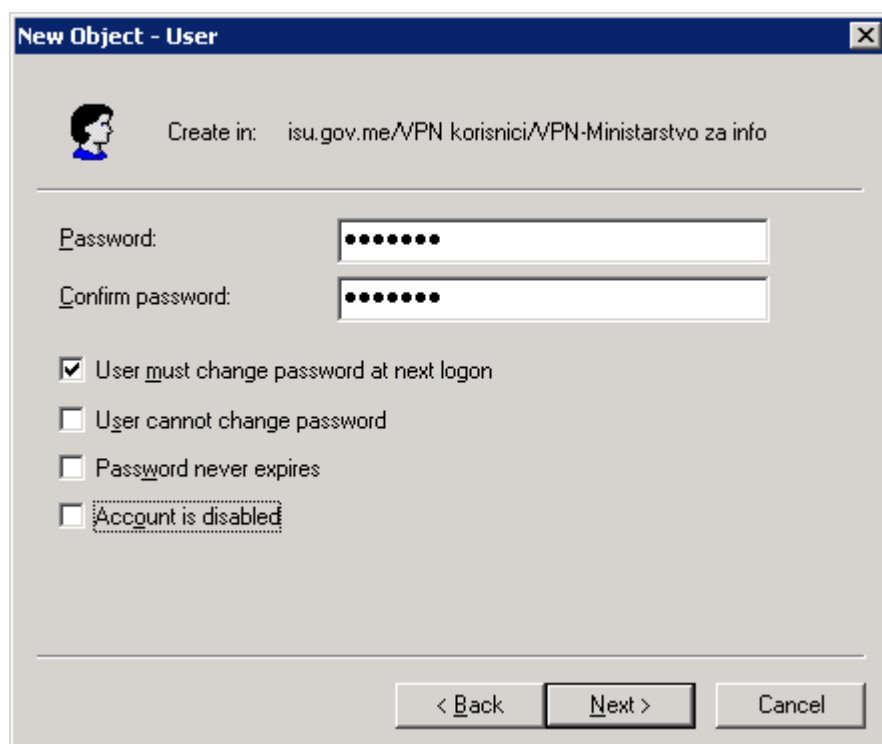
Full name: Vuk Marjanovic

User logon name: vuk @isu.gov.me

User logon name (pre-Windows 2000): ISU\ vuk

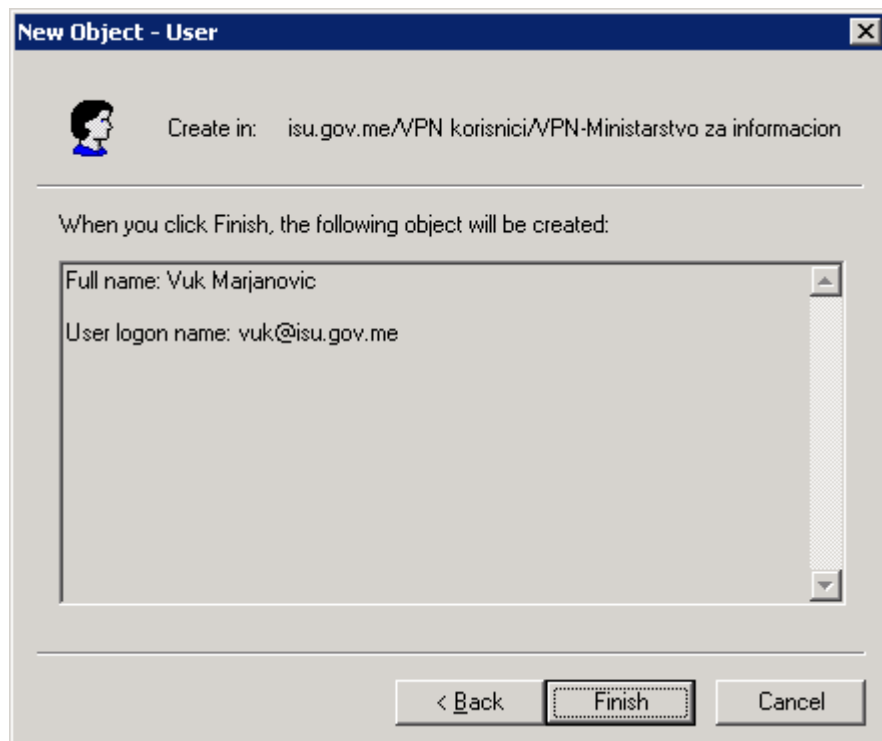
< Back Next > Cancel

Slika 46.



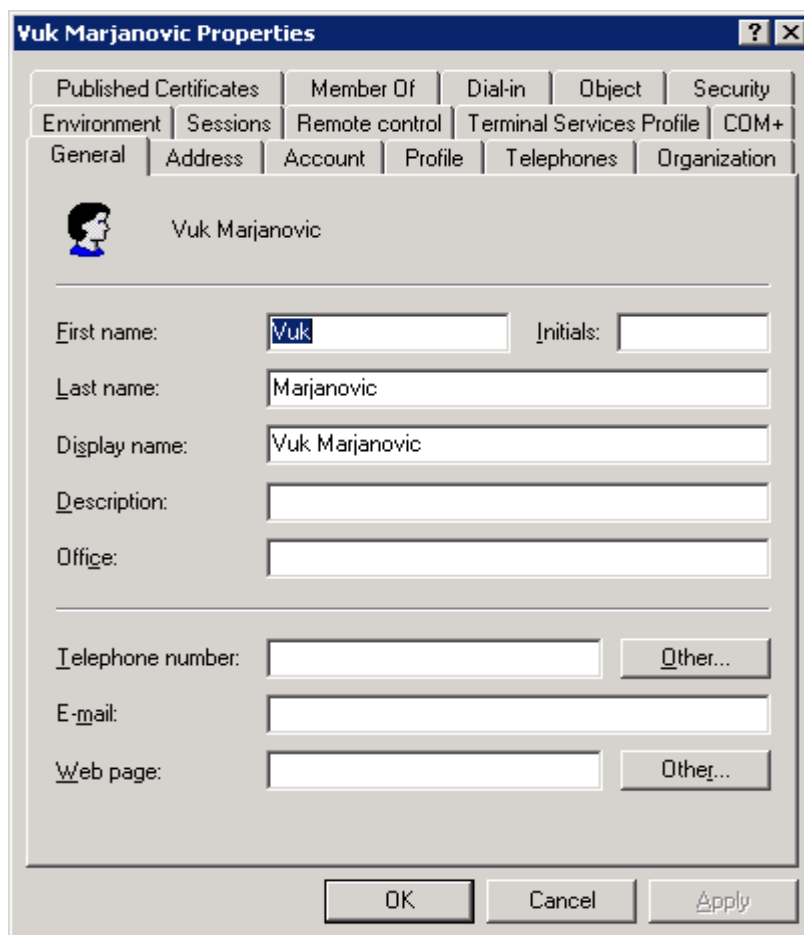
The screenshot shows a Windows-style dialog box titled "New Object - User". At the top, it says "Create in: isu.gov.me/VPN korisnici/VPN-Ministarstvo za info". Below this, there are two password input fields: "Password:" and "Confirm password:", both containing masked characters (dots). Under the password fields, there are four checkboxes with labels: "User must change password at next logon" (checked), "User cannot change password", "Password never expires", and "Account is disabled". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Slika 47. Setovanje password-a za korisnika



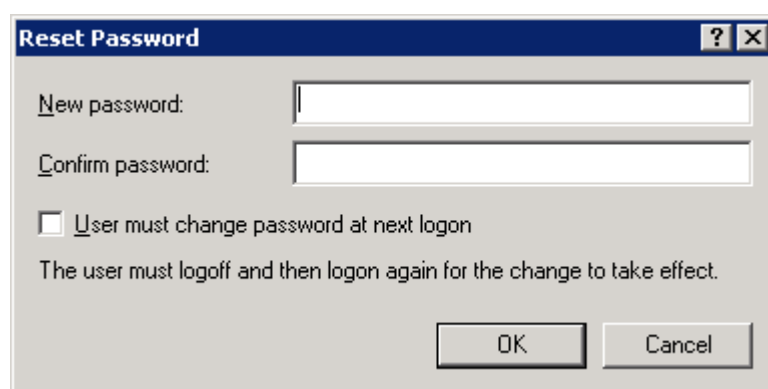
The screenshot shows the same "New Object - User" dialog box, but at a later stage. It now displays a summary of the user object to be created. The text "When you click Finish, the following object will be created:" is followed by a list box containing two items: "Full name: Vuk Marjanovic" and "User logon name: vuk@isu.gov.me". At the bottom, the buttons are "< Back", "Finish", and "Cancel".

Slika 48.



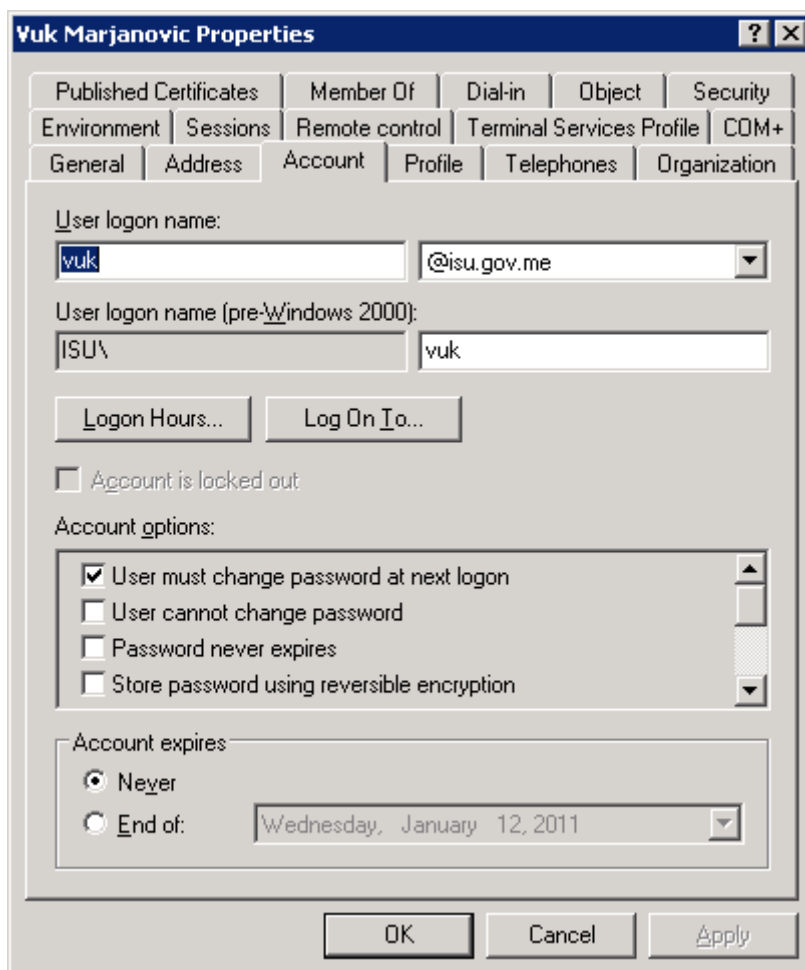
Slika 50. Setovanje korisnika u AD bazi

Na nalogu korisnika imamo niz mogućnosti gde možemo podešavati prava korisnika i unositi određene informacije o njemu.



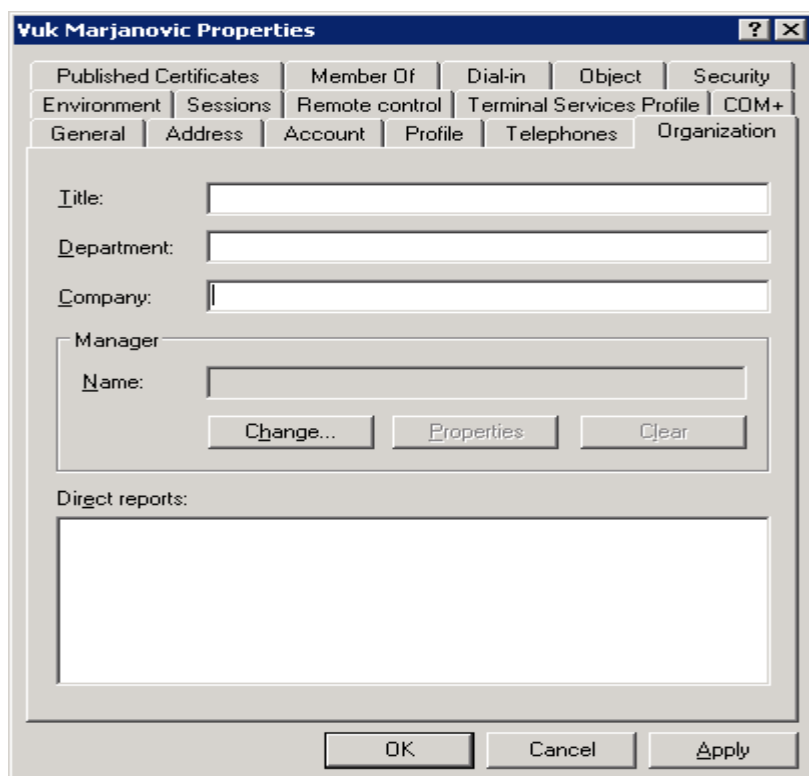
Slika 51. Prikaz prozora za logovanje od kuće

Unosi se ime koje je dodelio administrator.

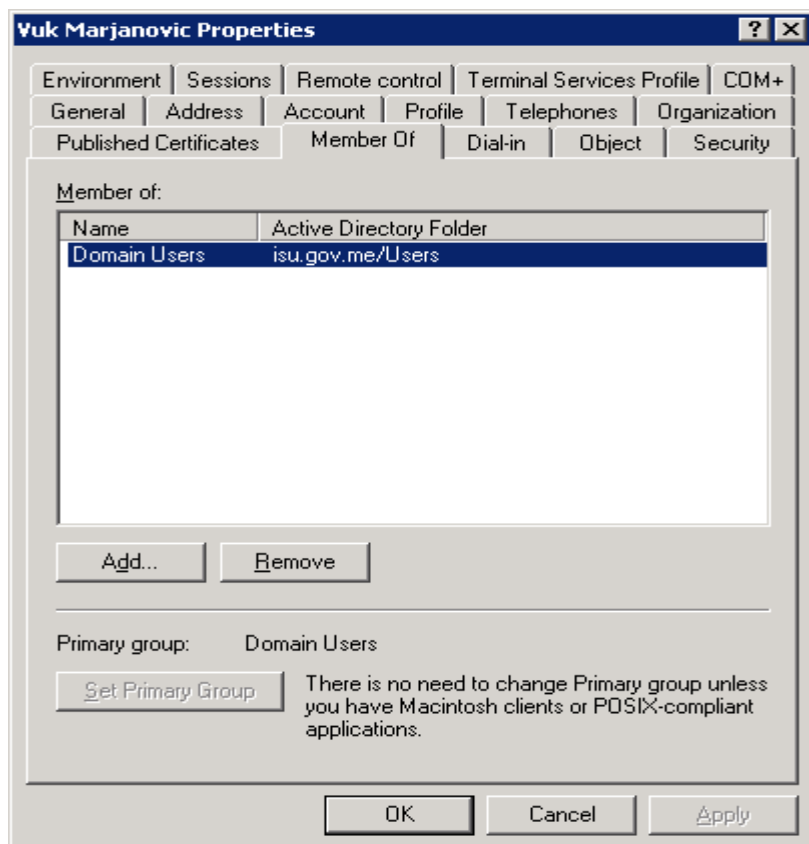


Slika 52. Prikaz naloga sa nazivom za logovanje

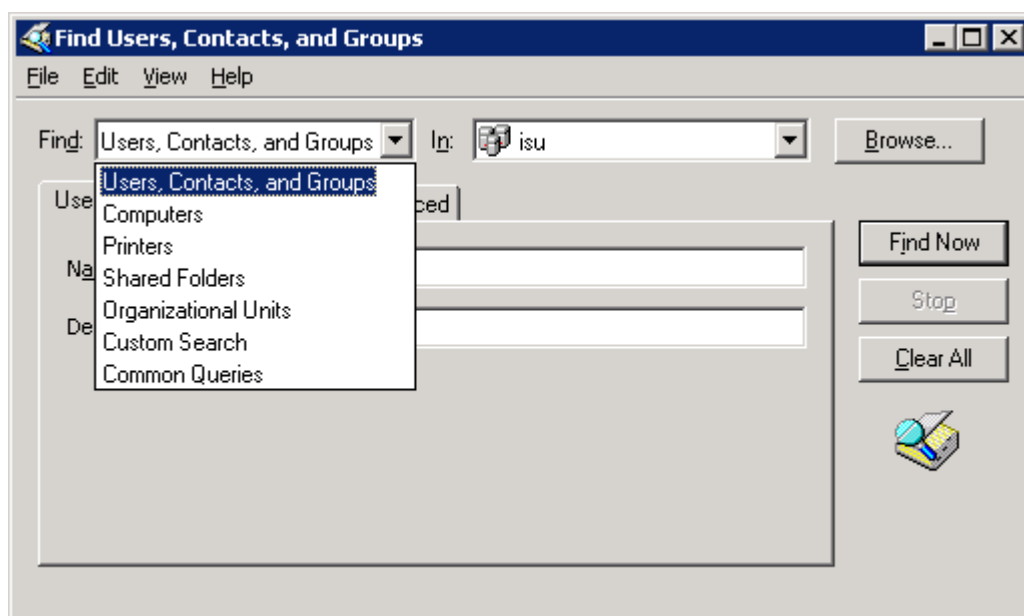
Na polju *Account options* mozemo podešavati određenu *password* politiku. U ovom slučaju poželjno je staviti da se *password* ne menja jer je po *default* podešeno da se *password* menja nakon 42 dana.



Slika 53. Prikaz dodavanja informacija o organizaciji korisnika



Slika 54. Prikaz dodeljivanja članstva korisniku



Slika 55. Pretraga korisnika u AD-u

Kao što vidimo pretraga se može izvršiti na osnovu niza karakteristika i informacija o korisniku koje se dodaju u prethodno prikazanom prozoru na slici 38.

17. Realizacija VPN-a u preduzeću TEHPRO D.O.O. Beograd



11250 Beograd, Jugoslovenska 2
Tel: 011/2580-785, 2580-795; Fax: 011/2580-778
office@tehpro.co.yu www.tehpro.co.yu
TEHPRO d.o.o. - Društvo za usluge u oblasti zaštite

Preduzeće TEHPRO je osnovano 1991. godine. Osnovna delatnost je pružanje usluga u oblastima:

- bezbednost i zdravlje na radu,
- zaštita od požara,
- zaštita životne sredine

Od 1996. godine na tržište Srbije plasira lična zaštitna sredstva, instrumente i sisteme za detekciju eksplozivnih i toksičnih gasova proizvođača MSA AUER. Usledila je distribucija i zastupništvo i drugih renomiranih svetskih proizvođača sredstava i opreme za ličnu i kolektivnu zaštitu.

Od osnivanja preduzeće neprestano ulaže u svoj razvoj, sa težištem na obrazovanje i usavršavanje kadrova, i ulaganje u opremu. Poslednjih godina, okosnicu razvoja čine inženjering i savremeno opremljene ekipe koje pružaju kompleksne usluge iz osnovne delatnosti.

U okviru svojih inženjerskih delatnosti preduzeće TEHPRO je sposobno da realizuje kompletne projekte. Posедуje sve licence i zakonska ovlašćenja za projektovanje, izvođenje, zastupanje stranih partnera i firmi, trgovinu, uvoz i izvoz komponenti, sistema, uređaja, sertifikaciju i puštanje u rad.

Kao odgovor na sve veću potrebu za obučanim kadrom u oblasti bezbednosti zdravlja na radu, pokrenut je i centar za edukaciju. Organizovanjem kurseva, seminara i savetovanja kao i izdavanjem stručne literature zaokružen je skup edukativnih aktivnosti koje za cilj imaju unapređenje sistema bezbednosti i zdravlja na radu.

Preduzeće TEHPRO sa sedištem u Beogradu trenutno pokriva veći deo Srbije preko svojih radnih jedinica.



Tehpro - RJ Kruševac
062/808-****

Tehpro - RJ Niš
062/808-****

Tehpro - RJ Čačak
062/808-****

Tehpro - RJ Paraćin
062/808-****

Tehpro - RJ Smederevo
062/808-****

Tehpro - RJ Pančevo
062/808-****

Zbog sve kompleksnijih poslovnih poduhvata, širenja firme i otvaranja novih radnih jedinica, javila se potreba unutar preduzeća da se svi računari povežu unutar jedne mreže radi lakšeg deljenja podataka i međusobne komunikacije. Firma sada broji 68 računara za čije potrebe je i realizovana VPN mreža. Uvođenjem VPN-a firma je umnogome napredovala a najveće prednosti odrazile su se na :

- smanjenje troškova poslovanja i uštedu vremena putem efikasnije komunikacije;
- centralizovano poslovanje i upravljanje preko novih ili postojećih programa za knjigovodstvo, menadžment, magacinsko poslovanje, finansije i sl. ;
- primenu integralnih sistema IP video nadzora i korporativne IP telefonije .

Trenutno je u procesu uvođenje VoIP VPN usluge čime će se praktično sve lokacije povezati u jedinstvenu korporativnu telefonsku mrežu. Svi pozivi između ovih lokacija će biti potpuno besplatni, a udaljene lokacije će moći da koriste sve pogodnosti koje su dostupne u sedištu kompanije.

VPN u preduzeću TEHPRO D.O.O. realizovan je na Microsoft platformi u okviru Small Bussines Servera. Obzirom da je sve u okviru Small Bussines servera glavna pogodnost je da je administracija mnogo lakša jer na istom serveru su i VPN i ostali servisi koji mogu da rade na jednoj mašini. Poboljšana je i kompatibilnost jer je svaki segment pod okriljem Microsofta.

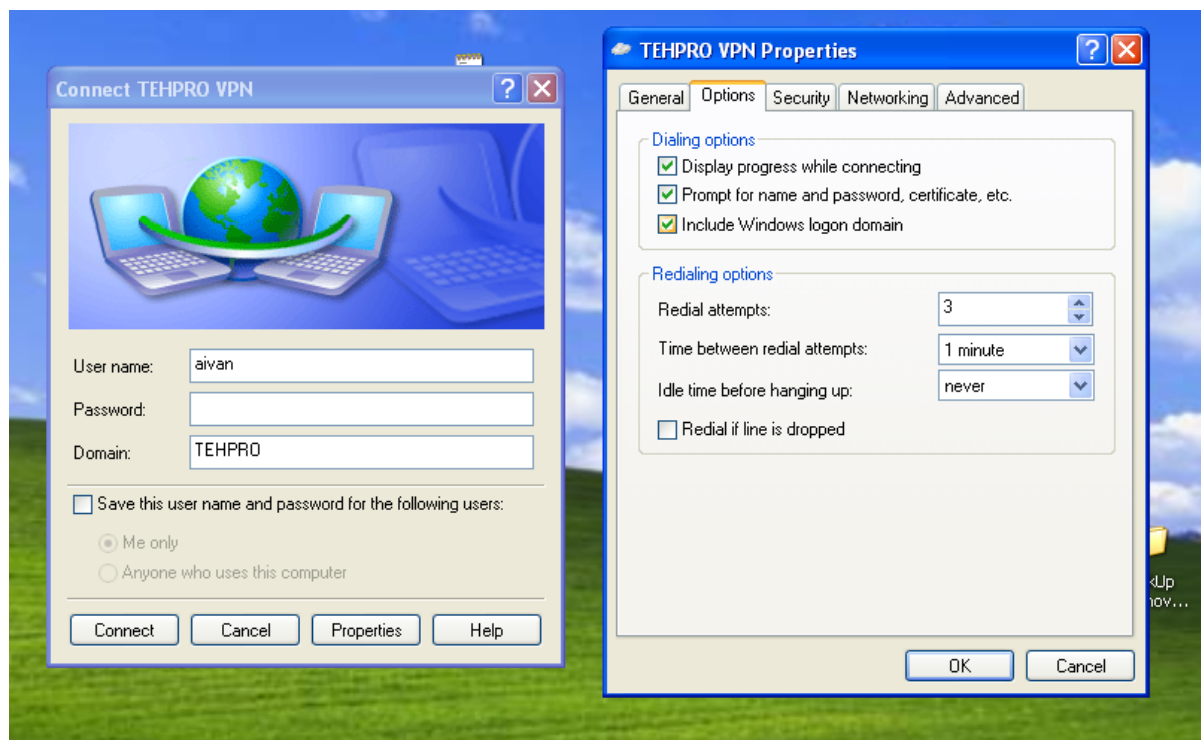
Kada govorimo o nepogodnostima prvo sa čime se možemo susresti je situacija kada port na ruteru nije otvoren. U slučaju da jeste (obzirom da je u pitanju softverski VPN), ruter propušta paket i server vrši autentifikaciju i dekripciju. Autentifikacija se vrši preko CHAP protokola i Microsoft CHAP Version 2. Drugi problem može biti da paket bude pogrešno prosleđen. Problemi se mogu javiti i zavisno od operativnog sistema. U ovom slučaju se radi o Windows 7 OS-u a njemu je zaštita pri konekciji postavljena na najviši nivo tako da se morao smanjiti nivo sigurnosti kako se pokušaj konekcije ne bi odbio.

Sledeći problem koji se može desiti je da server ima konflikt sa DHCP-om oko davanja adresa. Da ne bi došlo do zabune potrebno je "reći" DHCP-u da Vi (server) dajete adrese korisnicima. Da bi se izbegao taj problem možete i podesiti da, recimo prvih 50 adresa budu za interne korisnike i da budu fiksne, a za udaljene korisnike napraviti od 51 pa na dalje, zavisno o koliko subneta se radi.

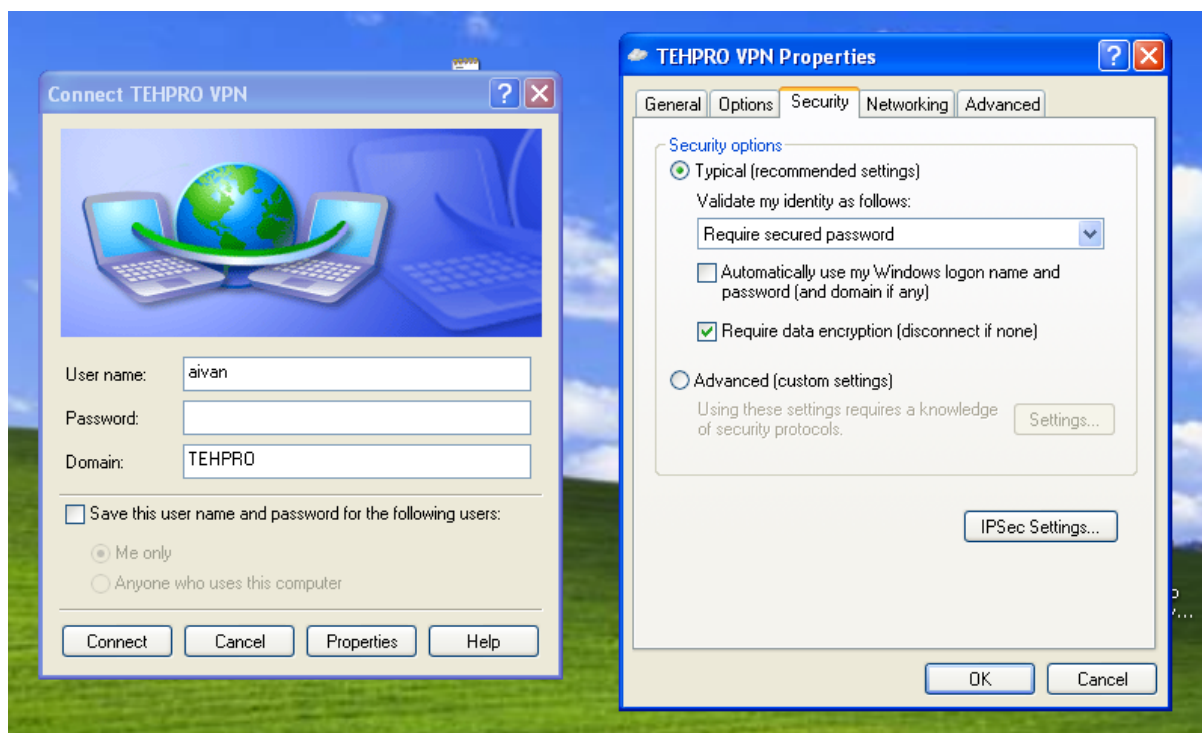
Što se tiče nekih podešavanja u ovom slučaju pažnja treba biti skrenuta na podešavanje prosleđivanja portova na ruteru tako da VPN paketi se dalje prosleđuju VPN serveru. Zatim, kod klijenta na konekciji treba "odčekirati" opciju "Use default gateway on remote desktop". Problematično je i može otežati saobraćaj jer za eksterne adrese svaki upit bi išao preko glavnog servera (kojeg bi koristio kao default gateway).

Ovaj VPN za komunikaciju koristi L2TP/SSL, PPTP i SSTP protokole. Važno je napomenuti i to da je ruter namešten da propušta unapred postavljene portove.

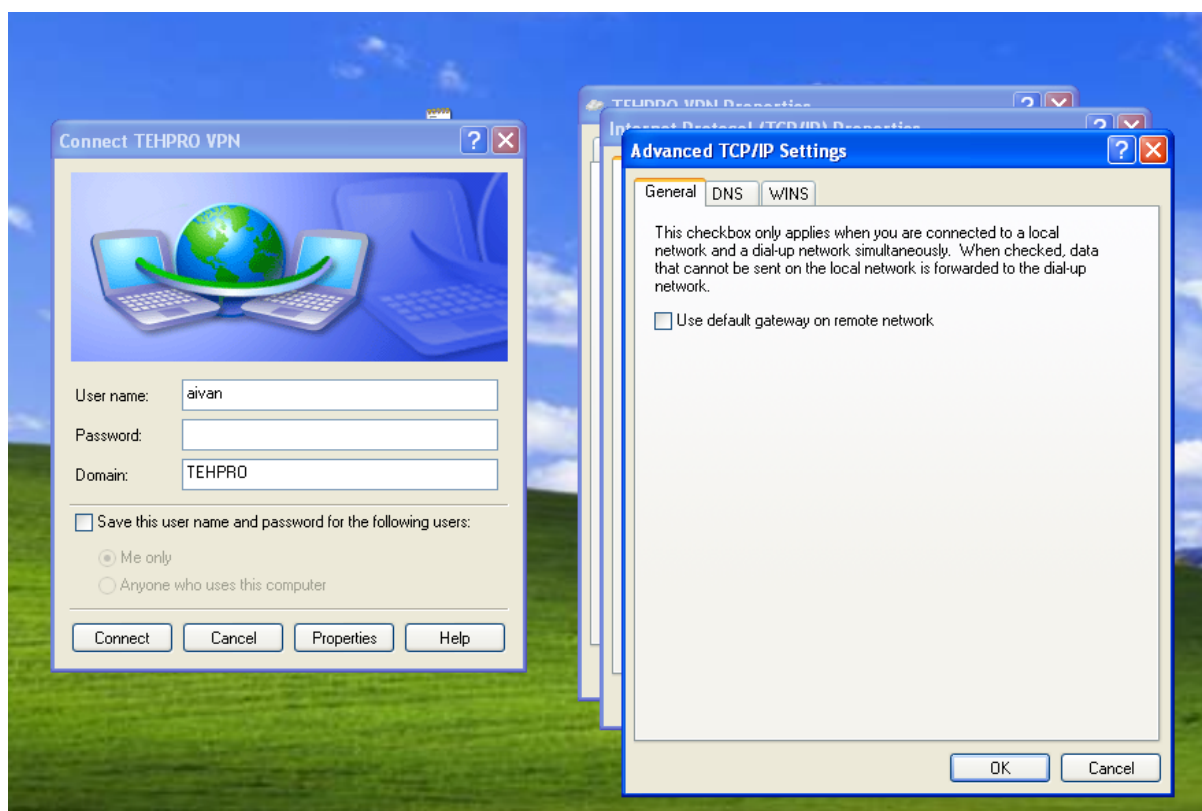
Na slikama koje slede videće se deo realizacije VPN-a u preduzeću Tehpro d.o.o. :



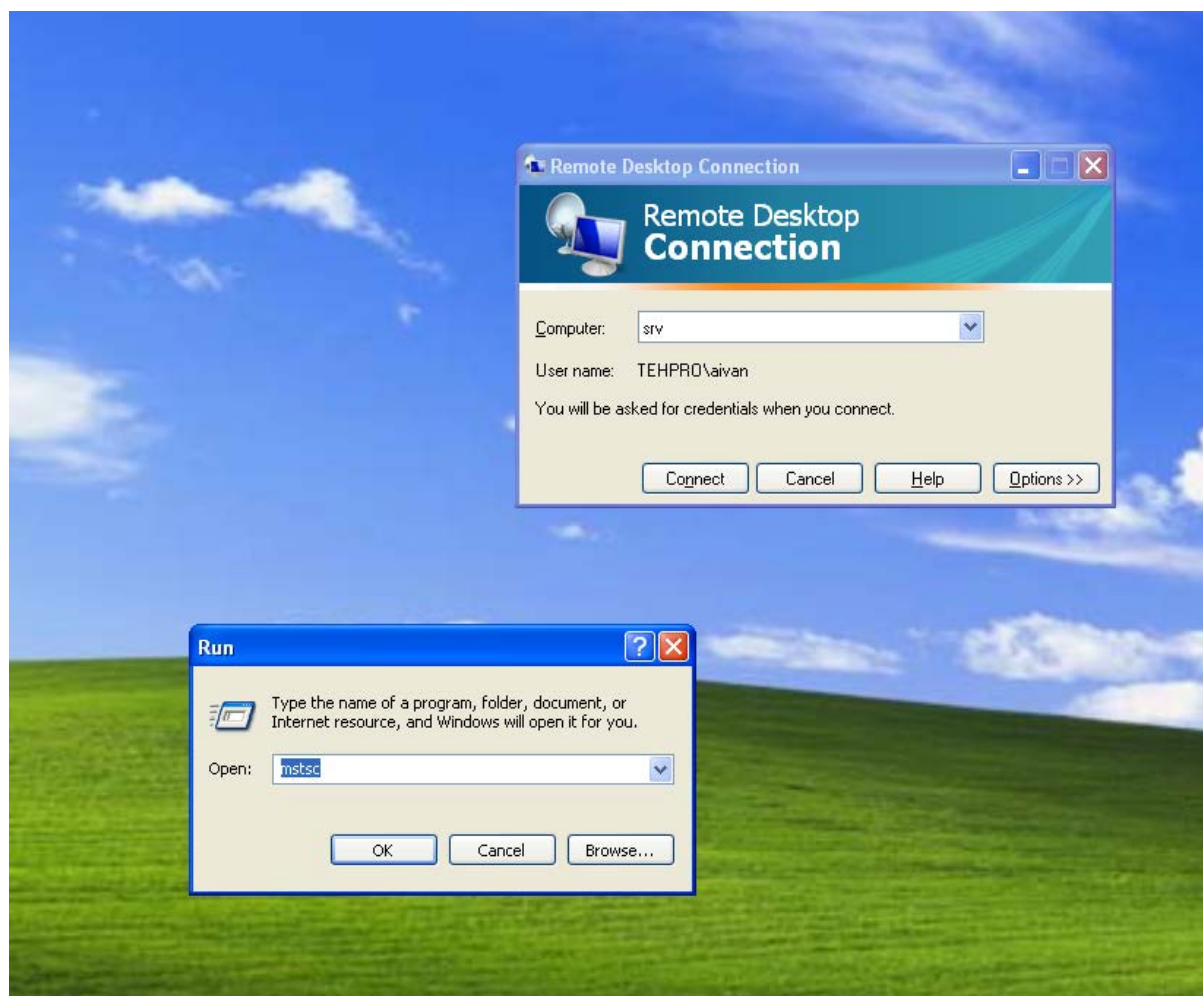
Slika 56. Pravljenje VPN konekcije na strani klijenta



Slika 57. Pravljenje VPN konekcije na strani klijenta na security tab-u

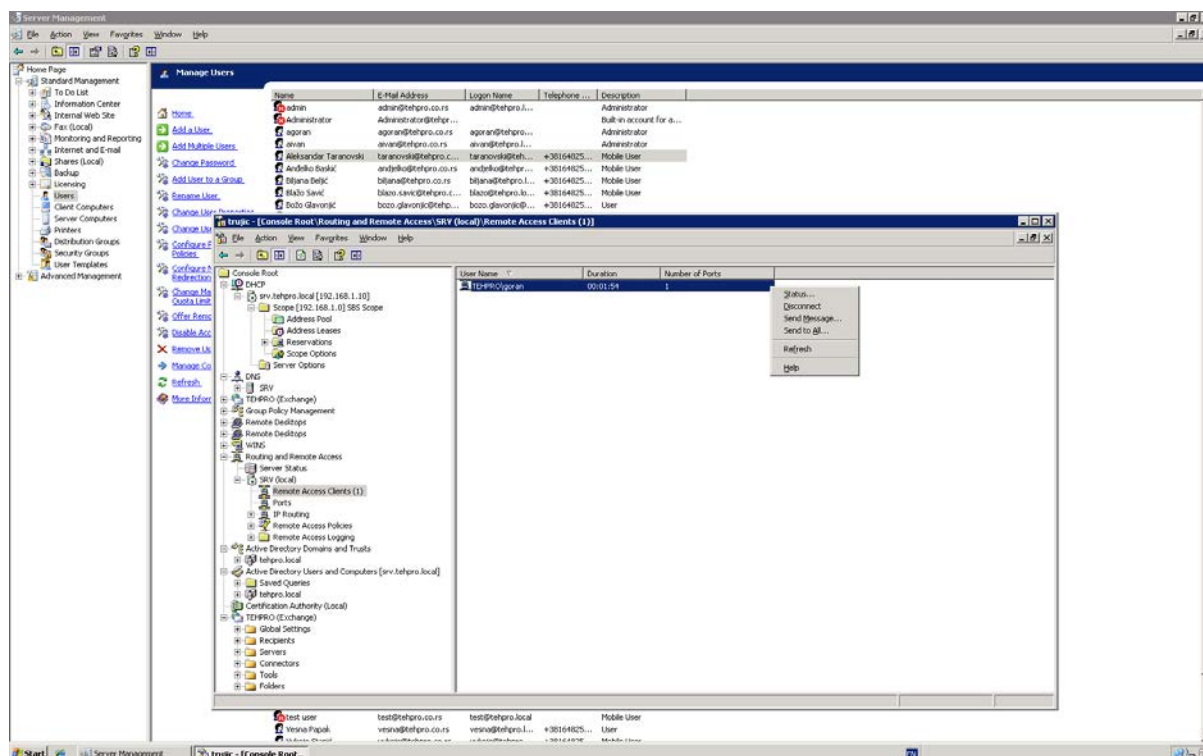


Slika 58. Advanced settings (tu se nalazi default gateway o kome prethodno je bilo reči)



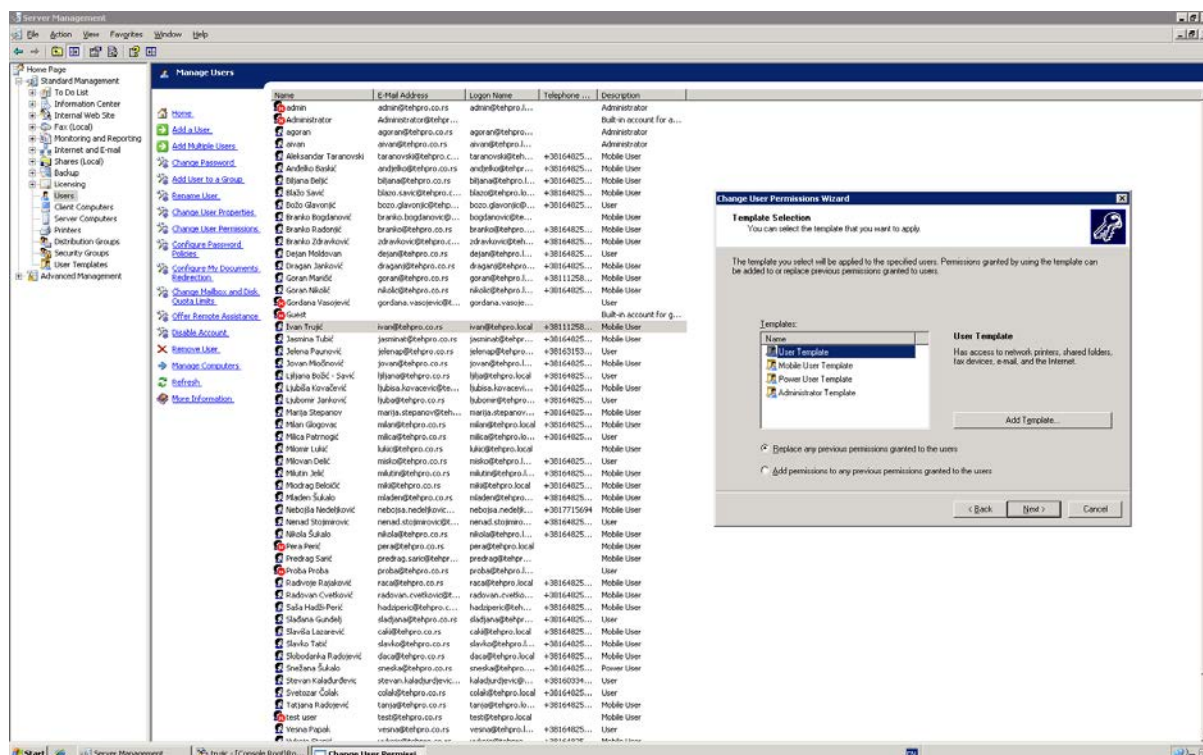
Slika 59. Konektovanje na server

Konektovanje na server vrši se preko Remote desktopa koji se pokreće komandom “mstsc”. To je osnovni alat administrator.

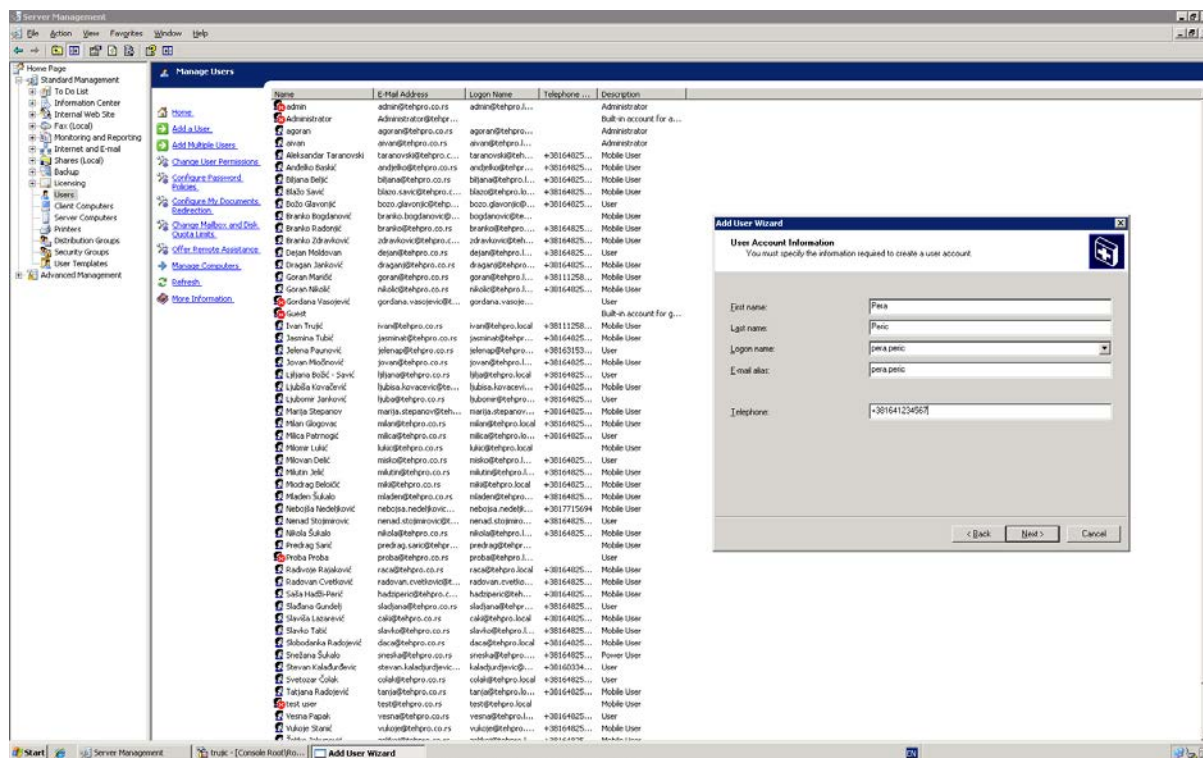


Slika 60. Prikaz klijenta

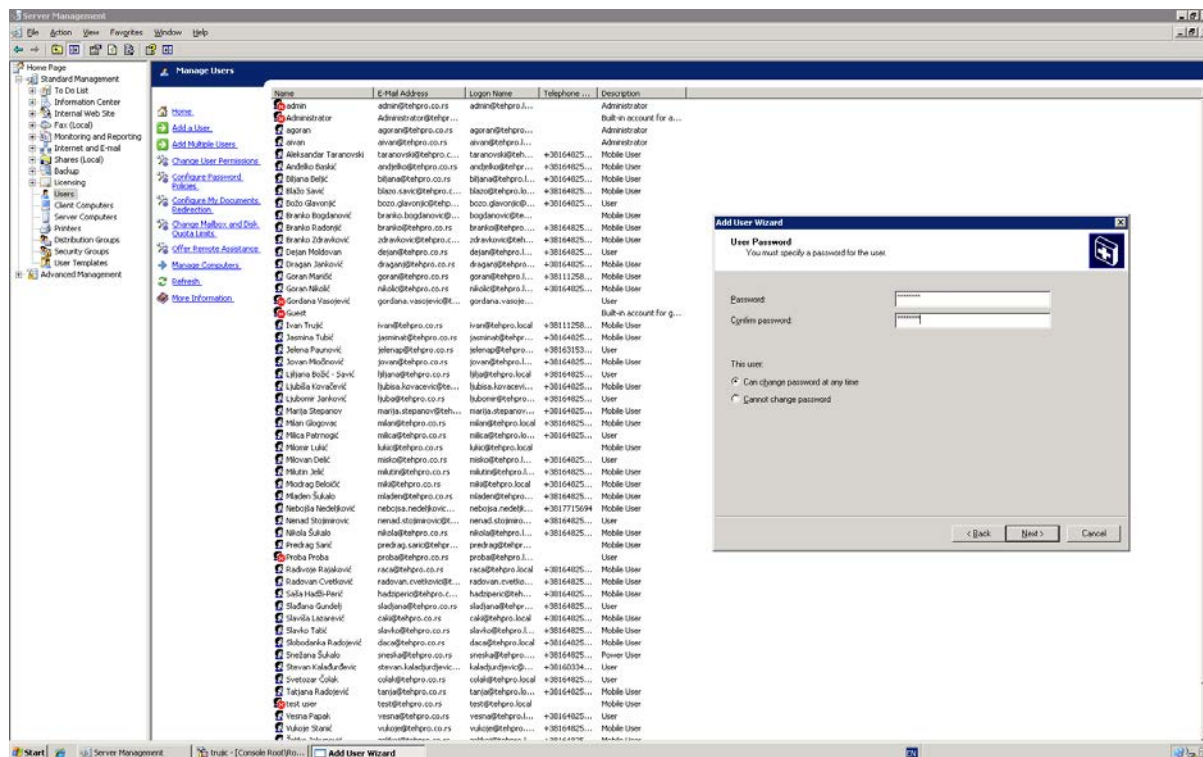
Desnim klikom na klijenta može se videti njegov trenutni status na mreži, koliko dugo je online, može se diskonektovati a može mu se i poslati privatna poruka.



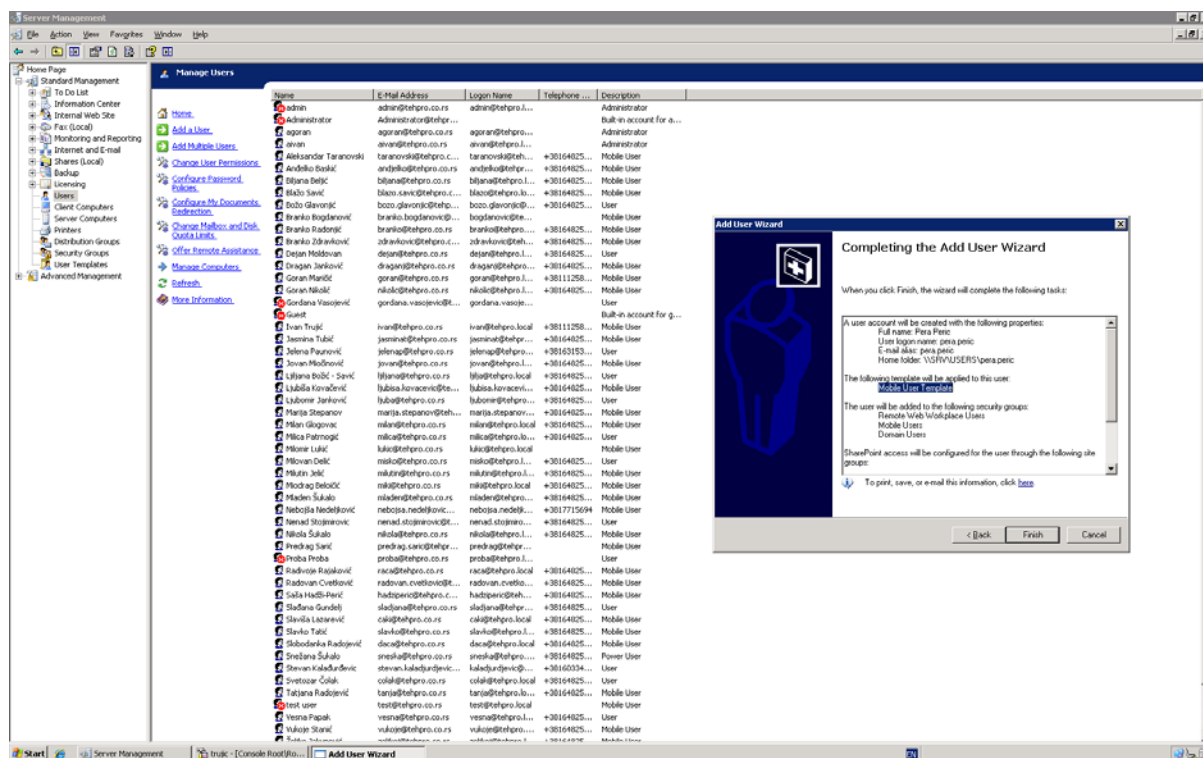
Slika 61 . Davanje dozvole klijentu da se konektuje na VPN server



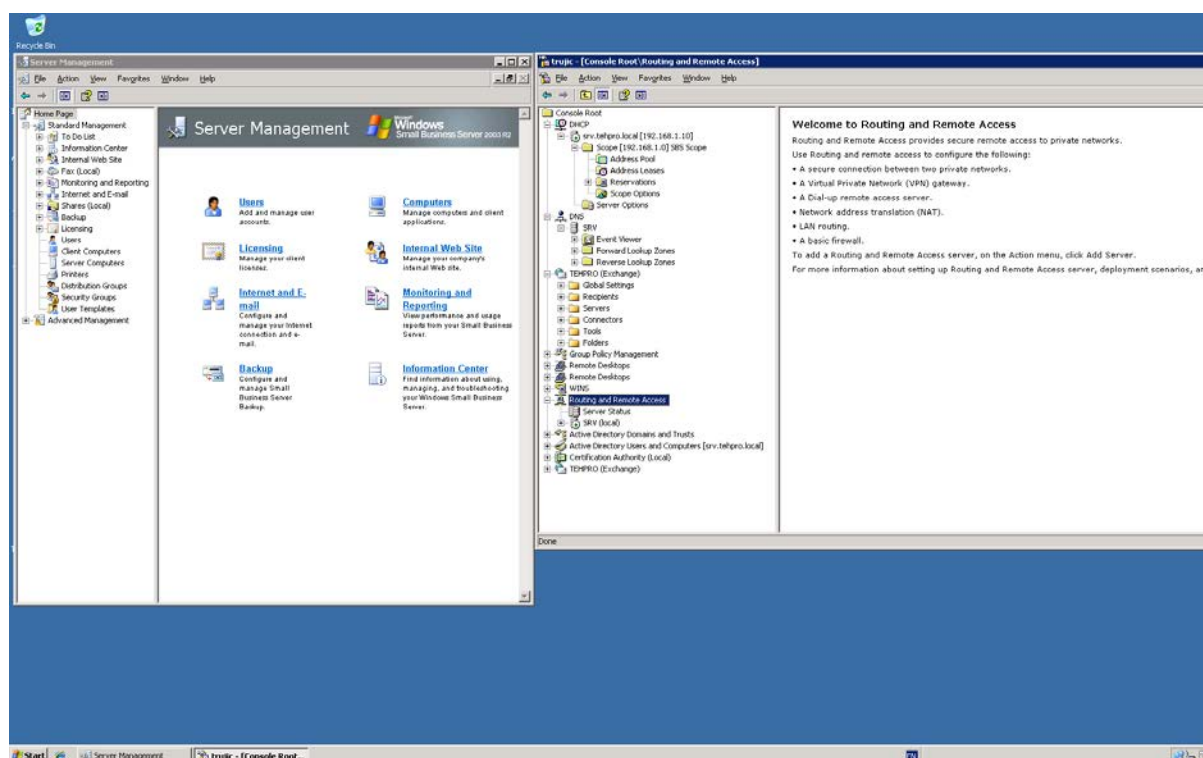
Slika 62. Kreiranje novog korisnika na server



Slika 63. Određivanje password-a korisniku



Slika 64. Završni prozor u Wizardu za kreiranje novog korisnika



Slika 65. Prikaz RAS konzole (Routing and Remote Access)

18. Zaključak

VPN je privukao pažnju mnogih organizacija koje žele povećati svoje sposobnosti umrežavanja i smanjiti njihove troškove. Uspeh VPN-a u budućnosti zavisi uglavnom od razvoja tehnologije.

VPN zahteva dobro razumevanje problema sigurnosti javih mreža i preduzimanje mera opreza kod postavljanja. Osim toga dostupnost i performanse VPN-a neke organizacije zavise od faktora koji su izvan njihove kontrole, a zbog nepostojanja standarda VPN tehnologije različitih proizvođača često su nekompatibilne.

Najveća vrednost VPN-a leži u potencijalnom smanjenju troškova firmi. Zato ako se VPN standardi usaglasa i različiti proizvodi postanu kompatibilni povećaće se potražnja. Uspeh VPN-a takođe zavisi i od mogućnosti intraneta i ektraneta da obave adekvatno svoje zadatke.

Rad sadrži kako teorijska objašnjenja tako i praktične prikaze VPN. Date su definicije, objašnjene su prednosti korišćenja VPN-a, data je njihova podela a obuhvaćena je i bezbednost. Pokazano je kako se vrši VPN konekcija i kako se postavlja VPN server. Postoje i dva su primera u radu gde se na slikama vidi kako se one realizuju u stvarnim uslovima.

19. Literatura

- [1] Implementation of Virtual private network based on IPSec, Jianwu Wu, 2009 ETP International Conference on Future Computer and Communication, 2009 IEEE.
- [2] Open VPN: building and operating virtual private networks, Markus Feilner, 2006.
- [3] Virtual Private Groups for Protecting Critical Infrastructure Networks, Richard C. O'Brien and Charles N. Payne, Jr. , 2009 IEEE.
- [4] VPN Applications Guide: Real Solutions for Enterprise Networks, Dave McDysan, 0- m 471-37175-0.
- [5] Ministarstvo za Informaciono društvo, Crna Gora, 2010.
- [6] MPLS and VPN Architectures, Volume II, Ivan Pepelnjak CCIE, Jim Guichard CCIE, Jeff Apcar, Cisco Press.
- [7] Business Data Communications & Networking, Dennis FitzGerald, Wiley Computer Publishing.
- [8] VPN Connections Options Expand, InfoWorld - Nov 5, 2001 - Page 33.
- [9] Virtual Private Groups for Protecting Critical Infrastructure Networks, Richard C. O'Brien and Charles N. Payne, Jr. , 2009 IEEE.
- [10] Open VPN: building and operating virtual private networks, Markus Feilner, 2006.
- [11] On the Design of Scalable, Self-Configuring Virtual Networks, David Isaac Wolinsky, Yonggang Liu, Pierre St. Juste, Girish Venkatasubramanian, Renato Figueiredo, 2009 IEEE