

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 1572

SIGURNOST U VIRTUALNIM PRIVATNIM MREŽAMA

Dario Hofman

Zagreb, prosinac 2005.

*Zahvaljujem se svom mentoru
Prof. dr. sc. Nikoli Bogunoviću
na stručnom vodstvu
i pomoći koju mi je pružio
pri izradi diplomskog rada*

*Zahvaljujem se i g. Željku Kučanu i g. Denisu Gluhaku
iz firme COMPUTECH na pomoći u otklanjanju problema*

*Najviše se zahvaljujem svojoj obitelji koja mi je oduvijek davala moralnu
podršku i pokazivala put kojim trebam kročiti,
te ovu radnju posebno posvećujem svojoj Omami.*

ORIGINAL DIPLOMSKOG ZADATKA

Sadržaj:

Sadržaj:	1
UVOD	3
I. Što je VPN?	3
II. Kom e je namijenjen?	4
1. OSNOVNI POJMOVI.....	5
1.1. Osnove	5
1.2. Zahtjevi.....	5
1.3. Vrste VPN rješenja	6
1.4. Tuneliranje	7
1.5. Mrežni slojevi	8
1.6. Osnove kriptografije.....	9
1.6.1. Ključevi	9
1.6.2. Najčešći algoritmi	9
1.6.3. Šifriranje i certifikati	10
2. VPN TEHNOLOGIJE.....	11
2.1. IPSec.....	11
2.2. PPTP	13
2.3. L2F.....	14
2.4. L2TP.....	14
2.5. Usporedba IPSe c, PPTP i L2TP protokola.....	16
2.6. Alternativni načini ostvarivanja VPN-a.....	17
3. ODABIR VPN SUSTAVA ZA RJEŠAVANJE PROBLEMA	18
3.1. Opis problema koji želim o rješiti	18
3.2. Odabir opreme za rješavanje problema.....	18
3.2.1. Odabir VPN servera	18
3.2.2. Odabir VPN klijenta.....	19
3.3. Opis sustava koji rješavamo	20
3.4. Odabrani protokoli za uspostavu VPN sustava	21
4. RJEŠAVANJE PROBLEMA	22
4.1. podešavanje usmjerivača	22
4.1.1. Kartica (meni) Home.....	22
4.1.2. Kartica (meni) Advanced.....	23

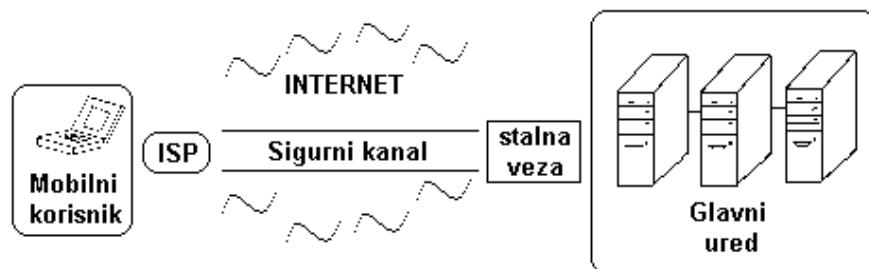
4.1.3. Kartica (meni) <i>Tools</i>	24
4.1.4. Kartica (meni) <i>Status</i>	25
4.2 Podešavanje VPN servera.....	25
4.2.1. Podešavanje PPTP protokola	25
4.2.2. Podešavanje L2TP protokola.....	26
4.2.3. Podešavanje IPSec protokola	27
4.2.4. Provjera statusa IPSec veze	31
4.3 Podešavanje klijenta i testiranje veze i raznih protokola.....	32
4.3.1. PPTP klijent	32
4.3.2. L2TP klijent	36
4.3.2.1. Razlike između PPTP i L2TP protokola	37
4.3.2.2. Testiranje veličine paketa zapakiranih PPTP i L2TP protokolom	38
4.3.3. IPSec klijent	38
4.3.3.1. Korištenje IP Security policy Management-a.....	39
4.3.3.2. Korištenje Smart VPN Client-a.....	40
4.3.3.3. Korištenje The GreenBow VPN Client-a.....	44
4.4 Testiranje veličine paketa zapakiranih PPTP, L2TP i IPSec protokolom	45
4.5 Najčešći problemi i korisne naredbe	45
4.6 Konačno razmatranje – PPTP protiv L2TP/IPSec	48
5. ZAKLJUČAK	49
Dodatak A: Popis IETF standarda i prijedloga	50
Dodatak B: Rječnik	51
LITERATURA	54
SAŽETAK	55

UVOD

I. Što je VPN?

VPN (*Virtual Private Network*) je kratica za virtualnu privatnu mrežu. To je tehnologija koja omogućava *sigurno* povezivanje računala ili privatnih mreža u zajedničku virtualnu privatnu mrežu i to kroz privatnu ili javnu mrežnu infrastrukturu (prvenstveno se to odnosi na Internet).

Za razliku od privatnih mreža koje koriste iznajmljene linije za komunikaciju, VPN može raditi i preko javne mreže prilikom čega se uspostavlja sigurnosni kanal između krajnjih točaka. To najčešće dovodi do određene, često velike, novčane uštede. VPN se često umjesto za tehnologiju koristi i kao skraćenica za privatnu mrežu uspostavljenu preko javne telekomunikacijske infrastrukture.



Slika I. Pojednostavljen primjer VPN-a

II. Kome je namijenjen?

Najveću korist od VPN-a imaju poduzeća koja imaju svoje podružnice raspoređene u više država [3]. Budući da je međusobna telefonska veza skupa, VPN se pojavljuje kao vrlo razumno rješenje. Veza prema ISP-u (davatelju Internet usluga) je ipak daleko jeftinija.

Osim njih koristi imaju i sva ostala poduzeća koja imaju geografski odvojene poslovnice, kao npr. INA, zastupnici određene auto marke i njihovi saloni, itd. Razlog tome je što je cijena običnog telefonskog poziva kod nas 4,5 puta skupljia od modemskega poziva (Dial-up) na Internet, a zakup linije na veće udaljenosti je ipak skuplij od zakupa stalne veze prema Internetu.

Treći najčešći slučaj je da se pojedinačni korisnici imaju potrebu spojiti na privatnu mrežu poduzeća u kojem rade. To mogu biti djelatnici poduzeća koji se moraju spojiti na privatnu mrežu poduzeća dok vrše mjerena na terenu, djelatnik poduzeća koji se želi od kuće spremiti za sutrašnji sastanak koji je nenadano iskrisnuo ili jednostavno trgovački putnik koji podnosi dnevni izvještaj o prodaji i naručuje robu za idući dan.

Osim podataka putem VPN-a je moguće vršiti i prijenos govora – VoIP (*Voice over IP*), što omogućuje značajnu uštedu, pogotovo ako poduzeće ima podružnice u više država. Ovisno o potrebi, ponekad je bolje koristiti neke druge, jednostavnije za implementirati, načine sigurnog komuniciranja umjesto VPN-a.

1. OSNOVNI POJMOVI

1.1. Osnove

Osnovna zamisao VPN tehnologije (u dalnjem tekstu umjesto VPN tehnologije koristiti će se samo naziv VPN) je osigurati sigurno povezivanje privatnih mreža preko javne mreže odnosno Interneta. To se najčešće izvodi tuneliranjem između dvije točke. Kod tuneliranja može se provoditi kompresija i/ili šifriranje podataka. Također VPN je moguće koristiti i unutar vlastite lokalne mreže, ali to se rjeđe koristi.

Implementacija može biti programska ili sklopovska, a često se koristi i kombinacija te dvije implementacije. U pravilu programska podrška je dovoljno brza za šifriranje/dešifriranje do 10Mbps podataka u realnom vremenu, a za veće brzine se koristi sklopovska podrška.

Korisnici žele sigurnu i stalnu povezanost unutar svoje mreže. VPN može osigurati sigurnost, ali stalnu vezu ne može garantirati. Propusnost veze je jednaka svojoj najslabijoj točki. Ako se korisnik spojio modemskom vezom, nitko ne može garantirati stabilnost veze. Ona može biti loša prema ISP-u ili jednostavno može doći do zagušenja prometa na Internetu ili "ispada" ISP-a iz Interneta. Tu su u prednosti (skuplje) iznajmljene linije koje u pravilu osiguravaju pouzdan medij za prijenos podataka.

1.2. Zahtjevi

VPN tehnologija mora osigurati određene zahtjeve. To su:

- *Upravljanje adresama* – VPN je zadužen za dodjeljivanje klijentskih adresa unutar privatnih mreža
- *Mehanizmi za upravljanje ključevima* – VPN mora osigurati generiranje i osvježavanje ključeva između klijenta i poslužitelja
- *Podršku za razne protokole* – VPN mora podržavati standardne protokole koji se koriste na javnim mrežama (IP, IPX, itd.)

Također tu su vrlo bitni i sigurnosni zahtjevi:

- *Pravo pristupa* – VPN osigurava provjeru identiteta korisnika i dozvoljava VPN pristup samo registriranim korisnicima. Također mora osigurati mogućnost praćenja događaja.
- *Autentifikaciju* – VPN mora osigurati da podaci koje dolaze zbilja dolaze s određista s kojeg tvrde da dolaze i da osoba koja tvrdi da je pošiljatelj podataka to i zbilja je. Za to se često koriste digitalni certifikati. (Često se izraz autentifikacija odnosi samo na provjeru imena korisnika i lozinke).
- *Cjelovitost (integritet) podataka* – VPN mora osigurati da nitko ne mijenja podatke dok putuju Internetom. Za to se najčešće koristi MD5 (algoritam za izračunavanje sažetka).

- *Povjerljivost (tajnost, šifriranje)* – VPN mora osigurati šifriranje podataka tako da ih ništa, osim klijenta odnosno poslužitelja, ne može pročitati. To se postiže raznim algoritmima poput DES, 3DES, RSA i Diffie-Hellman algoritma.

1.3. Vrste VPN rješenja

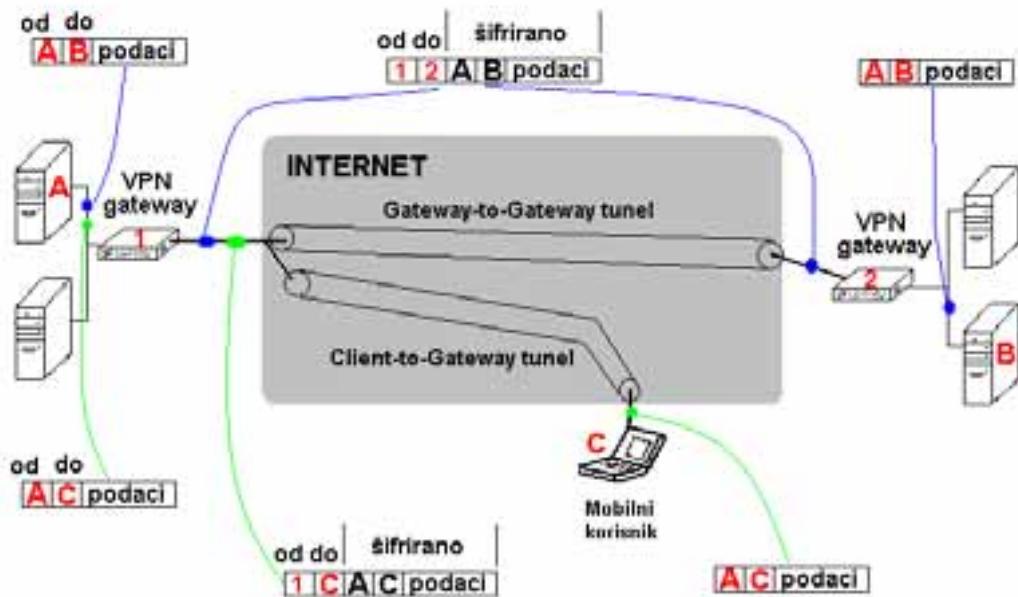
S obzirom na mogućnost primjene postoje slijedeća rješenja [1]:

- *Intranet VPN*
Koristi se za povezivanje više lokacija unutar jedne organizacije. Za prijenos podataka se koristi Internet ili WAN.
- *Extranet VPN*
Koristi se za povezivanje dva ili više dobavljača i/ili poslovnih partnera. Za prijenos podataka se koristi Internet ili WAN.
- *Udaljeni pristup*
Povezuje udaljene korisnike (ili manje urede) sa lokalnom mrežom poduzeća. Povezivanje se obavlja putem modemske veze preko Interneta (ponekad se to naziva VPDN = Virtual Private Dial Network).
Prednosti ovog načina spajanja naspram direktnog modemskog povezivanja s tvrtkom:
-niža cijena povezivanja putem Interneta
-nema potrebe kupiti i održavati modemske ulaze, te plaćati telefonsku pretplatu za njih
-korištenjem ADSL tehnologije kod nas nije moguće međusobno spojiti dva korisnika,
već se je moguće jedino spojiti na Internet

Podjela VPN rješenja u ovisnosti o konfiguracijama:

- “client-to-server” (ili “client-to-gateway”) rješenja
Koristi se kod modemskih (Dial-up) rješenja. Najčešći slučaj za to je kad se zaposlenik poduzeća želi spojiti na mrežnu infrastrukturu svog poduzeća preko ISP-a sa terena ili od kuće.
- “server-to-server” (ili “gateway-to-gateway”) rješenja
Koristi se kod spajanja dvije (ili više) odvojenih lokalnih mreža. Za to je najčešći primjer poduzeće koje se želi spojiti preko Interneta sa svojom podružnicom (podružnicama) koje su fizički udaljene.

Slika 1.1 prikazuje razliku između te dvije konfiguracije



Slika 1.1 Prijenos podataka tuneliranjem

1.4. Tuneliranje

Tuneliranje predstavlja tehniku prijenosa podataka namijenjenu jednoj mreži preko neke druge mreže. Podaci koji se šalju mogu biti okviri (ili paketi) od nekog drugog protokola. Protokol, kojim se implementira tuneliranje, enkapsulira originalnom okviru posebno oblikovano zaglavje. Takvo zaglavje sadrži dodatne podatke (za usmjeravanje) kako bi enkapsulirani paket stigao, kroz mrežu koja služi za prijenos, do odredišta. Enkapsulirani podaci se onda šalju između krajnjih točaka tunela. Tunel je logički put kroz koji enkapsulirani podaci prolaze kroz mrežu koja služi kao medij za prijenos. Kada takav okvir dođe do svog odredišta podaci se ekstrahiraju i zatim se šalju na ciljno odredište. Tuneliranje uključuje čitav navedeni proces (enkapsulacija, prijenos i ekstrakcija).

VPN se može podijeliti i u ovisnosti o tipu tuneliranja koji koriste:

- *Stalni* – nisu isplativi radi toga što traže određenu protočnost podataka (bandwidth) čak i kada se prijenos podataka ne koristi, a ISP-ovi često naplaćuju prosječno zahtjevanu protočnost, pri čemu prednost imaju privremeni VPN-ovi
- *Privremeni* – uspostavljaju se kada klijent zatraži spajanje u VPN i nestaju kada se veza završi

Ako se VPN uspostavlja preko ISP-a moguća su dva rješenja [4]:

- *Dobrovoljno tuneliranje* (Voluntary Tunneling)

To je slučaj kada računalno ili usmjerivač koristi klijentsku programsku podršku za tuneliranje za uspostavljanje VPN-a. Najčešći primjer za to je kada modemski Internet korisnik prvo uspostavi vezu sa svojim ISP-om da bi mogao uspostaviti tuneliranje kroz Internet.

- *Obvezno tuneliranje* (Compulsory Tunneling)

Veliki broj poslužitelja s modemskim ulazima koje koriste ISP-ovi imaju implementiranu mogućnost automatskog kreiranja tunela za modemskog korisnika. Taj poslužitelj (ili mrežni uređaj) koji pruža tuneliranje klijentskom računalu se naziva Front End Processor (FEP) kod PPTP-a, L2TC Access Concentrator (LAC) kod L2TP-a ili IP Security Gateway kod IPSec-a.

Danas postoje razne tehnologije koje omogućuju tuneliranje. Najpoznatije od njih su:

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

1.5. Mrežni slojevi

Da bi bolje razumjeли neke razlike između različitih implementacija VPN-a trebamo se upoznati sa mrežnim slojevima. OSI RM-om (Open System Interconnection (Basic) Reference Model) je komunikacijski model za računalne mreže standardiziran 1983 godine od strane ISO-a. Model se sastoji od 7 slojeva:

1. *Fizički sloj* (najniži sloj) – osigurava ispravan prijenos bitova (0 i 1)
2. *Podatkovni sloj* – obavlja pretvorbu podataka iz fizičkog sloja u okvire podataka koje upotrebljava mrežni sloj
– tu se vrši retransmisija lošeg ili izgubljenog okvira i obrada dvostrukog primljenog okvira
3. *Mrežni sloj* – obavlja usmjeravanje paketa od izvora do odredišta, sprječava zakrčivanje, povezuje heterogene mreže
4. *Prijenosni (transportni) sloj* – obavlja uslugu prijenosa od kraja do kraja koja treba biti pouzdana, efikasna i neovisna o korištenoj fizičkoj mreži
5. *Sjednički sloj* – obavlja uspostavljanje sjednica (spojeva između aplikacijskih procesa)
6. *Predodžbeni sloj* – brine se za usklajivanje prikaza i predstavljanje informacija (konverzija, šifriranje/dešifriranje i kompresija podataka)
7. *Aplikacijski sloj* – obavlja modeliranje putem elemenata usluge

Prva 4 sloja osiguravaju pouzdan prijenos podataka, a preostala 3 su zaduženi za povezivanje i skladnu suradnju sa aplikacijskim procesom (procesima).

IPS (Internet Protocol Suite) je popularniji komunikacijski model od OSI RM-a. On se sastoji od 4 sloja. IPS sloj 1 obuhvaća OSI slojeve 1 i 2, a IPS sloj 4 obuhvaća OSI slojeve 5, 6 i 7. Slojevi 2 i 3 su isti OSI RM slojevima 3 i 4.

Od prve četiri tehnologije koje su bile namijenjene kao VPN rješenja tri rade na 2. mrežnom sloju (PPTP, L2F i L2TP), dok jedna (IPSec) radi na 3. mrežnom sloju.

1.6. Osnove kriptografije

1.6.1. Ključevi

Simetrični (tajni) ključevi (Symmetric, Secret ili Private key)

Prednosti:

- Vrlo brzi
- Mogu biti lagano implementirani u sklopovlje

Nedostaci:

- Koriste se dva ista ključa
- Nije ih jednostavno za distribuirati

Asimetrični (javni) ključevi (Asymmetric ili Public key)

Prednosti:

- Koriste se dva različita ključa
- Vrlo se jednostavno distribuira
- Koriste se digitalni potpisi da bi se osigurao integritet

Nedostaci:

- Spori su

1.6.2. Najčešći algoritmi

DES (Data Encryption Standard)

- koristi 56 bitni ključ nad 64 bitnim blokovima podataka
- algoritam je zaštićen američkim patentom
- bilo je slučajeva probijanja u roku samo nekoliko dana
- simetričan algoritam
- relativno brz algoritam

3DES

- blok podataka se šifrira 3 puta, svaki puta sa različitim ključem
- simetričan algoritam

RSA (Rivest, Shamir i Adalman)

- najčešći ključ je 512 bitni (danasa ga je već moguće razbiti, ali 1024 bitni još ne)
- asimetričan algoritam
- spori algoritam
- ključ može biti varijabilne duljine

IDEA

- koristi se 128 bitni ključ na 64 bitnim blokovima podataka
- algoritam, programski izведен, je dvostruko brž od DES šifriranja
- simetričan algoritam
- nudi dobru sigurnost šifriranja

RC2 i RC4

- razvio Ron Rivest iz RSA Data Security Inc.
- brži od DES algoritma
- ključ je varijabilne duljine

Skipjack

- preporučila ga je Američka vlada
- implementiran je u Clipper čipu
- 80 bitni ključ

Diffie-Hellman

- najstariji asimetrični algoritam ali je još uvijek u upotrebi
- služi za dogovor oko zajedničkog tajnog ključa putem javne infrastrukture
- opasnost je da se pojavi "napadač u sredini" (preseće međusobne poruke i lažira ih)

MD5

- to je funkcija koja od teksta proizvoljne duljine proizvodi 128 bitni sažetak (hash)
- općenito, vjerojatnost da dva različita teksta imaju isti sažetak je vrlo mala

SHA

- kao i MD5 samo što proizvodi 160 bitni sažetak

Usporedba sigurnosti ključeva ovisno o algoritmu:

<i>Simetrični</i>	<i>Asimetrični</i>
56 bitni	384 bitni
64 bitni	512 bitni
80 bitni	768 bitni
112 bitni	1792 bitni
128 bitni	2304 bitni

1.6.3. Šifriranje i certifikati

Kod simetričnog šifriranja, i pošiljatelj i primatelj imaju ključ koji trebaju provjeriti. Razmjena tog ključa se mora napraviti sa određenom zaštitom. Kod asimetričnog šifriranja pošiljatelj koristi privatni ključ za šifriranje poruke, a primatelj koristi javni ključ za dešifriranje poruke. Javni ključ može biti dostupan bilo kom, dok se zaštiti mora samo privatni ključ. Da bi se osigurao integritet javnog ključa, javni ključ se mora objaviti sa certifikatom. Certifikat (ili public key certificate) je podatkovna struktura digitalno potpisana od strane CA-a (Certificate Authority) – ustanove kojoj korisnici certifikata vjeruju. Certifikat se sastoji od različitih podataka: naziva certifikata i vlasnika javnog ključa, javnog ključa, datuma do kada vrijedi i naziva ustanove koja ga je izdala. CA koristi svoj privatni ključ da potpiše certifikat. Ako primatelj zna javni ključ od CA-a, on može provjeriti da li je zbilja certifikat izdan od valjanog CA-a i da su informacije u njemu pravovaljane. Certifikat se može primiti putem e-mail-a, web-a, a može se nalaziti i na pametnim karticama (smart card) [4].

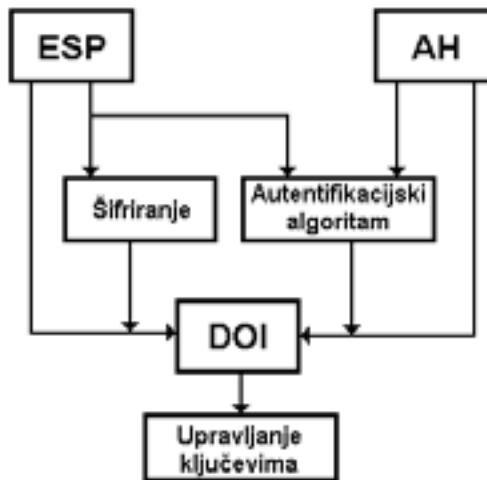
2. VPN TEHNOLOGIJE

2.1. IPSec

IPSec je standard definiran od strane IETF-a. To je protokol koji radi na trećem mrežnom sloju. Pri razvoju iduće generacije IP protokola (IPv6) vodilo se dosta brige i o sigurnosti. Tako je u IPv6 implementiran IPSec. Kako do zamjene današnjeg IP protokola koji se masovno koristi (IPv4) neće tako skoro doći, IPSec je modificiran kako bi bio kompatibilan sa IPv4.

IPSec prilikom rada koristi slijedeće protokole i standarde kako bi osigurao povjerljivost, integritet i autentifikaciju:

- Diffie-Hellman-ovu metodu za razmjenu tajnog ključa putem javne mreže
- kriptografiju temeljenu na javnim ključevima za digitalno potpisivanje komunikacije prilikom Diffie-Hellman-ove razmjene ključeva - da bi se osigurao identitet obju strana u komunikaciji i izbjegla mogućnost napada "napadača u sredini" (Man-in-the-middle)
- DES, 3DES ili neki drugi poznati algoritam za šifriranje
- algoritme za izračunavanje sažetka (HMAC, MD5 i SHA) kako bi se osigurala autentičnost paketa
- digitalne certifikate za provjeru pravovaljanosti javnih ključeva



Slika 2.1 Dijagram strukture IPSec komponenata

Dijagram strukture IPSec protokola prikazan je na slici 2.1. IPSec struktura se sastoji od tri glavne komponente. To su AH (Authentication Header) i ESP (Encapsulated) protokoli i upravljanje ključevima. Autentifikacijska zaglavila (AH) se koriste za autentifikaciju i integritet, bez mogućnosti šifriranja (znači netko treći može pročitati, ali ne može mijenjati poslane podatke). ESP osigurava iste mogućnosti, ali

dodaje i mehanizam za šifriranje. Sigurni ključ poznaju samo pošiljatelj i primatelj tako da ako su autentifikacijski podaci valjni primatelj može biti siguran da je podatak stigao od pošiljatelja te da nije promijenjen tijekom prijenosa. U IPSec-u se mogu koristiti razni algoritmi šifriranja, ključevi različite duljine i sl., pa je potrebno da se i pošiljatelj i primatelj dogovore o standardima koje će koristiti. Za to je zadužen DOI (Domain of Interpretation).

IPSec podržava dva načina rada [1]:

- *Prijenosni način rada* (Transport mode)

Kod prijenosnog načina rad šifrira se samo podatkovni dio IP paketa, dok zaglavla ostaju u originalnom obliku. To znači da potencijalni napadač može vidjeti adrese od računala s kojeg paketi dolazi i na koji odlaze. Prednost ovog načina rada je to što se svakom paketu dodaje samo nekoliko okteta. Ovaj način rada namijenjen je kada se komunicira direktno između dva računala (sa vlastitom IP adresom), što znači da na taj način ne mogu komunicirati računala koja su spojena na Internet preko usmjerivača ili sličnog uređaja.

Adresa pošiljaoca	Adresa primaoca	Šifirani podaci
--------------------------	------------------------	------------------------

- *Tuneliranje* (Tunnel mode)

IPSec tuneliranje se sastoji od klijenta i poslužioca koji su oboje konfigurirani da koriste IPSec tuneliranje i imaju dogovorene mehanizme za šifriranje. Prilikom IPSec tuneliranja cijeli IP paket se šifrira (adresa pošiljaoca, adresa primaoca i podaci), i na takav paket se nadodaje nešifrirano zaglavje sa adresom IPSec poslužioca i IPSec klijenta. IPSec adrese poslužioca i klijenta su ustvari adrese početka i kraja tunela. Za razliku od prijenosnog načina rada, kod tuneliranja potencijalni napadač može otkriti sa koje se adrese šalju podaci i na koju adresu trebaju stići. Ovaj način rada, radi dodatnih zaglavila, traži nešto veću propusnost mreže preko koje se podaci prenose.

Adresa početka tunela	Adresa kraja tunela	Šifrirana adresa pošiljaoca	Šifrirana adresa primaoca	Šifirani podaci
------------------------------	----------------------------	------------------------------------	----------------------------------	------------------------

Više od godinu dana je trajalo odlučivanje koju metodu da se koristi za automatsko upravljanje ključevima. Na kraju je odabrana ISAKMP/Oakley metoda, na koju se danas misli kad se govori o IKE-u (Internet Key Exchange). Upravljanje ključevima se može vršiti na dva načina: ručno ili IKE (za automatsko upravljanje). Ručno upravljanje je praktično za manje tvrtke, dok se KE predlaže kod povezivanja većeg broja mreža ili kada ima više modemskih korisnika [2].

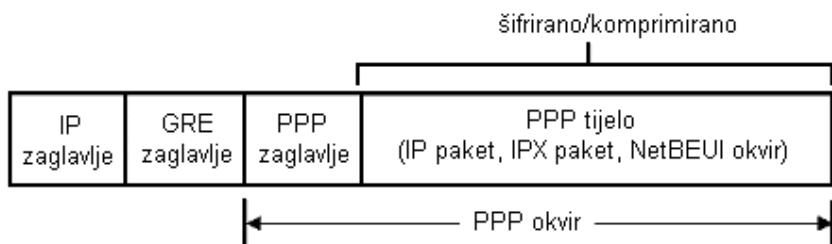
2.2. PPTP

PPTP protokol je razvilo udruženje nekoliko proizvođača: Microsoft, US Robotics (danasm 3Com), Ascend Communications, 3Com, ECI Telematics. On, kao i L2F i L2TP, radi na drugom mrežnom sloju.

PPTP se temelji na PPP-u (point-to-point protocol) koji omogućava autentifikaciju, šifriranje i kompresiju podataka. Dakle PPTP koristi mehanizme za autentifikaciju koji se koriste u PPP-u, a to su PAP (password authentication protocol) i CHAP. Kako su PPTP i Windows NT usko povezani, Microsoft je razvio poboljšanu verziju CHAP-a nazvanu MS-CHAP, koja za autentifikaciju koristi podatke o korisnicima pohranjene u bazi korisnika Windows-a NT. Budući da su u MS-CHAP-u pronađeni sigurnosni nedostaci, izdan je MS-CHAPv2.

U početku je PPTP bio zamislen kao mehanizam koji omogućava i prijenos protokola koji nisu temeljeni na IP-u, poput IPX-a, NetBEUI-a i AppleTalk-a putem Interneta. To se obavlja s modificiranim verzijom GRE protokola. PPTP koristi TCP spoj za održavanje tunela i modificiranu verziju GRE-a za enkapsuliranje PPP okvira za tuneliranje podataka.

Podatkovni dio enkapsuliranih PPP okvira može biti šifriran i/ili komprimiran. Slika 2.2 prikazuje strukturu PPTP paketa [4].



Slika 2.2 Struktura PPTP paketa

Nakon što paket dođe do svog odredišta, vanjska zaglavlja se uklanaju omogućavajući tako originalnim paketima (tj. PPP tijelu) dolazak do krajnjeg odredišta. Enkapsulacija omogućava prijenos paketa koji inače ne bi zadovojili standarde adresiranja na Internetu.

Microsoft RAS (Remote Access Server) je dizajniran da upravlja s podacima o korisnicima smještenim u bazi korisnika. Budući da već postoji baza korisnika, jednostavno je pridjeliti modemska (dial-up) prava korisnicima koji se već ionako nalaze u bazi. U početku je RAS služio kao poslužitelj koji određuje prava modemskim korisnicima. Danas RAS podržava i tuneliranje za PPTP i L2TP veze.

Microsoft je u svoju verziju PPTP protokola implementirao vlastiti način šifriranja i kompresije. On se naziva MPPE (Microsoft Point-to-Point Encryption) i on je optionalan. Bazira se na RSA/RC4 algoritmima.

PPTP koristi 40, 56 ili 128 bitnu enkripciju, ali je čitav proces oslabljen upotrebom korisničkih zaporki za generiranje sjedničkih ključeva. Dugi ključevi generirani na potpuno slučajan način predstavljaju jedinu zaštitu od takvih napada.

Sigurnosni problemi

PPTP je često proglašavan nesigurnim iz slijedećih razloga:

- ključevi se ne generiraju na slučajan način
- sjednički ključevi nisu adekvatni
- duljine ključeva su prekratke i nije ih moguće konfigurirati
- nesiguran je i prijenos sažetka (hash vrijednosti) korisničkih zaporki
- problemi u sigurnosti sa statičkim zaporkama u MS Windowsima
- autentifikacija nije implementirana

2.3. L2F

L2F, kao i PPTP, se pojavio u samim početcima razvoja VPN-a. On je također bio namijenjen za tuneliranje između modemskih korisnika i njihovih tvrtka. Tu tehnologiju je predložio CISCO.

Za razliku od PPTP-a koji putuje samo preko IP-a, L2F je neovisan o prijenosnom protokolu, što mu daje mogućnost da podaci putuju preko npr. Frame Relay-a ili ATM-a (Asynchronous Transfer Mode). Osnovna funkcija L2F protokola je ostvarivanje tunela za okvire prijenosnog sloja (HDLC, PPP ili SLP) ili protokole viših slojeva. Enkapsulirani paketi se prenose preko WAN spojeva do L2F poslužitelja (usmjerivača) koji zatim ekstrahiraju podatke i proslijeđuju ih u mrežu.

Koriste se dva nivoa za autentifikaciju korisnika. Prvo se korisnik prijavljuje kod ISP-a, koji onda uspostavlja tunel do poduzeća, a zatim se korisnik prijavljuje na poslužitelj od poduzeća. Kao i PPTP, L2F koristi PPP za autentifikaciju korisnika i pruža mogućnost korištenja TACACS (terminal access controller access control system) ili RADIUS-a za autentifikaciju.

L2F ne definira klijente i djeluje samo u obveznom definiranim tunelima. L2F je unapred īvan zajedno sa PPTP-om, da bi ga konačno nadgradio L2TP.

2.4. L2TP

Kao što sam naziv kaže L2TP radi na drugom mrežnom sloju. Razvili su ga Microsoft i CISCO kao kombinaciju najboljih značajki njihovih PPTP i L2F protokola.

L2TP je mrežni protokol koji enkapsulira PPP okvire za slanje preko IP-a, X.25, Frame Relay-a ili ATM mreža.

Kada protokol koristi IP za slanje paketa, L2TP se može koristiti za tuneliranje kroz Internet. L2TP se također može koristiti direktno preko različitih WAN medija (poput Frame Relay-a) bez transportnog sloja.

L2TP koristi UDP i nizove L2TP poruka za održavanje tunela preko IP mreža. Također moguće je stvaranje više tunela između istih krajinjih točaka. Podaci iz enkapsuliranih PPP okvira mogu biti šifrirani i/ili komprimirani. Kako izgledaju podaci koji putuju tunelom od modemskog (PPP) korisnika može se vidjeti u donjoj tablici. Sličan izgled imaju i podaci kod PPTP tuneliranja.

PPP	IP	UDP	PPP	IP	TCP/UDP	Podaci
ovisno o odabiru – šifrirano i/ili komprimirano						

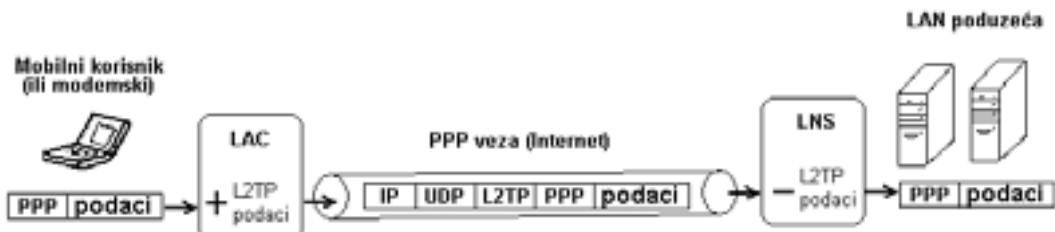
Princip rada obveznog tuneliranja opisan je slijedećim koracima:

1. Modemski (udaljeni) korisnik inicira PPP spoj prema svom ISP-u
2. ISP prihvata spoj i PPP sjednica je uspostavljena
3. ISP zahtjeva korisničko ime
4. U ISP-ovoj bazi korisničko ime je povezano sa servisima i LNS (L2TP Network Server) krajnjim točkama
5. LAC (L2TP Access Concentrator) inicira L2TP tunel prema LNS-u
6. Ako LNS prihvati spoj, LAC enkapsulira PPP u L2TP i proslijeđuje podatke preko odgovarajućeg tunela
7. LNS prihvata okvire, odvaja iz njih L2TP zaglavlja i obrađuje ih kao normalne PPP okvire
8. LNS zatim koristi standardnu PPP autentifikaciju da bi utvrdio identitet korisnika i dodijelio mu IP adresu

Ako se koristi dobrovoljno tuneliranje princip je slijedeći:

1. Modemski korisnik uspostavi vezu sa svojim ISP-om
2. L2TP klijent (LAC) inicira L2TP tunel prema LNS-u
3. Ako LNS prihvati spoj, LAC enkapsulira PPP u L2TP i proslijeđuje podatke kroz tunel
4. LNS prihvata okvire, odvaja iz njih L2TP zaglavlja i obrađuje ih kao normalne dolazne zahtjeve
5. LNS zatim koristi standardnu PPP autentifikaciju da bi utvrdio identitet korisnika i dodijelio mu IP adresu

Slika 2.3 prikazuje princip rada kod L2TP tuneliranja.



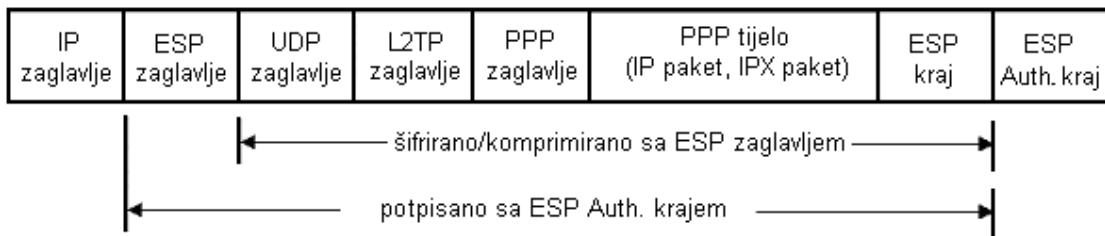
Slika 2.3 Prikaz tuneliranja kod L2TP veze

L2TP koristi dvije vrste poruka:

- *kontrolne poruke* – koriste se prilikom uspostave, održavanja i zatvaranja tunela
- *podatkovne poruke* – koriste se za enkapsulaciju PPP okvira koji se prenose kroz tunel

Kontrolne poruke definiraju pouzdani kontrolni kanal unutar L2TP-a koji garantira dostavu. U slučaju gubljenja podatkovnih poruka, one se zahvaljujući kontrolnim porukama ponovo šalju. PPP okviri se, prije slanja preko nepouzdanog podatkovnog kanala, enkapsuliraju sa L2TP zaglavljima, a zatim i sa prijenosnim zaglavljima poput UDP-a, Frame Relay-a, ATM-a itd. Kontrolne poruke, koje sadrže sljedne brojeve, se šalju preko pouzdanog L2TP kontrolnog kanala. Podatkovne poruke mogu imati sljedne brojeve za utvrđivanje ispravnog redoslijeda i detekciju paketa koji nedostaju.

L2TP koristi NCP (Network Control Protocol) za dodjelu IP adresa i autentifikaciju korisnika (PAP, CHAP) i kontrolu pristupa mrežnim resursima. L2TP za šifriranje, provjeru integriteta i autentifikaciju koristi IPSec protokol. Kada L2TP radi preko IP-a, IPSec sigurnost osigurava korištenjem ESP-a ili AH-a. Izgled L2TP paketa u suradnji sa IPSecom prikazan je na slici 2.4.



Slika 2.4 Izgled L2TP/IPSec paketa

2.5. Usporedba IPSec, PPTP i L2TP protokola

Bilo što se nastoji postaviti L2TP kao standard za sigurno komuniciranje, PPTP ostaje vrlo raširen. Razlog tome je što je podrška za njega implementirana u većinu Windows OS-ova (operacijskih sustava), a za one za koje nije postoje besplatni programski dodaci. Microsoft je L2TP počeo implementirati tek u Windows-e 2000.

L2TP prenosi podatke preko UDP-a za razliku od PPTP-a koji ih prenosi preko TCP-a. UDP je brži, ali manje siguran protokol. P2TP može za razliku od L2TP-a imati problema sa zaštitnim stijenama (firewall-ovima) zbog toga što oni, u pravilu, ne prepoznaju GRE zaglavje.

IPSec se često smatra najboljim VPN rješenjem za IP okruženja budući da sadrži najjače sigurnosne mjere – šifriranje, autentifikaciju, integritet i upravljanje ključevima. Budući da IPSec može baratati samo sa IP paketima, PPTP i L2TP su praktičniji za korištenje u okruženjima u kojima se koriste drugi protokoli poput IPX-a, NetBEUI-a i AppleTalk-a.

Trenutačni L2TP standard predlaže da se s njim koristi IPSec, koji je onda zadužen za šifriranje i upravljanje ključevima u IP okolini. Ako L2TP otkrije da ne može uspostaviti komunikaciju putem IPSec-a, on onda uspostavlja komunikaciju putem manje sigurnog PPP-a. Možda i budući PPTP standardi budu propisivali isto korištenje IPSec-a.

IPSec, u standardnom obliku, koristi samo autentifikaciju računala, bez autentifikacije korisnika. To je razlog zbog kojeg se za modemske korisnike predlaže korištenje PPTP-a ili L2TP-a, pak većina proizvođača u svoja IPSec rješenja ugrađuju i podršku za autentifikaciju korisnika.

2.6. Alternativni načini ostvarivanja VPN-a

Uz opisane načine ostvarivanja VPN-a, postoje i druge zanimljive varijante. Jedna od njih je SOCKS, koja radi na TCP sloju. Prava SOCKS klijenta se provjeravaju u sigurnosnoj bazi i ako autentifikacija prođe poslužitelj se ponaša kao proxy poslužitelj. Prednost je što mrežni administrator može lagano ograničiti koje se aplikacije mogu koristiti preko VPN-a. Nedostatak je što se SOCKS mora kompajlirati u jezgru sistema i u aplikacije. Zato se najčešće koristi na Linux/Unix sistemima.

SSL (Secure Sockets Layer) radi samo sa TCP baziranim aplikacijama [3]. Prvostenstveno je namijenjen za sigurnu vezu između web preglednika i web poslužitelja (npr. koristi se u Internet bankarstvu). Koristi se RSA javnim ključem za šifriranje podataka. SSL zahtjeva da stranica kojoj se pristupa ima važeći certifikat izdan od strane CA-a (Certificate Authority). Razvio ga je Netscape, a adrese poslužitelja koje koriste SSL za prijenos podataka počinju sa "https://" za razliku od nesigurnih adresa koje počinju sa "http://". IETF je na temelju SSL-a, propisao standard nazvan TLS (Transport Layer Security) koji ima istu svrhu kao i SSL. On radi na 4-tom mrežnom sloju, te u zadnje vrijeme predstavlja sve veću konkurenčiju IPSec-u, pogotovo u Client-to-Server slučajevima.

SSH standard ima podršku za sigurno udaljeno prijavljivanje, siguran prijenos datoteka i sigurno preusmjeravanje TCP/IP podataka. On ima podršku za šifriranje, autentifikaciju i kompresiju prenošenih podataka. SSH se koristi za kreiranje tunela, a onda se kroz njega, uz pomoć nekih Linux/Unix programa, šalju podaci enkapsulirani u PPP pakete.

CIPE je namijenjen za velika poduzeća za izgradnju IP usmjerivača. On se integrira u jezgru operacijskog Linux/Unix sustava. Radi na principu tuneliranja IP paketa u šifriranim UDP paketima. CIPE nije tako fleksibilan kao IPSec, ali je dovoljno dobar za svoju originalnu zamisao: siguran povezivanje lokalnih mreža preko nesigurne mreže. Postoji verzija za Windows-e NT4.0 i 2000.

Linux FreeSWAN je besplatna implementacija IPSec-a & IKE-a za Linux. Zamisao FreeSWAN projekta je omogućiti da IPSec postane rašireni standard neovisan o platformi i operacijskom sustavu na kojem se izvodi. Njegov kod je raspoloživ svima i ne podliježe američkim ili drugim nacionalnim zahtjevima vezanim uz izvozna prava. Također postoji SWAN inicijativa od RSA-a.

Ako se nema potrebe za VPN-om nego samo za nekom specifičnom uslugom postoji još više mogućnosti. Za sigurno komuniciranje putem e-mail-a može se koristiti PGP, za siguran transfer podataka može se koristiti SFTP, za sigurno udaljeno prijavljivanje SSH, itd.

3. ODABIR VPN SUSTAVA ZA RJEŠAVANJE PROBLEMA

3.1. Opis problema koji želimo riješiti

Problem koji želimo riješiti je tipična računalna infrastruktura kakva se koristi u manjim poduzećima u Hrvatskoj. Najčešće se ona sastoji od dva do desetak kompjutera koji u pravilu rade na MS Windows operativnom sustavu.

3.2. Odabir opreme za rješavanje problema

3.2.1. Odabir VPN servera

VPN server se može izvesti hardverski ili softverski. Za VPN server je preporučljivo da se koristi hardverski iz sljedećih razloga:

- ključevi definirani za VPN komunikaciju su spremjeni u samom uređaju i do njih je puno teže doći nego kod softverskog kod kojeg su ključevi ustvari spremjeni na računalu
- algoritmi za kriptiranje hardverski su implementirani u sam uređaj i zbog toga u pravilu brži od softverskih
- VPN uređaj često zna biti implementiran u preusmjerivač (router) ili vatrozidni (firewall) uređaj što još više pojednostavljuje implementaciju i povećava sigurnost sustava

Prednost softverskih VPN servera je što se može koristiti bilo koji algoritam za kriptiranje (ako ga je dotični proizvođač softvera ugradio) jer se ne koristi specijaliziran hardver za kompresiju (bilj što i bolji hardverski izvedeni VPN serveri imaju mogućnost nadogradnje).

Na našem tržištu u trenutku potrage za uređajem odnosno preusmjerivačem koji podržava VPN i WAN nalazili su se sljedeći proizvođači:

- ASUS
- D-LINK
- LINKSYS (Cisco)
- MCRONET
- SMC
- TRUST
- TRENDNET
- ZyXEL

Na žalost NETGEARovi uređaji (koji podržavaju certifikate) su se našli u ponudi tek kad je izrada ove radnje bila toku. Većina tih uređaja podržava VPN pass-through (to znači da će kroz usmjerivač VPN paketi, odnosno promet, moći prolaziti bez problema). Na kraju su u uži izbor ušli LINKSYS i D-LINK, koji osim VPN servera, vatrozida i WAN-a služe i kao AP-ovi (bežične pristupne točke). Za ured koji se ne koristi bežičnim umrežavanje ova opcija nije potrebna. Na kraju je odabran D-LINK DI-824VUP+ koji je imao bolju podršku tehničkoj dokumentaciji, specifikacijama,

emulator web sučelja za upravljanje, nižu cijenu (oko 1.000kn naspram LINKSYS-a koji je koštao oko 1.300kn) te distributera koji kod nas ima veći dio njihovog programa, za razliku od LINKSYS-a koji je slabo zastupljen.

Ovakav uređaj biti će dovoljan za gore navedeno mrežno okruženje, dok je za veće mreže, specifične uvjete i modularnost preporučljivo koristiti opremu proizvođača CISCO koja je ustvari nepisani etalon što se tiče mrežne opreme i sigurnosti, te nju prodaju firme koje ujedno vrše i izvođenje cijele instalacije. Mrežna oprema Cisco nije korištena u ovoj radnji budući da je njezina cijena višestruko veća, a za ljude koji žele dobro upoznati tu opremu i naučiti više o mrežnom konfiguriranju postoje posebne akademije što prelazi opseg ove radnje.

Od bitnijih stvari D-LINK DI-824VUP+ podržava [8]:

- 4 portni komutator (switch) 10/100Mbps
- LPT/USB print server
- Cable/DSL modem + Dial-up modem
- Bežična mreža (wireless LAN) – 802.11g
- VPN pass-through za PPTP, L2TP i IPSec
- VPN server za PPTP, L2TP i IPSec
- Autentifikacija: MD5 i SHA-1
- Enkripcija: Null, DES, 3DES
- Podržava do 40 VPN tunela
- Vatrogodna zaštita (firewall)

3.2.2 Odabir VPN klijenta

MS Windows

Klijentska VPN podrška ugrađena je u Windows 2000 i XP. Za Windows od MS Windows 98 nadalje (a po nekim navodima postoji i podrška za Windows 95) Microsoft je izdao zakrpe/programe koji im također omogućuju stvaranje VPN tunela. Za korištenje VPN-a u Windows 2000 predlaže se da je instaliran Service pack 2, dok je kod Windowsa XP potreban Service pack 1. Oni će raditi i bez tih zakrpa, ali možda neće raditi neke funkcionalnosti opisane u ovoj radnji.

DrayTek Smart VPN Client

Drugi program koji je korišten u testiranjima bio je DrayTek Smart VPN Client (ver. 3.2.2). To je besplatan program koji omogućuje uspostavljanje VPN veze pomoću PPTP, L2TP, IPSec i L2TP/IPSec protokola. (Napomena: Prilikom uspostave L2TP veze, kod DrayTekovog softvera se koristi CHAP algoritam za provjeru vjerodostojnosti (Authentication protocol), te se ne može odabrati niti jedan drugi, što rezultira greškom nemogućnosti spajanja na port ako se odabere krivi algoritam).

TheGreenBow IPSec Client

Treći odabrani softver je TheGreenBow IPSec Client. On omogućuje samo IPSec tuneliranje. Microsoft za uspostavu IPSec veze koristi Local Security Policy. DrayTek također koristi isti servis, dok TheGreenBow koristi vlastiti servis, zbog čega je neovisan o Microsoftovoj implementaciji te ga je moguće uspostaviti i na Windows 95.

3.3. Opis sustava koji rješavamo

Za testni sustav odabrana je lokalna mreža koja se sastoji od 2 računala (povremeno je korišteno i treće računalo, ali radi jednostavnosti prikaza koristiti će se samo 2 računala) sa sljedećim specifikacijama:

Računalo 1:

Operativni sustav: MS Windows 2000 Professional

IP adresa: 192.168.0.200

Naziv računala: Jagoda

Računalo 2:

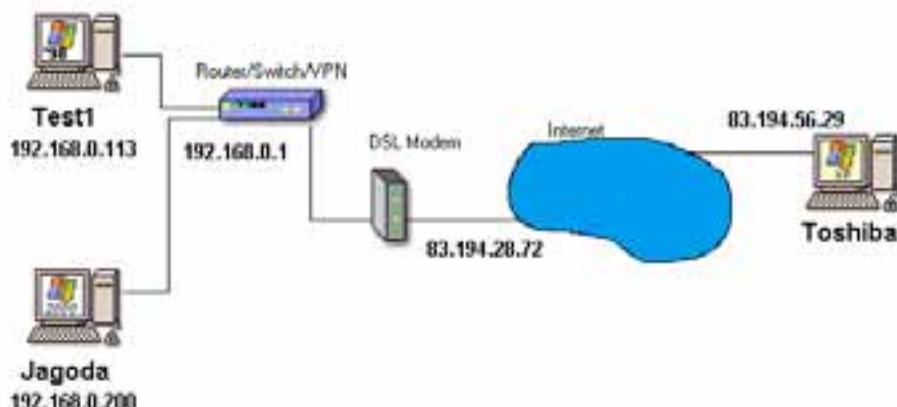
Operativni sustav: MS Windows 98 SE

IP adresa: 192.168.0.113

Naziv računala: Test1

Oba računa spojena su na lokalnu mrežu TCP/IP protokolom sa statičkom IP adresom. Budući da se na mreži nalazi i Windows 98 računalo potrebno je uključiti opciju Enable NetBIOS over TCP/IP u TCP/IP postavkama mrežne kartice. Maska podmreže (Subnet mask) je 255.255.255.0, a usmjerivač (gateway) je na adresi 192.168.0.1. Usmjerivač je D-LINK DI-824VUP+ koji se koristi se kao VPN server, vratovid i poveznik na Internet. IP adresa koju će usmjerivač dobiti od ISP-a (Internet Service Provider) biti će dinamička. Kako bi klijent mogao znati na kojoj se adresi nalazi usmjerivač koristi se usluga DDNS (Dynamic DNS) odnosno dinamičkog DNS-a na adresi hof505.dyndns.org.

Sa klijentske strane imamo Windows XP SP1 računale koje se spaja preko analognog 56kbps modema. Nema razlike u pripremi i upotrebi VPN-a kad se koristi adsl tehnologija za spajanje na Internet umjesto analognog modema, pa se ovdje navedene postavke i činjenice mogu upotrijebiti i u slučaju da se umjesto analognog modema koristi, kod nas, sve rašireniji pristup Internetu putem adsl tehnologije. Naravno predhost adsl-a je daleko brža veza od analognog modema.



Slika 3.1 Sustav koji rješavamo

3.4. Odabrani protokoli za uspostavu VPN sustava

Kako je dosad u razmatranju rečeno serversku stranu za VPN osigurati će D-LINK-ov usmjerivač, te će na njemu biti uspostavljena veza putem tri najpopularnija protokola. To su:

- PPTP
- L2TP
- IPSec

Budući da je PPTP i L2TP vezu vrlo jednostavno za uspostaviti, glavna koncentracija biti će na opisu, konfiguriranju te rješavanje problema IPSec protokola. Kako D-LINK DI-824VUP+ ne podržava L2TP/IPSec protokol tako ta kombinacija neće biti opisana u praksi. U dolje navedenom razmatranju opisuje se kako uspostaviti samo L2TP i samo IPSec vezu, pa ako je to moguće te ako se koristi adekvatan usmjerivač sa podrškom za L2TP/IPSec ne bi trebalo biti problema i za korištenje tog protokola.

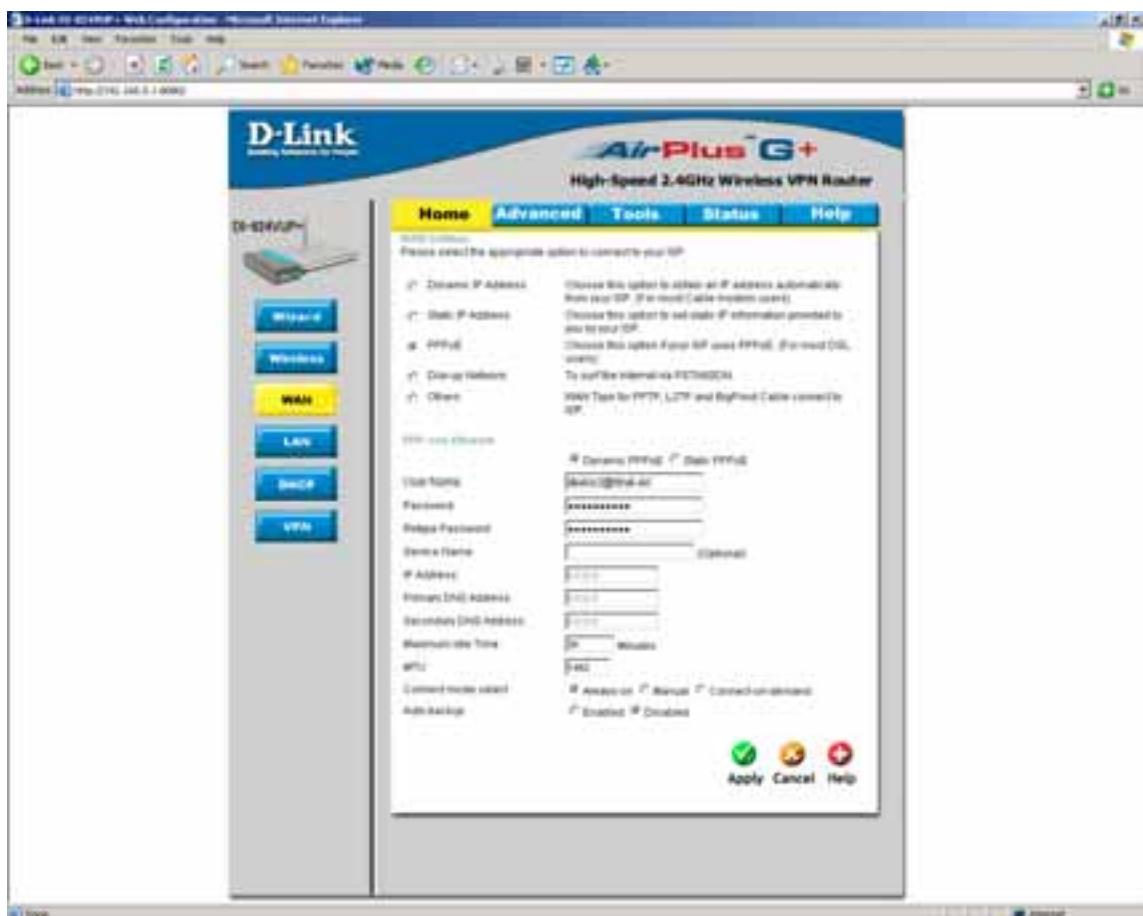
4. RJEŠAVANJE PROBLEMA

4.1. Podešavanje usmjerivača

4.1.1. Kartica (meni) Home

Nakon raspakiravanja, te spajanja D-LINK-a DL-824VUP+ (u daljem tekstu D-LINK) osnovno konfiguriranje se može napraviti pomoću Čardbnjaka (Wizard-a). Opcije pod Wireless nisu potrebne za ovu radnju.

Za vezu prema Internetu može se koristiti analogni modemski ulaz (PSTN), ISDN linija, kabelska veza (preko UTP kabела), te PPPoE za DSL vezu. Također ako ISP podržava obvezno tuneliranje (opisano na početku radnje) podržana je i ta opcija. Za vezu na Internet koristiti će se DSL. Pod *Connect mode select* obavezno treba odabrati *Always-on* kako bi lokalna mreža bila stalno spojena na Internet. Količina prenesenih podataka za samo održavanje veze je zanemariva i na mjesecnoj razini iznosi < 50MB.



Slika 4.1 Osnovne postavke za Internet vezu

Pod LAN opcijama podešavaju se mrežne postavke lokalne mreže:

IP Address: 192.168.0.1 (može biti i neka druga npr. 10.0.0.1)

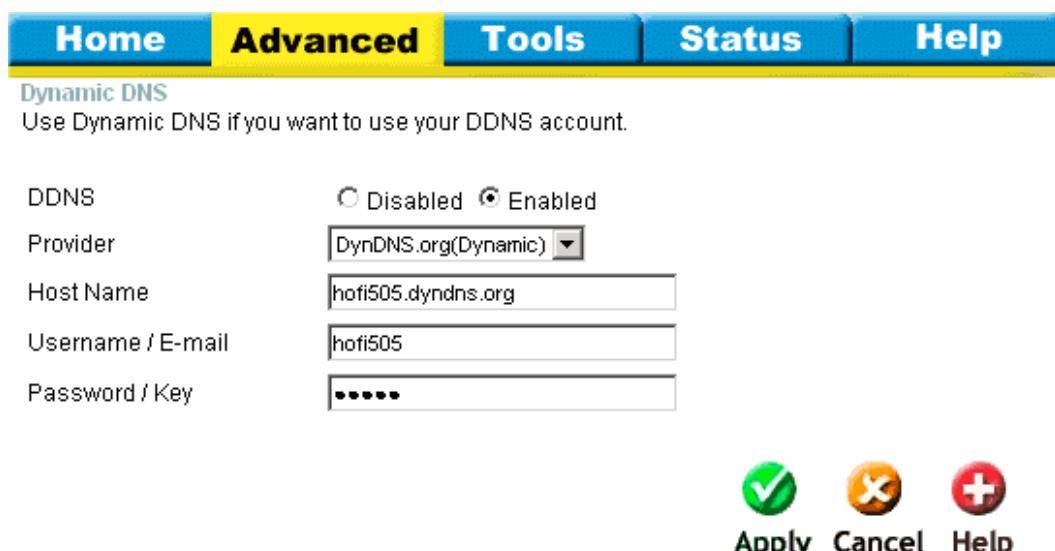
Subnet Mask: 255.255.255.0 (D-LINK podržava samo adrese oblika 255.255.255.x)

Domain Name: KOMTEH

Po potrebi u meniju DHCP moguće je podesiti dinamičko dodjeljivanje IP adresa, dok su za potrebe ove radnje korištene statičke IP adrese.

4.1.2 Kartica (meni) Advanced

D-LINK je automatski podešen za korištenje za VPN, tako da jedino što se ovdje treba podesiti je DDNS. Budući da se za ostvarivanje veze koristi adsl, adresa koja se dobije prilikom spajanja na Internet je svaki put druga. Kako bi netko izvan lokalne mreže znao koja je Internetska IP adresa D-LINK-a koristi se DDNS. Upotreboom naredbe ping može se dobiti trenutna adresa usmjerivača. Upotreba DDNS servisa je besplatna, a za njezinu uspostavu potrebno se je registrirati na neki od podržanih servisa.



Slika 4.2 Podešavanje DDNS servera

Primjer upotrebe ping naredbe i pronalaženje adrese od D-LINK-a:

C:\>ping hofi505.dyndns.org

Pinging hofi505.dyndns.org [83.131.43.22] with 32 bytes of data:

Reply from 83.131.43.22: bytes=32 time<1ms TTL=64

Reply from 83.131.43.22: bytes=32 time<1ms TTL=64

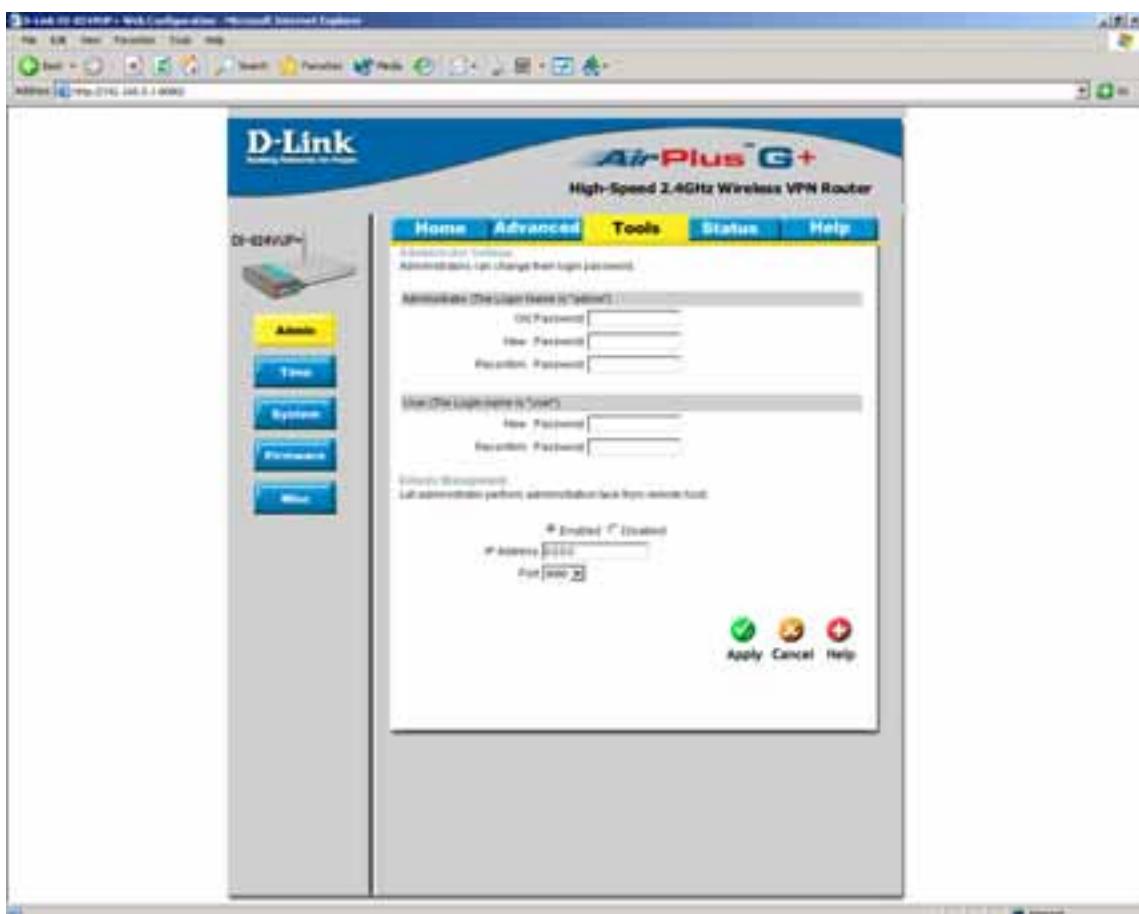
.....

Iz primjera je vidljivo da je trenutno dodijeljena adresa D-LINK-u: 83.131.43.22.

U slučaju da je D-LINK spojen stalnom vezom sa statičkim IP-em na Internet, nije potrebno koristiti DDNS, već je dovoljno koristiti statičku adresu pri uspostavi VPN-a.

4.1.3. Kartica (meni) *Tools*

Udaljeno upravljanje (Remote Management) je potrebno uključiti za vrijeme podešavanja i testiranja ako su klijentsko računalo i D-LINK fizički odvojeni, kako bi se eventualne izmjene u podešavanju D-LINK-a mogle izvesti i preko Interneta. Nakon što sve proradi, udaljeno upravljanje je poželjno isključiti, kako ne bi potencijalnim napadačima ostavili rupu za upad na lokalnu mrežu.



Slika 4.3 Privremeno je potrebno uključiti udaljeno upravljanje

Pod opcijama MSC treba isključiti *Discard PING from WAN side* kako bi se izvana (sa Interneta) moglo koristiti naredbu ping.

4.1.4. Kartica (meni) Status

Ako pod opcijama *Device Info* u rubrici *IP address* piše bilo koja adresa različita od 0.0.0.0 znači da je veza prema Internetu uspostavljena.

U opcijama Log nalaze se evidencije pokušaja upada u lokalnu mrežu, ali i evidencije o pokušajima uspostave te o uspješno uspostavljenim VPN konekcijama.



Slika 4.4 Izgled kartice Status prilikom uspješno uspostavljene veze

4.2. Podešavanje VPN servera

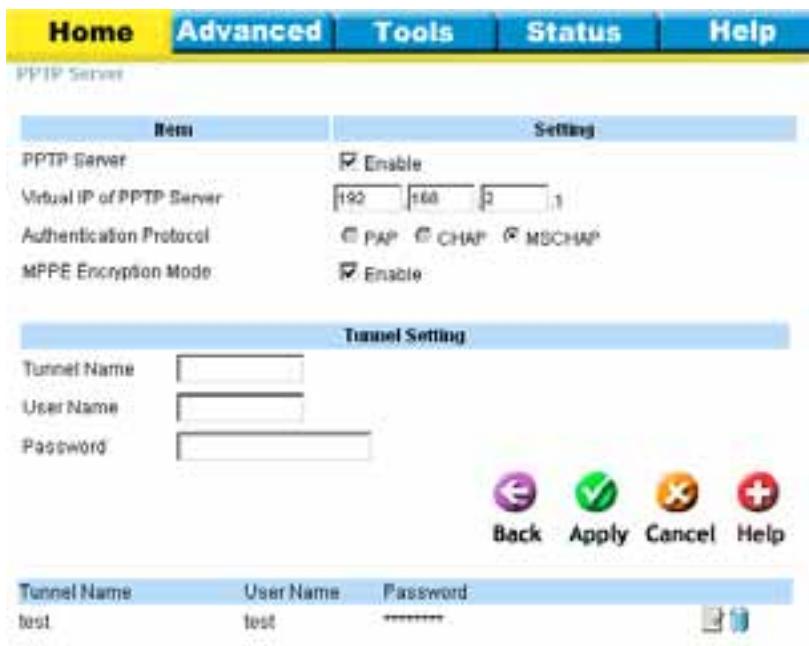
4.2.1. Podešavanje PPTP protokola

Pod menijem Home → VPN → PPTP Server Setting.. potrebno je podešiti slijedeće:

- uključiti PPTPserver
- pod *Virtual IP of PPTP Server* upisati 192.168.2.1*
- pod *Authentication Protocol* odabran je MS-CHAP budući da se spajamo sa MS Widnow s klijentskog računala (ostale opcije: PAP, CHAP)
- uključimo *MPPE Encryption Mode* – to se može koristiti samo ako se koristi MS-CHAP. Dok Microsoft kod L2TP tuneliranja za šifriranje koristi IPSec (odnosno DES/3DES algoritam), kod PPTP protokola on za šifriranje koristi MPPE (odnosno RSA RC4 algoritam – može biti 40, 56 ili 128bitni)

* D-LINK ne podržava da virtualna klijentova i serverska PPTP IP adresa budu u spektru lokalne poddomene.

Tunnel name i *User Name* su proizvoljni kao i šifra. Kako bi šifru bilo što teže probiti predlaže se korištenje šifre od minimalno 8 znamenki u kojoj se osim brojaka i slova nalaze i simboli. Primjer dobre šifre: a4R\$glj2. Ova pravila za generiranje šifara predlažu se za generiranje bilo koje šifre koju trebamo koristiti, ne samo za PPTP protokol već općenito.



Slika 4.5 Postavke za PPTP server

4.2.2 Podešavanje L2TP protokola

Pod menijem Home → VRN → L2TP Server Setting.. potrebno je podesiti slijedeće:

- uključiti L2TPserver
- pod *Virtual IP of PPTP Server* upisati 10.0.0.1*
- pod *Authentication Protocol* odabran je CHAP budući da Smart VPN client nema mogućnost odabira protokola kao što to ima Windowsov klijent (ostale opcije: PAP, MS-CHAP)

* D-LINK ne podržava da virtualna klijentska i serverska L2TP IP adresa budu u spektru lokalne poddomene.

Tunnel name i *User Name* su proizvoljni kao i šifra (vrijedi isto kao i za PPTP protokol)



Slika 4.6 Postavke za L2TP server

4.2.3. Podešavanje IP Sec protokola

U meniju Home → VPN potrebno je uključiti VPN kako bi D-LINK služio kao VPN server (često se koristi izraz VPN *endpoint*, budući da se VPN server najčešće koristi kao krajnja točka u VPN tunelu). Također potrebno je uključiti NetBIOS broadcast. NetBIOS broadcast Microsoft koristi u lokalnim mrežama kako bi se računala koja koriste Windows se mogla pronaći i komunicirati. On omogućuje da se priklom odabira Windows Network Neighborhood-a vide ostala računala spojena na mrežu. Na žalost D-LINK i Windows se pokazuju nekompatibilnost što se toga tiče te nije bilo moguće podesiti D-LINK i Windows se (niti 2000 bez SP-a, niti 2000 SP3, niti XP) da NetBIOS proradi kako bi trebao.

Budući da se klijentska strana spaja na VPN putem Dial-up (56k analogni modem), odnosno svaki put mu je dodijeljena druga IP adresa, potrebno je konfigurirati dinamički VPNserver Home → VPN → Dynamic VPN Settings...



Slika 4.7 Osnovne postavke za dinamički IPSec

Pod *Tunnel Name* upisati *test*, ovaj naziv koristi se samo kod pregleda statusa VPN veze. *Dynamic VPN* treba uključiti budući da se to koristi. *Local Subnet* je 192.168.0.0, dok je *Local Netmask* 255.255.255.0. Za potrebe testiranja *Preshare Key* je podešen na 123456 dok se za upotrebu u stvarnom sustavu predlaže korištenje teže pamtljivih šifri kako je to opisano gore. PPTP i L2TP koriste korisničko ime i šifru prilikom provjere vjerodostojnosti, a IPSec vjerodostojnost ne provjerava na korisničkom nivou nego na bazi računala pa je za provjeru vjerodostojnosti (autentičnosti) uveden xAUTH protokol. Taj protokol Microsoft ne podržava pa ga treba isključiti. Razlog tome je prestanak standardizacije tog protokola od strane IETF-a, te neki sigurnosni problemi i slaba kompatibilnost raznih proizvođača prilikom korištenja xAUTH protokola. Umjesto toga Microsoft predlaže korištenje L2TP/IPSec protokola, odnosno da se za provjeru vjerodostojnosti brine L2TP protokol.

Osim osnovnih postavki potrebno je podesiti *Home* → *VPN* → *Select IKE Proposal* i *Home* → *VPN* → *Select IPSec Proposal*. U ta dva menija biramo koji će se algoritmi koristiti za raznjenju ključeva i šifriranje. Postavke koje se ovdje postave trebaju biti iste i na strani klijenta inače se klijent i D-LINK neće moći dogovoriti oko algoritama za komunikaciju te se VPN veza neće moći uspostaviti.



Slika 4.8 Odabir IKE algoritama za dogovor oko ključeva

Za IKE Proposal za komunikaciju može se odabrati više algoritama, odnosno stvoriti više predložaka. Ako ne uspije onaj najviši na listi uspostavu komunikacije probati će uspostaviti idući na listi, i tako redom do zadnjeg predloška.

Pod DH Group odabiremo *Group 2*. DH group je skraćenica od Diffie-Hellman group, a često se naziva i Oakley group.

Diffie-Hellman Group	Modulus	Reference
Group 1	768 bits	RFC2409
Group 2	1024 bits	RFC2409
Group 5	1536 bits	RFC3526
Group 14	2048 bits	RFC3526
Group 15	3072 bits	RFC3526
Group 16	4096 bits	RFC3526
Group 18	8192 bits	RFC3526

Tablica 4.1 Najčešće DH grupe

RFC2409 standard je predlagao korištenje DH group 1 algoritma za upotrebu u IKEv1, ali kako njegovo šifriranje nije više toliko sigurno standard je predložio slijedeće izmjene:

ALGORITAM	RFC 2409	Predložene promjene u RFC 2409 (5m j.2005)
DES za šifriranje	OBVEZAN	MOŽE (potencijalno slaba sigurnosna zaštita)
TripleDES za šifriranje	POŽELJAN	OBVEZAN
AES-128 za šifriranje	N/A	POŽELJAN
MD5 za hashing i HMAC	OBVEZAN	MOŽE (potencijalno slaba sigurnosna zaštita)
SHA1 za hashing i HMAC	OBVEZAN	OBVEZAN
RSA sa potpisima DSA sa potpisima RSA sa šifriranjem	POŽELJAN POŽELJAN POŽELJAN	POŽELJAN MOŽE (nedostaje implementacije) MOŽE (nedostaje implementacije)
D-H Group 1 (768) D-H Group 2 (1024) D-H Group 14 (2048) DHelliptic curves	OBVEZAN POŽELJAN N/A POŽELJAN	MOŽE (potenc. slaba sigurnosna zaštita) OBVEZAN POŽELJAN MOŽE (nedostaje implementacije)

Tablica 4.2 IKEv1 – predložene promjene

Pod *Encrypt algorithm* potrebno je odabrat 3DES (sami DES algoritam nije više dovoljno siguran). Za *Auth algorithm* odabran je SHA1. MD5 više nije siguran, a ima glasina da je već i SHA1 probijen [6], odnosno da više nije siguran. Ipak za to probijanje potrebno je puno procesorske snage, te se mali korisnici ne bi trebali posebno zabrinjavati. U budućnosti možemo očekivati da će i ovaj algoritam biti zamjenjen sa nekim drugim.

Life Time je potrebno podesiti na 28800 sec .Ako jedna od strana predloži manji *Life Time* onda će taj *Life Time* biti prihvacen. *Life Time* označava koliko je vrijeme trajanja VPN tunela i ono je najčešće 28800 sekunda (= 8 sati).

Opcije pod *IPSec Proposal* vrlo su slične opcijama pod *IKE proposal*. Korištene postavke su slijedeće:

- *DH Group*: N/A
- *Encap protocol*: ESP (odabran je ESP, a ne AH budući da je ESP jači algoritam jer omogućuje i šifriranje poruka, odnosno treća stana ne može čitati poslane poruke, ako nema za to ovlaštenje odnosno ključ)
- *Encrypt algorithm*: 3DES
- *Auth algorithm*: MD5
- *Life Time*: 28800 sec



Slika 4.9 IPSec postavke za dinamički tunel

Gornji postupak podešavanja IPSec-a opisan je za dinamički tunel. Za potrebe ove radnje uspostavljen je i statički IPSec tunel. Statički IPSec tunel namijenjen je rješenjima server-to-server, te se ne koristi kod client-to-server rješenja. Za uspostavu client-to-server rješenja potrebno je nakon što klijent dobije svoju IP adresu, koristiti Remote Management za D-LINK te u opcijama *Remote Subnet* upisati IP adresu klijentskog računala, a pod *Subnet Mask* 255.255.255.255.

4.2.4. Provjera statusa IP Sec veze

Nakon uspješne uspostave IP Sec veze u rubrici Status → VPN Status možemo vidjeti podatke o IP Sec vezi koji uključuju dogovorenou vrijeme trajanja veze te IP adrese klijenta i mreže na koju se spojio.

VPN Status
VPN status display VPN connection state.

Refresh **VPN setting...**

Name	Remote Network	Local Network	Type	State	Life Time	Drop
	IP Address/ Subnet Mask/ Gateway	IP Address/ Subnet Mask				
ttt	195.29.140.30/ 255.255.255.255/ 195.29.140.30	192.168.0.0/ 255.255.255.0	ESP tunnel	IKE established	566	Drop
ttt	0.0.0.0/ 255.255.255.255/ 255.255.255.255	192.168.0.0/ 255.255.255.0		Dynamic IPSec	0	

Slika 4.10 Podaci o uspješno uspostavljenoj IPSec vezi

4.3. Podešavanje klijenta i testiranje veze i raznih protokola

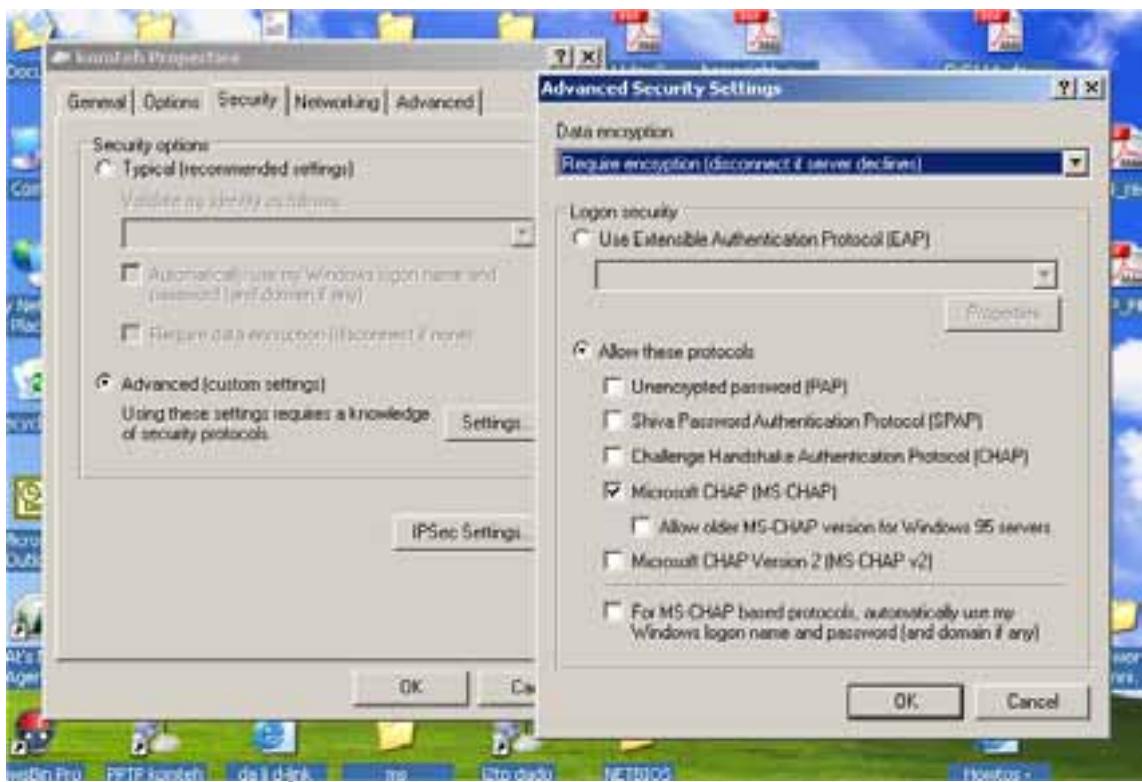
4.3.1. PPTP klijent

Microsoft je u Windows 2000 i XP implementirao podršku za PPTP protokol. Za Windows u kojima nije implementirana klijentska podrška za PPTP, podršku je moguće skinuti sa web stranica www.microsoft.com. Dakle podršku za PPTP imaju svi Windows osim Windows 95 i starijih verzija Windowsa.

Postupak uspostave PPTP veze u Windowsima:

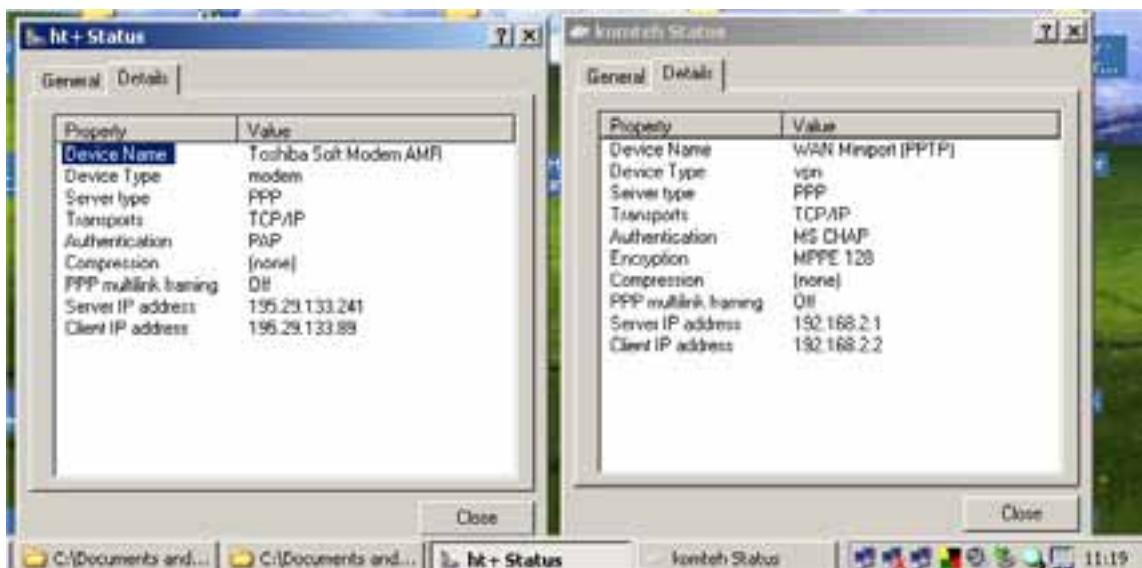
Treba pokrenuti New Connection Wizard (Start → Settings → New Connection Wizard). Odabratи: Connect to my network at my workplace → Next → Virtual private Network connection → upisati: KOMTEH → Next → Next → upisati hofi505.dyndns.org (ili neku drugu adresu na kojoj se nalazi VPN server) → Next → odabratи da napravi prečac na Desktopu → Finish. Nakon pokretanja stvorene veze potrebno je upisati User name: test, te Password. Također treba odabratи Properties → Security → Advanced → Settings. Tu treba odabratи Require encryption te odabratи samo Microsoft CHAP kako je to i napravljeno na D-LINK-u. Ako se ne podese isti protokoli na D-LINK-u i kod klijenta neće uspjeti faza dogovaranja (negotiation) i veza će se prekinuti.

U meniju Networking može se odabratи da li se želi koristiti Automatski, PPTP ili L2TP/IPSec protokol za stvaranje VPN tunela. Ako se odabere Automatski Windows si će prvo probati uspostaviti L2TP/IPSec vezu, pa kad to ne uspije probati će se uspostaviti PPTP veza.



Slika 4.11 Postavke za spajanje PPTP protokolom

Nakon što je uspostavljena PPTP veza moći ćemo normalno koristiti *My Network Places* kao da se fizički nalazimo spojeni u lokalnu mrežu. Kao što se može vidjeti na slici 4.12 uz normalnu Dial-up vezu spojeni smo i PPTP protokolom, te nam je dodijeljena lokalna adresa 192.168.2.2, dok je virtualna serverska adresa 192.168.2.1. Kako se MS-CHAP koristi za provjeru vjerodostojnosti moguće je uklučiti i MPPE algoritam za šifriranje.



Slika 4.12 Postavke nakon uspostave PPTPveze

Za provjeru da li je PPTP veza ostvarena uspješno korištena je naredba ping 192.168.0.200. rezultat je bio slijedeći:

```
C:\Documents and Settings>ping 192.168.0.200
```

Pinging 192.168.0.200 with 32 bytes of data:

```
Reply from 192.168.0.200: bytes=32 time=263ms TTL=128
```

```
Reply from 192.168.0.200: bytes=32 time=254ms TTL=128
```

```
Reply from 192.168.0.200: bytes=32 time=261ms TTL=128
```

```
Reply from 192.168.0.200: bytes=32 time=248ms TTL=128
```

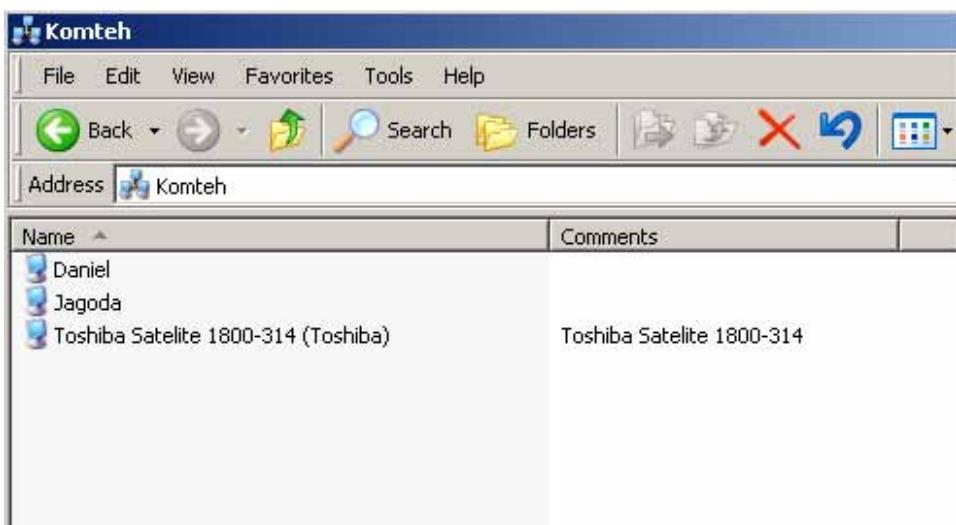
Ping statistics for 192.168.0.200:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum =248ms, Maximum =263ms, Average =256ms

Na žalost nije bilo moguće pristupati grupi KOMTEH. Razlog tome je što je LAN kartica bila uključena, pa je uzrokovala pomutnju u usmjerivačkoj (routing) tablici. Nakon isključivanja mrežne kartice te resetiranja kompjutera sve je proradilo normalno.



Slika 4.13 Prikaz trenutno aktivnih kompjutera u grupi KOMTEH

Nakon spajanja modema na Internet imamo slijedeću usmjerivačku tablicu (naredba *route print*):

Active Routes:

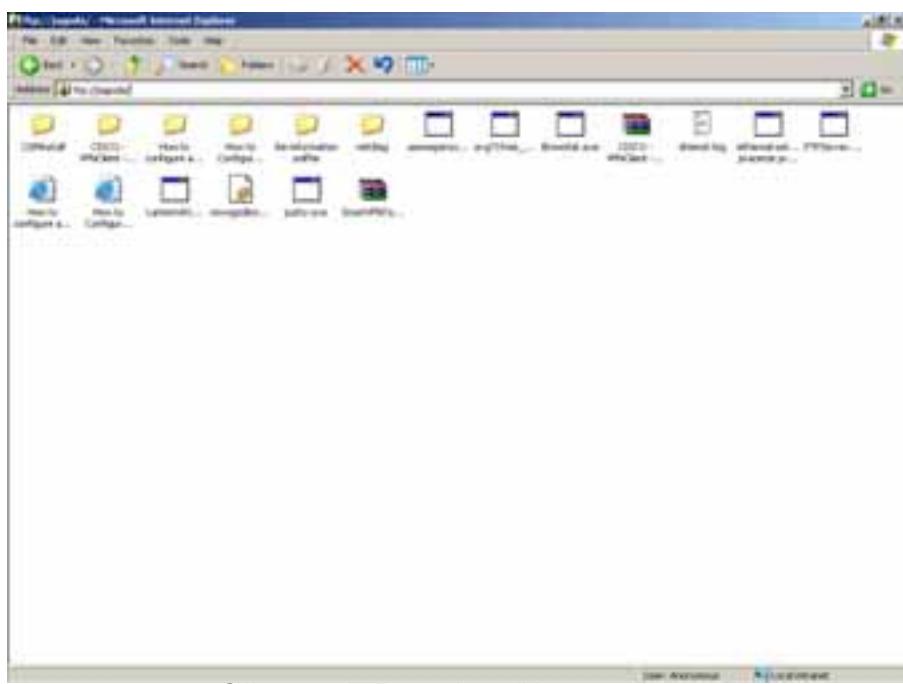
Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	83.131.124.203	83.131.124.203	1
83.131.124.203	255.255.255.255	127.0.0.1	127.0.0.1	50
83.131.125.241	255.255.255.255	83.131.124.203	83.131.124.203	1
83.255.255.255	255.255.255.255	83.131.124.203	83.131.124.203	50
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	240.0.0.0	83.131.124.203	83.131.124.203	1
<i>Default Gateway:</i> 83.131.124.203				

Nakon stvaranja PPTP tunela usmjerivačka tablica izgleda ovako:

Active Routes:					
Network Destination	Netmask	Gateway	Interface	Metric	
0.0.0.0	0.0.0.0	83.131.124.203	83.131.124.203	2	
0.0.0.0	0.0.0.0	192.168.2.4	192.168.2.4	1	
83.131.43.22	255.255.255.255	83.131.124.203	83.131.124.203	1	
83.131.124.203	255.255.255.255	127.0.0.1	127.0.0.1	50	
83.131.125.241	255.255.255.255	83.131.124.203	83.131.124.203	1	
83.255.255.255	255.255.255.255	83.131.124.203	83.131.124.203	50	
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	
192.168.2.4	255.255.255.255	127.0.0.1	127.0.0.1	50	
192.168.2.255	255.255.255.255	192.168.2.4	192.168.2.4	50	
224.0.0.0	240.0.0.0	83.131.124.203	83.131.124.203	2	
224.0.0.0	240.0.0.0	192.168.2.4	192.168.2.4	1	
Default Gateway: 192.168.2.4					

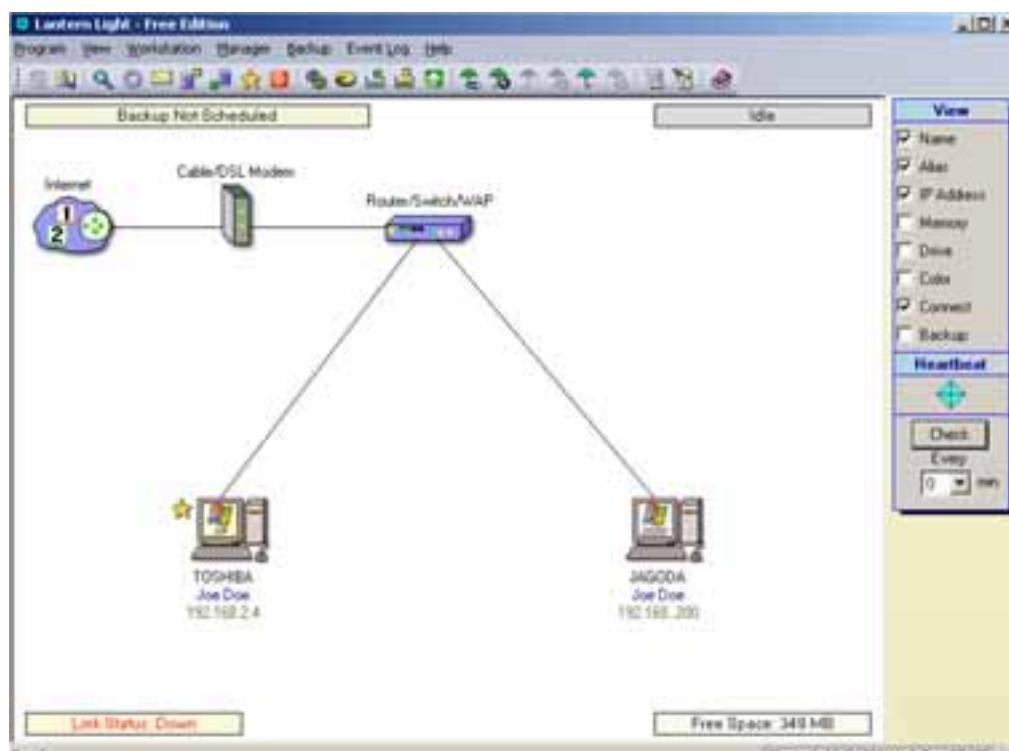
Kao što je vidljivo iz ispisa tablice, sav promet namijenjen za lokalnu mrežu (uključujući i Internet promet) će ići preko virtualne IP adrese 192.168.2.4 koju je klijent dobio kao virtualnu adresu u lokalnoj mreži D-LINK-a. Ako se za korištenje Interneta ne želi ići preko D-LINK-a nego preko vlastite Dial-up veze potrebno je opciju *Use default gateway on remote network* (U PPTP opcijama → Networking → Internet Protocol (TCP/IP) → Properties → Advanced → Use default gateway on remote network). Često je bolje ostaviti opciju uključenu jer onda usmjerivač filtrira napade, web stranice kao da se osoba nalazi iza usmjerivača u firmi.

Na kompjuteru Jagoda pokrenut je FTP servis pomoću programa *Quick 'n Easy FTP Server-a*. Prijenos podataka radi bez problema.



Slika 4.14 FTP servis radi bez problema

Također za testiranje rada mreže korišten je i program Lantern Manager tvrtke Coralis Corporation (besplatna verzija za do 5 umreženih računala). Za korištenje tog programa instaliran je serverski (Lantern Manager) i klijentski (Lantern Agent) softver na klijentsko VPN računalo, te je instaliran klijentski softver na računalo Jagoda (na računalo Test1 zbog premalenih memorijskih resursa nije instaliran Lantern Agent, zato ga i nema u shemama koje Lantern Manager prikazuje). Taj program omogućuje ispis informacija o računalima u lokalnoj mreži, način kako su spojeni, a ima i program VNC koji služi za udaljeno upravljanje računabm. Lantern Manager je našao virtualnu lokalnu mrežu i za njega ne postoji fizička udaljenost ovih računala.

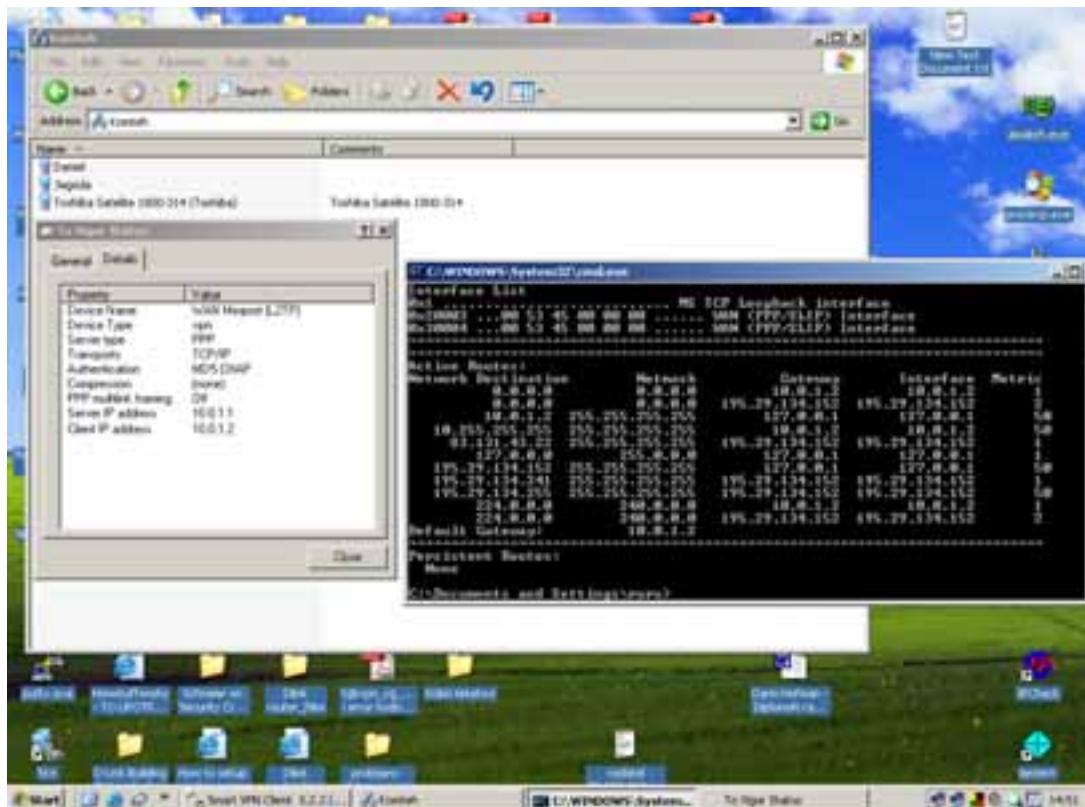


Slika 4.15 Za Lantern Manager mreža izgleda kao da je fizički spojena

4.3.2 L2TP klijent

Kako D-LINK ne podržava L2TP/IPSec vezu ovde će biti opisana samo uspostava L2TP veze. Da bi se mogla koristiti samo L2TP veza potrebno je zabraniti automatsko korištenje IPSec-a. Više o tome se nalazi u Microsoftovoj bazi znanja (Microsoft Knowledge Base), članak Q310109. Tamo piše da ako se želi isključiti IPSec treba se u Windowsovom registru (Windows Registry) vrijednost ključa `HKLM\System\CurrentControlSet\Services\Rasman\Parameters\ProhibitIpSec` promijeniti u 1. Sva podešavanja za IPSec i certifikate za nas može obaviti program Smart VPN Client. On podržava sva 4 načina spajanja i za razliku od Windowsa može se spojiti i samo L2TP protokolom.

Način spajanja je isti kao i kod PPTP protokola jedino je razlika što je podešeno da virtuálna adresa klijenta bude u domeni 10.0.0.0/255.255.255.0. Nakon spajanja L2TP protokolom za korisnika nema vidljivih razlika (slika 4.16) između tog i PPTP protokola.



Slika 4.16 Postavke nakon spajanja L2TP protokolom slične su kao i kod PPTP protokola

4.3.2.1. Razlike između PPTP i L2TP protokola

L2TP ide preko UDP protokola, dok PPTP koristi TCP protokol. Zbog toga je L2TP brži, manje zauzimaju paketi, ali je ujedno i manje siguran, jer se izgubljeni paketi neće ponovo poslati. PPTP za razliku od L2TP-a odvojeno šalje kontrolne informacije i podatke – prve putem TCP-a, a druge putem GRE-a (manje popularan Internet standard). Zbog kombiniranja kontrolnih informacija i podataka zajedno, L2TP je ustvari bolji protokol gledajući od strane vatrozidnih uređaja, budući da dio vatrozidova ne podržavaju GRE.

L2TP najčešće dolazi u kombinaciji sa IPSec protokolom te ako uređaj ne podržava tu kombinaciju najbolje je koristiti PPTP.

4.3.2.2. Testiranje veličine paketa zapakiranih PPTP i L2TP protokolom

Kako bi vidjeli razliku u veličini prometa koji uzrokuje PPTP i L2TP protokol na klijentskoj strani koristio sam istu testnu datoteku. Datoteka je u binarnom formatu i iznosila je 421.888 bajta. Rezultati testiranja za prijenos te datoteke sa računala Jagoda na klijentsko računalo vidjivi su u tablici.

	PPTP		L2TP	
	Internet	Virtualna mreža	Internet	Virtualna mreža
IP adresa adaptera	195.29.48.11	192.168.2.5	195.29.138.188	10.0.1.3
Primljeno podataka	507.992	488.572	505.322	487.516
Poslano podataka	58.674	28.756	36.839	23.079

Tablica 4.3 Količina podataka prenesena Internetom da bi se prenijela testna datoteka

Iz tablice je vidljivo da su količine podataka primjene htemetom približno slične, ali ipak je kod L2TP-a ta količina manja. Ukoliko usporedimo ukupnu količinu prenesenih podataka (slanje + primanje) kod PPTP-a to je: 566.666 bajta, dok je to kod L2TP-a: 542.161 bajta. To je ipak primjetna razlika od oko 4% posto. Ove rezultate treba uzeti samo kao okvirne rezultate, za prave rezultate trebalo bi povećati testnu datoteku, te što je više moguće smanjiti utjecaj prometa na lokalnoj mreži.

Prilikom testiranja nije bilo izgubljenih UDP paketa, te je upotreba UDP paketa preporučljiva za mreže gdje je međusobna veza relativno dobra, odnosno nema potrebe za ponovnim slanjem paketa.

4.3.3. IPSec klijent

Microsoft podržava unaprijed dogovoren dijeljeni ključ (pre-shared key) za IKE u slučaju korištenja L2TP/IPSec server-to-server implementacije. Po Microsoftu (članak Q240262) korištenje unaprijed dogovorenog dijeljenog ključa za client-to-server je podržano u Windowsima 2000 (samo radi svrhe testiranja), ali ne i u Windowsima XP. Ipak moguće ga je koristi i u Windowsima XP uz pomoć programa poput Smart VPN Client-a ili ručnim podešavanjem u Local Security Policy-a.

U Microsoft Windowsima u Local Security Policy uz podešavanje prava i lokalnih sigurnosnih pravila moguće je odrediti sigurnosne postavke vezane uz IP promet. Local Security Policy može se startati sljedećim putem: Start → Settings → Control Panel → Administrative Tools → Local Security Policy (ili Start → Run → secpoco.msc). IPSec i servise vezane uz njega u Windowsima je implementirao

Microsoft u zajedničkoj suradnji sa Cisco System-om, dok je L2TP Microsoft implementirao sami integriran je sa IPSec-om od verzije beta 2 nadalje.

Microsoft Windows koristi svoj servis za IPSec politiku (IPSec policy). Kada se neki od IPSec profila primjeni (Apply), IPSec koristi filtere paketa (packet filters) da bi odlučio koji promet treba osigurati, koji treba propusiti, a koji blokirati. Kada se osigurava promet, za dogovor oko sigurnosnih postavki i razmjenu ključeva koristi se IKE Po IETF standardu (RFC 2409) za upotrebu IKE-a u IPSec-u mogu se koristiti sljedeća tri algoritma za provjeru vjerodostojnosti: Kerberos v5.0, Certifikati ili unaprijed dogovoren ključ.

Microsoft predlaže korištenje IPSec tunela samo kada imamo server-to-server VPN sustav koji ne podržava L2TP/IPSec, ili kada imamo client-to-server sustav sa statičkim IP adresama. Prema njegovim navodima IPSec nije moguće koristiti kod VPN klijenta koji koristi dinamičku IP adresu. Ipak, to nije u potpunosti točno, jer IP adresu klijenta u Local Security Policy je moguće mijenjati ručno pa je moguće i uspostaviti PSec vezu. Kako bi se izbjegao taj postupak, koji zahtjeva dosta klikanja i podešavanja, može se koristiti klijent poput Smart VPN Client-a koji to sve sam podešava.

Budući da je za L2TP napisan standard (RFC 2661), njegova upotreba je raširena, ali za osiguranje L2TP prometa pomoći IPSec-a još nije napisan RFC standard. IETF (Internet Engineering Task Force) organizacija radi na tome (podaci preuzeti iz Microsoftovog dokumenta broj: 265112, objavljenog 21.10.2005). Prema tome, popularizacija i bolja kompatibilnost L2TP/IPSec standarda se može očekivati nakon usvajanja standarda.

IKE dogovor sastoji se od dvije faze:

Prva faza (Phase 1) – brine se za sigurnu provjeru vjerodostojnosti. Nakon što se obje strane izvrše provjeru vjerodostojnosti stvara se takozvani IKE SA (IKE Security Associations). Njegovo standardno vrijeme trajanja je 8 sati.

Druga faza (Phase 2) – u njoj se dogovara koji će se od protokola iz ESP-a ili AH-a koristiti. Da bi mogla započeti druga faza prvo se mora uspješno završiti prva faza. Primjer za drugu fazu: Klijent ponudi da može komunicirati preko ESP-a sa 3DES-om i preko AH-a sa SHA-1. Server odgovara da on želi koristiti samo ESP sa 3DES-om. Oni onda uspostavljaju sigurni kanal zaštićen ESP-om koristeći 3DES.

4.3.3.1. Korištenje IP Security policy Management-a

Za stvaranje nove politike za IPSec, potrebno je u Local Security Policy-u desnom tipkom miša kliknuti na IP Security Policies on Local Computer i odabratи Create IP Security Policy...[9].

Korak 1. Na idućem meniju odabratи Next→ pod ime upisati: IPsec Policy - VPN to DI-824VUP+ → Next → isključiti Activate the default response rule → Next → ostaviti označenu kučicu pokraj Edit properties → Finish.

Korak 2. U IPsec policy properties odznačiti Use Add Wizard i kliknuti na Add...

- U IP filter list kliknuti na Add... Pod Name upisati WinXP to DI-824VUP+ te kliknuti Add... Pod Source address odabratи My IP Address. Pod Destination Address odabratи Specified IP Subnet i upisati 192.168.0.1 za IP adress i 255.255.255.0 za Subnet Mask. Kliknuti OK tako da se dođe u IP Filter List izbornik.
- Ponovo u IP filter list kliknuti na Add... Pod Name upisati DI-824VUP+ to WinXP te kliknuti Add... Pod Source address odabratи Specified IP Subnet i upisati 192.168.0.1 za IP adress i 255.255.255.0 za Subnet Mask. Pod Destination Address odabratи My IP Address. Kliknuti OK tako da se dođe u IP Filter List izbornik.

Korak 3. U IP Filter list označiti WinXP to DI-824VUP+ te odabratи izbornik Filter Action, па Require Security te Edit... Odabratи Negotiate Security (u popisu protokola bi se trebao nalaziti protokol podešen na D-LINK-u: 3DES sa SHA-1) te označiti Accept unsecured communication but always respond using IPSec, te kliknuti na OK. Odabratи Authentication Methods te kliknuti Edit... Odabratи Use this string (preshared key) te unesti ključ 123456. (Za sigurnu upotrebu predlaže se korištenje kvalitetnijeg ključa nego što je opisano ovdje u primjeru ili upotreba certifikata). Odabratи OK Odabratи Tunnel Settings i odabratи The tunnel endpoint is specified by this IP address. Tu je potrebno upisati IP adresu od VPN servera. Iz Connection type odabratи All network connections pa odabratи Applyte OK.

Korak 4. U IPSec policy properties označiti Use Add Wizard i kliknuti na Add...

U IP Filter list označiti DI-824VUP+ to WinXP te odabratи izbornik Filter Action, па Require Security. Nakon toga odabratи Authentication Methods te kliknuti Edit... Odabratи Use this string (preshared key) te unesti ključ 123456. Odabratи OK Odabratи Tunnel Settings i odabratи The tunnel endpoint is specified by this IP address. Tu je potrebno upisati IP adresu od VPN klijenta. Iz Connection type odabratи All network connections pa odabratи Apply te OK Nakon toga zatvoriti IPSec Policy Properties prozor klikom na Close.

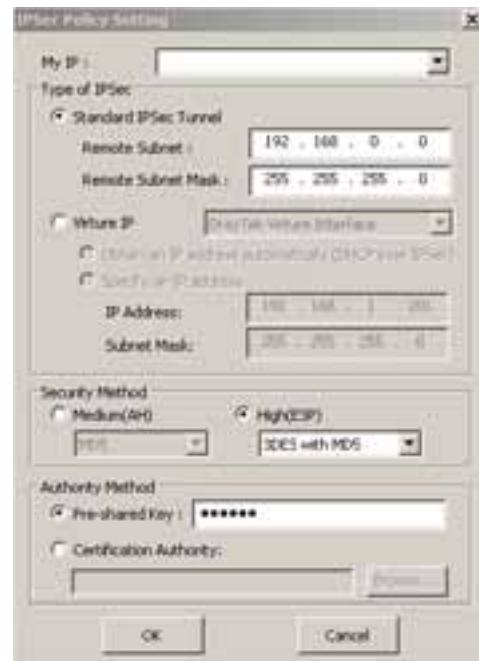
Nakon toga desnim klikom miša na IPSec Policy – VPN to DI-824VUP+ i odabriom na Assign novodefinirana IPSec politika postaje aktivna. To se može vidjeti i po zelenom znaku plus na ikoni od IPSec politike koju smo odabrali. Za uspostavu IPSec veze potrebno je poslati neki upit (npr. ping) D-LINK-u. To je detaljnije opisano u idućem poglavljju.

4.3.3.2. Korištenje Smart VPN Client-a

DrayTek Smart VPN Client je program koji će većinu podešavanja navedena u prethodnom poglavljju obaviti automatski.



Slika 4.17 Odabir tunela



Slika 4.18 Detaljne postavke PSec-a

Pod *VPN Server IP/HOST Name* se upisuje *DDNS Host Name* podešen u D-LNK-u: *hof505.dyndns.org*. Odaberemo naziv profila, obilježimo *IPSec Tunnel* te odaberemo *Use default gateway on remote network* i kliknemo na *OK*. Otvoriti će se prozor *IPSec Policy Settings*. U njemu će se pod *My IP* nalaziti IP adresa VPN klijenta kada je spojen na Internet. Pod *Standard IPSec Tunnel* treba pisati *192.168.0.0* za *Remote Subnet* i *255.255.255.0* za *Remote Subnet Mask*. Pod *SecurityMethod* treba bit označeno *High(ESP)* te *3DES with MD5* kao što je to i podešeno na D-LINK-u. U rubriku *Pre-shared Key* treba upisati *123456*. Kliknuti *OK* za kraj, te *Active* za uspostavljanje veze.

Nakon što su primijenjena pravila zadana za IPSec tunel u Smart VPN Clientu upaliti će se zelena lampica desno od oznake VPN, u donjem desnom dijelu prozora Smart VPN Client-a. S time IPSec veza još nije uspostavljena. Da bi uspostavili vezu potrebno je poslati neki upit VPN serveru. To se najjednostavnije učiniti naredbom *ping*:

C:\Documents and Settings>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Negotiating IP Security.

Negotiating IP Security.

Reply from 192.168.0.1: bytes=32 time=251ms TTL=64

Reply from 192.168.0.1: bytes=32 time=264ms TTL=64

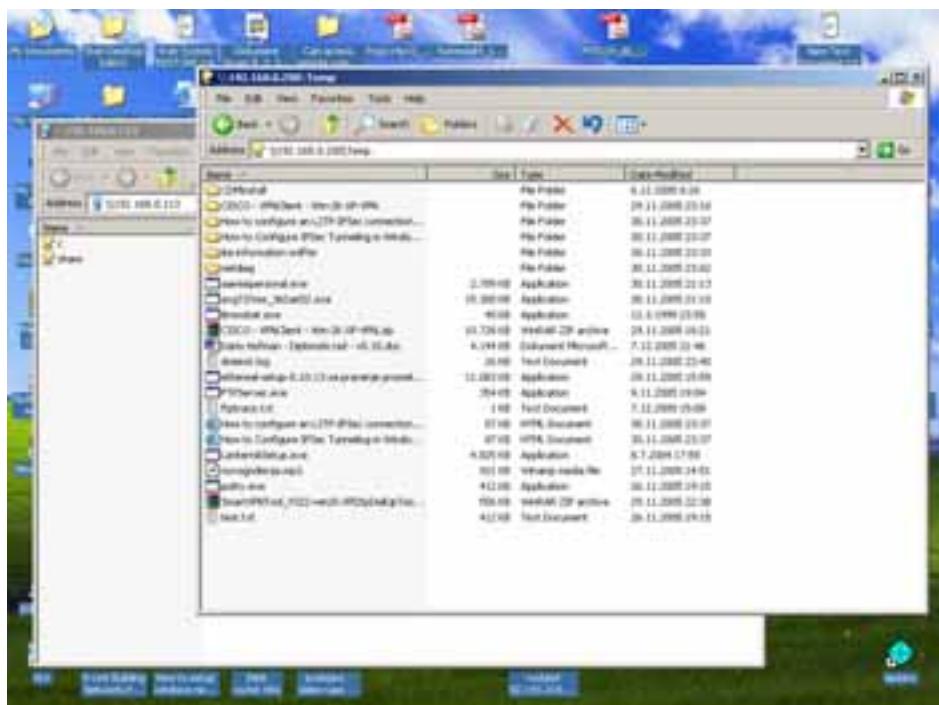
Ping statistics for 192.168.0.1:

Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),

Approximate round trip times in milli-seconds:

Minimum = 251ms, Maximum = 264ms, Average = 257ms

Može se vidjeti da se pri prvom i drugom pokušaju slanja *ping* paketa odvija međusobno dogovaranje (*Negotiating IP Security*) VPN klijenta i servera. Već kod trećeg pokušaja veza je uspostavljena (*Reply from 192.168.0.1...*).

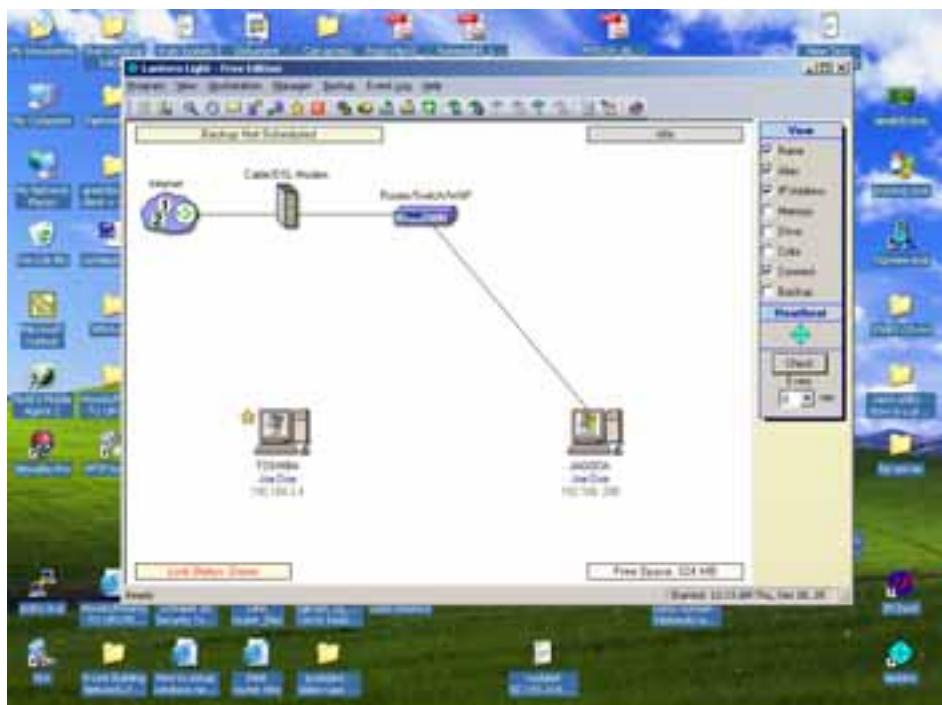


Slika 4.19 Korištenje mreže preko IP adresa

Korištenje FTP servera na računalu *Jagoda* radi bez problema. Jedino što ne radi je korištenje imena kompjutera oblika `\Jagoda` te *Microsoft Network*. Razlog tome je što protokol NetBIOS, kojeg koriste MS Windows za komuniciranje u lokalnoj mreži radi na 2. mrežnom sloju kao i Ipsec protokol.

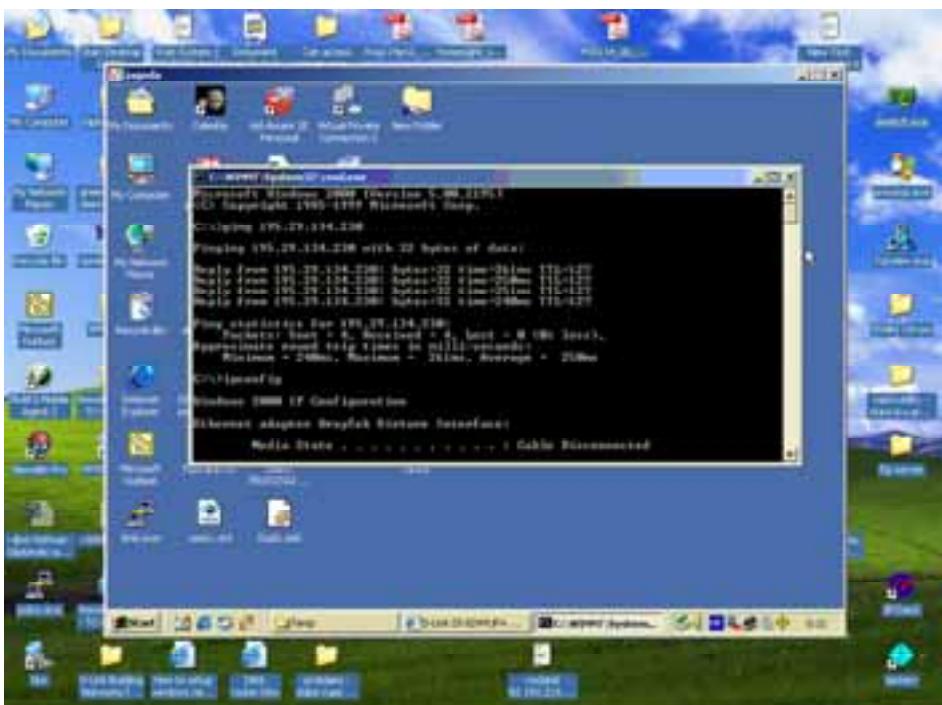
Jedno od rješenja tog problema je u implementaciji *NetBIOS broadcasta* što je izvedeno kod D-LINK-a, ali očito ne radi dobro niti sa Windowsima 2000, niti sa Windowsima 2000 SP3, niti sa Windowsima XP SP1. Pravilno se taj problem može riješiti podizanjem *MS domain controllera*. Također podizanje WINS servera (njegova svrha u lokalnoj mreži je kao i svrha DNS-a na Internetu) bi trebalo pomoći. Ako se u lokalnoj mreži koriste fiksne IP adrese u Windowsima se može napraviti LMHOSTS tablica u kojoj će se nalaziti popis svih računala sa lokalne mreže.

Što se tiče ostalih servisa oni su testirani, te rade kao i kod PPTP odnosno L2TP veze, bez ikakvih problema.



Slika 4.20 Program Lantern je normalno našao uređaje u mreži preko njihove IP adrese

Program Lantern Manager uspio je normalno naći računača spojena u mreži preko njihove IP adrese, ali klijentsko VPN računalo za njega je nevidljivo u toj mreži jer ono kao svoju virtualnu adresu u lokalnoj mreži ustvari koristi IP adresu koju je dobio prilikom spajanja na Internet.



Slika 4.21 Udaljeno upravljanje radi bez većih trzavica

Za testiranje IPSec veze korišten je i VNC, koji dolazi u sklopu programa Lantern, te se može reći da radi bez poteškoća i vrlo brzo računajući da je testiranje obavljeno na 56kbps modemu. Na slici 4.21 može se vidjeti da je na klijentu pokrenut VNC sa radnom površinom od računala Jagoda, te da je na računalu Jagoda, kroz VNC, pokrenuta naredba *ping* koja je slala *ping* upite na virtualnu IP adresu od klijenta u lokalnoj mreži. Sve to radi bez greške.

Razlike prije i poslije uspostave IPSec veze, što se tiče naredbe *route print*, nema budući da se IPSec ne miješa u *routing tablicu*.

C:\Documents and Settings\ruru>route print

Active Routes:

<i>Network Destination</i>	<i>Netmask</i>	<i>Gateway</i>	<i>Interface</i>	<i>Metric</i>
0.0.0.0	0.0.0.0	195.29.48.16	195.29.48.16	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
195.29.48.16	255.255.255.255	127.0.0.1	127.0.0.1	50
195.29.48.241	255.255.255.255	195.29.48.16	195.29.48.16	1
195.29.48.255	255.255.255.255	195.29.48.16	195.29.48.16	50
224.0.0.0	240.0.0.0	195.29.48.16	195.29.48.16	1
<i>Default Gateway:</i> 195.29.48.16				

4.3.3.3. Korištenje TheGreenBow VPN Client-a

Od korištenih VPN klijentskih programa Sistech-ov TheGreenBow VPN Client je jedini program koji se plaća za uporabu. On je drugačiji od gore navedenih programa/postupaka uspostave PSec veze po tome što ne koristi Windows s-ove rutine za uspostavu PSec veze, nego svoje vlastite (Cisco i mogi drugi također koriste vlastite servise). Upravo iz toga moguće ga je koristiti na bilo kojoj Windows s platformi. Također je zanimljivo Sistech-ovo rješenje da se tajne informacije za uspostavu veze pohranjuju na *USB stick* te su na taj način skriveni od potencijalnih napadača. Prilikom ukopčavanja *USB sticka* VPN veza se može automatski ostvariti.



Slika 4.22 Postavke za prvu i drugu fazu za uspostavu IPSec tunela

Postavke za IPSec vezu su prikazane na slici 4.22. Nakon uspostave veze pod opcijama *Connections* se može vidjeti da li je veza uspostavljena, te koji se algoritmi koriste. TheGreenBow VPN Client ima mogućnost dodjeljivanja proizvoljne virtualne IP adrese za IPSec klijenta. Ta adresa, radi ograničenja D-LINK-a, ne smije biti unutar spektra lokalne poddomene (Cisco takve stvari dopušta).

4.4. Testiranje veličine paketa zapakiranih PPTP, L2TP i IPSec protokolom

	PPTP		L2TP		IPSec
	Internet	Virtualna mreža	Internet	Virtualna mreža	Internet
IP adresa adaptera	83.131.123.7	192.168.2.2	195.29.134.195	10.0.1.2	83.131.123.182
Primljeno podataka	2.045.157	1.972.429	2.038.883	1.974.589	2.056.912
Poslano podataka	188.726	81.216	147.375	82.797	185.663

Tablica 4.4 Količina podataka prenesena Internetom da bi se prenijela testna datoteka

Kako bi usporedio sva tri protokola, koristio sam binarnu testnu datoteku veličine 1.822.520 bajta. Ovaj put rezultati su bili precizniji jer je prenesena veća količina podataka. Mjerenja su ponavljana još jednom kako bi se dobili točniji rezultati, te je uzeta srednja vrijednost mjerenja. L2TP promet je opet ispašao manji za oko 2% u odnosu na PPTP protokola, a IPSec je također koristio TCP/IP protokol, a ne UDP pa je zato po rezultatima sličniji PPTP-u nego UDP-u.

4.5. Najčešći problemi i korisne naredbe

Browsing server [5]

Browsing server je kompjuter koji u MS Windows mreži daje listu radnih grupa i servera u toj radnoj grupi (workgroup). Jedan kompjuter na mreži je glavni *browsing server* te on može imati i rezervne (backup) servere. Računala spojena na domenu ne mogu biti *browsing server*. Da bi radio ovaj servis u Windowsima treba biti uključen *File and Printer Sharing for Microsoft Networks*. U Windowsima XP se može provjeriti da li sve radi na sljedeći način:

Korak 1. Odabratи Start → Help and Support

Korak 2. Pod Pick a Help Topic odabratи Networking and the Web

Korak 3. Pod Networking and the Web odabratи Fixing networking or Web problems

Korak 4. Pod Pick a task odabratи Diagnose network configuration and run automated networking tests.

Korak 5. Pod Network Diagnostics odabratи Scan your system.

Ako pod nekim od rezultata piše *FAILED* to znači da to možda uzrokuje grešku.

Za provjeru da li je servis za *browsing server* startan u Windowsima:

Korak 1. Odabrat *Start* → *Control Panel* → *Performance and Maintenance* → *Administrative Tools* → *Services*.

Korak 2. Napraviti dvostruki klik na *Computer Browser service*.

Startup type bi trebao biti podešen na *Automatic*, a za *Service status* bi trebalo pisati *Started*.

Ispis informacija o trenutnom *browsing server*-u na mreži može se dobiti pomoću naredbe *browstat* sta. Da bi se ta naredba koristila potrebno je sa Windows instalacijskog CD-a instalirati Brow stat.exe koji se nalazi u Support\Tools direktoriju.

Informacije o mrežnom /Dial-up adapteru

Za prikupljanje informacija o vlastitoj IP adresi, usmjerivaču koristi se naredba *ipconfig*.

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

<i>Connection-specific DNS Suffix</i>	: Komteh
<i>IP Address</i>	: 192.168.0.182
<i>Subnet Mask</i>	: 255.255.255.0
<i>Default Gateway</i>	: 192.168.0.1

Ako se traže opšimiji opis (npr. da li je *NetBIOS over TCP/IP* uključen) treba koristiti naredbu *ipconfig* sa prekidačem */all*. Za tu naredbu u radnoj grupi sa NT Serverom 4.0 ispis je slijedeći:

C:\Documents and Settings>ipconfig /all

Windows IP Configuration

<i>Host Name</i>	: Toshiba
<i>Primary Dns Suffix</i>	:
<i>Node Type</i>	: Unknown
<i>IP Routing Enabled</i>	: No
<i>WINS Proxy Enabled</i>	: No

Ethernet adapter Local Area Connection 3:

<i>Connection-specific DNS Suffix</i>	: Komteh
<i>Description</i>	: D-Link DFE-680TXD-Based CardBus Fast

Ethernet Adapter #2

<i>Physical Address</i>	: 00-E0-98-98-FB-D3
<i>Dhcp Enabled</i>	: Yes
<i>Autoconfiguration Enabled</i>	: Yes
<i>IP Address</i>	: 192.168.0.182
<i>Subnet Mask</i>	: 255.255.255.0
<i>Default Gateway</i>	: 192.168.0.1
<i>DHCP Server</i>	: 192.168.0.2
<i>DNS Servers</i>	: 192.168.0.1
<i>Lease Obtained</i>	: 11. prosinac 2005 19:24:04
<i>Lease Expires</i>	: 14. prosinac 2005 19:24:04

Naredba NET

Naredba *net* ima mnoge prekidače od kojih su za ovu radnju najzanimljiviji prekidač *view* te prekidač *use*. Naredba *net view* prikazati će nam sve vidljive kompjutere na našoj mreži. Naredba *net use* se može koristiti za pridjeljivanje nekog mrežnog direktorija nekom nazivu diskovnog pogona na lokalnom kompjuteru. To je praktično iz razloga jer se naredba *net* može pokretati i iz *.bat* datoteke koja se može ručno pokretati kada želimo koristiti neke mrežne resurse (npr. prilikom upotrebe VPN-a).

Naredba IPSECCMD

Naredba čija je svrha konfiguriranje IPSec politike. Radi isto što i *Local Security Policy* samo iz *command prompt*-a.

Naredba NBTSTAT

Naredba koja ispisuje informacije o *NetBIOS over TCP/IP (NetBT)* protokolu. Najkorisniji prekidači za ispitivanje VPN-a su: *-c, -n, -R*.

Naredba ROUTE i PING

Ove dvije naredbe objašnjene su ranije u tekstu. Pomoću naredbe *route* može se uočiti kada se zaboravi isključiti mrežnu karticu (koju se koristi u poduzeću), te zbog toga promet ne ide preko Dial-up-a nego preko mrežne. Naredba *ping* nam koristi za provjeru da li je VPN veza uspostavljena, te za iniciranje IPSec veze.

Upotreba Windows Network Service-a - WINS-a

WINS služi za razrješavanje kompjuterskih imena u IP adresu. On može također konvertirati NetBIOS naziv u IP adresu. Osim Microsoftovog rješenja za WINS server može se koristiti i Samba na Linux operativnom sustavu. Problemi sa D-LINK-om da bi razrješavanje imena radio kod IPSec-a trebalo bi konfigurirati DNS, WINS ili LMHOSTS (izvor: <http://www.chicagotech.net/dlinkrouter.htm>).

IPSec NAT (Network Address Translator) Traversal

IPSec mreže ne mogu biti smještene iza NAT uređaja. Većina malih uređaja koristi NAT kako bi djelila jednu Internetsku IP adresu, koju je dobila od ISP-a, sa cijelom lokalnom mrežom. Bib što NAT omogućuje u štednji preostalog svjetskog IP adresnog prostora, on prouzrokuje probleme protokolima poput IPSec koji koriste komunikaciju krajnjih točaka. Upravo zbog toga propisana nova tehnologija nazvana *IPSec NAT Traversal* – NAT-T (RFC 3947 i RFC 3948). Ona bi trebala rješiti taj problem. Kako bi NAT-T radio u MS Windows 2000 potrebno je instalirati SP3, a za MS Windows XP je potreban SP2 [7].

Korisne Internet stranice vezane uz rješavanje VPN problem a

Internet stranice koje imaju mnoštvo odgovora za najčešće probleme koji nastaju prilikom stvaranja VPN sustava:

- <http://www.microsoft.com/windows2000/techinfo/howto/networks/communications/remoteaccess/l2tpclientfaq.asp>
- <http://www.chicagotech.net/vpnindex.htm>
- <http://www.howtonetworking.com/sitemap.htm>

4.6. Konačno razmatranje – PPTP protiv L2TP/IPSec

Prednosti L2TP/IPSec-a nad PPTP-om :

Šifriranje kod IPSec-a je jače nego PPTP-a. PPTP koristi MPPE za šifriranje podataka, dok L2TP/IPSec koristi DES (odnosno 3DES).

PPTP zahtjeva autentifikaciju samo na razini korisnika, dok L2TP/IPSec zahtjeva istu autentifikaciju na razini korisnika i još autentifikaciju računa koju obavlja pomoću certifikata. To znači da je L2TP/IPSec sigurniji.

IPSec omogućuje nepromjenjivost ishodišta podataka (dokaz da su podaci poslati od autoriziranog korisnika), integritet podataka (dokaz da podaci nisu mijenjani na svom putu) i tajnost podataka (nitičko ne može čitati podatke koji su poslati bez poznavanja tajnog ključa). PPTP omogućuje samo tajnost podataka.

L2TP je brži od PPTP, odnosno njegovi paketi zauzimaju manje budući da on koristi UDP, a ne TCP.

Prednosti PPTP-a nad L2TP/IPSec-om :

Za implementaciju IPSec protokola potrebno je koristiti certifikate, dok se PPTP veza može uspostaviti sa dogovorenim ključevima.

IPSec ima problema sa NAT-om, što je riješeno novom tehnologijom nazvanom NAT Traversal. Ipak neki tvrde da to nije najbolje rješenje za taj problem.

SSL kao alternativno rješenje:

U zadnje vrijeme se podosta koristi i SSL kao mogući protokol za uspostavu VPN-a. On radi na četvrtom mrežnom sloju. Za korištenje ne treba klijentski softver – on koristi Internet preglednik kao klijentsku aplikaciju. To mu je velika prednost nad VPN protokolima koji rade na nižoj razini. Ali to znači da on nema direktni pristup lokalnoj mreži već je ograničen na određene programe. To može s jedne strane biti mana (nema pristup cijeloj mreži), a sa druge strane predhost (nema pristup cijeloj mreži).

5. ZAKLJUČAK

Svaka radna grupa ima svoje specifične želje i potrebe što se tiče sigurnosti i treba biti razmatrana pojedinačno. Zbog toga je ova radnja ograničena na pronašetak najboljeg mogućeg načina, s obzirom na sigurnost i jednostavnost implementacije, za uspostavu VPN komunikacije između klijenta i malog lokalnog uređaja.

Najbolje rješenje su VPN serveri koji podržavaju L2TP/IPSec protokol, certifikate i dovoljno jake algoritme, te koji su dobro podešeni. Ipak za manja poduzeća biti će dovoljan i PPTP protokol ako se koristi sa dovoljno sigurnim algoritmima (trenutno su to: 3DES, ESP, SHA-1 umjesto DES, AH i MD5), te sa prihvatljivom šifrom - šifrom koja nije nigdje zapisana, a dovoljno je jaka (minimalno 8 znakova, koji uključuju brojke, slova i posebne znakove). PPTP je namijenjen baš za poduzeća čija je OS platforma MS Windows, a čiji klijenti koriste modemsku vezu.

Prema statistici preko 80% napada na sigurnost mreže se događa unutar lokalne mreže. Dakle treba voditi brigu o zaštiti lokalne mreže iznutra (to se može izvesti također IPSec-om), te na zaštitu od napada izvana – vatrozidom i od virusa - antivirusnim softverom.

Protokoli poredani po svojoj kvaliteti: L2TP/IPSec, IPSec, L2TP, PPTP. Treba težiti što sigurnijem protokolu, ali svakako treba obratiti pozornost na obranu od ostalih potencijalnih povreda sigurnosti mreže.

Dodatak A: Popis IETF standarda i prijedloga

RFC	Opis	Datum
2401	Security Architecture for the Internet Protocol	11 / 1998
2402	IP Authentication Header	11 / 1998
2406	IP Encapsulating Security Payload (ESP)	11 / 1998
2407	The Internet IP Security Domain of Interpretation for ISAKMP	11 / 1998
2408	Internet Security Association and Key Management Protocol (ISAKMP)	11 / 1998
2409	The Internet Key Exchange (IKE)	11 / 1998
2412	The OAKLEY Key Determination Protocol	11 / 1998
2661	Layer Two Tunneling Protocol L2TP	08 / 1999
2808	Secure Remote Access with L2TP	04 / 2000
2888	Securing L2TP using IPsec	08 / 2000
3145	L2TP Disconnect Cause Information	07 / 2001
3193	Securing L2TP using IPsec	11 / 2001
3456	Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode	01 / 2003
3457	Requirements for IPsec Remote Access Scenarios	01 / 2003
3715	IPsec-Network Address Translation (NAT) Compatibility Requirements	03 / 2004
3948	UDP Encapsulation of IPsec ESP Packets	01 / 2005
3931	Layer Two Tunneling Protocol - Version 3 (L2TPv3)	03 / 2005
4109	Algorithms for Internet Key Exchange version 1 (IKEv1)	05 / 2005 (nadopuna za RFC 2409)

Gore su navedeni neki od važnijih standarda vezanih uz IPsec i L2TP protokole.

Dodatak B: Rječnik

Aggressive mode (agresivan način)

Ako je kod uspostave VPN veze uključena ova opcija na obje strane, onda će se u prvoj fazi prilikom uspostavljanja SA razmjeniti ključevi u tri umjesto u standardnih šest koraka. Zbog nekih sigurnosnih nedostataka predlaže se ne koristiti taj način prilikom uspostave veze.

Authentication (provjera vjerodostojnosti, autentifikacija)

U kriptografiji je to način osiguravanja da podaci zabilja stižu sa mjesta od kojeg tvrde da stižu.

Authentication Header – AH (zaglavje za provjeru vjerodostojnosti)

UIPSec protokolu AH zaglavje osigurava da tijelo paketa ne bude promjenjeno.

Certificate Authority – CA (tijelo sa ovlastima za izdavanje certifikata)

Tijelo koje izdaje certifikat za upotrebu u IPSec protokolu.

Challenge Handshake Authentication Protocol (CHAP)

Protokol koji služi za autentifikaciju udaljenih korisnika.

Com pulsory tunnel (obvezni tunel)

Tunel stvoren bez specijalnog odobrenja krajnjeg korisnika. Klijentska strana se prilikom uspostave veze automatski spaja preko RAS servera na mrežu.

Data Encryption Standard (DES)

Standard za šifriranje podataka. Napravio ga je IBM, a potvrđen je od strane Američke vlade 1977 godine. Koristi 56-bitni ključ koji se primjenjuje na blokovima od 64 bita.

Diffie-Hellman

Sustav dizajniran da dozvoli dvojici pojedinaca da se dogovore oko dijeljenog ključa na siguran način bilo što poruke razmjenjuju samo kroz javnu mrežu.

Digital Certificate (digitalni certifikat)

Elektronski dokument stvoren od strane CA, koji je namijenjen da potvrdi identitet tvrtke pomoću svog javnog ključa.

Domain Name Services (DNS)

Mrežni servis zadužen za pretvaranje numeričkih adresa u tekstualne adrese i obrnuto.

Encapsulating Security Payload (ESP)

UIPSec-u, IP zaglavje koje sadrži šifrirani sadržaj IP paketa.

Encapsulation (učahurivanje, omatanje podataka)

Postupak stavljanja podataka iz jedne mreže u pakete koji putuju drugom mrežom.

Encryption (šifriranje, enkripcija)

Pretvaranje čitkog (nekriptiranog) teksta pomoću nekog od algoritama za šifriranje u šifrirani tekst.

Internet Engineering Task Force - IETF

Svjetska organizacija za propisivanje standarda vezanih uz Internet i nove tehnologije.

Internet Key Exchange – IKE

Protokol za upravljanje ključevima koji se koristi u IPSec protokolu.

Internet Service Provider – ISP (davatelj Internet usluge)

Tvrka koja pruža usluge Internet-a privatnim korisnicima i tvrtkama.

IPSec

Mrežni protokol za šifriranje podataka. Radi na trećem mrežnom slobu.

ISAKMP

Protokol za upravljanje ključevima prihvaćen za upotrebu sa IPSec-om. Sada zajedno sa Oakley-em formira IKE protokol.

Layer2 Forwarding – L2F

Protokol za tuneliranje kojeg je razvio Cisco.

Layer2 Tunneling Protocol - L2TP

Protokol za tuneliranje koji sadrži mnoge prednosti L2F i PPTP protokola. On koristi IPSec za šifriranje, te se najčešće kad se misli na L2TP ustvari misli na L2TP/IPSec protokol.

Network Address Translation – NAT (prevođenje mrežnih adresa)

Postupak pretvaranja privatne IP adrese koja se koristi na lokalnoj mreži u adresu koja se onda koristi u infrastrukturi Interneta.

NetBIOS

To ustvari nije protokol već set komandi (API) koje se koriste za kreiranje, održavanje i upotrebu veze između računala koja koriste Microsoftove operativne sisteme.

Oakley

Protokol za izmjenu ključeva koji se koristi u IPSec-u kao dio IKE protokola.

Password Authentication Protocol - PAP

Jednostavan protokol koji koristi šifre za autentifikaciju. Budući da se šifre šalju kao čisti tekst, one nisu zaštićene.

Point to Point Tunneling Protocol - PPTP

Protokol za tuneliranje razvijen od strane Ascenda i Microsofta.

Public Key Certificate

Specijalno formirani blok podataka koji sadrži vrijednosti javnog ključa, ime vlasnika javnog ključa te digitalni potpis organizacije koja je izdala taj javni ključ. Ti certifikati se koriste da bi se identificirao vlasnik pojedinog javnog ključa.

Public Switched Telephone Network - PSTN

Općeniti naziv za javnu telefonsku mrežu. Tu se misli na analognu telefonsku mrežu namijenjenu za prijenos glasa. Tu ne pripadaju digitalne telefonske mreže poput ISDN-a.

Remote user (udaljeni korisnik)

U slučaju VPN veza, naziv za korisnika koji se spaja sa svog računala, spojenog na Internet, na lokalnu mrežu u tvrtci gdje radi.

Secure Sockets Layer - SSL

Protokol koji je prvenstveno bio namijenjen za sigurnu komunikaciju između Internet preglednika i servera. On omogućuje autentifikaciju, povjerljivost podataka i integritet. Radi na 4-tom mrežnom sloju, te postaje sve popularniji, radi jednostavnosti implementacije, u sigurnoj komunikaciji u slučajevima kada imamo pristup zaštićenoj mreži sa udaljenih računala.

Triple DES – 3DES

Algoritam za šifriranje podataka, koji podatke šifrira koristeći DES algoritam tri puta sa dva ili tri različita ključa.

Wide Area Network - WAN

Mrežno okruženje u kojem su elementi prilično udaljeni geografski gledano. Računala spojena na WAN su često spojena preko javne mreže, poput telefonske mreže. Na WAN računala također mogu biti spojena preko iznajmljenih vodova ili satelita. Najveći WAN koji trenutno postoji je Internet.

LITERATURA

knjiga:

- [1] Dave Kosiur , *Building and Managing Virtual Private Networks*, Wiley Computer Publishing, John Wiley & Sons, Inc., 1998.

elektronička-knjiga/publikacija:

- [2] Check Point Software Technologies Ltd., *CheckPoint™ Virtual Private Networks – Check Point 2000 Service Pack 2*, 2000., www.checkpoint.com
- [3] Martin W. Murhammer, *IBM – VPN overview*, IBM Corporation, 1999.
- [4] Microsoft, *Virtual Private Networking in Windows 2000: An Overview(White Paper)*, 2001, <http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remoteaccess/vpnoverview.asp>
- [5] Microsoft, *Troubleshooting Computer Browsing on SOHO Networks with Microsoft Windows*, god. izdanja: 2004, <http://www.microsoft.com/downloads/details.aspx?familyid=BB89501A-3609-45DE-8E35-38251E1349F6>

Internet:

- [6] http://www.schneier.com/blog/archives/2005/02/sha1_broken.html
- [7] <http://www.microsoft.com/technet/community/columns/cableguy/cg0802.mspx>
- [8] <http://www.dlink.com/products/?pid=274>
- [9] <http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp>

SAŽETAK

Tema ove radnje je realizacija VPN sustava koji bi omogućio zaposlenicima u nekom poduzeću udaljeni pristup svojoj lokalnoj mreži u tom poduzeću (*client-to-server* slučaj). Kako je uspostava VPN-a moguća u raznim kombinacijama i sa raznim protokolima za uspostavu VPN-a u ovoj radnji korišteni su sljedeći protokoli: PPTP, L2TP i PSec. Područja koja ova radnja ne obrađuje je uspostava VPN-a pomoću SSL-a te uspostava VPN-a između dvije ili više lokalnih mreža (*server-to-server* slučaj). Glavna područja obrađena u ovoj radnji su: osnove šifriranja, osnove VPN protokola, podešavanje VPN servera te podešavanje VPN klijenta te uspostava i testiranje VPN veze.