Kreiranje mobilne virtualne privatne mreže

Radoš, Ante

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni studij

KREIRANJE MOBILNE VIRTUALNE PRIVATNE MREŽE

Završni rad

Ante Radoš

Osijek, 2018.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju

Osijek, 14.09.2018.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada

Ime i prezime studenta:	Ante Radoš
Studij, smjer:	Preddiplomski sveučilišni studij Elektrotehnika i informacijska tehnologija
Mat. br. studenta, godina upisa:	4118, 29.09.2017.
OIB studenta:	76010933713
Mentor:	Doc. dr. sc. Višnja Križanović
Sumentor:	
Sumentor iz tvrtke:	
Naslov završnog rada:	Kreiranje mobilne virtualne privatne mreže
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Predložena ocjena završnog rada:	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 3 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 3 bod/boda Jasnoća pismenog izražavanja: 3 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene mentora:	14.09.2018.
Datum potvrde ocjene Odbora:	26.09.2018.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 27.09.2018.

Ime i prezime studenta:	Ante Radoš
Studij:	Preddiplomski sveučilišni studij Elektrotehnika i informacijska tehnologija
Mat. br. studenta, godina upisa:	4118, 29.09.2017.
Ephorus podudaranje [%]:	3%

Ovom izjavom izjavljujem da je rad pod nazivom**: Kreiranje mobilne virtualne privatne mreže**

izrađen pod vodstvom mentora Doc. dr. sc. Višnja Križanović

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SADRŽAJ

1. UVOD

Javne komunikacijske mreže su u kratkom vremenu postale osnovni oblik komunikacije u svijetu. Privatni i poslovni subjekti koriste Internet i slične mreže svakodnevno, u razne svrhe. Problem nastaje kada podaci koji putuju mrežom nisu adekvatno zaštićeni, jer u takvim slučajevima može doći do neželjenih posljedica, poput neovlaštenog pristupa podacima. Iz tog razloga su nastale virtualne privatne mreže, poznatije kao VPN-ovi, kao način da se osigura prijenos osjetljivih podataka preko javne mreže. Nadalje, razvojem novih tehnologija i konstantnim porastom broja korisnika, došlo je do potrebe i za mobilnim oblicima VPN-ova. U ovom radu objašnjene su osnovne značajke takvih mreža, njihove vrste i protokoli koji se danas najčešće primjenjuju. Također, ukratko su opisani i neki dodatni sigurnosni mehanizmi koji se primjenjuju u računalnim mrežama, a ne spadaju u klasičnu definiciju VPN-ova. Praktični dio sastoji se od opisa postupka kreiranja jedne takve jednostavne mreže, korak po korak, koristeći jedan od softvera za postavljanje virtualnih privatnih mreža. Osim toga, u praktičnom dijelu je ta ista mreža testirana odgovarajućim softverom.

1.1. Zadatak završnog rada

U radu je potrebno opisati postupak uspostavljanja virtualne privatne mreže (*Virtual Private Network*, VPN) te usporediti postojeća rješenja. Praktični dio rada obuhvaća postupak konfiguriranja VPN poslužitelja i mobilnih VPN klijenata te testiranje komunikacije u odabranom mobilnom VPN scenariju.

2. VIRTUALNE PRIVATNE MREŽE (VPN)

2.1. Osnovne značajke virtualnih privatnih mreža

VPN (*Virtual private network*) je skraćeni naziv za virtualne privatne mreže. Svrha takvih mreža je siguran prijenos podataka preko dijeljene ili javne komunikacijske mreže (Internet, ATM, ...), na način da su podaci dostupni samo stranama kojima su namijenjeni [1]. To se može postići kreiranjem posebnih veza, takozvanih tunela, koji čine direktnu sigurnu vezu između računala koja imaju pristup VPN-u. Pristup VPN-u se postiže putem odgovarajućih metoda identifikacije i autentifikacije, poput lozinki, tokena i sl., čime se osigurava da pristup mreži imaju samo ovlašteni korisnici. Poopćeno, VPN predstavlja proširenje privatne mreže, gdje se korisnici mogu promatrati kao da su spojeni na istu lokalnu ili privatnu mrežu, što znači postoji slična razina sigurnosti i povjerenja među uključenim stranama. Ono što VPN radi, je da stvara sigurnu vezu između strana koje razmjenjuju podatke, koristeći enkripciju i metode provjere korisnika kako bi osigurao zaštićenost podataka koji se prenose komunikacijskim kanalom, a to se osigurava korištenjem posebnih protokola za tuneliranje i enkripciju. VPN je popularno rješenje za problem sigurne komunikacije jer su alternativna rješenja često neusporedivo skuplja, kao primjerice izgradnja vlastite fizičke komunikacijske infrastrukture (WAN), a uz to je i puno fleksibilniji (mobilnost korisnika). Dva osnovna topološka oblika VPN mreža su udaljeni pristup (*remote-access*) i točka-do-točke (*site-to-site*). Kod *remote-access* oblika povezivanja, korisnik se povezuje na udaljeni server pomoću VPN softvera koji stvara siguran tunel za prijenos podataka. *Site-to-site* oblik povezivanja se najčeše koristi za veći broj korisnika, npr. u organizacijama sa udaljenim odjelima, no u ovom slučaju su korisnici najčešće povezani na intranet, koji je zatim sigurnom vezom povezan s intranetom na drugoj lokaciji, te se tako svim korisnicima omogućuje sigurno dijeljenje podataka, bez obzira na njihovu fizičku udaljenost.

2.2. Mobilne virtualne privatne mreže

Pojavom mobilnih uređaja i bežičnog povezivanja na mrežu te konstantnim porastom broja korisnika mrežnih tehnologija došlo je do potrebe za novijim vrstama virtualnih privatnih mreža [2]. Također, Internet je postao dominantni medij za komunikaciju, kako privatnu tako i poslovnu. Mobilno okruženje sa sobom je donijelo drugačije uvjete od onih na „statičnim“ uređajima. Prvenstveno, pojavio se problem prekida trenutnih sesija prelaskom sa jedne mreže na drugu. To znači da se prekida i sigurna veza ukoliko je korisnik spojen na virtualnu privatnu mrežu, te se on ponovno mora spajati na nju nakon svakog prekida. Klasični VPN-ovi nisu se

mogli nositi s tim problemom, pa su razvijeni mobilni VPN-ovi koji su u mogućnosti nositi se sa novonastalim zahtjevima. Dakle, glavna značajka mobilnih VPN-ova je sposobnost da obavljaju prebacivanje s mreže na mrežu zajedno sa svim popratnim radnjama (autorizacija, prijava, odjava,…) bez primjetnih smetnji za krajnjeg korisnika. Također, mobilni VPN sustavi trebaju biti optimizirani sukladno promjenjivim zahtjevima kao što su: konstantno mijenjanje broja korisnika (skalabilnost), kretanje korisnika, što manja potrošnja resursa (procesora, baterije,…) itd.

2.3. Primjena koncepta tuneliranja

Tuneliranje je tehnika prijenosa podataka namijenjenih jednoj mreži preko neke druge mreže. Podaci koji se šalju mogu biti okviri (ili paketi) nekog drugog protokola. Protokol kojim se implementira tuneliranje enkapsulira originalni okvir u posebno oblikovano zaglavlje. U tom zaglavlju se nalaze podaci potrebni za prijenos paketa preko željene mreže. Tunel je logički put kroz koji prethodno enkapsulirani podaci prolaze kroz mrežu na putu do odredišta. Kada enkapsulirani podatak dosegne odredište, podaci se ekstrahiraju te se šalju do krajnjeg odredišta u privatnoj mreži [3]. Proces tuneliranja obuhvaća postupke enkapsulacije, prijenosa i ekstrakcije. VPN mreže se oslanjaju na princip tuneliranja za siguran prijenos podataka do odredišta preko nezaštićene mreže.

2.4. Primjena enkripcije

Enkripcija je proces šifriranja podataka sa ciljem da informaciju koja se prenosi mogu pročitati samo subjekti koji znaju ključ za dešifriranje odnosno oni kojima je informacija zapravo namijenjena. U VPN sustavima enkripcijom se osigurava zaštita podataka od neovlaštenog čitanja ili izmjena. Najčešće se koriste metode simetrične i asimetrične enkripcije. Metoda simetrične enkripcije zasniva se na jednom tajnom ključu kojeg moraju posjedovati sve strane koje sudjeluju u komunikaciji, jer se on koristi i za šifriranje i za dešifriranje. Problem ove metode je da dolaskom ključa u posjed strane kojoj nije namijenjen, ona može dešifrirati sve podatke koji su enkriptirani tim ključem. Iz tog razloga je preporučljivo često mijenjati tajni ključ, gdje dodatan problem stvara činjenica da je tajni ključ često najranjiviji kod njegove promjene, odnosno razmjene među ovlaštenim stranama. Metoda asimetrične enkripcije je nešto kompliciranija ali i sigurnija, jer podrazumijeva da svaki korisnik ima svoj javni i tajni ključ. Podatak enkriptiran javnim ključem moguće je dekriptirati samo pomoću njemu pripadajućeg tajnog ključa [4]. Tako pošiljatelj, nakon što sazna javni ključ primatelja, pomoću njega šifrira

podatke te ih zatim šalje primatelju koji ih dešifrira uz pomoć svog tajnog ključa. Velika prednost ove metode je upravo u činjenici da tajni ključ zna samo strana koja mora dešifrirati podatke, i taj ključ ne mora dijeliti ni sa jednom drugom stranom.

2.5. VPN protokoli

Kako postoje razne vrste VPN-ova, tako postoje i njihova različita tehnološka rješenja, pri čemu važnu ulogu imaju komunikacijski protokoli. Protokoli su skupovi pravila i standarda koji se koriste u komunikaciji putem računalnih mreža. U kontekstu VPN-a, glavna uloga protokola je pružanje sigurnosti i brzine prijenosa podataka, te oni time čine središnji dio VPN rješenja. Način na koji podaci putuju kroz mrežu ovisi o odabiru protokola, pri čemu protokoli imaju različite načine djelovanja sa drugačijim krajnjim rezultatima, pa tako neki protokoli prioritiziraju brzinu, dok je kod drugih poboljšana sigurnost, i sl. Glavni protokoli potrebni za realizaciju VPN-a su protokoli za tuneliranje i enkripcijski protokoli. U praksi se koriste i kombinacije više različitih protokola od kojih svaki ima određenu ulogu, a sve u svrhu postizanja željenog rezultata, odnosno kreiranja VPN-a koji najbolje odgovara potrebama korisnika.

2.5.1. PPTP (*Point-to-Point Tunneling protocol*)

PPTP je jedan od najstarijih VPN protokola, nastao 1995. godine. Zasniva se na PPP (*Point-to-point*) protokolu, na način da se GRE (*Generic Routing Encapsulation*) protokolom enkapsuliraju PPP paketi tj. okviri koji se zatim tuneliraju do odredišta [5]. Sa gledišta sigurnosti i privatnosti, autentikacijski protokoli i manjkavi načini šifriranja koje koristi davno su proglašeni nedovoljno sigurnima i prešlo se na sigurnije protokole. Ipak, i dalje se koristi upravo iz razloga što smanjena sigurnost omogućuje veću brzinu prijenosa podataka. Zbog toga se koristi primjerice za zaobilaženje geografskih zapreka (npr. ograničenja pristupa sadržajima ovisno o fizičkoj lokaciji korisnika), pri čemu je pribavljanje sadržaja često važnije od sigurnosti veze, te za slanje/preuzimanje audio i video sadržaja u realnom vremenu *(streaming*).

2.5.2. L2TP/IPSec (*Layer 2 Tunneling Protocol/Internet Protocol Security*)

Ovo je zapravo kombinacija dvaju protokola, kojom je dobiven jedan od najsigurnijih i najčešće korištenih načina uspostave VPN veze. L2TP protokol je svojevrsni nasljednik PPTP i L2F (*Layer 2 Forwarding*) protokola, i sam po sebi on ne pruža enkripciju ni privatnost već samo stvara „tunel“ između povezanih strana. Tim se tunelom, kao i kod PPTP-a, prenose PPP podatkovni okviri. Zbog slabe sigurnosti, L2TP se kombinira sa IPSec protokolom koji koristi dva načina enkripcije podataka. On enkriptira poruku koja se šalje unutar paketa, kao i sami

podatkovni paket, no zbog te dvostruke enkripcije tj. enkapsulacije podataka, smanjena je brzina prijenosa.

2.5.3. SSTP (*Secure Socket Tunneling Protocol*)

Tunelski protokol koji omogućuje prijenos PPP ili L2TP prometa kroz SSL/TLS kanal. SSTP je protokol koji se smatra jako sigurnim zbog jake enkripcije (zaštitna sekvenca duljine 2048 bita). Korištenjem SSL/TLS protokola na TCP portu 443, uspijeva zaobići gotovo sve vatrozide i proxy servere. Uz to, koristi se HTTPS protokolom koji je danas u širokoj upotrebi, pa ga zbog toga većina vatrozida i *proxy* servera ne blokira. Vlasništvo je *Microsoft*-a, i kao takav nije dostupan na konkurentskim operativnim sustavima, no ima ugrađenu podršku na *Windows* operacijskim sustavima pa je samim time poprilično zastupljen u praksi.

2.5.4. SSL/TLS (*Secure Sockets Layer/Transport Layer Security*)

SSL je najšire korišteni kriptografski protokol kojeg je 1999. naslijedio TLS. Osnova protokola je ostala ista. Ovi protokoli osiguravaju privatnost podataka i njihovu cjelovitost. Enkripcija se provodi pomoću algoritama simetričnog ključa pri čemu obje strane moraju posjedovati isti tajni ključ. To onemogućuje interpretaciju podataka trećim stranama koje nemaju ključ, čak niti u slučajevima kada oni te podatke mogu čitati. TLS se sastoji od dva sloja - sloja rukovanja i sloja zapisa. Sloj rukovanja je zadužen za međusobnu autentikaciju servera i klijenta, te dogovor o ključu i enkripciji koja će biti korištena. Ta interakcija se odvija prije izmjene bilo kakvih podataka [6]. Sloj zapisa se bavi sigurnošću podataka koristeći poznate podatke iz sloja rukovanja. On enkriptira i dekriptira podatke, osigurava cjelovitost (integritet) podataka, te ih štiti od neovlaštenog čitanja. Danas ovi protokoli, a pretežito TLS, imaju široku primjenu u području sigurnog prijenosa podataka, sigurnom pristupu web stranicama i sl. Tako je protokol HTTPS, koji je poznatiji kao sigurna verzija HTTP protokola, zapravo kombinacija protokola HTTP i SSL/TLS

2.5.5. IKEv2 (*Internet Key Exchange version 2*)

IKEv2 je protokol koji osigurava razmjenu ključeva, no on sam po sebi nije VPN protokol. Radi slično kao sloj rukovanja kod TLS protokola, što znači da osigurava identitet i prava pristupa svih strana u komunikaciji. Također koristi tajne ključeve i certifikate. To je jedan od osnovnih protokola koji čine IPSec protokole (koristi se u kombinaciji s IPSec-om slično kao L2TP), pa se koristi i naziv IKEv2/IPSec. Nije toliko korišten kao drugi protokoli, no dobro je rješenje za mobilne VPN-ove iz razloga što u slučaju prekida veze ili prelaska na drugu mrežu, on istu vrlo brzo ponovno uspostavlja. Ima podjednak omjer brzine i sigurnosti.

3. DODATNI SIGURNOSNI MEHANIZMI U RAČUNALNIM MREŽAMA

Osim klasičnih VPN mreža koje koriste tuneliranje i enkripcijske protokole, moguća su i druga rješenja kojima je svrha također sigurna komunikacija preko nesigurne mreže, no izvedba im je nešto drugačija. Virtualne privatne mreže obuhvaćaju široki raspon različitih rješenja, pa se tako i ova rješenja mogu smatrati sigurnosnim mehanizmima iako ne koriste navedene protokole kao VPN. Rješenja mogu biti hardverska, softverska ili kombinirana.

3.1. Primjena *proxy* servera

Temelji se na korištenju posredničkih (*proxy*) servera preko kojih se usmjeravaju zahtjevi poslani sa korisničkog računala (klijenta). Najčešća primjena im je vezana uz jednostavno maskiranje IP adrese korisnika u svrhu anonimnosti, gdje odredišni server vidi da zahtjev dolazi sa IP adrese proxy servera odnosno mrežnog čvora (node), iako je on ustvari prethodno poslan sa adrese klijenta. Na taj način se mogu zaobići geografska ograničenja ili vatrozidi, u slučaju kada blokiraju pristup određenim mrežnim sadržajima sa adrese klijenta. *Proxy* poslužitelji u osnovi ne pružaju nikakvu enkripcijsku zaštitu podataka, i zato su manje sigurni od klasičnih VPN-ova, posebno iz razloga što onaj tko kontrolira *proxy* server može lako pregledavati podatke koji prolaze kroz njega.

3.2. Primjena SSH (*Secure Shell*) protokola

SSH je kriptografski protokol koji omogućava sigurnu komunikaciju udaljenih računala i zaobilaženje vatrozida. Pomoću njega je moguće realizirati i VPN vezu odnosno mrežu jer podržava tuneliranje. SSH tuneliranje je svojim tehničkim rješenjem sličan klasičnim VPN-ovima, no potrebno je ručno podešavati korištenje SSH tunela za svaku aplikaciju zasebno, što ima svoje prednosti, ali i mane.

3.3. Primjena *DirectAccess* tehnologije

To je tehnologija slična VPN-u namijenjena prvenstveno za kreiranje intranet mreže, tako da pristup mreži imaju samo klijenti sa dodijeljenim pravima, no za razliku od klasičnih VPN veza, ovi klijenti su povezivanjem na Internet automatski spojeni na intranet, bez potrebe za uspostavljanjem ili prekidanjem veze. IPSec protokol je zadužen za tuneliranje, a komunikacija s drugim klijentima se vrši pomoću IPv6 protokola.

3.4. Primjena različitih hardverskih rješenja

Ovakva izvedba VPN-a je najskuplja ali je često i najsigurnija, a osnova su joj posebni fizički uređaji koji obavljaju funkcije VPN-a, poput autentikacije, enkripcije i sl. Oni su najčešće kombinacija hardverskih i softverskih rješenja i postavljaju se točno po zahtjevima i potrebama korisnika. Mogu zahtijevati veća infrastrukturna ulaganja (posebni uređaji, fizičke veze,…) pa se najčešće koriste u državne ili korporativne svrhe.

4. KREIRANJE VIRTUALNE PRIVATNE MREŽE

4.1. Primjena *SoftEther* VPN softvera

Uspostavljanje mobilne virtualne privatne mreže, kao praktični dio zadatka, izvedeno je pomoću *SoftEther VPN* softvera, korak po korak. SoftEther VPN je besplatan, *open source* softver za kreiranje virtualnih privatnih mreža, razvijen 2014. godine na Sveučilištu Tskuba u Japanu [7]. Koristi nekoliko VPN protokola – SSL, L2TP/IPsec, OpenVPN i SSTP. Trenutno se smatra jednim od pouzdanijih VPN softvera, a uz to je i vrlo jednostavan za korištenje. Velika sigurnost ovog softvera temelji se na korištenju 256-bitne AES (*Advanced Encription Standard*) enkripcije, što znači da se podaci enkriptiraju/dekriptiraju pomoću 256-bitnog ključa – ključa koji ima 2^{256} kombinacija. Podržavaju ga svi veći operativni sustavi, kako na računalima tako i na mobilnim uređajima.

4.2. Odabir i preuzimanje softvera

Kao što je već navedeno, mreža će biti kreirana pomoću *SoftEther* softvera, pa je prvi korak besplatno preuzimanje istog sa službenih stranica proizvođača. Kako bi veza mogla biti uspostavljena, moraju biti definirani server i klijent. Server pruža uslugu VPN-a, pomoću softverskik i/ili hardverskih rješenja. Izvedbom servera definira se tehnološko rješenje VPN-a, protokoli, ograničenja, sigurnosne provjere, itd. Klijenti su uređaji koji se povezuju na virtualnu privatnu mrežu. Ukoliko ispune sigurnosne uvjete koje server traži, oni se mogu povezati sa serverom i postati dijelom mreže.

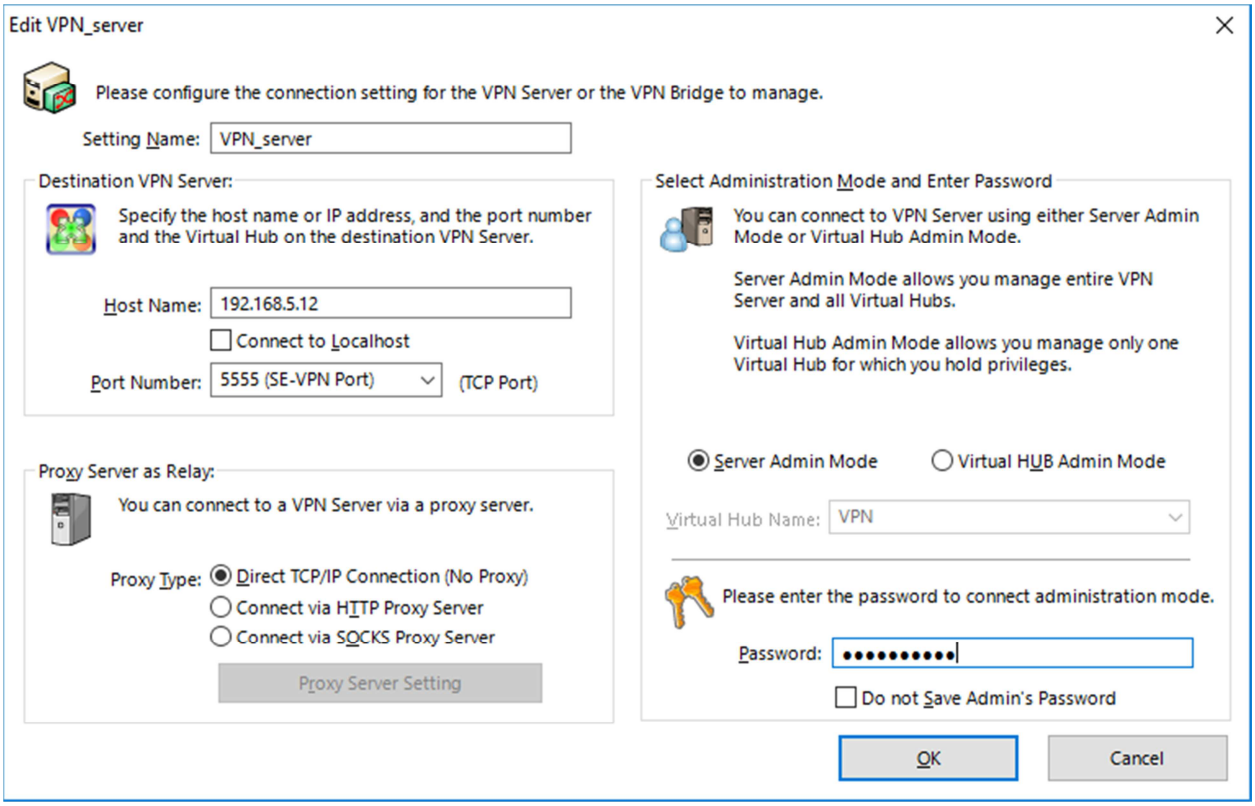
SoftEther nudi nekoliko opcija preuzimanja sofvera, ovisno o potrebama korisnika. U slučaju potrebnom za rješavanje zadatka, potrebni su bili server i klijent, pa su tako preuzeti odgovarajući paketi. Pod opcijom „*SoftEther VPN Server Manager for Windows*“ preuzet je „*SoftEther VPN Server and VPN Bridge*“ koji služi za postavljanje servera, a pod opcijom „*SoftEther VPN Client“, odabran je* „*SoftEther VPN Client*“ koji ima ulogu klijenta. Serverski paket je preuzet i instaliran na stolno računalo sa *Windows 10* operativnim sustavom, dok je za klijenta poslužilo prijenosno računalo, također sa *Windows 10* operativnim sustavom. Važno je napomenuti da je pri samoj instalaciji servera na računalo, od nekoliko ponuđenih opcija odabrana opcija „*SoftEther VPN Server“*, dok je za klijenta odabrana opcija „*SoftEther VPN Client“*. Detalji preuzimanja i instalacije su zbog svoje jednostavnosti izostavljeni iz ovog rada, a više pažnje je posvećeno postavljanju servera i klijenta.

4.3. Konfiguriranje servera

Po uspješnoj instalaciji serverskog softvera, pomoću njega se može pristupiti postavljanju servera. Tako, pri prvom pokretanju softvera, otvara se prozor sa slike 3.1.

Slika 4.1. *Početni prozor Server Manager-a*

Ovdje je moguće započeti sa postavljanjem servera. To je najlakše učiniti tako da se jednim klikom odabere ponuđena predefinirana (*default*) opcija, a zatim se pritisne „*Edit Setting*“. To otvara novi prozor u kojem se postavljaju osnovni podaci o serveru (Sl. 4.2.).

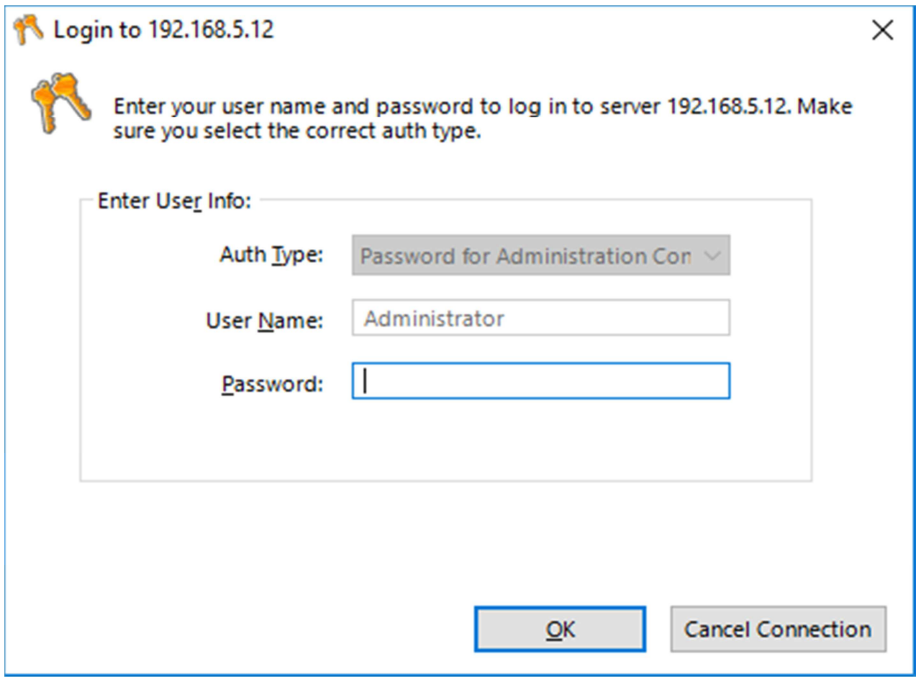


Slika 4.2. *Podešavanje osnovnih postavki servera*

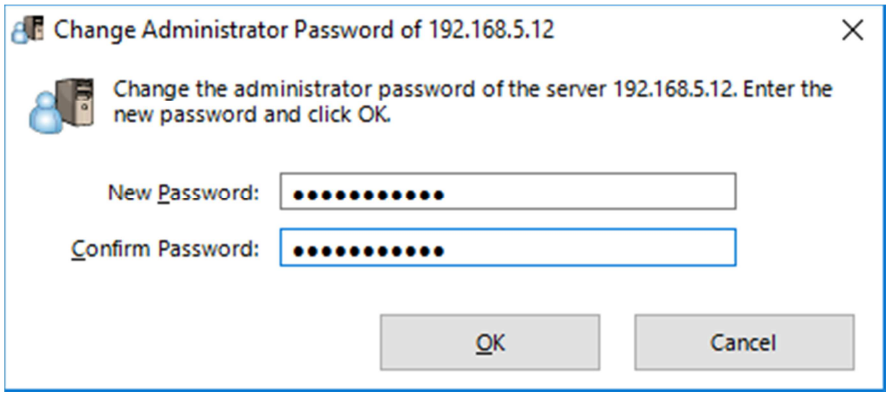
Ovdje se može podesiti naziv općih postavki servera (*Setting Name*), što može biti bilo kakav string znakova, u ovom slučaju odabran je naziv „*VPN_server*“. Zatim, potrebno je unijeti IP adresu servera, odnosno IP adresu računala na kojem server postavljamo. Ta adresa je pronađena u *Command prompt*-u pomoću naredbe *ipconfig*. Nakon toga, traži se unos broja TCP porta putem kojeg će se odvijati VPN promet. Od nekoliko portova koje ovaj softver koristi, odabran je port 5555 zbog preporuke proizvođača. Uz to, odabrana su administratorska prava za cijeli server (*Server Admin Mode*) čime su osigurana sva prava kasnije uređivanje. Kao dodatna mjera sigurnosti, dodijeljena je lozinka za pristup administratorskim pravima. Ovdje postoji i dodatna opcija za povezivanje putem *proxy* servera koja je izostavljena radi jednostavnosti. Nakon što su odabrane željene postavke potvrđuje se odabir pritiskom na *OK* nakon čega se ponovno otvara prethodni prozor, sada sa izmijenjenim podacima (Sl. 4.3.).

Slika 4.3. *Početni prozor Server Manager-a*

Sada se može odabrati kreirana veza i odabrati opcija *Connect*. Pojavljuje se prozor koji traži unos lozinke za pristup serveru, koja, pri prvom otvaranju, još ne postoji, te se odmah može nastaviti dalje pritiskom na *OK* (Sl. 4.4.). Time se otvara novi prozor koji nudi postavljanje odnosno izmjenu lozinke. Tu se postavlja željena lozinka za administratora servera, te se odabir potvrđuje pritiskom na *OK* (Sl. 4.5.).

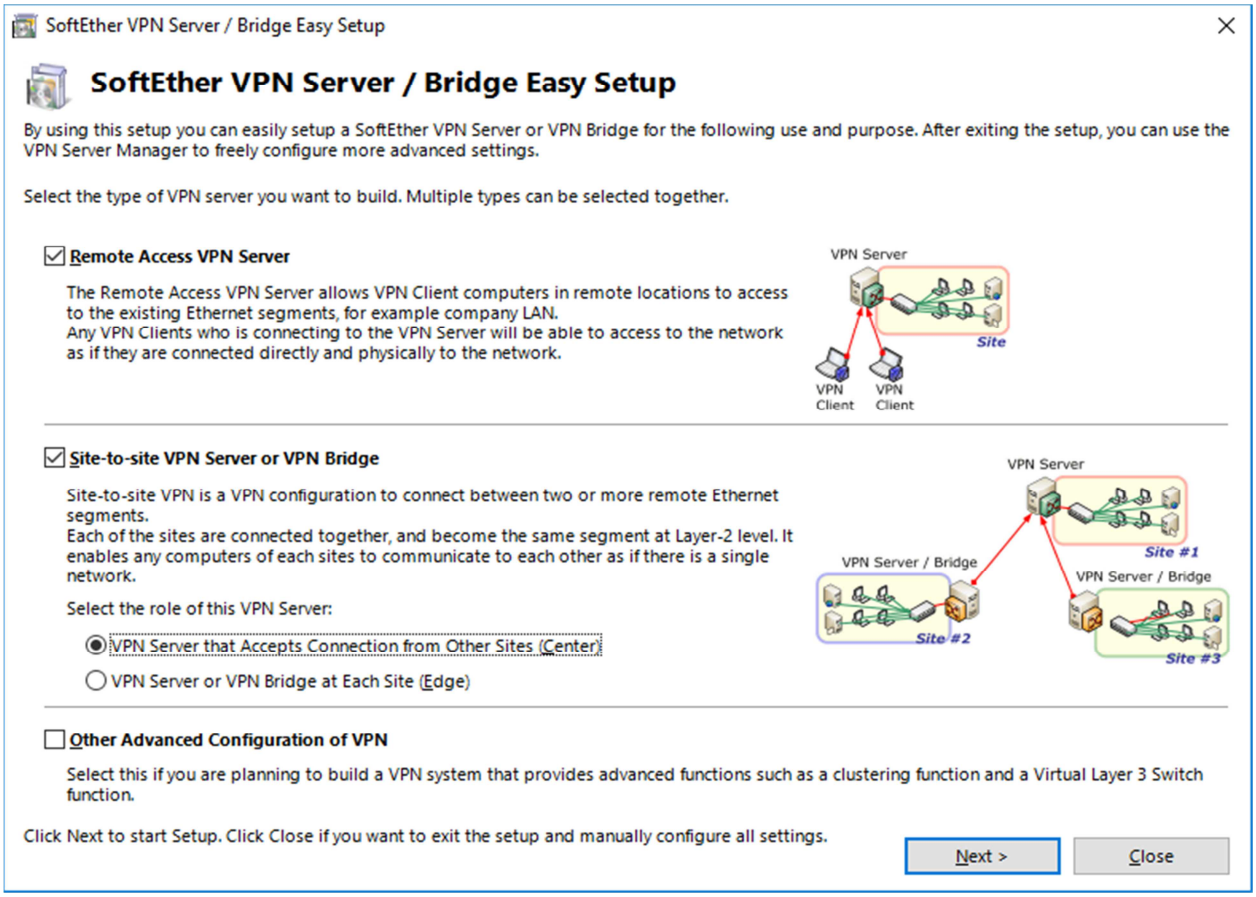


Slika 4.4. *Prostor za unos administratorskih podataka*



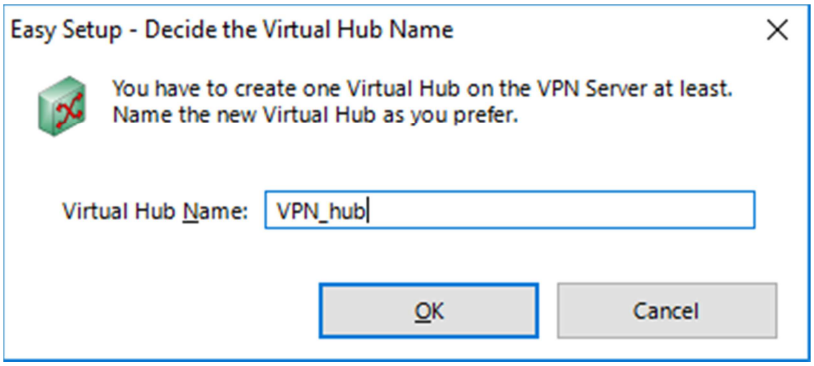
Slika 4.5. *Postavljanje novih administratorskih podataka*

Nakon prethodnih, osnovnih postavki, sada je potrebno odabrati vrstu VPN servera. Ponuđene su opcije *Remote VPN Server* i *Site-to-Site VPN Server or VPN Bridge* (Sl. 4.6.). Također, nude se i posebne opcije za naprednu konfiguraciju servera, koje u ovom slučaju nisu potrebne. Moguće je bilo odabrati obje opcije istovremeno, pa je tako učinjeno, iako bi za potrebe zadatka bila dostatna i samo prva, *Remote Access* opcija, jer je za ovaj zadatak potrebno jednostavno spajanje klijenta i servera.



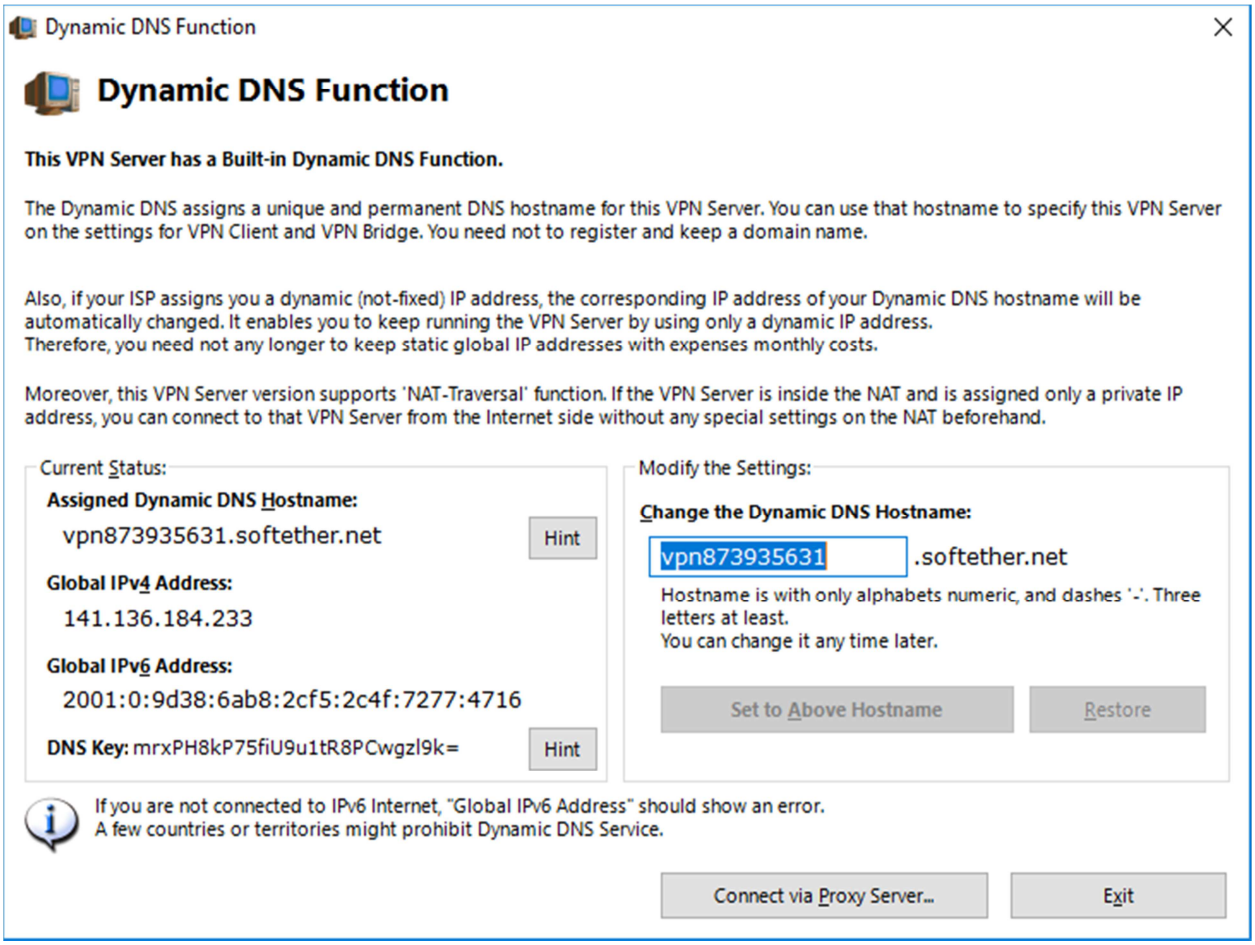
Slika 4.6. *Odabir željene topologije mreže*

Nakon što su željene opcije odabrane, nastavlja se pritiskom na *Next*, što otvara prozor koji obavještava o kreiranju virtualnog *hub*-a (Sl. 4.7.), te traži unos njegovog naziva, što može biti bilo kakav, proizvoljan niz znakova. Nakon unosa nastavlja se dalje pritiskom na OK.



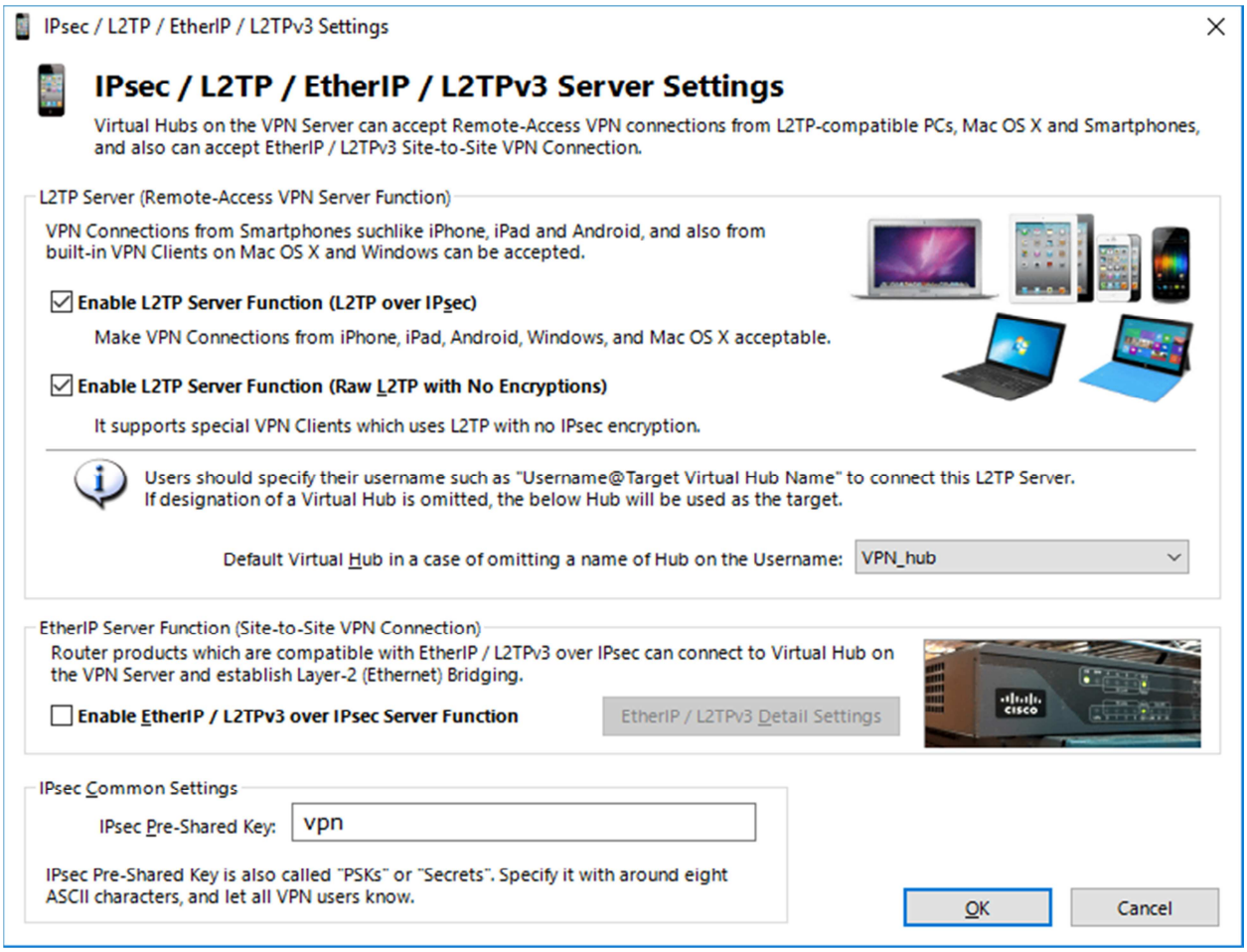
Slika 4.7. *Dodjeljivanje imena hub-u*

Sada se otvara prozor „*Dynamic DNS Function*“ koji nudi opciju generiranja dinamičke DNS adrese (Sl. 4.8.). DNS (*Domain Name System*) povezuje ime sa IP adresom. Može se postaviti kako bi server imao jednostavniji naziv, no taj korak je za zadatak suvišan, pa se iz prozora jednostavno izlazi pritiskom na *Exit*.



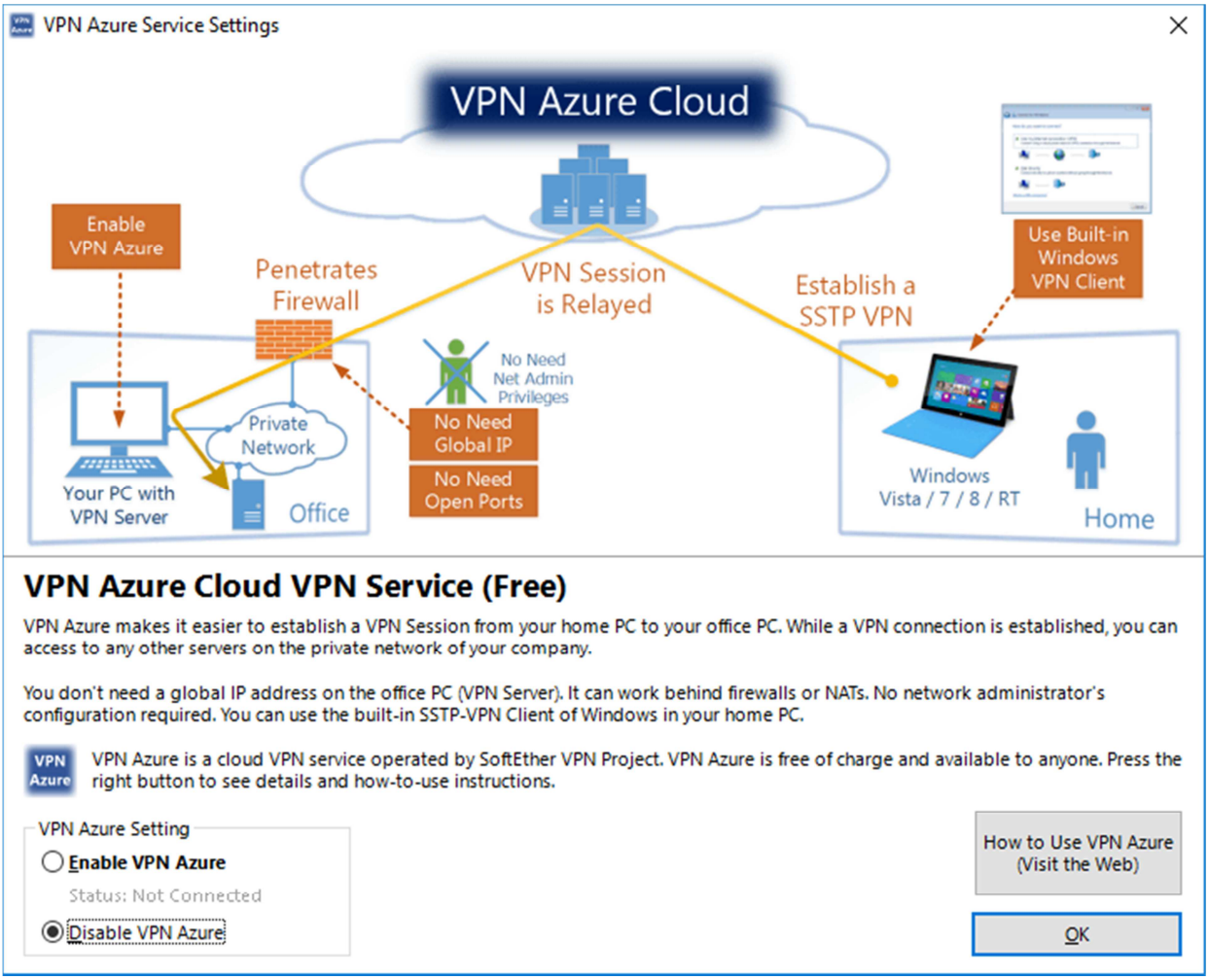
Slika 4.8. *Opcije postavljanja dinamičke DNS adrese*

U sljedećem koraku bira se opcija za omogućavanje povezivanja mobilnih uređaja te uređaja sa ugrađenim VPN klijentom na server (Sl. 4.9.). Odabrane su dvije opcije za *Remote-Access* povezivanje, dok je opcija za *Site-to-Site* povezivanje izostavljena, iz razloga što su za nju potrebni napredni uređaji koji se koriste za tu vrstu povezivanja. Unutar ovog prozora se pod opcijom *IPSec Pre-Shared Key* može unijeti željeni niz znakova, što ustvari predstavlja jednostavnu metodu autentikacije, a taj niz znakova je jednostavni „tajni“ ključ koji će kasnije biti potreban za povezivanje mobilnog uređaja sa VPN serverom. Ova opcija u postavljanju servera nije mijenjana, već je ostavljen unaprijed ponuđeni string „*vpn*“. Kada su sve željene opcije podešene, pritiskom na *OK* nastavlja se dalje.



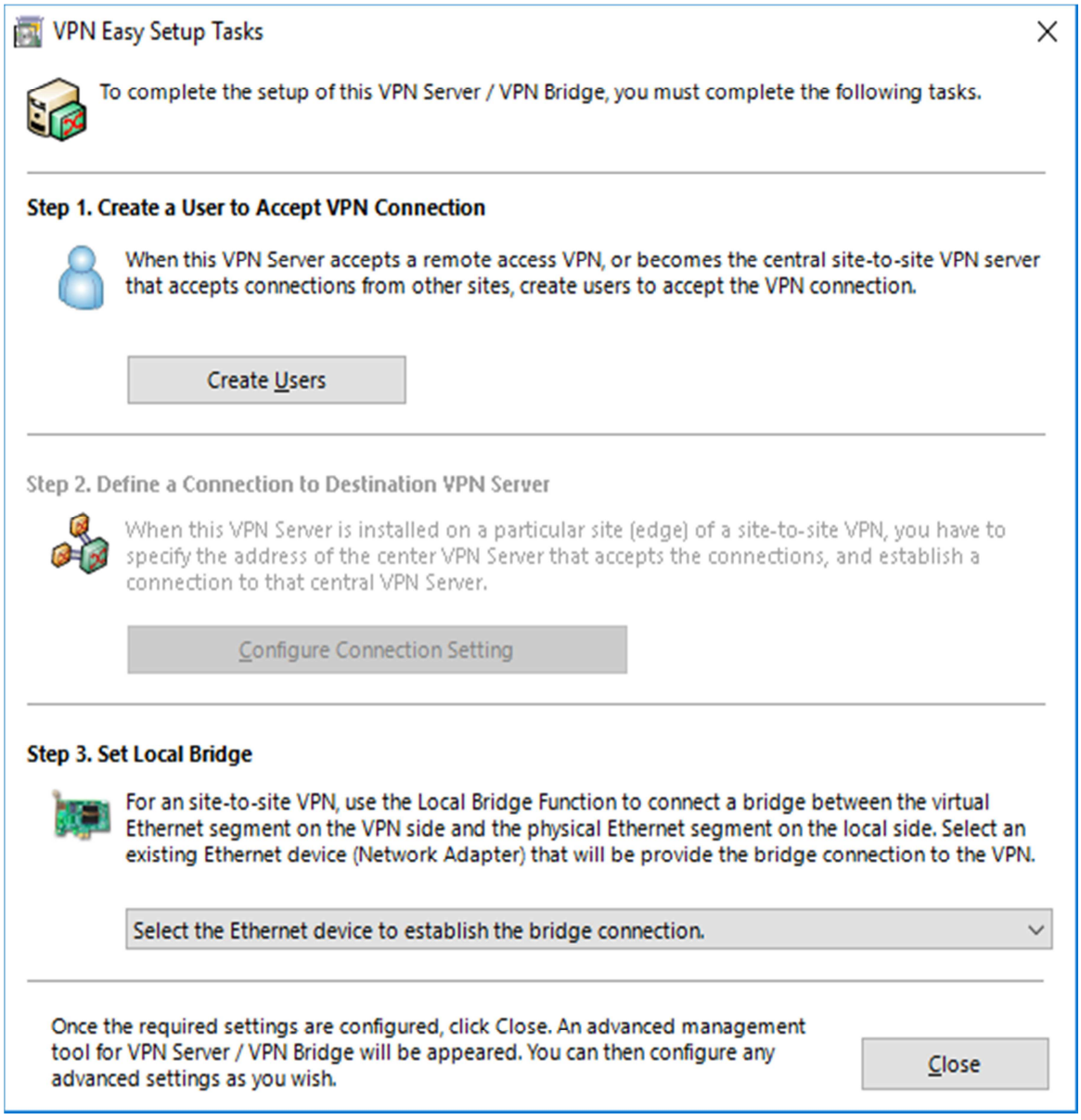
Slika 4.9. *Odabir dodatnih načina spajanja na server*

Sljedeći prozor nudi mogućnost odabira opcije sav promet između servera i klijenta ide preko *cloud* VPN-a u vlasništvu proizvođača, što ima određene dodatne pogodnosti poput zaobilaženja vatrozida i slično, a omogućio bi dodatan stupanj sigurnosti mreže (Sl. 4.10.). Ta mogućnost je odbijena odabirom opcije „*Disable VPN Azure*“, jer za potrebe ovog primjera nije potrebna, te se nastavlja dalje pritiskom na *OK*.



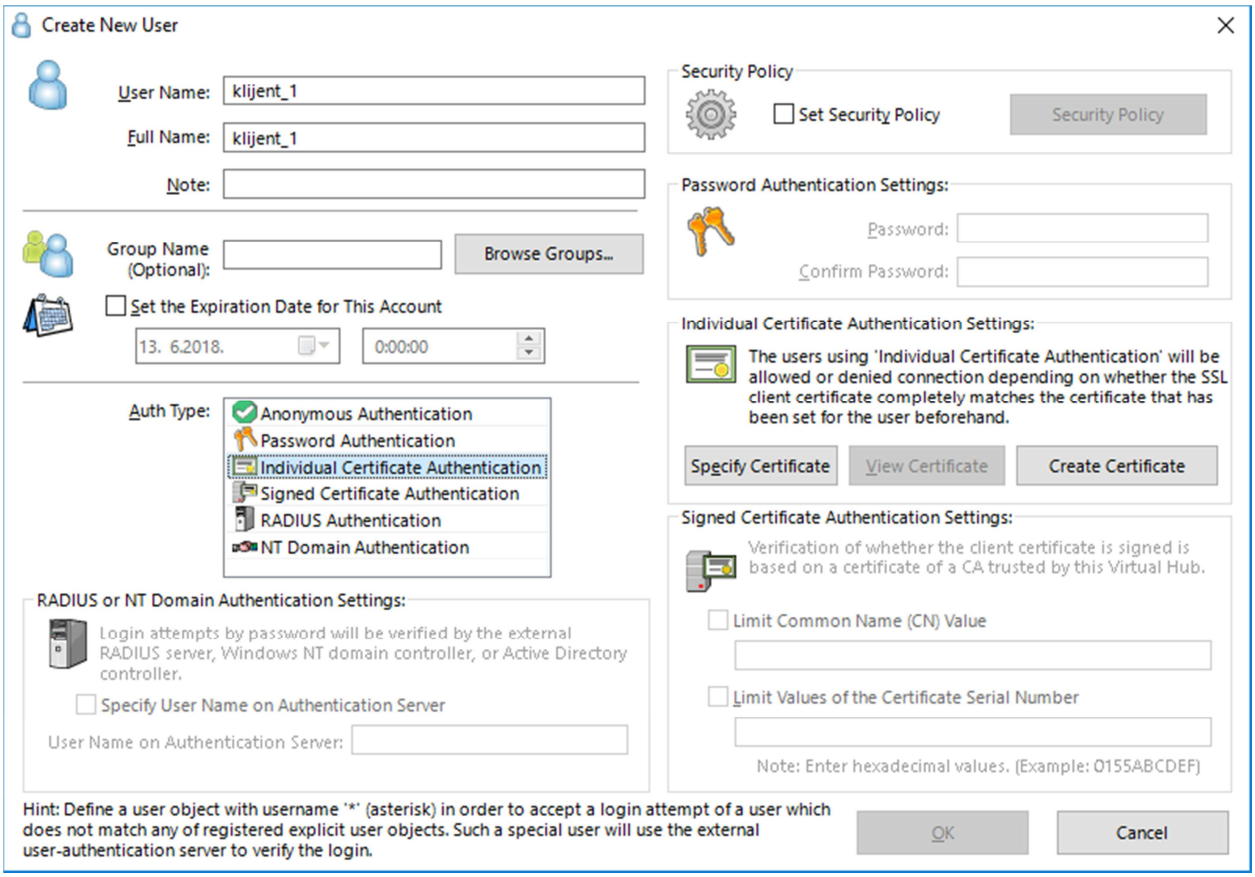
Slika 4.10. *VPN Azure opcija*

Pojavljuje se novi prozor koji zahtijeva još nekoliko koraka kako bi postavljanje VPN servera bilo dovršeno (Sl. 4.11.). Od ukupno tri koraka, zadana su dva, i to zbog prethodno odrađenih odabira (korak 2 se odnosi samo na *site-to-site* mreže).



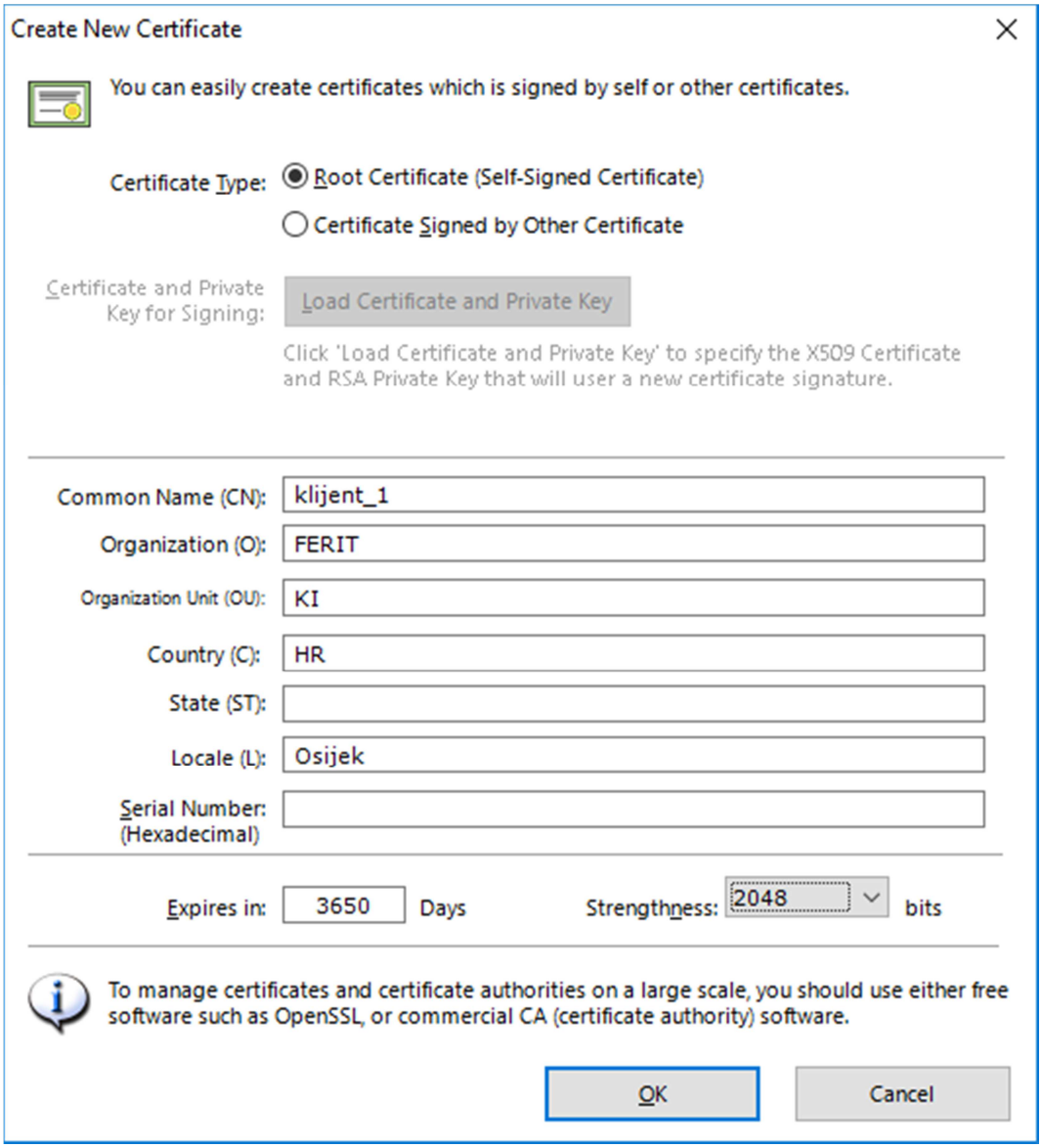
Slika 4.11. *Posljednje postavke prije dovršetka servera*

Prvi korak je kreiranje korisnika odnosno klijenta, čime će biti kreiran prvi korisnički profil sa željenim uvjetima (dopuštenjima i ograničenjima), i odabire se pritiskom na „*Create Users*“, te se time otvara novi prozor sa postavkama korisnika (Sl. 4.12.).



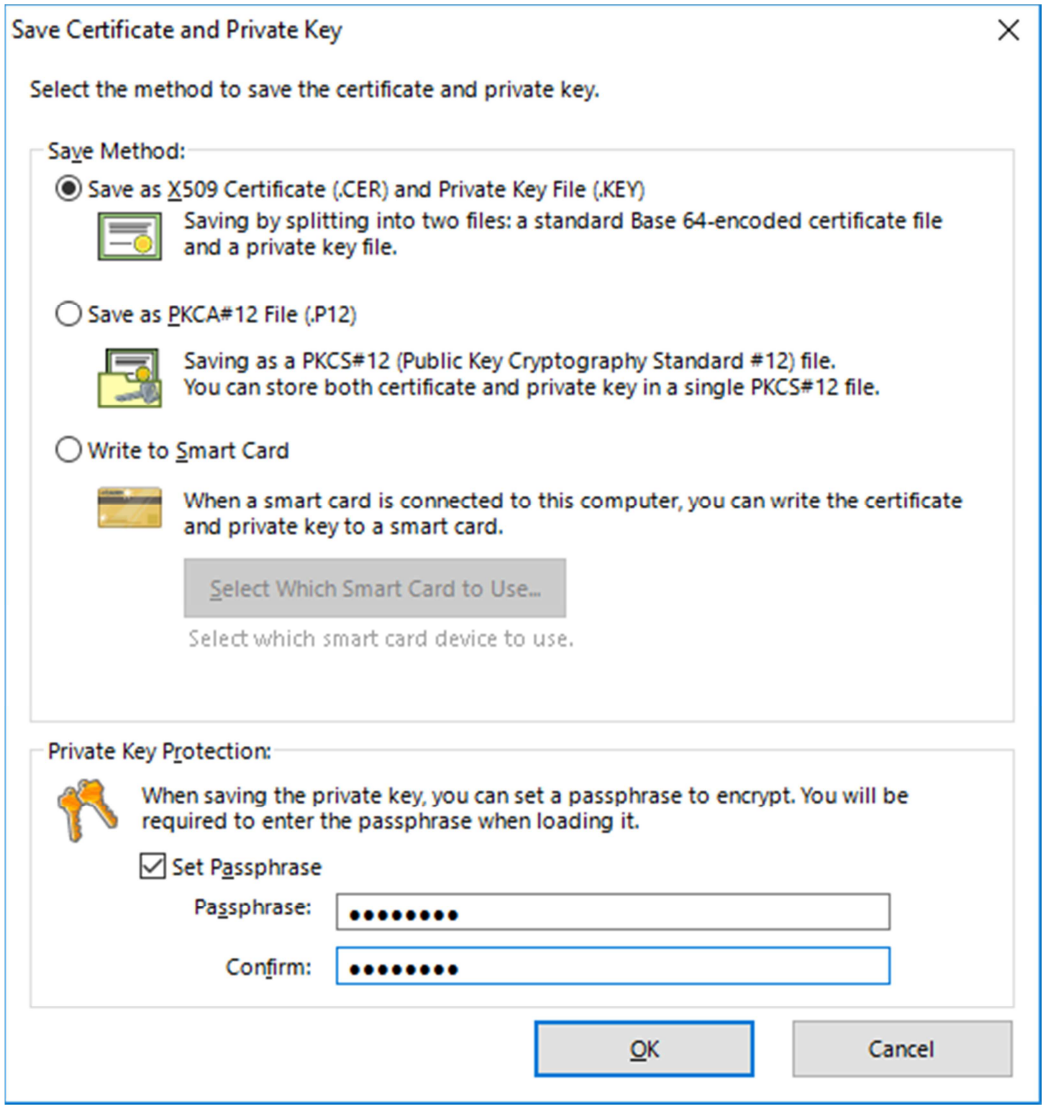
Slika 4.12. *Početni prozor pri kreiranju novog klijenta*

Ovdje je ponuđeno mnoštvo opcija za definiranje korisnika, kao i načina na koji će određeni korisnik pristupati našoj virtualnoj privatnoj mreži tj. način autentikacije korisnika. Potrebno je dodijeliti naziv korisniku, pa je u polja „*User Name*“ i“ *Full Name*“ unešen naziv *klijent_1*. Opcija *Set Security Policy* nudi mogućnost postavljanja raznih sigurnosnih uvjeta koji će se odnositi na klijenta (dopušteni protokoli, filtriranje, korištenje lozinke i sl.), ali za takvim naprednim podešavanjem u ovom slučaju nema potrebe. Način autentikacije klijenta odabire se iz padajućeg izbornika, te je za potrebe ovog rada odabrana opcija autentikacije pomoću individualnih certifikata. Ta vrsta autentikacije zahtijeva da korisnik tj. klijent serveru uz korisničko ime dostavi certifikat i privatni ključ na osnovu kojih se onda klijentu odobrava ili odbija spajanje na server. Takva metoda je puno sigurnija od klasičnih metoda poput primjerice kombinacije korisničkog imena i lozinke. Nakon što je u izborniku odabrana navedena opcija, automatski se na otvorenom prozoru ističe odjeljak vezan za nju. Tu se odabire „*Create Certificate*“, što otvara novi prozor u kojem se unose podaci o korisniku (Sl. 4.13.) .



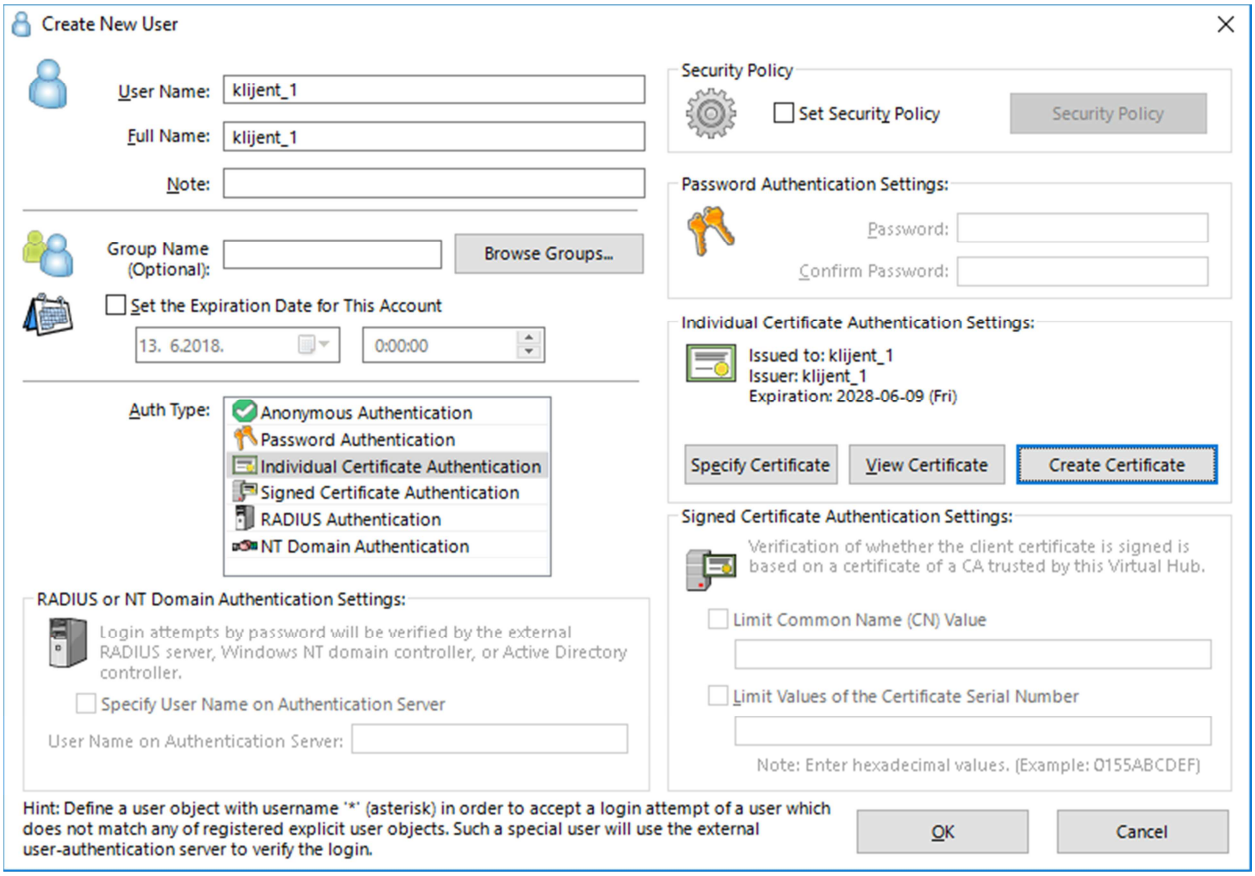
Slika 4.13. *Postavke certifikata*

Prvo se odabire vrsta certifikata, gdje je odabran *Root Certificate*. Zatim se unose osnovni podaci o korisniku kojem se dodjeljuje certifikat. Ti podaci nisu toliko bitni i većina ih se može izostaviti, no preporuča se odrediti barem naziv korisnika. Ovdje je korisniku opet dodijeljen naziv *klijent_1*. Moguće je podesiti i duljinu valjanosti certifikata odnosno broj dana nakon kojeg on ističe, kao i jačinu enkripcije privatnog ključa. Ove vrijednosti nisu mijenjane već su zadržane prethodno zadane vrijednosti. Pritiskom na OK otvara se sljedeći prozor na kojem odabiremo u kojem formatu datoteke će biti spremljeni certifikat i ključ (Sl. 4.14.).



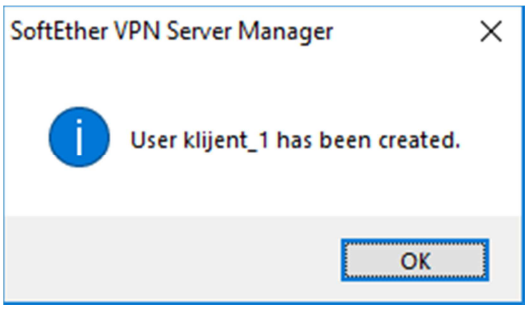
Slika 4.14. *Postavke certifikata i privatnog ključa*

U ovom koraku je odabrana prva opcija koja sprema certifikat i ključ u dvije zasebne datoteke (.CER i .KEY). Uz to, privatni ključ je dodatno zaštićen lozinkom iako je ta opcija proizvoljna. Nakon što se postave prethodno navedene stavke, pritiskom na OK se kreiraju datoteke certifikata i ključa, te se automatski otvaraju zasebni prozori za odabir mjesta pohrane tih datoteka na računalo. Datoteke su spremljene u istu mapu kako bi se zajednički dostavile korisniku koji će zatim pomoću njih moći pristupiti serveru pod korisničkim imenom *klijent_1*. Po spremanju obje datoteke na računalo program se vraća na prozor sa slike 4.12., no on se sada promijenio na način da je sada vidljivo da postoji certifikat koji je izdan za korisnika, te se vidi datum kada certifikat prestaje vrijediti. (Sl. 4.15.).



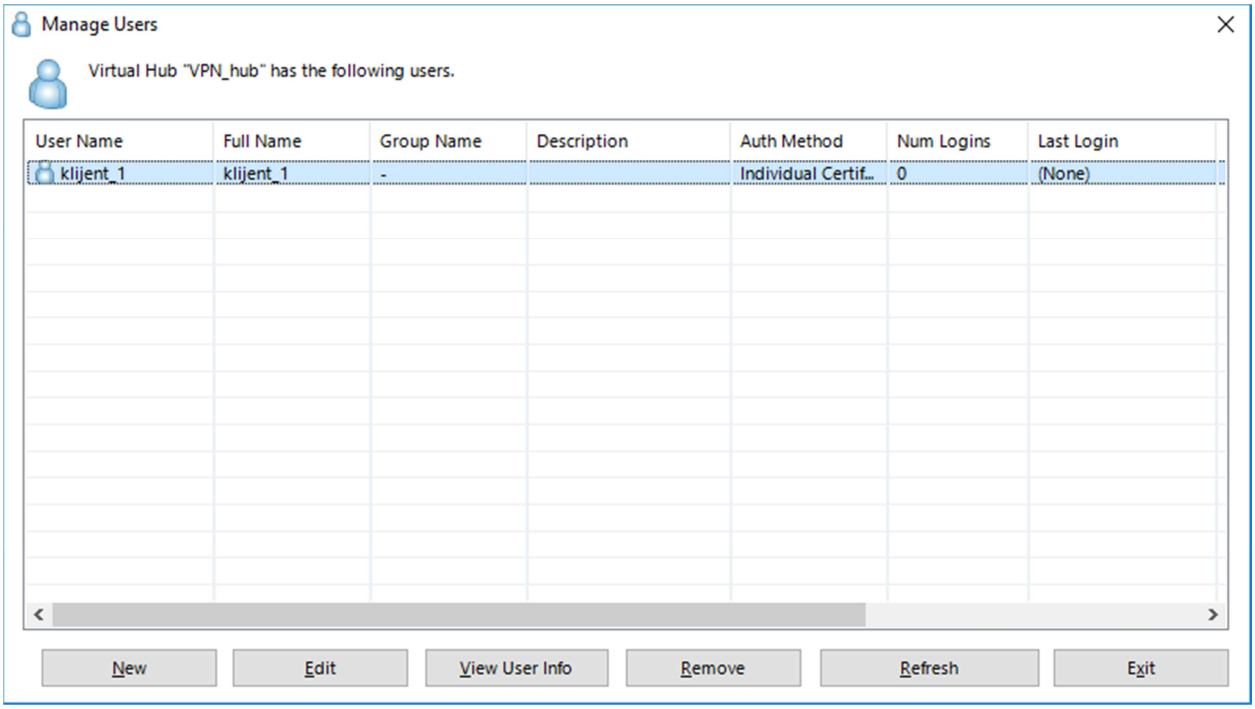
Slika 4.15. *Početni prozor pri kreiranju novog klijenta*

Ako su svi željeni koraci izvršeni, pritiskom na OK se nastavlja dalje, te ukoliko je korisnik uspješno kreiran prikazuje se odgovarajuća obavijest (Sl. 4.16).



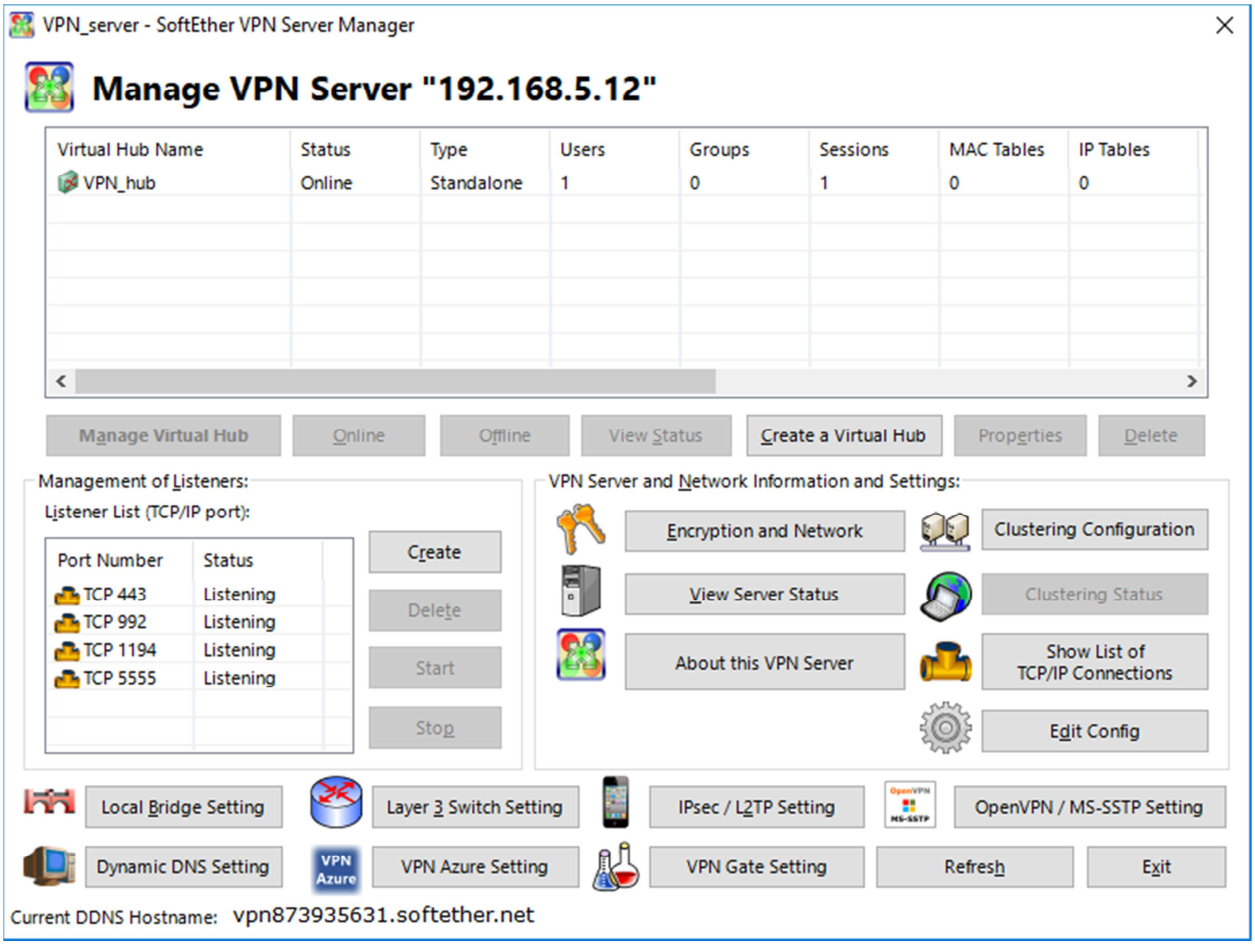
Slika 4.16. *Obavijest o uspješnom kreiranju klijenta*

Ponovnim pritiskom na OK zatvara se obavijest, te se pojavljuje lista korisnika na kojoj se sada nalazi i prethodno definirani korisnik (Sl. 4.17.).



Slika 4.17. *Popis korisnika servera*

Lista sadrži sve kreirane korisnike, te se može pristupiti detaljima o svakom od njih. Isto tako, ovdje se mogu kreirati novi, te editirati i brisati postojeći korisnici. Za nastavak rada potrebno je pritisnuti *Exit*, čime se vraćamo na prozor sa slike 4.11. Sada je potrebno odraditi zadnji korak, a to je povezivanje virtualnog i fizičkog dijela odnosno povezivanje virtualnog *hub*-a sa mrežnom karticom što se vrši uspostavom mosta (*Local Bridge*). U opcijama padajućeg izbornika odabire se željena mrežna kartica, i time je zadnji korak gotov. Pritiskom na *Close* zatvara se trenutni prozor, i pojavljuje se upravljačko sučelje servera kojeg smo upravo kreirali (Sl. 4.18.). Ovdje je vidljiva lista svih *hub*-ova koji pripadaju serveru, te se mogu vidjeti detalji svakog od njih. Putem ovog sučelja moguće je naknadno mijenjati gotovo sve podatke o serveru i *hub*-ovima, a dostupan je i prikaz dodijeljenih portova kojima je također moguće upravljati (portovi koji će služiti za sigurnu komunikaciju VPN-a). Za vrijeme rada servera, ovdje je moguće vidjeti sve podatke o događajima na njemu u realnom vremenu.

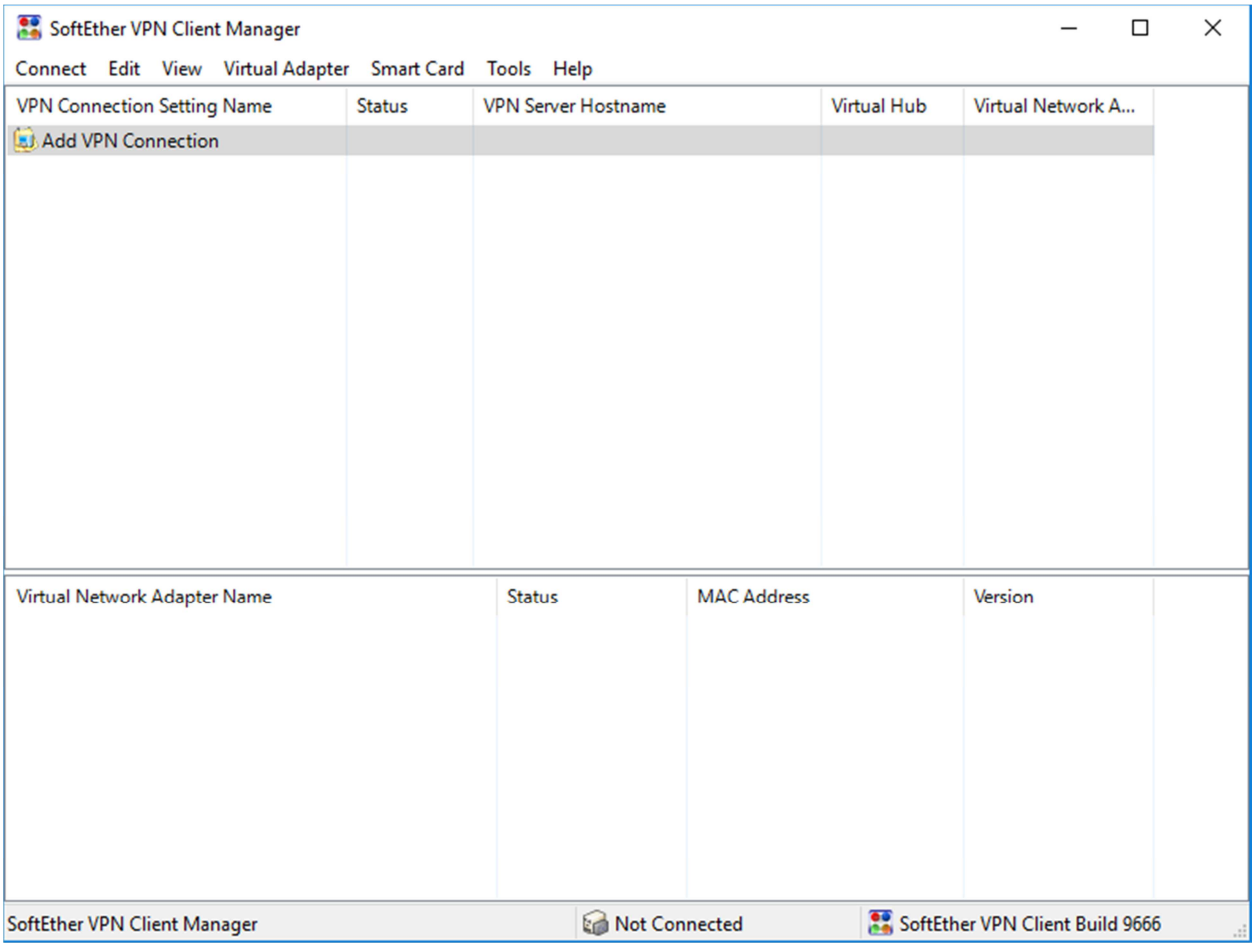


Slika 4.18. *Prozor za kontrolu i upravljanje serverima*

Prethodnim koracima su postavljeni osnovni zahtjevi za kreiranje VPN servera, i sada se može prijeći na uspostavu veze između klijenta i servera.

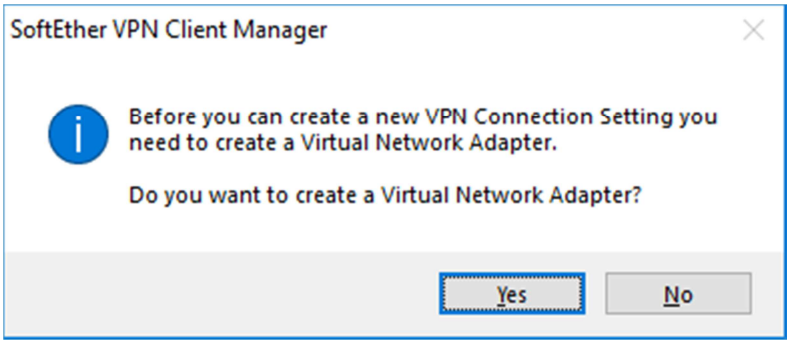
4.4. Konfiguriranje klijenta

Kao predkorak u postavljanju klijenta i uspostavi veze sa serverom, mapa koja sadrži prethodno kreirani ključ i certifikat kopirana je na računalo koje će se povezivati sa serverom. U realnim uvjetima taj je korak relativno ranjiva točka, jer se riskira da pri dostavljanju ključa strani kojoj je namijenjen, ključ dođe u posjed neovlaštene strane (npr. ključ je ukraden...). Kada se posjeduju ključ i certifikat, moguće je uspostaviti vezu sa serverom. Samo uspostavljanje veze započinje otvaranjem softvera „*SoftEther VPN Client*“. Na početnom prozoru vidljiva je lista postojećih veza koja je pri prvom pokretanju prazna (Sl. 4.19.).



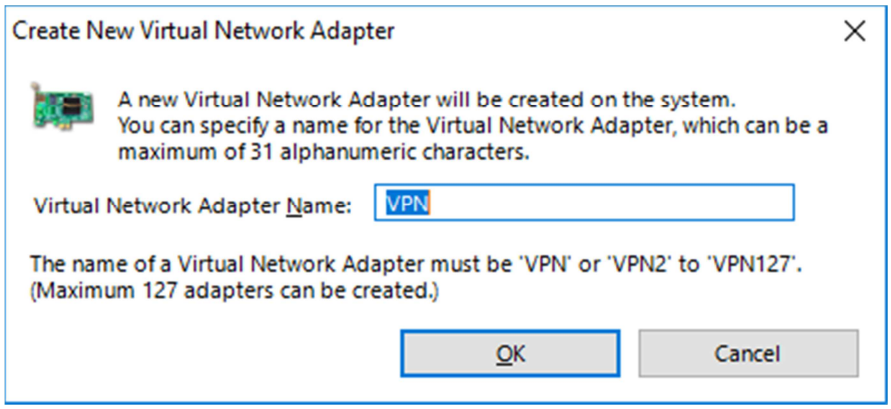
Slika 4.19. *Početni prozor Client Manager-a*

Dvostrukim klikom na opciju „*Add VPN Connection*“ pojavljuje se prozor koji upozorava korisnika da ne postoji *Virtual Network Adapter* (Sl. 4.20.).



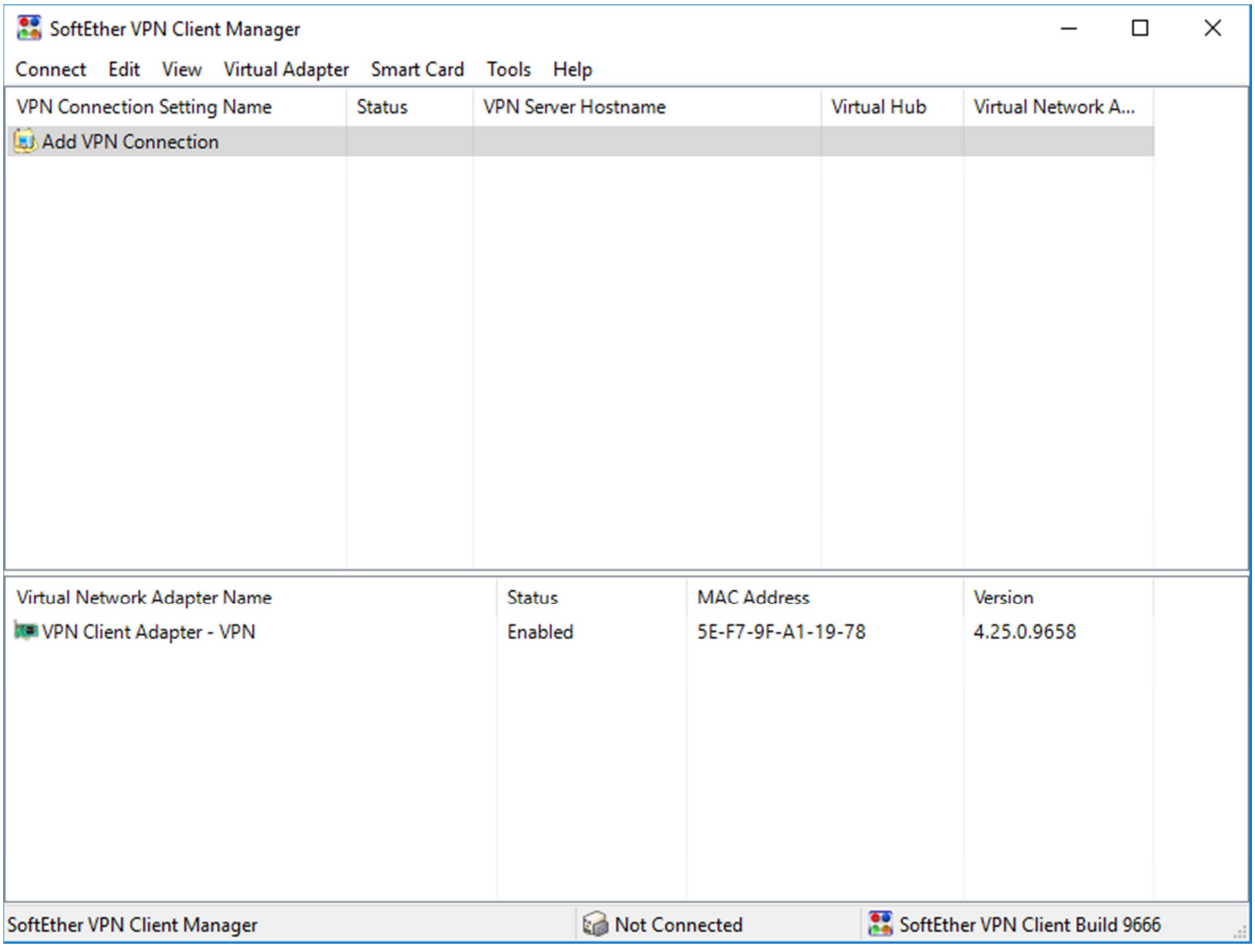
Slika 4.20. *Obavijest o kreiranju virtualnog adaptera*

Potrebno je pritisnuti „*Yes*“ nakon čega se pojavljuje novi prozor u kojem se upisuje ime novog adaptera (Sl. 4.21.).



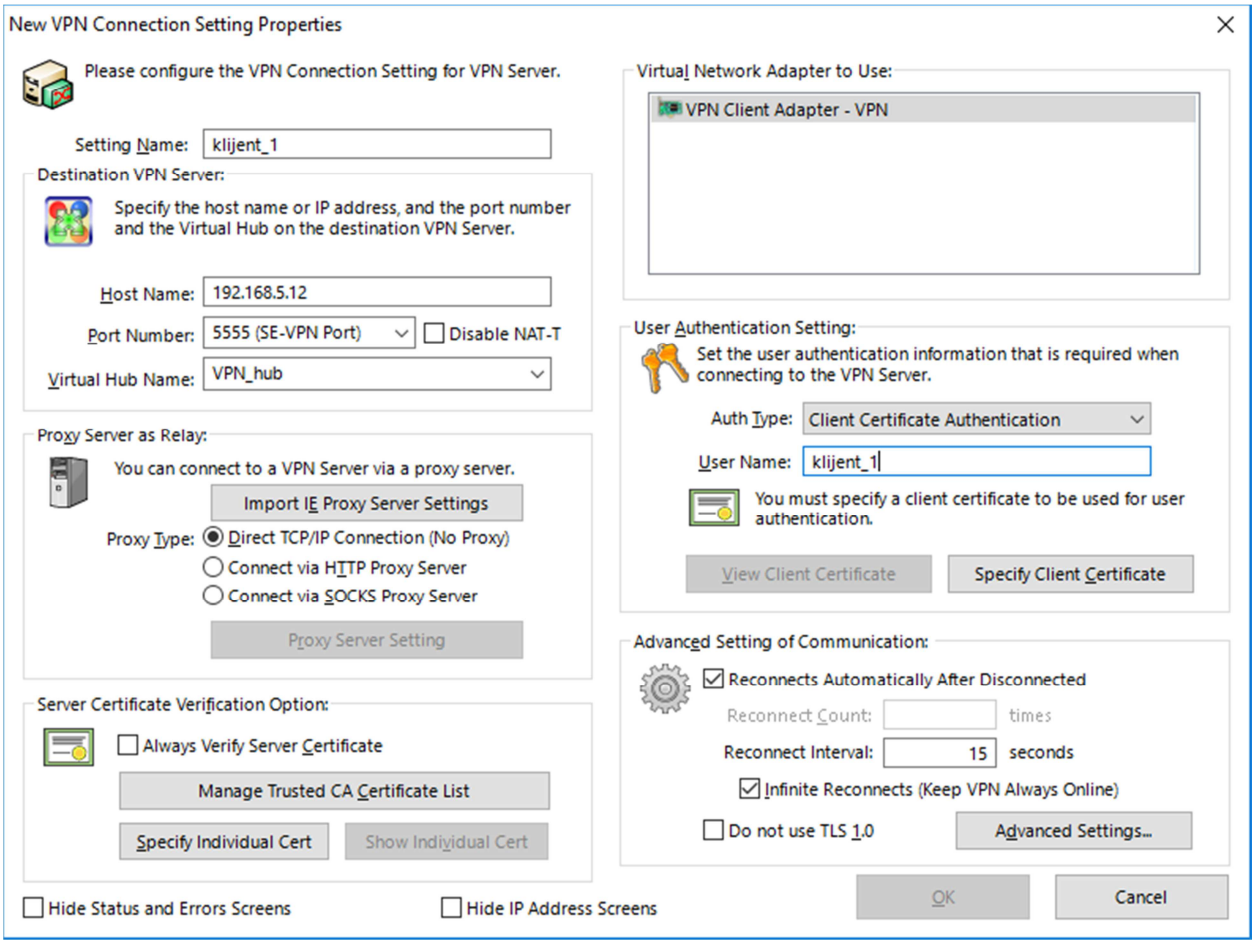
Slika 4.21. *Dodjeljivanje naziva virtualnom adapteru*

Naziv može biti bilo kakav string, u ovom slučaju „VPN“. Nakon pritiska na *OK*, na početnom prozoru se pojavljuje novi adapter (Sl. 4.22.).



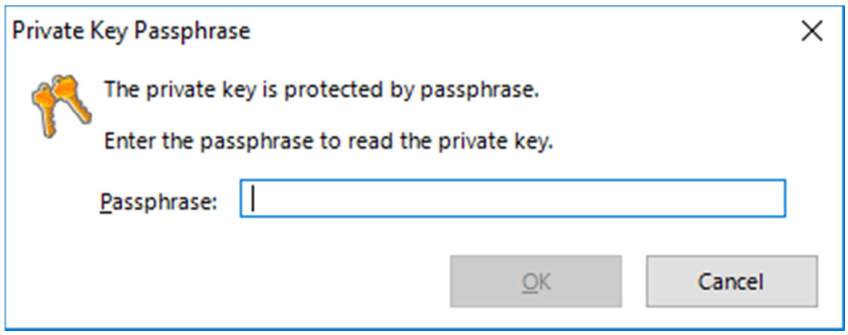
Slika 4.22. *Prikaz novog adaptera na početnom prozoru*

Sada ponovno možemo pokrenuti opciju „*Add VPN Connection*“ i time kreirati novu VPN vezu čija svojstva se određuju na novom prozoru (Sl. 4.23.).



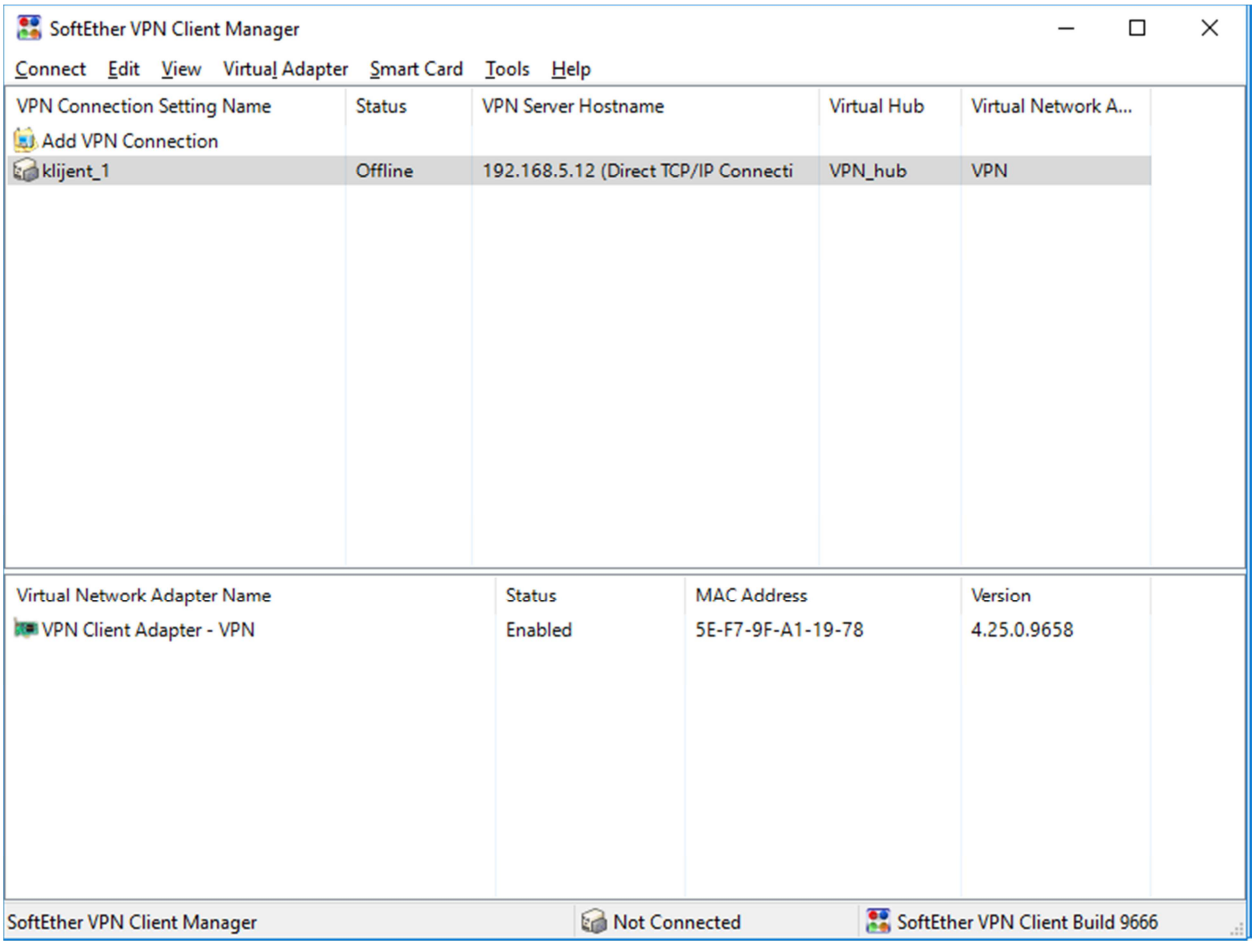
Slika 4.23. *Uređivanje postavki nove VPN veze*

Potrebno je podesiti postavke veze u skladu sa onima koje su prethodno zadane na serveru. Tako je za ime veze postavljeno „*klijent_1*“ te su pod opcijama VPN servera unesena imena servera i *hub*-a, kao i broj odgovarajući port. Adapter je automatski odabran jer je jedini trenutno ponuđen. Nakon toga potrebno je odabrati opciju autentikacije, a to je autentikacija putem certifikata, kao što je zadano pri kreiranju servera. Potom se unosi korisničko ime klijenta i odabire opcija „*Specify Client Certificate*“. Otvara se sučelje za pretraživanje datoteka gdje se pronalazi mapa sa certifikatom i ključem. Njih je potrebno otvoriti pritiskom na „*Open*“. Po otvaranja ključa potrebno je još upisati lozinku koja je kod kreiranja ključa odabrana kao dodatna mjera sigurnosti (Sl. 4.24.).



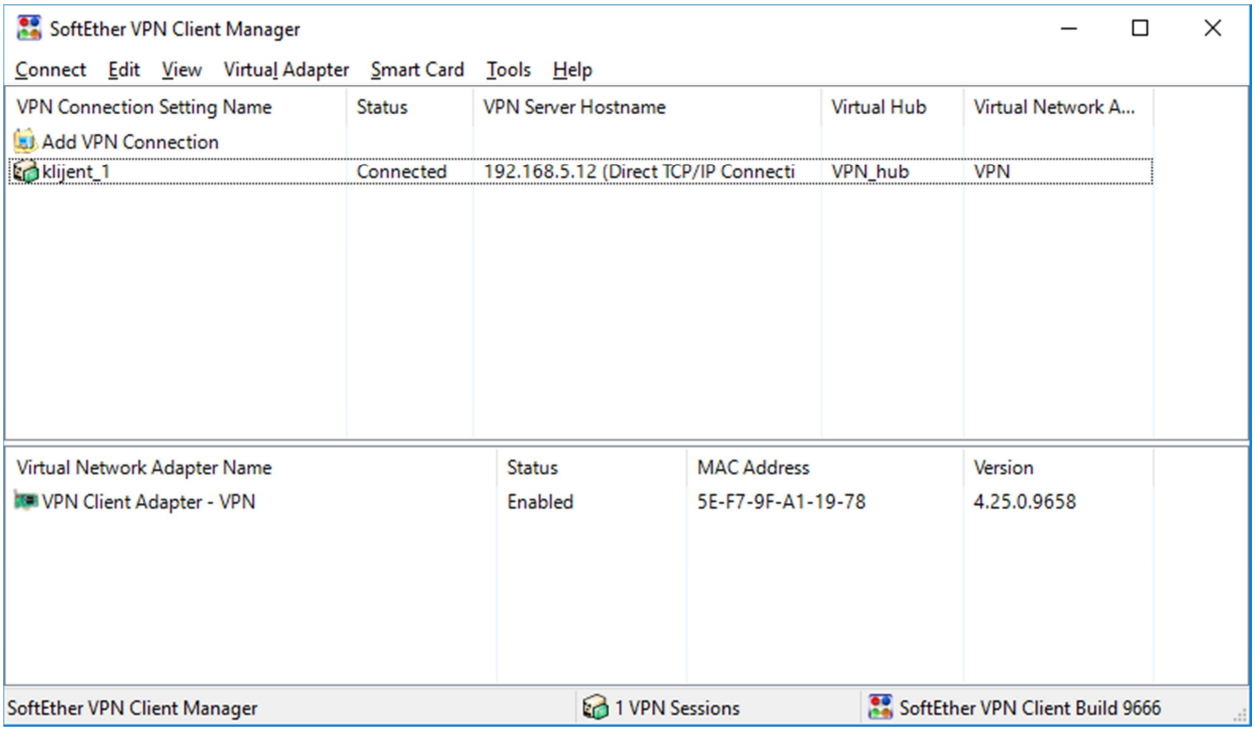
Slika 4.24. *Prostor za unos lozinke servera*

Unošenjem lozinke i pritiskom na *OK* program nas vraća na početni prozor gdje je sada vidljiva novonastala veza između klijenta i servera (Sl. 4.25.).



Slika 4.25. *Prikaz nove veze na početnom prozoru*

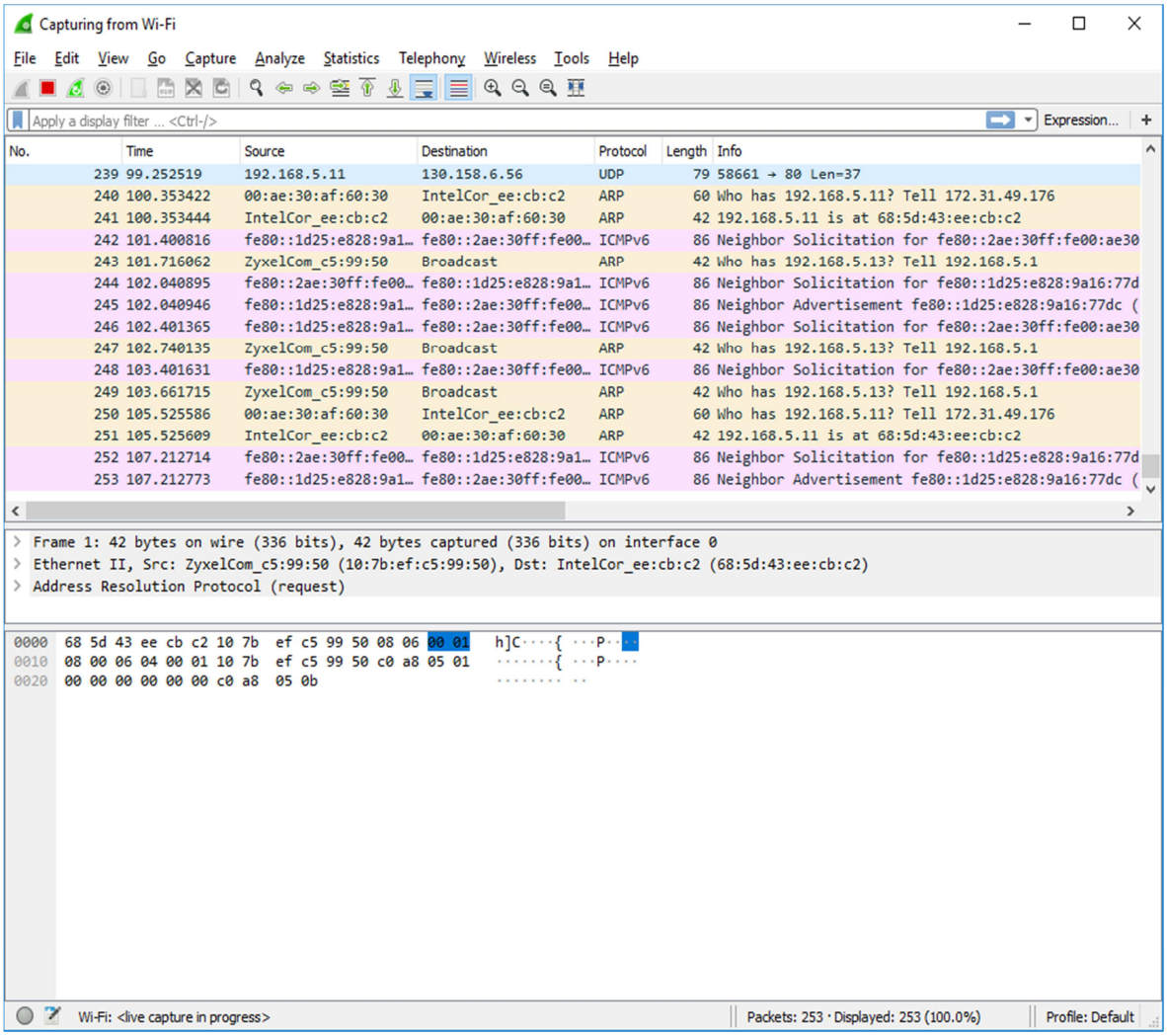
Pregledom osnovnih podataka prikazanih na zaslonu vidljivo je da je veza kreirana, i da je trenutni status *offline*. Sada je samo preostalo desnim klikom na vezu otvoriti izbornik na kojem se odabire opcija „*Connect*“, i ova veza će postati aktivna što znači da sada klijent i server komuniciraju putem sigurnog kanala (Sl. 4.26.).



Slika 4.26. *Prozor za upravljanje klijentiima*

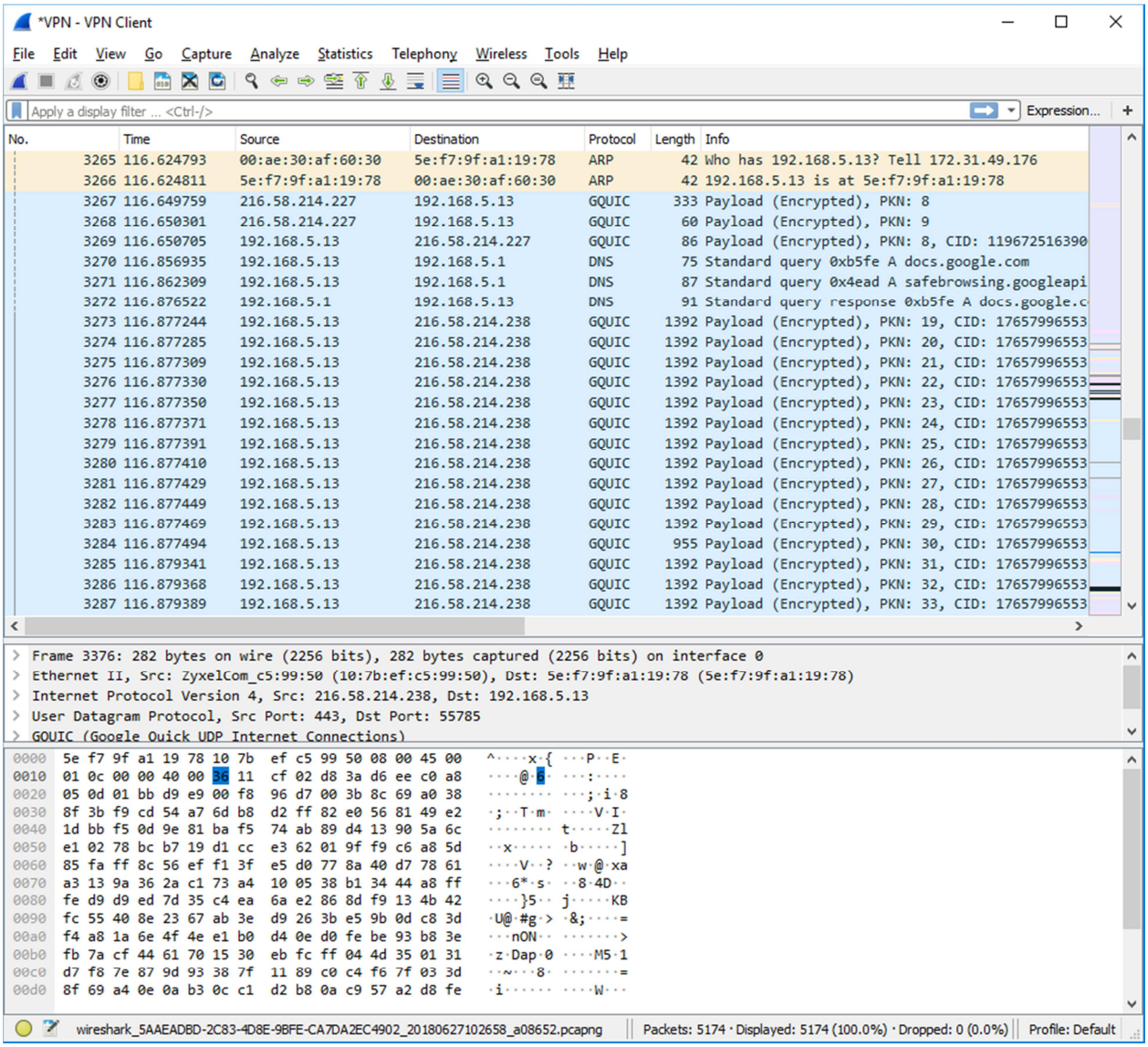
5. TESTIRANJE VEZE

Za utvrđivanje povezanosti klijenta sa serverom korišten je *Wireshark* softver. To je besplatan, *open-source* softver za analizu prometa na mreži odnosno mrežnih paketa. Njime je snimljen promet prije i nakon uspostavljanja VPN veze, te su vidljive razlike u vrsti prometa. Prvo je potrebno odabrati aktivnu vezu na kojoj će se snimati promet. Prije spajanja na VPN, vidljivi su paketi koji prolaze mrežom putem raznih protokola karakterističnih za internetski promet (Sl. 5.1.).



Slika 5.1. *Snimka dijela paketnog prometa – prije povezivanja*

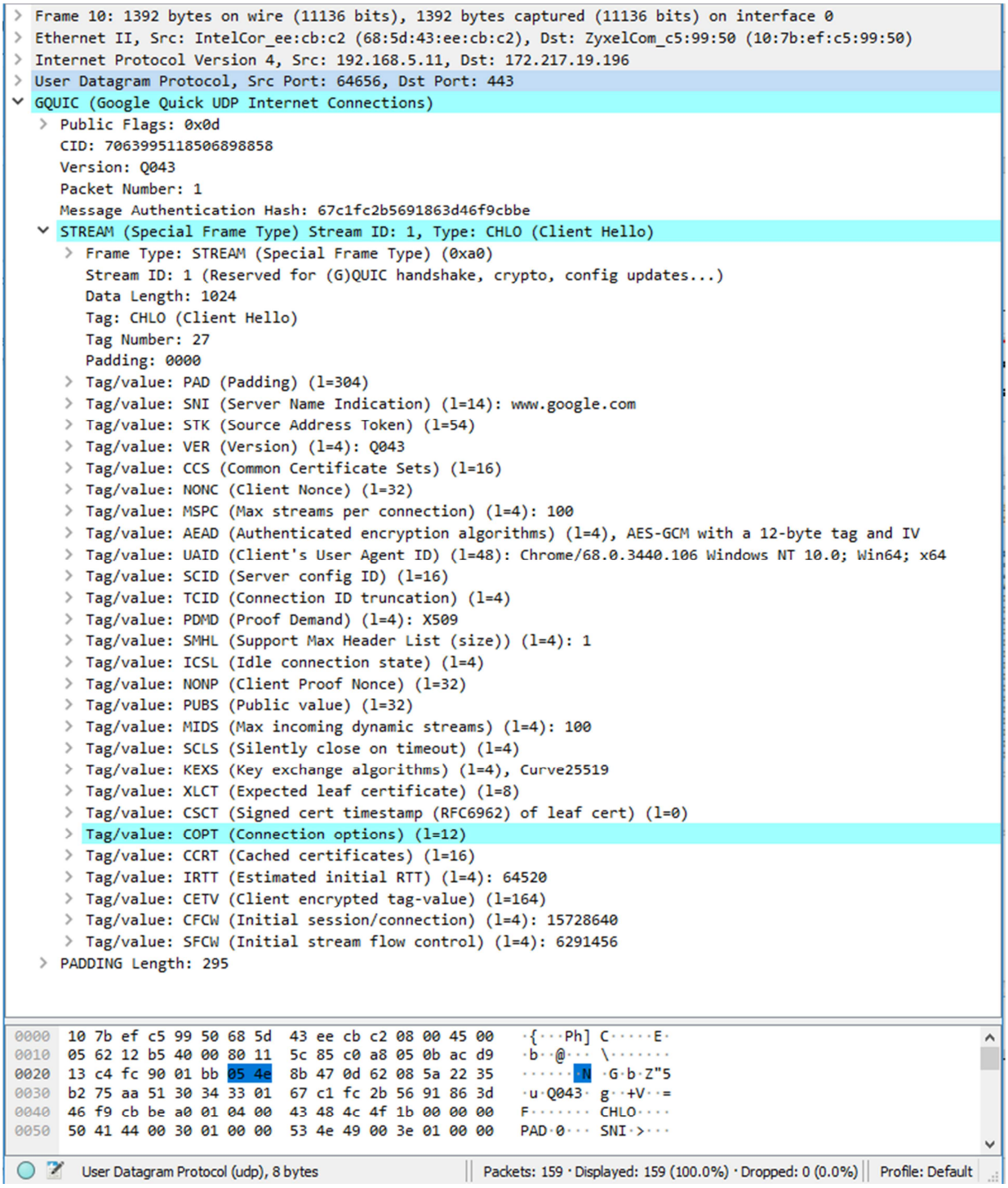
Kod uspostavljene VPN veze je da ne bi trebalo biti moguće iščitati određene podatke iz paketa koji prolaze mrežom. Nakon povezivanja klijenta sa serverom, veza između njih trebala bi biti zaštićena. U idućem koraku uspostavljena je veza sa serverom, te je pomoću *Wireshark*-a snimljen promet na toj vezi (*Wireshark* automatski raspoznaje VPN vezu). Očito je da je došlo do promjene u paketima koji se razmjenjuju između računala (klijenta i servera), kao što je vidljivo na slici 5.2.



Slika 5.2. *Snimka dijela paketnog prometa – nakon povezivanja*

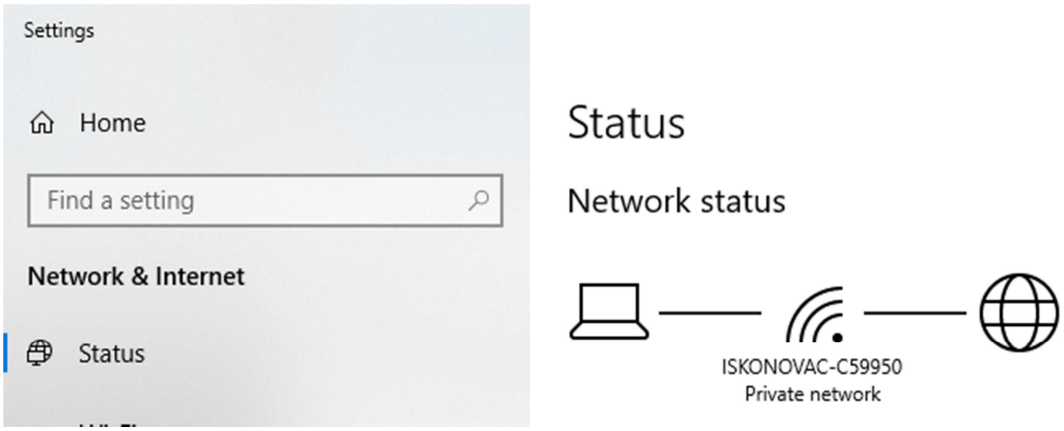
Tu vidimo kako je većina paketa poslana GQUIC protokolom, te da je veza enkriptirana (u Info). QUIC (*Quick UDP Internet Connections*) odnosno GQUIC, je noviji, eksperimentalni protokol, razvijen od strane Google-a 2012. godine. Implementacijom QUIC-a postiže se veća učinkovitost veza koje ovise o brzini prijenosa podataka. Glavna značajka mu je korištenje UDP protokola za prijenos podataka, za razliku od često korištenog TCP protokola. Prednost UDP-a

nad TCP-om je brzina prijenosa podataka zbog toga što UDP ne provodi provjeru grešaka pri slanju, a time se smanjuje kašnjenje. Uz to, QUIC smanjuje broj *round-trip time* (RTT) parametara potrebnih za komunikaciju čime se također povećava brzina, te podržava multipleksiranje, što znači da se ovim protokolom može poslati više zahtjeva serveru istovremeno [8]. Neke od svojih odlika (multipleksiranje, smanjen broj RTT-ova,…) QUIC preuzima od HTTP/2 protokola, ali s ciljem dodatnog poboljšanja njihove izvedbe. Na slici 5.3., prikazan je sadržaj jednog GQUIC paketa iz čega je vidljiva složenost tog protokola.

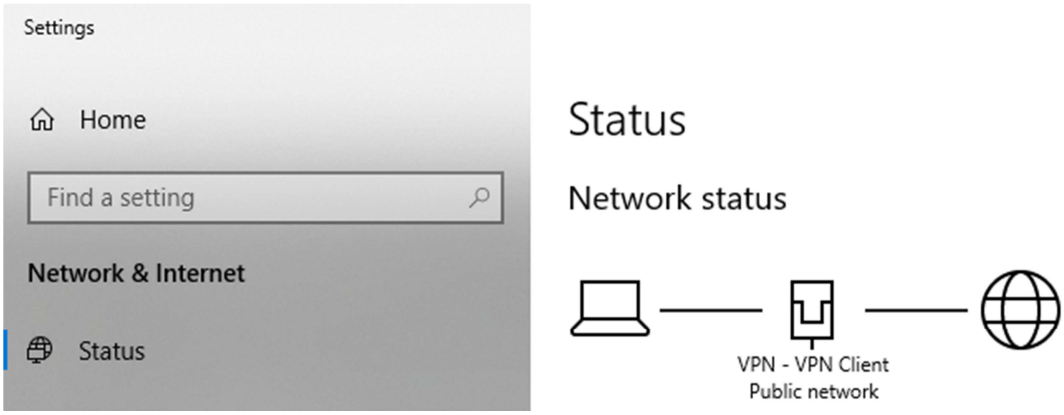


Slika 5.3. *Detaljnji prikaz podataka o jednom GQUIC paketu*

Nadalje, i u sučelju Windows 10 *sustava* se može lako vidjeti razlika u statusu mreže, odlaskom na *Start* > *Settings* > *Network & Internet.* Tu se pri vrhu kartice prikazuje aktivna mrežna veza, te se status mijenja nakon spajanja na VPN server (Sl. 5.4., 5.5.).



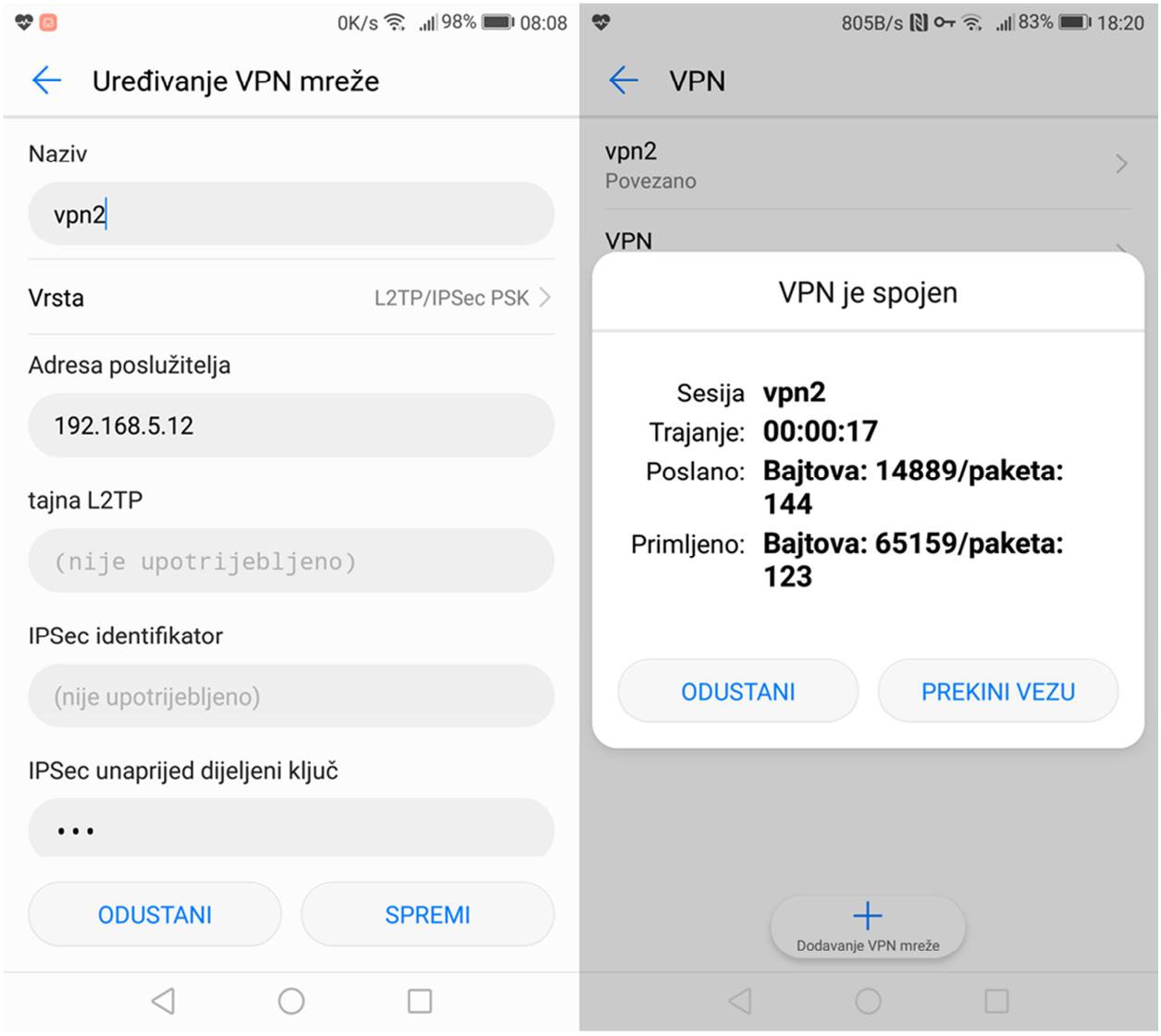
Slika 5.4. *Stanje prije povezivanja*



Slika 5.5. *Stanje nakon povezivanja*

Osim putem računala sa *Windows* operativnim sustavom, uspješno je odrađena i veza sa serverom putem *Android* mobilnog uređaja. Prethodno tome, uređen je profil *klijent_2* na isti način kao i prvi profil. U postavkama uređaja koji imaju tu mogućnost, nalazi se opcija VPN.

Unutar nje, odabirom dodavanja VPN mreže, otvara se sučelje za unos podataka za spajanje (Sl.5.6). Unosi se vrsta veze i adresa poslužitelja, kako je prethodno zadana, i tu sada postaje koristan u početku kreirani *IpSec Preshared Key* pomoću kojega je se sada moguće spojiti na server. Nakon spremanja veze i uspješnog povezivanja, trebalo bi biti moguće vidjeti obavijest o stanju trenutne veze, kao na slici 5.6. desno. Uz to, u gornjem desnom kutu ekrana pojavljuje se znak ključa koji označava da uređaj koristi sigurnu vezu.



Slika 5.6. *Snimka zaslona Android uređaja*

6. ZAKLJUČAK

Kroz ovaj rad bilo je potrebno objasniti što su to mobilne virtualne privatne mreže te uspostaviti jednu takvu mrežu koristeći jedno od mnogih softverskih rješenja. Najprije je bilo potrebno objasniti što su to virtualne privatne mreže, koja im je svrha, te na koji način se realiziraju i kako rade.

Kao temelj za funkcioniranje virtualnih privatnih mreža, obrađeni su protokoli koji se trenutno koriste za njihovu izvedu. To su protokoli za enkripciju i prijenos preko mreže koji se često kombiniraju za poboljšan krajnji rezultat u vidu sigurnosti i brzine prijenosa.

Praktični dio rada odnosi se na kreiranje jednostavne mobilne virtualne privatne mreže pri čemu je korišten *SoftEther* softverski alat. Pomoću njega su kreirani server i klijent između kojih se vrši komunikacija putem sigurnog kanala na kojem su podaci zaštićeni. Proces kreiranja veze je objašnjen korak po korak, pomoću slika i popratnog objašnjenja svakog dijela procesa.

Nadalje, nakon što je veza uspješno kreirana, dobiveni rezultati su analizirani programom *Wireshark* na način da su snimani paketi koji prolaze sigurnim komunikacijskim kanalom, iz čega je vidljivo da su paketi zaštićeni, odnosno da se komunikacija vrši putem sigurnosnih protokola.

LITERATURA

[1] CARNet CERT i LSS, Osnovni koncepti VPN tehnologije [online], Centar informacijske sigurnosti, 2003., dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf [11.6.2018.]

[2] A. Shneyderman, A. Casati, Mobile VPN: Delivering Advanced Services in Next Generation Wireless Systems [online], John Wiley & Sons, 2003., dostupno na: http://media.wiley.com/product_data/excerpt/10/04712190/0471219010.pdf [11.6.2018.]

[3] CARNet CERT i LSS, Sigurnost bežičnih LAN-ova [online], Centar informacijske sigurnosti, 2003., dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-05-22.pdf [11.9.2018.]

[4] I. Jakopiček, Asimetrični kriptografski RSA algoritam, diplomski rad, Osijek, 2010. dosupno na: http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/JAK19.pdf [11.9.2018.]

[5] A. Shrivastava, M. A. Rizvi, Analysis and Comparison of major mechanisms implementing Virtual Private Networks, IJARCET, Volume 3 Issue 7, 2014.., dostupno na: http://ijarcet.org/wp-content/uploads/IJARCET-VOL-3-ISSUE-7-2374-2381.pdf [13.9.2018.]

[6] Wikipedia: the free encyclopedia [online], Transport Layer Security, Wikimedia Foundation, Inc. 2001, dostupno na: https://en.wikipedia.org/wiki/Transport_Layer_Security [11.9.2018]

[7] SoftEther VPN Project, [online], SoftEther VPN, Universiy of Tsukuba, Japan, dostupno na: https://www.softether.org/ [12.9.2018]

[8] C. Vincent, C.Pearce, A “quick” guide to QUIC, [online], Cisco Blogs, Cisco, 2016, dostupno na: https://blogs.cisco.com/security/a-quick-guide-to-quic [12.9.2018.]

SAŽETAK

Ovaj rad obuhvaća opis osnovnih pojmova vezanih uz virtualne privatne mreže, uključujući i primjer kreiranja jedne takve mreže. Opisana je svrha virtualnih privatnih mreža i načini njihove izvedbe te neka od osnovnih rješenja i protokola koji se koriste za njihovu realizaciju. Uz to, predstavljena su neka od postojećih rješenja sličnih virtualnim privatnim mrežama. Praktični dio obuhvaća detaljan postupak uspostavljanja mobilne virtualne privatne mreže pomoću *SoftEther VPN* softverskog paketa, te testiranje uspostavljene veze pomoću programa *Wireshark*.

Ključne riječi: virtualna privatna mreža, VPN, VPN protokol, *SoftEther*

ABSTRACT

This paper covers the description of virtual private networks, including a simple example of a network setup. The purpose and types of virtual private networks, as well as the underlying technology and protocols are described. In addition, some of the existing solutions, similar to virtual private networks are pointed out. The practical part of the paper includes a detailed procedure of mobile virtual private network setup, using the *SoftEther VPN* software, along with the testing of the network once it was set up, using the *Wireshark* software.

Keywords: virtual private network, VPN, VPN protocol, *SoftEther*

ŽIVOTOPIS

Ante Radoš je rođen 21. ožujka 1994. godine u Osijeku. Pohađao je Osnovnu školu Vladimira Nazora u Đakovu, nakon čega upisuje Gimnaziju Antuna Gustava Matoša u Đakovu, prirodoslovno matematički smjer. 2012. godine upisuje se na Građevinski fakultet u Osijeku, s kojeg se ispisuje 2014. godine. 2015. godine upisuje preddiplomski studij Elektrotehnike na Elektrotehničkom fakultetu u Osijeku, današnjem FERIT-u, te na drugoj godini studija odabire smjer Komunikacije i informatika. 2018. sudjeluje na STEM Games-ima u Poreču kao predstavnik FERIT-a u kategoriji Engineering.