

Što je VPN poslužitelj i kako ga postaviti

Studentski tim: Dubravko Lukačević

Dominik Marjanović

Tomislav Markovac

Josip Trbuščić

Mentor: izv. prof. dr. sc. Miljenko Mikuc

Sadržaj

Sadržaj	2
1 Puni naziv projekta	3
2 Skraćeni naziv projekta	3
3 Opis problema/teme projekta	3
4 Cilj projekta	4
5 Voditelj studentskog tima	4
6 Rezultati	5
6.1 Windows	5
6.1.1 Windows 10 VPN	5
6.1.2 SoftEther VPN	12
6.1.3 Tinc	24
6.1.4 OpenVPN za Windows	26
6.2 FreeBSD	35
6.2.1 OpenVPN	35
6.3 Linux	45
6.3.1 OpenVPN	45
6.3.2 Libreswan IPsec/L2TP VPN poslužitelj	55
7 Usporedba	58
8 Slični projekti	59
9 Resursi	59
10 Glavni rizici	59
11 Smanjivanje rizika	59
12 Glavne faze projekta	59
13 Struktura raspodijeljenog posla(engl. Work Breakdown Structure - WBS)	59
14 Kontrolne točke projekta	59
15 Gantogram	59
16 Zapisnici sastanaka	59
Literatura	60
A Dodatak A: Indeks (slika, tablica, ispisa koda)	61

1 Puni naziv projekta

Metode uspostave VPN servera, VPN kijenta te njihovo povezivanje prikazano za operacijske sustave Windows, Linux i FreeBSD

2 Skraćeni naziv projekta

Što je VPN poslužitelj i kako ga postaviti

3 Opis problema/teme projekta

Virtualna privatna mreža (engl. VPN, virtual private network) je tehnologija koja omogućava sigurno povezivanje privatnih mreža preko javne mrežne infrastrukture. VPN je razvijen kako bi se geografski udaljenim korisnicima omogućio siguran pristup privatnoj mreži.^[1] Do potrebe za takvom tehnologijom je došlo devedesetih godina te se ona u početku razvijala samo za velike organizacije koje su zahtijevale siguran prijenos osjetljivih podataka putem interneta. Kroz godine komercijalizacija interneta omogućila je većini država pristup najvećoj mreži što je drastično povećalo broj potencijalnih žrtava tadašnjih hakera. Nakon brojnih provala u sustave velikih tvrtki svakodnevni korisnici postali su svjesni loše sigurnosti interneta zbog čega raste potražnja tehnologija koje poboljšavaju mrežnu sigurnost.

Zaštita podataka osigurava se šifriranjem i dodavanjem posebnih zaglavlja na postojeći paket kako bi se osigurala njegova autentičnost, integritet i povjerljivost, koji su neki od osnovnih sigurnosnih zahtjeva. Šifriranje se odnosi na postupak pretvaranja izvornog teksta u šifrirani tekst pri čemu se koriste ključevi i prikladni algoritmi (npr. AES, RSA). Obrnuti proces, dešifriranje, provodi se kako bi samo korisnik koji posjeduje odgovarajući ključ mogao čitati izvoran tekst. U kontekstu mrežne sigurnosti šifriranje koristimo za zaštitu zaglavlja i podataka koji se nalaze unutar paketa.^[2]

Jedan od najpoznatijih i najsigurnijih skupova protokola koji se koristi u VPN tehnologijama je sigurni IP (engl. Internet Protocol Security, IPsec). IPsec uključuje protokole mrežnog sloja kako bi se omogućila sigurna razmjena podataka između parova mreža (engl. network-to-network), računala (engl. host-to-host) ili računala i mreža (netwerk-to-host). Neki od korištenih protokola su AH (engl. Authentication Header) kojim se postiže autentičnost paketa i ESP (engl. Encapsulating Security Payload) čija je zadaća da osigura povjerljivost podataka i informacija. Uz IPsec često korišteni skupovi protokola su: OpenVPN, PPTP, SoftEther i WireGuard.

U današnje vrijeme moguće je birati između mnogo pružatelja VPN usluga od kojih su neki besplatni dok su ostali dostupni kroz mjesecne ili godišnje pretplate. Besplatne se VPN usluge možda čine kao dobro rješenje za siguran prijenos podataka, ali pružatelje takvih usluga ništa ne sprječava od prodaje naših podataka ili korištenja istih u vlastitu korist. Još jedna opcija je postavljanje vlastitog VPN poslužitelja što može izgledati kao

dugotrajan i naporan posao, ali ovakvo nam rješenje omogućava da sami odlučimo kako želimo zaštititi prijenos vlastitih podataka. U ostaku rada nalazi se pregled, usporedba i upute za instalaciju poznatijih VPN tehnologija na različitim platformama.

4 Cilj projekta

Cilj je ovoga projekta objasniti i prikazati neke od načina na koje svaki korisnik može uspostaviti svoj VPN poslužitelj, konfigurirati ga, stvoriti VPN klijente te povezati ih na vlastiti poslužitelj. Kako bi što više čitatelja moglo koristiti ovaj dokument, prikazan je postupak instalacije više nekomercionalnih programa na tri često korištena operacijska sustava: Microsoft Windows, Linux i FreeBSD. Budući da većina korisnika ne razlikuje funkcionalne detalje pojedinih programa, na kraju dokumenta dostupna je usporedba nekih značajki pojedinih programske rješenja.

Načini uporabe i detaljne funkcionalnosti programa izlaze van okvira ovog dokumenta.

5 Voditelj studentskog tima

6 Rezultati

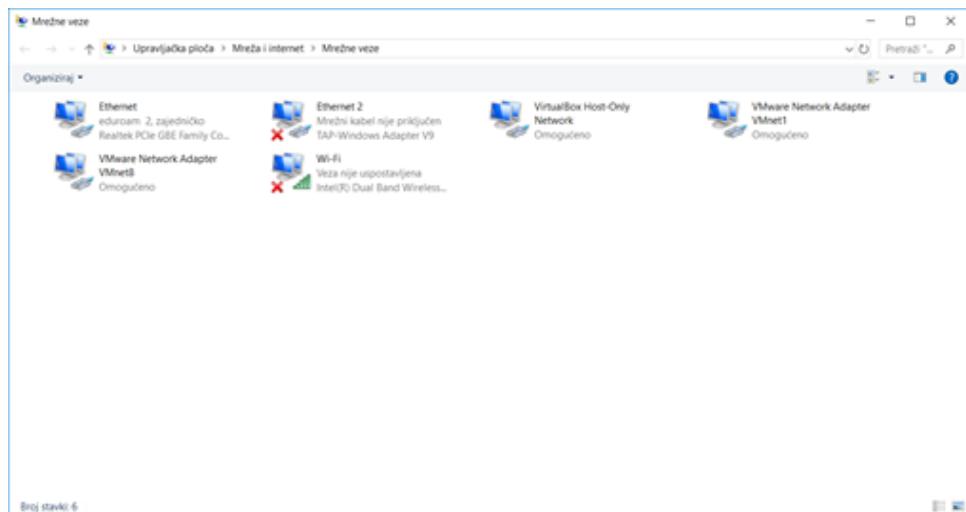
6.1 Windows

6.1.1 Windows 10 VPN

Kada želimo uspostaviti vlastiti besplatan VPN, jedna opcija je ugrađeni VPN koji Windows 10 ima. U ovom poglavlju nalazi se objašnjenje korak po korak kako ga uspostaviti.

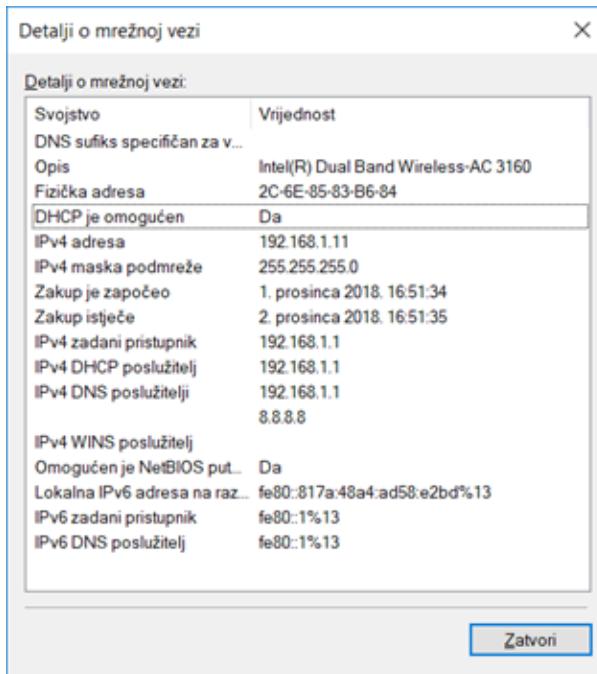
1. Korak: moramo računalu dodijeliti statičku lokalnu IP adresu

Otvorimo Postavke, Mreža i Internet, u izborniku s lijeve strane Ethernet i naposljetku opciju Promjena mogućnosti prilagodnika.Nakon toga dobili smo ovakav prozor:



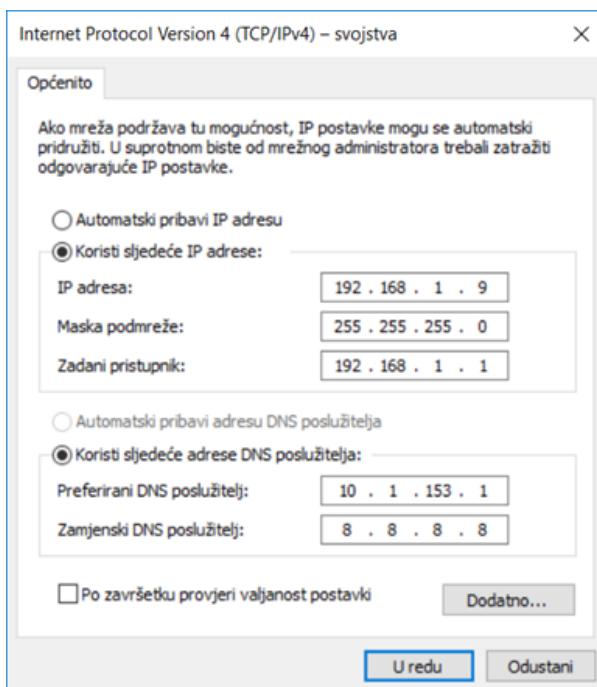
Slika 1: Prozor Promjena mogućnosti prilagodnika

Ovdje nam je bitna samo ikona Ethernet, otvorit ćemo ju desnim klikom miša te odabratи Stanje, Detalji... i dobit ćemo ovakav prozor:



Slika 2: Prozor Detalji o mrežnoj dijagnostici

Pogledamo podatak o IPv4 adresi, zapamtimo te brojeve i moramo ih upisati kada zatvorimo trenutni prozor i u prošlom prozoru gdje smo otvorili detalje sada otvorimo Svojstva te odaberemo stavku Internet Protocol Version 4 (TCP/IPv4) te ponovno odaberemo Svojstva. U novom prozoru koji smo dobili ponovno nam trebaju oni brojevi koje smo zapamtili(IP adresa) i s njima popunimo podatke kao na slici:

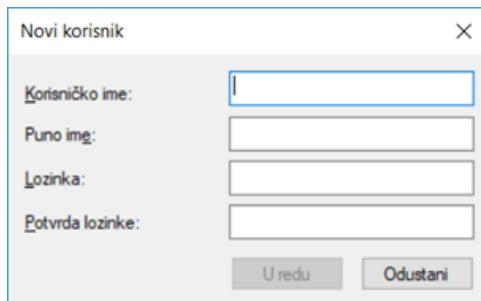


Slika 3: Svojstva (IPv4)

Kliknemo U redu i gotovi smo s prvim korakom.

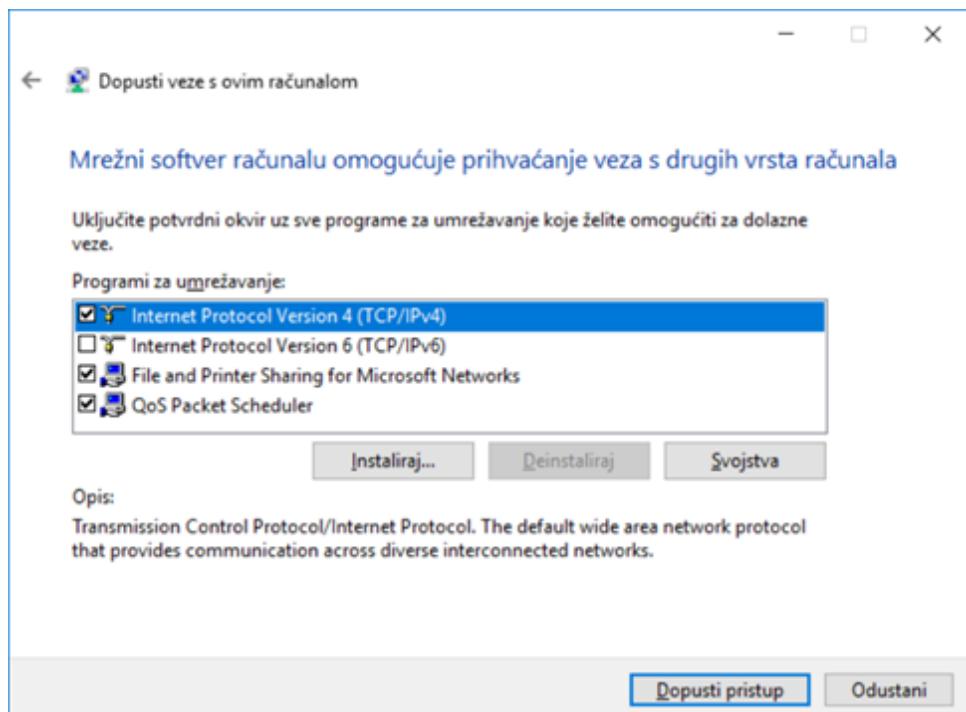
2. Korak: Postaviti VPN server

Vratimo se u prozor Promjena mogućnosti prilagodnika sa slike 1, tamo pritisnemo tipku Alt te u alatnoj traci koja se pojavila odaberemo karticu Datoteka, Nova dolazna veza. U dobivenom prozoru odaberemo Dodaj osobu te popunimo prozor Novi korisnik po želji, ali pazeći pri tome da lozinka bude jaka (kombinacija brojeva, velikih i malih slova).



Slika 4: Prozor Novi korisnik

Nakon toga označimo stvoreni profil i odaberemo Dalje, u novom prozoru označimo kvačicom opciju koju nam nudi te ponovno stisnemo Dalje. U sljedećem koraku kliknemo Dopusti pristup ako su polja označena kao na slici 5.



Slika 5: Dopusti veze s ovim računalom

Dobili smo prozor koji prikazuje ime računala koje će nam trebati kasnije da se spojimo na naš VPN.

3. Korak: Postaviti usmjeritelj da prosljeđuje priključak 1723

Ponovno otvorimo prozor detalji o mrežnoj dijagnostici sa slike 2. i brojeve u retku IPv4 zadani pristupnik prepišemo u web-preglednik kako bi pristupili postavkama usmjeritelja. Ako ne znamo korisničko ime i lozinku, a nismo ih mijenjali možemo pronaći pretpostavljene za svaki usmjeritelj na stranici <https://portforward.com/router-password/>. Kada se prijavimo u izborniku odaberemo prvo Application, a zatim Port Forwarding. Upišemo podatke kao sa slike 6. te odaberemo Add.

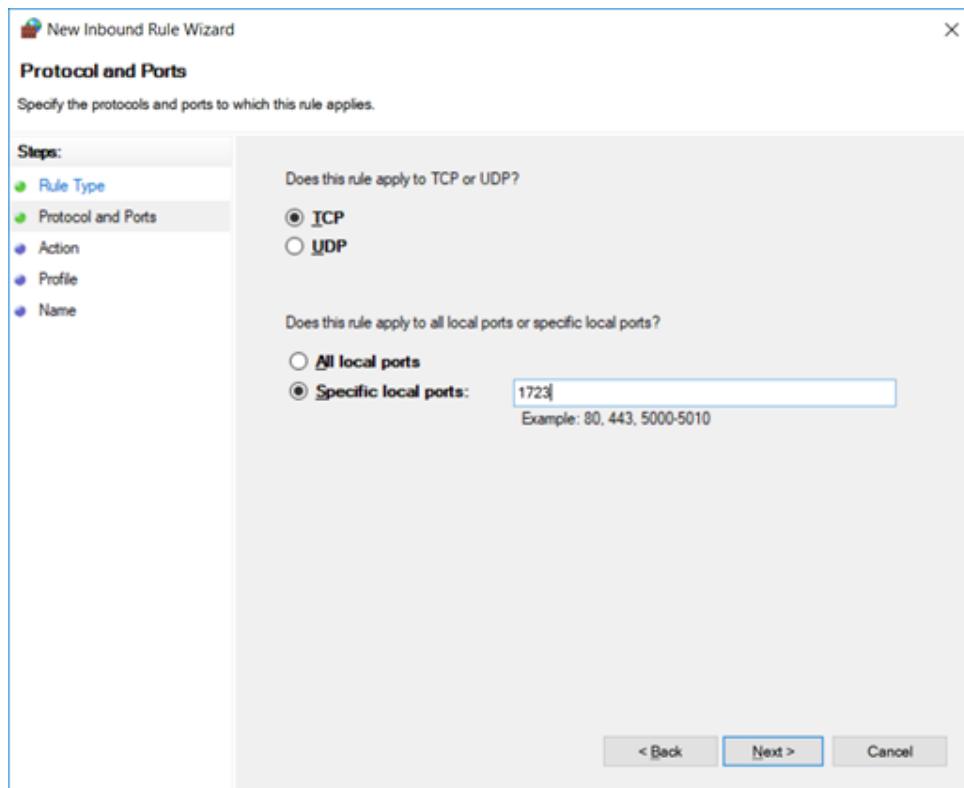
Path:Application-Port Forwarding Logout

<input checked="" type="checkbox"/> Enable	Name <input type="text" value="1723"/>	Protocol <input type="button" value="TCP AND UDP"/>					
WAN Host Start IP Address <input type="text"/>	WAN Host End IP Address <input type="text"/>	WAN Connection <input type="button" value="Internet_VDSL"/>					
WAN Start Port <input type="text" value="1723"/>	WAN End Port <input type="text" value="1723"/>	Enable MAC Mapping <input type="checkbox"/>					
LAN Host IP Address <input type="text" value="192.168.1.9"/>	LAN Host Start Port <input type="text" value="1723"/>	LAN Host End Port <input type="text" value="1723"/>					
<input type="button" value="Add"/>							
Enable	Name	WAN Host Start IP Address	WAN Start Port	LAN Host Start Port	WAN Connection	Modify	Delete
Protocol		WAN Host End IP Address	WAN End Port	LAN Host End Port	LAN Host Address		
There is no data, please add one first.							

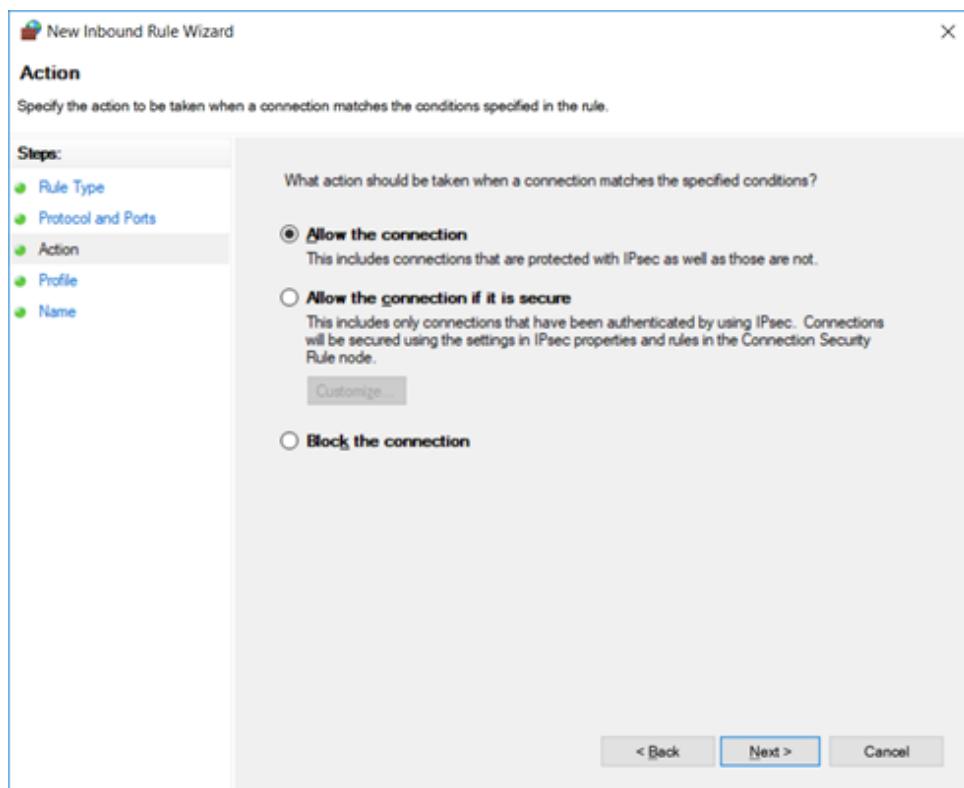
Slika 6: Postavke usmjeritelja za prosljeđivanje

4. Korak: Postavke Vatrozida za VPN promet

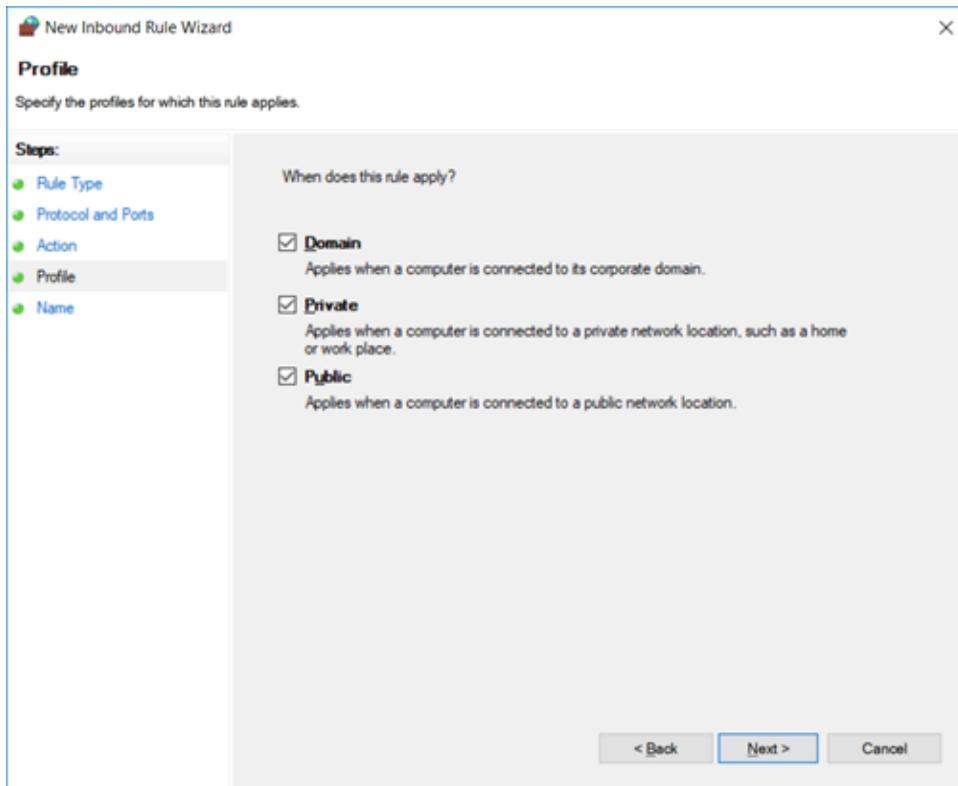
Na Upravljačkoj ploči odaberemo Vatrozid, Dodatne postavke, Inbound Rules, New Rule. U prozoru koji se otvori odaberemo Port i stisnemo Next. Na slici 7., 8. i 9. vidimo kako trebaju izgledati sljedeći prozori. Kada ih popunimo tako kliknemo Next.



Slika 7: Dodavanje pravila za port 1723



Slika 8: Doprštanje veze



Slika 9: Odabir kada se pravilo primjenjuje

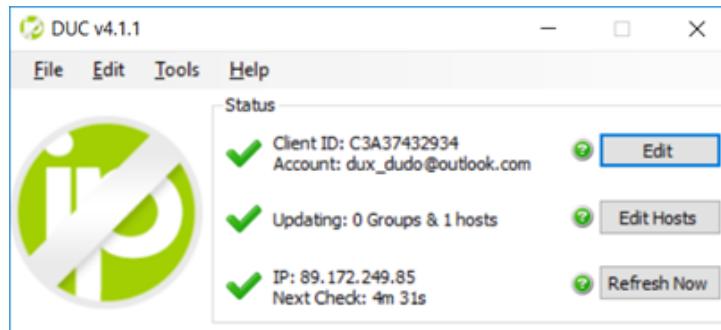
U sljedećem prozoru za ime napišemo 1723, a polje za opis možemo i ostaviti prazno te odaberemo Finish. Sada ponovno odaberemo New Rule i sve ponovimo osim što u prozoru sa slike 7. odaberemo UTP te u zadnjem koraku odaberemo različito ime, npr. 1723udp. Sada na stranici

<https://www.yougetsignal.com/tools/open-ports/> testiramo je li port 1723 zaista otvoren i ako dobijemo poruku da je sve je u redu i gotovi smo s korakom 4.

5. Korak: Postavljanje domene

Na stranici

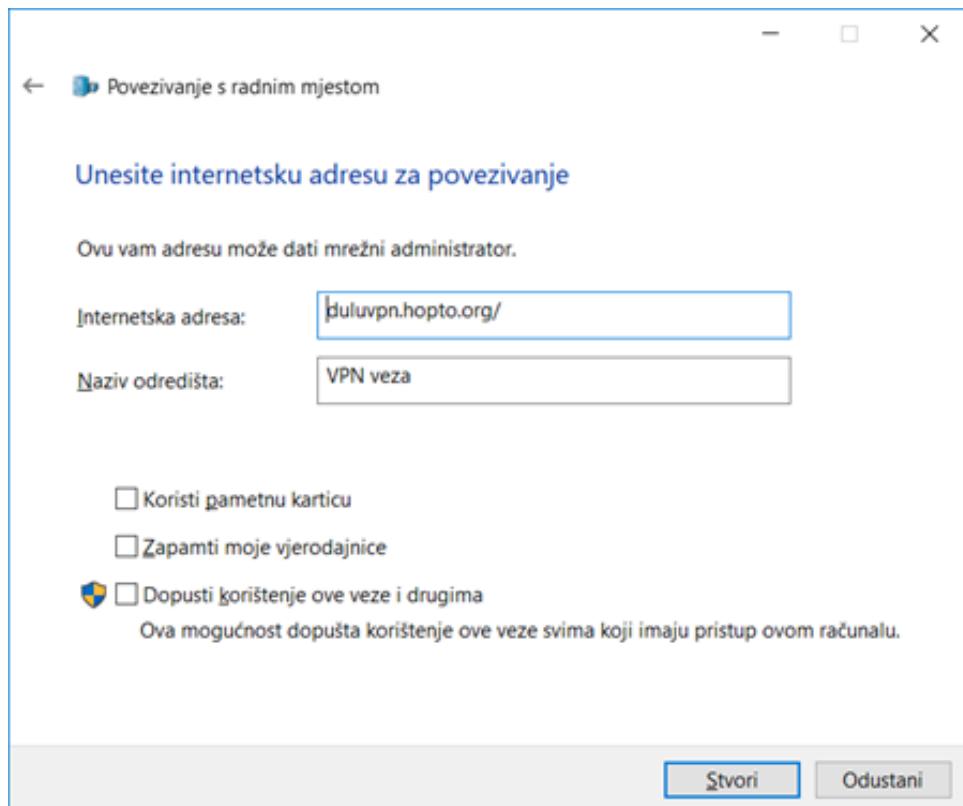
<https://www.noip.com/> izradimo besplatan račun i odaberemo slobodnu domenu koju ćemo lako zapamtiti. Sada je naša javna IP-adresa povezana s imenom domene. Nakon aktivacije računa trebamo skinuti i instalirati Dynamic DNS Update Client (<https://www.noip.com/download?page=win>) koji stalno provjerava promjene vezane za IP-adresu. U zadnjem koraku instalacije označimo obadvije kućice (Launch i Run DUC as System Service in the background). Nakon instalacije otvoriti se prostor za prijavu pa se prijavimo s podacima s kojima smo izradili račun. Označimo kućicu kraj imena stvorene domene i odaberemo Save i dobijemo ovakav prozor:



Slika 10: DUC

6. Korak: Povezivanje na VPN

Sada je sve spremno za povezivanje na naš VPN. Na računalu s kojim se želimo povezati otvorimo Centar za mreže i zajedničko korištenje, Postavljanje nove veze ili mreže, Povezivanje s radnim mjestom, Koristi internetsku vezu (VPN). U prozoru na slici 11. za polje Internetska adresa možemo upisati domenu ili javnu IP-adresu.



Slika 11: Adresa povezivanja

I zadnja stvar koju treba napraviti je na klijentskom računalu u postavkama mreže i interneta odabrati VPN vezu te upisati korisničko ime i lozinku iz drugog koraka i sada smo povezani na naš VPN.

6.1.2 SoftEther VPN

Što je SoftEther VPN?

SoftEther VPN^[3] besplatan je višeplatformski program otvorenog koda koji podržava korištenje različitih VPN protokola. Program je nastao 2013. godine kao akademski projekt na sveučilištu u Tsukubi i podržan je na različitim operacijskim sustavima kao što su Linux, FreeBSD, Mac, Solaris i Windows za koji je u ovom poglavljju prikazan postupak postavljanja i uporabe.

Program SoftEther otvorenog je koda pa ga može bilo tko koristiti za vlastite ili komercijalne svrhe.

SoftEther VPN koristi HTTPS preko SSL (Secure Sockets Layer)^[4] protokola kako bi omogućio siguran prijenos kriptiranih podataka preko Interneta. Uz njega su podržani unutar programa i ostali poznatiji protokoli kao što su OpenVpn, IPsec, L2TP, ... Unutar programa sve postavke detaljno su objašnjene i mogu se podesiti korištenjem grafičkog sučelja što ovaj program čini jednostavnim za uporabu.

Instalacija SoftEther servera

Za početak potrebno je preuzeti instalaciju VPN servera sa službene stranice SoftEthera:

<https://www.softether.org>



Slika 13: Put do instalacije

Odabirom "Download" iz izborne trake prikazuje se stranica s ponuđenim poveznicama za preuzimanje.

Download

SoftEther VPN is [open-source free software](#). You may use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of SoftEther VPN.

Primary Download Server (hosted by Windows Azure):

- [Download SoftEther VPN](#) ↗

Language: English, Japanese and Simplified Chinese.
OS: Windows, Linux, Mac OS X, FreeBSD and Solaris.

Slika 14: Poveznica za odabir preuzimanja

Sljedeći isječak prikazuje stranicu koja se otvori odabirom prve poveznice. Na stranici se nalaze izborni okviri u kojima je potrebno odabrati željeni program. Za preuzimanje VPN servera potrebno je odabrati postavke prikazane na sljedećem isječku te odabrati prvu poveznicu za početak preuzimanja.

Select Software
SoftEther VPN (Freeware)

Select Component
SoftEther VPN Server Manager for Windows

Select Platform
Windows

Select CPU
Intel (x86 and x64)

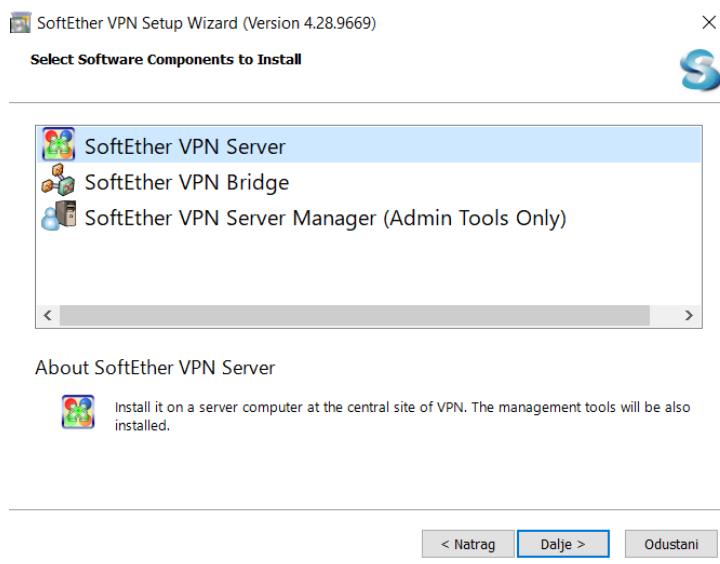
Download Files (68)

Note: The following program uses the network functions of the operating system because this is VPN software.
Some anti-virus software or firewalls warn that such behavior might be dangerous.
If your anti-virus disturbs the VPN function, add the VPN program file or the installer to the exception list.

SoftEther VPN Server and VPN Bridge (Ver 4.28, Build 9669, beta) ↗
softether-vpnserver_vpnbridge-v4.28-9669-beta-2018.09.11-windows-x86_x64-intel.exe (44.89 MB)
[Non-SSL (HTTP) Download Link] Try this if the above link fails because your HTTP client doesn't support TLS 1.2.
Release Date: 2018-09-11 <[Latest Build](#)>
What's new ([ChangeLog](#))
Languages: English, Japanese, Simplified Chinese
OS: Windows, CPU: Intel (x86 and x64)
(Windows 98 / 98 SE / ME / NT 4.0 SP6a / 2000 SP4 / XP SP2, SP3 / Vista SP1, SP2 / 7 SP1 / 8 / 8.1 / 10 / Server 2003 SP2 / Server 2008 SP1, SP2 / Hyper-V Server 2008 / Server 2008 R2 SP1 / Hyper-V Server 2008 R2 / Server 2012 / Hyper-V Server 2012 / Server 2012 R2 / Hyper-V Server 2012 R2 / Server 2016)

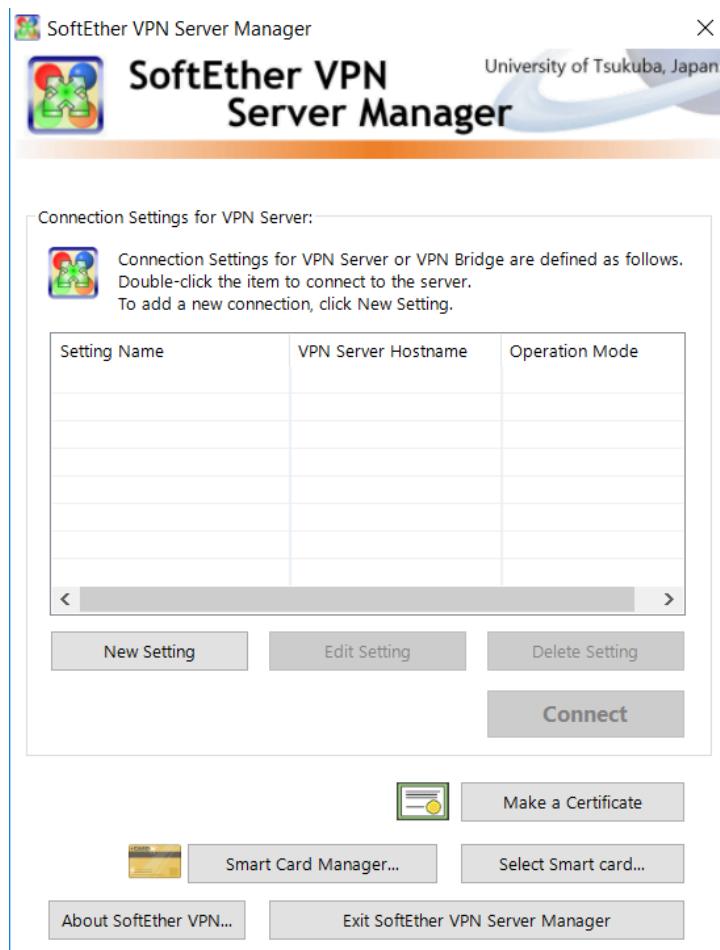
Slika 15: Prikaz povaznice za preuzimanje

Nakon preuzimanja i pokretanja instalacije otvara se sljedeći prozor u kojemu se predlaže odabir prvog ponuđenog jer nudi potpunu instalaciju.



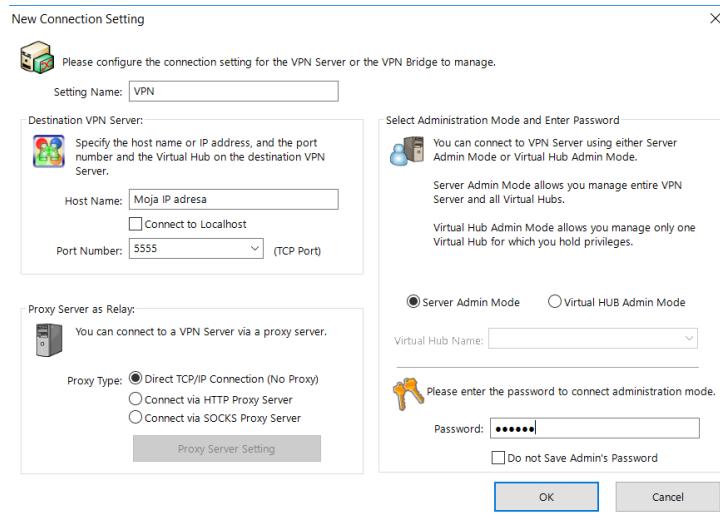
Slika 16: Odabir servera

Nakon uspješne instalacije prikazuje se sljedeći okvir u kojem još nema niti jednog servera. Dodavanje servera započinje se odabirom "New Setting".



Slika 17: Početni prozor aplikacije SoftEther

Stvaranje servera započinje se upisom željenog naziva u polje “setting name” i upisom vlastite IP adrese preko koje je trenutno računalo spojeno na Internet. Preporuka je dodati lozinku za pristup serveru radi dodatne sigurnosti u polje “password”.



Slika 18: Dodavanje nove veze

U tablici sada vidimo da je dodan novi server kojeg je potrebno konfigurirati odabriom “Connect” opcije.

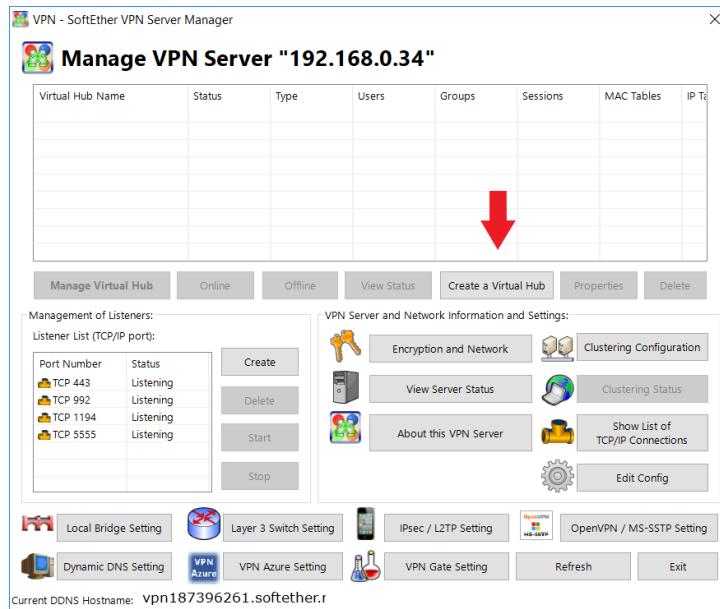
Setting Name	VPN Server Hostname	Operation Mode
VPN	192.168.0.34	Entire VPN Server
< >		

New Setting Edit Setting Delete Setting

Connect

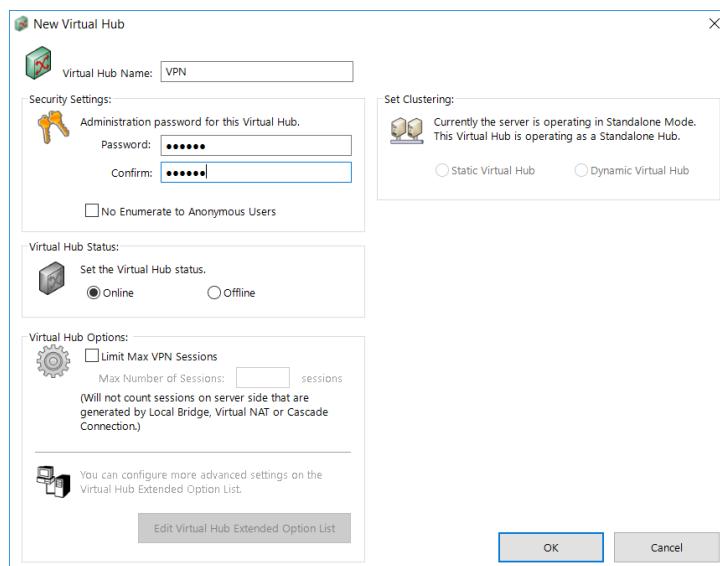
Slika 19: Odabir konfiguracije

Kako bi se druga računala uspjela povezati s napravljenim serverom, potrebno je dodati virtualno čvorište odabriom opcije “Create a Virtual Hub”.



Slika 20: Mogućnosti servera

Virtualnom čvorištu postavljamo proizvoljno ime te dodajemo lozinku radi dodatne sigurnosti.



Slika 21: Dodavanje virtualnog čvorišta

Sada se može vidjeti novo dodano čvorište u tablici.

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
VPN	Online	Standalone	0	0	1	0	0

[Manage Virtual Hub](#) [Online](#) [Offline](#) [View Status](#) [Create a Virtual Hub](#) [Properties](#) [Delete](#)

Slika 22: Dodavanje virtualnog čvorista

Sljedeći je korak odrediti tko se sve može povezati na naš server, a to se radi odabirom gumba “Manage Virtual Hub”.

Item	Value
Virtual Hub Name	VPN
Status	Online
Type	Standalone
SecureNAT	Disabled
Sessions	1
Access Lists	0
Users	0
Groups	0
MAC Tables	0
IP Tables	0

Slika 23: Korisnici servera

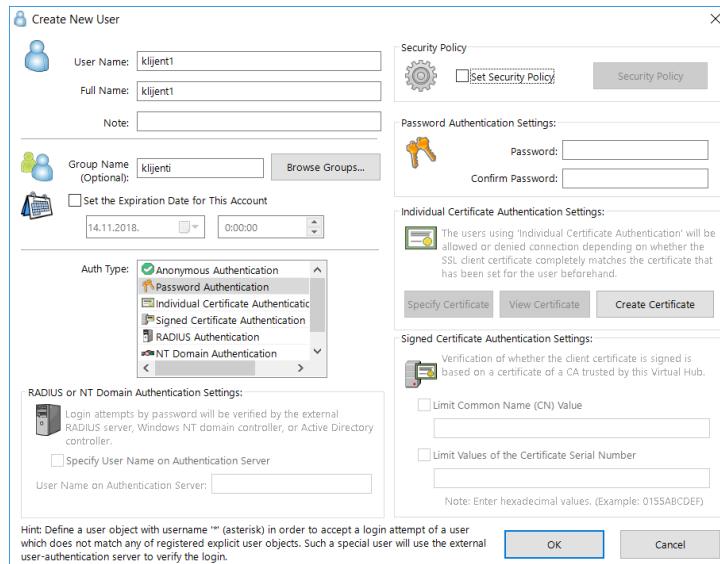
Na ovom prozoru odabiremo “Manage Users”.

User Name	Full Name	Group Name	Description	Auth Method	Num Logins	Last Login

[New](#) [Edit](#) [View User Info](#) [Remove](#) [Refresh](#) [Exit](#)

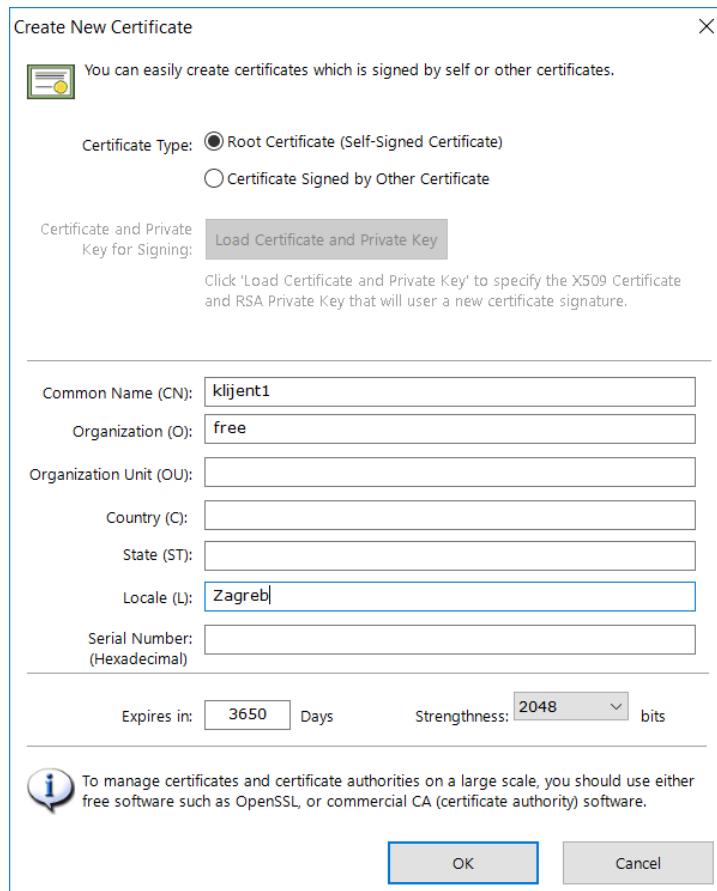
Slika 24: Popis korisnika

Sada dodajemo korisnika kojem ćemo dodati proizvoljno ime (u ovim je uputama korisnik nazvan “klijent1” i u svim narednim koracima gdje se to ime pojavljuje vama će se pojaviti vaše odabrano ime). Kako bismo smanjili vjerojatnost zlouporabe VPN-a, odabiremo mogućnost prijave klijenta uporabom našeg certifikata i lozinke. Zbog toga odabiremo “Create Certificate”.



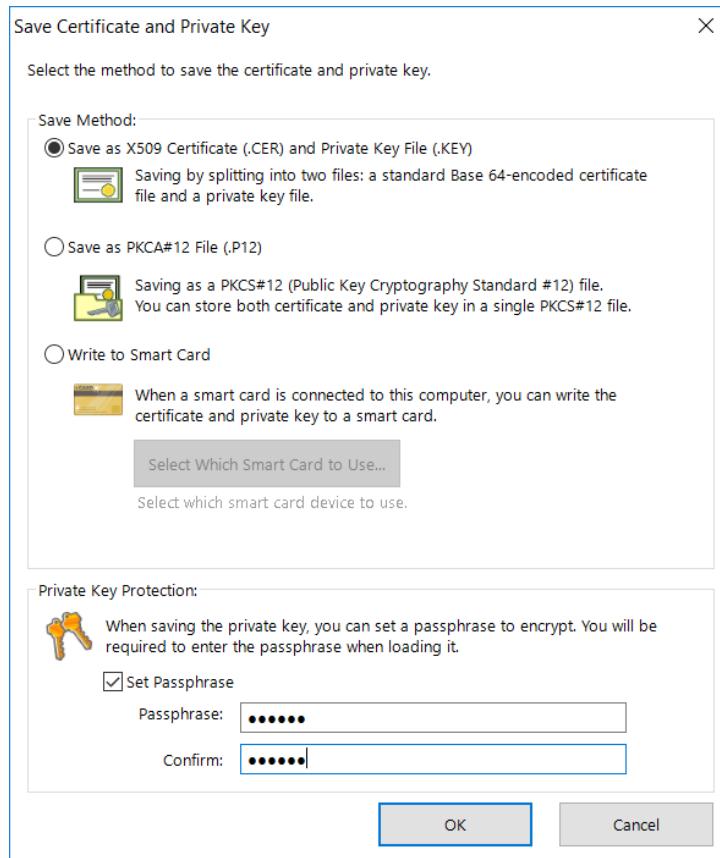
Slika 25: Stvaranje korisnika

U sljedećim je poljima moguće detaljno odrediti opis stvorenog klijenta kao i vrijeme njegovog postojanja.



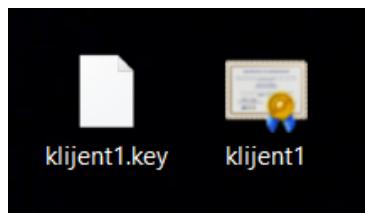
Slika 26: Stvaranje certifikata korisnika

Nakon otvaranja ovog prozora postavljamo lozinku kojom će se naš klijent prijavljivati na server i koja će samo njemu biti poznata.



Slika 27: Stvaranje ključa korisnika

Nakon potvrde nastaju dvije datoteke: jedna je .cer, a druga je .key i obje su neophodne za prijavu na naš server zato ih mi moramo spremiti i prebaciti na računala koja će se htjeti povezati na server. Povezivanje na server objašnjeno je u jednom od sljedećih dijelova poglavlja.



Slika 28: Datoteke ključ i certifikat

Nakon potvrde vidljiv je korisnik koji se može spojiti na naš server. Moguće je naravno dodavanje više različitih korisnika i brisanje istih.

Virtual Hub "VPN" has the following users.						
User Name	Full Name	Group Name	Description	Auth Method	Num Logins	Last Login
klijent1	klijent1	-		Individual Certific...	0	(None)

Slika 29: Prikaz dodanog korisnika

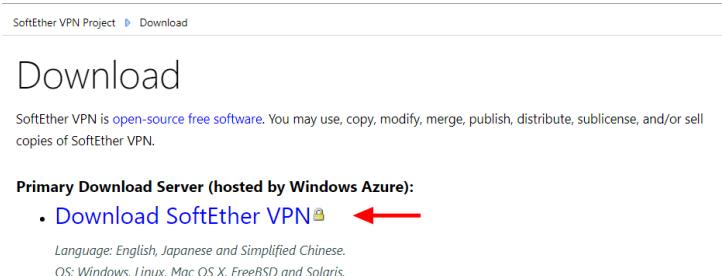
Instalacija SoftEther klijenta

Za razliku od instalacije i konfiguracije servera, instalacija je SoftEther klijenta jednostavnija. Prvi je korak preuzimanje instalacije sa službene stranice SoftEthera:
<https://www.softether.org>



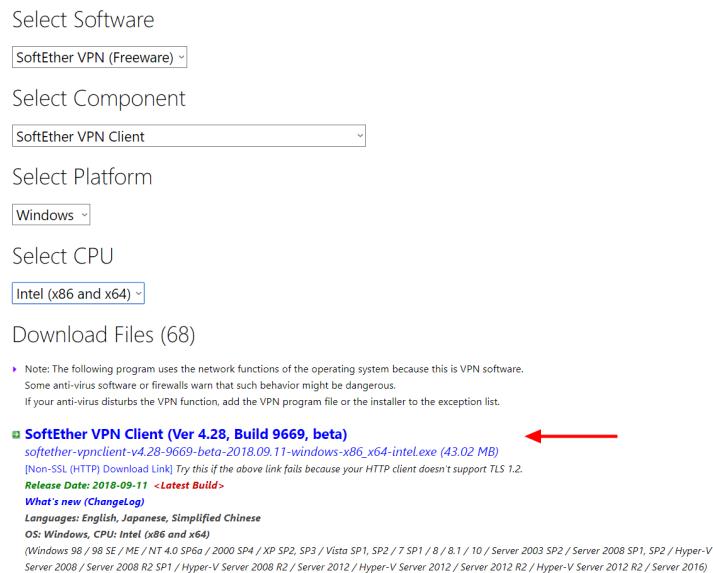
Slika 30: Put do instalacije

Odabirom "Download" iz izborne trake prikazuje se stranica s ponuđenim poveznicama za preuzimanje.



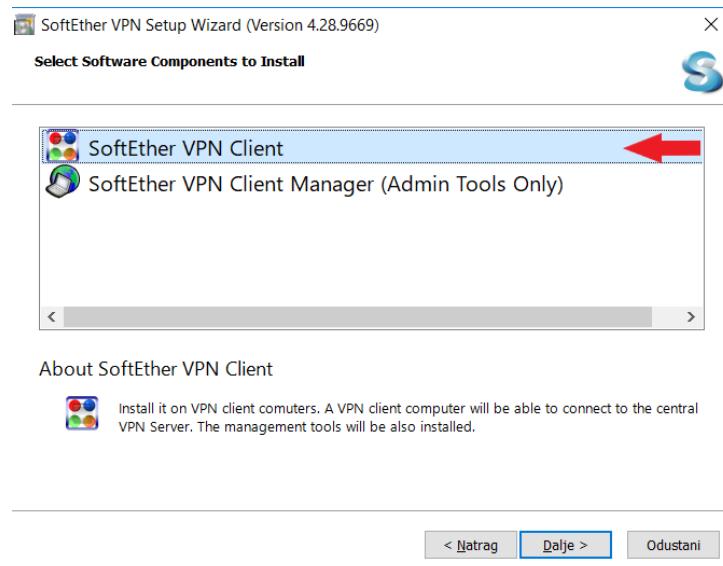
Slika 31: Poveznica za odabir preuzimanja

Sljedeći isječak prikazuje stranicu koja se otvori odabirom prve poveznice. Na stranici se nalaze izborni okviri u kojima je potrebno odabrati željeni program. Za preuzimanje VPN klijenta potrebno je odabrati postavke prikazane na sljedećem isječku te odabrati prvu poveznicu za početak preuzimanja.



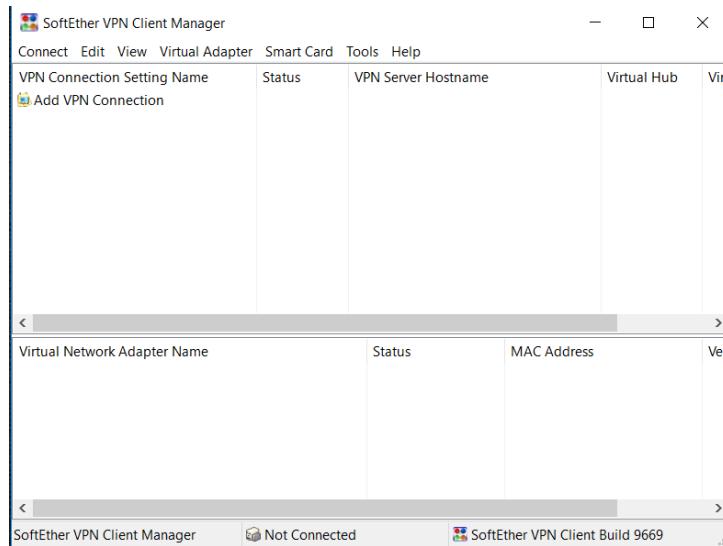
Slika 32: Prikaz povaznice za preuzimanje

Nakon završetka preuzimanja i pokretanja instalacije prikazuje se sljedeći prozor. Preporuka je odabrati prvo ponuđeno jer nudi potpunu instalaciju programa.



Slika 33: Prikaz odabira klijentske instalacije

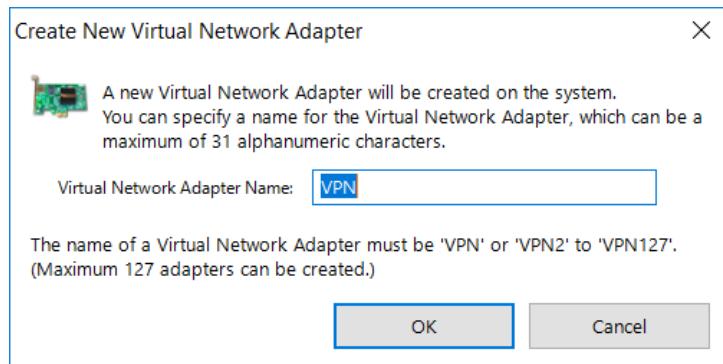
Ukoliko je instalacija uspješno završena, prikazuje se sljedeći prozor.



Slika 34: Prikaz upravitelja VPN veza

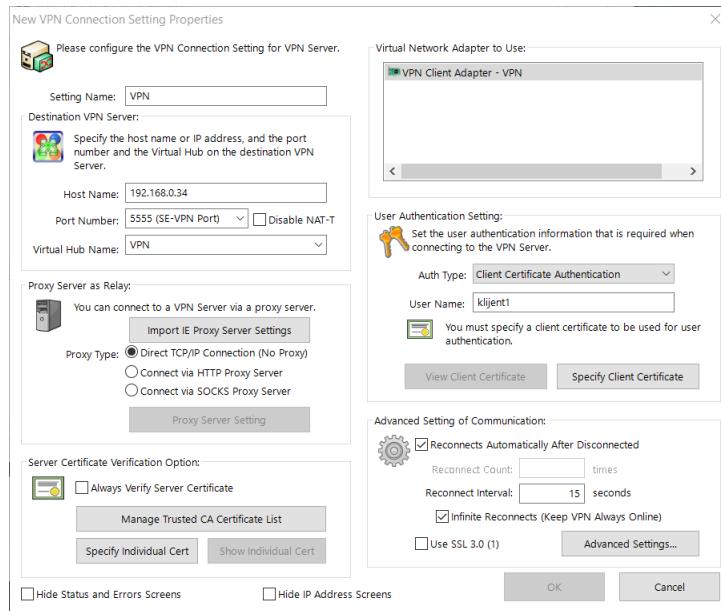
Povezivanje klijenta sa SoftEther serverom

Za uspješno povezivanje s napravljenim serverom potrebno je pokrenuti aplikaciju SoftEther VPN Client i odabrati opciju dodavanja novog VPN-a. Ako nije postavljen virtualni mrežni adapter, kao što je prikazano u sljedećem primjeru, potrebno je stvoriti novi. Prikazano je stvaranje VPN adaptora.



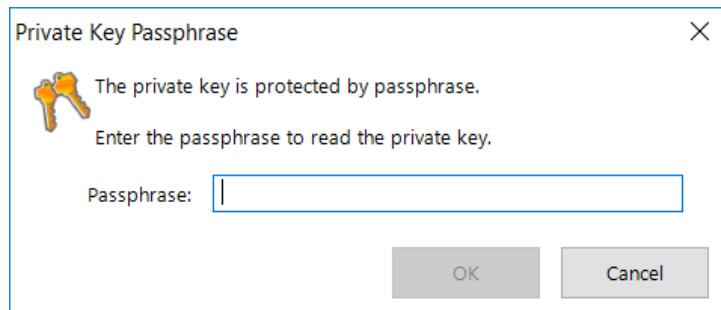
Slika 35: Stvaranje adaptora

Nakon stvaranja adaptora moramo dodati server na koji se želimo povezati. Na slici je prikazano stvaranje veze koja se zove VPN. Slično kao i kod stvaranja servera, potrebno je upisati IP adresu preko koje se može serveru pristupiti u polje "Host name". Aplikacija nakon upisa IP adrese dohvaca portove na koje se moguće spojiti. Izbor je nekog od ponuđenih portova proizvoljan, kao i postojećih virtualnih mrežnih adaptera. Budući da smo prilikom stvaranja korisnika servera odabrali da se on može prijaviti samo uporabom certifikata i pripadnog ključa, potrebno je stvorene datoteke "klijent1.cer" i "klijent1.key" prebaciti na računalo s kojeg se pokušava povezati na server. Učitavanje certifikata i ključa u aplikaciju obavlja se odabirom opcije "specify client certificate".



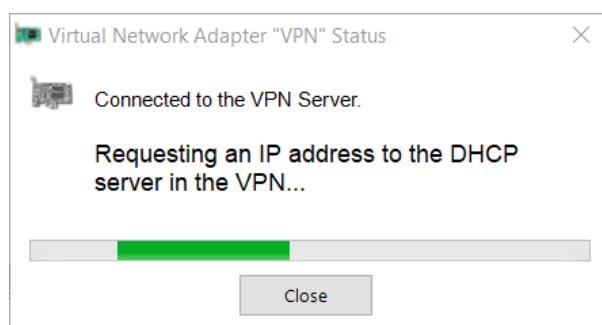
Slika 36: Dodavanje VPN veze

Nakon učitavanja datoteke prikazuje se prozor sa sljedećeg isječka u koji se upisuje lozinka koju smo postavili prilikom stvaranja klijenta.



Slika 37: Polje lozinke

Ako smo učitali ispravni certifikat i unijeli ispravnu lozinku, tada će se prikazati prozor na kojem vidimo povezivanje s VPN serverom.



Slika 38: Spajanje na server

6.1.3 Tinc

Tinc je besplatan program za uspostavu VPN veze. Ono po čemu se tinc razlikuje od drugih programa je niz jedinstvenih mogućnosti koje uključuje, kao što su enkripcija, neobavezna kompresija, automatsko usmjeravanje u mreži „svatko sa svakim“, lagano proširivanje... Ove mogućnosti čine tinc jako dobrom rješenjem za poslovne mreže koje su sastavljene od velikog broja manjih udaljenih mreža.

Instalacija

Preuzmemmo instalacijski paket s adrese

<http://www.tinc-vpn.org/packages/windows/tinc-1.1pre15-install.exe> te obavimo standardi instalacijski postupak, pokrenemo installer, next, prihvativmo uvjete korištenja, Ok, označimo sva polja kada nas pita koje komponente želimo instalirati, next, install, finish. Sada otvorimo mapu u koju smo instalirali tinc (vjerojatno C:\Program Files\tinc) unutar komandne linije koju smo pokrenuli kao administrator, pozicioniramo se u mapu C:\Program Files\tinc te upisujemo redom naredbe:

- tinc -n vpn init master
- tinc -n vpn add subnet 20.0.0.1
- tinc -n vpn add address=public.domain-or-ip
- cd tap-win64
- addtap.bat
- cd ..
- netsh interface ipv4 show interfaces (pogledamo što je odspojeno, vjerojatno Ethernet 2)
- netsh interface set interface name = "Ethernet 2" newname = "tinc"
- netsh interface ip set address "tinc" static 20.0.0.1 255.255.255.0
- netsh interface ipv4 show config (sada bi trebali imati sučelje „tinc“ s maskom podmreže i IP-adresom)

Time je postavljen glavni čvor, sada sličan postupak moramo ponoviti za računalo klijent. Na njemu također pokrenemo komandnu liniju kao administrator i pozicioniramo se u mapu gdje je tinc instaliran te upišemo sljedeće naredbe:

- tinc -n vpn init client1
- tinc -n vpn add connectto master

-
- tinc -n vpn add subnet 20.0.0.2
 - cd tap-win64
 - addtap.bat
 - cd ..
 - netsh interface ipv4 show interfaces (pogledamo što je odspojeno, vjerojatno Ethernet 2)
 - netsh interface set interface name = "Ethernet 2" newname = "tinc"
 - netsh interface ip set address "tinc" static 20.0.0.2 255.255.255.0

Potrebno je još samo s klijentskog računala kopirati datoteku vpn/hosts/client1 na računalo glavnog čvora u mapu vpn/hosts i s računala glavnog čvora kopirati datoteku vpn/hosts/master na klijentsko računalo u mapu vpn/hosts. Sada je sve spremno za korištenje.

Pokretanje

Kada je završena instalacija, tince se pokrene jednostavnom naredbom koja je jednaka za klijenta i poslužitelja:

- tincd -n vpn -D -d3

6.1.4 OpenVPN za Windows

Ukratko o OpenVPN tehnologiji

OpenVPN^[5] besplatan je program za ostvarenje vlastitog virtualnog privatnog tunela preko interneta. OpenVPN-om možemo ostvariti brojna rješenja povezivanja kao što su prijenos podataka, uporaba servera kao pristupne točke na internet, povezivanje udaljenih uređaja u logičku LAN mrežu,...

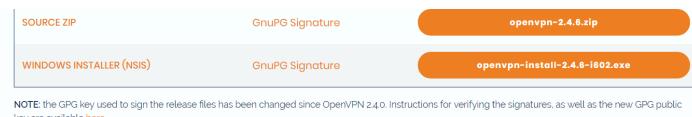
Neke svojstva OpenVPN povezivanja:

- sigurni virtualni tunel na internetu
- prijenos podataka TCP ili UDP protokolom
- odabir željene vrste šifriranja
- višestruko povezivanje
- povezivanje računala s različitim operacijskim sustavima

Instalacija OpenVPN servera

Za početak potrebno je preuzeti instalaciju VPN-a sa službene stranice OpenVPN-a:
<https://openvpn.net/community-downloads/>

Na službenoj stranici potrebno je pokrenuti preuzimanje verzije za operacijski sustav Windows:



Slika 39: Prikaz poveznice za preuzimanje

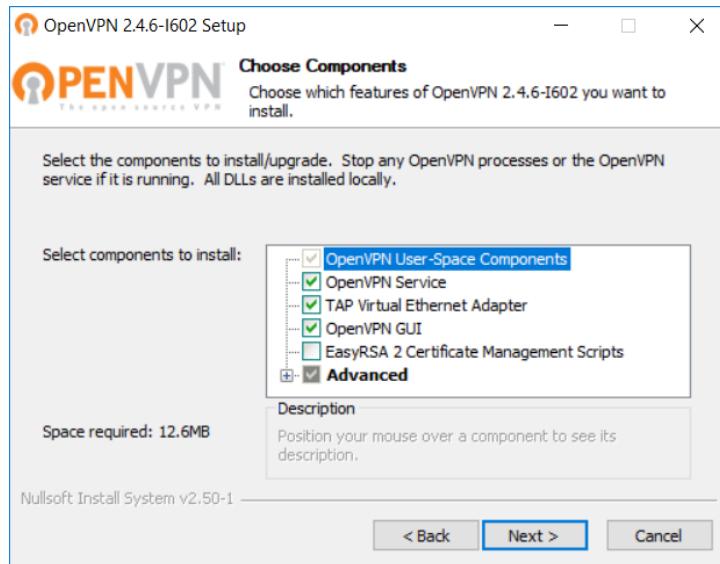
Ako je uspješno obavljeno preuzimanje, može se započeti instalacija pokretanjem programa s ovakvom ikonom.

Dalje je potrebno pratiti klasične korake instalacije programa. Kada vam program ponudi odabir direktorija instalacije, preporuka je da odaberete prepostavljeni direktorij jer su daljnje upute i konfiguracija pravljeni prema tom uzoru. Ako odaberete vlastiti, morate puteve prikazane u dalnjim koracima preoblikovati tako da vode do vašeg direktorija instalacije.

Obratite pažnju na sljedeću sliku jer prikazuje uz prepostavljene i važan odabir za uspješnu instalaciju. Potrebno je odabrati i instalirati “EasyRSA 2 Certificate Management Scripts”.



Slika 40: Ikona instalacije

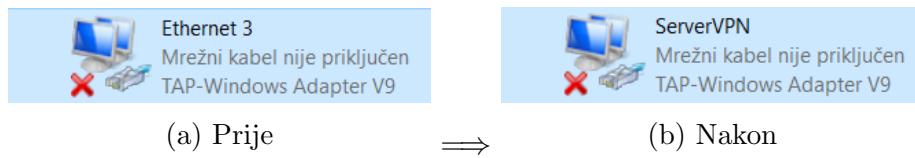


Slika 41: Prikaz dodataka instalacije

U sklopu instalacije programa obavljena je i instalacija virtualnog mrežnog priključka na računalu. Taj će se priključak koristiti za povezivanje poslužitelja i klijenata te je vidljiv u postavkama mreže računala:

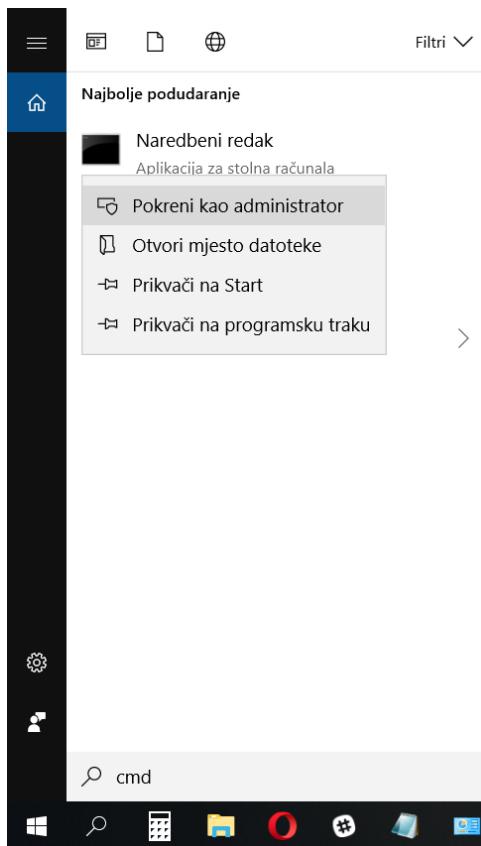
Upravljačka ploča/Sve stavke upravljačke ploče/Mrežne veze

Kako bismo ga lakše adresirali kasnije, promijenit ćemo mu ime u “ServerVPN”. Adapter se razlikuje od ostalih jer mu je opis “TAP-Windows Adapter V9”.



Slika 42: Preimenovanje TAP adaptera

Naredni se koraci izvode upisom naredbi u naredbeni redak. Potrebno je naredbeni redak pokrenuti kao administrator za što je prikazan jedan od mogućih načina na sljedećem isječku.



Slika 43: Pokretanje naredbenog retka u administratorskom načinu

Potrebno se pozicionirati u “easy-rsa” direktorij u instalacijskom direktoriju upisom naredbe:

```
cd "C:\Program Files\OpenVPN\easy-rsa"
```

Sada je potrebno upisivati po redu sljedeće naredbe.

```
init-config.bat
```

Naredba inicijalizira konfiguracijsku datoteku u kojoj možemo dodati informacije o vezi koju uspostavljamo. Ti podaci neće utjecati na rad servera i klijenata.

```
vars
```

```
clean-all
```

```
build-dh
```

```
C:\Program Files\OpenVPN\easy-rsa\openssl\bin>Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....
```

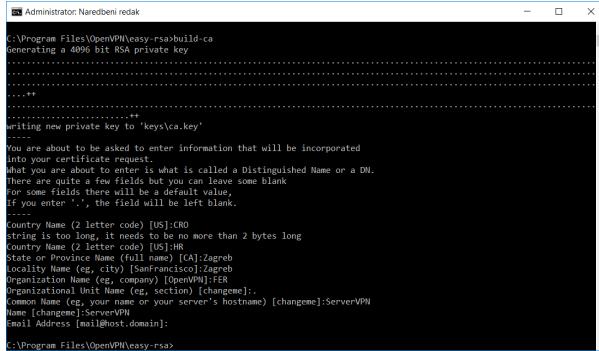
Slika 44: Prikaz pokretanja build-dh naredbe

Naredbom se stvara potrebna “.dh” datoteka. Na nekim inačicama operacijskog sustava Windows moguća je greška: “openssl” is not recognized ...

U tom slučaju otici u napredne postavke sustava i dodati “PATH” varijablu, tj. put do bin datoteke OpenVPN-a : C:\Program Files\OpenVPN\bin

```
build-ca
```

Ovom je naredbom započeto stvaranje certifikata potrebnih za sigurno povezivanje servera i klijentata. Prilikom izvršavanja naredbe program nudi polja koja je potrebno popuniti, tj. informacije o našem serveru kako bi se ugradile u ključ.



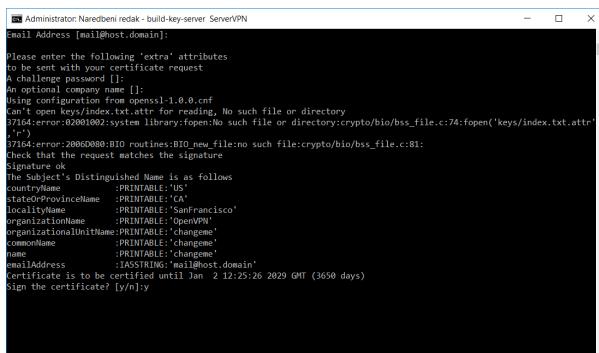
```
C:\Program Files\OpenVPN\easyrsa build-ca
Generating a 4096 bit RSA private key
.....+
.....+
writing new private key to 'keys\ca.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [US]:CR0
string is too long, it needs to be no more than 2 bytes long
Country Name (2 letter code) [US]:CR0
State or Province Name (full name) [CA]:Zagreb
Locality Name (eg, city) [SanFrancisco]:Zagreb
Organization Name (eg, company) [OpenVPN]:FER
Organization Unit Name (eg, section) [changeme]:.
Common Name (eg, your name or your server's hostname) [changeme]:ServerVPN
Email Address [mail@host.domain]:CR0
C:\Program Files\OpenVPN\easyrsa>
```

Slika 45: Stvaranje certifikata povezivanja

[build-key-server ServerVPN](#)

Ova naredba također nudi upis podataka, ali ovdje su polja ostavljena prazna jer nisu ključna za rad. Naredbom su nastale 3 datoteke u instalacijskom direktoriju “.crt”, “.csr” i “.key”.



```
Email Address [mail@host.domain]:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using C:\Program Files\OpenVPN\bin\openssl-1.0.0.cnf
Can't open keys/index.txt.attr for reading, No such file or directory
37164:error:02000080:system library:fopen:No such file or directory:crypto/bio/bss_file.c:74:fopen('keys/index.txt.attr','r')
37164:error:02000080:BIO routines:BIO_new_file:no such file:crypto/bio/bss_file.c:81:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'CR'
stateOrProvinceName :PRINTABLE:'CA'
localityName :PRINTABLE:'SanFrancisco'
organizationName :PRINTABLE:'OpenVPN'
organizationUnitName:PRINTABLE:'changeme'
commonName :PRINTABLE:'ServerVPN'
emailAddress :IA5STRING:'changeme'
(Certificate is to be certified until Jan 2 12:25:26 2029 GMT (3658 days)
Sign the certificate? [y/n]:y
```

Slika 46: Stvaranje certifikata servera

Idući korak stvaranje je certifikata klijenta.

[build-key KlijentVPN](#)

Po potrebi popuniti podacima o klijentu. Kako bi se razlikovao od ostalih, važno je popuniti polje “Common Name” kao na sljedećem isječku i potvrditi stvaranje.

```

Administrator: Naredbeni redak - build-key KlijentVPN
commonName :PRINTABLE:'changeMe'
name :PRINTABLE:'changeMe'
emailAddress :IASISTRING:'mail@host.domain'
Certificate is to be certified until Jan 2 12:25:26 2029 GMT (3650 days)
Sign the certificate? [y/n]y

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

C:\Program Files\OpenVPN\easy-rsa\build-key KlijentVPN
generating RSA private key
.....+-----+
.....+-----+
writing new private key to "keys\KlijentVPN.key"

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
If you enter '.', the field will be left blank.
.
.
.
Country Name (2 letter code) [US]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [changeMe]:
Common Name (eg, your name or your server's hostname) [changeMe]:KlijentVPN

```

Slika 47: Stvaranje certifikata klijenta

Kao i u prethodnom koraku nastale su 3 datoteke. Sve su neophodne za prijavu na naš server zato ih mi moramo spremiti i prebaciti na računala koja će se htjeti povezati na server. Povezivanje na server objašnjeno je u jednom od sljedećih dijelova poglavlja.

Moguće je naravno dodavanje više različitih korisnika i brisanje istih.

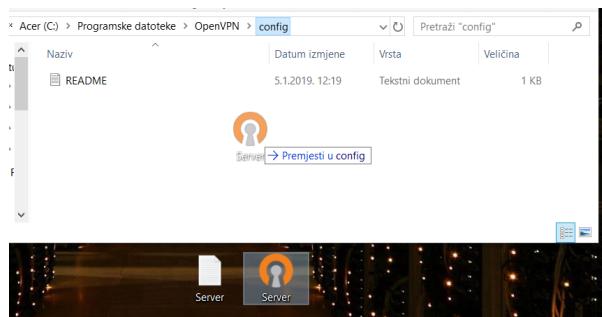
`openvpn --genkey --secret keys/ta.key`

Ovom naredbom stvara se ključ kojim se autentificiraju podaci između servera i klijenata.

Konfiguracija OpenVPN servera

Konfiguracijske datoteke ne postoje same po sebi pa ih je potrebno stvoriti na radnoj površini kao prazan tekstualni dokument, spremiti u obliku “ServerVPN.ovpn” datoteke pa kopirati u direktorij OpenVPN-a na lokaciju:

`C:\Program Files\OpenVPN\config`



Slika 48: Direktorij za konfiguraciju

“Server.ovpn” jest konfiguracijska datoteka stvorenog servera. OpenVPN nudi brojne postavke koje serveru daju širok izbor svojstava i mogućnosti. Naglasak ovih uputa je na povezivanju klijenata i servera te su dodane mogućnosti samo s tim ciljem.

Konfiguracijska datoteka treba sadržavati:

```

dev-node "ServerVPN" ;ime
mode server ;uloga u mreži
port 12345 ;vrata preko kojih ide komunikacija
proto tcp4-server ;protokol prijenosa
dev tun ;stvara se virtualni tunel

```

```

tls-server                                     ; za autentifikaciju
tls-auth "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\ta.key" 0
; put do datoteke ključa(ta.key) te broj 0 koja označava server
tun-mtu 1500                                    ;veličina MTU paketa
tun-mtu-extra 32                                ;veličina MTU paketa
mssfix 1450                                     ;veličina MTU paketa
ca "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\ca.crt"
; put do datoteke ca.crt
cert "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\ServerVPN.crt"
; put do certifikata servera
key "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\ServerVPN.key"
; put do ključa servera
dh "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\dh2048.pem"
; put do .dh datoteke
server 10.10.10.0 255.255.255.0
; virtualna adresa servera i maska podmreže
client-to-client                               ; klijenti se vide
keepalive 10 120                                ; vrijeme čekanja na vezu
cipher AES-128-CBC                            ; vrsta šifriranja
comp-lzo                                         ; kompresija podataka u tunelu
persist-key                                      ; za slučaj prekida veze
persist-tun                                       ; za slučaj prekida veze
client-config-dir "C:\\Program Files\\OpenVPN\\config"
;direktorij konfiguracije
verb 3                                           ;stupanj ispisa grešaka i upozorenja
route-delay 5                                    ;čekanje do početka primanja zahtjeva
route-method exe                                ;način unosa rute
push "route 161.53.63.0 255.255.255.0"
route 161.53.63.204 255.255.255.0
;adresa koju je router dodijelio računalu na kojem uspostavljamo
server

```

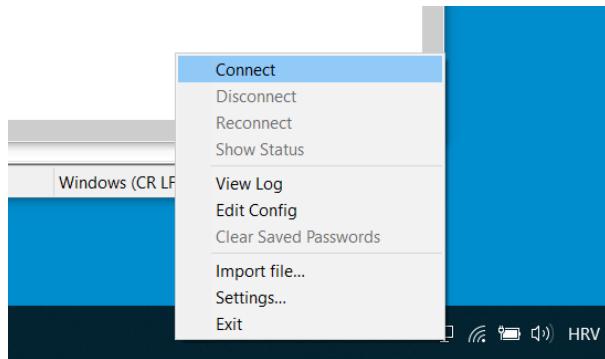
Za upute i pojašnjenja kako odabrati ispravne vlastite parametre za ovu datoteku molimo pogledajte detaljnije upute na adresi:

<https://openvpn.net/community-resources/how-to/#config>

Osim toga potrebno je:

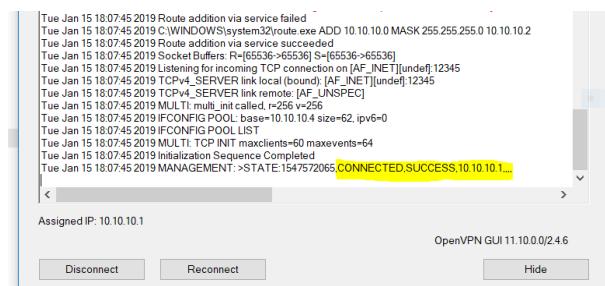
- imati stabilnu vezu na internet i statičku IP adresu
- imati omogućenu razmjenu TCP paketa u firewallu
- imati omogućeno prosljeđivanje prometa s routera na vrata na kojima server sluša (Port forwarding)

Ako je konfiguracija dobro odrđena moguće je pokrenuti server. Povezivanje se započinje pokretanjem “OpenVPN GUI” datoteke na radnoj površini, odabirom ikone računala s alatne trake i odabirom “Connect” mogućnosti.



Slika 49: Povezivanje sa serverom

Pokrenut server izgleda ovako:



Slika 50: Status servera

Konfiguracija OpenVPN klijenta

Kao prvi korak potrebno je instalirati OpenVPN kao i za server sa adresom:

<https://openvpn.net/community-downloads/>

Prilikom instalacije nije potrebno odabrati dodatne mogućnosti.

Na klijentskom računalu stvorite datoteku "Klijent.ovpn" i kopirajte ju u
<C:\Program Files\OpenVPN\easy-rsa\keys>



Slika 51: Prikaz Klijent.ovpn datoteke

Konfiguracijska datoteka treba sadržavati:

```
remote 161.53.63.204      ; javna IP adresa računala sa serverom
client                           ; ime uloge u mreži
port 12345                         ; broj vrata veze
proto tcp4-client                  ; protokol prijenosa
dev tun                            ; stvara se virtualni tunel
tls-client                          ; za autentifikaciju
tls-auth "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\ta.key" 1
; put do datoteke ključa(ta.key) te broj 1 koja označava klijenta
remote-cert-tls server
tun-mtu 1500                        ; veličina MTU paketa
tun-mtu-extra 32                     ; veličina MTU paketa
mssfix 1450                          ; veličina MTU paketa
ca "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\ca.crt"
; put do datoteke ca.crt
cert "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\KlijentVPN.crt"
; put do certifikata klijenta
key "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\KlijentVPN.key"
; put do ključa klijenta
cipher AES-128-CBC                 ; vrsta šifriranja
comp-lzo                            ; kompresija podataka u tunelu
persist-key                          ; za slučaj prekida veze
persist-tun                           ; za slučaj prekida veze
verb 3                               ; stupanj ispisa grešaka i upozorenja
```

Za upute i pojašnjenja kako odabrati ispravne vlastite parametre za ovu datoteku molimo pogledajte detaljnije upute na adresi:

<https://openvpn.net/community-resources/how-to/#config>

Osim toga potrebno je:

- imati stabilnu vezu na internet

-
- imati omogućenu razmjenu TCP paketa u firewallu

Povezivanje klijenta i servera

Kako bi se klijent uspješno povezao na server, iz instalacijskog direktorija SERVERA kopirajte sljedeće datoteke u novu mapu koju ćete prebaciti na računala klijenata:

ta.key
KlijentVPN.key
KlijentVPN.csr
KlijentVPN.crt
ca.crt

Prebaciti željenim načinom na klijentsko računalo ili računala koja će se povezivati na server i kopirati u instalacijski direktorij na adresi:

<C:\Program Files\OpenVPN\easy-rsa\keys>

Ako je konfiguracija dobro održena, moguće je povezivanje na server. Povezivanje se započinje pokretanjem “OpenVPN GUI” datoteke na radnoj površini, odabirom ikone računala s alatne trake i odabirom “Connect” mogućnosti.

Na nekim verzijama operacijskih sustava Windows potrebno je dodatno omogućiti povezivanje na interne adrese servera(npr. kao što smo postavili na 10.10.10.5) na sljedeći način:

1. U tražilicu računala upisati [regedit](#)
2. Pozicionirati se na lokaciju s adresom [Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters](#)
3. Pronaći IPEnableRouter te postaviti vrijednost na 1 i na računalu servera i na računalu klijenta

Prilikom komplikacija ili nejasnoća pogledati detaljnije upute na adresi:

<https://openvpn.net/community-resources/how-to/#config>

6.2 FreeBSD

6.2.1 OpenVPN

Ovo poglavlje će uključivati postavljanje VPN-a na FreeBSD inačici operacijskog sustava BSD. Potreban nam je poslužitelj za po mogućnosti sa statičkom IP adresom. Ovdje ćemo koristiti platformu DigitalOcean koja omogućuje brzo i jednostavno podizanje i upravljanje poslužiteljem. Za pristup poslužitelju koristit ćemo ssh protokol za što nam je potreban par ključeva koje generiramo naredbom

```
$ ssh-keygen -t rsa -b 2048
```

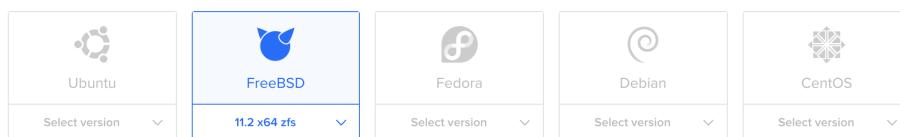
Javni ključ se nalazi u datoteci `/ .ssh/id_rsa.pub`, a privatni, koji mora ostati tajan, u `/ .ssh/id_rsa`.

Nakon registracije na Digital Ocean na svojem profilu možemo dodati javni ključ koji ćemo kasnije koristiti za pristup poslužitelju. Sada možemo stvoriti poslužitelja. Odabrat ćemo opciju *Create Droplet* i odabrat sljedeće postavke:

Create Droplets

Choose an image [?](#)

Distributions Container distributions One-click apps Custom images



This distribution requires an SSH Key.

Choose a size

Standard Droplets

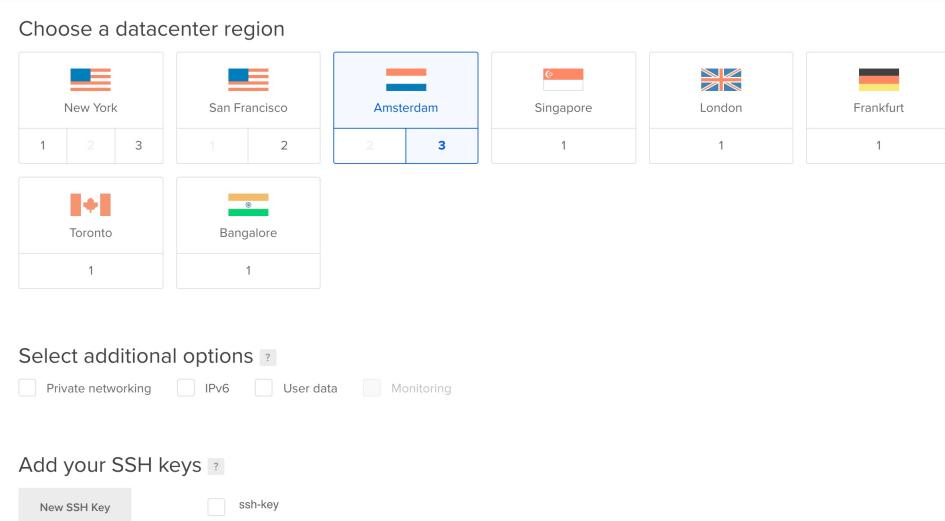
Balanced virtual machines with a healthy amount of memory tuned to host and scale applications like blogs, web applications, testing / staging environments, in-memory caching and databases.

\$5/mo \$0.007/hour	\$10/mo \$0.015/hour	\$15/mo \$0.022/hour	\$15/mo \$0.022/hour
1 GB / 1 CPU 25 GB SSD disk 1000 GB transfer	2 GB / 1 CPU 50 GB SSD disk 2 TB transfer	3 GB / 1 CPU 60 GB SSD disk 3 TB transfer	2 GB / 2 CPUs 60 GB SSD disk 3 TB transfer

• ● ● ●

Slika 52: Postavke DigitalOcean poslužitelja

Digitl Ocean nam također nudi opciju da odaberemo lokaciju našeg poslužitelja i pri-premimo ssh ključeve kako bi si olakšali pristup



Slika 53: Odabir lokacije i ssh ključeva

Kako sada prvi puta pristupamo poslužitelju jedini korisnik koji postoji je root. Root je korisnik na unixoidima koji može izvršiti svaku naredbu i pristupiti svakoj datoteci. Njemu pristupamo naredbom

```
$ ssh root@139.59.159.111
```

Kada smo se prijavili na poslužitelja prvu stavr koju moramo napraviti je ažurirati sustav. To ćemo napraviti koristeći FreeBSD-ov upravitelj paketima `pkg` i njegove naredbe `update` i `upgrade`.

```
# pkg update  
# pkg upgrade
```

Sada možemo instalirati OpenVPN.

```
# pkg install openvpn
```

Konfiguracijske datoteke ćemo smjestiti u direktorij `/usr/local/etc/openvpn` koji prvo moramo stvoriti.

```
# mkdir /usr/local/etc/openvpn
```

Openvpn nudi predloške konfiguracijskih datoteka stoga ćemo kopirati predložak za konfiguraciju poslužitelja u naš direktorij

```
# cp /usr/local/share/examples/openvpn/sample-config-files/server.conf \  
/usr/local/etc/openvpn/openvpn.conf
```

Kako bi mogli zaštитiti našu vezu potrebno je šifrirati sav promet između poslužitelja

i klijenta i osigurati inegritet svake poruke. Za šifriranje podataka ćemo koristiti simetrično šifriranje zbog svoje brzine, a za to nam je potreban simetrični ključ odnosno više ukoliko netko uspije dešifrirati jednu od naših poruka. Kako bi osigurali integritet poruka potrebno ih je potpisati i omogućiti provjeru potpisa. Ovaj problem ćemo rješiti digitalnim certifikatima koje ćemo sami napraviti. OpenVPN dolazi sa alatom Easy-RSA koji će nam poslužiti za izgradnju infrastrukture javnog ključa (*engl. PKI - public key infrastructure*). PKI služi kako bi se javni ključevi povezali s pripadajućim osobama ili organizacijama. Proces povezivanja izvršava tijelo za certificiranje (*engl. CA - certification authority*). CA također potvrđuje pripada li javni ključ osobi navedenoj u certifikatu. U praksi se CA nalazi na posebnom računalu, ali kako ovo radimo za privatnu uporabu naš CA će se nalaziti na poslužitelju.

Kako je Easy-RSA omotač oko složene programske knjižnice OpenSSL ona nam je jedini preduvjet te ćemo ju instalirati naredbom

```
# pkg install openssl
```

Nakon toga ćemo kopirati `easy-rsa` direktorij u naš direktorij sa svom konfiguracijom.

```
# cp -r /usr/local/share/easy-rsa /usr/local/etc/openvpn/easy-rsa
```

Sada ćemo se premjestiti u Easy-RSA direktoriji i urediti njegovu konfiguraciju skriptu `vars`.

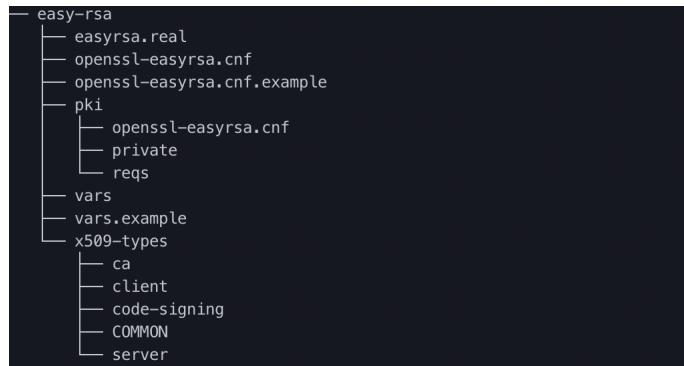
```
# cd /usr/local/etc/openvpn/easy-rsa
# vim vars
```

U nastavku su navedena polja koja je potrebno izmjeniti:

```
set_var EASYRSA_REQ_COUNTRY "<ZEMLJA>"
set_var EASYRSA_REQ_PROVINCE "<ZUPANIJA>"
set_var EASYRSA_REQ_CITY "<GRAD>"
set_var EASYRSA_REQ_ORG "<ORGANIZACIJA>"
set_var EASYRSA_REQ_EMAIL "<EMAIL>"
set_var EASYRSA_REQ_OU "<ORGANIZACIJSKA JEDINICA>"
set_var EASYRSA_KEY_SIZE <broj> # duljina rsa ključa u bitovima
set_var EASYRSA_CA_EXPIRE <broj> # trajanje CA ključa u danima
set_var EASYRSA_CERT_EXPIRE <broj> # trajanje certifikata u danima
```

Kako je `easy-rsa` skripta pisana za ljsku sh, dok FreeBSD koristi csh potrebno je naredbom `sh` pokrenuti sh ljsuksu. Sada možemo inicijalizirati PKI

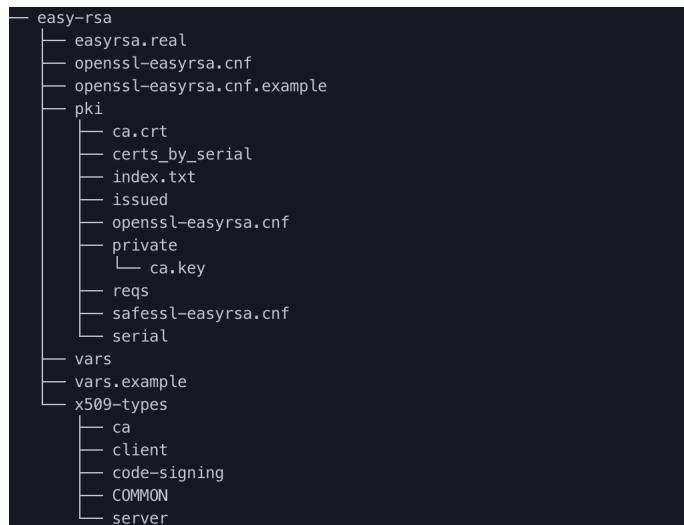
```
# ./easy-rsa.real init-pki
```



Slika 54: Struktura direktorija nakon inicijalizacije PKI

nakon čega ćemo stvoriti CA

```
# ./easy-rsa.real build-ca
```



Slika 55: Struktura direktorija nakon stvaranja korjenskog certifikata

Ovom naredbom smo stvorili par ključeva koji ćemo koristiti za potpisivanje izdanih certifikata.

Sada ćemo generirati serverov certifikat naredbom

```
# ./easy-rsa.real build-server-full <ime-server> nopass
```

gdje je `<ime-server>` ime certifikata, a s `nopass` opcijom ćemo generirati nešifrirani ključ kako bi mogli automatski pokrenuti OpenVPN uslugu prilikom pokretanja sustava bez upisivanja lozinke ključa.

Na sličan način ćemo generirati klijentove certifikate

```
# ./easy-rsa.real build-client-full <ime-klijent> nopass
```

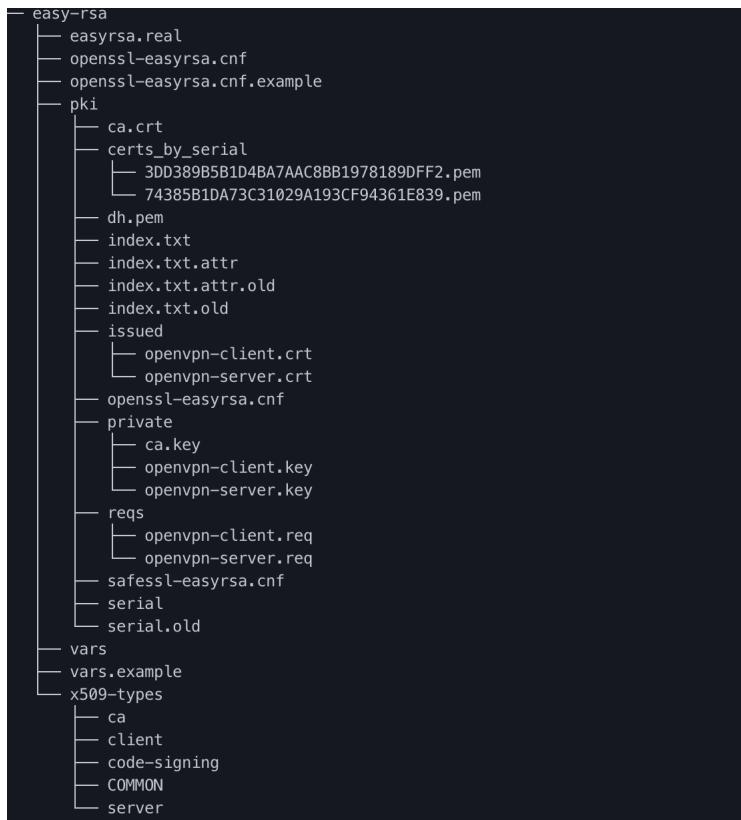
```
# ./easyrsa.real build-client-full openvpn-client

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.0.2o-freBSD 27 Mar 2018
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/usr/local/etc/openvpn/easy-rsa/pki/private/openvpn-client.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
Using configuration from /usr/local/etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf
Enter pass phrase for /usr/local/etc/openvpn/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'openvpn-client'
Certificate is to be certified until Jan 10 20:59:06 2029 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
```

Slika 56: Stvaranje certifikata



Slika 57: Struktura direktorija nakon stvaranja klijentskog i poslužiteljevog certifikata

Za šifriranje same poruke koristit ćemo simetričan ključ generiran Diffie-Hellman razmjenom. Za to su nam potrebni Diffie-Hellman parametri koje stvaramo naredbom

```
# ./easyrsa.real gen-dh
```

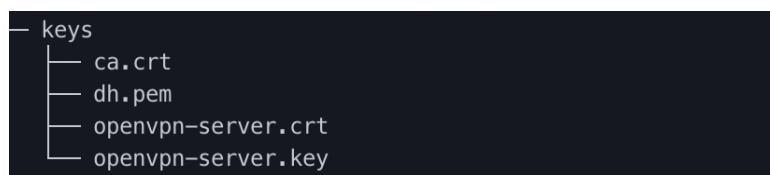
Do sada smo sve naredbe izvršavali na poslužitelju te smo generirali velik broj datoteka od kojih ćemo neke morati premjestiti na klijentsko računalo. Kako bi znali koje datoteke premejstiti potrebno je razumjeti čemu svaka od njih služi. Sve su datoteke stvorene u

`easy-rsa/pki/` direktoriju pa ćemo se u njega pozicionirati.

- `ca.crt` - certifikat koji se koristi za validaciju ostalih certifikata, potrebno ga je kopirati na poslužitelja i sve klijente
- `ca.key` - ključ koji CA koristi za izdavanje certifikata
- `reqs/` - direktorij koji sadrži zahtjeve za izdajom certifikata
- `issued/<ime-server>.crt` - certifikat servera koji služi za provjeru potpisa na poruci, potrebno ga je prebaciti na poslužitelja
- `private/<ime-server>.key` - privatni ključ polužitelja koji se koristi za potpisivanje poruke, potrebno ga je prebaciti na poslužitelja
- `issued/<ime-klijent>.crt` - certifikat klijenta koji služi za provjeru potpisa na poruci, potrebno ga je prebaciti na klijentsko računalo
- `private/<ime-klijent>.key` - privatni ključ klijenta koji se koristi za potpisivanje poruke, potrebno ga je prebaciti na klijentsko računalo
- `dh.pem` - Diffie Hellman parametri, potrebno ih je prebaciti na poslužitelja

Ključeve poslužitelja ćemo premjestiti u poseban direktorij

```
# mkdir /usr/local/etc/openvpn/keys
# cp pki/dh.pem \
    pki/ca.crt \
    pki/issued/<ime-server>.crt \
    pki/private/<ime-server>.key \
    /usr/local/etc/openvpn/keys
```



Slika 58: Sadržaj `keys` direktorija na poslužitelju

Prije nego što počnemo konfigurirati klijentsko računalo, potrebno je u konfiguraciji poslužitelja navesti putanje do certifikata, ključeva i parametara. To ćemo napraviti u datoteci `openvpn.conf` koju smo na samom početku kopirali u `/usr/local/etc/openvpn`.

```
# vim /usr/local/etc/openvpn/openvpn.conf
```

Potrebno je urediti sljedeće linije

```
ca /usr/local/etc/openvpn/keys/ca.crt
cert /usr/local/etc/openvpn/keys/<ime-server>.crt
key /usr/local/etc/openvpn/keys/<ime-server>.key
dh /usr/local/etc/openvpn/keys/dh.pem
```

```
# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key). Each client
# and the server must have their own cert and
# key file. The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys. Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca /usr/local/etc/openvpn/keys/ca.crt
cert /usr/local/etc/openvpn/keys/openvpn-server.crt
key /usr/local/etc/openvpn/keys/openvpn-server.key # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh2048.pem 2048
dh /usr/local/etc/openvpn/keys/dh.pem
```

Slika 59: Putanje do ključeva i certifikata u datoteci `openvpn.conf`

Sada možemo postaviti klijentsko računalo. Kako smo već pripremili većinu klijentovih datoteka na poslužitelju, potrebno ih je kopirati. Radi se o osjetljivim datotekama stoga nam je potreban siguran način slanja datoteka preko mreže za što ćemo koristiti program *secure copy*. Nakon što instaliramo openvpn isto kao i na poslužiteljskom računalu možemo kopirati predložak konfiguracije

```
# cp /usr/local/share/examples/openvpn/sample-config-files/client.config \
/usr/local/etc/openvpn/openvpn.conf
```

Također stvorit ćemo direktorij u koji ćemo spremiti ključeve i certifikate

```
# mkdir /usr/local/etc/openvpn/keys
```

Sada možemo kopirati potrebne datoteke sa poslužitelja

```
$ scp root@<ip-server>:/usr/local/etc/openvpn/easy-rsa/pki/ca.crt keys
$ scp root@<ip-server>:\ 
    /usr/local/etc/openvpn/easy-rsa/pki/issued/<ime-klijent>.crt \
    keys
$ scp root@<ip-server>:\ 
    /usr/local/etc/openvpn/easy-rsa/pki/private/<ime-klijent>.key \
```

keys

```
-- openvpn
  |-- keys
  |   |-- ca.crt
  |   |-- openvpn-client.crt
  |   '-- openvpn-client.key
  '-- openvpn.conf
```

Slika 60: Sadržaj `keys` direktorija na klijentu

U konfiguraciji (`openvpn.conf`) osim putanja do certifikata i ključeva potrebno je unjeti ip adresu poslužitelja

```
remote <ip-server> 1194
ca /usr/local/etc/openvpn/keys/ca.crt
cert /usr/local/etc/openvpn/keys/<ime-server>.crt
key /usr/local/etc/openvpn/keys/<ime-server>.key
```

Za upravljanje servisima koristimo naredbu `service`. Prvo ćemo njome pokrenuti OpenVPN servis na poslužitelju i nakon toga na klijentu

```
# service openvpn run
```

Sada možemo alatom `ifconfig` provjeriti stanje mrežnih sučelja na klijentu:

```
root@:~ # ifconfig
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
  options=9b<RXCSUM,TXCSUM,ULAN_MTU,ULAN_HWTAGGING,ULAN_HWCSUM>
  ether 08:00:27:17:df:37
  hwaddr 08:00:27:17:df:37
  inet6 fe80::a00:27ff:fe17:df37%em0 prefixlen 64 scopeid 0x1
    inet 10.0.2.15 netmask 0xffffffff broadcast 10.0.2.255
    nd6 options=23<PERFORMNUD,ACCEPT_RTADU,AUTO_LINKLOCAL>
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
  options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
  inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
    inet 127.0.0.1 netmask 0xff000000
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
    groups: lo
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1500
  options=80000<LINKSTATE>
  inet6 fe80::a00:27ff:fe17:df37%tun0 prefixlen 64 scopeid 0x3
    inet 10.8.0.10 --> 10.8.0.9 netmask 0xffffffff
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
    groups: tun
      Opened by PID 615
```

Slika 61: Mrežna sučelja klijenta

na poslužitelju:

```
# ifconfig
vtnet0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=6c07bb=RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSUM,TS04,TS06,LRO
    ether 76:60:93:60:0b:b5
    hwaddr 76:60:93:60:0b:b5
    inet 139.59.159.111 netmask 0xffffffff broadcast 139.59.159.255
        inet 10.19.0.7 netmask 0xffffffff broadcast 10.19.255.255
        inet6 fe80::7460:93ff:fe60:bb%vtnet0 prefixlen 64 scopeid 0x1
            nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
            media: Ethernet 10Gbase-T <full-duplex>
            status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
    options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
    inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
        inet 127.0.0.1 netmask 0xffffffff
            nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
            groups: lo
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1500
    options=80000<LINKSTATE>
    ether fe80::60b:3eea:228d:6a69%tun0 prefixlen 64 scopeid 0x3
    inet 10.8.0.1 --> 10.8.0.2 netmask 0xffffffff
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: tun
    Opened by PID 44264
```

Slika 62: Mrežna sučelja poslužitelja

Možemo uočiti novo sučelje `tun0` koje predstavlja virtualno sučelje mrežnog sloja. Izvršavanjem naredbe `ping` možemo provjeriti je li klijentsko računalo stvarno povezano s poslužiteljem.

```
$ ping 10.8.0.1
```

Kako nam je cilj povezati dva klijenta koji se nalaze u različitim privatnim mrežama na isti ćemo pripremiti još jednog klijenta. Njegova konfiguracija će biti jednaka konfiguraciji prvog klijenta, a izlaz naredbe `ifconfig`:

```
root@: # ifconfig
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM,TXCSUM,ULAN_MTU,ULAN_HWTAGGING,ULAN_HWCSUM>
    ether 08:00:27:e2:49:4b
    hwaddr 08:00:27:e2:49:4b
    inet6 fe80::a00:27ff:fe2:494b%em0 prefixlen 64 scopeid 0x1
        inet 10.0.2.15 netmask 0xffffffff broadcast 10.0.2.255
            nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
            media: Ethernet autoselect (1000baseT <full-duplex>)
            status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
    options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
    inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
        inet 127.0.0.1 netmask 0xffffffff
            nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
            groups: lo
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1500
    options=80000<LINKSTATE>
    ether fe80::a00:27ff:fee2:494b%tun0 prefixlen 64 scopeid 0x3
    inet 10.8.0.6 --> 10.8.0.5 netmask 0xffffffff
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: tun
    Opened by PID 580
```

Slika 63: Mrežna sučelja drugog klijenta

Ako sada pokušamo naredbom `$ ping 10.8.0.6` provjeriti jesu li klijenti međusobno povezani nećemo dobiti nikakav rezultat. Razlog tome je što prepostavljena konfiguracija poslužitelja ne dozvoljava komunikaciju između klijenata. Kako bi to omogućili potrebno je u konfiguracijskoj datoteci poslužitelja otkomentirati liniju `client-to-client`

Sada ćemo ponovo pokrenuti OpenVPN i ispitati jesu li klijenti međusobno povezani

```
# service openvpn restart  
$ ping 10.8.0.6
```

```
root@:~ # ping 10.8.0.6  
PING 10.8.0.6 (10.8.0.6): 56 data bytes  
64 bytes from 10.8.0.6: icmp_seq=0 ttl=64 time=46.694 ms  
64 bytes from 10.8.0.6: icmp_seq=1 ttl=64 time=47.087 ms  
64 bytes from 10.8.0.6: icmp_seq=2 ttl=64 time=45.318 ms  
64 bytes from 10.8.0.6: icmp_seq=3 ttl=64 time=58.107 ms  
64 bytes from 10.8.0.6: icmp_seq=4 ttl=64 time=50.414 ms  
64 bytes from 10.8.0.6: icmp_seq=5 ttl=64 time=44.427 ms  
64 bytes from 10.8.0.6: icmp_seq=6 ttl=64 time=50.799 ms  
64 bytes from 10.8.0.6: icmp_seq=7 ttl=64 time=51.458 ms  
^C  
--- 10.8.0.6 ping statistics ---  
3 packets transmitted, 8 packets received, 0.0% packet loss  
round-trip min/avg/max/stddev = 44.427/49.288/58.107/4.138 ms
```

Slika 64: Izlaz naredbe ping

Za kraj možemo pokušati kopirati datoteku s jednog klijenta na drugi koristeći `tun0` sučelja. Na klijentu s adresom `10.8.0.6` stvorit ćemo datoteku `pozdrav.txt` i u nju nešto zapisati

```
$ touch pozdrav.txt  
$ echo "Bok" > pozdrav.txt
```

Sada ćemo sa drugog klijenta (adresa `10.8.0.10`) kopirati `pozdrav.txt` datoteku i ispitati ju

```
$ scp root@10.8.0.6:/root/pozdrav.txt .  
$ cat /root/pozdrav.txt
```

```
root@:~ # scp root@10.8.0.6:/root/pozdrav.txt .  
Password for root@:  
pozdrav.txt  
root@:~ # tree  
:-- pozdrav.txt  
0 directories, 1 file  
root@:~ # cat pozdrav.txt  
Bok
```

Slika 65: Kopiranje i ispis datoteke `pozdrav.txt`

6.3 Linux

Linux distribucije podržavaju mnogobrojni VPN-ovi. U sljedećim poglavljima bit će opisana instalacija dva različita VPN-a na Ubuntu distribuciju Linux operacijskog sustava. Upute za OpenVPN su složenije i namijenjene su naprednjim korisnicima, dok upute za StrongSwan koriste već unaprijed napisanu skriptu i prilagođene su korisnicima koji su početnici ili žele što brže uspostaviti VPN, a uz što manje truda.

6.3.1 OpenVPN

Što je OpenVPN?

OpenVPN^[5] je potpuno otvoreni kod za SSL VPN soluciju koji zastupa širok raspon različitih konfiguracija, pritom uključujući udaljeni pristup, *site-to-site* VPN-ove, sigurnost Wi-Fi-a te nudi rješenja za udaljeni pristup prilagođen profesionalnim okruženjima. Sigurnosni model OpenVPN-a bazira se na protokolima SSL/TLS, koji su industrijski standard za sigurnu komunikaciju preko interneta.

Prije početka instalacije

Ove upute^[6] prilagođene su za verziju 16.04 Ubuntu distribucije operacijskog sustava Linux. Za uspješno instaliranje OpenVPN-a potrebna vam je javna IP adresa te je istu potrebno doznati prije početka instalacije. To se može doznati klikom na sljedeću stranicu <https://www.whatismyip.com/>. Isto tako potrebno je otvoriti određena vrata (eng. *port*) na vašem usmjeritelju ili ako je to zabranjeno od vašeg pružatelja internetskih usluga onda možete računalo potpuno izložiti internetu tako da se u postavkama usmjeritelja podesi opcija DMZ Host na IP adresu vašeg računala (ovaj način se ne preporučuje jer vašu lokalnu mrežu izlaže internetu što predstavlja sigurnosni problem).

Sljedeći koraci izvedeni su u Ubuntu v. 16.04 u virtualnom okruženju.

Instalacija OpenVPN-a

Prvi korak je instalacija OpenVPN-a te paketa easy-rsa (koji će poslužiti kao naše privatno lokalno certifikacijsko tijelo) na naš operacijski sustav.

Počnimo prvo s osvježavanjem sustava te instalacijom nužnih paketa:

```
sudo apt-get update  
sudo apt-get install openvpn easy-rsa
```

Sljedeći korak je uspostava certifikacijskog tijela. Kopirat ćemo easy-rsa predložak u novi direktorij te se nakon toga pozicionirati u njega:

```
make-cadir ~/openvpn-ca  
cd ~/openvpn-ca
```

Konfigurirajmo sada vrijednosti koje će naše tijelo koristiti otvaranjem datoteke vars:

```
nano vars
```

Unutra se nalaze neke varijable koje definiraju način stvaranja certifikata. Nas zanimaju samo neke od njih. Plave vrijednosti postavite po želji, a ako za KEY NAME koristite neku drugu vrijednost zapamtite ju jer će nam kasnije biti potrebna.

```

export KEY_COUNTRY="HR"
export KEY_PROVINCE="ZG"
export KEY_CITY="Zagreb"
export KEY_ORG="FER"
export KEY_EMAIL="info@primjer.hr"
export KEY_OU="Grupa za projekt"

export KEY_NAME="server"

```

Nakon što ste završili spremite i izadžite.

```

dominik@dominik-VirtualBox: ~/openvpn-ca
File Edit View Search Terminal Help
GNU nano 2.9.3 vars Modified
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="HR"
export KEY_PROVINCE="ZG"
export KEY_CITY="Zagreb"
export KEY_ORG="FER"
export KEY_EMAIL="info@primjer.hr"
export KEY_OU="Grupa Za Projekt"

# X509 Subject Field
export KEY_NAME="server"

# PKCS11 Smart Card
# export PKCS11_MODULE_PATH="/usr/lib/changeme.so"
# export PKCS11_PIN=1234

# If you'd like to sign all keys with the same Common Name, uncomment the KEY_C
# You will also need to make sure your OpenVPN server config has the duplicate-
Save modified buffer? (Answering "No" will DISCARD changes.) |||
Y Yes
N No          ^C Cancel

```

Slika 66: Postavljanje vrijednosti za CA

Izgradnja certifikacijskog tijela

Osigurajte da se nalazite u dobrom direktoriju i onda postavite datoteku vars kao izvor:

```

cd ~/openvpn-ca
source vars

```

```

NOTE: If you run ./clean-all, I will be doing a rm -rf on /home/dominik/openvpn-
ca/keys
dominik@dominik-VirtualBox:~/openvpn-ca$ ./clean-all
dominik@dominik-VirtualBox:~/openvpn-ca$ ./build-ca

```

Slika 67: Dobar ispis nakon postavljanja izvorišta

Ako je sve prošlo kako trebali bi imati ispis kao na slici 67 te nakon toga osigurat ćemo čisti start i krenut ćemo u izgradnju našeg tijela. Zadnja naredba će inicirati izgradnju tijela - pritisnite ENTER na već ponuđene parametre.

```

./clean-all
./build-ca

```

U slučaju pogreške, kao što je prikazano na slici 68 , unesite sljedeće naredbe:

```
dominik@dominik-VirtualBox:~/openvpn-ca$ ./clean-all
dominik@dominik-VirtualBox:~/openvpn-ca$ ./build-ca
grep: /home/dominik/openvpn-ca/openssl.cnf: No such file or directory
pkictool: KEY_CONFIG (set by the ./vars script) is pointing to the wrong
version of openssl.cnf: /home/dominik/openvpn-ca/openssl.cnf
The correct version should have a comment that says: easy-rsa version 2.x
```

Slika 68: Dogodila se pogreška prilikom izgradnje CA

```
ln -s openssl-1.0.0.cnf openssl.cnf
./build-ca
```

Sada bi sve trebalo biti uredu.

Nastavimo dalje s izradom poslužiteljskog certifikata, ključa te enkripcijskih datoteka. Prvo ćemo generirati ključ za poslužitelj. Prihvativite unaprijed određene parametre pritiskom tipke ENTER i ne unosite lozinku. Pred kraj bit će te pitani dva pitanja, na oba odgovorite sa **y**.

NAPOMENA: U slučaju da ste odabrali neko drugo ime, a ne server onda u sljedećim koracima svaku pojavu riječi server zamijenite s vašim imenom!

```
./build-key-server server
```

Generirat ćemo još neke dijelove poput Diffie-Hellman ključeva koji će se koristiti prilikom razmjene ključeva:

```
./build-dh
openvpn --genkey --secret keys/ta.key
```

Generiranje klijentskog certifikata

Sljedeći korak nam je generiranje certifikata za klijenta te par ključa. Iako se ovo može izvesti na računalu klijenta zbog jednostavnosti ovdje ćemo odraditi te korake. Za ime klijenta koristit ćemo client1. Kasnije se možete vratiti na ovaj korak za generiranje ključeva za druge klijente.

Za izradu lozinkom ne zaštićenih podataka upišite:

```
cd ~/openvpn-ca
source vars
./build-key client1
```

U slučaju da želite lozinkom zaštiti:

```
cd ~/openvpn-ca
source vars
./build-key-pass client1
```

Opet kao i prije prihvativite ponuđene argumente pritiskom na tipku ENTER te odgovorite na pitanja sa **y**.

Konfiguracija OpenVPN usluge

Pozicionirajmo se prvo u /openvpn-ca-keys te zatim kopirajmo datoteke u /etc/openvpn:

```
cd ~/openvpn-ca/keys  
sudo cp ca.crt server.crt server.key ta.key dh2048.pem /etc/openvpn
```

Idući korak je kopiranje i raspakiravanje primjera konfiguracije:

```
gunzip -c /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz | sudo tee /etc/openvpn/server.conf
```

Sada ćemo raspakiranu konfiguraciju otvoriti:

```
sudo nano /etc/openvpn/server.conf
```

Nadite dio koji se odnosi na HMAC tražeći tls-auth. Otkomentirajte tu liniju tako da obrišete ; ispred linije te dodajmo liniju vezanu uz smjer ključa :

```
tls-auth ta.key 0 # This file is secret  
key-direction 0
```

Sljedeće nadite liniju vezanu uz kriptografske šifrante te ju otkomentirajte. Ispod toga dodajte algoritam za HMAC poruke:

```
cipher AES-256-CBC  
auth SHA256
```

Potom otkomentirajte i sljedeće dvije linije:

```
user nobody  
group nogroup
```

Sljedeći dio nije potreban, ali se preporučuje. Inače VPN konekcija nije postavljena tako da sav internet promet ide kroz nju. U slučaju da želite sav internet promet preusmjeriti kroz internet konekciju otkomentirajte liniju:

```
push "redirect-gateway def1 bypass-dhcp"
```

Otkomentirajte obje linije koje se odnose na dhcp:

```
push "dhcp-option DNS 208.67.222.222"  
push "dhcp-option DNS 208.67.220.220"
```

Neobavezno-promijenite port i protokol koji se koriste. OpenVPN koristi vrata 1194 i protokol UDP za prihvat klijentskih konekcija. U slučaju da iz nekog razloga to vam ne odgovara postavite vrata na neka druga (npr. 443):

```
port 443
```

```
proto tcp  
;proto udp
```

U slučaju da niste koristili ime server onda ga sad promijenite u sljedećim linijama:

```
cert server.crt  
key server.key
```

Spremite datoteku te izadžite.

Prilagodavanje mrežnih postavka poslužitelja

Modificirajmo postavke otvarajući datoteku:

```
sudo nano /etc/sysctl.conf
```

Potražite sljedeću liniju te maknite znak # kako bi ju otkomentirali.

```
net.ipv4.ip_forward=1
```

Spremite i izadite.

Kako bi pročitali datoteku i namjestili vrijednosti za trenutnu sesiju upišite:

```
sudo sysctl -p
```

Prilagodimo sada pravila vatrozida, a za to nam treba mrežno sučelje pa iz tog razloga upisujemo:

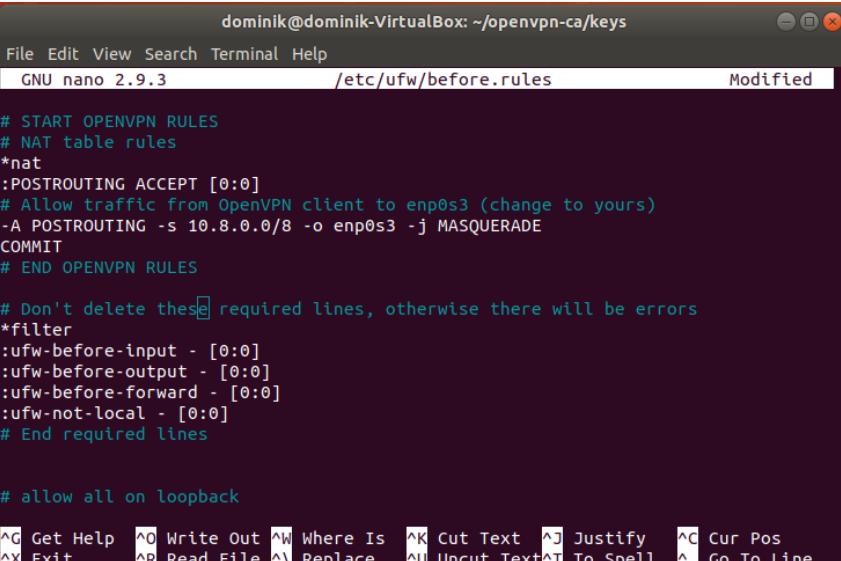
```
ip route | grep default
```

Izlaz bi vam trebao sličiti na doljnji ispis. Nama je važan plavo pobojan dio:

```
default via 192.168.0.1 dev enp0s3 proto dhcp metric 600
```

Otvorimo sad konfiguracijsku datoteku:

```
sudo nano /etc/ufw/before.rules
```



```
# START OPENVPN RULES
# NAT table rules
*nat
:POSTROUTING ACCEPT [0:0]
# Allow traffic from OpenVPN client to enp0s3 (change to yours)
-A POSTROUTING -s 10.8.0.0/8 -o enp0s3 -j MASQUERADE
COMMIT
# END OPENVPN RULES

# Don't delete these required lines, otherwise there will be errors
*filter
:ufw-before-input - [0:0]
:ufw-before-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-not-local - [0:0]
# End required lines

# allow all on loopback
```

Slika 69: Izgled konfiguracijske datoteke - UFW Firewall

U konfiguraciju dodajmo plavo označene dijelove pritom zamjenite enp0s3 za ime mrežnog sučelja koje ste maloprije otkrili. Konačan izgled trebao bi biti kao na slici 69.

```
# 
# rules.before
#
# Rules that should be run before the ufw command line added rules.
# Custom rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward
```

```

# START OPENVPN RULES
# NAT table rules
*nat
:POSTROUTING ACCEPT [0:0]
# Dopusti promet od OpenVPN klijenta prema enp0s3
-A POSTROUTING -s 10.8.0.0/8 -o enp0s3 -j MASQUERADE
COMMIT
# END OPENVPN RULES

```

Don't delete these required lines, otherwise there will be errors

Sada trebamo reći UFW-u da automatski proslijedi pakete. Otvorimo datoteku:

```
sudo nano /etc/default/ufw
```

Promijenimo sljedeću liniju iz DROP u ACCEPT. Spremimo datoteku i izadimo.

```
DEFAULT_FORWARD_POLICY="ACCEPT"
```

Otvorimo sada port 1194 tako da prima UDP promet. U slučaju da ste mijenjali port i/ili protokol promijenite vrijednosti u svoje. Isto tako dopustit ćemo SSH promet te ćemo onda onemogućiti pa ponovno omogućiti naša nova pravila.

```
sudo ufw allow 1194/udp
sudo ufw allow OpenSSH
sudo ufw disable
sudo ufw enable
```

Omogućavanje i pokretanje OpenVPN usluge

Pokrenimo uslugu te odmah potom provjerimo je li uspješno pokrenuta. U slučaju da vam se ime razlikuje od imena server, promijenite ga.

```
sudo systemctl start openvpn@server
sudo systemctl status openvpn@server
```

Ispis, ako nije došlo do greske trebao bi biti kao na slici 70. Možete isto tako provjeriti

```

● openvpn@server.service - OpenVPN connection to server
   Loaded: loaded (/lib/systemd/system/openvpn@.service; disabled; vendor preset
   Active: active (running) since Fri 2018-12-14 19:09:46 CET; 17s ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 10500 (openvpn)
      Status: "Initialization Sequence Completed"
        Tasks: 1 (limit: 3530)
       CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
               └─10500 /usr/sbin/openvpn --daemon ovpn-server --status /run/openvpn/

```

Slika 70: Pokrenuta usluga OpenVPN

je li dostupno OpenVPN sučelje tun0. Ispis bi trebao biti kao na slici 71.

```
ip addr show tun0
```

Konačno ako je sve prošlo kako treba omogućimo automatsko pokretanje usluge:

```
sudo systemctl enable openvpn@server
```

```
dominik@dominik-VirtualBox:~/openvpn-ca/keys$ ip addr show tun0
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UNKNOWN group default qlen 100
    link/none
        inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0
            valid_lft forever preferred_lft forever
        inet6 fe80::bfdb:393c:7667:9ecf/64 scope link stable-privacy
            valid_lft forever preferred_lft forever
```

Slika 71: OpenVPN sučelje tun0

Izrada konfiguracijske strukture klijenta

Stvorimo novi direktorij, podesimo mu postavke te nakon toga kopirajmo primjer konfiguracije u njega. Otvorimo tu konfiguraciju kako bi ju mogli urediti:

```
mkdir -p ~/client-configs/files
chmod 700 ~/client-configs/files

cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client-configs/base.conf

nano ~/client-configs/base.conf
```

Nadite dio konfiguracije koji se odnosi na udaljeni pristup. Ta linija upućuje klijenta na naš server. Zamijenite plavi dio linije javnom IP adresom servera ili domenom servera te napišite port koji ste odabrali.

```
.
.
.

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 88.207.10.226 1194
.
.
```

Provjerite da je dobar protokol postavljen:

```
proto udp
```

Otkomentirajte korisnika i grupu:

```
# Downgrade privileges after initialization (non-Windows only)
user nobody
group nogroup
```

Zakomentirajte sljedeće linije:

```
#ca ca.crt
#cert client.crt
#key client.key
```

Unesite šifrant koji ste unijeli u /etc/openvpn/server.conf

```
cipher AES-256-CBC
auth SHA256
```

Negdje u dokumentu dodajte sljedeću liniju:

```
key-direction 1
```

Na kraju dodajte par zakomentiranih linija. Njih želimo uključiti u svaku konfiguraciju iz razloga ako klijent pristupa s Linux operativnog sustava koji u sebi ima /etc/openvpn/update-resolv-conf tada će ova skripta osvježavati DNS postavke za Linux klijente.

```
# script-security 2
# up /etc/openvpn/update-resolv-conf
# down /etc/openvpn/update-resolv-conf
```

Kreirajmo sada konfiguracijsku skriptu. Stvorite i otvorite skriptu:

```
nano ~/client-configs/make_config.sh
```

Kopirajte sljedeću skriptu i spremite datoteku te potom izadžite.

```
#!/bin/bash

# First argument: Client identifier

KEY_DIR=~/openvpn-ca/keys
OUTPUT_DIR=~/client-configs/files
BASE_CONFIG=~/client-configs/base.conf

cat ${BASE_CONFIG} \
<(echo -e '<ca>') \
${KEY_DIR}/ca.crt \
<(echo -e '</ca>\n<cert>') \
${KEY_DIR}/${1}.crt \
<(echo -e '</cert>\n<key>') \
${KEY_DIR}/${1}.key \
<(echo -e '</key>\n<tls-auth>') \
${KEY_DIR}/ta.key \
<(echo -e '</tls-auth>') \
> ${OUTPUT_DIR}/${1}.ovpn
```

Napravimo skriptu izvršnom:

```
chmod 700 ~/client-configs/make_config.sh
```

Generiranje klijentske konfiguracije

U slučaju da ste pratili ove upute od riječi do riječi sada već imamo certifikat i ključ za client1. Generirajmo sada konfiguraciju za client1 pozicionirajući se u direktorij `~/client-configs` i koristeći skriptu iz prošlog poglavlja:

```
cd ~/client-configs
./make_config.sh client1
ls ~/client-configs/files
```

Sada bi trebali imati konfiguraciju. Nakon izvršavanja sljedeće naredbe izlaz bi trebao biti kao na slici .

```
ls ~/client-configs/files
```

S ovime ste završili s instalacijom poslužitelja i vaš VPN bi sada trebao raditi. U slučaju da želite još neke klijentske konfiguracije trebate samo ponoviti korake opisane u poglavljima generiranja klijentskog certifikata i generiranje klijentske konfiguracije. Dobivenu konfiguraciju prebacite na računalo klijenta.

```
dominik@dominik-VirtualBox:~/openvpn-ca/keys$ cd ~/client-configs  
dominik@dominik-VirtualBox:~/client-configs$ ./make_config.sh client1  
dominik@dominik-VirtualBox:~/client-configs$ ls ~/client-configs/files  
client1.ovpn
```

Slika 72: Konfiguracija klijenta - client1

Instalacija OpenVPN-a na računalu klijenta

Sada treba testirati novo napravljeni VPN, ali prije toga trebamo instalirati OpenVPN na računalo klijenta.

Linux

Na Ubuntu i Debian distribuciji potrebno je upisati:

```
sudo apt-get update  
sudo apt-get install openvpn
```

Provjerite je li vaša distribucija dolazi sa /etc/openvpn/update-resolv-conf skriptom:

```
ls /etc/openvpn
```

U slučaju da dolazi tada uredite konfiguraciju:

```
nano client1.ovpn
```

Otkomentirajte zadnje tri linije i spremite datoteku.

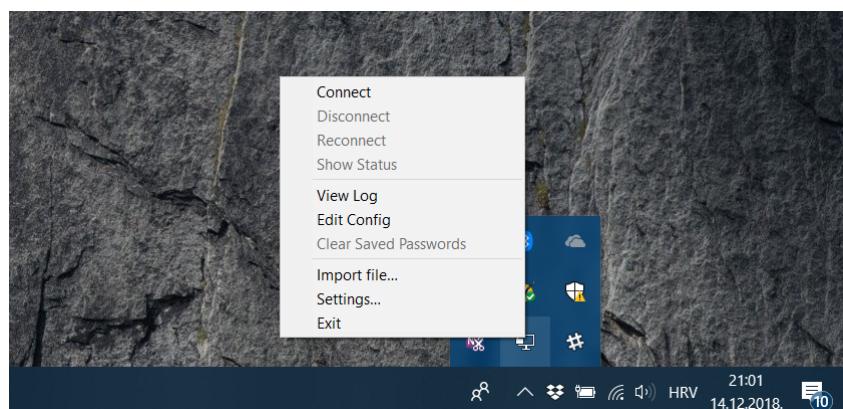
```
script-security 2  
up /etc/openvpn/update-resolv-conf  
down /etc/openvpn/update-resolv-conf
```

Sada se možete spojiti unošenjem sljedeće naredbe.

```
sudo openvpn --config client1.ovpn
```

Windows

Otvorite sljedeći link <https://openvpn.net/community-downloads/> i skinite program za Windows te pokrenite instalaciju. Nakon instalacije u donjem desnom kutu vašeg ekrana pojavit će se ikona OpenVPN-a kao na slici 73. Desni klik na nju i oda-

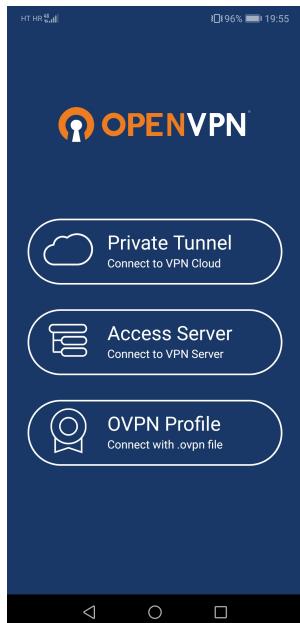


Slika 73: Uvoz klijentske konfiguracije na Windowsima

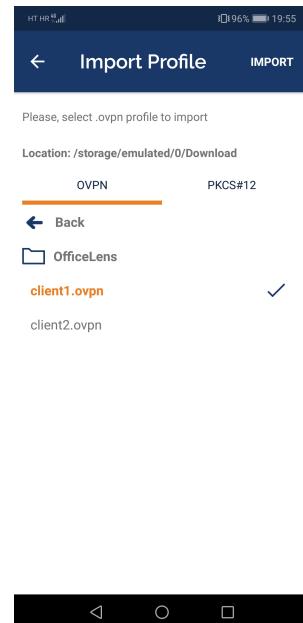
berite Import file. Nakon toga navigirajte do mesta gdje ste spremili client1.ovpn i odaberite datoteku. Zadnji korak je stisnuti na opciju Connect. Nakon toga će se pokrenuti proces spajanja i ako je sve prošlo uredno bit će te spojeni na vaš VPN poslužitelj i bit će vam dodijeljena nova IP adresa.

Instalacija na mobilnim uređajima

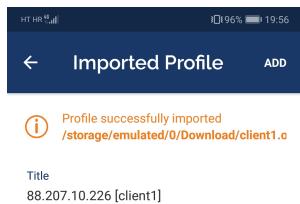
Instalacija na Android i iOS sustavima je gotovo identična. Ovdje će biti opisano spajanje na Android 8.1 operacijskom sustavu.



(a) Početni ekran OpenVPN aplikacije



(b) Odabir klijentske konfiguracije



(c) Uspješno učitavanje profila

(d) Profil je uspješno dodan

Slika 74: OpenVPN aplikacija

Skinite aplikaciju OpenVPN i otvorite ju, bit će vam prikazan početni ekran kao na

slici 74a. Odaberite opciju spajanja preko OVPN profila. Profil bi već sada trebao biti dostupan ako ste ga skinuli s interneta, a ako niste onda navigirajte do njega. Odaberite profil client1.ovpn kao što je prikazano na slici 74b. Nakon toga dobit će te poruku o uspješnom učitavanju profila (slika: 74c). Stisnite na opciju ADD u gornjem desnom kutu. I na kraju se povežite s VPN poslužiteljem pritiskajući na sivi gumb (slika: 74d).

6.3.2 Libreswan IPsec/L2TP VPN poslužitelj

Što je Libreswan?

Libreswan^[7] je besplatna programska implementacija najpodržavаниjeg i standardiziranog VPN protokola baziranog na IPsec-u i IKE-u (eng. *Internet Key Exchange*). Ti standardi se održavaju od strane IETF-a.

Prije početka instalacije

Za sljedeće upute potrebna je nova, čista, bez ikakvih dodataka instalacija Ubuntu **Server** 18.04 LTS distribucije Linux operacijskog sustava. Upute su prilagođene potpunim početnicima i ne zahtijeva se nikakvo prethodno znanje osim unosa tri naredbe. Kao i u prošloj cjelini kod OpenVPN-a potrebno je postaviti preusmjeravanje vrata, ali ovaj put se čak ne mora znati javna IP adresa. Za te detalje pobrinut će se skripta^[8] koju ćemo pokrenuti i preuzeti. U slučaju da želite sličnu napredniju instalaciju koja koristi StrongSwan i IKEv2 pročitajte ovaj članak^[9].

Instalacija poslužitelja

Prvi korak instalacije je kao i uvijek osvježavanje operacijskog sustava. To ćemo učiniti pomoću sljedećih naredbi:

```
sudo apt-get update  
sudo apt-get upgrade
```

Sljedeći te ujedno i zadnji korak je povlačenje skripte s interneta te njezino pokretanje:

```
wget https://git.io/vpnsetup -O vpnsetup.sh && sudo sh vpnsetup.sh
```

Skripta automatski generira korisničko ime, lozinku i IPSec unaprijed dijeljeni ključ, ali u slučaju da želite sami postaviti svoje ime, lozinku i ključ umjesto gornje naredbe upišite sljedeće naredbe:

```
wget https://git.io/vpnsetup -O vpnsetup.sh  
nano -w vpnsetup.sh
```

U dokumentu sada promijenite YOUR_IPSEC_PSK, YOUR_USERNAME and YOUR_PASSWORD u svoje vrijednosti. Imajte na umu da bi se ključ trebao sastojati od minimalno 20 nasičenih simbola. Zatim pokrenite skriptu:

```
sudo sh vpnsetup.sh
```

Nakon ovih koraka trebali bi imati ispis kao na slici 75. Sljedeći korak je povezivanje klijenta s poslužiteljom. Više o tome u sljedećim poglavljima.

```
*****  
.../OBJ.linux.x86_64/testing/enumcheck/enumcheck -> /usr/local/libexec/ipsec/enumcheck  
## Creating VPN configuration...  
  
## Updating sysctl settings...  
  
## Updating IPTables rules...  
  
## Enabling services on boot...  
  
## Starting services...  
  
=====  
IPsec VPN server is now ready for use!  
Connect to your new VPN with these details:  
  
Server IP: 88.207.40.217  
IPsec PSK: sD5A9oRCgNRCAyumoWEt  
Username: vpnuser  
Password: r4ytMSVDFdyf5UHD  
  
Write these down. You'll need them to connect!  
  
Important notes: https://git.io/vpnnotes  
Setup VPN clients: https://git.io/vpnclients  
=====  
dominik@server:~$ _
```

Slika 75: Uspješno izvođenje Libreswan skripte

Spajanje s poslužiteljom na Windows 10 OS-u

Za spajanje s poslužiteljom nije potrebno ništa instalirati već samo poduzeti sljedeće korake:

- desni klik na Wi-Fi/mrežnu ikonu u *taskbar*-u
- stisnite **Open Network & Internet settings** te na stranici koja se otvorí stisnite **Network and Sharing Center**
- stisnite **Set up a new connection or network**
- označite **Connect to a workplace** i stisnite **Next**
- stisnite **Use my Internet connection (VPN)**
- upišite IP adresu vašeg poslužitelja u polje **Internet address**
- u polje **Destination name** upišite što želite i stisnite **Create**
- vratite se u **Network and Sharing Center** i na lijevoj strani stisnite opciju **Change adapter settings**
- desni klik na novu VPN opciju i odaberite **Properties**
- stisnite **Security** polje i za **Type of VPN** odaberite "Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)"
- stisnite **Allow these protocols** te označite "Challenge Handshake Authentication Protocol (CHAP)" i "Microsoft CHAP Version 2 (MS-CHAP v2)"
- stisnite **Advanced settings**
- odaberite **Use preshared key for authentication** i unesite svoj PSK ključ

-
- stisnite **OK** kako bi zatvorili napredne postavke
 - stisnite **OK** kako bi spremili postavke VPN konekcije

Sada možete ponovno stisnuti na ikonu mreže te bi vam se trebala pojaviti opcija spajanja na VPN. Stisnite na nju te unosite korisničko ime te lozinku. Nakon toga bi trebali biti spojeni s vašim VPN poslužiteljem. U slučaju da je spajanje neuspješno probajte otkloniti kvar koristeći sljedeći link <https://github.com/hwds12/setup-ipsec-vpn/blob/master/docs/clients.md#troubleshooting>.

Spajanje s poslužiteljom na Linuxu

Upute su za Ubuntu Linux. Za ostale provjerite postoje li paketi network-manager-l2tp i network-manager-l2tp-gnome, ako postoje preuzmite ih i instalirajte te slijedite upute ispod. Korisnicima Ubuntu distribucija potreban je dostupan paket network-manager-l2tp-gnome koji isto moraju preuzeti i instalirati nakon toga pratite sljedeće upute.

Idite na **Settings** zatim **Network** te onda **VPN**. Stisnite + gumb. Odaberite **Layer 2 Tunneling Protocol (L2TP)**, polje **Name** popunite kako želite, u polje **Gateway** upišite IP adresu vašeg poslužitelja, a pod **User name** upišite vaše korisničko ime. U polje **Password** upišite lozinku, polje **NT Domain** ostavite praznim. Stisnite na gumb **IPSec Settings** te odaberite **Enable IPsec tunnel to L2TP host**, ostavite polje **Gateway ID** prazno. Upišite svoj PSK ključ u polje **Pre-shared key**. Otvorite **Advanced** sekciju te upišite aes128-sha1-modp2048! u polja **Phase1 Algorithms** i **Phase2 Algorithms**. Stisnite **OK** i potom **Add** kako bi spremili konekciju. Na kraju upalite **VPN** prekidač. Sada bi trebali biti spojeni na vaš poslužitelj. U slučaju da je došlo do pogreške probajte otkloniti kvar koristeći stranicu <https://github.com/hwds12/setup-ipsec-vpn/blob/master/docs/clients.md#troubleshooting>.

Spajanje s mobilnim uređajima

Spajanje na iOS-u i Android-u gotovo je isto pa ćemo iz tog razloga dati upute samo za Android.

Otvorite **Postavke** zatim **Bežično povezivanje i mreže** i odaberite **VPN**. Stisnite **Dodavanje VPN mreže** te zatim upišite proizvoljni **Naziv**, odaberite **L2TP/IPSec PSK** za vrstu konekcije. Popunite **Adresu poslužitelja** IP adresom vašeg poslužitelja te unesite vaš ključ u polje **IPSec unaprijed dijeljeni ključ**. Stisnite **Spremi** te sada odaberite vašu novu VPN konekciju. Upišite **Korisničko ime** i **Lozinku** te odaberite opciju Spremi podatke o računu. Na kraju stisnite **Poveži**.

7 Usporedba

	Windws	Linux	FreeBSD	Složenost(1-5)
Windows 10 VPN	*			
Tinc VPN	*			
SoftEther VPN	*			
OpenVPN	*	*	*	3
LibreSwan VPN		*	*	2

-
- 8 Slični projekti**
 - 9 Resursi**
 - 10 Glavni rizici**
 - 11 Smanjivanje rizika**
 - 12 Glavne faze projekta**
 - 13 Struktura raspodijeljenog posla(engl. Work Breakdown Structure - WBS)**
 - 14 Kontrolne točke projekta**
 - 15 Gantogram**
 - 16 Zapisnici sastanaka**

Literatura

- [1] CARNet CERT. Osnovni koncepti vpn tehnologije, 2003. <https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf>.
- [2] James Henry Carmouche. *IPsec Virtual Private Network Fundamentals*. Cisco Press, 2006.
- [3] D. Nobori, T. Sugiyama, G. Hatakeyama, and C. Smith. Softether vpn project, 2013. Online; accessed 12 November 2018.
- [4] Margaret Rouse. Ssl vpn (secure sockets layer virtual private network), 2018. Online; accessed 12 November 2018.
- [5] OpenVPN. Overview of openvpn. <https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn>, 2015. Online; pristupljeno: 10. siječnja 2019.
- [6] Justin Ellingwood. How to set up an openvpn server on ubuntu 16.04. <https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-16-04>, May 2016. Online; pristupljeno: 14. prosinca 2018.
- [7] Libreswan. Libreswan vpn software. <https://libreswan.org/>. Online; pristupljeno: 11. siječnja 2019.
- [8] Lin Song. Ipsec vpn server auto setup scripts. <https://github.com/hwds12/setup-ipsec-vpn>, 2018. Online; pristupljeno: 15. prosinca 2019.
- [9] Justin Ellingwood. How to set up an ikev2 vpn server with strongswan on ubuntu 18.04. <https://www.digitalocean.com/community/tutorials/how-to-set-up-an-ikev2-vpn-server-with-strongswan-on-ubuntu-18-04-2>, July 2018. Online; pristupljeno: 14. prosinca 2018.
- [10] Latex. <https://www.overleaf.com>. Online; accessed 12 November 2018.

A Dodatak A: Indeks (slika, tablica, ispisa koda)

1	Prozor Promjena mogućnosti prilagodnika	5
2	Prozor Detalji o mrežnoj dijagnostici	6
3	Svojstva (IPv4)	6
4	Prozor Novi korisnik	7
5	Dopusti veze s ovim računalom	7
6	Postavke usmjeritelja za prosljedivanje	8
7	Dodavanje pravila za port 1723	9
8	Dopuštanje veze	9
9	Odabir kada se pravilo primjenjuje	10
10	DUC	11
11	Adresa povezivanja	11
12	Službeni logo SoftEther VPN-a	12
13	Put do instalacije	12
14	Poveznica za odabir preuzimanja	13
15	Prikaz povaznice za preuzimanje	13
16	Odabir servera	14
17	Početni prozor aplikacije SoftEther	14
18	Dodavanje nove veze	15
19	Odabir konfiguracije	15
20	Mogućnosti servera	16
21	Dodavanje virtualnog čvorišta	16
22	Dodavanje virtualnog čvorišta	17
23	Korisnici servera	17
24	Popis korisnika	17
25	Stvaranje korisnika	18
26	Stvaranje certifikata korisnika	18
27	Stvaranje ključa korisnika	19
28	Datoteke ključ i certifikat	19
29	Prikaz dodanog korisnika	19
30	Put do instalacije	20
31	Poveznica za odabir preuzimanja	20
32	Prikaz povaznice za preuzimanje	21
33	Prikaz odabira klijentske instalacije	21
34	Prikaz upravitelja VPN veza	22
35	Stvaranje adaptera	22
36	Dodavanje VPN veze	23
37	Polje lozinke	23
38	Spajanje na server	23
39	Prikaz poveznice za preuzimanje	26
40	Ikona instalacije	26
41	Prikaz dodataka instalacije	27
42	Preimenovanje TAP adaptera	27
43	Pokretanje naredbenog retka u administratorskom načinu	28
44	Prikaz pokretanja build-dh naredbe	28

45	Stvaranje certifikata povezivanja	29
46	Stvaranje certifikata servera	29
47	Stvaranje certifikata klijenta	30
48	Direktorij za konfiguraciju	30
49	Povezivanje sa serverom	32
50	Status servera	32
51	Prikaz Klijent.ovpn datoteke	33
52	Postavke DigitalOcean poslužitelja	35
53	Odabir lokacije i ssh ključeva	36
54	Struktura direktorija nakon inicijalizacije PKI	38
55	Struktura direktorija nakon stvaranja korjenskog certifikata	38
56	Stvaranje certifikata	39
57	Struktura direktorija nakon stvaranja klijentskog i poslužiteljevog certifikata	39
58	Sadržaj <code>keys</code> direktorija na poslužitelju	40
59	Putanje do ključeva i certifikata u datoteci <code>openvpn.conf</code>	41
60	Sadržaj <code>keys</code> direktorija na klijentu	42
61	Mrežna sučelja klijenta	42
62	Mrežna sučelja poslužitelja	43
63	Mrežna sučelja drugog klijenta	43
64	Izlaz naredbe ping	44
65	Kopiranje i ispis datoteke <code>pozdrav.txt</code>	44
66	Postavljanje vrijednosti za certifikacijsko tijelo	46
67	Dobar ispis nakon postavljanja izvořišta	46
68	Dogodila se pogreška prilikom izgradnje CA	47
69	Izgled konfiguracijske datoteke - UFW Firewall	49
70	Pokrenuta usluga OpenVPN	50
71	OpenVPN sučelje tun0	51
72	Konfiguracija klijenta - client1	53
73	Uvoz klijentske konfiguracije na Windowsima	53
74	OpenVPN aplikacija	54
75	Uspješno izvođenje Libreswan skripte	56