

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	6
6.1.3 Provjera vlastite IP adrese	16
6.2 FreeBSD	17
6.2.1 FreeBSD VPN over IPsec	17
6.3 Linux	18
6.3.1 OpenVPN	18
6.3.2 StrongSwan IKEv2 VPN Server	27
7 Slični projekti	28
8 Resursi	28
9 Glavni rizici	28
10 Smanjivanje rizika	28
11 Glavne faze projekta	28
12 Struktura raspodijeljenog posla(engl. Work Breakdown Structure - WBS)	28
13 Kontrolne točke projekta	28
14 Gantogram	28
15 Zapisnici sastanaka	28
Literatura	29
A Dodatak A: Indeks (slika, tablica, ispisa koda)	30

1 Puni naziv projekta

Metode uspostave VPN servera, VPN klijenta 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 (network-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 mjesečne 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 ostatku 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 nekomercijalnih 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 programskih rješenja.

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

5 Voditelj studentskog tima

6 Rezultati

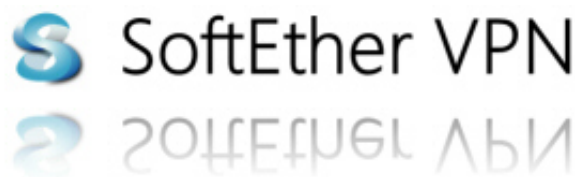
6.1 Windows

6.1.1 Windows 10 VPN

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 poglavlju prikazan postupak postavljanja i uporabe.



Slika 1: Službeni logo SoftEther VPN-a

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.

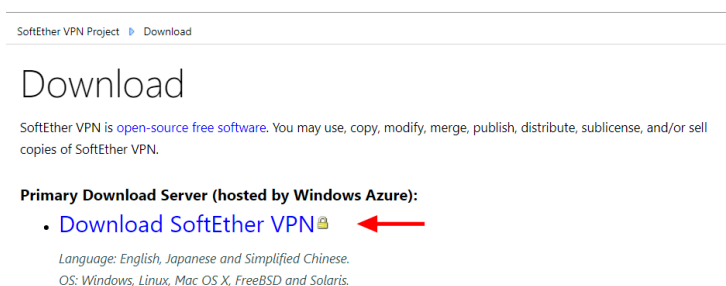
Instalacija SoftEther servera

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

<https://www.softether.org>



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



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)

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

SoftEther VPN Setup Wizard (Version 4.28.9669) X

Select Software Components to Install

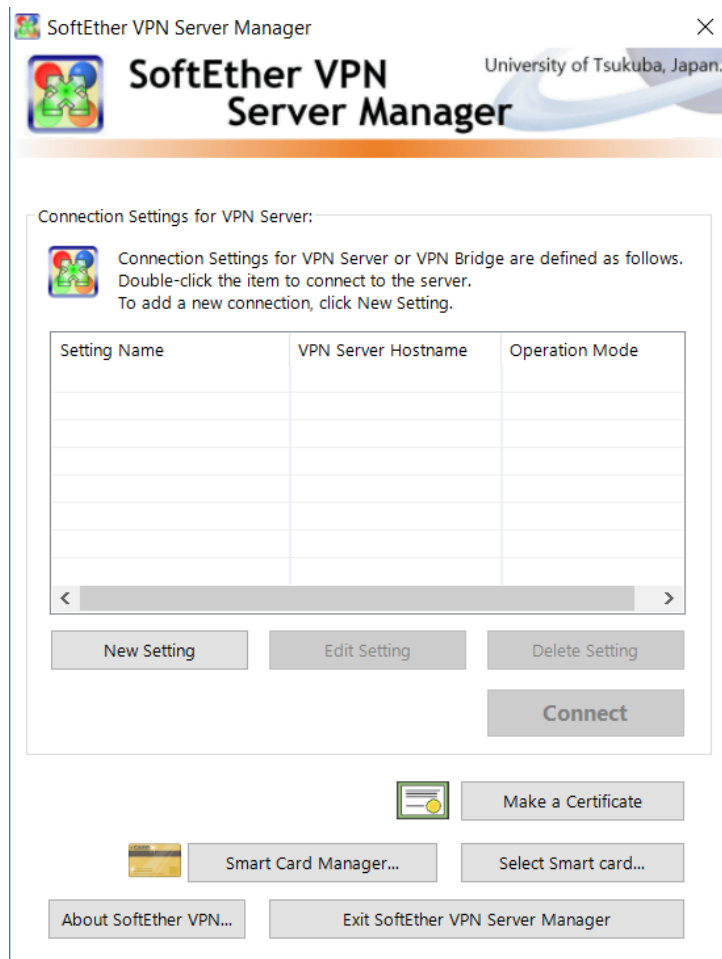
SoftEther VPN Server
SoftEther VPN Bridge
SoftEther VPN Server Manager (Admin Tools Only)

About SoftEther VPN Server

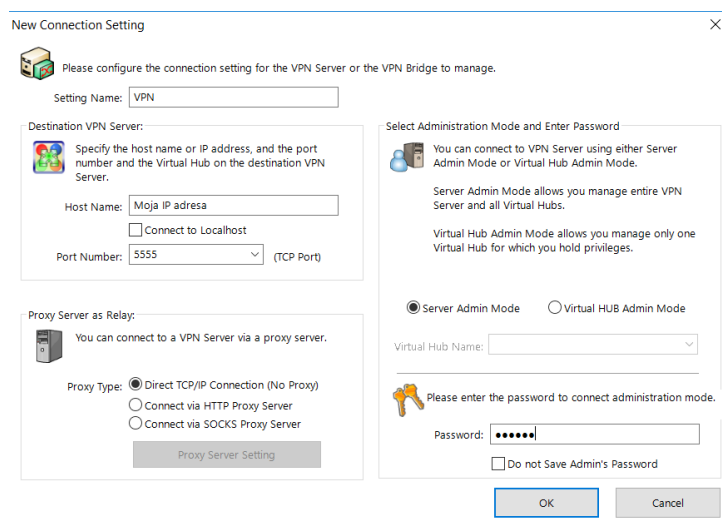
Install it on a server computer at the central site of VPN. The management tools will be also installed.

< Natrag Dalje > Odustani

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



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



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

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

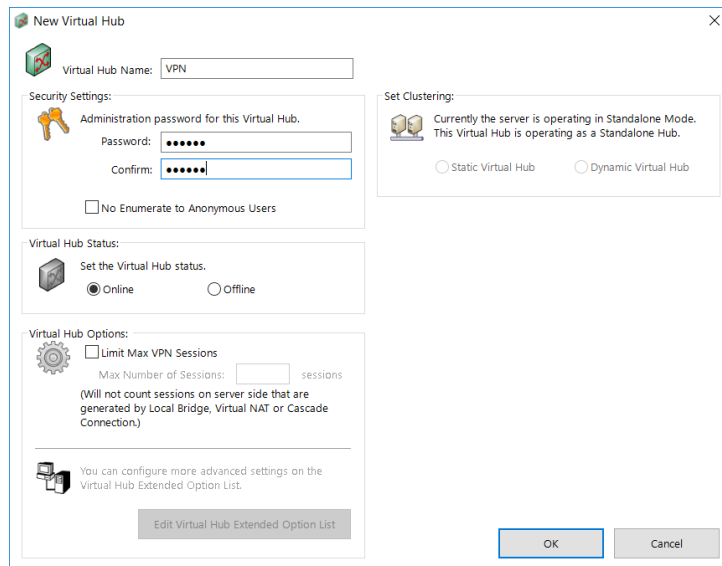
<
>

New Setting
Edit Setting
Delete Setting

Connect

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

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



New Virtual Hub

Virtual Hub Name:

Security Settings:

Administration password for this Virtual Hub.

Password:

Confirm:

☐ No Enumerate to Anonymous Users

Set Clustering:

Currently the server is operating in Standalone Mode. This Virtual Hub is operating as a Standalone Hub.

☐ Static Virtual Hub ☐ Dynamic Virtual Hub

Virtual Hub Status:

Set the Virtual Hub status.

☒ Online ☐ Offline

Virtual Hub Options:

☐ Limit Max VPN Sessions

Max Number of Sessions: sessions

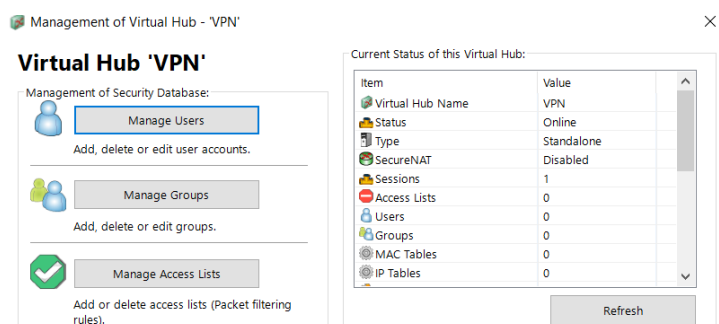
(Will not count sessions on server side that are generated by Local Bridge, Virtual NAT or Cascade Connection.)

You can configure more advanced settings on the Virtual Hub Extended Option List.

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

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



Management of Virtual Hub - 'VPN'

Virtual Hub 'VPN'

Management of Security Database:

Add, delete or edit user accounts.

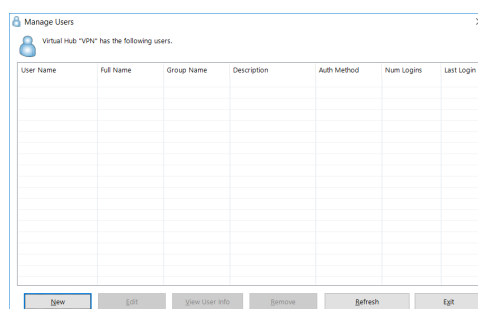
Add, delete or edit groups.

Add or delete access lists (Packet filtering rules).

Current Status of this 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

Na ovom prozoru odabiremo “Manage Users”.



Manage Users

Virtual Hub "VPN" has the following users.

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

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 zloporabe VPN-a, odabiremo mogućnost prijave klijenta uporabom našeg certifikata i lozinke. Zbog toga odabiremo “Create Certificate”.

Create New User

User Name: klijent1
Full Name: klijent1
Note:
Group Name (Optional): klijenti
Set the Expiration Date for This Account: 14.11.2018. 0:00:00
Auth Type: Anonymous Authentication, Password Authentication, Individual Certificate Authentication, Signed Certificate Authentication, RADIUS Authentication, NT Domain Authentication
RADIUS or NT Domain Authentication Settings: Login attempts by password will be verified by the external RADIUS server, Windows NT domain controller, or Active Directory controller. Specify User Name on Authentication Server: User Name on Authentication Server:
Security Policy: Set Security Policy Security Policy
Password Authentication Settings: Password: Confirm Password:
Individual Certificate Authentication Settings: The users using 'Individual Certificate Authentication' will be allowed or denied connection depending on whether the SSL client certificate completely matches the certificate that has been set for the user beforehand. Specify Certificate View Certificate Create Certificate
Signed Certificate Authentication Settings: Verification of whether the client certificate is signed is based on a certificate of a CA trusted by this Virtual Hub. Limit Common Name (CN) Value Limit Values of the Certificate Serial Number Note: Enter hexadecimal values. (Example: 0155ABCDDEF)
Hint: Define a user object with username "*" (asterisk) in order to accept a login attempt of a user which does not match any of registered explicit user objects. Such a special user will use the external user-authentication server to verify the login.
OK Cancel

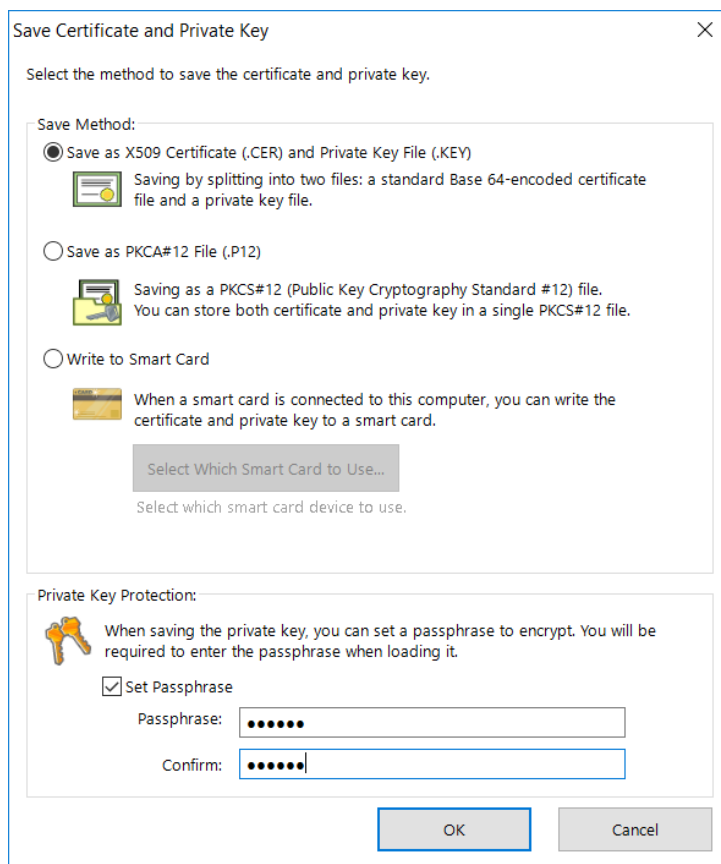
U sljedećim je poljima moguće detaljno odrediti opis stvorenog klijenta kao i vrijeme njegovog postojanja.

Create New Certificate

You can easily create certificates which is signed by self or other certificates.

Certificate Type: Root Certificate (Self-Signed Certificate) Certificate Signed by Other Certificate
Certificate and Private Key for Signing: Load Certificate and Private Key
Click 'Load Certificate and Private Key' to specify the X509 Certificate and RSA Private Key that will use a new certificate signature.
Common Name (CN): klijent1
Organization (O): free
Organization Unit (OU):
Country (C):
State (ST):
Locale (L): Zagreb
Serial Number (Hexadecimal):
Expires in: 3650 Days Strengthness: 2048 bits
To manage certificates and certificate authorities on a large scale, you should use either free software such as OpenSSL, or commercial CA (certificate authority) software.
OK Cancel

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



Save Certificate and Private Key

Select the method to save the certificate and private key.

Save Method:

☒ Save as X509 Certificate (.CER) and Private Key File (.KEY)
Saving by splitting into two files: a standard Base 64-encoded certificate file and a private key file.

☐ Save as PKCS#12 File (.P12)
Saving as a PKCS#12 (Public Key Cryptography Standard #12) file. You can store both certificate and private key in a single PKCS#12 file.

☐ Write to Smart Card
When a smart card is connected to this computer, you can write the certificate and private key to a smart card.
Select Which Smart Card to Use...
Select which smart card device to use.

Private Key Protection:

When saving the private key, you can set a passphrase to encrypt. You will be required to enter the passphrase when loading it.

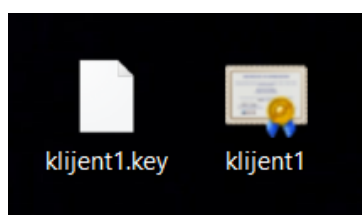
☒ Set Passphrase

Passphrase:

Confirm:

OK Cancel

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.



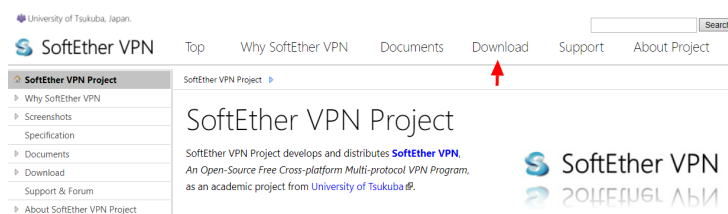
Nakon potvrde vidljiv je korisnik koji se može spojiti na naš server. Moguće je naravno dodavanje više različitih korisnika i brisanje istih.

Virtual Hub "VPN" has the following users.

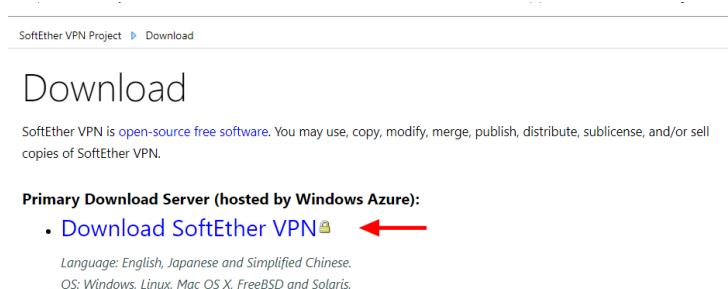
User Name	Full Name	Group Name	Description	Auth Method	Num Logins	Last Login
klijent1	klijent1	-		Individual Certific...	0	(None)

Instalacija SoftEther klijenta

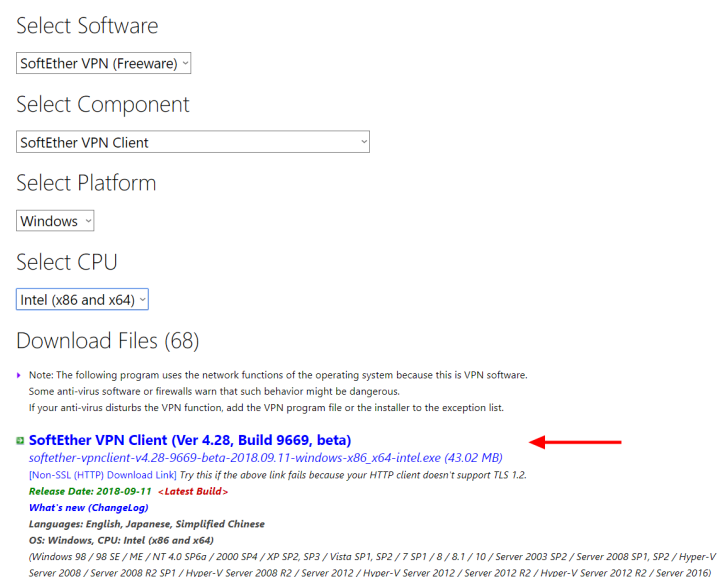
Za razliku od instalacije i konfiguracije servera, instalacija je SoftEther klijenta jednostavnija. Prvi je korak preuzimanje instalacije sa službene stranice SoftEthera:
<https://www.softether.org>



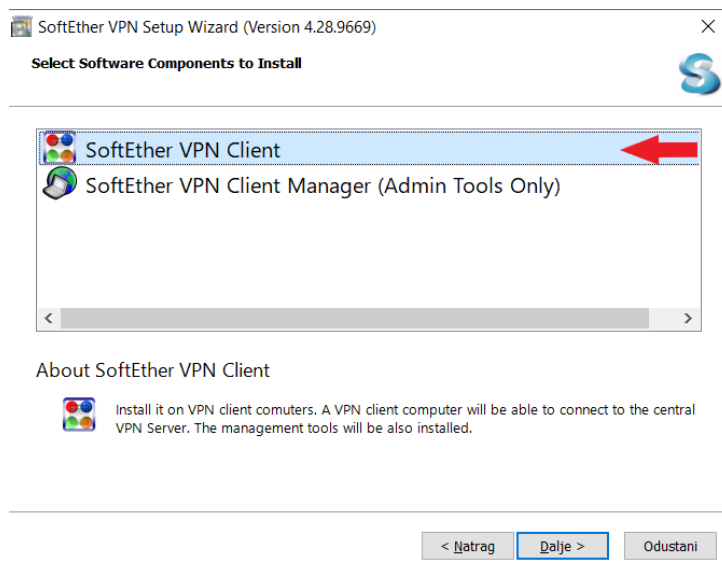
Odabirom “Download” iz izborne trake prikazuje se stranica s ponuđenim poveznicama za preuzimanje.



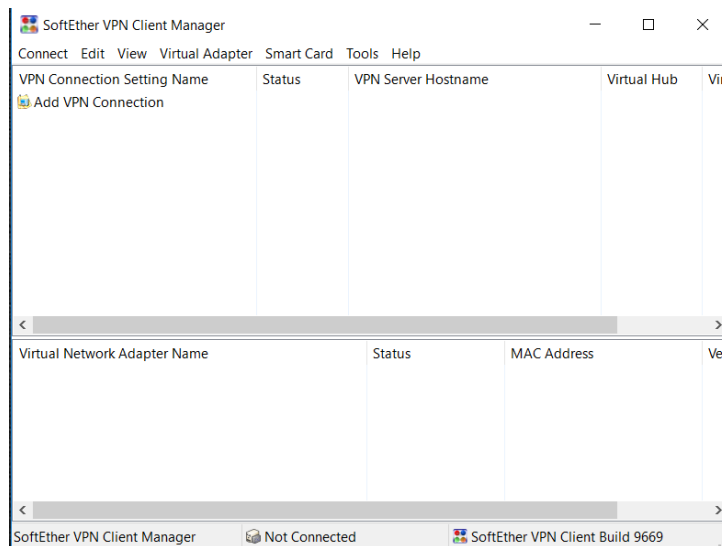
Sljedeći isječak prikazuje stranicu koja se otvori odabirom prve poveznice. Na stranici se nalaze izborni okviri u kojima je potrebno odabrati željeni program. Za preuzimanje VPN klijenta potrebno je odabrati postavke prikazane na sljedećem isječku te odabrati prvu poveznicu za početak preuzimanja.



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

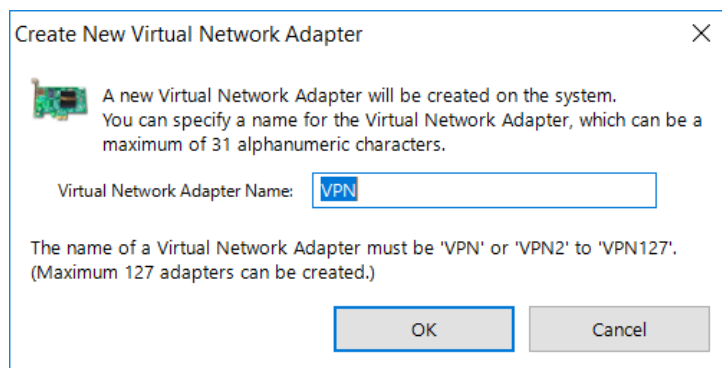


Ukoliko je instalacija uspješno završena, prikazuje se sljedeći prozor.

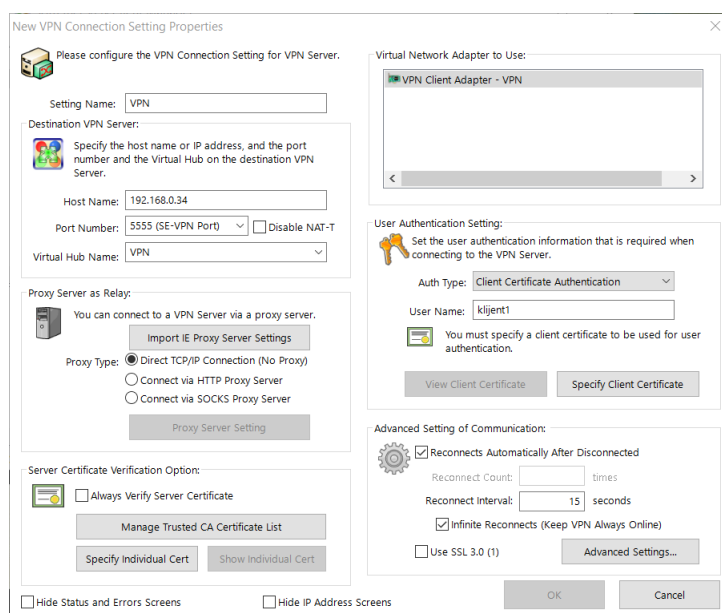


Povezivanje klijenta sa SoftEther serverom

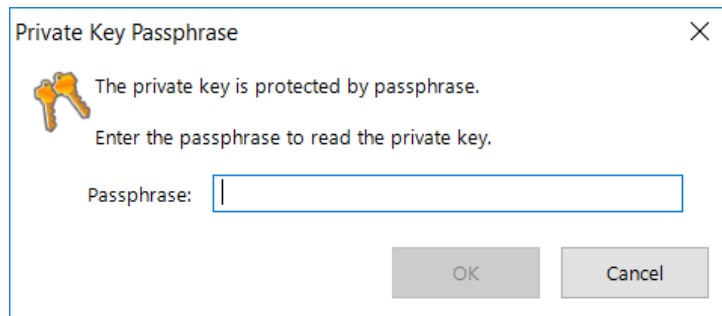
Za uspješno povezivanje s napravljenim serverom potrebno je pokrenuti aplikaciju SoftEther VPN Client i odabrati opciju dodavanja novog VPN-a. Ako nije postavljen virtualni mrežni adapter, kao što je prikazano u sljedećem primjeru, potrebno je stvoriti novi. Prikazano je stvaranje VPN adaptera.



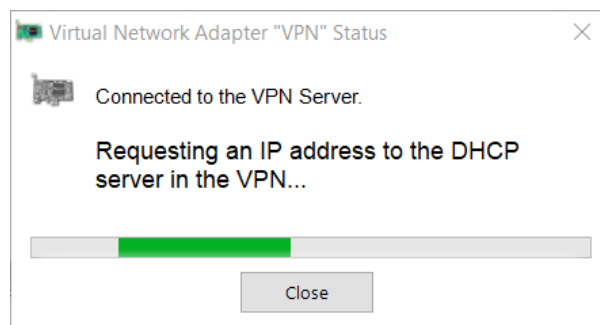
Nakon stvaranja adaptera moramo dodati server na koji se želimo povezati. Na slici je prikazano stvaranje veze koja se zove VPN. Slično kao i kod stvaranja servera, potrebno je upisati IP adresu preko koje se može serveru pristupiti u polje "Host name". Aplikacija nakon upisa IP adrese dohvaća portove 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".



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

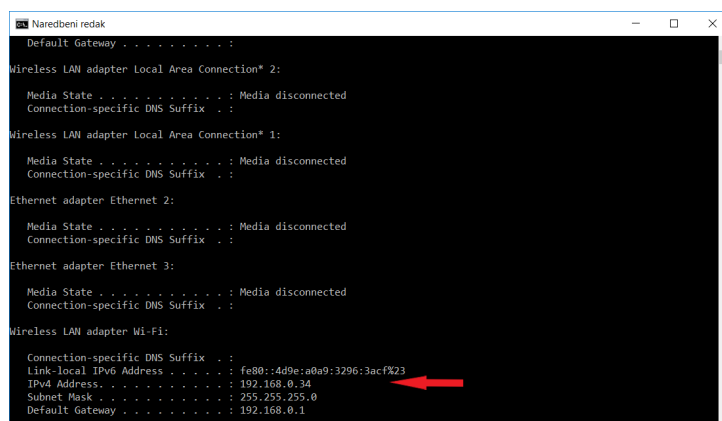


Ako smo učitali ispravni certifikat i unijeli ispravnu lozinku, tada će se prikazati prozor na kojem vidimo povezivanje s VPN serverom.



6.1.3 Provjera vlastite IP adrese

Kako bi server bio uspješno uspostavljen, potrebna mu je IP adresa dodijeljena računalu na kojem se nalazi. Najbrži način na koji se ona može odrediti jest otvaranje naredbenog retka i upis naredbe IPCONFIG. Rezultat te naredbe bit će prikaz mrežnih postavki za trenutno aktivne mrežne adaptere. Crvenom je strelicom označena IP adresa na trenutno aktivnom adapteru.



6.2 FreeBSD

6.2.1 FreeBSD VPN over IPsec

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 naprednijim 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^[7] 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`:

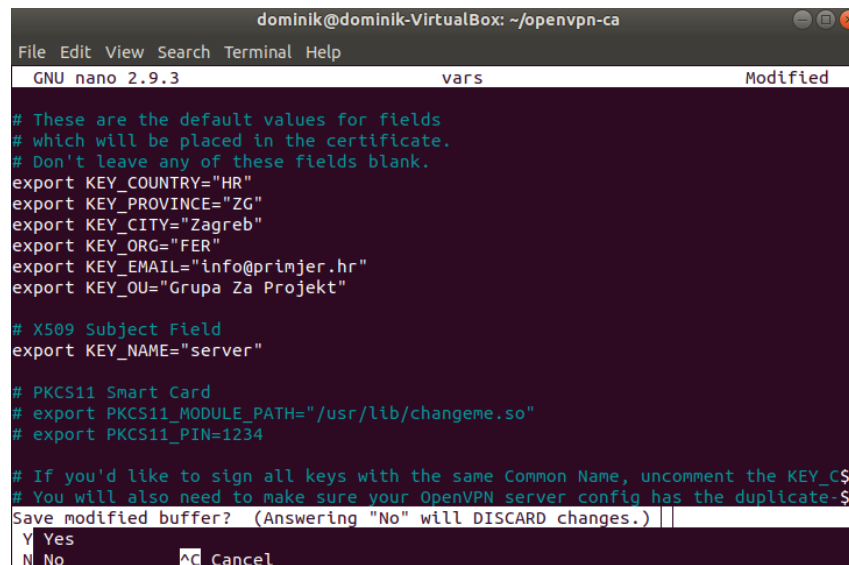
```
nano vars
```

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 izađite.

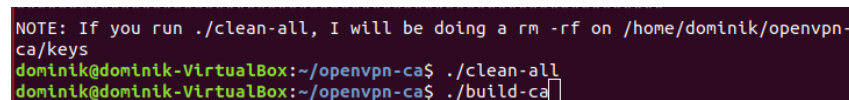


Slika 2: Postavljanje vrijednosti za CA

Izgradnja certifikacijskog tijela

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

```
cd ~/openvpn-ca
source vars
```



Slika 3: Dobar ispis nakon postavljanja izvorišta

Ako je sve prošlo kako treba trebali bi imati ispis kao na slici 3 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 4 , 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
pkitool: 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 4: 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. Prihvatite 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 podatak upišite:

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

U slučaju da želite lozinkom zaštititi:

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

Opet kao i prije prihvatite ponudene 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
```

Nađite 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 nađite liniju vezanu uz kriptografske šifrantе 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 prihvāt 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 izađite.

Prilagođavanje 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 izađite.

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:

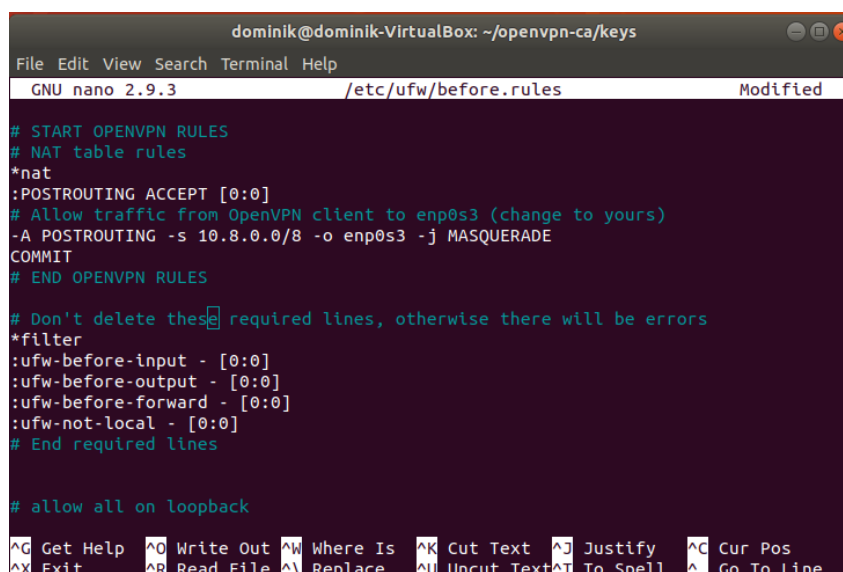
```
ip route | grep default
```

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
```



Slika 5: Izgled konfiguracijske datoteke - UFW Firewall

U konfiguraciju dodajmo plavo označene dijelove pritom zamijenite enp0s3 za ime mrežnog sučelja koje ste maloprije otkrili. Konačan izgled trebao bi biti kao na slici 5.

```
#
# 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 izađimo.

```
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.

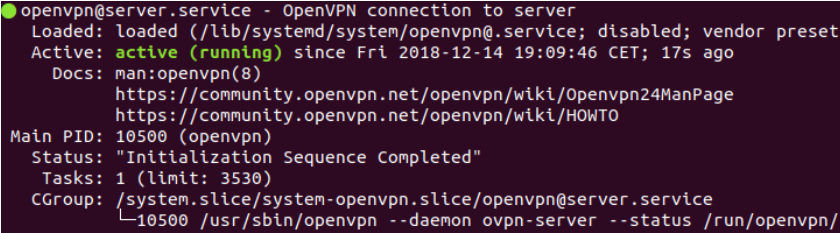
```
sudo ufw allow 1194/udp  
sudo ufw allow OpenSSH  
sudo ufw disable  
sudo ufw enable
```

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 greške trebao bi biti kao na slici 6. Možete isto tako provjeriti je



```
● 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 6: Pokrenuta usluga OpenVPN

li dostupno OpenVPN sučelje tun0. Ispis bi trebao biti kao na slici 7.

```
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::bfb:393c:7667:9ecf/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
```

Slika 7: 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
```

Nađite 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 izađite.

```
#!/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 8: Konfiguracija klijenta - client1

Instalacija OpenVPN-a na računalo 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

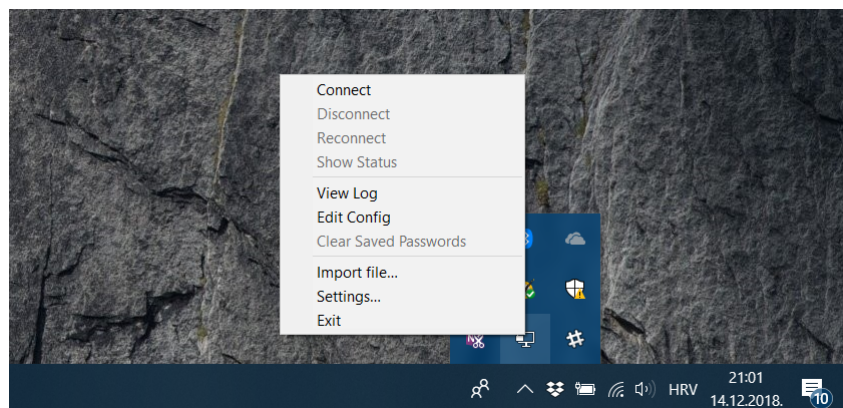
Otvorite sljedeći link <https://openvpn.net/community-downloads/> i skinite program za Windowse te pokrenite instalaciju. Nakon instalacije u donjem desnom kutu vašeg ekrana pojaviti će se ikona OpenVPN-a kao na slici . Desni klik na nju i odaberite Import file. Nakon toga navigirajte do mjesta gdje 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 uredi 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.

Skinite aplikaciju OpenVPN i otvorite ju, bit će vam prikazan početni ekran kao na slici 10a. 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 10b.

Nakon toga dobit će te poruku o uspješnom učitavanju profila (slika: 10c). Stisnite na opciju ADD u gornjem desnom kutu. I na kraju se povežite s VPN poslužiteljem pritiskajući na sivi gumb (slika: 10d).



Slika 9: Uvoz klijentske konfiguracije na Windowsima

6.3.2 StrongSwan IKEv2 VPN Server

Što je StrongSwan?

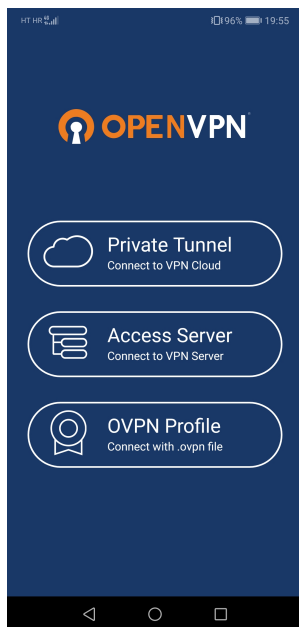
-
- 7 Slični projekti
 - 8 Resursi
 - 9 Glavni rizici
 - 10 Smanjivanje rizika
 - 11 Glavne faze projekta
 - 12 Struktura raspodijeljenog posla(engl. Work Breakdown Structure - WBS)
 - 13 Kontrolne točke projekta
 - 14 Gantogram
 - 15 Zapisnici sastanaka

Literatura

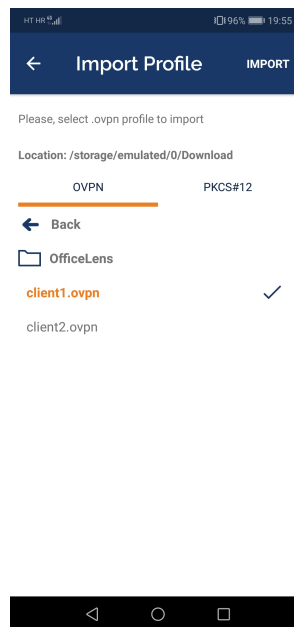
- [1] CARNet CERT. Osnovni koncepti vpn tehnologije, 2003. <https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf>.
- [2] James Henry Carmouche. *IPsec Virtual Private Network Fundamentals*. Cisco Press, 2006.
- [3] D. Nobori, T. Sugiyama, G. Hatakeyama, and C. Smith. Softether vpn 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] Latex. <https://www.overleaf.com>. Online; accessed 12 November 2018.
- [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] OpenVPN. Overview of openvpn. <https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn>, 2015. Online; pristupljeno: 10. siječnja 2019.

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

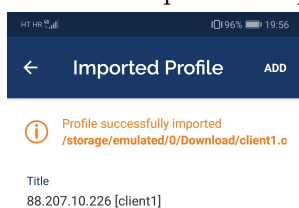
1	Službeni logo SoftEther VPN-a	6
2	Postavljanje vrijednosti za certifikacijsko tijelo	19
3	Dobar ispis nakon postavljanja izvorišta	19
4	Dogodila se pogreška prilikom izgradnje CA	20
5	Izgled konfiguracijske datoteke - UFW Firewall	22
6	Pokrenuta usluga OpenVPN	23
7	OpenVPN sučelje tun0	24
8	Konfiguracija klijenta - client1	26
9	Uvoz klijentske konfiguracije na Windowsima	27
10	OpenVPN aplikacija	31



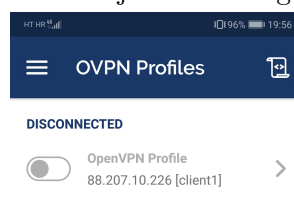
(a) Početni ekran OpenVPN aplikacije



(b) Odabir klijentske konfiguracije



(c) Uspješno učitavanje profila



(d) Profil je uspješno dodan

Slika 10: OpenVPN aplikacija