

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 Uvod	3
2 Windows	4
2.1 Windows 10 VPN	4
2.2 SoftEther VPN	5
3 FreeBSD	16
3.1 FreeBSD VPN over IPsec	16
4 Linux	17
4.1 OpenVPN za Ubuntu distribuciju Linux operacijskog sustava	17
Literatura	18
A Dodatak A: Indeks (slika, tablica, ispisa koda)	19

1 Uvod

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 devedestih godina te se ona u početku razvijala samo za velike organizacije koje su zahtjevale siguran prijenos osjetljivih podataka putem interneta. Kroz godine komercijalizacija interneta je omogućila većini država pristup najvećoj mreži što je drastično povećalo broj potencijalnih žrtava tadašnjih hakera. Nakon brojnih provala u sustave velikih tvrtki svakodnevni korisnici su postali svjesni loše sigurnosti interneta zbog čega raste potražnja tehnologija koje poboljšavaju mrežnu sigurnost.

Zaštita podataka se osigurava 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 VPN usluge se 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 rješenje nam omogućava da sami odlučimo kako želimo zaštititi prijenos vlastitih podataka. U ostatku rada se nalazi pregled, usporedba i upute za instalaciju poznatijih VPN tehnologija na različitim platformama.

2 Windows

2.1 Windows 10 VPN

2.2 SoftEther VPN

Što je SoftEther VPN?

SoftEther VPN je besplatan 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

Zbog toga što je SoftEther otvorenog koda može ga bilo tko koristiti za osobnu ili komercijalnu uporabu bez plaćanja.

SoftEther VPN koristi HTTPS preko SSL (Secure Sockets Layer) 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.

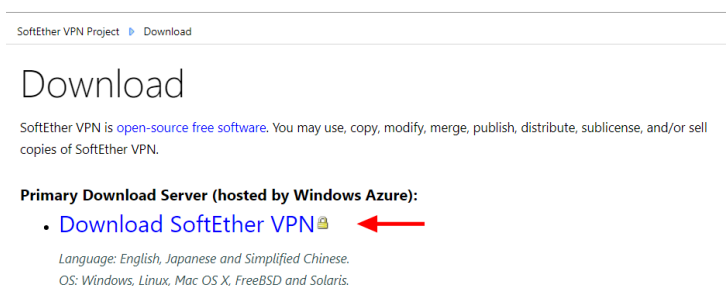
Instalacija SoftEther servera

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 vezama za preuzimanje.



Sljedeći isječak prikazuje stranicu koja se otvori odabirom prve veze. 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 vezu za početak preuzimanja.

Select Software
SoftEther VPN (Freeware) ▾

Select Component
SoftEther VPN Server Manager for Windows ▾

Select Platform
Windows ▾

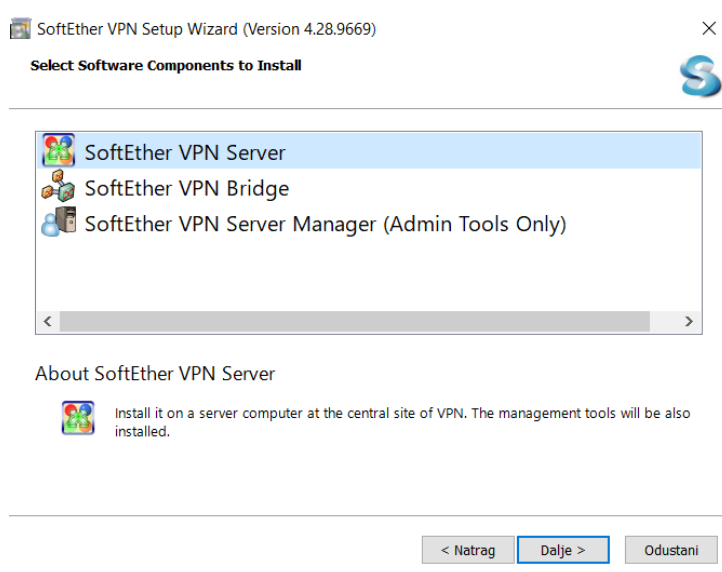
Select CPU
Intel (x86 and x64) ▾

Download Files (68)

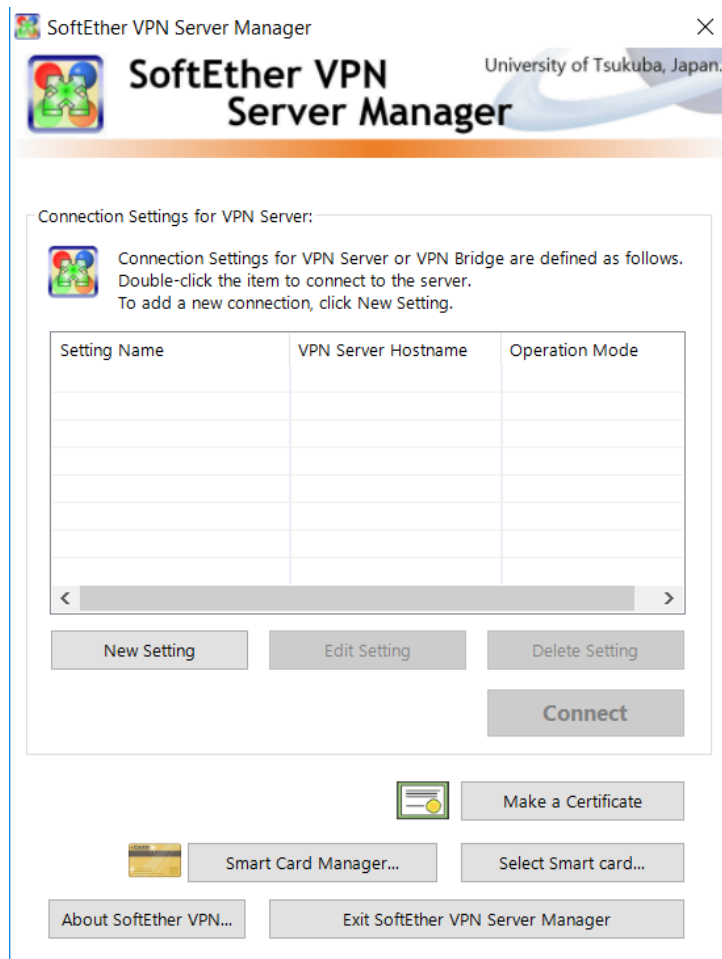
▶ Note: The following program uses the network functions of the operating system because this is VPN software. Some anti-virus software or firewalls warn that such behavior might be dangerous. If your anti-virus disturbs the VPN function, add the VPN program file or the installer to the exception list.

■ **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)

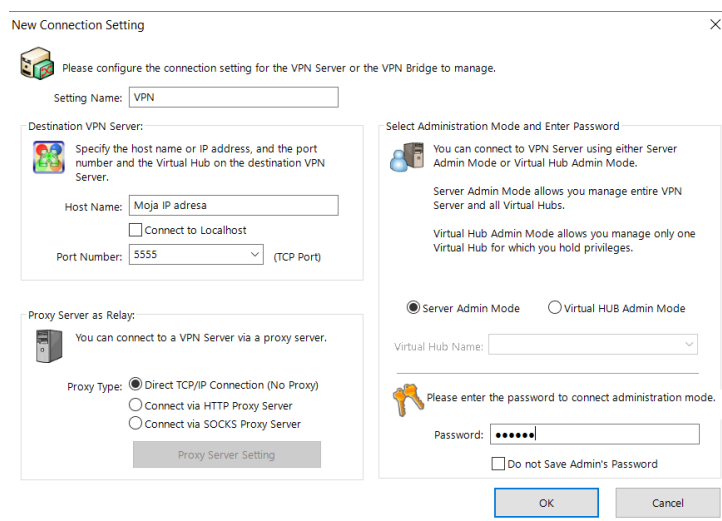
Nakon preuzimanja i pokretanja instalacije otvara se sljedeći prozor u kojemu se predlaže instaliranje prvog ponuđenog jer nudi potpunu instalaciju.



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 imena servera u polje “setting name” i upisom vlastite IP adrese preko koje je trenutno računalo spojeno na Internet. Upute za pronalazak IP adrese mogu se naći na kraju ovog poglavlja. Preporuka je dodati lozinku za pristup serveru zbog dodatnog osiguranja u polje “password”.



U tablici servera vidimo da je dodan novi kojega je sada 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”.

VPN - SoftEther VPN Server Manager

Manage VPN Server "192.168.0.34"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables

Manage Virtual Hub

Online

Offline

View Status

Create a Virtual Hub

Properties

Delete

Management of Listeners:
Listener List (TCP/IP port):

Port Number	Status
TCP 443	Listening
TCP 992	Listening
TCP 1194	Listening
TCP 5555	Listening

Create

Delete

Start

Stop

VPN Server and Network Information and Settings:

Encryption and Network

View Server Status

About this VPN Server

Edit Config

Clustering Configuration

Clustering Status

Show List of TCP/IP Connections

Local Bridge Setting

Layer 3 Switch Setting

IPsec / L2TP Setting

OpenVPN / MS-SSTP Setting

Dynamic DNS Setting

VPN Azure Setting

VPN Gate Setting

Refresh

Exit

Current DNS Hostname: vpn187396261.softether.r

Virtualnom čvorištu postavljamo proizvoljno ime te dodajemo lozinku zbog 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 “Menage 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 “Menage 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 dati proizvoljno ime (u ovim uputama nazvan je korisnik `klijent1` i u svim koracima gdje se to ime pojavi vama će se pojaviti vaše odabrano ime). Kako bi smanjili mogućnost zloporabe VPN-a, odabiremo mogućnost prijave klijenta uporabom našeg certifikata i lozinke. Zbog toga odabiremo “Create Certificate”.

Create New User

User Name:

Full Name:

Note:

Group Name (Optional):

☐ Set the Expiration Date for This Account

14.11.2018.

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:

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.

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: 0155ABCDEF)

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.

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:

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):

Organization (O):

Organization Unit (OU):

Country (C):

State (ST):

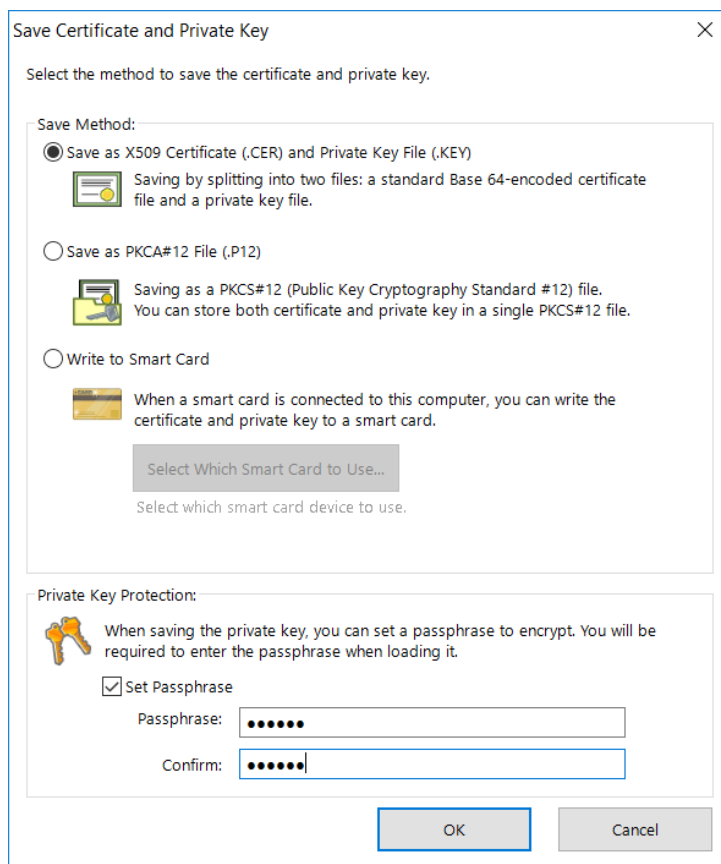
Locale (L):

Serial Number (Hexadecimal):

Expires in: Days Strengthness: 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.

Kada nam se otvori ovaj prozor postaviti ćemo 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.

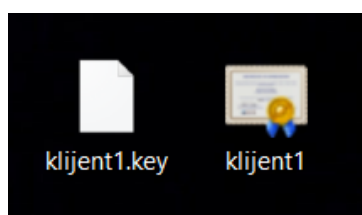
☒ Set Passphrase

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 stoga 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.

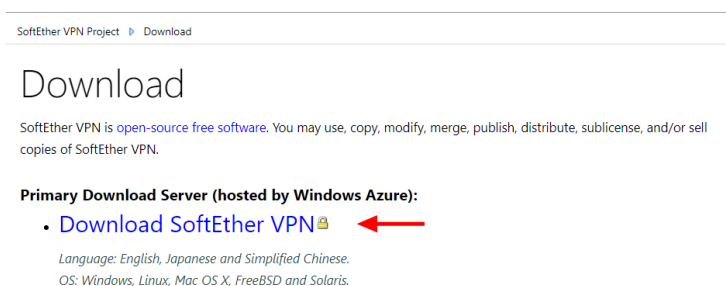
User Name	Full Name	Group Name	Description	Auth Method	Num Logins	Last Login
klijent1	klijent1	-		Individual Certific...	0	(None)

Instalacija SoftEther klijenta

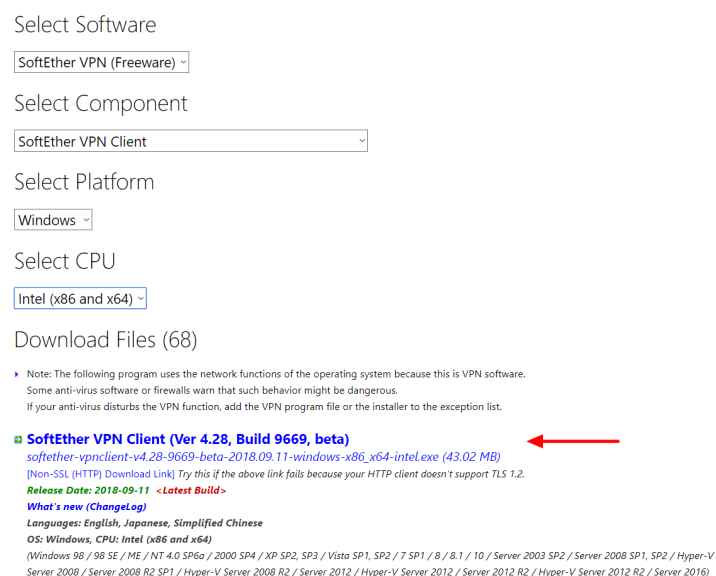
Za razliku od instalacije i konfiguracije servera, instalacija je SoftEther klijenta jednostavnija. Prvi je korak preuzimanje instalacije sa službene stranice SoftEthera: <https://www.softether.org>



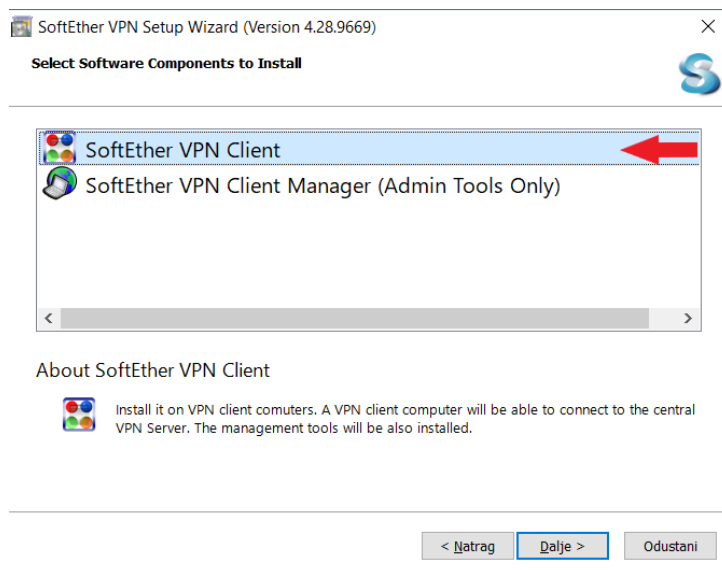
Odabirom Download iz izborne trake prikazuje se stranica s ponuđenim vezama za preuzimanje.



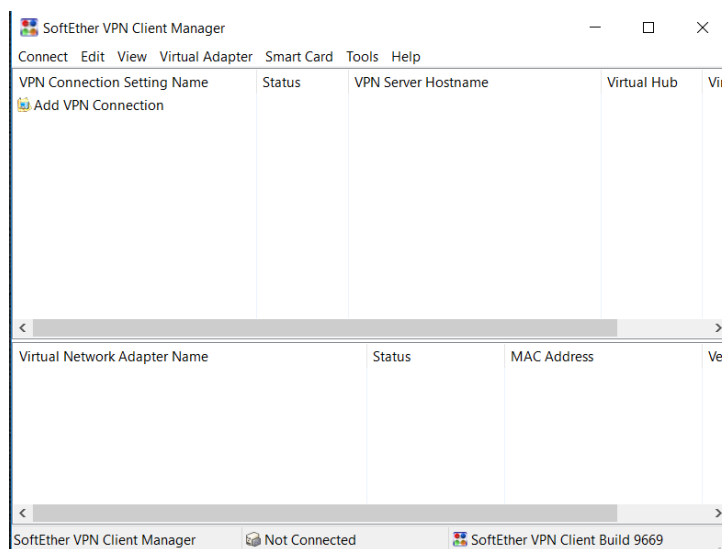
Sljedeći isječak prikazuje stranicu koja se otvori odabirom prve veze. Na stranici se nalaze izborni okviri u kojima je potrebno odabrati željeni program. Za preuzimanje VPN klijenta potrebno je odabrati postavke prikazane na sljedećem isječku te odabrati prvu vezu za početak preuzimanja.



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

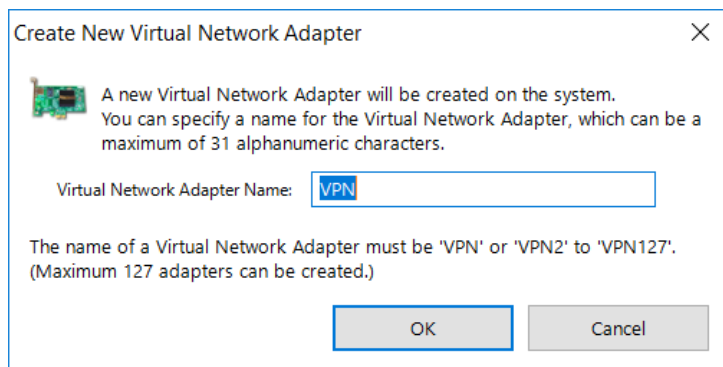


Ukoliko je instalacija uspješno završena prikazuje se sljedeći prozor.

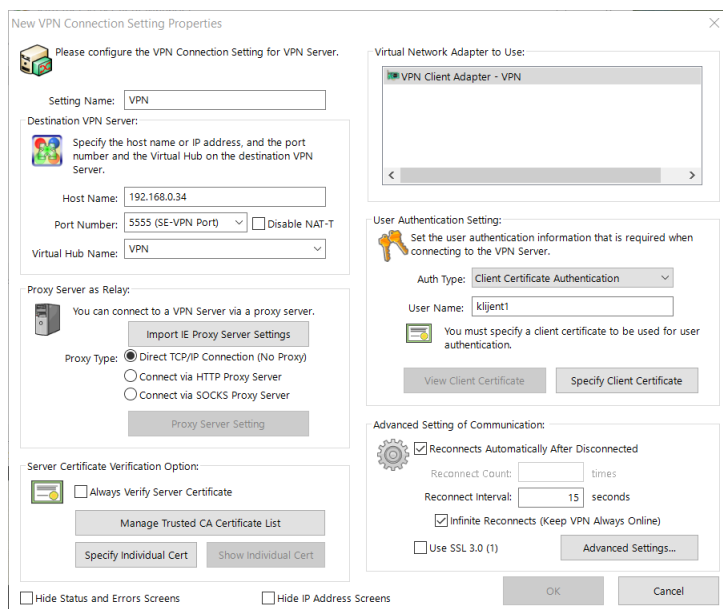


Povezivanje klijenta sa SoftEther serverom

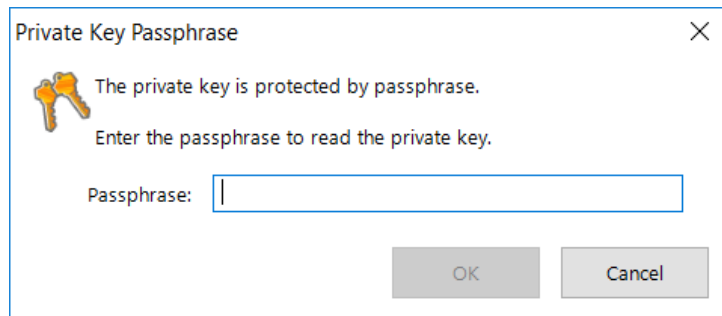
Kako bi se povezali uspješno s napravljenim serverom, potrebno je pokrenuti aplikaciju SoftEther VPN Client i odabrati opciju dodavanja novog VPN-a. Ako nije postavljen virtualni mrežni adapter, kao što je prikazano, potrebno je stvoriti novi. Prikazano je stvaranje VPN adaptera.



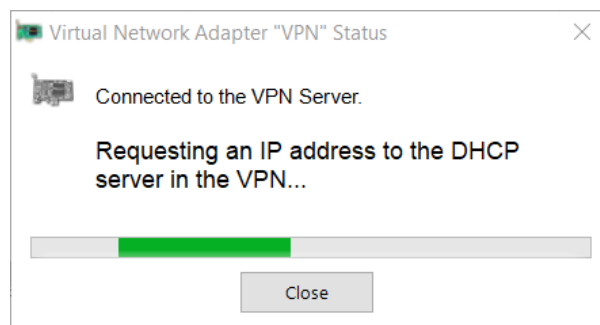
Nakon stvaranja adaptera moguće je dodati server na koji se želimo povezati. Na slici je prikazano stvaranje veze koja se zove VPN. Slično kao i kod stvaranja servera, potrebno je upisati IP adresu preko koje se može serveru pristupiti u polje "Host name". Nakon upisa IP adrese aplikacija dohvaća portove na koje moguće spojiti. Izbor je nekog od ponuđenih portova proizvoljan kao i postojećih virtualnih mrežnih adaptera. Pošto 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 na sljedećem isječku u koji se upisuje lozinka koju smo postavili prilikom stvaranja klijenta.

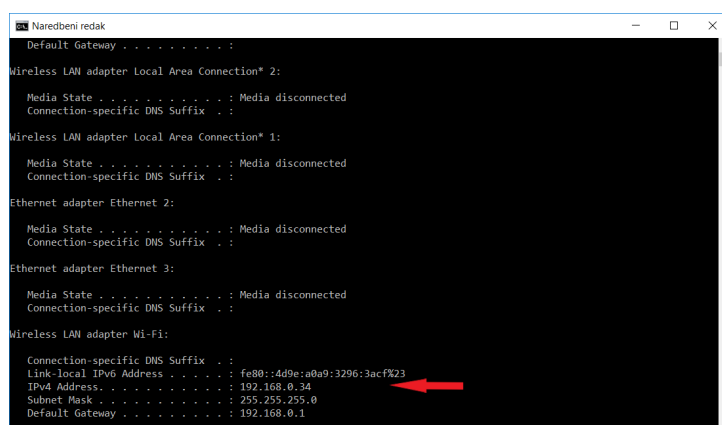


Ako smo učitali ispravan certifikat i unijeli ispravnu lozinku, tada će se prikazati prozor koji prikazuje spajanje na server.



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 strjelicom označena IP adresa na trenutno aktivnom adapteru.



3 FreeBSD

3.1 FreeBSD VPN over IPsec

4 Linux

4.1 OpenVPN za Ubuntu distribuciju Linux operacijskog sustava

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.

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

1	Službeni logo SoftEther VPN-a	5
---	---	---