CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

OpenVPN

NCERT-PUBDOC-2010-04-298

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

U vremenu globalne povezanosti Internet je postao gotovo najbitniji način komunikacije između korisnika. Virtualna privatna mreža (VPN) predstavlja komunikacijski sustav koji koristi infrastrukturu Interneta za prilagodljiv i ekonomičan prijenos podataka između udaljenih ili virtualnih ureda, te djelatnika koji se putem kućnih računala povezuju u privatnu računalnu mrežu. Osim Interneta, za ostvarivanje VPN veze moguće je koristiti različite tehnologije i komunikacijske kanale kao što su dijeljene ATM mreže, privatne mreže ISP-a, i dr. Korištenje VPN metode za povezivanje udaljenih lokacija ima nekoliko prednosti u odnosu na nekadašnje metode (koje su uključivale različite izvedbe iznajmljenih vodova), a to su:

- cijena,
- transparentnost komunikacije i
- omogućena mobilnost korisnika.

Osnovni zahtjevi koji se postavljaju za ovakav način povezivanja jesu:

- očuvanje tajnosti - zaštita od neovlaštenog pristupa informacijama
- integritet podataka - zaštita od neovlaštene izmjene podataka
- autentikacija korisnika - dokazivanje identiteta između računala ili uređaja na krajevima tunela

Jedno od rješenja koje je moguće koristiti u ovu svrhu je alat OpenVPN. Riječ je o programu koji koristi SSL/TLS protokol za enkripciju podataka stvarajući virtualni tunel između krajnjih točaka.

U ovom dokumentu su opisana osnovna obilježja OpenVPN tehnologije i postupak instalacije na različitim operacijskim sustavima. Također, navedeni su i osnovni sigurnosni koncepti koje je moguće primijeniti u svrhu zaštite podataka koji se razmjenjuju u komunikaciji. Osim toga, spomenuti su i drugi tipovi VPN rješenja, njihova usporedba kao i statistika sigurnosnih ranjivosti za alat OpenVPN.

2. VPN

Otkako je sredinom 90-ih godina širokopojasni Internet postao dostupniji većini korisnika (koji su dotad koristili samo modem) pojavila se potreba za razvojem različitih novih tehnologija. To je, između ostalog, vodilo i do osiguravanja pouzdanih veza između ogranaka tvrtki, ali i djelatnika koji su radili na udaljenim lokacijama, a imali su potrebu pristupati pojedinim programima i podacima tvrtke. Takvim dijelovima mreže ili sustava nije poželjno pristupati kroz nesigurne javne mreže (kao što je Internet) nego je bilo potrebno osigurati pristup pomoću tzv „privatnog tunela" koji se prenosi preko javne mreže.

VPN (eng. *virtual private network*) je tehnologija koja omogućava siguran prijenos potencijalno osjetljivih informacija (podaci/govor/video) preko nesigurnih mreža. VPN uspostavlja „tunel" za komunikaciju sa središnjom lokacijom, a za uspostavu sigurne komunikacije koriste se različiti kriptografski algoritmi.

Postoje dva osnovna tipa VPN-a:

1. *Site-to-Site* – primjer ovakvog povezivanja je podružnica tvrtke koja ima potrebu stalnog ili povremenog povezivanja s glavnom lokacijom
2. *Remote access VPN* – koristi se povremeno za spajanje pojedinačnih korisnika na poslužitelj tvrtke s mobilnih telefona ili ukoliko djelatnik tvrtke radi od kuće

Osnovna prednost korištenja ovakvog oblika komunikacije je cijena. S jedne strane tvrtka može koristiti skupe iznajmljene linije (eng. *leased lines*) prema željenim lokacijama ili može primijeniti neka od brojnih VPN rješenja koja danas postoje na tržištu. Neke od tih tehnologija su potpuno besplatne i jednostavne za korištenje, dok druge zahtijevaju znatna financijska sredstva i stručno osoblje koje će administrirati takve sustave.

2.1. OpenVPN

OpenVPN je programski paket otvorenog koda koji se koristi za implementiranje virtualnih privatnih mreža. Trenutno je aktualna inačica 2.1.1 izdana 11. prosinca 2009. godine.

OpenVPN koristi SSL/TLS (eng. *Secure Sockets Layer /Transport Layer Security*) protokol za uspostavu sigurne komunikacije između određenih točaka VPN veze. Za razliku od ostalih VPN rješenja ovoga tipa koja koriste web preglednik na strani klijenta, paket OpenVPN potrebno je instalirati na strani poslužitelja i klijenta. Isti se program instalira na obje strane, a osnovno podešavanje je relativno jednostavno s tim da složenost raste ovisno o topologiji same mreže (i stupnju sigurnosti koje se želi primijeniti). Stoga se OpenVPN može smatrati i P2P (eng. *peer-to-peer*) aplikacijom. Ovo je rješenje moguće koristiti za stalno (eng. *site-to-site*) ili povremeno povezivanje pojedinih korisnika te udaljenih lokacija na središnju.

Neke od osnovnih prednosti korištenja OpenVPN-a su:

- postupak instalacije i početno podešavanje programa je relativno jednostavno.
- prilagodljivost - prilikom uspostave VPN veze moguće je mijenjati programsku skriptu kako bi se zadovoljile potrebe korisnika. Jedan primjer je automatsko preusmjeravanje zahtjeva korisnika na alternativni poslužitelj ako dođe do pada primarnog (eng. *failover*). Sljedeći primjer je uravnoteženje opterećenja između više poslužitelja (eng. *load balancing*) u slučaju velikog broja zahtjeva korisnika za uspostavom veze.
- portabilnost – spomenuti je paket moguće koristiti na gotovo svim danas popularnim operacijskim sustavima (Windows, Linux, Mac OS, Solaris, FreeBSD, NetBSD i OpenBSD).
- podaci koji se razmjenjuju usmjeravaju se na TCP ili češće na UDP priključak (eng. *port*) 1194. Od inačice 2.0 moguće je koristiti i neki drugi UDP/TCP priključak, ovisno o želji korisnika. Osnovna razlika između njih je što TCP osigurava pouzdanu isporuku podataka od pošiljatelja prema primatelju (traži ponavljanje izgubljenog ili neispravnog paketa). Za razliku od njega, UDP je jednostavniji, nema provjeru razmjene podataka, te je pogodan za komunikacije gdje su greške dozvoljene (npr. prijenos video materijala).
- u radu koristi virtualna mrežna sučelja korištenjem TUN ili TAP upravljačkih programa. Stvarajući virtualno mrežno sučelje i prisiljavajući sve programe da mu prosljeđuju svoje podatke, VPN klijent je u stanju kriptirati sav odlazni promet bez potrebe za ikakvim promjenama na postojećim programima. TUN sučelje predstavlja virtualnu mrežnu karticu, u primjeni sličnu uređajima koji povezuju dvije točke na krajevima pojedinih mreža (npr. povezivanje dvije mreže s iznajmljenom T1 linijom). Međutim, tako realizirani uređaj neće podatke usmjeravati na fizički sloj (komunikacijsku liniju), nego prema programu koji primljene

pakete čita i piše u oba smjera. TAP sučelje je slično, samo što se koristi za složenije mrežne topologije, za razliku od „točka-točka" komunikacije, gdje se koristi TUN.

- osigurana programska podrška za istovremenim održavanjem više tunela prema klijentima (u inačici 1.x poslužitelj je mogao istovremeno imati vezu prema samo jednom klijentu).
- autentikacija korisnika je omogućena korištenjem tajnog (statičkog) ključa, certifikata ili provjerom korisničkog imena i pristupne lozinke.
- za brzo komprimiranje podataka u stvarnom vremenu koristi LZO biblioteku koja podatke komprimira prije postupka enkripcije.
- na vatrozidu (eng. *firewall*) je dovoljno otvoriti samo jedan priključak (TCP ili UDP) kako bi se udaljeni korisnici mogli spojiti na lokalnu mrežu tj. poslužitelj.
- moguće ga je koristiti u NAT okruženjima. NAT (eng. *Network Address Translation*) mehanizam omogućuje prevođenje javnih adresa u privatne.
- pokreće se u korisničkom prostoru, a ne u jezgri operacijskog sustava kao neka druga VPN rješenja (npr. IPSec). Osim povećanja sigurnosti na ovaj se način pojednostavljuje postupak instalacije i održavanja na različitim platformama.
- omogućuje prijenos različitih tipova podataka (npr. Ethernet okvira, IPX ili NETBIOS paketa) između udaljenih položaja.
- široka zajednica korisnika (preko 3 milijuna) i podrška dostupna u svakom trenutku Tako je, primjerice, moguće sve upute za konfiguriranje klijenta i poslužitelja pronaći na službenim stranicama te forumima posvećenim ovom programu. Registracija je besplatna, ali se korisnike potiče na donacije kako bi se osigurala daljnja podrška i razvoj novih funkcionalnosti.

2.2. Razvoj

Ideju i programsko ostvarenje OpenVPN projekta realizirao je James Yonan 2002. godine. Zatim je uslijedilo partnersko udruživanje sa Francis Dinhaom te je nastala tvrtka OpenVPN Technologies Inc. koja se brine o budućem razvoju i nadogradnji ovog proizvoda. Kroz svoj rad stalno unaprjeđuju program, dodaju nove funkcionalnosti, provode sigurnosne testove, pružaju tehničku podršku te održavaju projektnu dokumentaciju kako bi trenutnim i budućim korisnicima olakšali korištenje ovog VPN rješenja.

Najbitnije poveznice preko kojih se korisnici mogu informirati su prikazane u tablici 1.

Izvor	Opis
Souceforge mailing lista	http://sourceforge.net/mail/?group_id=48978
OpenVPN dokumentacija	http://openvpn.net/index.php/open-source/documentation/manuals/65-openvpn-20x-manpage.html http://openvpn.net/index.php/open-source/documentation/manuals/69-openvpn-21.html
IRC	#openvpn na stranicama irc.freenode.net
Forum	http://ovpnforum.com/
Zajednica	http://openvpn.eu/index.php?id=23&L=0

Tablica 1. Pregled stranica za praćenje novosti o OpenVPN-u

Također, razvijeno je i mnoštvo alata koji omogućuju korištenje OpenVPN-a (tablica 2):

Naziv programa	Operacijski sustav	Cijena
OpenVPN GUI	Microsoft Windows	Besplatan
Tunnelblick	Mac OS X	Besplatan
Viscosity	Mac OS X	€ 13,95
Shimo	Mac OS X	$ 9
OpenVPN	DD-WRT	Besplatan
TomatoVPN	Tomato	Besplatan
TunnelDroid	Android	Besplatan

Tablica 2. Programska podrška za OpenVPN

Osim toga OpenVPN je integriran i u programsku podršku (eng. *firmware*) Vyatta, DD-WRT, OpenWRT i Tomato platformi za usmjerivače (eng. *router*). To znači da korisnici na svojim računalima u mreži ne moraju imati instaliran OpenVPN kako bi se spajali na udaljene adrese i poslužitelje.

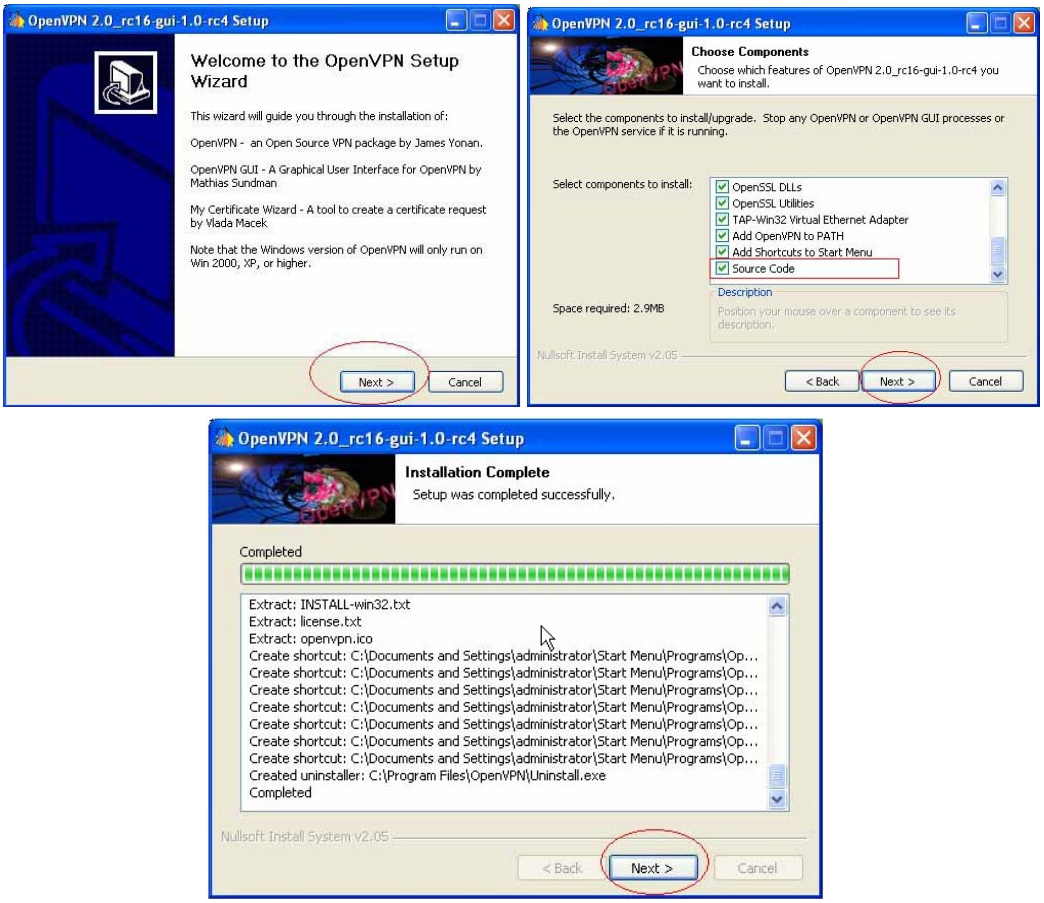
Dostupan je i na mobilnim uređajima s Windows Mobile i Nokia Maemo platformama.

3. Primjena

Programski paket OpenVPN je realiziran pod Open Source GNU licencom i moguće ga je koristiti na različitim operacijskim sustavima. Tako je, između ostalog, podržan na Mac OS, FreeBSD, NetBSD, Linux, Solaris i Windows platformama, a radi se i na inačici OpenVPN PocketPC za mobilne uređaje.

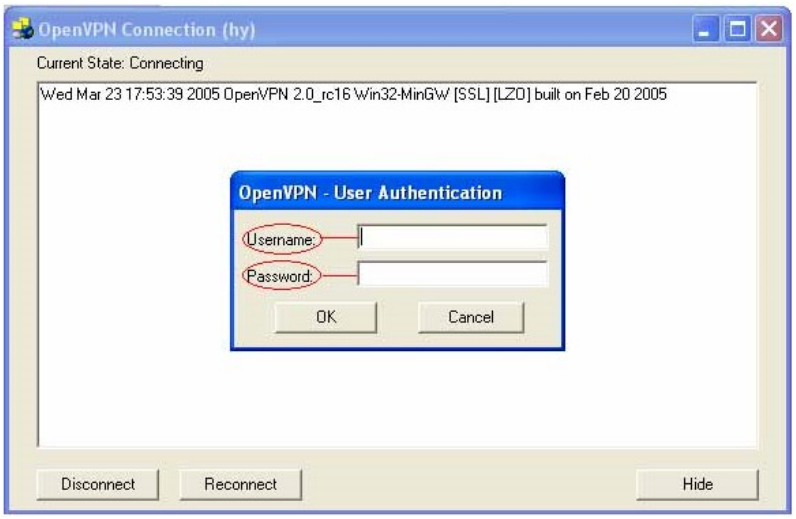
3.1. Instalacija i uporaba na Windows platformama

Ovaj paket je dostupan kao izvršna datoteka (openvpn-2.0-gui-1.0-install.exe), a instalacija traje desetak minuta. Postupak je jednostavan (slika 1.), ali zahtijeva administratorske ovlasti na sustavu.



Slika 1. Postupak instalacije na platformi Windows XP
Izvor: Packtub

Ukoliko se želi koristiti VPN veza pokrene se program: Start →Programs → OpenVPN. Zatim je potrebno upisati korisničko ime i zaporku (koji se prilikom slanja mrežom kriptiraju).

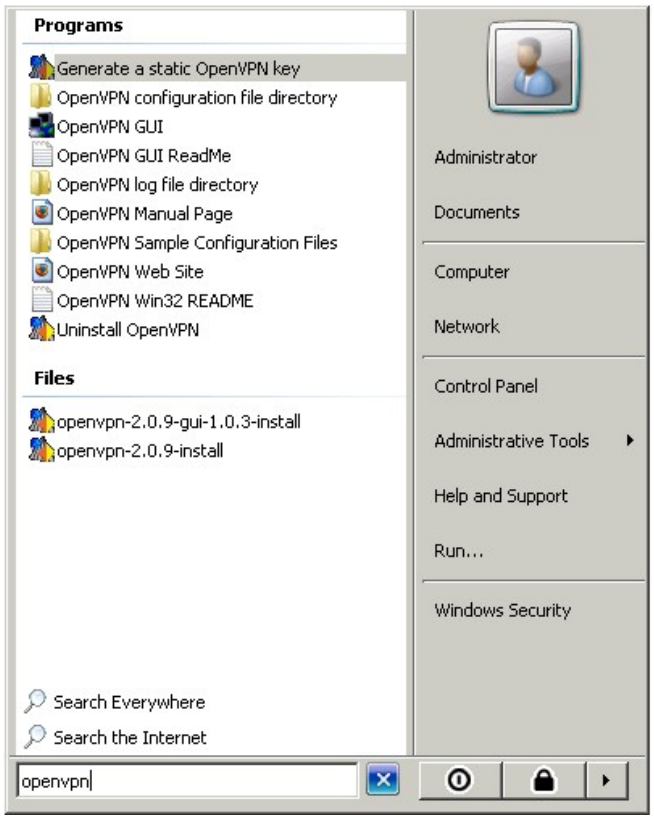


Slika 2. Upis korisničkog imena i zaporke

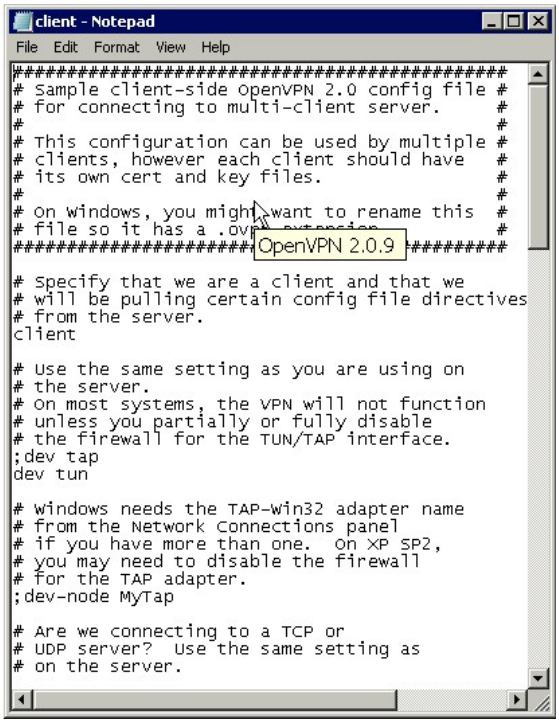
Primjer uspješno uspostavljene veze vidi se na slici 3.

Slika 3 Uspješno uspostavljena veza 1

Nakon instalacije programa, preko Start menija moguće je mijenjati različite postavke programa (slika 4 i 5). Te se promjene obavljaju pomoću programa za uređivanje teksta, kao što je primjerice Notepad. OpenVPN se konfigurira pomoću konfiguracijske (`config`) datoteke. Jedna od bitnih prednosti je to što je format te datoteke isti na svim operacijskim sustavima. Tako da je nju moguće kopirati na više sustava što je bitno uzimajući u obzir razlike između Windows i Unix/Linux platformi.



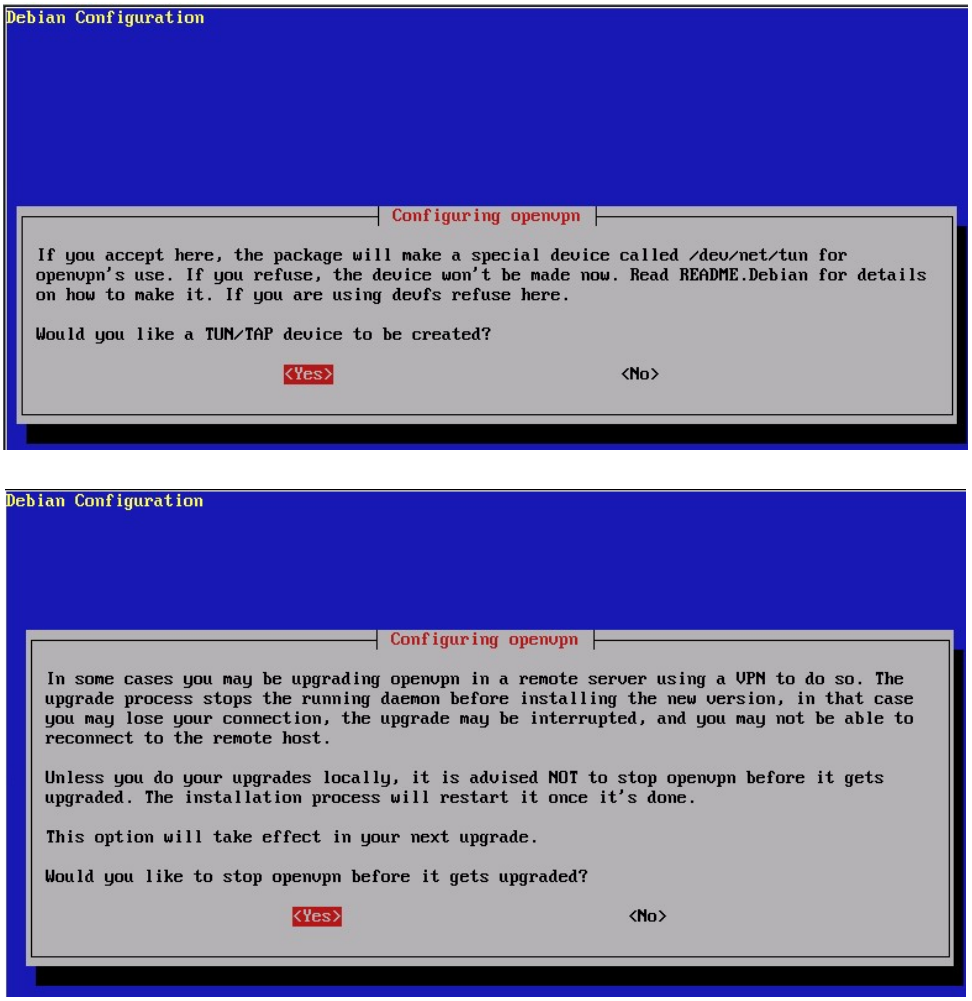
Slika 4. Opcije za konfiguriranje postavki veze
Izvor: Packtub



Slika 5. Izmjena konfiguracijske datoteke pomoću Notepad-a

3.2. Instalacija na operacijskom sustavu Debian

Najjednostavnija instalacija OpenVPN-a je na Debian platformi. Instalacija se pokreće naredbom `apt-get install openvpn`. Tijekom postupka pojavljuju se prozori prikazani na slici 6. Korisnicima se preporuča potvrditi unaprijed ponuđene vrijednosti.



Slika 6. Instalacija OpenVPN-a na Debian sustavu
Izvor: Wikipedia

Naredbom `apt-cache show openvpn` izlistavaju se podaci o instaliranom programu (slika 7).

```
debian:~# apt-cache show openvpn
Package: openvpn
Priority: optional
Section: net
Installed-Size: 744
Maintainer: Alberto Gonzalez Iniesta <agi@inittab.org>
Architecture: i386
Version: 2.0-4
Depends: debconf, libc6 (>= 2.3.2.ds1-21), liblzo1, libssl0.9.7
Filename: pool/main/o/openvpn/openvpn_2.0-4_i386.deb
Size: 293492
MD5sum: dcc638e084f7b3143c614a33b26d5750
Description: Virtual Private Network daemon
An application to securely tunnel IP networks over a single UDP or TCP port.
It can be used to access remote sites, make secure point to point connnections,
enhance WiFi security, etc.
.
OpenVPN uses all of the encryption, authentication, and certification features
of the OpenSSL library (any cipher, key size, or HMAC digest).
.
OpenVPN may use static, pre-shared keys or TLS-based dynamic key exchange. It
also supports VPNs with dynamic endpoints (DHCP or dial-up clients), tunnels
over NAT or connection-oriented stateful firewalls (like Linux's iptables).
Tag: security::cryptography, interface::daemon

debian:~#
```

Slika 7. Podaci o programu OpenVPN
Izvor: Wikipedia

4. Osnovni sigurnosni koncepti

Zaštita podataka koji se razmjenjuju prilikom korištenja OpenVPN-a ostvaruje se enkripcijom i zaštitom integriteta podataka. Za enkripciju se koriste različiti simetrični i asimetrični algoritmi, dok se za zaštitu integriteta poruka koriste funkcije za izračunavanje sažetka (eng. *hash*).

Enkripcija je postupak koji pretvara običan tekst u kriptirani tekst korištenjem određenih algoritama te tajnih i javnih ključeva.

Kod simetričnih kriptosustava isti tajni ključ koristi se za kriptiranje i dekriptiranje. Očiti nedostatak ove metode je proces dogovora oko ključa budući da je razmjenu ključeva potrebno obaviti nesigurnim putem (telefon, putem Interneta, itd.).

Osim toga, postoje i asimetrični algoritmi koji se još nazivaju i algoritmi s javnim ključem (eng. *public-key algorithms*). Njihova primjena se zasniva na korištenju dva ključa - javnog i tajnog. Tajni ključ je strogo povjerljiv i poznat je samo njegovom vlasniku, dok se javni ključ slobodno distribuira svim korisnicima s kojima se želi komunicirati ovim putem.

Koncept koji povezuje vlasnike i njihove javne ključeve na siguran način naziva se infrastruktura javnih ključeva, odnosno PKI (eng. *Public Key Infrastructure*) infrastruktura, a u tu svrhu se koriste digitalni certifikati. Nadalje, digitalni potpisi, zajedno s certifikatima, osiguravaju svojstva poput integriteta, tajnosti i autentičnosti podataka. Pritom se potpis kriptira privatnim ključem te je primatelj u mogućnosti provjeriti autentičnost poruke dekriptiranjem potpisa javnim ključem entiteta koji je poslao poruku. Uobičajeno je da se potpisom smatra sažetak same poruke.

Više detalja o ovoj temi moguće je pročitati u dokumentu „Nedostaci PKI infrastrukture“ (CCERT-PUBDOC-2009-02-255).

4.1. Statički ključ

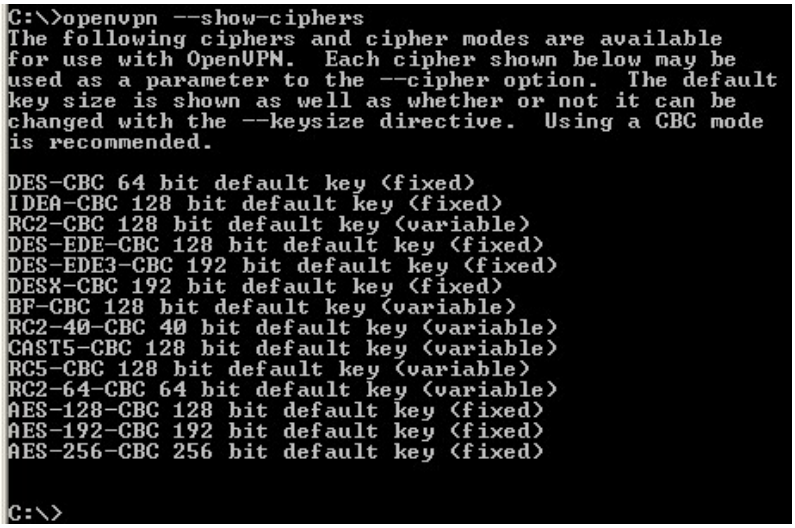
Korištenje statičkog ključa u svrhu tajnosti komunikacije, iako je jednostavno za primijeniti, nije preporučljivo iz sljedećih razloga:

- Ključ je uvijek isti tj. ne obnavlja se (moguće ga je obnoviti, ali je zatim potrebno sve sudionike obavijestiti o tome).
- Distribucija ključa se najčešće obavlja putem neodgovarajućih medija.
- Nema autentikacije sudionika u komunikaciji.

Uobičajeno, OpenVPN za kriptiranje koristi Blowfish algoritam s ključem duljine 128 bita.

Ostali simetrični algoritmi koji su dostupni kod OpenVPN-a mogu se na Windows platformi provjeriti korištenjem naredbe:

```
C:\>openvpn –show-ciphers
```



Slika 8. Simetrični algoritmi
Izvor: Openmaniak

4.1.1. Primjer spajanja dviju lokacija uporabom statičkog ključa na Windows XP platformi

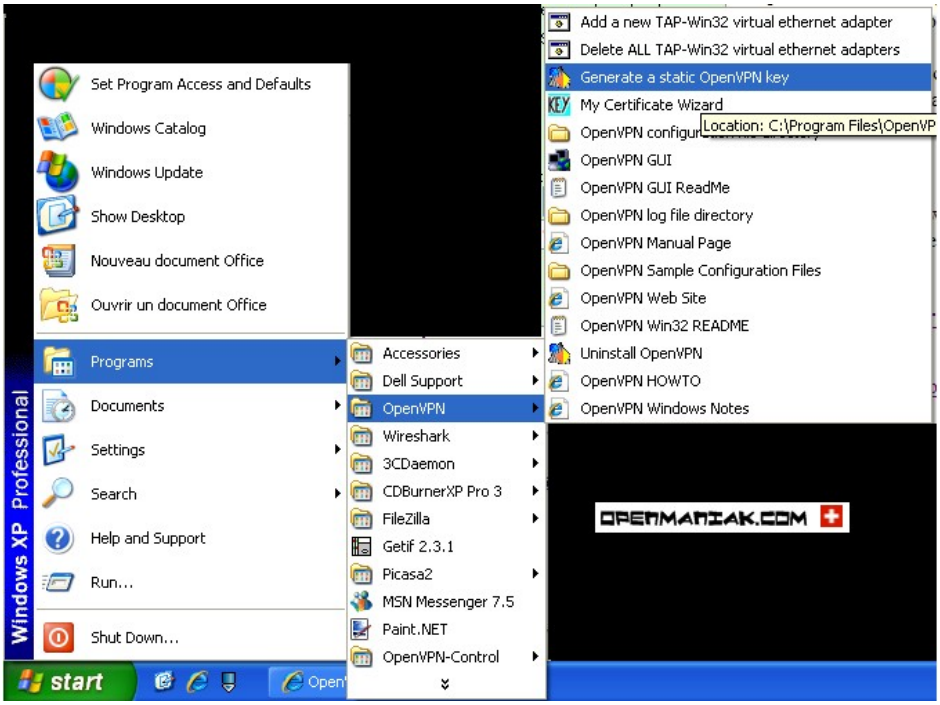
Izrada tajnog ključa je vrlo jednostavan postupak. Najprije se ključ izrađuje na strani poslužitelja i zatim kopira kod klijenata. Početno podešavanje uključuje postavke u konfiguracijskoj datoteci. Pritom se može koristiti već postojeći predložak koji se nalazi u mapi „`C:\ProgramFiles\OpenVPN\sample-config`“, pod imenom: „`sample.opvpn.txt`“, a koji se kopira u „`C:\ProgramFiles\OpenVPN\config`“ pod imenom „`server.ovpn`“.

Konfiguracijsku datoteku otvori se uređivačem teksta i potraži se redak u kojem se nalazi tekst: „`remote myremote`“. Ako se želi dozvoliti pristup s točno određene adrese npr. 213.191.134.11, tada ta linija treba glasiti „`remote 213.191.134.11`“.

Ukoliko se želi promijeniti uobičajeni broj UDP priključka 1194, potrebno je promijeniti linije koje počinju s `port` (broj priključka) i `proto` (odabir protokola).

Nakon toga se određuje način spajanja na poslužitelj. Ako se želi omogućiti povezivanje dviju mreža, ispred linije „`dev tap`“ postavlja se znak „#“ (eng. *comment*) koji označava liniju s komentarom koja se ne izvodi unutar skripte. U protivnom je riječ o spajanju s više različitih lokacija na jednu središnju i tada se bira „`dev tun`“ mogućnost.

Unutar programskog izbornika odabire se naredba „`Generate a static OpenVPN key`“, nakon čega se u mapi „`C:\ProgramFiles\OpenVPN\config`“ stvara 2048 bitni ključ za kriptiranje komunikacije pod imenom „`key.txt`“.



Slika 9. Izrada statičkog ključa
Izvor: Openmaniak

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
c909bcf7aaf9245714a745264ddb7f53
82803396bebcbe899ec5d4aae237ef0e
7cf529d52dd7d808b8c143548b3943f2
3ebc82ca0e76d413407a7d3d6cca8ba9
15ec779b2295f753981cad67a908a7d5
2b82b1a4685bbdfda202901a4e50ae20
68091a94713cf4a0c402fd0d02920a20
1de03f7848ad791d5b53b18b329d7d58
b69bc0e03203688f4c6e8c367a213f35
b7fbac77c212f96314838fcab9a11b5a
137742e4c60515d736078188d5be5085
7c894e6749ad4d4a795ed354360cd920
5b137933f8b4bb5fb5627155dbf59f70
4bf8b5a86ca8593959732e72636e84e1
4c45338cd8ffb99db42dca974e8480e5
5ad23df3d4674f4218cd691e403f33b2
-----END OpenVPN Static key V1-----
```

Slika 10. Statički ključ

Da bi ključ postao važeći mora se u konfiguracijskoj datoteci dodati linija „`secret key.txt`“. Preostaje još konfiguriranje dva parametra - `verb` i `mute`.

Parametar `verb` određuje koliko se detaljno bilježi trenutno stanje programa u dnevničkom zapisu. Minimalna vrijednost je 0 (bilježe se samo greške), a najviša 11. Parametar `mute` određuje koliko puta se pokušava ponoviti povezivanje, ukoliko prvo povezivanje nije bilo uspješno.

Početna konfiguracijska datoteka na strani poslužitelja ima oblik:

```
dev tap
proto udp
secret key.txt
persist-tun
ifconfig 192.168.122.1 255.255.255.0
verb 4
mute 10
```

Klijent se podešava s gotovo istim parametrima kao i poslužitelj, ali uz nekoliko odstupanja. Tako parametar `remote` na strani klijenta predstavlja IP adresu mreže kojoj se pristupa. Uobičajeno je, također, na strani klijenta postaviti `ifconfig` parametar kojim se definira IP adresa koju će klijent dobiti prilikom povezivanja na udaljenu mrežu.

Ako se, primjerice, klijent spaja na udaljenu mrežu s javnom IP adresom 213.191.134.11 tada konfiguracijska datoteka na strani klijenta ima oblik:

```
remote 213.191.134.11
dev tap
ifconfig 192.168.122.100 255.255.255.0
secret key.txt
verb 4
mute 10
```

Na Linux platformama konfiguracijska datoteka može izgledati identično kao na Windowsima. Za izradu ključa u konzolnom načinu rada potrebno je upisati:

```
##openvpn --genkey --secret /home/user/key.txt
```

4.2. OpenSSL

OpenVPN u radu koristi paket OpenSSL. Riječ je o besplatnom programskom paketu koji implementira SSL v2/3 i TLS v1 sigurnosne protokole, te uz to pruža i osnovnu kriptografsku podršku. Alat se temelji na biblioteci SSLeay koju su razvili Eric A. Young i Tim J. Hudson.

SSL je globalni standard sigurnosne tehnologije koji je razvio Netscape 1994. godine. SSL tehnologijom se kriptira veza između web poslužitelja i preglednika (eng. *browser*) tako da podaci koji se razmjenjuju ne mogu biti vidljivi, presretani i dešifrirani. SSLv3 inačica je korištena kao osnova za razvoj TLS protokola inačice 1.0 kao IETF (eng. *Internet Engineering Task Force*) standarda definiranog u dokumentu RFC 2246 u siječnju 1999. Za više detalja preporuča se pogledati dokument „TLS protokol“ (CCERT-PUBDOC-2009-03-257).

Ukoliko se objavi nova inačica OpenSSL programa moguće je „nadograditi“ OpenVPN da koristi nove funkcionalnosti (tako je primjerice od inačice 0.9.7 bilo moguće koristiti AES-256 algoritam).

OpenSSL sadrži sljedeće komponente:

- SSL biblioteka – za korištenje SSL/TLS protokola
- Crypto biblioteka – sadrži niz kriptografskih algoritama. Uključuje podršku za:
  - Simetrične algoritme: Blowfish, CAST, DES, AES, IDEA. RC2, RC4 i RC5.
  - Asimetrične algoritme: DSA, RSA, DH.
  - Certifikate: X509.
  - Hash funkcije: HMAC, MD2, MD4, MD5, MDC2, SHA, RIPEMD.

Tablica 3. prikazuje prednosti i nedostatke korištenja tajnog ključa i OpenSSL paketa.

OpenVPN	Korištenje statičkog ključa	Korištenje OpenSSL biblioteke
Algoritam enkripcije	Simetričan	Asimetričan
Primjena	Jednostavna	Složena
Brzina	Veća	Sporija
Potrošnja CPU resursa	Manja	Veća
Autentikacija korisnika	Ne	Da
Problem razmjene ključa	Da	Ne

Tablica 3. Korištenje tajnog ključa i OpenSSL biblioteke

Bez obzira na složenost oko postavljanja početnih postavki, za zaštitu podataka kod OpenVPN-a se preporuča korištenje asimetričnih algoritama.

4.2.1. Primjer povezivanja lokacija uporabom certifikata

Izrada certifikata sastoji se od nekoliko koraka:

1. Provjera inačice OpenSSL biblioteke na poslužitelju i klijentu. Poželjno je da budu iste.

   `c:\Program Files\OpenVPN\bin` →pokrenuti `openssl.exe` → zadati naredbu `version` (na ekranu se potom ispisuje inačica biblioteke)

2. Upisati podatke o vlasniku certifikata. Da bi se to napravilo, potrebno je pokrenuti

   „`init-config.bat`“ datoteku u mapi: „`c:\Program Files\OpenVPN\easy-rsa`“.

   Na Linux-u spomenuta datoteka je u „`/usr/share/doc/packages/openvpn`“ ili „`/usr/share/doc/openvpn-2.0`“.

   Rezultat je datoteka `vars.bat`. Zatim se postavljaju sljedeći parametri (koji određuju vlasnika certifikata):

```
set KEY_SIZE=2048
set KEY_COUNTRY=HR
set KEY_PROVINCE=ZG
set KEY_CITY=ZAGREB
set KEY_ORG=LSS
set KEY_EMAIL=ime.prezime@lss.hr
```

   Pokrene se uređeni `vars.bat`, a nakon njega `clean-all.bat`, kako bi se “očistila” mapa s ključevima.

3. Stvara se CA root certifikat pokretanjem `build-ca.bat`.

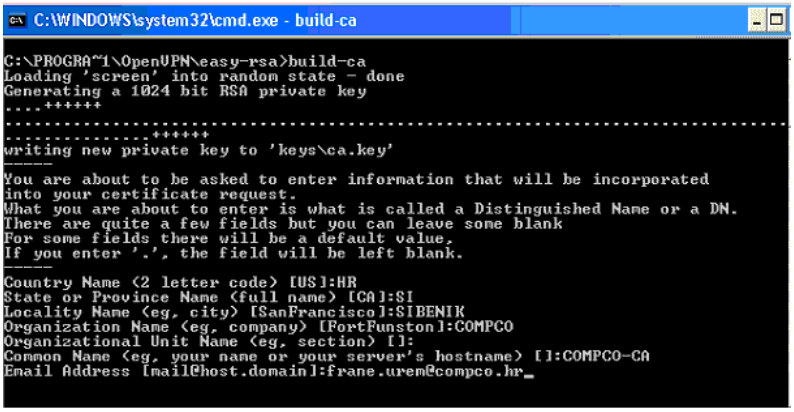
   Linux:

```
./vars
./clean-all
./build-ca
```

   Windows:

```
vars
clean-all
build-ca
```

   Prilikom izrade certifikata potrebno je upisati iste podatke kao i u datoteci `vars.bat`. Za polje „`Common Name`“ može se upisati naziv tvrtke koja izdaje certifikat s dodatkom “-CA”, kao u primjeru na slici 11.



Slika 11. Izrada CA root certifikata

Konačni rezultat su datoteke „ca.cert“ i „ca.key“ u mapi „c:\Program FIles\OpenVPN\easy-rsa\keys“.

„ca.key“ je privatni CA ključ i mora se čuvati na sigurnom računalu (preporuča se ne spajati takav PC na mrežu).

Slika 12. Lista CA root datoteka

4. Zatim se izrađuje certifikat i privatni ključ za VPN poslužitelj pokretanjem naredbe:

   Linux:

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

   Windows:

```
build-key-server.bat server
```

   Upisuju se traženi podaci o izdanom certifikatu kao i kod izrade javnog CA certifikata.

   Rezultat pokretanja su privatni ključ i certifikat za poslužitelj (`server.key`, `server.crt`), potpisani CA ključem, izdani na rok od 10 godina. Rok izdavanja moguće je mijenjati u datoteci „`build-key-server.bat`“.

Slika 13. Stvaranje certifikata i ključa za poslužitelj

5. Izrađuju se certifikati i ključevi za klijente koji će pristupati poslužitelju. Npr. ukoliko postoje 3 klijenta (klijent1, klijent2, klijent3), pokrene se tri puta `build-key.bat`, za svaki klijent posebno:

   Linux:

```
./build-key client1
./build-key client2
./build-key client3
```

   Windows:

```
build-key klijent1
build-key klijent2
build-key klijent3
```

   Rezultat su parovi ključeva i certifikata za svakog klijenta (datoteka „`\keys`“).

6. Izrađuje se Diffie Hellman parametar

   Diffie Hellman protokol dogovora ključeva razvili su kriptografi Diffie i Hellman 1976. godine. Spomenuti protokol omogućuje korisnicima razmjenu tajnog ključa preko nesigurnog medija bez prethodno dogovorenih tajni. Detaljna specifikacija opisana je u dokumentu RFC 2631.

   Linux:

```
./build-dh
```

   Windows:

```
build-dh
```

   Rezultat je veliki, nasumično stvoreni broj, koji se kopira samo na poslužitelj.

Na kraju je potrebno kopirati ključeve, prema tablici 3, na pripadna računala:

Ime datoteke	Koristi ju	Svrha	Tajnost
ca.crt	poslužitelj i svi klijenti	Root CA certifikat	Ne
ca.key	samo sigurno računalo za generiranje ključeva	Root CA ključ	Da
dh{n}.pem	samo poslužitelj	Diffie Hellman parametar	Ne
server.crt	samo poslužitelj	Cerifikat za poslužitelj	Ne
server.key	samo poslužitelj	Ključ za poslužitelj	Da
client1.crt	Klijent 1	Klijent 1 certifikat	Ne
client1.key	Klijent 1	Klijent 1 ključ	Da
client2.crt	Klijent 2	Klijent 2 certifikat	Ne
client2.key	Klijent 2	Klijent 2 ključ	Da
client3.crt	Klijent 3	Klijent3 certifikat	Ne
client3.key	Klijent 3	Klijent 3 ključ	Da

Tablica 3. Raspodjela certifikata u primjeru jedan poslužitelj i tri klijenta

Konfiguracijske datoteke se postavljaju kao i u primjeru sa statičkim ključem, ali se umjesto statičkog ključa zadaju imena certifikata i ključeva za poslužitelj i klijente.

Primjer konfiguracijske datoteke za poslužitelj:

```
dev tap
proto udp
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
persist-tun
ifconfig 192.168.122.1 255.255.255.0
verb 4
mute 10>
```

Primjer konfiguracijske datoteke za klijenta koji pristupa na udaljenu IP adresu 213.191.134.11:

```
remote 213.191.134.11
dev tap
ifconfig 192.168.122.100 255.255.255.0
ca ca.crt
cert klijent1.crt
key klijent1.key
verb 4
mute 10
```

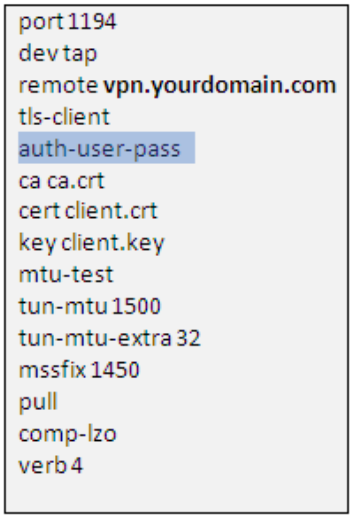
4.3. Alternativne metode autentikacije

Osim već navedenih metoda autentikacije, kao što su korištenje statičkog ključa i certifikata, OpenVPN uključuje programsku podršku za autentikaciju koja se temelji na razmjeni korisničkog imena i pristupne lozinke. Ova je funkcionalnost dostupna tek od inačice 2.0, a zasniva se na ideji da udaljeni korisnik upisuje svoje pristupne podatke čija se valjanost provjerava pomoću zasebnih skripti.

Prvo je na strani klijenta potrebno u konfiguracijskoj datoteci upisati:

```
auth-user-pass
```

Time klijent „traži“ od poslužitelja da upiše svoje podatke jer će mu inače biti onemogućen pristup.

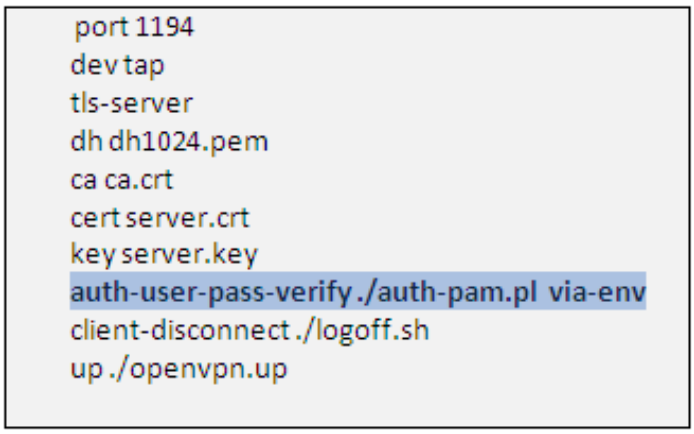


Slika 14. Konfiguracija autentikacije na strani klijenta
Izvor: Wikipedia

Zatim se kod poslužitelja definira upotreba dodatka (eng. *plugin*) za autentikaciju koji obavlja provjeru dozvole pristupa VPN poslužitelju. Najčešće se radi o specijaliziranoj skripti, DLL (eng. *Dynamic Link Library*) ili dijeljenoj (.so) biblioteci. Pritom se, zbog veće brzine rada, preporuča korištenje biblioteka. Poslužitelj će pozvati spomenutu skriptu/biblioteku svaki put kada se neki od klijenata pokuša spojiti i proslijediti podatke koje je unio korisnik.

U konfiguracijskoj datoteci poslužitelja skripta se dodaje pomoću retka:

```
auth-user-pass-verify /putanja do skripte/auth-pam.pl via-file
```



Slika 15. Konfiguracija autentikacije na strani poslužitelja
Izvor: Wikipedia

`Auth-pam.pl` skripta je sastavni dio OpenVPN paketa, a nalazi se u poddirektoriju „`sample-scripts`“.

Auth-LDAP dodatak implementira autentikaciju korisnika putem LDAP protokola korištenjem dijeljene biblioteke „openvpn-auth-ldap.so“.

LDAP (eng. *Lightweight Directory Access Protocol*) je komunikacijski protokol koji se koristi za pristup imeničkim servisima (repozitorij informacija o identitetima korisnika pojedine tvrtke/organizacije). LDAP je definiran u nekoliko dokumenata , a njegov koncept opisan je u dokumentu RFC 3377.

Dodatak je moguće preuzeti sa stranice:

http://code.google.com/p/openvpn-auth-ldap/downloads/list

Kako bi se koristila navedena biblioteka, potrebno je u konfiguracijskoj datoteci poslužitelja postaviti:

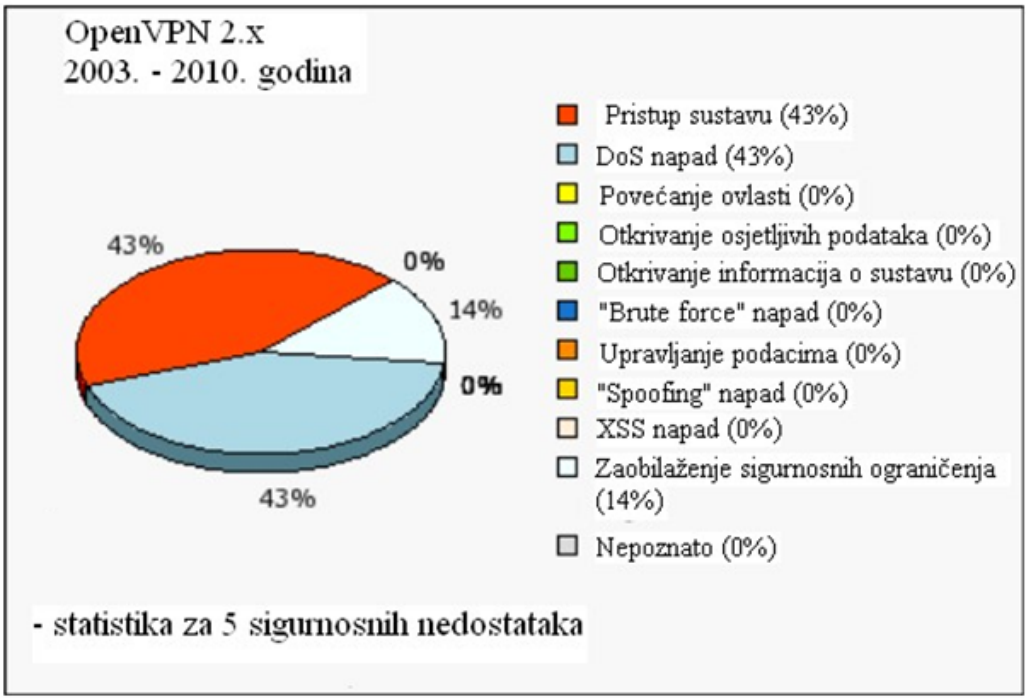
```
plugin /usr/local/lib/openvpn-auth-ldap.so "<config>"
```

Ovaj redak će OpenVPN poslužitelju „reći“ da provjeri korisničko ime i lozinku korištenjem LDAP modula.

4.4. Pregled sigurnosnih propusta

U razdoblju od 2003. do 2010. godine za programski paket OpenVPN je otkriveno 5 sigurnosnih nedostataka te je za sve objavljena odgovarajuća zakrpa koja otklanja otkriveni problem. U svim slučajevima se radilo o mogućnosti da udaljeni napadač iskoristiti nedostatke. Od toga ih je 20% ocijenjeno visoko rizičnima, 40% srednjeg stupnja rizika te preostalih 40% niskog stupnja rizika.

Udjeli pojedinog tipa propusta su prikazani na slici 14.



Slika 16. Pregled ranjivosti za razdoblje 2003.-2010.
Izvor: Secunia

5. Ostale VPN tehnologije

Za potrebe uspostave zaštićenog kanala komunikacije preko medija kao što je Internet moguće je koristiti različita programska rješenja. Danas postoji više VPN skupina protokola od kojih su najpoznatiji IPSec, SSL/TLS, PPTP i L2TP.

IPSec

IPsec (eng. *Internet Protokol Security*) je skup protokola koji uključuje mehanizme za zaštitu prometa na razini trećeg sloja OSI modela kriptiranjem i/ili autentifikacijom IP paketa. IPSec se često smatra najboljim VPN rješenjem za IP okruženja, ali korištenje spomenutog protokola zahtijeva podršku u samoj jezgri operacijskog sustava, pa se ne preporuča neiskusnim korisnicima kako ne bi ugrozili sigurnost cijelog sustava. Također, potrebno ga je instalirati na strani klijenta i poslužitelja, što znatno povećava cijenu ovakvog rješenja ukoliko se radi o većem broju korisnika.

SSL/TLS

SSL (eng. *Secure Sockets Layer*) i TLS (eng. *Transport Layer Security*) su kriptografski protokoli za uspostavu sigurnog komunikacijskog kanala između klijenta i poslužitelja. Prednost ovog tipa VPN rješenja je to što nije potrebno instalirati specijalizirani program na strani klijenta, već se sva komunikacija odvija preko web preglednika. Kao takav, pogodan je za Internet bankarstvo ili kada se zaposlenici neke tvrtke spajaju na pojedine programe zasnovane na webu.

PPTP

PPTP (eng. *Point to Point Tunelling Protocol*) protokol je razvio konzorcij proizvođača - US Robotics, Ascend Communications, 3Com, ECI Telematics i Microsoft. Navedeni protokol je primijenjen na razini mrežnog sloja (OSI razina 3) i temelji se na PPP (engl. Point to Point Protocol) protokolu. PPP sam po sebi omogućuje autentikaciju te podržava kriptiranje i kompresiju podataka, no isto tako podržava samo *end-to-end* komunikaciju preko namjenskog medija (npr. telefonske linije). PPTP ponajviše koriste manje tvrtke i organizacije iz razloga što klijentski program dolazi u paketu s licenciranom inačicom operacijskih sustava Windows.

L2TP

L2TP (eng. *Layer 2 Tunneling Protocol*) je IETF standard koji je nastao kombinacijom funkcionalnosti PPTP i L2F (eng. Layer 2 Forwarding Protocol) protokola, a razvili su ga Microsoft i CISCO. Definiran je RFC-om 2661. L2TP radi na drugom sloju OSI modela, a koristi se kao protokol tuneliranja za IP, X.25, Frame Relay ili ATM mreže. Ovu vrstu VPN-a ponajviše koriste pružatelji usluga kako bi saželi i prenijeli VPN promet kroz tzv. *back-bone* arhitekturu.

Svaki od ovih protokola ima svojih prednosti i nedostataka. Osnovna prednost OpenVPN-a je jednostavnost instalacije i korištenja te činjenica da je besplatan i podržan na svim platformama. Također, za razliku od pojedinih protokola, kompatibilan je s NAT translacijom i omogućuje dinamičko adresiranje korisnika koji se spajaju na poslužitelj.

6. Zaključak

U današnje vrijeme većina tvrtki ili organizacija nastoji osigurati siguran pristup korporativnoj mreži svojim djelatnicima koji se nalaze u izdvojenim uredima, na terenu ili koji rade od kuće. Bitna stavka koja se pritom uzima u obzir je rješenje koje će biti primjereno cijenom i načinom održavanja.

Osnovna prednost OpenVPN tehnologije je njegova jednostavnost prilikom instalacije i održavanja, ali i činjenica da je podržan na gotovo svim danas popularnim platformama. U svom radu koristi napredne algoritme za kriptiranje podataka, a pritom ne opterećuje previše resurse računala na kojima je instaliran. Budući da je besplatan (ali i siguran za korištenje) sve se više korisnika opredjeljuje upravo za njega pa je za očekivati kako će se ovaj proizvod razvijati i dalje nudeći nova sigurnosna rješenja i zaštitu podataka što je od glavne važnosti svim potencijalnim korisnicima.

7. Reference

[1] M.Karlovčec, Enkripcija, http://e.foi.hr/wiki/mediaWiki/index.php/Enkripcija, listopad 2009.

[2] Z.Rajić: Enkripcija putem javnih ključeva i digitalni potpisi, http://fly.srk.fer.hr/~zox/diplomski/DodD_Kriptografija.html, 2008.

[3] Wikipedia:,OpenVPN, http://wiki.contribs.org/OpenVPN, ožujak 2010.

[4] Openvpn-auth-ldap, http://code.google.com/p/openvpn-auth-ldap, siječanj 2010.

[5] D.Korunić: Diffie Hellman razmjena ključeva, http://os2.zemris.fer.hr/algoritmi/asimetricni/2002_korunic/DiffieHellman-Korunic.pdf, 2002.

[6] Secunia: OpenVPN statistika, http://secunia.com/advisories/product/5568/?task=statistics, travanj 2010.

[7] Openmaniak, OpenVPN, http://openmaniak.com/openvpn.php, ožujak 2008.

[8] Packtub, http://www.packtpub.com/article/installing-openvpn-on-windows-and-mac, 2010.

[9] OpenVPN, http://openvpn.net, 2010.

[10] F.Urem: OpenVPN, http://os2.zemris.fer.hr/ns/2007_Urem/pog10.html, 2007.

[11] Wikipedia, OpenVPN, http://en.wikipedia.org/wiki/OpenVPN, travanj 2010.

[12] B.Mitchell: OpenVPN, http://compnetworking.about.com/od/vpnclientsoftware/p/openvpn-free-vpn-software.htm, 2010.