Univerza v Ljubljani

Fakulteta za elektrotehniko

Miran Halilovič

Primerjava rešitev za varen oddaljen dostop do poslovnega omrežja

Diplomsko delo visokošolskega strokovnega študija

Mentor: viš. pred. dr. Anton Kos

Ljubljana, 2016

Zahvala

V prvi vrsti se zahvaljujem mentorju, viš. pred. dr. Antonu Kosu, predvsem za vso strokovno pomoč in odgovore na moja vprašanja pri pisanju diplomske naloge.
Zahvaljujem se tudi podjetjem Amadeus d.o.o., Adria Airways d.d, Unistar d.o.o, Univerzi v Ljubljani, Fakulteti za gradbeništvo in geodezijo ter podjetju Brinox d.o.o, kjer sem skozi leta pridobival izkušnje iz področja VPN sistemov.

Povzetek

Diplomska naloga opisuje različne rešitve, ki se uporabljajo za varen dostop do poslovnega omrežja. Najprej so na splošno opisani najpogosteje uporabljeni sistemi VPN (virtualna privatna mreža), ki se uporabljajo v ta namen. Sledi razlaga osnovnih principov simetričnega ter asimetričnega šifriranja in enosmerne zgostitvene funkcije. Vse troje je osnova za uspešno varno povezavo med oddaljenim uporabnikom ali oddaljenim omrežjem in poslovnim omrežjem.

Naslednje poglavje opisuje praktično testiranje dveh najpogosteje uporabljenih sistemov VPN, in sicer L2TP/IPsec in OpenVPN. Oba sistema sta bila testirana na dveh različnih mrežnih usmerjevalnikih, kjer eden predstavlja nizkocenovno rešitev za mala podjetja in domačo uporabo, drugi pa rešitev srednjega razreda za malo večja podjetja. Zaradi boljšega razumevanja samega testiranja je bilo najprej potrebno podrobneje opisati uporabljene šifrirne algoritme in zgostitvene funkcije. Pomembno je namreč vedeti, kateri algoritmi so priporočljivi za uporabo, kateri niso in katere se odsvetuje. Testiranje je simuliralo dva scenarija. V prvem se oddaljeni uporabnik s prenosnim računalnikom povezuje v poslovno omrežje, v drugem pa je bila simulirana povezava dveh oddaljenih omrežij.

V zadnjem delu so podane praktične izkušnje in spoznanja, ki sem jih pridobil v dolgih letih uporabe in vzdrževanja različnih sistemov VPN. Podal sem tudi svoje izkušnje pri uporabi tako odprtokodnih kot komercialnih zaprtokodnih rešitev. Tako eni kot drugi imajo prednosti in slabosti, univerzalna rešitev pa žal ne obstaja. Z vidika varnosti so odprtokodne rešitve celo v prednosti, še posebej po razkritjih varnostnih spodrsljajev nekaterih priznanih proizvajalcev zaprtokodnih rešitev. Vendar obstajajo tudi razlogi, zaradi katerih se večina podjetij še vedno odloča za zaprtokodne rešitve.

Ključne besede: sistem VPN, oddaljeno omrežje, L2TP/IPsec, OpenVPN, šifrirni algoritmi, zgostitvena funkcija, odprtokodna rešitev, mrežni usmerjevalnik

Abstract

This thesis describes different solutions for secure remote access to a corporate network. At the beginning, there is a general description of the most commonly used VPN systems. It follows with an explanation of basic principles about symmetrical encryption, asymmetrical encryption and one way hashing function. These are also fundamentals for secure remote connection between remote user or remote network and corporate network.

Next chapter talks about a practical experiment of two most widely used VPN systems, L2TP/IPsec and OpenVPN. Both VPN systems were tested on two different network routers. One router was a low cost unit intended for home and small office use, while the other one was a router intended for corporate use. For better understanding of the experiment, we first describe the used encryption algorithms and hashing functions. It is important to know which algorithms are recommended for use and which are not. The experiment was simulating two scenarios. The first scenario was simulating a remote user connecting to corporate network. In the second scenario was simulating a connection between two remote networks.

In the last part of this thesis, we discuss experiences and discoveries gathered over the years of use and support of various VPN systems. I have also described my experience regarding use of open source and commercial proprietary VPN solutions. They both have their strengths and weaknesses, but no universal solution exists. From security point of view, open source solutions have an advantage, especially after several security blunders of some prominent proprietary solutions manufacturers. Despite that, there are still reasons why most of the companies are still choosing proprietary solutions.

Key words: VPN system, remote network, L2TP/IPsec, OpenVPN, encryption agorithm, hashing function, open source solution, network router

Vsebina

1 Uvod **11**

2 Protokoli VPN **13**

2.1 Point-to-Point Tunneling Protocol 13

2.2 Layer 2 Tunnel Protocol 14

2.3 Secure Sockets Layer virtual private network 16

2.4 OpenVPN 17

2.5 Primerjava protokolov VPN 18

3 Načini šifriranja in njihov namen **19**

3.1 Simetrično šifriranje 19

3.2 Asimetrično šifriranje 20

3.3 Zgoščevalna funkcija (Hashing) 22

4 Testiranje različnih sistemov VPN **25**

4.1 L2TP/IPsec povezava med končnim uporabnikom in VPN strežnikom 28

4.2 Povezava OpenVPN med končnim uporabnikom in strežnikom VPN 30

4.3 Povezava oddaljenih omrežij (Site-to-Site VPN) 32

5 Sistemi VPN v praksi **35**

6 Zaključek **41**

Seznam uporabljenih simbolov **43**

Seznam slik **45**

Seznam tabel **45**

Literatura **47**

1 Uvod

V podjetjih vse več uporabnikov pri svojem delu uporablja prenosne računalnike, v veliko primerih je to tudi edini računalnik, ki ga uporabljajo za službene namene. Večinoma je to v kombinaciji s pametnim telefonom, včasih pa celo s tabličnim računalnikom. Tako lahko opravljajo svoje delo tudi doma ali na službeni poti. Za polno operativnost potrebujejo dostop do elektronske pošte in dokumentov. Vse to se lahko nahaja na strežnikih nekje v oblaku, kar uporabnikom zelo poenostavi dostop do podatkov, saj je vse, kar potrebujejo, dostop do interneta. Vendar se večina podjetij ne odloča za takšne rešitve, predvsem zaradi varnosti. Zelo težko je namreč zagotoviti varnost podatkov, če se hranijo na strežnikih, ki jih podjetje ne nadzoruje. Kako varni so naši podatki lahko zgolj ugibamo. Zato ima veliko podjetij interno politiko, ki preprečuje uporabo oblačnih storitev za hranjenje in prenašanje podatkov.

Kot sem že omenil, veliko uporabnikov uporablja službene prenosne računalnike za delo tudi izven podjetja in potrebujejo dostop do podatkov, ki se nahajajo na centralnih strežnikih znotraj poslovnega omrežja. Problem je še bolj pereč, če podjetje veliko posluje s tujino, kjer so uporabniki lahko dalj časa odsotni. Hranjenje podatkov na samem prenosniku ni ne praktično niti pretirano varno. Podatki niso statični in na prenosniku zaposlenega je lahko le posnetek trenutnega stanja, hkrati pa lahko pride do izgube ali odtujitve prenosnega računalnika, ki je poln občutljivih podatkov. Da zaobidemo te težave, je uporabnikom potrebno zagotoviti varen oddaljen dostop do poslovnega omrežja podjetja. Za to potrebujemo VPN (virtualna privatno omrežje), sistem, ki omogoča šifriran podatkovni tunel od računalnika uporabnika do poslovnega omrežja podjetja. Prav tako lahko s sistemom VPN med seboj povežemo matično podjetje in dislocirane izpostave ali hčerinska podjetja, ki prav tako potrebujejo varno podatkovno povezavo do poslovnega omrežja matičnega podjetja.

Izbira sistemov za oddaljen dostop (VPN) je zelo pestra, zato moramo biti zelo pozorni, da izberemo rešitev, ki našim potrebam najbolj ustreza. V obzir moramo vzeti

predvsem tri kriterije; zagotoviti moramo ustrezen nivo varnosti, prav tako mora biti sistem uporabnikom dovolj prijazen, da ne ovira njihovega dela, in jasno cena, kajti podjetja imajo pogosto zelo omejen proračun za takšne projekte.
Na voljo so nam rešitve, ki bazirajo na tehnologijah, kot so PPTP, L2TP/IPsec, SSTP in SSL.
Večina teh tehnologij nam je na voljo v različnih oblikah, lahko je odprtokodna programska oprema, komercialna programska oprema različnih proizvajalcev ali namenska strojna oprema (požarni zidovi) različnih proizvajalcev. Rešitve se močno razlikujejo, zato moramo najti kompromis, ki se kar se da približa prvima dvema kriterijema in hkrati cenovno ne preseže našega proračuna.

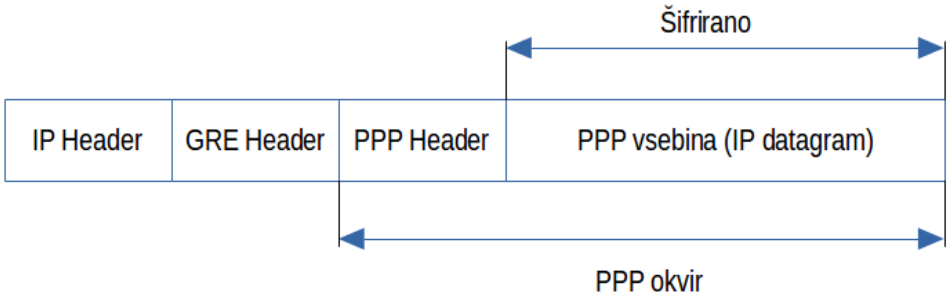
2 Protokoli VPN

Za začetek bomo najprej opisali glavne značilnosti različnih protokolov VPN [1] in njihove prednosti ter slabosti. Pomembno je, da na začetku izberemo protokol, ki je varen, saj imajo nekateri protokoli znane ranljivosti in se njihova uporaba odsvetuje.

2.1 Point-to-Point Tunneling Protocol

PPTP [2] »Point-to-Point Tunneling Protocol« je bil razvit s strani konzorcija, ki ga je ustanovil Microsoft. Njihova naloga je bila razviti protokol VPN za uporabo na omrežjih za klic (dail-up). Prvič je bil predstavljen leta 1999 kot del operacijskega sistema Microsoft Windows 95 OSR2. PPTP je samo protokol VPN in se za varnost zanaša na različne avtentikacijske metode. Največkrat uporabljena metoda je »MS-CHAP v2«. Na voljo je praktično povsod, od mrežnih usmerjevalnikov za domačo rabo, do velikih požarnih zidov za podjetja. Prav tako je na voljo v vseh sodobnih operacijskih sistemih brez nalaganja dodatne programske opreme. Zaradi tega je zelo enostaven za postavitev in upravljanje. Je tudi zelo nezahteven in potrebuje zelo malo procesorske moči.

Čeprav se dandanes uporablja zgolj v kombinaciji s 128-bitnimi šifrirnimi ključi, se je od njegove predstavitve leta 1999 do danes našlo že kar nekaj ranljivosti. Najhujša ranljivost je možnost uporabe ne enkapsulirane avtentikacije MS-CHAP v2. Microsoft je sicer zakrpal ranljivost z uporabo avtentikacije PEAP, vendar je vseeno izdal priporočilo, kjer odsvetuje uporabo protokola PPTP.



Slika 2.1: Struktura paketa PPTP z vsebovanim datagramom IP

Prednosti protokola PPTP

- Klient vgrajen v vse platforme
- Zelo enostavna postavitev
- Hitrost

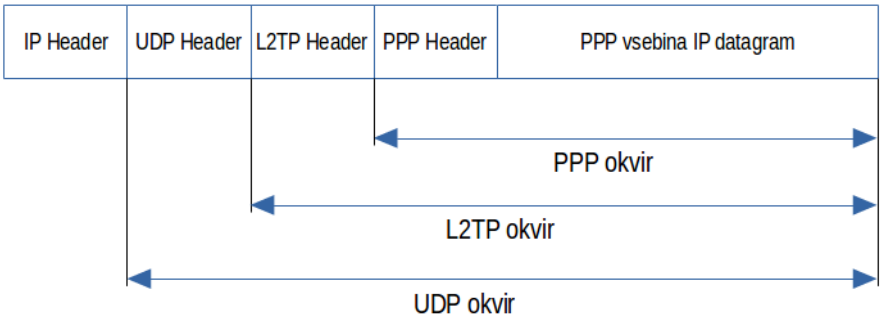
Slabosti protokola PPTP

- Ni varen, obstajajo mnoge ranljivosti, ki še vedno niso zakrpane
- Najbolj razširjena avtentikacija PPTP protokola je še vedno MS-CHAP v2

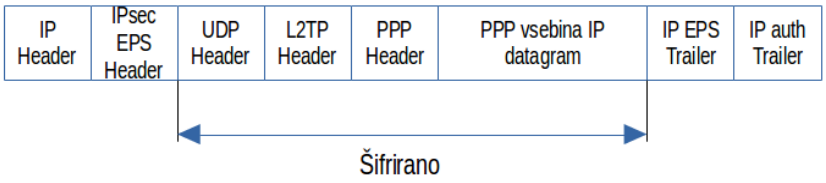
2.2 Layer 2 Tunnel Protocol

L2TP/IPsec [3] »Layer 2 Tunnel Protocol« je protokol VPN, ki prav tako kot PPTP, sam po sebi ne vsebuje šifriranja za promet, ki teče skozenj. Zaradi tega večina implementacij vsebuje tudi šifriranje IPsec, ki omogoča varen pretok podatkov.
Protokol L2TP za vzpostavitev tunela uporablja vrata UDP 500, ki jih požarni zidovi blokirajo, zato moramo spremeniti nastavitev našega požarnega zidu, da preslika vrata UDP 500 na strežnik VPN, ki se nahaja za požarnim zidom.
L2TP/IPsec uporablja dvojno enkapsulacijo prometa, kar bistveno upočasni pretok, vendar obenem omogoča večnitnost in tudi strojno pospeševanje šifriranja IPsec, kar močno vpliva na hitrost pretoka podatkovnega prometa.
Večina mrežnih usmerjevalnikov in požarnih zidov za podjetja podpira L2TP/IPsec. To so tradicionalno dražje naprave, namenjene za srednja in večja podjetja. Vendar se stvari na tem področju premikajo in imamo sedaj na trgu cenovno zelo ugodne usmerjevalnike proizvajalcev, kot so Ubiquiti in Mikrotik, ki podpirajo L2TP/IPsec.
Implementacije L2TP/IPsec se med seboj lahko precej razlikujejo, tako da v mnogih primerih na uporabniški strani ne moremo uporabljati programsko opremo drugega proizvajalca, predvsem imam tukaj v mislih večje proizvajalce, kot so Cisco, Juniper, Sonicwall in podobni.

Varnostno gledano, šifriranje IPsec v primeru, da je pravilno implementirano, nima nobenih večjih znanih ranljivosti. Vendar po Edward Snowdenovih razkritjih vemo, da je NSA (National Security Agency) poskušala in v nekaterih primerih tudi uspela z načrtnim spodkopavanjem varnosti standarda. Lep primer je generator naključnih števil DUAL_EC_DRBG [4], certificiran s strani NIST (National Institute of Standards and Technology), ki ima vgrajena stranska vrata. Nedavno je bilo ugotovljeno, da je Juniper več let v svojih požarnih zidovih uporabljal ravno ta generator naključnih števil s parametri, ki omogočajo zlorabo teh stranskih vrat [5].



Slika 2.2: Struktura paketa L2TP z vsebovanim datagramom IP



Slika 2.3: Prikaz enkapsulacije paketa L2TP z IPsec ESP

Prednosti protokola L2TP/IPsec

- Ob pravilni implementaciji velja za varen protokol
- Postavitev načeloma ni zahtevna
- Na trgu so tudi cenovno dostopne naprave, ki podpirajo ta protokola
- Omogoča večnitnost, IPsec pa je lahko tudi strojno pospešen

Slabosti protokola L2TP/IPsec

- Obstajajo slabe implementacije, ki imajo ranljivosti
- NSA je načrtno spodkopavala varnost protokola
- Potrebna prilagoditev požarnega zidu

2.3 Secure Sockets Layer virtual private network

SSL-VPN [6] »Secure Sockets Layer virtual private network« je zelo fleksibilen protokol, ki je zelo razširjen. Večina proizvajalcev požarnih zidov in namenskih strežnikov VPN ponuja neko implementacijo tega protokola, kot dopolnilo protokolu L2TP/IPsec. Razlog za to je izredna fleksibilnost protokola SSL-VPN, saj lahko teče skozi katerakoli vrata, lahko celo skozi TCP 443.

V to skupino spada tudi Microsoftov SSTP, ki je integriran v Windows Vista SP1 in novejše. Čeprav je to primarno Microsoftov protokol, je sedaj na voljo tudi za Linux in RouterOS (Mikrotik).

Večina implementacij SSL-VPN proizvajalcev požarnih zidov in namenskih strežnikov VPN uporablja knjižnico OpenSSL. To je po eni strani dobro, ker OpenSSL podpira mnogo različnih šifrirnih algoritmov, kot so AES, Blowfish, Twofish, Camellia in še mnoge druge, poleg tega je OpenSSL tudi dobro preizkušena tehnologija. Po drugi strani je vsesplošna uporaba te knjižnice lahko tudi problem, saj kljub temu, da je OpenSSL dobro preizkušena tehnologija, ni brez napak in v zadnjem času se je našlo nekaj zelo kritičnih ranljivosti. Najbolj znana in nevarna ranljivost je bila Heartbleed. Pred kratkim pa je mednarodna skupina raziskovalcev našla še eno kritično ranljivost, ki so jo poimenovali DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). Popravki za te ranljivosti so vedno na voljo še pred javnim razkritjem teh ranljivosti. Vendar mnogi proizvajalci požarnih zidov in strežnikov VPN ne uspejo pravočasno integrirati teh popravkov v svoje implementacije. Verjetno je problem v tem, da ne morejo izdati popravka, ki bi vseboval samo to knjižnico, pač pa v obliki celotnega operacijskega sistema in zaradi tega se zavleče tudi testiranje tega popravka.

Prednosti SSL-VPN

- Zelo fleksibilno
- Zaradi uporabe knjižnice OpenSSL velika izbira različnih šifrirnih algoritmov
- Prehod skozi požarne zidove ni problematičen, ker lahko celo uporablja vrata TCP 443

Slabosti SSL-VPN

- Ne podpira večnitnosti, strojno pospeševanje na voljo le na redkih požarnih strežnikih
- Prav tako kot L2TP v mnogih primerih potrebuje posebno programsko opremo istega proizvajalca tudi na uporabniški strani

2.4 OpenVPN

OpenVPN [7] je odprtokodni VPN sistem, ki prav tako kot SSL-VPN bazira na SSL tehnologiji ter uporablja knjižnico OpenSSL.
OpenVPN je zelo popularen, saj ga najdemo kot del odprtokodnih operacijskih sistemov za nizkocenovne mrežne usmerjevalnike (DD-WRT, OpenWRT, Tomato), kot tudi del odprtokodnih požarnih zidovih (pFsense, Untangle, IPfire in še mnogo drugih), ki so namenjeni za uporabo na x86 platformi. Nekateri proizvajalci profesionalnih in polprofesionalnih usmerjevalnikov prav tako integrirajo OpenVPN v svoje izdelke. Lep primer tega sta proizvajalca Mikrotik in Ubiquiti.

Varnost sistema OpenVPN je zelo podobna kot pri sistemih SSL-VPN, saj prav tako uporablja knjižnico OpenSSL in ga prav tako prizadenejo ranljivosti te knjižnice, kot recimo že omenjena Heartbleed in DRAWN. Vendar odprtokodna skupnost popravke zelo hitro integrira v projekt OpenVPN in so na voljo vsem uporabnikom tega sistema še pred javnim razkritjem ranljivosti. OpenVPN ima zaradi uporabe knjižnice OpenSSL prav tako kot SSL-VPN na voljo mnogo različnih algoritmov šifriranj, ki pa so nam vsi na voljo. Za razliko od mnogih proizvajalcev SSL-VPN sistemov, ki nam omejijo izbiro na samo nekaj šifrirnih algoritmov.

Prednosti OpenVPN

- Velika fleksibilnost
- Velika izbira različnih šifrirnih algoritmov
- Hiter odziv na varnostne ranljivosti, popravki so praviloma na voljo še pred javnim razkritjem
- Prehod skozi požarne zidove ni problematičen, ker lahko celo uporablja vrata TCP 443

Slabosti OpenVPN

- Ne podpira večnitnosti, ostajajo sicer ideje, kako bi to omogočili, vendar je stvar še daleč od izvedbe v praksi
- Potrebuje programsko opremo, naloženo tudi na uporabniški strani

2.5 Primerjava protokolov VPN

Kot vidimo, se različni protokoli VPN med seboj precej razlikujejo. Slonijo na različnih tehnologijah, temu primerno imajo tudi različne prednosti in slabosti. Protokol PPTP je zelo razširjen in praktično ni operacijskega sistem, ki ga ne bi podpiral, vendar zaradi slabe varnosti ni primeren za uporabo. Veliko bolj varen je protokol L2TP/IPsec, ki za razliko od protokola PPTP, nima javno znanih ranljivosti. Ta protokol je tudi zelo razširjen in se uporablja tako v zaprtokodnih, kot odprtokodnih rešitvah. Priljubljen je predvsem zaradi varnosti, enostavne postavitve in podpore strojnemu pospeševanju. Ima pa protokol L2TP/IPsec tudi svoje slabosti, saj zahteva posebne prilagoditve požarnih zidov. Teh težav protokola OpenVPN in SSL-VPN nimata, saj lahko uporabljata celo vrata TCP 443. Oba protokola tudi slonita na isti tehnologiji (OpenSSL) in sta si zaradi tega zelo podobna. Imata tudi enake slabosti, saj oba ne podpirata večnitnosti in zahtevata posebno programsko opremo naloženo na računalnikih uporabnikov. Razlika med njima je v implementaciji, kjer je OpenVPN odprtokodna, SSL-VPN pa zaprtokodna implementacija iste tehnologije. To je tudi razlog, da OpenVPN vedno prvi prejme varnostne popravke, medtem, ko pri SSL-VPN, mora vsak proizvajalec sam, varnostne popravke integrirati v svojo implementacijo tega protokola.
Vsi opisan protokoli VPN, razen PPTP, veljajo za varne protokole, saj nimajo nobenih javno znanih ranljivosti. Vendar so problem implementacije protokolov VPN, ki imajo pogosto ranljivosti, zato je zelo pomembno, kako hitro so te zakrpane.

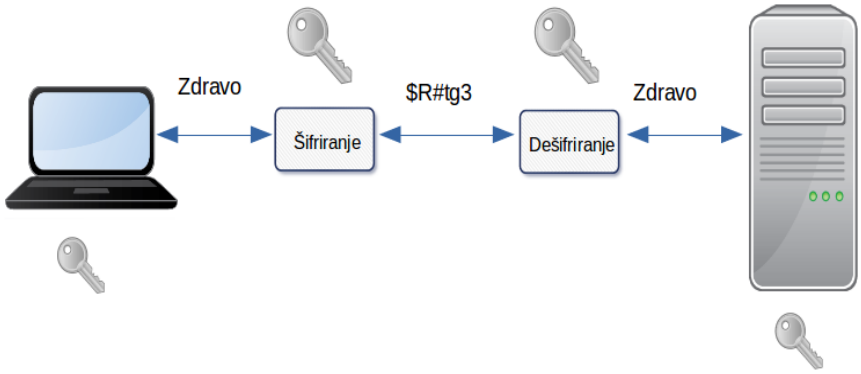
3 Načini šifriranja in njihov namen

Da so protokoli VPN sploh varni, potrebujemo šifriranje. Poznamo dve vrsti šifriranj, to sta simetrično in asimetrično šifriranje. Poleg tega poznamo tudi enosmerno zgoščevalno funkcijo, ki ni šifriranje, pač pa varnostna kriptografija, ki preverja, ali so prispeli podatki res enaki poslanim. V praksi se pri sistemih VPN vedno uporablja vse troje skupaj.

3.1 Simetrično šifriranje

Simetrično šifriranje [8] se imenuje tudi deljen ključ (shared key) ali deljena skrivnost (shared secret). Isti ključ se uporablja tako za šifriranje kot za dešifriranje prometa.

Pogosti algoritmi simetričnega šifriranja so DES (Data Encryption Standard) [9], 3DES (Triple Data Encryption Algorithm) [10], AES (Advanced Encryption Standard) [11] in RC4 (Rivest Cipher 4) [12]. 3DES in AES se najpogosteje uporabljata pri različnih protokolih VPN, RC4 pa se zaradi več ranljivosti opušča. 3DES za enkrat še velja za varen algoritem, vendar obstaja kar nekaj napadov, ki močno znižajo njegovo varnost, zato je bolj priporočljivo uporabljati AES ali po možnosti še bolj varni varianti AES192 in AES256.



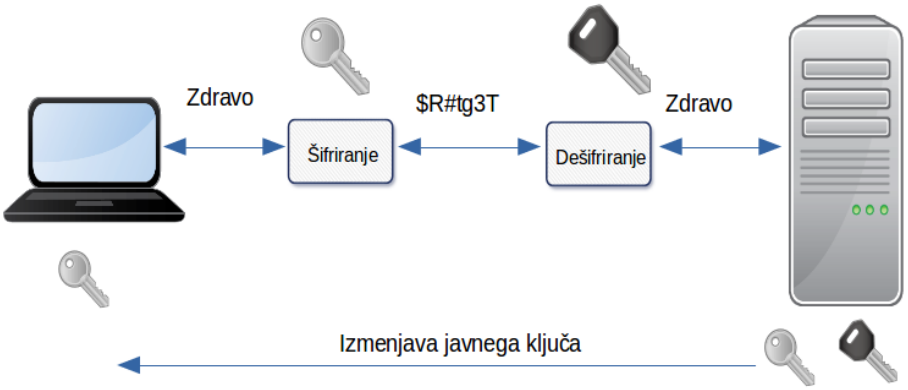
Slika 3.1: Prikaz simetričnega šifriranja z deljenim ključem

Algoritmi za simetrično šifriranje so lahko izredno hitri in jih je zaradi njihove relativno nizke kompleksnosti možno implementirati v strojni obliki. Je pa tudi tukaj problem izmenjave skrivnega ključa, saj morajo vse stranke, ki pri tem šifriranju sodelujejo, na nek način pridobiti ta ključ.

3.2 Asimetrično šifriranje

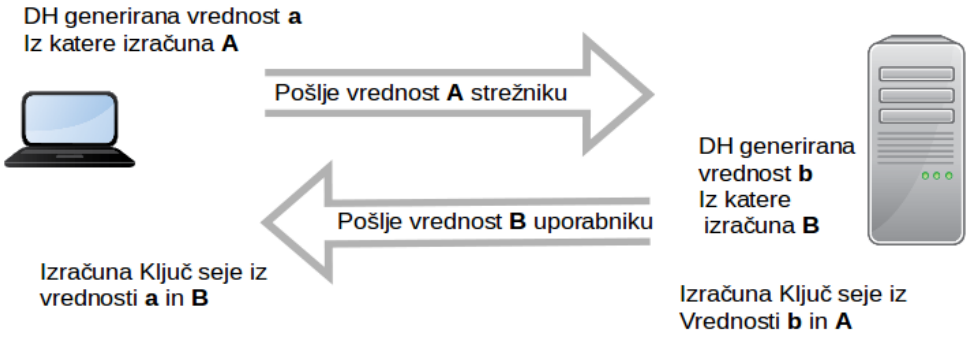
Asimetrično šifriranje [13] imenujemo tudi kriptografija z javnim in zasebnim ključem. Od simetričnega šifriranja se razlikuje predvsem po tem, da uporablja dva ključa. Eden za šifriranje in drugi za dešifriranje. Najbolj pogost algoritem za asimetrično šifriranje je RSA.

Za razliko od simetričnega šifriranja je asimetrično šifriranje računsko zelo zahtevno in posledično zaradi tega tudi veliko počasnejše. To je tudi razlog, zakaj se pri prenosu ne uporablja za varovanje podatkov, pač pa za vzpostavitev varnega kanala po nevarnem mediju, kot je to internet. To se izvede tako, da si obe strani izmenjata javni ključ, ki se lahko uporabi samo za šifriranje podatkov, za dešifriranje pa poskrbi privatni ključ, ki se nikoli ne izmenja.



Slika 3.2: Prikaz asimetričnega šifriranja z izmenjavo javnega ključa

Še bolj varen način vzpostavitve varnega kanala je asimetrično šifriranje PFS (Perfect Forward Secrecy) [14], z DH (Diffie-Hellman) algoritmom [15].
PFS poteka tako, da na uporabnikovi strani DH (Diffie-Hellman) najprej generira naključno vrednost **a**, nato iz te vrednosti izračuna vrednost **A** in jo pošlje strežniku. Medtem na strani strežnika DH generira naključno vrednost **b** in iz nje izračuna vrednost **B** ter jo pošlje uporabniku. DH nato na uporabnikovi strani iz lastne naključno generirane vrednosti **a** in vrednosti **B**, prejeti od strežnika, izračuna ključ seje. Enako na strani strežnika DH, iz lastne naključno generirane vrednosti **b** in vrednosti **A**, prejeti od uporabnika, izračuna ključ seje.
Pomembno je poudariti, da se šifrirni ključ generira za vsako sejo posebej, to pomeni, da je v primeru, če pride do razkritja ključa, ogrožena samo trenutna seja. Vse pretekle in prihodnje seje so še vedno varne. To pa je velika prednost pred asimetričnim šifriranjem z RSA ključem, kjer se za vse seje uporablja isti RSA ključ. V primeru, da pride do razkritja tega RSA ključa, so ogrožene vse pretekle in prihodnje seje, dokler ne zamenjamo RSA ključa. Še ena prednost PFS pred RSA je to, da se ključa nikoli ne izmenjata po nevarnem mediju, kot je to internet, kar še dodatno pripomore k višji varnosti.

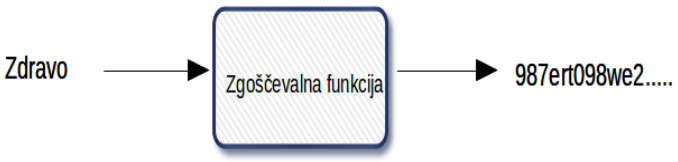


Slika 3.3: Prikaz asimetričnega šifriranja PFS z Diffie-Hellman algoritmom

Robustne šifrirne rešitve, kot je IPsec, implementirajo pozitivne lastnosti tako simetričnega kot asimetričnega šifriranja. Najprej si obe strani izmenjata javni ključ, ali v primeru DH, vrednosti A in B, ki omogoči vzpostavitev počasnega, vendar varnega kanala. Nato se dogovorita za simetrični šifrirni ključ in si ga izmenjata, s tem lahko vzpostavita veliko hitrejši simetrično šifriran kanal, ki pa je primeren za prenos podatkov.

3.3 Zgoščevalna funkcija (Hashing)

Zgoščevalna funkcija »Hashing« [16] je vrsta varnostne kriptografije, ki se razlikuje od šifriranja. Pri šifriranju uporabljamo dva koraka, in sicer najprej sporočilo šifriramo, nato pa ga dešifriramo. Zgoščevalna funkcija sporočilo samo zapakira nepovratno v vrednost fiksne dolžine (hash). Najpogostejši algoritmi za zgoščevanje, ki se uporabljajo pri prenašanju podatkov, so MD5 (message-digest) [17], SHA-1 (Secure Hash Algorithm 1) [18] in SHA-2 (Secure Hash Algorithm 2) [19]. Zaradi zelo šibke varnosti algoritma MD5 se njegova uporaba odsvetuje. SHA-1 je veliko močnejši algoritem, vendar tudi ta kmalu ne bo več dovolj močan, zato se priporoča uporaba algoritma SHA-2, kjer je to le mogoče.



Slika 3.4: Prikaz zgoščevalne funkcije

Zgoščevalna funkcija se uporablja samo za preverjanje, če so podatki, ki so prispeli, enaki poslanim in se med transportom niso spremenili. Ne moremo pa iz zgoščevalne funkcije nazaj pridobiti originalnega sporočila.

4 Testiranje različnih sistemov VPN

Za boljše razumevanje testiranja je najprej potrebno razložiti predvsem, kako varni so izbrani šifrirni algoritmi in zgostitvene funkcije, kajti nekateri algoritmi, ki se ponekod še vedno uporabljajo, varnostno nikakor več ne ustrezajo. Pomembno je, da se tega zavedamo, saj se dogaja, da so pri nekaterih sistemih VPN privzete nastavitve ali pa celo priporočljive nastavitve s strani proizvajalca popolnoma neprimerne. V primeru, da stvari ne poznamo dovolj dobro, lahko postane naš sistem VPN lahek plen za nepovabljene goste. Zaradi tega najprej poglejmo lastnosti šifrirnih algoritmov, ki so bili izbrani za testiranje.

Najosnovnejši šifrirni algoritem, ki se uporablja, je DES (data encryption standard). Ima šifrirni ključ dolžine 56 bit ter bloke dolžine 64 bit, kar pa je pri današnji računski moči računalnikov prešibko. Zaradi tega se namesto DES priporoča derivat 3DES (triple DES), ki uporablja 3 x 56 bitne šifrirne ključe in bloke dolžine 64 bitov. To bi moralo zagotoviti 168 bitov varnosti, vendar je zaradi napada »meet-in-the-middle attack« efektivna varnost 112 bitov. Takšen nivo varnosti pomeni, da je potrebno izvesti operacij za razbitje ključa, kar je za današnje računalnike še vedno nedosegljivo. Torej 3DES še vedno velja za varen algoritem glede velikosti šifrirnega ključa. Vendar je tu problematična velikost blokov, ki so dolžine samo 64 bitov. To pomeni možnih različnih blokov, dokler ne naletimo na podvojen blok. Teoretično lahko z istim ključem varno prenesemo samo 32 GB podatkov. DES algoritem ima še to težavo, da je počasen. Še posebej je neučinkovit in počasen, če je implementiran v programski opremi. 3DES je še trikrat počasnejši, strojno pospešeni algoritmi DES, pa postajajo vse bolj redkost.
Zaradi teh težav s 3DES je bil razvit nov algoritem, ki se imenuje AES (Advanced Encryption Standard), ki popravi vse pomanjkljivosti predhodnika. Uporablja šifrirne ključe dolžine 128, 192 in 256 bitov in bloke velikosti 128 bitov. Dolžina šifrirnega ključa 128 bitov zadostuje za varnost danes in bo zadostovala še kar nekaj časa, daljši ključi za enkrat še niso potrebni. Velika prednost AES je tudi velikost blokov 128

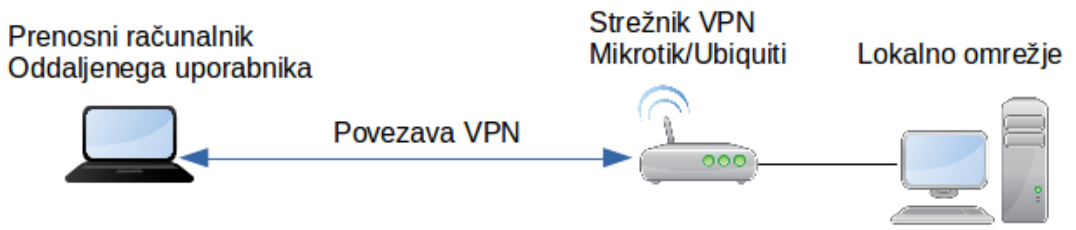
bitov, kar nam teoretično omogoča varen prenos 256 EB (Exabyte) podatkov z istim ključem. AES algoritem velja za nezlomljiv algoritem, saj javno ni znana nobena ranljivost, ki bi zmanjšala njegovo varnost, ter je tudi zelo učinkovit in hiter algoritem. Celo brez strojnega pospeševanja je zelo hiter, mnogo hitrejši od svojega predhodnika 3DES. Strojno pospeševanje AES še močno poveča njegovo učinkovitost in je vse pogostejše, saj večina današnjih procesnih enot za osebne računalnike vsebuje strojno pospeševanje AES. To pa se sedaj seli tudi v procesne enote, ki se uporabljajo tudi že v nekaterih cenejših mrežnih usmerjevalnikih. Tako je priporočljiva uporaba AES algoritma namesto 3DES, če je to le možno, saj ni več nobenega razloga za uporabo 3DES. Razen če imamo strojno opremo, ki omogoča strojno pospeševanje 3DES, ne omogoča pa strojnega pospeševanja AES ali pa celo ne omogoča AES algoritma. V tem primeru bi bila morda celo smiselna menjava te strojne opreme.
Še en pogosto uporabljen šifrirni algoritem je Blowfish [20], ki je tudi privzeti šifrirni algoritem v sistemu OpenVPN. Uporablja ključe dolžine od 32 do 448 bitov, najpogostejša je uporaba ključev dolžine 128 bitov. Je relativno varen in tudi zelo učinkovit in hiter algoritem. Ima pa enako napako kot 3DES, ker prav tako uporablja bloke velikosti samo 64 bitov, kar nas spet omeji na teoretičnih 32 GB varno prenesenih podatkov, z istim šifrirnim ključem. Zaradi tega se namesto algoritma Blowfish priporoča uporaba njegovega naslednika Twofish [21], ki uporablja šifrirne ključe velikosti do 256 bitov in velikosti blokov 128 bitov. Žal pa je algoritem Twofish zelo slabo razširjen in nam je zelo redko na voljo.

Zgoščevalna funkcija služi drugemu namenu kot šifriranje. Kot je bilo že omenjeno, je zgoščevalna funkcija namenjena preverjanju, če so paketi, ki so prispeli na cilj res tisti paketi, ki so bili poslani in niso bili med transportom kakorkoli spremenjeni ali celo zamenjani.
Najosnovnejša zgoščevalna funkcija, ki nam je na voljo, je MD5 (message-digest). Uporaba MD5 se odsvetuje, saj obstajajo napadi, ki funkcijo razbijejo v manj kot minuti z uporabo povprečnega prenosnega računalnika.
Bolj varna zgoščevalna funkcija je SHA-1 (Secure Hash Algorithm 1), ki generira zgostitvene vrednosti velikosti 160 bitov. Obstaja sicer nekaj teoretičnih napadov na SHA-1, vendar v praksi še nobeden ni bil dokazan, da res deluje. Kljub temu pa je vseeno priporočljivo, če je možno, uporabljati zgoščevalno funkcijo SHA-2, in sicer varianta SHA-256, ki generira zgostitveno vrednost velikosti 256 bitov, ter SHA-512, ki generira zgostitveno vrednost velikosti 512 bitov.

Testiranje je bilo opravljeno z dvema najbolj tipičnima sistemoma VPN, in sicer z L2TP/IPsec in OpenVPN, ki tukaj predstavljata tudi ostale sisteme SSL-VPN, saj večinoma slonijo na isti tehnologiji.

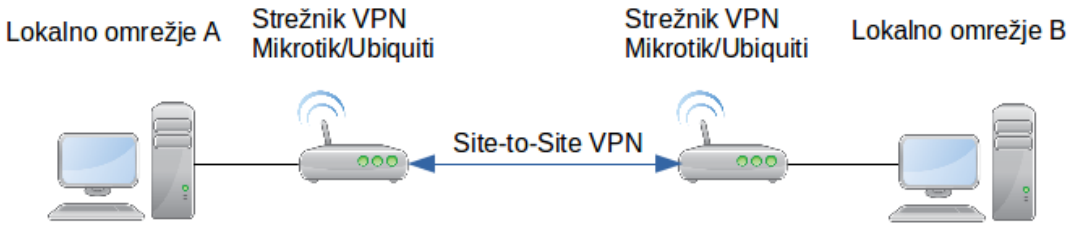
Uporabljena je bila naslednja strojna oprema:
Kot nizkocenovna rešitev je bil uporabljen mrežni usmerjevalnik Mikrotik RB751G-2HnD, ki bazira na strojni platformi, bolj tipični za usmerjevalnike za domačo uporabo (Atheros AR7242). Centralna procesna enota je enojedrna s hitrostjo 400 MHz. Vsebuje tudi samo 64 MB delovnega spomina, vendar naložena programska oprema (RouterOS) omogoča veliko funkcij in ta mrežni usmerjevalnik je primeren tudi za profesionalno rabo.
Kot rešitev za bolj zahtevne uporabnike je bil uporabljen mrežni usmerjevalnik Ubiquiti EdgeRouter Lite-3. Ta usmerjevalnik bazira na strojni platformi, pogosto uporabljeni tudi v veliko dražjih napravah (Cavium CN5020). Centralna procesna enota je dvojedrna s hitrostjo 500 MHz. Vsebuje tudi kar zajetnih 512 MB delovnega spomina. Poleg mnogih naprednih funkcij omogoča tudi strojno pospeševanje IPsec šifriranja, kar je zelo pomembno za to testiranje.

Simulirali smo dva scenarija. V prvem scenariju smo simulirali povezavo oddaljenega uporabnika, ki se s prenosnim računalnikom povezuje v poslovno omrežje. Na sliki 4.1 je prikazana postavitev računalnikov in komunikacijske opreme za prvi scenarij.



Slika 4.1: Prvi scenarij, povezava oddaljenega uporabnika v poslovno omrežje

V drugem scenariju smo simulirali povezavo dveh oddaljenih omrežij (Site-to-Site VPN). Na sliki 4.2 je prikazana postavitev računalnikov in komunikacijske opreme za drugi scenarij.



Slika 4.2: Drugi scenarij, povezava oddaljenih omrežij (Site-to-Site VPN)

Testiranja so bila opravljena s programom iPerf3. Za vsak test so bile opravljene 4 meritve po 10 sekund in 4 meritve po 30 sekund. Spodaj predstavljeni rezultati so povprečja vseh teh meritev.
Program iPerf3 ni tekel na usmerjevalnikih (Ubiquiti ima iPerf3 že integriran), pač pa na osebnih računalnikih pred in za usmerjevalnikom. Tako sta usmerjevalnika lahko vso procesorsko moč uporabila za poganjanje VPN strežnika.

4.1 L2TP/IPsec povezava med končnim uporabnikom in VPN strežnikom

Rezultati v tabelah in na grafih prikazujejo različne kombinacije šifriranj in zgostitvenih funkcij.

Najprej si poglejmo rezultate testiranja protokola L2TP/IPsec z mrežnima usmerjevalnikoma Mikrotik RB751G-2HnD in Ubiquiti EdgeRouter Lite-3.

Šifriranje	**Hitrost (Mb/s) Mikrotik**	**Hitrost (Mb/s) Ubiquiti**
3DES/MD5	8,15	175
3DES/SHA1	7,7	178,5
AES128/MD5	25	192
AES128/SHA1	27,5	200
AES256/SHA1	19	171

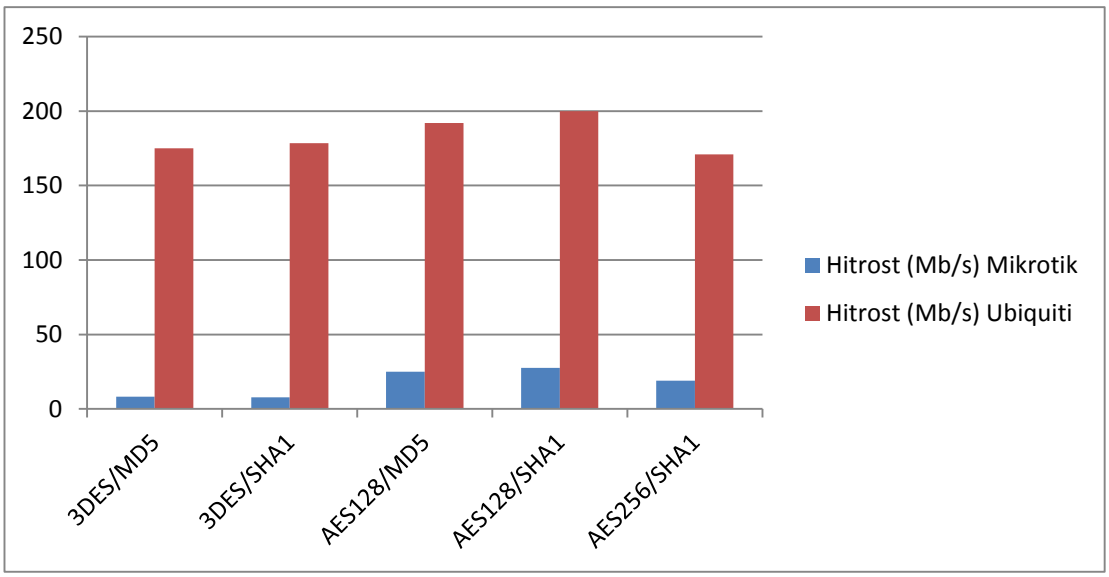
Tabela 4.1: Rezultati L2TP/IPsec za Mikrotik in Ubiquiti

Iz rezultatov v tabeli 4.1 lahko vidimo, da je Mikrotik zabeležil mnogo slabše rezultate pri šifriranju z algoritmom 3DES kot AES, vsaj delno lahko to pripišemo dejstvu, da je protokol AES mnogo bolj optimiziran kakor 3DES. Prav tako vidimo, da je zgostitvena funkcija SHA-1 v kombinaciji s šifriranjem AES128 malo hitrejša kot MD5, čeprav je SHA-1 računsko mnogo bolj zahtevna. To pomeni, da razvijalci programske opreme za Mikrotik veliko več pozornosti namenjajo optimiziranju

delovanja algoritma AES in zgostitvene funkcije SHA-1 kot manj varnim algoritmom, kot je 3DES in zgostitveni funkciji MD5, katere uporaba se odsvetuje.

V isti tabeli lahko vidimo rezultate testiranja protokola L2TP/IPsec z mrežnim usmerjevalnikom Ubiquiti EdgeRouter Lite-3. Tukaj je uporabljena strojna pospešitev IPsec protokola, to pomeni, da večino IPsec operacij prevzame specializirana logična enota, ki to delo opravi mnogo hitreje in s tem tudi razbremeni centralno procesno enoto.
Najprej jasno opazimo, da so rezultati neprimerljivo boljši kot pri Mikrotiku, tukaj odločilno vlogo odigra strojno pospeševanje protokola IPsec. Tako kot pri rezultatih za Mikrotik, ima Ubiquiti podoben trend, kjer računsko bolj zahtevni algoritem 3DES zaostaja za mnogo bolj optimiziranim ter varnim algoritmom AES, prav tako je podobna situacija z zgostitvenima funkcijama MD5 in SHA-1. Vsekakor pa razlika ni tako dramatična, kot je pri Mikrotiku.

Za lažjo primerjavo med obema usmerjevalnikoma so na spodnji sliki grafično prikazani rezultati vseh L2TP/IPsec testiranj.



Slika 4.3: Primerjava rezultatov L2TP/IPsec

Kot lahko vidimo iz grafa na slike 4.3, je razlika zelo velika. Največ k temu pripomore že prej omenjeno strojno pospeševanje protokola IPsec v mrežnem usmerjevalniku Ubiquiti. Procesna enota v tem usmerjevalniku nikoli ni presegla 50 % zasedenosti, medtem ko je bila procesna enota v mrežnem usmerjevalniku Mikrotik vedno polno zasedena.

4.2 Povezava OpenVPN med končnim uporabnikom in strežnikom VPN

Pri sistemu OpenVPN sta mrežna usmerjevalnika Mikrotik in Ubiquiti v bolj enakovrednem položaju, saj Ubiquiti podpira samo strojno pospeševanje IPsec, pri sistemih SSL-VPN mora vse delo opraviti centralna procesna enota.
OpenVPN nam na obeh usmerjevalnikih omogoča več različnih kombinacij šifriranj in zgostitvenih funkcij. To je še posebej opazno na usmerjevalniku Ubiquiti, kjer je izbira res pestra.

Mikrotik ima pri sistemu OpenVPN na izbiro poleg šifriranja AES tudi šifriranje BlowFish (BF), ki je sicer šibkejše od AES, vendar je še vedno veliko boljša izbira kot 3DES. Mikrotik pa vseeno razočara pri izbiri zgostitvenih funkcij, saj sta nam na izbiro samo MD5 in SHA-1.

Ubiquiti ima enako izbiro šifriranj kot Mikrotik, vendar ima drugačno izbiro zgostitvenih funkcij. Tu so se odpovedali zgostitveni funkciji MD5, kar je pozitivno, še bolj razveseljivo je dejstvo, da so nam dali na izbiro poleg zgostitvene funkcije SHA-1 tudi SHA-2, in sicer v obliki SHA256 in SHA512. To nam omogoči izbiro res varne kombinacije šifriranja in zgostitvne funkcije, recimo AES256/SHA256.

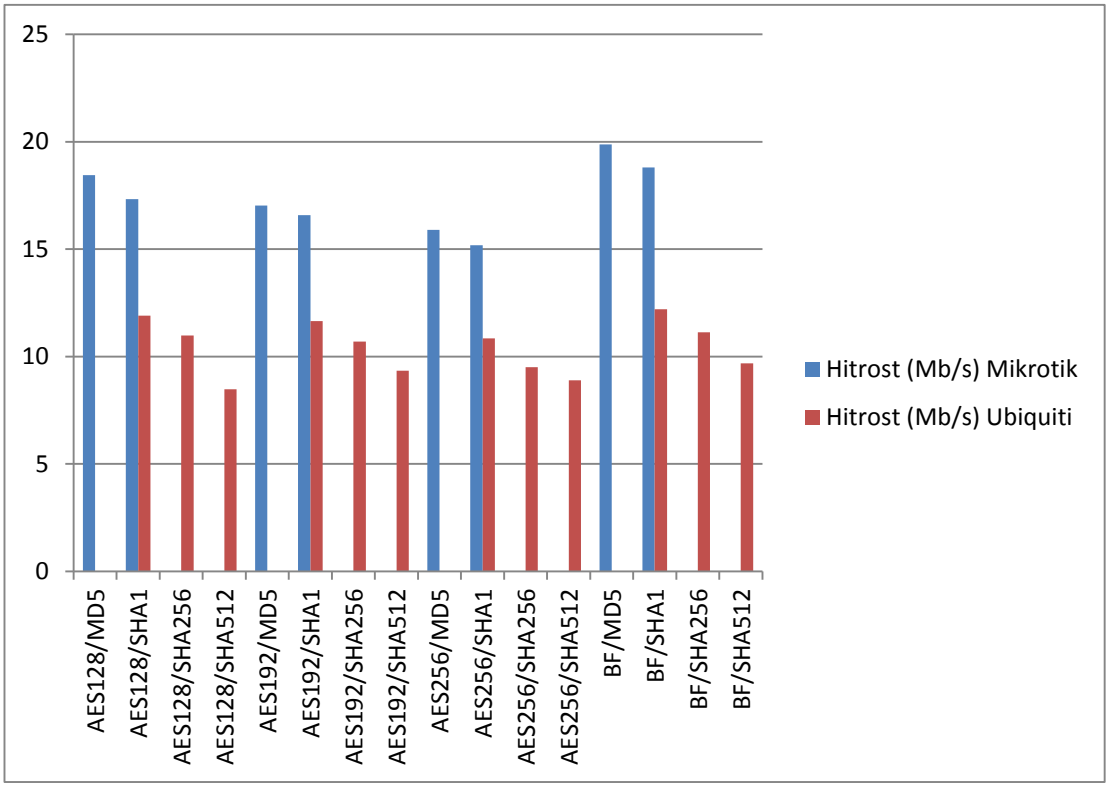
Šifriranje	**Hitrost (Mb/s) Mikrotik**	**Hitrost (Mb/s) Ubiquiti**
AES128/MD5	18,450	
AES128/SHA1	17,325	11,9000
AES128/SHA256		10,9750
AES128/SHA512		8,4680
AES192/MD5	17,025	
AES192/SHA1	16,575	11,6500
AES192/SHA256		10,6875
AES192/SHA512		9,3325
AES256/MD5	15,900	
AES256/SHA1	15,175	10,8500
AES256/SHA256		9,5075
AES256/SHA512		8,8920
BF/MD5	19,875	
BF/SHA1	18,800	12,2000
BF/SHA256		11,1250
BF/SHA512		9,6775

Tabela 4.2: Rezultati OpenVPN za Mikrotik in Ubiquiti

Rezultat OpenVPN za mrežni usmerjevalnik Mikrotik RB751G-2HnD, prikazan v tabeli 4.2, je precej pričakovan, saj z izbiranjem vse bolj zahtevnega šifriranja AES in zgostitvene funkcije, hitrost pada skoraj linearno. Izjema je tukaj šifriranje BlowFish, ki je sicer privzeto šifriranje sistema OpenVPN in je verjetno zato tudi najboljše optimizirano.

Rezultati OpenVPN za mrežni usmerjevalnik Ubiquiti EdgeRouter Lite-3, prav tako prikazani v tabeli 4.2, se držijo trenda, bolj kompleksno je šifriranje in bolj kompleksna je zgostitvena funkcija, nižja je hitrost. Vendar so sami rezultati na splošno nižji, kot bi to lahko pričakovali od tako močne strojne platforme.

Primerjava rezultatov testiranj OpenVPN obeh mrežnih usmerjevalnikov v grafični obliki. Izbrane so bile vse kombinacije šifriranj in zgostitvenih funkcij, ki jih podpirata oba mrežna usmerjevalnika. Nekatera šifriranja in zgostitvene funkcije ne podpirata oba mrežna usmerjevalnika, zaradi tega na sliki ti rezultati manjkajo.



Slika 4.4: Primerjava rezultatov OpenVPN

Iz grafa na sliki 4.4 vidimo, da je kljub veliki premoči centralne procesne enote na strani Ubiquiti le-ta precej zaostajal za Mikrotikom. Procesni enoti v obeh usmerjevalnikih sta bili med testiranjem polno obremenjeni, tako lahko zaključimo, da je programska oprema na Mikrotiku veliko bolje optimizirana za sistem OpenVPN in deluje veliko bolj učinkovito. Žal pa Mikrotik ne podpira bolj varne zgostitvene funkcije SHA-2. Morda bo to v prihodnosti dodano z nadgradnjo programske opreme.

4.3 Povezava oddaljenih omrežij (Site-to-Site VPN)

Strežniki VPN se lahko povežejo tudi med seboj (Site-to-Site VPN) [22]. Na tak način lahko po varnem tunelu med seboj povežemo več oddaljenih omrežij. Za to potrebujemo mrežno opremo, ki podpira takšne povezave VPN.
Oba v prejšnjih testih uporabljena mrežna usmerjevalnika Mikrotik in Ubiquiti podpirata takšne povezave.
Za testiraje je bil izbran sitem VPN L2TP/IPsec, ki se v praksi skoraj izključno uporablja za takšne povezave.

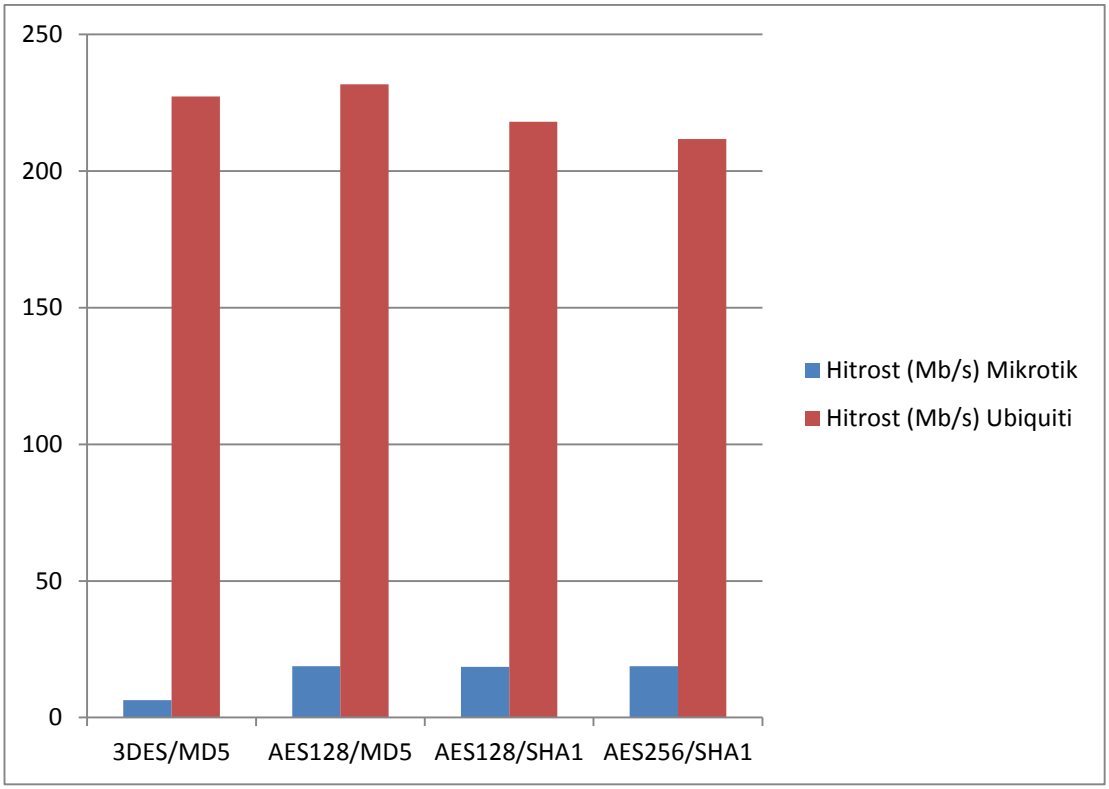
Šifriranje	**Hitrost (Mb/s) Mikrotik**	**Hitrost (Mb/s) Ubiquiti**
3DES/MD5	6,347	227,250
AES128/MD5	18,733	231,750
AES128/SHA1	18,525	218,000
AES256/SHA1	18,750	211,750

Tabela 4.3: Rezultati VPN L2TP/IPsec Site-to-Site za Mikrotik in Ubiquiti

Rezultati L2TP/IPsec Site-to-Site za Mikrotik, prikazani v tabeli 4.3, so podobni, kot so bili pri testu s končnim uporabnikom, kjer kombinacija šifriranja in zgostitvene funkcije 3DES/MD5 močno zaostaja. Je pa zanimivo, da so kombinacije AES128/MD5, AES128/SHA1 in AES256/SHA1 praktično izenačene.

Ubiquiti se pri tem testu še bolje odreže kot pri testu s končnim uporabnikom. Spet močno prehiti Mikrotik, strojno pospeševanje razbremeni centralno procesno enoto in močno pospeši promet IPsec.

Primerjava rezultatov testiranj Site-to-Site VPN L2TP/IPsec za Mikrotik in Ubiquiti v grafični obliki za lažjo predstavo.



Slika 4.5: Primerjava rezultatov VPN L2TP/IPsec Site-to-site

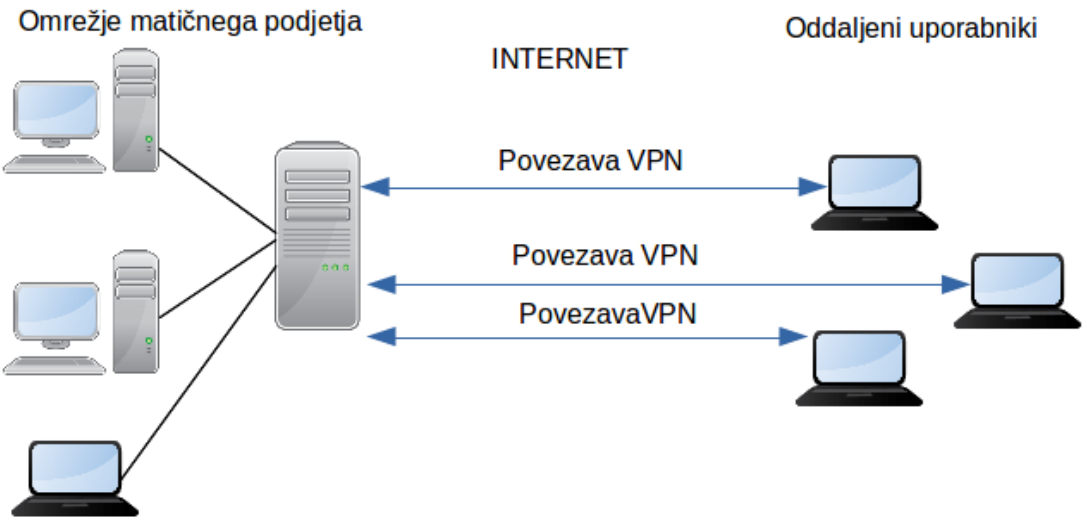
Iz grafa na sliki 4.5 lahko lepo razberemo, da je Ubiquiti platforma res neverjetno učinkovita pri prometu IPsec. Vendar spet manjka bolj varna zgostitvena funkcija SHA-2. Enaka pomanjkljivost, kot jo ima Mikrotik tudi pri OpenVPN. Spet lahko le upamo, da bodo z nadaljnjimi popravki odpravili tudi to pomanjkljivost.

5 Sistemi VPN v praksi

Pravi preizkus sistema VPN je šele v praksi, ko je izpostavljen dolgotrajnim obremenitvam, nepredvidenim prekinitvam internetnih povezav in raznim drugim nepredvidenim situacijam.
Nekateri sistemi VPN so bolj občutljivi na prekinitve internetne povezave kot drugi. V nekaterih primerih je vzrok za prenehanje delovanja nestabilnost samega klienta VPN. Pri drugih pa je vzrok vgrajen varnostni mehanizem, ki prekine povezavo, če zazna večje število izgubljenih paketov. Tipična posledica napada »man in the middle« je namreč velika izguba paketov.
Zanimiv pojav je tudi blokiranje vrat UDP 500 s strani internetnih ponudnikov. Vrata UDP 500 uporablja VPN sistem L2TP/IPsec za vzpostavitev šifriranega tunela. Ta pojav je zaslediti večinoma pri uporabnikih, ki se povezujejo iz tujine, predvsem iz Ruske federacije.
Blokiranje vrat UDP 500 je lahko namerno ali nenamerno. Zgodi se, da neka naprava na prenosni poti privzeto blokira ta vrata in se ponudnik interneta tega sploh ne zaveda. Včasih pa ponudnik interneta protokol IPsec prav aktivno blokira. V takem primeru je edina rešitev uporaba drugačnega VPN protokola, predvsem SSL-VPN ali OpenVPN, katere je precej težje blokirati, saj je takšen promet zelo težko ločiti od običajnega HTTPS prometa. Zaradi varnostnih pomanjkljivosti samega protokola pa uporaba VPN protokola PPTP ni priporočljiva.

Pri večjem številu uporabnikov je pomembno, koliko vzporednih povezav je sistem VPN zmožen vzdrževati in kakšno pasovno širino lahko zagotovi tem povezavam. V takih primerih nam zelo pomaga strojna pospešitev šifriranja, ki pa je na različnih platformah različno podprta. Na mrežnih usmerjevalnikih in požarnih zidovih nižjega in srednjega razreda je to po navadi omejeno zgolj na IPsec. Medtem lahko odprtokodni požarni zid pfSense, ki bazira na operacijskem sistemu FreeBSD, izkoristi katerokoli strojno pospeševanje, ki je prisotno v procesni enoti in je podprto v operacijskem sistemu.

Tako lahko na požarnem zidu pfSense precej pospešimo promet sistema OpenVPN in ne samo IPsec, kar je še posebej dobrodošlo, če imamo težave z blokiranimi vrati UDP 500. Žal pa ima OpenVPN tudi svoje omejitve, saj ne pozna večnitnosti in tako ne more izkoristiti več jeder v sodobnih procesnih enotah. Obstaja sicer način, da zaobidemo to omejitev, in sicer tako, da poganjamo vzporedno več instanc OpenVPN-ja in vsaka instanca potem posluša na drugih vratih.

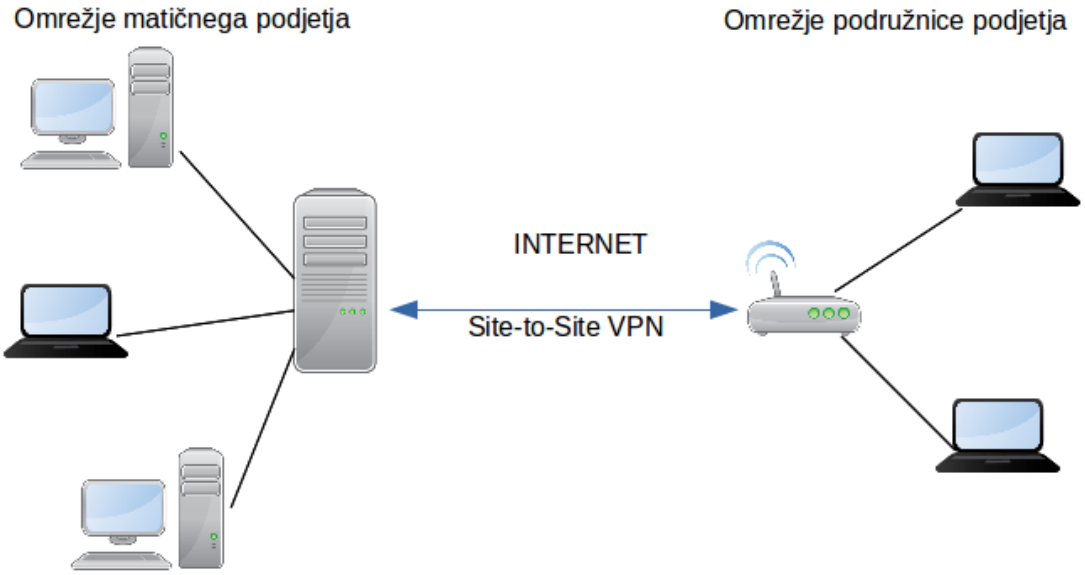


Slika 5.1: Prikaz VPN povezave med oddaljenimi uporabniki in matičnim podjetjem

V primerih, da imamo opravka z izpostavami ali hčerinskimi družbami na drugih lokacijah po državi ali tujini, za katere potrebujejo varno povezavo do matičnega podjetja, moramo vzpostaviti povezavo VPN med lokacijami (Site-to-Site VPN). Veliko bolj priročno je, da med seboj povežemo omrežja matičnega podjetja in oddaljene lokacije, namesto da vsak uporabnik posebej vzpostavlja povezavo. To povezavo realiziramo s strežnikom VPN na obeh straneh varne povezave. Po navadi v obliki požarnega zidu ali mrežnega usmerjevalnika. Protokol VPN, ki ga komercialni proizvajalci po navadi uporabljajo za varne povezave med lokacijami, je L2TP/IPsec. Pri odprtokodnih rešitvah pa načeloma lahko izbiramo med L2TP/IPsec in OpenVPN. Seveda je pogosta tudi podpora za protokol PPTP, vendar se zaradi varnostnih pomanjkljivosti uporaba tega protokola močno odsvetuje.

Za uspešno povezavo morata napravi na obeh straneh podpirati isti protokol VPN in isto šifriranje. Uporabimo lahko naprave različnih proizvajalcev, vendar je največja verjetnost za uspešno povezavo uporaba naprav istega proizvajalca na obeh straneh povezave. Tudi naprave različnih proizvajalcev, ki podpirajo isti protokol VPN in isto

šifriranje, teoretično ne bi smeli imeti težav z vzpostavitvijo varne povezave. Vendar to v praksi vedno ne drži, saj implementacije protokolov in šifriranj niso identične med različnimi proizvajalci. Tako se lahko zgodi, da na papirju dve napravi različnih proizvajalcev podpirata isti protokol VPN in isto šifriranje, vendar vzpostavitev varne povezave spodleti ali pa je povezava nestabilna. V takem primeru je lahko rešitev uporaba starejšega in manj varnega šifriranja. To načeloma zagotovi večjo verjetnost uspešne vzpostavitve povezave, vendar hkrati tudi zniža varnost te povezave. V primeru, da pride do tega, da je edino šifriranje, ki omogoča stabilno povezavo, varnostno neustrezno, nimamo druge izbire, kot da eno od teh naprav enostavno zamenjamo.



Slika 5.2: Prikaz VPN povezave med oddaljenima omrežjema (Site-to-Site VPN)

Poleg varnosti protokolov VPN in šifriranj je potrebno podrobno preučiti tudi, kako so ti protokoli ter šifriranja implementirana. Pomembno je tudi, kako hitro proizvajalci izdajo popravke za ranljivosti, ki so odkrite v njihovih produktih, in kako kvalitetni so ti popravki.

Na žalost večina komercialnih proizvajalcev zamuja s popravki, saj jih po navadi ne uspejo izdati pred javnim razkritjem ranljivosti. S tem pa svoje stranke izpostavijo napadom, ki izkoriščajo to ranljivost. V tem primeru imajo odprtokodne rešitve prednost, saj so popravki za ranljivosti zelo hitro na voljo in to večinoma še pred javnim razkritjem ranljivosti. Tudi kvaliteta teh popravkov ni vedno na strani

komercialnih proizvajalcev, saj so primeri, ko popravek sicer odpravi ranljivost, vendar hkrati povzroči druge težave.

V zadnjem času smo bili priča varnostnim spodrsljajem nekaterih priznanih proizvajalcev zaprtokodnih požarnih zidov. Najbolj odmeven je bil primer priznanega proizvajalca Juniper, kjer so varnostni raziskovalci ugotovili, da njihov operacijski sistem ScreenOS vsebuje generator naključnih števil (Dual_EC) s parametri, ki omogočajo napadalcu dešifriranje celotnega prometa požarnega zidu. Nenavadno je predvsem to, da tukaj ni bila samo ena napaka ali napačna odločitev, ki bi to povzročila, pač pa cela serija napak ali napačnih odločitev. Kar je sicer lahko zelo neverjetno naključje, vendar obstaja utemeljen sum, da so bile to namerne poteze za vgradnjo stranskih vrat v naprave, ki so v široki uporabi. Zanimivo je tudi, da je bil generator naključnih števil Dual_EC dodan že leta 2009 ali celo 2008, kar je po svoje zaskrbljujoče. Še bolj pa je zaskrbljujoče dejstvo, da sta leta 2007 Dan Shumow in Neils Ferguson na konferenci CRYPTO prvič pokazala možnost, da je v protokol Dual_EC NSA (Nationa Security Agency) vgradila stranska vrata [23]. Torej že vsaj leto preden je Juniper vgradil sporni algoritem za generiranje naključnih števil (Dual_EC) v ScreenOS. Bilo je razkrito, da ima algoritem varnostne težave, pa so ga kljub temu uporabili. Žal to ni edini Juniperjev spodrsljaj, saj je bilo razkrito, da je imel operacijski sistem ScreenOS še ena stranska vrata. Imeli so dodatno administratorsko geslo, zamaskirano kot programska koda, ki je omogočalo popolni dostop do požarnega zidu preko Telnet in protokola SSH (Secure Shell) [24]. Če za Dual_EC ne moremo z zagotovostjo trditi, da je bila napaka namerna, za drug primer ni dvomov o tem. Juniper ni edini proizvajalec, ki je imel v svojih produktih stranska vrata. Podobna neprijetnost je doletela tudi priznanega proizvajalca požarnih zidov Fortinet, ki je imel v svojem operacijskem sistemu FortiOS več let vgrajen nedokumentiran uporabniški račun z najvišjimi pravicami in statičnim geslom [25].
Noben od proizvajalcev ni znal razložiti, kako so se te napake in stranska vrata znašla v njunih operacijskih sistemih, še manj pa, kdo jih je vgradil. V takem primeru se lahko vprašamo, kako učinkovita je njihova interna kontrola izvorne kode za naprave, ki so namenjene varovanju omrežij. Hkrati pa to tudi meče negativno luč na ostale proizvajalce zaprtokodnih požarnih zidov, kajti če se to lahko zgodi Juniperju in Fortinetu, se lahko zgodi tudi ostalim.

Vse zgoraj omenjeno vpliva na odločitev podjetja pri izbiri VPN rešitve. Vendar je še vedno odločilno to, koliko je podjetje pripravljeno vložiti v rešitev. Sistem VPN je po navadi del požarnega zidu ali mrežnega usmerjevalnika in takšne komercialne rešitve

niso nikoli poceni. To še podkrepi dejstvo, da moramo poleg samega nakupa naprave dokupiti še dodatne licence za sočasne povezave VPN klientov, saj privzeto po navadi dobimo samo eno ali dve licenci. Poleg tega pa moramo tudi podpisati drago vzdrževalno pogodbo s proizvajalcem ali njihovim zastopnikom. S podpisom te pogodbe dobimo dostop do popravkov in novih verzij njihove programske opreme ter tehnične podpore, katere stopnja je odvisna od dogovora in jasno cene.

Na drugi stani pa za odprtokodne rešitve načeloma ne potrebujemo dragih licenc in vzdrževalnih pogodb. Vendar pa potrebujemo nekoga v podjetju ali zunanjega izvajalca, ki je usposobljen za vzdrževanje teh rešitev, kar pa je pri nas precej redek pojav. Podjetja so tudi zelo redko pripravljena zaposliti ali najeti človeka, ki bi vpeljal odprtokodni VPN sistem. Tako se skoraj vedno odločijo za neko komercialno zaprtokodno rešitev.

6 Zaključek

V diplomskem delu je predstavljena primerjava različnih sistemov VPN za varen oddaljen dostop uporabnikov in oddaljenih omrežij do omrežja matičnega podjetja.
Na začetku je bilo potrebno razjasniti osnovne pojme, kaj različni sistemi VPN predstavljajo, katere so njihove prednosti in slabosti. Potrebno je bilo tudi razjasniti, kaj pomeni simetrično šifriranje, asimetrično šifriranje ter zgoščevalna funkcija in čemu služijo pri vzpostavitvi varnega tunela do oddaljenega omrežja in varnega prenosa podatkov med obema koncema tunela.
Sledil je opis različnih algoritmov šifriranja in algoritmov zgoščevalnih funkcij. Pomembno je razumeti, kaj nam določeni algoritmi prinesejo glede varnosti, učinkovitosti in kako podprti so v različnih sistemih. Nekateri algoritmi, čeprav so nam na voljo v različnih sistemih, zaradi zelo šibke varnosti niso priporočljivi za uporabo. Prav tako moramo poznati omejitve ostalih algoritmov, ki veljajo za varne, vendar ne preveč učinkovite. Tako lahko iz teh podatkov teoretično določimo, kakšna bi bila optimalna kombinacija šifriranja in zgoščevalne funkcije. V največ primerih bi bila optimalna kombinacija šifriranje AES128 in zgoščevalna funkcija SHA-2. Najti moramo namreč neko ravnovesje, kjer je naša VPN povezava še vedno varna, naprave, ki se uporabljajo za to povezavo, pa niso preveč obremenjene, da bi zaradi tega trpela sama hitrost prometa, ki potuje skozi VPN povezavo.
Oboroženi z vsem tem znanjem smo se lotili testiranja dveh različnih mrežnih usmerjevalnikov, ki sta predstavljala različna razreda naprav, namenjenih vzpostavljanju varnih VPN povezav. Takoj smo lahko potrdili, da je šifrirni algoritem AES veliko hitrejši od 3DES, saj ga je v vseh preizkusih prekašal. Prav tako smo ugotovili, da pri sistemih VPN L2TP/IPsec strojno pospeševanje močno vpliva na rezultat meritve. Saj je mrežni usmerjevalnik s strojnim pospeševanjem zabeležil hitrosti, ki so skoraj za faktor 10 višje, kot jih je zabeležil mrežni usmerjevalnik brez strojnega pospeševanja. Takšna kombinacija sistema VPN L2TP/IPsec na napravah, ki podpirajo strojno pospeševanje, je zelo primerna za varno povezavo med omrežji (Site-to-Site VPN). V taki situaciji potrebujemo veliko večjo pasovno širino kot pri

običajni VPN povezavi, ker si v tem primeru več uporabnikov med seboj deli pasovno širino. Pri VPN sistemu OpenVPN smo naleteli na zanimiv pojav, saj je imel mrežni usmerjevalnik, ki je na papirju precej slabši, v vseh testih precej boljše rezultate, kot jih je imel na papirju precej boljši mrežni usmerjevalnik. To nam pove, da vse implementacije niso enakovredne in tudi še tako velika strojna premoč ne more prikriti slabe ali neoptimizirane implementacije.

V praksi pogosto naletimo tudi na blokiranje protokola IPsec s strani internetnih ponudnikov, kar nas prisili v uporabo sistemov SSL-VPN ali OpenVPN. Spoznamo tudi, da najdražje rešitve niso vedno tudi najboljše. Še posebej, če pogledamo varnostne spodrsljaje nekaterih priznanih proizvajalcev zaprtokodnih požarnih zidov, kjer so vede ali nevede prodajali naprave z vgrajenimi stranskimi vrati. Seveda imajo tudi odprtokodne rešitve svoje negativne plati, saj mora podjetje, ki se odloči za tak sistem, samo poskrbeti za postavitev sistema in njegovo vzdrževanje. To pa večino podjetij odvrne od odprtokodnih rešitev in se raje odločijo za neko zaprtokodno rešitev. S proizvajalcem ali njihovim zastopnikom podpišejo vzdrževalno pogodbo, ki jim zagotovi postavitev in vzdrževanje VPN sistema.

Seznam uporabljenih kartic

3DES	ang. Triple Data Encryption Algorithm
AES	ang. Advanced Encryption Standard
DES	ang. Data Encryption Standard
DH	ang. Diffie-Hellman
Dual_EC_DRBG	ang. Dual Elliptic Curve Deterministic Random Bit Generator
IPsec	ang. Internet Protocol Security
L2TP	ang. Layer 2 Tunneling Protocol
MD5	ang. message-digest algorithm
MS-CHAP	ang. Microsoft version of the Challenge-Handshake Authentication Protocol
NIST	ang. National Institute of Standards and Technology
NSA	ang. National Security Agency
OpenSSL	ang. Open Secure Sockets Layer
OpenVPN	ang. Open virtual private network
PEAP	ang. Protected Extensible Authentication Protocol
PFS	ang. perfect forward secrecy
PPTP	ang. Point-to-Point Tunneling Protocol
RC4	ang. Rivest Cipher 4
RSA	ang. Ron Rivest, Adi Shamir, and Leonard Adleman
SHA	ang. Secure Hash Algorithm

SSL	ang. Secure Sockets Layer
SSL-VPN	ang. Secure Sockets Layer virtual private network
SSTP	ang. Secure Socket Tunneling Protocol
TCP	ang. Transmission Control Protocol
UDP	ang. User Datagram Protocol
VPN	ang. Virtual Privat Network

Seznam slik

Slika 2.1: Struktura PPTP paketa z vsebovanim IP datagramom……..…..…….14
Slika 2.2: Struktura L2TP paketa z vsebovanim IP datagramom..……..…….....15
Slika 2.3: Prikaz enkapsulacije L2TP paketa z IPsec ESP……...…….……..…15
Slika 3.1: Prikaz simetričnega šifriranja z deljenim ključem…..…..……..…….20
Slika 3.2: Prikaz asimetričnega šifriranja z izmenjavo javnega ključa….....21
Slika 3.3: Prikaz asimetričnega šifriranja PFS z Diffie-Hellman algoritmom.....22
Slika 3.4: Prikaz zgoščevalne funkcije……..…….…….....…....22
Slika 4.1: Povezava oddaljenega uporabnika v poslovno omrežje.…...…….…..….27
Slika 4.2: Povezava oddaljenih omrežij…..…….…….…..…….....28
Slika 4.3: Primerjava rezultatov L2TP/IPsec…….……..……..…….29
Slika 4.4: Primerjava rezultatov OpenVPN…..……..……..……..…31
Slika 4.5: Primerjava rezultatov VPN L2TP/IPsec Site-to-site…..…..……..…..…33
Slika 5.1: Povezava VPN med oddaljenim uporabnikom in podjetjem….……36
Slika 5.2: Prikaz Site-to-Site VPN…….…….…...…37

Seznam tabel

Tabela 4.1: Rezultati L2TP/IPsec za Mikrotik in Ubiquiti.……..……..……28
Tabela 4.2: Razultati OpenVPN za Mikrotik in Ubiquiti…..…….……..30
Tabela 4.3: Rezultati VPN L2TP/IPsec Site-to-Site..……..……..…..……..32

Literatura

[1] Wikipedia:Virtual private network VPN
https://en.wikipedia.org/wiki/Virtual_private_network

[2] Wikipedia: Point-to-Point Tunneling Protocol PPTP
https://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol

[3] Wikipedia: Layer 2 Tunneling Protocol L2TP/IPsec
https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol

[4] Projectbullrun.org: Dual_EC
https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

[5] Threatpost: QUESTIONS LINGER AS JUNIPER REMOVES BACKDOORED DUAL_EC RNG
https://threatpost.com/questions-linger-as-juniper-removes-backdoored-dual_ec-rng/115849/

[6] Cisco: SSL VPN
http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t11/htwebvpn.html

[7] Wikipedia: OpenVPN
https://en.wikipedia.org/wiki/OpenVPN

[8] Wikipedia: Symmetric-key algorithm
https://en.wikipedia.org/wiki/Symmetric-key_algorithm

[9] Wikipedia: DES
https://sl.wikipedia.org/wiki/DES

[10] Wikipedia: Triple DES
https://en.wikipedia.org/wiki/Triple_DES

[11] Wikipedia: Advanced Encryption Standard
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[12] Wikipedia: RC4
https://sl.wikipedia.org/wiki/RC4

[13] Wikipedia: Public-key cryptography
https://en.wikipedia.org/wiki/Public-key_cryptography

[14] Wikipedia: Forward secrecy
https://en.wikipedia.org/wiki/Forward_secrecy

[15] Wikipedia: Diffieâ€“Hellman key exchange
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

[16] Wikipedia: Hash function
https://en.wikipedia.org/wiki/Hash_function

[17] Wikipedia: MD5
https://en.wikipedia.org/wiki/MD5

[18] Wikipedia: SHA-1
https://en.wikipedia.org/wiki/SHA-1

[19] Wikipedia: SHA-2
https://en.wikipedia.org/wiki/SHA-2

[20] Wikipedia: Blowfish (cipher)
https://en.wikipedia.org/wiki/Blowfish_(cipher)

[21] Wikipedia: Twofish
https://en.wikipedia.org/wiki/Twofish

[22] Cisco: Site-to-Site and Extranet VPN Business Scenarios
http://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342site3.html

[23] rump2007: On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng
http://rump2007.cr.yp.to/15-shumow.pdf

[24] Arstechnica: Researchers confirm backdoor password in Juniper firewall code
http://arstechnica.com/security/2015/12/researchers-confirm-backdoor-password-in-juniper-firewall-code/

[25] Arstechnica: Secret SSH backdoor in Fortinet hardware found in more products
http://arstechnica.com/security/2016/01/secret-ssh-backdoor-in-fortinet-hardware-found-in-more-products/