DOI: 10.19279/TVZ.PD.2015-3-2-14

GETVPN ENKRIPCIJA

GETVPN ENCRIPTION

Goran Combaj[1], Danijela Pongrac[2], Dubravko Žigman[3]

[1]Privredna banka Zagreb d.d.
[2]Tehničko veleučilište u Zagrebu, Informatičko–računarski odjel
[3]Tehničko veleučilište u Zagrebu, Elektrotehnički odjel

Sažetak

U današnje doba računalnih komunikacija tvrtke, pokušavajući smanjiti troškove, centraliziraju svoje servise u podatkovnim centrima. Zbog toga komunikacija se odvija preko IP prometa koristeći iznajmljene vodove i pojavljuje se problem sigurnog prijenosa podataka između radne stanice korisnika i servisa u podatkovnom centru. Specijalizirane tvrtke poput Cisco-a su pristupile rješavanju ovog problema razvijanjem tehnologija enkripcije IP prometa u svojim uređajima koristeći standardne algoritme enkripcije. Razvijene su tehnologije koje se mogu koristiti bez obzira na vrstu prijenosnog medija. Jedna od tehnologija koje pobuđuju interes među mrežnim administratorima je Cisco GETVPN.

Ključne riječi: *GETVPN, IPSec, DMVPN, Cisco*

Abstract

In today's era of computer communications, the companies, trying to reduce the costs, are centralizing their services in database centres. Therefore, communication is provided via IP traffic using hired tunnels where the issue of data transport security arises between a user's working station and service in a database centre. Specialized companies like Cisco tried to solve the issue by developing the IP traffic encryption technology for their devices using standard encryption algorithms. New technologies have been developed, which can be used regardless of the transmission media. One of the technologies that attracts the interest of network administrators is Cisco GET VPN.

Keywords: *GETVPN, IPSec, DMVPN, Cisco*

1. Uvod

1. Introduction

Razvojem tehnologija širokopojasnog pristupa računalnim podacima stvorili su se preduvjeti da tvrtke centraliziraju svoje servise i podatke na jedno mjesto. Kod manjih tvrtki to je često jedan do dva servera, a kod većih podatkovni centri koji zauzimaju ogromne površine.
Tvrtke, s ciljem smanjenja troškova, realiziraju pristup podatkovnom centru koristeći iznajmljene veze. S obzirom da vlasnik iznajmljene veze može s lakoćom doći do podataka koji putuju njima, tvrtke traže načine kako zaštiti svoje podatke. Odgovor na pitanje zaštite podataka dan je u obliku enkripcije komunikacija. Razvijeno je nekoliko tehnologija i standarda. U radu dan je pregled mogućnosti relativno nove tehnologije u ponudi tvrtke Cisco pod imenom GETVPN.

2. IPSec

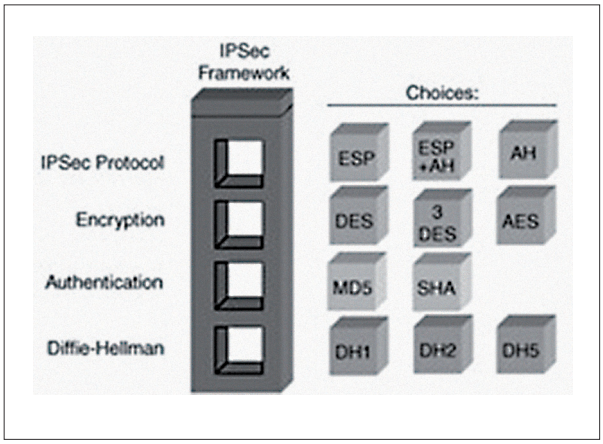
2. IPSec

IPSec je otvoreni standard, skupina protokola s namjenom zaštite IP komunikacija. Pojedine IPSec komponente osiguravaju povjerljivost, integritet i autentičnost podataka [1].

IPSec se sastoji od idućih komponenti, koje u potpunosti rješavaju zadatke navedene u općem modelu: [1]:

- Protokoli za zaštitu podataka: AH i ESP
- Protokol za upravljanje ključevima (IKE)
- Algoritmi za enkripciju i autentikaciju

IPSec definira metode kako specificirati promet koji će se zaštiti, način na koji će biti zaštićeni i kome je namijenjen (slika 1).



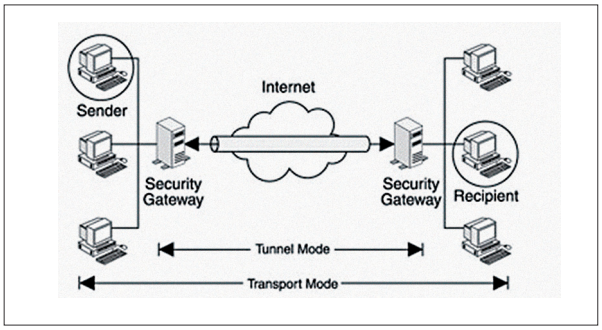
Slika 1 *Komponente IPSec-a* [2]

Figure 1 *IPSec Componente* [2]

Pomoću IPSec-a je moguće zaštiti komunikaciju između dvije radne stanice, dva mrežna uređaja ili radnih stanica i mrežnih uređaja. S obzirom da je IPSec običan IP paket moguće je pomoću njega prenositi mrežne servise. Zaštita se ostvaruje pomoću protokola AH i ESP [1].

3. IPSec načini rada

3. IPSec operation modes



Slika 2 *Načini rada IPSec-a* [3]

Figure 2 *IPSec operation modes* [3]

IPSec je dizajniran da podržava dva različita načina rada (slika 2). To su transportni i tunel način rada [2]. Načini rada se razlikuju u tehnici kojom štite podatke.

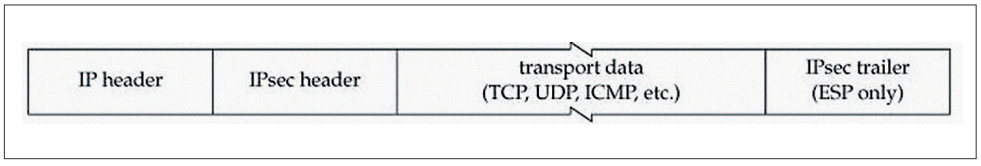
U transportnom načinu rada IPSec zaglavlje (eng. *header*) je umetnuto između IP zaglavlja i viših protokola (slika 3). U ovom načinu rada IP adrese u zaglavlju se ne mijenjaju, štite se podaci, dok su originalne IP adrese uređaja vidljive svakome u kanalu. Transportni način rada se koristi za komunikaciju između dva krajnja uređaja (npr. računala i servera – Slika 9).
Prednost ovog načina rada jest što se ne moraju definirati nove mreže na mrežnoj opremi i osigurati komunikacija s drugim IP adresama. Ovaj način rada pruža zaštitu podataka do krajnjih točaka komunikacijskog kanala. Zaštita (kriptiranje) se vrši na podacima koji se prenose (tj. sve što je iza IP zaglavlja).

U tunel načinu rada originalni IP paket je zaštićen unutar drugog paketa sa IPSec zaglavljem koje sadrži IP adrese graničnih uređaja mreža koje se povezuju (Slika 4). Originalni paket putuje kroz privremeni tunel koristeći javnu ili privatnu mrežu. Tunel način rada se koristi kada želimo kroz javno dostupnu mrežu spojiti dvije odvojene privatne mreže (npr. udaljeni ured i centralu). Prednost ovog načina rada jest što neautorizirana osoba ne može vidjeti stvarne IP adrese, te možemo udaljeni ured prikazat kao da je spojen lokalno u centralu (kao da je na istom LAN-u).

4. GETVPN

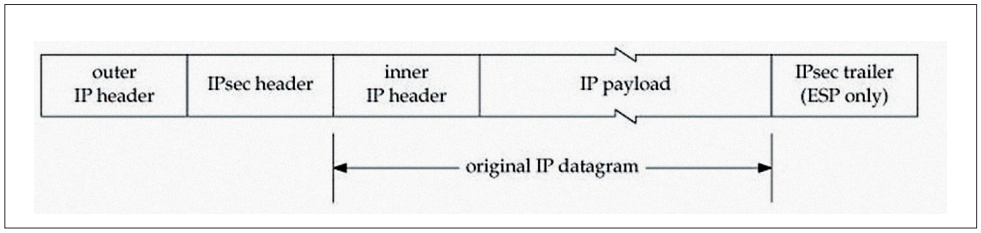
4. GETVPN

Zbog uočenih mana na tehnologijama enkripcije prometa, te sve većim potrebama za zaštitom



Slika 3 *(gore) Enkapsulacija paketa u transportnom načinu prijenosa.*[4]

Figure 3 *(above) Package encapsulation in data transport* [4]



Slika 4 *(dolje) Enkapsulacija paketa u tunel načinu prijenosa* [4]

Figure 4 *(bellow) Package encapsulation in tunneled mode of transport* [4]

podataka kroz privatne mreže Cisco je razvio novu tehnologiju enkripcije GETVPN (eng. *Group Encrypted Transport VPN*). Iz samog imena se vidi da se radi o enkripciji koja radi na IPSec transport načinu rada, tj. više nije potrebno kreirati tunele. Zbog toga što nisu potrebni tuneli moguće je i dalje koristiti postojeće tehnologije u mreži (routing, QoS, multicast) i mrežne adrese kao da uopće nema enkripcije. GETVPN nudi novi model enkripcije koji se zasniva na modelu "vjerovanja" članu grupe [5]. Članovi jedne GET grupe koriste zajedničku politiku komunikacije (ključeve, algoritme). GETVPN tehnologija je temeljena na postojećim standardima enkripcije, podržani su algoritmi 3DES, AES (128,192 i 256 bit), te na IETF standardu GDOI (eng. *Group Domain of Interpretation*) [3].

Trenutno je GETVPN tehnologija podržavan kod proizvođača Juniper i Cisco. S obzirom da je tehnologija temeljena na otvorenom dokumentu "RFC 3547" [6] (GDOI protokol) ne postoji prepreka da i drugi proizvođači naprave svoju implementaciju. Uređaji tvrtke Juniper i Cisco mogu zajedno komunicirati unutar GETVPN grupe pod uvjetom da je "key server" uređaj od tvrtke Cisco [7].

Neke od prednosti GETVPN tehnologije u odnosu na ostale su [8]:

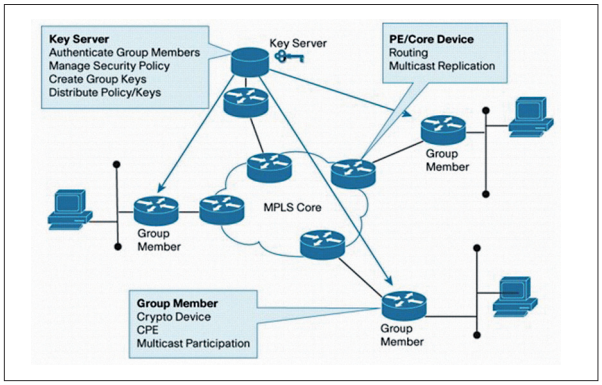
- Pruža visoko–skalabilnu svatko sa svakim topologiju, te ukida potrebu za kompleksnim tunelima između članova.
- Zadržava postojeću inteligenciju mreže (routing, QoS), što je bitno kod MPLS mreža.
- Osigurava nisku latenciju i titranje jer su sve veze stalno aktivne i nije potreban prolazak kroz centralni uređaj (kako kod zvijezda topologije).
- Dopuštena je replikacija paketa nakon enkripcije. Ovo omogućava replikaciju multicast prometa, s čime se smanjuje opterećenje uređaja na krajnjim lokacijama.
- Očuvanje IP zaglavlja omogućava da se zadrže originalne IP adrese odašiljatelja i primatelja. Tehnika se naziva IPSec tunel način rada s očuvanjem IP adresa. Očuvani su i neki parametri iz IP zaglavlja. Time se omogućava očuvanje postojećeg routinga, QoS, upravljanja prometom i funkcionalnosti vatrozida. Zbog toga sve postojeće funkcionalnosti mreže će raditi kao i prije enkripcije.
- Održavanje niskih latencija i titranje (eng. *jitter*) za audio, video i ostale komunikacije koje su osjetljive na latenciju omogućavajući direktnu komunikaciju između svih udaljenih lokacija bez potrebe za prolaskom kroz centralnu lokaciju. Isto tako smanjuje se opterećenje uređaja prilikom multicast komunikacije jer se ukida potreba za replikacijom broadcast prometa koja je inače prisutna kod drugih IPSec baziranih tehnologija.

4.1. Arhitektura GETVPN-a

4.1. GET VPN Architecture

GETVPN tehnologija je temeljena na otvorenim standardima i patentiranoj Cisco tehnologiji. Cilj je što bolje iskoristiti postojeću infrastrukturu organizacije kako bi se pružila efikasnija usluga kriptiranja komunikacija. Uz postojeće IKE, IPSec i multicast tehnologije, tehnologija koristi još iduće standarde i koncepte za ostvarenje komunikacija [3]:

- GDOI (RFC 6407)
- Key server
- Kooperativni key serveri
- članovi grupe
- očuvanje IP zaglavlja
- Grupna sigurnosna asocijacija
- Mehanizam za distribuciju ključeva (eng. *rekey*)
- vremenska zaštita od napada ponavljanja (eng. *anti –replay*) – TBAR



Slika 5 *Komponente GETVPN tehnologije* [3]

Figure 5 *GET VPN technology components* [3]

Key server je mrežni usmjernik, koji se brine o kreiranju i održavanju GETVPN kontrolnog

sloja [3]. Sve politike enkripcije (što se kriptira, algoritmi, trajanje ključeva) se definiraju na njemu. Članovi grupe se registriraju s key serverom koristeći GDOI protokol, te nakon uspješne registracije preuzimaju politiku enkripcije i ključeve za rad GETVPN-a. Ovaj uređaj je odgovoran za osvježavanje i ponovnu distribuciju svježih ključeva.

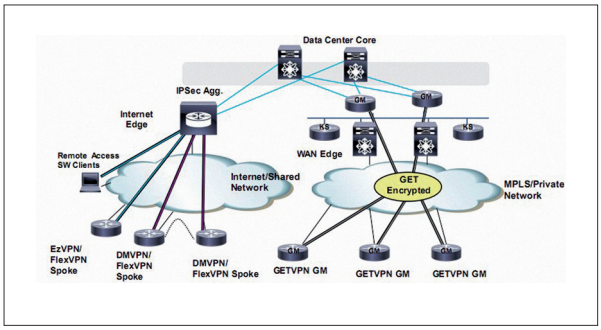
Član grupe je mrežni usmjerivač koji radi enkripciju i dekripciju komunikacija [3]. Na osnovu preuzete politike enkripcije član odlučuje koji promet će biti kriptiran, dekriptiran te koji će se ključevi koristiti.

5. Usporedba GETVPN-a s DMVPN i FlexVPN

5. Comparison of GETVPN with DMVPN and FlexVPN

Tvrtka Cisco, uz GETVPN, nudi još tehnologije DMVPN i FlexVPN za enkripciju komunikacija. Na slici 6 prikazan je prijedlog tvrtke gdje se koristi pojedina tehnologija.

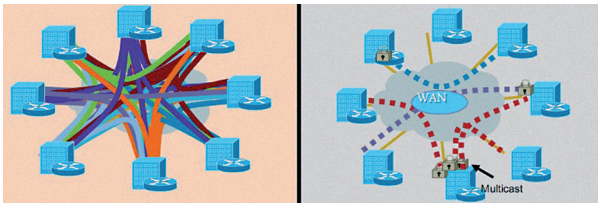
Prema slici GETVPN tehnologija je izričito namijenjena korištenju unutar WAN mreže organizacije gdje su vidljive stvarne IP adrese krajnjih uređaja. Postoje i druge tehnologije koje je moguće iskoristit za realizaciju enkripcije WAN mreže. Drugo popularno rješenje je do sada bilo korištenje DMVPN tehnologije u različitim fazama. Nova obećavajuće rješenje je FlexVPN. Tehnologija FlexVPN je svojevrsni spoj postojećih Cisco IPSec tehnologija koristeći novi IKEv2 protokol za dogovor komunikacije [10].



Slika 6 *Pozicioniranje GETVPN tehnologije* [10]

Figure 6 *GET VPN technology positioning* [10]

Osnovna razlika u konceptu ostvarenja komunikacije u tehnologijama prikazano je na slici 7. GETVPN kreira transparente (transport način rada) veze koje se koriste postojećom infrastrukturom. Kod tehnologije DMVPN i FlexVPN (site –to –site) potrebno je, koristeći postojeću infrastrukturu, kreirati dodatnu virtualnu kroz koju će putovati kriptirani promet (tunel način rada). Time se povećava kompleksnost administracije [10].



Slika 7 *Osnovna razlika GETVPN, DMVPN i FLEXVPN* [4]

Figure 7 *Basic difference between GETVPN, DMVPN and FLEXVPN* [4]

Prednosti GETVPN nad FlexVPN i DMVPN su [5]:

- jednostavno rješenje, ako je manja mreža (< 5000 routera)
- nema potrebe za virtualnim mrežnim slojem i dodatnim usmjeravanjem
- nema preferirane pozicije (centralne točke enkripcije)

S druge strane prednosti FlexVPN i DMVPN rješenja nad GETVPN-om su:

- bolja skalabilnost
- bolja sigurnost podataka (ne znaju se stvarne IP adrese komunikacije)
- kompletna podrška za IPv6

Tablica 1 *Usporedba GETVPN, DMVPN, FlexVPN* [8][9][13]

Table 1 *Comparison: GET VPN, DMVPN, FlexVPN* [8][9][13]

Tehnologija	***DMPVN***	***FlexVPN***	***GETVPN***
Tip infrastrukture	Javne mreže, Internet	Javne mreže, Internet	privatne mreže, WAN
Oblik mreže	Zvijezda, svatko sa svakim	Zvijezda, svatko sa svakim, udaljeni pristup	svatko sa svakim
Routing	Dinamični routing u tunelima	Dinamični routing u tunelima ili IKEv2 distribucija ruta	routing na postojećoj infrastrukturi

Redundancija	Pomoću routinga	Pomoću routing klaster rješenja	pomoću routinga + COOP
Virtualizacija	DA	DA	NE
IP Multicast	Replikacija prometa na centralnoj točci	Replikacija prometa na centralnoj točci	Replikacija unutar mreže
Upravljanje autorizacijom	IKE profili	IKE profili	IP adrese, na temelju ID-a routera
Skalabilnost	Neograničeno	Neograničeno	5000 članova u grupi
Stil enkripcije	ključ između dva člana	ključ između dva člana	jedan ključ za sve članove
Kompleksnost	Kreira još jedan sloj mreže.	Kreira još jedan sloj mreže.	Ne kreira dodatni sloj mreže.
Namjena	spajanja dvije lokacije, dinamične "svatko sa svakim" veze	spajanja dvije lokacije, dinamične "svatko sa svakim", udaljeni pristup	"svatko sa svakim" transparentne mreže

U tablici 2 dan je pregled uređaja koji podržavaju sve tri tehnologije od hardverski najslabijih prema najjačima. Vidljivo je da tehnologiju FlexVPN podržava samo najnovija generacija uređaja (to je zbog podrške za IKEv2 protokol). Zbog te činjenice veća je financijska investicija ukoliko se želi implementirati FlexVPN u mrežu, a tvrtka trenutno ne dobiva ništa više u odnosu na implementaciju DMVPN-a.

Tablica 2 *Podrška tehnologije u uređajima* [8][9][13]
Table 2 *Technology support of platforms* [8][9][13]

Platforma	GETVPN	DMVPN	FlexVPN
Cisco 870 Series Integrated Services Routers	X	X	
Cisco 1800 Series Integrated Services Routers	X	X	
Cisco 2800 Series Integrated Services Routers	X	X	
Cisco 3800 Series Integrated Services Routers	X	X	
Cisco 1900, 2900, and 3900 Integrated Services Routers	X	X	X
Cisco 7200 Series Routers	X	X	
Cisco 7301 Routers	X	X	
Cisco 7600 Series Routers		X	
Cisco Catalyst 6500 Series Switches		X	
Cisco ASR 1000 Series Routers	X	X	X

6. Hardverski zahtjevi za GETVPN

6. Hardware requirements for GETVPN

S obzirom da su kriptiranje i dekriptiranje hardverski zahtjevne operacije, tvrtka Cisco predlaže korištenje idućih uređaja kao članova grupe, te kao key servere (slika 30). Dodatno postoje dodaci za uređaje u obliku kartica – VPN ubrzivači (eng. *VPN Accelerators*). Dodaci omogućuju veće brzine (propusnost) prilikom kriptiranja komunikacija [8]. U tablici 3 prikazani su uređaji koji podržavaju GETVPN.

Tablica 3 *Podržani Cisco uređaji za GETVPN* [8]
Table 3 *GET VPN supported Cisco platforms* [8]

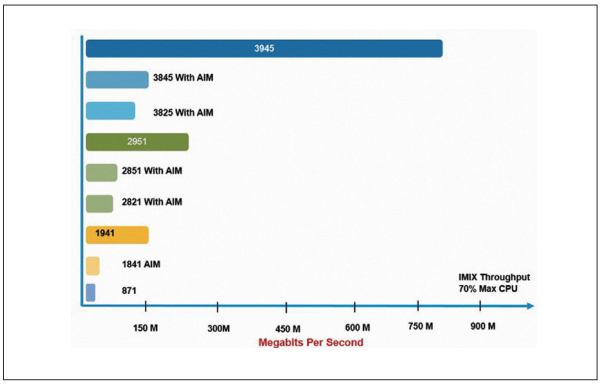
Feature	***Platform***
GETVPN Group Member	Cisco 870, 880, 890, 1800, 1900, 2800, 2900, 3800, 3900
	Cisco 7200
	Cisco 7301
	Cisco ASR 1000
GETVPN Key Server	Cisco 1841, 1900, 2800, 2900, 3800, 3900
	Cisco 7200
	Cisco 7301

Mrežni uređaji koji su zaduženi za upravljanje GETVPN enkripcijom, tj. Key serveri moraju biti u mogućnosti obraditi registracije članova grupe i svu kontrolnu komunikaciju (npr. slanje novih ključeva ili politike enkripcije). Iz tog razloga potrebno je odgovarajuće dimenzionirati te uređaje, tj. Izabrati odgovarajući model u ponudi tvrtke Cisco. U tablici 4 dan je prikaz koliko članova grupe podržava koja platforma Cisco usmjerivača.

Tablica 4 *Cisco Platforme za key server funkcionalnost* [12]
Table 4. *Cisco Platforms for key server functionality* [12]

Platform	Crypto Card	Tested GM	Max Registration CPU/Max Rekey CPU	Time to register to single KS
7200	VAM2+	2000	40/18%	25 sec
3845	AIM-VPN/SSL-3	1000	46/20%	25 sec
3825	AIM-VPN/SSL-3	500	34/14%	15 sec
2851	AIM-VPN/SSL-2	200	25/15%	15 sec
2821	AIM-VPN/SSL-2	100	30/14%	15 sec
1841	AIM-VPN/SSL-1	50	16/8%	15 sec
7200/PKI	VAM2+	500	30/10%	40+sec

Slično kao što je potrebno odgovarajuće dimenzionirati key server uređaje, potrebno je obratiti pažnju i na performanse uređaja na krajnjim lokacijama koji će biti članovi grupe. Oni rade kompletnu enkripciju i dekripciju prometa s obzirom na dobivenu politiku enkripcije. Na slici 8 dana je usporedba performansi pojedinih tipova Cisco usmjerivača prilikom korištenja enkripcije.



Slika 8 *Usporedba performansi Cisco usmjerivača.* [11]
Figure 8 *Comparison of the Cisco router performances.* [11]

7. Zaključak

7. Conclusion

GETVPN tehnologija predstavlja zanimljivo i jednostavno rješenje za implementaciju virtualnih privatnih mreža koristeći postojeću telekomunikacijsku infrastrukturu. Prednost nad ostalim tehnologijama jest transparentnost za postojeće tehnologije (QoS, multicast, usmjeravanje), minimalni utjecaj na komunikacije osjetljive na kašnjenje (telefonski i video pozivi). Konfiguracija je vrlo jednostavna, sva politika se određuje na jednom centralnom mjestu. Nedostatak trenutne implementacije jest mogućnost rada samo na privatnim mrežama, te djelomična podrška za IPv6. S obzirom da Cisco nastavlja s daljnjim razvojem GETVPN-a, uvodi nove i bolje algoritme enkripcije komunikacija, podršku za enkripciju IPV6 komunikacija, podršku za do 8000 članova grupe, hijerarhijske grupe i standardizaciju protokola kroz IETF organizaciju, vrlo vjerojatno će i ti nedostaci biti uklonjeni.

8. Reference

8. References

[1] Doraswamy, N., et. Al IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, Second Edition, 2003

[2] Bollapragada V., et al. IPSec VPN Design, 2005

[3] Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide;s Interneta: http://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN_DIG_version_1_0_External.pdf

[4] Snader Jon; VPNs Illustrated: Tunnels, VPNs, and IPsec; 2005

[5] Lewis, M. Comparing, Designing, and Deploying VPNs; 2006

[6] The Group Domain of Interpretation(RFC3547); s Interneta: http://tools.ietf.org/rfc/rfc3547.txt;27.01.2014.

[7] Group VPN Interoperability with Cisco's GET VPN; http://www.juniper.net/techpubs/en_US/junos10.2/information-products/topic-collections/release-notes/10.2/index.html?topic-46054.html;27.01.2014.

[8] Cisco Group Encrypted Transport VPN Data Sheet;s Interneta: http://www.cisco.com/c/en/us/products/collateral/security/group-encrypted-transport-vpn/product_data_sheet0900aecd80582067.html

[9] Cisco DMVPN Data Sheet; http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps6658/data_sheet_c78-468520.html;06.01.2014.

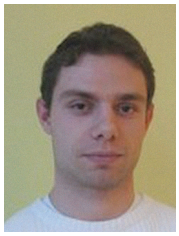
[10] Detienne F., et al.; Designing & Deploying Secure VPN's with IOS FlexVPN & GETVPN, TECSEC-3725; Cisco Live Milan 2014

[11] Advanced IPsec with GET VPN; BRKSEC-4011, Cisco Live 2010 Las Vegas

[12] Honore Alexandre; Deploying and Troubleshooting GETVPN, BRKSEC-3011, Cisco Live 2012

[13] Moraes, Alexandre, FlexVPN Overview; Cisco public 2012

AUTORI · AUTHORS



Goran Combaj

Goran Combaj rođen je 1985. godine u Zagrebu, završava srednju elektrotehničku školu u Sesvetama, smjer elektrotehničar. Godine 2005. upisuje stručni studij na Tehničkom Veleučilištu Zagreb, smjer elektrotehnika koji završava 2008. godine. U 2008. godini sudjeluje na Cisco NetRiders natjecanju te osvaja prvo mjesto u pojedinačnom natjecanju. Upisuje specijalistički studij informatike na TVZ-u, smjer: Projektiranje i implementacija računalnih mreža kojeg završava 2014. godine. Nakon završetka stručnog studija zapošljava se u Privredna Banka Zagreb na poziciji: sistem inženjer za WAN mreže Posjeduje RHCA certifikat.

Danijela Pongrac - nepromjenjena biografija nalazi se u časopisu Polytechnic & Design Vol. 2, No. 1, 2014.

Dubravko Žigman - nepromjenjena biografija nalazi se u časopisu Polytechnic & Design Vol. 1, No. 1, 2013.