Zaštita prenosa paketskog telefonskog saobraćaja upotrebom tehnologije virtuelnih privatnih mreža

Mićo Živanović, Jovan Bajčetić, Ivan Tot

***Apstrakt*—Istraživanje predstavljeno u ovom radu prikazuje jednu realizaciju zaštite paketskog telefonskog saobraćaja primenom tehnologije virtuelnih privatnih mreža kroz konfiguraciju servera za prenos paketskog telefonskog saobraćaja i zaštićeni prenos uz primenu tehnologije virtuelnih privatnih mreža u tunel modu, primenom odgovarajućeg protokola za zaštitu tajnosti, autentifikaciju, zaštitu integriteta i razmenu kriptografskih ključeva. Izvršeno je snimanje i analiza saobraćaja primenom softvera Wireshark u zaštićenom i nezaštićenom prenosu. Prikazani rezultati omogućavaju lakše razumevanje kompleksnog procesa uspostave tunela upotrebom simulacionog softvera u edukaciji.**

***Ključne reči*—paketski telefonski saobraćaj; virtuelne privatne mreže; zaštićena komunikacija; kriptografski ključ.**

I. Uvod

Stalan razvoj Interneta ima za posledicu da je Internet postao univerzalno sredstvo za komunikaciju. U toku razvoja, postavio se zahtev za bezbednošću prenošenih informacija koji se ogledao u obezbeđenju bezbednosnih servisa: autentifikacije, poverljivosti, neporecivosti i integriteta podataka [1]. Razvijeni su sistemi zaštite u tri ravni: upravljačkoj, kontrolnoj i ravni podataka. Za potrebe ovog rada biće razmotreni mehanizmi zaštite u ravni podataka koji se odnose na informacioni saobraćaj. Ravan podataka se štiti pomoću implementiranja pravila (bezbednosnih polisa) po kojima se informacioni sadržaj prenosi upotrebom mrežnih uređaja.

Jedna od tehnologija koja omogućava zaštitu prenosa podataka u ravni podataka je tehnologija virtuelnih privatnih mreža (VPN – Virtual Private Networks). Navedena tehnologija pruža sledeće mogućnosti umrežavanja:
– Intranet, umrežavanje geografski dislociranih objekata;
– Udaljeni pristup mobilnih korisnika (rad od kuće);
– Ekstranet, ograničeni pristup nekoj mreži iz drugih mreža (pristup poslovnih partnera korporativnom WAN-u) [2].

Za realizaciju virtuelne privatne mreže mogu se koristiti periferni korisnički uređaji (host, ruter ili svič), na lokaciji korisnika (CE – Customer Edge) i periferni mrežni uređaji provajdera (PE – Provider Edge).

Virtuelnu privatnu mrežu čini više udaljenih mreža koje su povezane preko Interneta. Zbog korišćenja zajedničkih resursa na Internetu, komunikacija među korisnicima virtuelne privatne mreže se mora zaštititi. Zaštita virtuelne privatne mreže se ostvaruje pomoću barijera koje implementiraju IPSec protokol u tunel modu [3].

VPN tunel je veza između dva PE rutera ili dva CE uređaja koji predstavljaju krajnje tačke tunela [2].

Prema IETF, IP VPN se mogu klasifikovati u zavisnosti od odgovornosti u pogledu upravljanja na:
– VPN kojima upravlja korisnik (Customer Provisioned VPN, CP VPN);
– VPN kojima upravlja provajder servisa (Provider Provisioned VPN, PP VPN) [2].

Prema lokaciji VPN opreme, PP VNP se mogu podeliti na:
– CE – bazirane, kod kojih su krajnje tačke VPN locirane kod korisnika;
– PE – bazirane, kod kojih su krajnje tačke VPN tunela locirane kod provajdera, na PE ruteru.

U zavisnosti od ponuđenog servisa, PE – bazirane VPN se dele na:
– PE – bazirane L2 VPN (koje pružaju servise OSI sloja 2);
– PE – bazirane L3 VPN (koje pružaju servise OSI sloja 3);
– CE – bazirane IP VPN pružaju samo servise OSI sloja 3.

Istovremeno sa razvojem bezbednosnih servisa razvijaju se arhitekture za pružanje različitih komunikacionih servisa koji koriste Internet protokol (telefonija, video, podaci, multimedijalni servisi). Prenos telefonije preko Interneta razvijao se postupno, pre svega zbog prethodno razvijenih sistema klasičnih javnih telefonskih mreža (PSTN) i digitalnih mreža sa integrisanim servisima (ISDN).

U cilju razvoja telefonije zasnovane na komutaciji paketa (VoIP telefonija), razvijene su grupe protokola za prenos VoIP telefonije i povezivanje VoIP telefonije sa telefonijom koja se prenosi u drugim sistemima prenosa (H.323 i SIP protokol) [4].

Prikaz istraživanja u ovom radu će se sastojati iz opisa načina realizacije zaštite informacije korišćenjem VPN tehnologije, a potom u jednoj realizaciji zaštite prenosa paketskog telefonskog saobraćaja upotrebom tehnologije

Mićo Živanović – Ministarstvo odbrane, Sektor za ljudske resurse, Nemanjina 15, 11000 Beograd, Srbija (e-mail: comiveza@yahoo.com).
Jovan Bajčetić – Vojna Akademija, Univerzitet odbrane u Beogradu, Veljka Lukića Kurjaka 33, 11042 Beograd, Srbija (e-mail: bajce05@gmail.com).
Ivan Tot – Vojna Akademija, Univerzitet odbrane u Beogradu, Veljka Lukića Kurjaka 33, 11042 Beograd, Srbija (e-mail: totivan@gmail.com).

 ISBN 978-86-7466-930-3

virtuelnih privatnih mreža, upotrebom IPSec protokola u tunel modu ka udaljenom korisniku, uz prikaz analize mrežnog saobraćaja korišćenjem programskog alata Wireshark.

II. ZAŠTITA PODATAKA PRIMENOM TEHNOLOGIJE VIRTUELNIH PRIVATNIH MREŽA

Za prenos informacionog sadržaja preko Interneta neophodno je obezbediti zaštitu u prenosu. Čest je slučaj da kompanije koriste Internet kao okosnicu za povezivanje svojih filijala ili klijenata kako bi ostvarili prenos podataka za svoje potrebe. Iz navedenog razloga nameće se potreba za zaštitu prenošenog saobraćaja. U tu svrhu koriste se različite tehnologije, od kojih je jedna - tehnologija virtuelnih privatnih mreža. Za realizaciju virtuelnih privatnih mreža na raspolaganju je više tehnologija, zavisno od toga da li se VPN realizuje kao "oblast – oblast" (site–to–site) ili kao "udaljeni pristup" (remote access). U oba navedena slučaja najčešće se koristi IPSec (IP security) protokol.

IPSec protokol štiti pakete između dva uređaja u mreži [3].

Uređaji kojima se realizuje IPSec su: server, ruteri, korisnički računari ili specijalizovani hardver. IPsec pruža dve vrste zaštite: autentifikaciju i poverljivost.

Mehanizam autentifikacije osigurava da je primljeni paket zaista poslao onaj ko je u zaglavlju paketa naveden kao izvor i da se paket nije promenio tokom prenosa, dok mehanizam poverljivosti omogućava entitetima u komunikaciji da šifruju poruke kako bi sprečili nepozvana lica da dođu do sadržaja poruka [1]. Za šifrovanje podataka se koriste simetrični algoritmi (DES, 3DES, AES), što zahteva pouzdanu razmenu ključeva strana u komunikaciji i za tu svrhu se koriste protokoli za autentifikaciju (neki od protokola iz IETF (IKE - Internet Key Exchange) standarda) [3].

Razvoj bezbednosti u arhitekturi Interneta se odvijao postepeno u čemu je značajno mesto imala Radna grupa za inženjering Interneta (IETF – Internet Engineering Task Force). Sâmo uvođenje standarda je išlo postepeno. Prvi u nizu standard IETF koji se odnosio na bezbednost u arhitekturi Interneta bio je standard RFC 1636 (Request for Comments). Standard se odnosio na osnove bezbednosti Interneta (upotreba firewall – a, servis autentifikacije, privatnost i dr.) [5].

Da bi se adekvatno razumeo način formiranja VPN sesije in a pravi način predstavio prilikom edukacije, biće razmotreno nekoliko najvažnijih dokumenata IETF kojima su definisani režimi rada VPN, mehanizam autentifikacije, razmena kriptografskih ključeva i zaštita poverljivosti.

IPSec koristi dva protokola za bezbednost: AH (Authentication Header) i ESP (Encapsulating Security Payload). Zaglavlje autentifikacije (AH) je definisano specifikacijom RFC 4302 (IP Authentication Header), dok je ESP enkapsulirajuće bezbedno pakovanje (Encapsulating Security Payload) definisan specifikacijom RFC 4303. AH i ESP podržavaju dva režima rada: transportni režim i tunelovanje.

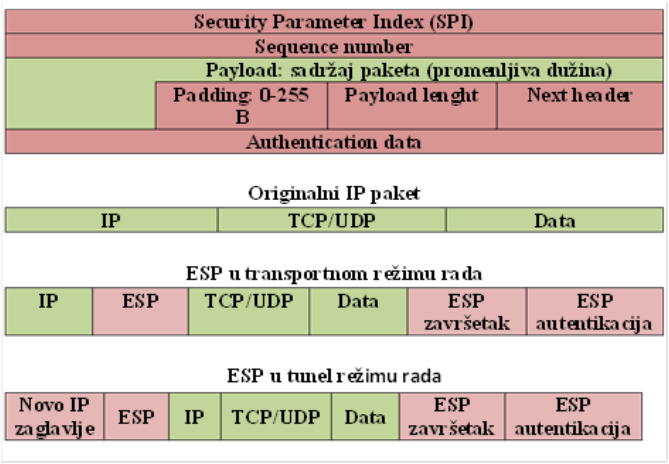
U transportnom režimu AH autentifikuje IP koristan sadržaj i odabrane delove IP zaglavlja, dok ESP šifruje i opciono autentifikuje IP koristan sadržaj. Tunelovanje vrši zaštitu celog IP paketa. Navedeno se postiže nakon dodavanja AH i ESP polja i tretiranja celog paketa kao korisnog sadržaja novog spoljnog IP paketa sa novim IP zaglavljem.

U režimu tunelovanja ESP šifruje i opciono autentifikuje ceo unutrašnji IP paket, uključujući unutrašnje IP zaglavlje, dok AH u režimu tunelovanja autentifikuje ceo unutrašnji IP paket i odabrane delove spoljnog IP zaglavlja [1].

Redosled postupaka sa paketima za rad ESP u transportnom i tunel režimu, je sledeći:

– U transport režimu blok podataka koji se sastoji od segmenta transportnog sloja sa dodatim ESP završnim blokom se šifruje, sa dodatim zaglavljem za autentifikaciju (opciono);

– U režimu tunelovanja, ESP se koristi za šifrovanje celog IP paketa, ESP zaglavlje ide ispred paketa i šifruje se paket zajedno sa ESP završnim blokom.



Sl. 1 Opseg ESP šifrovanja u transportnom i tunel modu [6]

Sl. 1 prikazuje format jednog ESP paketa. Indeks bezbednosnih parametara (SPI) definiše jednu bezbednosnu asocijaciju kojom se određuje algoritam šifrovanja i autentifikacije, ključevi, inicijalizacione vrednosti, životni vek ključeva i vezani parametri koji se koriste uz ESP. Broj sekvence je vrednost brojača paketa kojom se sprečava ponavljanje paketa. Sadržaj paketa je promenljive dužine i predstavlja segment transportnog sloja (transport režim) ili IP paket (tunel režim). U tunel modu, celom paketu se dodaje novo IP zaglavlje koje ima dovoljno informacija za rutiranje, ali ne i za analizu saobraćaja [6].

Važan deo IPSec koji se odnosi na upravljanje ključevima obuhvata određivanje i distribuciju ključeva. Dokumentom RFC 4301 definisane su dve vrste upravljanja ključevima:

– Ručno (administrator definiše sistem sopstvenim ključevima i ključevima drugih sistema sa kojima komunicira);

– Automatizovano (omogućava generisanje ključeva za bezbednosnu asocijaciju na zahtev koji je pogodan za velike sisteme sa rastućom konfiguracijom) [7].

Protokol koji se koristi za automatizovano upravljanje ključevima za IPSec je ISAKMP (Internet Security

 ISBN 978-86-7466-930-3

Association and key Management Protocol) i definisan je dokumentom IETF RFC 2408. ISAKMP definiše procedure za kreiranje i upravljanje bezbednosnim asocijacijama, tehnike generisanja ključeva, ublažavanje pretnji (npr. od DDoS napada) [8].

ISAKMP ne nalaže konkretan algoritam za razmenu ključeva, već se sastoji od jednog skupa tipova poruka koje omogućavaju upotrebu raznovrsnih algoritama za razmenu ključeva.

Karakteristike IKE određivanja ključeva su:
- Osujećenje DDoS napada;
- Omogućava razmenu ključeva za pregovaranje oko grupe ključeva;
- Obezbeđuje od napada ponavljanjem korišćenjem jednokratnih brojeva;
- Omogućava razmenu javnih ključeva;
- Onemogućava napad tipa "čovek u sredini".

IKE potprotokol obezbeđuje dogovaranje protokola, algoritama i ključeva između učesnika u komunikaciji, proverava autentičnost učesnika koji učestvuju u postupku dogovaranja, omogućava razmenu podataka na osnovu kojih će se generisati ključevi i upravljati razmenom ključeva. IKE potprotokol obavlja se u dve faze [9].

U prvoj fazi dva učesnika uspostavljaju bezbedni komunikacioni kanal kojim će se obaviti dogovaranje bezbednosnih parametara i razmena ključeva. Dogovaranje parametara i razmena ključeva, odnosno uspostava bezbednosne asocijacije obavlja se u drugoj fazi. Za sprovođenje postupka koriste se tri načina razmene informacija, dva za prvu fazu i jedan za drugu fazu IKE potprotokola:
- Osnovni način;
- Agresivni način;
- Brzi način.

Osnovni način razmene informacija (engl. Main mode) koristi se u prvoj fazi IKE potprotokola i služi da bi se uspostavio bezbednosni komunikacioni kanal kojim će se obaviti razmena podataka potrebnih za kasniju komunikaciju AH ili ESP potprotokolima.

Agresivni način razmene, slično kao i osnovni, koristi se u prvoj fazi IKE potprotokola i služi za uspostavljanje sigurnog komunikacionog kanala za dogovor učesnika i ne obavlja se kroz bezbedni kanal. Agresivni način koristi samo tri poruke u razmeni i nešto je jednostavniji i brži od osnovnog načina, ali se dokazivanje identiteta ne vrši kroz bezbedan kanal.

Nakon uspostave bezbednog kanala primenom osnovnog ili agresivnog načina razmene, započinje druga faza IKE potprotokola. Druga faza koristi se brzim načinom razmene ključeva koja služi za dogovaranje bezbednosnih parametara komunikacije AH ili ESP potprotokolom i za razmenu tajnih simetričnih ključeva.

III. JEDNA REALIZACIJA ZAŠTITE PAKETSKOG TELEFONSKOG SAOBRAĆAJA UPOTREBOM TEHNOLOGIJE VIRTUELNIH PRIVATNIH MREŽA

U uvodu rada predstavljena je podela VPN prema tome ko je odgovoran za uspostavu zaštićene komunikacije (provajder ili korisnik), kao i koja vrsta servisa se ostvaruje (sloj 2 ili 3 OSI referentnog modela). Predloženi model koje će u nastavku biti prikazan omogućava realizaciju jedne VPN koja bi predstavljala primer uspostave zaštite VoIP putem VPN za koju je „odgovoran" provajder, na OSI sloju 3 i da se primenom programskog alata „Wireshark" snimi i analizira ostvareni saobraćaj. Za navedene potrebe je uspostavljena mrežna topologija prikazana na Sl. 2.

Ruteri predstavljaju periferne rutere provajdera na kojima se vrši konfigurisanje VPN konekcije, po modelu "oblast – oblast". Na ruteru 1 su konfigurisani i uspostavljeni VPN, VoIP i DHCP server.

VPN server je konfigurisan sledećim parametrima:
- ISAKMP razmena kripto ključeva (policy 10);
- Kripto algoritam 3DES;
- Algoritam za autentifikaciju MD5 [10];
- Rad u tunel modu.

VoIP server je određen sledećim parametrima:
- Konekcija SIP protokolom;
- Kodek g711 ulaw.

Za razumevanje rada VoIP, ukratko će biti objašnjen prenos signalizacije i kontrola saobraćaja u VoIP prenosnim sistemima, u kojima se najčešće koriste H.323 i SIP protokoli.

H.323 preporuka je deo familije ITU-T preporuka sa zajedničkom oznakom H.32x koje se odnose na multimedijalne komunikacije preko različitih mreža. H.323 definiše protokole zadužene za usluge multimedijalnih komunikacija preko mreža zasnovanih na komutaciji paketa. H.323 se najčešće koristi kao signalizacioni i kontrolni protokol u VoIP i za video konferencije, a bio je prvi standard koji je koristio RTP protokol (Real-time Transfer Protocol) za konkretni prenos audio i video signala preko mreže.

H.323 je standard koji omogućava multimedijalnu komunikaciju preko različitih mreža (usko pojasne ISDN, širokopojasne B-ISDN, lokalne računarske mreže, mreže na bazi komutacije kola). Cilj je postizanje interoperabilnosti sa različitim mrežama za prenos multimedijalnih informacija, kroz upotrebu zajedničkih preporuka, procedura i poruka, kao i uvođenjem komponente mrežnog prolaza. H.323 standard predstavlja skup protokola namenjenih za obavljanje različitih funkcija u okviru H.323 sistema i to: audio kodere i dekodere, video kodere i dekodere, signaliziranje poziva, kontrola poziva, protokol prenosa u realnom vremenu (RTP), protokol kontrole prenosa u realnom vremenu (RTCP), registraciju, pristup i status i ostale protokole za prenos podataka u realnom vremenu [4].

 ISBN 978-86-7466-930-3

SIP je protokol za uspostavljanje, modifikaciju i raskidanje multimedijalnih sesija u paketskim mrežama. SIP u kombinaciji sa drugim protokolima se koristi za opis karakteristika sesije potencijalnim učesnicima [11]. SIP je delo IETF (Internet Engineering Task Force) i razvijen je kao mehanizam za uspostavljanje raznovrsnih sesija, a može se koristiti za unicast i multicast komunikaciju. SIP je peer-to-peer protokol, što znači da nije centralizovan, već je servisna inteligencija izmeštena prema krajevima mreže ka krajnjim korisnicima, kao kod računarskih mreža. U okviru SIP poruka se najčešće prenosi SDP (Session Description Protocol), mada standard ostavlja otvorenim i druge mogućnosti [12].

H.323 i SIP su dva konkurentska protokola za multimedijalne komunikacije na paketskim mrežama.

SIP se odlikuje sledećim prednostima:

– Fleksibilnost (omogućava korišćenje sa različitim transportnim i drugim protokolima);
– Arhitektura i osobine mu se prirodno uklapaju Internet okruženje, dok H.323 ima neke osobine protokola fiksne telefonije;
– Poseduje mnoga proširenja potrebna za različite sisteme ličnih komunikacija (prisutnost, instant poruke, posredno upravljanje pozivom) [13].

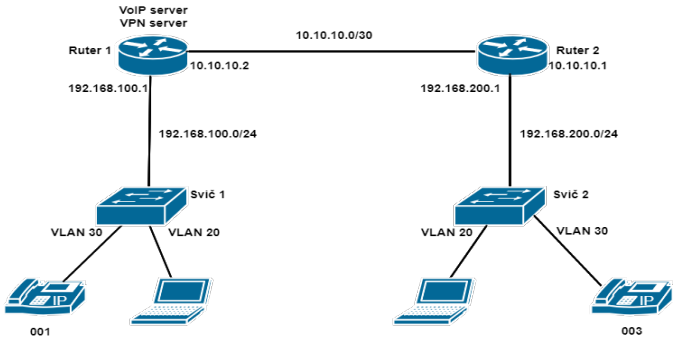
DHCP server je uspostavljen za opseg adresa koji obezbeđuje formiranje logički odvojenih mreža sa opsegom adresa 20.20.20.0 i 30.30.30.0 u različitim virtuelnim lokalnim mrežama. Prema mrežnoj topologiji formirane su dve LAN mreže u okviru kojih je izvršeno razdvajanje saobraćaja (telefonskog i podaci), uspostavom dve VLAN na OSI sloju L2, konfigurisanjem svičeva 1 i 2 (VLAN 20 i 30), dok je po jedan interfejs na svičevima konfigurisan kao trank interfejs [14]. Nakon provere konektivnosti, uspostavljen je paketski telefonski saobraćaj bez zaštite pomoću virtuelne privatne mreže i realizovano snimanje saobraćaja, upotrebom programskog alata “Wireshark”. Rezultat i procesi analize nezaštićenog saobraćaja prikazani su u Tabeli 1. Uspostavljena je VPN sesija između dva rutera i realizovano snimanje saobraćaja u zaštićenom modu. Procesi u toku uspostave zaštićenog paketskog telefonskog saobraćaja prikazani su u Tabeli 2.

Za realizaciju mrežne topologije na slici 2 korišćena je sledeća mrežna oprema:

– CISCO 2900 ruter…….2 kom;
– CATALIST 3650 svič ……..2 kom;
– Računar sa ETH mrežnim interfejsom…. 2 kom;
– IP telefoni……..2 kom.

Procesi prikazani u Tabeli 1, a koji se odnose na uspostavu i održavanje nezaštićenog telefonskog saobraćaja prikazuju proces uspostavljanja prisutnosti uređaja u mreži i utvrđivanja mrežnih usluga (SSDP), uspostavu logičke topologije mreže i saobraćaja protokola za sprečavanje petlji (STP). Pozivanjem jednog korisnika od strane drugog korisnika ustanovljava se IP adresa pozvanog korisnika kroz broadcast upit od strane pozivajućeg korisnika (ARP proces). Kroz DNS proces se povezuju IP adresa i ime domena pozvanog korisnika. Istovremeno se šalje poruka radi utvrđivanja dostupnosti korisnika (ICMP poruka). U toku uspostave VoIP komunikacije šalje se “hello poruka” u OSPF procesu, radi konstruisanja putanje između dva rutera. Kroz SIP signalizaciju vrši se pozivanje jednog od strane drugog korisnika, nakon čega se ostvaruje TCP sesija kroz proces “trostrukog rukovanja”. U sklopu SIP procesa razlikuju se faze (traying, ringing i OK), u kojima se mogu uočiti status procesa pozivanja, koji se na kraju završava uspešnom uspostavom komunikacije. Ceo proces je praćen slanjem kontrolnih TCP poruka (ACK), kojima se određuje broj bajtova koji se može poslati pre dobijanja sledeće dozvole za slanje, kao i slanjem poruka kojima se vrši sinhronizacija uspostave TCP sesije (SYN). Poseban segment kontrole komunikacije predstavlja kontrola konektivnosti na L2 nivou (LOOP). Dalji proces komuniciranja je praćen razmenom paketa u realnom vremenu (RTP) koji nose govorni informacioni sadržaj.

Procesi prikazani u Tabeli 2, a koji se odnose na uspostavu i održavanje zaštićenog telefonskog saobraćaja, pored na početku navedenih procesa u nezaštićenom prenosu, sadrži proces razmene kripto ključeva u procesu uspostave IPSec tunela (ISAKMP). Specifično za proces prenosa u zaštićenom modu je uspostavljen trank između dva sviča na kojima su konfigurisane dve VLAN (DTP).



Sl. 2 Mrežna topologija za potrebe jedne realizacije zaštite paketskog telefonskog saobraćaja upotrebom tehnologije virtuelnih privatnih mreža

Prikazana realizacija mrežne topologije, snimanje i analiza mrežnog saobraćaja omogućava detaljno razumevanje uspostave VPN tunela, uz upotrebu simulacionog softvera, kao i praćenje procesa razmene informacionog sadržaja u realnom vremenu. Tokom procesa prenosa informacionog sadržaja u realnom vremenu, periodično se uočavaju procesi uspostavljanja prisutnosti uređaja u mreži (SSDP), obaveštavanja o nedostupnosti uređaja u slučaju prekida konektivnosti (ICMP poruke) i razmena “hello” poruka u OSPF procesu. Navedena realizacija stoga omogućava potpun uvid u sve procese u toku prenosa paketskog telefonskog saobraćaja, što može poslužiti u edukaciji i o procesima prenosa multimedijalnih informacionih sadržaja.

 ISBN 978-86-7466-930-3

TABELA I
POZIV UČESNIKA 001 KA UČESNIKU 003 BEZ VPN ZAŠTITE

R.br.	Vreme [s]	Izvorišna adresa	Odredišna adresa	Protokol	Veličina [B]
1.	0,00	Cisco_e1:aa:81	Spanning_tree	STP	60
2.	0,17	Fe80:e010:c683:5106:f3e8	Ff02::c	SSDP	208
3.	1,99	Cisco_e1:aa:81	Spanning_tree	STP	60
4.	2,73	ASUSTEkC_9d:86:8a	Cisco_00:e3:e1	ARP	42
5.	2,74	Cisco_00:e3:e1	ASUSTEkC_9d:86:8a	ARP	60
6.	3,433	40.40.40.3	192.168.100.1	DNS	75
7.	3,434	40.40.40.1	40.40.40.3	ICMP	70
8.	4,00	Cisco_e1:aa:81	Spanning_tree	STP	60
9.	4,18	Fe80:e010:c683:5106:f3e8	Ff02::c	SSDP	208
10.	5,32	40.40.40.1	224.0.0.5	OSPF	90
11.	5,99	Cisco_e1:aa:81	Spanning_tree	STP	60
12.	6,56	40.40.40.3	192.168.100.1	DNS	75
13.	6,561	40.40.40.1	40.40.40.3	ICMP	70
14.	6,83	40.40.40.3	30.30.30.1	SIP/SDP	922
15.	7,16	40.40.40.3	30.30.30.1	TCP	590
16.	7,16	30.30.30.1	40.40.40.3	TCP	60
17.	7,16	40.40.40.3	30.30.30.1	TCP	386
18.	7,16	30.30.30.1	40.40.40.3	SIP	418
19.	7,18	Fe80:e010:c683:5106:f3e8	Ff02::c	SSDP	208
20.	7,36	40.40.40.3	30.30.30.1	TCP	54
21.	7,99	Cisco_e1:aa:81	Spanning_tree	STP	60
22.	8,30	40.40.40.3	30.30.30.1	TCP	58
23.	8,32	Cisco_e1:aa:81	Cisco_e1:aa:81	LOOP	60
24.	8,37	30.30.30.1	40.40.40.3	TCP	590
25.	8,37	30.30.30.1	40.40.40.3	SIP	124
26.	8,37	40.40.40.3	30.30.30.1	TCP	54
27.	9,99	Cisco_e1:aa:81	Spanning_tree	STP	60
28.	10,18	Fe80:e010:c683:5106:f3e8	Ff02::c	SSDP	208
29.	11,97	10.10.10.2	40.40.40.3	RTP	214
30.	11,97	30.30.30.1	40.40.40.3	TCP	590
31.	11,97	30.30.30.1	40.40.40.3	SIP/SDP	424
32.	11,97	40.40.40.3	30.30.30.1	TCP	54
33.	11,98	40.40.40.3	10.10.10.2	RTP	55
34.	11,98	40.40.40.3	10.10.10.2	TCP	66
35.	11,98	10.10.10.2	40.40.40.3	TCP	60
36.	11,98	40.40.40.3	10.10.10.2	TCP	54
37.	11,98	40.40.40.3	10.10.10.2	SIP	459
38.	11,98	10.10.10.2	40.40.40.3	TCP	60
39.	11,99	10.10.10.2	40.40.40.3	RTP	214
40.	11,99	Cisco_e1:aa:81	Spanning_tree	STP	60
41.	12,01	10.10.10.2	40.40.40.3	RTP	214
42.	12,03	10.10.10.2	40.40.40.3	RTP	214
43.	12,25	40.40.40.3	10.10.10.2	RTP	214

TABELA II
POZIV UČESNIKA 001 KA UČESNIKU 003 SA VPN ZAŠTITOM

R.br.	Vreme [s]	Izvorišna adresa	Odredišna adresa	Protokol	Veličina [B]
1.	0,00	Fe80:e010:c683:5106:f3e8	Ff02::c	SSDP	208
2.	0,03	Cisco_e1:aa:81	Spanning_tree	STP	60
3.	0,73	40.40.40.3	10.10.10.2	ISAKMP	126
4.	0,73	10.10.10.2	40.40.40.3	ISAKMP	126
5.	2,03	Cisco_e1:aa:81	Spanning_tree	STP	60
6.	4,00	Fe80:e010:c683:5106:f3e8	Ff02::c	SSDP	208
7.	4,03	Cisco_e1:aa:81	Spanning_tree	STP	60
8.	6,03	Cisco_e1:aa:81	Spanning_tree	STP	60
9.	6,88	Fe80:e010:c683:5106:f3e8	Ff02::1:2	DHCPv6	149
10.	7,00	Fe80:e010:c683:5106:f3e8	Ff02::c	SSDP	208
11.	8,03	Cisco_e1:aa:81	Spanning_tree	STP	60
12.	8,67	Cisco_e1:aa:81	Cisco_e1:aa:81	LOOP	60
13.	10,00	Fe80:e010:c683:5106:f3e8	Ff02::c	SSDP	208
14.	10,03	Cisco_e1:aa:81	Spanning_tree	STP	60
15.	10,88	Fe80:e010:c683:5106:f3e8	Ff02::1:2	DHCPv6	154
16.	12,03	Cisco_e1:aa:81	Spanning_tree	STP	60
17.	13,30	Cisco_e1:aa:81	CDP/VTP/DTP	DTP	60
18.	13,30	Cisco_e1:aa:81	CDP/VTP/DTP	DTP	90
19.	14,00	Fe80:e010:c683:5106:f3e8	Ff02::c	SSDP	208
20.	14,03	Cisco_e1:aa:81	Spanning_tree	STP	60
21.	16,03	Cisco_e1:aa:81	Spanning_tree	STP	60
22.	17,00	Fe80:e010:c683:5106:f3e8	Ff02::c	SSDP	208
23.	18,03	Cisco_e1:aa:81	Spanning_tree	STP	60
24.	18,67	Cisco_e1:aa:81	Cisco_e1:aa:81	LOOP	60
25.	19,32	Cisco_e1:aa:81	ASUSTEkC_9d:86:8a	ARP	60
26.	19,32	ASUSTEkC_9d:86:8a	Cisco_e1:aa:81	ARP	42
27.	20,00	Fe80:e010:c683:5106:f3e8	Ff02::c	SSDP	208
28.	20,03	Cisco_e1:aa:81	Spanning_tree	STP	60
29.	20,51	40.40.40.3	10.10.10.2	TCP	66
30.	22,03	Cisco_e1:aa:81	Spanning_tree	STP	60
31.	23,51	40.40.40.3	10.10.10.2	TCP	66
32.	24,00	Fe80:e010:c683:5106:f3e8	Ff02::c	SSDP	208
33.	24,03	Cisco_e1:aa:81	Spanning_tree	STP	60
34.	25,22	ASUSTEkC_9d:86:8a	Cisco_00:e3:e1	ARP	42
35.	25,23	Cisco_00:e3:e1	ASUSTEkC_9d:86:8a	ARP	60
36.	26,03	Cisco_e1:aa:81	Spanning_tree	STP	60
37.	27,00	Fe80:e010:c683:5106:f3e8	Ff02::c	SSDP	208
38.	27,50	40.40.40.3	10.10.10.2	SIP/SDP	1095
39.	27,50	10.10.10.2	40.40.40.3	SIP	284
40.	28,30	40.40.40.3	10.10.10.2	SIP	831
41.	30,25	10.10.10.2	40.40.40.3	RTP	214
42.	31,50	40.40.40.3	10.10.10.2	RTP	214
43.	31,75	10.10.10.2	40.40.40.3	RTP	214

 ISBN 978-86-7466-930-3

IV. ZAKLJUČAK

Rezultat jedne realizacije zaštite paketskog telefonskog saobraćaja, predstavljen u ovom radu prikazuje da uspostava i održavanje VPN tunela kao načina zaštite paketskog telefonskog saobraćaja podrazumeva primenu niza protokola, specifično dizajniranih za prenos informacionih sadržaja u realnom vremenu (SIP, SSDP, RTP) kao i protokola za obezbeđenje zaštite u toku prenosa (ISAKMP, IPSec). Specifično za predstavljenu realizaciju predstavlja upotreba linka za prenos različitih servisa i time korišćenje protokola kojima se omogućava konvergencija servisa u prenosu (DTP, SSDP).

LITERATURA

[1] W.Stallings, Osnove bezbednosti mreža: Aplikacije i standardi, Računarski fakultet, Beograd, 2014.
[2] M.Stojanović, V.Aćimović-Raspopović, Savremene IP mreže: Arhitekture, tehnologije i protokoli, Akademska misao, Beograd, 2012.
[3] A.Smiljanić, Osnove i primena Interneta, Elektrotehnički fakultet Univerziteta u Beogradu, Beograd, 2015.
[4] D.Nemec, D.Vukobratović, V.Crnojević, Č.Stefanović, Tehnologija VoIP sistema, Fakultet tehničkih nauka, Novi Sad, 2007.
[5] Security in the Internet Architecture, RFC: 1636, jun 1994, https://datatracker.ietf.org/doc/html/rfc1636
[6] IP Encapsulating Security Payload, RFC: 4303, decembar 2005, https://datatracker.ietf.org/doc/html/rfc4303
[7] Security Architecture for the Internet protocol, RFC: 4301, decembar 2005, https://datatracker.ietf.org/doc/html/rfc4301
[8] Internet Security Association and key Management Protocol, RFC: 2408, novembar 1998, https://datatracker.ietf.org/doc/html/rfc2408
[9] Internet Key Exchange Protocol Version 2 (IKEv2), RFC: 5996, septembar 2010, https://datatracker.ietf.org/doc/html/rfc5996
[10] B.Scheiner, Primenjena kriptografija, Mikro knjiga, Beograd, 2007.
[11] R.Swale, D.Collins, Carrier Grade Voice Over IP, McGraw Hill Professional, 2004.
[12] M.Jevtović, Komunikacioni protokoli Interneta, Akademska misao, Beograd, 2011.
[13] I.Bašičević, "Prilog razvoju arhitekture za obezbeđivanje usluga u računarskim mrežama nove generacije", doktorska disertacija, Fakultet tehničkih nauka, Novi Sad, 2008.
[14] S.Gajin , Principi konfigurisanja računarskih mreža, Akademska misao, Beograd, 2018.

ABSTRACT

The research presented in this paper addresses an example of how to execute packet telephone traffic protection using virtual private network technology through configuring servers for packet telephone traffic and also demonstrates the secure transfer with the use of virtual private network technology in tunnel mode by applying the appropriate protocols for privacy protection, authentication, integrity protection and crypto key exchange. Traffic recording and analysis has been performed using the Wireshark software in both secure and non-secure transfer. The results obtained can help better understand the complex process of setting up a tunnel through the use of simulation software in education.

Packet Telephone Traffic Transfer Protection Using Technology of Virtual Private Networks

Mićo Živanović, Jovan Bajčetić, Ivan Tot

 ISBN 978-86-7466-930-3