



UNIVERZITET SINGIDUNUM

**-MASTER STUDIJSKI PROGRAM-
SAVREMENE INFORMACIONE TEHNOLOGIJE**

Uticaj izbora kripto algoritma na performanse IPSec VPN tunela

- Master rad -

Mentor:
Prof. dr. Mladen Veinović

Student:
Radovan Dragović, spec.
Br.indeksa 410454/2014



Beograd, 2017

Uticaj izbora krypto algoritma na performanse IPSec VPN tunela

Sažetak: U radu je predstavljeno istraživanje čiji je cilj bio da odgovori na pitanje kakav je uticaj krypto algoritama na performanse VPN tunela, konkretno - razlika u performansama IPSec VPN tunela pri upotrebi 3DES u odnosu na AES šifarski sistem. Pored teorijskih objašnjenja različitih pojmova (TCP/IP model, protokoli transportnog sloja, protokol interneta, šifarski sistemi, specifične kriptografske (heš) funkcije, VPN tunelovanje) opisan je eksperiment tokom kog su u laboratorijskim uslovim izmerene performanse mreže. Istraživanjem se došlo do zaključka da, za pojedine protokole, postoji merljiva razlika u performansama mreže i da ista može da ima uticaj na rad pojedinih servisa .

Ključne reči: IPSec, Throughput, 3DES, AES, TCP.

Crypto algorithm influence on IPSec VPN tunnel performance

Abstract: In this paper one will find a description of a research answering a question on crypto algorithm's influence on VPN network's performance. Specifically - 3DES's compared to AES's influence on an IPSec VPN performances. Besides theoretical explanations on different subjects (TCP/IP model, transport layer protocols, internet layer protocol, cryptographic systems, specific cryptographic (hash) functions, VPN tunneling) one can find an experiment evaluating network performance in a laboratory environment. The research led to a conclusion that, for some protocols, there is a difference in performance influences and that the difference might effect specific network services.

Keywords: IPSec, Throughput, 3DES, AES, TCP.

SADRŽAJ

1. Metodologija	1
1.1 Uvodne napomene	1
1.2 Problem istraživanja	1
1.3 Predmet istraživanja	2
1.4 Hipoteza.....	2
1.5 Ciljevi istraživanja.....	2
1.6 Naučne metode	2
2. Uvod	3
3. TCP/IP referentni model.....	4
4. Protokoli transportnog sloja.....	6
4.1 Transmission Control Protocol (TCP).....	7
4.2 User Datagram Protocol (UDP).....	9
5. Protokol internet sloja - IP protokol verzije 4	11
6. Šifarski sistemi	12
6.1 Data Encryption Standard (DES) šifarski sistem	13
6.2 Advanced Encryption Standard (AES) šifarski sistem.....	15
6.3 Triple Data Encryption Standard (3DES) šifarski sistem.....	16
6.4 Poređenje DES, 3DES i AES šifarskih sistema.....	17
7. Kriptografske heš funkcije -SHA.....	18
8. Diffie-Hellman (DH) protokol	19
9. Internet Protocol Security (IPSec) skup protokola	20
9.1 Internet Key Exchange - IKE	21
9.2 Transportni režim i režim tunelovanja.....	23
9.3 Authentication Header (AH) i Encapsulating Security Payload (ESP).....	23
10. Postavka eksperimenta	27
10.1 Fizička topologija i korišćena oprema.....	27

10.2 Specifikacija softvera	28
10.3 Smer prenosa, korišćeni protokoli i metod enkripcije	29
10.3.1 Konfigurisanje smera prenosa i izbor protokola.....	30
10.3.2 Konfigurisanje parametara TCP protokola	31
10.3.3 Konfigurisanje parametara UDP protokola	34
10.3.4 Konfigurisanje krypto parametara	35
11. Tok eksperimenta	39
12. Prikupljanje, način obrade i analiza podataka.....	42
12.1 Prikupljanje podataka	42
12.2 Način obrade podataka	44
13. Rezultati eksperimenta	46
14. Zaključak.....	53
Literatura	54

1. Metodologija

1.1 Uvodne napomene

U prethodnom periodu, tokom proučavanja materijala koji se odnose na implementaciju mehanizama zaštite podataka na mrežama za prenos podataka, stekao sam utisak da, iako to u konkretnim materijalima nije eksplicitno navedeno, mehanizmi zaštite utiču na degradaciju karakteristika mreža.

Naročito su mi se interesantnim učinili VPN tuneli zbog sveprisutnosti u različitim mrežama i zbog široke lepeze servisa za čije potrebe se implementiraju, kao i pitanje u kojoj meri se razlikuju karakteristike mreže u zavisnosti od mehanizama enkripcije koji se u pomenutim tunelima koriste.

Ovo istraživanje se bavi uticajem mehanizama zaštite informacija, konkretno kriptografskih algoritama, na performanse (karakteristike) IPSec VPN tunela.

Sprovodi se da bi se utvrdilo na koje karakteristike mreže i u kojoj meri utiču pomenuti mehanizmi zaštite.

1.2 Problem istraživanja

Savremene komunikacije je nemoguće zamisliti bez mreža za prenos podataka baziranih na TCP/IP protokol stacku (eng. *protocol stack*: skup protokola). Činjenica da ovaj skup protokola ne obezbeđuje poverljivost, integritet i neporecivost štićenih sadržaja dovela je do razvoja mehanizama koji to čine.

Navedene tri komponente se, bazično, obezbeđuju upotrebom sledećih, osnovnih, mehanizama: šifarskih algoritama (za poverljivost), algoritama za hash-ovanje (za integritet, neporecivost i autentikaciju). Dalji razvoj i varijacije osnovnih mehanizama, njihovo kombinovanje, kreiranje i razvoj protokola za bezbednu komunikaciju, prpratni protokoli (za razmenu ključeva i slično) su doveli do pojave kompleksnijih mehanizama koji omogućavaju zaštitu podataka u različitim situacijama (različitim mrežnim topologijama sa različitim servisima).

VPN-ovi su jedan od kompleksnijih mehanizama koji omogućava bezbednu komunikaciju kroz druge - nezaštićene komunikacione mreže. Različita softverska i hardverska rešenja omogućavaju formiranje VPN tunela, baziranih na različitim protokolima.

Protokoli za formiranje VPN tunela (s obzirom na prisutnu enkripciju, hash-ovanje i enkapsulaciju) uslovljavaju dodatno angažovanje softverskih i/ili hardverskih resursa i povećavaju količinu saobraćaja dodatnim zaglavlјima. Pored navedenog, mehanizmi enkripcije ostvaruju uticaj angažujući hardverske i softverske resurse pojedinih mrežnih elemenata.

Za očekivati je da će VPN tunel u kom je primenjen zahtevniji algoritam za enkripciju imati lošije performanse nego u slučaju korišćenja manje zahtevnog algoritma.

Postavlja se pitanje da li i u kojoj meri dolazi do degradacije performansi.

Po ovom i sličnim pitanjima vršena su istraživanja i ista su realizovana kroz eksperimente sa različitim postavkama (različite topologije, hardversko-softverske platforme), različitim metodologijama merenja (razlike u mernim aplikacijama), korišćenjem različitih opštih protokola, mehanizama za kriptovanje i da su merene različite performanse mreža.

Ovo istraživanje je značajno zato što će utvrditi razliku u uticajima pojedinih mehanizama zaštite, na karakteristike mreže. Samim tim, omogućiće predviđanje uticaja primenjenih mehanizama zaštite na prenos podataka određenih tipova. Ovi podaci mogu da posluže kao smernice projektantima mreže u procesu izbora mehanizama zaštite, odnosno istraživačima kao jedan od validnih elemenata za buduća istraživanja.

1.3 Predmet istraživanja

Predmet ovog istraživanja jeste razlika u performansama IPSec VPN tunela (kao mreže za prenos podataka) u zavisnosti od primenjenog krypto algoritma. Istraživanje obuhvata opis protokola za prenos podataka, metoda za hash-ovanje, autentikaciju i kriptovanje, protokola za formiranje VPN tunela, zatim realizaciju eksperimenta, obradu i analizu podataka, izbor metodologije merenja, eksperimentalnu proveru uticaja izvođenje zaključaka.

1.4 Hipoteza

Opšta hipoteza: Performanse mreže za prenos podataka na kojoj je primenjen VPN tunel se razlikuju u zavisnosti od primenjenog mehanizma enkripcije.

Posebne hipoteze:

Performanse mreže za prenos podataka na kojoj je primenjen VPN tunel su niže ukoliko je primenjeni mehanizam enkripcije kompleksniji.

Degradacija performansi nastala na ovaj način, može da dovede do nemogućnosti korišćenja pojedinih servisa preko mreže za prenos podataka.

Degradacija performansi nema isti praktičan uticaj na sve tipove podataka i servisa.

1.5 Ciljevi istraživanja

Naučni cilj: Kroz ovo istraživanje biće opisani i ispitan uticaj izabranog mehanizama enkripcije na performanse prenosa podataka kroz IPSec VPN tunel. Dodatno, istraživanje će omogućiti naučno predviđanje uticaja pomenutih mehanizama na performanse mreže.

Praktični cilj: Podaci dobijeni istraživanjem mogu da posluže kao smernice projektantima mreže u izboru mehanizama zaštite koji neće degradirati performanse mreže ispod zahtevanog nivoa. Pored navedenog, drugim istraživačima će se obezbediti podaci koji mogu da služe za buduća istraživanja.

1.6 Naučne metode

Radi sprovođenja istraživanja primenjene su slede naučne metode: analiza sadržaja (primenjena na materijalima koji se odnose na opis pojmova i implementaciju VPN tunela), indukcija, dedukcija, analiza (tokom izbora mehanizama čiji uticaj će se razmatrati, izbora metodologije merenja i postavke eksperimenta), modelovanje i eksperiment. U izvođenju zaključaka primenjuju se metode sinteze i generalizacije.

2. Uvod

"Računarska mreža može biti prost skup dva ili više računara, koji su povezani adekvatnim medijumom i koji međusobno mogu da komuniciraju i dele resurse. Koristi se za prenos kako digitalnih tako i analognih podataka, koji moraju biti prilagođeni odgovarajućim sistemima za prenos. Mrežom se prenose računarski podaci, govor, slika, video, a aplikacije na stranama korisnika mogu biti takve da se zahteva prenos podataka u realnom vremenu (govor, video i sl.) ili to ne mora biti uslov (elektronska pošta, prenos datoteka i sl.). Mreža se sastoji od računara, medijuma za prenos (žica, optičko vlakno, vazduh i sl.) i uređaja kao što su čvorišta, svičevi, ruteri itd. koji čine infrastrukturu mreže. Neki od uređaja, kao što su mrežne kartice, omogućavaju vezu između računara i mreže."¹

Koreni računarskih mreža se vezuju za pojavu ARPANET-a² sedamdesetih godina prošlog veka. Sada, u 21.-om veku, kada spomenemo ovu sintagmu, misli se na milione kućnih, akademskih, poslovnih i vladinih mreža povezanih u globalnu, svetsku mrežu ili izolovanih, radi obezbeđenja komunikacije u zatvorenim sistemima.

Komunikacija između korisnika računarskih mreža je bazirana na TCP/IP skupu protokola koji je "...de facto standard..² kada je reč o savremenim računarskim mrežama. TCP/IP omogućava implementaciju protokola i protokol stackova štite podatke od zloupotrebe od strane entiteta koji ne učestvuju u komunikaciji.

Različiti mehanizmi zaštite su razvijeni upravo sa ovim ciljem - zaštita informacija. Jedan od mehanizama zaštite, koji je deo ovog istraživanja jeste IPSec VPN tunel.

U poglavljima 1, 2, 3, 4, 5, 6, 7, 8 i 9 su opisani: TCP/IP skup protokola (referentni model), protokoli transportnog sloja (TCP i UDP), protokol internet sloja (IP), šifarski sistemi, kriptografske hash funkcije, protokoli koji obezbeđuju zaštitu IP paketima i IPSec VPN tuneli. U poglavljima 10 i 11 opisani su postavka i tok eksperimenta. Način prikupljanja i obrade i analiza podataka su predmet poglavlja 12. Rezultati eksperimenta i interpretacija rezultata su dati u poglavlju 13.

¹ M. Veinović, A. Jevremović, **Uvod u računarske mreže**, Univerzitet Singidunum, Beograd, 2007.

² "ARPANET, in full Advanced Research Projects Agency Network, experimental computer network that was the forerunner of the Internet. The Advanced Research Projects Agency (ARPA), an arm of the U.S. Defense Department, funded the development of the Advanced Research Projects Agency Network (ARPANET) in the late 1960s. Its initial purpose was to link computers at Pentagon-funded research institutions over telephone lines." ; **ARPANET, United States defense program**, Enciclopedia Britannica, <https://www.britannica.com/topic/ARPANET>, (pristup 17.03.2017.godine)

3. TCP/IP referentni model

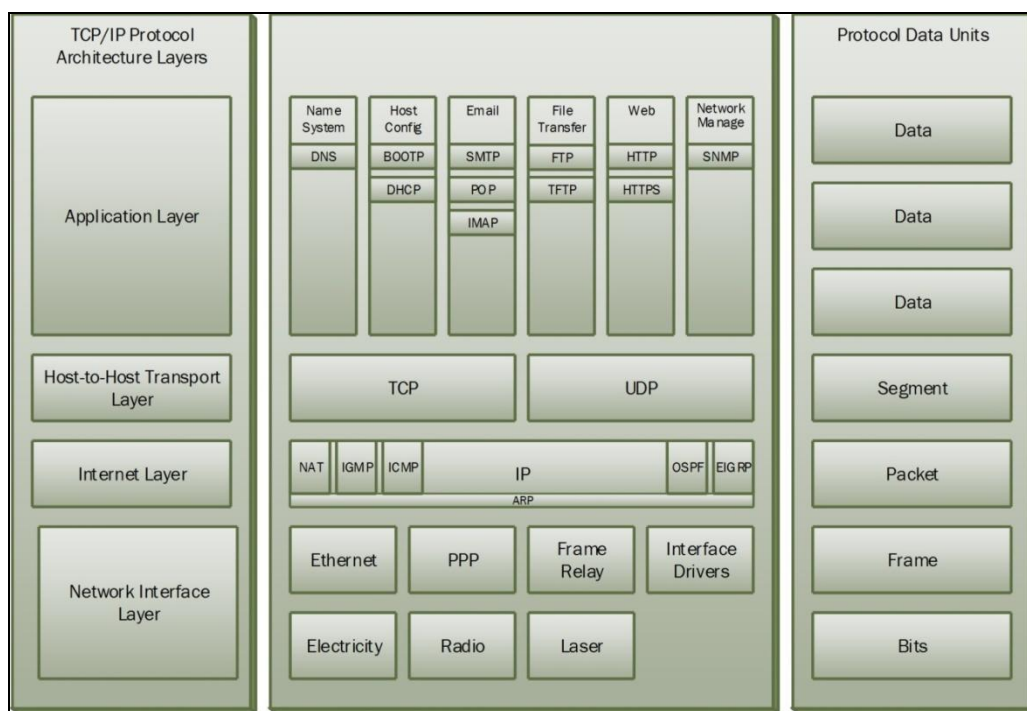
U ovom poglavlju opisan je TCP/IP model prenosa podataka.

Pojam TCP/IP (Eng.: *Transmission Control Protocol /Internet Protocol*) se odnosi na jedan od dva modela kojima se opisuje prenos podataka u računarskim mrežama. U literaturi na engleskom jeziku koristi se još i termin *IP Protocol Suite*, odnosno "skup IP protokola". Pored ovog modela koristi se i takozvani OSI model (Open Systems Interconnection model).

Na TCP/IP modelu je, u najvećoj meri, baziran prenos podataka u lokalnim mrežama, kao i na Internetu.

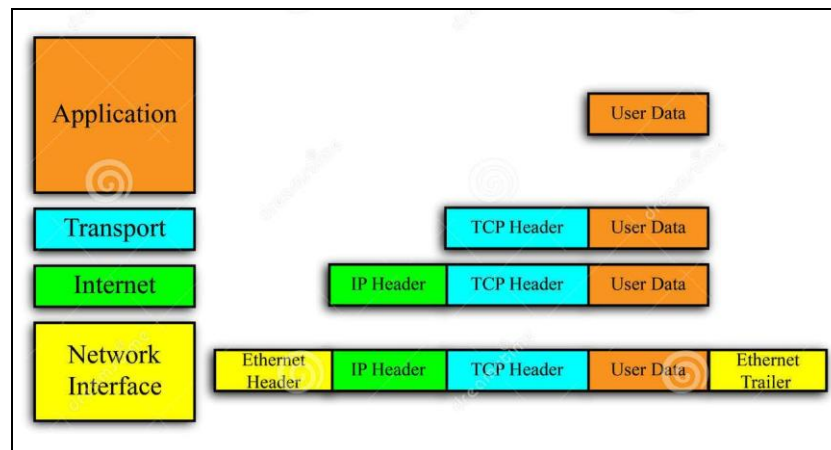
Za razliku od OSI modela koji definiše 7 slojeva (eng. *layer*), TCP/IP model prepoznaje 4 sloja: aplikacije, transportni, internet i mrežni (eng. *application, transport, internet, network*). Iako se u nazivu spominju dva (Transmission Control i IP protocol) ovaj model obuhvata više protokola. Podaci se prenose od jednog do drugog sloja koji im dodaju (u slučaju slanja) odn. oduzimaju (u slučaju prijema) sopstvene dodatke - zaglavlja (headers). Ovaj proces naziva se enkapsulacija (dodavanje) odnosno de-enkapsulacija (oduzimanje zaglavlja). U zavisnosti od toga na kom se sloju podaci (Protocol Data Units) nalaze, referenciraju se kao Data, Segment, Packet, Frame ili Bit.

Slojevi, protokoli, PDU i proces enkapsulacije su prikazani na slikama 1 i 2.



Slika 1: TCP/IP model³

³ preuzeto sa <https://www.pinterest.com/nebougezplus/osi> (datum pristupanja 16.03.2017.godine)



Slika 2: Enkapsulacija podataka na primeru TCP-IP-Ethernet kombinacije protokola⁴

TCP/IP model je opisan na osnovu [1].

⁴ Preuzeto sa <https://www.dreamstime.com> (datum pristupanja 16.03.2017.godine)

4. Protokoli transportnog sloja

U ovom poglavlju opisane su osnovne karakteristike i funkcije protokola transportnog sloja. Isto je izrađeno na osnovu [2].

Suštinska uloga protokola transportnog sloja jeste uspostava privremene sesije (pojedinačne komunikacije) između dve aplikacije i razmena podataka među njima. Podaci se šalju od aplikacije izvornog do aplikacije odredišnog hosta (eng. *host*). Ovaj proces se realizuje bez obzira na tip hosta, vrstu medija, putanju, zagušenje linka, ili veličinu mreže.

Osnovna razlika između dva protokola ovog sloja (TCP i UDP) jeste pouzdanost u isporuci podataka. TCP obezbeđuje sigurnu isporuku podataka, dok UDP ne garantuje istu. U zavisnosti od prirode aplikacije višeg sloja, koristiće se jedan ili drugi protokol transportnog sloja.

Protokoli transportnog sloja segmentiraju i numerišu podatke dobijene od sloja aplikacije. Ovim se obezbeđuje pravilan redosled podataka koji se od transportnog sloja (kroz proces de-segmentacije) prosleđuju sloju aplikacije odredišta.

Osnovne funkcije protokola transportnog sloja su:

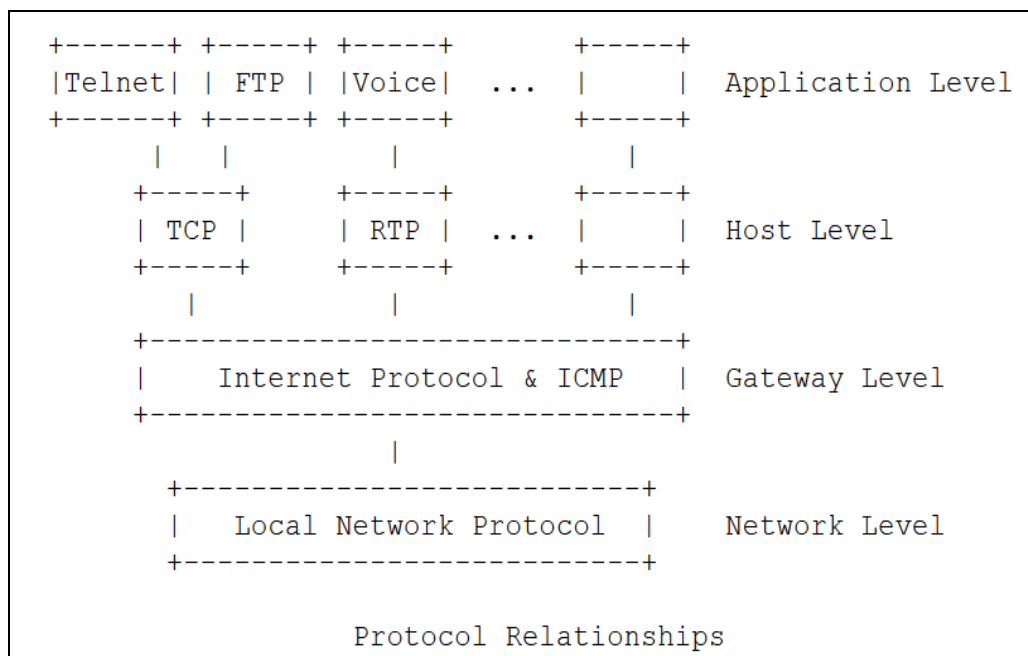
- Praćenje sesija između aplikacija na izvoru i na odredištu
Ova funkcija je značajna zbog vremenskog preplitanja (multipleksiranja) segmenata podataka u sesijama između različitih parova aplikacija na izvoru i odredištu (ili odredištima) komunikacije.
- Segmentacija podataka
Većina mreža ima ograničenje po pitanju količine podataka koja se može poslati u jednom paketu. Protokoli transportnog sloja dele (segmentiraju) podatke dobijene od aplikacija u blokove podataka (segmente) odgovarajuće veličine (slika 2). Pored procesa segmentacije, vrši i enkapsulaciju. Enkapsulacija podrazumeva dodavanje zaglavlja protokola transportnog sloja svakom bloku podataka. Zaglavlja obezbeđuju ponovno sklapanje na izvoru, odnosno, praćenje toka podataka. Transportni sloj, na odredištu, mora biti u stanju da rekonstruiše delove podataka tako da sloj aplikacije može da ih iskoristi. Protokoli na transportnom sloju opisuju kako se informacije iz zaglavlja koriste za spajanje rasutih delova podataka radi pravilne isporuke sloju aplikacije.
- Identifikacija odgovarajućih aplikacija za svaku pojedinačnu sesiju.
Na svakom hostu u mreži može biti više aktivnih aplikacija i servisa (eng. *services*). Transportni sloj mora da identifikuje ciljnu aplikaciju da bi joj prosledio odgovarajuće podatke. U tom cilju, svakoj aplikaciji dodeljuje identifikator. Ovaj identifikator se zove broj porta (eng. *port number*). Svakom softverskom procesu koji pristupa mreži se dodeljuje broj porta jedinstven za tog hosta. Transportni sloj koristi portove da bi identifikovao aplikaciju ili servis.
Port, u ovom slučaju, predstavlja jedinstvenu "adresu" aplikacije, odnosno servisa na hostu.

Protokoli transportnog sloja mogu biti:

- pouzdani (TCP) i
- nepouzdani (UDP).

Ova karakteristika predstavlja osnovu razliku između navednih protokola.

U zavisnosti od procesa na sloju aplikacije za čije potrebe se realizuje prenos podataka, koristiće se jedan ili drugi protokol transportnog sloja. Slika 3 ovo ilustruje.



Slika 3: Veza TCP/UDP protokola sa protokolima drugih slojeva⁵

4.1 Transmission Control Protocol (TCP)

TCP protokol transportnog sloja je u potpunosti opisan u IETF RFC 793 [3]. Kao što je ranije navedeno, smatra se pouzdanim transportnim protokolom što znači da obezbeđuje sigurnu isporuku podataka između aplikacija korišćenjem potvrde prijema (eng. *acknowledged delivery*).

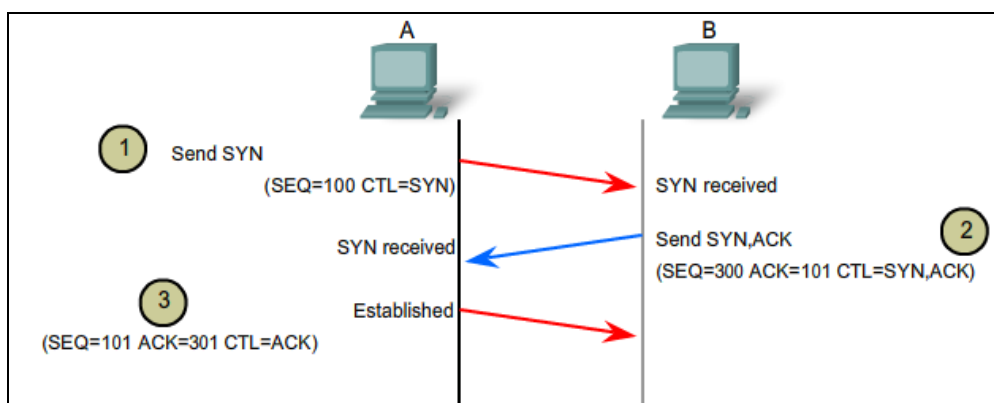
Osnovne operacije koje obezbeđuju pouzdanost su:

- Praćenje segmenata;
TCP numeričke segmente i prosleđuje ih IP protokolu radi formiranja paketa. Vodi evidenciju o broju segmenata koji su poslani ka konkretnom hostu i aplikaciji na njemu.
- Potvrda prijema podataka;
Odredišni host šalje potvrdu prijema za ispravno primljene pakete.
- Ponovno slanje podataka za koje nije dobijena potvrda prijema;
Ako pošiljalac ne primi potvrdu u određenom vremenskom periodu, pretpostavlja da su segmenti izgubljeni i reemituje ih. Šalje se samo deo poruke koji se izgubio, ne cela poruka.

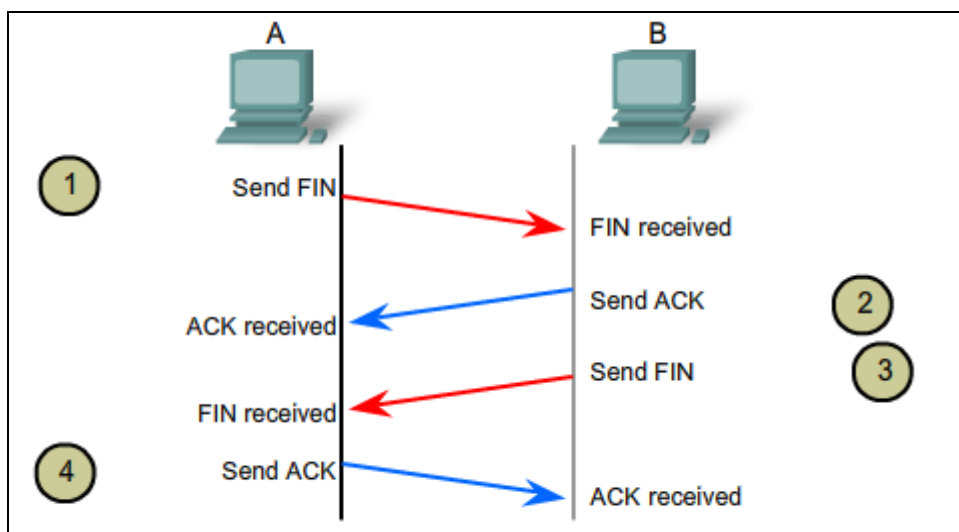
⁵Preuzeto iz [3]

Ove operacije utiču na pojavu dodatnih podataka (kontrolni podaci u zaglavlju) koji se šalju (eng. *overhead*). Kontrolni podaci, odn. zaglavlja, ovog i drugih protokola zauzimaju deo resursa mreže namenjenih za prenos podataka koji čine informacije potrebne aplikacijama i procesima viših slojeva.

Pored overheada i korisničkih podataka, kod ovog protokola, prisutna je razmena poruka namenjenih za uspostavu (SYN, SYN-ACK, ACK), održavanje i prekid sesija (FIN). Proces uspostave (tzv. three way handshake) i prekida sesije ilustrovani su slikama 4 i 5.



Slika 4: TCP - uspostava sesije⁶

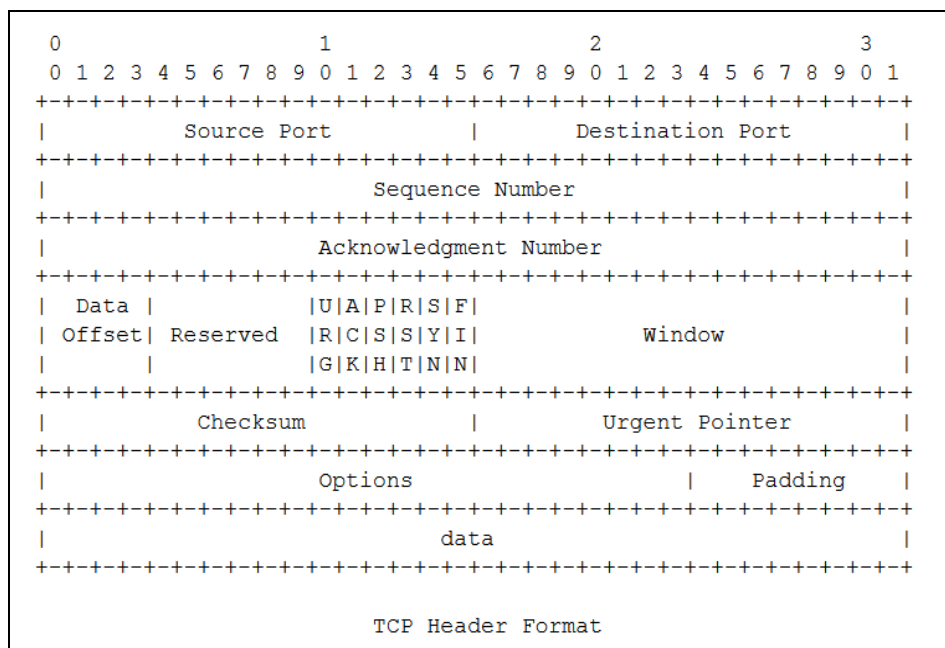


Slika 5: TCP -prekid sesije⁷

Izgled zaglavlja TCP protokola sa podacima protokola viših slojeva (data) prikazan je na slici 6.

⁶ Preuzeto iz [2]

⁷ Preuzeto iz [2]

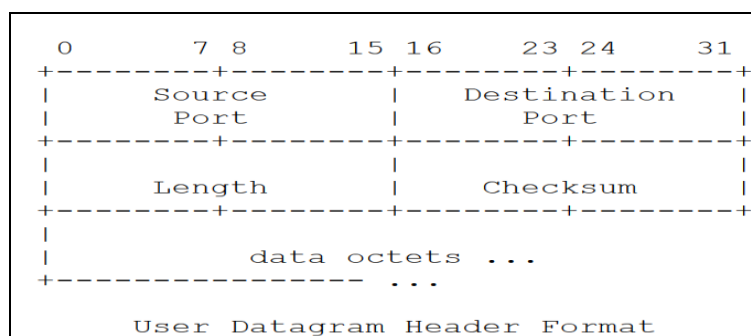
Slika 6: TCP paket⁸

4.2 User Datagram Protocol (UDP)

Još jedan protokol transportnog sloja značajan za ovo istraživanje jeste UDP. Ovaj je jednostavan protokol koji obezbeđuje osnovne funkcije transportnog sloja je opisan u IETF RFC 768 [4]. Za razliku od TCP protokola, ne obezbeđuje sigurnu isporuku niti originalan redosled podataka koji se desegmentiraju na odredištu.

Pogodan je za aplikacije koje zahtevaju brzu ili real-time isporuku podataka sa malim overhead-om. Tipične, u ovom kontekstu, su aplikacije namenjene za prenos glasa i real-time video signala. U vezi sa ovim istraživanjem treba imati u vidu da je osnovni transportni protokol za Voice over IP (VoIP) aplikacije [1].

Ima mnogo manji overhead nego TCP, zato što nije konekciono orijentisan, odnosno zato što ne poseduje mehanizme reemitovanja, sekvenciranja i kontrole protoka koji pružaju pouzdanost. Izgleda datagrama ovog protokola prikazan je na slici 7.

Slika 7: UDP paket⁹

⁸ Preuzeto iz [3]

U ovom istraživanju, tokom eksperimenta, izvršeno je merenje performansi prenosom paketa UDP / VoIP. Način funkcionisanja VoIP servisa neće biti detaljno opisan. U ovom kontekstu dovoljno je ovaj tip prenosa (UDP/VoIP) posmatrati kao unidirekcionu prenos UDP paketa konstantnom brzinom 64 kbps.

⁹ Preuzeto iz [4]

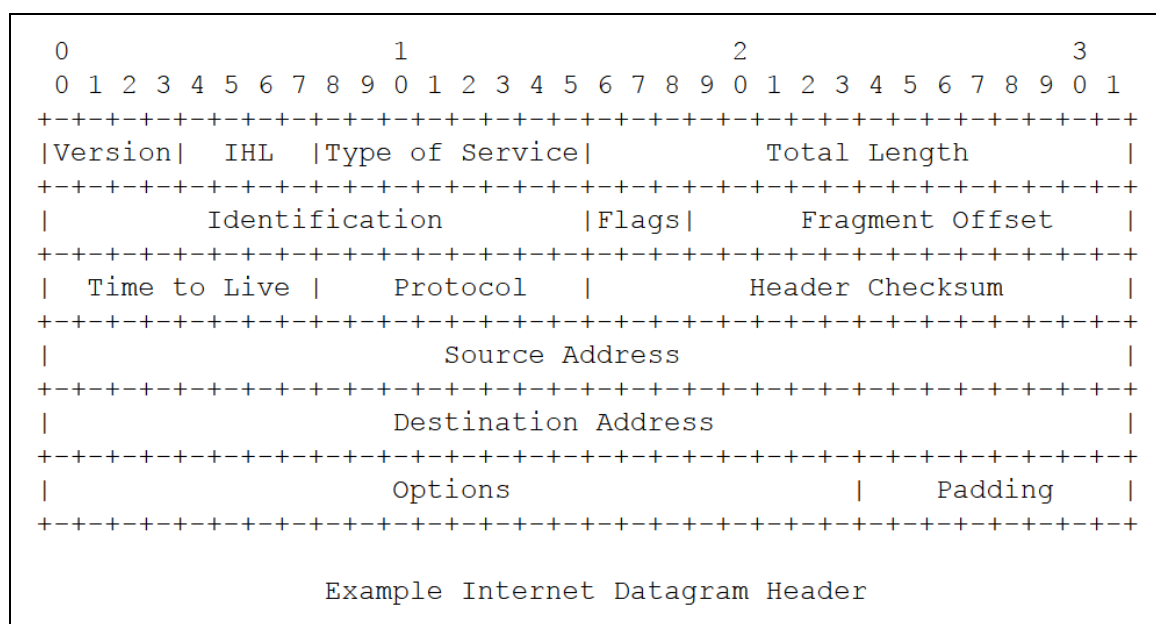
5. Protokol internet sloja - IP protokol verzije 4

IPv4 je u potpunosti opisan u IETF RFC 791 [5]. U ovom poglavlju je dat kratak opis istog, a na osnovu pomenute literature.

Pored toga što postoji više protokola ovog sloja, u upotrebi su isključivo Internet protokol verzije 4 (IPv4) i Internet protokol verzije 6 (IPv6). U ovom istraživanju će se razmatrati IPv4.

Ovaj protokol formira pakete vršeći enkapsulaciju segmenata dobijenih od transportnog sloja (u predajnom), odnosno de-enkapsulaciju okvira (eng. *frames*) primljenih od sloja mreže (eng. *network layer*).

Osnovna funkcija ovog protokola jeste da obezbedi logičko adresiranje paketa podataka što omogućava njihovo usmeravanje (eng. *routing*) kroz mrežu za prenos podataka. Osim (IP) adrese, prisutni su i drugi podaci koji nisu od značaja za ovo istraživanje. IPv4 paket prikazan je na slici 8.



Slika 8: Izgled IPv4 paketa¹⁰

¹⁰ Preuzeto iz [5]

6. Šifarski sistemi

U prvom delu ovog poglavlja objašnjeni su osnovni pojmovi u vezi sa šifarskim sistemima, navedene su podele i opisan je Feistel model šifarskog sistema. U podpoglavljima su u osnovnim crtama opisani DES, 3DES i AES šifarski sistemi. Poglavlje se, najvećim svojim delom bazira na udžbeniku [6].

Šifrovanje (eng. *encryption*) je procedura kojom se vrednosti ulaznog podatka (**otvoreni tekst**) zamenjuje drugim vrednostima čime se dobija **šifrat**. **Dešifrovanje** (eng. *decryption*) je obrnut proces gde se od šifrata, primenom ključa za šifrovanje (kriptološkog ključa) i algoritma, dobija otvoreni tekst. Ove zamene se obavljaju na osnovu **ključa** i **algoritma**.

Šifarski sistem se, minimalno, sastoji od: algoritma za šifrovanje, algoritma za dešifrovanje i algoritma za generisanje ključa.

Prepoznamo dva, osnovna, tipa šifarskih sistema: **simetrični** i **asimetrični**. Osnovna razlika počiva na ključu. Dok se simetričnim sistemima koristi isti (simetrični) ključ za obe procedure (šifrovanje i dešifrovanje), kod asimetričnih sistema postoje dva ključa (javni - za šifrovanje, tajni - za dešifrovanje). Ovi sistemi se razlikuju po pojedinim karakteristikama pri čemu i jedni i drugi pronalaze svoje mesto u modernim kriptološkim sistemima.

Poznatiji **simetrični šifarski** sistemi su: DES, **3DES**, **AES**, RC itd., dok u asimetrične sisteme ulaze: RSA, Eliptic Curves, DSS i tako dalje.

Simetrični šifarski sistemi mogu da se podele na **sekvencijalne** i **blokove**. Za **sekvencijalne** je karakteristično da se ključem dužine n bita inicijalizuje generator pseudoslučajnog niza. Ovaj generator na svom izlazu daje niz bita (pseudoslučajnu sekvencu, radni ključ, eng. *keystream*) koji se periodično ponavlja. XOR operacijom (koja se vrši na bitima radnog ključa i otvorenog teksta) dobija se šifrat. Primeri ovog tipa šifarskih sistema su A5/1 i RC4.

Blokovski šifarski sistemi, za razliku od prethodnih, otvoreni tekst dele na blokove. Na svaki od blokova se primenjuje jedna, jedinstvena, funkcija. Ova funkcija ima različite karakteristike tokom primene na svakom, pojedinačnom, bloku. Jedna primena ove funkcije naziva se runda (eng. *round*). Razlike između funkcija rundi (funkcija šifarskog sistema koje su primenjene na jedan blok) uslovljene su ključem i izlazom iz prethodne runde. U svakoj rundi, pored funkcije runde, primenjuje se drugačiji "podključ".

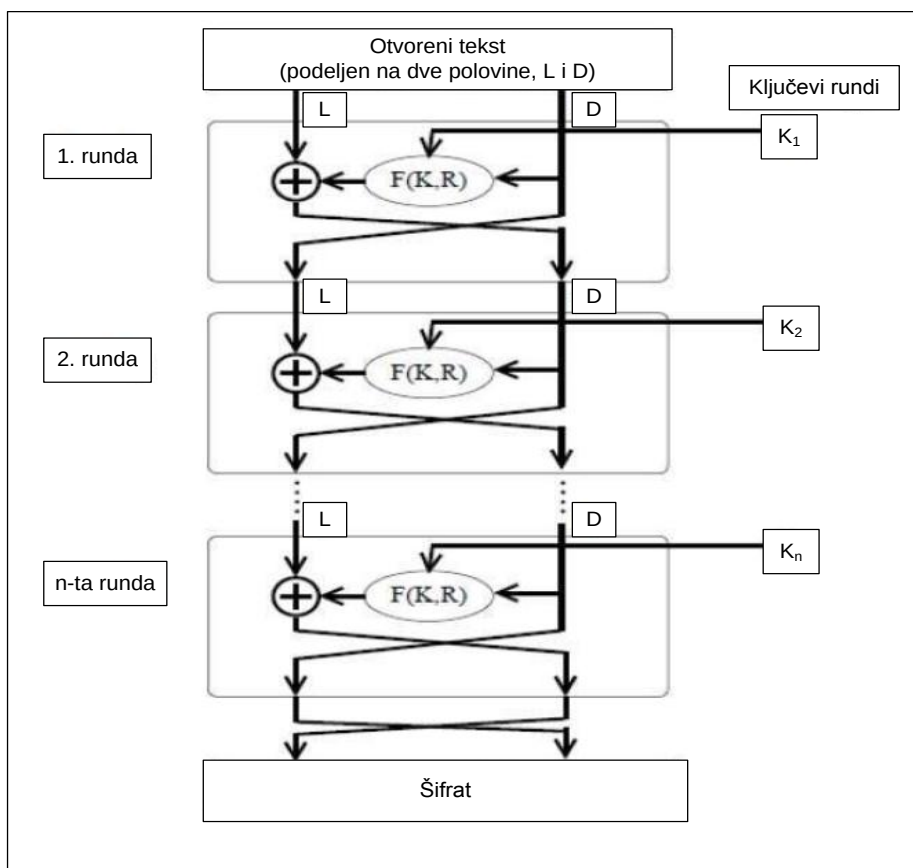
Tipični predstavnici ovog tipa šifarskih sistema su DES, **3DES**, **AES** i RC.

Princip funkcionisanja ovih sistema biće objašnjen na primeru Feistel (Feistel) šifre. Šifra koju je dizajnirao Horst Feistel (*Horst Feistel*) je, prvenstveno, model na kom su razvijani drugi blokovski šifarski sistemi.

Šifrovanje se vrši po sledećem (slika 9):

- Blok otvorenog teksta se deli na levu i desnu polovinu (L i D).
- D kroz runde prolazi nepromenjeno.

- Na L, sa druge strane, se primenjuje operacija koja zavisi od D i od ključa (K).
- Prvo se primenjuje funkcija F koja ima dva ulaza: ključ K i D. Izlaz ove funkcije je $F(D, K)$. XOR operacija se primenjuje na ovaj, $F(D, K)$, izlaz i L.
- U pravim implementacijama (DES npr.), u svakoj rundi se primenjuje "podključ" (K_1, K_2, K_n) koji predstavlja derivat originalnog (K).
- Ono što može da se primeti na slici jesu permutacije, kojima D i L u svakoj rundi menjaju mesta. Broj rundi je uslovljen algoritmom konkretnog šifarskog sistema.
- Po završetku poslednje runde L_n i D_n se spajaju u jedinstven šifrat.

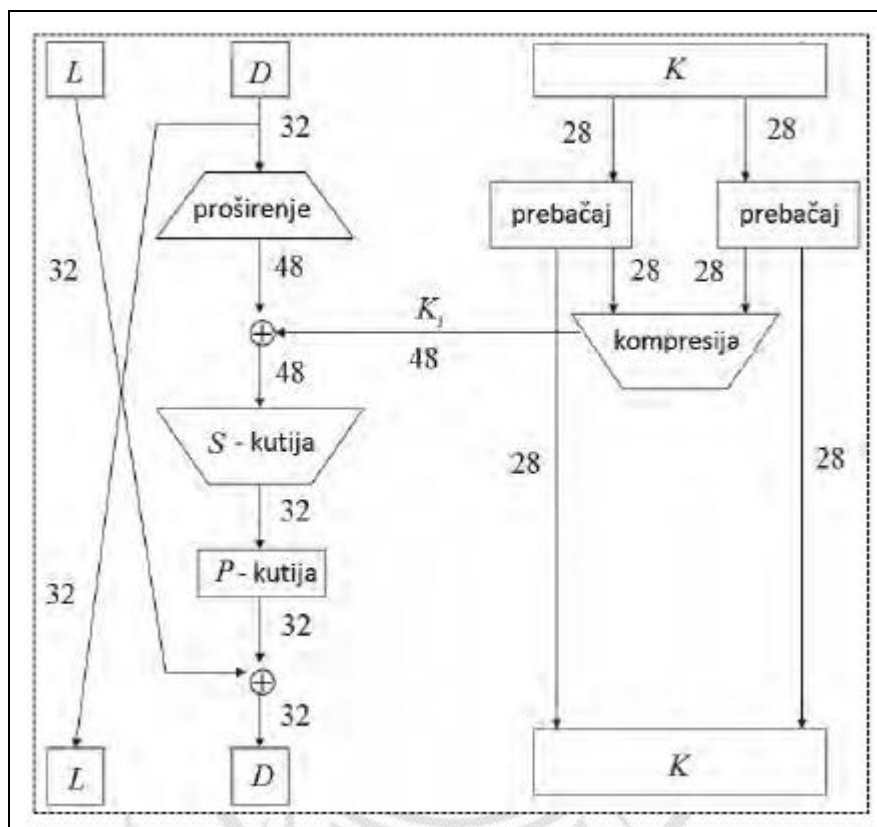
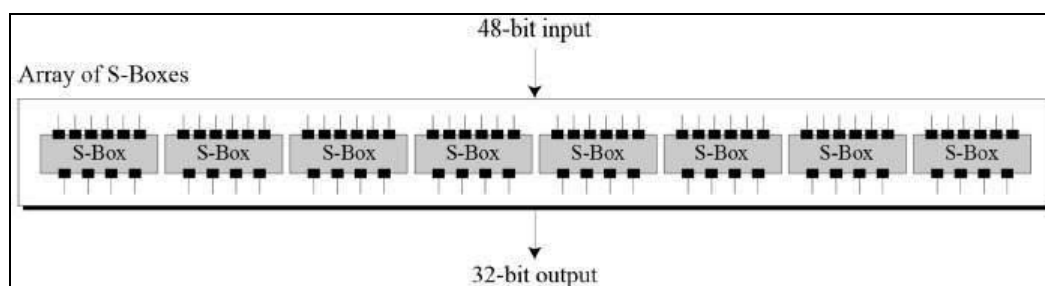
Slika 9: Fejstel šifra - struktura¹¹

6.1 Data Encryption Standard (DES) šifarski sistem

DES je baziran na Fejstel šifarskom sistemu. Koristi 16 rundi sa veličinom bloka od 64 bita. Iako je ključ dužine 64 bita, algoritam koristi prvih 56. Koristi 16 podključeva (za svaku rundu po jedan) baziranih na početnom ključu.

¹¹ Preuzeto sa https://www.tutorialspoint.com/cryptography/feistel_block_cipher.htm (datum pristupanja 28.03.2017.godine) i dodatno obrađeno

DES šifarski sistem (slika 10) deli blokove od 64 bita na L (32 bit) i D (32 bit). L i D proširuje na 48 bitne u kutiji za proširenje (eng. *P-box*). 48 bitni izlaz iz P-boxa se XOR-uje sa 48 bitnim ključem (K_i) i ovako dobijen blok se dovodi na ulaz 8 S-kutija (slika 11). Na svaku od njih se dovodi po 6 bita 48-bitnog bloka. Na izlazu svake od ovih se dobija 4 bita, što u zbiru (na izlazu iz grupe S-kutija,) daje blok od 32 bita. Grupa S-kutija vrši kompresiju i supstituciju (48 ulaznih u odnosu na 32 izlazna bita) i predstavlja jednu od najvažnijih komponenti DES-a. Po izlazu iz S-kutije, 32 bita (D) se XOR-uje sa (nepromenjenim) L i ostaje na desnoj poziciji. Na levu poziciju se postavlja početni (nepromenjeni) D blok podatka. Ovim je jedna runda završena.

Slika 10: DES - algoritam¹²Slika 11: DES - Sbox¹³¹² Preuzeto iz [6]¹³ Preuzeto sa https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm (datum pristupanja 28.03.2017.godine)

Kako je opisano u [6], razvoj tehnologije (tokom 90-ih godina prošlog veka) , doveo je do toga da je dužina ključa primenjenog u DES šifarskom sistemu postala nedovoljna. Iz tog razloga pojavio se novi šifarski sistem pod nazivom AES.

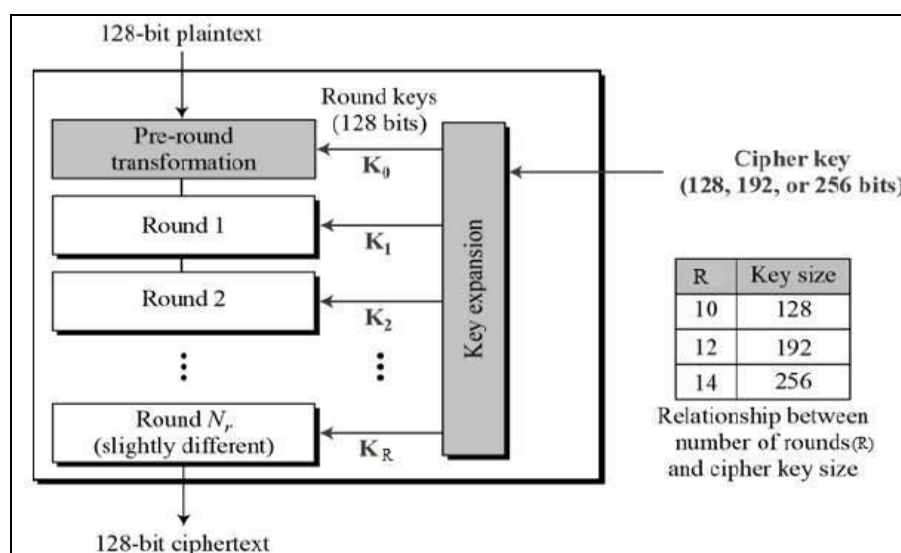
6.2 Advanced Encryption Standard (AES) šifarski sistem

AES je baziran na "Rijndael" algoritmu, odnosno ne koristi Feistel šifarskom sistemu na kom je baziran DES. AES je razvijen kako bi se zamenio DES. Ovaj algoritam je predstavljao rešenje sa dužim ključevima, većom brzinom i višom kriptografskom vrednošću.

Osnovne karakteristike ovog algoritma su:

- blokovi teksta su dužne 128, 192 ili 256 bit,
- ključ od 128, 192 ili 256 bit,
- broj rundi je od 10 do 16 (zavisi od dužine ključa),
- dužina ključa ne zavisi od veličine blokova otvorenog teksta,
- podatke obrađuje na nivou bajta (byte), ne bita (karakteristično za DES) i
- u svakoj rundi koristi četiri funkcije:
 - ByteSub,
 - ShiftRow,
 - MixColumns i
 - AddRoundKey.

Šematski prikaz AES-a dat je na slici 12.



Slika 12: AES - šematski prikaz¹⁴

¹⁴ Preuzeto sa https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm (datum pristupanja 28.03.2017.godine)

Bez obzira na, očigledne, kvalitete ovog šifarskog sistema, prelazak na novi algoritam (sa DES na AES), globalno gledano, predstavljao je finansijski zahtevan potez. Iz tog razloga se nije odustalo od DES-a.

6.3 Tripple Data Encryption Standard (3DES) šifarski sistem

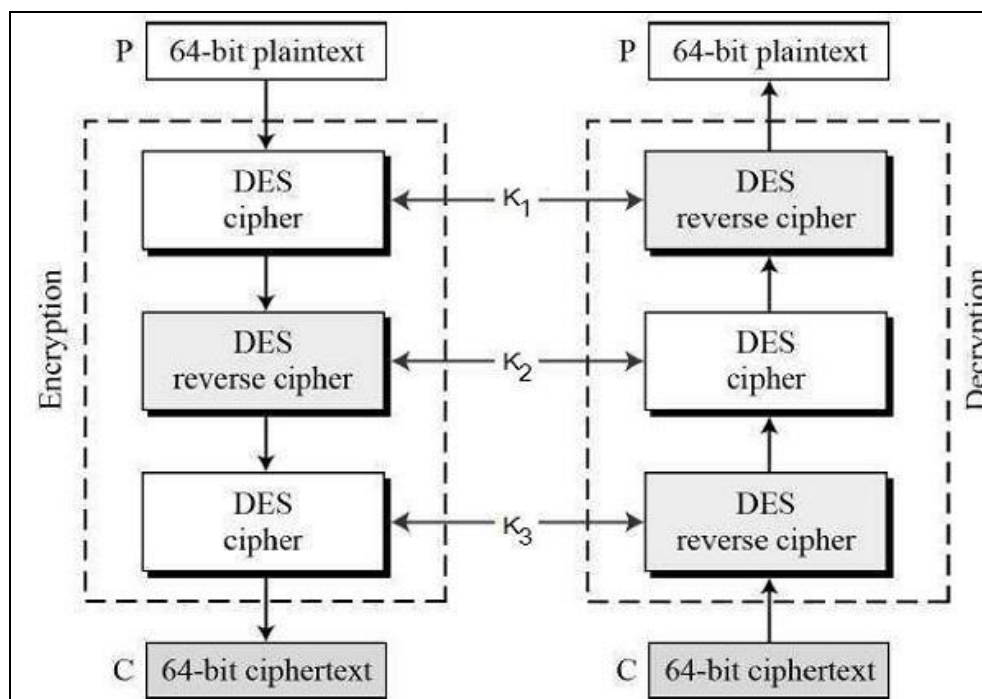
3DES (poznat još kao TDES, TDEA ili Tripple DEA) objavljen je 1999. godine od strane NIST (U.S. National Institute for Standards and Technology) u okviru PUB 46-3. Ovaj šifarski sistem, kako opisuje W. Stallings [7], svojim 168-bitnim ključem eliminiše slabosti, originalnog, DES šifarskog sistema.

Suštinska razlika između DES i 3DES počiva na činjenici da 3DES realizuje 3 x 16 rundi (u odnosu na DES-ovih 1 x 16). Ovim rundama se realizuje šifrovanje-dešifrovanje-šifrovanje (na strani pošiljaoca), a obrnut proces na strani primaoca šifrovanog teksta.

Prisutne su dve varijante 3DES-a: sa dva i sa tri ključa. Korisnik, u svakom slučaju, na početku generiše jedan (osnovni) ključ. Kod varijante sa dva ključa, ključ K1 se duplira i koristi umesto K3.

3DES obezbeđuje kompatibilnost sa DES-om tako što se vrednosti ključeva K1, K2 i K3 postave tako da budu jednake.

Način rada 3DES šifarskog sistema sa tri ključa prikazan je na slici 13.



Slika 13: 3DES - šematski prikaz¹⁵

Loše strane ovog šifarskog sistema se ogledaju u [7]:

- sporiji od 3DES

¹⁵ Preuzeto sa https://www.tutorialspoint.com/cryptography/triple_des.htm (datum pristupanja 28.03.2017.godine)

- obrađuje 64-bitne blokove otvorenog teksta (poželjni duži zbog otpornosti)

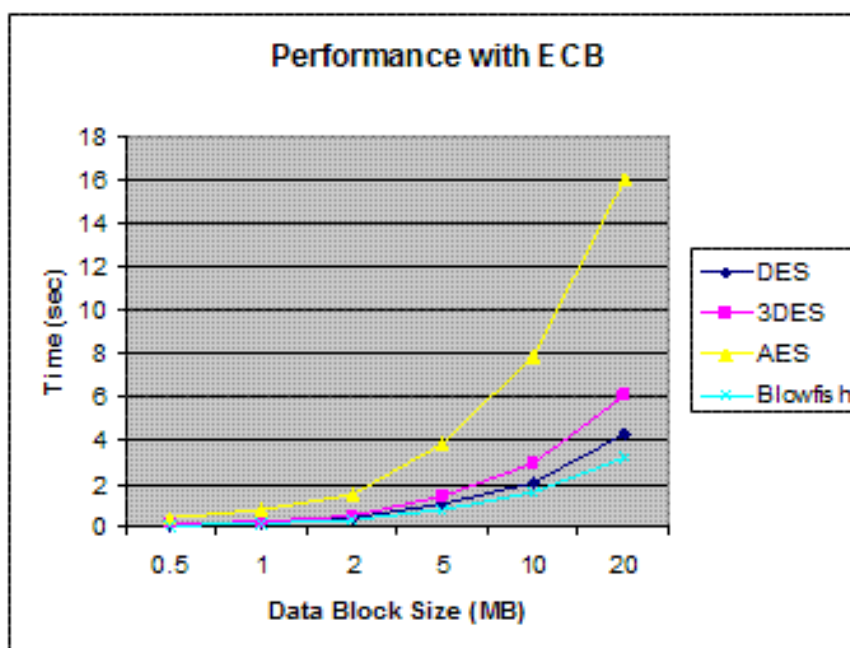
6.4 Poređenje DES, 3DES i AES šifarskih sistema

U tabeli 1 prikazane su osnovne karakteristike DES, 3DES i AES šifarskog sistema.

Tabela 1: Karakteristike šifarskih sistema ¹⁶

Činioci	AES	3DES	DES
Dužina ključa	128, 192 ili 256 bit	168 bit (3 ključa) 112 bit (2 ključa)	56 bit
Veličina bloka	128, 192 ili 256 bit	64 bit	64 bit

Kada je reč o razlici u brzini obrade informacija, istraživanje koje je sproveo A. Al-Tamimi [8], upućuje na nesumnjivu prednost AES-a u odnosu na 3DES i DES (slika 15).



Slika 15: Brzina šifarskih sistema - poređenje ¹⁷

¹⁶ Otpornost na kriptanalizu nije razmatrana s obzirom da nije od značaja za ovo istraživanje

¹⁷ Preuzeto iz [8]

7. Kriptografske heš funkcije -SHA

U ovom poglavlju je, u dovoljnoj meri, opisana kriptografska hash funkcija koja se pojavljuje kao jedan od elemenata u formiranju IPSec VPN tunela u kontekstu ovog istraživanja.

"**Heš** (eng. *hash*) **funkcija** predstavlja, u najosnovnijem, sumu poruke." [6] Ova suma (eng. *message digest*, *digest*) je brojčana vrednost koja, na određeni način, reprezentuje ulazni podatak (podatak na koji je primenjena hash funkcija).

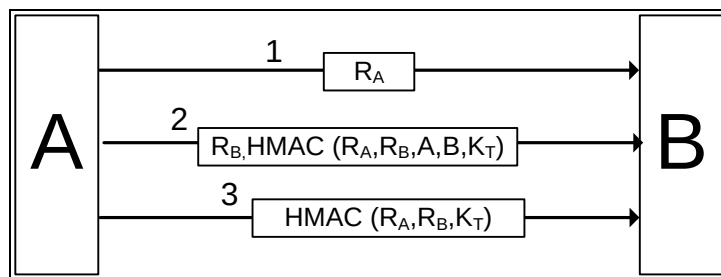
Da bi imala upotrebnu vrednost u kriptografskom smislu, hash funkcija mora biti takva da obezbeđuje jedinstvenu vrednost za ulazni podatak. Drugim rečima, **kriptografska heš funkcija** primenjena na bilo koja dva različita podatka **ne sme** na izlazu da proizvede istu brojčanu vrednost (isti heš).

Kriptografskim heš funkcijama se (u osnovi) obezbeđuje integritet podatka, a, pojedinim protokolima i neporecivost ili **autentikacija**.

Jedna od kriptografskih heš funkcija koje su trenutno u upotrebi, opisano u [6] jeste SHA. SHA je skraćenica koja označava Secure Hash Algorithm, publikovan od strane U.S.A. NSA (National Security Agency). Poslednje verzije ovog algoritma publikovane su 2002. (SHA-224, 256, 384 i 512) odnosno 2004.godine (SHA-224).

Iako su navedene verzije kriptološki znatno otpornije, u industrijskoj kriptologiji se, i dalje, koristi SHA-1 objavljen 1995. godine.

Autentikacija pomoću heša (slika 16) se bazira na hash-iranju strukture podataka sastavljene od više podataka. A šalje jednokratni uzorak R_A . B odgovara porukom koja se sastoji od jednokratnog uzorka R_B i strukture hash-irane u HMAC (Hash Message Authentication Code), npr. korišćenjem SHA-1 (R_A , R_B , dva identiteta tj. A i B i deljenog ključa – K_T). Kada A primi poruku 2, ona ima R_A , R_B koji služi kao tekst kojim treba da dokaže svoj identitet, dva identiteta i deljeni ključ (poslednja dva su joj poznata). Sama izračunava MAC i ako se dobijeni i izračunati poklapaju, izvršena je identifikacija strane B. Zlonamerna strana nema podatak K_T tako da nije u mogućnosti da generiše HMAC. A šalje ka odgovor u poruci 3 čime se završava obostrana autentikacija.

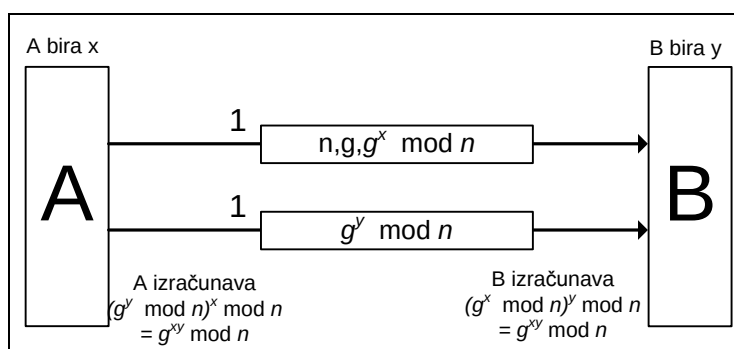


Slika 16: Provera identiteta pomoću HMAC - SHA

8. Diffie-Hellman (DH) protokol

U ovom poglavlju je opisan DH protokol kao jedan od mehanizama za formiranje IPSec VPN tunela.

Diffie-Hellman protokol (slika 17) se koristi u slučaju kada je potrebno da strane podele tajni ključ. Funkcioniše tako što A i B dogovaraju dva velika broja n i g (javni brojevi). Strana A bira tajni broj x , a strana B y . Strana A šalje: $n, g, (g^x \bmod n)$. Strana B šalje: $(g^y \bmod n)$. Strana A računa: $(g^y \bmod n)^x \bmod n = g^{xy} \bmod n$. Strana B računa: $(g^x \bmod n)^y \bmod n = g^{xy} \bmod n$. Na ovaj način obe strane dele tajni ključ $g^{xy} \bmod n$. Snaga ovog protokola počiva na sledećim momentima: trećoj strani nisu poznati x i y i nema mogućnost da izračuna x ili y iz dostupnih podataka g i n (odn. $g^x \bmod n$ ili $g^y \bmod n$).



Slika 17: Diffie-Hellman protokol

9. Internet Protocol Security (IPSec) skup protokola

U ovom poglavlju je opisan IPSec protokol stack. Za razumevanje ovog, potrebno je dobro razumevanje protokola i mehanizama opisanih u prethodnim poglavljima.

Potreba za bezbednom komunikacijom preko nebezbednih mreža dovela je do razvoja i implementacije grupe mehanizama koje poznajemo pod nazivom **virtualne privatne mreže** (eng. *Virtual Private Networks-VPN*). Ovi mehanizmi omogućavaju formiranje zaštićene virtuelne konekcije između dve ili više tačaka (mrežnog uređaja i mrežnog uređaja, hosta i mrežnog uređaja, hosta i hosta ili više hostova, odnosno mrežnih uređaja) kroz tuđu mrežu. Pod tuđom mrežom se misli na Internet ili ekstranet (eng. extranet).

Drugi naziv za ovu virtuelnu konekciju jeste "**tunel**". Za njih se može reći da predstavljaju produžetak privatne preko javne mreže i omogućavaju udaljenim korisnicima pristup pojedinim resursima.

VPN-ovi su jedan od kompleksnijih mehanizama koji omogućava bezbednu komunikaciju kroz druge - nezaštićene komunikacione mreže. Različita softverska i hardverska rešenja omogućavaju formiranje VPN tunela, baziranih na različitim protokolima. "Tunelovanje je proces u kom se vrši enkapsulacija paketa protokola jednog tipa, datagramom drugog protokola."¹⁸.

Prvi VPN-ovi su bili isključivo IP tuneli. Autentikacija i kriptovanje nisu bili prisutni.

VPN tunelovanje, u savremenom smislu, podrazumeva da protokol kojim je izvršena enkapsulacija vrši zaštitu enkapsuliranih podataka. Najčeće korišćeni protokoli po, tj. protokol stackovi, su IPSec, PPTP i SSL [10].

Prisutno je više tipova VPN tunela namenjenih za IP saobraćaj. Neki od njih su: Internet Protocol Security (IPsec), Transport Layer Security (SSL/TLS), Datagram Transport Layer Security (DTLS), Microsoft Point-to-Point Encryption (MPPE), Secure Socket Tunneling Protocol (SSTP), Multi Path Virtual Private Network (MPVPN), Multiprotocol Label Switching (MPLS) VPN, Dynamic Multipoint VPN (DMVPN), Group Encrypted Transport VPN (GETVPN) .

Ovde je u najbitnijim crtama opisan **Internet Protocol Security (IPsec)** protokol stack. Detalji u vezi sa istim mogu se pronaći u IETF standardima RFC 2403, RFC 2404, RFC 2405, RFC 2410, RFC 3168, RFC 4109, RFC 4301, RFC 4302 RFC 4303, RFC 7296 i RFC 7321. Količina RFC-ova koji ga opisuju dovoljno govori o kompleksnosti protokola.

IPSec (sa svojim mehanizmima) se nalazi na mrežnom sloju OSI modela. Prepoznajemo dva tipa IPSec tunela. Jedan je remote-access (za udaljene korisnike čija je

¹⁸ "Tunneling enables the encapsulation of a packet from one type of protocol within the datagram of a different protocol."

VPN Tunneling Protocols, Microsoft Corporation, [https://technet.microsoft.com/en-us/library/cc771298\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc771298(v=ws.10).aspx) (pristup 17.03.2017.godine)

lokacija promenljiva) i site-to-site (za statičke korisnike). Ovim istraživanjem obuhvaćen je drugi tip tunela.

IPSec, skup protokola, može se opisati kroz tri glavna dela (u pogledu korišćenih protokola):

- **IKE** (eng. *Internet Key Exchange*)
 - kreiranje ključeva za kriptovanje
 - distribucija ključeva za kriptovanje
 - utvrđivanje identiteta drugog hosta
- **AH** (eng. *Authentication Header*)
 - Obezbeđenje integriteta
- **ESP** (eng. *Encapsulating Security Payload*)
 - Obezbeđenje šifrovanja i/ili zaštite integriteta

Drugi pristup je opis kroz dva glavna dela (u pogledu faza funkcionalnosti tunela):

- Faza formiranja (realizuje se IKE protokolom) i
- Faza postojanja-eksploatacije tunela (realizuje se ESP ili AH protokolom).

9.1 Internet Key Exchange - IKE

IKE protokol, u kontekstu ovog istraživanja, je protokol na kom se bazira formiranje IPSec tunela.¹⁹

IKE protokol (formiranje VPN tunela) može da se podeli u **2 faze** od kojih svaka ima svoj **cilj**:

1. faza IKE²⁰: Usaglašavanje parametara radi prelaska u 2. fazu IKE
2. faza IKE: Usaglašavanje parametara radi prelaska u fazu eksploatacije IPSec tunela.

Tokom realizacije ovih faza, nakon usaglašavanja parametara, formiraju se tzv. SAs (eng. *security associations*):

1. faza IKE: Formiranje IKE SAs.
2. faza IKE: Formiranje IPSec (tunel) SAs.

U zavisnosti od IKE faze, radi formiranja SAs, usklađuju se različiti parametri sigurnosnih polisa:

¹⁹ IKE protokol je baziran na sledećim protokolima: ISAKMP (eng. *Internet Security Association and Key Management Protocol*), Oakley i SKEME (eng. *Versatile Secure Key Exchange Mechanism for Internet*). Elementi ovih protokola su kroz IKE prisutni u okviru 1. faze formiranja IPSec tunela. Samostalno ima više funkcija [9] koje nisu u domenu ovog istraživanja.

²⁰ Može da se realizuje u tzv. *Aggressive* i *Main Mode*-u. Analiza istih nema značaja za istraživanje.

1. faza IKE: Formiranje SA za 2. fazu IKE

- Algoritam za enkripciju (DES, 3DES).
- Heš algoritam (MD5, SHA1).
- DH grupa ²¹
- Metoda autentikacije (preshared key, public key signature, public key encryption ili revised public key encryption).

2. faza IKE: Formiranje SA za IPSec tunel

- AH ili ESP,
- MD5 ili SHA1,
- 3DES ili DES.

Pored usaglašavanja parametara radi formiranja SAs i samog formiranja SAs, u okviru IKE, realizuje se i:

1. faza IKE:

- Razmena DH javnih vrednosti (razmena elemenata pomoću kojih DH alg. utvrđuje deljeni tajni ključ); kada se ovaj deo realizuje, na suprotnim stranama se generiše ključ kojim se štiti autentifikacija (*master key*).
- Autentifikacija; podaci za autentifikaciju se hešuju, nakon toga kriptuju kreiranim DH ključem.

2. faza IKE:

- Razmena ključeva sesije
- Dostavljanje podataka IPSec-u
- (opciono) PFS (Perfect Forward Security), upotrebom DH

Po završetku faze 1 i faze dva, željeno stanje je:

1 faza:

- Autentifikacija je izvršena
- Obe strane imaju deljeni simetrični ključ
- Formiran je IKE SA

2 faza:

- Formiran IPSec SA

²¹ group 1 - 768 bit modulus, group 2 - 1024 bit modulus, group 5 - 1536 bit modulus, group 14 - 2048 bit modulus, group 19 - 256 bit elliptic curve, group 20 - 384 bit elliptic curve – Next Generation Encryption, group 21 - 521 bit elliptic curve – Next Generation Encryption, group 24 - modular exponentiation group with a 2048-bit modulus and 256-bit prime order subgroup – Next Generation Encryption[11]

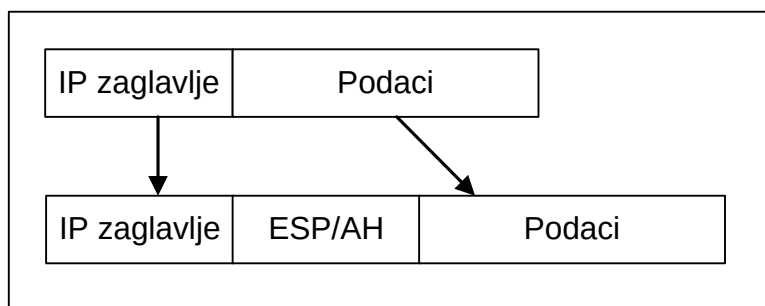
9.2 Transportni režim i režim tunelovanja

Dva su moguća režima rada za IPSec tunele. Izbor se vrši u zavisnosti od toga da li je VPN tunel planiran za realizaciju host-host ili VPN Gateway- VPN Gateway komunikaciju. U prvom slučaju koristi se transportni, u drugom režim tunelovanja.

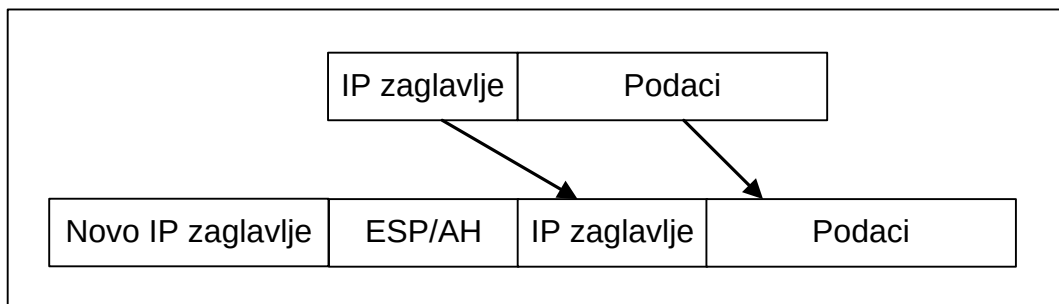
Suštinska razlika između ova dva režima počiva na tome da li je originalno IP zaglavlje zaštićeno ili nije.

U slučaju transportnog režima IP zaglavlje nije zaštićeno. Originalno IP zaglavlje ostaje na početku paketa, dok se zaglavlja ESP ili AH protokola umeću između njega i podataka (slika 18).

U tunelskom režimu se čitav originalni paket (uključujući IP zaglavlje) kriptuje. ESP/AH zaglavlje se, u ovom slučaju, nalaze ispred originalnog paketa. Novo IP zaglavlje svoje mesto pronalazi ispred ESP/AH zaglavlja (slika 19).



Slika 18: ESP/AH u transportnom režimu



Slika 19: ESP/AH u tunelskom režimu

9.3 Authentication Header (AH) i Encapsulating Security Payload (ESP)

AH i ESP (opisani u RFC 4302 i RFC 4303) su dva protokola koji mogu da se primene u fazi eksploatacije IPSec tunela. Čine sastavni deo IPSec protokol stacka. Mogu da se primene odvojeno ili istovremeno na IP paket.

Osnovna namena ovih protokola je da obezbede zaštitu IP datagrama:

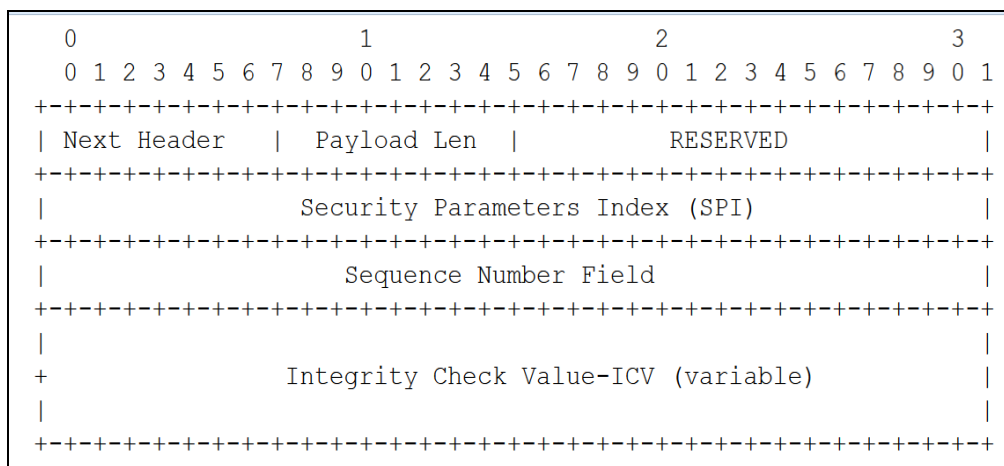
- AH: obezbeđuje samo integritet

- ESP: obezbeđuje integritet i poverljivost²².

Oba protokola (opciono) obezbeđuju od replay napada, anti-replay mehanizmom.

Potrebno je napomenuti da je AH zaštita integriteta bolja kod AH protokola, te se zato ne isključuje iz upotrebe.

AH obezbeđuje integritet na sve iznad IP zaglavlja i na, samo, neka-nepromenljiva polja u IP zaglavlju. ESP svoju funkciju obavlja na podacima van IP zaglavlja. Izgled paketa ova dva protokola prikazan je na slikama 20 i 21.



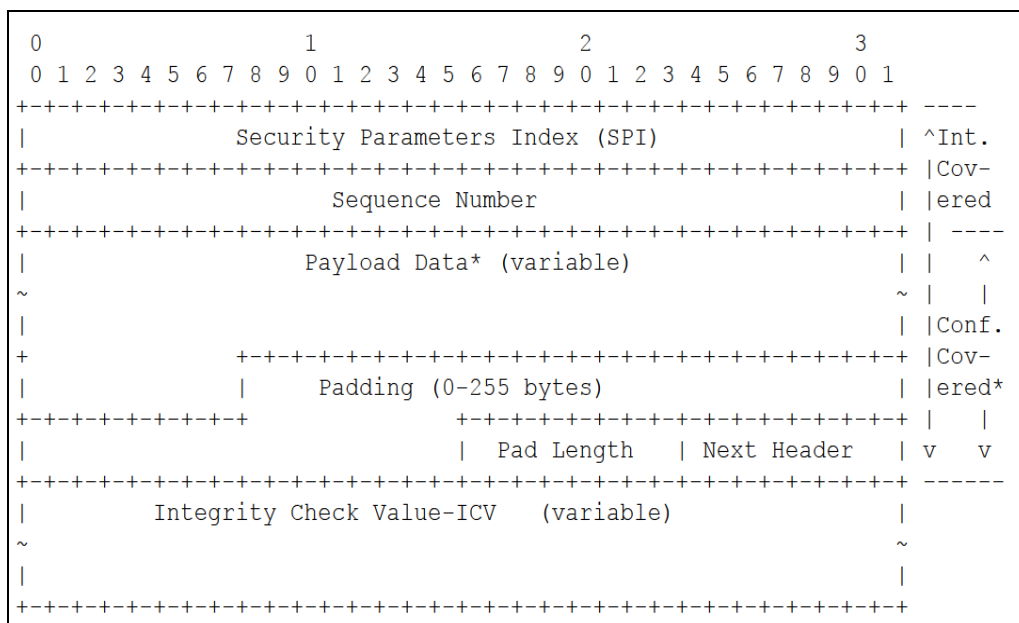
Slika 20: AH - izgled paketa²³

Objašnjenje bitnih polja AH paketa:

- Payload Len: ukazuje na dužinu AH
- SPI: omogućava identifikaciju SA na prijemnoj strani
- Seq.Number Field: sprečava replay napade
- ICV: vrednost koja se proverava

²² Ukoliko učesnici u komunikaciji, tokom pregovora oko krypto algoritma koji će koristiti, dogovore opciju NULL, ESP će obezbeđivati samo integritet (RFC 2410)

²³ Preuzeto iz RFC 4302

Slika 21: ESP - izgled paketa ²⁴

Objašnjenje bitnih polja ESP protokola:

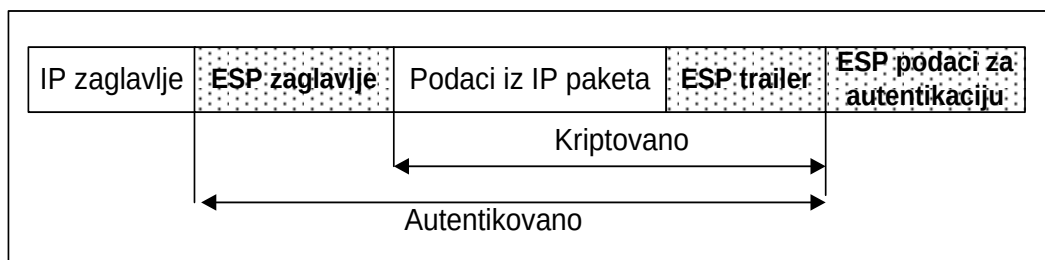
- SPI: omogućava identifikaciju SA na prijemnoj strani
- Seq.Number: sprečava replay napade
- Payload Data: Sadrži originalni IP paket, uključujući sve podatke korišćene za zaštitu sadržaja. Tip zaštićenog sadržaja ovog polja je naznačen u polju "Next Header"
- Padding: popunjava veličinu podataka do vrednosti pogodne za šifrovanje
- Next Header: ukazuje na tip narednog poglavlja
- ICV: vrednost koja se proverava

Na slikama 22, 23, 24 i 25 ilustrovana je realizacija bezbednosnih funkcija koje obavljaju AH i ESP u zavisnosti od primenjenog režima (transportni i tunelski).

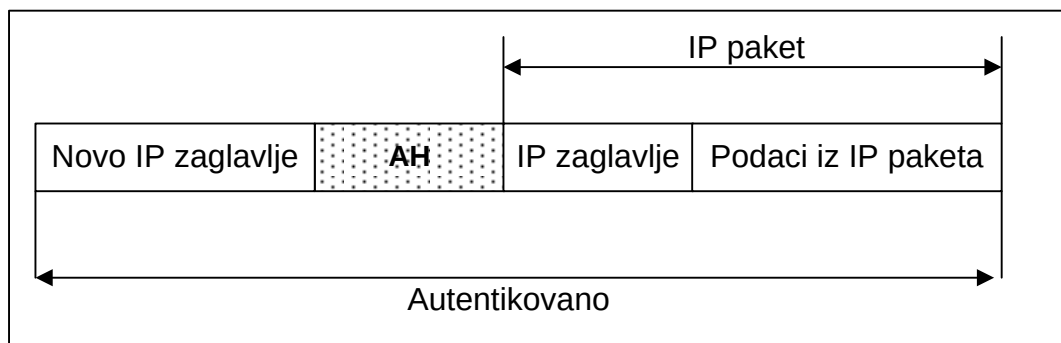


Slika 22: AH - IPv4 paket enkapsuliran AH protokolom u transportnom režimu

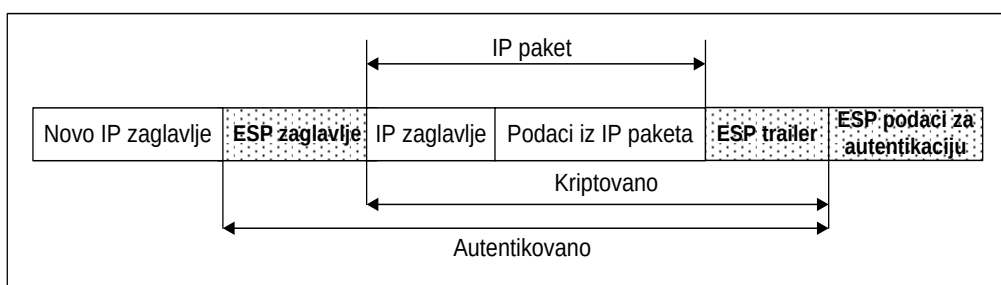
²⁴ Preuzeto iz RFC 4303



Slika 23: ESP - IPv4 paket enkapsuliran ESP protokolom u transportnom režimu



Slika 24: AH - IPv4 paket enkapsuliran AH protokolom u tunelskom režimu



Slika 25: ESP - IPv4 paket enkapsuliran ESP protokolom u tunelskom režimu

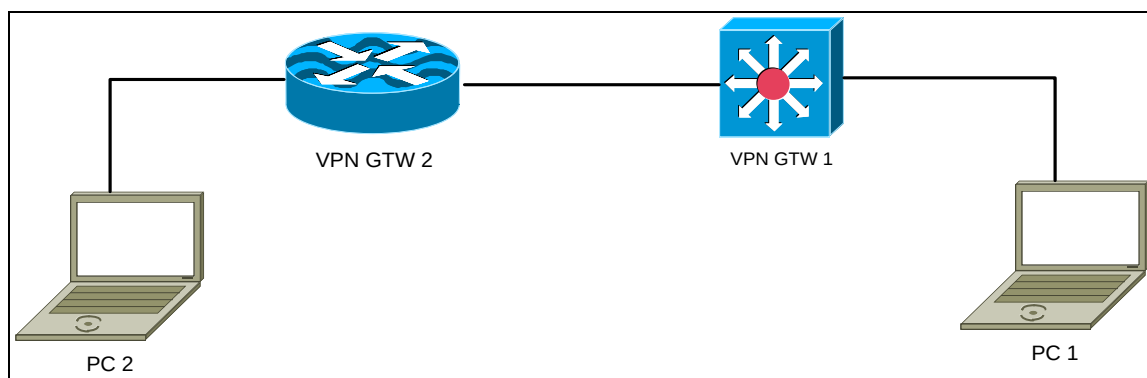
10. Postavka eksperimenta

U ovom poglavlju opisana je fizička i logička topologija mreže na kojoj je realizovano merenje, navedene su bitne karakteristike hardvera i sofvera kao i konkretni parametri vezani za konfigurisanje opreme koji imaju uticaja na predmet istraživanja.

10.1 Fizička topologija i korišćena oprema

Radi prikupljanja podataka o performansama mreže sa VPN tunelom, a u cilju ostvarivanja cilja istraživanja, eksperiment je realizovan realizovan u laboratorijskim uslovima. Na ovaj način eliminisan je uticaj nepredvidljivih činilaca, odnosno nekontrolisano generisanog saobraćaja.

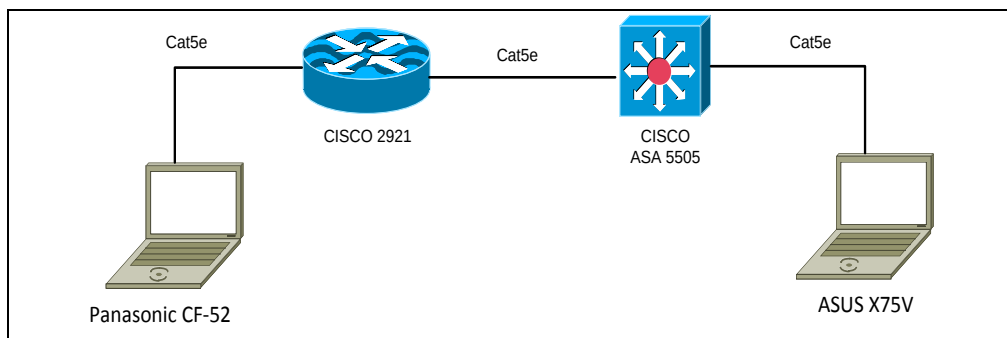
Eksperiment je realizovan na mrežnoj topologiji (slika 26) koju su sačinjavala dva mrežna uređaja (VPN GTW 1 i 2) i dva hosta (PC1 i 2).



Slika 26: Fizička topologija za realizaciju eksperimenta

Za potrebe realizacije eksperimenta korišćene su sledeće hardverske komponente (slika 27):

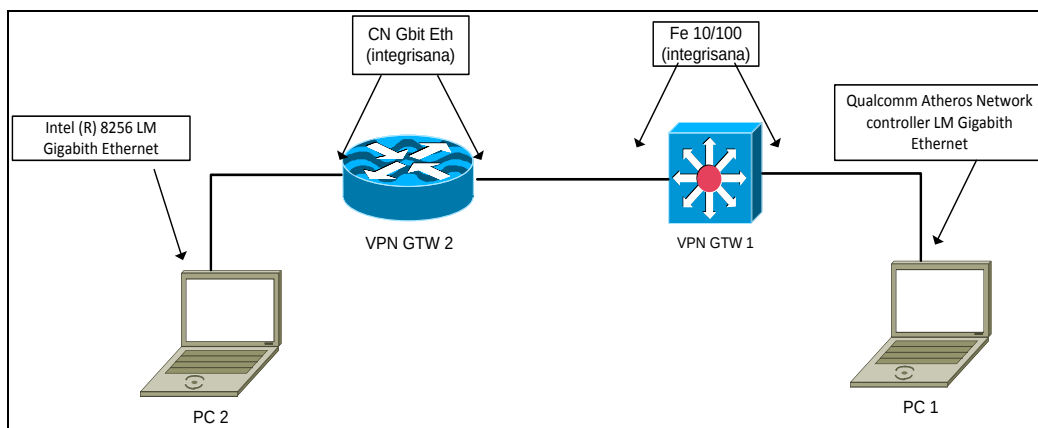
- PC 1 - ASUS X75V Lap Top,
- PC 2 - Panasonic CF-52 Lap Top,
- VPN GTW 1- ASA Cisco AdaptiveSecurityAppliance 5505,
- VPN GTW 2- Ruter Cisco 2921 i
- Kablovi - Cat5e.



Slik

a 27: Hardverske komponente korišćene za realizaciju eksperimenta

Bitna karakteristika uređaja, od uticaja na performanse mreže, jesu njihovi interfejsi i isti su navedeni na slici 28.



Slika 28: Interfejsi uređaja korišćenih za realizaciju eksperimenta

10.2 Specifikacija softvera

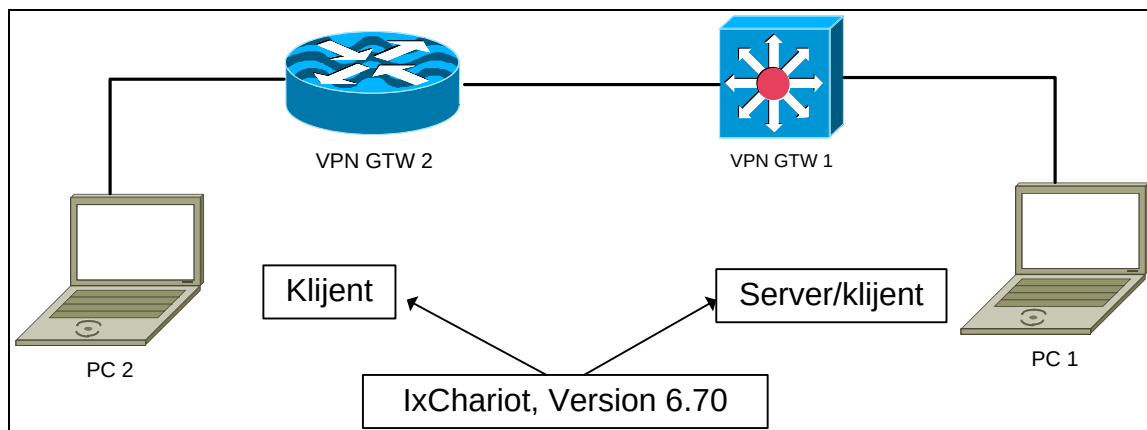
Tokom realizacije eksperimenta su korišćeni hostovi sa Microsoft Windows XP i Windows 10 OS, a na VPN Gateway-ima Cisco IOS sa odgovarajućim licencama. Detaljniji prikaz korišćenog softvera prikazan je u tabeli 2.

Tabela 29: Softver na uređajima korišćenim za realizaciju eksperimenta

PC 1	Windows 10 Pro
PC 2	Windows XP Pro SP2
VPN GTW 1	Cisco Adaptive Security Appliance Software Version 9.1(6)4 Device Manager Version 7.5(1)
VPN GTW 2	Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.5(3)M, RELEASE SOFTWARE (fc1) ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1) SECURITY LICENCE: Security K9

Tabela 2: Softver na uređajima korišćenim za realizaciju eksperimenta

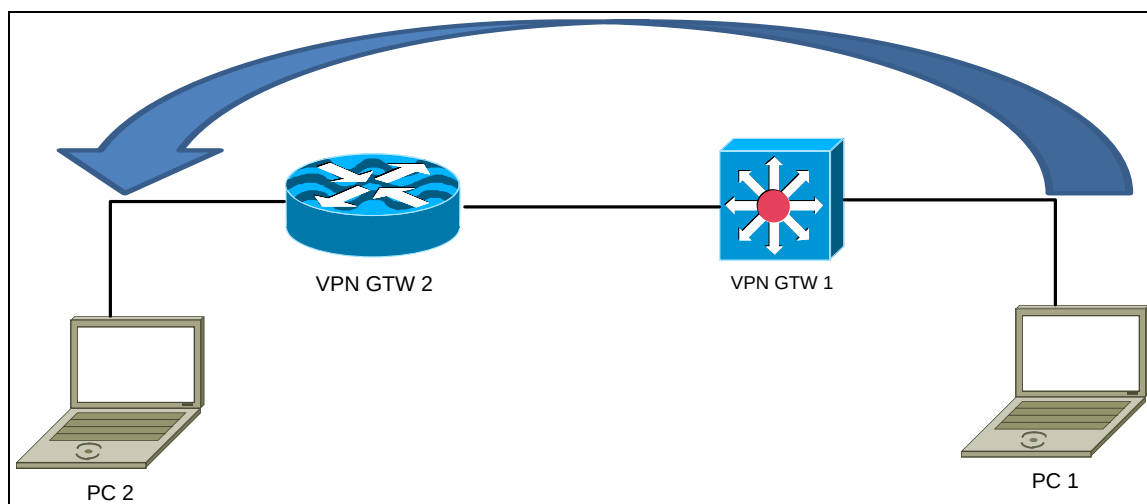
Za potrebe merenja korišćena je aplikacija IxChariot, Version 6.70. Serverski (upravljački) deo aplikacije i jedan od dva klijenta je pokrenuti na PC 1, dok je drugi klijent pokrenut na PC 2 (slika 29). U iXchariot aplikaciji se, umesto termina server i klijent, koriste termini konzola (eng. *console*) i krajnja tačka (eng. *endpoint*).



Slika 29: Merna aplikacija

10.3 Smer prenosa, korišćeni protokoli i metod enkripcije

Prenos podataka vršen je u smeru (slika 30) PC 2 - PC 1 (odn. Endpoint 1 - Endpoint 2), posmatrano kroz mernu aplikaciju, korišćenjem dva protokola transportnog sloja (TCP i UDP), u IPSec režimu uz korišćenje dva mehanizma enkripcije (AES i 3DES).

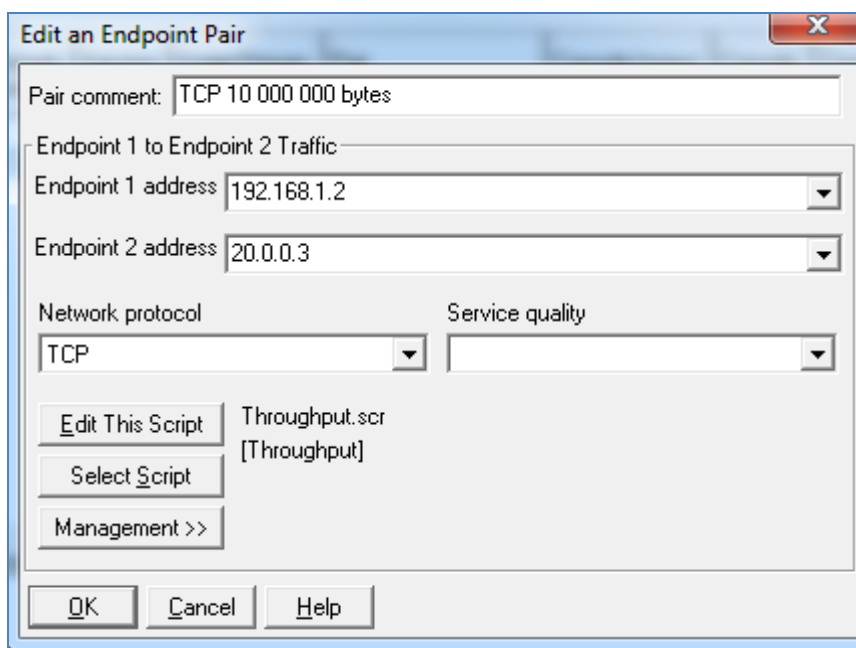


Slika 30: Smer prenosa tokom realizacije eksperimenta

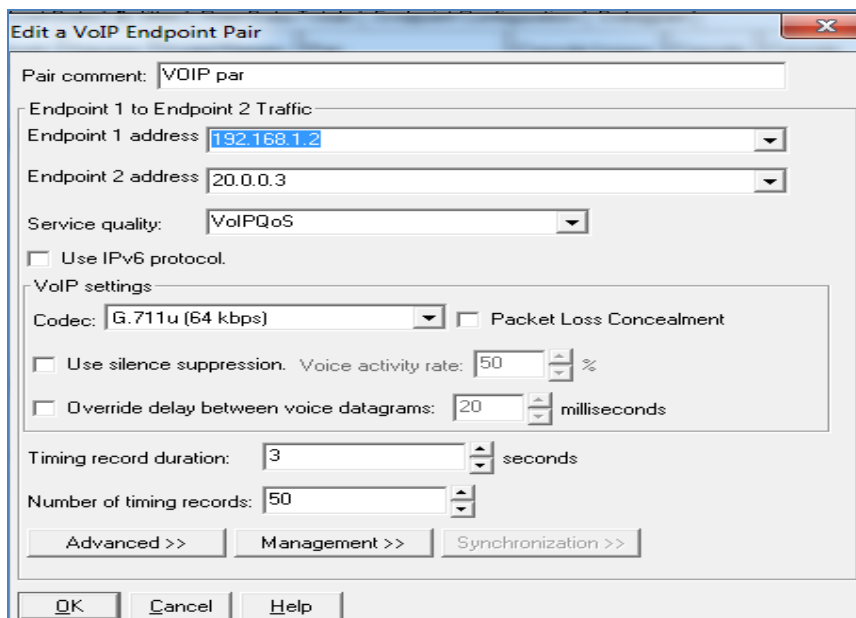
Parametri za prenos (smer, protokol i enkripcija) su konfigurisani na tri instance: iXchariot aplikacija, GTW 1 i GTW 2. Na prvoj instanci konfigurisani su parametri vezani za smer prenosa i protokol, dok su na druge dve konfigurisani krypto parametri.

10.3.1 Konfigurisanje smera prenosa i izbor protokola

Smer prenosa i protokol su konfigurisani u iXchariot aplikaciji. Izbor smera prenosa je određen numeracijom hostova (Endpoint 1 ka Endpoint 2) kojima se dodeljuju IP v4 adrese (slike 31 i 32). Na ovaj način formira se, takozvani Endpoint Pair. Protokol transportnog sloja bira se u okviru opcije "Network protocol".



Slika 31: iXchariot-Konfigurisanje Endpoint Pair-a i izbor protokola za TCP

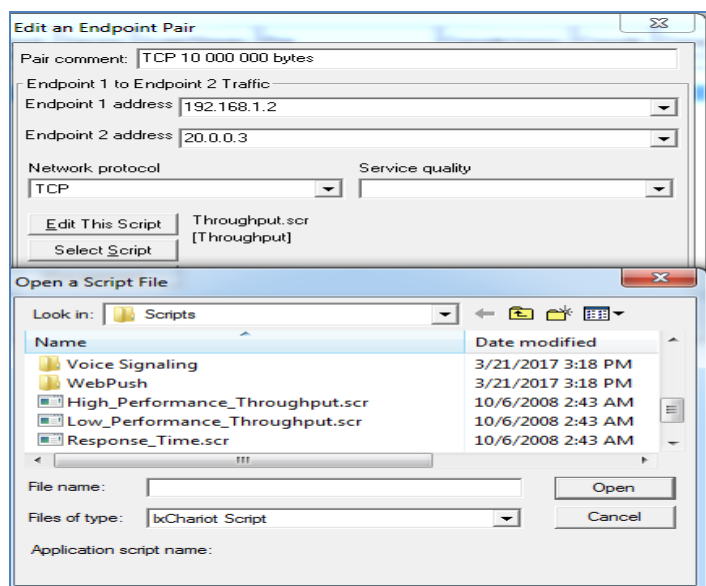


Slika 32: iXchariot-Konfigurisanje Endpoint Pair-a i izbor protokola za UDP

Izboru i konfigurisanju detaljnih parametara prenosa (za TCP protokol) pristupa se preko "Select Script" opcije. Za VoIP saobraćaj je potrebno izabrati "Advanced" opciju.

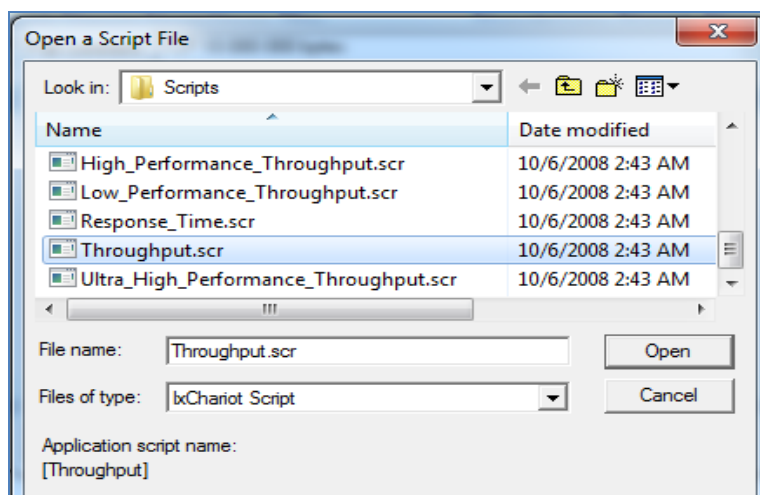
10.3.2 Konfigurisanje parametara TCP protokola

Aktivacijom Select Script opcije omogućen je izbor jedne od mnogobrojnih, predefinisanih, skripti. Skripte sadrže detaljne parametre koji se odnose na izabrani protokol (slika 33).



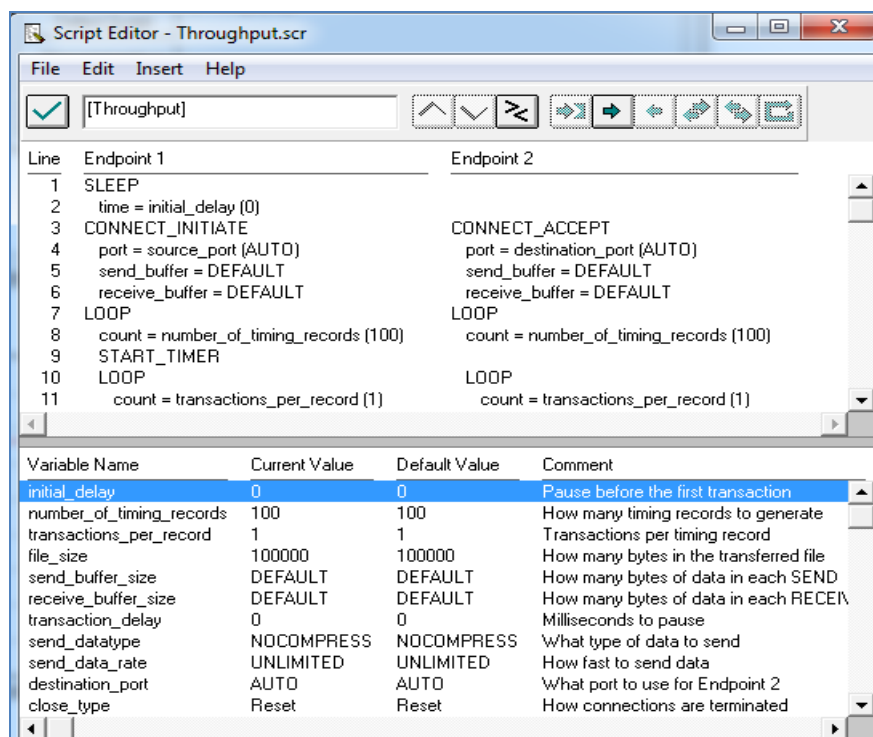
Slika 33: iXchariot-Izbor skripte

U ovom slučaju izvršen je izbor skripte pod nazivom **Throughput.scr** za TCP (slika 34).



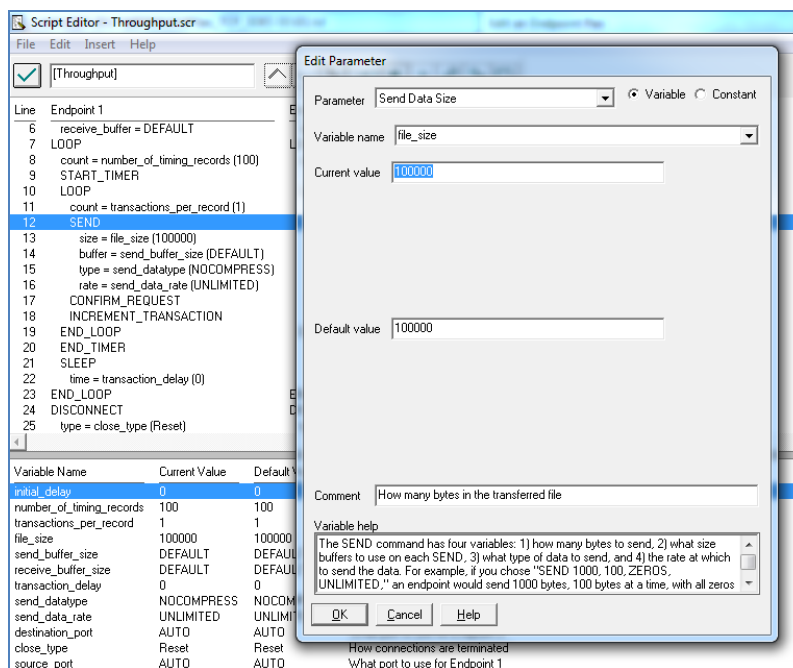
Slika 34: iXchariot-Izbor Throughput.scr skripte

Po izvršenom izboru skripte, opcijom Edit this script (na slici 32) stiće se uvid u parametre koje skripta definiše (Slika 35).



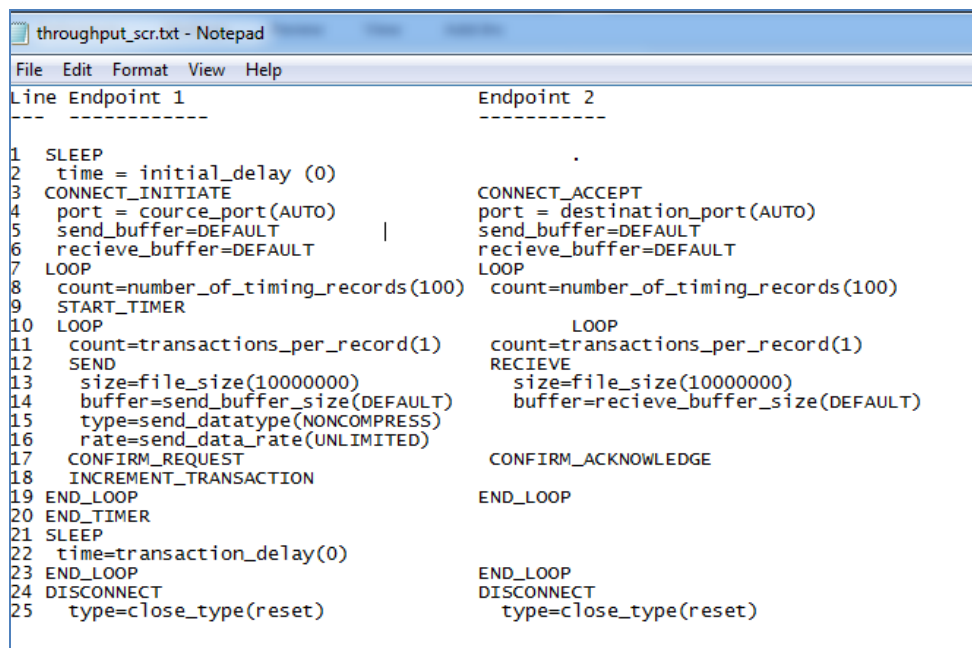
Slika 35: iXchariot-Parametri koje skripta definiše

U ovoj fazi (editovanjem), moguće je izvršiti izmenu dela parametara. Na slici 36 prikazan je prozor u kom može da se izvrši promena predefinisane količine podataka koju će aplikacija generisati.



Slika 36: iXchariot-Promena jednog od parametara skripte

U konkretnom slučaju izabrana (throughput.scr) skripta obuhvata elemente na slici 37.



Slika 37: iXchariot-Deo elemenata throughput.scr skripte

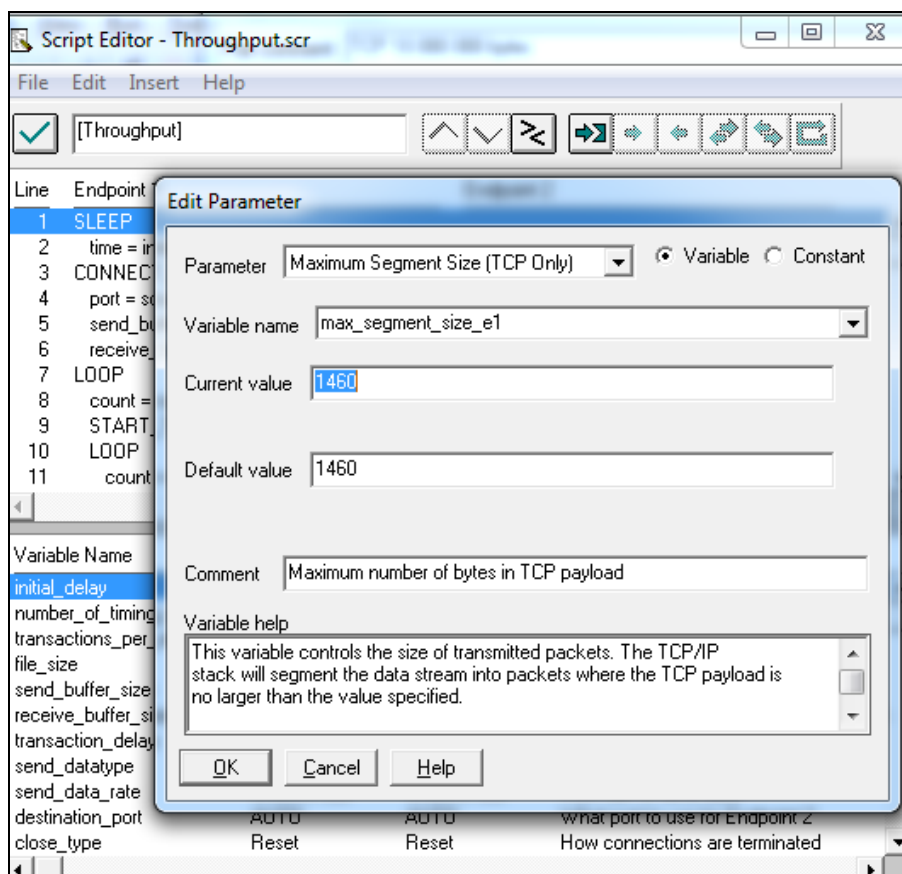
Za potrebe realizacije eksperimenta promenjena je vrednost samo jedne promenljive (file_size) dok su ostale zadržale DEFAULT vrednosti.

Postojeće promenljive, sa kratkim opisom, korišćenim i predefinisanim vrednostima prikazane su u tabeli 3.

Tabela 3: iXchariot-Deo elemenata throughput.scr skripte

Ime promenljive	Trenutna vrednost	Default vrednost	Opis
initial_delay	0	0	Pauza pre naredne transakcije
number_of_timing_records	100	100	Broj vremenskih zapisa
transactions_per_record	1		Broj transakcija po vremenskom zapisu
file_size [byte]	10000000	100000	Veličina datoteke za slanje
send_buffer_size [byte]	DEFAULT	DEFAULT	Koliko podataka (od ukupne količine - file_size) poslati na svaki SEND. DEFAULT=32767 byte
receive_buffer_size	DEFAULT	DEFAULT	Koliko podataka (od ukupne količine - file_size) primiti na svaki RECEIVE
transaction_delay [ms]	0	0	Pauza do sledeće transakcije
send_datatype	NONCOMPRESS	NONCOMPRESS	Tip podataka od kojih se formira datoteka za slanje. U ovom slučaju reč je o slučajno generisanom nizu 0 i 1.
send_data_rate	UNLIMITED	UNLIMITED	Brzina slanja podataka.
destination_port	AUTO	AUTO	Port na Endpoint 2
close_type	Reset	Reset	
source_port	AUTO		Port na Endpoint 2

Još jedna promenljiva, koja nije prikazana u tabeli 3, a utiče na vrednost throughput-a za TCP saobraćaj, jeste Maximum Segment Size (MSS). Korišćena vrednost je prikazana na slici 38.



Slika 38: iXchariot- MSS definisana za potrebe eksperimenta

10.3.3 Konfigurisanje parametara UDP protokola

Aktivacijom **Advanced** opcije (slika 31) dobija se pristup dodatnim opcijama za izbor i promenu parametara za UDP/VoIP. Ove opcije prikazane su na slici 39.

Edit a VoIP Endpoint Pair

Pair comment:

Endpoint 1 to Endpoint 2 Traffic

Endpoint 1 address:

Endpoint 2 address:

Service quality:

☐ Use IPv6 protocol.

VoIP settings

Codec: ☐ Packet Loss Concealment

☐ Use silence suppression. Voice activity rate: %

☐ Override delay between voice datagrams: milliseconds

Timing record duration: seconds

Number of timing records:

Initial delay

Value: Upper limit (milliseconds)

Additional fixed delay milliseconds

Jitter buffer

☒ Specify a jitter buffer.

☐ milliseconds ☐ voice datagrams

Port number

Source port number: Destination port number:

Payload

☒ Random payload ☐ Payload file

Filename:

☒ Embedded payload data ☐ Referenced payload file

Slika 39: iXchariot-Parametri za UDP/VoIP

Za potrebe realizacije eksperimenta nije vršena promena predefinisanih parametara.

10.3.4 Konfigurisanje krypto parametara

Radi realizacije cilja istraživanja, bilo je potrebno izvršiti konfigurisanje mehanizma enkripcije. U ovom slučaju razmatrani su 3DES i AES. Navedeni mehanizmi se koriste u okviru VPN tunela, odnosno predstavljaju deo parametara koji se može konfigurisati u vezi sa istim.

Parametri VPN tunela se konfigurišu na VPN gateway-ima. S obzirom da su za potrebe realizacije eksperimenta korišćena dva različita VPN gateway-a, postoji razlika u načinu konfiguiranja kao i u terminologiji primenjenoj u IOS-u jednog, odnosno drugog uređaja.

Uvid u podatke (parametre) postavljene na GTW 1 (Cisco ASA 5505) i GTW 2 (Cisco 2921 ruter) može se ostvariti unosom komande "show running configuration" čiji izlaz je prikazan u nastavku. Kripto parametri su zadebljani (bold).

Izlaz komande # show running configuration na GTW 1:

```
ciscoasa#show running config
:
ASA Version 9.1(6)4
!
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
 switchport access vlan 1
!
interface Vlan1
 nameif INSIDE
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif OUTSIDE
 security-level 0
 ip address 10.0.0.2 255.255.255.0
!
ftp mode passive
object-group network LOCAL-NETWORK
 network-object 192.168.1.0 255.255.255.0
object-group network REMOTE-NETWORK
 network-object 20.0.0.0 255.255.255.0
access-list 101 extended permit ip object-group LOCAL-NETWORK object-
group REMOTE-NETWORK
!
!
crypto ipsec ikev1 transform-set R1-ASA esp-aes esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map R1-ASA_MAP 10 match address 101
crypto map R1-ASA_MAP 10 set peer 10.0.0.1
crypto map R1-ASA_MAP 10 set ikev1 transform-set R1-ASA
crypto map R1-ASA_MAP 10 set reverse-route
crypto map R1-ASA_MAP interface OUTSIDE
crypto ca trustpool policy
no crypto isakmp nat-traversal
crypto ikev1 enable OUTSIDE
crypto ikev1 policy 10
authentication pre-share
encryption aes
```

```

hash sha
group 2
lifetime 86400
!!
!!
vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-clientless
!!
tunnel-group 10.0.0.1 type ipsec-l2l
tunnel-group 10.0.0.1 ipsec-attributes
ikev1 pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
!
!
ciscoasa#

```

Izlaz komande # show running configuration na GTW 1:

```

RUTER1# show running configuration
!
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
crypto isakmp key ***** address 10.0.0.2
!
crypto ipsec transform-set R1-ASA esp-aes esp-sha-hmac
mode tunnel
!
crypto map R1-ASA_MAP 10 ipsec-isakmp
set peer 10.0.0.2
set transform-set R1-ASA
match address 110
!
interface GigabitEthernet0/0
ip address 20.0.0.1 255.255.255.0
!
interface GigabitEthernet0/1
ip address 10.0.0.1 255.255.255.0
crypto map R1-ASA_MAP
!
!
end

RUTER1#

```

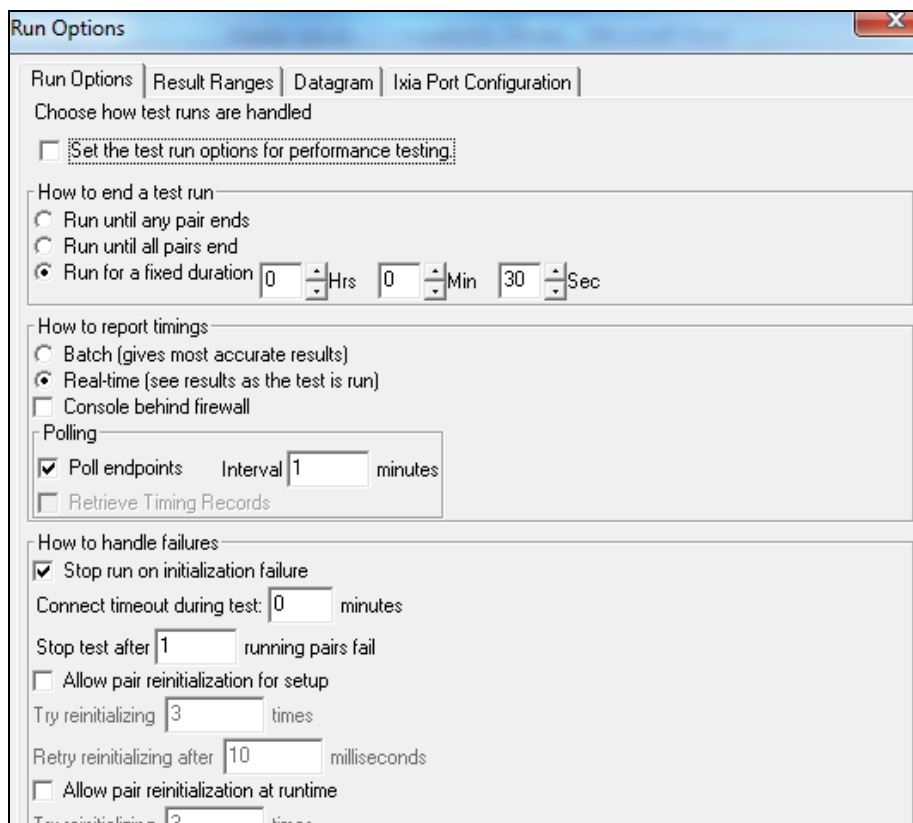
U tabeli 4 su izdvojeni bitni parametri IPSec VPN tunela. Ovde može da se uoči različita terminologija primenjena na različitim uređajima (ASA-IKEv1, Ruter - ISAKMP) kao i (donekle) razlika u sintaksi.

Tabela 4: Kripto parametri na gateway-ima

Parametar		Cisco ASA 5505	Cisco 2921
1	2	3	4
Enkripcija za ESP	AES/3DES	encryption aes (drugo podešavanje:3DES)	encr aes (drugo podešavanje:3DES)
Autentikacija	sha	hash sha	
Diffie Helman grupa	2 / 5	group 2 (5 za 3DES)	group 2 (5 za 3DES)
ISAKMP (IKEv1) Autentikacija	pre-share	authentication pre-share tunnel-group 10.0.0.1 ipsec- attributes ikev1 pre-shared-key *****	authentication pre-share crypto isakmp key ***** address 10.0.0.2
IPSec parametri	esp - aes sha esp - 3des sha	ipsec ikev1 transform-set esp-aes esp-sha-hmac	crypto ipsec transform-set esp-aes esp-sha-hmac
IPSec mode	Tunelski	tunnel-group 10.0.0.1 type ipsec-l2l	mode tunnel

11. Tok eksperimenta

Eksperiment je vršen pokretanjem testova u iXchariot aplikaciji. Vremenski interval za realizaciju jednog testa je 30 sekundi (slika 40).



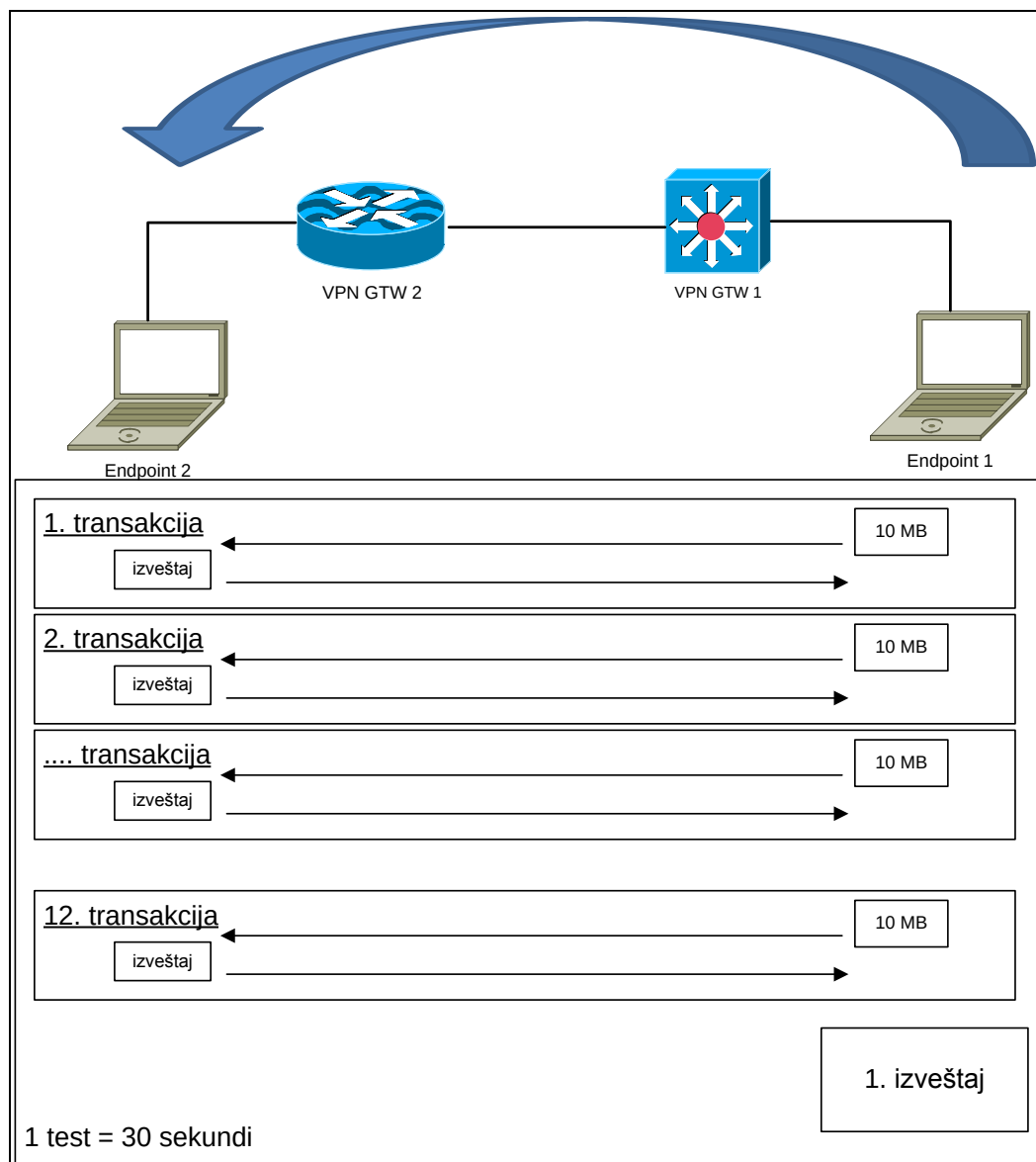
Slika 40: iXchariot-Konfigurisanje trajanja testa

Po pokretanju testa, Endpoint 1 (E1) šalje Endpointu 2 (E2) skriptu kojom su definisani parametri testa nakon čega se realizuju transakcije.

Za TCP je realizovano 12 transakcija. Jedna transakcija podrazumeva dve transmisije podataka: jedno slanje datoteke 10 MB (smer E1-E2) i slanje izveštaja o količini primljenih podataka (smer E2-E1). Slika 41 ilustruje jedan test.

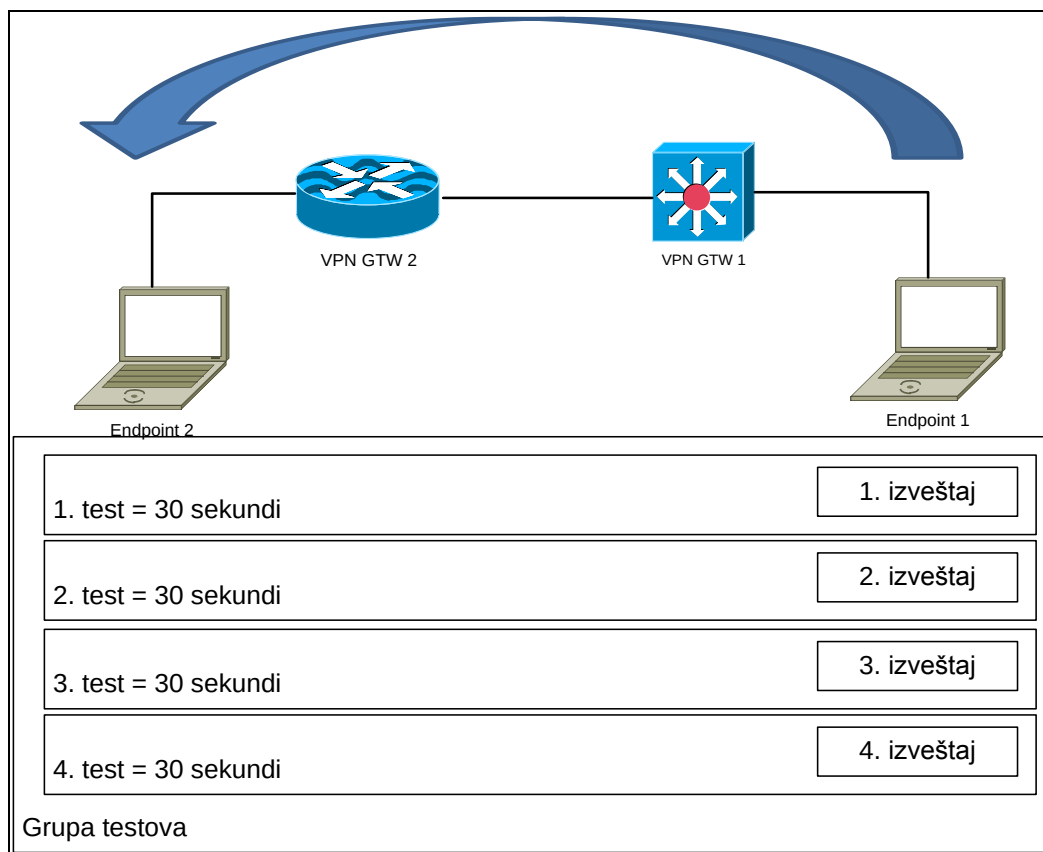
Kod UDP/VoIP realizovano je 10 transakcija. Po transakciji se šalje 24000 byte podeljenih na UDP datagrame.

Dodatna razlika između ove dve vrste prenosa jeste ta što je brzina slanja (iz ugla aplikacije) u slučaju TCP-a bila maksimalno moguća, a u slučaju UDP/VoIP fiksirana na 64 kbps (jedan govorni kanal).



Slika 41: Prikaz jednog testa

Za sve kombinacije parametara, testovi su realizovani po četiri puta. Četiri testa čine grupu testova za jednu od kombinacija parametara (slika 42).

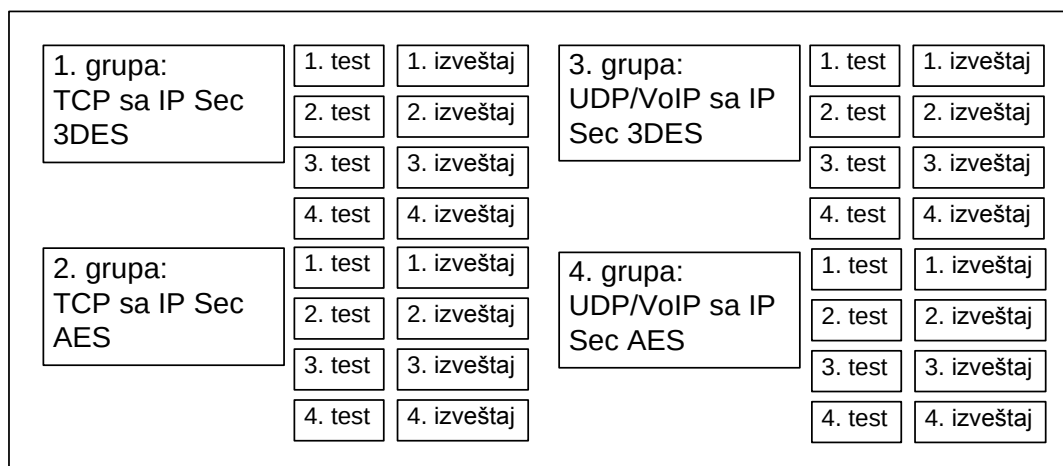


Slika 42: Prikaz grupe testova

Ukupno je realizovano 4 grupe testova:

- 1. grupa TCP IP Sec 3DES,
- 2. grupa TCP IP Sec AES,
- 3. grupa UDP/VoIP 3DES,
- 4. grupa UDP/VoIP AES,

i, na taj način, generisano 4 grupe izveštaja (slika 43).



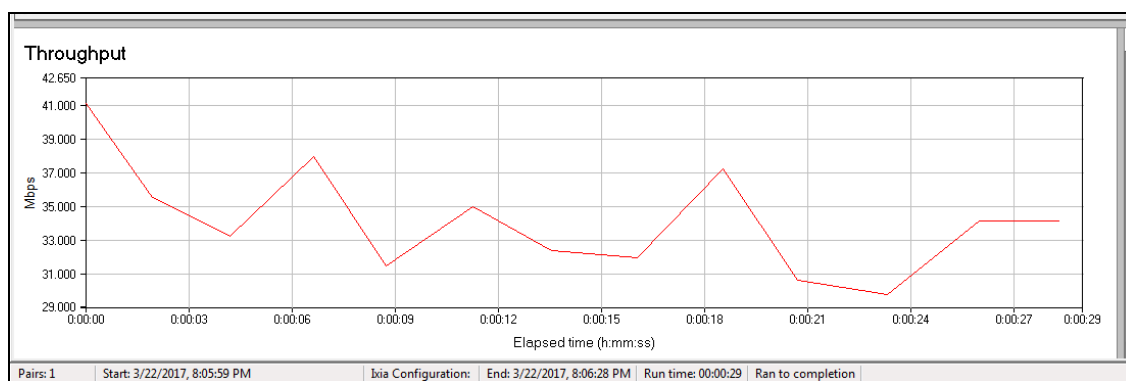
Slika 43: Grupe testova i generisani izveštaji

12. Prikupljanje, način obrade i analiza podataka

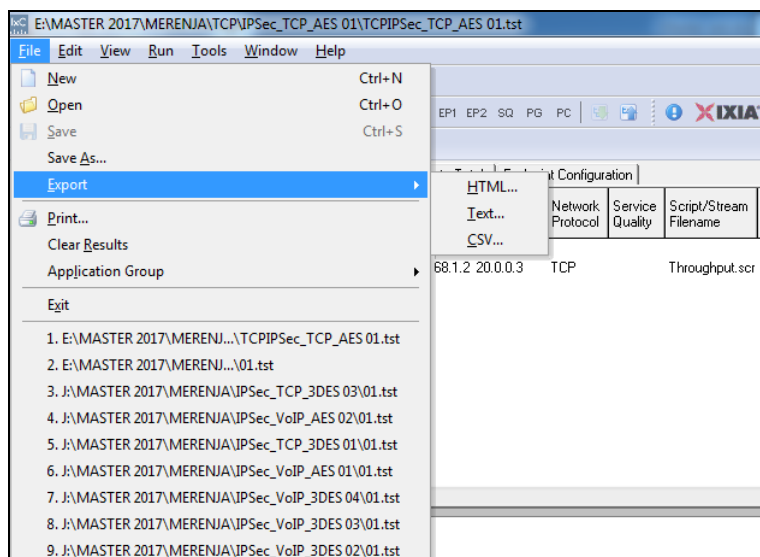
U ovom poglavlju opisan je tip generisanih podataka i način na koji ih merna aplikacija generiše. Pored ovoga objašnjeno je koji su i kako obrađeni da bi se iskoristili za potrebe analize.

12.1 Prikupljanje podataka

Po završetku svakog testa, kao što je već pomenuto, iXchariot generiše grafike (slika 44) i izveštaj. Izveštaj može da se sačuva u više formata: html, txt i cvs (slika 45). Za obradu podataka najpogodniji je .cvs tip izveštaja (slika 46) i upravo ovaj tip je iskorišćen.



Slika 44: Primer grafika generisanog u iXchariot



Slika 45: Opcije za čuvanje izveštaja u iXchariot

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
4																									
5																									
6																									
7																									
8																									
9																									
10																									
11																									
12																									
13																									
14																									
15																									
16																									
17																									
18																									
19																									
20																									
21																									
22																									
23																									
24																									
25																									
26																									
27																									
28																									
29																									
30																									
31																									
32																									
33																									
34																									
35																									

Slika 46: Primer izveštaja sačuvanog u .csv formatu

Po završetku svakog testa sačuvani su svi tipovi izveštaja. Nakon četiri ponovljena testa, formirana je grupa izveštaja za konkretan tip prenosa. Na slici 47 prikazane su grupe izveštaja za TCP protokol sa IPSec.

Name	Date modified	Type
IPSec_TCP_3DES 01	3/22/2017 6:35 PM	File folder
IPSec_TCP_3DES 02	3/22/2017 6:40 PM	File folder
IPSec_TCP_3DES 03	3/22/2017 6:42 PM	File folder
IPSec_TCP_3DES 04	3/22/2017 6:43 PM	File folder
IPSec_TCP_AES 01	3/22/2017 7:07 PM	File folder
IPSec_TCP_AES 02	3/22/2017 7:08 PM	File folder
IPSec_TCP_AES 03	3/22/2017 7:09 PM	File folder
IPSec_TCP_AES 04	3/22/2017 7:10 PM	File folder

Slika 47: Grupe izveštaja za TCP-IPsec-3DES

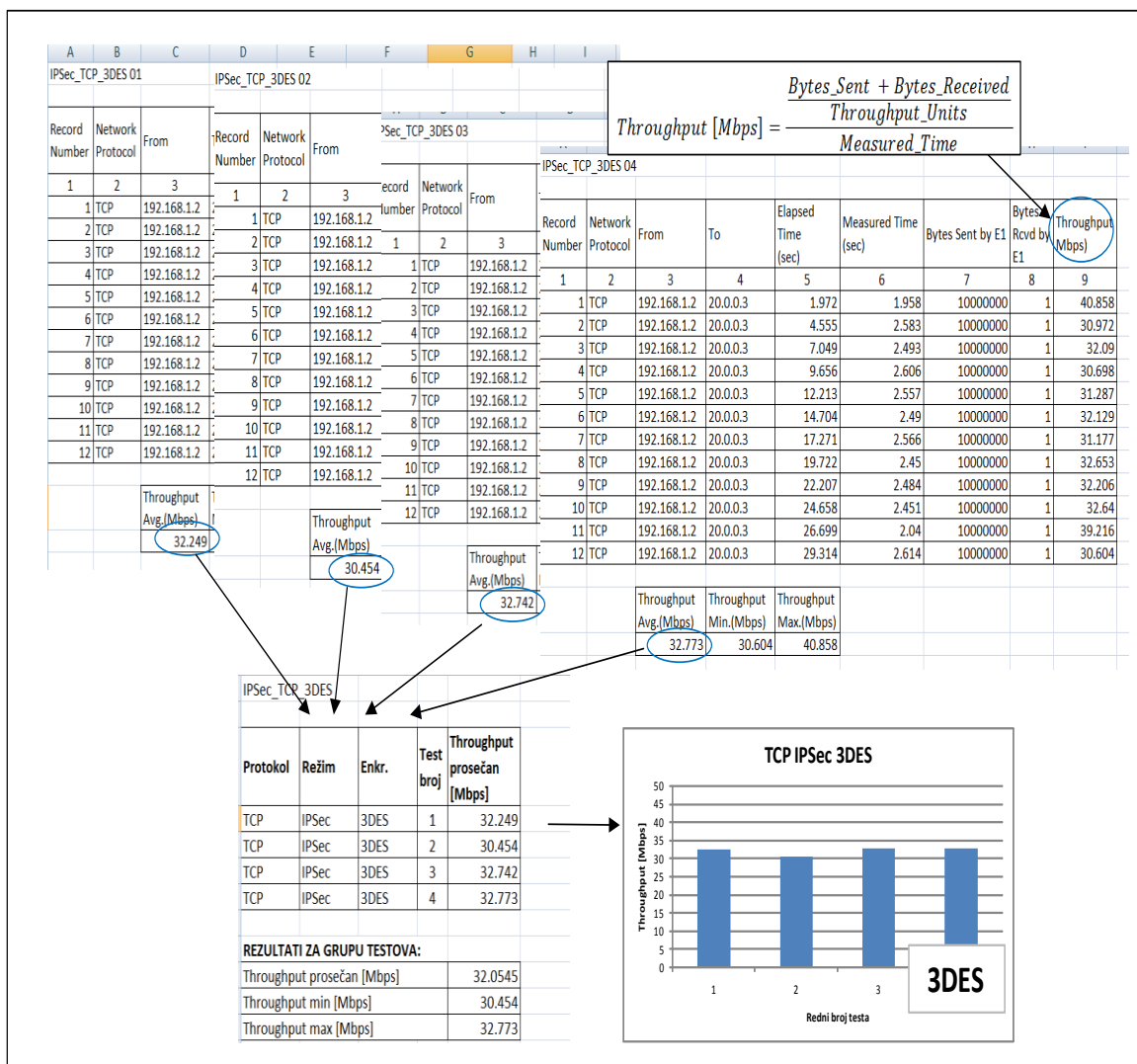
12.2 Način obrade podataka

Interesantni podaci su, radi obrade, uzimani iz izveštaja u .csv formatu. U zavisnosti od tipa saobraćaj (TCP ili UDP/VoIP) razmatrani su različiti podaci. Kod TCP protokola kao početni ulaz za obradu uzimana je vrednost parametra **throughput**.

Aplikacija, u konkretnom izveštaju a na osnovu izmerene vrednosti jedne transakcije, izračunava throughput po formuli:

$$[1] \quad \text{Throughput [Mbps]} = \frac{\frac{\text{Bytes}_{Sent} + \text{Bytes}_{Received}}{\text{Throughput}_{Units}}}{\text{Measured}_{Time}}$$

Za obradu podataka uzete su prosečne vrednosti throughput-a za čitav test (12 transakcija). Četiri prosečne vrednosti (iz četiri testa) korišćene su za formiranje tabela i grafika za potrebe analize podataka. Ova metodologija ilustrovana je na slikom 48.



Slika 48: Grupe izveštaja za TCP-IPSec-3DES

Sličan princip je korišćen prilikom obrade podataka za UDP/VoIP podatke. Razlika je u tome što su, pored throughput-a, obrađeni i podaci koji se odnose na jitter i one-way delay. Pored navedenog, aplikacija parametar throughput računa na drugačiji način nego za TCP protokol.

13. Rezultati eksperimenta

Nakon obrade, izvršena je analiza dobijenih podataka. Analiza je izvršena prvo za pojedinačne protokole sa jednim mehanizmom enkripcije, a nakon toga uporedna analiza za pojedinačne protokole sa oba mehanizma enkripcije.

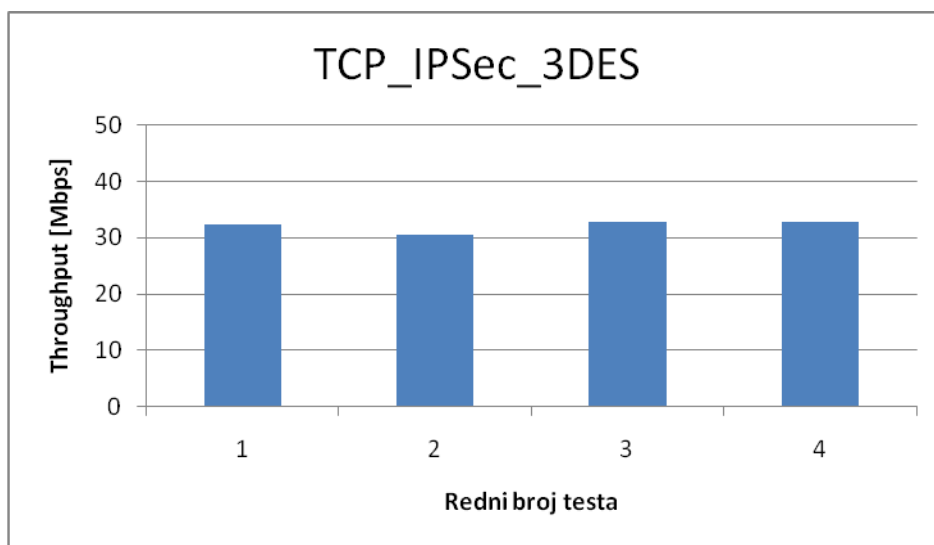
Analizom je utvrđeno da prosečna vrednost throughput-a za **TCP** protokol sa primenjenim **3DES** algoritmom enkripcije iznosi 32,054 Mbps. Odstupanja od prosečne vrednosti su u granicama koje ne ukazuju na mogućnost nepredviđene greške u merenju. Ovaj zaključak se izvodi na osnovu činjenice da je minimalna vrednost 30,454 a maksimalna 32,773 Mbps što predstavlja varijaciju u rasponu od - 4,99 do + 2,24 % u odnosu na prosečnu vrednost. Rezultati su prikazani u tabelama: 5 i 6, odnosno i na slici 49.

Tabela 5: Throughput za TCP sa 3DES - pojedinačni testovi

Protokol	Režim	Enkr.	Test broj	Throughput prosečan [Mbps]
1	2	3	4	5
TCP	IPSec	3DES	1	32.249
TCP	IPSec	3DES	2	30.454
TCP	IPSec	3DES	3	32.742
TCP	IPSec	3DES	4	32.773

Tabela 6: Throughput za TCP sa 3DES - grupa testova

Throughput prosečan [Mbps]	32.0545
Throughput min [Mbps]	30.454
Throughput max [Mbps]	32.773



Slika 49 : Throughput za TCP sa 3DES - pojedinačni testovi

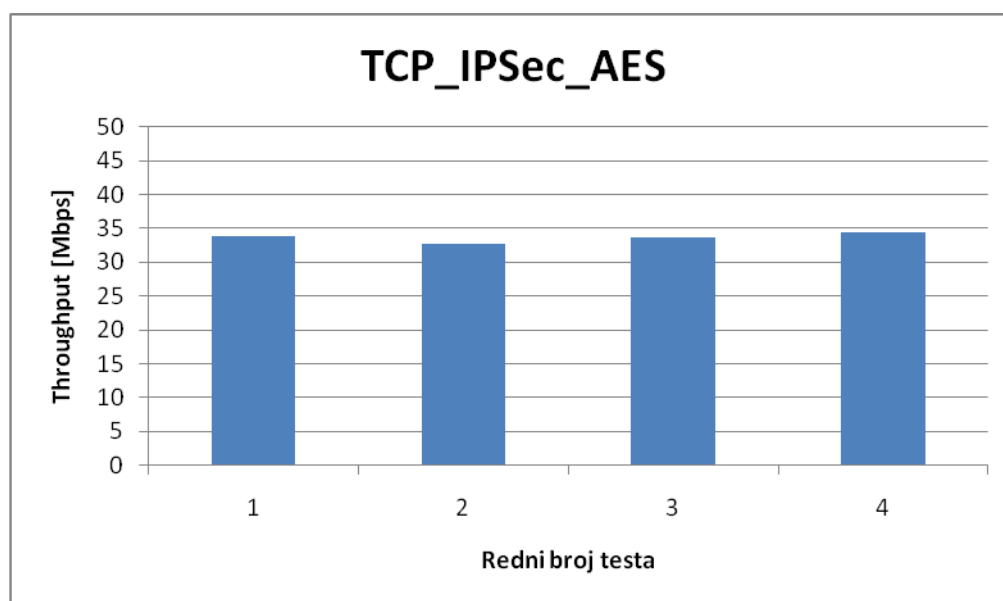
Prosečna vrednost throughput-a za **TCP** protokol sa primenjenim **AES** algoritmom enkripcije iznosi 32,892 Mbps. Odstupanja od prosečne vrednosti su, takođe, u prihvatljivim granicama. Minimalna vrednost je 32, 75 a maksimalna 34,479 Mbps, odnosno što predstavlja varijaciju u rasponu od - 2,8 do + 2,4 % u odnosu na prosečnu vrednost. Rezultati su prikazani u tabelama 7 i 8, kao i na slici 50.

Tabela 7 : Throughput za TCP sa AES - pojedinačni testovi

Protokol	Režim	Enkr.	Test broj	Throughput prosečan [Mbps]
1	2	3	4	5
TCP	IPSec	AES	1	33.892
TCP	IPSec	AES	2	32.75
TCP	IPSec	AES	3	33.61
TCP	IPSec	AES	4	34.479

Tabela 8: Throughput za TCP sa AES - grupa testova

Throughput prosečan [Mbps]	33.68275
Throughput min [Mbps]	32.75
Throughput max [Mbps]	34.479



Slika 50 : Throughput za TCP sa AES - pojedinačni testovi

Uporedna analiza za **TCP** sa **3DES** i **AES** enkripcijom izvršena je poređenjem prosečnih vrednosti throughput-a za svaki test pojedinačno, kao i za grupu testova. Izračunata je prosečna vrednost (tabela 7, kolona 5), utvrđeno je kod kog algoritma je veća, kao i za koliko (u mernim jedinicama, odnosno procentima, u odnosu na izračunatu srednju vrednost).

Ovom analizom, dolazi se do sledećih podataka:

- Prosečna vrednost throughput-a je viša za AES nego za 3DES enkripciju u svakom pojedinačnom testu (tabela 9, kolona 7) kao i za grupu testova (tabela 59, kolona 3);
- Razlika u korist AES-a se kreće od 2,62 do 7,97 % (0,868 do 2,296 Mbps) po pojedinačnim testovima, odnosno od 5,07 do 7,27 % (1,706 do 2,296 Mbps) za grupu testova.

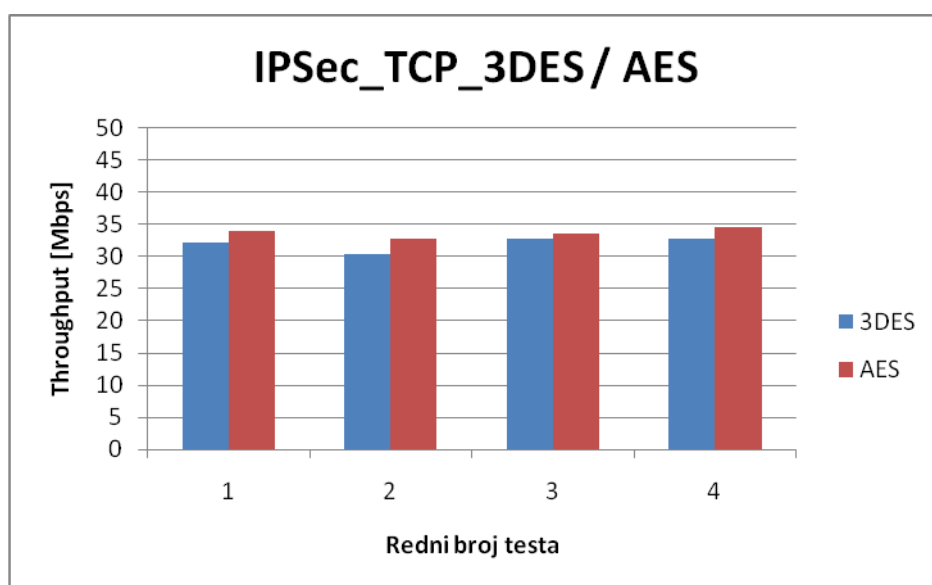
Podaci su prikazani u tabelama 9 i 10, kao i na slici 51.

Tabela 9: Komparacija throughput-a za TCP sa 3DES i AES - pojedinačni testovi

Protokol	Režim	Test broj	3DES Throughput prosečan [Mbps]	AES Throughput prosečan [Mbps]	Prosečna vrednost za 3DES i AES	Veći throughput ima	Za Mbps	% u odnosu prosečnu vrednost
1	2	3	4	5	6	7	8	9
TCP	IPSec	1	32.249	33.892	33.0705	AES	1.643	4.97
TCP	IPSec	2	30.454	32.75	31.602	AES	2.296	7.27
TCP	IPSec	3	32.742	33.61	33.176	AES	0.868	2.62
TCP	IPSec	4	32.773	34.479	33.626	AES	1.706	5.07

Tabela 10: Komparacija throughput-a za TCP sa 3DES i AES - grupa testova

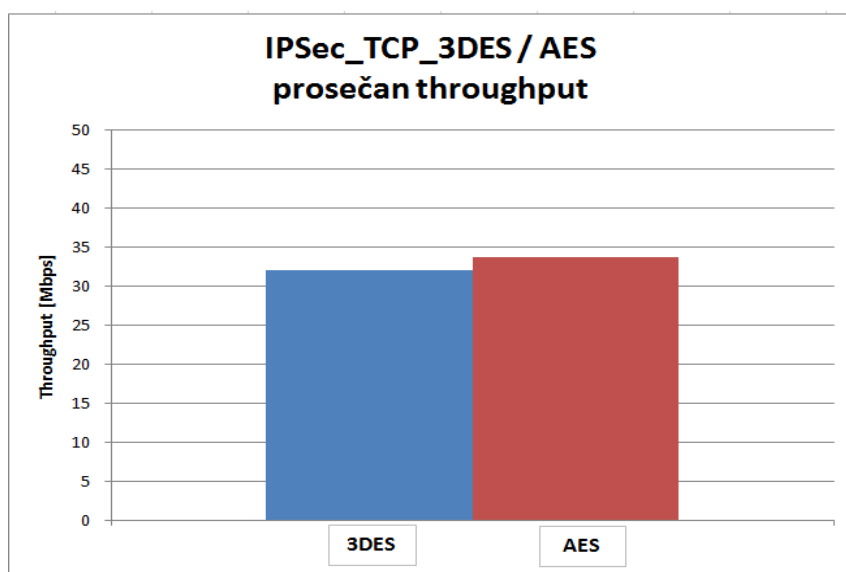
	3DES	AES	Prosek	Brži	Za Mbps	%
	1	2	3	4	5	6
Throughput prosečan [Mbps]	32.0545	33.68275	32.86863	AES	1.62825	4.95
Throughput min [Mbps]	30.454	32.75	31.602	AES	2.296	7.27
Throughput max [Mbps]	32.773	34.479	33.626	AES	1.706	5.07



Slika 51: Komparacija throughput-a za TCP sa 3DES i AES - pojedinačni testovi

Rezultati merenja pokazuju da postoji razlika u uticaju na performanse prenosa TCP saobraćaja u situaciji kada se koriste različiti mehanizmi enkripcije. Ova razlika počiva na razlici u algoritmima, odnosno njihovoj kompleksnosti. Različiti algoritmi uslovljavaju veće vreme potrebno za obradu (kriptovanje/dekriptovanje) paketa prilikom slanja i prijema. Koliko će to vreme biti zavisi od sposobnosti (procesorske moći) VPN gateway-a.

Razlika koja je uočena tokom ovog eksperimenta (5-7 %) u korist AES-a (slika 52), ne deluje značajno. Međutim, može da bude značajna ukoliko preko IPSec VPN tunela komuniciraju aplikacije za koje je granična vrednost koja obezbeđuje neometan rad oko 30Mbps.



Slika 52: Komparacija throughput-a za TCP sa 3DES i AES - grupa testova

Kada je reč o **UDP/VoIP** saobraćaju, izvršeno je poređenje throughput, jitter i delay parametara.

Analiza pokazuje da ne postoje apsolutno nikakve razlike između pomenutih parametara kod 3DES i AES enkripcije. Rezultati su prikazani u tabelama 11 i 12.

Tabela 11: Komparacija parametara za UDP/VoIP sa 3DES i AES - pojedinačni testovi

Test broj	Throughput Avg.(Mbps) 3DES	Throughput Avg.(Mbps) AES	Jitter Average (ms) 3DES	Jitter Average (ms) AES	One-Way Delay Average (ms) 3DES	One-Way Delay Average (ms) AES
1	2	3	4	5	6	7
1	0.064	0.064	0	0	1	1
2	0.064	0.064	0	0	1	1
3	0.064	0.064	0	0	1	1
4	0.064	0.064	0	0	1	1

Tabela 12: Komparacija parametara za UDP/VoIP sa 3DES i AES - grupa testova

	Throughput 3DES	Throughput AES	Jitter 3DES	Jitter AES	Delay 3DES	Delay AES
	1	2	3	4	5	6
Prosečan	0.064	0.064	0	0	1	1
Min	0.064	0.064	0	0	1	1
Max	0.064	0.064	0	0	1	1

Ovi podaci, na prvi pogled, mogu delovati čudno. Ali, ukoliko se razmotri način na koji iXchariot proračunava parametre (formula 2), kao i konkretne vrednosti za svaku transakciju, možemo da zaključimo da se razlike pojavljuju na trećoj i, ponegde, na drugoj decimali vremena izraženog u sekundama. Drugim rečima, razlika je reda veličina mili sekunde. Ova razlika se na throughput u Mbps odražava na četvrtoj decimali. Zaokruživanje throughput-a na treću decimalu dovodi do toga da se pomenuta razlika gubi. Opisana situacija je ilustrovana slikom 53 (UDP/VoIP sa AES enkripcijom, test broj 1).

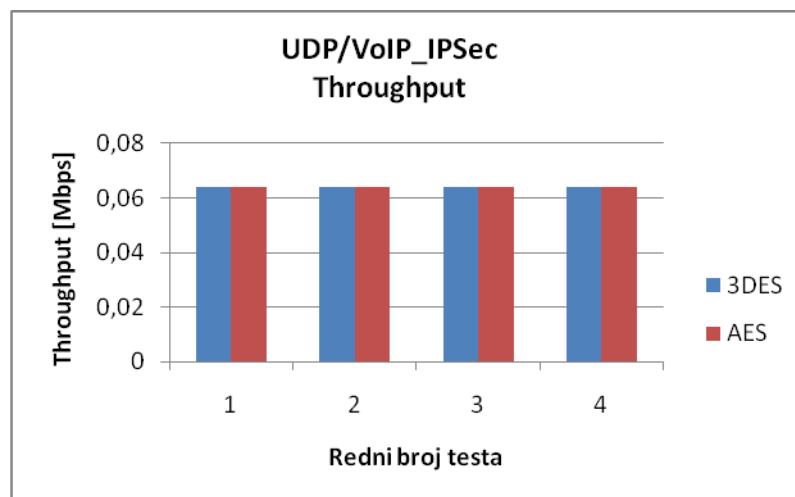
$$[2] \quad \text{Throughput}[\text{Mbps}] = \frac{\frac{\text{bytes}_{\text{received}}(\text{by E2})}{\text{Measured time [s]}}}{125000}$$

Record Number	Elapsed Time (sec)	Measured Time (sec)	Bytes Sent by E1	Bytes Rcvd by E2	Throughput (Mbps)	Izračunat throughput (Mbps)
1	2	3	4	5	6	7
1	2.985	2.981	24000	24000	0.064	0.06440792
2	5.985	3	24000	24000	0.064	0.064
3	8.987	3.002	24000	24000	0.064	0.06395736
4	11.987	3	24000	24000	0.064	0.064
5	14.988	3	24000	24000	0.064	0.064
6	17.989	3	24000	24000	0.064	0.064
7	20.99	3.001	24000	24000	0.064	0.06397867
8	23.991	3	24000	24000	0.064	0.064
9	26.994	3.002	24000	24000	0.064	0.06395736
10	29.994	2.999	24000	24000	0.064	0.06402134

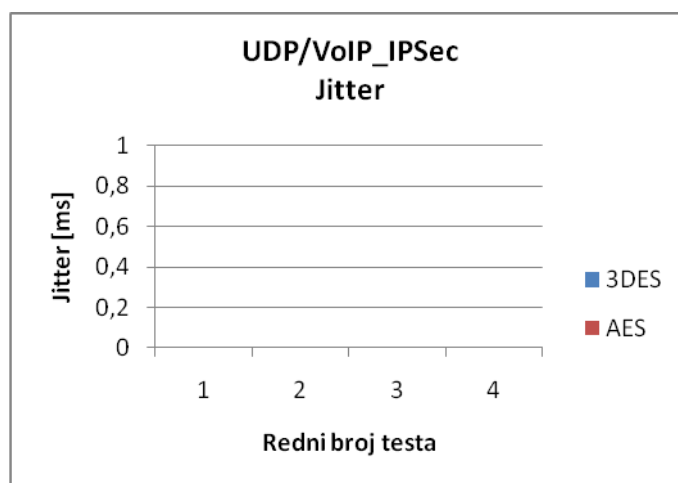
Slika 53: Primer razlike u vrednosti prikazanog i izračunatog throughput-a

S obzirom da je uticaj opisane razlike zanemarljiv, što se tiče konkretnog tipa prenosa (UDP/VoIP), ne uzima se u razmatranje, a analiza se vrši na zaokruženim vrednostima.

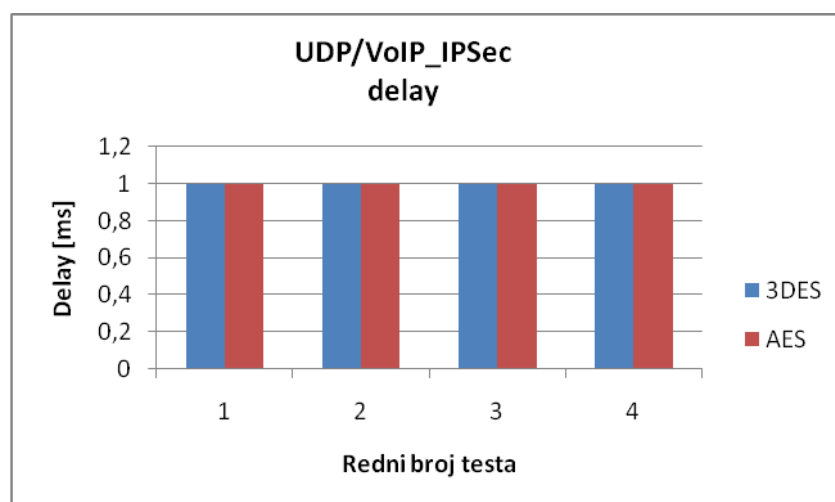
Vrednosti parametara za UDP/VoIP prikazane su na slikama 54, 55 i 56.



Slika 54: Komparacija throughput-a za UDP/VoIP sa 3DES i AES - pojedinačni testovi



Slika 55: Komparacija jitter-a za UDP/VoIP sa 3DES i AES - pojedinačni testovi



Slika 56: Komparacija delay-a za UDP/VoIP sa 3DES i AES - pojedinačni testovi

Ovde je očigledno da izbor tipa enkripcije nema nikakvog, praktičnog, uticaja na UDP/VoIP tip saobraćaja sa parametrima koji su postavljeni za potrebe realizacije merenja. Početni uslov po kom aplikacija iXchariot šalje podatke brzinom 64 kbps (u odnosu na teorijski moguć throughput VPN GTW 1 interfejsa - do 100 MB) predstavlja značajnu "olakšicu" hardverskim i softverskim resursima VPN gateway-a. Drugim rečima: količina podataka koju je potrebno obraditi po jedinici vremena je značajno manja od količina podataka za koje su konstruisani gateway-i.

U ovim okolnostima proces kriptovanja i dekriptovanja se realizuje brzinom koja omogućava, praktično, neometanu obradu UDP paketa za potrebe VoIP saobraćaja.

Vrednost delay-a (1 ms) ne utiče na kvalitet servisa, a ono što je još bitnije jeste da se ne pojavljuje, praktično, nikakva varijacija delay-a (jitter).

14. Zaključak

VPN-ovi, kao kompleksni mehanizmi zaštite informacija svoje funkcije vrše različitim protokolima

Ovi protokoli (s obzirom na prisutnu enkripciju, hash-ovanje i enkapsulaciju) uslovljavaju dodatno angažovanje softverskih i/ili hardverskih resursa i povećavaju količinu saobraćaja dodatnim zaglavlјima. Pored navedenog, mehanizmi enkripcije ostvaruju uticaj angažujući hardverske i softverske resurse pojedinih mrežnih elemenata.

Šifarski sistemi su jedan od delova VPN protokol stackova koji ostvaruju svoj uticaj u pomenutom smislu.

U ovom radu opisano je istraživanje uticaja različitih šifarskih sistema na performanse (karakteristike) IPSec VPN tunela. Istraživanje je realizovano analizom funkcionisanja mehanizama i podprotokola koji ulaze u sastav IPSec protokol stacka, sprovođenjem eksperimenta i analizom dobijenih rezultata.

Eksperiment je sproveden, na realnoj topologiji u laboratorijskim uslovima, formiranjem IPSec VPN tunela u tunelskom režimu. Vršen je prenos dva tipa podataka korišćenjem dva protokola transportnog sloja (datoteka veličine 100 MB-TCP protokol i VoIP datagrami-UDP protokol). U oba slučaja vršena je promena šifarskog sistema (jednog od parametara IPSec tunela). Reč je o 3DES i AES šifarskim sistemima.

Sprovedenim eksperimentom došlo se do podataka koji nedvosmisleno ukazuju da, kada je reč o TCP saobraćaju kojim se prenosi datoteka određene veličine, postoji razlika u performansama mreže u zavisnosti od primenjenog šifarskog sistema. Prosečna vrednost ove razlike (za throughput) iznosi 6%. Izmereni throughput je viši tokom primene 3DES šifarskog sistema.

Značajne razlike, kada je reč o performansama mreže pri prenosu VoIP/UDP saobraćaju, nisu uočene.

Ovim istraživanjem je dokazano da se performanse mreže za prenos podataka na kojoj je primenjen VPN tunel razlikuju u zavisnosti od primenjenog mehanizma enkripcije. Pored ovoga, dokazano je da su performanse niže ukoliko je primenjeni mehanizam enkripcije kompleksniji.

Degradacija performansi nastala na ovaj način, može da dovede do nemogućnosti korišćenja aplikacija baziranih na TCP protokolu ukoliko je granični throughput oko 30 Mbps. Aplikacije koje funkcionišu na UDP protokolu sa niskim throughputom neće imati poteškoće u funkcionisanju.

Literatura

- [1] CCNA Online Curriculum Version 5, Cisco Systems, <http://ccna-v5.weebly.com>, (pristup mart 2017.godine)
- [2] CCNA Exploration v4.0 Curriculum, Cisco Systems, 2007
- [3] TCP (Transport Control Protocol), RFC 793 (Septembar 1981). The Internet Engineering Task Force. IETF.
- [4] UDP (User Datagram Protocol), RFC 768 (Avgust 1980). The Internet Engineering Task Force. IETF.
- [5] IPv4 (Internet Protocol version 4), RFC 791 (Septembar 1981). The Internet Engineering Task Force. IETF.
- [6] M. Veinović, S. Adamović, Kriptologija I, Univerzitet Singidunum, Beograd, 2013.
- [7] W. Stallings, Cryptography and Network Security, Prentice Hall, 2005.
- [8] A. Al-Tamimi (2011). Performance analysis of data encryption algorithms. Electronics Computer Technology (ICECT), 2011 3rd International Conference on Vol.5 (pp. 399-403). IEEE
- [9] M. Milosavljević, S. Adamović, Kriptologija 2, Univerzitet Singidunum, Beograd, 2014.
- [10] S. Narayan, S. Kolahi, K. Brooking, S. de Vere (2008). Performance Evaluation of Virtual Private Network Protocols in Windows 2003 Environment. International Conference on Advanced Computer Theory and Engineering, 2008. ICACTE '08 2008. International Conference on Advanced Computer Theory and Engineering. IEEE
- [11] CCNA Security: Implementing Network Security 2.0, Cisco Systems, 2016
- [12] M. Veinović, A. Jevremović, Uvod u računarske mreže, Univerzitet Singidunum, Beograd, 2007.