

**UNIVERZITET SINGIDUNUM**
DEPARTMAN ZA POSTDIPLOMSKE STUDIJE

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

Davor Grce

# Zaštita računarskih mreža – Primena politika bezbednosti i procedura u kontekstu povećanja pouzdanosti i bezbednosti računarskih mreža

**- Master rad –**

Mentor:
Prof. dr. Aleksandar Jevremović

Student:
Davor Grce
Br. indeksa: 2015/410351

Univerzitet Singidunum

# Sadržaj

Uvod....6
1 Pojam metodologije....7
1.1 Metodologija istraživačkog projekta....7
1.2 Definisanje strategije i oblasti prilikom istraživanja....7
1.3 Analitički osvrt na vrstu korišćenih hipoteza....7
1.3.1 Opšta hipoteza....7
1.3.2 Radna hipoteza....8
2 Računarske mreže....8
2.1 Istorija računarskih mreža....8
2.2 Vrste prenosa informacija kroz računarsku mrežu....8
2.2.1 Postupak prenosa informacija sa komutacijom linkova....8
2.2.2 Postupak prenosa informacija sa komutacijom paketa....9
2.3 Podela računarskih mreža....10
2.3.1 Lokalna mrežna okruženja (LAN)....10
2.3.2 Regionalna mrežna okruženja (WAN)....11
2.3.3 Gradske ili kampus računarske mreže (MAN)....11
2.3.4 Personalne regionalne računarske mreže (PAN)....11
2.4 Referentni OSI model....11
2.4.1 Istorija Referentnog OSI modela....12
2.4.2 Fizički sloj....14
2.4.3 Sloj veze....14
2.4.3.1 Kontrola pristupa mediju (MAC)....14
2.4.3.2 Kontrola logičkih linkova (LLC)....14
2.4.4 Mrežni sloj....15
2.4.5 Transportni sloj....15
2.4.6 Sloj sesije....16
2.4.7 Prezentacioni sloj....16
2.4.8 Aplikativni sloj....16
2.5 Serverske mreže....17
2.5.1 Serveri podataka i štampanja....18
2.5.2 Serveri kontrole pristupa....18
2.5.3 Serveri za manipulaciju sa podacima....19
2.5.4 Aplikacioni serveri....20
2.5.5 Komunikacioni serveri....21

2.6 Sistem kontrole pristupa – bezbednost sistema i smanjenje rizika ..... 21
2.6.1 Ograničenje fizičkog pristupa resursima ..... 21
2.6.2 Parametri pristupa ..... 22
2.6.3 Nivoi pristupa ..... 23
2.6.3.1 Pristup operativnom sistemu ..... 23
2.6.3.2 Pristup aplikacijama ..... 23
2.6.3.3 Pristup bazi podataka ..... 24
2.6.3.4 Pristup mrežnoj opremi ..... 25
2.6.3.5 Pristup računarskim mrežama preko privatnih virtualnih mreža ..... 26
2.6.4 Centralizacija kontrole pristupa AAA (Authentication, Authorization and Accounting) ..... 27
2.6.5 „AAA“protokoli ..... 28
2.6.5.1 RADIUS ..... 28
2.6.5.2 Kerberos ..... 31
2.6.5.3 TACACS+ ..... 32
2.6.5.4 Diameter ..... 32
3 Kriptografija ..... 34
3.1 Osnovni pojmovi ..... 35
3.1.1 Simetričan model ..... 35
3.1.1.1 DES ..... 36
3.1.1.2 AES ..... 37
3.1.2 Asimetričan model ..... 38
4 Digitalna forenzika ..... 39
4.1 Uopšteno ..... 39
4.2 Procesi ..... 40
4.3 Korisni alati ..... 40
4.3.1 Kratak opis korišćenijih forenzičkih alata ..... 40
5 Studijsko istraživački rad – Primenjeno tehnološko rešenje ..... 44
5.1 Uloga ..... 44
5.2 Tipovi ..... 45
5.3 Klasifikacija ..... 45
5.4 Tehničke karakteristike izabranog uređaja ..... 46
5.5 IPSec VPN ..... 47
5.5.1 Podela IPSec VPN mreža ..... 48
5.5.2 Koraci prilikom realizaciji sigurnog tunela ..... 48
5.6 Konfigurisanje daljinskog pristupa VPN klijenta (studija slučaja) ..... 49
5.6.1 Korak 1: Konfiguracija IP adresnog opsega ..... 49

5.6.2 Korak 2. Izuzimanje NAT-a nad kriptovanim saobraćajem ....49
5.6.3 Korak 3: Kreiranje i konfigurisanje grupne polise ....49
5.6.4 Korak 4: Konfigurisanje parametara pristupa ....50
5.6.5 Korak 5: Konfigurisanje IPSec FAZA 1 (IKEv1-Policy) ....50
5.6.6 Korak 6: Konfigurisanje IPSec FAZA 2 (Parametrizacija) ....50
5.6.7 Korak 7: Kreiranje i konfigurisanje tunel grupe ....50
5.6.8 Korak 8: Konfiguracija VPN klijenta ....51
5.6.9 Korak 9: Verifikacija uspostavljenog tunela zaštićenog saobraćaja ....51
6 Studijska praksa - Primenjena procedura prema ISO/IEC 27001 – ISMS ....52
6.1 Procedura regulisanja prava pristupa – opšta pravila ....52
6.1.1 Svrha dokumenta ....52
6.1.2 Korišćeni termini ....52
6.1.3 Skraćenice ....53
6.1.4 Opšte informacije ....53
6.1.4.1 Podnosilac zahteva za pristup ....53
6.1.4.2 Način pristupa ....53
6.1.4.3 Tip pristupa ....54
6.1.4.4 Dužina trajanja pristupa ....54
6.1.4.5 Prioritet pristupa ....54
6.1.4.6 Nadležne osobe za realizaciju ....54
6.1.5 PROCEDURA ....54
6.2 Procedura regulisanja prava VPN pristupa ....56
6.2.1 Svrha ....56
6.2.2 Korišćeni termini ....56
6.2.3 Skraćenice ....57
6.2.4 Opšte informacije ....57
6.2.4.1 Opšte karakteristike VPN pristupa sistemu ....57
6.2.4.2 Pravila upotrebe i ograničenja VPN pristupa ....57
6.2.5 PROCEDURA ....58
6.2.6 Aktivnosti prilikom kreiranja VPN korisničkih naloga ....58
6.2.7 PRILOZI ....60
6.2.7.1 Prilog 1 – Zahtev za VPN pristup ....60
6.2.7.2 Prilog 2 – Evidencija lica sa odobrenim stalnim VPN pristupom ....61
6.2.7.3 Prilog 3 – Evidencija lica sa odobrenim privremenim VPN pristupom ..61
6.3 Procedura administracije korisničkih naloga ....62
6.3.1 Svrha ....62
6.3.2 Opšte informacije ....62

6.3.2.1 Definicija korisničkih naloga.....62
6.3.2.2 Administracija aplikativnih korisničkih naloga.....62
6.3.2.3 Administriranje sistemskih korisničkih naloga .....62
6.3.2.4 Opšta pravila upotrebe i čuvanja korisničkih naloga.....63
6.3.2.5 Opšta pravila kreiranja, upotrebe i čuvanja korisničkih imena i lozinki .63
*ZAKLJUČAK*.....65
*LITERATURA* .....66

# Uvod

Pojam računarskih mreža ili računarske mreže za prenos podataka predstavlja sistem telekomunikacionih linkova kojima se ostvaruje veza između računara, pomoću permanentnog ili privremenog linka. Kako bi se ostvarila pomenuta komunikacija potrebno je postojanje odgovarajućeg hardvera i softvera, te poznavanje procesa umrežavanja kroz implementaciju određenih standarda, pravila ili protokola.
Cilj umrežavanja je ostvarivanje kvalitetne veze u cilju razmene informacija (podataka) i resursa između definisanih tačaka prenosa. Ostarena veza je realizovana fizičkim linkom između više instanci preko kabla ili bežičnim putem. Pomenuta komunikacija ne bi bila moguća bez postojanja aktivne mrežne opreme, neophodne za prenos (svič), usmerenje paketa (ruter) i blokade mrežnog saobraćaj (fajervol) po predefinisanim pravilima.
U modernom poslovanju vreme i novac su u bliskoj vezi, i shodno tome brzina prenosa podataka predstavlja esenciju razvoja savremenih računarskih sistema. Imajući u vidu kvalitet podataka, interes za zloupotrebu i krađu intelektualne svojine krajnjeg korisnika sa vremenom postaje sve veća. Sa tim u vezi, razvili su se razni modaliteti napada i zloupotrebe podataka krajnjeg korisnika. U cilju sprečavanja i potpune zaštite intelektualne svojine primenjeni su razni sigurnosni sistemi i procedure kao što su fajervol, antivirusni programi, napredni antimalver sistemi detekcije i prevencije napada IDS i IPS i napredni kriptografski protokoli, politike bezbednosti i procedure. U prvom delu rada ću opisati metodologiju naučnog istraživanja i analizu projekta u kontekstu ekspertize računarskih komponenti i protokola neophodnih za pouzdanu mrežnu komunikaciju, primenjenu u cilju ostvarivanja bezbednog toka informacija.
Drugi deo rada ogleda se u definisanju digitalne forenzičke analize kao naučne discipline, opisu izabranog infrastrukturnog rešenja, strukturi upućenog zahteva od strane spoljnog saradnika i realizaciji zahteva uz poštovanje pisanih procedura, koje čine sastavni deo ove prezentacije. Naime, pisane procedure predstavljaju dobru proizvođačku praksu, u oblasti strukovnog delovanja uz njihovu punu primenljivost. Uzimajući u obzir mogućnost čestih promena, koje se u informatici dešavaju periodično (promena zaposlenih i pozicija delovanja, promena adresa bitnih instanci sistema i ostalih zakonskih izmena), potrebno ih je menjati u skladu sa dinamikom koja prati realno stanje stvari. Politike bezbednosti informacija i njihovu implementaciju, tj. ciljeve bezbednosnih mera, primenjene mere i politike, procese i procedure koje čine sastavni deo, treba nezavisno preispitivati u planiranim intervalima, ili kada nastupe značajne izmene u implementaciji bezbednosti informacija kako bi se osigurala kontinuirana pogodnost, adekvatnost i efektivnost pristupa upravljanju bezbednosti informacija. Studija slučaja praktično je pokazala algoritam po kojem se realizuje dospeli zahtev od strane ugovorno vezanih spoljnih saradnika.

Imajući u vidu rasprostranjenost i široka upotreba računara i mobilnih uređaja, kao i količine informacija koje se svakodnevno mere egzaktnom materijalnom vrednošću, jasno definisanje pravila predstavlja esenciju informatičke pismenosti. Propisani zakoni i standardi iz oblasti informacionih tehnologija usmeravaju društvo u pravcu povećanja bezbednosti informacija i podataka kao i aktivno i proaktivno delovanje kroz forenzičke analize potencijalnih pretnji i incidenata uz sankcionisanje prevara i zloupotreba.

# 1 Pojam metodologije

Metodologija predstavlja egzaktnu nauku koja proučava moguće puteve i metode, kojima se omogućava dolaženje do naučnih spoznaja o društvenim, materijalnim i duhovnim vrednostima sveta. Metodologija kao nauka predstavlja meta nauku u celini, čiji je cilj uspešno definisanje jezgra naučne discipline, tj., spoznaje i definisanje osnovnih principa dostizanja kritičkog preispitivanja u okviru nje. Suština nauke o Metodologiji je težnja za dostizanje što tačnije i objektivnije spoznaje o nama samima i svetu oko nas..

## 1.1 Metodologija istraživačkog projekta

Prvi pristupni rad ima za cilj da definiše pojmove vezane za savremene računarske mreže, njihovu konstrukciju, politike bezbednosti, procedure i protokole. Projektni zadatak predstavlja kako organizacione tako i tehnološke aspekte zaštite računarskih mreža. Predstavljena su brojna savremena rešenja u pogledu implementacije i funkcionalnosti, kao i mnoga koja su u fazi buduće upotrebljivosti.
Projektni zadatak izrađen je korišćenjem praktičnih i teoretskih znanja iz oblasti računarskih mreža, sa akcentom na raspoložive tehnike daljinskog pristupa kroz slobodnu mrežu Internet.

## 1.2 Definisanje strategije i oblasti prilikom istraživanja

Oblast istraživanja su računarske mreže, odnosno tehnike daljinskog pristupa, autentifikacije, autorizacije i monitoring korisnika i/ili procesa.
Može se reći da je bezbednost računarskih mreža direktno povezana sa samim IT administratorom koji je zadužen za održavanje te mreže. Ključna pitanja na koja su traženi odgovori tokom istraživanja su:

- Funkcionisanje računarskih mreža;
- Koje vrste zaštita računarskih mreža postoje i kako se one uvode;
- Koje vrste daljinskog VPN pristupa postoje i kako se one sprovode;
- Koji protokoli su korišćeni za proveru identiteta korisnika na zahtev;
- Sistem generisanja i distribucija kriptoloških ključeva u procesu ostvarivanja;
- Metodologija i primenjeni alati prilikom procesa Digitalne forenzičke analize;
- Primena pisanih procedura i pravila u kontekstu potovanja bezbednog pristupa korporativnom okruženju kroz nesigurnu mediju;

## 1.3 Analitički osvrt na vrstu korišćenih hipoteza

### 1.3.1 Opšta hipoteza

U prvom delu ove prezentacije težište istraživanja se zasnovano na opisu tehničkih karakteristika računarskih mreža, vrstama i pod vrstama, logičkim modelom sistema interkonekcije, metodama, tehnikama i protokolima zaštite podataka kroz šifrovanje i dešifrovanje paketa u prenosu preko nesigurnog medija. Učesnici u transferu podataka su skoro sigurni da neće doći do zloupotrebe, korupcije ili izmene šifrovanog paketa.
U drugom delu rada opisan je praktičan primer sprovodljivosti pisanih procedura i pravila koja su proizašle iz pisanog međunarodnog standarda u vezi sa bezbednošću informacija i podataka ISO/IEC 27001. Takođe, opisana je i oblast Digitalne forenzičke analize, sa akcentom na primenjene alate u realnom okruženju i njihove sprovodljivosti u aktivnom i proaktivnom delovanju.

### 1.3.2 Radna hipoteza

U ovom radu prezentuje se i sublimira praktičan primer sprovodljivosti pisanih procedura i pravila sa usvojenim tehnologijama prenosa podataka, kontrole pristupa i šifrovanja mrežnog saobraćaja. Procedure i pravila su proizašle iz pisanog standarda u vezi sa bezbednošću informacija i podataka ISO/IEC 27001. Takođe, u dela radu je pokrivena oblast Digitalne forenzičke analize, sa akcentom na primenjene alate u realnom okruženju i njihove sprovodljivosti u aktivnom i proaktivnom delovanju.

# 2 Računarske mreže

Računarska mreža predstavljaju grupu računara i drugog računarskog hardvera, koja je vezana preko permanentnog komunikacionog linka (kanala) u cilju razmene podataka i resursa između velikog broja korisnika na mreži. U zavisnosti od trajanja uspostave sesije razlikujemo stalne (permanentne) i privremene veze. Mreže se kategorizuju na osnovu njihovih bazičnih karakteristika. Za uspešnu uspostavu veze potreban je odgovarajući hardver i softver. Uopšteno, opseg informacija koji se prenosi kroz širopojasne i druge mreže je velik, od tekstualnih informacija, govora, videa do elektronske pošte i drugog.

## 2.1 Istorija računarskih mreža

Jedan od najranijih primera računarskih mreža je grupa umreženih računara u funkciji razvoja sistema odbrane za američku vojsku, pod nazivom "SAGE". Tokom 1969. godine, Univerzitet u Kaliforniji i Univerzitet u Utah su se mrežno povezali čineći deo projekta zvanog „ARPANET“. Osnova pomenute mreže, tokom vremena, je evoluirala u ono što danas nazivamo Internetom. ARPANET je u osnovi računarska mreža sa komutativnom razmenom paketa.
Ubrzo nakon postavljanja bazičnih standarda u pogledu razmene podataka pojavile su se mreže:

- ALOHAnet;
- Telnet;
- Cyclades;
- Tymnet
- SNA (IBM-ova mreža).

## 2.2 Vrste prenosa informacija kroz računarsku mrežu

U složenim mrežnim okruženjima razlikujemo dva tipa (načina) prenosa informacije u elektronskom obliku. Prvo uspostavljeni način prenosa podataka se odnosi na fiksiranje putanje tokom uspostave sesije između dve instance (komutacijom linka).
Drugo uspostavljeni način prenosa se odnosi na segmentiranje poslate informacije (paketni prenos podataka) koji se šalje prema odredištu sa potencijalno različitim uspostavljenim putevima.
Komutacija po svojoj definiciji prestavlja zamenu redosleda, koja se u računarskim mrežama odnosi na prenos podataka na zahtev, skupom dve ili više instanci uključenih u mrežnu komunikaciju.

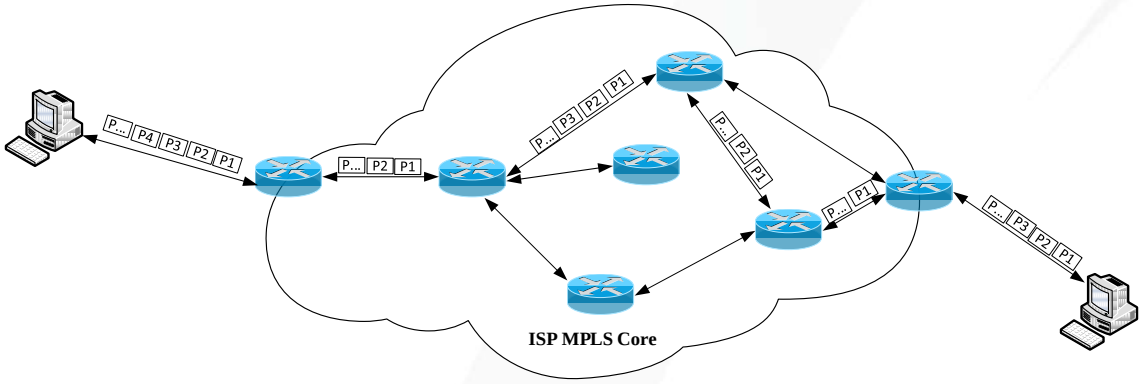
### 2.2.1 Postupak prenosa informacija sa komutacijom linkova

U ovom postupku prenosa informacija uspostavlja se direktna veza između dve ili vise komutacionih jedinica čiji je zadatak uspostava konzistentnog linka instanci u prenosu.
Čitava komunikacija se inicira od strane predajnika (pošiljaoca), koji pokušava da uspostavi konzistentan link sa destinacionim prijemnikom (primaocem) informacija,

kreirajući virtualnu privatnu mrežu, čija će sesija trajati do prekida linka. Praktičniji primer prenosa informacija sa komutacijom linka je uspostavljanje telefonske sesije dva korisnika. U računarskim mrežama prenos informacija sa komutacijom linkova opisuje se u tri faze:

- Faza 1. opisuje direktnu uspostavu linka/sesije;
- Faza 2. opisuje prenos informacije u elektronskom obliku;
- Faza 3. opisuje prekid linka.

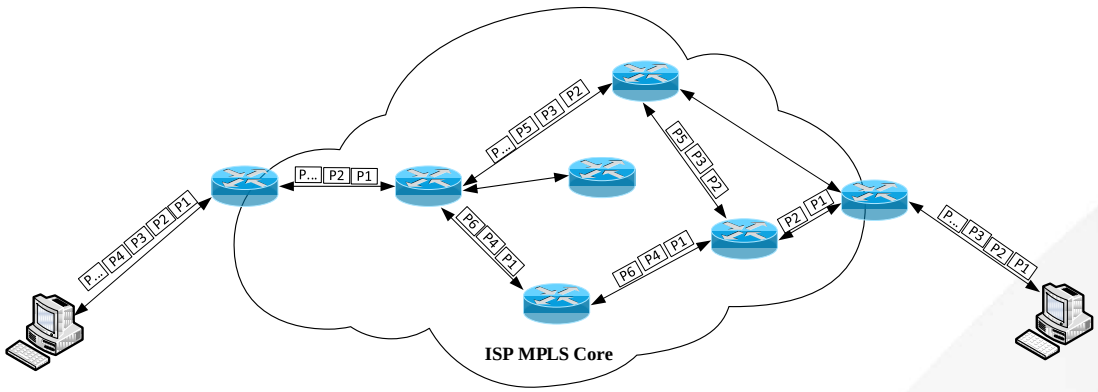
Ako računar (PC1 sa leve strane, slika 1.), želi da komunicira sa računarom (PC2 sa desne strane, slika 1.), računar PC1 šalje zahtev komutatorskoj jedinici R2 da se uspostavi željena veza. Komutatorska jedinica povezuje liniju PC1-R1 sa linijom PC2-R2 i tako uspostavljaju vezu PC1-PC2. Linija PC1-PC2 postoji sve dok se odvija komunikacija između stanice PC1 i PC2. Veza se raskida kada se komunikacija završi. Na isti način stanica PC1 može da uspostavi vezu sa bio kojom drugom stanicom.
U tom slučaju ne moraju postojati stalne veze između svake instance, već samo između onih koji komuniciraju. Ovim načinom je potrebno manje linija nego kod potpunog međusobnog povezivanja. Komutator je elektronski ili elektro-mehanički uređaj koji nema mogućnost pamćenja poruke i njenog kasnijeg otpremanja: ako su sve izlazne linije zauzete zahtevana veza se ne može uspostaviti [3].




Slika 1. Prenos podataka sa komutacijom veza

### 2.2.2 Postupak prenosa informacija sa komutacijom paketa

Prenos informacija sa paketnom komutacijom predstavlja povezivanje instanci u cilju uspostavljanja konzistentnog linka, paketnom segmentacijom na manje celine, poštujući pravila i procedure transportnih protokola. Logički gledano, svaki paket se šalje do prvog i najbližeg mrežnog čvorišta, koji prosleđuje pakete do odredišnog rutera, preusmeravajući se po predefinisanim pravilima, nezavisno, na mrežnim uređajima (ruterima) u prenosu paketa. Imajući u vidu činjenicu da se paketi mogu slati različitim putanjama, u zavisnosti od mnogih faktora u trenutku prenosa (prolaznom prostoru, propusnom opsegu, dostupnosti određenih ruta, itd), informacija je kompletirana u trenutku pristizanja svih paketa na destinacionu instancu. Ovaj način prenosa ne može dovesti do prekida tokom sesije, sem u iznimnim situacijama prilikom direktnog prekida mrežne komunikacije predajnika i prijemnika sa prvom fizičkom instancom na liniji prenosa. Primer pomenutog prenosa je ostvaren u svim savremenim mrežnim komunikacijama.[3]




Slika 2. Prenos podataka sa komutacijom paketa

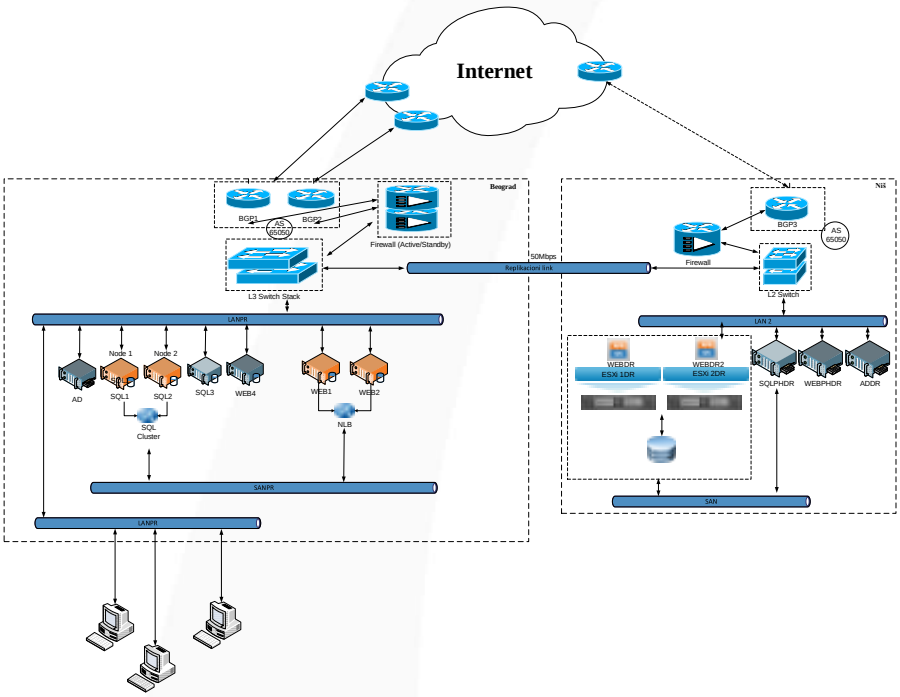
## 2.3 Podela računarskih mreža

Prema prostoru na kojem se prostiru, mrežna okruženja se dele na:

- Lokalna mrežna okruženja LAN
- Regionalna mrežna okruženja WAN
- Gradske ili kampus računarske mreže MAN
- Male regionalne računarske mreže PAN

### 2.3.1 Lokalna mrežna okruženja (LAN)

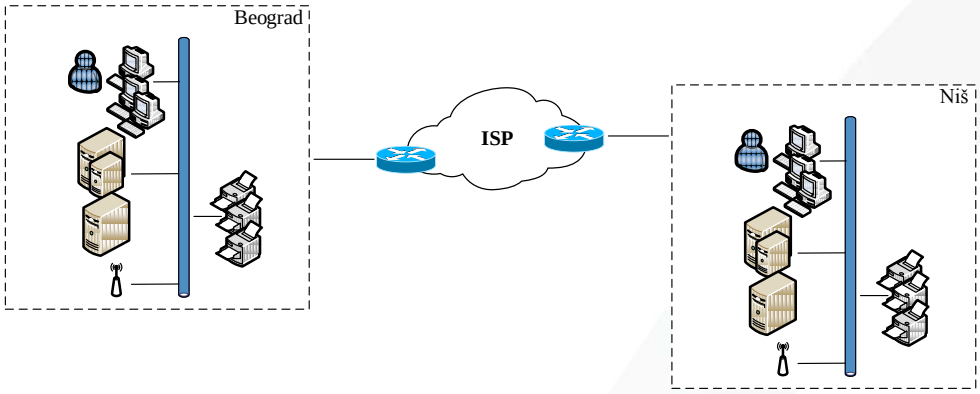
Mala lokalna mreža je mreža velike brzine, koja predstavlja osnov svake mreže. U zavisnosti od broja računara na mreži može biti jednostavna ili složena. U svakom slučaju računarska mreža je prostorno ograničena. Komunikacija se odvija na drugom sloju lejer 2 (svičevi, habovi).[3]




Slika 3. Lokalna mrežna okruženja

### 2.3.2 Regionalna mrežna okruženja (WAN)

Mreža nije prostorno ograničena i može povezivati računare širom sveta (gradova, regiona ili država). Mreža je segmentirana i međusobno povezana u regionalnu računarsku mrežu. Protokoli kao što su SONET/SDH, MPLS, ATM i frejm rilej se često koriste kako bi omogućili funkcionisanje regionalne računarske mreže. U ranim fazama za realizaciju mreže korišćen je X.25 protokol koji se smatra pretečom frejm rilej protokola. Brzina prenosa kod ovakvih mreža kretale su se od 1200 b/s do 6 Mbit/s, dok je kod određenih DSL linkova brzina prenosa išla do 156Mbit/s (telefonski, bežični i satelitski linkovi).




Slika 4. Regionalne računarske mreže

### 2.3.3 Gradske ili kampus računarske mreže (MAN)

Računarska mreža koja povezuje korisnike sa računarskim resursima u geografskom području ili regionu, koja je ponekad prostorno veća i od same lokalne računarske mreže LAN, ali je ipak manja nego što pokriva regionalna mrežna okruženja. Termin se vezuje za računarske mreže locirane u gradu, koje su vezane za prostorno veće računarske mreže WAN. Takođe se koriste da povežu nekoliko lokalnih mreža kreirajući centralnu mrežu za određeni region (kampus).
Mreža je koncipirana na način da pruža konzistentne i brze širokopojasne linkove, brzih servisa, u okvirima definisanih geografskih celina, gradova, kampusa i opština.

### 2.3.4 Personalne regionalne računarske mreže (PAN)

Personalne regionalne mreže PAN su geografski lokalizovane računarske mreže od svega nekoliko metara, korišćenje u cilju prenosa podataka između uređaja (računara, telefonskih uređaja i personalnih digitalnih asistenata). PAN mreža se može koristiti za komunikaciju između personalnih uređaja inter personalno (među sobom), ili veza sa višim nivoima mreža prema Internetu (uplink).
Primeri mreža koji se u osnovi oslanjaju na PAN arhitekturu su: bežična personalna regionalna mreža – WPAN (IrDA, blutut, vajrles USB, BAN).[3]

## 2.4 Referentni OSI model

Referentni model otvorenog sistema interkonektivnosti OSI je konceptualan model koji globalno karakteriše i standardizuje komunikacione funkcionalnosti u okviru telekomunikacija ili računarskih sistema bez obzira na njihove bazične interne strukture i tehnologije. Referentni model opisuje kretanje informacija kroz medije, sa jednog računara do drugog. Osnovni cilj modela je interoperabilnost različitih komunikacionih sistema sa pripadajućim standardizovanim protokolima i procedurama. Originalna verzija OSI modela

se sastoji od sedam jasno definisanih slojeva. Slojevi referentnog modela su koncipirani na način da svaki sloj služi sloju iznad i ispod njega. Na primer, sloj koji je odgovoran za mrežnu komunikaciju bez grešaka (statefull connection - TCP, 4 lejer) generiše putanju koja je neophodna aplikacijama na višim nivoima, dok upitom nižih slojeva šalje i prima pakete koji sadrže i sadržaj tog puta. Dve instance na istom nivou su prikazane da su u vezi, horizontalnom konekcijom po istom sloju na obe strane komunikacije.
OSI model je u osnovi projekat usvojen od strane Internacionalne organizacije za standardizaciju ISO, koji se vodi pod jedinstvenim oznakom ISO/IEC 7498-1.

### 2.4.1 Istorija Referentnog OSI modela

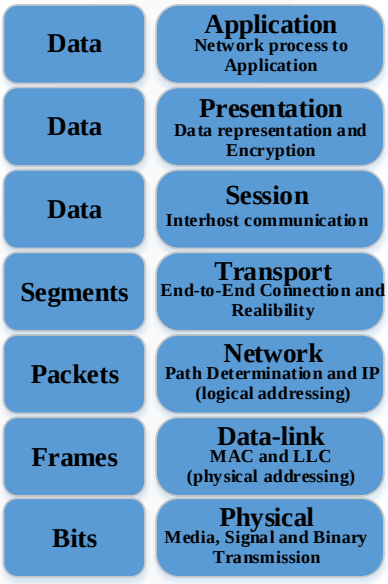
Krajem sedamdesetih godina prošlog veka pojavio se interes za definisanjem jedinstvenog standarda u vezi sa arhitekturom mrežnog sistema i njihovom interkonektivnošću. U izradi i definisanju jedinstvenog standarda učestvovali su International Organisation for Standardisation (ISO) i International Telegraph and Telephone Consultative Committee (CCITT).
Tokom 1983.godine usaglašeni su stavovi zainteresovanih grupacija u formi jedinstvenog dokumenta zvanog „Bazični referencijalni model za interkonektivne otvorene sisteme BRMOSI". [4]

<table>
<tr><th colspan="2">Slojevi</th><th>Protokoli</th><th>Uređaji</th><th>Enkapsulacija</th></tr>
<tr><td colspan="2">Aplikacije</td><td>• HTTP<br>• TELNET<br>• FTP<br>• TFTP<br>• SNMP</td><td rowspan="4"></td><td>Korisničke informacije i podaci</td></tr>
<tr><td colspan="2">Prezentacije</td><td>• JPEG, BMP, TIFF, PICT<br>• MPEG,WMV, AVI<br>• ASCII, EBCDIC<br>• MIDI, WAV</td><td>Podaci</td></tr>
<tr><td colspan="2">Sesije</td><td>• SQL<br>• NFS<br>• ASP<br>• RPC<br>• X window</td><td>Podaci</td></tr>
<tr><td colspan="2">Transport</td><td>• TCP<br>• UDP</td><td>Segmenti</td></tr>
<tr><td colspan="2">Mreže</td><td>• IP<br>• IPX<br>• AppleTalk<br>• DECNET</td><td>• Router<br>• Layer 3 Switch</td><td>Paketi</td></tr>
<tr><td rowspan="2">Sloj veze</td><td>LLC</td><td rowspan="2">• LAN protocol: 802.2 (LLC), 802.3 (Ethernet), 802.5 (Token Ring), 802.11 (Wireless)<br>• WAN protocols: HDLC, PPP, Frame</td><td rowspan="2">• Network instance Card (NIC) transceivers<br>• Switch<br>• Bridge</td><td rowspan="2">Okviri</td></tr>
<tr><td>MAC</td></tr>
</table>

| | | | | |
|---|---|---|---|---|
| | | Relay, ISDN, ATM | | |
| Fizički | | • EIA/TIA 232 (serial signalling)<br>• V.35 (modem signalling)<br>• Cat5, Cat6<br>• RJ45 | • Transmission media (cable and wires)<br>• Media connectors<br>• Transceivers (including transceivers built into NICs)<br>• Modems<br>• Repeaters<br>• Hubs<br>• Multiplexers<br>• CSUs/DSUs | Bit -a |

Tabela 1. Tabelarni prikaz primenjenih protokola po slojevima referentnog OSI modela

OSI referentni model ima dve glavne komponente, apstraktni model mreže, nazvan Osnovni Referentni model (engl. „Basic Reference Model“) (sedmo-slojni model) i set određenih protokola.
Koncept modela sedam slojeva je proistekao iz rada Charles Bachman i "Honeywell Information Services". Različiti aspekt dizajna OSI modela proistekli su iz logike mreža *ARPANET, NPLNET, EIN i CYCLADES* i rada u IFIP WG6.1. Novi dizajn je dokumentovan u standardu ISO 7498 sa njegovim različitim dopuna. Dokumentacija OSI standarda je dostupna preko ITU-T ka X.200 serija preporuka. Neki od specifikacija protokola su takođe dostupni kao deo ITU-T X serije. [4]




Slika 5. Referentni OSI model

### 2.4.2 Fizički sloj

Fizički sloj veze ima sledeće funkcionalnosti:

- Definiše električne i fizičke specifikacije. U modelu je specificiran odnos između uređaja i fizičkih transmisionih medija (bakar, optički kabl i bežična komunikacija). Sloj uključuje i opisuje broj i raspored pin-ova na konektorima pripadajućih interfejsa, napona, impedansi, raznih specifikacija kablova, jačine i tajminga signala i sličnih karakteristika vezanih za uređaje i frekvencije signala, u rasponu od 2,4 GHz do 5 GHz, neophodnih u procesu bežične komunikacije;
- Definiše mrežnu topologiju: magistrala (BUS), prstena (Token Ring) i mreža (Mesh);
- Na ovom sloju se vrši dešifrovanje (enkodovanje) bit -ova;
- Definiše transmisionog (prenosnog) moda: simpleks, ful dupleks i half dupleks;
- Najčešće se susreće sa sirovim podacima.

Fizički sloj modela P-SCSI funkcioniše takođe na fizičkom sloju kao i fizički sloj Ethernet-a i drugih LAN-ova (Token, IEEE 802.11, FDI. ITU-T) kao i PAN mreža.

### 2.4.3 Sloj veze

Sloj veze sastoji se od dva pod sloja, i to:

- Kontrola pristupa mediju
- Kontrola logičkog linka

#### 2.4.3.1 Kontrola pristupa mediju (MAC)

Pod sloj definiše specifikacije za kontrolu pristupa mediji. MAC pod sloj odgovoran je za sledeće:

- Dodavanje okvira start i stop informacija referentnog paketu;
- Dodavanje Ciklične redundantne provere (CRC) za korekciju grešaka u prenosu;
- Konverzija okvira u bit –e koji se šalju kroz mrežu;
- Određuje mrežne uređaje i mrežne topologije u pripremi transportnog medija za slanje podataka;
- Utvrđivanje fizičke adrese (MAC/BIA) za svaki fizički uređaj u mreži;
- Kontrolisanje pristupa transmisionom mediju.

#### 2.4.3.2 Kontrola logičkih linkova (LLC)

Kontrola logičkih linkova (LLC) predstavlja sloj koji obezbeđuje interfejs između MAC sloja i protokola i gornji slojeva OSI modela. LLC protokoli su definisani od strane IEEE 802.2 komiteta. LLC pod sloj je odgovoran za sledeće:

- Održavanje uređene isporuke okvira kroz sekvence;
- Kontrola protoka korišćenjem sledećeg:
  - Eknolidžment;
  - Bafering;
  - Vindoving.

- Obezbeđivanje prijema bez grešaka u prenosu poruka;
- Konvertuje podatak u procesu prihvatanja formi za gornje slojeve;
- Uklanjanje okvira informacija iz paketa i prosleđuje ga prema mrežnom sloju;
- Omogućava gornjim slojevima korišćenje protokola MAC sloja;
- Definiše Service Access Point (SAP) praćenjem i upravljanjem različitih protokola.

### 2.4.4 Mrežni sloj

Mrežni sloj obezbeđuje funcionalno i proceduralno značenje transfera promenljjivih dužina sekvenci-podataka (segmenata) sa jednog čvorišta prema drugom konektovanom u istoj mreži. Mrežni sloj prevodi mrežne adrese u fizičke adrese računara ili uređaja. Mreža je medijum koja povezuje mnoge čvorove, na čijoj svaki čvor ima svoju adresu i čija prava čvorova koji su u vezi omogućavaju prenos poruke prema drugim čvorovima u mreži, uz pomoć određenih dinamičih rutabilnih protokola. Time se ostvaruje rutabilnost paketa, tj. ostvaruje se konektivnost (veza) između krajeva u komunikaciji. Ukoliko su poruke i paketi suviše veliki za prenos preko čvora, na sloju podataka se vrši deljenje poruka i paketa u nekoliko fragmenata, šaljući fragmente nezavisno, respektabilno sastavljajući na drugom čvoru u mreži.
Broj protokola koji pripada mrežnom sloju za upravljanje je definisan u aneksu upravljanja br. ISO 7498/4. Aneks uključuje ruting protokole, upravljanje multikast grupama i mrežnim slojem informacija. Funkcija mrežnog sloja uključuje sledeće:

- Čuvanje adresa direktno vezanih rutera;
- Čuvanje liste poznatih mreža;
- Određivanje sledećeg mrežnog skoka paketa koji se šalje;
- Ruteri koriste protokole koji nose podatke različitih vrednosti kao što su: broj skokova u putanji paketa, brzina linka, pouzdanost linka;

### 2.4.5 Transportni sloj

Transportni sloj (engl. Transport Layer) je četvrti sloj OSI modela koji omogućava pouzdano slanje paketa između instanci, dodeljenim adresnim opsezima. Obezbeđuje translaciju između gornjih i donjih slojeva OSI referentnog modela. Transportni sloj kontroliše pouzdanost uspostavljenog linka kroz kontrolu protoka segmentiranjem i grupisanjem, kao i kontrolom grešaka Neki od protokola su konekciono orijentisani, tj. obezbeđuju sigurnu konektivnost tehnikama kontrole komunikacije u tri kruga verifikacije. Znači, transportni sloj prati segmente u prenosu i ponovnom prenosu ukoliko je segment bio ne uspešno dostavljen na odredišni sloj. Na ovom sloju OSI modela segment se enkapsulira dodatno sa zaglavljem definisanih parametara koji se u daljem klasifikuju na:

- Verifikacija translacija;
- Port (socket) je broj koji je korišćen da identifikuje različite aplikacije na istim sistemima;
- Konekciono orijentisani protokoli (TCP) vrše detekciju grešaka u prenosu i uspostavljanju slanje oštećenih segmenata na zahtev. Konekciono orijentisani protokoli su dobro rešenje u sledećim slučajevima:
    - Pouzdana, komunikacija bez grešaka, gde je brzina prenosa u drugom planu;
    - Kada se šalju veći delovi/ fragmenti podataka.
- (Ne)konekciono orijentisani protokoli (UDP) omogućavaju prenos podataka bez intenzivne kontrole prenosa i verifikacije oštećenih ili ne dospelih segmenata. Protokoli su dobro rešenje u sledećim slučajevima:
    - Kada je važna brzina prenosa;
    - Kada se šalju manji fragmenti podataka.
- Segmentiranje informacija sa viših slojevima;
- Reassembling – spajanje segmenata;
- Određivanje neophodnih aplikativnih komponenti;
- Kontrola translacija prema određenim zahtevima.

### 2.4.6 Sloj sesije

Sloj sesije kontroliše vezu između računara. Takođe, sloj sesije uspostavlja, upravlja i prekida konekciju između lokalne i daljinske aplikacije, obezbeđujući funkcionalnosti ful-dupleksa, half-dupleksa i simpleks operacija. Protokoli sloja uspostavlju tačku provere, odlaganja, prekida i ponovnog pokretanja procedura uspostave sesije. Sloj sesije je odgovoran za regularno zatvaranje sesije, a u skladu sa instrukcijama protokola za kontrolu transmisije.
Funkcionalnosti na ovom sloju uključuju:

- Uspostavljanje i održavanje komunikacione sesije između mrežnih hostova, obezbeđujući protok informacija. Server je u stanju da održava hiljade sesija uporedo;
- Dodela ID broja sesije (svaka klijentska konekcija se zove sesija), koja se koristi na transportnom sloju za pravilno rutiranje poruka;
- Kontrola dijaloga/komunikacije – određivanje kako mrežni uređaji komuniciraju između sebe (simplex, half-duplex i full-duplex);
- Terminacija aktivne sesije između hostova se dešava nakon završene sesije.

Korišćeni protokoli i interfejsi sloja sesije koordiniraju zahteve i odgovore između različitih slojeva uz pomoć iste aplikacije. Ovi protokoli i interfejsi uključuju:

- X Window;
- Apple Session Protocol;
- Network File System;
- Remote procedure call;
- Structured Query Language.

### 2.4.7 Prezentacioni sloj

Primarna funkcija prezentacionog sloja je da formira ili prezentuje podatke u prihvatljivu formu aplikacionom sloju ili destinaciji (korisniku). Uspostavlja se kontekst između entiteta sloja aplikacije koristeći različite sintakse i šeme. Prezentacioni sloj obezbeđuje sledeće:

- Formatiranje i transport informacija između sistema;
- Usaglašavanje transfera podataka između referentnih sistema, prolazeći kroz konverziju karaktera u korisnički prihvatljiv format;
- Kompatibilnost sa korisnikom;
- Enkapsulacija podataka;
- Restauracija podataka dešifrovanjem i dekompresijom.

Prezentacioni sloj formatira podatke na način da su prihvatljivi za Aplikativni sloj. Ovo uključuje standardne formate fajlova kao što su:

- Slika: JPEG, PDF, BMP
- Video: MPEG, MKV, AVI, RM, WMV
- Tekst: EBCDIC, ASCII
- Zvuk: MIDI, MP3, WAV

### 2.4.8 Aplikativni sloj

Aplikativni sloj OSI modela je najbliži krajnjem korisniku, što znači da su i sloj i korisnik u direktnoj interakciji sa aplikacijom. Ovom sloju u interakciji sa softverom aplikacije implementira se komunikaciona komponenta. Takva komponenta nije u opsegu definisanih OSI modela. Aplikacioni sloj funkcioniše na tipičan način tako što proces komunikacije

započinje utvrđivanjem partnera u komunikaciji, utvrđuje dostupnost potrebnih resursa i sinhronizuje komunikaciju. Kada se završi započeta idetifikacija partnera, vrši se utvrđivanje identiteta i dostupnosti partnera u komunikaciji, za datu aplikaciju sa prenosom podataka. Nakon što se utvrdi dostupnost resursa, aplikacioni sloj odlučuje o tome da li su mrežni propusni opseg i zahtevana komunikacija u skladu sa zahtevima, predefinisanim kriterijumima za uspešnu komunikaciju između instanci u vezi. Smatra se da je sloj aplikativno specificiran nakon sledećih koraka: Partneri u komunikaciji su identifikovani, izvršena je verifikacija kvaliteta pruženih servisa QoS, utvrđen su i verifikovane korisničke autentifikacije i privatnosti.
Aplikacioni sloj specificira mnoge važne mrežne servise protokole koji su u širokoj upotrebi na internetu:

- HTTP; DNS; NFS
- Telnet; Gopher; FCIP
- TFTP, FTP;
- SNMP, SMPP, NNTP, SMTP.

## 2.5 Serverske mreže

Serversku mrežnu infrastruru čine hardverski i softverski resursi u čitavoj postavljenoj mreži, koji omogućavaju mrežnu konektivnost, komunikativnost, funkcionisanje sistema i njihovo upravljanje duž čitave postavljene računarske mreže. Mrežna infrastruktura obezbeđuje komunikacione servise i puteve između: korisnika, procesa, aplikacija, servisa i eksternih mreža (Interneta). U serverskom mrežnom okruženju sa više od 10 računara javlja se potreba za centralizacijom resursa i uvođenjem namenskih servera.
Prema tipu serverskih okruženja delimo ih na:

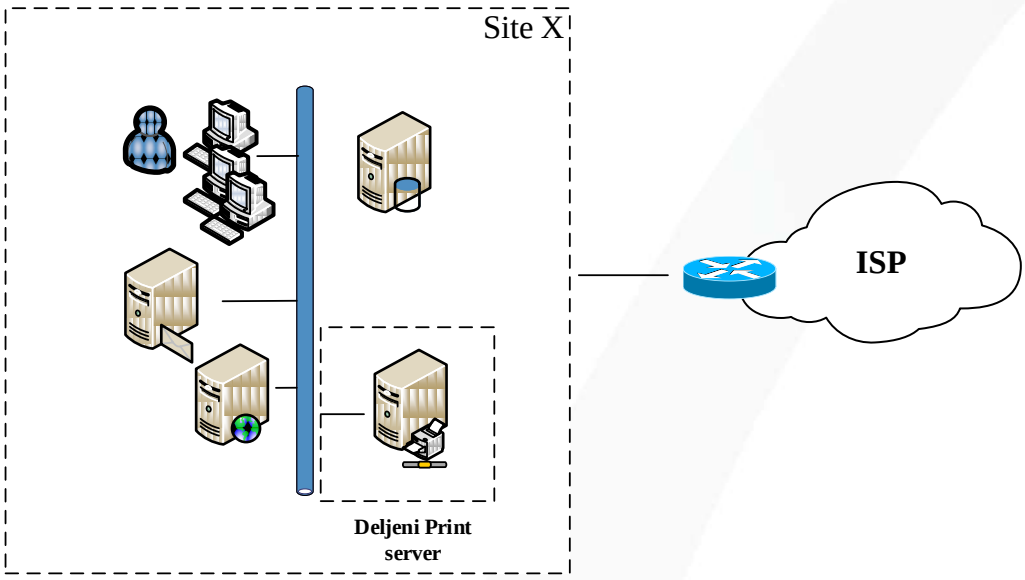
- **Radne grupe ravnopravnih računara** - Mreža ravnopravnih učesnika (P2P) kreira distribuiranu aplikativnu arhitekturu čije zadatke i radna opterećenja obavljaju članova grupe između sebe. Članovi grupe su predstavljeni kao podjednako privilegovani učesnici u komunikaciji. Članovi grupe dele delove svojih resursa (procesorska snaga, prostor na disku ili mrežni propusni opseg) direktno sa drugim članovima u mreži, bez potrebe za centralizacijom resursa od strane nekog servera ili druge jedinstvene instance u mreži. Članovi grupe obezbeđuju i preuzimaju svoje resurse, suprotno tradicionalnim klijentsko serverskim modelima koji ih dele. Dok su prethodno P2P mreže primenjene u mnogim oblastima, arhitekturu je popularizovao Napster, prvobitno objavljenu 1999. godine. Koncept je inspirisao mnoge strukture u raznim oblastima ljudske interakcije. U takvim društvenim kontekstima, P2P se odnosio na egalitarne (jednakost) društvene veze, koje su kasnije primenjene na Internet tehnologije u celini.
- **Domenska ili centralizovana serverska okruženja** - Domenska mreža predstavlja formu koju čine računarske mreže u kojima svi principali (korisnički nalozi, kompjuteri, printeri, servisi i drugi) su registrovani i smešteni u centralnoj bazi ili registru podataka lociranoj na jednom ili više čvorova mreže, na kojem je lociran centralni računar poznatog pod imenom kontroler domena. Autentifikacija instanci u komunikaciji se obavlja na kontroleru domena. Svaki korisnik koji koristi računar registrovan na kontroleru domena preuzima jedinstven korisnički nalog, sa pripadajućom lozinkom, kojem dodeljuje prava pristupa resursima unutar istog domena. Počev od MS Windows 2k, servis aktivnog direktorijuma je komponenta odgovorna za čuvanje centralne baze NTDS. Koncept MS Windows domena je suprotan modelu radne grupe u kojem svaki računar ima svoju lokalnu bazu sigurnih principala, sa njihovim definisanim pravima u sistemu. [3]

U zavisnosti od namene i tipa deljenih poslova, servere možemo podelimo na:

- Serveri datoteka i štampanja
- Serveri kontrole pristupa
- Serveri za organizaciju podataka
- Aplikacioni serveri
- Komunikacioni serveri

### 2.5.1 Serveri podataka i štampanja

Server datoteka i štampe upravlja pristupom korisnika i deli resurs štampe, prati korišćenje datoteka, kontroliše i upravlja jednim ili više štampača, prihvata zahteve za štampanjem od drugih klijenata. Takođe može da obavlja sve ostale zadatke kao i bilo koja druga radna stanica ako je štampač povezan direktno na printer port radne stanice.




Slika 6. Serverska mreža deljenog servera štampe

### 2.5.2 Serveri kontrole pristupa

Servis aktivnog direktorijuma je razvijen od strane Majkrosofta u cilju funkcionisanja mreža zasnovanih na Windows domenima. Čitav sistem uključuje mnoštvo serverskih operativnih sistema u cilju procesiranja i pružanja servisa krajnjem korisniku tražene usluge. Inicijalno, aktivni direktorijum je zadužen za centralizaciju i upravljanje domenom. Server koju upravlja funkcijom AD DS se naziva kontroler domena. jedna od bazičnih uloga servisa aktivnog direktorijuma i kontrolera domena su sledeći procesi: autentikacija, autorizacija i nadzor. Čitav proces se obavlja i primenjuje na sve korisnike, kompjutere i druge sigurnosne principale na tom domenu. Na primer, u trenutku kada se korisnik loguje na računar, koji je deo Windows domena, servis aktivnog direktorijuma potvrđuje pravo pristupa slanjem upita u bazu NTDS, prosleđujući podatke sa pripadajućom lozinkom, utvrđujući da li korisnik (sigurnosni principal) upita ima pravo pristupa ili ne. Takođe, vrši se i provera nasleđenih prava iz pripadajućih grupa sa predefinisanim pravima. Servis aktivnog direktorijuma koristi protokol LDAP verzije 2 i 3, Microsoft Kerberosa i domenskog servera imena.
Server koji pruža uslugu servisa aktivnog direktorijuma, tj. kontrolera domena omogućava funkcionalnosti:

- **Autetikacija** –Predstavlja čin potvrde prava atributa ili jedinstvenog dela podatka koji potvrđuje entitet tačnosti;
- **Autorizacija** – Predstavlja fukciju provere specifičnih prava i nivoa pristupa sigurnosnih principala, koji se odnose na prava korišćenja objekata i resursa na serveru ili domenu;
- **Nadzor** – Ima za cilja praćenje svega što je urađeno, generisanjem i čuvanje svakog sistemskog zapisa o svim procesima na sistemu.

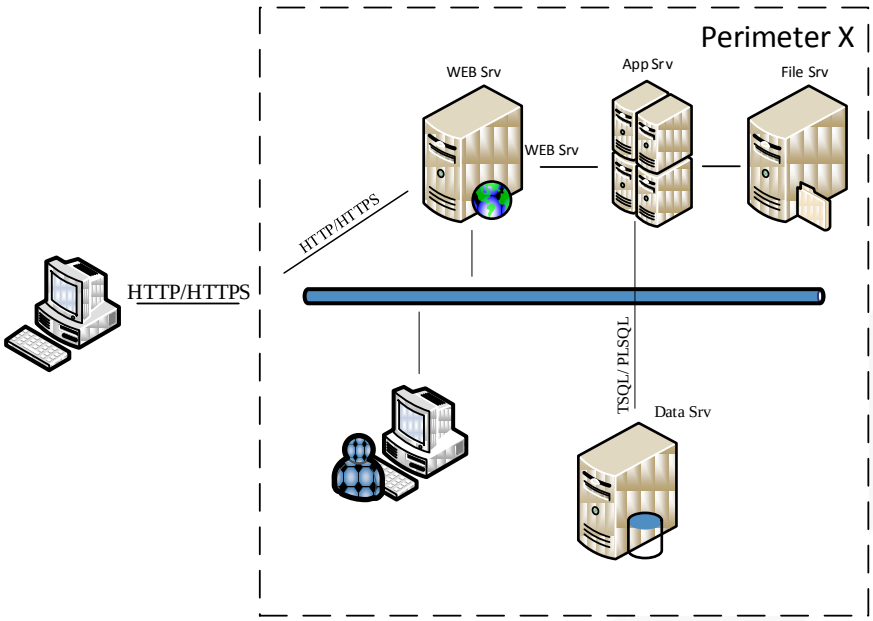
Parametri pristupa (korisničko ime, lozinka) na jedinstven način identifikuju sigurnosnog principala (korisnika) prilikom njegovog zahteva za pristup sistemu. Uobičajena kontrola pristupa se vrši pretragom, slanjem upita prema lokalnoj ili udaljenoj bazi sa korisnicima, kao i njihovim pravima pristupa. Korisnički ID i lozinka se kroz mrežu mogu dostaviti u formi teksta ili šifrovano.




Slika 7. Proces prijave na sistem

### 2.5.3 Serveri za manipulaciju sa podacima

Funkcionalnost ovih servera je da realizuje zahteve korisnika za smeštanjem podataka, indeksiranje i zaštite informacija na računarskoj mreži od neželjenih pristupa, izmene ili zloupotrebe. Mrežni softver je u mogućnosti da centralizuje grupiše i logički organizuje grupe resursa u domen, što daje korisnicima permanentno mogućnost da pristupe bilo kom resursu na mreži. U procesu planiranja mreže, arhitekta uključuje sve aspekte mrežne ekspanzije i tako dimenzioniše resurse.



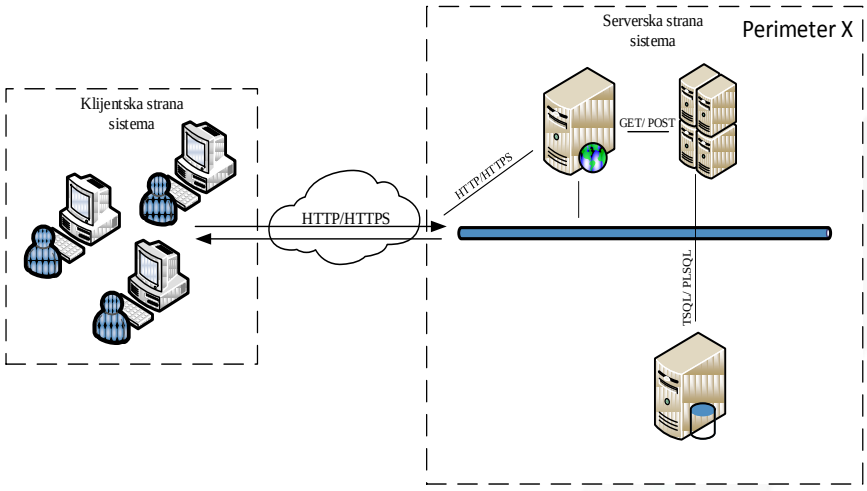

Slika 8. Serveri za organizaciju podataka

### 2.5.4 Aplikacioni serveri

Aplikativni server predstavlja instancu koja je sastavljena od komponenti sistema, koje su logički postavljene u sredini sloja centralne serverske arhitekture. Server obezbeđuje servise srednjeg sloja, koji su odgovorni za sigurnost i održavanje konzistentnosti sistema, zajedno sa pristupom podacima i postojanošću aplikacionog okruženja. Serveri dostavljaju serversku stranu aplikacije u klijent/server okruženju. Kod servera aplikacije baza servera može ostati na lokalnom disku ili izdvojena da drugom računaru ili grupi računara (klasteru, farmi). Na primer, veb aplikacija je smeštena na aplikativni server, koji je instaliran na farmi fizičkih servera NLB, dok se produkciona baza nalazi pohranjena na klasteru druge logičke i fizičke grupe računara ili na eksternom storidž sistemu. Infrastruktura sistema u primeru logički/fizički je koncipirana pod imenom SAN arhitektura.
U zavisnosti od specifičnosti aplikativnog servera razlikujemo dva tipa aplikacije:

- **Klasične prozorske aplikacije**: Struktura distribuirane aplikacije je bazirana na klijent-server modelu, koji raspoređuje zadatke ili tokove između pružaoca resursa (servisa, servera) i zahtevaoca usluge (klijenta). Često se dešava da klijenti i serveri komuniciraju preko računarske mreže, preko zasebnog hardvera i softvera, ili se mogu naći na istom sistemu. Na glavnom serveru je funkcionalan jedan ili više komponenti servera koji dele svoje resurse sa klijentima. Klijenti ne dele svoje resurse, ali traže resurse ili funkcionalnosti od servera. Klijenti iniciraju komunikacione sesije dok serveri očekuju/slušaju dolazne zahteve. U pojedinim slučajevima razvija se i srednji sloj aplikacione logike (Application logic) koji je logički postavljen u sredini klijent-server komunikacije. Primeri računarskih aplikacija koji koriste klijent-server model su e-mail, mrežni servisi štampanja, www, i tako dalje;
- **Aplikacija bazirana na veb tehnologijama**: Veb aplikacija ili veb klijent-softver aplikacija je ona na koju se klijent (ili korisničko okruženje) poziva sa veb-pretraživačem. Veb aplikacije su popularne zbog široke pristupnosti sa mnogih

popularnih veb pretraživača, a pogodnost je pristup pomoću veb-pretraživača kao klijenta, sa kojeg je moguće ažurirati i održavati veb aplikacije bez distribucije i instalacije softvera na potencijalno klijentski računar. Ključan razlog za njihovu popularnost je nasleđena podrška i kompatibilnost za cross-platforme. Uobičajene veb aplikacije uključuju webmail, online maloprodaje, online aukcije, usluge instant poruka i mnoge druge funkcije.




Slika 9. Aplikacioni server

### 2.5.5 Komunikacioni serveri

Komunikacioni podaci su odgovorni za komunikaciju i protok informacijama i porukama između mreže u kojoj je sam računar sa drugim računarom izvan mreže. E-mail je važan servis u savremenoj komunikaciji. U većini slučajeva emajl serveri su mnogome slični aplikativnim serverima.

## 2.6 Sistem kontrole pristupa – bezbednost sistema i smanjenje rizika

Kontrola pristupa prestavlja kljucan segment čitavog sistema zaštite informacionog sistema. Definisanjem prava pristupa kao i prava u procesu autorizacije omogućavamo kontrolisan pristup resursima na zahtev korisnika. Administratori sistema koriste različite bezbednosne metode zaštite sistema, svakodnevno primenom funkcionalnosti hardvera i softvera, primenom šifarničkih tehnika (šifrovanja) i bio metrike pri zaštiti identiteta korisnika i resursa.

### 2.6.1 Ograničenje fizičkog pristupa resursima

Smanjenje rizika od izlaganja računarskih sistema je omogućavanje pristupa samo onim korisnicima kojima se veruje. Od postavljenog sistema zaštite za pristup računarskom sistemu razlikujemo:

- Posedovanje dokumenata:
  - Digitalni sertifikat;
  - Kartica za personalnu identifikaciju sa slikom;
  - Pametna kartica sa šifrovanom identifikacijom.

- Poznavanje i pamćenje: lozinka, identifikacioni broj, kombinacija ili podatak iz istorije;
- Biometrijski podatak: glas, otisak prsta, skeniranje mrežnjače, karakteristične crte lica, pojedine telesne karakteristike.

I pored svih (digitalnih i/ili fizičkih) bezbednosnih provera potrebno je ih stalno kombinovati u cilju što uspešnije/sigurnije kontrole.

### 2.6.2 Parametri pristupa

Zaštita sistema može biti implementirana na više različitih načina. Fizička sigurnost pristupa sistemu uključuje pravila i procedure prilikom pristupa objektima, zaštićenim prostorijama sa visokim stepenom kontrole i provere identiteta određenih instance, na zahtev. Digitalna kontrola uključuje digitalne provere: korisničkog naloga i lozinke, ID kartica, biometriskih karakteristika i tome sl.
Glavni problem zaštite kod svih operativnih sistema je autentifikacije. Najčešće prihvaćen način zaštite sistema je dostavljanje korisničkom imena i lozinke, koji se sistemski šalju određenoj instanci sistema (AAA server), i time proverava validnost (autentikacija) i prava nad objektima (autorizaciju) principala. Time se sprečava pristup neidentifikovanim principalima. Tajnost lozinke je glavni deo sistema kojim se na ovaj način obezbeđuje zaštita. Od načina implementacije sistema lozinki najviše zavisi koliko će sistem biti zaštićen. Zato većina današnjih sistema ne omogućava korisnicima unos onih lozinki koje nisu dovoljno sigurne i koje se nazivaju slabe lozinke. Primeru slabih lozinki su ime i prezime, reč iz rečnika, ime člana porodice, itd. U cilju što bolje parametrizacije pristupa sistema, prateći preporuke vendora, parametri moraju ispunjavati sledeće kriterijume:

- Parametri pristupa treba da uključe upotrebu jedinstvenih reči i/ili fraza koje su što jedinstvenije, tj. teško se mogu naći pretragom bilo kojeg rečnika;
- Parametri pristupa ne smeju biti kraći od 8 karaktera, predstavljajući najčešće preporučene vrednost od strane informatičke javnosti;
- Parametri pristupa moraju biti sastavljeni od četiri tipa karaktera: mala slova (apkja), velika slova (AJBH), brojevi (1345) i razni drugi karakteri ($#%&!?);
- Parametrima pristupa treba definisati maksimalan period važenja parametara;
- Konfigurisana istorija bi trebala da bude vezana za poslednjih 12 korišćenih tajnih reči;
- Permanentna promena parametara pristupa na svakih 30 dana;
- Potrebno je definisati maksimalan broj bezuspešnih pokušaja provere dostavljenih parametara pristupa.

Najvažnija lozinka u datom sistemu je lozinka sistem administratora, jer ona ima kompletnu kontrolu nad sistemom. Upravo zbog toga najveći broj napada na sistem ima za cilj pronalaženje lozinke sa pravima sistem administratora. Postavljeni sistem zaštite, upotrebom tajnih i jedinstvenih parametara pristupa, predstavlja sistema za koga se smatra da ga je teško preći. Ukoliko se pravila prilikom generisanja tajnih reči i karaktera prekrši pristup sistemu se lako se može provaliti.
Jedan od načina zloupotrebe je primena aplikacije grube sile koja servis pristupa zatrpava sa uobičajenim rečima i parametrima po utvrđenim algoritmima ukrštanja karaktera. Vizuelni monitoring nastaje gledanjem u tastaturu prilikom unosa korisničkog imena i lozinke. Elektronski monitoring se može uraditi pomoću sniffing alata kojim se može snimiti identitet korisnika i njegova lozinka. Šifrovanje podataka koji sadrže lozinku rešava ovaj problem.
Autentikaciju korisnika može se vršiti na dva načina: jednostruka i/ili dvostruka.
Dvostruka autetifikacija funkcioniše kao kartica i PIN. Realizacija zahteva nije moguća u slučaju da nije dostavljen PIN u procesu realizacije. PIN može biti dostavljen i preko SMS –a. Imajući na umu da su verifikacioni podaci poslati na lični uređaj i da su jedinstveni,

drugačiji svaki put prilikom zahteva za realizaciju naloga ili autentikacije obezbeđena je dodatna zaštita informacija.

### 2.6.3 Nivoi pristupa

Razlikujemo više nivoa pristupa u zavisnosti od okruženja i resursa:

- Pristup operativnom sistemu;
- Pristup aplikacijama;
- Pristup bazi podataka;
- Pristup mrežnoj opremi;
- Daljinski pritup korporativnoj mreži preko uspostavljenog Virtualnog Privatnog Linka (VPN).

#### 2.6.3.1 Pristup operativnom sistemu

Pristup operativnom sistemu se ostvaruje kreiranjem korisničkog naloga na aktivnom direktorijumu i/ili lokalno, na operativnim sistemu kome se pristupa. Aktivni direktorijum obezbeđuje centralizovanu administraciju svih objekata u okviru mreže. Pristup operativnom sistemu se ostvaruje u cilju redovne upotrebe, kontrole i održavanja IT opreme, sistemskog i aplikativnog softvera, i/ili u slučaju incidenta.
Korisnički nalozi za pristup sistemskom softveru u zavisnosti od sistema razlikujemo:

- Predefinisani (Built-in) nalog – ugrađeni nalog neograničenih privilegija (npr. „Administrator“ – Microsoft Windows OS i sl.);
- Administratorski nalog – definisani korisnički nalog sa dodeljenim neograničenim ili ograničenim privilegijama;
- Servisni nalog – definisani korisnički nalog namenjen za pokretanje sistemskih servisa (npr. nalog za pokretanje SQL Server-a i sl.);
- Korisnički nalog za pristup – definisani korisnički nalog ograničenih privilegija.

#### 2.6.3.2 Pristup aplikacijama

Tradicionalan pristup klijentsko serverskim aplikacijama različito se karakterišu od samih aplikacija koje pristup baziraju preko Interneta, na osnovu kojeg administratori projektuju najbolji način za podršku aplikaciji.
Upravljanje autorizacijom (engl. Authorization Manager) API i MMC snap-in omogućavaju fleksibilno okruženje koje kontroliše pristup na osnovu deljenih prava. Ova funkcionalnost uključuje skup COM objekata za veb i linijski poslovne aplikacije. Razlikujemo sledeće tipove kontrole pristupa resursima aplikacije:

- Kontrola pristupa zasnovana na deljenim pravima
- Kontrola pristupa zasnovana na ALM (engl. Access Control Models)

Neki od najčešćih metoda korišćenih za autentifikaciju su:

- **Active Directory**: Aktivni direktorijum predstavlja servis direktorijuma koji hijerarhijski grupiše sve objekte u domenu. Aktivni direktorijum predstavlja specifičnu bazu podataka koja u suštini nije zamena za bazu registra. Dizajniran je na način da uspešno manipuliše sa veliki brojem operacija (čitanja i pretrage) nad objektima, kao i da aplikacijama u komunikaciji omogući autentikaciju korisnika sa predefinisanim pravima. Aktivni direktorijum predstavlja replikativnu i proširivu bazu statičkih podataka, zbog čega se ne koristi za smeštanje dinamičkih podataka npr. performansi CPU ili cena akcije na referentnoj berzi. Specifični podaci od objekta iz baze smeštaju se u registar. Tipičan primer podataka koji se nalaze u aktivnom direktorijumu su računari, korisnici, servisi, štampači kao i svi meta

podaci koji opisuju objekat i mrežu. Baza aktivnog direktorijuma se sastoji od objekata i atributa. Definicije objekata i atributa se čuvaju u šemi aktivnog direktorijuma. Aktivni direktorijum se sastoji od tri particije: domeni, šeme i konfiguracije. Domen particija sadrži korisnike, grupe, kontakte, kompjutere, organizacione jedinice i mnoge druge tipove objekata. Šema particija sadrži definicije klasa i atributa. Konfiguracija uključuje podatke za servise, particije i lokacije. Uloge ADNS su podeljene po ulogova/rolama koje se stručno nazivaju fizmo role. Svaka od rola zadužuje obaveze koji su sastavni deo jednog domenskog okruženja. U zavisnosti od vlasnika role zavisi i raspodela odgovornosti na osnovu čega se kvalitativno dimenzioniše afektirana infrastruktura;

- **LDAP**: LDAP (engl. Lightweight Directory Access Protocol) predstavlja protokol servisa direktorijuma koji radi na sloju iznad TCP/IP i obezbeđuje mehanizam za uspostavu linka, pretragu i modifikovanje Internet direktorijuma. LDAP je servis direktorijuma zasnovan na klijent-server modelu. Takođe, omogućava pristup informacijama u različitim direktorijumima. LDAP API je primenljiv za upravljanje direktorijumima i pretragu aplikacija koje nemaju podršku za servis direktorijuma kao njihovu primarnu funkciju;
- **Internal**: Pojedine aplikacije su razvijene tako da autorizuju korisnik upitom iz interne/lokalne baze SAM, koja je pozicionirana unutar same aplikacije i/ili na lokalnom operativnom sistemu. Interna/lokalna baza nije vezana za servis aktivnog direktorijuma i upravljanje se obavlja nezavisno. Ukupna autentifikacija je segmentirana, tj. primenjena su parcijalno nasleđena prava pristupa.

#### 2.6.3.3 Pristup bazi podataka

Sigurnost baze i servera baze podataka odnosi se na korišćenje širokog spektra informacija i sigurnosnih kontrola namenjenih za zaštitu baze podataka (potencijalno uključene podatke, servere baza podataka, i vezane mrežne linkove) u cilju zaštite od kompromitovanja poverljivosti integriteta i visoke dostupnosti. To uključuje različite tipove ili kategorije kontrola, kao što su tehničke, proceduralno/administrativne i fizičke. Sigurnost baza je u suštini specijalizovana tema koja uključuje veoma široki domen kompjuterske sigurnosti, informacione sigurnosti i rizik upravljanja. Sigurnosni rizici sistema baza podataka uključuju sledeće:

- Neautorizovane ili nenamerne aktivnosti ili zloupotrebe od strane autorizovanih korisnika baza, administratora baza, ili mrežno/sistemskih menadžera, ili od neautorizovanih korisnika ili hakera (npr. ne odgovarajući pristup poverljivim podacima, meta-podacima ili funkcionalnim komponentama unutar baze, neodgovarajućim izmenama u bazi podataka, ili izmeni strukturnih ili sigurnosnih konfiguracija);
- Fault-positive incidenti koji prouzrokuju neautorizovani pristup, curenje i obelodanjivanje privatnih i drugih vrednih podataka, brisanje ili štetu koju mogu na načine na programskim podacima, prekid i negiranje pristupa autorizovanim korisnicima;
- Fizičko oštećenje servera baze podata uzrokovanih požarom ili poplavom, pregrevanjem server sala, jakih elektrostatičkih pražnjenja, elektronskih prekida ili zastarelosti;
- Dizajnerski nedostaci ili programski bagovi u bazi podataka ili vezanih programskih sistemima;

- Korupcija i/ili gubitak podataka prouzrokovani prodorom štetnih podataka ili komandi, greške u bazi i/ili procesima od strane sistem administratora, sabotaža i/ili kriminalan akt;

Razlikujemo vrste naloga nalog za pristup na bazu podataka i to:

- **Predefinisani (Built-in) nalog** – ugrađeni nalog neograničenih privilegija (npr. „sa“
- **Login** – Microsoft SQL Server i sl.;
- **Administratorski nalog** – definisani korisnički nalog sa dodeljenim ograničenim ili neograničenim privilegijama;
- **Korisnički nalog za pristup** – definisani korisnički nalog ograničenih privilegija.
  U zavisnosti od kreatora baze (software vendor) i okruženja najčešće razlikujemo više autentifikacionih modova – Authentication mode, i to:
- **Mešoviti autentifikacioni mod** – Mixed Mode Authentication: Mogućnost pristupa serveru baze podataka sa pravima koja su data kroz AD DC i/ili Native SQL respektibilno;
- **SQL Server autentifikacioni mod** – SQL Server Authentication: Mogućnost pristupa serveru baze podataka isključivo sa pravima naloga kreiranom na SQL serveru.

#### 2.6.3.4 Pristup mrežnoj opremi

Nisu sve aplikacije pisane tako da u potpunosti štite workflow, potrebno je pružiti veću zaštitu koja se vrši na mrežnim uređajima. Pristup mrežnom okruženju, kasnije kontroli protoka/inspekciji paketa u mnogome zavisi od tehnologije koja je primenjena za efikasnu autorizaciju korisnika u procesu ostvarivanju sigurne veze. Razlikujemo više načina pristupa mrežnim uređajima i servisima:

- **Konzolni port** – Konzolni port je terminalni interfejs koji se koristi za pristup mrežnim i drugim uređajima, čije se tekst instrukcije, uređaja prilikom komunikacije, koristi za administraciju uređaja. Razmena instrukcija šalje se preko zasebnog kabla a ne kroz računarsku mrežu. Prilikom komunikacije koristi se terminalan pristup pomoću CLI regulatora veze. Najčešće korišćeni terminalni emulatori su: Dave's Telnet, SecureCRT, KiTTy, mRemoteCT i Putty;
  Na savremenim računarima fizički interfejs RS-232 je zamenjen sa USB-to-RS232 adapterima. Kabl koji se koristi u terminalnoj konzolnoj komunikaciji zove se Rolover, koji se u mnogim literaturama pojavljuje pod imenom Cisco konzolni kabl ili Yost kabl.
- **AUX** – Pomoćni port je definisan kao standardni komunikacioni port. AUX je asinhroni interfejs serijskog porta, koji najčešće predstavlja pomoćni ulaz za audio signala, što je njegova uobičajna primena: MP3, slušalice, portabilni muzički uređaji za reprodukciju zvuka, pojačala i zvučnici. AUX predstavlja interfejs koji dozvoljava računaru ili drugim uređajima da pošalju i prime podatke asinhrono. Prema tome, AUX interfejs je port na mrežnom uređaju kome je dodeljen ekvivalent (serijski uređaj) , na primer PC, sa koga se šalju tekstualne instrukcije za administraciju uređaja.
  U opisu porta, koji se tiče ovog rada, najčešća upotreba AUX interfejsa je uspostava modemske Dial Up konekcije u cilju daljinske administracije uređaja i uspostavu u rezervnog linka na zahtev. Kao mnogi konzolni portovi AUX port je asinhroni RJ-45 interfejs. Najčešće je obeležen na mrežnim uređajima kao MODEM.

- **Out-of Band** – Pružaoci usluga i/ili servisa rezervišu menadžment portove, kojima dodeljuju IP adrese, omogućavajući pristup na određene podržane mrežne protokole: Telnet, SSH, HTTP/HTTPS
- **Dedikovan fizički interfejs** – U kontekstu rada, dedukovani interfejs je još jedan od pristupa upravljačkom segmentu. Uzimajući u obzir limitiran broj interfejsa na savremenim ruterima, smatra se veoma skupim rešenjem. Razvojem sistema na mrežnim uređajima, dedikovanje upravljačkog interfejsa SVI u te svrhe u mnogome pojeftinjunje i smanjuje dodatnu administraciju. Najčešća upotreba, i najjeftinija primena fizičkog interfejsa u upravljačke svrhe je u okviru centra podataka, gde se ne zahteva dopuna pasivne i aktivne mrežne infrastrukture.
- **VLAN-MGMT** – Virtualni interfejs je još jedan od izabranih metoda pristupa upravljačkom segmentu. Kreiranje rezervisanog virtualnog interfejsa za upravljanje mrežnom infrastrukturom je široko prihvaćena funkcionalnost, gde se fizički interfejsi za upravljanje zamenjuju virtualnim, korišćenjem postojećeg ASIC's –a (deo hardvera za procesiranje u okviru mrežnog uređaja). U zavisnosti od uređaja razlikujemo:
    - **Svičevi** – Svičevi u okviru imena domena moraju imati konfigurisan određeni VTP v1/v2/v3 status sa pripadajućim modom. Linkovi između redundantnih i drugih mrežnih resursa u domenu moraju biti trankovani, zbog markiranja (flagging) i transfera različitih VLAN-ova, zajedno sa upravljačkim VLAN-MGMT. Najčešće korišćena enkapsulacija je IEEE 802.1Q (dot.1Q) ili Cisco-v preferencijalni protokol ISL. Kreiranje interfejsa SVI je imenovan upravljačkim VLAN-om.
    - **Ruteri** – Virtualni interfejsi sviča je zamenjen pod-interfejsom koji se kreira na nivou fizičkog interfejsa. Pod-interfejs je kreiran sa pripadajućom adresnim opsegom i pripadajućim VLAN. Linkovi između redundantnih i drugih mrežnih resursa u domenu moraju biti trankovani, zbog markiranja (flaging) i transfera različitih VLAN-ova, zajedno sa upravljačkim VLAN-MGMT. Najčešća enkapsulacija je IEEE 802.1Q (dot.1Q) ili Cisco -v preferencijalni protokol ISL.

Razlikujemo više primenjenih metodologija autorizacije (AAA) pristupa:

- Autorizacija korisnika proverom lokalne baze, locirane na uređaju pristupa ili centralizovano za definisanu grupu uređaja (mrežni uređaj);
- Autorizacija korisnika korišćenjem jednog od nekoliko najčešće korišćenih tehnologija (protokola) daljinske kontrole, i to:
    - RADIUS (RFC 2865)
    - TACACS+ (nisu standardizovani od IEEE, preferencijalno pravo Cisco)
    - Diameter (RFC 6733)
    - Kerberos (RFC 4120 ver.2005.godina)
    - TACACS (Nisu standardizovani od IEEE, preferencijalno pravo Cisco)

#### 2.6.3.5 Pristup računarskim mrežama preko privatnih virtualnih mreža

Privatna virtualna mreža omogućava siguran pristup sistemu sa udaljenih mreža i/ili lokacija putem interneta. Opšte karakteristike VPN pristupa sistemu čini:

- VPN pristup predstavlja servis za ostvarivanje sigurnog pristupa sistemsko aplikativnim resursima organizacije;
- Obezbeđuje centralno praćenje i kontrolu pristupa organizacije;
- Omogućava proceduralno kreiranje/ukidanje i personalizaciju pristupa organizaciji.

Koncepti realizacije:

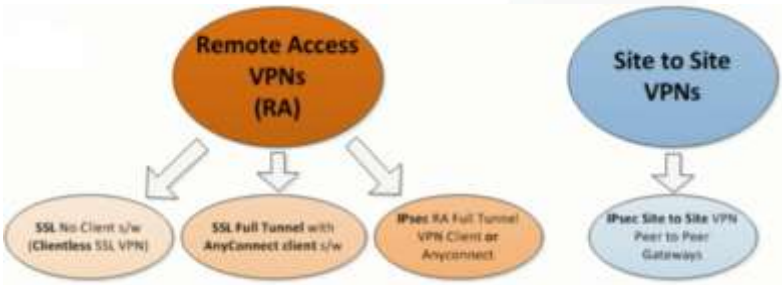
- Virtualne privatne mreže aplikativnog sloja;
- Virtualne privatne mreže sloja mreže;
- Virtualne privatne mreže sloja podatka.

Tipovi konekcija od strane zahtevaoca servisa:

- Virtualne privatne mreže sa permanentnim pravom pristup;
- Virtualne privatne mreže sa privremenim pravom pristupa.

Razlikujemo dva tipa VPN pristupa, i to:

- Remote Access VPNs (RA)
  - SSL No Client s/w (Clientless SSL VPN)
  - SSL Full Tunnel (AnyConnect client s/w)
  - IPsec RA Full Tunnel (VPN Client i/ili AnyConnect)
- Site-to Site
  - IPsec Site-Site VPN (Peer to Peer Gateway)




Slika 10. Tipovi VPN pristupa, sa pripadajućim podgrupama [4]

Kako bi podaci i integritet korisnika ostali sigurni zadatak virtualnih privatnih mreža je da ispune tri osnovna kriterijuma, i to: poverljivost, integritet podataka, dostupnost.

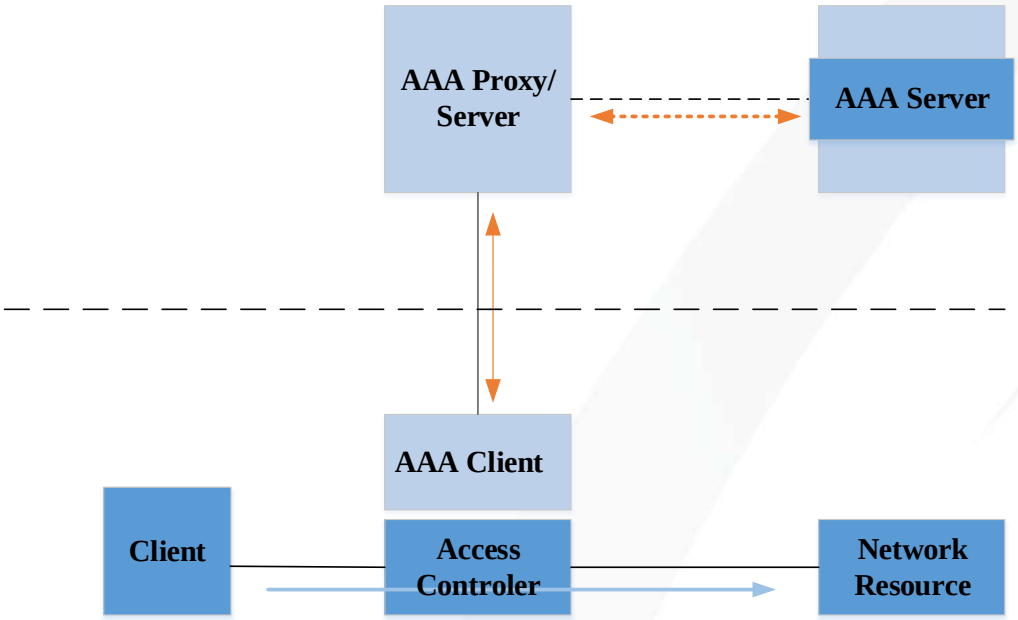
Izabrane metode i protokoli prilikom provere identiteta i deljenih prava korisnika korišćeni u procesu daljinskog pristupa korisnika opisano je u odeljku 2.6.3.4 ovog rada.

### 2.6.4 Centralizacija kontrole pristupa AAA (Authentication, Authorization and Accounting)

- **Autentikacija** – Autentikacija predstavlja čin potvrde prava atributa ili jedinstvenog dela podatka koji potvrđuje entitet tačnosti. Suprotno procesu identifikacije koji se odnosi na čin utvrđivanja na potpuno drugi način, koji ukazuje na tvrdnju navodne tačnosti osobe ili stvari identiteta, autentifikacija je proces trenutne potvrde tog identiteta. U tom procesu autentikacije uključuje se identitet principala validiranjem njegovih dokumenata o identitetu, proverom baze poslatim upitom ka NTDS, proveru autentičnosti sa pripadajućim sertifikatom ili proveru da li je korisnik taj za koga se predstavlja da jeste;
- **Kontrola Pristupa** – Autorizacija koja predstavlja fukciju provere specifičnih prava i nivoa pristupa sigurnosnih principala, koji se odnose na prava korišćenja objekata i resursa na serveru ili domenu. Na primer, administrator nekog kontrolera domena daje pravo pristupa određenom korisničkom nalogu, procedura koja je uobičajeno formalizovana u proceduri pravila prilikom kontrole pristupa računarskim i drugim infrastrukturnim resursima (npr. korisnici, računari, mrežna

oprema, VoIP telefonska centrala, pristup server salama, itd), nakon kojeg sistem koristi pravila kontrole pristupa kako bi odlučio o nivou i načinu korišćenja usluge, a koja se traži;

- **Monitoring** – Funkcionalnost nadzora ima za cilja praćenje svega što je urađeno na sistemu, generisanjem i čuvanje svakog sistemskog zapisa o svim procesima na sistemu. Sve operacije nad fajlovima i folderima deljanih resursa, izmene nad čitavim aktivnom direktorijumom domena i praćenje kompletne funcionalnosti sistema koje administrator domena može analizirati i pratiti, su uključenu u obim ove funkcionalnosti.




Slika 11. Prikaz generičkog troslojnog „AAA“ model

### 2.6.5 „AAA“protokoli

„AAA Protokoli“ označavaju IP protokole:

- Korišćeni za transport AAA informacija,
- U komunikaciji AAA klijenta i AAA servera,
- U tzv. back-end infrastrukturi,
- Koji ne uključuju protokole između hosta i AAA klijenta (npr. PPP).

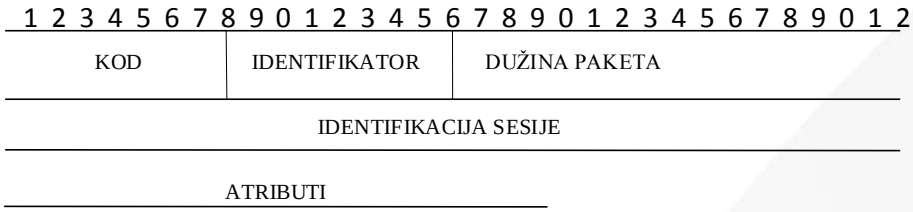
AAA protokoli:

- RADIUS (RFC2865)
- TACACS (preferencijalni Cisco –v protocol, ne uključuje specifikaciju IEEE)
- Kerberos (RFC 4120 v.2005.godina)
- Diameter (RFC6733)
- TACACS+ (referencijalni Cisco –v protocol, ne uključuje specifikaciju IEEE)

#### 2.6.5.1 RADIUS

RADIUS protokol je dizajniran da omogući interoperabilnost sa tačka-do-tačke protokolom (PPP – RFC 1661), korišćen za enkapsulaciju IP paketa kroz telefonsku liniju. Livingstone Enterprises je za svoje potrebe razvio RADIUS protokol. Godine 1997. protokol je

objavljen u RFC 2058 i 2059 (zadnja verzija RFC 2865 i RFC 2866). RADIUS protokol koristi UDP transportni protokol.
RADIUS protokol se pojavljuje kao potreba prilikom centralizacije pristupa korisnicima na zahtev, usled limitirane mogućnosti mrežnih uređaja za pohranjivanjem većeg broja zapisa i autentifikacionih parametara i pružanja određenog nivoa bezbednosti od pristupa neovlašćenih korisnika uz veliku kompatibilnost proizvođača računarske opreme.[6]




Slika 12. Format RADIUS paketa

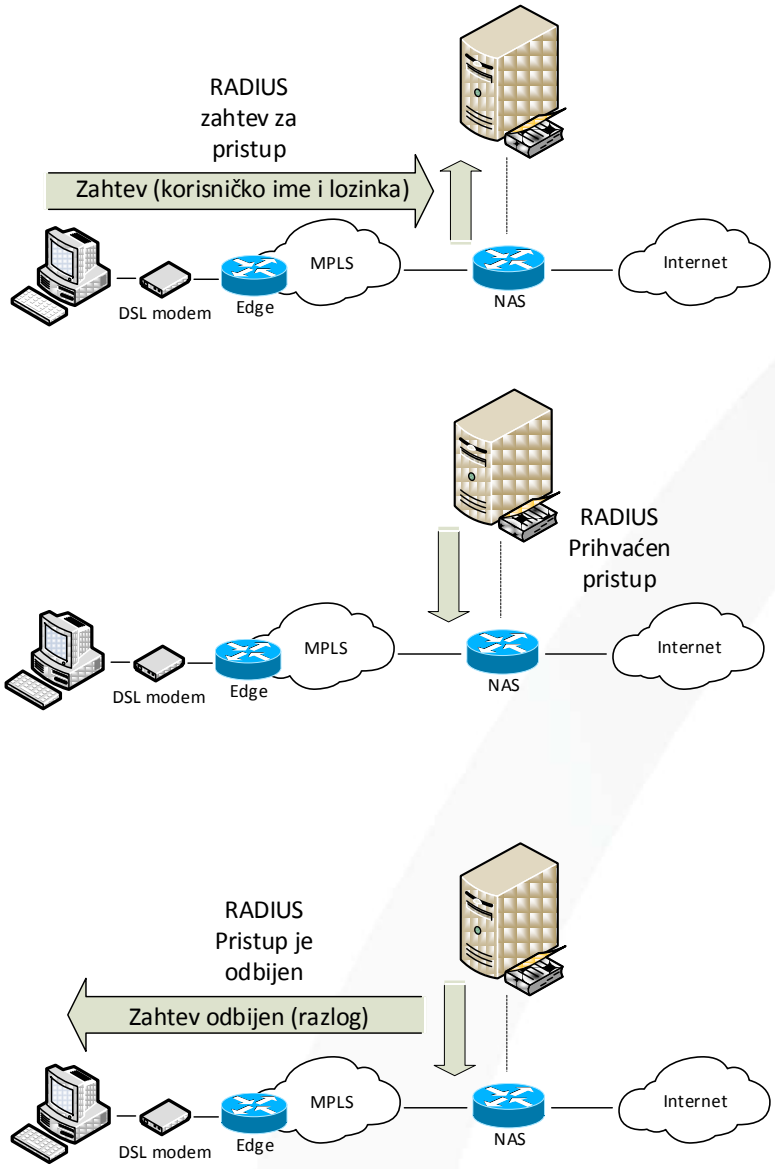
**Značenje pojedinih polja**:
KOD – Definiše tip RADIUS –a.

| Vrednost | Opis |
|---|---|
| 00000001 | Access-Request |
| 00000010 | Access-Accept |
| 00000011 | Access-Reject |
| 00000100 | Accounting-Request |
| 00000101 | Accounting-Response |
| 00001011 | Access-Challenge |
| 00001100 | Status-Server (Experimental) |
| 00001101 | Status-Client (Experimental) |
| 11111111 | Reserved |

Tabela 2. Vrednosti KOD -a RADIUS paketa

IDENTIFIKATOR – definiše jedinstvenost parova;
DUŽINA PAKETA – utvrđivanje dužine paketa (2 byte -a);
AUTENTIKATORI – provera ispravnosti odgovora;
ATRIBUTI – korisničko ime i lozinka atributa.

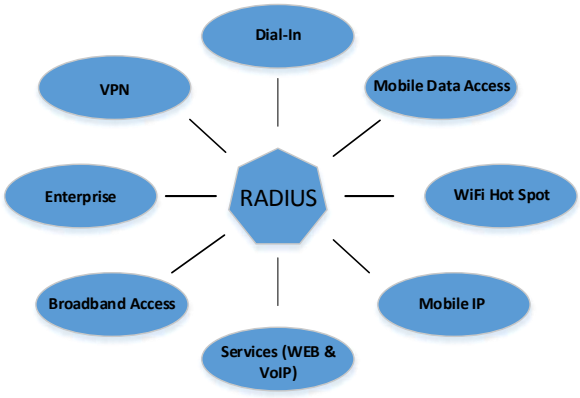
**Postupak autentikacije:**
Kategorizovani sigurnosni principal uspostavlja proces slanjem kreiranog RADIUS zahteva, prosleđivanjem "Zahteva za pristup". Dostavljeni kod, u svojoj poruci, mora da bude sačinjen od atributa (korisničkog imena i lozinke). Kreirano polje „Autentikator“, u dostavljenom upitu, sadrži „Zahtev autentikatora“ (RA). Uz pomoć RA i tajnog ključa vrši se šifrovanje korisničke lozinke (korisničkog imena i lozinke). Nakon primljenog upita RADIUS server proverava postojanje tajnog ključa za tog korisnika. Ukoliko postoji sledi postupak provera ispravnosti lozinke, i ukoliko je ispravna vraća „Prihvaćen pristupu” suprotnom vraća „Odbijen pristup“ paket. Na osnovu Identifikacije (ID) korisnik verifikuje validnost odgovora.




Slika 13. Proces RADIUS autentikacije

Nedostaci izbora RADIUS su:

- Izbor algoritma za generisanje odgovora nije dovoljno siguran, tj. postoji velika mogućnost od probijanja vrednosti tajnog ključa;
- Korišćen je MD5 hash algoritam za enkripciju parametara pristupa, čiji je ciphertext lako čitljiv (algoritam je dostupan), koji se smatra ne prikladnim izborom;
- Mogućnost probijanja tajnog ključa i provala korisničke lozinke




Slika 14. Rasprostranjenost RADIUS protokola

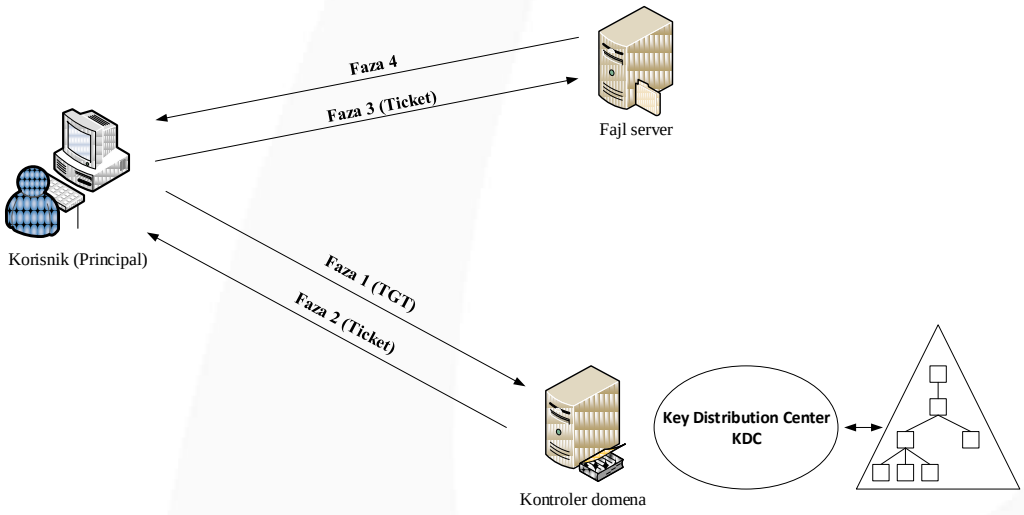
### 2.6.5.2 Kerberos

Kerberos je protokol koji učestvuje u procesu autentikacije. Takođe, omogućava jedinstveni transport duž neosiguranog linka u cilju što tačnije verifikacije principala. Obezbeđuje identitet informacija i sprečava slušanje i razumevanje poslatih poruka. Zamišljen je kao klijentsko serverski model u obezbeđivanju uzajamne autentikacije identiteta. Massachusetts Institute of Technology je odgovoran za kreiranje i razvoj Kerberos autentikacionog protokola, koji je implementiran na projektu Athena. Prve tri se koriste interno dok je četvrtu verziju objavio Steve Miller i Cliford Neuman u kasnim 80-tim. 1993.godine objavljuje se verzija 5 kao RFC 1510 i RFC 4120 iz 2005 [23]. Kerberos se bazira na Needham-Schroeder protokolu. Zahteva Key Distribution Centre (KDC), sastoji se od dva logička dela:

- Autentikacioni server;
- Server za tiketiranje.

Kerberos protokol je razložen prema sledećim fazama:

- F 1:KBC_AS_REQ;
- F 2: KRB_AS_REP;
- F 3: KRB_TGS_REQ;
- F 4: KRB_TGS_REP.




Slika 15. Proces autentikacije korisnika

### 2.6.5.3 TACACS+

TACACS je kontroler terminalnog pristupa i predstavlja protokol koji se koristi za autentikaciju principala na zahtev. Najčešće se primenjuje za autentikaciju korisnika na računarskim mrežama baziranim na Unix sistemu. Kontroler terminalnog pritupa je detaljno opisan u dokumentu RFC 1492. Protokol svoje instrukcije transportuje preko UDP i TCP, po jedinstvenom portu 49. Godine 1990. pojavila se nova verzija protokola pod nazivom XTACACS. U danima koji slede predstavljen je novi protokol pod nazivom TACACS+. Novi protokol nije u saglasnosti sa prohodnim protokolima (TACACS, XTACACS)
TACACS+ protokol osigurava kontrolu pristupa mrežnim uređajima preko jednog ili više centralizovanih servera. Sistem obezbeđuje odvojenu autentikaciju i autorizaciju [6].

<table>
<tr><td colspan="2">12345678</td><td>12345678</td><td>12345678</td><td>12345678</td></tr>
<tr><td>MAJOR_V</td><td>MINOR_V</td><td>TIP PAKETA</td><td>SEKVENCIJALNI BROJ</td><td>MARKER POLJA</td></tr>
<tr><td colspan="5">IDENTIFIKACIJA SESIJE</td></tr>
<tr><td colspan="5">DUŽINA PAKETA</td></tr>
</table>

Slika 16. TACACS+ zaglavlje

Značenje pojedinih polja:

- TIP PAKETA:
  - TAC_PLUS_AUTHEN:= 0x01 Autentikacija;
  - TAC_PLUS_AUTHOR:= 0x02 Autorizacija:
  - TAC_PLUS_ACCT:= 0x03 Monitoring;
- SEKVENCIJALNI BROJ – broj trenutnog paketa u trenutnoj sesiji;
- MARKER POLJA – određivanje statusa paketa (šifrovan ili ne);
- IDENTIFIKACIJA SESIJE – identifikacija trenutne sesije
- DUŽINA PAKETA – dužina podatka bez zaglavlja

### 2.6.5.4 Diameter

Diameter je protokol koji predstavlja logičkog naslednika RADIJUS. Dizajniran je da bude generalni radni okvir za bilo koju AAA aplikaciju. Funkcionalnosti Diametar protokola uključuju sledeće:

- Peer-to-Peer protokol
- Pouzdan i siguran transport
- Failover
- Podrška agentima
- Serverski inicirane poruke
- Uspostavljanje veze na nivou kvaliteta
- Dinamička pretraga peer-ova i konfiguracija

✓ Pouzdan transportni sloj:
  - TCP ili SCTP konekcija sa TLS, DTLS ili IPsec. Set

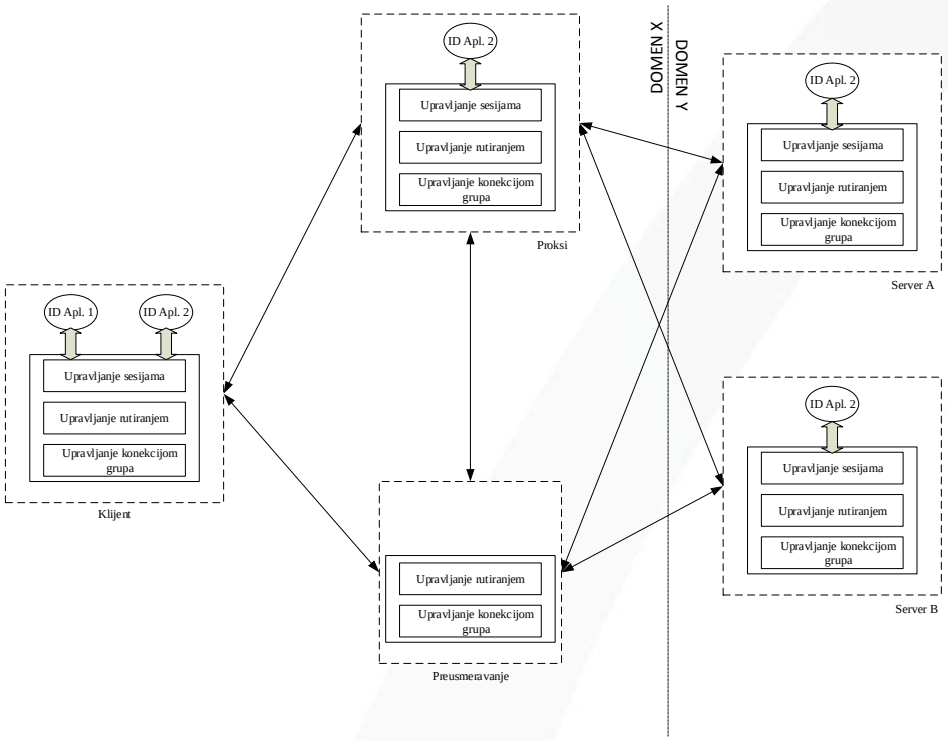
✓ Skup opštih komandi i Attribute-Value-Pairs (AVP's) podržanih od bilo kog Diameter peer-a, korišćen za:
  - Dinamičku pretragu peer-ova i upravljanje kolektivnostima;
  - Dinamički routing zasnovan na domenu
  - Upravljanje sesijama

- Monitoring
- Osnova upravljanja greškama

✓ Skup aplikacija korišćenih u dodatku Base protokola za specijalne namene

**Sigurnost Diametar protokola**

- TLS, DTLS ili IPsec su korišćeni prilikom zaštite konekcije;
- Diameter čvorovi su uzajavno autentifikovani kao deo TLS/TCP, DTLS/SCTP ili IPsec
- Sve Diametar poruke će se poslati kroz konekciju samo nakon uspešnog sigurnog konektovanja.




Slika 17. Arhitektura Diameter protokola

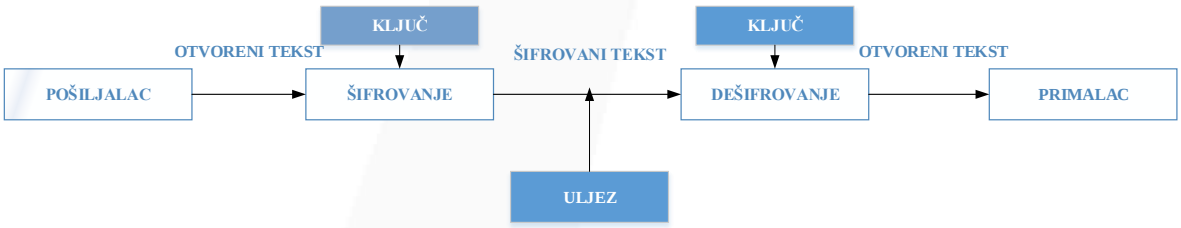
| Funkcionalnost | RADIJUS (RFC 2865) | Diameter (RFC 6733) |
|---|---|---|
| Transport | UDP: 1812 & 1813 | TCP i/ili SCTP |
| Security | IPsec | TLS, DTLS, IPsec |
| Operation Model | Client-Server | Peer-to-Peer |
| Intermediaries | Only Proxy | Relay, Redirect, Proxy |
| Peer Discovery | Static | Static ili DNS |
| Routing | IP routing | Realm-based + App-id |
| Max # Application | 1 (AAA) | 2^32 |
| Capability negotiation | No | Yes |
| Data Type | 5 Basic | 8 Basic + 7 complex |

| | | |
|---|---|---|
| Max # command | Up to 256 | Up to 2^24 |
| Max # packet size | 4096 octets | 2^24 octets |
| Max # attributes | 256 | 2^32 (standard) |
| Max # attributes size | 253 octets | 2^24 |
| Data Grouping | Tags (bad) | Generic |
| Compatibility | No | Yes |
| Failover | No | Yes |
| Keep-Alive | No | Yes |

Tabla 3. Poređenje funkcionalnosti

## 3 Kriptografija

Ljudsko biće je od svog nastajanja predodređeno da prati sledeće potrebe: komunikaciju i deljenje informacija i mišljenja, selektivnost ostvarene komunikacije. Ove dve potrebe će dovesti do razvoja umetnosti kodiranja informacija, na način da samo učesnici kojima je namenjena poruka mogu znati informaciju. Ne autorizovani korisnici neće biti u mogućnosti da vide informaciju, čak iako šifrovana poruka dospe u njihove ruke.
Umetnost i nauka o prikrivanju sadržaja poslatih poruka u komunikaciji je poznata kao kriptografija. Reč kriptografija je nastala kombinacijom grčkih reči "Kripto" od skrivenog i "graphene" od pisanog.
Zadatak kriptografije je da ostvari sigurnu komunikaciju, dve strane u interakciji (pošiljalac i primalac), ostvarenu preko nezavisnog komunikacionog linka (Interneta). Takva komunikacije moraju da spreče uljeza, koji osluškuje nesigurni komunikacioni link, da ima uvid u sadržaj poslate poruke. Tekst koji se šalje od strane pošiljaoca je u formi čistog teksta, i u zavisnosti od tipa primenjenog algoritma transformiše ga u šifrovani (ciphertext) tekst. Takav tekst (šifrat) se šalje kroz nesigurnu mrežu i dolazi do primaoca poruke. Uljez koji je u sredini komunikacije može u trenutku slanja slušati ne sigurni link i kao posledicu toga presresti i neovlašćeno preuzeti šifrat. Takva preuzeta poruka za njega kao uljeza mora ostati potpuno ne razumljiva, čime je ispunjen glavni zadatak primenjenog algoritma šifrovane poruke. Nakon dospeća šifrovanog testa primaocu, isti se dešifruje korišćenjem određenog ključa, razmenjenog pre komunikacije[1][2].




Slika 18. Grafički prikaz šifrovanja poruke

**Protokoli:**
U cilju obezbeđivanja privatnosti i autentičnosti, kreirani su šifarnički protokoli. Protokol predstavlja skup matematičkih pravila koji se primenjuju u šifrovanoj komunikaciji. Pomoću pomenutih protokola određuje se izbor algoritma za šifrovanje/dešifrovanje, međusobno se dogovaraju ključevi i drugi šifarnički parametri. Iz opisa se vidi da komunikacija dve strane mora da ima poznatu komponentu više od protivnika kako bi komunikacija bila sigurna.

## 3.1 Osnovni pojmovi

- Alfabet (engl. Alphabet) je konačan skup. Grčko slovo ∑ se koristi za označavanje pisma, npr. ∑ = {0,1,2,3,4,5,6,7,8,9} je pismo koje se sastoji od 10 karaktera, ∑ = {0,1} je pismo koje se sastoji od 2 binarna karaktera;
- Niz (engl. string) je konačan broj karaktera;
- Dužina (engl. Length) predstavlja broj karaktera u nizu, na primer: dužina niza X se označava sa |X|; niz Y = *matematika* je dužine 10 karaktera. Niz dužine nula naziva se „prazan niz" i označava se sa φ; ako su X i Y nizovi i njihov spoj se označava sa X||Y;
- Jezik (engl. Language) je grupa nizova koji nastaju iz jednog niza, na primer: ∑ pisma i ∑* predstavljaju sve nizove čiji karakteri počinju sa ∑:{0,1}* ={ φ,01,000,110,1,0,0111,… }

U kriptografiji postoje dva osnovna bezbednosna modela:

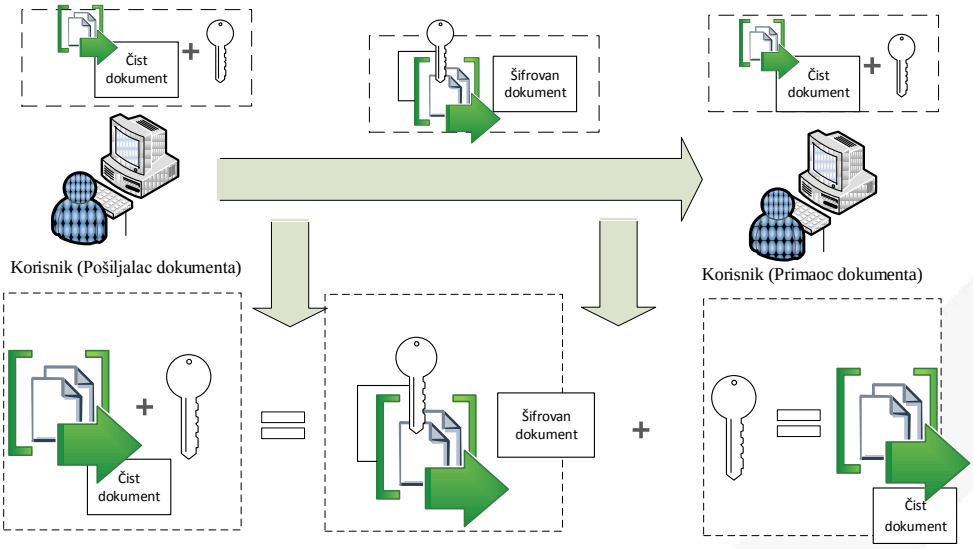
- Simetričan (engl. Simmetric) model sa tajnim ključevima;
- Asimetrični (engl. Asymmetric) model sa javnim i privatnim ključevima.

### 3.1.1 Simetričan model

Simetrična enkripcija je najstarija i dobro poznata tehnika šifrovanja podataka. Simetrična enkripcija i algoritam simetričnog ključa je model koji koristi isti kriptografski ključ prilikom šifrovanja poruke, na obe strane u komunikaciji (pošiljalac i primalac). U ovom modelu koristi se ključ koji može biti identičan ili malo izmenjen. Praktično, ključ predstavlja deljenu tajnu između dva ili više učesnika u očuvanju sigurnosti komunikacionog linka.
Tajni ključ može biti broj, reč ili bilo koji niz nasumičnih karaktera, koji se primenjuje na tekst poruke i menja sadržinu teksta na poseban način. Na primer: izmena svakog slova u poruci za određeni broj mesta, pomerenih prema početku ili kraju alfabeta. Dokle god svaki od učenika u komunikaciji zna tajni ključ, enkripcija i dekripcija poruke je moguća. Zahtevi koji se nameću na obe strane u komunikaciji su dostupnost sigurnog ključa, što čini najveći nedostatak modela simetrične enkripcije, u poređenju sa drugim modelom asimetrične enkripcije i razmene javnog ključa[1].
Simetrična enkripcija razlikuje dva tipa, i to:

- Tok šifre (stream cipher) - vrši enkripciju poruke u jednom nizu;
- Blok šifre (block cipher) - vrši segmentiranje poruke kreiranjem enkriptovanih jedinica ili blokova, koji se kasnije šalju kao celina. Najčešća veličina bloka je 64 bit -a. Standardni AES algoritam od decembra 2001. godine koristi blokove od 128 bit.

Primer implementacije simetrične enkripcije uključuju: AES, CAST5, 3DES, IDEA, ...



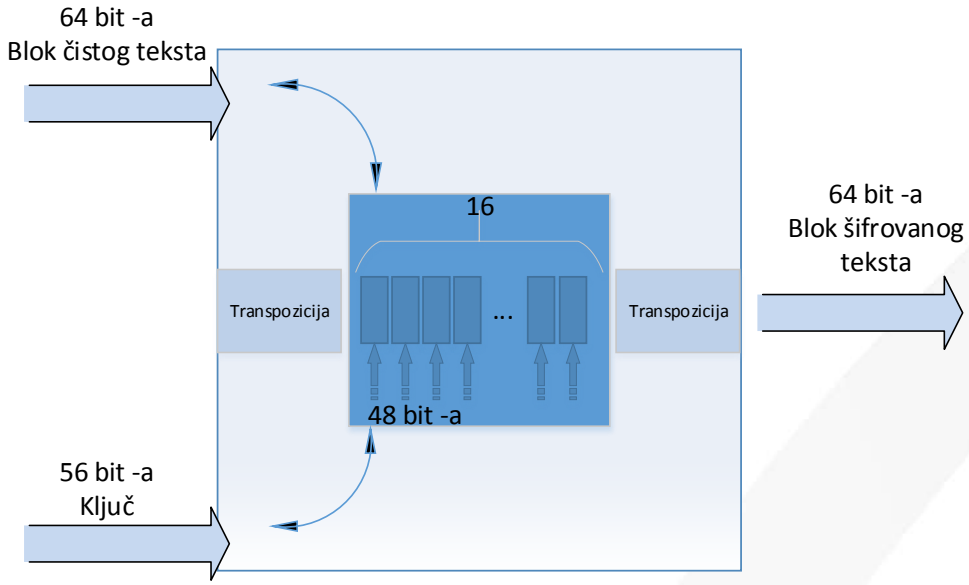

Slika 19. Simetrično šifrovanje

| DES prethodnici/naslednici | AES kandidati | Jednostavni | Šifrovanje toka podataka |
|---|---|---|---|
| Lucifer | AES (Rijndael) | 3-Way | A-5 |
| DES | FROG | ENIGMA | Helix |
| DESX | LOKI97-sim<br>LOKI91 -sim | Solitaire | Pike, Pike |
| 3-DES | MARS | TEA | RC4 |
| Blowfish | RC6 | | SEAL |
| DEAL | Magenta | | SOBER |
| FEAL | Serpent | | WAKE |
| ICE | Twofish | | |

Tabela 4. Popis primenjenih simetričnih algoritama

### 3.1.1.1 DES

Standardni enkripcioni algoritam podataka DES donedavno je bio jedan od standardnih algoritama enkripcije simetričnog ključa. Algoritam sa svojom logikom je bio presudan u kreiranju moderne kriptografije u akademskom svetu. Algoritam je razvijen početkom 1970. godina od strane IBM i zasnovan na ranije dizajniranoj logici od strane Horst Feistel -a. Nakon pojave konačne verzije, algoritam je prosleđen Nacionalnom Birou za Standardizaciju (NBS). Tokom 1976. godine, nakon konsultacija sa Agencijom za Nacionalnom Sigurnosnom (NSA), NBS je odabrao nešto modifikovaniju verziju (ojačanu na kriptoanalizu ali oslabljenu prema napadima "brutalne sile"), koju je objavio 1977. godine kao oficijalni Federalni Informacioni Standard. Publikacija od strane NSA je rezultovala interno prihvatanje i širenje uz permanentno akademsko promatranje i analizu.
Danas je DES algoritam nesiguran za mnoge aplikacije, zbog 56 bit (64 bit -a) efektivne veličine ključa, koji je veoma slab.




Slika 20. DES algoritam za enkripciju3DES i 2-Key 3DES

Enkripcija DES -a upotrebljava pod ključ veličine 48 bit-a. Tokom januara 1999.godine, dve ujedinjene grupacije su javno organizovali razbijanje DES enkripcije, do tada široko primenjene, u trajanju od 22 sata i 15 minuta. Time je dokazana slabost enkripcije. U narednim danima je razvijen 3DES algoritam, koji se smatra sigurnijim izborom od svog prethodnika. 3DES enkripcija koristi više ključeva prilikom enkripcije izvornog bloka podataka. Kasnije je razvijen AES koji je u potpunosti zamenio DES i 3DES algoritam [1].

### 3.1.1.2 AES

Napredni Enkripcioni Standard AES, takođe poznat pod imenom Rijndael (originalno ime) je novi način enkripcije koji je zamenio DES. Razlog je veoma jasan, razvojem informatičke pismenosti, kriptoanaliza (kao i kriptografija) koja je u mnogome napredovala. Algoritam DES je kompromitovan (smatra se slabim) i iz tog razloga je razvijen AES.
Prihvatanje AES, kao stan je započeo Nacionalni Institut za Standardizaciju (NIST) 1997.godine raspisivanjem javnog izbora. 3DES je izabran kao privremeni standard. AES je definisan u svakom od sledećih dokumenta: FIPS PUB 197 – AES i ISO/IEC 18033-3- Informacione tehnologije – Sigurnosne tehnike – Enkripcioni algoritam – Deo 3: Šifre bloka
AES je zasnovan na principima kriptografskog dizajna poznatog kao supstitucija-permutacija mreže, kombinacijom oba principa i brzinama tranzicije na softveru i hardveru. Za razliku od prethodnika, AES ne koristi Feistel mrežu. AES je varijanta Rijndael –a, koji ima fiksnu vrednost bloka od 128 bit –a i veličinu ključa od 128, 192 i 256 bit –a. AES operiše u matrici 4x4 bajta. Dužina ključa korišćenog za AES šifriranje definiše broj ponavljanja transformacionih krugova koji konvertuje ulaz (čist tekst) u finalni izlazni dokument (šifrirani tekst). Broj krugova ponavljanja je sledeći: 10 krugova ponavljanja za ključ dužine 128 bit –a; 12 krugova ponavljanja za dužinu ključa od 192 bit –a; 14 krugova ponavljanja za dužinu ključa od 256 bit –a.
Svaki krug je sačinjen od nekoliko procesnih koraka, gde svaki sadrži četiri slična ali različita stanja, uključujući jedno koje zavisi od enkripcionog ključa za sebe. Set reverznih krugova se primenjuje na transformaciju šifriranog teksta nazad (u originalno stanje), korišćenjem istog enkripcionog ključa.

Na svakih pet godina NIST vrši reviziju AES –a i predlaže korekcije ukoliko naiđe na problem [1].

### 3.1.2 Asimetričan model

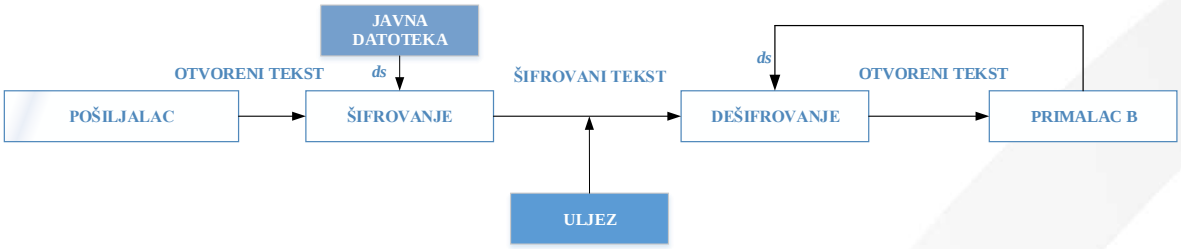
Asimetričnost u šifrovanju teksta predstavlja najveći napredak u istoriji kriptografije. Korišćenje javnog i privatnog ključa je u mnogome povećalo sigurnost razmene ključeva jer učesnici u komunikaciji nemaju istu ulogu. Ovaj Koncepti koji se koriste u logici ovog modela uključuju teoriju brojeva. Imajući u vidu da se česta razmena šifrovanih podataka istim ključem mogla kompromitovati tajnost podataka, pribeglo se izboru druge metode.
Witfield Diffie i Martin Hellman, istraživači sa univerziteta Stanford, su prvi publikovali ideju u vezi sa asimetričnom enkripcijom, prezentovanu na 1977 strana publikacije pod nazivom "Novi Pravci u Kriptografiji". Asimetričan algoritam, kako je predstavljeno u Diffie-Hellman publikaciji je funkcija u jednom pravcu. Takvu funkciju je lako jednosmerno primeniti, ali je teško ili nemoguće preokrenuti. Na primer: Prilično je lako sračunati proizvod dva broja, ali je mnogo teže sračunati faktore ako je poznat samo njihov rezultat. Ako je na primer poznata vrednost proizvoda i jednog faktora, lako se može sračunati vrednost drugog faktor. U tom kontekstu, funkcija je iskorišćena i algoritam je poznat. Ovo saznanje ne omogućava dešifrovanje poruke kod asimetrične enkripcije. Jedina informacija koja je neophodna u čitavom procesu dešifrovanja je tajni ključ primaoca poruke.
U slučaju gde se koristi isti algoritam za šifrovanje i dešifrovanje , kao što je RSA, poruka se može potpisati od strane određenog pošiljaoca: i ako pošiljalac šifriranu poruku potpiše privatnim ključem, onda se poruka može dešifrovati samo ako se koristi javni ključ pošiljaoca, autetikujući pošiljaoca poruke.
Kriptografija javnog ključa predstavlja fundamentalan činilac kriptosistema, aplikacija i protokola. Ona podupire razne Internet standarde, kao što su Transportni Sigurnosni Sloj (TLS), GPG, S/MIME i drugi. Neki od algoritama javnog ključa obezbeđuju distribuciju ključa (Diffie-Hellman razmena ključa), digitalni potpis (algoritam Digitalnog Potpisa) i neki drugi koji obezbeđuju oba (RSA). Asimetrična kriptografija je primenjena metoda koji pruža poverljivost, autentičnost i neporecivost elektronske komunikacije [7].

| Široko prihvaćene tehnike | Usko prihvaćene tehnike | Još uvek nesigurne tehnike |
|---|---|---|
| Diffie-Hellman | NTRUEncrypt | Markle-Hellman knapsack |
| Digital Signature Standard | McEliece | |
| RSA | | |
| Paillier cryptosystem | | |
| YAK | | |
| Password-Authenticated key agreement | | |
| ElGamal | | |

Tabela 5. Primer primenjenih tehnika asimetričnog ključa

Imajući u vidu sve prednosti koje pruža primena asimetričnog ključa, nije moguć potpuni supstitut za simetričnu razmenu ključa. I dalje su neke od ostvarenih komunikacija

afektirane primenom simetrične enkripcije, gde se zahteva brza konverzija. Asimetrična enkripcija je u mnogome sporija od simetrične, do 1000 puta od savremenih izbora simetričnih algoritama. U analizi se pojavljuje još jedna od slabosti asimetričnog algoritma, poznata kao ranjivost na poznate pretnje "otvoreni tekst".




Slika 21. Šematski prikaz metode asimetrične kriptografija

| | Simetričan model | Asimetričan model |
|---|---|---|
| Privatnost poruke | Simetrično šifrovanje (tajni ključ) | Asimetrično šifrovanje (javni ključ strane primaoca) |
| Autentičnost i integritet poruke | Kod autentičnosti poruke (MAC) | Šema digitalnog potpisivanja (privatni ključ pošiljaoca) |

Tabela 6. Prikaz simetričnog i asimetričnog modela

# 4 Digitalna forenzika

## 4.1 Uopšteno

Digitalna forenzika (poznata pod imenom nauka o digitalnoj forenzici) je grana u okviru forenzičke nauke koja obuhvata procese restauracije i istrage korisnog materijala koji je nađen i zaplenjen na digitalnoj mediji, najčešće je u vezi sa računarskim kriminalom. Termin digitalna forenzika se bazično koristi kao sinonim za kompjutersku forenziku, od koje se očekuje da pokriva sve uređaje koji su sposobni da sačuvaju digitalne podatke. Sa korenima u revoluciji personalnih računara, kasnih sedamdesetih i početkom osamdesetih godina prošlog veka, disciplina je evoluirala, i sa sporadičnim primenama tokom devedesetih godina pa sve do početka 21. veka, kada su usvojene relevantne preporuke, pravila i procedure iz te oblasti.

Digitalna forenzička istraga uključuje različite alate i aplikacije, a najčešće u toku procesa gde se brani, podržava ili odbija postavljena hipoteza pre i tokom sudskog procesa (kao deo elektronskog istraživačkog procesa). Forenzicari se takođe pojavljuju i u privatnim istragama, u okviru internih korporativnih istraga sistema (aktivna i proaktivna analiza).

Tehnički aspekt istrage podeljen je u nekoliko podgrana, koje su vezane za sve tipove digitalnih uređaja (medija) koje su u to uključene; kompjuterska forenzika, mrežna forenzika, analiza forenzičkih podataka i forenzika mobilnih uređaja. Tipičan forenzički proces objedinjuje konfiskaciju digitalne imovine, forenzičke akvizicije i analize digitalnih medija i generisanje izveštaja u procesu prikupljanja relevantnih dokaza.

Pored utvrđivanja direktnih dokaza počinjenog kriminalnog akta, digitalna forenzika se bavi dokaznim postupkom specifično za sumnjive događaje, potvrde alibija i datih izjava,

determinacija identiteta, utvrđivanje izvora (u slučaju zaštite *copyright* prava) ili autentičnosti dokumenata [12].
Istraživanje je mnogo šire u svom polju delovanja nego druge oblasti u forenzičkoj analizi, često uključujući kompleksne vremenske linije i hipoteze

## 4.2 Procesi

Digitalna forenzička istraga se najčešće sastoji od tri ključne faze: akvizicija ili imidžovanje dokaznog materijala, analiza i izveštavanje. Idealna akvizicija uključuje prikupljanje i pravljenje imidža (identične softverske kopije) računarskih nosioca podataka i kreiranje identičnog duplikata na nivou sektora (forenzički duplikat) medije, najčešće korišćenog uređaja bloka pisanja, kako bi sprečili izmenu originala. Međutim, rapidni razvoj i uvećanje prostora na mediju, kao i razvoj servisa u oblaku sve više vodi u pravcu žive akvizicije, pri čemu se postiže logika prilikom kopiranja podataka, i pre nego izvršavanje procesa bekapovanja fizičkog storidž uređaja. Obe metode zahtevaju imidž (ili logičku kopiju) i original (mediju ili podatke), koji su hešovani
(korišćenjem algoritma kao što su SHA-1 ili MD5) zajedno sa uporednim vrednostima za proveru tačnosti kreirane kopije.
Tokom faza prilikom analize istraživač rekreira dokazni materijal koristeći brojne metode i alate. Tokom 2002. godine, u International Journal of Digital Evidence je predstavljen članak koji je opisao neophodne korake, referencirane na način "duboka sistemska pretraga materijalnih dokaza vezano za osumljičeni događaj“. U 2006. godini forenzički istraživač Brajan Kerijer opisao je "intuitivne procedure" u kojima se na prvom mestu vrši identifikacija očiglednih dokaza, a nakon toga iscrpna istraga koja bi ispunila moguće praznine u istrazi koje nedostaju [14].
Sam proces analize može varirati između istrage, ili zajedničkih metodologija koje uključuju sledeće faktore: dobijanje vrednosti po ključnim rečima u pretrazi kroz digitalne medije (unutar fajlova kao i nealociranog i labavog prostora), reparacija obrisanih fajlova i ekstrakcija informacija iz registra (lista korisničkih naloga ili prikačenih USB uređaja). Rekreirani dokazni materijal se prvo analizira kako bi se u daljem događaj rekonstruisao, a nakon toga doneo određeni zaključak [9].

## 4.3 Korisni alati

U zavisnosti od karakteristika, namene i okruženja alati digitalne forenzike imaju za cilj da prikupljaju odgovarajuće logove i podatke sa servera, desktop računara, mrežne opreme i mobilnih uređaja u svrhu kvalitativne analize korisne za rekreiranje nastalog incidenta. Isto tako, alati se koriste za rekreiranje oštećenih ili obrisanih podataka sa hardverskih ili softverski oštećenih medija. Najrasprostranjeniji alati za tu namenu su: EnCase, Paessler Network Monitor PRTG, Safe Back, ManageEngine EventLog, NetWrix, Access Data, Get Data Back, i drugi [21][17].

### 4.3.1 Kratak opis korišćenijih forenzičkih alata

**Manage Engine eventlog Analyzer** - Manage Engine predstavlja veb aplikaciju koja se koristi za monitoring mrežne infrastrukture, servera i aplikacija, tj. servisa aktivnog direktorijuma, desktop računara i mobilnih uređaja. U našem primeru aplikacija prikuplja logove događaja sa servera i uređaja na mreži. Po indikaciji predefinisanog alerta događaj se šalje na mail administratoru sistema na uvid i dalje postupanje. Manage Engine je instaliran na serveru koji ima predefinisanu ulogu menadžera mreže tj. servera sabirnika svih logova izabranih uređaja sa mreže (AD DC, i drugih servera). Imajući u vidu servis autentikacije, koji je u upotrebi, RADIJUS protokol, poželjno je pulirati logove radi kontrole ili forenzičke analize mogućeg incidenta koji može nastati nesmotrenim radom na

infrastrukturi i sistemu uopšte. Takođe, prati se daljinski pristup sistemima uređajima (RDP, Telnet, SHH, i drugi) na servere i servise (SQL, MMC produkcionih servera, i drugi) i mrežne opreme (ona koja pita RADIJUS server prilikom verifikacije korisnika).
Nakon instalacije Manage Engine –a pristupa se podešavanju porta po kom će server slušati. Dedikovan pristup se kasnije brani na mrežnoj opremi, po portu i adresi pirova u komunikaciji, tj. limitiranjem pristupa po portu i pod-mreži dozvoljenog saobraćaja. Daljinski pristup korisničkom interfejsu (slika 22. ) ostvaruje se putem veb pretraživača, izborom soketa u adresnom polju (na primer:192.168.36.1:8081).



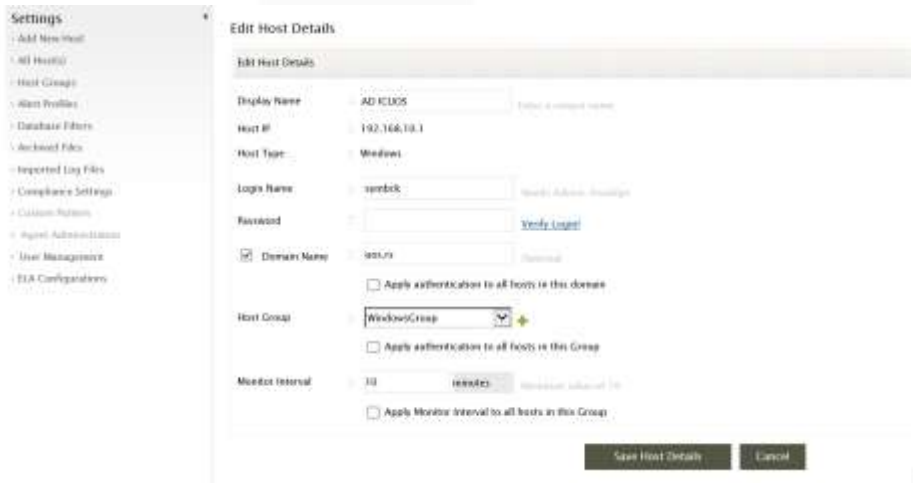
Slika 22. Forma zahteva za pristup aplikativnom korisničkom interfejsu

Nakon uspešnog logovanja na aplikaciju, na glavnoj strani je moguće pratiti sistemske promene u okviru grafičkog prikaza svih događaja, predefinisanih alarma, vaznih događaja, izdvojenih kategorija događaja, sigurnosnih događaja i trenutnih trendova.



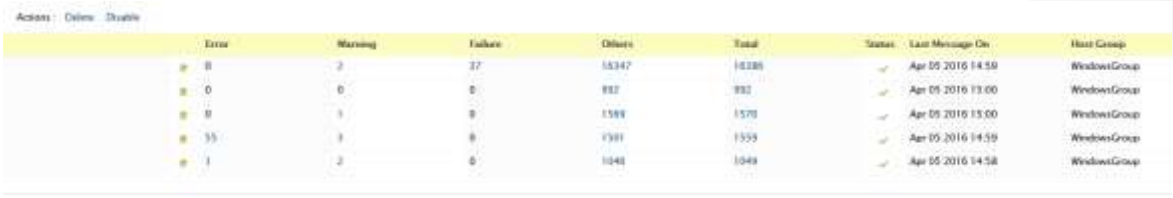
Slika 23. Prikaz glavne strane alata Manage Event-a

Kontrola izabranih servera i/ili mrežne opreme se odvija na delu glavne strane, koja se poziva preko taba hostova.
Pozivom na dodaj otvara se pod meni u kome se kucaju sledeće generalije: ime servera, IP adresa servera, parametri servisnog naloga koji se vrti na serverskoj strani, pripadajući domen i pulirajući vremenski interval.



Slika 24. Forma za unos novog hosta u aplikaciju

Nakon unosa traženih podataka i snimanja detalja trebali bi se uočiti uvećanje broja puliranih zapisa, koji će se svrstavati u definisane grupe: grešaka, upozorenja, zabrana i drugo.
Status i vreme zapisa moraju biti potvrđeni i vremenski se poklapati sa vremenom zadnjeg uspešnog puliranja događaja.



Slika 25. Prikaz grupisanih logova

Posle verifikacije uspešnog prikupljenih logova možemo krenuti u kreiranje predefinisanih alarma koje ćemo, po njihovom izuzeću slati na e-mail administratoru sistema, na uvid i dalje postupanje. Na osnovu modifikovanih kriterijuma kreiramo uslove i filtere imenovanog alarma. Na slici 26. prikazan je predefinisani filter koji prikuplja sve događaje iz svih grupa po uslovu iz alerta i momentalno generiše određeni e-mail sa sadržajem izabranih promenljivih administratoru sistema na dalje postupanje. Događaj se vezuje za RDP po generisanom event ID 4624, kao na slici [18].



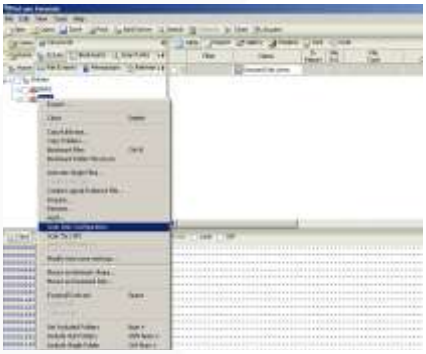

Slika 26. Prikaz okvira za definisanje alerta po definisanom kriterijumu.

Na slici 27. je prikazan primer puliranog mail-a od predefinisanog alerta RADIUS loga na sistem, daljinskog pristupa preko koncentratora sistema ASA 5510.




Slika 27. Forma generisanog mail-a na osnovu generisanog RADIUS loga

**EnCase** - EnCase predstavlja moćan forenzički alat, jedan od najkorisnijih alata iz familije forenzičkih softverskih dodataka poznatog proizvođača Guidence Software. U grupu alata iz familije proizvoda uključeni su: EnCase Enterprise, EnCase Forensic Edition, EnCase Forensic eDiscovery, i EnCase Lab Edition. Svi ti programi koriste vlastite image file formate. Kako bi se automatizovao proces proizvođač je ostavio mogućnost pravljenja skript komandi. Imajući u vidu tačnost i pouzdanost alata, dokazi koji se generišu su prihvaćeni kao validan dokaz u toku suđenja ili pravdanje odredbenih hipoteza za nastali incident. Kako sudskim veštacima tako i stručnjacima iz oblasti IT pomaže u rešavanju i istraživanju slučajeva, analizu medija bez mogućnosti promene izvornih podataka. Aplikacija je dostupna samo kvalifikovanim korisnicima ih oblasti obrazovanja i državnim organizacijama. EnCase koristi MD5 SHA-1 heš koji smešta podatke u vlastiti EnCase haš fajl format. Heš je obavezan metod zaštite podataka i imidža originalnog zapisa dokaznog materijala. Takvom zaštitom se omogućava validnost digitalnog dokaznog materijala od naknadne izmene [15].



Slika 28. Ovih EnCase-a pre skeniranja konfiguracije afektiranog diska

**Paessler Network monitor PRTG –** predstavlja kompleksan forenzički alat koji omogućava sledeće: analizu ukupne serverske iskorišćenosti, mrežni monitoring, analizu iskorišćenosti i kontrolu mrežnog propusnog opsega (SNMP, Packet Sniffing i Netflow).

Aplikaciju je moguće instalirati na Majkrosoft i Unix operativnim sistemima. PRTG predstavlja veb aplikaciju koja se koristi za monitoring mrežne infrastrukture, servera i aplikacija, tj. servisa aktivnog direktorijuma, desktop računara i mobilnih uređaja. U našem primeru aplikacija prikuplja sistemske logove (Syslog) događaja sa mrežnih uređaja u mreži. Forenzički alat sadrži veliku biblioteku MIB[1] OID[2], koji predstavljaju kolekciju definicija definisanih osobina praćenog objekta [19].



Slika 29. Forma grafičkog prikaza senzora različitih OID-a.

Primer jednog OID senzora se predstavlja na sledeći način:

1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3

# 5 Studijsko istraživački rad – Primenjeno tehnološko rešenje

## 5.1 Uloga

Termin mrežna barijera se u informatici reprezentuje kao mrežni sigurnosni sistem koji prati i kontroliše dolazni i odlazni saobraćaj, zasnovan na predefinisanim sigurnosnim parametrima. Njena uloga je da uspostavi mrežnu barijeru između sigurne mreže sa jedne strane, i mreže locirane izvan zaštićenog perimetra (Internet), koji se smatra nesigurnim. Mrežna barijera se može predstaviti i kao deo hardvera i/ili softvera, implementirana na lokalnom i/ili centralnom računaru. U osnovi, mrežna barijera predstavlja komponentu koji obavlja kontrolu mrežnog transporta, preko određenog komunikacionog kanala, upućenog prema i od sistema (mrežnih resursa). Kao primer najbazičnijeg modela mrežne barijere može se predstaviti kablovski modem koji bi trebao da usmerava mrežni saobraćaj prema izlazu mreže, ali u isto vreme sprečava mrežni saobraćaj usmeren sa interneta prema internoj mreži. Npr.: mrežne barijere iz Cisco familije proizvoda ASA, štiti korporativno mrežno okruženje na način da brani sigurnu mrežu od slobodnog pristupa bez dozvole. Takođe, obezbeđuje pristup korisnicima sa najvišim pravima pristupa na siguran i bezbedan način.
Servisi koji se dostupni na komercijalnim mrežnim barijerama uključuju sledeće funkcionalnosti:

- Kontrola i upravljanje mrežnog saobraćaja;
- Autentikacija pristupa;
- Uspostavljanje servisa „ u sredini“;
- Zaštita organizacionih resursa (uključujući prevenciju i detekciju uljeza);

[1] *Management Information Base*
[2] *Object Identifiers*

- Translacija mrežnih adresa;
- Sistem sprečavanja mrežnih upada;
- Sistem detekcije mrežnih upada;
- Praćenje, logovanje i izveštavanje na događaj;
- VPN[3] koncentracija.

## 5.2 Tipovi

Razlikujemo dva tipa mrežnih barijera:

1. **Personalni** – najčešće su predstavljeni u formi softverske aplikacije koje se instalira na personalnim računarima, štiteći samo zasebne računarske stanice i/ili servere. Takve aplikacije najčešće se prepoznaju kao host-based firewall, na primer: Windows Defender - komponenta koja se ugrađuje u novije verzije operativnih sistema, ZoneAlarm, Comodo, Norton Internet Security, McAfee Personal Firewall;
2. **Mrežni** – uređaji koji su proizvedeni i optimizovani za operacije koje uključuju zaštitu računarske i mrežne infrastrukture na njenim obodima, čineći mrežu sigurnom od potencijalnih pretnji upućenih sa interneta i/ili drugih manje sigurnih mreža. Potencijalni izbor uređaja zavisi od mnogih faktora (cena, omogućenih funcionalnosti, skalabilnos sa ostatkom infrastrukture, i dr.), a najčešći izbor uključuje sledeću listu proizvoda: Cisco ASA Security Appliance, Barakuda, CheckPoint, Fortinet, Juniper, McAfee Firewall Enterprise, Palo Alto Networks, Dell SonicWall i dr.

## 5.3 Klasifikacija

Klasifikacija mrežnih barijera[4] je zasnovana na referenciranju funcionalnosti servisa prema sloju OSI modela[5]:

| Tip mrežne barijere | Opis |
|---|---|
| **Statička filtracija paketa** | Prva generacija mrežnih barijera, koje vrše inspekciju paketa na 3 sloju OSI modela, na osnovu predefinisanih pravila. |
| **Sklopni nivo**<br>Operiše na 4. sloj OSI modela | Druga generacija mrežnih barijera, vrši validaciju paketa ili na zahtev prilikom uspostave linka ili u delu uspostavljene sesije dve instance, koja se obavlja na 4 sloju OSI modela. |
| **Aplikacioni sloj**<br>Operišu na 3., 4., 5. i 7. sloj OSI modela | Aplikativni proksi sloj, nudi najviši stepen sigurnosti, vršeći inspekciju mrežnog saobraćaja na svih sedam slojeva OSI modela, uz određeno povećanja latencije. |
| **Dinamička filtracija paketa**<br>Operišu na 3.,4., i 5. Sloju OSI modela | Mrežna barijera koja je poznata po sigurnosti uspostavljenih sesija, prateći trenutne mrežne komunikacije, unoseći statuse ostvarenih sesija u zasebnoj tabeli. |
| **Transparentni firewall**<br>Operiše na 2. sloju OSI modela | Mrežna barijera nema IP adrese, izuzev upravljačkog interfejsa. Lak je za implementaciju, koji prati mrežni saobraćaj po unapred definisana pravila. |

[3] Virtual Private Network
[4] Engl. Firewall
[5] Engl. Open Systems Interconnection model

Tabela 7. Klasifikacija mrežnih barijera




Slika 30. Grafički prikaz „Gartnet magic quadrant enterprise network firewall“ za 2015.godinu [21]

Globalna istraživačka kompanija Gartner je u svom magičnom kvadrantu prepoznala kompanije iz oblasti razvoja mrežne infrastrukture, koje su vezane za razvoj mrežnih barijera, klasifikujući ih u određene kvadrante na osnovu njihovih tendencija i tehnološkog razvoja. Na slici 30. prikazan je magični kvadrant, koji je po oceni globalne istraživačke kompanije Gartner za 2015. godinu, refenetni pokazatelj razvoja i tendencija iz oblasti mrežnih barijera. Iz prikazanog grafika se jasno vide favoriti u referentnom segmentu industrije. Kompanije koje se ističu i zaslužuju pomen su sledeće: Cisco, Fortinet, Palo Alto, Check Point [15].

## 5.4 Tehničke karakteristike izabranog uređaja

Renomirani proizvođač mrežne i računarske opreme Cisco je u martu 2005. godine predstavio novu familiju proizvoda ASA[6]. Novi uređaj je u mnogome sublimirao funkcionalnosti svojih prethodnika (PIX, VPN[7] 3000), širokopojasnih koncentratora velikih mogućnosti i primene, uključujući IDS liniju proizvoda. Sa pojavom iOS v7.x, ASA i PIX su počeli da se razlikuju po mnogo čemu. Počev od ASA 5505, koja pokriva segment poslovanja malih i kućnih poslovnih okruženja, sve do ASA 5585-X izbor je velik, u zavisnosti od realnih potreba i zahteva mrežnog okruženja.

[6] Engl. Cisco Adaptive Security Appliance, Firewall Device
[7] Engl. Virtual Private Network

| Cisco ASA Model | ASA 5505 /Security Plus | ASA 5510 /Security Plus | ASA 5512-X /Security Plus | ASA 5515-X /Security Plus |
|---|---|---|---|---|
| Propusni opseg | <=150 Mbps | <= 300 Mbps | 1 Gbps | 1.2 Gbps |
| Propusni opseg sistema za prevenciju napada | <= 75 Mbps sa IPS hardverskim modulom | <= 150 Mbps IPS hardverskim modulom | 250 Mbps (dodatni hardver nije potreban) | 400 Mbps (dodatni hardver nije potreban) |
| Konkurentnost sesija | 10k/25k | 50k/130k | 100k | 250k |
| Paketa po sekundi | 85k | 190k | 450k | 500k |
| VPN propusni opseg | 100 Mbps | 170 Mbps | 200 Mbps | 250 Mbps |
| L2L i IKEv1 VPN korisničke sesije | 10/25 | 250 | 250 | 250 |
| VLAN - ova | 3/20 | 50/100 | 50/100 | 100 |
| Podržana funkcionalnost visoke dostupnosti | Active/Standby | Active/Standby i Active/Active | Active/Standby i Active/Active | Active/Standby i Active/Active |
| Redundantnost napajanja | Ne | Ne | Ne | Ne |

Tabela 8. Komparativna analiza nekoliko modela iz familije ASA

U skladu sa zahtevom okruženja, izabrani uređaj je ASA 5510 /Security Plus, i u daljem tekstu ću aplikovati sve na izabranom uređaju.

### 5.5 IPSec VPN

Cisco ASA predstavlja uređaj koji je optimizovan za uspostavljanje virtualnih konekcija sa drugim računarskim mrežama (Site-to Site VPN) i korisnicima (Remote-Access VPN), preko nesigurne računarske mreže (npr. Internet).
IPSec VPN-a je zasnovan na staroj IKEv1 IPSec tehnologiji. Međutim, novi IKEv2 IPSec, već implementiran, čeka širu primenu u danima koji slede.
IPSec čini otvoren IETF standard koji omogućava šifrovanu mrežnu komunikaciju između pirova na mreži. Standard je sačinjen od steka protokola koji obezbeđuju poverljivost, integritet i autentičnost podataka. Virtualna privatna mreža obezbeđuje sigurni privatni tunel uspostavljen preko nesigurne računarske mreže, tako da predstavlja idealno rešenje tokom realizacije VPN –a, ostvarenog preko Interneta ili drugih, manje sigurnih mreža [4].
Protokoli i standardi koji su uključeni u stek IPSec su:

- **ESP**[8] – predstavlja prvi od dva glavna protokola koja čine stek IPSec-a, obezbeđujući servise integriteta, autentičnosti i poverljivosti podataka;

[8] Engl. Encapsulation Security Payload

- **AH**[9] – Predstavlja drugi najvažniji protokola iz IPSec steka. Protokol obezbeđuje digitalni potpis za pakete prilikom prenosa kroz računarsku mrežu, obezbeđujući da ne dođe do neovlašćene izmene podatka;
- **IKE**[10] – Predstavlja mehanizam korišćen prilikom razmene ključeva tokom enkripcije, autentikovanjem IPSec pirova i tokom pregovaranja IPSec-a. Na ASA mrežnoj barijeri, mehanizam predstavlja sinonim sa ISAKMP;
- **DES, 3DES, AES:** Predstavljaju enkripcioni algoritam podržan od ASA firewall-a. DES je najslabiji (koristi 56-bit enkripcioni ključ), AES je najjači (koristi 128, 192 i 256 bit enkripcioni ključ). 3DES predstavlja optimalan izbor koristeći 168 bit enkripcioni ključ;
- **Diffie-Helman Group (DH)** – predstavlja kriptografski protokol javnog ključa korišćen od strane IKE prilikom uspostave ključa sesije;
- **MD5, SHA-1** – Predstavljaju hash algoritam korišćen prilikom autentikacije paketa podataka. SHA je jači nego MD5 algoritma;
- **Security Association (SA)** – Predstavlja konekciju između pirova. Svaki IPSec pir čuva SA bazu podataka u svojoj memoriji sa pripadajućim SA parametrima. SA je jedinstveno identifikovan od IPSec pira, sigurnosnih protokola i sigurnosnih indeksnih parametara (SPI) [16].

### 5.5.1 Podela IPSec VPN mreža

IPSec VPN delimo u dve glavne kategorije:

- VPN zasnovan na IPSec[11] ostvarenoj vezi
  - Site-to-Site IPSec VPN
  - Remote Access IPSEC VPN Client
- VPN zasnovan na SSL[12] ostvarenoj vezi
  - Clientless Mode WebVPN – uspostavljanje VPN tunela preko veb pretraživača;
  - AnyConnect VPN – klijent koji je razvijen na Java platformi, obezbeđujući korisniku ostvarivanje SSL sigurnog tunela do centralne lokacije (ASA - koncentratora).

### 5.5.2 Koraci prilikom realizaciji sigurnog tunela

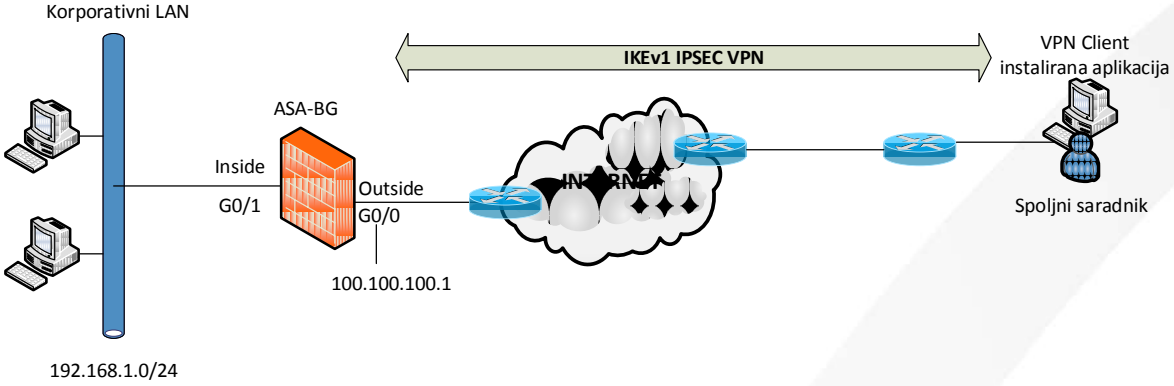
Prilikom uspostavljanja sigurnog tunela potrebno je definisati pet proceduralnih koraka, direktno na mrežnom uređaju, i to:

1. Definisanje interesantnog saobraćaj: Uređaj prepoznaje saobraćaj koji se štiti;
2. Faza 1 (ISAKMP): Uređaj pregovara IKE sigurnosnu politiku i uspostavlja sigurni kanal komunikacije;
3. Faza 2 (IPSec): Uređaj pregovara IKE sigurnosnu politiku u cilju zaštite podataka;
4. Transfer podataka: Podaci se prebacuju sigurnim putem između pireva na IPSec parametrima i ključevima dogovorenim tokom prethodnih faza;
5. IPSec prekidanje tunela: SA[13] se prekida kada je isteklo definisano vreme ili je limit vezan za prenos podataka prešao zadatu granicu [13].

[9] Engl. Authentication Header
[10] Engl. Internet Key Exchange
[11] Engl. IPSec Based VPN
[12] Engl. SSL Based VPN (WebVPN)
[13] Engl. Security Association

## 5.6 Konfigurisanje daljinskog pristupa VPN klijenta[14] (studija slučaja)

Na zahtev spoljnog saradnika, uz poštovanje pisanih procedura opisan u tačkama 4.1, 4.2, 4.3 ovog rada, realizaciju VPN-a. Na slici 10. prikazana je logička šema mrežnog okruženja pre realizacije zahteva [10].




Slika 31. Logička šema mrežnog okruženja pre realizacije VPN

### 5.6.1 Korak 1: Konfiguracija IP adresnog opsega

Komandna linija, koja definiše pul raspoloživih adresa, koji će automatski dostaviti parametre prilikom uspostavljanja daljinske sesije izgleda:

```
FW-BG(config)#ip local pool SS-POOL 10.0.50.1 – 10.0.50.254
```

Kako bi se adresa zaista i dodelila korisniku, potrebno je dostavi sledeća instrukciju:

```
FW-BG(config)#vpn-addr-assign local
```

### 5.6.2 Korak 2. Izuzimanje NAT-a nad kriptovanim saobraćajem

Prvo je potrebno kreirati odgovarajući ACL, kojom bi izvršili potrebnu filtraciju saobraćaja, iz lokalne mreže (10.0.1.0/24) prema korisniku daljinskog pristupa (10.0.50.0/24). Kasnije ćemo ime pristupne liste referencirati u konfiguraciji nat-a.

```
FW-BG(config)#access-list NAT0 extended permit ip 10.0.1.0 255.255.255.0 10.0.50.0 255.255.255.0
```

```
FW-BG(config)#nat(inside) 0 access-list NAT0
```

### 5.6.3 Korak 3: Kreiranje i konfigurisanje grupne polise

Grupna polisa omogućava separaciju daljinskog pristupa korisnika, sa različitim atributima. Polisa se predstavlja u formi određenog profila, sa predefinisanim karakteristikama u skladu sa zahtevom. Na primer: Administratoru sistema se može dati pravo VPN pristupa od 0-24h, dok je redovnom korisniku ograničen pristup u periodu od 08-17h. Grupna polisa dostavlja i druge mrežne parametre (DNS, filterovanje konekcije, trajanje praznog hoda, i dr.)

```
FW-BG(config)#group-policy ss-remoteuser internal
```

[14] Engl. IPSec VPN Client

```
FW-BG(config)#group-policy ss-remoteuser attributes
FW-BG(config)#vpn-idle-timeout 60
FW-BG(config)#dns-server value 10.0.1.3
FW-BG(config)#split-tunnel-policy tunnelspecified
```

### 5.6.4 Korak 4: Konfigurisanje parametara pristupa

U trenutku kreiranja VPN, od korisnika će se tražiti validni parametri pristupa, korisničko ime i lozinka. Korisničko ime i lozinka će se uneti u lokalnu bazu mrežnog uređaja pre prve autorizacije, kako bi se mogla izvršiti autentikacija korisnika.
Autentikacija korisnika se, u većini slučajeva, može centralizovati. Naime, najčešće primenjeni protokoli su RADIJUS i TACACS+. Pomenuti protokoli se koriste kao potreba za centralizacijom pristupa, usled limitirane mogućnosti mrežnih uređaja za pohranjivanje većeg broja zapisa i autentifikacionih parametara.

```
FW-BG(config)username davor password BiHH&beoD12$
```

### 5.6.5 Korak 5: Konfigurisanje IPSec FAZA 1 (IKEv1-Policy)

```
FW-BG(config)# crypto ikev1 policy 3
FW-BG(config-ikev1-policy)# encryption aes
FW-BG(config-ikev1-policy)# hash sha
FW-BG(config-ikev1-policy)# authentication pre-share
FW-BG(config-ikev1-policy)# group 2
FW-BG(config-ikev1-policy)# lifetime 36000
FW-BG(config-ikev1-policy)# exit
```

```
FW-BG (config)# crypto ikev1 enable outside
FW-BG (config)# crypto isakmp identity address
```

### 5.6.6 Korak 6: Konfigurisanje IPSec FAZA 2 (Parametrizacija)

U daljem toku parametrizacije potrebno je kreirati transformacioni set, tj. definisati skup protokola koji će izvršiti enkripciju i autentikaciju podataka u toku faze 2. Takođe, potrebno je konfigurisati dinamičku kripto mapu koja će dinamički dodeliti statičku kripto mapu.

*! Konfigurisanje transformacionog seta*

```
FW-BG (config)# crypto ipsec ikev1 transform-set TS-SS esp-3des esp-sha-hmac
```

*! Konfigurisanje dinamičke kripto mape*

```
FW-BG (config)# crypto dynamic-map DM 3 set ikev1 transform-set TS-SS
```

*! Pripajanje dinamičke kripto mape (DM) statičkoj (SM)*

```
FW-BG (config)# crypto map VM 30 ipsec-isakmp dynamic DM
FW-BG config)# crypto map VM interface outside
```

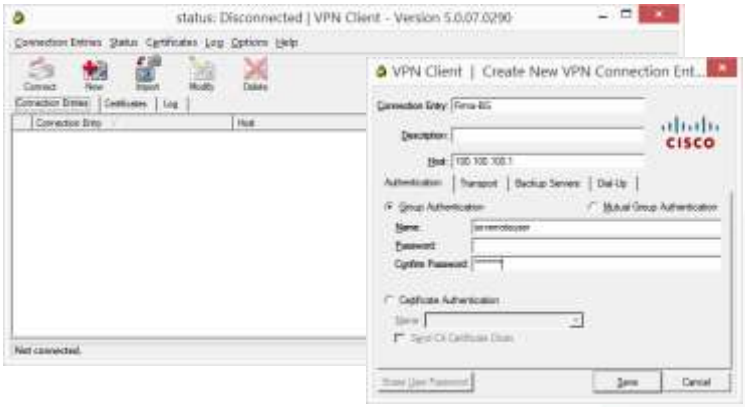
### 5.6.7 Korak 7: Kreiranje i konfigurisanje tunel grupe

Konfiguracija tunela grupe prestavlja srce pristupa VPN. Zadatak kreirane tunel grupe je da zajedno spaja: grupnu polisu, IP opseg deljenih adresa, pre-deljeni ključ i dr.

```
FW-BG (config)# tunnel-group ss-remoteuser type remote-access
FW-BG (config)# tunnel-group ss-remoteuser general-attributes
```

```
FW-BG (config-tunnel-general)# address-pool SS-POOL
FW-BG (config-tunnel-general)# default-group-policy ss-remoteuser
FW-BG (config)# tunnel-group ss-remoteuser ipsec-attributes
FW-BG (config-tunnel-ipsec)# ikev1 pre-shared-key So#asdhf245!$
```

### 5.6.8 Korak 8: Konfiguracija VPN klijenta




Slika 32. Grafički prikaz forme VPN profila/konekcionog priključka

Nakon instalacije VPN klijenta, startovanja aplikacije i pritiska na „New“ kreira se novi konekcioni profil/ulaz „Firma-BG.pcf“. U polju „Host“ se unosi javna IP adresa spoljnog interfejsa koncentratora - ASA. Takođe, u polje grupne autentikacije (ime i lozinka) upisuje se ime koje je vezano za tunel grupu i pre definisani ključ iz koraka 7.. U našem primeru, ime grupne autentikacije je „**ss-remoteuser“** i lozinka „**So#asdhf245!$“.** Nakon unosa neophodnih parametara snima se profil, potvrdom na polje „Save“.



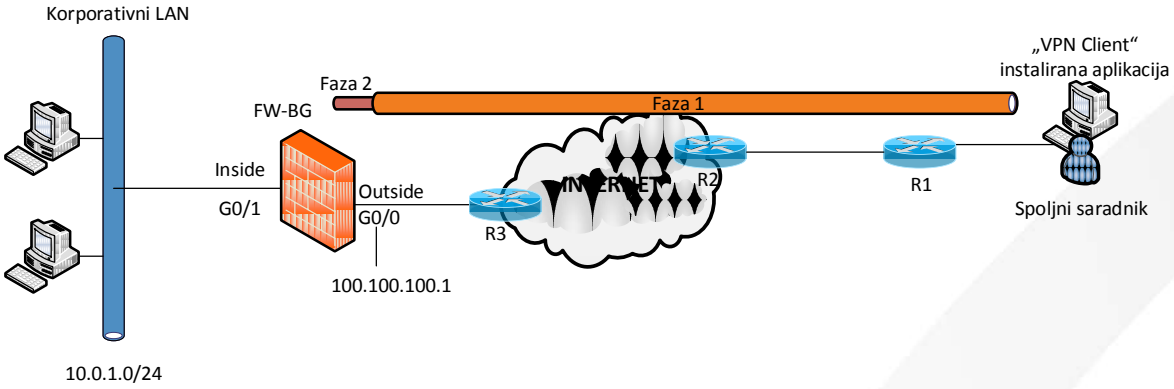

Slika 33. Grafički prikaz zahteva sa parametrima pristupa

Nakon snimanja konfiguracije, sesija je pokreće pozivom na „Connect“ dugme. Nakon uspešnog autorizovanja, sigurni VPN tunel je uspostavljen. Ako se iskoristi ipconfig /all komanda na računaru daljinskog korisnika, videćemo IP adresu iz opsega 10.0.50.0 /24 mreže, koja je dodeljena virtualnom konekcionom interfejsu.

### 5.6.9 Korak 9: Verifikacija uspostavljenog tunela zaštićenog saobraćaja

Sada je potrebno verifikovati konzistentnost linka, i to ćemo uraditi na sledeći način:

FW-BG#show crypto ipces sa




Slika 34. Logička šema mrežnog okruženja nakon realizacije VPN

# 6 Studijska praksa - Primenjena procedura prema ISO/IEC 27001 – ISMS

Standard ISO/IEC 27000 definiše postizanje željenog nivoa bezbednosti informacija kroz uspostavljanje, implementaciju, primenu, nadgledanje, reviziju, održavanje i unapređivanje Sistema za upravljanje bezbednošću informacija[15].
Sam proces uspostavljanja, implementacije, primene, nadgledanja, revizije, održavanja i unapređivanja Sistema za upravljanje bezbednošću informacija naziva se Proces upravljanja bezbednošću informacija [8].
Korišćene procedure prilikom realizacije zahteva za VPN pristup su:

1. Procedura regulisanja prava pristupa – opšta pravila;
2. Procedura regulisanja prava VPN pristupa;
3. Procedura administracije korisničkih naloga.

## 6.1 Procedura regulisanja prava pristupa – opšta pravila

### 6.1.1 Svrha dokumenta

Svrha ovog dokumenta je da opiše poslove regulisanja prava pristupa i korišćenja informacionog sistema. Pristup i korišćenje sistemskih i aplikativnih resursa informacionog sistema određeni su saglasno opisima radnih mesta korisnika i funkcijama koje obavljaju. U nastavku će biti definisane sve aktivnosti i procedure koje se tiču dodele i ukidanja prava pristupa svim delovima informacionog sistema.

### 6.1.2 Korišćeni termini

**Odeljenje IT** – Organizaciona jedinica koja obavlja poslove upravljanja, održavanja, razvoja i unapređenja informacionog sistema.
**Sistemski resursi** – Sva informatička oprema i sistemski softver neophodni za funkcionisanje informacionog sistema.
**Aplikativni resursi** – Sve aplikacije obuhvaćene informacionim sistemom.
**Spoljni saradnik** – Eksterni dobavljač računarske opreme i/ili usluga za potrebe informacionog sistema angažovan.
**Daljinski pristup** – Mogućnost pristupa i korišćenja digitalnih informacija sa lokacija koje su udaljene od mesta gde se podaci fizički nalaze.

[15] Eng. *Information Security Management System - ISMS*

**Incident** – Događaj na informacionom sistemu koji zahteva intervenciju zaposlenih.
**Sistemska sala** – Prostorija u kojoj je smeštena korisna informatička imovina (kao što su: serveri, mrežna oprema, oprema za čuvanje podataka, i tome sl.)

### 6.1.3 Skraćenice

- **IT** – Odeljenje IT;
- **DIT** – Direktor odeljenja IT:
- **ZIT** – Zaposleni u odeljenju IT:
- **DBA** – Zaposleni zadužen za administraciju baze podataka;
- **ZSI** – Zaposleni zadužen za infrastrukturu;
- **ZAIT** – Zaposleni zadužen za administraciju aplikacija i servisa u odeljenju IT;
- **KKIT** – Krajnji korisnik servisa koje pruža odeljenje IT;
- **PZ** – Podnosilac zahteva;
- **SS** – Spoljni saradnik.

### 6.1.4 Opšte informacije

Pristup informacionom sistemu definisan je sledećim kriterijumima:

1. Podnosilac zahteva za pristup;
2. Način pristupa;
3. Tip pristupa;
4. Dužina trajanja pristupa;
5. Prioritet pristupa;
6. Nadležna osoba za realizaciju.

#### 6.1.4.1 Podnosilac zahteva za pristup

U opštem slučaju, podnosilac zahteva može biti:

- Zaposleni u IT;
- Spoljni saradnik SS;
- Korisnik aplikacija i servisa;

U zavisnosti od načina pristupa, razlikuje se spisak osoba koja mogu zahtevati pristup sistemu.

#### 6.1.4.2 Način pristupa

Shodno različitim načinima na koji se može pristupiti delovima informacionog sistema, razlikujemo više nivoa pristupa:

- Pristup sistemskim resursima
  - **Pristup uređajima**:
    - Fizički – pristup fizičkim lokacijama u kojima se nalaze sistemski resursi (sistemske sale);
    - Mrežni – pristup uređajima koristeći tehnike daljinskog pristupa (Kao što su: RDC[16], Telnet, SSH[17], FTP, VPN, itd.).
  - **Pristup sistemskom softveru**:
    - Pristup operativnom sistemu
    - Pristup bazi podataka

  Pristup svim sistemskim resursima mogu zahtevati SS i zaposleni u IT u cilju redovne kontrole i održavanja informatičke opreme i/ili u slučaju incidenta;

[16] Engl. Remote Desktop Connection
[17] Engl. Secure Shell

- Pristup aplikacijama – Pristup aplikativnim resursima mogu zahtevati administratori korisnika aplikacije, u ulozi među korisnika veb aplikacije i servisa u cilju pružanja podrške krajnjim korisnicima informacionog sistema.

Svaki od navedenih načina pristupa informacionom sistemu detaljno je regulisan posebnom procedurom i to:

- Fizički pristup – „Procedura regulisanja prava pristupa sistemskim salama“;
- Mrežni pristup – „Procedura regulisanja prava VPN pristup“;
- Pristup operativnom sistemu – „Procedura regulisanja prava pristupa operativnom sistemu“;
- Pristup bazi podataka – „Procedura regulisanja prava pristupa bazi podatak“;
- Pristup aplikacijama – „Procedura regulisanja prava pristupa aplikacijama“.

#### 6.1.4.3 Tip pristupa

Shodno ovlašćenjima koja se dodeljuju podnosiocu zahteva, razlikujemo dva tipa pristupa:

- **Administratorski pristup** – Dodeljivanje administratorskih ovlašćenja;
- **Korisnički pristup** – Dodeljivanje korisničkih ovlašćenja.

#### 6.1.4.4 Dužina trajanja pristupa

- **Stalni pristup** – Pristup u bilo kom trenutku i u neograničenom vremenskom trajanju;
- **Privremeni pristup** - Pristup u ograničenom vremenskom trajanju.

#### 6.1.4.5 Prioritet pristupa

Shodno urgentnosti, prioritet pristupa može biti:

- **Visok** – Primalac zahteva za pristup je u obavezi da obavesti podnosioca o realizaciji/odbijanju zahteva u roku od dva (2) sata od trenutka prijema zahteva;
- **Srednji** - Primalac zahteva za pristup je u obavezi da obavesti podnosioca o realizaciji/odbijanju zahteva u roku od dva (2) dana od trenutka prijema zahteva;
- **Nizak** - Primalac zahteva za pristup je u obavezi da obavesti podnosioca o realizaciji/odbijanju zahteva u roku od sedam (7) dana od trenutka prijema zahteva.

#### 6.1.4.6 Nadležne osobe za realizaciju

Poslove realizacije zahteva obavljaju saradnici u IT. Shodno opisu radnih mesta i funkciji koju obavljaju, razlikujemo sledeće nadležnosti saradnika u IT:

1. **ZAIT** – regulisanje prava pristupa aplikacijama;
2. **DBA** – regulisanje prava pristupa bazi podataka;
3. **ZSI** – regulisanje prava pristupa na fizičkom, mrežnom i nivou operativnog sistema.

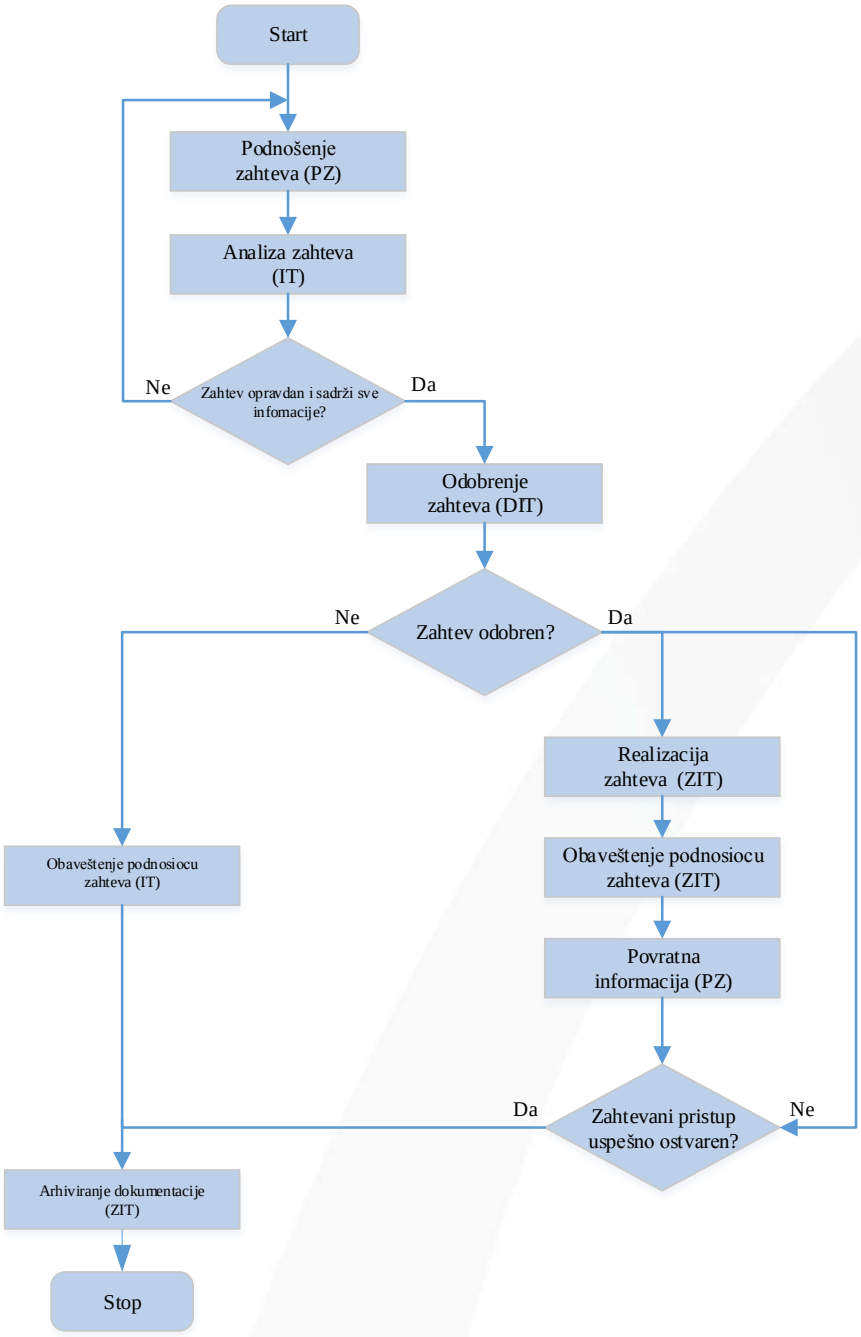
### 6.1.5 PROCEDURA

Proces dodele prava pristupa informacionom sistemu sastoji se iz sledećih aktivnosti:

| Br. | Aktivnost | Opis | Ko |
|---|---|---|---|
| 1. | Podnošenje zahteva | Podnosilac zahteva za pristup popunjava odgovarajući obrazac zahteva (nalazi se u prilogu svake od procedura) sa svim neophodnim | PZ |

| | | | |
|---|---|---|---|
| | | informacijama. Popunjen zahtev se dostavlja putem e-mail-a. Preporuka je da se u zahtevu specificira osoba za koju se smatra da je nadležna za realizaciju. U slučaju da je prioritet zahteva visok, podnošenje se može izvršiti i usmeno, odnosno telefonskim putem na određeni broj telefona. Nakon telefonskog podnošenja zahteva, podnosilac je u obavezi da u najkraćem roku zahtev dostavi i u formi obrasca. | |
| 2. | Analiza zahteva | Po prijemu zahteva, saradnici u IT razmatraju specifikacije zahteva i shodno načinu pristupa određuju osobe odgovorne za dalju analizu i realizaciju. Saradnici u IT vrše procenu opravdanosti i tehničke izvodljivosti zahteva, daju svoje mišljenje i zahtev prosleđuju ručno ili putem e-mail-a DIT na odobrenje. U slučaju nepotpune specifikacije zahteva ili neosnovanosti zahteva, saradnici u IT vraćaju zahtev podnosiocu uz odgovarajuće obrazloženje. Napomena: Saradnici u IT obavljaju delatnosti iz gore opisanih nadležnosti. | IT |
| 3. | Odobrenje zahteva | DIT sagledava kompletnu specifikaciju zahteva, razmatra mišljenje saradnika u IT i donosi odluku o realizaciji ili odbijanju zahteva. | DIT |
| 4. | Realizacija zahteva | Saradnici u IT realizuju zahtev po utvrđenoj proceduri, svako iz svoje nadležnosti, a u skladu sa odlukom DIT. | ZIT |
| 5. | Obaveštavanje podnosioca zahteva | Saradnik u IT obaveštava podnosioca zahteva o realizaciji zahteva i prosleđuje mu sve neophodne informacije za pristup (npr. korisničko ime, lozinka i sl.) na način detaljno opisan u odgovarajućoj proceduri, tj. diversifikovanjem mogućeg rizika, dostavljanje informacija za pristup preko najmanje dva kanala komunikacije (SMS i e-mail) . | ZIT |
| 6. | Povratna informacija | Podnosilac zahteva izveštava saradnika u odeljenju IT o uspešno/neuspešno ostvarenom pristupu. U slučaju neuspeha, saradnik u odeljenju IT pristupa novoj realizaciji zahteva, dok se u slučaju uspeha prelazi na arhiviranje dokumentacije. | PZ |
| 7. | Arhiviranje dokumentacije | Obrazac zahteva i sva prateća dokumentacija se odlaže u odgovarajući registrator zahteva koji se čuva u prostorijama odeljenja IT. | ZIT |

Tabela 9. Prikazan je opšti dijagram toka procesa realizacije zahteva za pristup.




Slika 35. Primenjeni algoritam prilikom realizacije zahteva za pristup

## 6.2 Procedura regulisanja prava VPN pristupa

### 6.2.1 Svrha

Svrha ove procedure je da opiše postupak kreiranja, korišćenja i ukidanja VPN naloga za pristup sistemu.

### 6.2.2 Korišćeni termini

**VPN** – Privatna komunikaciona mreža koja se koristi za sigurnu komunikaciju.
**VPN klijent** – Program za uspostavljanje VPN konekcije.

### 6.2.3 Skraćenice

- **DBA** – Zaposleni zadužen za administraciju baze podataka;
- **ZSI** – Zaposleni zadužen za infrastrukturu;
- **ZAIT** – Zaposleni zadužen za administraciju aplikacija i servisa u odeljenju IT;
- **KVPM** – Korisnik virtualne privatne mreže;
- **PZ** – Podnosilac zahteva;
- **SS** – Spoljni saradnik.
- **SIT** – Saradnik u IT

### 6.2.4 Opšte informacije

Virtuelna privatna mreža omogućava bezbedan pristup sistemu sa udaljenih mreža i lokacija putem interneta.

#### 6.2.4.1 Opšte karakteristike VPN pristupa sistemu

- VPN pristup predstavlja servis za ostvarenje sigurnog pristupa sistemsko/aplikativnim resursima;
- Obezbeđuje centralizovano praćenje i kontrolu pristupa;
- Omogućava proceduralno kreiranje/ukidanje i personalizaciju pristupa.

#### 6.2.4.2 Pravila upotrebe i ograničenja VPN pristupa

- U opštem slučaju, podnosilac zahteva za VPN korisnički nalog može biti:
  - Zaposleni u firmi;
  - Spoljni saradnik sa kojim postoji ugovorni odnos;
  - Korisnik aplikacija i servisa (korisnici usluga i njihovi ovlašćeni predstavnici).
- VPN korisničke naloge odobrava DIT;
- VPN korisničke naloge kreira ZSI;
- Stalni VPN pristup može se odobriti jedino zaposlenima u IT;
- Evidencija lica sa odobrenim stalnim pristupom vodi se u **prilogu 2** i čuva se u papirnoj formi u prostorijama IT;
- Evidencija lica sa odobrenim privremenim pristupom vodi se u **prilogu 3** i čuva se u papirnoj formi u prostorijama IT;
- Prilikom kreiranja VPN korisničkih naloga moraju se poštovati pravila iz procedure „Procedura administracije korisničkih naloga“;
- Dodeljivanje VPN pristupa po hitnom postupku u slučaju vanrednih situacija, moguće je u periodu od 00:00 – 24:00 na osnovu usmenog odobrenja od strane DIT, a u skladu sa procedurom „Procedura postupanja u slučaju problema u radu“;
- Praćenje i kontrola VPN pristupa vrši se na dnevnom nivou od strane ZSI evidentiranjem u tabeli iz **priloga 4**. ZSI je u obavezi da ažurnu evidenciju za prethodni dan, svakodnevno dostavlja DIT;
- KVPM ostvaruje VPN pristup upotrebom VPN klijenta instaliranog na svojoj radnoj stanici uz korišćenje dodeljenog korisničkog naloga.
- Podaci o VPN nalogu koji su prosleđeni KVPM su personalizovani i KVPM je odgovoran za svaku vrstu zloupotrebe naloga;
- KVPM je dužan da ima instaliran antivirusni program sa ažurnim antivirusnim definicijama na radnoj stanici sa koje ostvaruje pristup;
- VPN sesija se automatski prekida u slučaju neaktivnosti duže od trideset (25) minuta.

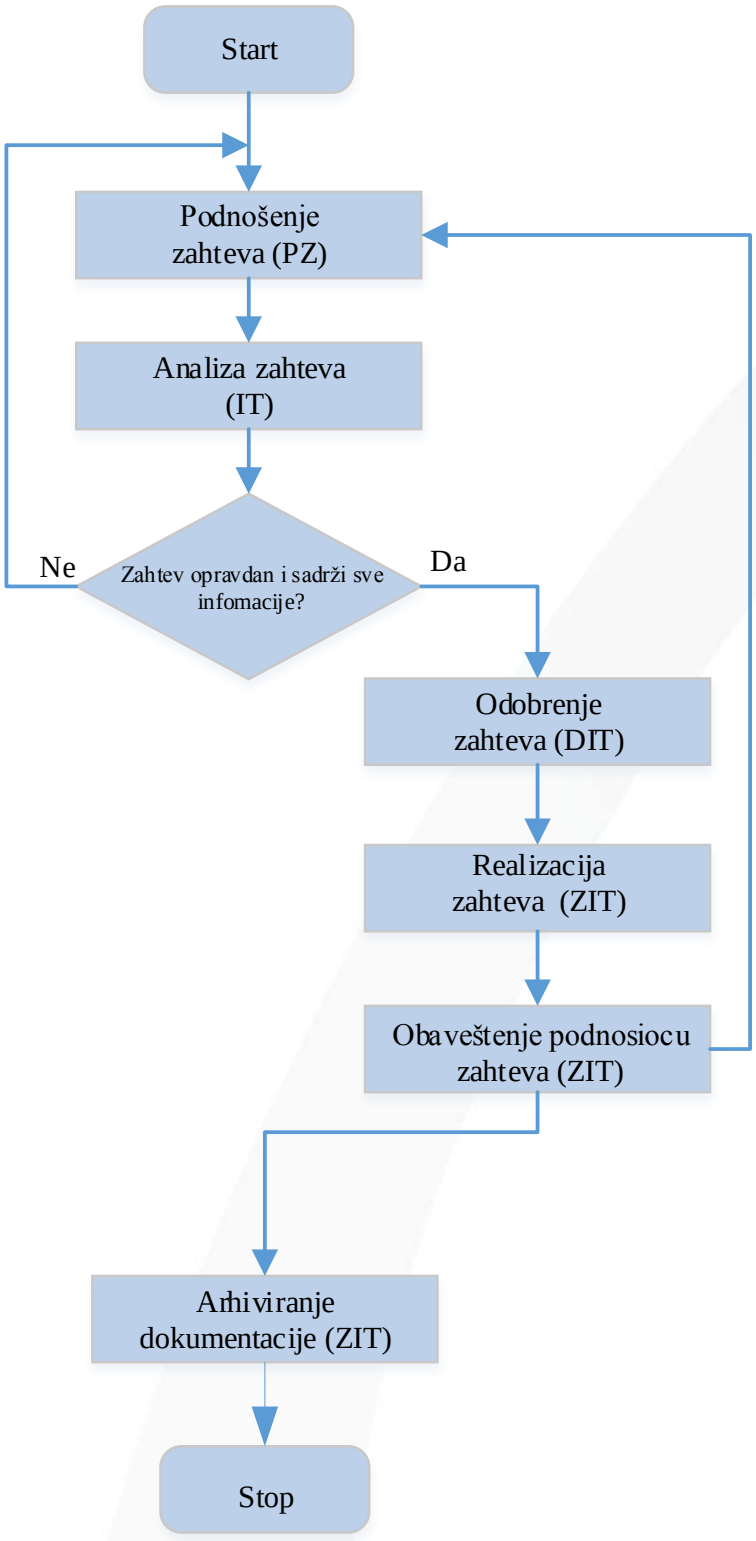
- Ukidanje VPN korisničkog naloga vrši ZSI, a na osnovu sumnje o zloupotrebi ili posedovanja parametara za pristup od strane neautorizovanog lica.

6.2.5 PROCEDURA

6.2.6 Aktivnosti prilikom kreiranja VPN korisničkih naloga

| Br. | Aktivnost | Opis | Ko |
|---|---|---|---|
| 1. | Podnošenje zahteva | PZ od IT traži VPN pristup popunjavajući obrazac iz **priloga 1** i dostavlja ga u skladu sa opštim pravilima podnošenja zahteva definisanih procedurom „Procedura regulisanja prava pristupa“ | PZ |
| 2. | Analiza zahteva | Po prispeću zahteva, SIT analizira potrebu za VPN pristupom, specificiranu u zahtevu, i shodno tome zahtev prosleđuje nadležnom SIT na tehničku analizu. U slučaju nepotpune specifikacije ili neosnovanosti zahteva, SIT vraća zahtev PZ uz odgovarajuće obrazloženje. Nadležni SIT (ZSI, DBA i/ili ZAIT) analizira opravdanost i tehničku izvodljivost zahteva i daje svoju saglasnost potpisujući obrazac zahteva. Saglasnost nivoa I moraju dati ZSI, DBA i/ili ZAIT, dok saglasnost nivoa II daje jedino ZSI.<br>Nakon dobijenih saglasnosti nivoa I i II zahtev se prosleđuje u papirnoj formi DIT na odobrenje. | SIT (ZSI, DBA, ZAIT) |
| 3. | Odobrenje zahteva | DIT daje saglasnost nivoa III. DIT odlučuje o odobrenju zahteva imajući u vidu mišljenja nadležnih SIT. DIT mora da odobri i potpiše obrazac pre nego što SSI krene u realizaciju. | DIT |
| 4. | Realizacija zahteva | Nakon odobrenja, ZSI kreira korisnički nalog sa specificiranim pravima u skladu sa pravilima iz procedure „Procedura administracije korisničkih naloga“. | ZSI |
| 5. | Obaveštavanje podnosioca zahteva | SIT obaveštava PZ o realizaciji zahteva i prosleđuje mu sve neophodne informacije za pristup (npr. korisničko ime, lozinka i sl.) poštujući pravila diversifikacije sigurnosnih rizika slanjem ključnih reči koristeći najmanje dve vrste medijuma za transport informacija (npr. korisničko ime se šalje putem e-mail-a, a korisnička lozinka SMS-om na unapred dogovoreni mobilni broj). | SIT |
| 6. | Arhiviranje | Nakon realizacije zahteva, SIT odlaže svu prateću dokumentaciju u registrator promena i realizacije VPN korisničkih zahteva koji se čuva u prostorijama IT. | SIT |

Tabela 10. Prikazan je opšti dijagram toka procesa realizacije zahteva za pristup




Slika 36. Primenjeni algoritam prilikom realizacije zahteva za pristup

### 6.2.7 PRILOZI

#### 6.2.7.1 Prilog 1 – Zahtev za VPN pristup

*Popunjava PZ*

| | | | | |
|---|---|---|---|---|
| Datum zahteva | | | | |
| Podnosilac zahteva | | Eksterni (ime i prezime) _____ | e-mail | |
| | | | telefon | |
| | | | faks | |
| | | | br. l.k. | |
| | | Interni – (Ime i prezime) _____ | | |
| Odredište (server, servis, aplikacija i sl.) | | | | |
| Nivo pristupa | | Windows/Domain | | |
| | | MSSQL | | |
| Detalji mrežnog pristupa | | TCP 1433 (SQL) | | |
| | | ICMP (PING) | | |
| | | All TCP | | |
| | | All IP | | |
| | | Navesti (_____) | | |
| Tip pristupa | | Administrator | | |
| | | Korisnik | | |
| Trajanje VPN pristupa | | Stalni | | |
| | | Privremeni | | 1 dan |
| | | | | 7 dana |
| | | | | 30 dana |
| | | | | Navesti (_____) |
| Prioritet VPN pristupa | | Visok | | |
| | | Srednji | | |
| | | Nizak | | |
| Razlog za pristup | | | | |

*Popunjava IT*

| Saglasnost<br>Nivo I | Saglasnost<br>Nivo II | Saglasnost<br>Nivo III |
|---|---|---|
| _____ | _____ | _____ |

### 6.2.7.2 Prilog 2 – Evidencija lica sa odobrenim stalnim VPN pristupom

| Br. | Ime i prezime | Korisničko ime | Radno mesto/ Kompanija | Telefon (stabilni) | Telefon (mobilni) | E-mail | Odobrio |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

### 6.2.7.3 Prilog 3 – Evidencija lica sa odobrenim privremenim VPN pristupom

| Br. | Ime i prezime | Korisničko ime | Trajanje pristupa od/do | Radno mesto/ Kompanija | Telefon (stabilni) | Telefon (mobilni) | E-mail | Odobrio |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

## 6.3 Procedura administracije korisničkih naloga

### 6.3.1 Svrha

Svrha ove procedure je da uspostavi pravila kreiranja, upotrebe i čuvanja korisničkih imena i lozinki u okviru.

### 6.3.2 Opšte informacije

#### 6.3.2.1 Definicija korisničkih naloga

- Aplikativni nalog – nalog za pristup aplikacijama;
- Sistemski nalog – nalog za pristup sistemskom softveru. U zavisnosti od sistema razlikujemo:
    - Nalog na serverskom operativnom sistemu i to:
        - Predefinisani (Built-in) nalog – ugrađeni nalog neograničenih privilegija (npr. „Administrator“ – Microsoft Windows OS i dr.);
        - Administratorski nalog – definisani korisnički nalog sa dodeljenim neograničenim ili ograničenim privilegijama;
        - Servisni nalog – definisani korisnički nalog namenjen za pokretanje sistemskih servisa (npr. nalog za pokretanje SQL Server-a i dr.);
        - Korisnički nalog za pristup – definisani korisnički nalog ograničenih privilegija.
    - Nalog na bazi podataka i to:
        - Predefinisani (Built-in) nalog – ugrađeni nalog neograničenih privilegija (npr. „sa“ (Login) – Microsoft SQL Server i sl.);
        - Administratorski nalog – definisani korisnički nalog sa dodeljenim ograničenim ili neograničenim privilegijama;
        - Korisnički nalog za pristup – definisani korisnički nalog ograničenih privilegija.
    - Nalog na mrežnoj opremi i to:
        - Predefinisani (Built-in) nalog – ugrađeni nalog neograničenih privilegija (npr. „root“ – iOS i dr.);
        - Korisnički nalog za pristup – definisani korisnički nalog ograničenih privilegija.

#### 6.3.2.2 Administracija aplikativnih korisničkih naloga

- Aplikativni korisnički nalozi se koriste za pristup aplikacijama i servisa;
- Aplikativni korisnički nalozi se među sobom razlikuju prema dodeljenim ovlašćenjima/ulogama;
- Aplikativne korisničke naloge mogu posedovati SIT i KKIT;
- Aplikativne korisničke naloge kreiraju i ukidaju ZAIT i KKIT u skladu sa procedurom „Procedura regulisanja prava pristupa“.
- ZAIT je nadležan za kreiranje prvog (ukidanje poslednjeg) korisničkog naloga KKIT, dok je KKIT nadležan za dalje administriranje (kreiranje, modifikaciju i ukidanje) naloga unutar svog korisnika.

#### 6.3.2.3 Administriranje sistemskih korisničkih naloga

- Sistemski korisnički nalozi se koriste za pristup sistemskom softveru i uređajima (npr. serverski operativni sistem, baza podataka, mrežna oprema i sl.);
- Sistemske korisničke naloge mogu posedovati ZIT i SS po potrebi;
- Sistemske korisničke naloge kreiraju ZIT shodno nadležnostima svojih radnih mesta i to:

    - ZSI kreira naloge na operativnim sistemima i mrežnoj opremi.
    - DBA kreira naloge na bazi podataka.
- Nalozi se kreiraju na načine opisane u tački n. i u skladu sa procedurom „Procedura regulisanja prava pristupa“;
- Predefinisani (Built-in) nalozi se koriste u vanrednim situacijama (npr. požar, poplava, zemljotres, i sl.) i u slučaju odsustva odgovornih osoba sa odgovarajućim administratorskim nalozima;
- Predefinisani (Built-in) nalozi se čuvaju kovertirani u sefu u prostorijama IT.
- Pravo pristupa predefinisanim (Built-in) nalozima imaju DIT, i/ili ZIT samo u vanrednim situacijama;
- Administratorske naloge na serverskim operativnim sistemima poseduju ZSI i DBA.
- Administratorske naloge na bazama podataka poseduju ZSI i DBA.
- Administratorske naloge na mrežnoj opremi poseduje ZSI.
- Ukidanje korisničkih naloga vrše ZSI i DBA, svako iz svoje nadležnosti, a u skladu sa procedurom „Procedura regulisanja prava pristupa“.

6.3.2.4 Opšta pravila upotrebe i čuvanja korisničkih naloga

- Korisnički nalog je personalizovani podatak i kao takav se dodeljuje svakom korisniku koji je odgovoran za njegovo korišćenje;
- Jedan korisnički nalog se dodeljuje samo jednom korisniku. Svaka zloupotreba naloga u bilo kom smislu će se smatrati prekršajem korisnika kome je dodeljen;
- Nakon otvaranja korisničkog naloga, odnosno prijema nove lozinke, korisnik je u obavezi da istu promeni prilikom prvog korišćenja. Tamo gde tehničke mogućnosti dozvoljavaju ova akcija će automatski biti zahtevana od strane korisnika;
- Servisni nalozi se ne smeju koristiti u svrhe prijavljivanja na sistem;
- Servisni nalozi ne podležu pravilima izmene lozinke iz tačke n;
- Više puta pogrešno uneta lozinka korisničkog naloga na nekim sistemima može izazvati automatsko zaključavanje naloga. Otključavanje naloga vrši ZIT nakon dobijanja pisanog zahteva od strane korisnika sa obrazloženjem;
- Ukidanje korisničkih naloga predstavlja čin privremenog ili trajnog ukidanja naloga za pristup;
- Ukidanje naloga može biti izazvano istekom perioda njegovog važenja, na zahtev korisnika ili odlukom DIT. Tamo gde to tehničke mogućnosti dozvoljavaju, ukidanje se vrši automatski, dok se u ostalim slučajevima vrši ručno od strane ZIT.

6.3.2.5 Opšta pravila kreiranja, upotrebe i čuvanja korisničkih imena i lozinki

- Lozinka mora biti kreirana u skladu sa sledećim pravilima:
    - Lozinke moraju ispuniti zahtev kompleksnosti. Moraju da se sastoje od kombinacije slova, simbola i brojeva (npr. Aa,!@#$*,123 i dr.);
    - Lozinka mora biti sačinjena od tri (4) vrste karaktera;
    - Lozinka mora da se sastoji od najmanje osam (12) karaktera;
- Istorija lozinki je definisana na poslednjih (6) unetih lozinki (password history). Tamo gde to sistem omogućava ovo ograničenje je automatski postavljeno;
- Lozinku treba menjati na svakih (30) dana. Tamo gde to sistem omogućava promena se od korisnika može zahtevati automatski;
- Lozinka ne sme da sadrži korisničko ime ili ime nekog od članova porodice, datume rođenja i dr;
- Lozinka ne sme da sadrži broj lične karte, registracioni broj automobila i broja mobilnog telefona;
- Lozinka ne sme da sadrži reč „password“ u bilo kojoj kombinaciji znakova (npr. %p@ssw0rd!Ass! i sl.).
- Dostavljanje korisničkog imena i lozinke treba vršiti korišćenjem različitih medijuma za transport informacija (npr. korisničko ime se šalje e-mail-om, a lozinka SMS-om i sl.). Takođe, ne preporučuje se spominjanje lozinke u razgovoru ili komunikaciji bilo koje vrste.

- Ukoliko korisnik posumnja u kompromitovanost postojeće lozinke, u obavezi je da istu odmah promeni i o tome obavesti ZIT.
- Korisnik mora da onemogući treće lice da dođe u posed lozinke (ne preporučuje se npr. zapisivanje na papirićima, na kompjuteru, čuvanje ispod tastature ili u fijokama radnog stola, i dr.)

## *ZAKLJUČAK*

Prvi deo rada opisuje metode, tehnologije i standarde primenjene u kontekstu povećanja pouzdanosti i bezbednosti podataka. Donošenje odluka o tome da li kriptografsko rešenje odgovara treba posmatrati kao deo šireg postupka ocenjivanja rizika i odabiranja bezbednosnih kontrola. Ovo ocenjivanje se potom može koristiti da bi se utvrdilo da li kriptografska kontrola odgovara, koji tip kontrole treba primeniti za koje svrhe i na koje poslovne procese. Politika korišćenja kriptografskih kontrola je neophodna da bi se ostvarila maksimalna korist i da bi se na minimum smanjili rizici od primene kriptografskih postupaka, kao i da bi se izbeglo neodgovarajuće ili nepravilno korišćenje. Pri upotrebi digitalnog potpisa treba uzeti u obzir zakonske i druge propise.

Kriptovanje informacija se koristi kada se želi postići poverljivost verodostojnost i neporecivost podataka u prenosu između dve i više instanci. Nakon dostavljanja zvaničnog zahteva, analize, realizacije do arhiviranja overene potvrde, koja potvrđuje doslednost u koracima definisanih pisanih procedura, pokazuje na nedvosmislenost u primeni politika bezbednosti informacija i poštovanja međunarodnog standarda ISO/IEC 27001.

Standard ISO/IEC 27000 jasno prikazuje smernice za dostizanje neophodnog nivoa bezbednosti podataka i informacija preko uspostavljanja, implementacije, primene, nadogradnje, neophodnih revizija, dodatnog unapređenja sistema za bezbednost informacija. Proces upravljanja bezbednosti informacija ima za cilj identifikaciju bezbednosnih zahteva i održi informacioni sistem na odgovarajućem nivou bezbednosti.

Imajući u vidu rasprostranjenost i upotrebu računara i mobilnih uređaja, kao i ogromne količine informacija, neophodnost poštovanja jasno definisanih pravila predstavlja esenciju informatičke pismenosti. Propisani zakoni i standardi usmeravaju društvo u pravcu povećanja bezbednosti informacija, kao i aktivno i proaktivno delovanje kroz forenzičke analize potencijalnih pretnji i incidenata uz dosledno sankcionisanje prevara i zloupotreba.

Prikazana studija slučaja pokazuje primer doslednosti u poštovanju i primeni pravila i preporuka iz pisanog/ih standarda. Pravila i preporuke su pretočene u politiku bezbednosti a dalje u procedure određenog segmenta delovanja. Proaktivno i aktivno delovanje u mnogome obezbeđuje održavanje permanentnog kontinuiranog poslovanja u okviru radne organizacije i dalje.

Predstavljeni forenzički alati čine samo segment celokupne slike o praćenju ili monitorisanju sistema u celini. Ništa manje važnu ulogu u održavanju kontinuiteta poslovanja čine alati za čuvanje rezervnih kopija sistema i baza, kroz fizičko i aplikativno instanciranje i segmentaciju infrastrukture. Takođe, sajtiranje na primarnu i rezervnu (redundantnu) lokacija, koje se mogu aplikovati kroz statuse (active-passive, active-active) dopunjuje sliku o tzv. pouzdanoj i dostupnog infrastrukturi.

U čitavom procesu ne smemo zapostaviti aktivnu podršku rukovodstva, uz pomoć jasnih smernica, pokazivanja posvećenosti i zainteresovanosti, implicitnim i eksplicitnim dodeljivanjem zaduženja uz priznanje odgovornosti vezanih za bezbednost informacija.

***LITERATURA***


[1] Kriptologija I, Mladen Veinovići i Saša Adamović, Beograd 2013.
[2] Kriptologija II, Milan Milosavljević i Saša Adamović, Beograd 2014.
[3] Informatika, Milan Milosavljević i Mladen Veinović i Gojko Grubor, Beograd 2013.
[4] CBT Nuggets, CCNP Security VPN v2.0 642-648, www.cbtnuggets.com/*
[5] CCNP Routing and Swathing SWITCH 300-115, Office Cert Guide, Kevin Wallace
[6] TACACS+ and RADIUS Comparison, http://www.cisco.com/*
[7] Description of Symmetric and Asymmetric Encryption, Microsoft Support
[8] ISO/IEC 27001 ISMS, Izvor: http://www.iso.org/iso/iso27001
[9] Milosavljević M., Grubor G., *Digitalna forenzika*, Univerzitet Singidunum, Beograd, 2008
[10] IPSec, *RFC4301*, Izvor: https://tools.ietf.org/html/rfc4301
[11] *InternetKeyExchangeProtocolVersion2*,*RFC7296*,Izvor: https://tools.ietf.org/html/rfc7296
[12] Milosavljević M., Grubor G., *Istraga kompjuterskog kriminala - metodološko tehnološke osnove*, Univerzitet Singidunum 2009
[13] Internet Key Exchange, *RFC2409*, https://tools.ietf.org/html/rfc2409
[14] Milosavljević M, Grubor G, *Digitalna Forenzika Računarskog Sistema*, Univerzitet Singidunum Beograd 2009
[15] *EnCase®ComputerForensics*,Izvor: http://www.bk.psu.edu/faculty/bowers/ist454/eBook.pdf
[16] VPN RFC4026, https://tools.ietf.org/html/rfc4026
[17] Milanović Z., Milanović T., *Digitalna anti-forenzika kao kriminogeno sredstvo zaštite kiber kriminala*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije IT veštak, 2010.
[18] ManageEngine ServiceDeskPlus 8 Help AdminGuide, Izvor: https://download.manageengine.com/products/service-desk/help/ManageEngine_ServiceDeskPlus_8_Help_AdminGuide.pdf
[19] PRTG, Izvor: https://download.manageengine.com/products/service-desk/help/ManageEngine_ServiceDeskPlus_8_Help_AdminGuide.pdf
[20] Vanja M. Korać, *Digitalna forenzika u funkciji zaštite informacionog sistema baziranog na linux i windows platformama*, doktorska disertacija, Centar za multidisciplinarne studije Univerziteta u Beogradu, Beograd 2014.
[21] Gartner,Izvor: https://www.gartner.com/doc/3035319?ref=SiteSearch&sthkw=firewall%20magic%20quadrant&fnl=search&srcId=1-3478922254
https://download.manageengine.com/products/service-desk/help/ManageEngine_ServiceDeskPlus_8_Help_AdminGuide.pdf
[22] PRTG,

https://download.manageengine.com/products/service-desk/help/ManageEngine_ServiceDeskPlus_8_Help_AdminGuide.pdf

[23] IPSec, *RFC4120*, Izvor: https://www.ietf.org/rfc/rfc4120.txt