IMPLEMENTACIJA SYSLOG WATCHER PROGRAMSKE PODRŠKE ZA PRIKUPLJANJE, POHRANU I ANALIZU SYSLOG PORUKA

Grubić, Roko

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Preddiplomski stručni studij Informacijska tehnologija

ROKO GRUBIĆ

Z A V R Š N I R A D

IMPLEMENTACIJA SYSLOG WATCHER PROGRAMSKE PODRŠKE ZA PRIKUPLJANJE, POHRANU I ANALIZU SYSLOG PORUKA

Split, rujan 2019.

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Preddiplomski stručni studij Informacijska tehnologija

Predmet: Projektiranje i upravljanje računalnim mrežama

Z A V R Š N I R A D

Kandidat: Roko Grubić

Naslov rada: Implementacija Syslog Watcher programske podrške za prikupljanje, pohranu i analizu syslog poruka

Mentor: mr. sc. Tatjana Listeš, viši predavač

Split, rujan 2019.

Sadržaj

SAŽETAK

Implementacija Syslog Watcher paketa za prikupljanje, pohranu i analizu syslog poruka

Cilj ovog završnog rada je implementacija *Syslog Watcher* paketa za prikupljanje, pohranu i analizu *syslog* poruka. U prvom dijelu rada opisane su syslog poruke i načini njihovog prijenosa te popis svih tehnologija potrebnih za izradu navedenog sustava. Nakon toga je opisan način implementacije potrebnih tehnologija kao i napravljenih podešavanja kako bi radili u skladu s očekivanjima.

Za prikazanu implementaciju sustava bio je potreban *Syslog Watcher* paket tvrtke "EZ5 Systems Ltd." koji prikuplja syslog poruke, *VMware Workstation Player* koji virtualizira više operativnih sustava koji su potrebni za izradu završnog rada (u pitanju su operativni sustavi Windows), GNS3 (engl. *Graphical Network Simulator 3*) mrežni simulator kojim je i simulirana mreža iz stvarnog života te Microsoft SQL (engl. *Stuctured Query Language*) server baza podataka u koju su pohranjivane syslog poruke.

Implementacijom Syslog Watcher paketa omogućeno je lakše nadgledanje i analiza mreže mrežnom administratoru ili sistem inženjeru koji je zadužen za održavanje sigurnosti mreže.

Ključne riječi: GNS3, Microsoft SQL Server baza podataka, operativni sustav Windows, Syslog Watcher, VMware Workstation Player

SUMMARY

Implementation of Syslog Watcher Packet for gathering, storing and analyzing syslog messages

The main goal of this final paper is the implementation of Syslog Watcher Packet for gathering, storing and analyzing syslog messages. Firstly, syslog messages and methods of their transport are explained and a list of all technologies needed for making mentioned system has been given. After that, methods of implementation required technologies and their settings after which they work in line with expectations has been described.

For presented system implementation Syslog Watcher packet by company named "EZ5 Systems Ltd." for gathering syslog messages was required, VMware Workstation Player for virtualization of operating systems which are needed for completing this final paper (in this case, there are Windows operating systems), GNS3 network simulator with which network, like those in real life, is simulated and Microsoft SQL Server database for storing syslog messages.

When finished, implementation of Syslog Watcher packet enables easier supervising and analyzing for network administrator or system engineer who is responsible for keeping network safe.

Keywords: GNS3, Microsoft SQL database, Syslog Watcher, VMware Workstation Player, Windows operating system

1 UVOD

Danas društvo živi u dobu sve većeg razvoja računala i gotovo je nemoguće zamisliti moderni svijet bez računala. Od samih početaka razvoja računala, ljude je zanimalo na koji ih način povezati u mrežu preko koje se može međusobno komunicirati i razmjenjivati podatke. Britanac Tim Berners Lee je 1989. godine u CERN-u (kratica za *Conseil européen pour la recherche nucléaire*) razvio servis *World Wide Web*, odnosno današnji moderni internet. Od tog trenutka započelo je potpuno novo poglavlje u razvoju računala, a ljudi su mogli biti povezani kao nikad prije. Samim razvojem interneta razvile su se i mreže računala koje su povezane na internet i preko njega komuniciraju.

Za komunikaciju preko mreže računala koriste skup TCP/IP protokola. TCP (engl. *Transmission Control Protocol*) je konekcijski protokol koji omogućuje pouzdanu komunikaciju između uređaja i programa preko IP-a (engl. *Internet Protocol*) uz provjeru greške. Drugi način prijenosa podataka je UDP (engl. *User Datagram Protocol*) protokol. UDP je, za razliku od TCP-a, beskonekcijski protokol koji ne osigurava točnost isporuke poslanih podataka. Današnji svijet je većinu vremena "na mreži" i sve je teže pronaći aplikacije koje rade izvanmrežno. U ovom radu posebna pozornost se pridaje mrežnim uređajima i krajnjim korisnicima u mreži te nadgledanju njihovog rada (engl. *auditing*).

U današnjem svijetu zahtjevi za dostupnost mreže su 99.99%, odnosno traži se da mreža bude skoro uvijek dostupna [1]. S obzirom na kompleksnost računalnih mreža veliku pažnju treba usmjeriti na njen nadzor i upravljanje. Administrator mreže po prirodi posla treba nadzirati mrežu te uklanjati probleme na njoj, a u tome mu pomažu dnevnici (engl. *logs*), na čijem se prikupljanju, pohrani i analizi temelji ovaj završni rad. Kao pomoć administratoru, postoje dvije kategorije srodnih alata, a to su alati za nadzor računalnih mreža (engl. *network monitoring tools*) i alati za upravljanje računalnim mrežama (engl. *network management tools*). U prikazanom završnom radu implementiran je centralni poslužitelj za prikupljanje, pohranu i analizu syslog poruka koji služi kao alat za nadgledanje računalne mreže. Prednost centraliziranog poslužitelja je u tome što na jednom mjestu sprema poruke s više uređaja na mreži i tako olakšavaju posao ljudima zaduženima za njenu sigurnost. Danas na tržištu postoje mnogi programi koji mogu analizirati i nadzirati mrežu u realnom vremenu i imaju mogućnost alarmiranja administratora o neobičnim radnjama na mreži i tako minimiziranja moguće štete kroz pravovremena upozorenja. Važno je naglasiti kako alarmiranje administratora mreže

predstavlja važnu stavku u postavljanju ovakvih poslužitelja. Specijalizirani programi su uglavnom gotova programska rješenja koja su najčešće skupa, ali nude programsku podršku i redovite nadogradnje. Program prikazan u završnom radu je "Syslog Watcher", programska podrška verzije 4.5.8 tvrtke "EZ5 Systems" za prikupljanje *syslog* poruka.

Motivacija ovakve implementacije je upravo mogućnost jednostavnijeg i bržeg nadgledanja događaja u mreži bez zasebnog spajanja na svako računalo ili usmjernik te pregledavanja događaja direktno na njima. Na ovaj način, svi događaji koji se odvijaju na važnim uređajima nalaze se na jednom mjestu i osobi zaduženoj za održavanje mreže je nemjerljivo lakše ju održavati.

Cilj ovog završnog rada je implementacija centralnog poslužitelja za prikupljanje, pohranu i analizu syslog poruka. Prvo poglavlje završnog rada predstavlja teoretski dio. Objašnjen je syslog poslužitelj, syslog poruke te način njihova prijenosa. Također su navedene i tehnologije korištene za izradu rada. Drugo poglavlje prikazuje praktični dio, odnosno implementaciju korištenih tehnologija u cjelinu koja zadovoljava krajnji cilj i njihove postavke kako bi sustav pravilno radio. U zadnjem poglavlju je napisan zaključak u kojem je napisano što se u završnom radu postiglo i autorovo mišljenje o zadatku.

2 CENTRALIZIRANO SKUPLJANJE SYSLOG PORUKA

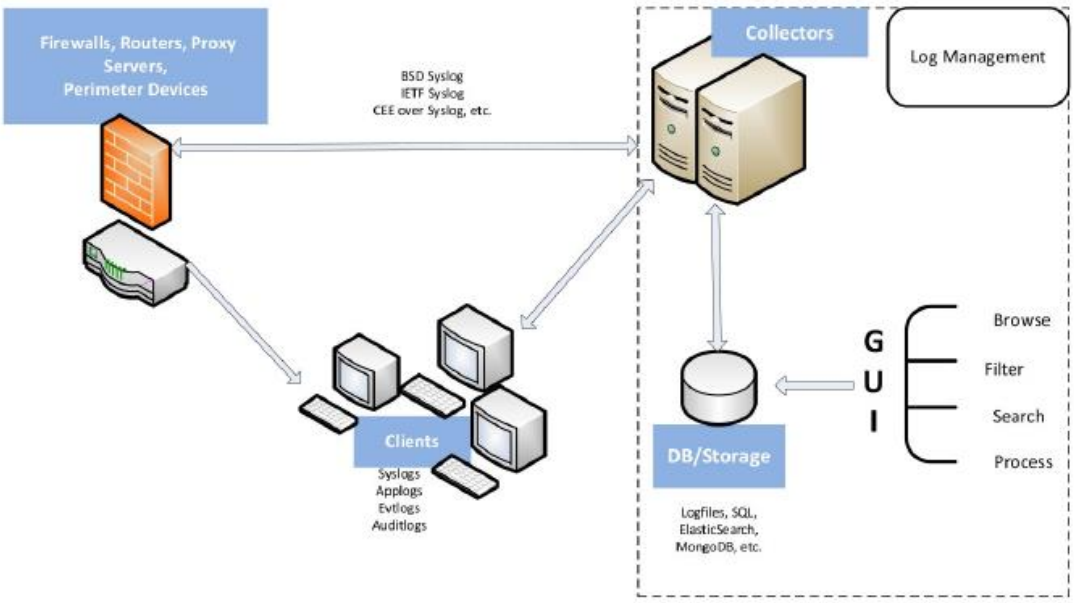
2.1 Syslog poslužitelj

Kod centraliziranog skupljanja syslog poruka najvažniji dio je syslog poslužitelj. Kao što je prethodno spomenuto, on omogućuje brže nadgledanje mreže i bržu reakciju na moguće probleme. Također, dobra je praksa da se koristi udaljeni syslog poslužitelj. Njegove prednosti su višestruke, a osim što povećava sigurnost mreže time što prikazuje sva događanja na mreži, veća je sigurnost i syslog poruka budući da eventualni napadač koji uđe u sustav može obrisati poruke na mrežnim uređajima i računalima te tako prekriti tragove ulaska u sustav. Na ovaj način, sve poruke ostaju pohranjene na uređajima, ali i na centralnom syslog poslužitelju.

Syslog poslužitelj bi trebao imati sljedeće značajke [2]:

- Syslog "prisluškivač", odnosno nekakav alat koji prikuplja i obrađuje poruke koje pristižu na UDP priključak 514; iako zbog naravi protokola ne može biti siguran kako ih je sve prikupio
- Prikupljanje syslog poruka od svih uređaja na mreži koji ih generiraju u stvarnom vremenu i na jednom mjestu
- Upozorenja o čudnom ponašanju na mreži putem elektroničke pošte na temelju definiranih uvjeta
- Gotovo trenutna analiza i mogućnost pretraživanja syslog zapisa na temelju zahtjeva (za rješavanje problema ili istraživanje mogućih nezakonitih radnji)
- Zadržavanje syslog poruka određeni vremenski period; ovisno o potrebama i resursima
- Mogućnost izrade izvještaja koji opisuju prikupljene poruke
- Mogućnost spremanja syslog poruka u vanjske baze podataka radi lakšeg i bržeg pristupa podacima

Na slici 1. se može vidjeti pojednostavljena shema syslog poslužitelja [3].



Slika 1: Shema centraliziranog syslog poslužitelja

2.1.1 Verzije syslog poslužitelja

Na tržištu postoje različite implementacije syslog poslužitelja [4]. Uz već spomenuti Syslog Watcher, neki od ostalih su:

- **Kiwi Syslog Server** – jedan od najboljih syslog poslužitelja koji je jednostavan za instaliranje i kreira izvješća u obliku čistog teksta ili u HTML obliku. Također postoji mogućnost automatske reakcije na nadolazeće syslog poruke u obliku slanja upozorenja putem elektroničke pošte, spremanja poruka u bazu podataka ili prosljeđivanja primljenih poruka. Upravlja sa Syslog i SNMP (engl. *Simple Network Message Protocol*) porukama i podržava Windows operativne sustave, ali i Linux.
- **Sawmill** – univerzalni program koji može obraditi gotovo sve oblike log podataka. Jednostavan za instaliranje i zahvaljujući intuitivnom sučelju lagan za korištenje. Kao i Syslog Watcher može pohranjivati podatke u bazu podataka, obrađuje poruke u stvarnom vremenu i može se podešavati po potrebama korisnika. Također, podržan je na većini platformi, odnosno operativnih sustava (Windows, Linux, Solaris itd.).

- **Datagram Suite** – poslužitelj koji se sastoji od 3 programa (Syslog Server, Syslog View i Syslog Agent) koji zajedno obavljaju funkciju centraliziranog poslužitelja. Omogućuje analizu, pohranjivanje poruka u bazu podataka i alarmiranje administratora ako postoji čudno ponašanje na mreži, ali ne uključuje slanje elektroničke pošte u slučaju problema na mreži. Uglavnom se koristi na Windows operativnim sustavima.
- **Nagios** – program koji omogućuje instalaciju više syslog poslužitelja koji služe istoj svrsi (redundancija). Uz analizu, omogućuje brze upite i pretraživanja poruka kao i mogućnost alarmiranja administratora. Prednost mu je i mogućnost instalacije na više vrsta operativnih sustava (Windows, Linux itd.).
- **WhatsUp Gold** – poslužitelj koji omogućuje primanje syslog porukâ od svih uređaja koji šalju takvu vrstu poruka. Obradi do 6000000 poruka po satu, a može ih sortirati po tipu, vremenu, ip adresi itd.. Također, može slati elektroničku poštu u slučaju greške na mreži ili je poslati na neko drugo računalo. Podržan je Windows operativni sustav.

Većina navedenih rješenja posjeduju plaćene verzije poslužiteljâ i verzije koje ne zahtjevaju naknadu. Kod verzija koje se ne plaćaju ograničenja su uglavnom u broju uređaja s kojih poslužitelj može primati poruke i tu se uglavnom radi o osobnim licencama koje služe za kućnu uporabu (osim kod Nagios sustava koji ograničava količinu generiranih poruka; kod verzije bez naknade 500 Mb/dan). Kod plaćenih verzija poslužitelja, postoje jeftinije i skuplje licence koje se razlikuju po broju uređaja od kojih skupljaju poruke. Jeftinija plaćena verzija omogućuje uglavnom do 10 uređaja, a skuplja nema ograničenja u broju uređaja. Također, plaćene verzije se plaćaju na godišnjoj bazi (svake godine se obnavlja), a za uzvrat se dobivaju nadogradnje i pomoć u radu putem elektroničke pošte ili internetskog foruma za podršku. Treba naglasiti kako svaka od verzija ima iste mogućnosti rada sa syslog porukama.

U završnom radu odabran je Syslog Watcher paket zbog svoje jednostavnosti korištenja, mogućnosti baratanja sa syslog porukama i relativno lakog postavljanja. Korištena je verzija 4.5.8 koja je dostupna bez naknade i s njom se dobiva osobna licenca s kojom poslužitelj može primati poruke s do 5 uređaja. Važno je napomenuti kako je to starija verzija Syslog Watchera, a novije verzije (5.0.X) se plaćaju dok korisnik ima pravo na mjesec dana probnog perioda bez plaćanja.

2.2 Syslog poruke

Syslog poruke su zapravo događaji koji se odvijaju ili su se odvili na pojedinom uređaju i kao takve mogu upućivati na pravilno, odnosno nepravilno ponašanje uređaja u mreži [5]. Koriste se u svrhu rješavanja problema na mrežnim uređajima i računalima, bilo za vrijeme instalacije ili kada dođe do problema na mreži. Također, syslog poruke su bitne kod otkrivanja upada u sustav, nadgledanja mreže na duže vrijeme, ali i za praćenje aktivnosti korisnika i administratora. Uređaji koji šalju syslog poruke su usmjernici, vatrozidi i preklopnici. Računala u mreži su također u mogućnosti slati poruke sa svog operativnog sustava (Windows, Linux itd.).

Format syslog zapisa je standardiziran i sastoji se od 3 dijela; **zaglavlja** (engl. *header*), **strukturiranih podataka** (engl. *structured-data; sd*) i **poruke** (engl. *message*). U zaglavlju poruke upisuju se podaci o prioritetu i verziji, vremenska oznaka, ime računala i aplikacije te podaci o procesu i aplikaciji [2]. Nakon zaglavlja, dolazi polje strukturiranih podataka u *"key=value"* formatu (format poruke u bazi podataka), a format poruke koji se nalazi na kraju zapisa je također standardiziran.

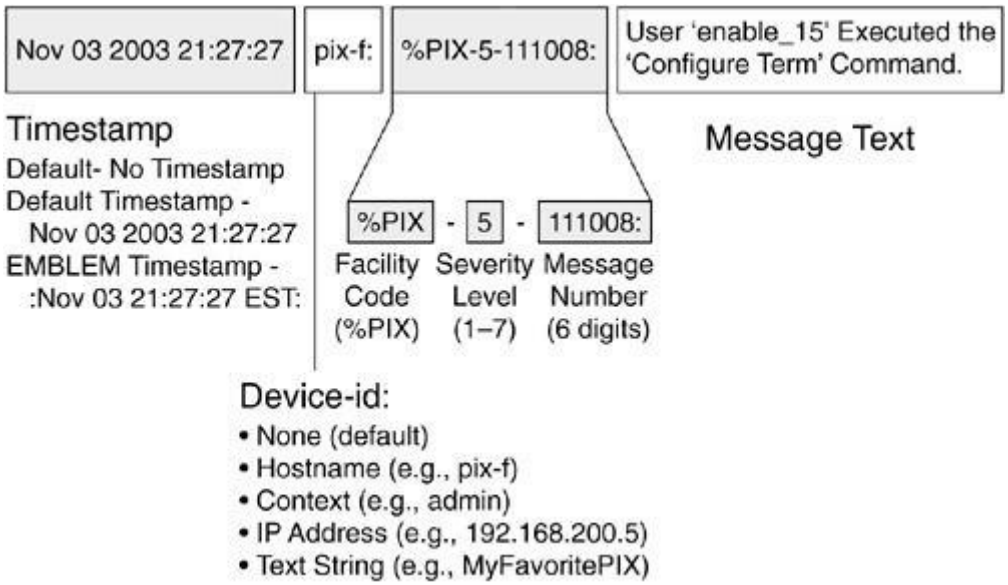
Centralizirano skupljanje syslog poruka bitno je zbog rezervne kopije porukâ, njihove naknadne analize ili pretrage. Osim toga, syslog poruke daju uvid administratoru mreže u način rada sustava i bržu dijagnostiku problema budući da su poruke na jednom mjestu. Kada se govori o količini syslog poruka koje syslog poslužitelj sakupi, svakog dana uređaji na mreži mogu poslati desetke tisuća porukâ, od koji samo neke mogu predstavljati opasnost i zahtijevati reakciju. Velike kompanije dnevno mogu generirati oko 4 GB syslog poruka (svaka syslog poruka zauzima najviše 1 KB ili manje jer je tako propisano u RFC 3164 standardu, ali nema najmanje određene veličine) i preko 95% njih nam govori o uspješnosti obavljenih zadataka [6]. Također, valja napomenuti kako se syslog poruke zadržavaju na uređajima, a nakon ponovnog pokretanja uređaja se prebrišu pa je prikladno syslogove, nakon što stignu na centralizirani poslužitelj, pohranjivati u bazu podataka što je i jedan od ciljeva u prikazanom završnom radu.

Ako su potrebe korisnika takve da je sistemske događaje potrebno pratiti i s Windows operativnog sustava, koji se po pretpostavci ne skupljaju na syslog poslužitelju budući da nisu istog formata, uz pomoć programa koji su napravljeni od strane neovisnih proizvođača, događaji koji se bilježe na Windows operativnim sustavima (naziva Event

Logovi) mogu se oblikovati u format poruke koji je propisan syslog standardom i kao takve poslati syslog poslužitelj [7].

2.3 Syslog protokol

Syslog poruke prenose se preko syslog protokola [8], a razvio ga je Eric Allman 1980-ih godina i u početku se koristio kao dio Sendmail projekta. Kako je od početka bio dobro napravljen, počeo se koristiti i u drugoj programskoj podršci. Od tada se syslog protokol koristi na Unix operativnim sustavima i na mrežnim uređajima (usmjernici, preklopnici, vatrozidi). U prvim godinama nakon razvoja, syslog protokola nije bio standardiziran niti je imao svoj propisani oblik. Standardiziran je u dokumentu RFC 3164. Nakon još nekih nadogradnji, taj dokument je 2009. godine naslijedio RFC 5424 koji je i danas na snazi. Na slici 2. je prikazan standardiziran format syslog zapisa iz tog dokumenta [2].



Slika 2: RFC 5424 format syslog zapisa

Syslog protokol funkcionira tako da se poruke šalju preko interneta, a njih "hvataju" syslog poslužitelji. Poruke se šalju UDP protokolom na priključnu točku (engl. *port*) 514 ili ponekad 601 [9]. Arhitektura syslog protokola je klijent-poslužitelj oblika, a to znači da mrežni uređaji i računala u mreži, koji predstavljaju klijente, šalju svoje poruke syslog poslužitelju koji se uobičajeno zove *syslogd*, *syslog deamon* (deamon označava program ili proces koji se odvija u pozadini) ili jednostavno syslog poslužitelj.

Većina syslog poslužitelja se sastoji od tri entiteta, odnosno objekta [10]:

- **Uređaj –** predstavlja uređaj, servis ili aplikaciju koja generira syslog poruke (u završnom radu to su usmjernici, vatrozid i Windows operativni sustav)
- **Syslog *relay* uređaj –** uređaj koji prima i prosljeđuje syslog poruke (jedan tip posrednika između klijenta i poslužitelja, koji može i ne mora postojati u određenoj mreži)
- **Syslog poslužitelj –** poslužitelj koji sakuplja syslog poruke

Poruke se šalju u obliku čistog teksta, ali kako bi se poboljšala sigurnost prijenosa mogu se slati enkriptirane putem SSL-a (engl. *Secure Socket Layer*; kriptografski standard za poboljšanje sigurnosti podataka na mreži) [9]. Kako bi upravljanje sa syslogovima bilo lakše, poruka mora imati dvije oznake. Prva oznaka govori o funkciji izvora (objekta) koji je poslao poruku (u Syslog poslužitelju naziv je *facility*). Funkcije (objekti) po standardu RFC 5424 su prikazani u tablici 1. [11].

Tablica 1: Objekti koji šalju poruke

Broj	**Ključna riječ**	**Opis objekta**
0	*kern*	Poruka od jezgre (kernel)
1	*user*	Poruke generirane na razini korisnika
2	*mail*	Poruka s mail sistema
3	*daemon*	Poruka od deamona (procesa)
4	*auth*	Sigurnosne/autorizacijske poruke
5	*syslog*	Poruke generirane od strane sysloga
6	*lpr*	Podsustav linijskog pisača
7	*News*	Podsustav mrežnih novosti
8	*Uucp*	Podsustav UUCP (Unix-to-Unix Copy)
9	/	Proces sata
10	*Authpriv*	Sigurnosne/autorizacijske poruke
11	*ftp*	FTP proces
12	/	NTP podsustav (sinkronizacija sata između uređaja na mreži)
13	/	Zapis s Linux OS-a (log audit)
14	/	Zapis o upozorenju (log alert)
15	*Cron*	Proces sata
16-23	*local0, local1…*	Lokalna uporaba 0-7

Objekti od kojih se skupljaju syslog poruke u prikazanom završnom radu su uglavnom mrežni objekti, a za njih su rezervirani brojevi od 16 do 23, odnosno brojevi za lokalnu uporabu. Druga oznaka govori o razini ozbiljnosti syslog poruke (engl. *severity*). Razine govore koliko je sustav ugrožen i samim time sugeriraju na sljedeće korake, a prikazane su u tablici 2. [12].

Tablica 2: Razine ozbiljnosti

Broj razine	**Razina ozbiljnosti**	**Opis**
0	Hitno (engl. *emergencies*)	Sustav je neupotrebljiv.
1	Uzbuna (engl. *alert*)	Potrebno je djelovati odmah.
2	Kritično (engl. *critical*)	Kritična stanja. Djelovati odmah.
3	Greška (engl. *error*)	Stanja greške.
4	Upozorenje (engl. *warning*)	Stanja upozorenja.
5	Obavijest (engl. *notice*)	Normalna, ali važna stanja.
6	Informacije (engl. *informational*)	Samo informativne poruke.
7	Otklanjanje grešaka (engl. *Debugging*)	Samo stanja koja zahtijevaju otklanjanje grešaka.

- Što se tiče razine ozbiljnosti 0, odnosno **Emergencies**, one se pojavljuju rijetko i ukazuju na neupotrebljivost sustava. Primjer poruke je da će se mrežni uređaj ugasiti zbog problema s ventilatorom. U prikazanom radu postavke okruženja mrežnih uređaja unutar simulatora su normalne budući da se radi o slikama operativnih sustava stvarnih uređaja. Ovakva poruka zahtjeva hitnu intervenciju kako bi sustav ponovno krenuo s radom.
- Razina ozbiljnosti 1, **Alert,** može se pojaviti kad je nestala rezervna poveznica s pružateljem internet usluge (ISP) ili je prekoračena temperatura uređaja i potrebno je alarmirati osobu zaduženu za popravak nastalog stanja.
- **Critical,** razina ozbiljnosti 2, pojavljuje se ako dođe do gubitka osnovne poveznice s pružateljem internet usluge.
- **Error**, razina ozbiljnosti 3 ne zahtijeva toliko brzu reakciju kao prethodne, ali problem mora biti riješen u nekom vremenskom periodu. Primjer je neuspjela NAT translacija na vatrozidu mreže.
- Razina ozbiljnosti 4, **Warning** ukazuje na to da će se dogoditi greška ako se ne poduzme određena mjera, na primjer disk je 85% ispunjen.
- **Notice**, razina ozbiljnosti 5 predstavlja stanja koja nisu ozbiljna, ali su neobična u usporedbi s uobičajenim događajima na mreži.
- Razina ozbiljnosti 6, **Informational**, govori o normalnim događajima na mreži, na primjer uspješnom pristupu nekog računala na internet stranicu

- **Debugging**, razina ozbiljnosti 7, prikazuje informacije bitne za ljude koji razvijaju aplikacije kako bi popravili moguće greške u radu.

U syslog postavkama svakog mrežnog uređaja potrebno je odrediti razinu ozbiljnosti poruka koje se šalju poslužitelju, a brojevi ispod broja koji je odabran su automatski uključeni. U prikazanoj implementaciji, ako se fizički ne nalazi u blizini radnog mjesta, mrežni administrator je upozorenjima poslanima na elektroničku poštu obavješten od strane centraliziranog syslog poslužitelja da je došlo do nekog problema na mreži i da je potrebna reakcija.

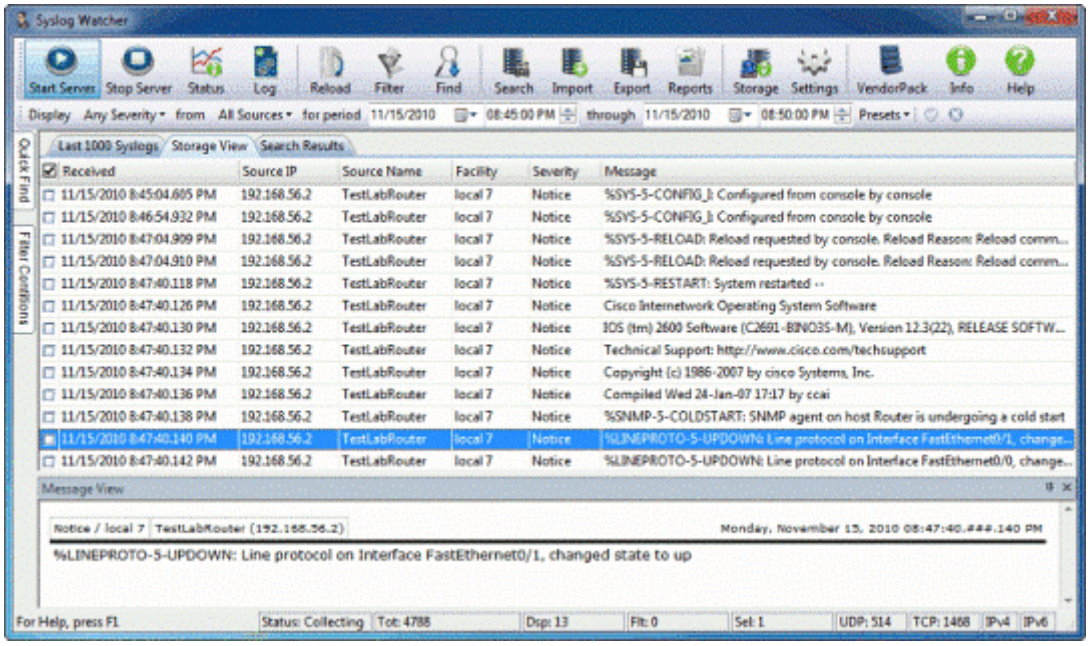
2.4 Tehnologije korištene u praktičnom djelu rada

GNS3 je program otvorenog koda, prvi put predstavljen 2008. godine, a napisan je u programskom jeziku Python [13]. GNS3 je, kao što mu i samo ime kaže, grafički simulator mreže, odnosno s njim korisnici konstruiraju mrežu onako kako su je zamislili ili onako kako im je zadano omogućavajući potpunu preglednost mreže, a samim time i lakše upravljanje. Mrežna oprema dodana i prikazana u simulatoru predstavlja operativne sustave fizičkih uređaja i ima iste mogućnosti kao i mrežni uređaji unutar stvarne mreže. Podržava mnogo uređaja, a u završnom radu korišteni su Ciscovi usmjernici i vatrozidi dok sam program ima ugrađene uređaje poput simulacije virtualnog računala i preklopnika. Ovaj program maksimalno dočarava mrežu u stvarnom svijetu i prednosti su mu upravo jednostavnost pregleda i postavljanja mreže. Zbog svega toga GNS3 je odličan za studente i osobe koji se tek upoznaju s mrežama, ali i za IT stručnjake kako bi nadogradili svoje znanje o mrežama.

Kako je u prethodnom poglavlju navedeno, syslog poslužitelj može spremati poruke u svoje datoteke, ali i u vanjske baze podataka. Prednosti spremanja syslog poruka u vanjsku bazu podataka su lakše i brže pretraživanje poruka, dulje vrijeme pohrane poruka i mogućnosti redovite izrade rezervne kopije podataka. Također, ako dođe do rušenja syslog poslužitelja, a rezervna kopija nije napravljena, sve poruke su spremljene u bazi podataka. Sustav upotrijebljen u ovom završnom radu je Microsoftov sustav za rad s relacijskim bazama podataka - SQL Server 2017, Express verzija. Kako bi na istom računalu moglo biti pokrenuto više operativnih sustava korišten je VMware Workstation Player. To je često korišten program (naziv je i virtualizator) koji omogućuje pokretanje

drugih operativnih sustava na već postojećem. VMware preko hipervizora (engl. *hypervisor*), sloja koji se nalazi između strojne opreme računala i operativnog sustava, dodjeljuje resurse računala (memoriju, procesorsko vrijeme) dodanim operativnim sustavima i oni se prikazuju kao zasebna računala. Verzije Windowsa koje su upotrijebljene za realizaciju ovog završnog rada su Windows 10 Educational i Windows Server 2012 R2.

Syslog Watcher je centralizirani **s**yslog poslužitelj koji služi za prikupljanje, analizu i pohranu syslog zapisa s mrežnih uređaja i računala koja se nalaze na mreži te tako omogućuje lakše praćenje svih događaja koji se u njoj zbivaju [14]. Poslužitelj pomaže pri održavanju mrežne stabilnosti i provjeri njene sigurnosti. Syslog Watcher je program tvrtke "EZ5 Systems", prije znane pod imenom "SNMP Soft" koja se specijalizirala u dizajnu programske podrške za inženjere informacijske tehnologije, a njeno je sjedište u Vancouveru, Kanada. Na slici 3. je prikazano grafičko, to jest korisničko sučelje Syslog Watcher programa verzije 4.5.8.



Slika 3: Korisničko sučelje Syslog Watchera

Korisničko sučelje je uredno i jednostavno i na njemu su dostupni svi zadaci koji se trebaju brzo odraditi kao što su početak i zaustavljanje rada poslužitelja, prikaz trenutnog stanja syslog poruka, filtriranje i pretraga do sad prikupljenih zapisa te njihovo unošenje ili izvoženje (engl. *export*) u ili iz programa. Također, poruke se mogu sortirati po datumu primitka, ozbiljnosti, IP adresi, objekta s kojeg su došli itd.. Jedna od prednosti Syslog Watchera je i mogućnost upravljanja poslužiteljem i sakupljanje poruka kako na lokalnom,

tako i na udaljenom uređaju. Syslog Watcher može upravljati s do 5000 syslog poruka u sekundi i pokreće se kao servis u operativnom sustavu Windows što ga čini dobrim izborom za manja okruženja u kojima nema puno poslužitelja, a samim time traži i manje procesorske snage za pokretanje. Pohrana poruka se odrađuje automatski, a one s većom važnosti se čuvaju duže kako administratoru ne bi promakao neki događaj na mreži koji zahtjeva njegovu pažnju ili reakciju. Povijest zapisa se također lako vidi i filtrira zbog dosta intuitivnog sučelja programa. Što se tiče kompatibilnosti s operativnim sustavima, program radi isključivo na Windowsu.

3 IZRADA I IMPLEMENTACIJA ZAVRŠNOG RADA

Praktični dio završnog rada dijeli se na instalaciju potrebnih alata za rad i konfiguraciju tih alata kako bi služili svrsi. U prikazanom završnom radu bilo je potrebno:

- instalirati GNS3 mrežni simulator i u njemu dodati potrebne uređaje (usmjernike, vatrozid, virtualne strojeve, vezu s internetom)
- unutar VMware Workstation 15 Playera dodati potrebne virtualne strojeve i konfigurirati ih
- konfigurirati Syslog Watcher paket za primanje syslog poruka
- izraditi bazu podataka u Microsoft SQL-u i izraditi upite za određene statistike

3.1 Izrada mreže u GNS3 mrežnom simulatoru

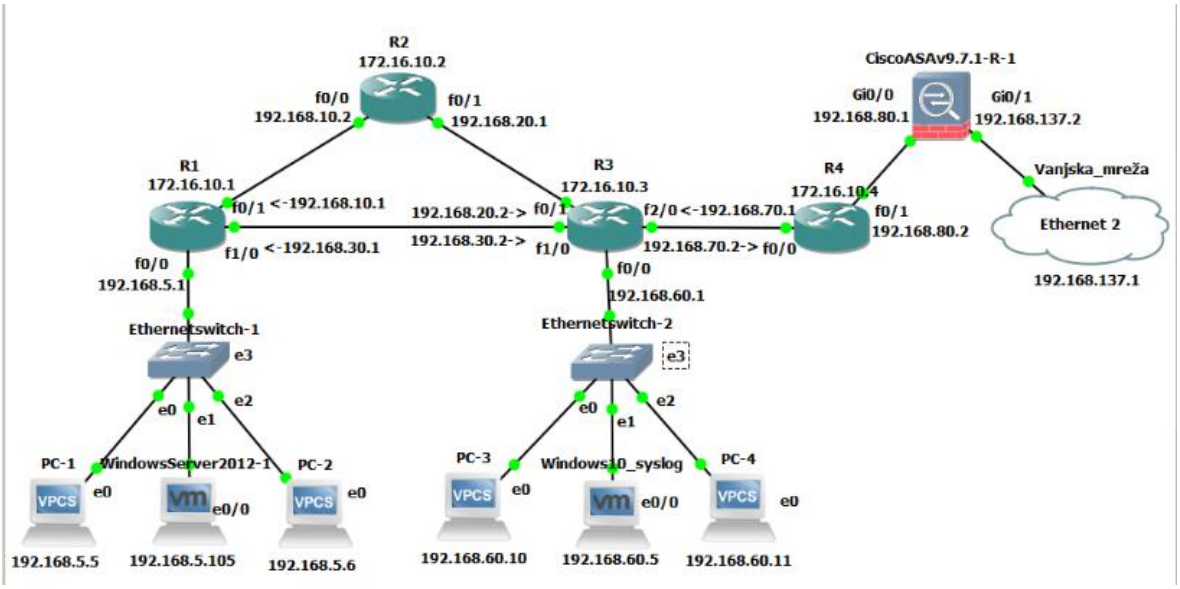
Uređaji koji su dodani u simulator i ostala pomagala koja su korištena za izradu mreže su:

- **Cisco usmjernik c3725**
- **Cisco ASAv 9.7.1** - Cisco Adaptive Security Virtual Appliance je virtualna verzija vatrozida koja se koristi u GNS3 virtualnom okruženju [15]. Pokreće se kao virtualni stroj unutar GNS3 simulatora i pruža većinu mogućnosti koje ima Ciscov fizički ASA vatrozid. ASAv sprječava prolazak nepotrebnog i/ili štetnog prometa izvan neke privatne mreže (odvaja privatnu od javne mreže) i konfigurira se prema potrebama korisnika. Na njemu se konfiguriraju pravila NAT translacije, povezuju sučelja i određuje tko smije ići na internet. Prednosti ovakve programske podrške su svakako manja potreba za strojnom opremom i mogućnost lakog upravljanja, ne samo iz naredbene linije, već i iz grafičkog sučelja
- **Ethernet Switch**
- **Virtualni strojevi** - računala koja su stvorena u Vmware Workstationu te predstavljaju prava računala koja se koriste u uredima ili drugim radnim mjestima i imaju sve komponente kao i fizičko računalo
- **Virtualna računala u sklopu GNS3 simulatora** – uređaj koji predstavlja simulaciju računala i omogućuje ručno postavljanje IP adrese, mrežne maske,

pristupnika i željenog DNS poslužitelja. Također omogućuje ping i DHCP (engl. *Dynamic Host Configuration Protocol*) zahtjev za mrežnim postavkama.

- **Oblak (engl. *Cloud*) –** Oblak predstavlja dodatak u GNS3 mrežnom simulatoru preko kojeg je moguće povezivanje simulirane mreže na internet koje se obavlja preko mrežne kartice uređaja koja je spojena na internet. Potrebno je u postavkama oblaka odabrati mrežnu karticu koja je spojena na mrežu i na drugim uređajima omogućiti pristup internetu što će biti prikazano u daljnjem tekstu.

  Na slici 4. je prikazana topologija simulirane mreže.



Slika 4: Topologija simulirane mreže

Kako bi mreža funkcionirala, potrebno je postaviti uređaje tako da paketi putuju kroz njih do odredišta. U ovom završnom radu su korištene FastEthernet veze između svih uređaja. Postavke jednog od usmjernika, točnije usmjernika R1 objašnjene su u nastavku.

U konfiguraciji usmjernika je postavljeno njegovo ime kao R1. Zbog točnosti unutarnjeg sata usmjernika za vremensku zonu je odabrana GMT +2 zona, odnosno zona za Republiku Hrvatsku, a za NTP (engl. *Network Time Protocol*) je odabran osnovni Googleov poslužitelj na adresi 216.239.35.0. Postavljen je DNS poslužitelj kako bi usmjernik mogao baratati s imenima određenih stranica na internetu umjesto s njihovim IP adresama. Za DNS poslužitelj odabran je Googleov DNS na adresi 8.8.8.8. Zbog intuitivnijeg baratanja postavkama usmjernika omogućen mu je pristup preko internet preglednika (http protokol) u koji je dovoljno upisati njegovu adresu te odabrano korisničko ime i lozinku. Nadalje,

uređene su postavke samih syslog poruka, odnosno postavljena je adresa syslog poslužitelja koji ih prikuplja, razina ozbiljnosti poruka je postavljena na warning (razine ispod ove su automatski uključene) i šalje se usmjernikov ID (engl. I*dentifier*). Uključeno je njihovo slanje s usmjernikove IP adrese, poruke se šalju u obliku teksta, a ako se postavlja neka vrsta lozinke, one se prikazuju u obliku zvjezdica tako da je osoba koja nije ovlaštena ne može vidjeti. Također, vide se i postavke sučelja samog usmjernika, Loopback0, i sučelja s kojim je usmjernik povezan s drugim uređajima u mreži. Kako bi usmjernik mogao komunicirati s drugim uređajima, bilo je potrebno postaviti usmjerivački protokol. Za tu svrhu odabran je OSPF (engl. *Open Shortest Path First*) protokol. To je protokol koji na temelju Dijkstra algoritma računa najkraći mogući put paketa do odredišta, odnosno onaj koji je najekonomičniji. Kroz OSPF naredbu, usmjerniku se kaže koju mrežu treba prepoznati i u kojem je području ta mreža. Za mrežu u prikazanom završnom radu odabrana su ista područja. Nakon postavljanja OSPF protokola, usmjernik sam prepozna svoje susjede, odnosno sučelja s kojima je povezan. Ako na usmjernik dođe paket čija se odredišna adresa ne nalazi u usmjerivačkoj tablici uređaja (to su najčešće adrese na internetu, a ne unutar mreže), usmjernik treba znati gdje poslati takav paket pa su zato potrebne statičke rute, odnosno ručno unesene putanje koje usmjeravaju paket ka odredišnoj adresi. Rute su postavljene na sučelje sljedećeg usmjernika. Za kraj, omogućen je i telnet pristup usmjerniku kako bi mu administrator mreže mogao pristupiti ako se nalazi na nekom udaljenom mjestu unutar iste mreže (zbog vatrozida usmjerniku se ne može pristupiti s interneta). U ispisu 1. je prikazana konfiguracija usmjernika R1.

```
Vremenska zona:
R1(config)# clock timezone GMT 2
R1(config)# hostname R1
DNS poslužitelj:
R1(config)# ip name-server 8.8.8.8
Korisničko ime i lozinka za pristup preko internet preglednika:
R1(config)# username server privilege 15 password 0 promet1
Postavke slanja syslog poruka u obliku teksta i skrivanje zaporki:
R1(config)# archive
R1(config-archive)# log config
R1(config-archive-log-config)# logging enable
R1(config-archive-log-config)# notify syslog contenttype plaintext
  R1(config-archive-log-config)# hidekeys
IP adresa usmjernika i adrese sučelja s kojima je povezan s ostalim uređajima:
R1(config)# interface Loopback0
R1(config-if)# ip address 172.16.10.1 255.255.255.0
R1(config)# interface FastEthernet0/0
R1(config-if)# ip address 192.168.5.1 255.255.255.0
 duplex auto
 speed auto
R1(config)# interface FastEthernet0/
R1(config-if)# ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
R1(config)# interface FastEthernet1/0
 R1(config-if)# ip address 192.168.30.1 255.255.255.0
 duplex auto
 speed auto
Usmjerivački protokol:
R1(config)# router ospf 1
R1(config-router)# network 172.16.10.0 0.0.0.255 area 0
R1(config-router)# network 192.168.0.0 0.0.255.255 area 0
Statičke rute za slanje paketa na internet:
R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.2
R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.30.2
Omogućavanje pristupa usmjerniku preko internet preglednika:
R1(config)# ip http server
R1(config)# ip http authentication local
no ip http secure-server
IP adresa na kojoj se nalazi syslog poslužitelj i razina ozbiljnosti poruka koje se šalju:
R1(config)# logging trap warning
R1(config)# logging source-interface Loopback0
R1(config)# logging origin-id
R1(config)# logging 192.168.60.5
Telnet pristup usmjerniku:
R1(config)# line vty 0 4
 R1(config-line)# password cisco
 R1(config-line)# login
Adresa NTP poslužitelja:
R1(config)# ntp server 216.239.35.0
end
```

Ispis 1: Konfiguracija usmjernika R1

Na sličan način, samo s ponešto izmijenjenim adresama su postavljeni i ostali usmjernici. Što se tiče postavki virtualnih računala, one su relativno jednostavne i dane su u ispisu 2. U primjeru je prikazano virtualno računalo 1 (oznaka u GNS3 simulatoru VPC 1),

postavljeno mu je ime računala PC-1, njegova IP adresa, pretpostavljeni pristupnik, mrežna maska (255.255.255.0) te adresa Google DNS poslužitelja:

```
PC1> set pcname PC-1
PC1> ip 192.168.5.5 192.168.5.1 24
PC1> ip dns 8.8.8.8
```

Ispis 2: Postavke virtualnog računala 1

Način na koji je omogućena komunikacija između unutarnje i vanjske mreže je NAT translacija što je podešeno na ASA vatrozidu [16]. To je postupak gdje mrežni uređaj; uglavnom i u prikazanom radu vatrozid, prije nego proslijedi pakete prema vanjskoj mreži, mijenja izvorišnu IP adresu računalima u javnu adresu sučelja koje je povezano na internet. Tako se ograničava broj javnih IP adresa s obzirom na to da ih ima konačan broj.

Što se tiče konfiguracije, naziv vatrozida je ostao pretpostavljeni, odnosno ciscoasa. Kako bi vatrozid mogao komunicirati s internetom i virtualnom mrežom namještene su postavke sučelja s kojima je povezan. Sučelja koja prikazani vatrozid koristi su GigabitEthernet tipa. GigabitEthernet0/0 sučelje je veza prema virtualnoj mreži, postavljena je IP adresa i maska te je ključna riječ *inside*, a sigurnosna razina se postavlja na 100, odnosno na maksimum. GigabitEthernet0/1 sučelje je veza prema internetu te su potrebne iste stavke kao i na prethodnom sučelju, ali je razlika u ključnoj riječi koja je *outside*, a sigurnosna razina se tada postavlja na 0, odnosno minimum. Vremenska zona za unutarnji sat vatrozida je GMT +2. Postavljen je i Googleov DNS poslužitelj koji se nalazi na internetu, stoga je sučelje *outside*. Za funkcioniranje samog vatrozida, potrebno mu je "reći" koje adrese i koje vrste paketa može propuštati. Za to služe postavljeni mrežni objekti i pristupne liste. Kod postavljenog mrežnog objekta naziva "*vani"* uključena su računala iz svih mreža, dok su i pristupne liste postavljene na isti način (služe za "odluku" koje IP adrese mogu slati IP pakete kroz vatrozid) te im je dodijeljeno sučelje outside kako bi uređaji unutar mreže mogli ići na internet. Također, dodana je jednostavna naredba za dinamičku NAT translaciju. Nakon što je računalima u virtualnoj mreži omogućen odlazak na internet, potrebne su postavke syslog poslužitelja, odnosno njegova IP adresa i razina ozbiljnosti poruka (razina warning). Osim toga, vremenska oznaka i ID vatrozida se također šalju poslužitelju. Što se tiče komunikacije vatrozida s drugim uređajima, kako bi se to omogućilo, potrebno je dodati usmjerivački protokol. Ovdje je također korišten OSPF protokol. Kako bi vatrozid znao gdje usmjeriti pakete koji idu izvan privatne mreže,

postavljena je statička ruta koja je usmjerena na Loopback prilagodnik računala koji služi sa spajanje virtualne mreže sa stvarnom. Za kraj postavljen je Googleov NTP poslužitelj (za usklađivanje vremena na mrežnim uređajima) koji se nalazi na adresi 216.239.35.0. Konfiguracija je prikazana u ispisu 3.

```
Naziv vatrozida:
ciscoasa(config)# hostname ciscoasa
Sučelja s kojima je vatrozid povezan:
Ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# nameif inside
security-level 100
ciscoasa(config-if)# ip address 192.168.80.1 255.255.255.0
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# nameif outside
security-level 0
ciscoasa(config-if)# ip address 192.168.137.2 255.255.255.0
Vremenska zona:
ciscoasa(config)# clock timezone GMT +2
Postavke DNS poslužitelja:
dns domain-lookup outside
dns server-group DefaultDNS
ciscoasa(config)# name-server 8.8.8.8
Mrežni objekt:
ciscoasa(config)# object network vani
ciscoasa(config-network-object)# subnet 0.0.0.0 0.0.0.0
Pristupna lista:
ciscoasa(config)# access-list 1 extended permit ip any any
ciscoasa(config)# access-list 1 extended permit icmp any any
Postavke sysloga:
ciscoasa(config)# logging enable
ciscoasa(config-if)# logging timestamp
ciscoasa(config-if)# logging trap warning
ciscoasa(config-if)# logging device-id hostname
ciscoasa(config-if)# logging host inside 192.168.60.5
Dinamička NAT translacija:
ciscoasa(config)# object network vani
ciscoasa(config-network-object)# nat (inside, outside) dynamic interface
Usmjerivački protokol:
ciscoasa(config)# router ospf 1
ciscoasa(config-router)# network 172.16.10.0 255.255.255.0 area 0
ciscoasa(config-if)# network 192.168.0.0 255.255.0.0 area 0
Statička ruta:
Ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.137.1 1
Adresa NTP poslužitelja:
ciscoasa(config-if)# ntp server 216.239.35.0
```

Ispis 3: Konfiguracija vatrozida

Kako bi mreža izašla izvan svog virtualnog okruženja i bila u mogućnosti komunicirati s vanjskim svijetom, odnosno internetom, bilo je potrebno spojiti je preko oblaka na internet i odabrati željeni mrežni prilagodnik koji služi za tu svrhu. U konkretnom primjeru, za povezivanje mreže na internet koristio se *Microsoft Loopback* mrežni prilagodnik. *Loopback* mrežni prilagodnik je zapravo virtualni mrežni prilagodnik koji nema strojnu opremu uz sebe već se može koristiti za testiranje mreže kao i za spajanje virtualnih mreža na internet, a svi paketi koji su poslani na mrežu, vraćaju se *Loopback* mrežnom prilagodniku i baš zbog toga je pogodan za testiranja mreže. Što se tiče inicijalnih postavki, Loopback mrežni prilagodnik je na adresi 192.168.137.1 s maskom /24. Na njega se ne dodaje pristupnik, jer da bi mrežni prilagodnik mogao otići na internet koristi se dijeljena mreža s fizičke mrežne kartice koja je trenutno spojena na internet (jednostavna postavka na kartici *Sharing* u postavkama mrežne kartice). On se jednostavno doda na računalo preko Windowsovog čarobnjaka za dodavanje strojne opreme.

3.2 Postavljanje virtualnih strojeva u VMware Workstation Playeru

Uz postavljanje mreže, potrebno je i dodati virtualne strojeve koji simuliraju računala u stvarnom svijetu. U prikazanom radu, obavljena je virtualizacija na razini sklopovlja, pa se tako čini da je virtualni stroj posebno računalo sa svojim sklopovljem i operativnim sustavom.

Operativni sustavi dodani u virtualizator su Windows 10 i Windows Server 2012 R2 te služe za simuliranje uredskih računala u stvarnom svijetu. Kako su virtualni strojevi povezani s virtualnom mrežom preko koje i idu na internet, bilo je potrebno statički postaviti i IP adresu, mrežnu masku, pretpostavljeni pristupnik te pretpostavljeni DNS poslužitelj. Tako su u mrežnim postavkama Windows Servera postavljeni sljedeći podaci:

- IP adresa: 192.168.5.105
- Mrežna maska: 255.255.255.0
- Pretpostavljeni pristupnik: 192.168.5.1
- Željeni DNS poslužitelj: 8.8.8.8

Postavke Windows 10 virtualnog stroja su sljedeće:

- IP adresa: 192.168.60.5
- Mrežna maska: 255.255.255.0
- Pretpostavljeni pristupnik: 192.168.60.1
- Željeni DNS poslužitelj: 8.8.8.8

Na Windowsu 10 se također nalazi Syslog Watcher paket na kojem se temelji čitav završni rad te Microsoft SQL Server Express baza podataka. Bilo je potrebno, uz postavke samog Syslog Watcher paketa te baze podataka, postaviti i pravila, to jest iznimke na Windowsovom vatrozidu. Tako je na dolazeća pravila dodano pravilo da se UDP paketi propuštaju na priključku 514, pretpostavljenom priključku za syslog poruke. Isto tako, dodano je i pravilo da se TCP paketi propuštaju na priključku 1433, što je pretpostavljeni priključak za Microsoft SQL Server. Nakon ovih postavki, oba virtualna stroja bila su u mogućnosti komunicirati jedan s drugim, s ostalim uređajima u virtualnoj mreži i s internetom.

Ako se ukaže potreba, korisnik može skupljati i Event logove s Windows radnih stanica. Kao što je prethodno spomenuto, Windows svoje Event logove može uz pomoć programa preoblikovati u syslog format i takve ih slati poslužitelju. U tu svrhu odabran je Eventlog to Syslog program koji se instalira kao servis i postavlja se preko PowerShell konzole unutar Windows Servera 2012 R2 [17]. U ispisu 4. su prikazane naredbe iz PowerShell konzole kojima je omogućeno slanje Event logova u syslog formatu poslužitelju.

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights
reserved.

PS C:\Users\Administrator> cd
C:\Users\Administrator\Downloads\Evtsys_4.5.1_64-bit\64-bit
PS C:\Users\Administrator\Downloads\Evtsys_4.5.1_64-bit\64-
bit> ls
    Directory:
C:\Users\Administrator\Downloads\Evtsys_4.5.1_64-bit\64-bit

Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-----         3.10.2013.      0:36     136704 evtsys.exe
-----         30.9.2013.      0:10     174715 Readme.pdf
-----         3.10.2013.      0:53        106 shasum.txt

PS C:\Users\Administrator\Downloads\Evtsys_4.5.1_64-bit\64-
bit> .\evtsys.exe -i -h 192.168.60.5 -p 514

Command completed successfully
PS C:\Users\Administrator\Downloads\Evtsys_4.5.1_64-bit\64-
bit> net start evtsys
The Eventlog to Syslog service is starting.
The Eventlog to Syslog service was started successfully.
```

Ispis 4: PowerShell naredbe za pokretanje servisa

Nakon pozicioniranja u direktorij gdje se program nalazi, pokreće se naredba koja govori da datoteku evtsys.exe treba instalirati (instalira se kao servis), napiše se IP adresa syslog poslužitelja kojem se šalju Event logovi te preko kojeg porta se isti šalju. Kada je potvrđeno da je instalacija uspješna, naredbom `net start evtsys` pokreće se servis i na poslužitelju se vide poruke poslane od strane Windows Servera 2012 R2.

3.3 Konfiguracija Syslog Watcher paketa za primanje syslog poruka

Nakon instalacije virtualnog stroja, u ovom slučaju Windows 10 operativnog sustava, bilo je potrebno instalirati Syslog Watcher programsku podršku. Mrežne uređaje treba postaviti tako da preusmjeravaju svoje syslog zapise prema operativnom sustavu gdje se nalazi Syslog Watcher paket (za to im je dovoljna IP adresa operativnog sustava, odnosno Syslog Watchera i omogućen priključak 514 na vatrozidu Windowsa). Nakon

toga, paket je u mogućnosti primati syslog poruke. Izgled syslog poruke s napravljene virtualne mreže koja je stigla s vatrozida je:

6/24/2019 // 7:22:33.442 PM // local4 // Notice // Jun 24 2019 17:22:32 // ciscoasa // % ASA-5-304001 : Accessed URL 172.217.20.110:http://www.youtube.com

Prve dvije stavke govore o vremenu primitka poruke. Local4 je objekt (facility) odakle je poruka stigla, a Notice je tip poruke. Nakon toga ide vremenska oznaka, pa mjesto, odnosno koji je mrežni objekt poslao poruku, i na kraju sama poruka. Treba napomenuti kako je takav format i kod svih drugih poruka, samo se može promjeniti ozbiljnost poruke, lokacija odakle dolazi i tekst poruke. Prikazana poruka kaže kako je uređaj na adresi 192.168.5.105 pristupio internetskoj stranici na adresi 172.217.20.110, odnosno www.youtube.com. Ova poruka predstavlja normalan tip poruke i takvih je 95% syslog poruka. Svakog administratora mreže više zanimaju one poruke koje mogu naštetiti mreži, a u postavkama mrežnihuređaja je postavljeno da šalju poruke tipa warning i niže kako bi se smanjio broj pristiglih poruka i kako bi osoba zadužena za mrežu mogla brže uočiti problem.

Sljedeća poruka predstavlja poruku kojoj je ozbiljnost Error i dolazi s IP adrese 172.16.10.1 (adresa usmjernika R1) i govori kako je sučelje FastEthernet 0/0 promijenilo svoje stanje, odnosno ili se upalilo ili ugasilo. Logično, to traži brzu intervenciju administratora, jer može značiti da se usmjernik pokvario ili je netko namjerno ugasio sučelje.

8/28/2019 // 5:05:29.546 PM // 172.16.10.1 // local7 // Error // Aug 28 15:06:04.770 // R1 // %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

Poruke koje dolaze s Windows Servera su preoblikovane u Syslog format, a primjer poruke tipa Error prikazana je u nastavku:

8/27/2019 // 3:47:52.117 PM // 192.168.5.105 // system // Error // Aug 27 15:47:50 // WIN-UU5F76LO6VQ // 4625: AUDIT_FAILURE An account failed to log on

Ova poruka govori kako se neki korisnik nije uspio prijaviti na Windows Server preko Remote Desktop Connectiona, a to može značiti da neko neovlašten pokušava ući na računalo, pa na primjer pokušava pogoditi lozinku.

Što se tiče vatrozida i njegovih "hitnijih" poruka, u nastavku se može vidjeti poruka tipa Critical koja govori kako je odbijena nadolazeća TCP konekcija s IP adrese 205.185.216.42 na IP adresu 192.168.60.5, a dolazila je izvana.

8/28/2019 // 4:34:48.957 PM // 192.168.80.1 // local4 // Critical // Aug 28 2019 16:34:44 // ciscoasa // %ASA-2-106001: Inbound TCP connection denied from 205.185.214.42/80 to 192.168.60.5/51080 flags ACK on interface outside

Međutim, za što bolji i korisniji rad potrebno je podesiti neke postavke u samom Syslog Watcheru. Postavke koje su podešene su:

- Organiziranje rezervne kopije (engl. *backup*)
- Izvoz syslog poruka u vanjsku bazu podataka
- Namještanje upozorenja koje dolazi preko elektroničke pošte

Organiziranje rezervne kopije je potrebno za svaki bitan posao pa tako i za nadgledanje mreže. Ako nije organiziran izvoz syslog poruka u vanjsku bazu podataka, moguće je podesiti izradu rezervne kopije syslog poruka. U postavkama programa postoji stranica Backup, tu je potrebno odabrati dan u tjednu kada se rezervna kopija radi, vrijeme i odredišnu mapu koja će sadržavati podatke.

Izvoz syslog poruka u vanjsku bazu podataka se obavlja preko ODBC (engl. *Open DataBase Connectivity*) *stringa* koji služi za spajanje na vanjsku bazu podataka [18]. ODBC je sučelje za pristup bazama podataka preko SQL upita. U ovom završnom radu pristupalo se SQL bazi podataka, a ODBC string za pristup bazi podataka u koju će Syslog Watcher upisivati podatke prikazan je u ispisu 5.

```
Driver={SQL
Server};Server=192.168.60.5;Database=SyslogDB;Uid=korisnik;Pwd=pa55w0rd;
```

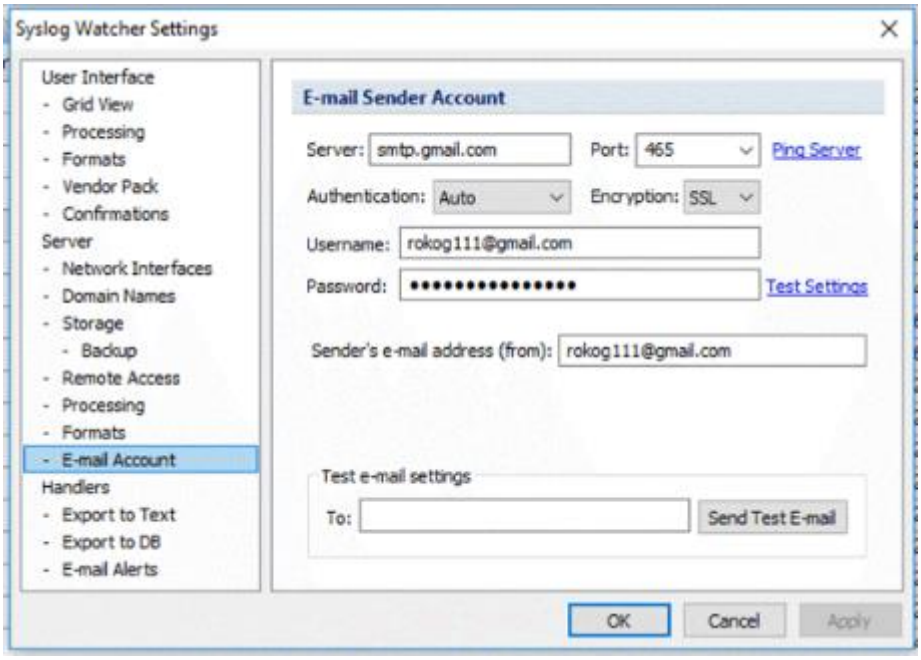
Ispis 5: ODBC String za pristup bazi podataka

Prvo se unese vrsta poslužitelja, zatim IP adresu na kojoj se poslužitelj nalazi te naziv baze podataka. Nakon toga dolazi korisničko ime koje se koristi za prijavu u bazu te lozinka. Kada je Syslog Watcher povezan s bazom podataka, potrebno mu je reći gdje da sprema podatke. To se radi preko jednostavne naredbe u SQL jeziku koja je dana u ispisu 6.

```
INSERT INTO Syslognew (Collected, IP, Facility, Severity, Message) VALUES ('$yyy-$M-
$d $H:$m:$s', '%SOURCE_IP%', '%FACILITY%', '%SEVERITY%', '%MESSAGE%');
```

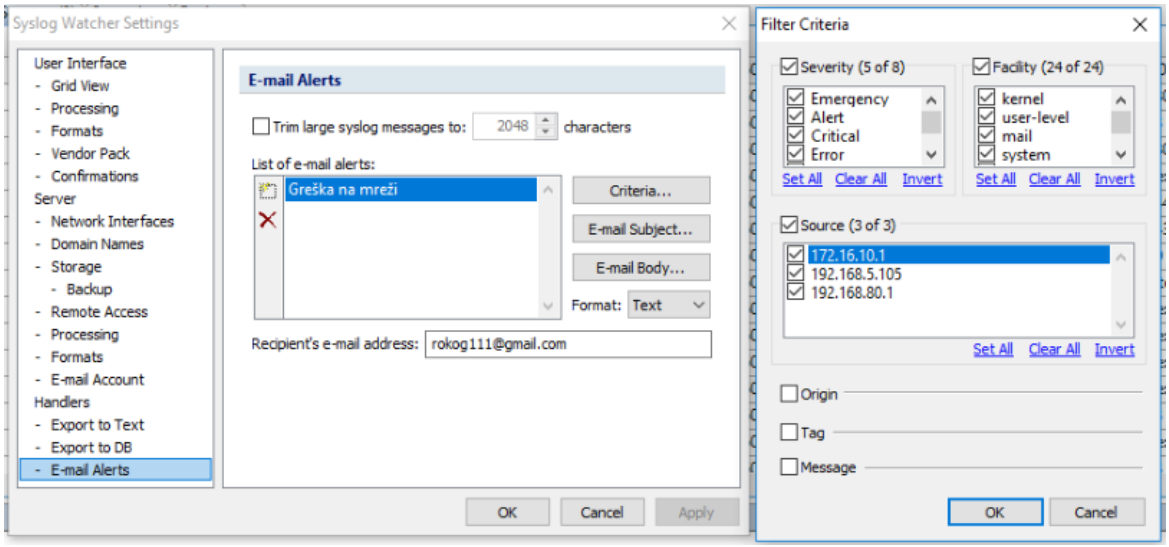
Ispis 6: SQL naredba za upis podataka u bazu

Namještanje upozorenja koje dolazi preko elektroničke pošte ide preko odabranog poslužitelja, u završnom radu to je Gmail. Nakon toga se upiše željena adresa i lozinka. Postavke se mogu vidjeti na Slika 5.



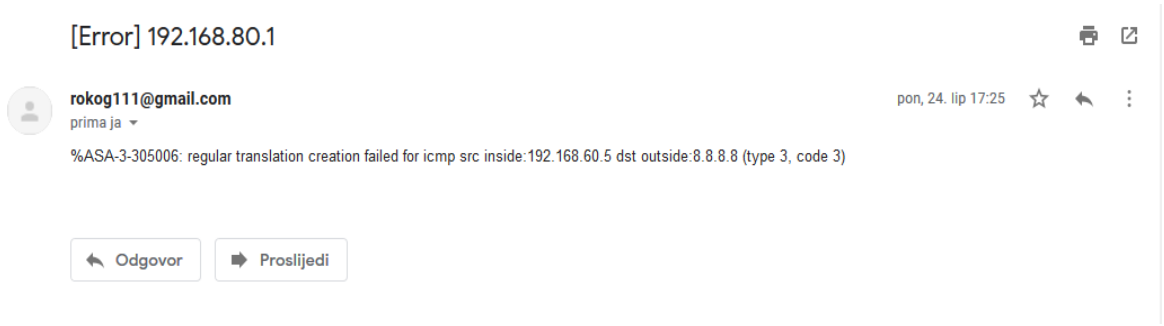
Slika 5: Postavke elektroničke pošte

Svakako je dobro postaviti kriterije na temelju kojih nam dolazi upozorenje. Također je potrebno odabrati i izvor s kojeg nam poruke dolaze. U završnom radu upozorenja dolaze isključivo za vrste poruka *Error* i *Critical* s IP adrese vatrozida jer zahtijevaju najbrže reagiranje i rješavanje problema. Kriteriji se mogu vidjeti na slici 6.



Slika 6: Kriteriji za upozorenja

Kada je elektronička adresa odabrana i kriteriji su postavljeni, a Syslog Watcher paket prikupi poruku bilo *Error* ili *Critical* ozbiljnosti, na adresu stiže upozorenje. Poruka koja stigne je prikazana na slici 7.



Slika 7: Upozorenje preko elektroničke pošte

Ovdje je prikazana poruka koja govori da NAT translacija nije uspješno obavljena za korisnika na IP adresi 192.168.60.5 kada je pokušavao pristupiti adresi 8.8.8.8, odnosno Googleovom DNS poslužitelju.

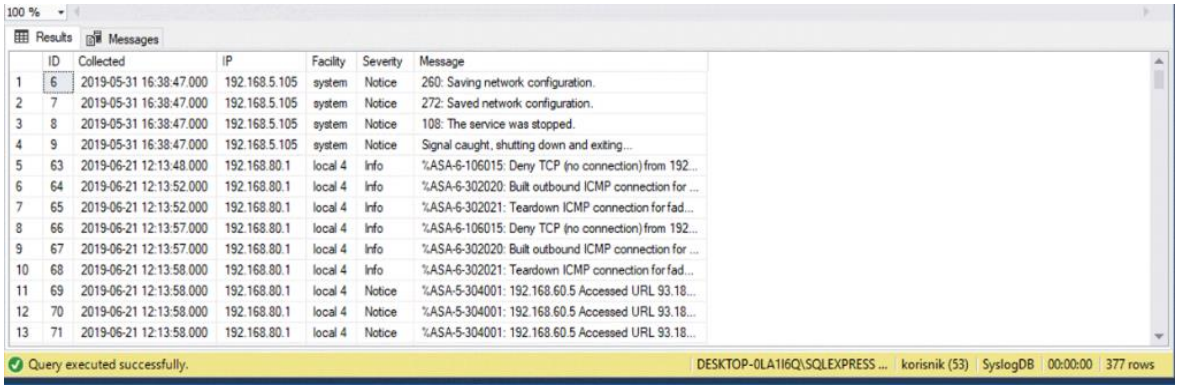
3.4 Izrada baze podataka u Microsoft SQL Serveru i kreiranje upita za određene statistike

U izradi završnog rada kao podloga za bazu podataka u koju će biti spremane syslog poruke iz Syslog Watcher paketa izabran je Microsoft SQL server. Njime se upravlja preko SSMS-a što je kratica za SQL Server Management Studio koji služi za grafički i jednostavniji prikaz bazâ podataka. U završnom radu kreirana je tablica *Syslognew*, a u tablici 3. je prikazan njen izgled.

Tablica 3: Tablica Syslognew

Naziv stupca	**Tip podatka**	**DozvoljenaNULL vrijednost**
ID (PK!)	int	Ne
Collected	datetime	Da
IP	varchar (50)	Da
Facility	varchar (50)	Da
Severity	varchar (50)	Da
Message	varchar (800)	Da

Nakon kreiranja baze i tablice unutar baze, Syslog Watcher počinje spremati svoje podatke u tablicu. Na slici 8. se vide podaci spremljeni u bazu.



100 %

Results | Messages

	ID	Collected	IP	Facility	Severity	Message
1	6	2019-05-31 16:38:47.000	192.168.5.105	system	Notice	260: Saving network configuration.
2	7	2019-05-31 16:38:47.000	192.168.5.105	system	Notice	272: Saved network configuration.
3	8	2019-05-31 16:38:47.000	192.168.5.105	system	Notice	108: The service was stopped.
4	9	2019-05-31 16:38:47.000	192.168.5.105	system	Notice	Signal caught, shutting down and exiting...
5	63	2019-06-21 12:13:48.000	192.168.80.1	local 4	Info	%ASA-6-106015: Deny TCP (no connection) from 192...
6	64	2019-06-21 12:13:52.000	192.168.80.1	local 4	Info	%ASA-6-302020: Built outbound ICMP connection for ...
7	65	2019-06-21 12:13:52.000	192.168.80.1	local 4	Info	%ASA-6-302021: Teardown ICMP connection for fad...
8	66	2019-06-21 12:13:57.000	192.168.80.1	local 4	Info	%ASA-6-106015: Deny TCP (no connection) from 192...
9	67	2019-06-21 12:13:57.000	192.168.80.1	local 4	Info	%ASA-6-302020: Built outbound ICMP connection for ...
10	68	2019-06-21 12:13:58.000	192.168.80.1	local 4	Info	%ASA-6-302021: Teardown ICMP connection for fad...
11	69	2019-06-21 12:13:58.000	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.18...
12	70	2019-06-21 12:13:58.000	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.18...
13	71	2019-06-21 12:13:58.000	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.18...

Query executed successfully. | DESKTOP-0LA1I6Q\SQLEXPRESS ... | korisnik (53) | SyslogDB | 00:00:00 | 377 rows

Slika 8: Podaci spremljeni u bazu

Izrada upita u svrhu statistike poruka je jako dobra stvar budući da jedan dokument sadržava veliku većinu ili gotovo sve poruke. Izrada statistike se radila preko SQL procedura koje su kasnije bile pozivane unutar Microsoftovog alata Excela. Napisano je više procedura, a njihov kôd je prikazan u nastavku. Prvo je prikazana procedura za izradu statistike syslog poruka po danima u tjednu. *PivotData* je zapravo jedan skupni podatak koji se sastoji od IP adrese izvorišta, polja *Collected* i ID-a retka koji pomažu lakšoj obradi većeg broja poruka i na kraju urednijoj statistici. Na kraju, upit po pivotu zbroji poruke za pojedini dan u tjednu i to prikaže u Excelovom dokumentu. Kôd procedure za izradu statistiku po godini, mjesecu i danu prikazan je u ispisu 7.

```
CREATE PROCEDURE [dbo].[StatisticsByDOW]
AS
BEGIN
WITH PivotData AS
(
SELECT
[IP] , -- grouping column
DATENAME(weekday, collected) AS 'Day', -- spreading column
[ID] -- aggregation column
FROM [SyslogDB].[dbo].[Syslognew]
 where datepart(week,collected) = datepart(week,getdate())
)
SELECT [Ip], [Monday], [Tuesday], [Wednesday], [Thursday],
[Friday], [Saturday], [Sunday]
FROM PivotData
PIVOT( count(id) FOR day IN ( [Monday], [Tuesday],
[Wednesday],[Thursday], [Friday],[Saturday],[Sunday] )) AS P;
END
GO
```

Ispis 7: Procedura za izradu statistike po godini, mjesecu i danu

U slijedećem primjeru kôda prikazana je procedura za izradu statistike na temelju ozbiljnosti poruke. U njoj su odabrana dva datuma koja su razlike mjesec dana te su iz baze odabrana polja *IP*, *Facility* i *Severity* preko kojih je i generiran ukupan broj poruka te su po istom tom rasporedu grupirani u tablici. Procedura je dana u ispisu 8.

```
CREATE PROCEDURE [dbo].[StatisticsBySeverity]
@date1  date =null,
@date2 date=null
AS
BEGIN
        -- SET NOCOUNT ON dodan da bi spriječio dodatne
rezultate
        -- zbog povezanosti sa SELECT naredbama.
        SET NOCOUNT ON;
SET @Date1 = ISNULL(@Date1, GETDATE()-30)
SET @Date2 = ISNULL(@Date2, GETDATE())
SELECT [IP], [Facility], [Severity] , count (*) AS BrojPoruka
 FROM  [SyslogDB].[dbo].[syslognew]
 WHERE collected >= @date1 and collected <= @date2
 GROUP BY [IP], [Facility], [Severity]
END
GO
```

Ispis 8: Procedura za izradu statistike po ozbiljnosti poruka

Kôd procedure za izradu statistike za pojedinu IP adresu u određenom periodu je dan u ispisu 9.

```
CREATE PROCEDURE [dbo].[StatisticsByIP]
@IP varchar(15) ='192.168.80.1',
@date1  date = null,
@date2  date = null
AS
BEGIN
-- SET NOCOUNT ON added to prevent extra result sets from
        -- interfering with SELECT statements.
        SET NOCOUNT ON;
SET @Date1 = ISNULL(@Date1, GETDATE()-30)
SET @Date2 = ISNULL(@Date2, GETDATE())
(    SELECT
         [ID],  [Collected],  [IP],  [Facility],  [Severity],
[Message]
    FROM  [dbo].[Syslognew]
     WHERE  ([IP]  like  @IP  )  and  [Collected]  >=@date1  and
[Collected] <= @date2)
END

GO
```

Ispis 9: Procedura za izradu statistike po IP adresi

Kôd za izradu statistike svih poruka za određeni vremenski period je prikazan u ispisu 10.

```
CREATE PROCEDURE [dbo].[MessagesDuringPeriods]

        @Date1 date = null,
        @Date2 date = null
AS
BEGIN
        -- SET NOCOUNT ON added to prevent extra result sets
from
        -- interfering with SELECT statements.
        SET NOCOUNT ON;
        SET @Date1 = ISNULL (@Date1, GETDATE()-30)
        SET @Date2 = ISNULL (@Date2, GETDATE())
(
    SELECT
        [ID],
       [Collected],[IP],[Facility],[Severity],[Message]
    FROM   [dbo].[Syslognew] WHERE [Collected] >= @Date1 and
[Collected] <= @Date2
)
END
GO
```

Ispis 10: Procedura za izradu statistike po vremenskom periodu

Kôd procedure za izradu statistike za syslog poruke pristigle po godini, mjesecu i danu je dan u ispisu 11.

```
CREATE PROCEDURE [dbo].[StatisticsByYMD]
AS
BEGIN
SELECT    DATEPART(YEAR, [Collected]) AS 'Year',
          DATEPART(MONTH, [Collected]) AS 'Month',
          DATEPART(DAY, [Collected]) AS 'Day',
          COUNT(*) AS 'BrojPoruka'
FROM      [dbo].[Syslognew]
GROUP BY  DATEPART(DAY, collected),
          DATEPART(MONTH, collected),
          DATEPART(YEAR, collected)
ORDER BY  'Year','Month','Day'
END

GO
```

Ispis 11: Procedura za izradu statistike po godini, mjesecu i danu

Na kraju je napravljena i procedura koja radi statistiku na temelju sâta kad je poruka pristigla, kako bi administrator pretpostavio u kojem je djelu dana mreža najkorištenija. Kôd je prikazan u ispisu 12.

```
CREATE PROCEDURE [dbo].[StatisticsByHour]

@date1 date = null,
@date2 date = null
AS
BEGIN
-- SET NOCOUNT ON added to prevent extra result sets from
        -- interfering with SELECT statements.
        SET NOCOUNT ON;
        SET @Date1 = ISNULL (@Date1, GETDATE()-30)
        SET @Date2 = ISNULL (@Date2, GETDATE())
;WITH PivotData AS
(
SELECT
datepart (hour, collected) AS 'hour', -- grouping column
[IP], -- spreading column
[ID]  -- aggregation column
FROM  [SyslogDB].[dbo].[syslognew]
where collected >= @date1 and collected <= @date2
)
SELECT hour, [192.168.5.105], [192.168.80.1]
FROM PivotData
PIVOT( count(ID) FOR IP IN ([192.168.5.105],
[192.168.80.1])) AS P;
END
GO
```

Ispis 12: Procedura za izradu statistike po satu

Što se tiče dokumenta u Excelu, on je izrađen tako da su se ove spremljene procedure samo pozivale unutar samog Excela [19]. Na kartici *Data*, potrebno je odabrati *From other sources* i tu se odabere *From Microsoft query*. Oblik SQL naredbe je jednostavan i prikazanom je u ispisu 13.

```
    exec [dbo].[StatisticsBySeverity]
```

Ispis 13: Pozivanje procedure u Excelu

StatisticsBySeverity je naziv procedure koja se izvršava unutar Excela. Na kraju, na slici 9. je prikazan dio Excelove statistike za syslog poruke.

	A	B	C	D
1	IP	Facility	Severity	BrojPoruka
2	11.11.11.11	local 7	Notice	1
3	192.168.0.1	local 0	Error	1
4	192.168.5.105	system	Notice	93
5	192.168.80.1	local 4	Critical	17
6	192.168.80.1	local 4	Error	23
7	192.168.80.1	local 4	Info	128
8	192.168.80.1	local 4	Notice	75
9	192.168.80.1	local 4	Warning	11

Slika 9: Statistika po ozbiljnosti

Statistika po danima u tjednu je vidljiva na slici 10.

	A	B	C	D	E	F	G	H
1	Ip	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
2	11.11.11.11	1	0	0	0	0	0	0
3	192.168.0.1	1	0	0	0	0	0	0
4	192.168.5.105	87	0	0	0	0	0	0
5	192.168.80.1	227	0	0	0	28	0	0

Slika 10: Statistika po danima u tjednu

Statistika po IP adresi izvora syslog poruke je vidljiva na slici 11.

	A	B	C	D	E	F
1	ID	Collected	IP	Facility	Severity	Message
2	63	21-06-19 12:13	192.168.80.1	local 4	Info	%ASA-6-106015: Deny TCP (no connection) from 192.168.60.5/49752 to 23.6.112.155/80 flags PSH ACK on interface inside
3	64	21-06-19 12:13	192.168.80.1	local 4	Info	%ASA-6-302020: Built outbound ICMP connection for faddr 8.8.8.8/0 gaddr 192.168.137.2/1 laddr 192.168.5.105/1
4	65	21-06-19 12:13	192.168.80.1	local 4	Info	%ASA-6-302021: Teardown ICMP connection for faddr 8.8.8.8/0 gaddr 192.168.137.2/1 laddr 192.168.5.105/1
5	66	21-06-19 12:13	192.168.80.1	local 4	Info	%ASA-6-106015: Deny TCP (no connection) from 192.168.60.5/49745 to 23.6.112.155/80 flags PSH ACK on interface inside
6	67	21-06-19 12:13	192.168.80.1	local 4	Info	%ASA-6-302020: Built outbound ICMP connection for faddr 8.8.8.8/0 gaddr 192.168.137.2/1 laddr 192.168.5.105/1
7	68	21-06-19 12:13	192.168.80.1	local 4	Info	%ASA-6-302021: Teardown ICMP connection for faddr 8.8.8.8/0 gaddr 192.168.137.2/1 laddr 192.168.5.105/1
8	69	21-06-19 12:13	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c
9	70	21-06-19 12:13	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c
10	71	21-06-19 12:13	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c
11	72	21-06-19 12:13	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c
12	73	21-06-19 12:13	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c
13	74	21-06-19 12:13	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c
14	75	21-06-19 12:13	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c
15	76	21-06-19 12:13	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c
16	77	21-06-19 12:13	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c
17	78	21-06-19 12:14	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c
18	79	21-06-19 12:14	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c
19	80	21-06-19 12:14	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c
20	82	21-06-19 12:16	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c
21	83	21-06-19 12:16	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 93.184.221.240:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am_c

Slika 11: Statistika po IP adresi

Statistika za određeni vremenski period je prikazana na slici 12.

	ID	Collected	IP	Facility	Severity	Message
165	227	24-06-19 17:18	192.168.5.105	system	Notice	7036: The Optimize drives service entered the running state.
166	229	24-06-19 17:18	192.168.5.105	system	Notice	4672: AUDIT_SUCCESS Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logo
167	230	24-06-19 17:18	192.168.80.1	local 4	Info	%ASA-6-106015: Deny TCP (no connection) from 192.168.60.5/49905 to 23.6.112.155/80 flags PSH ACK on interface inside
168	231	24-06-19 17:18	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 23.6.112.145:http://download.windowsupdate.com/d/msdownload/update/others/2019/06/29314809_22efa9
169	232	24-06-19 17:18	192.168.80.1	local 4	Critical	%ASA-2-106001: Inbound TCP connection denied from 205.185.216.42/80 to 192.168.60.5/49742 flags ACK on interface outside
170	233	24-06-19 17:18	192.168.80.1	local 4	Critical	%ASA-2-106001: Inbound TCP connection denied from 205.185.216.42/80 to 192.168.60.5/49742 flags ACK on interface outside
171	234	24-06-19 17:19	192.168.80.1	local 4	Info	%ASA-6-106015: Deny TCP (no connection) from 192.168.60.5/49821 to 204.79.197.200/443 flags ACK on interface inside
172	235	24-06-19 17:19	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 205.185.216.42:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am
173	236	24-06-19 17:19	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 205.185.216.42:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am
174	237	24-06-19 17:19	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 205.185.216.42:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am
175	238	24-06-19 17:19	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 205.185.216.42:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am
176	239	24-06-19 17:19	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 205.185.216.42:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am
177	240	24-06-19 17:19	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 205.185.216.42:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am
178	241	24-06-19 17:19	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 205.185.216.42:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am
179	242	24-06-19 17:19	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 205.185.216.42:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am
180	243	24-06-19 17:19	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 205.185.216.42:http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/06/am
181	244	24-06-19 17:19	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 99.86.243.117:http://www.snmpsoft.com/downloads/SyslogWatcherSetup.vern
182	245	24-06-19 17:19	192.168.80.1	local 4	Error	%ASA-3-305006: regular translation creation failed for icmp src inside:192.168.60.5 dst outside:8.8.8.8 (type 3, code 3)
183	246	24-06-19 17:19	192.168.80.1	local 4	Info	%ASA-6-302020: Built outbound ICMP connection for faddr 8.8.8.8/0 gaddr 192.168.137.2/0 laddr 192.168.60.5/0
184	247	24-06-19 17:19	192.168.80.1	local 4	Info	%ASA-6-302021: Teardown ICMP connection for faddr 8.8.8.8/0 gaddr 192.168.137.2/0 laddr 192.168.60.5/0
185	248	24-06-19 17:19	192.168.80.1	local 4	Notice	%ASA-5-304001: 192.168.60.5 Accessed URL 99.86.245.201:http://o.ss2.us//MEowSDBGMEQwQjAJBgUrDgMCGgUABBSLwZ6EW5gdYc9UaSEaaLjJETNtkAQUv1

Slika 12: Statistika za određeni vremenski period

Na slici 13. je prikazana statistika po godini, mjesecu i danu.

	A	B	C	D
1	Year	Month	Day	BrojPoruka
2	2019	5	31	4
3	2019	6	21	29
4	2019	6	24	316
5	2019	6	28	28

Slika 13: Statistika po godini, mjesecu i danu

Za kraj, statistika po satima u danu je prikazana na slici 14.

	A	B	C	D
1	hour	192.168.0.1	192.168.5.105	192.168.80.1
2	11	1	0	0
3	12	0	2	27
4	16	0	4	0
5	17	0	53	141
6	19	0	34	86

Slika 14: Statistika po satima u danu

4 ZAKLJUČAK

Cilj izrade prikazanog završnog rada bila je implementacija Syslog Watcher programske podrške za prikupljanje, pohranu i analizu syslog zapisa.

Ova tema je odabrana kao tema završnog rada zbog toga što se u današnjem svijetu, razvojem tehnologije, samog interneta i sve strojne opreme vezane uz računarstvo, javlja sve veća potreba za jednostavnim praćenjem mreže budući da je internetski promet svakog dana sve veći. Uz pomoć Syslog Watcher paketa, sistem inženjer ili mrežni administrator može u bilo kojem trenutku vidjeti kakvo je stanje na mreži, postoji li uređaj na mreži koji stvara probleme ili postoji nekakav sigurnosni rizik. Sigurnosni rizik predstavljaju osobe koje žele neovlašteno ući u sustav i uzeti podatke ili načiniti štetu samoj mreži, a isto tako I korisnici koji posjećuju stranice koje nisu pouzdane

Mjesta na kojima se ovaj rad može primijeniti su sve one ustanove koje imaju neki vid unutarnje mreže, odnosno intraneta koje pristupaju vanjskoj mreži, internetu, preko određenih mrežnih uređaja (usmjernika, vatrozida i slično). Na ovaj način, implementirani programska podrška daje osobi zaduženoj za mrežu podatke o prometu na mreži na jednom mjestu, bez provjeravanja svakog uređaja zasebno.

Može se zaključiti kako je Syslog Watcher programska podrška jako dobar alat koji je olakšao život mnogim ljudima koji se bave mrežama i osigurao lakši i brži pronalazak problema i njegovo rješavanje. Isto tako, uvjeren sam da će se uz razvoj tehnologije smanjiti broj grešaka na uređajima i povećati njihova sigurnost te tako smanjiti intervencije ljudi odgovornih za pravilan rad mreže.

LITERATURA

[1] Listeš, T.: Projektiranje i upravljanje računalnim mrežama; „Šesto poglavlje“ (posjećeno 6.9.2019.).

[2] Stackify, „Syslog tutorial: How it works, Examples, Best Practices, and More ,“ https://stackify.com/syslog-101/ (posjećeno 6.9.2019.)

[3] Ciberseguridad.blog, „Soluciones open source para la gestíon de logs en ciberseguridad,“ https://ciberseguridad.blog/soluciones-open-source-para-la-gestion-de-logs-en-ciberseguridad/ (posjećeno 6.9.2019.)

[4] Network Admin Tools, „Top Syslog Server Software Free & Paid for Windows,“ https://www.netadmintools.com/syslog-server (posjećeno 6.9.2019.)

[5] iTT Systems, „What is Syslog? A Quick Overwiev of Event Logging Protocol,“ https://www.ittsystems.com/what-is-syslog/ (posjećeno 6.9.2019.)

[6] WhatsUp Gold, „Event Log Management for Security and Compliance,“ https://www.whatsupgold.com/best-practices/event-log-management/4/#1562951025462-69a895c1-64fe (posjećeno 6.9.2019.)

[7] TechGenix, „Configuring a Syslog Agent in Windows Server 2012,“ http://techgenix.com/configuring-syslog-agent-windows-server-2012/ (posjećeno 6.9.2019.)

[8] SANS Institute Information Security Reading Room, „The Ins and Outs of System Logging Using Syslog,“ https://www.sans.org/reading-room/whitepapers/logging/paper/1168 (posjećeno 6.9.2019.)

[9] Geek University, „syslog protocol explained,“ https://geek-university.com/linux/syslog-protocol-explained/ (posjećeno 6.9.2019.)

[10] Carnet, „Implementacija syslog protokola u Windows okruženju,“ https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2005-05-120.pdf (posjećeno 6.9.2019.)

[11] Business Support, „What are Syslog Facilities and Levels?,“ https://success.trendmicro.com/solution/TP000086250-What-are-Syslog-Facilities-and-Levels (posjećeno 6.9.2019.)

[12] Cisco, „How to configure logging in Cisco IOS,“ https://community.cisco.com/t5/networking-documents/how-to-configure-logging-in-cisco-ios/ta-p/3132434 (posjećeno 6.9.2019.)

[13] GNS3, „Documentation,“ https://docs.gns3.com/ (posjećeno 6.9.2019.)

[14] Syslog Watcher, „Syslog Watcher, “ : https://syslogwatcher.com/ (posjećeno 6.9.2019.)

[15] Cisco, „Cisco Adaptive Security Appliance (ASAv) Data Sheet,“ https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/datasheet-c78-733399.html (posjećeno 6.9.2019.)

[16] WhatIs MyIPAddress, „What is Network Address Translation“ https://whatismyipaddress.com/nat (posjećeno 6.9.2019.)

[17] Google Code, „eventlog-to-syslog,“ https://code.google.com/archive/p/eventlog-to-syslog/downloads (posjećeno 6.9.2019.)

[18] Solarwinds customer success, „Kiwi Syslog logs to store with SQL database setup screen shots,“ https://support.solarwinds.com/Success_Center/Kiwi_Syslog_Server/Knowledgebase_Articles/Kiwi_Syslog_logs_to_store_with_SQL_database_setup_screen_shots (posjećeno 6.9.2019.)

[19] Youtube, „Call Stored Procedure with multiple parameters from Excel,“ https://www.youtube.com/watch?v=dfySPaBQwSk (posjećeno 6.9.2019.)

I Z J A V A

O AKADEMSKOJ ČESTITOSTI

Ja, Roko Grubić , 0009075115

(ime i prezime studenta) (matični broj studenta/JMBAG)

izjavljujem

da je moj završni rad pod naslovom

Implementacija Syslog Watcher programske podrške za prikupljanje, pohranu i analizu syslog poruka

rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Nijedan dio ovoga rada nije napisan na nedopušten način, odnosno nije prepisan bez citiranja i ne krši ičija autorska prava.

Izjavljujem da nijedan dio ovoga rada nije iskorišten u ijednom drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga rada.

Split, _____

Student _____

(potpis)