UNIVERZITET SINGIDUNUM

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE I MEĐUNARODNU SARADNJU

MASTER RAD

Studijski program: SAVREMENE INFORMACIONE TEHNOLOGIJE

Tema: Softverska firewall tehnologija u funkciji zaštite računarskog sistema

Mentor: prof. dr Zoltan Jegeš Student: Kaćanski Tihomir

Broj indeksa: 2012/410385

Beograd,_____ 2013.

SADRŽAJ

Uvod: 6

1. Metodologija naučnog istraživanja 8

1.1 Uvodne napomene i obrazloženje rada: 8

1.2 Predmet istraživanja 9

1.3 Ciljevi i zadaci istraživanja 9

1.4 Hipotetički okvir istraživačkog rada 10

1.5 Metode i tehnike istraživačkog procesa 11

1.6 Struktura rada 12

2. Zašto koristiti firewall ? 13

2.1 Tri najosnovnije funkcije firewall-a 15

2.1.1 Filtriranje paketa 15

2.1.2 NAT (Network Address Translation) – prevod mrežnih adresa 17

2.1.3 Proxy servisi 18

3. Osnovne firewall konfiguracije 19

3.1 Dual-Homed Gateway – međusistemski firewall 19

3.2 Screened host gateway – zaklonjeni firewall 20

3.3 Virtuelne privatne mreže (VPN - Virtual Private Networks) 21

3.4 Konfiguracija mreže bez servera 22

3.5 Konfiguracija mreže sa jednim serverom i jednim firewall-om 22

3.6 Konfiguracija mreže sa jednim serverom i dva firewall-a 23

3.7 Konfiguracija mreže sa demilitarizovanom zonom 24

3.8 Firewall-i zasnovani na hostu 26

3.9 Mreža zasnovana na firewall-u 27

4. Hardverski firewall sistemi 27

5. Softverski firewall sistem 28

6. Politika zaštite i skup pravila firewall-a 29

6.1 Pisanje firewall pravila 29
7. Hardverski ili softverski firewall - poređenja 30
7.1 Ključne prednosti hardverskog firewall-a : 31
7.2 Ključne prednosti softverskog firewall-a : 31
7.3 Poređenje softverskog i hardverskog firewall-a : 31
8. Socijalne i tehnološke prednosti firewall-a 32
9. Buduće generacije hardverskog i softverskog firewall-a 33
9.1 Hardverski firewall - budućnost 34
9.2 Softverski firewall - budućnosti 36
10. Poređenja, karakteristike i tehnološke novine firewall-a 38
10.1 Comodo Personal Firewall 2.0.0.0 40
10.2 Agnitum Outpust Pro Firewall 43
10.3. McAfee Firewall 47
10.4 Norton 360 Firewall 49
10.5 ZoneAlarm Pro Firewall 6.1 52
11. Programi za testiranje firewall-a: 54
11.1 Test programi (Matousec, 2013) 57
11.1.1 Testirani firewall: Comodo Personal Firewall 2.0.0.0 61
11.1.2 Testirani firewall: Agnitum Outpust Pro Firewall 62
11.1.3 Testirani firewall: McAfee Firewall 64
11.1.4 Testirani firewall: Norton 360 Firewall 66
11.1.5 Testirani firewall: ZoneAlarm Pro Firewall 6.1 67
12. Događaji tokom testiranja 69
13. Kriterijumi sotverskog firewall-a 70
13.1 Konfiguracija računara gde su testirani programi: 70
13.2 Najosnovniji kriterijumi kod firewall-a: 71
Zaključak: 76

Literatura: 78

Popis slika: 81

Popis tabela:.....82

SOFTVERSKA FIREWALL TEHNOLOGIJA U FUNKCIJI ZAŠTITE RAČUNARSKOG SISTEMA

Sažetak:

Računarska mreža tj. internet mreža služi za povezivanje, komunikaciju, prodaju. Ova mogućnost se koristi za zastrašivanje i manipulaciju velikih ljudskih masa. Možemo da konstatujemo da se kompjuterski kriminal može podeliti na različite nivoe zloupotrebe. Misli se na internet kriminal, kriminal u elektronskom poslovanju, kriminal u mrežnim komunikacijama. Svaki od ovih oblika treba da zaokupi pažnju pravnih organa i vremenom da se spreči njegovo širenje na društvo. Veliki napori treba da se ulože u razvoj novih tehnologija i da se obezbedi sigurniju budućnost računarskih sistema. U ovom radu opisana je zaštite računarskih sistema pomoću firewall tehnologije. Gde će kroz rad biti detaljno objašnjeno korišćenje firewall-a, poređenja i testiranja različitih softverskih firewall-a. Čak i uz dobar firewall, još uvek je potrebno koristiti antivirusni i anti-spyware program. Firewall-i se mogu kombinovati sa antivirusnim programima, malware i spyware programima. U slučaju većih računarskih mreža i više korisnika poželjno je imati instaliran vatreni zid u računarskom sistemu. Bez obzira na to koji tip vatrenog zida izaberemo, jedno je sigurno, ako se spojite na Internet sa računara ili laptopa, potrebnon je imati firewall zaštitu. Kako firewall tehnologija zadržava uljeze, viruse i tako štiti podatke, ne korišćenjem vatrenog zida dovodimo računarski sistem u stanje slobodnog napada. Čak i ako nemamo ništa vredno za zaštitu postajemo meta neželjenih korisnika. Vatreni zid bi trebao biti prva linija odbrane kada je u pitanju kompjuterska sigurnost, ali nipošto ne bi trebala biti samo zaštita.

Ključne reči:

Softverski firewall, filtriranje paketa, proxy servisi, malware kod, konfiguracija firewall-a, virtuelna privatna mreža, testirani programi, kriterijumi firewall-a, demilitarizovana zona.

SOFTWARE FIREWALL TECHNOLOGY IN ORDER TO PROTECT A COMPUTER SYSTEM

Abstract:

Computer network or internet network is used to connect, communicate, sell, etc. This asset serves for intimidation and manipulation of the masses. It can be ascertained that computer crime can be divided into different levels of abuse. We are talking about internet crime, crime in electronic banking, abuse of network communication. Every type should get the attention of the right departments and they should put a stop to their spreading in society. Huge effort should be invested in the development of new technologies and to provide a safer future for computer systems.

The protection of computer systems with the help of firewalls is described in this work. The use of firewalls, comparison and testing of different software firewalls will be explained in full detail. Even with a good firewall, antivirus and anti-spyware programs should still be applied.

Firewalls can be combined with antivirus programs, malware and spyware programs. In case of bigger computer networks and multiple users it's desirable to have an installed firewall in the computer system. No matter which type of firewall we choose, one thing is sure – if we connect to the internet from a PC or laptop, it's necessary to have a firewall protection. Since the firewall technology protects data by keeping intruders, viruses out, not using one will put our computer system at risk of free attack. Even if we haven't got anything valuable to protect, we become targets of unwanted users. Firewall should be the first line of protection when it comes to computer security but it shouldn't be the protection itself.

Key words:

Software firewall, packet filtering, proxy services, malware code, configuration firewall, virtual private network, tested programs, criteria firewall, demilitarized zones.

Uvod:

Kompjuteri danas imaju veliku primenu u komunikaciji ljudi pa su zato i postali neizbežna potreba ljudi. [•] (Ragnarsson, 2010) Iz tog razloga određena grupacija ljudi pokušava da sruši sistem zaštite i onemogući njihovo korišćenje. Ovo je ozbiljan problem u budućnosti i smešten je odmah posle organizovanog kriminala i terorizma. Naravno, da se ova priča ne bi razvijala u složeniji problem sadašnjice, velike svetske kompanije poput Microsofta i drugih firmi softvera i hardvera pokušavaju da spreče zloupotrebu nad njihovim proizvodima. Priključivanjem računarskog sistema na Internet bez adekvatne zaštite otvorili smo vrata neželjenim gostima da pristupe u naš računarski sistem. [•] (Cheswick, 2003) Da bi korisnici internet usluga obezbedili svoje računarske sisteme potrebno je instalirate neke od tehnologija zaštite.

Postoji više sistema zaštite računarskih sistema, najpoznatije tehnologije zaštite su pomoću antivirusnih programa, pomoću *firewall*-a, pomoću NAP-a (pristup mreži), pomoću sistema za detekciju upada, pomoću autentifikacije, pomoću kriptografije podataka i td. Svaka od ovih tehnologija je dobra za zaštitu ako se postavi na adekvatan i stručan način. Korisnici se često nalaze u dilemi koju tehnologiju zaštite izabrati. Potrebno je odabrati tehnologiju zaštite koja se nalazi prva na udaru neželjenih posetilaca, malicioznog koda, a da se pri tome ne uspe probijanje računarski sistem. [•] (Gollmann, 2011)

Izvorno značenje termina "zaštitni zid" potiče od engleske reči "firewall" što znači " vatreni zid". Računarski vatreni zidovi su kreirani tako da blokiraju neželjeni saobraćaj sa Interneta. [•] (Cameron, 2005) Svaki put kada se upotrebi internet pregledač (web browser), programi za pregled elektronskih poruka ili neki od programa sa kojima se može pristupiti Internetu tada svi podaci se kreću preko računarskih portova, internet provajdera ili sa udaljenog servera. Bez obzira na to da li je u pitanju haker koji pokušava da pristupi računaru ili špijunski program koji

---

- Ragnarsson, P. (2010). *Firewall implementation and testing. .* Sweden: Linkpings universitetet.
- Cheswick, W. R. (2003). *Firewalls and Internet Security, Second Edition. .* Boston: AT&T and Lumeta Corporation.
- Gollmann, D. (2011). *Computer Security.* United Kingdom: John Wiley & Sons.
- Cameron, R. (2005). *Configuring NetScreen Firewalls.* Rockland: Syngress Publishing.

pokušava da komunicira s udaljenim serverom, strategija je ista, pronaći otvoreni priključak koji vodi u računar. Zaštitni zidovi vode računa o hiljadama takvih priključaka koji postoje i u širokopojasnim i u modemskim vezama i onemogućavaju neautorizovan saobraćaj. Softverski zaštitni zidovi rade na računaru. Hardverski zaštitni zidovi su obično integrisani u usmerivače i mrežne prolaze i nalaze se između računara i kablovskog ili DSL modema, i odlični su za zaštitu mreže računara koji dele širokopojasnu vezu.[•] (Spanbauer, 2003)

Ukoliko je računar spojen na Internet direktno, preko telefonske linije ili bežičnim putem s time on postaje deo velike računarske mreže. Pritom se dodeljuje računaru adresa internet protokola s kojom svaki računar na mreži ima pristup do računara. Svaki računar na Internetu, mail server, web server ili drugi vid servera može u sebi da sadrži neki vid malicioznog koda s kojima mogu da zaraze i ostale računare na mreži. Takvi programi nastoje da ne odaju svoje prisustvo i po prirodi tajno prikupljaju email adrese, lozinke, kupovne navike, adrese posećenih sajtova i slične podatke koji su vrlo vredni zlonamernim stranama.[•] (Kompjuterska.biblioteka, 2007)

Svaki od tehnologija ima svoje prednosti i mane, ali kod firewall-a preovlađuju svakako dobre osobine, jer svaki proizvođač hardvera ili softvera pokušava da unapredi svoje proizvode do najviših mogućnosti, ali mesta za rizik ne sme da bude. Firewall je kao zaštitni sloj svakako koristan za računarski sistem ali isto tako i neophodan za nesmetan dalji rad ostalih tehnologija zaštite. I kao takav vatreni zid mora da bude najstabilniji bedem na putu dospeća poruka. Svi ostali slojevi zaštite se nalaze posle firewall-a. Svaki vid komunikacije mora proći preko firewall-a. Odabitom ove tehnologije korisniku se pruža mogućnost nadogradnje i kombinacije sa ostalim tehnologijama zaštite.

[•] Spanbauer, S. (2003, Decembar). *Mrežna bezbednost: kako instalirati zaštitni zid*. Retrieved from mikro.rs: http://www.mikro.rs/main/tekstprint.php?tekstID=4159

1. Metodologija naučnog istraživanja

1.1 Uvodne napomene i obrazloženje rada:

U današnje vreme možemo slobodno konstatovati da ni jedan računarski sistem nije 100% bezbedan od zlonamernih korisnika. Zato se velike kompanije i pribojavaju za bezbednost podataka. Brzim razvojem Internet usluga šire se i pretnje sa Interneta koje uzurpiraju sigurnost kompjuterskim korisnicima. Stavljanjem zabrane na svaki računar, pa čak i elektronskih medija (DVD, e-knjige, itd.) dolazi do nepoverenja i izazivanja na upad zlonamernih korisnika.[•] (Denning, 1990) Vlasnici informacija koji pokušavaju zadržati nešto ili osigurati svoju imovinu ulažu u svoju kompjutersku sigurnost tj. u nove tehnologije koje su svakim danom sve savršenije, ali u funkciji predstavljaju dobru metu za hakere. Danas, kako se širi era Interneta, sa njom raste i potreba za računarima, a budući da se danas svugde koriste kompjuteri, pojedinci su se dosetili da bi mogli da iskoriste nečiju slabost i zloupotrebe sadržaj na kojem mogu da profitiraju. Uvek će postojati mrtva trka sa onima koji ulažu u nove tehnologije i one koji te tehnologije žele da sabotiraju.

Danas se napadaju servisi velikih kompanija i vladinih ili nevladinih organizacija i menja se njihov sadržaj. Krade se svaka informacija, podatak koji može da naškodi domaćinu sajta ili se uništava cela mreža, a sa njom povlači i računarski sistem. Postoje različite metoda da se onesposobe funkcionalnosti njihovog rada, ubacivanjem različitih malicioznih programa ili se prepravljaju informacije u netačne i lažne. Koriste se različite vrste upada u sistem, najčešće dobro opremljeni računari sa velikom brzinom i dobro osposobljeni hakeri, koji kreiraju programe za uznemiravanje i uzurpiranje, koriste slabosti računarskih sistema. Naša najveća briga jeste to što se ovakvi napadi teško pronalaze i suzbijaju, jer ovako spretni pojedinci menjaju svoje lokacije iz dana u dan i predstavljaju veliki problem za organe reda.[•] (Casey, 2011)

[•] Denning, P. J. (1990). *Computers Under Attack: Intruders, Worms, and Viruses.* ADDISON WESLEY.

[•] Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* San Diego: Elsevier.

1.2 Predmet istraživanja

U ovom radu predmet istraživanja je kako zaštititi računarski sistem pomoću firewall tehnologije, pomoću kojih se sve tehnika, metoda i alata može sprečiti neželjeni ulazak u sistem. Rad je predstavljen pomoću nekoliko softverskih aplikacija koje imaju zadatak da zaštite rad korisnika u mreži i predstavljena su rizična mesta u računarskom sistemu koja se mogu probiti. Testiranjem softverskog firewall-a prikazuju se potencionalne pretnje koje mogu da ugroze rad programa i pomoću malicioznih test programa podiže se svest kod korisnika da uvidi koliko je njegov računarski sistem ranjiv.

1.3 Ciljevi i zadaci istraživanja

Glavni cilj ovog rada je da se prikaže tehnologija zaštite računarskih sistema pomoću firewall tehnologije i da se kroz različite konfiguracije firewall-a prikaže odbrana sistema. Korišćenje različitih tehnika, alata, metoda i testiranje softverskog firewall-a.

Konkretan cilj ovog istraživanje je pronalaženje odgovora na pitanja:

Čemu služi firewall tehnologija?
Koje su njene osobine i mogućnosti?
Kako se zaštiti pomoću ove tehnologije?
Koji se alati koriste za zaštitu?
Dali je ova tehnologija pouzdana za naš računarski sitem?
Za koji se firewall odlučiti i zašto?
Ima li firewall svoju budućnost u IT svetu?

Društveni cilj istraživanja jeste da se dokaže praktična primena i da se potvrdi koliko je neophodna firewall tehnologija u računarskom sistemu. Kako se kompjuterski kriminal sve više širi u informatičkom svetu i informacija je ključan dokaz za uspešnost poslovnja, iz ovih razloga je zaštita informacije važna pa je i primena ove tehnologije interesantna za dalja istraživanja i praćenja.

1.4 Hipotetički okvir istraživačkog rada

Generalna hipoteza rada je: kako se svakim danom globalna mreža sve više širi tako postaje potreba za zaštitom računarskih sistema, jer svakim je danom sve više zlonamernih korisnika. Ukoliko želimo da zaštitimo računarski sistem potrebno je postaviti firewall tehnologiju na ona mesta koja bi bila prvi odbrambeni sistem protiv pomenutih korisnika. Postavljanjem vatrenog zida smanjuje se rizik upada u računarski sistem, a povećava se nivo bezbednosti.

Posebne hipoteze rada su: ako neželjeni korisnik želi da pristupi računarskoj mreži može da pokuša na nekoliko načina:

- Ulazak se može izvesti preko Interneta i to preko različitih protokola gde se oslobađa prolaz preko njih.
- Potencijalni ulazak se može očekivati i preko e-mail poruka koje u sebi takođe mogu da sadrže maliciozne programe.
- Napad se ne mora samo izvršiti izvan računarske mreže već se isto tako može očekivati napad sa unutrašnje strane mreže.
- Od pomenutih razloga svaka je na svoj način kompleksna za analizu, ali isto tako nije ne moguća da se zaustavi napad i prati dalji tok istraživanja.

Pojedinačne hipoteze rada su:

Potencijalni napad preko Interneta vreba sa različitih protokola kao na primer sa TCP[1], UDP[2], ICMP[3] HTTP[4], FTP[5] i SMTP[6] protokola, na kojima je stavljen poseban akcenat na dalja istraživanja i pokušaj da se spreči napad. Slanjem atačment poruka omogućava se prenošenje malicioznih fajlova koje treba sprečiti ali isto tako razviti sistem za njihovo filtriranje. Korisnik unutar računarske mreže može da postavi

---

[1] Transmition control protocol je protokol koji pripada *sloju 4 OSI* referentnog modela, ima za ulogu da obezbezbedi pouzdan transfer podataka u *IP* okruženju.
[2] *User Datagram Protocol* je jednostavan protokol koji obezbeđuje osnovne funkcije transportnog sloja OSI modela
[3] *Internet Control Messageing Protocol* je protokol sloja mreže koji obezbeđuje pojedine mehanizme oglašavanja.
[4] HTTP (*engl.* HyperText Transfer Protocol) je mrežni protokol koji pripada sloju aplikacije OSI referentnog modela
[5] FTP (*engl.* File transfer protocol) – protokol za prenos datoteka) je najčešće korišćen protokol za prenos podataka između dva računara na mreži.
[6] SMTP (*engl.* Simple Mail Transfer Protocol) predstavlja osnovni protokol sloja aplikacija za elektronsku poštu

maliciozni kod i poremeti rad firewall-a, moguće je ako firewall nije pravilno konfigurisan. Softverski firewall-i su izloženi testiranju kako bi se ustanovili mogući nedostaci u konfiguraciji samog vatrenog zida.

1.5 Metode i tehnike istraživačkog procesa

Budućnost firewall leži između nivoa mrežnih firewall-a i na aplikativnom nivou firewal-a. Vrlo je verovatno da će na mrežnom nivou firewall postati sve "zahtevniji" od informacija koje prolaze kroz njih, ali i aplikacijski firewall-i će postati sve transparentniji. Krajnji rezultat treba da bude brza provera paketa koji prolaze kroz sistem. Sve vrste firewall-a (mrežni i aplikativni sloj) uključujući i enkripciju, moraju zaštititi promet koji prolazi između njih preko Interneta. Dalja istraživanja će se sprovoditi ka softverskim firewall-ima, njihovo međusobno upoređivanje i dokazivanje koji od njih je najkompletniji program koji ispunjava sve uslove gore navedene. Kao što su filtriranje paketa, autentifikacija, provera protiv virusa, blokiranje internet saobraćaja.

Metoda naučnog istraživanja je ponovljivi proces, kritički, sistematski, kontrolisani za sticanje novih znanja potrebnih u rešavanju naučnih problema. U naučnom istraživanju glavni principi su :

- sistematičnost - dobra uređenost istraživanja i obezbeđivanje prirodnog i logičkog sleda procesa
- kontrolisanost - sprovođenje istraživanja u što moguće boljim i kontrolisanim uslovima, kako bi se isključila alternativa rešenja
- kritičnost - sve važne tvrdnje o pojavama, procesima, odnosima i svojstvima moraju se ozbiljno, iskreno i strogo procenjivati, proveravati i obrazložiti

Na osnovu podele naučnog istraživanja prema prirodi istraživanja na teorijska i empirijska, prema cilju istraživanja na fundamentalna i primenjena i prema funkciji istraživanja na eksplorativna i usmerena na proveravanje hipoteze, u ovom radu primenjena su uglavnom fundamentalna, primenjena i istraživanja usmerena na proveravanje hipoteze.[•] (Miljević, 2007) Fundamentalna istraživanja primenjena su radi sticanja novih znanja o ovoj oblasti, a primenjena i istraživanja usmerena na

[•] Miljević. (2007). *Metodologija naučnog rada.* Sarajevo: Filozofski fakultet.

proveravanje hipoteze radi sticanja novih znanja i rešavanje hipotezom postavljenih zadataka u ovom radu.

Metodološki pristup istraživanja postavljen je veoma kompleksno i zahtevao je primenu :

- analitičkih osnovnih metoda: metod analize, metod apstrakcije, metod specijalizacije i metod dedukcije;
- sintetičkih osnovnih metoda: sinitezu, konkretizaciju, generalizaciju i indukciju;
- opšte naučnih metoda: hipotetičko - deduktivnu, analitičko - deduktivnu, komparativnu, statističku i metodu modelovanja.

Kao tehnika prikupljanja podataka koriste se izbor i selekcija dostupnih literaturnih i Internet izvora, analiza dokumenata na primarnom i sekundarnom nivou, kao i studija slučaja, anketa i ispitivanja. Pregled literature u oblasti komputerske sigurnosti, firewall tehnologija, zaštite računarskih sistema i ostalih srodnih tema.

1.6 Struktura rada

Sistem postavljenih hipoteza i ciljevi istraživanja odredili su sledeću strukturu rada:

- U prvom delu rada objašnjena je metodologija istraživanja naučnog rada, predmet istraživanja, ciljevi i zadaci, hipoteza istraživačkog rada, metode, tehnike i tok istraživanja.
- U drugom delu rada objašnjena je teza čemu služi firewall i koji su njegovi najosnovniji delovi za otkrivanje i sprečavanje ulaska u sistem.
- U trećem delu rada je objašnjene su različite vrste konfiguracija i tipova postavljanja firewall tehnologije.
- U četvrtom delu rada je objašnjen je hardverska vrsta firewall-a, njegova primena , konfiguracija i namena.
- U petom delu rada je objašnjena upotreba softverskog firewall-a, način njegove upotrebe i namena.
- Šesti deo rada je posvećen za prikaz pisanja firewall pravila i njihovo integrisanje u firewall konfiguracije. Politika zaštite je deo uspešnosti funkcionisanja vatrenog zida tako da je i ovo deo pristupnog rada.
- Sedmo poglavlje je namenjeno za upoređivanje hardverskog i softverskog firewall-a, kao i budućnost firewall-a koji tek treba da stupe na informatičku

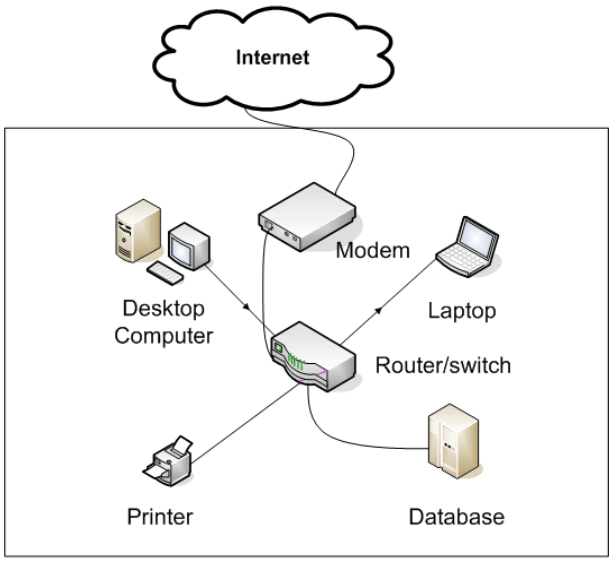
scenu. Stavljen je akcenat na upoređivanje najpoznatijih kompanija koje proizvode uređaje i aplikacije za kreiranje vatrenog zida, njihovo viđenje budućnosti u kojoj će se dalje razvijati.

- Osmi deo rada se bavi sociološkim i tehnološkim pitanjima firewall-a. Koje su prednosti s kojima firewall raspolaže kako bi ga korisnik mogao iskoristiti za odbranu svog računarskog sistema.
- Deveto poglavlje se bavi budućim generacija firewall-a. Softverski i hardverski firewall-i su objašnjeni sa novinama kojim proizvođači vatrenih zidova ugrađuju u svoje proizvode.
- U desetom poglavlju su objašnjeni najpoznatiji softverski firewall-i. Poređenja, karakteristike, tehnološke novine i izgled svakog programa je objašnjeno u ovom delu rada.
- Jedanaesto poglavlje se bavi testiranim programima koji imaju za zadatak da ugroze računarski sistem različitim zlonamernim kodom. Svi testovi su sprovedeni na softverskim firewall-ima sa objašnjenim reakcijama posle testiranja.
- Dvanaesto poglavlje se bavi događajima koji su se događali tokom testiranja na svakom od vatrenih zidova. Moguće reakcije operativnog sistema, programa i analiza štete koja je nastala tokom pokretanja test programa dok se testirao firewall.
- Trinaesto poglavlje opisuje kriterijume koji treba da budu deo softverskog firewall-a i s kojima proizvođač treba da izađe na tržište.

2. Zašto koristiti firewall ?

Firewall je zaštitni sigurnosni sistem koji je smešten između lokalne i javne mreže tj. Interneta, njegova uloga je da zaštiti poverljive podatke od neautorizovanih korisnika tako što će zabraniti i blokirati upad u sistem. Postavkom firewall-a može se kontrolisati protok podataka i određivati pristup korisnicima na delovima računarske mreže. Samim tim firewall je jedan od dobrih rešenja za kreiranje virtuelne privatne mreže jer se stvara virtualni prolaz za kriptovane podatke. Firewall se koristi na serverima gde internet korisnici mogu da pristupe određenim podacima, a on ima ulogu da brine i o sistemskim i drugim fajlovima koji su važni za rad računara. Zaštita

firewall-om može biti hardverska ili softverska zaštita koja omogućava TCP/IP[7] komunikaciju između dve tačke u računarskoj mreži. Na ovaj način se može kontrolisati protok saobraćaja i sprečava se konekcija na Internet da ne bi došlo do infekcije računara. Filtracija TCP/IP paketa može se vršiti na nekoliko nivoa i to ispitivanjem sadržaja poruke, ispitivanjem lokacije sa koje je poruka pristigla u smislu IP adrese i ispitivanjem porta računara. • (Brian Komar, 2003)



Slika 1 – mreža bez firewall-a

Firewall se sastoji iz nekoliko osnovnih metoda zaštite:

• filtriranje paketa (packet filtering) - odbija se pristup TCP/IP paketa koji pristižu sa neautorizovanih stanica i servisa

• NAT (Network Address Translation) - metod koji prevodi IP adrese sa unutrašnjih i spoljašnjih adresa i omogućava pristup unutrašnjim hostovima Internetu.

• proxy servisi - metod koji omogućava pristup servisima na javnim serverima.

• kriptovana autentifikacija - omogućava korisnicima da sa spoljašnje mreže mogu da pristupe unutrašnjoj mreži, ali samo ako izvrše identifikaciju.

• podrška za virtualne privatne mreže ili VPN (Virtual Private Networking) - tehnologija koja uspostavlja vezu sa Internetom i virtuelnom privatnom mrežom

• skeniranje virusa - mogućnost da se vrši skeniranje dolaznih podataka da bi se otkrili i uklonili virusi.

---

[7] ***TCP/IP***-najstariji mrežni standard. Koristi ga 50% svih instaliranih BN,MAN i WAN mreža. Vrši funkcije transportnog nivoa u OSI modelu.

• Brian Komar, R. B. (2003). *Firewalls for Dummies 2nd Edition.* Indianapolis: Wiley Publishing.

• filtriranje sadržaja (content filtering) - mogućnost filtriranja sadržaja kojem se pristupa ili njegovo blokiranje.

Prednosti koje firewall pruža su:

Sprovodi politiku sigurnosti u slučaju da neka radnja nije dozvoljena on mora to da spreči.
Firewall treba da obaveštava administratora u slučaju napada na sistem.
Sprečava servise sa slabim sigurnosnim karakteristikama.
Mogu da dozvole prolaz samo određenim IP adresama.
Mogu da zabrane pristupanje određenom direktorijumu i delu mreže koji ga koristi.
Firewall sistemi i njihovo održavanje nije skupo.

Mane firewall sistema:

Mogu da predstavljaju ključnu tačku napada.
Može da ograniči korišćenje nekih određenih servisa .
Mogu da predstavljaju problem u protoku informacija koje prolaze kroz njih tj. u slučaju zagušenja saobraćaja.
Ne mogu da filtriraju atačment poruke[8] .
Ne mogu da štite sistem od napada iz unutrašnjosti mreže.

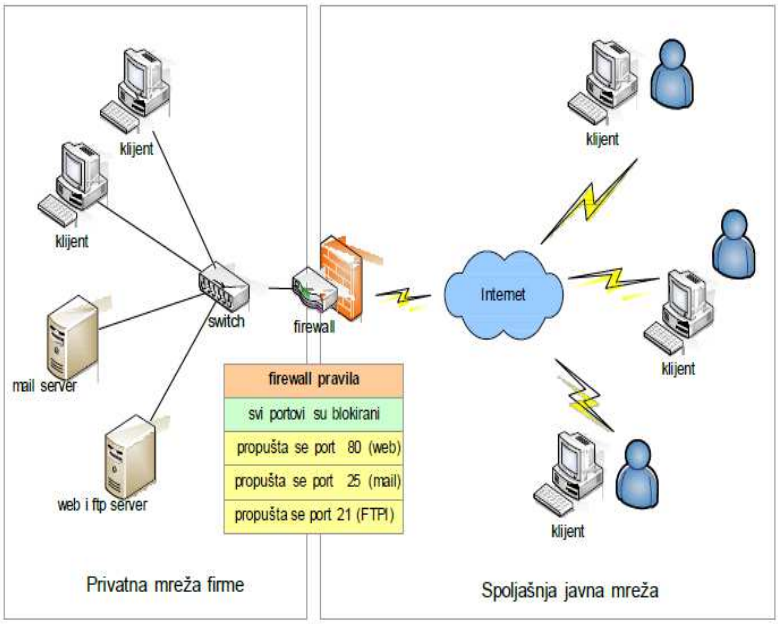
2.1 Tri najosnovnije funkcije firewall-a

2.1.1 Filtriranje paketa

Filtriranje paketa je jedna od osnovnih funkcija firewall sistema. Firewall proverava pakete mrežnog protokola, IP adrese, TCP – i, transport paketa i filtrira sadržaj sumnjivog karaktera.• (Oppliger, 2002) Paketi se proveravaju na osnovu pravila koji se mogu naći na ruteru ili na nekom od računara koji ima odgovarajuću aplikaciju za filtriranje.

[8] Atačment poruka – poruka koja sadrži u sebi sem teksta još i neku sliku ili zapakovan fajl
• Oppliger, R. (2002). *Internet and Intranet Security.* Norwood: Artech House.

Ruteri se postavljaju na ulaz u računarsku mrežu i njihova uloga je da ceo saobraćaj koji se odvija kroz taj sistem mora da prođe preko njih. Filteri koji su ugrađeni u njih propuštaju samo one pakete koji imaju pravo prolaska, a već smo rekli da se to određuje pravilom koji administrator dodeli tom ruteru ili softveru koji reguliše tok saobraćaja. Pravila koja administrator određuje obično se razlikuju od sistema do sistema koji se štiti, obično se ograničava pristupom nekom određenom opsegu IP adresa, kao i kontrolisanje ulazno-izlaznog saobraćaja. Firewall ima mogućnost sprečavanja pristupa onim portovima koji se nalaze unutar računarske mreže kao i da portovi ne budu vidljivi na Internetu. [•] (Cameron, 2005)



Slika 2 – postavljanje rutera

Recimo da računar koji se nalazi u računarskom sistemu i želi da komunicira sa spoljašnjim svetom mora da uspostavi vezu pomoću TCP konekcije, on tada šalje TCP poruku sa IP adresom odredišnog hosta i broj porta preko koga će se uspostaviti komunikacija. Kroz port će se vršiti ulazna i izlazna komunikacija. Kada se uspostavi komunikacija sa spoljašnjom IP adresom, server tada šalje povratnu poruku na port sa kog je zahtev za komunikaciju poslat. Firewall tada proverava saobraćaj koji se odvija i propušta pakete između dva hosta jer je veza bila zatražena sa unutrašnje strane računarske mreže. Svaki server ima neke od otvorenih portova za pristup Internetu i kroz njih je moguć pristup mreži. U tabeli su portovi koji se najčešće koriste za rad Internet servera.

[•] Cameron, R. (2005). *Configuring NetScreen Firewalls.* Rockland: Syngress Publishing.

Port	Server
20	File Transfer Protocol (FTP-data)
21	File Transfer Protocol (FTP)
22	SSH - Secure Shell (Enkriptovani udaljeni pristup)
23	Telnet
25	Simple Mail Transfer Protocol (za međuserversku razmenu pošte)
53	Domain Name Service (DNS servis, ako postoji)
80	World Wide Web (HTTP)
110	Post Office Protocol version 3 (za preuzimanje pošte sa servera)
119	Net News (NNTP)
143	Internet Mail Access Protocol (za pristup klijenta mail serveru)
443	Secure HTTP (HTTPS)
8080	HTTP - proxy (squid)

Tabela 1 – portovi za rad Internet servera

2.1.2 NAT (Network Address Translation) – prevod mrežnih adresa

Network Address Translation ima mogućnost skrivanja hostova[9] i informacija o njima od potencijalnih napadača.• (Angelescu, 2010) Ovaj servis zastupa mrežni sloj i suština ovog servisa jeste ostvarivanje konekcije hostova ka spoljašnjim javnim serverima. NAT krije unutrašnje hostove od spoljašnjeg sveta, ovaj servis je ugrađen u novije operativne sisteme tipa Windows server 2000, Windows XP, Windows Vista, Windows 7 i 8, Linux i Unix sisteme. NAT sakriva unutrašnje IP adrese pretvaranjem u adrese firewall-a sistema. Kada host želi pristup spoljašnjoj mreži i da korisnik ne bi otkrio svoju IP[10] adresu tada u njegovo ime firewall koristi svoj TCP[11] port i uspostavlja vezu sa javnim hostom. NAT sakriva sve informacije TCP/IP sloja o unutrašnjim hostovima. Prevođenje adrese omogućava upotrebu privatnih IP adresa i one bez tog servisa nemaju pristup Internetu. Ova mogućnost je dobra, jer, u slučaju da administrator ne raspolaže dovoljnim brojem IP adresa i u slučaju da se ne može izvršiti adresiranje svih hostova koji žele da pristupe u spoljašnju mrežu, hostovi se adresiraju unutar mreže sa različitim IP adresama, ali ovo može da predstavlja problem kod pristupa Internetu gde se mogu naći iste IP adrese. Iz tog razloga se unutar mreže dodeljuju IP adrese koje počinju od nekog standardnog opsega, a to je

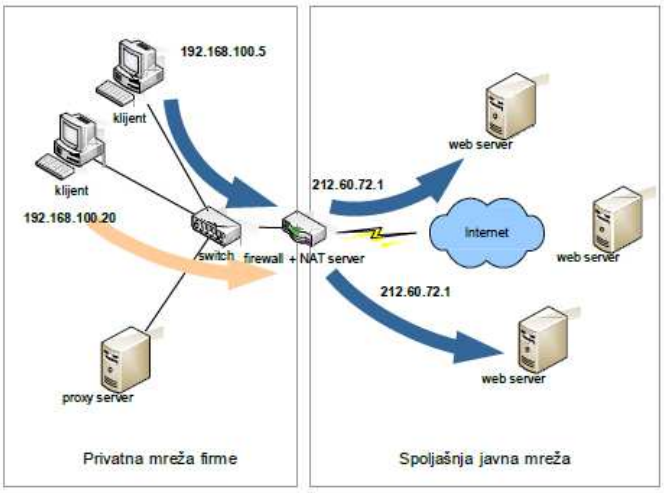
[9] Domaćini (stanice)

• Angelescu, S. (2010). *CCNA Certification All-In-One For Dummies.* Indiana: Wiley Publishing.

[10] *IP (internet protokol)* - Protokol koji se koristi pri mrežnim komunikacijama

[11] (*engl.* Transmition control protocol) ima za ulogu da obezbezbedi pouzdan transfer podataka u IP okruženju.

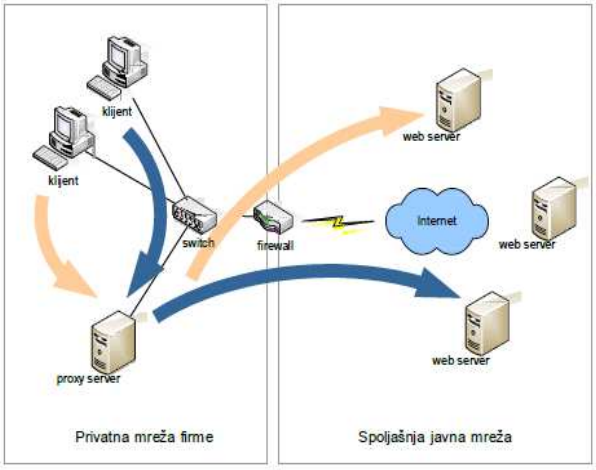
u intervalu od 192.168.0.0 ili 10.0.0.0. NAT ima mogućnost da dozvoli pristup više računara sa unutrašnje mreže prema Interenetu i to preko samo jedne javne IP adrese.• (Angelescu, 2010) Ova mogućnost pomaže računarskim mrežama koje raspolažu sa malo javnih IP adresa da nesmetano pristupe Internetu sa više računara u mreži.



Slika 3 – postavljanje NAT servisa sa firewall-om

2.1.3 Proxy[12] servisi

Proxy programi zasnivaju se na sloju aplikacija. Njegova uloga je da zabrani pristup i protok informacija na sloju mreže. Proxy softver omogućava firewall-u da dozvoli saobraćaj samo višem sloju u mreži kao što su HTTP[13], FTP[14] i SMTP[15] protokoli. Proxy softver je kombinacija klijenta i servera. • (Brian Komar, 2003)Kada proxy server primi konekciju od klijenta sa unutrašnje mreže on uspostavlja vezu preko svog proxy klijent servera ka spoljašnjem svetu, kada se konekcija ostvari sa spoljašnje



Slika 4 - delovanje proxy servisa

[12] U prevodu engleski pojam proxy server znači server posrednik.
[13] **HTTP** (*engl.* HyperText Transfer Protocol) je mrežni protokol koji pripada sloju aplikacije OSI referentnog modela
[14] **FTP** (*engl.* File transfer protocol – protokol za prenos datoteka) je najčešće korišćen protokol za prenos podataka između dva računara na mreži.
[15] **SMTP** (*engl.* Simple Mail Transfer Protocol) predstavlja osnovni protokol sloja aplikacija za elektronsku poštu
• Brian Komar, R. B. (2003). *Firewalls for Dummies 2nd Edition.* Indianapolis: Wiley Publishing.

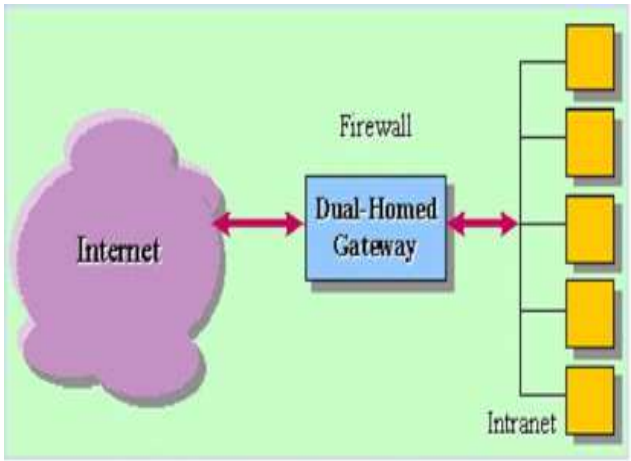
strane mreže tada klijentska strana proxy servera prosleđuje podatke klijentu.

Proxy servis uspostavlja komunikaciju sa dve mreže gde je zabranjena komunikacija. Možemo reći da proxy servis ima ulogu posrednika i da preko njega mora da prođe svaki podatak. Softverski proxy servisi se razlikuju od NAT-a i filtriranje paketa po tome što se koriste samo onda ako se konfiguriše u aplikaciji. Potrebno je podesiti u nekom od internet pretraživača korišćenje proxy servisa i tada pretraživač sve svoje zahteve šalje proxy servisu gde pristup Internetu ide preko njega, a ne pristupa direktno na Internet. Obično za pristup Internetu ide preko porta 8080.

3. Osnovne firewall konfiguracije

3.1 Dual-Homed Gateway – međusistemski firewall

Dual-Homed Gateway ("međusistemski") – vatreni zid koji sadrži ugrađena minimum dva mrežna adaptera. Kod ovakvog sistema konfiguracija se zasniva tako da se paketi ne šalju direktno sa Intraneta na Internet. Računarski sistem na Internetu može da komunicira sa firewall-om ali je direktan saobraćaj zabranjen. Mana ovog **Dual-Homed Gateway** sistema jeste to što se blokira IP saobraćaj u oba pravca i predstavlja problem programa koji koriste TCP/IP protokole. Rešenje ovakvog problema može se otkloniti pomoću proxy servisa koji prosleđuje pakete između dve mreže, koji takođe reguliše saobraćaj tako da se ne bi direktno ostvario kontakt između servera i klijenta, on usmerava ceo tok radnje na sebe. Iz ovog razloga poželjno je da proxy bude vidljiv za korisnike.[•] (Oppliger, 2002)

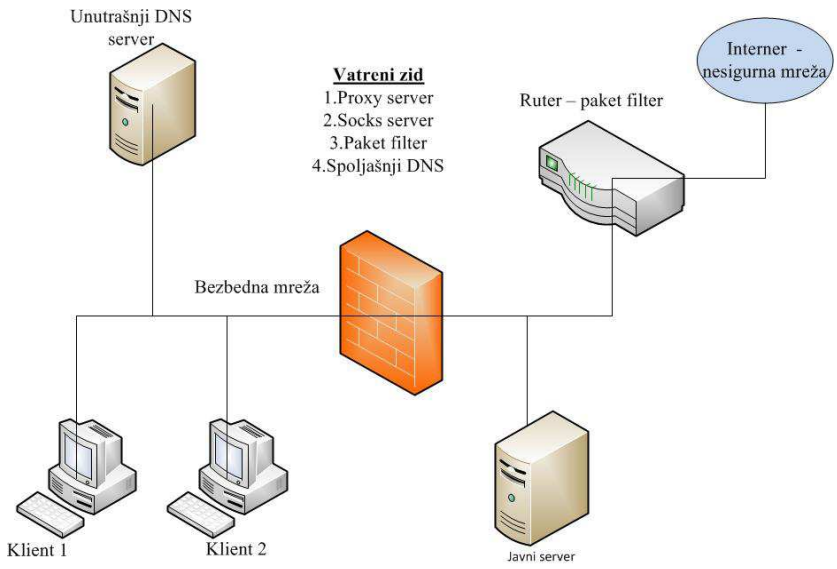


Slika 5. – postavljanje Dual-Homed Gateway firewall-a

[•] Oppliger, R. (2002). *Internet and Intranet Security.* Norwood: Artech House.

3.2 Screened host gateway – zaklonjeni firewall

Screened Host Gateway ("zaklonjeni") firewall slična je konfiguraciji **Dual-Homed Gatewa firewall-u,** zaštita unutrašnje sigurnosne mreže od spoljašnje mreže je više logičko nego fizičko. Ova konfiguracija se oslanja na filtriranje paketa pomoću rutera kako bi se omogućio promet između unutrašnje mreže i Interneta. Pomoću ove konfiguracije Web server može lako da komunicira sa unutrašnjom mrežom. Preko ove komunikacije može se lako doći do podataka sa unutrašnje mreže iz razloga ako neko želi da pristupi u mrežu kompjuterskog sistema on će koristiti pristup preko Web servera. Generalno rečeno, ovaj sistem nije poželjan za korišćenje, jer se politika zaštite zasniva između rutera i firewall-a. Što znači da oba sistema moraju biti usaglašena i konstantno proveravana, jer u slučaju da neki od sistema zakaže napadač lako prolazi zaštitu.[•] (Wack, 1995)



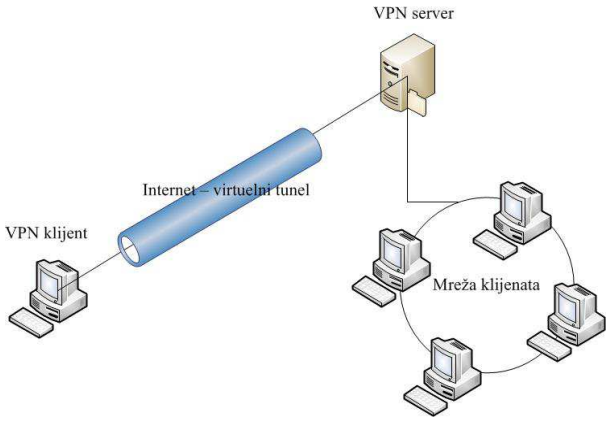
Slika 6. – postavljanje Screened Host Gateway firewall-a

Konfiguracija je zasnovana pomoću jednog mrežnog adaptera u firewall-u, što dovodi da je ovaj sistem jedan od jeftinijih sistema i troškovi održavanja nisu veliki. U ovoj konfiguraciji ruter je glavna liniji odbrane. Kao što je rečeno, moramo dobro proveriti politiku konfiguracije filtriranja paketa u ruteru jer ne postoji fizička odvojenost od spoljašnje mreže.

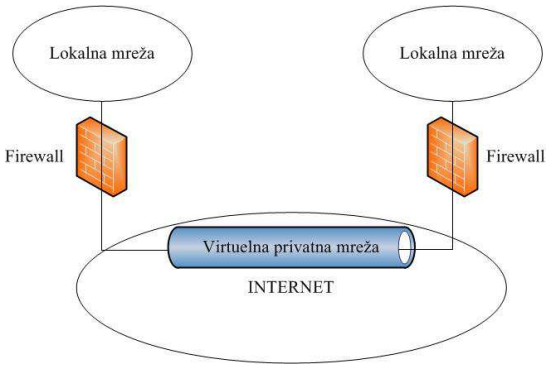
[•] Wack, J. (1995, Februar). *Screened Subnet Firewall*. Retrieved from Sunet: http://ftp.sunet.se/pub/security/docs/nistpubs/800-10/node58.html

3.3 Virtuelne privatne mreže (VPN - Virtual Private Networks)

Virtelna privatna mreža je tehnologija koja ostvaruje sigurnu komunikaciju dva udaljena privatna korisnika i to preko javne mreže (Interneta) .[•] (Attribution, 2013)Velike kompanije, vladine agencije, obrazovne institucije i mnogi drugi korisnici koriste VPN za sigurnu komunikaciju. Virtuelna privatna mreža se koristi za udaljeni pristup računarima. Za sprovođenje provere pomoću virtualne privatne mreže potrebno je da server ima instalirane servise Network Policy and Access Services i servis za Routing and Remote Access Services. [•] (Attribution, 2013) Da bi se dobio pristup VPN, korisnik mora da poseduje korisničko ime i lozinku za pristup. Autentičnost tokena mora se koristiti za pristup privatnoj mreži putem identifikacionog broja PIN.



Slika 7. – virtuelna privatna mreža



Slika 8 - primer uspostavljanja VPN-a između dve lokalne mreže

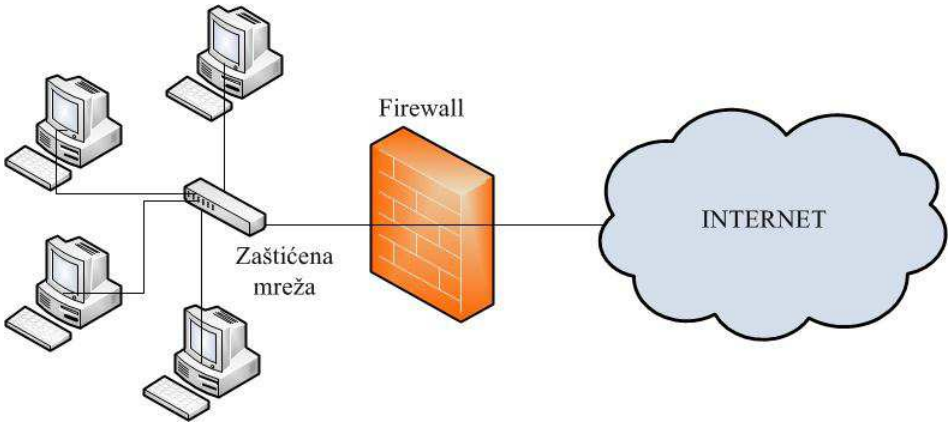
Ovaj način provere korisnika radi tako što, kada korisnik zatraži pristup mreži, tada server šalje potrebnu skriptu korisniku, koja proverava stanje njegovog računara i proverava da li su na računaru instalirane potrebne zakrpe koje su definisane na serveru Slika8. Jedini problem može da bude to što svaki put kada Microsoft objavi listu zakrpa, potrebno ih je redovno ažurirati i instalirati na server da bi on mogao da šalje najnovije skripte korisniku.Brzina kojom dva korisnika komuniciraju mnogo

[•] Attribution, C. C. (2013). *Virtual private network*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Virtual_private_network

zavisi od brzine Interneta, šifrovanja i dešifrovanja podataka, filtriranje podataka kroz firewall kao i koliko su korisnici fizički udaljeni .

3.4 Konfiguracija mreže bez servera

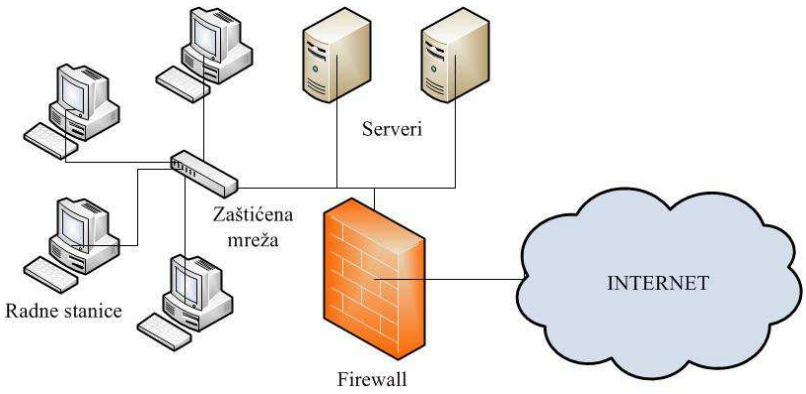
Konfiguracija mreže bez servera je veoma neisplativ poduhvat za kompanije, jer je potrebno povezati računare fizičkim putem. Zbog toga je ova konfiguracija ređa u velikim kompanijama. Najviše se primenjuje u kućnim varijantama.



Slika 9. - konfiguracije mreže bez servera

3.5 Konfiguracija mreže sa jednim serverom i jednim firewall-om

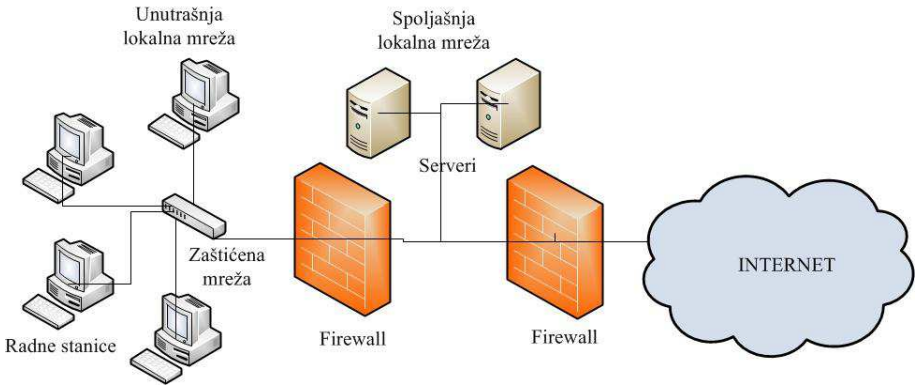
Ako u računarskom sistemu postoje više servera koje treba zaštititi potrebno je konfigurisati firewall zaštitu na složeniji način od prethodnog primera. Firewall se postavlja u unutrašnju mrežu tako da se server koji se štiti nalazi posle firewall-a. Ukoliko dođe do probijanja vatrenog zida i ulaska u lokalnu mrežu, neželjeni korisnici su u stanju da izvedu DOS napad pri čemu mogu da kontrolišu lokalne korisnike korišćenjem lokalnog server, u najgorem slučaju napadači mogu da preinače podatke sa servera, ubacujući viruse ili lažne podatke. Serveri koji se nalaze unutar lokalne mreže i firewall koji ga štiti potrebno je konfigurisati tako da paketi koji dolaze i odlaze mogu da prođu do odredišta. Ova konfiguracija firewall-a predstavlja problem jer ima dosta rupa koje vešt napadač može da iskoristi. Firewall propušta pakete do servera i server ih prosleđuje korisnicima.



Slika 10. - konfiguracije mreže sa serverima lociranim unutar lokalne mreže

3.6 Konfiguracija mreže sa jednim serverom i dva firewall-a

Konfiguracijom dva firewall-a mogu se sprečiti napadi koji su bili mogući u gore navedenim primerima. U ovom slučaju prvi firewall se postavlja za pristup Internetu i serverima, koju možemo nazvati spoljna lokalna mreža. Dok se dugi firewall postavlja između lokalne mreže i mreže servera. Zaštita servera ovim putem je složenija od prethodnog primera i teže je pristupiti do mreže servera. Mreža servera može samo da šalje pakete koji su uspostavljeni nekom komunikacijom i to samo do drugog firewall, dok prvi firewall koji je spojen na Internet mora da propusti pakete sa uspostavljenom komunikacijom i pakete koji su namenjeni serverima.

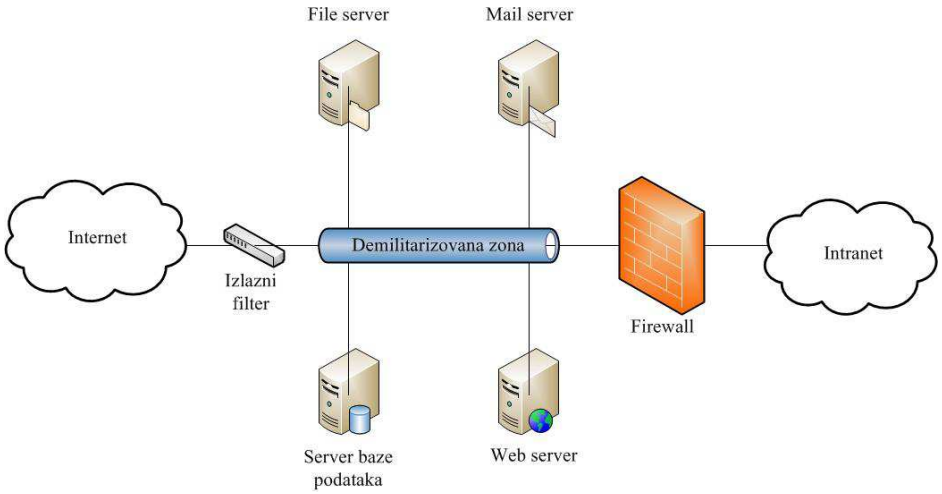


Slika 11. konfiguracije mreže sa serverom lociranim između dva firewall

Konfiguracija mreže pomoću dva firewall-a ima neke svoje mane, a mane su zbog toga što se koristi dva firewall-a i paketi se moraju dva puta obraditi, čime se usporava protok i brzina prenosa podataka.

3.7 Konfiguracija mreže sa demilitarizovanom zonom

Demilitarizovana zona (neutralna zona) je oblast koja se postavlja između lokalne i spoljašnje mreže. Ako postavimo mail server u demilitarizovanu zonu sprečavamo neželjene korisnike da pristupe lokalnoj mreži.[•] (Danny Briere, 2011) Demilitarizovana zona omogućava pristup mail serveru , korisnicima iz lokalne mreže i korisnicima sa Interneta. Kada se konfiguriše demilitarizovana zona onda se najčešće firewall postavlja između izlaznog rutera i unutrašnje mreže i sa ovom konfiguracijom se kreira novi vid mreže gde se može postaviti mail server.



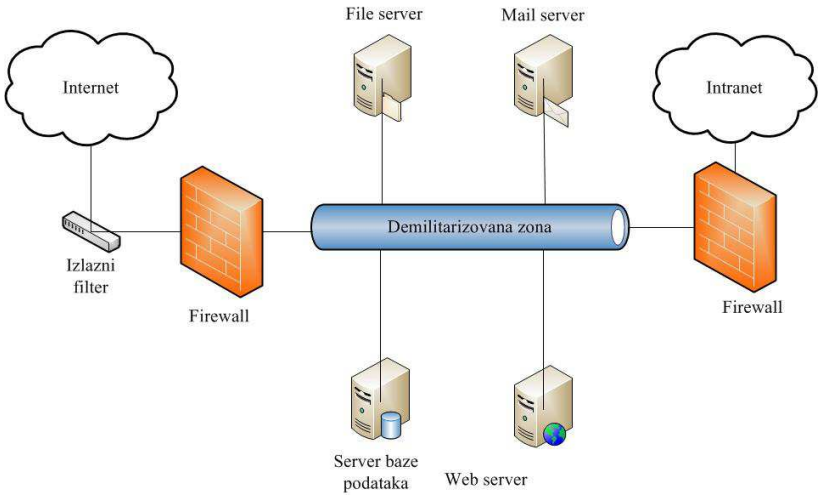
Slika 12. - konfiguracije mreže sa demilitarizovanom zonom

U ovom primeru zaštita mail servera se vrši pomoću liste za kontrolu pristupa ACL[16] (access control lists) koja se postavlja na izlaznom ruteru i kojim se ograničava određeni tip saobraćaja u i iz DMZ-a. Ova konfiguracija DMZ je jednostavno i jeftino rešenje, a prisutna je i zaštita mail servera od strane izlaznog ruter-a. Ovo rešenje može biti odgovarajuće za male organizacije koje su izložene minimalnim pretnjama. Glavni nedostatak konfiguracije je u tome što izlazni ruter nije "svestan" mail protokola na aplikativnom sloju (SMTP, POP3, IMAP) tako da on nije u stanju da spreči napade takvog tipa na mail server. Pored toga ruter nije u stanju da pruži anti-virusnu zaštitu i da skenira dolaznu e-poštu. Poboljšanje konfiguracije postiže se

[•] Danny Briere, H. F. (2011). *Wireless Home Networking For Dummies.* Indiana: Wiley Publishing.

[16] Popis kontrole pristupa (ACL), s obzirom na sistem računarske datoteke koja ima pristup dozvolama za objekte.

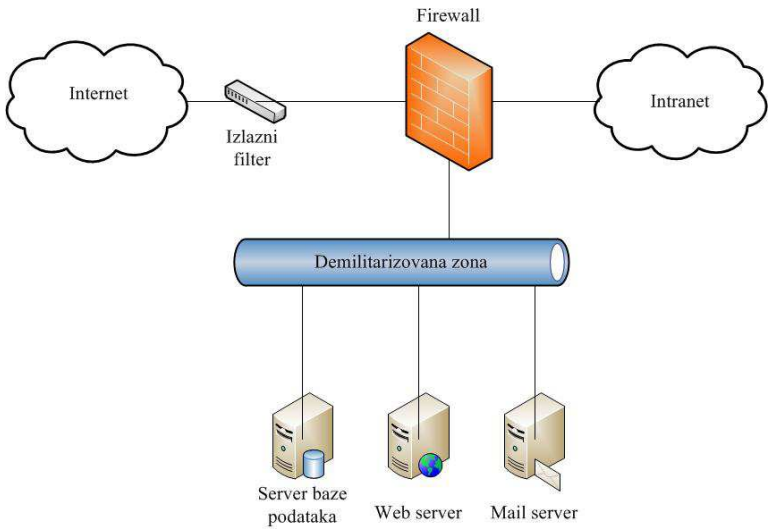
postavljanjem još jednog firewall-a između izlaznog ruter-a i DMZ-a. Konfiguracija je prikazana na Slici 13.



Slika 13. - DMZ sa dva firewall-a

Konfiguracija DMZ-a pomoću dva firewall-a pruža veoma dobru zaštitu mail servera. Sigurnosna pravila koja se mogu podesiti na firewall-u su mnogo efikasnija i složenija nego ona koja se mogu dobiti sa ruter-om. Osim toga firewall-ovi su često sposobni da analiziraju ulazni i izlazni saobraćaj e-pošte, mogu registrovati i sprečiti napade na aplikativnom sloju.[•] (Brian Komar, 2003) Mana ovakve konfiguracije DMZ je u tome što u zavisnosti od konfiguracije firewall-ova i sa velikom količinom saobraćaja dolazi do značajnijeg gubitka performansi sistema. Za organizacije koje žele nivo zaštite koju pruža konfiguracija sa dva firewall-a, a nemaju materijalne mogućnosti da ih nabave, postoji rešenje sa jednim firewall-om koji poseduje tri (ili više) mrežnih adaptera. Jedan mrežni adapter se povezuje sa lokalnom mrežom, drugi adapter se povezuje sa izlaznim ruter-om,a treći adapter se povezuje sa DMZ-om. Ako postoji više od tri mrežna adaptera moguće je formirati konfiguraciju sa više demilitarizovanih zona. Konfiguracija DMZ-a sa jednim firewall-om sa tri mrežna adaptera prikazana je na slici 14.

[•] Brian Komar, R. B. (2003). *Firewalls for Dummies 2nd Edition.* Indianapolis: Wiley Publishing.



Slika 14. – konfiguracija sa tri mrežna adaptera

3.8 Firewall-i zasnovani na hostu

Ovu tehnologiju koristi računar za zaštitu umesto rutera, sa kojom ima više mogućnosti praćenja aktivnosti samog firewall-a. Firewall koji je konfigurisan na nivou rutera može da proverava pakete samo na nivou IP adresa, dok hostovi prenose kontrolu na aplikativnom nivou. Da bi se osigurali od potencijalnih problema koji bi se mogli pojaviti zbog propusta u implementaciji sigurnosti u uobičajenoj programskoj podršci za mrežne usluge, firewall-i zasnovani na hostovima obično koriste posebne verzije programa koji pružaju podršku potrebnim servisima. To su najčešće osnovne verzije originalnih programa koji su zbog svoje kratkoće puno jednostavniji za održavanje, pa je i manja mogućnost za slučajne propuste koji narušavaju sigurnost.

Prednosti firewall-a zasnovanih na hostu:

Zaštita firewall-om protiv pada sistema – dodavanjem drugog firewall-a u mrežu je od koristi jer u slučaju pada prvog firewall-a sistem se ne može naći u situaciji slobodnog prolaza kroz njega. Višestruki firewall-i ne nude povećanu zaštitu protiv napada usmerenih na aplikacije ili operativne sisteme.

Jednostavnost - konfigurisanje Host-based firewall-a je obično daleko jednostavnije nego konfigurisanje parametera firewall-a, jer korisnik obično zahteva podršku za samo nekoliko protokola.

Šira zaštita protiv brojnih pretnji - host-based firewall može da zaštiti od pretnji koje dolaze iz lokalne mreže, a može pomoći u ublažavanju rizika od loše konfigurisanog softvera na računaru

Specifičnost - host-based firewall može biti podešen tako da podrži jedan set aplikacija i blokira sve ostalo. Softverski firewall obično je konfigurisan pravilno i dizajniran tako da podrži mnoge aplikacije.

3.9 Mreža zasnovana na firewall-u

Izolacijske mreže su vrlo slične firewall-ima zasnovanim na hostu, osim što se između privatne mreže i Interneta ne postavlja host nego mreža. Međutim, ta se mreža može sastojati i od samo jednog čvora konfigurisanog tako da i jedna i druga mreža može pristupiti izolacijskoj mreži, ali istovremeno tako da izolacijska mreža ne propušta direktan promet između privatne mreže i Interneta. Glavna prednost izolacijske mreže je u tome što omogućava jednostavnije postavljanje i dodeljivanje novih Internet adresa, naročito kod velikih privatnih mreža koje bi se inače morale znatno rekonstruisati.• (Bolakis & Furnell, 2004)To u osnovi znači da računari "iza" izolacijske mreže ne moraju imati adrese koje su poznate računarima na Internetu. Na taj način se može priključiti cela mreža računara "iza" firewall-a na Internet korištenjem samo jedne Internet adrese.

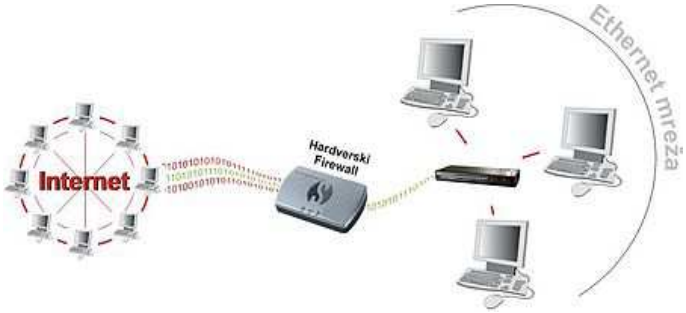
4. Hardverski firewall sistemi

Hardverski firewall - je uređaj koji je deo računarske mreže i ima mogućnost da spreči nekontrolisan prenos podataka izvan mreže. Ovaj vatreni zid kontroliše protok svih podataka u računarskoj mreži. Hardverski uređaj firewall-a sprečava ulazak virusa u sistem ali ih ne može ukloniti tj. brisati. Zaštitni zid ne može da radi sam već je potreban iskusan administrator da podesi uređaj i dozvoli pristup konekcije na

• Bolakis, S., & Furnell, S. M. (2004). *Helping us to help ourselves: Assessing administrator's use of security tools. Network Security.* United Kingdom: Browse journals.

Internet, obično se postavlja između računarskog sistema i Interneta.

• (Technology, 2013)



Slika15 - postavka hardverskog *firewall*-a u sistem

Slika - predstavlja prikaz protoka informacija između **računara-hardverskog firewalla-interneta**. Kako možemo da vidimo poruke sa crveno zelenim brojevima koje dolaze sa Interneta i ulaze u hardverski firewall sistem, filtriraju se kroz njega i propuštaju se u računarski sistem. Crvene jedinice i nule su štetni kodovi, dok je zeleni kod valjani kod koji je korisnik i želeo da vidi. Uređaj koji se danas koristi u bankarskim sistemima, a veoma je pouzdan u svom delovanju jeste zaštitni zid kompanije Cisco. Ovaj uređaj je višenamenski uređaj za bezbednost mreže i može se konfigurisati za zaštitu svih veličina bankarskih sistema. Njegova uloga u bankarskim sistemima je odbrana od pretnji sa Interneta i sprečava- nje eventualnih pokušaja napada na računarski sistem i time pomaže bankama da zaštite svoje delove mreže.• (Cheswick, 2003)

5. Softverski firewall sistem

Softverski firewall sistem je softver koji je instaliran na računaru korisnika i on kontroliše komunikaciju prema i sa računara i s tim dozvoljava ili zabranjuje komunikaciju u mreži. Kod ovog firewall-a je mana to što on samo štiti računar na kojem je instaliran. Problemi koji mogu da se jave korišćenjem ovog firewall sistema su ti što su instalirani na sistem koji se štiti i samim tim mogu da ugroze sistem ako

---

• Technology, I. S. (2013). *How Firewalls Work*. Retrieved from Information Services & Technology: http://www.bu.edu/tech/security/resources/host-based/intro/

• Cheswick, W. R. (2003). *Firewalls and Internet Security, Second Edition.* . Boston: AT&T and Lumeta Corporation.

dođe do napada na njega. Ovaj takoreći sistemski firewall troši resurse sa računara i predstavlja potencijalnu metu napada. Loša strana jeste ta da u slučaju da u sistemu postoji neki od *Malware*[17] *i Spyware*[18] malicioznih programa može da dođe do kontrolisanja i manipulisanja firewall-a od strane njih jer se nalaze na istom sistemu. Mogu da budu pomalo dosadni u smislu da korisnika obaveštavaju ako je došlo do napada na zatvoreni port računara ili pogrešno mrežni saobraćaj tretiraju kao napad. Danas imamo neke od najpoznatijih *softverskih* firewall-a, a to su *Zone Alarm, Black ICE, Norton Firewall, Kerio Personal Firewall, Symantec* i drugi.

6. Politika zaštite i skup pravila firewall-a

Firewall određuje koji od paketa bi trebali biti prihvaćeni, odbijeni, ili propušteni na osnovu njegove politike zaštite. Kada neko želi da postavi firewall, on uglavnom ima ideju kako i šta bi trebalo zaštititi. Na primer, vatreni zid bi trebao omogućiti promet do web servera, a treba da odbije sav ostali promet. Ovo je politika zaštite firewall-a. Osoba koja podešava i konfiguriše politiku zaštite u firewall-u, poznata je kao firewall administrator, on će prevesti ovu politiku u niz tehničkih izveštaja i skup pravila koja govore hardveru ili softveru šta da izvršavaju.

Kad Firewall ima zadatu politiku zaštite, ta zadata politika se uopšteno primenjuje na propuštanje prometa ili zabrane prometa. Windows Firewall se ponaša na takav način da windows korisnici koji su aktivirali windows vatreni zid mogu biti upoznati s dobijanjem dijaloških okvira s upitom ako je u redu da se omogući primena prihvatanja veze na mrežu. Ako pak korisnik želi, može dodati u softver Windows Firewall-a pravilo na skup pravila koja pokazuju da je promet na tom zahtevu dopušten. Kroz kontrolne Windows Firewall-a možemo dodati i ukloniti pravila iz politike zaštite.

6.1 Pisanje firewall pravila

Kontrolni panel firewall-a je definisan tako da korisnici ne mogu izvršiti menjanje pravila tj. dodavanje ili brisanje postojećih pravila. Ako sumiramo broj napada i potencijalnih putanja odakle nas napad može zadesiti možemo doći do zaključka da se napadi izvršavaju sa Interneta. Većina prometa koji prolazi kroz firewall jeste

[17] U prevodu „maliciozni“ ili „zloćudni“ softver.
[18] Špijun (*engl.* Spyware) je široka kategorija štetnog softvera

pomoću Internet protokola i to preko tri glavna transportna sloj: TCP[19], UDP[20], ICMP[21]. • (Cheswick, 2003)Sve tri vrste imaju adresu izvora i odredišnu adresu računara koje je poslalo ili slalo. Oba TCP i UDP sloja imaju brojeve portova, broj između 0 i 65535 koja pomažu u identifikovanju aplikacije koja je inicirala vezu. Na primer, većina web brovzera koriste TCP port 80, tako da bi paket koji je krenuo na web server trebao imati odredišnu adresu web brovzera i broj odredišta od 80. ICMP ne koristi brojeve porta, ali umesto toga ima kod vrste koja identifikuje ono što je svrha paketa. ICMP se obično koriste za ispravljanje mrežnih problema i grešaka ili informisanje o problemu sistema. Korisnici takođe žele da znaju da TCP paketi imaju oznake koje označavaju stanje veze između dva računara. Ove oznake imaju imena poput SYN, FIN, ACK i RST.• (Inforamtion_services, 2012) Paket koji je namenjen za pokretanje veze će imati samo SYN oznaku. Sve naknadne komunikacije između dva sistema će imati ACK oznaku. Firewall može biti konfigurisan za pakete koji izgledaju da imaju samo skup SYN oznaka i da se tretiraju kao nove veze gde se za pakete s ACK oznakom pretpostavlja da su deo postojeće veze. To su sigurnosne mere, jer pošiljalac paketa može kontrolisati oznake prisutnih paketa, ali to može da bude i učinkovita pomoć na prepoznavanju novih u odnosu na postojeće veze.

7. Hardverski ili softverski firewall - poređenja

Jedan od najvažnijih koraka zaštite računarskog sistema od napada ili ulaska neželjenih gostiju u sistem jeste zaštita pomoću firewalla-a. Istraživanja pokazuju da je potrebno imati firewall kao sigurnosni sloj na našem računaru ili računarskoj mreži. Firewall-e smo podelili u dve kategorije: hardverske i softverske. Izbor firewall-a iz

---

[19] *Transmition control protocol* je protokol koji pripada sloju 4 OSI referentnog modela, ima za ulogu da obezbezbedi pouzdan transfer podataka u IP okruženju.

[20] *User Datagram Protocol* je jednostavan protokol koji obezbeđuje osnovne funkcije transportnog sloja OSI modela

[21] *Internet Control Messageing Protocol* je protokol sloja mreže koji obezbeđuje pojedine mehanizme oglašavanja.

• Cheswick, W. R. (2003). *Firewalls and Internet Security, Second Edition. .* Boston: AT&T and Lumeta Corporation.

• Inforamtion_services. (2012, 2012). *Inforamtion services and technology*. Retrieved from How Firewalls Work: http://www.bu.edu/tech/security/resources/host-based/intro/

ove dve kategorije je samo lični i zavisi koliko smo spremni zaštititi naše podatke od spoljašnjeg uticaja. Faktori rizika postoje u obe kategorije ali svaka kategorija je dobra na svoj način i pruža svoj maksimum sigurnosti. Predstavljen je brzi pregled obe kategorije tako da zainteresovani korisnik može po svom izboru napraviti informisani izbor i odabir povoljnog firewall-a. Svaki prodavač ima svoj pristup u izgradnji firewall-a U daljem tekstu će biti predstavljeni vodeći proizvođači vatrenog zida.

7.1 Ključne prednosti hardverskog firewall-a :

1. Brzina: Hardvarski firewall-i su konfigurisani tako da imaju brže vreme odziva, tako da se mogu nositi s više prometnih opterećenja.

2. Sigurnost: vatreni zid je s vlastitim operativnim sistemom manje sklon za napade. Što se smanjuje sigurnosni rizik i pored toga, hardverskom firewall-u su poboljšane sigurnosne kontrole .

3. Nema smetnji: Od hardverskog vatrenog zida je izolovana računarska mreža , može se upravljati bolje, a ne opterećuje ili usporava druge aplikacije. Vatreni zid može biti premešten, ugašen, ili rekonfigurisan sa minimalnim smetnjama u mreži. Ako se koristi više računara za izlaz ka Internetu, hardverski firewall je bolji izbor, jer je u mogućnosti da obrađuje promet za više korisnika i može razlikovati koji promet je dopušten jednom korisniku, a koji je zabranjen.

7.2 Ključne prednosti softverskog firewall-a :

1.Softverski firewall-i su lakši za konfigurisanje i postavljanje.

2.Možemo ograničiti neke specifične aplikacije s Interneta. To čini vatreni zid fleksibilnijim.

3.Korisnici imaju potpunu kontrolu nad svojim Internet prometom.

7.3 Poređenje softverskog i hardverskog firewall-a :

Postavljanje i jednostavnost ima softverski firewall

(Softverski firewall može biti instaliran u roku od nekoliko minuta, bez zastoja, dok kod hardverskog firewall-a treba oko 4 sata čekanja)

Umrežavanje zauzima hardvarski firewall

(Hardverski firewall daje centralizovano firewall rešenje)

Održavanje nije zahtevno kod hardvarskog firewall-a

(Često održavanje nije potrebno za hardverski firewall)

Jednostavnost korišćenja pripada softverskom firewall-u

(Može se konfiguristi sa njegove radne platforme)

Manji su troškovi kod softverskog firewall-a

(Hardverski firewall je skuplji za održavanje od softverskog firewall-a)

8. Socijalne i tehnološke prednosti firewall-a

Softverski firewall-i su dizajniran za korišćenje na jednom računaru. Lični firewall blokira uljeze i sprečava upad u računar. Softverski firewall-i treba da nude mogućnosti koje nadilaze standardnu zaštitu, uključivanjem alata za upravljanje spyware, cookies i virusnom zaštitom, internet filtriranje, ograničavanje sadržaja itd. Veliki vatreni zidovi uključuju dodatke poput antiphishing, antivirusnih i antimalware alata. Korisnički paneli kontrole i instant poruke zaštite su takođe dobre mogućnosti za snalaženje u tim vrstama programa. Računar bi trebao biti u stanju da razume i koristi firewall proizvod bez pomoći. Tako da početnik ne treba da ima veliko pred znanje za postavljanje konfiguracije firewall-a. Korisnički interfejs treba da bude jednostavan i lak za korišćenje. Preporučuje se kombinacija sa ostalim programima koji imaju funkciju zaštite od ulaska neželjenih gostiju u računarski sistem. Ovde se prvenstveno misli na antivirusne programe, antimalware, antispyware i sve ostale programe iz ove kategorije. Nikako se ne preporučuje instalacija dva ili više softverskih firewall-a na isti sistem, jer dolazi do zajedničkog sudaranja, usporavanja računara , gubitka konekcije ka internetu, dakle ovakva mogućnost se ne preporučuje. Ali se svakako preporučuje korišćenje kombinacije hardverskog i softverskog firewall-a. Virusi koji se nalaze prikačeni u sadržaju poruke ne mogu se otkriti, kao i phishing prevare koje imaju zadatak da od korisnika saznaju važne lične informacije tipa lični podaci, broj računa u banci, važne lozinke.

Vatreni zid bi trebao biti što jednostavniji za početnika da postavi proizvod bez pomoći. Proizvođač takođe treba da ima pomoć online, odgovori na uobičajena pitanja. Telefonska podrška treba da bude dostupna 24 sata, kao i tehnička. Neki

proizvođači koriste elektronsku poštu ili online pitanja, forume, ali neki softveri nude podršku uživo chat online.

9. Buduće generacije hardverskog i softverskog firewall-a

Za svega par godina unazad "uspeli" smo da se popnemo visoko na lestvici opasnih i nesigurnih regija sa akterima kojima raste ugled u kompjuterskom podzemlju. S druge strane zakona, nedovoljna opremljenost pravosudnih organa i sporost državnih organa olakšali su brz transfer zlonamernih pojedinaca u sferu "čistog" kriminala. To je ohrabrilo i mnoge druge korisnike Interneta koji su mislili da mogu da profitiraju preko Interneta na nelegalan način, a da pri tom ne misle da ugrožavaju nečiju privatnost. Sigurnost je potrebna samo u okruženju gde postoji velika količina nepoštovanja između onih koji imaju nešto za zaštitu i onih koji žele dobiti te informacije.

Era razvoja internet tehnologija tek predstoji. Iako su obe tehnologije dobre, hardverski i softverski firewall-i imaju mogućnost nadogradnje na neke od tehnologija zaštite. Svaka vrsta firewall-a nudi jedinstvenu vrstu zaštite. Korišćenjem oba hardver i softver firewall-a, može se dobiti apsolutno najbolju zaštitu od hakera, spyware, virusa, i krađe identiteta. Mnogi firewall dobavljači nude nove generacije vatrenog zida, ali se svađaju oko toga čija je tehnika najbolja. Nova generacija firewall aplikacija je svesnija u pronalaženju neželjenog koda. Za razliku od prethodne generacije firewall-a, koja se bavila protokolima, sledeće generacije firewal-a prodiru u mrežni promet i identifikuju aplikacije preko mreže. Uz sadašnje trendove, viši nivo je stavljen na detalje i potrebu da se osigura pravilan dolazak podataka u mrežu preduzeća.

Dalji tok istraživanja se sprovoditi ka upoređivanju najbolji softverski firewall-i koje se nude na tržištu. Odabirom najboljih pet softverskih firewall-a, njihova detaljna objašnjenja i prikaz njihovih mogućnosti. Istraživanje će se sprovoditi ka uspešnosti pronalaženja malicioznog koda, njegovo brisanje i neutralisanje. Na testiranom firewall-u će se ocenjivati njegova učinkovitost i nivo zaštite s kojom raspolaže. Testirani firewall-i će biti podvrgnuti nizom test programa sa malicioznim kodom gde će se kroz razne tehnike napada ocenjivati reakcije samog firewall-a. Potrebno je postaviti kriterijume ocenjivanja firewall proizvoda gde će se uporediti sadržaj samog

zaštitnog zida, tehnike sa kojim raspolaže, stepen učinkovitosti tj. odbrane, impementacija sa drugim tehnologija zaštite, lakoća postavljanja i konfigurisanja, dostupnost na tržištu i cena samog proizvoda.

9.1 Hardverski firewall- budućnost

Hardverski firewall-i su integrisani u ruter koji se nalazi između računara i Interneta. Oni obično koriste filtriranje paketa, što znači da skeniraju ulazno izlazne pakete proveravajući njihov izvor, poreklo, odredišnu adresu i proveravaju sve kroz protokole koje je odredio administrator sa definisanim pravilima.

Glavne osobine:[•] (Crasto, 2012)

•**McAfee Firewall Enterprise (hardver)** nedavno je kupio Intel, koristi McAfee AppPrism tehnologiju za primenu otkrića i svesti u McAfee Firewall Enterprise. AppPrism identifikuje hiljade aplikacija, bez obzira na port ili protokol. Firma tvrdi da AppPrism takođe pruža visok nivo kontrole, omogućavajući administratorima da onemoguće samo rizičnije delove aplikacija. Na primer, administratori mogu koristiti tehnologiju za blokiranje mogućnosti za razmenu datoteka i instant messaging aplikacije bez blokiranja korisničkih sposobnosti za razgovor. McAfee tvrdi da njegova nova generacija vatrenog zida ima prednost jer njegova primena nove tehnologije je osnovni deo firewall arhitekture. Ima jaku politiku zaštite temeljenu na kontroli. Blokira najnovije pretnje i eliminiše neželjeni promet. Ovaj firewall je u stanju da identifikuje korisnike i proverava aplikacije koje služe za pokretanje mrežne veze.

• **Cisco SA 520 (hardver)** uređaj je sve-u-jednom sigurnosno rešenje koje kombinuje high-speed povezivanja i integrira sigurnosne sposobnosti. Uz četiri 10/100/1000 LAN portova, dva 10/100/1000 WAN porta, VPN, firewall, i e-mail i web zaštita. Cisco SA 520 je jednostavan za instalaciju i korišćenje, sve-u-jednom sigurnosno rešenje posebno dizajniran za preduzeća manja od 100 zaposlenih. Kombinuje sigurnost ka Internetu, site-to-site, i daljinsko povezivanje sa firewall-om, e-mail. Radi besprekorno sa ostalim Cisco Small Business Pro proizvodima. Cisco nije skup za održavanje i ne košta mnogo novca, ali daje punu sigurnost mreži. Cisco Systems je

---

• Cheswick, W. R. (2003). *Firewalls and Internet Security, Second Edition. .* Boston: AT&T and Lumeta Corporation.

najavio planove za dodavanje na nivo vidljivost u svojoj Adaptive Security Appliance (ASA), kao deo novog SecureX sloja. Cisco tvrdi da je ova nova arhitektura rešavanje zahteva svesti, tj. da korisnik i uređaj prolaze deo identifikacije.

•**Astaro (hardver)** koristi bazu podataka sa aplikacijama potpisanu od strane partnerske firme Vineyard Networks. Kroz ovo partnerstvo, Astaro firewall može razlikovati različite aplikacije sa iste web stranice i može da primeni Quality of Service i odredi prioritete za propuštanje aplikacija. Najnovija verzija Astaro Security Gateway-a poboljšava proizvod pomoću informacija upućenih ka firewall administratorima. Nudi široku mrežu sigurnosti i omogućava administratorima da brzo definišu sigurnosne politika temeljene na stvarnom vremenu i situacijama. Astaro je omogućio da administratori reaguju na nove pretnje tako da firewall funkcioniše brzo i jednostavno. Astaro takođe je usmeren na prepoznavanje novih, nepoznatih aplikacija. Kompanija planira da za nadolazeća izdanja, sistem omogući administratorima da prikupljene podatke primene za identifikaciju i da ih primene za ažuriranje baze podataka o potencijalnim pretnjama.

•**Palo Alto Networks (hardver)** kompanija tvrdi da je prvi prodavac sledeće generacije firewall-a koji klasifikuju aplikacije. Palo Alto proizvodi su na temelju klasifikacije poznate kao App-ID. App-ID identifikuje aplikacije pomoću nekoliko tehnika, uključujući dešifrovanje, otkrivanje, dekodiranje, potpise i td. Sledeća generacija firewall-a omogućuje aplikacijama - bez obzira na port, protokol ili SSL enkripcije da skenira sadržaj i zaustavi moguće pretnje i spreči curenje podataka. Po prvi put, korisniku se omogućava sigurno korišćenje aplikacija, održavanje potpune preglednosti i kontrole. Pojedinačna App-ID za određenu primenu može osloniti na bilo koju kombinaciju tih tehnika u jednom paketu, čime je motiv softvera identifikovati sve verzije aplikacije. App-ID, kao srž Palo Alto vatrenog zida, radi tako da može utvrditi kada je primenjena obavljena funkcija, kao što je prenos datoteka, a na svaku funkciju se može primeniti politika zaštite. Kompanija takođe napominje da App-ID kao deo standardne opreme, bude dostupna sa cenom i kvalitetom proizvoda svim korisnicima. • (Docstoct, 2012)

• Docstoct. (2012). Next generation firewall: Palo Alto Networks. *Docstoct* .

•**Sonicwall (hardver)** je proizvod DELL kompanije koji za sledeću generaciju firewall-a kombinuje Deep Packet inspekcije (DPI) i povećava broj potpisa za bazu podataka koja trenutno može identifikovati i kontrolisati više od 3.500 aplikacija i aplikacijskih funkcija. Sa SONICWALL uređajima isporučuje se funkcija Deep Packet inspekcije (RFDPI)koja skenira svaki paket preko svakog protokola i porta. SONICWALL raspolaže tehnologijom koja istražuje stalno nove potpise, što se automatski isporučuju i prevode bez potrebe za dodatni rad mrežnim administratorima. SONICWALL firewall je rešenje koje uključuje vizualizaciju sa Dashboard i real-time praćenjem koji omogućava administratorima da vide određene aplikacije na mreži, uključujući i podatke o tome ko ih koristi i koliko se koriste. Ideja SONICWALL-a je da administratori koriste ove informacije za podešavanje politike zaštite i rešavanje problema.Mnogi od firewall uređaja, uključujući Cisco ASA serije i Juniper SSG serije, pruža napredne tehnologije i omogućavaju dobru funkcionalnost poput VPN pristupne tačke. S druge strane, to može pružiti pristup krajnjim korisnicima Internet mreže na siguran i pouzdan način.

9.2 Softverski firewall - budućnosti

Softverski firewall-i su instalirani na pojedinačnim računarima. Oni mogu da presretnu svaki zahtev veze, a zatim da utvrde da li je zahtev valjan ili ne. Softverski firewall obrađuje sve zahteve. Osim performansi ograničenja, vatreni zid ima brojne prednosti.

- **McAfee Personal Firewall (softver)** je softver sa jednostavnim panelom za konfiguraciju i veoma je brza i laka konfiguracija. Cena ovog programa ne igra veliku ulogu, jer sam softver nije skup i može ga svako priuštiti. Softver može da traje dosta dugo, u odnosu na konkurenciju, jer se osvežavanje softvera vrši mesečno. Firma preporučuje korišćenje i ostalih proizvoda sa njene palete proizvoda, a tu spadaju i antivirusi, antispywer i drugi alati. Nudi poboljšanu zaštitu od opasnih web stranica. McAfee Internet Security je dvosmerni firewall koji je dizajniran da blokira pokušaje upadanje u sistem izvana i iznutra.

- **Comodo Internet Security Plus (softver)** iz Comodo Grupe. Ovaj vatreni zid može skenirati, filtrirati, blokirati pakete, i tako ga čini teško dostupnim za kriminalce. Comodo firewall je najbolji izbor za korisnike koji traže punu uslugu sigurnosti. Comodo firma tvrdi da je njihov firewall jedinstven po tome što prolazi sve poznate

testove protiv „curenja“ podataka, kako bi se osigurao i zaštitio integritet podataka sa ulaskom i izlaskom iz sistema. Comodo je stavio firewall kroz sve vrste testova da bi dokazali da je dovoljno snažan za odbranu od napada.

- **Norton Personal Firewall (softver)-**firewall blokira, filtrira, skenira pretnje i skriva IP adrese. Firewall blokira spyware, trojance, viruse i crve. Svakih pet do petnaest minuta, proizvod se osvežava sa potpisima najnovijih pretnji. Proizvod identifikuje web stranice koje mogu biti verodostojne i blokira web stranice koje pokušavaju izvršiti phishing. Softver pruža dosta sigurnosnih pravila koja se mogu menjati. Zaštita naše privatnosti, koja ne dolazi sa ostalim programima koje spominjemo, je vrlo dobra funkcija koju ne bi trebali zanemariti.

- **ZoneAlarm/ZoneAlarmPro (softver)** je veoma jednostavan za korišćenje, rad u programu je jednostavan. Profesionalci pribegavaju korišćenje ovog programa iz razloga što je kontrolni panel jednostavnog dizajna što daje dobar povod početnicima da ga lako savladaju tj. konfigurišu sigurnost na brz i jednostavan način. ZoneAlarm je jedini firewall koji, osim pokušaja ulaska u naš računar, posmatra i programe koji šalju informacije sa našeg računara. Ova funkcija je korisna, jer ako je računar zaražen virusom, svaka aktivnost aplikacije koja želi pristup Internetu biće prekinuta .

- **Check Point (softver)** je razvio aplikaciju AppWiki, firma tvrdi da može identifikovati više od 5.000 aplikacija i 100.000 umrežavanja widgetima. Softver se takođe integriše s Active Directory identitet korisnika, omogućavajući administratorima da prilagode detaljnije sigurnosne politike. Check Point takođe nudi mogućnost da se korisnici obrazuju u stvarnom vremenu. Agent softvera na korisnikovom računaru, UserCheck, pojavljuje se kao prozor kada korisnik krši sigurnosnu politiku. Ovaj softver takođe omogućava korisnicima povratnu informaciju od administratora, pojednostavljuje proces prilagođavanja sigurnosne politike i kao odgovor na potrebe korisnika.

Ako imamo jedan ili dva računara, tad je bolje da se odluči za softverski, nego hardverski firewall. Kad uporedimo ove dve vrste firewall-a hardverski firewall ili softverski firewall, obe tehnologije imaju svoje prednosti i nedostatke. Dakle, obe

imaju svoju vlastitu ulogu u web hosting industriji. Ako imate obe, onda uopšte nemate brige .

10. Poređenja, karakteristike i tehnološke novine firewall-a

Učinkovitost i sigurnost firewall-a zavisi od dobro postavljenih sigurnosnih pravila • (Furnell, 2004). Njihovom implementacijom u sistem dajemo korisniku vreme da reaguje na upozorenja. Loše konfigurisani firewall-i mogu dati lažnu sigurnost korisniku u slučaju napada • (Bolakis & Furnell, 2004) jer korisnik misli da ima dobro konfigurisan firewall.

Softverski zaštitini zidovi se instaliraju na svaki računar u mreži. Mnogo su lakši za konfiguraciju i održavanje nego hardverski firewall-i. Osim toga što sprečavaju nesiguran saobraćaj ka korisnikovom računaru, takođe imaju za zadatak da spreče ulaz programima sa sumnjivim sadržajem (trojanski konji, malware, spyware, rootkit virusi i ostali maliciozni kodovi). • (Denning, 1990) Dobar softverski firewall mora da spreči maliciozne programe da pristupe na računarski sistem. Ukoliko se konekcija ka Internetu izvršava preko modema, softverski zid pruža veće mogućnosti od hardverskog firewall-a. Tokom istraživačkog rada uspostavljena je konekcija ka Internetu preko modema kako bi se mogli testirati softverski firewall-i. Testiranje je izvršeno na pet softverskih firewall-a, Comodo Personal Firewall 2.0.0.0, Agnitum Outpust Pro Firewall, McAfee Firewall, Norton 360 Firewall, ZoneAlarm Pro Firewall 6.1. Razlog za odabir ovih pet firewall-a jeste zbog toga što su na tržištu zaštitnih zidova najpopularniji među korisnicima. Na osnovu pregleda raznih foruma gde korisnici komentarišu zaštitne zidove, besplatno ponuđenih i lako dostupnih na tržištu ovi zaštitni zidovi se izdvajaju od mnogobrojne konkurencije. Na odabir je uticala i činjenica da se u mom okruženju kroz razgovor sa korisnicima vatrenih zidova došlo do zaključka da treba ispitati da li ovi besplatni firewall-i su zaista dobro koncipirani za naš računarski sistem. Svaki od ovih zaštitnih zidova se može besplatno skinuti

---

- Furnell, S. M. (2004). Using security: easier said than done. Computer Fraud & Security. United Kingdom: Browse journals.
- Bolakis, S., & Furnell, S. M. (2004). Helping us to help ourselves: Assessing administrator's use of security tools. Network Security. United Kingdom: Browse journals.
- Denning, P. J. (1990). Computers Under Attack: Intruders, Worms, and Viruses. ADDISON WESLEY.

sa Interneta. Korišteni su sajtovi sa matičnim nazivom softverskih proizvoda, iz razloga što se tako mogu naći najsvežije verzije programa i korisnik je siguran da će preuzeti program za kojim traga. Svaki od ovih softverskih firewall-a je lak za instaliranje i ne zahteva veliko iskustvo oko implementacije na sistem. Tok istraživačkog procesa se odvijao ka programima za testiranje vatrenog zida. Gde su testirane sve mogućnost i odkrivani nedostaci za koje proizvođač ne reklamira. Za funkcionalnost vatrenog zida korištene su tehnike za curenje podataka ka Internetu gde korisnici mogu da primete da li postoji saobraćaj koji se ne registruje od strane firewall-a, špijunske tehnike gde korisnikov računar može da bude ugrožen od strane malicioznog koda , tehnike za samopokretanje malicioznih programa gde korisnik nema uticaja na procese koji su štetni na proizvod, testovi samoodbrane sistema gde korisnik može da pojača svoju odbranu zaštite i ostale tehnike koje mogu da ugroze sistem ali da se posledice po sistem javljaju tek nakon određenog perioda. [•] (Matousec, 2013)

Testovi su sprovođeni kako bi se prikazao postupak ugrožavanja i ranjivosti sistema gde korisnik može da uoči problem po svoj sistem, a nikako da se reklamira softverski firewall. Svaka od ovih tehnika je detaljno objašnjena u istraživačkom radu, gde je postavljen i izvorni kod svakog test programa. Korisnik može da primeni izvorni kod za konfiguraciju svog firewall-a tako što će konfigurisati vatreni zid po svojim zahtevima. Firewall programi su detaljno objašnjeni od trenutka instalacije na sistem, njihovo prvo konfigurisanje, korisnički interfejs i opis glavnih ikonica za korišćenje menija, zaštita i konfiguracija sistema, dodatne sigurnosne postavke firewall-a, pomoć korisnika, prikaz log fajlova, potrebni zahtevi računara. Svaki od pet softverskih firewall-a bio je podrvrgnut testiranju i prikazan sa mogućim ranjivostima po sistem. Kroz sprovedene testove korisnik može da se odluči za neki o pet programa ili da primeni iste test programe za simulaciju napada na svoj računarski sistem. Prilikom testiranja treba napomenuti da su svi test programi štetni po sistem i da je potrebno ponovno podizanje operativnog sistema. Svaki test je tako koncipiran da spreči pojedine procese u operativnom sistemu ili pak da zarazi pojedine aplikacije za pristup Internetu ili slično. Kako korisnik ne bi došao u situaciju da mu

---

[•] Matousec. (2013). *Matousec*. From matousec.com: www.matousec.com/projects/proactive-security-challenge-64

izabrani firewall ne registruje pretnju, potrebno je praviti backup sistema ili da simulacije izvede na virtuelnoj mašini. Prilikom ovog istraživačkog rada svaka simulacija se sprovodila na virtuelnoj mašini sa operativnim sistemom Windows 7 i pristupom na Internet.

10.1 Comodo Personal Firewall 2.0.0.0

Instalacija i deinstalacija :

Tokom instalacije korisnik ima tri opcije odabira vatrenog zida, gde bira između : firewall-a, ili firewall-a sa optimalnim podešavanjima ili firewall-a sa maksimalnim sistemom zaštite. Nakon instalacije Comodo firewall automatski prebacuje na "Safe Mode", koji generiše brojna popup upozorenja za aplikacije koje nisu na listi pouzdanih aplikacija. Comodo firewall ograničava učestala upozorenja za automatsko ažuriranje nekih programa gde ograničavaju neke aplikacije da pristupe internetu.

Interfejs programa:

Osnovni izgled prozora ima tri glavna menija: rezime, bezbednosti i aktivnosti, a većina podešavanja se vrši preko srednjeg menija. Postoji kategorija pod imenom napredna bezbednost, gde se nalaze složenija podešavanja, što korisnici mogu da iskoriste ako žele da utanače sistem zaštite.

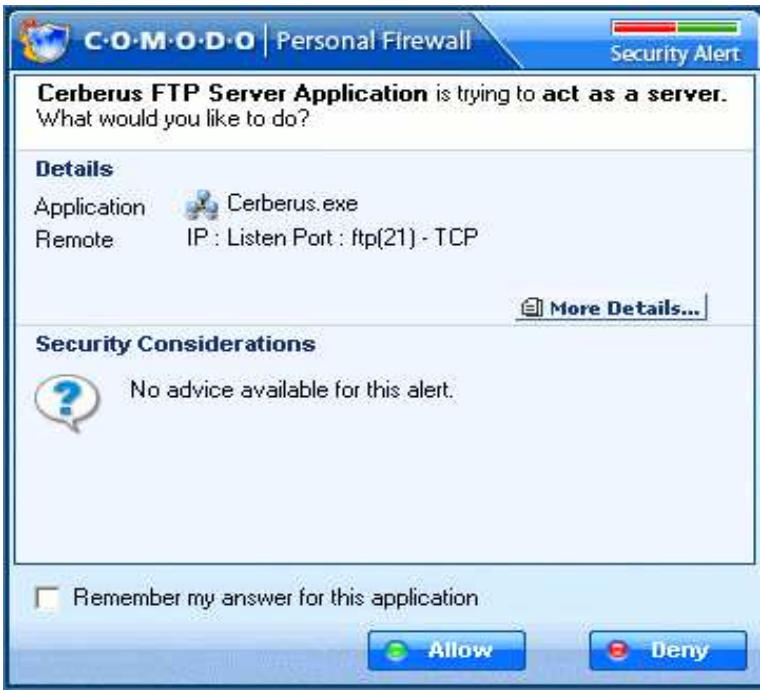


Slika 16 - početna strana programa

Zaštita i konekcija:

Comodo firewall je više od zaštitnog zida, ima sredstva za detekciju i blokadu virusa, trojanaca, crva, rutkit virusa i drugih zlonamernih programa u realnom vremenu.

• (Brown, 2011). Bilo koja aplikacija koja pokušava da radi na računaru, firewall proverava ovlašćenja u odnosu na bazu podataka fajlova gde se proverava da li je aplikacija dobra ili loša.



Slika 17 - pokušaj pristupa mreži

Comodo proverava nepoznate datoteke u virtuelnoj sobi "sandbook" gde se odkriva njihova namera i tako biva puštena ili odbijena kroz sistem. Iako firewall sadrži i antivirusni proizvod koji može posebno da se instalira ili deinstalira, antivirus se može instalirati nezavisno od zida. Korisnici mogu da odluče da li će uporedno koristiti Comodo Antivirusni program ili samo Comodo firewall.

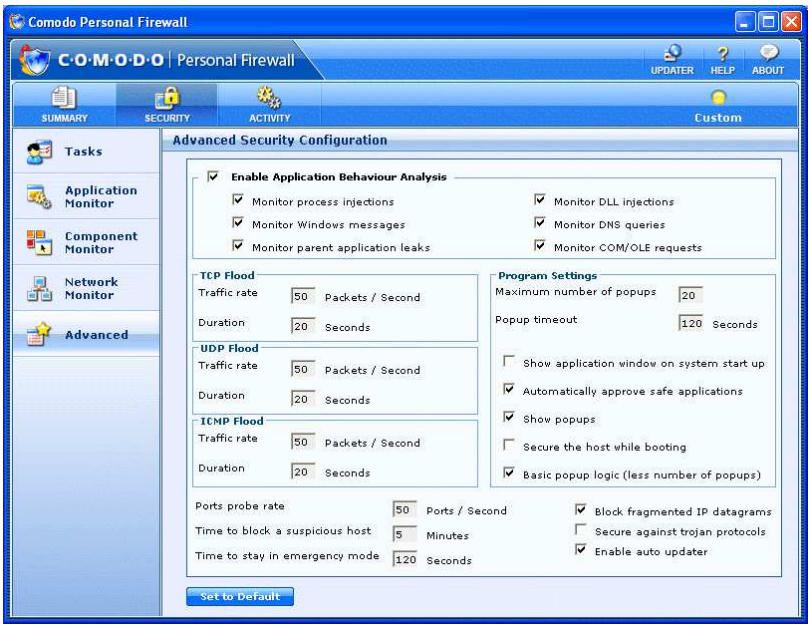
U cilju zaštite korisnika koji mogu da pristupe sa javne Wi-Fi mreže, Comodo obezbeđuje šifrovani internet proxy servis (128-bitna enkripcija). Firewall obaveštava korisnika da pravi rezervne kopije podataka i takođe obezbeđuje 2 GB prostora za online skladištenje podataka na mreži. • (10TopTenRewiews, 2013)

• Brown, B. C. (2011). How to Stop E-Mail Spam, Spyware, Malware, Computer Viruses and Hackers. Ocala, Florida: Atlantic Publishing Company.

• 10TopTenRewiews. (2013). *Personal Firewall Software Review*. Retrieved 2013 from 10TopTenRewiews: http://personal-firewall-software-review.toptenreviews.com/comodo-internet-security-pro-review.html

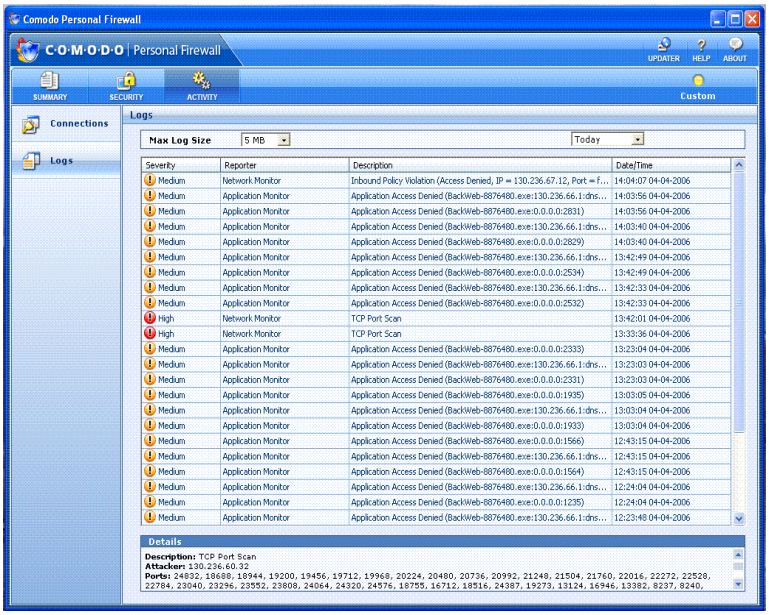
Dodatne bezbednosne funkcije:

Comodo firewall pruža funkcije koje olakšavaju početnicima da shvate kako da se odgovori na iskačuće prozore i upozori kada nastupa zlonamerni napad. Korisnik može da vidi "Izbor bezbednosti" koji su generisani u Comodo bazu podataka i s time da se odgovori na moguću pretnju. Ukoliko korisnik ne može da odgovori na datu pretnju, tada može da nađe dodatne informacije na funkciji "ThreatCast" gde može da razmeni iskustva sa milionima korisnika koji su možda imali sličan napad. Nakon pronalaženja odgovor od Threatcast zajednice, korisnik može da dozvoli, blokira ili primeni predefinisane sigurnosne polise. Na osnovu baveštenja, Comodo podstiče korisnika da odluči da li treba da zapamti mogući napad i tako primeni odgovor na slične situacije u budućnosti bez upozorenja.



Slika 18 - dodatne sigurnosne postavke

Comodo uključuje "memorijsku firewall" (protiv preteranih napada) gde ograničava put nepoznatih programa i novijih softvera koji pristupaju na računar tako da instalacija može da poremeti rad računara. Korišćenjem opcije sandbox, zaštita je ograničena na negativna delovanja malware programa. Sa ovom opcijom održava se popis poznatih sigurnih aplikacija, ali i ograničava se ulazak nepoznatih aplikacija kroz vatreni zid. Comodo firewall pre pristupa na sistem pita korisnik koju funkciju da koristi. Novo izdanje sadrži user friendly opcije po defaultu, gde omogućava iskusnim korisnicima da imaju kontrolu nad portovima, protokolima i konfiguracijama.



Slika 19 - prikaz log fajlov

Pomoć, podrška i dnevnik aktivnosti:

Uputstvo za upotrebu je odlično, precizno i potpuno. Svaki korisnik ima 24/7 pristup ćaskanju na ("LivePCSupport") gde komunicira sa tehničarima o proizvodu i to bez dodatnih troškova.

Potrebni resursi računara:

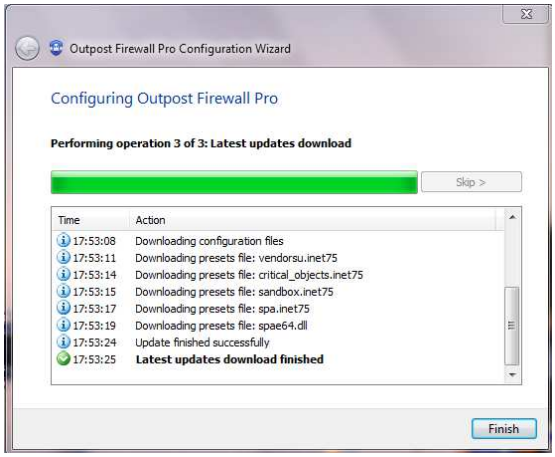
Windows XP SP3 ili više (32-bit), Windows Vista SP1 (32- i 64-bit),Windows 7 (32- i 64-bit), Windows 8 (32- i 64-bit), 512 MB RAM za XP, 2 GB RAM za Vistu i Windows 7, 550 MB slobodnog prostora, 1 GHz processor

10.2 Agnitum Outpust Pro Firewall

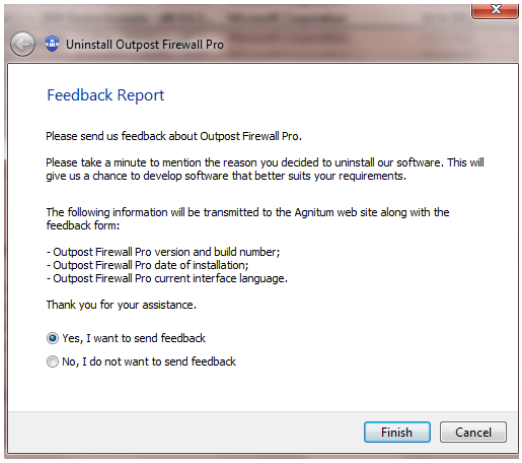
Instalacija i deinstalacija :

Instalacija se sastoji od niza pitanja, u kojem direktorijumu da se istalira program, da li se prihvataju licence programa, proverava se da li ima slično instaliranih programa i obaveštava korisnika ako postoje programi koji nisu kompatabilni sa firewall-om. Tokom instalacije program skida potrebne dopune za proizvod i instalira ih u direktorijum sa firewall-om. Korisnik može da bira između automatske konfiguracije sistema ili između čarobnjaka koji vodi korisnika kroz sistem podešavanja programa. Nakon instalacije, ako korisnik izabere opciju čarobnjaka, tada se preuzima kontrola i stvara nova konfiguracija ili se učitava konfiguracija ako je korisnik instalirao stariju

verziju Outpost Firewall Pro. Čarobnjak pita korisnika da li želi da program automatski postavi pravila za sistem i dopuni ih sa sajta proizvođača ili da ostavi korisniku da ih samostalno unese. Nakon instalacije potrebno je restartovati sistem da bi firewall mogao da se konfiguriše za operativni sistem. Deinstalacija programa se može uraditi veoma brzo, gde korisnik može kroz nekoliko koraka da obriše program sa svog računara. Kada se deinstalacija izvrši, Agnitum firewall pita korisnika iz kojih razloga se briše proizvod sa sistema.



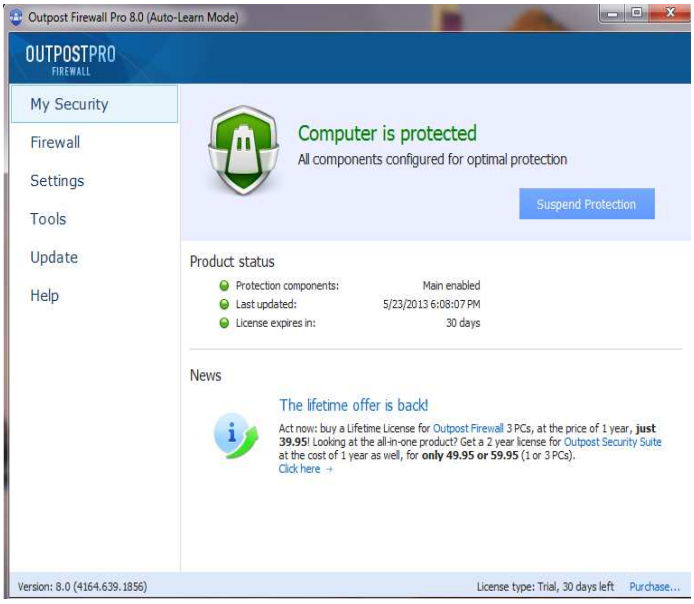
Slika 20 - instalacija programa



Slika 21 - deinstalacija programa

Korisnički interfejs:

Korisnički interfejs prikazuje kontrole na jasan način. Na početnoj strani interfejsa nalazi se nekoliko glavnih komandi za konfiguraciju firewall-a. Meni pod imenom "Firewall" prikazuje trenutno uključene programe koji se lako mogu deaktivirati. U meniju "Settings" korisnik može da postavi ručno pravila filtriranja paketa, kao i naprednija -

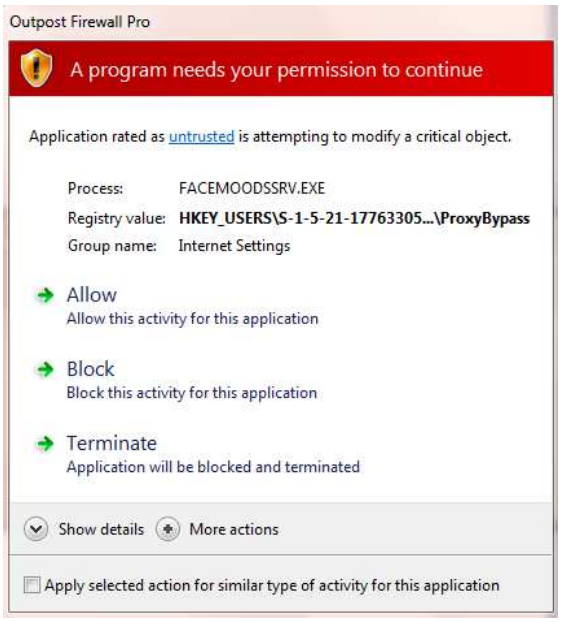


Slika 22 - izgled glavnog prozora

podešavanja mogu da se izvrše pod komandom "Advanced settings". Alatka "Tools" prikazuje koji procesi se odvijaju u pozadini sistema. Interfejs Outpost firewall-a je osmišljen za korisnike koji nemaju dovoljno iskustva sa administriranjem programa. [•] (Rubenking, 2006)

Zaštita i konekcija:

Portovi na računaru su blokirani i zaštićeni po defaultu programa. Automatskom konfiguracijom sistema se podrazumeva da nema iskačućih prozora tj. prozora obaveštenja ako se vrši prenos paketa. Korisnici ne mogu da pristupe podešavanjima koje je firewall administator odredio. Firewall u sebi sadrži dodatak za otkrivanje i skeniranje dodatnih uređaja koji se kače na sistem.



Slika 23 - blokiranje pristupa

Kada korisnik želi da pristupi Internetu, dobijaju se upozorenja koja su prikazana u pozadini ekrana. Tada se traži od korisnika da dopusti ili blokira vezu.

Agnitum Outpust firewall ne obaveštava korisnika o pokušaju upada u sistem ovaj nedostatak može da predstavlja problem kod odabira proizvoda. Nedostatak se može odkloniti pomoću konfiguracije firewall pravila, ali se mora dodeliti tačno pravilo za dolazni FTP saobraćaj tako da firewall prepoznaje šta je dobar, a šta zlonameran saobraćaj. [•] (Kompjuterska.biblioteka, 2007) Nedostatak Outpust firewall-a predstavlja nedovoljna obaveštenost korisnika. Nema obaveštenja o postojanosti novije verzije programa ili ne postoji obaveštenje o dopuni baze samog programa.

[•] Rubenking, N. J. (2006, Februar 21). Spyware. *PC Magazine* , 99.

[•] Kompjuterska.biblioteka. (2007, Septembar 20). *KAKO DA vaš računar ostane bezbedan*. Retrieved from Kompjuterska biblioteka: http://saveti.kombib.rs/KAKO_DA_vas_racunar_ostane_bezbedan_-_7._deo.html

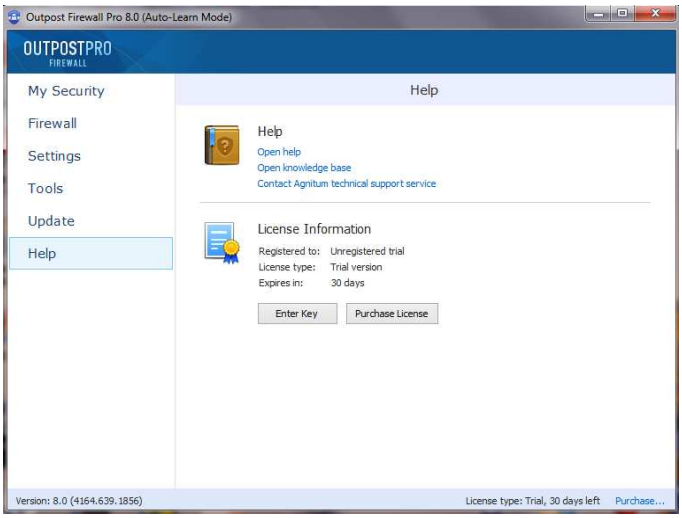
Korisnik se nalazi u situaciji ne informisanosti . Što se tiče same aktivacije i deaktivacije firewalla postoji opcija za ovu aktivnost koja se može naći na statusnoj liniji windowsa.

Dodatne bezbednosne funkcije:

Ključna konkurentna razlika za ovaj softver jeste sposobnost zaštite na određenim datotekama i direktorijumima. Korisnički interfejs je koncipiran tako da je moguće učitati program da radi u pozadini sistema, tako da administratori sistema mogu blokirati sadržaj ili promet u skladu s pravilima koje korisnici ne mogu videti. Kad firewall radi u pozadini ekrana, igre i druge aplikacija koje zahtevaju full-screen mod mogu se pokrenuti bez uplitanja firewall upozorenja . Ovaj softver je namenjen još i za borbu protiv spyware koji pokušavaju pristupiti na sistem putem USB uređaja . • (10TopTenRewiews, 2013)

Pomoć, podrška i dnevnik aktivnosti:

Firewall ima ugrađenu opciju za pomoć korisniku. U većini prikaza postoji dugme sa upitnikom preko kojeg se mogu dobiti informacije sa sajta proizvođača. Online resursi se sastoje od blogova, foruma korisnika i baze znanja. Kompletna dokumentacija se može lako pronaći na web stranici Agnituma. Podrška je dostupna putem e-maila ili preko chat (07:00-16:00 GMT).Web stranica nudi prečice koje omogućavaju posetiocima da pročitaju stranice na engleskom, nemačkom, francuskom, mađarskom, poljskom



Slika 24 - meni za pomoć korisniku

• 10TopTenRewiews. (2013). *Personal Firewall Software Review*. Retrieved 2013 from 10TopTenRewiews: http://personal-firewall-software-review.toptenreviews.com/-Agnitum_Outpust_firewall_review.html

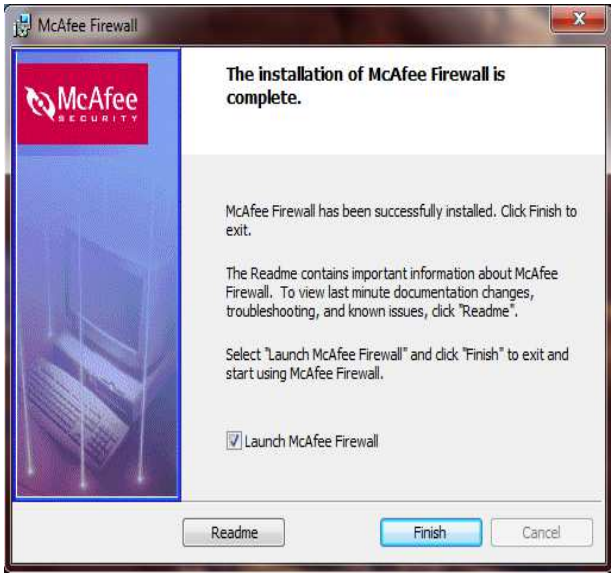
i ruskom jeziku. Log fajlovi koje firewall kreira se mogu naći u log pregledaču. Ovaj pregledač daje uvid u funkcionalnost firewall-a gde se mogu naći zapisi svih aktivnosti i pravila koja su izvršila filtriranje i prekid saobraćaja.

Potrebni resursi računara:

Testirana verzija programa je : 2009 - v6.51, veličina programa: 98,81 MB
Kompatibilnost sa operativnim sistemima: Windows 7, Vista, XP
Zahtevi računara: Windows XP (SP2), 450 MHz CPU, 256 MB RAM, 200 MB slobodnog diska.

10.3. McAfee Firewall

Instalacija i deinstalacija: Instalacija proizvoda je brza i laka. Nije potrebno restartovati računar posle instalacije. Firewall se konfiguriše sam po fabričkim postavkama, tako da ne iskusan korisnik može odmah da koristi program. Nakon instalacije potrebno je omogućiti pristup Internetu za aplikacije, a zatim korisnik može odlučiti koji nivo ograničenja da koristi. Deinstalacija programa se odvija brzo, uz par koraka program se briše potpuno sa sistema.



Slika25- instalacija programa.

Interfejs programa:

Interfejs programa se sastoji iz četiri menija. U meniju "Summary" se može videti da li je sistem u funkciji, koliki je dnevni promet i koliko je pravila promenjeno. Ostali meniji se odnose na Internet saobraćaj, log fajlove i konfiguracija firewall-a.



Slika26 - izgled glavne strane programa

Zaštita i konekcija:

McAfee Internet Security je dvosmerni firewall program koji je osmišljen kako bi blokirao pokušaje upada u sistem izvana i iznutra mreže. McAfee u sebi sadrži listu pretnji i ne dopušta da se one izvršavaju. Nažalost, McAfee firewall ne pokazuje visoku stopu uspeha kada je podvrgnut simulacijama naprednih hakerskih tehnika. Često ne štiti od zlonamernog koda koji pokušava preživeti ponovno podizanje sistema. Mnoge testove curenja podataka takođe dizajnirani da prevare rad firewall-a prolaze kroz firewall komunicirajući sa spoljnim svetom. Često se pokazuje kao slabost napad na procese koji McAfee koristi u svom radu.



Slika27 - prozor upozorenja

Po fabričkim postavkama samo se izlazne konekcije alarmiraju, ali mogu se sve ulazno izlazne konekcije konfigurisati u programu tako da korisnik može da vidi aktivan saobaćaj.

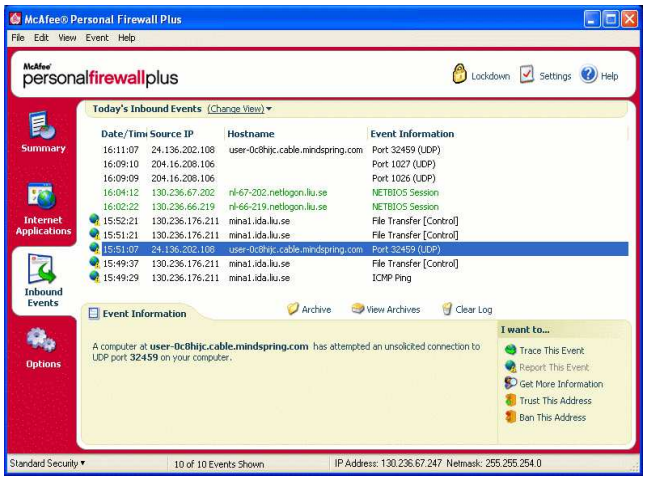
Dodatne bezbednosne funkcije:

McAfee proizvod je više nego firewall, on takođe pronalazi adware i rootkit viruse. Razne vrste skeniranja su dostupna za otkrivanje virusa i spywarea. Proizvod otkriva i blokira spam. Pruža upozorenja o Antiphishingu i daje mogućnosti korisniku da u slučaju napada odluči šta da čini. Web stranice proverava od malwarea koda i daje upozorenja, tako da korisnik može da izbegne rizik. Postoji opcija za roditeljsku kontrolu-saobraćaja koja omogućava korisniku da ograniči ono što dete može učiniti ili videti. Roditelj može primeniti lozinku za administraciju roditeljske kontrole, tako da niko ne može promeniti postavke firewall-a. Firewall sadrži i dodatne korisne alate kao što su sposobnost za brisanje nepotrebnih datoteka koje utiču na performanse

sistema. Proizvod takođe daje korisnu alatku za defragmentaciju diska, optimizaciju diska i skladištenje podataka. [•] (10TopTenRewiews, 2013)

Pomoć, podrška i dnevnik aktivnosti:

McAfee Internet Security firewall uključuje virtualnog tehničara koji pokušava dijagnosticirati i zatim rešiti probleme. Ako virtuelni tehničar ne uspe rešiti problem, postoji prečica za korisnika s relevantnim informacijama u online bazi znanja. Podrška putem e-maila i chat je dostupan za besplatno korištenje. Telefonska podrška je besplatna za prvih 30 dana od pretplate. McAfee takođe ima blog i stranicu na Facebooku.



Slika 28- log fajlovi

Potrebni resursi računara:

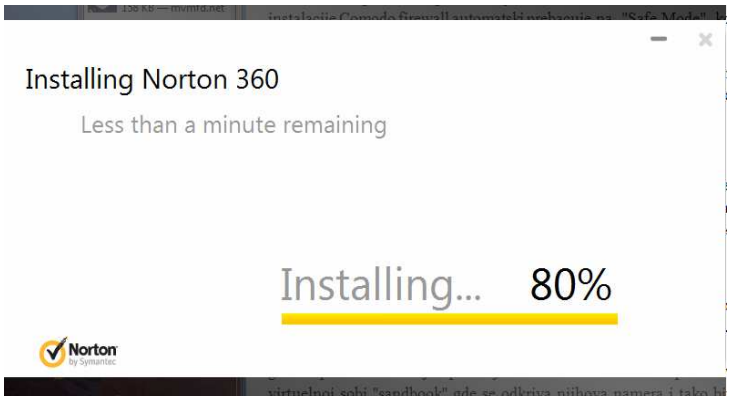
Windows XP SP3 ili više (32-bit), Windows Vista SP1 (32- i 64-bit), Windows 7 (32- i 64-bit), Windows 8 (32- i 64-bit), 512 MB RAM za XP, 2 GB RAM za Vistu i Windows 7, 600 MB slobodnog prostora , 1.2 GHz processor

10.4 Norton 360 Firewall

Instalacija i deinstalacija :

Tokom instalacije Norton Personal firewall traži sigurnosne stavke o programu, tipa licence i registracije korisnika. Odmah nakon restarta računara , firewall dopunjava svoju bazu podataka i dopunjuje firewall program potrebnim zakrpama sa Interneta. Zatim je potrebno još jedno podizanje sistema da bi se instalirale i utvrdile skinute zakrpe. Deinstalacija programa je brza i uklanjaju se svi ostaci od programa.

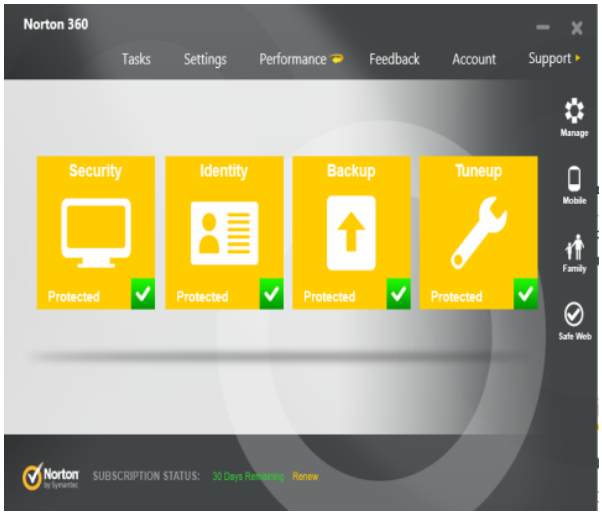
[•] 10TopTenRewiews. (2013). *Personal Firewall Software Review*. Retrieved 2013 from 10TopTenRewiews: http://personal-firewall-software-review.toptenreviews.com/mcafee-internet- security-review.html



Slika 29- instalacija programa

Interfejs programa:

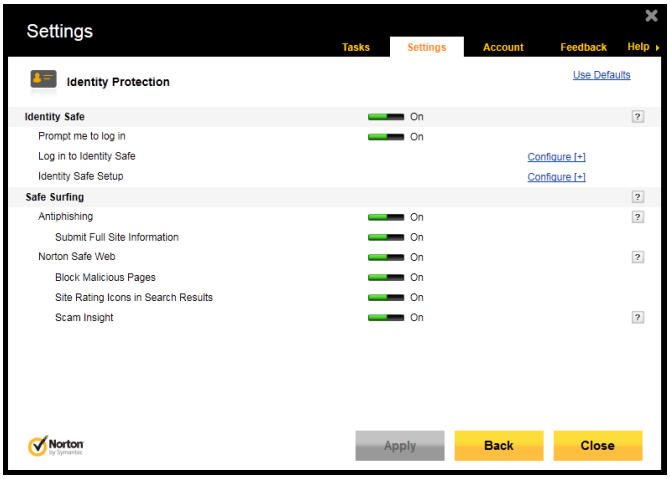
Symantec proizvodi su dizajnirani kako bi bili jednostavniji za korištenje. Pa tako i interfejs programa izgleda veoma jednostavno i pregledan je za korisnika. U cilju zaštite i bezbednosti korisnika, Norton Internet Security skenira računar u stanju mirovanja, a ne prikazuje upozorenja, dopune i druge iskačuće prozore ako korisnik gleda film ili igra igru u full-screen modu.



Slika 30- izgled glavnog proz

Zaštita i konekcija:

Po fabričkim postavkama programa, firewall je postavljen u stanje "učenja", gde sve aplikacije mogu da pristupe Internetu bez upozoreja. Kad WinSCP želi da pristupi mreži, firewall obaveštava da je usvojio postojeću aktivnost kao sigurnu konekciju.

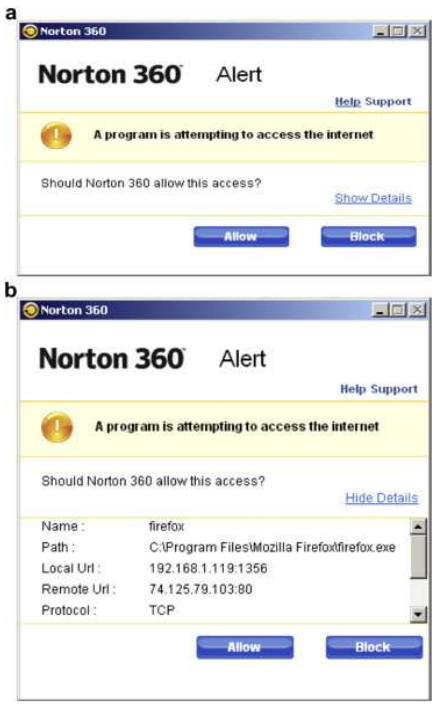


Slika31 - prozor za konfiguraciju firewall-a

Neke aplikacije kao što su Firefox i Internet Explorer preko kojih se želi pristupiti Internetu, Norton Personal firewall kreira skriptu konekcija koje se mogu izvršavati. Pravila se odnose na konekcije tipa Http, ftp cliente i DNS saobraćaj tako da svaki korisnik može preko njih da pristupi Internetu. Što se tiče dolazne konekcije po fabričkim postavkama je nameštено da se sav dolazni saobraćaj dozvoljava. Firewall kreira listu aktivnosti i alarmira.

Dodatne bezbednosne funkcije:

Na osnovni nivo zaštite, Norton Security nadilazi firewall zaštitu blokiranjem portova, rootkit, spyware, trojanski konja, virusa i crva. Svakih pet do petnaest minuta, proizvod se osvežava s potpisima najnovijih pretnji. Pretnje se sakupljaju preko obaveštajne Symantec Global mreže.• (Smith, 2012) Proizvod proverava autentičnost web stranice i blokira internet stranice koje pokušavaju izvršiti phishing ekspedicije. Na naprednom nivou, Norton Internet Security filtrira spam i uključuje roditeljsku kontrolu. Proizvod takođe skenira pristigle poruke od malware. Ako je računar već zaražen, Norton proizvod koristi Recovery alatku za ponovno uspostavljanje sistema.



Slika 32- upozorenje o napadu

Pomoć, podrška i dnevnik aktivnosti:

Symantec nudi dobru online bazu znanja, obrazovne videa i 24/7 podršku putem chata, e-maila ili telefona. Symantec takođe poseduje interaktivni korisnički forum, ali se takođe može pristupiti i informisati preko Facebook i Twitter naloga.

Potrebni resursi računara:

Windows XP SP3 ili više (32-bit), Windows Vista SP1 (32- i 64-bit),Windows 7 (32- i

---

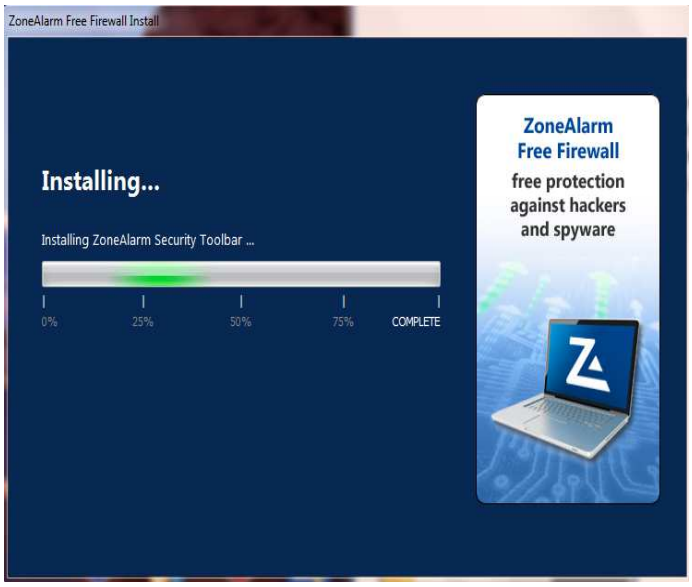
• Smith, T. J. (2012). Pricing Strategy: Setting Price Levels, Managing Price Discounts. Mason, USA: CengageBrain.

64-bit), Windows 8 (32- i 64-bit), 512 MB RAM za XP, 2 GB RAM za Vistu i Windows 7, 550 MB slobodnog prostora, 1000 MHz processor.

10.5 ZoneAlarm Pro Firewall 6.1

Instalacija i deinstalacija :

Instalacijski postupak je prijateljski nastrojen prema korisniku, sastoji se od niza dijaloški okvira koji vode korisnika kroz proces. Nema posebno teških pitanja. Treba napomenuti da se postavlja pitanje preglednika tj. da li bi trebao biti dopušten pristup mreži po defaultu. Deinstalacija traje kratko. Posle deinstalacije programa potrebno je restartovati sistem da bi se uklonili svi ostaci programa.



Slika 33- instalacija programa

Interfejs programa:

Interfejs programa je osmišljen tako da korisnik može lako da se snađe sa postavkama firewall-a. Zone alarm firewall blokira hakere da se infiltriraju u kućni PC, skrivanjem računara od neželjenog mrežnog saobraćaja. [•] (Bennett, 2004).Ovaj softver između ostalog donosi osnovnu firewall zaštitu, omogućava da budete - nevidljivi za druge korisnike koji su online, dok novi interfejs olakšava rad sa softverom. Nova verzija rešava probleme koji su postojali vezano za kompatibilnost



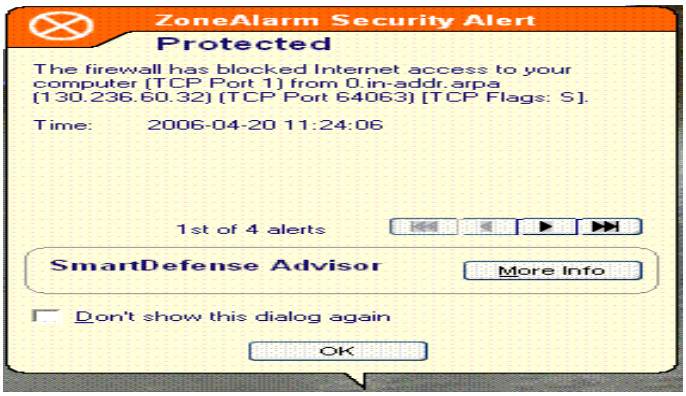
Slika 34 - izgled glavnog prozora programa

[•] Bennett, J. (2004). The Digital Umbrella: Technology's Attack on Personal Privacy in America. Boca Raton, Florida: Brown Walker Press.

sa XP SP2. Na početnoj strani su vidljiva četiri menija od kojih svaki ima opciju za konfiguraciju. Korisnik može da vidi da li je firewall uključen . Postoje i napredna podešavanja, ali ona su veoma komplikovana za korisnike početnike.

Zaštita i konekcija:

Firewall sprečava pokušaj skeniranja portova. Sve pokušaje pristupa Internetu obaveštava se korisnik za svaku konekciju i javlja se da li je veza bila blokirana. Po defaultu firewall upozorava samo na izlazni saobraćaj i pokušaj spajanja prethodno nepoznatih aplikacija.

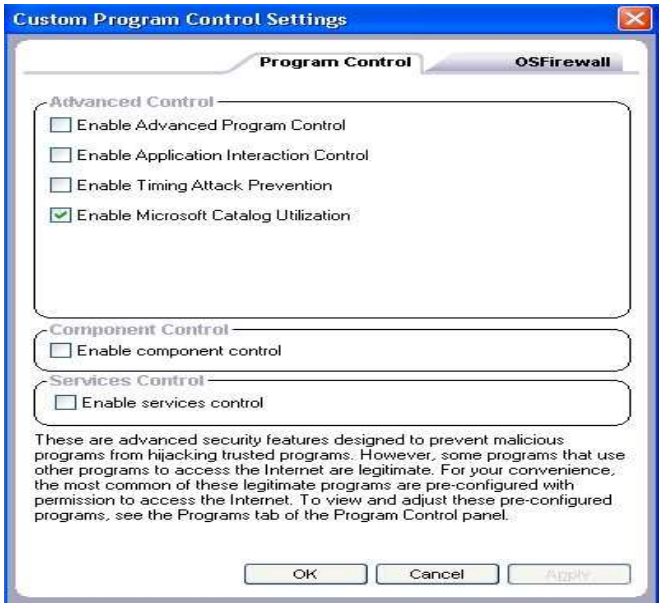


Slika 35 - obaveštenje o blokiranju saobraćaja

Dodatne bezbednosne funkcije:

Dodatne bezbednosne funkcije u Zonealarm firewall-u uključuju mogućnost analize programa prilikom preuzimanja sa Interneta i sposobnost za proveru autentičnosti web stranica jesu li opasne ili sigurne po korisnika. Proizvod sadrži opciju za testiranje i preuzimanje u sigurnom virtualnom okruženju u slučaju da se manifestuju opasne karakteristike.

- (10TopTenRewiews, 2013)



Slika 36 - dodatne kontrole programa

- 10TopTenRewiews. (2013). *Personal Firewall Software Review*. Retrieved 2013 fr 10TopTenRewiews: http://personal-firewall-software-review.toptenreviews.com/zonealarm-pro- review.html

Pomoć, podrška i dnevnik aktivnosti:

Osim on-line baze znanja, blog, forum korisnika i prisutnost na Facebooku i Twitteru, Check Point nudi korisnicima usluga chat-24/7. Tehnička podrška-chat je dostupan radnim danom od 8:00-22:00 u Sjedinjenim Američkim Državama (CST). Verzije za nadogradnju programa su besplatne za prvih 12 meseci. Dnevnik aktivnosti je integrisan u glavnom prozoru vatrenog zida. Važno je napomenuti da samo 999 stavki se mogu pregledati, što znači da log informacije mogu nestati pre nego što korisnici žele da provere aktivnosti sistema. Ne postoji filtriranje log sadržaja po stavkama što otežava pregled.

Potrebni resursi računara:

Windows XP SP3 ili više (32-bit), Windows Vista SP1 (32- i 64-bit), Windows 7 (32- i 64-bit), Windows 8 (32- i 64-bit), 256 MB RAM za XP, 2 GB RAM za Vistu i Windows 7, 480 MB slobodnog prostora, 700 GHz processor

11. Programi za testiranje firewall-a:

Programi za testiranje na firewall-u su kreirani tako da prikažu korisniku koje su to tehnike za primenu nad firewall-om kako bi zlonamerni korisnik pristupio računarskom sistemu. Najpopularnije tehnike koje se koriste za proveru zaštitnog zida su testovi protiv curenja podataka, špijunski testovi, autorun testovi, testovi samoodbrane i ostali testovi koji prikazuju reakciju sistema posle nekog perioda. • (Matousec, 2013). Ove tehnike su izabrane zbog toga što se treba voditi na tri osnovna principa zaštite. Prvi princip zaštite se odnosi na spoljšnji uticaj zlonamernih korisnika (saobraćaj izvan računarske mreže) gde su testovi samoodbrane idealni za proveru sistema. Korisnici mogu da provere svoje firewall programe da li propuštaju spoljašnji saobraćaj tj. saobraćaj sa interneta.• (Ec-Council, 2011) Drugi princip zaštite se odnosi na testiranje unutar računarske mreže, gde korisnici mogu da

- Matousec. (2013). *Matousec*. From matousec.com: www.matousec.com/projects/proactive-security-challenge-64
- Ec-Council. (2011). *Network Defense: Security Policy and Threats.* New York: Ec-Council.
- Joshi, J. (2008). *Network Security: Know It All: Know It All.* Burlington: Morgan Kaufman Publischers.

provere da li zaštitini zid može da se izbori sa napadima koji se dešavaju u samom sistemu. Najbolji vid testiranja su testovi za curenje podataka i autorun testovi. [•] (Joshi, 2008) . Ove dve vrste testova treba da odkriju da li postoji pretnja po sistem sa unutrašnje strane mreže. Treći princip zaštite se odnosi na testove koji imaju zadatak da manipulišu s računarskim sistemom posle nekog određenog perioda, tj. korisnici ne primećuju promene sve do sledećeg uključivanja sistema . Ova tri principa treba da budu stub svakog testiranja firewall-a i zbog bezbednosti sistema izabrani su jer predstavljaju najosnovnije procese napada koje firewall treba da prepozna i spreči.

Svi testovi su dostupni sa izvornim kodovima. Detaljno su objašnjeni i nalaze se na CD-u sa drugim pristupnim radom. Za svaki sprovedeni test na sistemu dodeljena je ocena po učinkovitosti testiranog programa. Svi testirani programi su ocenjeni između 0% i 100%. Testovi su izvršavani tako da su bili pokrenuti na računaru gde je pre testiranja bio instaliran testirani firewall. Kako su test programi zahtevali izlaz ka Internetu zbog slanja podataka, na testiranom računaru je postojao priključak ka Internet. Test programi su klasifikovani po sistemu na kojem rade i svi testovi su podeljeni po kategorijama. Za svaku kategoriju se nalazi nekoliko metoda testiranja. Svaki test je bio pokrenut nekoliko puta iz razloga da se proveri da li je sistem lažno alarmirao ili je propustio napad. U mnogim slučajevima su metode testiranja prolazile ili bile sprečene. Kategorije su podeljene po vrstama i svakoj vrsti je dodeljeno nekoliko test programa (simulacije napada).

Podela i vrsta testova :

Leak-test: Ovi testovi imaju za zadatak da prikažu curenje podataka iz sistema. Leak-testovi pokušavaju poslati podatke na Internet preko izlaznih portova i putem Internet Explorera[•] (Furnell, 2004) . Da bi ovi testovi mogli da se ispitaju potrebno je obezbediti računar sa stalnom konekcijom na Internet. Od testiranog firewall-a se očekuje da prepozna pomenutu aktivnost i spreči konekciju.[•] (Matousec, 2013)

• Furnell, S. M. (2004). Using security: easier said than done. Computer Fraud & Security. United Kingdom: Browse journals.

• Heng Yin, D. S. (2013). Automatic Malware Analysis: An Emulator Based Approach. New York: Springer.

Špijunski testovi: Ova vrsta testiranja simulira pokušaj napada na špijunažu korisnika ili podataka. Prati se rad korisnika i pokušava se pristupiti njegovim korisničkim nalozima, lozinkama, podacima, aktivnostima. Keylogger i paket sniffer su tipični primeri špijunskih programa[•] (Heng Yin, 2013). Od testiranog firewall-a se očekuje prepoznavanje napada i brisanje aktivnosti pa čak i malicioznog programa koji izvršava napad.[•] (Matousec, 2013)

Autorun testovi: Ovi testovi se pokušavaju sami instalirati na sistem kako bi se osigurali da se ponovo pokrenu. Njihova uloga je da rade u pozadini operativnog sistema i da opstruiraju njegov rad. Najčešći cilj Autorun testova je ponovno podizanje sistema. Autorun testovi su tipični primeri za sve vrste malwarea koda. [•] (Matousec, 2013)

Test samoobrane: Ova kategorija testova uključuje razne napade na sigurnost samog firewall-a. Testovi imaju zadatak da ispitaju štetu na sistemu i procese koji se izvršavaju. Osim procesa, firewall softveri se obično oslanjaju na razne datoteke, stavke iz registra i politiku zaštite samog firewall-a. Testovi koji pokušavaju ukloniti, uništiti ili oštetiti postavke sistema se takođe nalaze u ovoj kategoriji.
[•] (Matousec, 2013)

Ostali testovi: Testovi koji se ne uklapaju u bilo koji od prethodno definisanih tipova testiranja. Na primer, testovi koji zlonamerno menjaju sistem, gase računar, brišu procese u sistemu, menjaju interfejs programa .

[•] Matousec. (2013). *Matousec*. From matousec.com: www.matousec.com/projects/proactive-security- challenge-64

[•] Matousec. (2013). *Matousec*. From matousec.com: www.matousec.com/projects/proactive-security-challenge-64

11.1 Test programi • (Matousec, 2013)

VBStest.exe - Test curenja podataka
*Opis:*Test proverava firewall da li zlonamerni program može da zaobiđe zaštitu pomoću Visual Basic skripte
IDENTIFIKOVAN - test je sprečen pomoću firewall-a da pošalje podatke na Internet
NEIDENTIFIKOVAN – test je bio u stanju da šalje podatke na Internet, a firewall ga ne tretira kao pretnju.
CopyCat.exe - Test curenja podataka
Opis: proverava firewall da li zlonamerni korisnik može da zarazi Internet Explorer i njegovu memoriju koristiti za slanje podataka na Internet server
IDENTIFIKOVAN - test je sprečen pomoću firewall-a da pošalje podatke na Internet
NEIDENTIFIKOVAN – test je bio u stanju da šalje podatke na Internet, a firewall ga ne tretira kao pretnju.
DDEexec.exe - Test curenja podataka
Opis: DDEexec.exe pokušava poslati podatke na Internet server manipulisanjem HTTP protokola
IDENTIFIKOVAN - test je sprečen pomoću firewall-a da pošalje podatke na Internet
NEIDENTIFIKOVAN – test je bio u stanju da šalje podatke na Internet, a firewall ga ne tretira kao pretnju.
Leaktest.exe - Test curenja podataka
Opis: **Leaktest.exe** proverava curenje podataka i paketa preko TCP porta na Internet.
IDENTIFIKOVAN - test je sprečen pomoću firewall-a da pošalje podatke na Internet
NEIDENTIFIKOVAN – test je bio u stanju da šalje podatke na Internet, a firewall ga ne tretira kao pretnju.
Yalta.exe - Test curenja podataka
Opis: **Yalta.exe** proverava curenje podataka - paketa preko UDP[22] porta na Internet.
IDENTIFIKOVAN - test je sprečen pomoću firewall-a da pošalje podatke na Internet
NEIDENTIFIKOVAN – test je bio u stanju da šalje podatke na Internet, a firewall ga ne tretira kao pretnju.
Eho.exe - Test curenja podataka
Opis: **Eho.exe** proverava da li testirani proizvod ima filtere za ICMP[23] saobraćaj .
IDENTIFIKOVAN - test je sprečen pomoću firewall-a da pošalje podatke na Internet
NEIDENTIFIKOVAN – test je bio u stanju da šalje podatke na Internet, a firewall ga ne tretira kao pretnju.
Coat.exe - Test curenja podataka
Opis: ***Coat.exe*** proverava da li testiran proizvod ispravno identifikuje pouzdane procese. Test pokušava da promeni svoju identifikaciju tako da izgleda kao Internet Ekplorer i šalje podatke na Internet.
IDENTIFIKOVAN -test je sprečen pomoću firewall-a da pošalje podatke na Internet
NEIDENTIFIKOVAN – test je bio u stanju da šalje podatke na Internet, a firewall ga nije registrovao i uklonio.

---

[22] ***UDP****(engl. User Datagram Protocol) je jednostavan protokol koji obezbeđuje osnovne funkcije transportnog sloja OSI modela.*
[23] ***ICMP*** *(engl. Internet Control Messageing Protocol) je protokol sloja mreže koji obezbeđuje pojedine mehanizme oglašavanja.*

Jumper.exe - Test curenja podataka
Opis: **Jumper.exe** konfiguriše Internet Ekplorer tako da kada se pokrene program odmah se šalju podaci na internet preko
IDENTIFIKOVAN - test je sprečen pomoću firewall-a da pošalje podatke na Interneti da konfiguriše Internet Explorer
NEIDENTIFIKOVAN – test je bio u stanju da šalje podatke na Internet, a firewall ga ne tretira kao pretnju.
DNStester.exe - Test curenja podataka
Opis: **DNStester.exe** test proverava da li testirani firewall prevodi imena računara DNS[24]
IDENTIFIKOVAN testu je sprečeno od strane firewall-a da prevodi imena računara
NEIDENTIFIKOVAN- testu je dozvoljeno od strane firewall-a da prevodi imena računara
Schedtest.exe - Test curenja podataka
Opis: **Schedtest.exe** ima zadatak da zakaže nove zadatke koristeći Task Scheduler
IDENTIFIKOVAN - test je sprečen da zakaže prilagođeni zadatak u Task Scheduleru
NEIDENTIFIKOVAN test je bio u mogućnosti da zakaže prilagođeni zadatak u Task Scheduler
AVFT4.exe - Test curenja podataka
Opis: **AVFT4.exe** proverava procese u Windows Ekploreru i proverava iskorištenu memoriju gde ubacuje zaraženi kod i tako gasi procese.
IDENTIFIKOVAN - test je sprečen pomoću firewall-a da manipuliše Windows Ekplorererom
NEIDENTIFIKOVAN – test je bio u stanju da šalje podatke na Internet, a firewall ga ne tretira kao pretnju.
Keylog4.exe - Test za špijuniranje
Opis: **Keylog4.exe** test koristi Windows prečice za prolazak kroz sistem i pomoću njih ulazi u sistem
IDENTIFIKOVAN -test je sprečen da pristupi sistemu i obrisan je od strane firewall-a
NEIDENTIFIKOVAN - test je propušten u sistem i nije detektovan od strane firewall-a
Screenlog.exe - Test za špijuniranje
Opis: **Screenlog.exe** test proverava da li maliciozni program može da uslikava slike sa ekrana.
IDENTIFIKOVAN -test je sprečen da pristupi sistemu i obrisan je od strane firewall-a
NEIDENTIFIKOVAN - test je propušten u sistem i nije detektovan od strane firewall-a
ProxyTest.exe - Test za špijuniranje
Opis: **ProxyTest.exe** proverava firewall da li je maliciozni program sproveo Internet saobraćaj na inficirani proxy server
IDENTIFIKOVAN -test je sprečen od strane firewall-a da usmeri saobraćaj ka inficiranom proxy serveru
NEIDENTIFIKOVAN- test je propušten od strane firewall-a da usmeri saobraćaj ka inficiranom serveru.
Autorun12.exe - Autorun test
*Opis:**Autorun12.exe*** proverava da li zlonamerni programi mogu da zaraze druge programe promenom registri baze koja sadrži listu DLL fajlova i tako ugrozi većinu aplikacija koje u sebi imaju DLL fajlove. Promena koda se izvršava u registriju

[24] ***DNS*** *(engl. Domain name system) je, u osnovi, sistem koji pretvara imena računara*

"HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows"
IDENTIFIKOVAN - test je sprečen da zarazi aplikacije sa DLL fajlovima i firewall ga uspešno otkriva, sprečava i briše sa sistema
NEIDENTIFIKOVAN - test je bio u stanju da zarazi barem jednu aplikaciju sa DLL fajlovima i firewall ga nije registrovao kao pretnju.
Autorun9.exe - Autorun test
Opis: **Autorun9.exe** proverava da li zlonamerni programi mogu da zaraze druge programe tako što će vratiti program na fabrička podešavanja.
IDENTIFIKOVAN - nakon restarta sistema ako svi procesi rade nesmetano i testirani proizvod funkcioniše bez problema firewall ga je identifikovao.
NEIDENTIFIKOVAN - nakon restarta sistema neki procesi su prekinuti i testirani proizvod ne funkcioniše ili ima problema sa konfiguracijom
Autorun19.exe - Autorun test
Opis: **Autorun19.exe** proverava da li zlonamerni programi mogu da promene registri bazu Windows Explorera
IDENTIFIKOVAN - nakon restarta sistema ako svi procesi rade nesmetano i testirani proizvod funkcioniše bez problema firewall ga je identifikovao.
NEIDENTIFIKOVAN - nakon restarta sistema neki procesi su prekinuti i testirani proizvod ne funkcioniše ili ima problema sa konfiguracijom
FileDel2.exe - Test samoodbrane
Opis: ***FileDel2.exe*** briše važne fajlove i direktorijume testiranog proizvoda pomoću API[25] interfejsa.
IDENTIFIKOVAN - nakon restarta sistema, test je sprečen da manipuliše sa podacima
NEIDENTIFIKOVAN - test je bio u stanju da manipuliše podacima nakon restarta
Kill1.exe - Test samoodbrane
Opis: ***Kill1.exe*** proverava da li testirani proizvod štiti svoje procese od prekida i izvršava se sve dok jedan od procesa ne bude prekinut
IDENTIFIKOVAN - test je sprečen da zaustavi procese i firewall ga briše kao pretnju.
NEIDENTIFIKOVAN test je bio u stanju da spreči neke od procesa i ugrozi sistem.
Svckill.exe - Test samoodbrane
Opis: **Svckill.exe** proverava firewall da li zlonamerni korisnik ili kod može da manipuliše sa servisima firewalla i drajverima sistema.
IDENTIFIKOVAN - nakon restarta sistema ako svi procesi rade nesmetano i testirani proizvod funkcioniše bez problema firewall ga je identifikovao.
NEIDENTIFIKOVAN - nakon restarta sistema neki procesi su prekinuti i testirani proizvod ne funkcioniše ili ima problema sa konfiguracijom.
FileVri1.exe - Test samoodbrane
Opis: **FileVri1.exe** proverava da li može zlonamerni program da zarazi fajlove i programe.
IDENTIFIKOVAN - nakon restarta sistema ako svi procesi rade nesmetano i testirani proizvod funkcioniše bez problema
NEIDENTIFIKOVAN - ako nakon restarta sistema neki procesi su prekinuti i testirani proizvod ne funkcioniše ili ima problema sa konfiguracijom .
FileDel1.exe - Test samoodbrane
Opis: **FileDel1.exe** test program briše datoteka i direktorijume testiranog proizvoda

[25] ***Aplikacioni programski interfejs*** (***API*** *engl. Application programming interface, API) je računarski interfejs koji definiše načine na koje aplikacioni program može da zahteva servise od biblioteka i(li) operativnih sistema.*

IDENTIFIKOVAN - nakon restarta sistema ako svi procesi rade nesmetano i testirani proizvod funkcioniše bez problema firewall ga je identifikovao.
NEIDENTIFIKOVAN - nakon restarta sistema neki procesi su prekinuti i testirani proizvod ne funkcioniše ili ima problema sa konfiguracijom

HostsBlock.exe - Test samoodbrane

Opis: **HostsBlock.exe** test pristupa korisničkim nalozima i menja ih, kao svim korisničkim podacima.

IDENTIFIKOVAN - test je sprečen da pristupi korisničkim podacima i nalozima
NEIDENTIFIKOVAN - testu je dozvoljeno da pristupi korisničkim podacima i nalozima

RegDel1.exe - Test samoodbrane

Opis: **RegDel1.exe** briše registri bazu i procese testiranog proizvoda.

IDENTIFIKOVAN - nakon restarta sistema ako svi procesi rade nesmetano i testirani proizvod funkcioniše bez problema firewall ga je identifikovao.
NEIDENTIFIKOVAN - nakon restarta sistema neki procesi su prekinuti i testirani proizvod ne funkcioniše ili ima problema sa konfiguracijom

Suspend2.exe - Test samoodbrane

Opis: **Suspend2** test za daljinsku manipulaciju nad testiranim firewall-om.

IDENTIFIKOVAN - nakon restarta sistema ako svi procesi rade nesmetano i testirani proizvod funkcioniše bez problema firewall ga je identifikovao.
NEIDENTIFIKOVAN - nakon restarta sistema neki procesi su prekinuti i testirani proizvod ne funkcioniše ili ima problema sa konfiguracijom

Crash1.exe - Test samoodbrane

Opis: **Crash1.exe** test manipuliše sa konfiguracijom administratora i procesima nad testiranim proizvodom.

IDENTIFIKOVAN - nakon restarta sistema ako svi procesi rade nesmetano i testirani proizvod funkcioniše bez problema firewall ga je identifikovao.
NEIDENTIFIKOVAN - nakon restarta sistema neki procesi su prekinuti i testirani proizvod ne funkcioniše ili ima problema sa konfiguracijom

FileMov1.exe - Test samoodbrane

Opis: **FileMov1.exe** test preimenuje datoteke i direktorijume testiranog proizvoda

IDENTIFIKOVAN - nakon restarta sistema ako svi procesi rade nesmetano i testirani proizvod funkcioniše bez problema firewall ga je identifikovao.
NEIDENTIFIKOVAN - nakon restarta sistema neki procesi su prekinuti i testirani proizvod ne funkcioniše ili ima problema sa konfiguracijom

SSS2.exe - Ostali testovi

Opis: **SSS2.exe** ima za zadatak da ugasi računar ili sistem

IDENTIFIKOVAN testu je sprečeno da ugasi računar i firewall ga briše kao pretnju
NEIDENTIFIKOVAN- testu je dozvoljeno da ugasi računar, firewall ga nije detektovao kao pretnju.

SSS3.exe - Ostali testovi

Opis: **SSS3.exe** proverava da li zlonamerni korisnik može isključiti sistem pomoću posebnog API[26] interfejsa

IDENTIFIKOVAN testu je sprečeno da ugasi računar i firewall ga briše kao pretnju
NEIDENTIFIKOVAN- testu je dozvoljeno da ugasi računar, firewall ga nije detektovao kao pretnju.

[26] ***Aplikacioni programski interfejs*** *(**API** engl. Application programming interface, API) je računarski interfejs koji definiše načine na koje aplikacioni program može da zahteva servise od biblioteka i(li) operativnih sistema.*

WFPblock.exe -Ostali testovi
Opis: **WFPblock.exe** proverava da li zlonamerni korisnik može isključiti sistem pomoću posebnog API[27] interfejsa i tako kontroliše ceo mrežni saobraćaj
IDENTIFIKOVAN testu je sprečeno da ugasi računar i firewall ga briše kao pretnju
NEIDENTIFIKOVAN- testu je dozvoljeno da ugasi računar, firewall ga nije detektovao kao pretnju

Testirani firewall-i su bili instalirani na virtuelnoj mašini sa operativnim sistemom Windows 7 Ultimate, Service pack 1 i sa internet pretraživačem Windows Explorer 9 gde isključen UAC[28] korisnički interfejs. Svaki testirani firewall je konfigurisan tako da radi u punoj pripravnosti, da prikazuje prozore obaveštenja u slučaju napada i pristupanje na Internet. Na svakom testiranom firewall-u je uključeno ažuriranje sistema i instaliranje potrebnih zakrpa. Pre samog testiranja pokrenuto je skeniranje sistema pomoću firewall programa kako bi se utvrdile potencionalne pretnje po sistem. Svaki firewall je registrovao neke od pretnji i obaveštavao o njihovom sankcionisanju. Tabele ispod prikazuju kako su testirani proizvodi reagovali na određene testove, podvrgnuti nizom simulacija.

11.1.1 Testirani firewall: Comodo Personal Firewall 2.0.0.0

VBStest.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
CopyCat.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
DDEexec.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Leaktest.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Yalta.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Eho.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Coat.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Jumper.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
DNStester.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Schedtest.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
AVFT4**.exe**	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Keylog4.exe	*Vrsta isp.:* Test za špijuniranje	IDENTIFIKOVAN	
ProxyTest.exe	*Vrsta isp.:* Test za špijuniranje	IDENTIFIKOVAN	
Screenlog.exe	*Vrsta isp.:* Test za špijuniranje	IDENTIFIKOVAN	
Autorun12.exe	*Vrsta isp.:* Autorun test	IDENTIFIKOVAN	
Autorun9.exe	*Vrsta isp.:* Autorun test	IDENTIFIKOVAN	

[27] ***Aplikacioni programski interfejs*** *(**API** engl. Application programming interface, API) je računarski interfejs koji definiše načine na koje aplikacioni program može da zahteva servise od biblioteka i(li) operativnih sistema.*
[28] **User Account Control** (**UAC**) – *korisnička kontrola računa (*UAC) *tehnologije*

Autorun19.exe	*Vrsta isp.:* Autorun test	IDENTIFIKOVAN	
FileDel2.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
Kill1.exe	*Vrsta isp.*: Test samoodbrane	IDENTIFIKOVAN	
FileVri1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
FileDel1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
HostsBlock.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
RegDel1.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN
Suspend2	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
Crash1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
Svckill.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
FileMov1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
SSS2.exe	*Vrsta isp.:* Ostali testovi	IDENTIFIKOVAN	
SSS3.exe	*Vrsta isp.:* Ostali testovi		NE IDENTIFIKOVAN
WFPblock.exe	*Vrsta isp.:* Ostali testovi		NE IDENTIFIKOVAN

Tabela 2 - test Comodo Internet Security Plus 2012 Firewall

Objašnjenje testiranog firewall-a:

Comodo Internet Security Plus 2012 Firewall - nakon testiranja proizvod je od ukupno 30 testiranih programa uspeo da detektuje pretnju po sistem 27 test programa. Uspešnost test firewall-a u procentima je 90 %. Firewall nije uspeo da detektuje **RegDel1.exe** program, došlo je do restarta računara i neki od procesa su bili prekinuti. Takođe su ne identifikovani programi bili **SSS3.exe i WFPblock.exe** koji su uspeli da prikažu pretnju za sistem tako što su malware programi mogli kontrolisati sistem pomoću API interfejsa. Firewall se u trenutku testiranja ovih programa ponašao kao da su deo procesa u Windows operativnom sistemu. Za ostale programe koje je firewall identifikovao prikazano je upozorenje sa pitanjem da li da briše, postavi u karantin ili da dozvoli proces. Odabirom dugmeta za brisanje, svaki test program je prekinut i detaljno uklonjen sa sistema.

11.1.2 Testirani firewall: Agnitum Outpust Pro Firewall

VBStest.exe	*Vrsta isp.:* Test curenja podataka		NEIDENTIFIKOVAN
CopyCat.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
DDEexec.exe	*Vrsta isp.:* Test curenja podataka		NEIDENTIFIKOVAN
Leaktest.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Yalta.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Eho.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	

Coat.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Jumper.exe	*Vrsta isp.:* Test curenja podataka		NEIDENTIFIKOVAN
DNStester.exe	*Vrsta isp.:* Test curenja podataka		NEIDENTIFIKOVAN
Schedtest.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
AVFT4**.exe**	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Keylog4.exe	*Vrsta isp.:* Test za špijuniranje	IDENTIFIKOVAN	
ProxyTest.exe	*Vrsta isp.:* Test za špijuniranje		NEIDENTIFIKOVAN
Screenlog.exe	*Vrsta isp.:* Test za špijuniranje	IDENTIFIKOVAN	
Autorun12.exe	*Vrsta isp.:* Autorun test	IDENTIFIKOVAN	
Autorun9.exe	*Vrsta isp.:* Autorun test	IDENTIFIKOVAN	
Autorun19.exe	*Vrsta isp.:* Autorun test	IDENTIFIKOVAN	
FileDel2.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
Kill1.exe	*Vrsta isp.*: Test samoodbrane	IDENTIFIKOVAN	
FileVri1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
FileDel1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
HostsBlock.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
RegDel1.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN
Suspend2	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
Crash1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
Svckill.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	NEIDENTIFIKOVAN
FileMov1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
SSS2.exe	*Vrsta isp.:* Ostali testovi	IDENTIFIKOVAN	NEIDENTIFIKOVAN
SSS3.exe	*Vrsta isp.:* Ostali testovi		NE IDENTIFIKOVAN
WFPblock.exe	*Vrsta isp.:* Ostali testovi		NE IDENTIFIKOVAN

Tabela 3 - test Agnitum Outpust Pro Firewall

Objašnjenje testiranog firewall-a:

Agnitum Outpust Pro Firewall - nakon testiranja proizvod je ukupno od 30 testiranih programa uspeo da detektuje pretnju po sistem 20 test programa. Uspešnost test firewall-a je u procentima 67 %. Firewall nije uspeo da detektuje **VBStest.exe** test gde je zlonamerni program zaobišao zaštitu pomoću Visual Basic skripte, nije detektovao test **DDEexec.exe ,** nije detektovan test **Jumper.exe** posle čega je računar imao izlaz na internet preko Windows Explorera i posle svakog uključivanja programa dolazilo je do iskačućih prozora sa Interneta. Nije uklonjen **DNStester.exe** test gde je program menjao imena računara posle svakog podizanja operativnog sistema. Nije detektovan test **ProxyTest.exe** gde se gubila konekcija ka Internetu, potrebno je bilo svaki put podesiti proxy server za konekciju na Internet.

Nije detektovan test **RegDel1.exe** gde su brisani procesi tipa explorer.exe i slični. Nije detektovan test **Svckill.exe** kada je dolazilo do ne podizanja operativnog sistema tj. pojedini drajveri su se ponašali kao ne kompatabilni sa operativnim sistemom**.** Nije uklonjen proces **SSS2.exe** i **SSS3.exe** kada je dolazilo do spontanog gašenja računara. Nije uklonjeni test **WFPblock.exe.** Može se zaključiti je deset test programa uspelo da ispuni svoju misiju i ugrozi računarski sistem. Agnitum Outpust Pro Firewall se pokazao kao program za zaštitu na srednjem nivou efikasnosti i pored brojnih testova program zadovoljava skromnu ocenu na skali od 1 do 10 celih 7.

11.1.3 Testirani firewall: McAfee Firewall

VBStest.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
CopyCat.exe	*Vrsta isp.:* Test curenja podataka		NEIDENTIFIKOVAN
DDEexec.exe	*Vrsta isp.:* Test curenja podataka		NEIDENTIFIKOVAN
Leaktest.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Yalta.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Eho.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Coat.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Jumper.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
DNStester.exe	*Vrsta isp.:* Test curenja podataka		NEIDENTIFIKOVAN
Schedtest.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
AVFT4**.exe**	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Keylog4.exe	*Vrsta isp.:* Test za špijuniranje		NEIDENTIFIKOVAN
ProxyTest.exe	*Vrsta isp.:* Test za špijuniranje	IDENTIFIKOVAN	
Screenlog.exe	*Vrsta isp.:* Test za špijuniranje		NEIDENTIFIKOVAN
Autorun12.exe	*Vrsta isp.:* Autorun test		NEIDENTIFIKOVAN
Autorun9.exe	*Vrsta isp.:* Autorun test		NEIDENTIFIKOVAN
Autorun19.exe	*Vrsta isp.:* Autorun test		NEIDENTIFIKOVAN
FileDel2.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN
Kill1.exe	*Vrsta isp.*: Test samoodbrane		NEIDENTIFIKOVAN
FileVri1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
FileDel1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
HostsBlock.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN
RegDel1.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN
Suspend2.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN
Crash1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
Svckill.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
FileMov1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	

SSS2.exe	*Vrsta isp.:* Ostali testovi		NEIDENTIFIKOVAN
SSS3.exe	*Vrsta isp.:* Ostali testovi		NE IDENTIFIKOVAN
WFPblock.exe	*Vrsta isp.:* Ostali testovi		NE IDENTIFIKOVAN

Tabela 4 - test McAfee Firewall

Objašnjenje testiranog firewall-a:

McAfee Firewall - nakon testiranja proizvod je od ukupno 30 testiranih programa uspeo da detektuje pretnju po sistem 14 test programa. Uspešnost test firewall-a u procentima je 47 %. Firewall nije uspeo da detektuje **CopyCat.exe** test nakon čega se Internet Explorer ponašao ne kontrolisano, pristizale su iskačuće poruke tokom surfovanja Internetom. Nije detektovan **DDEexec.exe** test koji je takođe manipulisao Internet Explorer. Nije detektovan **DNStester.exe** test nakon čega su menjane adrese računara i gubila se konekcija. Nije detektovan test **Keylog4.exe** gde je nakon restarta sistema utvrđeno da se sistem zarazio malicioznim kodom. Nije detektovan test **Screenlog.exe** koji ima za ulogu da uslikava izgled desktop ekrana i tako špijunira korisnika. Nisu detektovani testovi za samopokretanje **Autorun12.exe, Autorun9.exe** i **Autorun19.exe** nakon testiranja računar se ponašao veoma usporeno, nisu se mogle otvoriti neke aplikacije, a operativni sistem je posle svakog podizanja javljao da nedostaju pojedini .dll fajlovi. Nije detektovan test **FileDel2.exe** i **RegDel1.exe** kada je došlo do restarta računara i neki od procesa su bili prekinuti. Firewall se nije uključio, a sistem je obaveštavao da je ugrožen. Nije detektovan test **Suspend2.exe** koji je za daljinsku manipulaciju namenjen. Nije detektovan test **HostsBlock.exe** koji menja korisničke naloge. Nije detektovan **Kill1.exe** test koji je prekidao pojedine procese. Takođe su ne identifikovani programi bili **SSS2.exe** **SSS3.exe** i **WFPblock.exe** koji su uspeli da prikažu pretnju po sistem tako što malware programi mogu kontrolisati sistem pomoću API interfejsa. Firewall se u trenutku testiranja ovih programa ponašao kao da su deo procesa u Windows operativnom sistemu. Za ostale programe koje je identifikovao firewall je prikazao upozorenje sa pitanjem da li da briše, postavi u karantin ili da dozvoli proces. Odabirom dugmeta za brisanje, svaki test program je prekinut i detaljno uklonjen sa sistema. Ocena na skali od 1 do 10 bila bi ocena 5. McAfee firewall nije detektovao veše od polovine testova.

11.1.4 Testirani firewall: Norton 360 Firewall

VBStest.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
CopyCat.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
DDEexec.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Leaktest.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Yalta.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Eho.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Coat.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Jumper.exe	*Vrsta isp.:* Test curenja podataka		NEIDENTIFIKOVAN
DNStester.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Schedtest.exe	*Vrsta isp.:* Test curenja podataka		NEIDENTIFIKOVAN
AVFT4**.exe**	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Keylog4.exe	*Vrsta isp.:* Test za špijuniranje	IDENTIFIKOVAN	
ProxyTest.exe	*Vrsta isp.:* Test za špijuniranje	IDENTIFIKOVAN	
Screenlog.exe	*Vrsta isp.:* Test za špijuniranje	IDENTIFIKOVAN	
Autorun12.exe	*Vrsta isp.:* Autorun test		NEIDENTIFIKOVAN
Autorun9.exe	*Vrsta isp.:* Autorun test		NEIDENTIFIKOVAN
Autorun19.exe	*Vrsta isp.:* Autorun test		NEIDENTIFIKOVAN
FileDel2.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
Kill1.exe	*Vrsta isp.*: Test samoodbrane	IDENTIFIKOVAN	
FileVri1.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN
FileDel1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
HostsBlock.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
RegDel1.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN
Suspend2	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
Crash1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
Svckill.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
FileMov1.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN
SSS2.exe	*Vrsta isp.:* Ostali testovi		NEIDENTIFIKOVAN
SSS3.exe	*Vrsta isp.:* Ostali testovi		NE IDENTIFIKOVAN
WFPblock.exe	*Vrsta isp.:* Ostali testovi		NE IDENTIFIKOVAN

Tabela 5 - test Norton 360 Firewall

Objašnjenje testiranog firewall-a:

Norton 360 Firewall - nakon testiranja proizvod je od ukupno 30 testiranih programa uspeo da detektuje pretnju po sistem 19 test programa. Uspešnost test firewall-a u procentima je 64 %. Firewall nije uspeo da detektuje **Jumper.exe** test nakon ponovnog podizanja operativnog sistema dolazilo je do konekcije na Internet gde je

firewall javljao da se saobraćaj izvršava. Nije detektovan **Schedtest.exe** test gde se manipulisao program Task Scheduler. Nisu detektovani programi **Autorun12.exe, Autorun9.exe** i **Autorun19.exe** nakon testiranja računar se ponašao veoma usporeno, nisu se mogle otvoriti neke aplikacije, a operativni sistem je posle svakog podizanja javljao da nedostaju pojedini .dll fajlovi. Nije detektovan **FileVri1.exe** i **RegDel1.exe** i **FileMov1.exe** test, nakon čega je dolazilo do restarta računara i neki od procesa su bili prekinuti i nisu se mogli ponovo pokrenuti. Firewall se nije uključio, a sistem je obaveštavao da je ugrožen. Takođe su ne identifikovani programi bili **SSS2.exe SSS3.exe** i **WFPblock.exe** koji imaju zadatak da prikažu pretnju za sistem tako što malware programi mogu kontrolisati sistem pomoću API interfejsa. Ostali testovi koji su detektovani uspešno su odklonjeni sa sistema tako da se više nemogu pokrenuti jer je firewall upisao u svoju bazu znanja o potencionalnim pretnjama po sistem. Ocena za ovaj firewall na skali od 1 do 10 bila bi 6-ica. Može se reći da Norton 360 Firewall ima sve predispozicije za dobar firewall jer je u sebi iako sadrži antivirusne i antispyware programe koji nisu bili pokrenuti na ovom testiranju mogli da pripomognu uspešnijem odklanjanju malicioznog koda.

11.1.5 Testirani firewall: ZoneAlarm Pro Firewall 6.1

VBStest.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
CopyCat.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
DDEexec.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Leaktest.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Yalta.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Eho.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Coat.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Jumper.exe	*Vrsta isp.:* Test curenja podataka		NEIDENTIFIKOVAN
DNStester.exe	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Schedtest.exe	*Vrsta isp.:* Test curenja podataka		NEIDENTIFIKOVAN
AVFT4**.exe**	*Vrsta isp.:* Test curenja podataka	IDENTIFIKOVAN	
Keylog4.exe	*Vrsta isp.:* Test za špijuniranje		NEIDENTIFIKOVAN
ProxyTest.exe	*Vrsta isp.:* Test za špijuniranje	IDENTIFIKOVAN	
Screenlog.exe	*Vrsta isp.:* Test za špijuniranje	IDENTIFIKOVAN	
Autorun12.exe	*Vrsta isp.:* Autorun test	IDENTIFIKOVAN	
Autorun9.exe	*Vrsta isp.:* Autorun test	IDENTIFIKOVAN	
Autorun19.exe	*Vrsta isp.:* Autorun test	IDENTIFIKOVAN	
FileDel2.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN

Kill1.exe	*Vrsta isp.*: Test samoodbrane	IDENTIFIKOVAN	
FileVri1.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN
FileDel1.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN
HostsBlock.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
RegDel1.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN
Suspend2	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
Crash1.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
Svckill.exe	*Vrsta isp.:* Test samoodbrane	IDENTIFIKOVAN	
FileMov1.exe	*Vrsta isp.:* Test samoodbrane		NEIDENTIFIKOVAN
SSS2.exe	*Vrsta isp.:* Ostali testovi		NEIDENTIFIKOVAN
SSS3.exe	*Vrsta isp.:* Ostali testovi		NE IDENTIFIKOVAN
WFPblock.exe	*Vrsta isp.:* Ostali testovi		NE IDENTIFIKOVAN

Tabela 6 - test ZoneAlarm Pro Firewall 6.1

Objašnjenje testiranog firewall-a:

ZoneAlarm Pro Firewall 6.1 - nakon testiranja proizvod je od ukupno 30 testiranih programa uspeo da detektuje pretnju po sistem 19 test programa. Uspešnost test firewall-a u procentima je 64 %. Firewall nije uspeo da detektuje **Jumper.exe** test nakon ponovnog podizanja operativnog sistema dolazilo je do konekcije na Internet gde je firewall javljao da se saobraćaj izvršava. Nije detektovan **Schedtest.exe** test gde se manipulisao program Task Scheduler. Nije detektovan program **Keylog4.exe** za upad u sistem preko windows prečica. Nisu sprečeni testovi **FileDel2.exe** , **FileVri1.exe, FileDel1.exe i FileMov1.exe** kada je dolazilo do brisanja sistemskih datoteka i posle ponovnog podizanja sistema windows se ponašao usporeno. Nije detektovan test **RegDel1.exe** gde došlo je do restarta računara i neki od procesa su bili prekinuti. Firewall se nije uključio, a sistem je obaveštavao da je ugrožen. Takođe su ne identifikovani programi bili **SSS2.exe SSS3.exe i WFPblock.exe** koji su uspeli da prikažu pretnju po sistem tako što se malware programi mogli kontrolisati sistem pomoću API interfejsa. ZoneAlarm Pro Firewall 6.1 se pokazao tokom ovih testiranja kao dostojan protivnik na sve testove koji su izvršavani i po nekoliko puta. Na skali od 1 do 10 ocena je 7.

12. Događaji tokom testiranja

Tokom testira firewall-a dolazilo je do različitih neočekivanih situacija i ponašanje sistema. Prilikom testiranja ovih pet vatrenih zidova dolazilo je do restartovanja sistema, brisanje sistemskih fajlova, menjanje izgleda i sadržaja instaliranih programa, gašenja procesa u operativnom sistemu, preimenovanja datoteka i direktorijuma, preimenovanja registri baze sistema, usporenost rada operativnog sistema. Tabela ispod prikazuje sve događaje koji su se desili tokom testiranja firewall-a. Simbol X prikazuje događaj koji se desio tokom testiranja.

Događaji tokom testiranja	Comodo Personal Firewall 2.0.0.0	Agnitum Outpust Pro Firewall	McAfee Firewall	Norton 360 Firewall	ZoneAlarm Pro Firewall 6.1
Restartovanje računara	X	X	X	X	X
Brisanje sistemskih fajlova		X	X	X	X
Menjanje izgleda i sadržaja programa			X		
Menjanje datoteka i direktorijuma			X		X
Preimenovanje registri baze operativnog sistema		X	X		X
Prekidanje procesa operativnog sistema	X	X	X	X	X
Usporen rad računara			X	X	X
Iskačući prozori upozorenja o saobraćaju		X	X	X	X
Usporena konekcija na Internetu		X	X	X	X

Prestanak rada firewall programa			X	X	X

Tabela 7 - događaji tokom testiranja firewall-a

13. Kriterijumi sotverskog firewall-a

Zaštitni zid je najvažniji deo opreme koja štiti celu mrežu, a mnogi kriterijumi razlikuju se u zavisnosti od verzijeprograma ili proizvođača. Određene karakteristike se nalaze na određenim zaštitnim zidovima. Mnogi proizvođači firewall-a pokušavaju da privuku pažnju korisnika na veoma niske cene i mogućnosti proizvoda, međutim, kada bi se želje i potreba za zaštitnim zidom pratile, ukupna cena proizvoda i mogućnosti koje pruža postale bi mnogo veće od očekivanog. Postavljanjem kriterijuma za odabir firewall proizvoda možemo da razgraničimo mogućnosti i kvalitet proizvoda za kojim tragamo.

Testirani su pet različitih softverskih firewall-a koji su bili dostupni na Internetu. Svih pet programa se može instalirati na Microsoft Windows operativne sisteme. Odabran je Microsoftov windowsov operativni sistem jer se najviše koriste u kućnoj upotrebi i dostupan je u slobodnoj prodaji.

Firewall-i koji su testirani su:

- Comodo Personal Firewall 2.0.0.0
- Agnitum Outpust Pro Firewall
- McAfee Firewall
- Norton 360 Firewall
- ZoneAlarm Pro Firewall 6.1

Ovo su firewall-i koji se najčešće koriste u kućnoj upotrebi, a ujedno su i najpopularniji kod korisnika računarskih mreža.

13.1 Konfiguracija računara gde su testirani programi:

Sve firewall programi su testirani na računaru sa konfiguracijom: procesor AMD Phenom 8450 Triple-Core 2.10 GHz, memorija 4 GB RAM. Na ovoj konfiguraciji je instaliran program WMWare za pokretanje virtuelne mašine na koju je bio instaliran operativni sistem Windows 7 Ultimate, 64-bit operativnim sistemom, Service Pack 1. Brzina interneta je bila za download: 5120 kbps, a za upload: 256 kbps.

Istraživanje se prvenstveno odnosilo na neodlučne i početne korisnike, ali nisu izostavljeni ni napredniji korisnici. Ne postoji formalna definicija firewall-a za koje kriterijume mora da ispunjava, pa sam umesto toga odredio kriterijume koje svaki zaštitni zid mora da ispunjava.

13.2 Najosnovniji kriterijumi kod firewall-a:

Vidljivost statusa sistema: Sistem uvek treba da bude vidljiv korisnicima i da javlja sve akcije u razumnom roku.[•] (Brian Komar, 2003)

Jednostavnost korišćenja: zaštitni zid koji ste odabrali mora biti jednostavan za konfiguraciju kako bi administratori mogli lako da ga podesite. Ukoliko je interfejs firewall-a suviše složen ili ne koncizan, zaštitni zid se neće moći bezbedno konfigurisati do nivoa koji zahteva organizacija, jer firewall administratori neće naći odgovarajuću konfiguraciju za njega.[•] (Cameron, 2005) Firewall mora biti jednostavan za upotrebu bez obzira na kojoj se lokaciji nalazi i sa koje se može upravljati. U nekim slučajevima, firewall administrator može da konfiguriše zaštitni zid sa spoljašnje mreže. Od organizacije zavisi da li postoji potreba za daljinsko konfigurisanje i upravljanje firewall-a.

Administrativne funkcije: pri izboru firewall-a, treba obratiti pažnju na trenutnu stručnost firewall adminitrstora. Potrebno je odabrati proizvod koji ima detaljnu dokumentaciju o konfiguraciji proizvoda. Ovo je važno zbog toga što se može skratiti vreme konfiguracije u daleko kraćem vremenskom roku. Dokumentacija za instalaciju firewall programa mora da obuhvata pismeni i / ili elektronski deo. Administrativne funkcije moraju postojati u okviru interfejsa gde samo administrator može da pristupi. Konfigurisanje i promena politike bezbednosti je dostupna samo za administratore. Podešavanje i promena administrativnih funkcija treba da se izvrši preko potvrde identiteta korisnika. Proizvođač firewall-a mora da integriše u svoj proizvod zahtev za

---

[•] Brian Komar, R. B. (2003). *Firewalls for Dummies 2nd Edition.* Indianapolis: Wiley Publishing.

[•] Cameron, R. (2005). *Configuring NetScreen Firewalls.* Rockland: Syngress Publishing.

potvrdu identiteta korisnika, ispravno korisničko ime i lozinke ili neki jači oblik autentifikacije pre dozvoljavanja pristupa svim administrativnim funkcijama. • (Cheswick, 2003)

Podržane platforme: Neke organizacije nisu zadovoljne svojim firewall proizvodima koje radi na operativnim sistema. Firewall administratori smatraju da zaštitni zid nasleđuje sve od osnovnog operativnog sistema. Iako ovo nije istina u većini slučajeva, taj problem se mora rešiti. Organizacija mora definisati koji operativni sistemi će se koristiti za firewall. Dobar firewall proizvod je onaj koji ne koristi puno od resursa sistema, koji ne koči i usporava sistema sa svojim radom.
• (KristianKőpsén, 2006)

Podrška za više zona: Prilikom odlučivanja koji firewall je najbolje rešenje, treba proveriti da li podržava sve bezbednosne zone koje su vam potrebne. Pored unutrašnje mreže, mnoge organizacije koriste mreže, koje su dostupne sa Interneta - ove odvojene mreže često nazivamo demilitarizovane zone ili DMZ-s. Konfiguracija DMZ treba da bude dizajnirana unapred. Kada znate kako želite da koristite DMZ pomaćiće vam da eliminišete proizvode firewall-a koji ne podržavaju ovu konfiguraciju.• (Danny Briere, 2011) Na primer, neki firewall proizvodi podržavaju samo dva interfejsa. Ako vaš DMZ zahteva tri zone koristeći jedan zaštitni zid, možete lako uklonite ove proizvode sa liste želja.

Zaštita od uobičajenih napada: mnogi različiti napadi dolaze najčešće sa Interneta, kao što su Denial of Service (DoS) napadi i usmeravanje napada ka web

---

• Cheswick, W. R. (2003). *Firewalls and Internet Security, Second Edition. .* Boston: AT&T and Lumeta Corporation.

• KristianKőpsén, M. (2006). *A comparison of the security ana usability of personal firewalls.* Linkőping: Linkőping University.

• Danny Briere, H. F. (2011). *Wireless Home Networking For Dummies.* Indiana: Wiley Publishing.

serverima. Zaštitni zid treba da otkrije sve napade, a dobar firewall treba sprovodi mere bezbednosti i da blokira te napade.

Detekciju upada: mogućnost otkrivanja i pokušaja upada ide ruku pod ruka sa zaštitom od uobičajenih napada. Intrusion Detection znači da zaštitni zid otkrije kada dođe do pokušaja hakovanja i upozorava Vas o tome šta se dešava. Neki zaštitni zidovi imaju odlične detekcije upada. Neki firewall-i mogu da blokiraju napade, ali nemaju način da se oglase alarmom kada se napad odvija. Treba obratiti pažnju na firewall-e koji imaju ovu funkciju, treba proveriti koje vrste napada firewall detektuje i da li se uopšte oglašava alarm kada dođe do njih.

Praćenje u realnom vremenu: zaštitni zid koji obezbeđuje nadgledanje u realnom vremenu omogućava administratoru zaštitnog zida da vidi tačnu upotrebu zaštitnog zida u bilo kojem trenutku u vremenu. Real-time praćenje omogućava administratoru zaštitnog zida da vidi tačno koji portovi su dostupni na računarskoj mreži i tako ispravi politiku zašite ako je potrebno. Real-time daje mogućnost administratoru zaštitnog zida da prekine vezu odmah ako je potrebno.[•] (Brian Komar, 2003)

Primena filtriranja na aplikativnom sloju: vatreni zid bi trebao da pruži više mogućnosti filtriranja saobraćaja od samog paket filtriranja. Filtriranje na aplikativnom sloju omogućuje firewall-u da pregleda naredbe ili radnje koje se odvijaju unutar protokola. Na primer, firewall je konfigurisan tako da dozvoljava aplikativnom sloju filtriranje samo FTP-GET komandama na FTP serveru, a sprečava FTP serveru izlaz sa FTP-PUT komandama ili pregleda dolazni saobraćaj sa HTTP protokola, uključujući i Nimda ili Code Red crva. .[•] (Brian Komar, 2003) Gotovo svi firewall proizvođači nude neki aplikativni sloj za filtriranje. Uobičajena primena aplikativnog sloja filtriranjem jeste za web-sadržaj, e-mail sadržaj, FTP datoteke i transfere, instant-poruke i viruse. Treba proveriti da li dodavanjem filtera pomoću aplikativnog sloja na firewall-u ne smanjujemo performanse i rad firewall proizvoda.

[•] Brian Komar, R. B. (2003). *Firewalls for Dummies 2nd Edition.* Indianapolis: Wiley Publishing.

Proširivanje: novi protokoli i usluge uvode se svake godine. Vatreni zid bi trebao omogućiti dodavanje novih usluga i protokola. Potrebno je odabrati takav firewall koji daje mogućnosti nadogradnje, proširivanja i mogućnosti konfigurisanja sa ostalim vidovima zaštite.

Plug-in dostupnosti: firewall mora da pruži dodatne mogućnosti, kao što je skeniranje virusa ili metode za raspodelu kapaciteta mreže između različitih vrsta prometa. Pri kupovini firewall, treba utvrditi koji su dodaci dostupni i da li se pružaju usluge za koje vaša mreža zahteva.

Netvork Address Translation (NAT) podrška: pre nego što se instalira zaštitni zid, treba preispitati sve IP adresne razmeštene u mreži. Ako mreža koristi privatne IP adrese na mreži,zaštitni zid mora da poseduje NAT kako bi omogućio korisnicima da pristupe Internetu. Isto tako NAT omogućava dodelu javnih IP adresa računarima u mreži koji žele da pristupe Internetu.• (Angelescu, 2010)

Dostupne licence: ako računarska mreža raste sa organizacijom, treba proveriti da li firewall podržava dodavanje licenci za nadogradnju i unapređenje sistema. Firewall mora da poseduje ove sertifikate **ICSA** je osnovni nivo za sertifikate, **Common Criteria** - napredni nivo za sertifikate, **EAL4 +** sertifikat je poželjan da postoji u firewall-u.

Podrška za virtuelne privatne mreže (VPN): ako jkorisnicima sa unutrašnje mreže potreban izlaze na Internet, firewall treba da poseduje VPN usluge u okviru svojih osnovnih usluga. VPN podržava protokole tipa IPSec koji je najčešće podržan, PPTP podržavaju samo neki od firewall-a, kao i SSL protokol koji neki zaštitni zidovi uključuju u korišćenje.• (Attribution, 2013)

Podrška za proizvod: ne treba pasti u zamku razmišljajući da je jednostavno instaliranje zaštitnog zida dovoljno i da će raditi tačno kako se očekivalo. Možda će

---

• Angelescu, S. (2010). *CCNA Certification All-In-One For Dummies.* Indiana: Wiley Publishing.

• Attribution, C. C. (2013). *Virtual private network*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Virtual_private_network

biti potrebe da se obratite proizvođaču softvera za tehničku podršku. Treba biti siguran u istraživačke metode koje su dostupne kod proizvođača. Da li je prodavac obezbedio E-mail podršku, telefonsku podršku, ili samo Web podršku? Čak je najvažnije koliko dugo će biti potrebno proizvođaču da odgovori na Vaša pitanja. Svaki firewall program bi morao da ima prečicu do proizvođača gde korisnik može da se informiše o najnovijim proizvodima i mogućim pitanjima u okviru proizvoda. Podrška za kupce treba da bude dostupna 24 sata u nedelji čitave godine, pa čak i da postoji kod proizvođača spremljena skripta u slučaju napada koju može da dostavi kupcu u najkraćem roku.[•] (Brian Komar, 2003)

Praćenje aktivnosti (log fajlovi): jedino mesto gde se mogu pronaći zapisi o napadima i svim aktivnostima na sistem jeste u log fajlovima. Treba proveriti da li vatreni zid daje izveštaj o aktivnosti mrežnog saobraćaja i ako postoje log fajlovi oni moraju biti veoma precizni, tačni i jasni za tumačenje firewall administratora. Pomoću log fajla može se dobiti dobra slika o tome koliko ljudi želi da pristupi sistemu, odakle dolaze, koliko često dolaze, kako se kreću po sistemu i slično.

Praćenje istorije firewall-a: treba proveriti da li postoji istorija usavršavanja firewall proizvoda. Neki firewall proizvodi imaju dugačku istoriju praćenja o svim svojim nedostacima i zakrpama koje su vremenom ispravljani, dok sa druge strane postoje firewall proizvodi čija je istorija nedostataka i zakrpa čista tj. ne postoji.

Cena: možda i naj važniji faktor koji postavlja kriterijume kod odabira firewall-a jeste cena samog proizvoda. Često se kupci pitaju zašto je cena jednog proizvoda toliko skupa od drugog i postavlja se pitanje da li uopšte vredi platiti toliko novca. Treba sagledati koje su mogućnosti firewall proizvoda i da li ispunjava sve gore navedene kriterijume i tek tada treba odabrati dobar firewall proizvod. Iznos koji ćete potrošiti na zid treba da bude u direktnoj vezi sa vrednostima podataka koji se štite. To ne znači da ako potrošite više novca da će biti bolji zaštitni zid. Samo budite sigurni da pogledate sve kriterijume i koliko ih svaki zid ispunjava . Kada pregledate sve kriterijume i izdvojite dve ili više zaštitnih zidova, svakako treba izabrati jeftinije

[•] Brian Komar, R. B. (2003). *Firewalls for Dummies 2nd Edition.* Indianapolis: Wiley Publishing.

rešenje. Ali nikako ne treba izabrati samo zaštitni zid samo zato što je jednostavno najjeftiniji.

Zaključak:

U današnje vreme kada je kompjuterska pismenost potrebna u svim sverama poslovanja, a Internet važan resurs u svim organizacijama i delotnostima, veoma je važno posvetiti pažnju na sigurnost računarskog sistem.[•] (Bishop, 2003) Zbog naše sigurnosti, firewall-i imaju veliku ulogu u očuvanju organizacije i poslova s kojim se bavimo. Odabir dobrog i sigurnog firewall-a je veoma teško izabrati jer se na tržištu nudi široka paleta softverskih firewall-a od kojih neki imaju ulogu samo za reklamiranje firme, a daleko su od učinkovitosti. Cene firewall-a se kreću od nekoliko eura pa da stotine eura, ali ne mora da znači da su skuplji firewall-i bolji za korisnika. Korisnici zaštitnih zidova se obično vode politikom da skuplji zaštitini zidovi su sigurniji i da se s njihovim postavljanjem sprečava svakojaki ulazak u sistem. Obično to nije uvek istina, ali se može izvadidti zaključak da skuplji firewall-i spadaju u kategoriju zaštitinih zidova gde se njihova konfiguracija i samo postavljanje u računarski sistem odvija brzo i jednostavno. Kategorisanjem firewall-a možemo još spomenuti zaštitine zidove koji su na tržištu besplatni ili ne zahtevaju velike finansijske troškove. Kod ove kategorije obično se postavlja dilema da li su ovi firewall-i zaista efikasni i učinkoviti. Korisnici obično imaju predrasude prema ovim firewall-ima, ali njihova efikasnost se ogleda tek u stručno postavljenom i konfigurisanom sistemu. Potrebno je osnovno iskustvo administriranja kod korisnika ovih firewall-a ili pak da se korisnici vode politikom "što je skupo znaš da je dobro". Cena ima ulogu kao faktor odabira vatrenog zida, ali se konkretno treba voditi smerom ka mogućnostima koje firewall proizvod pruža[•] (Brian Komar, 2003).

Testiranje svakog softverskog firewall-a koji se danas nudi na paleti bezbroj proizvođača prosto je nemoguća. Nekolicina proizvođača se grčevito bori za titulu najboljeg softverskog firewall proizvoda, obećavajući nerealne osobine i mogućnosti svojih proizvoda. Testiranjem samih proizvoda se dolazi do zaključka da ne treba

[•] Bishop, M. (2003). *Computer Security: Art and Science.* Boston: Pearson Edukation.

[•] Brian Komar, R. B. (2003). *Firewalls for Dummies 2nd Edition.* Indianapolis: Wiley Publishing.

uvek verovati onom što je lepo i nahvaljeno da je i dobro. Jednakim pristupom na svaki zaštitini zid i testiranjem protiv ranjivosti samog operativnog sistema, špijunaže s malware kodom, testiranja protiv curenja podataka, ponašanje operativnog sistema posle testova, dolazi se do zaključka da se najbolje pokazao Comodo Personal Firewall 2.0.0.0 koji se i posle nekoliko puta podvrgnutih testova ostao dosledan svog imena i obećanja s kojim firma raspolaže.

S obzirom da se u master radu treba voditi putem preciznosti, tačnosti podataka i ocenom kvaliteta teži se ka uspostavljanju svesti kod korisnika za odabir najboljeg softverskog firewall-a.

Dalji tok istraživanja treba da ide ka uspostavljanju novih kriterijuma koje firewall proizvod mora da ispunjava. Dobar zaštitni zid treba da ispunjava ciljeve za koje svaki proizvođač vatrenog zida poseduje ili bar deo od traženih zahteva treba da sadrži. Osnovni kriterijumi za ocenjivanje kompletnog sadržaja i mogućnosti firewall-a se voditi ka tome da firewall bude jednostavan za korišćenje tj. da bude jednostavan za samu konfiguraciju na sistem. Svaki zaštitini zid bi trebao da bude kompatabilan sa svim dosadašnje napravljenim operativnim sistemima bez ograničenja na vremenske zone. Firewall treba da sadrži u sebi tri osnovna principa zaštite o kojima je bilo reči u poglavlju o testiranju (11.Programi za testiranje firewall-a) Kriterijume treba sprovesti i na cenu koja je jedan od glavnih faktora za odabir vatrenog zida, ali i takođe treba napomenuti da firewall treba da podržava opcije za log fajlove, istorijat praćenja firewall-a, tehnička podrška, podrška za uspostavljanje i kombinovanje sa ostalim zaštitinim tehnologijama.[•] (KristianKőpsén, 2006). Hipoteze rada su ostvarene i dolazi se do zaključka da dobro konfigurisan firewall može da se odbrani od različitih vrsta napada. Kod odabira zaštitinog zida treba se pridržavati postavljenih kriterijuma. Budućnost softverskog firewall-a se ogleda u raznovrsnim tehnikama odbrane i kombinovanjem sa ostalim tehnologijama zaštite. Korisniku se daje potpuna bezbednost pomoću ove tehnologije i pruža se mogućnost daljnjeg poboljšanja i unapređivanja sigurnosti svog računarskog sistema.

[•] KristianKőpsén, M. (2006). A comparison of the security ana usability of personal firewalls. Linkőping: Linkőping University.

Literatura:

[1] Angelescu, S. (2010). *CCNA Certification All-In-One For Dummies.* Indiana: Wiley Publishing.

[2] Attribution, C. C. (2013). *Virtual private network*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Virtual_private_network

[3] Baggili, I. (2010). *Digital Forensics and Cyber Crime.* New York: Springer Publishing.

[4] Bennett, J. (2004). *The Digital Umbrella: Technology's Attack on Personal Privacy in America.* Boca Raton, Florida: Brown Walker Press.

[5] Bishop, M. (2003). *Computer Security: Art and Science.* Boston: Pearson Edukation.

[6] Bolakis, S., & Furnell, S. M. (2004). *Helping us to help ourselves: Assessing administrator's use of security tools. Network Security.* United Kingdom: Browse journals.

[7] Brian Komar, R. B. (2003). *Firewalls for Dummies 2nd Edition.* Indianapolis: Wiley Publishing.

[8] Brown, B. C. (2011). *How to Stop E-Mail Spam, Spyware, Malware, Computer Viruses and Hackers.* Ocala, Florida: Atlantic Publishing Company.

[9] Cameron, R. (2005). *Configuring NetScreen Firewalls.* Rockland: Syngress Publishing.

[10] Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* San Diego: Elsevier.

[11] Cheswick, W. R. (2003). *Firewalls and Internet Security, Second Edition. .* Boston: AT&T and Lumeta Corporation.

[12] Crasto, D. (2012). *8 Best firewall for windows*. Retrieved from Techshout.com: http://www.techshout.com/features/2012/25/best-firewall-for-windows-7/

[13] Danny Briere, H. F. (2011). *Wireless Home Networking For Dummies.* Indiana: Wiley Publishing.

[14] Denning, P. J. (1990). *Computers Under Attack: Intruders, Worms, and Viruses.* ADDISON WESLEY.

[15] Docstoct. (2012). Next generation firewall: Palo Alto Networks. *Docstoct* .

[16] Ec-Council. (2011). *Network Defense: Security Policy and Threats.* New York: Ec-Council.

[17] Furnell, S. M. (2004). *Using security: easier said than done. Computer Fraud & Security.* United Kingdom: Browse journals.

[18] Gollmann, D. (2011). *Computer Security.* United Kingdom: John Wiley & Sons.

[19] Heng Yin, D. S. (2013). *Automatic Malware Analysis: An Emulator Based Approach.* New York: Springer.

[20] Inforamtion_services. (2012, 2012). *Inforamtion services and technology*. Retrieved from How Firewalls Work: http://www.bu.edu/tech/security/resources/host-based/intro/

[21] Joshi, J. (2008). *Network Security: Know It All: Know It All.* Burlington: Morgan Kaufman Publischers.

[22] Kompjuterska.biblioteka. (2007, Septembar 20). *KAKO DA vaš računar ostane bezbedan*. Retrieved from Kompjuterska biblioteka: http://saveti.kombib.rs/KAKO_DA_vas_racunar_ostane_bezbedan_-_7._deo.html

[23] KristianKőpsén, M. (2006). *A comparison of the security ana usability of personal firewalls.* Linkőping: Linkőping University.

[24] Matousec. (2013). *Matousec*. From matousec.com: www.matousec.com/projects/proactive-security-challenge-64

[25] Mike Harwood, M. G. (2011). *Security Strategies in Web Applications and Social Networking.* Ontario: Jones & Bartlett Learning.

[26] Miljević. (2007). *Metodologija naučnog rada.* Sarajevo: Filozofski fakultet.

[27] Oppliger, R. (2002). *Internet and Intranet Security.* Norwood: Artech House.

[28] Ragnarsson, P. (2010). *Firewall implementation and testing. .* Sweden: Linkpings universitetet.

[29] Rubenking, N. J. (2006, Februar 21). Spyware. *PC Magazine* , 99.

[30] services, I. a. (n.d.). *How Firewalls Work*. Retrieved from Information and services: http://www.bu.edu/tech/security/resources/host-based/intro/

[31] Smith, T. J. (2012). *Pricing Strategy: Setting Price Levels, Managing Price Discounts.* Mason, USA: CengageBrain.

[32] Spanbauer, S. (2003, Decembar). *Mrežna bezbednost: kako instalirati zaštitni zid*. Retrieved from mikro.rs: http://www.mikro.rs/main/tekstprint.php?tekstID=4159

[33] Technology, I. S. (2013). *How Firewalls Work*. Retrieved from Information Services & Technology: http://www.bu.edu/tech/security/resources/host-based/intro/

[34] Wack, J. (1995, Februar). *Screened Subnet Firewall*. Retrieved from Sunet: http://ftp.sunet.se/pub/security/docs/nistpubs/800-10/node58.html

[35] 10TopTenRewiews. (2013). *Personal Firewall Software Review*. Retrieved 2013 from 10TopTenRewiews: http://personal-firewall-software-review.toptenreviews.com/mcafee- internet-security-review.html

[36] 10TopTenRewiews. (2013). *Personal Firewall Software Review*. Retrieved 2013 from 10TopTenRewiews: http://personal-firewall-software-review.toptenreviews.com/mcafee-internet-security-review.html

[37] http://www.techsupportalert.com/best-free-firewall.htm

[38] https://www.grc.com/securable.htm

[39] http://www.ida.liu.se/~iislab/projects/firewall-comparison/

[40] http://www.techrepublic.com/blog/window-on-windows/review-zonealarm-free-antivirus-firewall- 2013/7561

[41] http://goweb.sgvisions.net/ser/_sigurnost/firewall.html

[42] http://hardware.ittoolbox.com/documents/criteria-in-choosing-a-firewall-15115

Popis slika:

Slika 1 – mreža bez firewall-a

Slika 2 – postavljanje rutera

Slika 3 – postavljanje NAT servisa sa firewall-om

Slika 4 - delovanje proxy servisa

Slika 5. – postavljanje Dual-Homed Gateway firewall-až

Slika 6. – postavljanje Screened Host Gateway firewall-a

Slika 7. – virtuelna privatna mreža

Slika 8 - primer uspostavljanja VPN-a između dve lokalne mreže

Slika 9 - konfiguracije mreže bez servera

Slika 10 - konfiguracije mreže sa serverima lociranim unutar lokalne mreže

Slika 11. konfiguracije mreže sa serverom lociranim između dva firewall

Slika 12 - konfiguracije mreže sa demilitarizovanom zonom

Slika 13 - DMZ sa dva firewall-a

Slika 14 – konfiguracija sa tri mrežna adaptera

Slika15 - postavka hardverskog *firewall*-a u sistem

Slika 16 - početna strana programa

Slika 17 - pokušaj pristupa mreži

Slika 18 - dodatne sigurnosne postavke

Slika 19 - prikaz log fajlov

Slika 20 - instalacija programa

Slika 21 - deinstalacija programa

Slika 23 - blokiranje pristupa

Slika 24 - meni za pomoć korisniku

Slika25- instalacija programa.

Slika26 - izgled glavne strane programa

Slika27 - prozor upozorenja

Slika 28- log fajlovi

Slika 29- instalacija programa

Slika 30- izgled glavnog proz

Slika31 - prozor za konfiguraciju firewall-a

Slika 32- upozorenje o napadu

Slika 33- instalacija programa

Slika 34 - izgled glavnog prozora programa

Slika 35 - obaveštenje o blokiranju saobraćaja

Slika 36 - dodatne kontrole programa

Popis tabela:

Tabela 1 – portovi za rad Internet servera

Tabela 2 - test Comodo Internet Security Plus 2012 Firewall

Tabela 3 - test Agnitum Outpust Pro Firewall

Tabela 4 - test McAfee Firewall

Tabela 5 - test Norton 360 Firewall

Tabela 5 - test ZoneAlarm Pro Firewall 6.1

Tabela 7 - događaji tokom testiranja firewall-a