Univerzitet Singidunum

DEPARTMAN ZA POSTDIPLOMSKE STUDIJE

MASTER STUDIJSKI PROGRAM
SAVREMENE INFORMACIONE TEHNOLOGIJE

ZAŠTITA RAČUNARA I RAČUNARSKIH MREŽA PRIMENOM AV SOFTVERA I FIREWALL-A

- Master rad -

Mentor:
Prof.dr MLADEN VEINOVIĆ

Kandidat:
ĐURO BORJAN
410279/2013

Beograd, 2014. godine

Zaštita računara i računarskih mreža primenom AV softvera i Firewall-a

Sažetak

U ovom master radu opisane su vrste potencijalnih zlonamernih programa i analizirani su načini zaštite. Detaljno je prikazana funkcionalnost zaštitnih zidova (eng. Firewall). Takođe, opisani su neki od tipova zlonamernih pretnji koje se odnose na računarske mreže i korisnike, kao i tipovi zaštite od istih.

U radu su opisani maliciozni programi i načini na koji se oni šire i deluju. Iz poznavanja tih metoda razvijaju se tehnike odbrane od malicioznih programa koje obuhvataju različite pristupe, od kojih su neki takođe opisani u ovom radu.

Zbog raznolikost malicioznih programa obuhvatanje svih aspekata zaštite je veoma težak zadatak. Zbog toga su opisani opšti pristupi problemu, koji mogu biti na različite načine implementirani u stvarnim programskim alatima za odbranu od zlonamernih programa.

Ključne reči: Zaštitni zid, lokalna mreža, virtuelna privatna mreža (VPN), server i filtriranje paketa, antivirus, maliciozni program, spyweare, bootnet, Symantec EndPoint.

Abstract

In this master thesis are described types of potentional malicious programs and analysed ways of protection from them. The Firewall functionality is presented to details. Furthermore, some of types of malicious threats related to Computer Network and users are described, as well as types of protections from them.

This paper describes malicious programs and the ways in which they spread and effect.
From the knowledge of these methods, the defence techniques against malicious programs are being developed which include different approaches and some of them are described in this paper as well.

Considering the malicious programs diversity, the coverage of all aspects of protection is very formidable task. Because of that, this paper describes the general approaches of the problem, which can be implemented in different ways in real programming tools for defence of malicious programs.

Keywords: Firewall, Local Area Network, Virtual Private Network (VPN),server, packet filtering, antivirus, malware, spyweare, bootnet, Symantec EndPoint.

Sadržaj

ZAŠTITA RAČUNARA I RAČUNARSKIH MREŽA PRIMENOM AV SOFTVERA I FIREWALL-A 2

SADRŽAJ 3

ZADATAK ZAVRŠNOG RADA 5

UVOD 6

1. FIREWALL (ZAŠTITNI ZID) – UOPŠTENO I NASTANAK 8

1.1. Šta je Firewall (zaštitni zid) 8
1.2. Vrste firewall-a 9
1.2.1. Firewall-i sa filtriranjem paketa 9
1.2.2 Firewall-i sa praćenjem stanja mreže 11
1.2.3 Firewall na nivou aplikacije (eng. Proxy firewalls) 13
1.2.4. Firewall-i za prevođenje adresa 15
1.2.5. Računarski orjentisani firewall-i 16
1.2.6. Hibridni firewall-i 16

2. STUDIJA SLUČAJA 17

2.1. Praktičan primer realne konfiguracije Firewall-a 17
2.2. Suzdržani (Halted) firewall 19
2.2.1. Uopšteno o Halted firewall-u 20
2.2.2. Prednosti Halted Firewall-a 21
2.2.3. Nedostatci Halted Firewall-a 21
2.3. Firewall programi za personalne računare (PC) 22

3. ZLONAMERNI PROGRAMI I KOMPJUTERSI VIRUSI – UOPŠTENO 24

3.1. Istorija kompjuterskih virusa 25
3.2. Podela malicioznih programa 27
3.2.1. Virusi 27
3.2.2. Crvi 27
3.2.3. Trojanski konji 27
3.2.4. Logičke bombe 28
3.2.5. Klice 28
3.2.6. Iskorištavanje ranjivosti 28
3.2.7. Downloaderi 28
3.2.8. Daileri 29
3.2.9. Dropperi 29
3.2.10. Generatori virusa 29
3.2.11. Keyloggeri 29
3.2.12. Rootkits 29
3.2.13. Spywares 29
3.3. Kako se šire virusi 30
3.3.1. Zaštita od zlonamernih programa (malware) 31

4. MREŽNI NAPADI I PRETNJE NOVE GENERACIJE (BOTNET) 32

4.1. Botnet mreže – nekad 32
4.2. Botnet – danas 32
4.2.1. Napad uskraćivanjem usluga (DoS) 32
4.2.2. Distribuirani napad uskraćivanjem usluga (DDoS) 33

4.3. Arhitektura botnet mreža 34
4.3.1. Moderna arhitektura botnet mreža 35
4.4. Primer botnet napada 35
4.4.1. Stvaranje botnet mreža 36
4.5. Zaštita od botnet napada 37
4.5.1. Zaštita servera od DDoS napada botnet mreže 37
4.5.2. Zaštita ličnih računara od zaraze i ulaska u botnet mrežu 37
4.6. Budućnost botnet mreža 38
4.6.1. Prednosti protokola P2P za napadače 38
4.6.2. Nedostaci P2P protokola za napadače 39
5. STUDIJA SLUČAJA: ANTI-VIRUSNI PROGRAM SYMANTEC ENDPOINT PROTECTION – UOPŠTE 40
5.1. Koje sve novitete nudi Symantec EndPoint Protection? 41
5.1.1. Komponente Symantec EndPoint zaštite 44
5.1.2. Novine u EndPoint tehnologiji 45
5.2. Instalacija EndPoint-a (EP) na radnim stanicama 47
5.2.1. Instalacija remote EndPoint manager consol-e 48
5.2.2. Ikone obaveštenja u Symantec EndPoint antivirusnom sisitemu 52
5.2.3. Ažuriranje polise (Update Policy) 54
5.2.4. Ažuriranje definicije programa (Update definition) 54
5.2.5. Organizacija EndPoint zaštite 56
5.2.6. Rešavanje problema komunikacije EndPoint Client Endpoint Manager 58
5.2.7. Unmanaged client 59
5.2.8. Izveštaj (Report) 59
ZAKLJUČAK 62
LITERATURA 64
BIOGRAFIJA 65

Zadatak završnog rada

Istražiti i objasniti savremene tipove malicioznih programa, kao i, a kroz studiju slučaja prikazati funkcionalnost jednog od poznatijih antivirusnih programa.

Uvod

Rad se bavi odbranom aplikativnog i sistemskog softvera od zlonamernih programa. Navedene su vrste zlonamernih programa i njihove osnovne karakteristike. Osim toga, opisani su principi rada zlonamernih programa, metode širenja i posledice koje mogu imati na zaraženi sistem.[1]

Posebno će biti opisan antivirusni program *Symantec EndPoint Protection*, program za detekciju, sprečavanje i otklanjanje kompjuterskih virusa, distribuiran od strane Symantec Corporation.

U ovom radu opisani su vrste malicioznih programa, te neki od načina na koji se oni šire i deluju. Iz poznavanja tih metoda razvijaju se tehnike odbrane od malicioznih programa koje obuhvataju različite pristupe od kojih su neki takođe opisani u ovom radu.

Raznolikost malicioznih programa čini obuhvatanje svih aspekata zaštite vrlo teškim zadatkom. Zbog toga su opisani opšti pristupi problemu, koji mogu biti na različite načine implementirani u stvarnim programskim alatima za odbranu od zlonamernih programa.

Kao praktični deo rada implementiran je antivirusni program *Symantec EndPoint Protection*, koji može pronaći neke vrste zlonamernih programa i čije se izvođenje temelji na nekim od pristupa opisanim u ovom radu. Iz opisa praktičnog dela mogu se uočiti prednosti i nedostatci jednog od mnogih pristupa ovom problemu.

Zaštitni zid (eng. Firewall) je sigurnosni elemenat koji je smešten između određene računarske mreže (LAN, MAN i WAN) i svetske mreže (Internet), a koji je dizajniran da zaštiti poverljive, korporativne i korisničke podatke od neautorizovanih korisnika (blokiranjem i zabranom komuniciranja pravilima koje definiše usvojena sigurnosna politika).

Nije obavezno da svi korisnici u lokalnoj mreži (LAN) imaju jednaka prava pristupa svetskoj mreži (Internet). Postavljanjem Firewall uređajaj između dva ili više mrežnih segmenata mogu se kontrolisati i prava pristupa pojedinih korisnika pojedinim delovima mreže. U tom slučaju Firewall je dizajniran da dopušta pristup dobrim zahtevima, a blokira sve ostale.

Firewall ujedno, predstavlja idealno rešenje za kreiranje Virtuelne privatne mreže (VPN) jer stvara virtuelni tunel kroz koji putuju kriptovani (zaštićeni) podaci. Takođe, omogućuje sigurnu razmenu osetljivih podataka između udaljenih korisnika (klijenata). Firewall je servis koji se obično sastoji od uređaja i politike pravilnika zaštite (eng. *Policy Security*), koji omogućava korisniku filtriranje određenih tipova mrežne komunikacije sa ciljem da poveća sigurnost i pruži određeni nivo zaštite od zlonamernih napada.

Osnovna namena Firewall-a je da spreči neautorizovani pristup sa jedne mreže na drugu. To znači zaštitu lokalne mreže (LAN) od svetske mreže (Internet). Ako neki informacioni sistem ima Firewall, to znači da je definisano sigurnosnom politikom (eng. Policy Security) šta je dozvoljeno, a šta nije dozvoljeno raditi u toj mreži. Pri planiranju ponude informacionih sistema, politika sigurnosti određuje opcije konfiguracije sistema.

[1] Zahvaljujem se prof dr Mladenu Veinoviću na saradnji i savetima tokom pisanja rada, kao i kolegama i prijateljima koji su pomogli oko nalaženja literature i na njihovim savetima.

Osnovni rad Firewall-a je u ispitivanju Internet Protokola (IP) paketa koji putuju između klijenata i servera, čime se ostvaruje kontrola protoka informacija za svaki servis po IP adresi i portu u oba smera. Za Firewall je tipičan kompromis između sigurnosti i lake upotrebe.

Firewall je odgovoran za više važnih stvari unutar informaciog sistema:

- Mora da implementira politiku sigurnosti. Ako određeno svojstvo nije dozvoljeno, Firewall mora da onemogući rad u tom smislu,
- Firewall treba da beleži sumnjive događaje,
- Firewall treba da upozori administratora na pokušaje proboja i kompromitovanja politike zaštite i
- U neki m slučajevima Firewall može da obezbedi statistiku korišćenja.

Firewall može biti softverski (software) ili hardverski (hardware). Softverski firewall omogućava zaštitu jednog računara, osim u slučaj kada je isti računar preodređen za zaštitu čitave mreže. Hardverski firewall omogućava zaštitu čitave mreže ili određenog broja računara. Za ispravan rad firewall-a, potrebno je precizno odrediti niz pravila koje definišu kakav je mrežni saobraćaj dopušten u pojedinom mrežnom segmentu. Takvom politikom se određuje nivo zaštite koji se želi postići implementacijom firewall usluge.

1. Zaštitni zid (Firewall) – Uopšteno i nastanak

Tehnologija zaštitnog zida (eng. *firewall*) mnogo se menjala tokom godina, od kada se prvi put pojavila na tržištu početkom 90-ih godina. Prvi firewall-i su bili jednostavnio uređaji za filtriranje paketa. Od tada su oni postali sve napredniji što se tiče mogućnosti filtriranja, ali i dodavali su neke nove funkcionalnosti, npr. kao što su:

- praćenje stanja veze (eng *stateful firewall*),
- virtuelne privatne mreže (eng. *Virtual Private Network – VPN*),
- sistemi za detekciju napada,
- provera autentičnosti komunikacije i
- virtuelni firewall.

Jedan od podsticaja za razvoj dodatnih usluga na zaštitnim zidovima (eng *firewall*) bio je veliko širenje usluga na Internetu koje su sa sobom dovele veliku količinu problema za mrežnu sigurnost.

1.1. Šta je Firewall (zaštitni zid)

Ime zaštitni zid, negde poznatiji kao zaštitni zid, ne potiče iz mrežne sigurnosti. Pravo poreklo naziva je poteklo kao metoda izgradnje zidova u slučaju stvarnih požara, kako bi vatra bila zadržana u jednom delu zgrade bez njenog daljnjeg širenja.

Kada se priča o mrežnoj sigurnosti, zaštitni zid (engl. *firewall*) ima sasvim drugo značenje, ali mu je suština ista, firewall štiti mrežu od potencijalnih napadača sa ciljem da ih zaustavi na tačno definisanim granicama.

Sama osnova firewall-a je uređaj koji kontroliše tok podataka između raznih delova mreže. Važno je primetiti da sama definicija firewall-a može uključivati i više uređaja. Kod male kućne mreže, sastoji se od jednog uređaja, dok kod neke veće implementacije može se sačinjavati od više komponenti, kao što su: pristupni firewall, firewall sa praćenjem stanja veze, virtuelna privatna mreža (eng. *Virtual Private Network*), sistem za detekciju instrukcija (eng. *Istructiona detection system – IDS*), itd.

Mnogi pretpostavljaju da je osnovna namena firewall-a zaštita mreže od spoljnih pretnji, prvenstveno sa Interneta gde se koristi TCP/IP protokol (eng. *Transmission Control Protocol/Internet Protocol*). Nasuprot tome, većina mrežnih pretnji i napada u mnogim slučajevima dolazi iz unutrašnjeg dela mreže, od samih radnika firme. Mnoge studije potvrđuju da čak 60% mrežnih napada dolazi iz unutrašnjosti, a ne sa Interneta. Osim toga, unutar nekih mreža koristi se više protokola, kao što su: TCP/IP, IPX (eng. *Internetwork Packet Exchange*), AppleTalk, SNA (eng. *System Network Architecture*), NetBIOS i dr. Samim tim, jasno je da firewall mora podržavati više protokola i da bude u mogućnosti da se suprostavi pretnjama koje dolaze sa svih strana.

Samo firewall rešenje je bolje posmatrati kao neku celinu, kao neki odbrambeni sistem jer će se obično koristiti više tehnologija i uređaja da bi se ono imlementovalo. Firewall sistem može biti smešten u jednoj matičnoj ploči ili može imati više samostalnih uređaja raspoređenih po mreži.

1.2. Vrste firewall-a

Firewall sistemi mogu izvršavati različite funkcije i ponuditi različita rešenja, ali primarna funkcija firewall-a je kontrola pristupa određenim resursima. Firewall sistem sastoji se od više različitih komponenti. Jedna od tih komponenti je i filtriranje mrežnog protoka koje većina ljudi zove firewall (zaštitni zid).

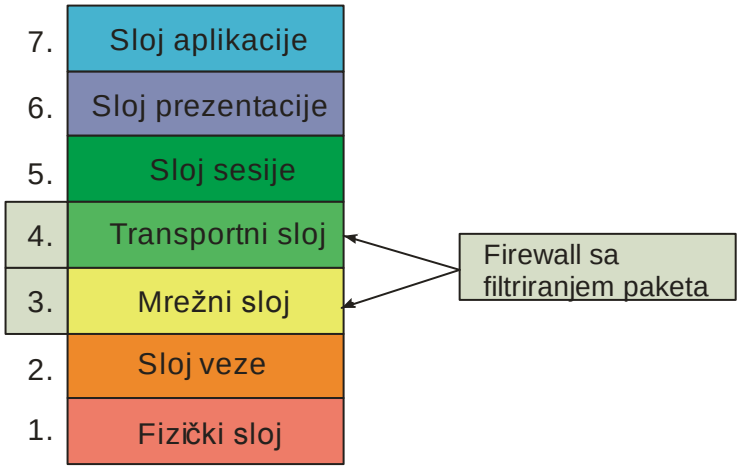
Zaštitni zid (eng. firewall) za filtriranje saobraćaja čine više različitih tipova, kao što su:

- Zaštitni zid za filtriranje paketa,
- Zaštitni zid sa praćenjem stanja veze (eng. *stateful firewall*),
- Zaštitni zid na nivou aplikacije (eng. *application gateway firewall*),
- Zaštitni zid za prevođenje adresa (eng. *address-translation firewall*),
- Firewall baziran na hostu (eng. host-based *firewall*) i
- Hibridni zaštitni zid.

Zavisno od načina rada firewall komponente za filtriranje, imaju različiti nivoi zaštite. Naravno, način rada firewall-a mnogo zavisi i od same performanse firewall-a.

1.2.1. Firewall-i sa filtriranjem paketa

Najjednostavniji oblik firewall-a je firewall sa filtriranjem paketa. On je napravljen kao usmerivač koji ima mogućnost filtriranja paketa zavisno od njegovog sadržaja. Informacije koje firewall sa filtriranjem paketa može koristiti kod filtriranja su informacije na mrežnom nivou, a ponekad i na transportnom nivou OSI referentnog modela. Na primer, kod Cisco rutera standardna pristupn lista (eng. *Access Control List - ACL*) može filtrirati informacije i na mrežnom nivou OSI modela, dok proširena preistupna lista (*ACL*) može filterirati informacije i na mrežnom i na transportnom nivou OSI modela. Slika br.1.



Slika br. 1. – Firewall sa filtriranjem paketa (OSI model)

Iako je danas TCP/IP standard u komunikacionim protokolima, svi firewall-i minimalno podržavaju taj protokol. Neki podržavaju i druge protokole kao što su IPX, AppleTalk, DECnet, ali u današnje vreme sve je manje potrebe za njima.

Kod implementacije filtriranja paketa, pravila filtriranja definišu se na samom firewall-u. Takva pravila koriste se za definisanje sadržaja paketa i na taj način se odlučuje koji paket se dopušta, a koji će se zabraniti i odbaciti. Kod odbacivanja paketa postoje dve mogućnosti. Jedna od njih je da se obavesti

pošiljaoc da je paket odbačen, a druga opcija je da se paket odbaci bez bilo kakvog obaveštenja. Ova funkcionalnost je jako bitna kod implementacije firewall rešenja.

Kod prve opcije, korisnik je obavešten da se njegov sadržaj filtrira pomoću firewall-a. Ako je reč o nekom lokalnom korisniku koji pokušava pristupiti nekim lokalnim resursima, on treba da kontaktira administratora kako bi mogao rešiti problem. Administrator na osnovu toga može promeniti pravila i dopustiti pristup do određenih resursa. Ako firewall ne pošalje povratnu poruku da je saobraćaj filtriran, postupak otkrivanja greške sa strane korisnika bi trajao mnogo duže.

Takođe, ako je reč o zlonamernom korisniku koji pristupa preko Interneta i želi da dospe do nekih resursa koji su predviđeni samo za zaposlene radnike neke firme, informacija o filtriranom saobraćaju otkrila bi i neke detalje o zaštiti mreže, pa bi napadač imao više informacija kako da otkrije potencijalnu rupu u zaštiti. U tom slučaju poželjno je da firewall odbaci paket bez nijednog obaveštenja pošiljaoca.

Firewall-i sa filtriranjem paketa mogu raditi filtriranje po sledećim informacijama:

- izvorna i odredišna adresa mrežnog nivoa (3. nivo OSI sistema),
- informacije o protokolu mrežnog nivoa (npr. specifična ICMP poruka, eng. *Internet Control Message Protocol*),
- informacije o protokolu transportnog nivoa (npr. određeni TCP ili UDP port) i
- Interfejs na koji je paket poslan ili primljen.

Neke od informacija koje TCP/IP firewall može koristiti za filtriranje saobraćaja. Tabela broj 1. Informacije su podeljene po slojevima OSI modela i jasno se može videti kojem sloju pripada određena informacija.

OSI nivo	Informacija za filtriranje
3.	IP adresa
3.	TCP/IP protokol, kao što su IP, ICMP, OSPF, TCP, UDP
3.	IP prednosti (tip servisa ToS)
4.	broj TCP i UDP porta
4.	TCP kontrolne zastavice SYN, ACK, FIN, PSH, RST i druge

Tabela br. 1. Informacije za filtriranje mrežnog saobraćaja

Kod filtriranja paketa jedna od bitnih činjenica je i smer prolaska samih paketa jer se pravila koja se definišu pridružuju se određenom interfejsu u određenom smeru, tako da mogu se imati različita pravila za odlazni i dolazni saobraćaj u istom interfejsu.

Osnovne prednosti firewall-a sa filtriranjem paketa svakako su velika brzina izvršenja samih paketa, kao i fleksibilnost izrade pravila koja uključuju filtriranje po delovima zaglavlja paketa na mrežnom i transportnom nivou. Iako je ta funkcionalnost prisutna kod većine rutera, sami ruteri mogu biti u ulozi krajnjih firewall-a, kao i jednostavnim filtriranjem na mežnom i transportnom nivou mogu pružiti zaštitu od mnogih vrsta napada što uključuje i neke vrste DoS napada i vrši filtriranje ostalog neželjenog saobraćaja.

Firewall sa filtriranjem paketa, takođe, imaju i nekih nedostataka. Osnovni nedostatak je nemogućnost filtriranja na aplikacionom nivou jer oni sami ne razlikuju mrežni promet određenih aplikacija. Uz to, takvi firewall-i su osetljivi na nekiim napadima na TCP/IP protokol i ne podržavaju ni jednu proveru autentičnosti prlikom ostvarivanja veze. Takođe, logovanje koje mogu da proizvedu je ograničeno sa obzirom na informacije koje se mogu koristiti za filtriranje, tj. informacije na mrežnom i transportnom nivou.

Pored navedenog, firewall sa filtriranjem paketa ne može sprečiti sve vrste napada. Administratori moraju dobro poznavati sve TCP/IP protokole kako slučajno lošom konfiguracijom ne bi blokirali loš saobraćaj, što daje jednu dozu kompleksnosti samom rešenju, kako kod planiranja, tako i kod održavanja.

Imajući u vidu sve prednosti i nedostatke takvog firewall-a, lako je uočiti gde se on može najbolje upotrebiti. Takav firewall se može koristiti kao prva linija odbrane i sa njim se može sprečiti veliku količinu DoS napada. Još jedna od njegovih primena jeste postavljanje firewall-a na deo mreže gde se sigurnosna politika može implementirati samo filtriranjem paketa ili gde je bitna cena samog firewall-a, kao npr kod rutera za kućnu upotrebu gde je razmera cene i performanse značajniji od samih funkcionalnosti.

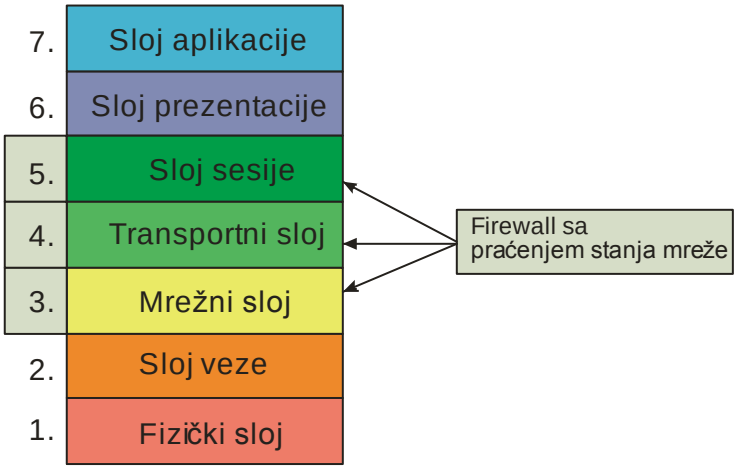
1.2.2 Firewall-i sa praćenjem stanja mreže

Za razliku od firewall-a sa filtriranjem paketa, firewall sa praćenjem stanja veze detaljno prati svaku konekciju. Takav firewall tačno poznaje da li je konekcija tek u uspostavljanju, ima li protoka kroz nju ili je čak u postupku isključivanja. To je mnogo korisno ako se želi zabraniti uspostavljanje neke konekcije sa uređaja koji su sa spoljne strane firewall-a, dok se korisnicima unutar lokalne mreže želi omogućiti konekcije prema spoljnim uređajima, kao i u isto vreme dopustiti povratni mrežni saobraćaj kroz firewall.

Ta fleksibilnost firewall-a sa praćenjem stanja veze uveliko olakšava konfiguraciju firewall-a, funkcija praćenja stanja veze doprinosi boljoj mrežnoj sigurnosti, ali i povećava kompleksnost samog firewall-a.

Postoji mnogo nesuglasica oko tačne definicije na kojem OSI nivou funkcioniše firewall sa praćenjem stanja mreže. Vodi se diskusija da li radi samo na trećem i četvrtom nivou (mrežni i transportni sloj) ili radi na tri nivoa tj. na mrežnom, transportnom i na nivou sesije. Iz perspektive transportnog niva OSI modela, firewall sa praćenjem stanja veze koristi informacije u interfejsima paketa sa trećeg nivoa i delovima sa četvrtog nivoa. Kao na primer, firewall traži u TCP interfejsu SYN, RST, ACK, FIN i ostale kontrolne zastavice da se utvrdi stanje konekcije.

Takođe, sloj sesije uspostavlja i prekida konekcije, a transportni nivo omogućava same mehanizme konekcije. Mnogi tvrde da firewall sa praćenjem stanja konekcije radi na nivou sesije. Slika br.2.

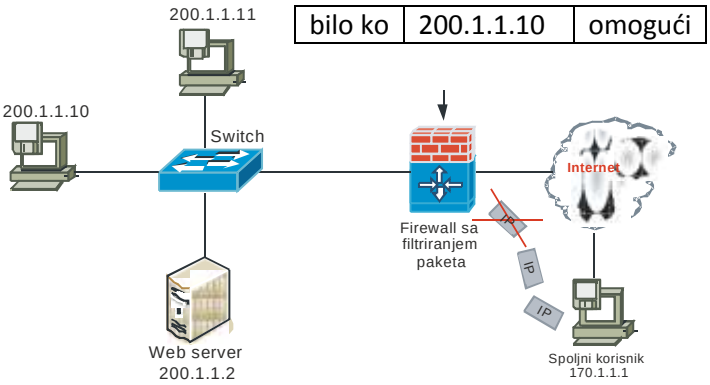


Slika br. 2. Šematski prikaz firewall-a sa praćenjem stanja mreže

U nastavku teksta biće opisani problemi koje sve ima firewall sa filtriranjem paketa i kako se u takvim problemima „snalazi“ firewall sa praćenjem stanja mreže.

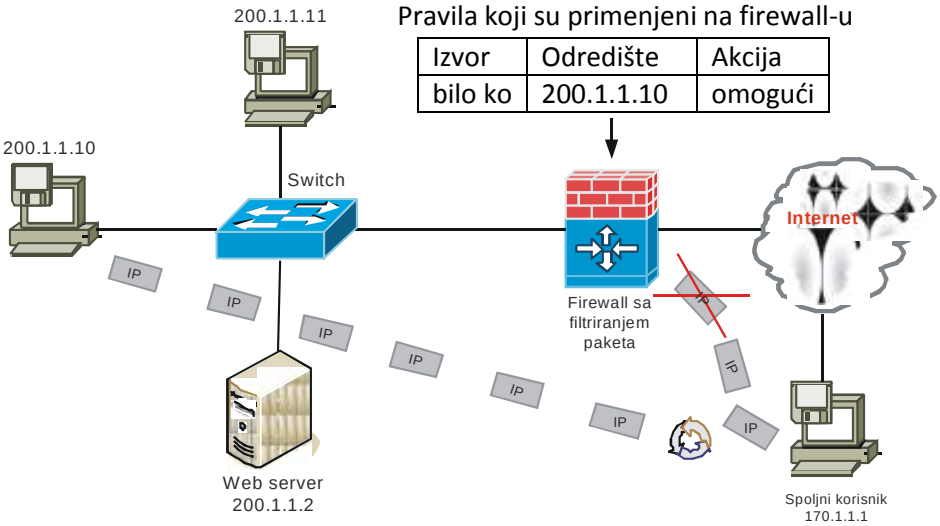
Pravila koji su primenjeni na firewall-u

Izvor	Odredište	Akcija



Slika br. 3. – Šematski prikaz načina rada firewall-a sa filtriranjem paketa

Jednostavna mreža sa firewall-om sa filtriranjem paketa koji mrežu štiti od spoljnih korisnika prikazana je na slici 3. Kao jedno od pravila koje je definisano da bilo koja konekcija sa spoljne strane firewall-a nije dozvoljena sa kompjuterom koji ima IP adresu 200.1.1.10.
Iako HTTP protokol koristi TCP, potrebno je ostvariti konekciju sa tzv. mehanizme trostrukog delovanja (eng. *tree-way handshake*). Računar sa IP adresom 200.1.1.10 će poslati SYN poruku sa izvornog porta koji je veći od 1023 (portovi do 1023 su rezervisani za poznate servise i operativni sistem ih obično dodeljuje korisniku), na ciljni računar 170.1.1.1 sa portom 80 gde se nelazi web servis. Da bi mehanizam trostrukog delovanja uspešno završio, potrebno je da računar 170.1.1.1 odgovori sa SYN/ACK porukom i da računar sa IP adresom 200.1.1.11 posalje poruku sa ACK odgovorom. Slika br.4.



Slika br. 4. Način rada firewall-a sa filtriranjem paketa sa trostrukim mehanizmom delovanja

Obzirom da je u pravilima definisano da paket sa ciljnom adresom 200.1.1.10 koji dolazi sa spoljne strane firewall-a treba biti odbačen, konekcija sa kojom je pokušana komunikacija sa unutrašnjom stranom firewall-a, neće se moći uspostaviti.

Takav problem se može rešiti na dva načina. Jedno od rešenja je naravno da se u tabelu pravila napravi izuzetak i da se svi portovi iznad 1023 propuste sa spoljne strane firewall-a do računara sa IP adresom

200.1.1.10. Ovakvo rešenje se ne preporučuje jer se narušava sigurnost cele mreže i stvara se velika rupa u sigurnosti sistema.

Drugo rešenje je da provera određenih paketa na transportnom nivou, da bi se odredilo da li je paket deo već ostvarene konekcije ili je to pokušaj uspostavljanja nove konekcije. Podaci koji se proveravaju su kontrolne zastavice u TCP interfejsu. Tabela br.2.

TCP	Opis
SYN	Koristi se kod pokretanja konekcije i sinhronizacije rednog broja paketa
ACK	Potvrđuje primljene pakete
FIN	Označava kraj konekcije
PSH	Obaveštava primaoca da isporučeni podatak isporuči aplikaciji
RST	Prekida TCP konekciju
URG	Pokazuje hitnost podataka u korisničkom sadržaju

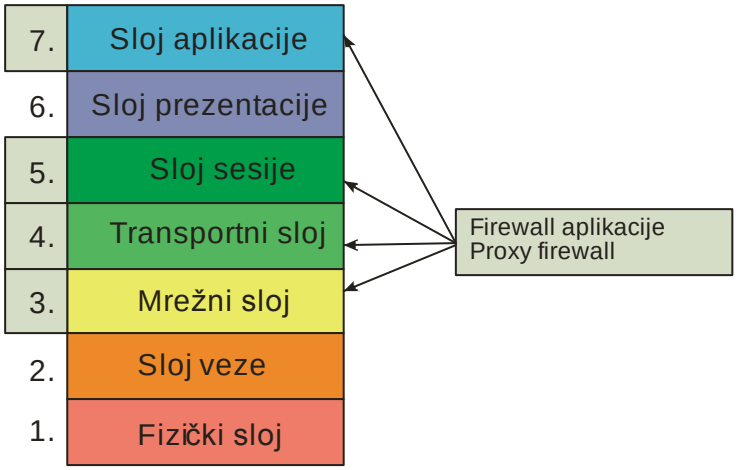
Tabela br. 2. Kontrolne zastavice u TCP interfejsu

1.2.3 Firewall na nivou aplikacije (eng. Proxy firewalls)

Firewall na nivou aplikacije ili firewall sa proksijem (eng. *proxy firewalls*) filtrira podatke od 3 do 7 nivoa OSI modela (mrežni, transportni, sloj sesije i sloj aplikacije). Iako su oni sposobni da određuju informacije na nivou aplikacije, većina funkcija za upravljanje i filtriranje odvija se uz pomoć programske podrške. Takav način filtriranja omogućava bolju kontrolu saobraćaja koji prolazi kroz firewall neko kod ostalih vrsta firewall-a.

Firewall-i na nivou aplikacije često podržavaju samo ograničen skup aplikacija i čest osu to samo e-mail, WWW, FTP, telnet, usnet, LDAP i finger.

Jedna od osnovnih funkcija firewall-a na nivou aplikacije je provera autentičnosti prilikom uspostavljanja konekcije, nije bitno da li se radi o konekciji koja je inicirana sa spoljne strane firewall-a prema unutra ka zaštićenim resursima ili obrnuto. Proksi firewall-i (eng. Proxy firewalls) mogu da koriste više različitih metoda provere autentičnosti prilikom uspostavljanja konekcije: korisničko ime i lozinku, token kartice, adresu mrežnog nivoa i biometrijske informacije. Adrese mrežnog sloja retko se koriste za proveru autentičnosti, osim ako se ne koriste u kombinaciji sa još nekom metodom. Slika br.5.



Slika br. 5. – Firewall na nivou aplikacije (Proxy firewall)

Firewall-i na nivou aplikacije grubo se mogu podeliti u dve kategorije:

- Connections gateway firewall i
- Cut-through proxy

Ove dve vrste firewall-a se razlikuju po nivou zaštite i resursima koje troše. *Cut-trough Proxy* je jednostavniji jer će kod konekcije tražiti proveru autentičnosti korisnika. Ako provera autentičnosti bude uspešna, ova vrsta firewall-a više neće raditi analizu saobraćaja od korisnika, već će analizirati ceo saobraćaj i nakon uspešne provere autentičnosti omogući će dodatne nivoe zaštite na nivou aplikacije.

Na primer, korisniku se može ograničiti pojedine Java aplikacije ili ActiveX skripte koje se mogu izvršavati, a kod TelNet i FTP konekcije koje se komande mogu izvršavati, kao i u kojima folderima korisnik može da pristupi, a kojima ne može. Ovde se može primetiti da *Connection gateway firewalls* koristi mnogo više resursa jer prati sve konekcije na nivou aplikacije.

Firewall-i na nivou aplikacije imaju neke prednosti u odnosu na firewall-e sa filtriranjem paketa i praćenjem stanja veza, a to su:

- Oni proveravaju autentičnost osobe, a ne komponente,
- Potencijalni napadači će mnogo teže implementirati neke od napada prisluškivanjem ili uskraćivanjem pojedinih resursa,
- Firewall-i na nivou aplikacije mogu kontrolisati i filtrirati određene podatke u samoj aplikaciji i
- Mogu detaljnije generisati logove.

Firewall-i na nivou aplikacije imaju i nedostatke, kao što su:

- Ceo proces paketa napravljen je u programskoj podršci i nije moguće ga ubrzati koristeći izloženi mehanizam,
- Ne podržavaju veliki broj aplikacija i
- Nekada zahtevaju od korisnika da koristi poseban program za pristup i proveru autentičnosti.

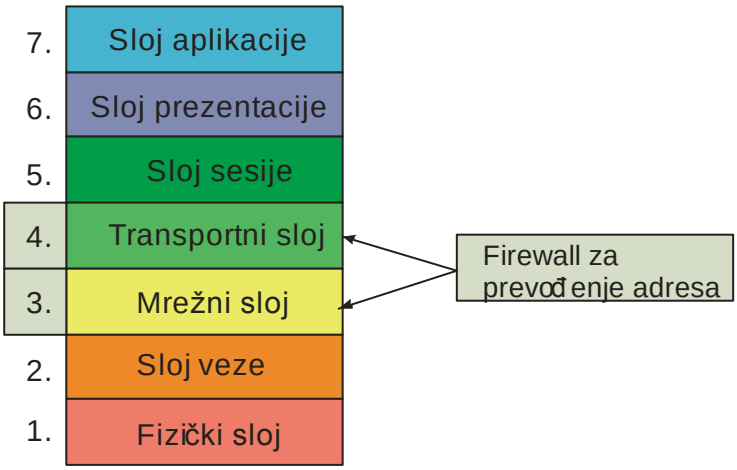
1.2.4. Firewall-i za prevođenje adresa

Firewall-i za prevođenje adresa (eng. *Network Address Translation*) su dizajnirani iz dva razloga:

- Proširenje broja adresa koje korisnik može koristiti i
- Skrivanje mrežne topologije i adresa koje se koriste iz spoljnog sveta.

Osnovni razlog njihove implementacije je definisanje standarda RFC1631 (NAT) i RFC1918 (privatne IP adrese) koji su definisali pojam privatne IP adrese i metode prevođenja tih privatnih IP adresa u javne, kako bi se mogle koristiti na Internetu. Takva prevođenja uključuju prevođenja izvorne i/ili krajnje adrese, kao i izvornog i/ili krajnjeg porta ako se radi o TCP/UDP paketima.

Sigurnost zasnovana na prevođenju adresa, oslanja se na to da ako se neko želi ponovo pristupiti uređaju koji se nalazi iza zaštitnog zida, mora se na firewall-u definisati prevođenje IP adresa. Kad se prevođenje ne bi definisalo paketi se ne bi mogli usmeriti do željenog firewall-a, kao ni do željenog servisa. Takođe, koristeći prevođenje adresa, servise koji se izvršavaju na različitim fizičkom serverima moguće je prikazati da se nalaze na istom serveru ili obrnuto. To omogućuje da se sakrije fizička i logička topologija mreže koja se nalazi iza zaštitnog zida. Slika br.6.



Slika br. 6. – Nivoi na kojima radi firewall za prevođenje adresa

Firewall-i za prevođenje adresa imaju određene nedostatke. Neki protokoli, kao na primer IPSec, određeni VoIP protokoli, kao i protokoli koji koriste dinamičke portove ne podržavaju prevođenje adresa i da bi oni mogli normalno funkcionisati, potrebno je koristiti kombinaciju firewall-a na nivou aplikacije i firewall-a za prevođenje IP adresa.

1.2.5. Računarski orjentisani firewall-i

Računarski orjentisani firewall-i (eng. Computer-oriented firewalls) su u stvari računari ili serveri na kojima se izvršava firewall program.

Ovi firewall-i obično nemaju iste mogućnosti kao prethodno navedeni. Oni pojednostavljeni firewall-i za filtriranje paketa i kao takvi sposobni su samo filtrirati IP saobraćaj po izvornim ili odredišnim IP adresama ili po izvornim i odredišnim portovima, ako je reč o TCP/UDP mrežnom saobraćaju.

Računarski orjentisani firewall-i su napravljeni kao jeftina alternativa ostalima verzijama firewall-a, ali sa nekim manjim mogućnostima zaštite. Lako je uočiti sve njihove prednosti i mane. Računarski orjentisane firewall-e ne treba koristiti kao jedini nivo zaštite u mrežama, nego samo kao dodatak na opštu sigurnost.

1.2.6. Hibridni firewall-i

Zbog velikog i brzog razvoja novih tehnologija, proširenosti Interneta i različitih poslovanja koji svakodnevno koriste Internet kao komunikaciju, potreba za mrežnom sigurnošću se mnogo povećala. Takođe, klasifikacija firewall-a potrebnih za određenu vrstu zaštite pokazala kao težak posao. Kako bi obezbedili jaku mrežnu sigurnost, određeni proizvođači mrežne opreme kombinuju više vrsta prethodno navedenih firewall-a u jednom uređaju.

Takvi firewall-i se nazivaju hibridni firewall-i i uz posedovanje više vrsta prethodno navedenih, mogu obavljati i ostale funkcije kao što su koncentrisanje VPN saobraćaja, filtriranje IDS zaštite i usmeravanje IP saobraćaja.

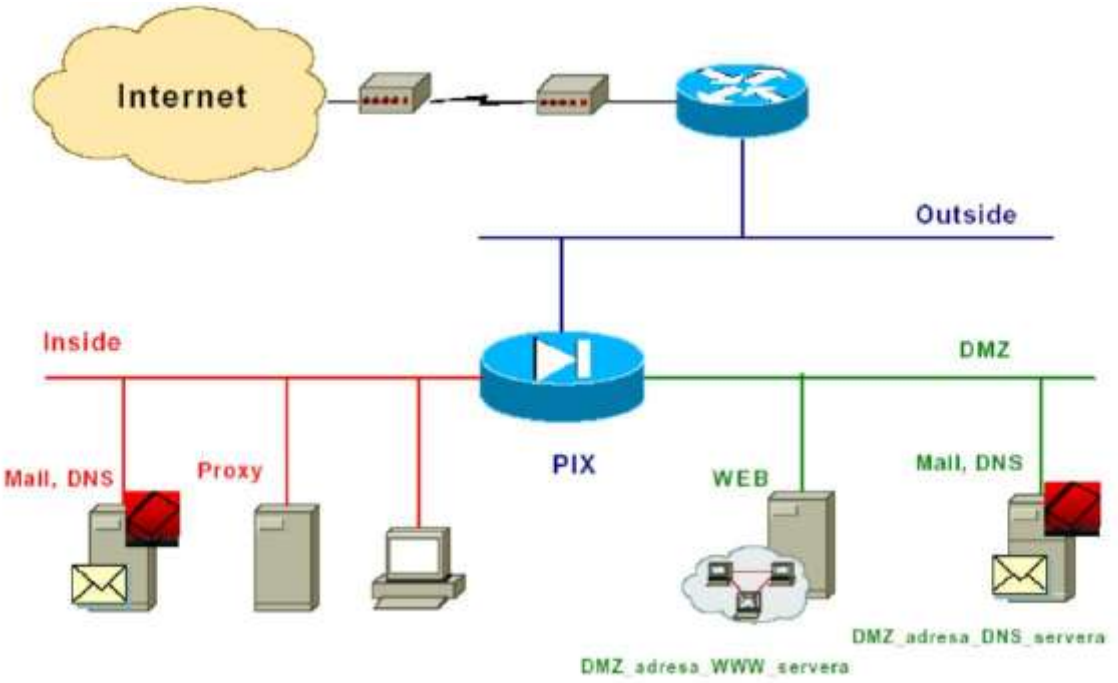
Hibridni firewall-i danas predstavljaju standard i vrlo retko se može naći firewall-e koji su specifični samo za jednu vrstu zaštite.

2. STUDIJA SLUČAJA

2.1. Praktičan primer realne konfiguracije Firewall-a

Bezbedno povezivanje lokalne mreže na Internet je ostvareno korišćenjem uređaja predviđenog za zaštitu Cisco 515 Firewall. Ovaj uređaj predstavlja rešenje kompanije Cisco koje pružaju veoma visoke nivoe sigurnosti za mala i srednja preduzeća. Platforma za privatnu razmenu podataka sa Internetom (eng. *Private Internet eXchange-PIX*) u potpunosti podržava implementaciju Internet protokola za sigurnost (eng. *Internet Protocol Security-IPSec*)-a i formiranje VPN tunela između dve platforme za privatnu razmenu podataka sa Internetom (*PIX*), između PIX -a i Cisco VPN rutera kao i između PIX -a i Cisco Secure VPN klijenta. Slika br.7.

PIX -515 sa softverom i sa ograničenom licencom ima dovoljno snage za više od 50.000 istovremenih konekcija i propusni opseg do 170 Mbps (eng. *Mega bits per second*). Tri mrežna adaptera, koje uređaj poseduje, omogućavajuju kreirenje privatne zone u kojoj se nalazi lokalna računarska mreža kompanije, demilitarizovane zone u kojoj su smešteni javni web, mail i DNS serveri, kao i javne zone za vezu ka Internet provajderu.



Slika br. 7. – Primer realne konfiguracije mreže sa Cisco-vim Fierewall-om

Između interfejsa se obavlja prevođenje adresa. Unutrašnja mreža ima privatne adrese, demilitarizovana zona (DMZ) ima standardne RFC 1918 adrese, a spoljašnja mreža ima legalno registrovane adrese (212.62.52.128/27).

Konfiguracija firewall-a je takva da je zabranjen ceo saobraćaj osim onog koji se posebno dozvoli. Sa spoljašnje mreže mora biti propušten Web, DNS i Mail ka odgovarajućim javnim serverima koji su smešteni u DMZ-u.

To se postiže statičkim mapiranjem adresa servera i upotrebom odgovarajućih pristupnih lista:

```
Static (DMZ,OutSide) 212.62.53.130 DMZ_adresa_DNS_servera netmask
255.255.255.255 0 0
```

```
Static (DMZ,OutSide) 212.62.53.132 DMZ_adresa_WWW_servera netmask
255.255.255.255 0 0
Access-list outside-intf permit TCP any host 212.62.53.130 eq SMTP
Access-list outside-intf permit UDP any host 212.62.53.130 eq domain
Access-list outside-intf permit TCP any host 212.62.53.130 eq domain
Access-list outside-intf permit tcp any host 212.62.53.132 eq www
access-group outside-intf in interface outside
```

Ceo ostali saobraćaj iz spoljašnje mreže prema DMZ-u je zabranjen. Iz DMZ-a prema spoljnoj mreži je propušten samo Mail i DNS sa Mail i DNS servera:

```
Access-list dmz-intf permit tcp host DMZ_adresa_DNS_servera any eq smtp
Access-list dmz-intf permit tcp host DMZ_adresa_DNS_servera any eq
domain Access-list dmz-intf permit udp host DMZ_adresa_DNS_servera any
eq domain Access-group dmz-intf in interface dmz
```

Što se tiče komunikacije između DMZ-a i privatne zone, iz DMZ-a je propušten samo Mail sa javnog Mail servera prema kompanijskom internom serveru za elektronsku poštu. Iz privatnog dela, dozvoljen je DNS saobraćaj sa Proxy servera prema DNS serveru i Mail konekcije od internog prema javnom Mail serveru.

Ovim tehničkom rešenju, izlazak korisnika na Internet je predviđen isključivo preko Proxy servera. Prema tome moraju biti propušteni odgovarajući portovi sa Proxy servera prema javnoj zoni. U obrnutom smeru, od javne prema privatnoj zoni, zabranjen je sav saobraćaj. Veoma korisnu opciju koju PIX (eng. *Private Internet eXchange)* podržava je dodatna zaštita javnog SMTP (eng. *Simple Mail Transfer Protocol*) servera podizanjem *Mail Guard*-a komandom:

```
 fixup protocol smtp
```

Na ovoj način SMTP server može primiti samo RFC 821 komande:

```
HELLO, RCPT, DATA, RSET, NOOP i QUIT.
```

Sve druge komande će biti odbačene sa porukom: "*500 command unrecognized*". Takođe, svi karakteri u SMTP baneru, osim "0" i "2" se menjaju u "*".
Karakterističan baner izgleda ovako:

```
220 ************************************************22*****2002***********0*00
```

"Fixup protocol" komande koje mogu menjati servise i protokole na aplikativnom nivou primenju se i za FTP, HTTP, h323, RSH, RTSP, SIP i SQLNet protokole.

2.2. Suzdržani (Halted) firewall

Suzdržani firewall *(*eng. *Halted* firewall) nije gotov proizvod, tj. nije ga moguće nabaviti u obliku programskog paketa ili neke konfiguracije. To je samo rešenje kako poboljšati sigurnosne karakteristike firewall-a baziranog na Linux alatima za filtriranje paketa (*IP Chains* i *IP Tables*).

Ideja suzdržanog (eng. *halted*) firewall-a bazira se na postupku isključenja računara sa Linux operativnim sistemom. Na modernim operativnim sistemima nije moguće jednostavno isključiti napajanje računara prilikom isključenja. Po pravilu, računar pre samog prekidanja napajanja mora obaviti radnje kao što su snimanje zaostalih podataka na hard disk i sl., tako da se isključenje računara mora pokrenuti zadavanjem određene komande operativnom sistemu. U Linux operativnom sistemu se isključenje računara pokreće komandama *shutdown -h* ili *halt* (ove naredbe su identične). Nakon upisivanja jedne od ovih dve komande na računaru se pokreće *halt* deo, tj. dešava se sledeće:

- Računar prelazi u *runlevel 0,*
- Izvršavaju se sve skripte iz /etc/rc0 direktorijuma (ove skripte su zadužene za isključivanje sviih servera i servisa pokrenutih na računaru),
- Gase se svi procesi koji su trenutno aktivni,
- Otklanjaju se svi sistemi datoteka (eng. *unmount*),
- Gase se sve mrežne maske (eng. *interfaces*) i
- Uklanjaju se svi vanjski moduli iz jezgra (*kernel*) operativnog sistema.

Nakon što su odrađene sve navedene radnje, odnosno nakon što se završila *halt* sekvenca, na računaru se može isključiti napajanje. Stanje u kojem se računar nalazi nakon završetka halt sekvence, a pre gašenja napajanja, naziva se *halted.* U *halted* stanju računar je, od strane korisnika, "mrtav", odnosno. na njemu se ne može ništa raditi jer su svi procesi, diskovi i mrežne maske (eng. interfaces) ugašeni. Ali iako su procesor i memorija još uvijek priključeni na napajanje, procesor i dalje izvršava instrukcije koje se nalaze u memoriji. U *halted* stanju u memoriji ostaje samo jezgro *(kernel)* operativnog sistema iako su svi procesi ugašeni tokom *halt* sekvence.

Halted firewall je običan Linux firewall realizovan pomoću Linux alata za filtriranje paketa (*IP Chains* ili *IP Tables*) kod kojeg se modifikacijama *halt* sekvence postiže zadržavanje funkcija za filtriranje paketa i u *halt* stanju. Nakon što je računar ušao u *halt* stanje, sve njegove funkcije (osim funkcija za filtriranje paketa) su ugašene i računar radi isključivo kao firewall.

To je vrlo povoljno sa sigurnosnih aspekata zato što su napadi prilikom kojih napadač dobija administratorska ovlaštenja nad računarom u potpunosti onemogućeni (računar je, u pogledu od strane korisnika, potpuno "mrtav"). U pogledu DoS napada, *halted* firewall nema nikakvih prednosti (ali niti mana) u odnosu na običan firewall baziran na Linux alatima za filtriranje paketa (*IP Chains* i *IP Tables*).
Detalji o instalaciji i konfiguraciji *halted* firewall-a pomoću *IP Tables* programskog paketa opisani su u sledećim poglavljima.

2.2.1. Uopšteno o Halted firewall-u

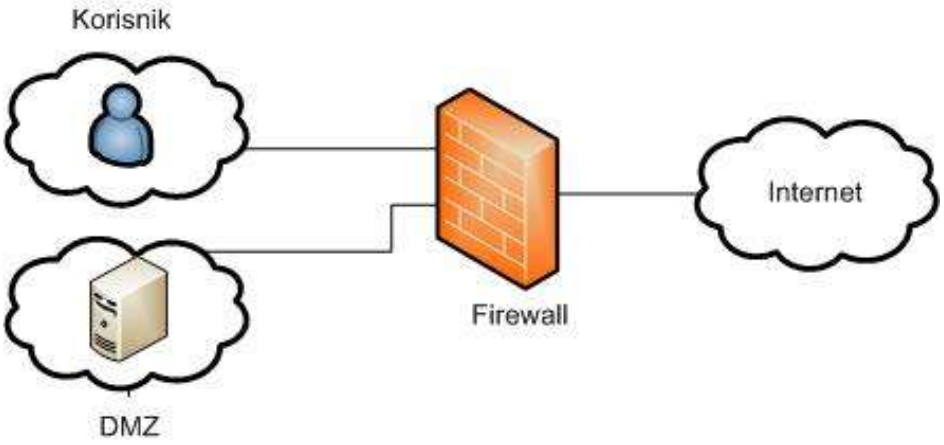
Halted firewall je softverski firewall koji se može implementirati na klasičnom računaru i nije vezan za konfiguracijska specifična rešenja. Konfiguracija računara na koje je firewall instalisan određuje performanse samog firewall-a (to se najviše odnosi na brzinu rada i propusnost firewall-a). Firewall je realizovan pomoću Linux alata za filtriranje paketa (*IP Tables*) koji imaju ugrađenu podršku za NAT i *stateful inspection,* ali im nedostaje podrška za VPN tehnologiju i podrška za VLAN-ove.
Programska podrška pomoću koje je firewall realizovan je besplatna i dolazi standardno sa svim Linux distribucijama.
Minimalni konfiguracioni zahtevi koji se preporučaju su sledeći:

- procesor brzine 800 MHz,
- 1 GB HARD diska,
- 256 MB RAM memorije i
- dve ili više mrežnih kartica.

Zbog činjenice da firewall radi u *halted* stanju u kojem su hard diskovi isključeni, zahtevi na veličinu hard diska nisu veliki. S druge strane, budući da u *halted* radu firewall-a nema tvrdih diskova (nema ni *swap* diska), za veće mreže (više od 10 računara) potrebno je obezbediti dovoljno RAM memorije kako bi firewall mogao obraditi celokupni mrežni saobraćaj. Isto tako, za veće mreže potrebno je koristiti i brže procesore.
Propusnost firewall-a zavisi od korištene konfiguracije. U slučaju da se koristi procesor brzine 500 MHz s 256MB RAM memorije, firewall ima propusnu moć od 80Mbps.

Prilikom ispitivanja firewall je bio spojen na javnu računarsku mrežu, a iza njega su se nalazile dve zone, interna i DMZ u kojima su postavljeni računari s Linux Debian operacionim sistemom. Testirani uređaj konfigurisan je sa tri Ethernet okruženja: spoljnje - spojeno na javnu mrežu, unutarašnje - spojeno na internu mrežu i DMZ - spojeno na zaštićenu DMZ zonu.

Kako je tokom testiranja simulirano stvarno pregledavanje mogućnosti uređaja, server koji se nalazi iza uređaja, a koji je spojen na DMZ okruženje između ostaloga je imao podignut Web server (Apache 1.3.24), prema kojem je s javne mreže bila uspostavljena statička putanja sa pripadajućom javnom adresom. S druge strane, na unutarašnje zaglavlje spojen je računar koji je predstavljao internu mrežu. Slika br.8.



Slika br.8. – Šematski prikaz Halted Firewall-a

Osim opisane konfiguracije, za omogućavanje konekcije sa spoljnje mreže na DMZ zonu korišteni su i tehnika virtualnih adresa (*VPN*) i *Proxy* ARP koji su u potpunosti podržani od strane IP tabele (eng. *IP Tables*) alata. Prilikom korišćenja tehnike virtualnih adresa svi legalni paketi pristigli na spoljašnjem okruženju , na port 80, preusmeravali su se prema Web serveru na adresi 192.168.200.2.

2.2.2. Prednosti Halted Firewall-a

Osnovna prednost *halted* firewall-a je činjenica da firewall radi na računaru koji je, u pogledu od strane korisnika, „mrtav". Na firewall-u u *halted* stanju nisu pokrenuti nikakvi servisi koji bi mogli poslužiti za neovlašteno dobijanje administratorskih (*root*) ovlaštenja na samom firewall-u.

Firewall, je ceo baziran na Linux operativnom sistemu i realizovan je pomoću standardnih Linux alata za filtriranje paketa (eng. *IP Tables*) koji su standardno uključeni u sve distribucije Linux-a. Programska podrška kojom je firewall realizovan je besplatna i dolazi u sklopu distribucije tako da nju nije potrebno skidati s Interneta. IP tabele (*IP tables*) programski paket se i dalje razvija, dodaju se nove funkcije tako da se očekuje da će mogućnosti firewall-a realizovanog pomoću njega u budućnosti biti veće.

Osim navedenog, velika prednost *halted* firewall-a je i njegova jednostavnost kao i cena. Čak i neiskusniji korisnici mogu vrlo lako i brzo svladati celoukupnu sintaksu *IP tables* programa. Na taj način mogu se kreirati firewall-i koji u potpunosti odgovaraju korisnikovim potrebama. Takođe, *halted* firewall je besplatan i za njegovu instalaciju nije potrebno veliko novčano ulaganje.

2.2.3. Nedostatci Halted Firewall-a

Nedostaci *halted* firewall-a potiču iz same ideje rada firewall-a na računaru koje je u *halted* stanju. Iako na firewall-u za vreme rada nije moguće pokrenuti ni jedan korisnički program ili servis, logiranje događaji na firewall-u nije moguće. Isto tako, administrator ne može pratiti događaje na firewall-u u realnom vremenu i ne postoji mogućnost da se obavesti administrator o neregularnim aktivnostima na firewall-u. Takođe, nije moguća ni udaljena administracija i nadzor.

Administracija firewall-a nije moguća za vreme normalnog rada. Da bi se unele promene u pravila za filtriranje paketa, računar je potrebno ponovo pokrenuti (za vrijeme pokretanja računara firewall je izvan funkcije) i nakon unosa promena, ponovo vratiti u *halted* stanje.

Na firewall-u su za vreme normalnog rada (u *halted* stanju) ugašeni hard diskovi tako da nema mogućnosti privremenog snimanja podataka na prenosivi disk (flash memorija). Ovo može biti veliki problem na mrežama sa velikim saobraćajem jer može doći do zagušenja firewall-a ako u računaru nema dovoljno memorije.
Preporučuje se da se kod realizacije *halted* firewall-a koristi računar s minimalno 256MB RAM memorije (za mreže do 10 računara). Za veće mreže potrebno je koristiti računar sa 512MB RAM memorije ili više.

2.3. Firewall programi za personalne računare (PC)

Sa pogleda korisnika personalnog računara (*PC*) firewall ima zadatak da kontroliše i ograničava pristup računaru sa Interneta ili lokalne mreže. Njegova ideja je da na personalnom računaru mogu pristupiti samo oni kojima se i dopusti da rade samo ono što im dopusti, a da svi ostali budu onemogućeni i da njihovi pokušaji budu zabeleženi.

Kako to funkcioniše? Za razumevanje rada firewall sistema potrebno je objasniti dva naziva, a to su IP adrese i TCP i UDP portovi. Sve što je povezano na Internet ima barem jednu jedinstvenu IP adresu. To može biti adresa nekog računara ili routera preko kojeg je neka lokalna mreža povezana na Internet. Svaki paket koji putuje Internetom u sebi nosi svoju izvornu i svoju krajnju IP adresu, tako se zna od koga i kome je paket poslat.

IP adresa (eng. *Internet Protocol address*) je jedinstveni broj, sličan telefonskom broju, koji koriste računari u međusobnom saobraćaju preko Interneta uz korištenje internet protokola (IP). Ovo dozvoljava računarima dalje sprovođenje informacije u ime pošiljaoca i kasnije primanje tih informacija (kako bi računari znali da je to početna i krajnja destinacija).
Drugi naziv su portovi TCP i UDP.

TCP i UDP port (eng. *Transmission Control Protocol* and *User Datagram Protocol*) je softverski zadati kanal kojim komuniciraju aplikacije putem računarskih mreža. Ovaj kanal na jednoj od strana komunikacije je predstavljen jedinstvenim brojem koji koriste protokoli transportnog sloja OSI modela u cilju razlikovanja (razdvajanja), identifikacije i praćenja komunikacije aplikacija.

Protokoli TCP i UDP navode brojeve portova u svojim zaglavljima kao izvorni i odredišni port. Pri klijent/server komunikaciji izvorišni port predstavlja broj porta koji označava aplikaciju koja inicira komunikaciju, dok odredišni port označava statički broj porta servisa na serveru. Klijenti dinamički biraju broj porta za svaku konverzaciju. Kao i pri određivanju različitih adresnih standarda IANA (eng. *Internet Assigned Numbers Authority*) je organizacija koja je odgovorna i za dodelu standardnih brojeva portova.

Korisnik putem mnogobrojnih programa (http, ftp, chat, ICQ, MSN i mail) koristi razne sadržaje na Internetu. Pitanja i odgovori prenose se u obliku TCP ili UDP paketa. Da bi se razlikovali paketi od različitih programa, svaki program ima svoj „kanal“ port po kojem šalje i prima pakete, pa tako npr. FTP koristi portove 20 i 21, Telnet port 23, HTPP port 80, ICQ portove 1508 i 1509. Na ovaj način korisnik preko firewall sistema (programa) može dozvoliti odnosno, zabraniti saobraćaj sa određenih adresa i ograničiti rad određenih programa dozvoljavajući rad samo na određenim portovima.

Neki od softverskih rešenja Firewall zaštite za personalne računare su:

- ***ZoneAlarm*** je jednostavan za nekog standardnog korisnika. Upozorenja su opisna. Za profesionalne korisnije možda nije idealan, jer se čini veoma jednostavnim. Za početnike, nema boljeg programa. ZoneAlarm je jedini firewall koji osim pokušaja ulaska u neki računar posmatra i programe koji šalju informacije sa nekog određenog računara.

  To je vrlo bitno ako je neki računar zaražen trojanskim konjem. Svaki program će da bude blokiran ako pokuša da se spoji na internet. Onda se može odlučiti da li se veza dozvoljava, da se dozvoli samo jednom ili da se nikad ne dozvoli spajanje tog programa sa Internetom. Kasnije se može predomisliti i promeniti odobrenja. Takođe, ZoneAlarm ima taster koji kada se pritisne, trenutno blokira svu vezu sa Internetom. Jedino bolje rešenje je da se isključi računar.

- ***BlackICE Defender;*** najveći razlog zbog kojeg je na ceni ovaj firwall je da ne samo da blokira napade, nego ih pamti i otkriva informacije o napadaču. Većina programa se oslanja na informacije koje se lako mogu otkriti, ali baš i nisu korisne. *BlackICE* pokušava (i vrlo često uspeva) da otkrije IP adresu napadača. Nakon toga ima opciju da pošalje te informacije internet servisu napadača. Posle toga često usledi isključenje korisnika. Loša osobina BlackICE-a jeste da ga je se teško rešiti ako ga neko više ne želi koristiti.

- ***Norton Personal Firewall*** - Razni stepeni sigurnosti i sigurnosna pravila koja se mogu menajti su glavne karakteristike ovog programa. Zaštita privatnosti, koja ne dolazi sa nekim drugim programima koji se spominju, je vrlo dobra funkcija koju ne treba zanemariti. Na primer, mogu se uneti ime, prezime, adresa ili broj telefona, i slanje tih informacija putem Internet aplikacija će biti sprečene (ali ne i e-mail).

- **Sygate Personal Firewall** ima mogućnost "zatvaranja" portova, ako programi koji obično koriste izlaze nisu aktivni. Takođe ima i mogućnost postavljanja različitog stepena sigurnosti za različito doba dana. Tako se može podesiti, da kad se ne želi isključiti računar, može se postaviti veća sigurnost kada korisnik nije u blizini računara. Slično kao *BlackICE Defender*, i ovo softversko rešenje firewall zaštite za personalne računare ima mogućnost otkrivanja uljeza kao i tehnike koju su koristili pri pokušaju ulaska u neki računar.

- **Tiny Personal Firewall** (slob. prev. „maleni“/ „sitni"), ovaj firewall ide ruku-pod-ruku sa ostalima na tržištu. Koristi manje resursa nekog računara nego ostali programi. Njegov nedostatak je da nije razumljiv početnicima. Upozorenja su veoma složena, te ga čak ni napredni korisnici ne mogu razumeti. Takođe ima mogućnost "udaljene" administracije, tako da kompanije mogu imati centralizovan pristup svakom računaru u mreži i menjati nivo zaštite za svakog korisnika ponaosob.

Takođe, postoji i veliki broj drugih programa koji se koriste za firewall programe, kao i antivirusnih programa koji u sebi sadrže firewall zaštitu, ali ih u ovom radu neću ni spominjati niti ih posebno objašnjavati.

3. Zlonamerni programi i kompjutersi virusi – uopšteno

U današnje vreme gotovo da nema grane ljudskog delovanja koja ne uključuje neki nivo korištenja računara. Korisnici su stručnjaci, preduzeća i pojedinci. Internetom se razmenjuju jako velike količine podataka. U takvom okruženju retki su sistemi koji se ne sretnu sa nekim oblikom malicioznog softvera.

Razlozi stvaranja takvog softvera mogu biti različiti, ali u današnje vreme nisu više toliko ni bitni. Činjenica je da sa razvojem tehnologije i otkrivanjem novih znanja rastu i mogućnosti autora malicioznog softvera. Moralne i etičke rasprave o zlonamernom softveru prepuštaju se nekim drugim strukama, ali na računarskim naukama ostaje zadatak zaštiti korisnike od takvog softvera.

Kada se govori o malicioznom softveru i borbi protiv njega, ne može se govoriti o samo jednom posebnom području računarstva. Obe strane se koriste celom paletom tehnika kako bi postigle svoj cilj. Najveći problem u borbi protiv takvog softvera je što su obično autori malicioznog softvera korak ispred naučnika koji se bave odbranom od takvih programa.

Često maliciozan program mora nastati kako bi nastala uspešna odbrambena metoda protiv njega. Naravno sve više se koriste tehnike koje pokušavaju predvideti sledeće poteze autora malicioznog softvera.
Kako bi bilo moguće stvoriti uspešnu obranu, potrebno je proučiti metode napada, ciljane objekte, mogućnosti sprečavanja delovanja i mogućnosti oporavka nakon delovanja takvog softvera.

Informatičkim početnicima je gotovo nemoguće objasniti šta je to virus. Onda se još neko setio, pa je i nekim podvrstama virusa dao drugačija imena, samo u svrhu zbunjivanja ljudi. Međutim, davanjem drugačijih imena određenim vrstama virusa, za malo naprednije informatičare bitno olakšava snalaženje i borbu protiv virusa.

Kompjuterski virusi se zovu virusi jer se nekome nekada činilo da je to pojam koji će neiskusnim korisnicima najlakše predočiti kako se oni šire i kakve su njihove posledice. Oni pravi virusi se ne vide golim okom, a kompjuterski još manje. Ukratko, kompjuterski virus je neka vrsta programa koji se na neki automatizovani način širi po računarima i radi neku štetu na tim računarima.

3.1. Istorija kompjuterskih virusa

Šezdesetih i sedamdesetih godina, još u vreme velikih mainframe računara, postojao je fenomen zvani zec (rabbit). Zec je najčešće nastajao slučajem ili greškom kada je "pomahnitali" kompjuterski program počeo sam sebe kopira po sistemu, izazivajući usporenje ili pad sistema. No nisu svi "zečevi" nastali slučajno. Prvi pravi predak današnjih virusa – Prevading animal (prožimajuća zver) bio je program sposoban da se nadodaje na druge kompjuterske programe na UNIVAC 1108 kompjuterskom sistemu.

Prvi potvrđen nalaz kompjuterskog virusa daleke 1981. godine bio je Elk Cloner – virus koji je inficirao BOOT sektor disketa za legendarni Apple II kompjuter. U novembru 1983. Leonard Adleman prvi put u istoriji upotrebio reč "virus" opisujući samokopirajući kod.

Prelomna je i 1986. godina kada se pojavljuje kopjuterski virus Brain (mozak). Ovaj virus, sposoban inficirati BOOT sektore 360 KB disketa IBM PC kompjutera brzo je osvojio svet. Na svu sreću, virus nije bio destruktivan, nego je u sebi samo nosio podatke o autorima. Nakon toga stvari kreću brže. Pojavljuje se kompjuterski virus Jerusalem (1988.) koji je brisao sve pokrenute programe, te prvi pravi destruktivac virus Datacrime (1989.) koji je bio sposoban izvršiti low-level format nulte staze na disku.

Godine 1989. aktivirana je industrija virusa u Bugarskoj. Izvesna osoba (ili skupina) koja sebe naziva Dark Avenger (Crni osvetnik) do danas je napisala najmanje 50-tak virusa uključujući neke od najpoznatijih kao što su New Zeland i Michelangelo.

Matematičar Federik Kohen (Frederick B. Cohen) se smatra „ocem" računarskih virusa. On je 1984. godine prvi uveo naziv *virus* na preporuku svog mentora, profesora Leonarda Adlemana koji je ime izabrao iz romana naučne fantastike.

Kohen je stvorio formalni model računarskog virusa. Za to se koristio Turingovom mašinom[2]. Njegov model vrlo je sličan Von Neumannovom modelu samoreplicirajućeg automata sa ćelijama. Model nije od neke praktične pomoći u smislu proučavanja i odbrane od stvarnih virusa, nego služi za pružanje formalne definicije i davanja teoretske osnove za ovaj rastući problem.

Kohen je dao i neformalnu definiciju računarskog virusa, koja se ne može shvaćati u najdoslovnijem smislu. Današnji virusi koriste razne taktike i metode napada, koje je teško obuhvatiti. Kohenova definicija glasi:
„Virus je program sposoban inficirati druge programe tako da ih modifikuje na način da sadrže eventualno evoluciranu kopiju tog virusa."

Ova definicija daje grubu sliku što računarski virus predstavlja, ali ne može se primeniti doslovno. Razlog tome može se naći u jednostavnom primeru *companion* (pratioc) virusa koji se ne modifikuju kod fajlova domaćina. Umesto toga oni iskorištavaju karakteristike okruženja u kojem napadnuti program radi, npr. operativnog sistema, na način da se postavljaju u putanju izvršavanja ispred legitimnih programa.

Striktno držanje za Cohenovu definiciju predstavljalo bi problem za antivirusne alate koji se oslanjaju na sprečavanje malicioznog ponašanja (*behavior-blocking*). *Companion* virusi ne menjaju strukturu fajlova domaćina i ne bi bili prepoznati kao pretnja.

[2] Turingova mašina je matematički model izumljen od strane britanskog matematičara Alana Turinga za stvaranje klase od predvidljivih funkcija. Turingova mašina modifikuje unos na traci po jednom datom programu. Ako je preračunavanje završeno, onda se rešenje nađe na traci. Tako se svakoj ulaznoj vrijednosti dodijeljuje izlazna. Turingova mašina ne mora za sve ulazne vrednosti da staje. U tom slučaju je funkcija unosa nedefinisana.

Kohen se u istraživanju odbrane od virusa oslanjao na proveru integriteta (*integrity-checking*) programa na računaru. Ta metoda se oslanja na bazu podataka koja sadrži podatke o „zdravom" stanju svakog programa koje se zabeleži u nekom inicijalnom trenutku koji smatramo sigurnim. Takva metoda takođe nije otporna na *companion* viruse s obzirom da oni ne menjaju integritet fajlova. Zbog toga se svaki program koji se pojavi na računaru, a nije u bazi podataka mora proveriti nekom drugom metodom.

Uzevši u obzir da nije bitno kako se virus kopira i nije nužno da postoji zaražena datoteka domaćin, može se postaviti nešto opštija definicija. Ali takva definicija i dalje obuhvata i neke druge programe osim virusa i ne može se smatrati apsolutnim pokazateljem za prepoznavanje virusa. Opštija definicija glasi:
„Računarski virus je program koji rekurzivno i eksplicitno kopira eventualno evoluirane kopije sebe samog."

Računarski virusi su samoupravljani programi koji se bez znanja korisnika kopiraju i šire na nova odredišta. Bitna je samo sposobnost da sami izvrše to kopiranje bez pomoći korisnika. Programi koji zahtevaju korisnikovu akciju (kopiranje, unošenje u memoriju, promenu koda datoteka…) ne mogu se smatrati računarskim virusima. Uprkos tome postoje programi koji pitaju korisnika želi li da se izvrše. Takvi programi jesu virusi zbog sposobnosti da sami sebe rekurzivno kopiraju [1].

3.2. Podela malicioznih programa

3.2.1. Virusi

Kao što je pre opisano, računarski virusi su maliciozni programi koji se rekurzivno kopiraju i šire se računarskim sistemima umetanjem kopija vlastitog koda u druge datoteke i ostale delove sistema. Ponašaju se slično virusima iz prirode koji inficiraju žive stanice. Kopiranje vlastitog malicioznog programskog koda u drugu datoteku naziva se „infekcija" (*infection*), a napadnuta datoteka „domaćin" (*host*).

Naziv „virus" često se koristi za sve vrste malware programa. Virusi koji su pušteni u opticaj tj. koji se neželjeno šire računarskim sistemima, nazivaju se virusi „u divljini" (*in the wild*), dok se virusi čuvani u kontrolisanim laboratorijskim uslovima radi istraživanja nazivaju „zoo-virusi".
Program koji se smatra prvim *in the wild* virusom na mikroračunarima je „*Elk Cloner*". Napisao ga je student Ričard Skrenta (Richard "Rich" Skrenta) 1982. godine, za računar *Apple II*, misleći da neće raditi. *Elk Cloner* je ispisivao pesmicu autora nakon svakih pedeset pristupa zaraženom disku kada je pritisnut reset.[1]

3.2.2. Crvi

Računarski crvi (eng. *worms*) su maliciozni samoreplicirajući programi koji se šire putem računarske mreže. Za razliku od virusa oni su najčešće zasebni programi i ne inficiraju datoteke domaćine, iako postoje i takvi slučajevi. Crvi koriste mrežu kako bi se raširili na udaljeni računarski sistem, najčešće koristeći propuste u dizajnu prenosa podataka, bez znanja i interakcije korisnika sistema. Dok teret (*payload*) može imati razne učinke, glavna karakteristika je da crvi zagušuju mrežu i smanjuju propusnost, za razliku od virusa koji narušavaju integritet napadnutih (inficiranih) datoteka.

Naziv crv (*worm*) nastao je prema romanu naučne fantastike *The Shockwave Rider* autora Džona Brunera (John Kilian Houston Brunner). Prvi put je upotrebljen u članku istraživača Johna F. Shocha i Johna A. Huppa, koji su uočili sličnost sa programima na kojima su radili, 1982.godine.
Prvi primer računarskog crva napravili su upravo dva navedena istraživača. Cilj je bio pronalazak neaktivnih procesora na mreži i ujednačavanja tereta, time poboljšavajući iskorištenost procesora (*CPU cycle use efficiency*). Ovaj program je bio ograničen tako da se nije mogao širiti izvan željenih granica i nije bio opasan.

Mailer i *mass-mailer* crvi su posebna kategorija računarskih crva koji koriste slanje e-mail poruka sa malicioznim programom kada primatelj jedne takve poruke pokrene maliciozni program. Razlika između *mailer* i *mass-mailer* crva je frekvencija kojom šalju e-mail poruke sa uključenom kopijom samog sebe. Primeri su slanje e-mail poruka svim adresama sačuvanim u e-mail klijentima na računaru, slanje pri svakom korisnikovom slanju e-mail poruke itd.
Hobotnica (eng. *octopus*) je sofisticiran oblik računarskog crva koji se sastoji od skupa programa raspoređenih na više računara. Tako se, na primer glava i krakovi *hobotnice* nalaze na udaljenim računarima i saraduju u izvršenju željene maliciozne funkcije. Ideja za ovakvu vrstu malicioznih programa potiče iz navedenog romana *The Shockwave Rider*. Iako nisu učestali, ovakvi crvi će se verovatno sve više pojavljivati u budućnosti, sa porastom kompleksnosti *malware*-a.

Zec (eng. *rabbit*) je kategorija crva koji održava samo jednu kopiju samog sebe koja „skače" sa računara na računar putem mreže. Druga upotreba ovog naziva je za programe koji se rekurzivno pokreću, ispunjavajući memoriju svojim kopijama. U sistemima na kojima rade i druge aplikacije koje nisu spremne na nedostatak memorije mogu uzrokovati znatnu štetu [1].

3.2.3. Trojanski konji

Jedan od najjednostavnijih oblika malicioznih programa su trojanski konji (eng. *trojan horses*). To su programi koji sadrže korisnu funkcionalnost, ili se barem takvima čine, te pokušavaju na taj način privući

korisnika da ih pokrenu i time omoguće izvršavanje malicioznog tereta (*payload*). U ostalim slučajevima, hakeri ostavljaju „trojanizirane" verzije originalnih alata na računaru kako bi im omogućio pristup i kontrolu nad zaraženim računarom. Postoje dve vrste trojanskih konja, oni koji su stopostotni trojanski programi i oni koji su modifikovani postojeći programi.

Jedan od najpoznatijih trojanskih konja je *AIDS TROJAN DISK* koji je poslan na disketi preko 7000 istraživačkih organizacija. Jednom pokrenut, trojanac bi izmešao imena datoteka i ispunio sav prazan prostor na disku. Autor virusa je nudio obnavljanje podataka za novčanu naknadu, ali uskoro je uhapšen.

Zadnji ulaz (eng. *backdoor*) je alat kojim se koriste zlonamerni hakeri kako bi dobili pristup udaljenom računaru. Ti alati se najčešće nalaze unutar funkcionalnosti trojanskog konja. Pri korisnikovom pokretanju trojanskog konja, otvara se mrežni pristup (TCP/UDP) na kojem *backdoor* čeka instrukcije napadača. Drugi oblik *backdoor* pristupa je greška u dizajnu programa ili operativnog sistema koji omogućava neželjeni pristup. Primer je rana implementacija SMTP protokola koja je omogućavala izvršavanje naredbi.

Kradljivci lozinki (eng. *password-stealing trojans*) su klasa trojanskih konja koji pamte korisnikove lozinke i šalju ih napadaču. Ova funkcionalnost je često u kombinaciji sa *keylogger* funkcijom koja pamti pritiske na tastaturu, npr. kod provere pristupa računaru (*logon*) [1].

3.2.4. Logičke bombe

Logičke bombe (eng. *logic bombs*) su delovi koda unešeni u inače legalan softver, koje izvršavaju maliciozni teret (*payload*) pri ispunjenju određenih uslova. Može se raditi o programu koji sam sebe izbriše nakon što istekne rok za korištenje, ali može se raditi i o puno opasnijim teretima. Uslovi koji iniciraju izvršavanje malicioznog koda mogu biti različiti, poput određenog datuma ili korištenja određenih reči u radu sa alatom koji sadrži logičku bombu.

Logičke bombe su slične „uskršnjim jajima" (*Easter eggs*) koja predstavljaju skrivene poruke autora softvera, ili dela softvera koji žele „ostaviti svoj trag" u softveru. Takve poruke često se teško otkrivaju, i nisu opasne. Logičke bombe se najčešće pojavljuju u velikim projektima čiji se kod retko ili nedovoljno proveravaju.
Primer logičke bombe je softver koji je stvorio zaposleni radnik *General Dynamics*-a 1992. godine koji je trebao izbrisati neke bitne podatke. Cilj je navodno bio da se navedeni radnik ponovo zaposli kao visoko plaćeni savetnik i reši stvoreni problem. Njegov kolega naišao je na logičku bombu pre nego što je pokrenuta i sprečio štetu. Krivac je uhapšen i optužen [1][7].

3.2.5. Klice

Klice (eng. *germs*) su prva generacija virusa koji nastaju nakon kompajliranja koda virusa. Oni nisu u obliku u kojem se šire i nisu dodeljeni datoteci domaćinu. Njihovim pokretanjem nastaje druga generacija virusa čiji je kod (najčešće) umetnut u druge datoteke domaćina. Klice polimorfnih i kriptovanih virusa obično nisu kriptovane nego su u jasnom obliku.

3.2.6. Iskorištavanje ranjivosti

Iskorištavanje ranjivosti (eng. *exploits*) je oznaka za programski kod specifičan za jednu ili skup ranjivosti određenog sistema. Cilj je iskorištavanje te ranjivosti i pokretanje programa na udaljenom računaru ili postizanje nekog drugog privilegovanog prava pristupa. Iako postoje maliciozni *exploit* kodovi, neki služe i za testiranje sigurnosti tj. mogućnosti probijanja sistema. Opasnost ovakvih programa zavisi o nameri napadača.

3.2.7. Downloaderi

Downloaderi su oblik zlonamernih programa koji pri pokretanju kopira druge maliciozne programe s interneta i pokreće ih, čime dolazi do infekcije računara na kojem je taj program pokrenut.

3.2.8. Daileri

Daileri su maliciozni programi koji su vrhunac doživili kada je većina ljudi koristila *dial-up* pristup internetu. Ovi programi bi koristili modem računara kako bi obavljali pozive na telefonske brojeve sa skupim tarifama i time zarađivali novac na štetu i bez znanja korisnika.

3.2.9. Dropperi

Dropperi su poput klica (*germs*) prva generacija virusa koja služi kao instalacioni program za programski kod virusa. Primeri korištenja su virusi početnog sektora (*boot sector virus*) koji inficiraju sektore za punjenje (*boot sector*) diskova. Oni koriste *droppere* (koji su obični programi sačuvani na disku) kako bi se prvi put upisali u *boot* sektor nekog diska i time pokrenuli svoje širenje.
Injectori su oblik *droppera* koji instališu kod virusa u memoriju. Nakon toga se virus širi uobičajnim načinima. Postoje i mrežni *injectori* koji koriste mrežu kako bi instalisali virus u memoriju udaljenog računara.

3.2.10. Generatori virusa

Autori *malware-a* stvorili su veliki broj programa koji automatski generišu viruse sa željenim karakteristikama. Ti alati su jednostavni za korištenje što je uzrokovalo da i početnici mogu stvoriti maliciozan softver korištenjem jednostavnih menija takvih alata.Iako veliki broj tako generisanih virusa ne postignu željenu destruktivnu nameru, postoje i primeri vrlo opasnih generisanih virusa poput *Anna Kournikova* virusa kojeg je stvorio holandski tinejdžer Jan de Wit.

3.2.11. Keyloggeri

Keyloggeri su maliciozni programi koji zapisuju pritiske na tastaturu pokušavajući time pronaći lične podatke i lozinke korisnika, te ih poslati napadaču. Ti podaci se mogu dalje koristiti za krađu, neovlašteni pristup, itd.

3.2.12. Rootkits

Rootkits je opšti naziv za skup programa koji omogućavaju tzv. „root" pristup računaru tj. pristup sa najvišim ovlašćenjima. Najčešće hakeri koriste *exploit-e* kako bi instalisali takve programe na napadnuti računar, poput *trojaniziranih* verzija uobičajnih programa, što im kasnije omogućava neovlašten upad na računar. Sofisticiranije verzije *rootkit* programa imaju i elemente koji rade u jezgrovom načinu rada što ih čini posebno opasnima s obzirom da mogu menjati ponašanje jezgra (kernela) operativnog sistema i time se kamuflirati. Za razliku od toga *rootkit* programi koji rade u korisničkom načinu rada (*user-mode rootkits*) lakše se otkrivaju sistemima odbrane koji rade u jezgrovitom načinu rada (*kernel mode)* [3].

3.2.13. Spywares

Spywares su programi koji prate rad računara i o tome obaveštavaju napadača. Postoje programi koje se namerno instališu po većim firmama, kako bi rukovodioci imali uvid u to šta se radi na njihovim računarima. Međutim, većina ovih programa služe da šalju podatke koji se pretražuju po internetu i šalju se napadačima kako bi napadač mogao doći do nekih informacija, kao i ličnih podataka.

3.3. Kako se šire virusi

U početku su se virusi širili preko disketa. Ljudi su se koristili disketama da bi izmenjivali datoteke (programe, tekstove, tabele, slike, ...). Kada se disketa ubaci u nečiji računar sa zaraženim programima i kada se pokrene, virus sam sebe kopira sa diskete na računar, a posle i na ostale diskete ubačene u računar. Te zaražene diskete dospevaju u drugi računar i tako se prenosi virus.

Kasnije su CD-ovi (Compact Disc) preuzeli ulogu disketa kao prenosioca podataka. Takođe, paralelan prenosnik CD-ima postao je i Internet. Internet je dosta pomogao brzini razmnožavanja virusa, jer se sa jednog kraja planete može poslati virus na drugi kraj planete za samo par sekundi. Međutim, popularnost Interneta je linearno rasla, tako da je na kraju Internet postao glavni „krivac“ za širenje virusa.
Na primer, kada neko sa zaraženog računara pošalje e-mali drugom računaru, virus se „naseli“ (bez korisnikovog znanja) u poruku i zajedno sa njom se prenese na sledeći računar. Naravno, sa računara primaoca, virus se širi na ostale računare. Virusi su toliko „napredovali“ i postali „pametniji“ da mogu sami sastaviti neku poruku i poslati nekom od korisnikovih prijatelja iz liste imenika. Obzirom, da se većina današnjih virusa širi na prethodno opisan način, često je od velike važnosti znati nešto više detalja o pristigloj poruci.

Ako poruka sadrži *exe* datoteku (fajl) ili datoteku sa dve ekstenije (npr. src.exe), velike su šanse da se radi o nekoj vrsti virusa. Ukoliko je poruka stigla od nepoznatog pošiljaoca, pa se u predmetu poruke (*body*) ne nalazi nikakav tekst, poruka je takođe potencijalno opasna. Čak, i ako poruka stiže sa poznate adrese, ne mora značiti da je bezbedna; današnji virusi su u stanju krivotvoriti zaglavlje (*header*) poruke ili se automatski poslati bez znanja vlasnika računara.

Malware programi mogu dospeti u operativni sistem na nekoliko načina od kojih su najčešće sledeći:

- Putem e-mail attachment-a,
- Kopiranjem zaraženog programa sa mobilnog medija, preko LAN mreže ili preuzimanjem sa Interneta putem FTP, HTTP, nekog od P2P protokola,
- Putem malicioznih ActiveX, Java i Javascript programa,
- Iskorištavanjem sigurnosnog propusta u sistemu (koristeći explorer), a to je put kojim se šire crvi (worms). Serverski program na napadnutom sistemom predstavlja prolaz i
- Preko multimedijalnih fajlova koji u sebi sadrže takav niz podataka, da iskorištavaju propuste u klijentskim aplikacijama sistema. Takav slučaj je i jedna verzija biblioteke *gdiplus.dll*, dela operativnog sistema Windows XP u nekoj od ranijih verzija.

Maliciozni ActiveX, Java i Javascript programi se uglavnom automatski izvršavaju posle uspešnog implementiranja u sistem, što nije slučaj sa virusima i trojancima koje korisnik treba sam pokrenuti, posle čega oni koriste jedan od načina za automatsko pokretanje pri dizanju sistema.

Pri korištenju web-a treba biti posebno pažljiv sa određenim tipovima sajtova, a najopasniji su sajtovi koji sadrže “crack” programe, jer se pokazalo da u relativno velikom broju slučajeva programi za krekovanje drugih programa u sebi sadrže i maliciozni kod, ako ne i isključivo maliciozni kod. U slučaju da se koriste sajtovi koji izvršavaju kod na klijentu, veoma je poželjno imati uključen rezidentni antivirusni skener, ali ni u njega se ne treba pouzdati previše.

Pri čitanju e-mail poruka, postoji relativno mala mogućnost da samim pozicioniranjem pointera na poruku ili skidanjem (download) e-mail poruke, e-mail klijent automatski pokrene maliciozni program, ali takvu mogućnost ne treba potpuno odbaciti, jer sigurnosni propusti u e-mail klijentima omogućavaju i to. E-mail attachment-e nikako ne treba pokretati ukoliko nismo sigurni da je to sigurno ono što je trebalo primiti.

3.3.1. Zaštita od zlonamernih programa (malware)

Zaštita od malware programa je jedna velika grana računarske industrije, a svakako jedna od najznačajnijih. U poslednje vreme zaista nije lako zaštiti sistem, a naročito Windows operativni sistem. Da bi se korisnik uspešno zaštitio od malicioznih programa potreban je određen nivo znanja i discipline u korišćenju računara.

Borba protiv malware programa se vodi na nekoliko polja. Veoma je bitno da korisnik bude svestan bar većine načina na koje malware programi mogu zaraziti računar i da postigne nivo discipline kako bi uspešno primenio to znanje.

Na osnovu raspoložive literature poznati su sledeći tipovi zaštite:

1.Anti-virusni programi,
2. Anti-spyware programi,
3. Firewall sistemi i
4. E-mail klijenti i serveri naprednih karakteristika sa prepoznavanjem virusa i SPAM-ova.

Granica između Antivirusnih programa i Antispyware programa sve više se briše, pa se i sve više pojavljuju programi koji kombinuju ove dve vrste zaštite

4. Mrežni napadi i pretnje nove generacije (Botnet)

Botnet mreža sastoji se od niza povezanih računara, koja međusobno sarađuju i kojima upravlja jedan haker(ili manja grupa njih), poznat pod nazivom *botmaster*. Bot je krajnji računar (ili server), koji je član botnet mreže. Isto tako, taj se naziv koristi i za zlonamerno oblikovane izvršne datoteke koje služe za dobijanje kontrole nad računarom i njegovo uključivanje u botnet mrežu.

Prva pojava takve mreže zabeležena je 1999. godine, a bila je povezana s primenom crva PrettyPark . Ta je mreža omogućavala spajanje na udaljeni IRC (eng. Internet Relay Chat) server, sticanje osnovnih informacija o sistemu (kao što je verzija operativnog sistema), korisničkim imenima, e-mail adresama, nadimcima i sl. Iako je imao tako ograničen skup mogućnosti, PrettyPark crv nije bio toliko štetan za Internet mrežu poput njegovih sledbenika. Glavna inovacija ovog crva u odnosu na sve prethodne je mogućnost udaljenog upravljanja velikim brojem kompromitiranih računara.
Njegova revolucionarna ideja iskorištavanja IRC servera kao diskretne i fleksibilne metode upravljanja (eng. Command and Control , C&C), uskoro je postala vrlo raširena te s godinama poboljšana i usavršena. Neki od najpoznatijih botova bili su AgoBot i SDBot. Njihovom pojavom, povećavaju se mogućnosti koje pružaju njihovi prethodnici te se integrišu s novim metodama napada. Takva nova vrsta botova postaje snažan alat za izgradnju računarske "vojske", koja može nametnuti ogromne pretnje Internet mreži danas.

4.1. Botnet mreže – nekad

Sami počeci zlonamernog korištenja botnet mreža potiču od 2000. godine. Tada je računarski entuzijasta, poznat pod imenom Mafia-boy, iskoristio prvu sličnu mrežu zaraženih računara da izvede distribuirani napad uskraćivanjem usluga (eng. *Distributed Denial-of-Service*, DDoS). Napad je izveden na internetske stranice firmi CNN, Amazon eBay i Dell. Distribuirani napad uskraćivanjem usluga se radi na način da svaki računar kojim napadač upravlja pošalje zahtev na određenu stranicu odnosno server. Veliki broj takvih zahteva poslanih odjednom može preopteretiti server i onemogućiti drugim korisnicima usluge koje on nudi. Kako firme sve više zavise o uslugama koje pružaju korisnicima preko Interneta, nedostupnost njihovih servera može im naneti značajne financijske gubitke.

4.2. Botnet – danas

Danas je puno veća verovatnoća da iza neke botnet mreže stoji kriminalna organizacija, a ne grupa računarskih entuzijasta. Glavni razlog tome je razlika u motivaciji, dok su pre 2000. godine Botnet mrežama upravljali entuzijasti željni slave pa ih koristili za međusobno „ratovanje“ i nadmetanje. Danas je glavna motivacija profit. Botnet mreže se danas najčešće koriste za pet vrsta napada, a to su:

- Napad uskraćivanjem usluga (Dos napad),
- Distribuirani napad uskraćivanjem usluga (DDoS napad),
- Slanje velikih količina neželjene elektronske pošte (eng. *SPAM*),
- Pokušaj krađe identiteta i privatnih korisničkih podataka (eng. *phishing*) i
- prevare klikom (eng. *Click fraud*).

4.2.1. Napad uskraćivanjem usluga (DoS)

Napad uskraćivanjem usluge (eng. *Denial-of-Service attack*, u daljnjem tekstu DoS) je napad na neki računar u kojem napadač želi resurse ili servise tog računara učiniti nedostupnim za njihove korisnike. Iako se motivi, načini i ciljane mete ovakvih napada menjaju, svima im je zajedničko želja da se pristup uslugama onemogući na kraće ili duže vreme. Svaki DoS napad ima tri uključene strane. To su:

- *Napadač* – osoba koja provodi napad. On želi oštetiti neki ciljani računar na Internetu,
- *Žrtva* – računar koji trpi napad. Rezultat napada je nemogućnost žrtve da isporuči uslugu svojim korisnicima i
- *Korisnici* – Sve osobe koje na legalan način koriste usluge žrtve. Za vrijeme DoS napada njima je pristup željenim uslugama onemogućen.

Važno je zapamtiti da DoS napadi ne omogućavaju napadaču neovlašteni pristup žrtvi ili krađu njegovih podataka. Ukoliko napadač uspešno provede DoS napad i on sam neće moći pristupiti resursima žrtve kao i svi ostali korisnici.

Termin DoS napad najčešće se pojavljuje u kontekstu računarskih mreža i mrežnih tehnologija s tim da se takvi napadi najčešće provode putem njih. Međutim, DoS napadi nisu ograničeni samo na računarske mreže. DoS napad moguće je provesti iskorištavanjem neke sigurnosne ranjivosti u softveru na ciljanom računaru. Npr. napadač može namerno srušiti poslužitelja elektronske pošte i time onemogućiti korisnicima da šalju i primaju elektronsku poštu. Provođenje takvih napada moguće je zbog lošeg kvaliteta softvera koji pokazuje brojne ranjivosti. Obrana od ovakvih napada pripada u domenu poboljšanja kvaliteta programskog koda i redovnog ispravljanja otkrivenih ranjivosti.

Osim problema sa softverom, svako fizičko uništavanje infrastrukture takođe je oblik DoS napada. Za uspešno provođenje takvog napada napadač mora imati fizički pristup infrastrukturi. Zaštita od njih spada u domenu kontrole fizičke sigurnosti.

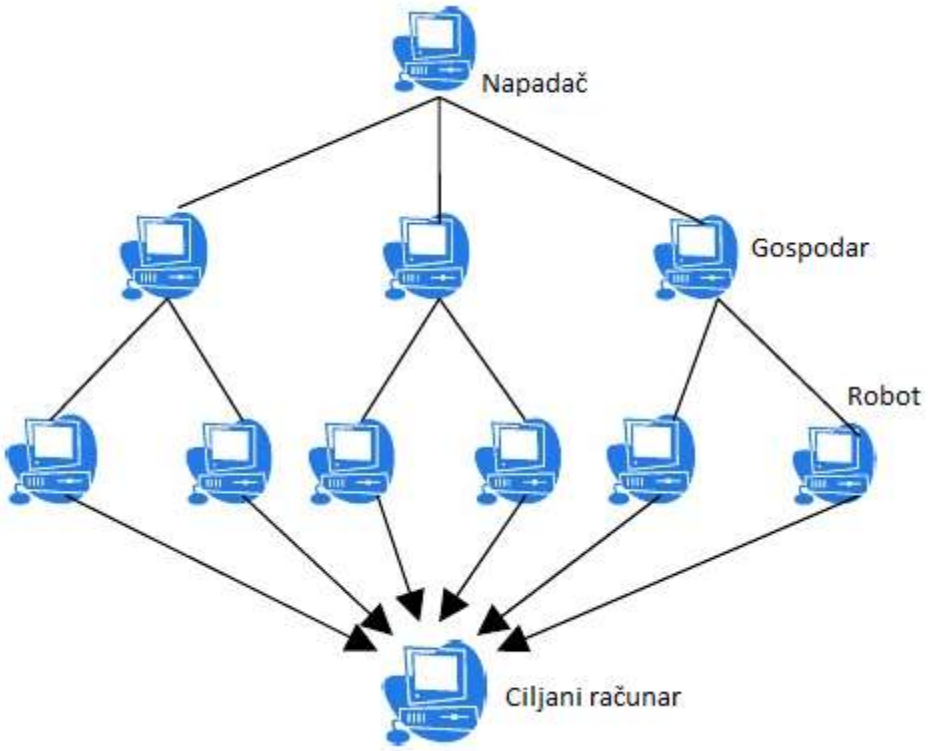
Za razliku od DoS napada putem ranjivosti nekog softvera, DoS napadi koji se odvijaju preko mreže ne ovise o kvalitetu softvera koji žrtva koristi. Bez obzira na kvalitet softvera, DoS napad preko mreže još uvek može u potpunosti uspeti. U poređenju sa fizičkim uništavanjem infrastrukture, za DoS napad putem mreže nije potreban fizički pristup „žrtvi“ i oni ne spadaju u domenu kontrole fizičke sigurnosti.

4.2.2. Distribuirani napad uskraćivanjem usluga (DDoS)

Svaki server ima neku granicu propusnosti podataka, odnosno kapacitet koliko najviše radnji može napraviti u određenoj jedinici vremena. Ako se ta granica pređe, server se može srušiti, odnosno postati nedostupan ili barem prespor za normalno korištenje. U današnje vreme većina preduzeća zavisi o svom „*on-line*“ identitetu, odnosno dostupnosti barem osnovnih informacija o preduzeća na Internetu. Šta više, veliki broj preduzeća obavlja barem deo svojih delatnosti preko Interneta. U današnje vreme, obavlja se i većina financijskih transakcija preko Interneta.

Iz svega navedenog očito je da je danas svakom preduzeću važna dostupnost, odnosno ispravan rad njihovog severa ili servera preduzeća koja za njih drži web stranice ili obavlja financijske usluge. Prilikom distribuiranog napada uskraćivanjem usluga, vlasnik botnet mreže naredi svim računarima koje nadzire, odnosno svim računarima u mreži da pristupe određenoj Internet stranici, usluzi, odnosno serveru u isto vreme. Na taj način, zavisno o broju računara koja nadzire, ozbiljno ugrozi rad tog servera. Financijska motivacija iza ovakve vrste napada najčešće je iznuda novca od napadnute firme za prestanak takvih napada.

Međutim moguć je i scenario u kojem konkurentska firma plati napadačima oštećivanje konkurencije zbog povećanja svog tržišta ili neke vrste odmazde. Šematski prikaz DDoS napada prikazan je na slici br. 9.



Slika 9. – Šematski prikaz DDoS napada

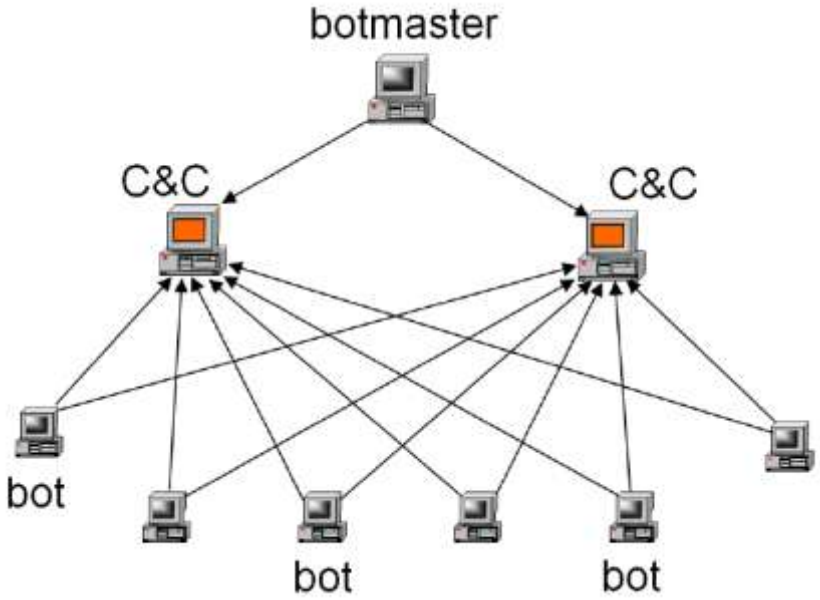
4.3. Arhitektura botnet mreža

Od samih početaka, odnosno genijalne ideje da se za komunikaciju i upravljanje drugim računarima iskoristi protokol za razgovor putem Interneta (eng. *internet relay chat,* IRC), napadači se prvenstveno oslanjaju na tu vrstu komunikacije u botnet mreži. Protokol IRC je razvijen za komunikaciju korisnika na forumima, masovnim ili privatnim porukama, u stvarnom vremenu odnosno bez kašnjenja, stoga je posebno pogodan za izdavanje naredbi većem broju računara u istom trenutku.

Napadač koji želi preuzeti nadzor nad drugim računarima, postavi jedan računar kao IRC server te ga koristi za komunikaciju sa drugim zaraženim odnosno ranjivim računarima. Preko tog servera napadač ustvari upravlja botnet mrežom.

4.3.1. Moderna arhitektura botnet mreža

U današnje vreme vlasnici botnet mreža, poznati i pod engleskim nazivima *botherder* ili *botmaster*, još uvek primarno koriste neku vrstu protokola IM (eng. *instant messaging*) za upravljanje botnet mrežom, odnosno protokola za komunikaciju u stvarnom vremenu. Kako se ti protokoli koriste na većini socijalnih mreža, onemogućavanje tih protokola za zaštitu računara nije primenjivo u većini slučajeva. Takođe se koristi i „klasičan" komunikacioni protokol HTTP (eng. *Hypertext Transfer Protocol*) preko kojeg se odvija većina www (eng. world wide web) prometa na Internetu. Pritom sama arhitektura botnet mreža nije bitno promenjena, međutim ono po čemu se današnje botnet mreže razlikuju od onih prije nekoliko godina jeste redundantnost. Naime, *botmasteri* koriste dva, tri ili više servera za komunikaciju sa celom mrežom zaraženih računara. Arhitektura botnet mreže koja koristi dva komunikaciona servera prikazana je na slici br. 10, a lako se može zamisliti mreža sa više od dva takva servera. Ti serveri poznati su još pod skraćenicom C&C koja dolazi od engleskih reči za naredbe i kontrolu (eng. *command and control*). Više C&C servera se koristi za slučaj da neki budu otkriveni, odnosno, iz bilo kojeg drugog razloga nedostupni. U tom slučaju, bez dodatnih servera, botnet mreža bi i dalje postojala, međutim niko ne bi imao nadzor nad njom te ne bi mogao njom upravljati zbog nemogućnosti podele zadataka zaraženim računarima.



Slika 10. – Arhitektura botnet mreže sa dva upravljačka servera

4.4. Primer botnet napada

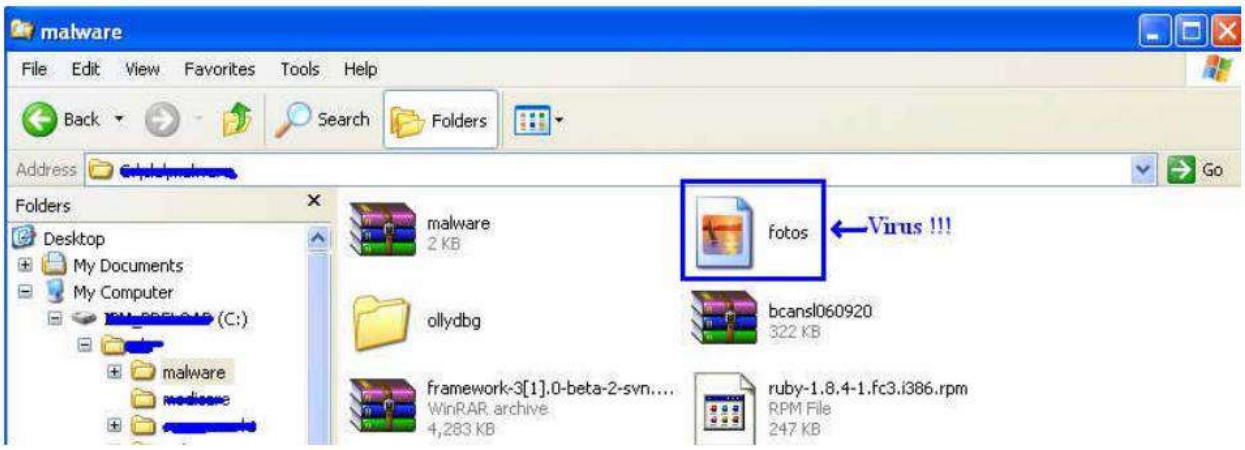
Važno je napomenuti da se vlasnici botnet mreža najčešće ne bave drugim vrstama kriminala, oni samo iznajmljuju računarske resurse zaraženih računara drugim kriminalnim organizacijama. Na taj način izbegavaju kriminalnu odgovornost za ilegalne radnje za koje su botnet mreže iskorišćene.

4.4.1. Stvaranje botnet mreža

Napadač, nakon postavljanja servera za upravljanje botnet mrežom kreće u „regrutaciju“ računara za botnet mrežu. Računari korisnika koji postanu deo botnet mreže najčešće ne sadrže poslednje sigurnosne zakrpe za operativni sistem ili odgovarajući program za zaštitu računara. Postoje dva načina na koji se zlonamerni program, odnosno klijent za botnet mrežu (bot) učitava na takav računar. Prvi od njih zahteva korisničku interakciju, odnosno napad računarskim virusom. Drugi način je napad računarskim crvom koji ne zahteva nikakvu korisničku interakciju, a sposoban je sam sebe dalje širiti.

Zaraza računara virusom

Računarski virus je vrsta zlonamernog programa za računar koji za svoje širenje treba datoteku domaćina, koja treba biti otvorena, da bi se zaraza proširila. Najčešće virusi dolaze kao lažne fotografije, video ili tekstualne datoteke odnosno datoteke programa Microsoft Word, kako je prikazano na slici br. 11. Najčešće se šire socijalnim mrežama ili elektronskom poštom, a koriste senzacionalističko ime ili opis, nešto kao: „ovo je presmešno“, „moraš ovo videti“ i slično.



Slika 11. – Primer zaraženog fajla u obliku lažne slike

Ovakvom načinu zaraze računara dodatno pogoduju podrazumevana podešavanja operativnog sistema Windows, što se tiče sakrivanja troslovnih oznaka poznatih vrsta datoteka. Naime ova datoteka je punim imenom fotos.exe, gde .exe dodatak označava izvršnu datoteku operativnog sistema Windows. Prilikom pokušaja otvaranja te datoteke, korisnik će pokrenuti program fotos.exe koji će otvoriti komunikacione kanale sa upravljačkim serverom botnet mreže. Taj program će tada svoju kopiju poslati svim korisnikovim kontaktima, bilo preko socijalne mreže ili elektronske pošte pa tako dalje širiti zarazu.

Zaraza računara crvom

Računarski crv je vrsta zlonamernog programa koji je sposoban sam širit zarazu, odnosno sposoban je „razmnožavati“ se bez korisnikove interakcije. Najčešće mrežom odnosno Internetom, ali može se kopirati i na spoljne memorije i tako nalaziti nove računare.

Ovo je učestaliji način širenja bot klijenata u poslednje vreme, a nakon uspešne zaraze odnosno instalacije na žrtvin računar, crv proverava mrežu za druge ranjive računare na koje bi se mogao proširiti i instalirati bot klijent.

4.5. Zaštita od botnet napada

4.5.1. Zaštita servera od DDoS napada botnet mreže

Zbog geografske rasprostranjenosti računara u botnet mreži, velike količine zaraženih računara i činjenice da zaraženi računari najčešće imaju promenjivu, odnosno dinamičku IP (eng. Internet protocol) adresu, zaštita servera filtriranjem IP adresa nije primenjiva. Ograničen uspeh može biti postignut analizom specifičnosti operativnih sistema računara koje izvode DDoS napad, te njihovim daljim onemogućavanjem pristupa serveru (eng. Passive OS fingerprinting). Skuplja metoda zaštite je korištenje specijalizovanog NIDS (eng. network based intrusion detection system) sistema.
Većina botnet mreža, odnosno botnet klijenata prima naredbe sa upravljačkog servera koji se nalazi iza stalne adrese. To najčešće nije statička IP adresa nego je server registrovan na nekoj od besplatnih usluga koje omogućavaju tu funkcionalnost, kao što su *DynDns.org*, *No-IP.com*, i *Afraid.org*. Te adrese se mogu lako iščitati iz bot klijenta na zaraženom računaru, pa se mogu poduzeti odgovarajuće mere da se taj botnet server onemogući u daljoj komunikaciji sa zaraženim računarima.

4.5.2. Zaštita ličnih računara od zaraze i ulaska u botnet mrežu

Iako odgovarajuće institucije onemogućavaju botnet upravljački server u daljoj komunikaciji sa zaraženim računarima u botnet mreži, to ne znači da ti računari više nisu zaražena. Lako je moguće da botnet vlasnik na neki način uspe osvežiti bot klijente sa novom adresom botnet upravljačkog servera ili da neki drugi napadač preuzme nadzor nad tim zaraženim računarima, ubacivši u bot klijente adresu svog botnet upravljačkog servera poslužitelja.

Neki od pokazatelja da je računar deo botnet mreže najčešće su povećan Internet promet na priključcima koje botnet vlasnici koriste za komunikaciju sa upravljačkim serverom:

- 445/TCP (eng. *Transmission Control Protocol*) kojeg koristi Microsoft-DS Service,
- 139/TCP (NetBIOS Session Service),
- 137/UDP (eng. *User Datagram Protocol*) kojeg koristi NetBIOS Name Service) i
- 135/TCP (Remote Procedure Call services, RPC).

Takođe, dobar pokazatelj je i povećan promet na priključcima koje klijentski bot program najčešće koristi kako bi se proširio na druge računare:

- 42 – WINS (eng. *Windows Internet Name Service*) kojeg koristi Host Name Server,
- 903 – trojanski konj NetDevil Backdoor,
- 1025 – (eng. Microsoft Remote Procedure Call, RPC),
- 1433 - MS-SQL-S (eng. Microsoft-SQL-Server),
- 2745 - Bagle crv koji se koristi za slanje neželjene pošte (spam),
- 3127 - MyDoom crv koji se koristi za slanje neželjene pošte,
- 3306 - MySQL korisnički definirane funkcije (eng. *User Defined Functions*, UDF),
- 3410 - Optix Backdoor trojanski konj,
- 5000 - UPNP (eng. Universal Plug and Play: MS01-059) i
- 6129 – DameWare.

Metode zaštite su jednake onima od svih zlonamernih programa, a najčešće su:

- korišćenje najsvežijih verzija programa za zaštitu računara,
- redovno instalisanje zakrpa za operativni sistem,
- povremeno proveriti listu o saobraćaju firewall-a,

- povećati sigurnost internet pretraživača onemogućavanjem izvođenja skripta u istom,
- izbegavati otvaranje sumnjivih priloga elektronske pošte i posetu sumnjivim internet stranicama i
- ograničiti prava korisničkog računa koji se koristi za svakodnevnu upotrebu, nema nikakve potrebe da se, pogotovo za pregledavanje sadržaja na internetu, koristi administratorski korisnički račun.

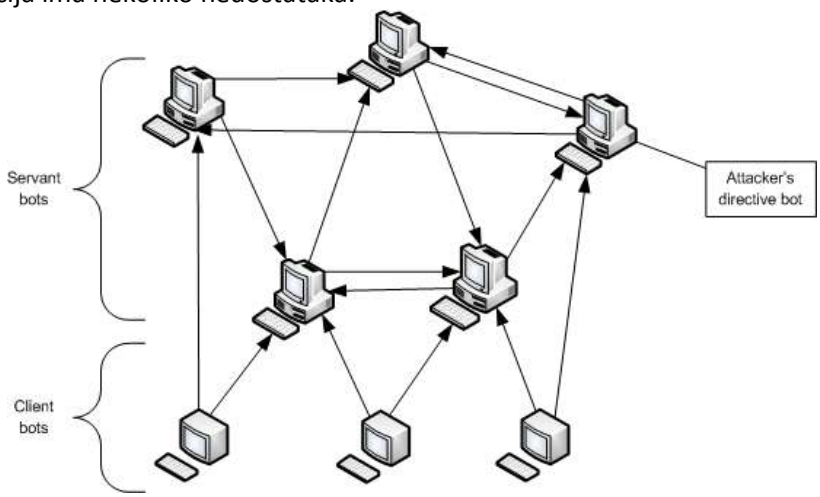
4.6. Budućnost botnet mreža

Jedno od zanimljivih svojstava novijih bot klijenata jeste ugrađeni antivirusni program koji će proveriti da li je na računaru instalisan neki drugi bot klijent, od konkurentskog vlasnika botnet mrežom pa će ga obrisati. Taj program će, popis svih programa učitanih u memoriju poslati na analizu nekoj od stranica koje nude besplatnu proveru na zlonamerne programe.

U poslednje vreme uočeni su i zlonamerni programi koji pretvaraju mobilne uređaje u zombi računare, a jedan takav je "ANDROIDOS_ANSERVER.A.“ Takođe, se za samo komunikaciju u botnet mreže sve više koristi protokol P2P (eng. *peer to peer*).

4.6.1. Prednosti protokola P2P za napadače

Upravo zbog ranjivosti botnet mreže za onemogućavanje upravljačkog servera u komunikaciji sa bot klijentima, u poslednje vreme pojavljuje se sve više botnet mreža koje koriste komunikacioni protokol P2P, kako je prikazano na slici br. 12. Taj protokol omogućava redundantnost u komunikaciji jer je svaki računar povezan sa svim ili barem nekoliko drugih. Tako je vlasniku botnet mreže dovoljno ostvariti komunikaciju sa samo jednim računarom u mreži, a on će najsvežije informacije proslediti ostalima. Na taj način se gubi potreba za klasičnim upravljačkim serverom. Takve mreže su otpornije na pokušaje njihovog uklanjanja, a taj način komunikacija ima nekoliko nedostataka.



Slika 12. – Arhitektura botnet mreže koja koristi P2P komunikacioni protokol

4.6.2. Nedostaci P2P protokola za napadače

Napadi koji zahtevaju visoku stopu koordinacije velikog broja bot računara nisu lako izvodivi sa botnet mrežama koje koriste protokol P2P za komunikaciju. Taj problem se dešava baš zbog nedostatka središnjeg upravljačkog servera koji bi poslao naredbu svim računarima u isto vreme. Još jedan mogući problem se dešava prilikom slanja sveže verzije bot klijenta zaraženim računarima, zbog nedostatka hijerarhije u P2P mrežama, može doći do kolizije između dva računara.

Tačnije oko toga ko od njih ima više ovlašćenja instalirati program na drugi računar, jer u takvoj botnet mreži svaki računar komunicira sa svakim pa svaki računar pokušava ažurirati program na drugima.

5. STUDIJA SLUČAJA: Anti-virusni program Symantec EndPoint Protection – Uopšte

EndPoint Protection Symantec-ov proizvod zaštite koji obuhvata zaštitu od virusa, spamova, trojanaca kao i napada sa mreže.

Symantec EndPoint Protection je proizvod poslednje generacije, koja je istovremeno i budućnost zaštite, koja kao takva zamenjuje specifične proizvode u oblasti zaštite i to:

a. Symantec AntiVirus Corporate Edition,
b. Symantec Client Security,
c. Symantec Sygate Enterprise Protection i
d. Sygate Secure Enterprise.

Primenom ove tehnologije obezbeđuje se napredan vid zaštite od štetnih kodova. Omogućava zaštitu od napada Maleware-a kao što su virusi,crvi,trojanci,spyware-a,adware-a.
Symantec EndPoint Protection menja Symantec AntiVirus Corporate Edition i Symantec Client Security.

Symantec EndPoint Protection sadrži:

a. Antivirus,
b. Anti-Spyware,
c. Firewall,
d. IPS i
e. Device Control.

Symantec EndPoint Protection integriše Symantec AntiVirus sa naprednim tehnikama otkrivanja i eliminisanja pretnji čime se postiže najveći stepen zaštite od zlonamernog softvera za laptop, desktop i serverske računare. U ovo rešenje uključene su proaktivne tehnologije koje automatski analiziraju ponašanje aplikacija i mrežnih komunikacija da bi se otkrile i aktivno blokirale pretnje.
Sadrži i funkcije kontrole uređaja i aplikacija da bi se upravljalo dešavanjima i obezbedili podaci.

Symantec EndPoint Protection savršeno integriše ove bezbednosne funkcionalnosti u jedinstvenom agentu i jedinstvenoj konzoli smanjujući na taj način troškove, kompleksnost i dodatni trud koji iziskuje upravljanje višestrukim bezbednosnim proizvodima.
Pored toga što su funkcionalnosti dodate i unapređene, prostor koji zauzima u memoriji šest puta je manji od onog koji je zauzimao Symantec Client Security [6].

5.1. Koje sve novitete nudi Symantec EndPoint Protection?

Proaktivna zaštita od pretnji:

- Proaktivno skeniranje

Otkrivanje i blokiranje, u realnom vremenu, zlonamernih pretnji za koje još uvek ne postoje potpisi.

- Tehnologija za proaktivno otkrivanje i blokiranje zloupotrebe ranjivosti u operativnom sistemu ili aplikacijama – čak i pre nego što proizvođač uradi popravku.
- Unapređeno otkrivanje i uklanjanje spyware/rootkit pretnji.

Pojednostavljena administracija:

- Jedinstvena konzola

Pomoću jedinstvene konzole, upravlja se svim funkcijama paketa Symantec EndPoint Protection, kao i funkcijama programa Symantec Network Access Control (licencira se zasebno).

- Jedinstveni agent

Jedinstveni agent podržava svih pet tehnologija koje se nalaze u rešenju Symantec EndPoint Protection. Na taj način, pojednostavljuje se upravljanje i smanjuje se opterećenje resursa. Agent podržava i Symantec Network Access Control tako da nema potrebe da se instalira novi agent kada korisnik proširi svoju zaštitu.

Bolje performanse, bolja bezbednost:

- Manje opterećenje računara

Novi, lakši agent programa Symantec EndPoint Protection koristi do 84% manje osnovne memorije u poređenju s prethodnim verzijama Symantec Client Security i Symantec AntiVirus, i troši onoliko klijentskih resursa koliko je potrebno da bi uticaj na performanse bio minimalan.

Kontrola aplikacija i uređaja:

- Kontrola aplikacija – omogućava administratorima da kontrolišu pristup korisnika i drugih aplikacija određenim procesima, datotekama i folderima. Obezbeđuje analizu aplikacija, kontrolu procesa, kontrolu pristupa datotekama i bazi i kontrolu modula i DLL-ova.

- Kontrola uređaja – omogućava administratorima da kontrolišu koji periferni uređaji mogu da se povežu na mašinu i da kontrolišu kako se ti uređaji koriste. Zaključava mašinu da bi se sprečilo povezivanje spoljašnih drajvova, CD rezača, štampača i drugih USB uređaja.

Klijentski firewall:

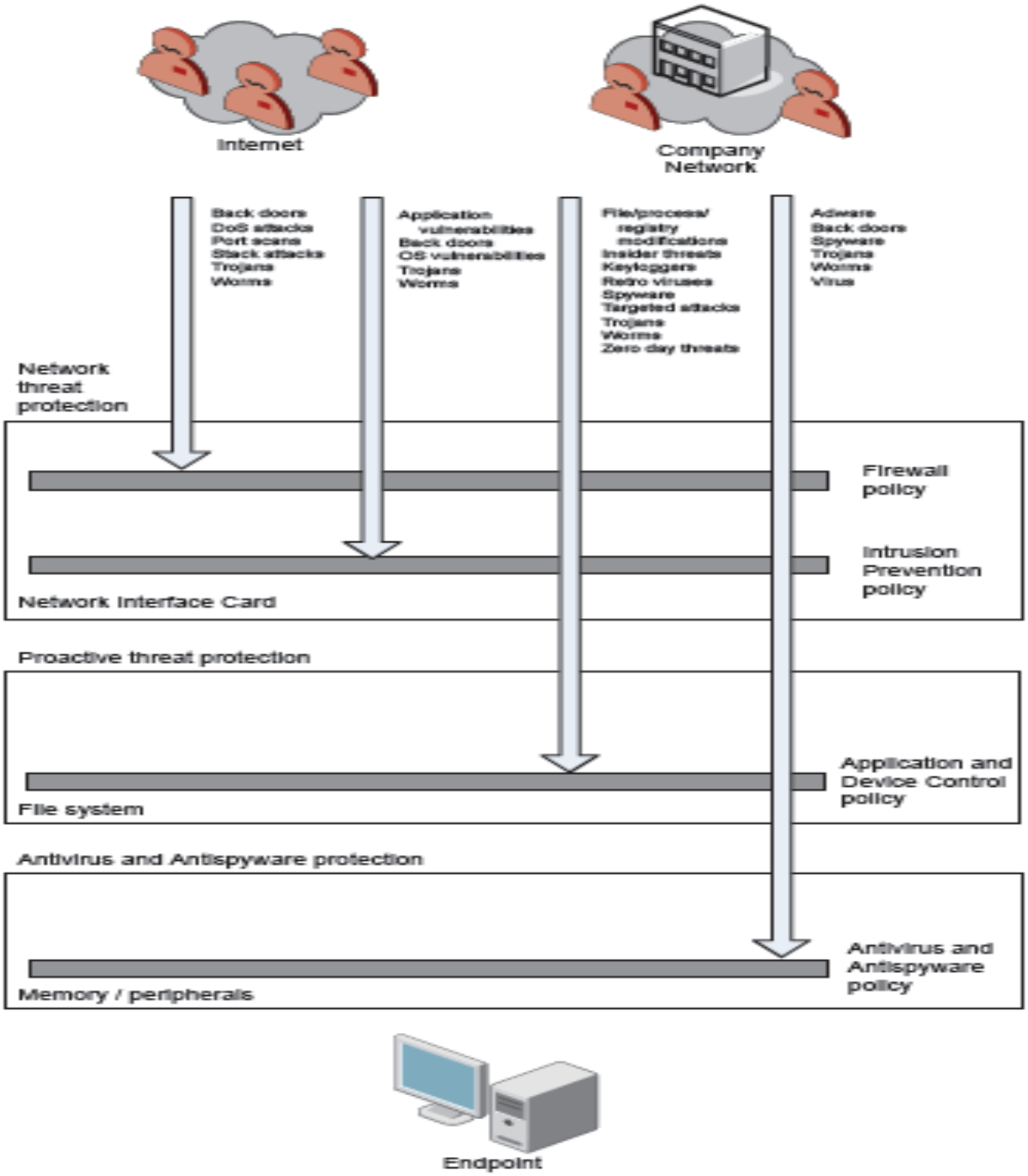
- Polise koje raspoznaju lokacije dozvoljavaju ili zabranjuju prenosnim računarima da pristupe mreži u zavisnosti od njihove fizičke ili mrežne lokacije, u skladu s polisama koje je definisao administrator. *Firewall* prati i dolazni i odlazni saobraćaj i sprečava zlonamerne programe da iznesu poverljive informacije izvan mreže korisnika.

Besplatan upgrade:

- Za korisnike koji imaju važeći maintenance za Symantec AntiVirus Corporate Edition i Symantec Client Security.

Kao dodatni element EndPoint zaštite uključen je Network Access Control. Ovaj segment omogućava potpunu kontolu EndPoint klijenta. Naime klijent se može konektovati na mrežu tek ukoliko su odredjeni elementi zadovoljeni. Tu se pre svega misli na najnoviju verziju polise,ili verzije definicija implementirane u okviru EndPoint manager-a.

Novina ovog proizvoda je ta što omogućava zašitu na nekoliko nivoa što je prikazano na slici br. 13.



Slika 13. – Nivo zaštite

5.1.1. Komponente Symantec EndPoint zaštite

EndPoint zaštita je vrlo kompleksan vid zaštite koji uključuje nekoliko elemenata:

a. Symantec EndPoint Protection client komponenta se instalira na krajnjoj tački zaštite (EndPoint), tj. tačku u računarskoj mreži koju želimo da zaštitimo. Ova komponenta se sastoji iz nekoliko podkomponenti i to: antivirus, antispyware, firewall, intrusion prevention, kontrola aplikacija, kontrola uređaja.Takođe uključuje i Network Access Control koja se mora dodatno aktivirati. Ova komponenta se ne instalira dodatno već je instalirana tokom instalacije EndPoint client-a, a aktivira se preko EndPoint Protection Managera.

b. Symantec EndPoint Protection Manager je komponenta koja se instalira na hostu na kome želimo da instaliramo software za management sistema. Naime preko ove komponente kontrolišemo komunikaciju EndPoint Managera i EndPoint clienta, a koja se obavlja preko Symantec EndPoint Protection Manager Console.

c. Symantec EndPoint Protection Manager Console ova komponenta omogućava centralizaciju u administraciji velike mreže EndPoint-a. Preko konzole moguće je uraditi instalaciju klijenata, kreiranje i forsiranje implementacije polisa, nadgledanje i izveštaj stanja u mreži EndPoint zaštite. Postoje dve vrste konzola. Jedna konzola se instalira sa instalacijom Managera, a druga je Remote Symantec EndPoint Protection consola ili Web consola koja se instalira na hostu sa koga želimo da administriramo sistemom.Ova konzola se startuje preko Internet Explorera ukucavanjem adrese http://ipadresamanagera:xxxx gde je xxxx port preko koga se uspostavlja sesija sa EndPoint manager. Ovaj port se može izmeniti.

Pored ovih komponenti postoje još dve opcione komponente koje se dodatno instaliraju i to:

a. Live Update server poznat kao Centralni LiveUpdate server, a koja omogućava preuzimanje security-a i updates sa Symantec sajta ili odgovarajućeg repozitorijuma. Symantec Manager i Symantec EndPoint Client se mogu konfigurisati da rade update sa Live Update server.

b. Centralni Quarantin predstavlja centralno spremište za sve identifikovane maliciozne kodove na EndPoint Client-ima [6].

5.1.2. Novine u EndPoint tehnologiji

Kada govorimo o novinama pre svega treba istaći integraciju antivirus i antispyware zaštite. Druga bitna stvar je uvođenje Network Threat Protection kojim se uvodi real firewall i preventivna zaštita od napada na EndPoint Client sa nekog hosta.

Bitna stvar koju treba napomenuti je i uvođenje modula Proactive Threat Protection kojim se sistem štiti od napada sličnih napadu Zero-day. Takođe omogućava potpunu centralizaciju u upravljanju procesima i hardverskim komponentama.
Zahtevi u pogledu operativnog sistema za instalaciju Symantec Managera su dati na slici br. 14.

Component	Requirement
Operating system	32-bit systems: ■ Windows 2000 Server/Advanced Server/Datacenter Server Editions, with Service Pack 3 or later ■ Small Business Server 2000 ■ Windows XP Professional Edition with SP 1 or later (x86 or x64) ■ Windows Server 2003 Web Edition Windows Server 2003 Standard/Enterprise/Datacenter Editions (x86 or x64) ■ Windows Small Business Server 2003 ■ Windows Compute Cluster Server 2003 ■ Windows Storage Server 2003 ■ Windows Server 2008 Standard/Windows Server 2008 Enterprise/Windows Server 2008 Datacenter/Windows Web Server 2008 64-bit systems: ■ Windows Essential Business Server 2008 Standard Edition/Windows Essential Business Server 2008 Premium Edition ■ Windows Small Business Server 2008 Standard Edition/Windows Small Business Server 2008 Premium Edition
Database	The Symantec Endpoint Protection Manager includes an embedded database. You can also use Microsoft SQL Server 2000 with SP3 or later, or Microsoft SQL Server 2005. SQL Server is optional.
Other software	■ Internet Information Services server 5.0 or later with Web services enabled. ■ Internet Explorer 6.0 or later ■ Static IP address recommended
Hardware	■ 1 GB RAM (2-4 GB recommended) ■ 4 GB on the hard disk for the server, plus 4 GB for the database ■ VGA (640x480) or higher resolution video adapter and monitor

Slika 14. - Zahtevi za Symantec EndPoint protection manager

Što se tiče instalacije EndPoint Manager Console takođe postoje zahtevi i oni su prikazani na slici br. 15.

Component	Requirement
Operating system	32-bit systems: ■ Windows 2000 with SP3 or later ■ Windows XP ■ Windows Server 2003 ■ Windows Vista 64-bit systems: ■ Windows Essential Business Server 2008 Standard Edition/Windows Essential Business Server 2008 Premium Edition ■ Windows Small Business Server 2008 Standard Edition/Windows Small Business Server 2008 Premium Edition
Hardware	■ 512 MB RAM, 1 GB recommended ■ 15 MB hard drive ■ VGA (640x480) or higher resolution video adapter and monitor

Slika 15. - Zahtevi za instalaciju EndPoint Console

Što se tiče Symantec EndPoint Client-a takođe postoje uslovi koji su dati u tabeli na slici br. 16.

Component	Requirement
Operating system	32-bit systems: ■ Windows 2000 Professional/Server/Advanced Server/Datacenter Server Editions, with SP 3 or later ■ Small Business Server 2000 ■ Windows XP Home/Tablet PC/Media Center Editions Windows XP Professional Edition /XP Embedded Edition (x86 or x64) ■ Windows Vista Home Basic Edition Windows Vista Home Premium/Business/Enterprise/Ultimate Editions (x86 or x64) ■ Windows Server 2003 Web Edition Windows Server 2003 Standard/Enterprise/Datacenter Editions (x86 or x64) ■ Windows Small Business Server 2003 ■ Windows Server 2008 Standard/Enterprise/ Datacenter Editions (x86 or x64) ■ Windows Web Server 2008 (x86 or x64) 64-bit systems: ■ Windows Essential Business Server 2008 Standard Edition/Windows Essential Business Server 2008 Premium Edition ■ Windows Small Business Server 2008 Standard Edition/Windows Small Business Server 2008 Premium Edition
Other software	Internet Explorer 6.0 or later Terminal Server clients connecting to a computer with antivirus protection have the following additional requirements: ■ Microsoft Terminal Server RDP (Remote Desktop Protocol) client ■ Citrix Metaframe (ICA) client 1.8 or later if you use Citrix Metaframe server on Terminal Server
Hardware	■ 256 MB RAM ■ 600 MB hard disk on 32-bit systems, 700 MB hard disk on 64-bit systems ■ VGA (640x480) or higher resolution video adapter and monitor

Slika 16. - Zahtevi za instalaciju EndPoint Client

5.2. Instalacija EndPoint-a (EP) na radnim stanicama

Da bi se uspešno instalisao antivirusni program Symatec EndPoint Protection na klijentskom računaru potrebno se ulogovati na računar sa *admin* nalogom i deinstalisati druge antivirusne programe koji već postoje na tom računaru.

Ručna Instalacija EP

1. Ulogovati se na radnu stanicu kao lokalni administrator,
2. Kliknuti na start/run,
3. Ukucati ***ipadresu domen kontrolera*** i pritisnuti enter,
4. Ako traži, ukucati korisničko ime (username) i lozinku (password) koji će te dobiti putem mail-a i on će služiti za administraciju EndPoint zaštite,
5. Pronaći folder ***EPInstall-ime-lokacije*** i u njemu folder ***ime-lokacije_32-bit,***
6. Otvoriti folder ***ime-lokacije_32-bit*** i kliknuti na *setup.exe i*
7. Odjaviti se (LogOut) i ulogovati (LogIn) se kao konkretan korisnik (user) i nikako ne isključivati računar 10 minuta.

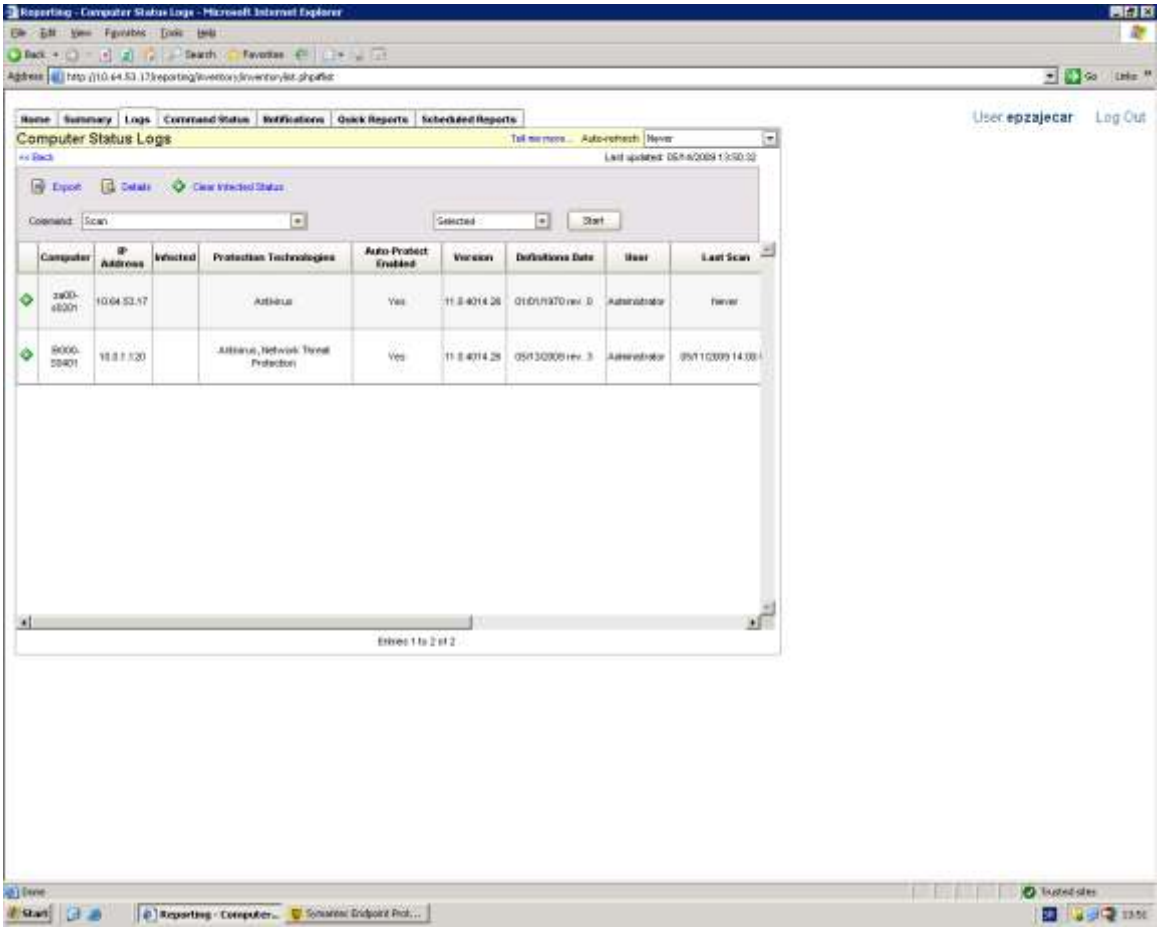
Da bi proverili postoji li kompletan pregled stanja EP Protection treba pristupiti sledećim operacijama:

1. Startovati internet explorer,
2. U polje address uneti http://ipadresaEPProtection-managera (to je ip adresa servera)/reporting. Primer.http://XX.XX.XX./reporting i
3. Nakon unosa adrese i pritiska entera na tastaturi pojaviće se maska za unos korisničko ime (username) i lozinka (password) za pristup serveru za izveštaje. Polje Domain ostaviti prazno.

Svaka filijala ima svoje korismičko ime i svoju lozinku koje treba držati u tajnosti. Odavanjem lozinke odgovorno lice snosi odgovornost i posledice koje mogu biti nanete filijali. Naime moguće je zlonamerno stopirati pristup mreži svim računarima u filijali.

Nakon unosa korisničkog imena i lozinke pojaviće se sledeća maska u kojoj se bira kreiranje raznih izveštaja. Jedan od izveštaja koji je zanimljiv je pregled klijenata sa definisanim datumima definicija, poslednjim skeniranjem itd. Navedeni izveštaji se mogu dobiti kada se pokrene opcija LOGS, a zatim *view report*. Pojaviće se izveštaj kao na slici br.17.

Pre nego što aktiviramo pregled izveštaja (view report) može se podesiti da prikaže onoliko klijenata na jednoj stranici koliko se želi da bude prikazano. Kliknuti na opciju *Advanced* i unese se broj klijenata. Tu su i ostali izveštaji [6].



Slika 17. Opcije kroz koje se treba proći tokom instalacije

5.2.1. Instalacija remote EndPoint manager consol-e

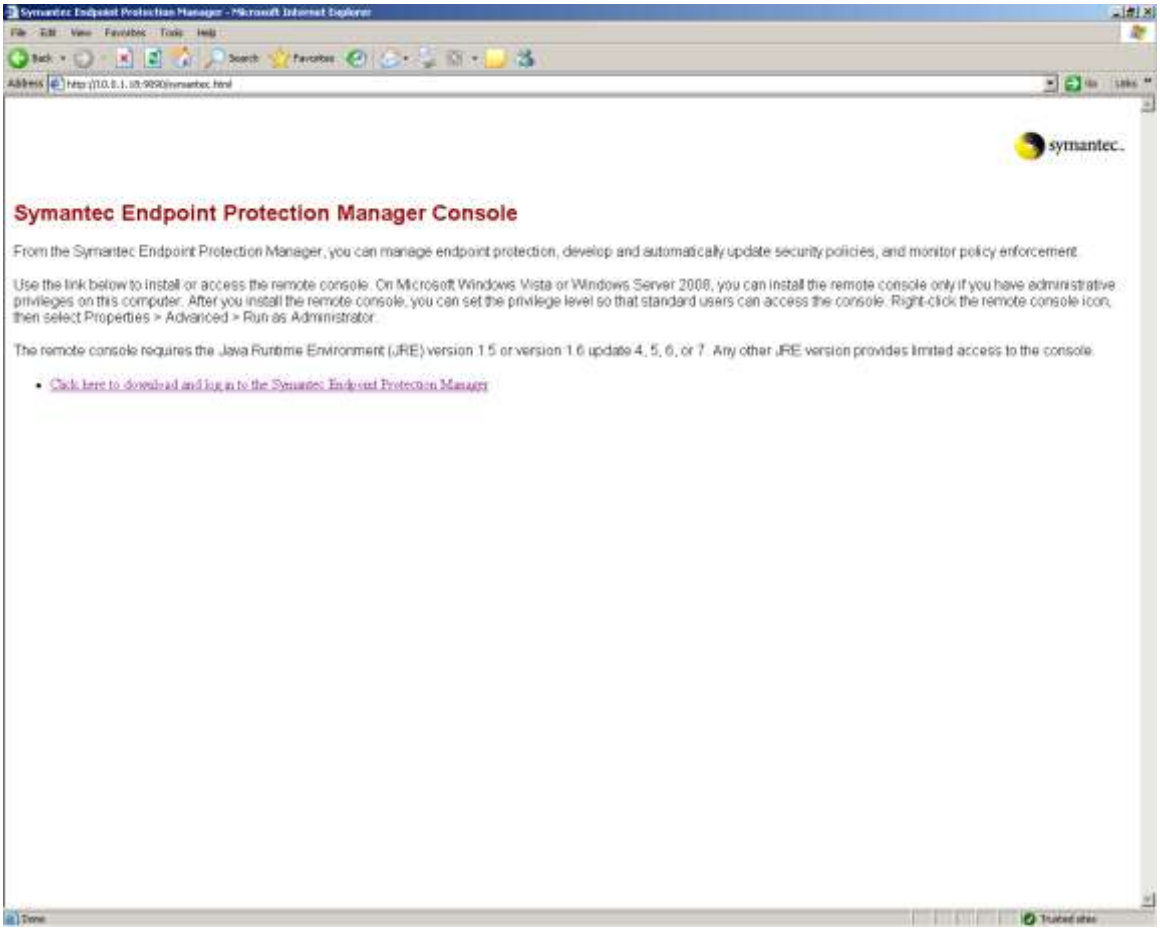
1. Na računaru na kome se podiže konzola mora se instalirati samo java 1.5
Ukoliko je Java 1.5 već instalirana prelazi se na tačku 5., u suprotnom na tačku 2.,

2. Pokrenuti internet explorer. U polje adresa (address) ukucati http://ipadresa pripadajućeg manager servera:XXXX. Slika br.18.,

3. Nakon toga pojaviće se maska na kojoj se zahteva instalacija JRE 1.5. To uraditi tako što treba kliknuti na reč *HERE*, nakon čega će započeti instalacija. Ako se ne pojavljuje maska za instalaciju podesiti ActiveX kontrolu na *enable*. To se radi tako što u Internet Exploreru (IE) treba kliknuti na *Tools*, a zatim na *Security*. Kliknuti na Local Internet i na dugme *Custom Level* i čekirati *Enable* u opcijama za ActiveX.

4. Nakon toga ponovo kliknzti na *HERE* i pojaviće se maska za instalaciju.

5. Nakon instalacije JRE 1.5 ponovo ukucati http://ipadresa pripadajućeg manager servera:XXXX ili sačekati da se pojavi sledeća maska u okviru IE



Slika 18. – Ukucavanje IP adrese u IE

6. Kliknuti na postojeći link i startovaće se *manager console*.

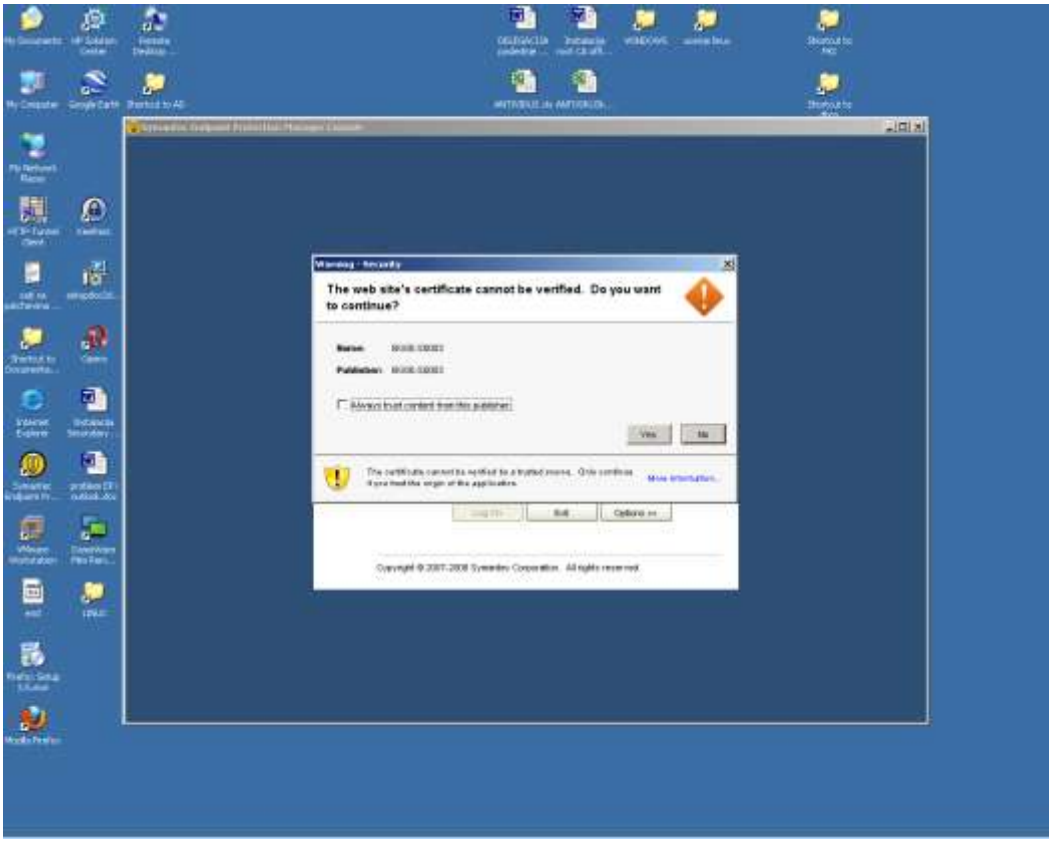
7. Pojaviće se učitavanje java

8. Kad se završi učitavanje pojaviće se prozor gde treba kliknuti na *Run*

9. Nakon toga pojaviće se maska za unos u kojoj treba unoseti korisničko ime i lozinku.

10. U polje *Server* uneti ime managament servera kome pripada lokacija koju treba administrirati i navodi se port XXXX.

11. Kliknuti na *LogIn* i pojaviće se maska, kao sto je prikazano na slici br. 19.

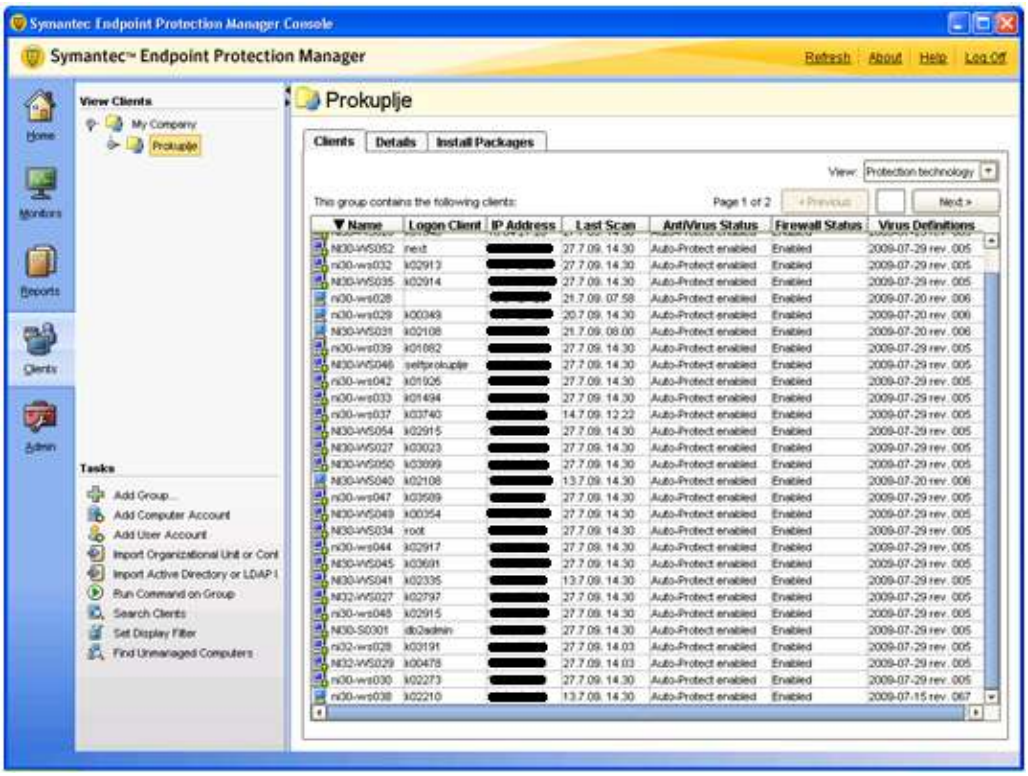


Slika 19. – Pokretanje instalacije JRE 1.5

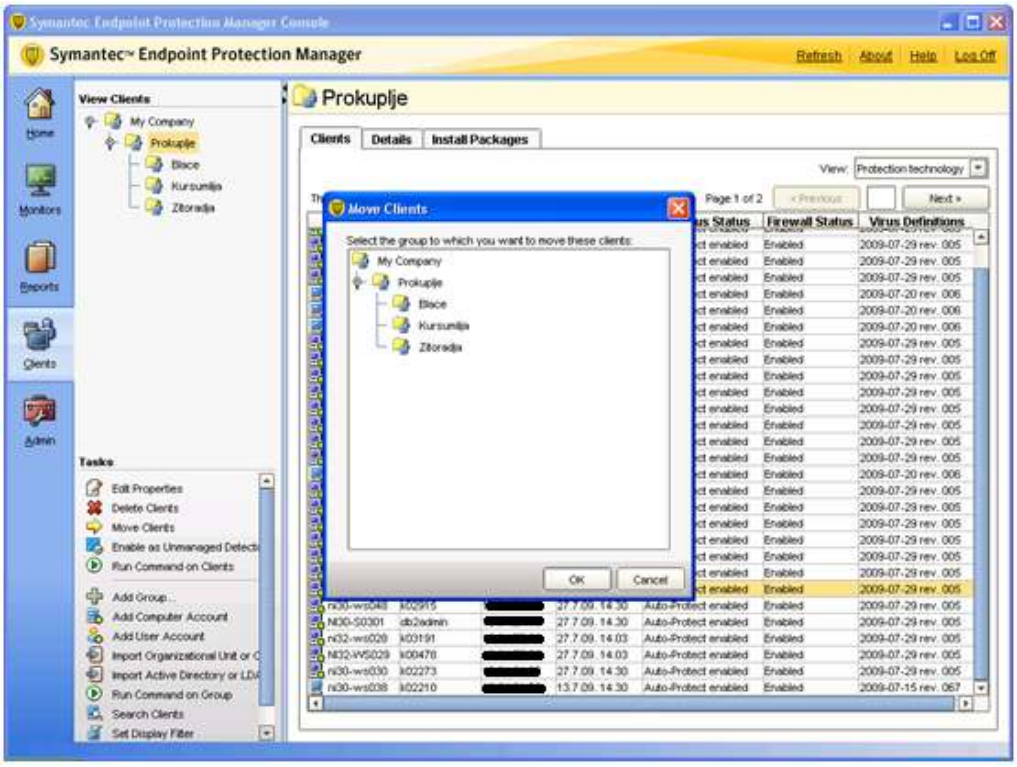
12. Čekirati opciju *Always trust* ….i kliknuti na *Yes* i nakon toga će se pojaviti maska u kojoj se administrira svojom lokacijom i odsecima ili ispostavama filijale kojoj pripada.

Kada se instalira klijent na lokaciji obavezno opcijom *Move* mora se preneti u grupu sa imenom lokacije na kojoj se nalazi. Na primer:

Ako se instalira računar u ispostavi *Kuršumlija* filijale *Prokuplje*. Taj računar će se pojaviti u grupi *Prokuplje* zato sto je *package Endpoint client* pravljen za grupu *Prokuplje*. Da bi povukao definicije i ostale elemente neophodno je da se *Endpoint client* prebaci iz grupe *Prokuplje* u grupu *Kuršumlija*. Tako što desnim klikom na klijenta u konzoli se izabere opcija *Move* i zatim se pozicionirati na *Kuršumliju* i kliknti na *OK* (Slika br.20 i 21).



Slika 20. – Izveštaj filijala Prokuplje



Slika 21. – Pomeranje klijenta iz jedne u drugu grupu

Tako isto se uradi i sa odsecima u filijali Beograd. Svi klijenti se nalaze u Grupi Gundulicev Venac.Iz ove grupe endpoint klijente treba da prebacite u grupu sa imenom lokacije na kojoj se nalazi.
Obavezno se proveri da li se http://ipadresa managament servera: XXXX nalazi u trusted sites u okviru local internet. To se podešava u Internet Exploreru u opciji Tools pa Security kartica [6].

Obavezno proveriti da li razrešava ime koje navodimo u remote endpoint console. Ako ne razrešava staviti ga u hosts fajl.
U hosts fajl dodati ime managament servera i njegovu ip adresu

5.2.2. Ikone obaveštenja u Symantec EndPoint antivirusnom sisitemu

Nakon instalacije EndPoint Client softvera u systray-u EndPoint će se pojaviti ikona u obliku štita.Ikona pokazuje status EndPoint clienta tj stanje u kome se on nalazi. Ikona se nalazi u desnom donjem delu desktopa gde desnim klikom na ikonu dobijamo meni sa komandama koje možemo primeniti u GUI režimu. Značenje grafičkog simbola ove ikone prikazana je u tabeli br. 3.

Ikona	Opis
	Klijent radi bez grešaka. Ovo je oznaka klijenta koji radi u režimu Off-line ili se radi o klijentu čije upravljanje nije centralizovano tj unmanaged klijentu.Takav klijent nije konektovan na management server.
	Klijent radi bez grešaka.Ovo je oznaka da klijent komunicira sa management serverom. Sve komponente su aktivne.
	Klijent ima zanemarljive greške. Primer neka od komponenta nije update-ovana
	Klijent radi sa greškom, tj ozbiljnim problemom. EndPoint client je u status disable.

Tabela 3. - Status ikona EndPoint Client-a

Za razliku od Symantec EndPoint Client-a takodje i Symantec Network Access Control ima svoju ikonu, čije značenje je definisano u tabeli br. 4.

Ikona	Opis
	Klijent radi bez grešaka, gde je obavljen Host čekiranje kao i update policy.Radi se o offline klijentu ili unmanaged.
	Klijent radi bez grešaka, stime da postoji komunikacija sa management serverom.
	Klijent radi sa greškom, tj nije uradjeno čekiranje integriteta niti update policy-a.

Tabela 4. – Status ikona Symantec Network Access Control-a

Što se tiče statusa klijenta moguće je takođe utvrditi sa centralizovane konzole. Značenje ikona u EndPoint manager console definisano je tabelom br. 5.

Ikona	Opis
	Klijent komunicira sa Manager-om. Klijent je u tzv. stanju computer mode
	Klijent ne komunicira sa Managament serverom. Klijent je u computer modu. Označava takođe da je klijent dodat sa konzole ili nema klijentskog software-a
	Klijent komunicira sa management Menager-om. Klijent je u computer modu. Radi se o unmanaged klijentu.
	Klijent ne komunicira sa Managament serverom. Klijent je u computer modu. Radi se o unmanaged klijentu.
	Klijent komunicira sa Managerom. Klijent je u tzv. stanju user mode.
	Klijent ne komunicira sa Managament serverom. Klijent je u user modu. Označava takođe da je klijent dodat sa konzole ili nema klijentskog software-a
	Klijent komunicira sa EndPoint Manager-om koji se nalazi u drugom sajtu. Klijent je u computer modu
	Klijent komunicira sa EndPoint Manager-om koji se nalazi u drugom sajtu. Klijent je u computer modu. Klijent je u statusu unmanaged klijenta
	Klijent komunicira sa EndPoint Manager-om koji se nalazi u drugom sajtu. Klijent je u user modu

Tabela 5. – Ikone u EndPoint-u

5.2.3. Ažuriranje polise (Update Policy)

Jedna od najvažnijih stvari od koje zavise sve komponente klijenta je polisa. Update polisa se radi automatski. U pojedinim slučajevima usled problema moguće je da se nije inicirao update polise na klijenta. U tom slučaju potrebno je ručno pokrenuti update na samom klijentu. Postoje dva načina i to su:

a. Na samom klijentu u okviru opcije Help and Support menu u polju Troubleshooting, u okviru Policy Profile neophodno je kliknuti na opciju Update.
b. U Nacionalnoj službi za zapošljavanje je podešen sistem PULL MODE što se tiče update polisa, (Managament server u jednakim vremenskim intervalima koje ručno podešavamo vrši update polisa tzv. Heartbeat). U ovakvom sistemu moguće je smanjiti navedeni interval vremena i na taj način prevazići problem Update policy.

5.2.4. Ažuriranje definicije programa (Update definition)

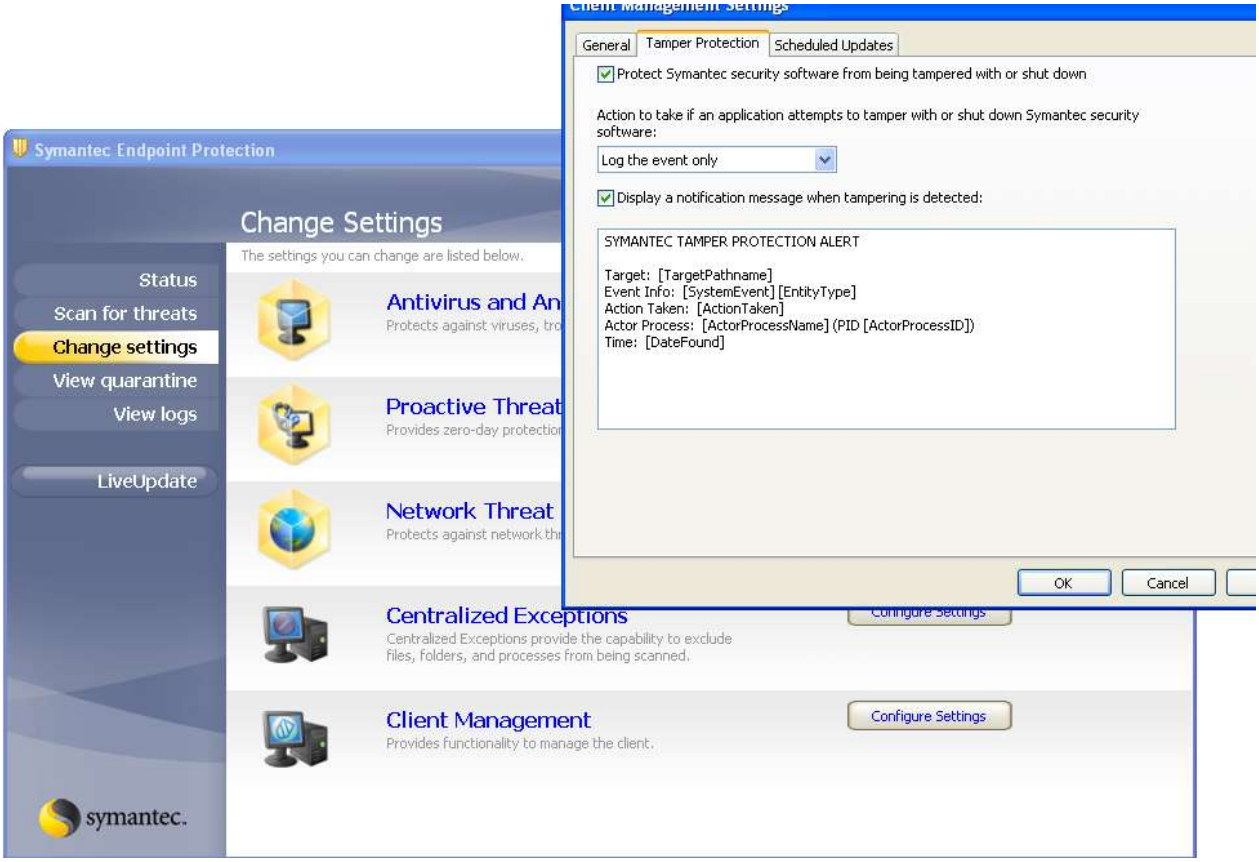
Kada govorimo o ažuriranju definicije (eng. *Update definitions*) možemo reći da mogu nastati brojni problemi. Različiti su uzroci zbog kojih klijent ne radi ažuriranje definicaja. Klijent može da preuzima sadržaje od različitih izvora među kojima su: Managament server, Group Update Provider, Internal Live Update server, Symantec Live update server, ili third-party management tool-a. Ukoliko klijent ne radi update definicija možemo primeniti različite akcije u zavisnosti od problema, a to su:

a. Neophodno je utvrditi da li je klijent pravilno konfigurisan. Naime potrebno je na samom klijentu startovati registry bazu. Nakon startovanja pozicionirati se na ključ HKEY_LOCAL_MACHINE\Software\Symantec\Symantec EndPointProtection\LiveUpdate. U Nacionalnoj službi za zapošljavanje je neophodno da vrednosti sledećih ključeva budu:
    a. UseLiveUpdateServer - *x*
    b. UseManagementServer - *x*
    c. UseMasterClient - *x*
    d. Maste Client - *ipadresa server lokacije sa koje se vrši update.*

b. Proveriti Contet Cache. Naime sadržaj foldera contet cache na klijentu treba uporediti sa mamagament serverom koji je nadležan za klijenta. Na klijentu se treba pozicionirati na folder \Program Files\Symantec\Symantec EndPoint Protection\ContentCache. Takođe na server se treba pozicionirati na folder \Program Files\Symantec\Symantec EndPoint ProtectionManager\Inetpub\content. Zatim je potrebno uporediti subfoldere u navedenim folderima i utvrditi da li je sadržaj identičan. Na server postoji fajl ContentInfo.txt u kome je upisana lista imena contenta i foldera u kojima se nalaze.

Oštećen folder za prijem definicija. U ovom slučaju treba primeniti sledeću akciju

c. Pozicionirati se u okviru Administartive tools na konzolu services. Potrebno je stopirati servis Symantec Managament Client i Symantec EndPoint Protection. Ukoliko Symantec Managament client nismo u mogućnosti da stopiramo onda je potrebno odčekirati opciju Temper Protection. Desnim klikom na ikonicu EndPoint otvoriti opcijom open. Zatim kliknuti na opciju Change settings i kliknuti na dugme Configure settings u opciji Client Managament. Pozicionirati se na karticu Temper Protection i odčekirati opciju prikazanoj na slici br. 22.



Slika 22. – Client Menagment Settings

Nakon ove operacije pozicionirati se na folder c.\Program Files\Comman Files\Symantec Shared\Virus defs i izbrisati celokupan sadržaj.
Nakon prethodno urađene operacije pozicionirati se na folder c:\Documents and Settings\AllUsers\Application data\Symantec\Live Update\Downloads i takođe u okviru ovog foldera izbrisati celokupan sadržaj.

Nakon brisanja sadržaja foldera startovati registry bazu.

Pozicionirati se na ključ HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\ Shareddefs i izbrisati sledeće ključeve
SRTSP
NAVCORP_XX
DEFWATCH_XX
SepCacheX
SepCacheX
SepCacheX
Zatvoriti bazu registry.
Nakon ovog startovati servise koje smo prethodno stopirali.

5.2.5. Organizacija EndPoint zaštite

Kada govorimo o organizaciji Endpoint zaštite treba izdvojiti nekoliko pojmova:

a. Sajt (Site) je osnovi element u organizaciji Symantec Endpoint Protection topologije. Sajt je logički skup baze podataka (databese), management server i EndPoint klienata. Informacije jednog sajta se repliciraju informacijama drugog sajta i obrnuto preko management server-a.

U Nacionalnoj službi za zapošljavanje je primenjen EndPoint Manager server sa Embedded Sybase database koji je u mogućnosti da podrži oko 1000 klijenata. Iz tog razloga u Nacionalnoj službi za zapošljavanje (NSZ) je primenjena topologija sa 4 sajta Beograd, Niš, Novi Sad i Jagodina u kojima su podignuti Managament server sa Embedded Sybase database. Pored ove opcije postoji i opcija sa SQL bazom koji bi mogao da opslužuje daleko veći broj klijenata ali koji se licencira.

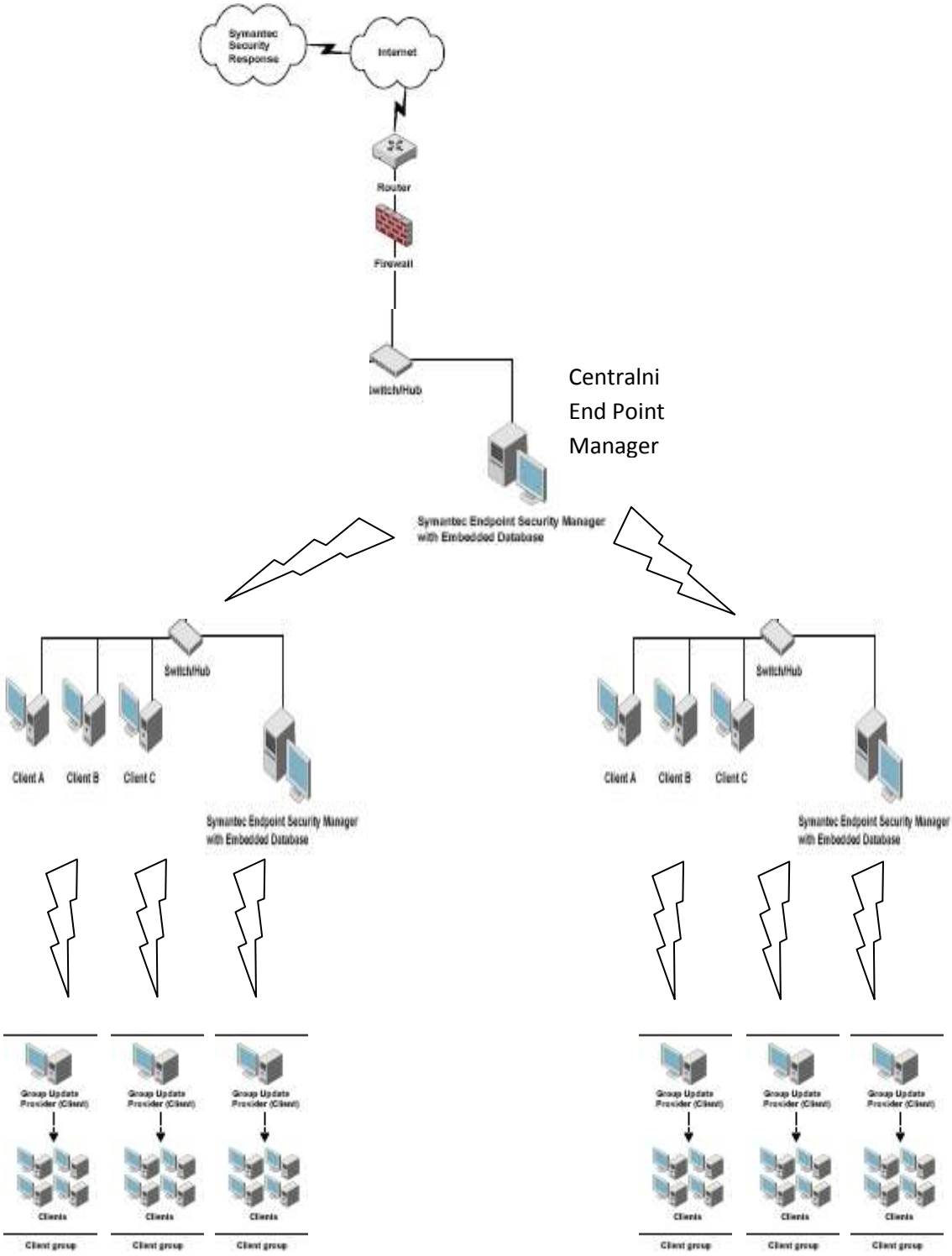
Postoji podela na male organizacije do 100 klijenata, organizacije sa manje od 1000 klijenata i velike organizacije sa vise od 1000 klijenata. Treći tip koji je i primenjen u NSZ je upravo tip sa nekoliko sajtova u okviru kojih se nalaze nekoliko management server-a.

b. Managament server je server na kome je instaliran Symantec EndPoint Protection Software, a koji se koristi za upravljanje klijentima, polisama, nadgledanjem i pravljenjem izveštaja. Kao interfejs prema Manageru koristimo EndPoint manager Consolu.

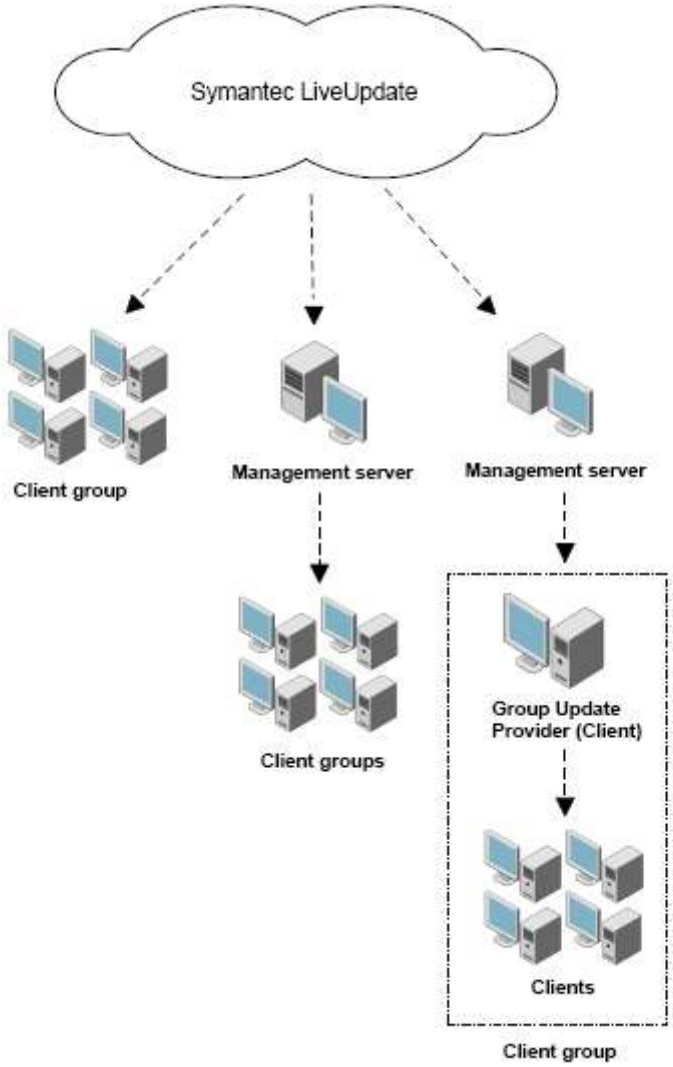
c. Group Update Provider (GUPs) je server-client koji preuzima sadržaj content od management server sajta kome pripada i tako preuzet sadržaj distribuira grupama za koje je nadležan. Treba napomenuti da GUP ne distribuira programske nadogradnje. GUP je u mogućnosti da obrađuje do 150 klijenata. Na taj način klijenti preuzimaju nadogradnje sa svog lokalnog GUP-a, a ne sa management server-a.

d. Grupa (group) je element koji omogućava grupisanje klijenata radi lakšeg upravljanja i administracije. U NSZ-u primenjen je sistem gde Group podrazumeva sve računare jedne lokacije, a koja je definisana Subnetom. Tako na filijalu Subotica je jedna grupa definisana nad subnetom xx.xx.xx.xx a druga grupa je njegova ispostava Bačka Topola definisana subnetom xx.xx.xx.xx i tako redom. Svaka grupa ima svog GUP-a [6].

Sistem primenjen u Nacionalnoj službi za zapošljavanje je prikazan na slici br. 23 i 24.



Slika 23. – Arhitektura EndPoint-a u NSZ



Slika 24. – Uprošćena šema EndPoint-a u NSZ

5.2.6. Rešavanje problema komunikacije EndPoint Client Endpoint Manager

Najbitniji element ispravnog funkcionisanja EndPoint Client-a je pravilno definisana komunikacija EndPoint Clienta i management server koji je nad njim nadležan. Provera se može podeliti u dva dela:
Prvi element koji se posmatra je ikona EndPoint-a. Ukoliko postoji štit sa zelenim kružićem, kao što je prethodno prikazano.

Drugi element je konfiguracioni fajl. Konfiguracioni fajl nadležan je za komunikaciju SyLink.xml koji se nalazi u folderu SymantecEndpointProtection. Fajl je potrebno otvoriti Notpad-om i proveriti ime Site pod nazivom DefaultManagament server i red u kome piše ip adresa, a koja mora da odgovara management server nadležnom za klijenta

Ukoliko klijent nije dobro konfigurisan neophodno je pristupiti sledećoj proceduri:

a. Stopirati servis SMC.exe komandom **smc –stop**
b. Nakon stopiranja servisa sa servera (domen kontrolera lokacije) iz foldera IME MANAGAMENT SERVERA_KONFIGURACINIFAJL iskoprati fajl SyLink.xml u folder SymantecEndPointProtection i uraditi zamenu.

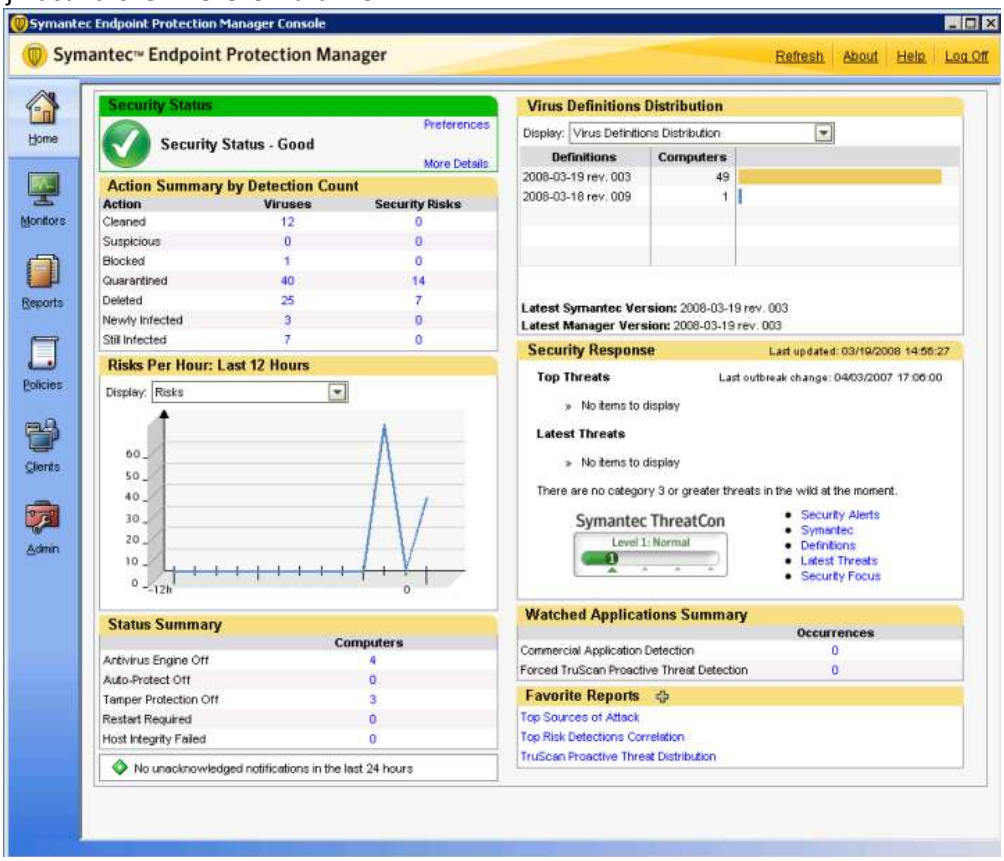
c. Startovati servis SMC.exe pomocu komande **smc –start.**

5.2.7. Unmanaged client

Pored managent client-a postoje i unmanaged client. To je klijent koji nije upravljiv sa management server-a već nezavisno pristupa sajtu Symantec-a i vrši nadogradnju (update). Instalira se direktno preko instalacionog CD ili setup-a i izborom opcije unmanaged. Bitno je naglasiti da je prelazak na managed verziju vrlo jednostavna, naime kopiranjem odgovarajuceg *Sylink.xml* fajla i restartom računara. Takođe sa management konzole moguće je, desnim klikom na grupu kojoj želimo da pripada, izaberemo opciju export communication server. Dobiće se fajl koji treba preneti na klijenta.

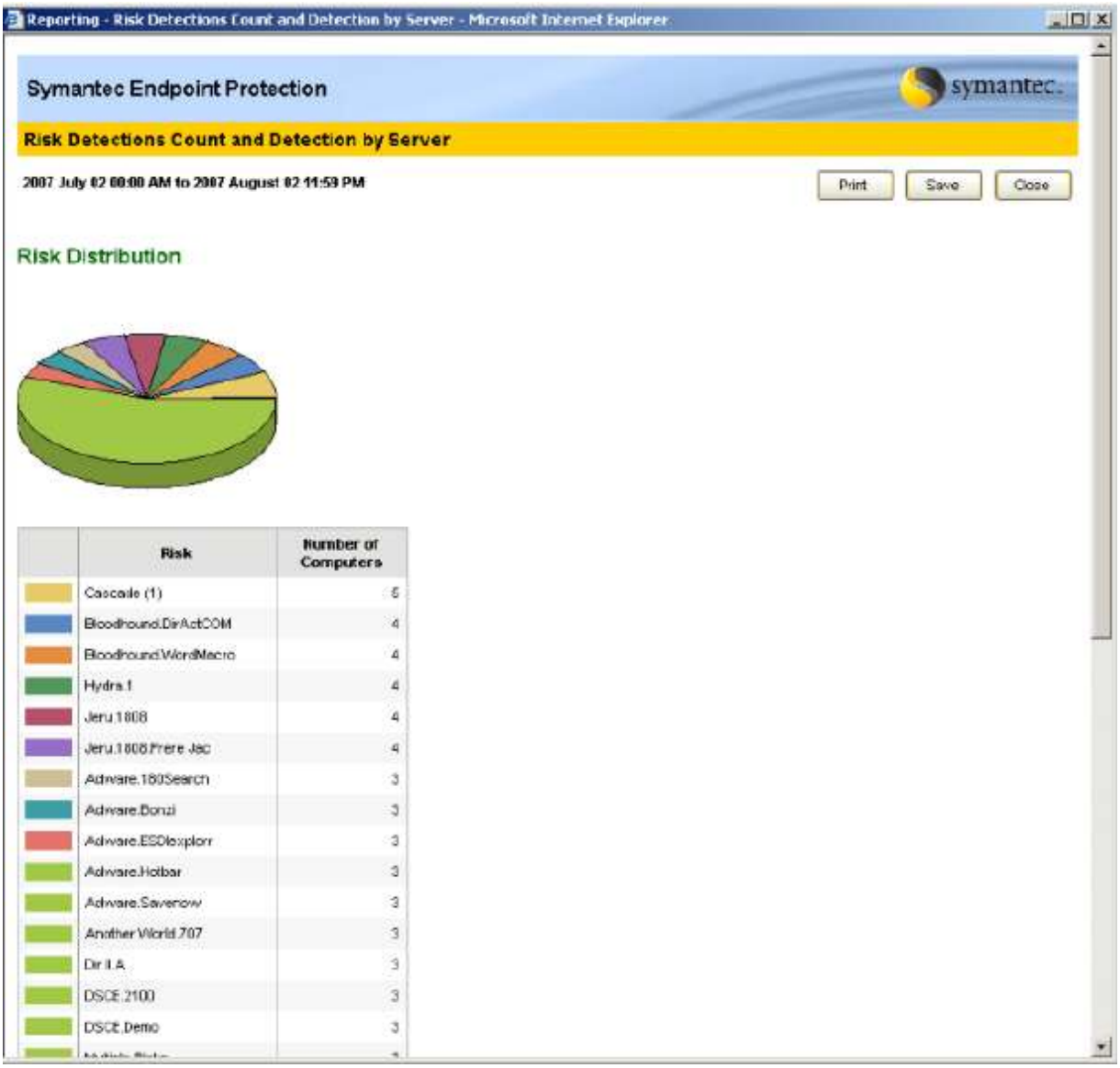
5.2.8. Izveštaj (Report)

Ovo je jedna od veoma važnih stranica koja omogućava veliki broj izveštaja koji može pomoći u administraciji računarske mreže. Slika br.25.



Slika 25. – Prozor koji prikazuje izveštaje EndPoint Antivirusnog sistema

Reportu možete pristupiti li startovanjem Remote Mnagament konzole (preko internet explorer kucajući adresu *http://ipadresa management_server_nadležan za_klijenta:xxxx/reporting* nakon toga pojaviće se maska za unos korisničkog imena (username) i lozinka (password).
Izgled jednog jednostavnog izveštaja (reporta) je prikazan na slici br. 26.



Slika 26. – Izveštaj rizika (Risk report)

Postoje dva tipa izveštaja tj *report*-a, to su: Brzi izveštaj (eng. *Quick report*) i celokupan izveštaj (Full report). Prvi tip reporta je Quick report. Tabela 6.

Tip reporta	Opis
Application and Device Control	Prikazuje informacije o aplikacijama kao i uređajima kojima nije dozvoljen pristup resursima u mreži
Audit	Sadrži informacije o polisama (modifikaciji,vremenu izmene…
Compliance	Prikazuje informacije o serveru,klijentima, saobraćaju
Computer Status	Prikazuje informaciju o realnom stanju klijenta
Network Threat Protection	Prikazuje aktivnosti klijenta i interakciju sa ostalim hostovima u mreži
Risk	Prikazuje risk dogadjaje na management server i klijentima
Scan	Prikazuje informacije o aktivnostima skeniranja
System	Prikazuje problem koji se pojavljuju na klijentima

Tabela 6. – Brzi izveštaj sa funkcijama i njihovim objašnjenjima

Pored navedenog izveštaja postoje brojni izveštaji za čije izlaganje bi zahtevalo dosta vremena. Međutim treba izdvojiti *Computer report* koji daje detaljne informacije o kljentu kao što su verziju definicija, imena kompjutera koji nisu čekirani, verziju endpoint-a, verziju intrusion prevention-a, inventory client-a (vrstu operativnog sistema, total memory, free memory, total disk space, free disk space, tip procesora, kao i vrstu patch primenjenog na sistem), status client-a, broj klijenata sa novom polisom, broj klijenata u grupi, status klijenta i preporuke (antivirus off ili on, auto protect, restart iz required, …), *virus definition rollout* koji se izvršava samo sa opcijom scheduled, a pokazuje informacije o kretanju definicija [6].

Svi izveštaji se mogu snimiti i dostaviti na uvid nadležim strukturama u Nacionalnoj službi za zapošljavanje.

Zaključak

U današnje vreme kada je Internet važan i potreban resurs u svim organizacijama veoma je bitno posvetiti određenu pažnju računarskoj sigurnosti. Pri tom firewall ima veliku ulogu jer štiti organizacije od brojnih zlonamernih korisnika Interneta. Oni su prva barijera koju napadač mora da prođe kako bi došao do željenog cilja-zaštićenih računara.

Odabir željenog firewall-a sve je teži, jer je sve veći broj ponuđenih firewall-a. Ti firewall-i mogu biti komercijalni ili besplatni. Komercijalni obično nude lakše konfiguracije i veći broj mogućnosti. Besplatni su obično beskorisni bez stručnjaka koji bi ih konfigurisali i održavali.

Osim podele na komercijalne i besplatne firewall-i se mogu podeliti i na one namenjene Windows operativnim sistemima, kao i na firewall-e namenjene za Unix/Linux operativne sisteme. Perfomanse i mogućnosti su im u osnovi jednake i neki proizvođači firewall-a izrađuju firewall-e koji rade na i jednom i drugom operativnom sistemu.

Zavisno od potreba korisnika moguće je konfigurisati firewall koji lokalnu mrežu štiti od neovlaštenih i zlonamernih korisnika na različite načine. Pri tome moguće je koristiti različita rešenja, ili konfiguraciona ili programska.

Razvojem računara usporedno dolazi do razvoja zlonamernih programa. Stvar koja je najviše podstakla razvoj i širenje ovih programa je računarska mreža. Pre pojave umreženih računara, jedini način prenosa zlonamernih programa je bio putem zaražene diskete, te su takvi program imali neuporedivo manje šansi za dalje širenje. Pojavom Interneta i servisa poput elektronske pošte, mogućnosti prenosa zlonamernih programa drastično rastu. Oni su ubrzo počeli da se šire mnogo većom brzinom i da koriste sofisticiranije načine prenosa.

Kako je broj računara sa pristupom Internetu rastao, a Internet postajao sve više globalna mreža, tako su i infekcije bile sve ozbiljnije i najčešće globalnog tipa. Rađaju se novi tipovi zlonamernih programa, kojima više nije glavni cilj nanošenje štete drugim korisnicima, već prikupljanje ili krađa informacija od istih. Upotreba Interneta u obavljanju finansijskih transakcija, dovodi do pojave novog vida kriminala, elektronskog kriminala.

Zlonamerni program poput trojanskih konja i rootkit-a predstavljaju glavno oružje u rukama tehnološki visoko obučenih kriminalaca. Činjenica je da zlonamerni programi postoje i na to se dalje ne može uticati. Jedino što je moguće u ovakvoj situaciji je pronalaženje načina zaštite od takvih programa. Najefikasniji način zaštite je upotreba nekog antivirusnog paketa. Pored operativnog sistema, antivirusni paket je druga obavezna komponenta savremenog računara.

Korisnici koji drže do svoje bezbednosti, moraju posvetiti vreme izboru za njihove potrebe najboljeg antivirusnog paketa i njegovom pravilnom konfigurisanju. Virusi,crvi i ostali nepoželjni programi se pojavljuju svakodnevno. Svaki korisnik, bez obzira na njegovu stručnost je u stanju da uz pomoć alata za generisanje zlonamernog koda napravi svoj primerak takvog programa. Jedini način da se sa sigurnošću zaključi koji je program maliciozan, je detekcija takvog koda na osnovu potpisa. Za tako nešto je neophodno da se definicija virusa nalazi u bazi antivirusnog paketa. Neredovno osvežavanje baze virusa najnovijim definicijama virusa, ima za posledicu slabljenje odbrambenog sistema antivirusnog programa.

Trenutno najveća briga korisnika koji poseduju redovno ažuriran antivirusni program na svom računaru, predstavljaju sam operativni sistem i loše implementirane aplikacije. Rešenje ovog problema se svodi na instaliranje najnovijih bezbednosnih zakrpa za operativni sistem i ostale loše implementisane programe koje korisnik ima instalirane na svom računaru.

Dobro konfigurisan firewall će predstavljati dodatnu prepreku za sve vrste malicioznih programa. Takođe, njegova loša konfiguracija firewall može doneti više štete nego koristi. Iz ovoga možemo videti da je poželjna zaštita u slojevima. Veći broj slojeva otežava posao zlonamernim programima, a time se smanjuje mogućnost infekcije.

Takođe, u radu su prezentovani i detaljno objašnjeni mailciozni programi , kao i njihov štetni uticaj.
Na drugoj strani je prikazana mogućnost antivirusne zaštite. Zadatak završnog rada pokazuje da se dobro organizovanom zaštitom, odnosno, legalnim antivirusnim programima može nesmetano odvijati proces rada, pogotovo u našem primeru prikazane su mogućnosti nesmetanog funkcionisanja informacionog sistema u državnoj i javnoj ustanovi, što u današnjim ustanovama nezvanično nije na nivou koji bi trebalo da bude.

Literatura

[1] Andrew S. Tanenbaum, Computer Networks, Fiveth edition, Prentice-Hall, Inc., 2011.,

[2] James F. Kurose, Keith W. Ross, Computer Networking: A Top-Down Approach Featuring the Internet, Addison Weslez, 2009,

[3] Chris Lathem, Benjamin W. Fortenberry, Kevin Lynn, Daniel H. Bendell, Joshua Reed, SonicWALL – Firewalls,

[4] Rob Pickering, Internet Firewall Tutorial, 2009,

[5] Cisco ASA Series Firewall CLI Configuration Guide,

[6] Peter Szor, The Art of Computer Virus Research and Defense, Addison Wesley,

2006

[7] Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song, Cliff Wang, Malware Detection, 2007

[8] Greg Hoglund and James Butler, Rootkits: Subverting the Windows Kernel, Addison

Wesley Professional, 2006

[9] John Ay cock, Computer Viruses and Malware, 2006

[10] Tetsu Iwata Masakatsu Nishigaki, Advances in Information and Computer Security, 2011

[11] Nepoznati autor, Skripta o podešavanju i instalaciji Symantec EndPoint antivirusa na mrežama Nacionalne službe za zapošljavanje, 2011-2012

Web sajt:

[12] http://www.tech-faq.com/logic-bomb.html (posećeno 04.07.2012. god.)

[13] http://www.apisgroup.org/sec.html?id=7 (posećeno 15.07.2012. god.)

[14] http://informatika.oshrs.edu.rs/izdvajamo/kompjuterski-virusi (posećeno 08.08.2012. god.)

[15] http://www.informacija.rs/Clanci/Kompjuterski-virusi.html(posećeno 14.08.2012. god.)

[16] http://helpdesk.co.me/index.php/stasuvirusi (posećeno 24.08.2012. god.)

[17] https://sites.google.com/site/stetniprograminainternetu/home (posećeno 10.09.2012. god.)

[18] http://www.icsi.berkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf (posećeno 25.09.2012. god.)

[19] https://secure.wikimedia.org/wikipedia/en/wiki/Botnet (posećeno 05.10.2012. god.)

[20] https://sigurnost.carnet.hr/vise-o-sigurnosti/enciklopedija/botnet/ (posećeno 10.09.2012. god.)

[21] http://en.wikipedia.org/wiki/Firewall (pogledano 10.5.2014.) i

[22] http://en.wikipedia.org/wiki/OSI_model, (pogledano 17.5.2014.).

Biografija

Rođen 17.12.1987. godine u Bihaću, BiH. Živeo u Donjem Lapcu (Hrvatska), gde je završio prvi razred osnovne škole. Osnovnu školu završio u OŠ “J. J. Zmaj“ u Subotici. Srednju tehničku školu, takođe završio u Subotici i stekao zvanje elektrotehničar elektromotornih pogona. Visoku tehničku školu strukovnih studija upisao je 2006. godine, na smer Informatičko inženjerstvo i stekao stručno zvanje strukovni inženjer elektrotehnike i računarstva. Univerzitet Singidunum je upisao 2011. godine, gde je, u septembru 2012. godine završio diplomski rad i stekao stručno zvanje diplomirani inženjer poslovne informatike. Master studije upisao 2013. godine. Poslednji ispit je položio u maju 2014. godiine.