Vatrozidovi: prikaz i primjena

Pavlek, Luka

Sveučilište u Rijeci – Odjel za informatiku

Diplomski studij- Poslovna informatika

Luka Pavlek

Vatrozidovi: prikaz i primjena

Diplomski rad

Rijeka, 10.8.2018.

Sveučilište u Rijeci – Odjel za informatiku

Diplomski studij- Poslovna informatika

Luka Pavlek

Vatrozidovi: prikaz i primjena

Diplomski rad

Mentor: prof.dr.sc. Mario Radovan

Rijeka, 10.8.2018.

Zadatak diplomskog rada

Pristupnik: Luka Pavlek

Naziv diplomskog rada: Vatrozidovi: prikaz i primjena

Naziv diplomskog rada na engleskom jeziku: Firewalls: representation and application

Sadržaj zadatka:

Treba dati prikaz temeljnih metoda rada vatrozidova (vatrenih zidova). Potrebno je prikazati protokole, sustave i procese na kojima se zasniva rad vatrozidova. Ukazati na glavne kvalitete vatrozidova, te na ograničenja mogućnosti zaštite pomoću sustava takve vrste.

Dio zadatka diplomskog rada je pronaći i ukratko prikazati nove izvore u kojima je dan kvalitetan prikaz protokola i sustava kojima se bavi ovaj rad.

Sažetak

U ovom diplomskom radu opisani su sustavi zaštite računalnih sustava naziva vatrozidovi. Dan je prikaz načina rada vatrozidova, prikazane su njihove prednosti i slabosti. U radu je odrađena podjela vatrozidova na nekoliko tipova vatrozidova te je svaki tip vatrozidova objašnjen. U prvom djelu rada opisane se razne prijetnje koje prijete računalnih sustavima, a koje se mogu vatrozidovima spriječiti. Na samom kraju rada prikazani su komercijalni vatrozidovi koji se koriste te je jedan od njih pobliže objašnjen, prikazano je njegovo postavljanje.

Ključne riječi: Vatrozidovi, zloćudni softveri, Denial of Service napadi, tipovi vatrozida, prednosti i mane vatrozida, komercijalni vatrozidi, „ZoneAlarm Free Firewall 2018.“

Sadržaj

1. Uvod

Internet se danas intenzivno koristi za privatnu i poslovnu komunikaciju. Zbog toga je potrebno i važno da se komunikaciju pomoću interneta zaštiti od raznih vrsta napad koji mogu biti vrlo štetni. Jedan od primjera zaštite računalnih mreža su i vatrozidovi (firewalls) o kojima ovaj diplomski rad govori. Sama definicija vatrozida je da je to sustav preko kojeg se odvija prijenos podataka u neku mrežu i iz te mreže. Vatrozidovi filtriraju tokove podataka koji hoće ući u neku štićenu mrežu, kao i tokove podataka koji hoće izaći iz te mreže. Što se tiče detaljnijeg opisa funkcioniranja vatrozidova taj dio je detaljno opisan u samom diplomskom radu. Također postoje i razni tipovi vatrozidova koji će biti navedeni u radu. U radu su navedeni i neki najpopularniji vatrozid softveri koji se danas koriste.

U prvom dijelu radu je fokus na prijetnjama koje prijete računalima, a koje je moguće spriječiti korištenjem vatrozidova dok je u nastavku rada fokus na samim vatrozidovima i njihovom principu rada.

2. Prijetnje za računalne mreže koje vatrozid može suzbiti

Kako živimo u doba u kojem su računala povezana u računalne mreže i dijele podatke međusobno tako su i mogućnosti za napad na računalne mreže sve veće. Napadači žele doći do povjerljivih informacija kako bi ih mogli zloupotrebljavati za vlastitu korist. Podaci na računalnoj mreži su vrlo izloženi te se napadaći koriste raznim trikovima i zlućudnim programima kako bi došli u posjed podataka koji su im potrebni. Također cilj nekih napada je i zaraziti računala kako bi usporili njihov rad ili pak u potpunosti taj rad onemogućili. Trenutno postoje brojne vrste programa koji rade štetu računalima te su u nastavku navedene i opisane te vrste zločudnih programa i raznih načina koji štete računalnoj mreži.

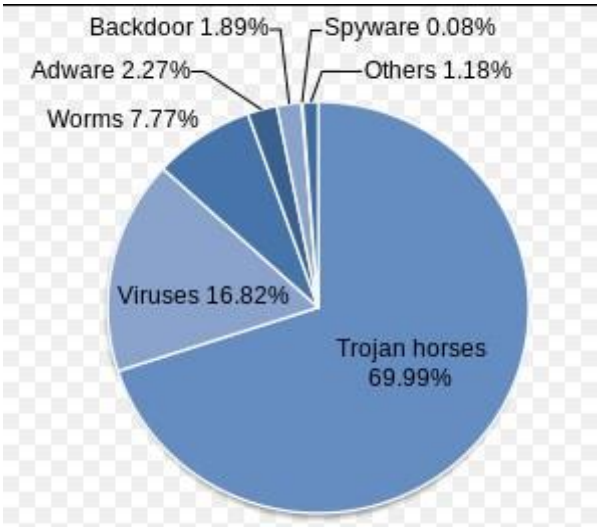
2.1. Zlućudni softver („Malware“)

Zlućudni softver (Malware-skraćenica od izraza malicious software) predstavlja program koji je izrađen sa svrhom da se neprimjetno ubaci preko računalne mreže u sustav nekog računala i učini neku vrstu štete. Ovaj pojam je nastao od riječi malicious i software što znači zlućudni softver. Radi se o računalnim programima koji se pokreću na računalu bez da je korisnik toga računala dao ikakav pristanak za to i njhova svrha je neka vrsta nepoželjnog učinka. To može biti oštećenje programa i podataka koji se nalaze na zaraženom računalu, širenje na druga računala, krađa raznih podataka, a osobito nekih povjerljivih podataka kao što su lozinke i brojevi kreditnih kartica. Također zločudni softver omogućava napadaču neovlašteni udaljeni pristup na računalo u svrhu nekog zlonamjernog djela, prikazivanje reklamnih poruka, masovno slanje neželjene elektroniče pošte (spam) , sudjelovanje u napadima na druga računala putem računalne mreže i slično.

Prema načinu širenja zlućudni programi mogu se podijeliti u više skupina: računalni virusi, računalni crvi, trojanski konji. Prema načinu djelovanja i cilju zlućudne programe dijelimo na špijunske programe, oglašivačke programe, fork bombe, ucjenjivački softver (softver koji traži otkupninu).

U početku, zlućudni programi uključujući i prvi „internetski crv“ su pisani u eksperimentalne svrhe ili kao šala no danas se koriste od strane hakera i vlada u loše svrhe kako bi ukrali osobne, financijske ili pak neke bitne poslovne informacije.

Na sljedećoj slici može se vidjeti udio pojedine vrste zloćudnog softvera koji rade štetu računalima diljem svijeta.



Slika 1. Udio napada prema vrsti zloćudnog programa

(Preuzeto s https://en.wikipedia.org/wiki/Malware)

2.1.1. Računalni virus

Računalni virusi predstavljaju vjerojatno najpoznatiju vrstu prijetnji za računala. To su računalni programi koji svojom reprodukcijom mogu zaraziti računala tako da bez dopuštenja ili znanja korisnika kopiraju sami sebe u datotečni sustav ili memoriju ciljanog računalnog sustava. Šire se inficiranjem datoteka, instaliranjem srodnih komponenti ili pak uklanjanjem određenih multimedijskih datoteka. Ovi programi u sebi sadrže destruktivne komponente koje je odredio sam autor virusa ovisno o tome što je njegova namjena. Tipičan virus inficira računalo, uništi ili obriše datoteke i foldere, preuzme druge opasne parazite na računalo, prikupi i zabilježi informacije o aktivnosti korisnika na internetu ili može drugima otkriti osjetljive podatke. Ako je računalo zaraženo od strane iznimno opasnog virusa, taj virus može

izbrisati ili šifrirati sve podatke koje nađe na hard disku. Najopasniji virusi nastoje oštetiti kompletan sustav računala ili samo neke dijelove. Najčešći načini širenja virusa na računala su putem interneta u obliku izvršnog zlonamjernog koda, zatim kao privitak u e-mail porukama ili pak putem medija kao što su vanjski hard disk, CD, DVD ili USB.

Računalni virusi imaju tri dijela, od kojih je prvi dio obavezan. Prvi dio omogućuje virusu da se replicira, drugi dio je nosiva komponenta koja je nakon širenja virusa njegova glavna aktivnost, a treći dio predstavlja trigger funkciju koja određuje okolnosti (vrijeme i događaj) u kojima će se izvršiti nosiva komponenta.

Kako bi se virus mogao replicirati pokretanjem izvršenja malicionznog (štetnog) koda, virusi se vežu za izvršne datoteke legitimnih programa. Tako se u slučaju pokretanja zaraženog legitimnog programa istovremeno pokreće izvršavanje virusnog koda. Virus radi tako da korisnik računala prvo pozove neki legitimni program, zatim nakon što je legitimni program pokrenut kod virusa koji je ubačen se izvršava umjesto legitimnog programa, a nakon toga kod virusa se završava i predaje kontrolu legitimnom programu.

Prema načinu djelovanja virusi se mogu podjeliti na rezidentne i nerezidentne. Rezidentni virusi se prilikom njihovog izvršenja učitaju u memoriju i njihov kod ostaje u memoriji cijelo vrijeme rada računala. Rezidentni virusi koriste tehnike TSR („terminate and stay resident“) i manipulaciju memorijskim blokovima (MBC) kako bi se cijelo vrijeme zadržali u memoriji računala. Zlonamjerni kod rezidentnih virusa koristi mehanizme operativnog sustava za svoje aktiviranje, na primjer, pokretanje koda pri svakom pokretanju bilo koje aplikacije. Tako se postiže efekt zaraze i nad novo instaliranim aplikacijama.

Nerezidentni virusi nalaze se u RAM-u samo u vrijeme njihovog izvršenja, odnosno od njihovog pokretanja pa do završetka rada. Njihovo širenje se svodi na princip da dio njihovog koda pronalazi datoteke koje mogu biti zaražene na sustavu (na primjer .exe, .doc i slično), a drugi dio koda kopira virusni kod u pronađenu datoteku.

Što se tiče vrsti virusa postoje tri osnovne vrste virusa, a to su boot sektor virusi, programski virusi i makro virusi.

Boot sektor virusi kopiraju svoj zlonamjerni kod u Master boot sektor i tako osiguravaju izvršenje zlonamjernog koda pri svakom startu računalnog sustava.

Programski virusi se aktiviraju pri izvršenju zaražene izvršne datoteke. To su najčešće datoteke s .exe ili .com ekstenzijom.

Makro virusi su virusi koji su napisani višim programskim makro jezikom, imaju mogućnost kopiranja i brisanja samih sebe te mijenjanja dokumenata.

Nakon podjele računalnih virusa na kategorije slijedi prikaz štetnih aktivnosti koje ti virusi mogu uzrokovati računalnom sustavu.

Nakon što se maliciozni program ubaci u računalo on može odraditi sljedeće aktivnosti:

- Inficira datoteke, piše preko njih ili ih briše
- Radi štetu nekim osobnim dokumentima, važnim sistemskim komponentama ili aplikacijama
- Mogu uništiti cijeli sustav brisanjem ključnih datoteka i foldera koji su bitni za njegovo funkcioniranje
- Dodaje štetne i opasne komponente u neki program ili modificira njegove postavke da bi inficirao dokumente koji se otvaraju ili kreiraju uz pomoć tog program
- Nanosi štetu računalu mijenjanjem bitnih hardverskih postavki brisanjem CMOS memorije ili brisanjem BIOS-a što dovodi do gubitka važnih podataka i kvara računala
- Prikazuje brojne lažne poruke, mijenja razne postavke sistema
- Krade ili šifrira osjetljive privatne informacije, vrijedne dokumente, lozinke, podatke za prijavu, detalje o identitetu ili kontakte korisnika
- Uzrokuje usporavanja, smanjuje sigurnost sistema i uzrokuje nestabilnost softvera

2.1.2. Računalni crvi

Računalni crvi su programi koji umnožavaju sami sebe te se šire putem računalne mreže. Za razliku od računalnih virusa, računalni crvi ne zahtijevaju postojanje neke domaćinske datoteke za svoj rad. Oni su samostalni programi te se u većini slučajeva šire bez ikakve interakcije korisnika. Glavna karakteristika im je razmnožavanje kao i kod računalnih virusa. S obzirom da crvu nije potrebna domaćinska datoteka kako bi radio štetu, može se reći da crv inficira okruženje (operativni sustav) prije nego objekte koji se lako inficiraju kao što su

datoteke. Računalni crv u sustav može ući i kao privitak u elektroničkoj pošti te mu pristup računalu omogućuju propusti u operacijskim sustavima i aplikacijama. Glavni zadatak računalnih crva je da otežavaju rad mreže te da oštete podatke i ugroze sigurnost računala.

Iako je danas najčešći medij za prijenos računalnih crva na računalo internet u prošlosti su se oni prenosili putem disketa, CD-a, DVD-a, a u novije vrijeme i preko USB-a.

Što se tiče načina širenja crva postoje dva osnovna. To je širenje računalnih crva bez interakcije korisnika te putem socijalnog inženjeringa.

„Širenje bez interakcije korisnika podrazumijeva iskorištavanje nekog sigurnosnog nedostatka na žrtvinom računalu. Sigurnosni nedostaci mogu biti prisutni u samom operacijskom sustavu ili u aplikacijama koje žrtva koristi u svakodnevnom radu. Crv će iskoristiti takav nedostatak kako bi instalirao svoju kopiju na žrtvino računalo bez njegova znanja. Odmah nakon instalacije počet će tražiti druga računala koja može zaraziti preko mreže. Zbog toga je važno redovito ažurirati softver na računalu kako bi crvima bilo onemogućeno iskorištavanje sigurnosnih nedostataka.

Širenje putem socijalnog inženjeringa podrazumijeva interakciju sa žrtvom. Autor crva lažima i različitim prijevarama pokušava potencijalnu žrtvu nagovoriti na njegovo pokretanje. Autor obično šalje e-mail poruku žrtvi u kojoj ga pokušava nagovoriti na preuzimanje i pokretanje izvršne datoteke crva. I dok su u prošlosti izvršne datoteke ovog zlonamjernog softvera dolazile u sklopu e-mail poruke kao privitak, danas se u e-mail porukama potencijalna žrtva samo upućuje na zlonamjernu stranicu s koje može preuzeti izvršnu datoteku crva. Osim slanja e-mail poruka, autori crva mogu slati i poruke na društvenim mrežama ili putem klijenata za trenutačnu razmjenu poruka.“ [preuzeto s CERT.hr, dostupno 11.7.2018. na https://www.cert.hr/crvi/]

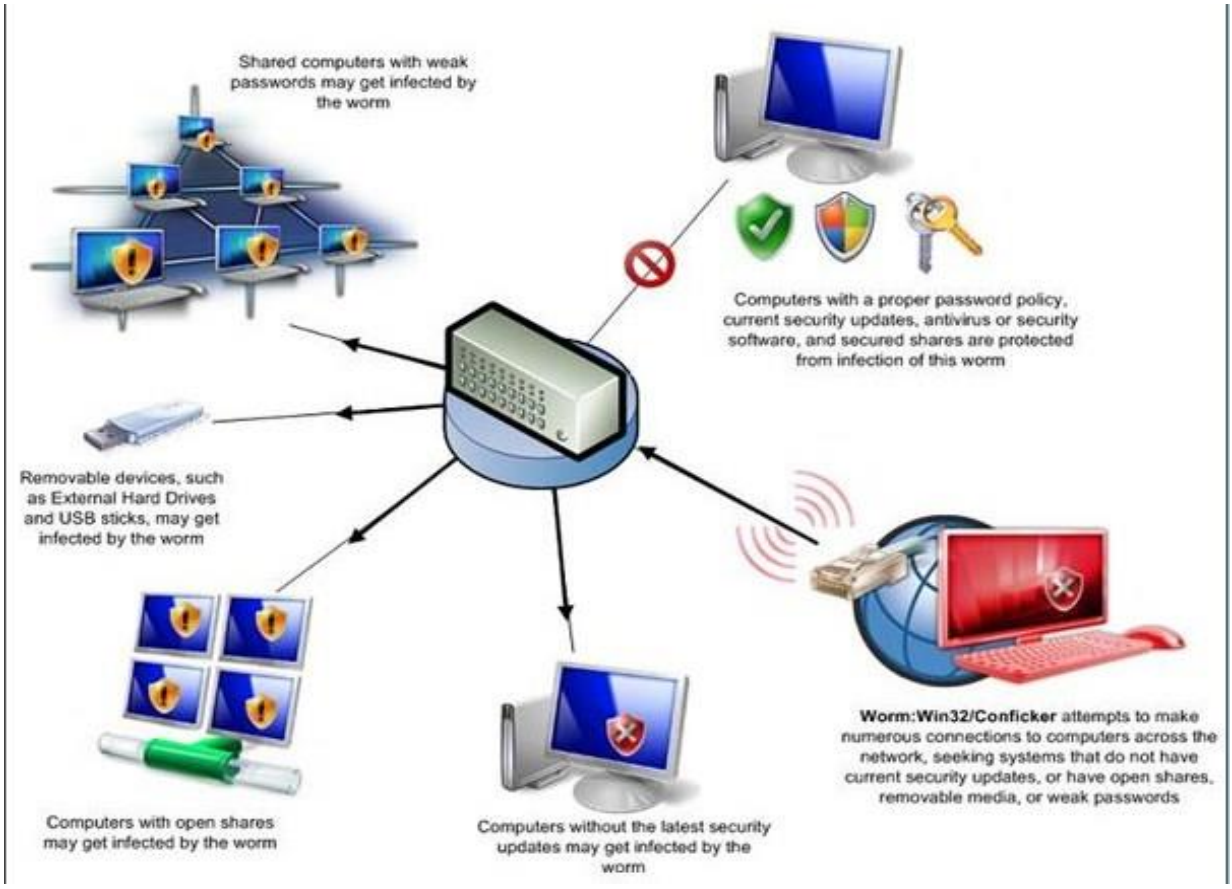
Crvi se sastoje od samokopirajućeg koda koji im omogućava razmnožavanje te od tereta (payload).

Podjela crva prema načinu djelovanja:

- Nepostojeći/nefunkcionalan – najčešći slučaj kod većine crva je upravo ovaj, kada ne postoji kod osim koda za širenje ili u njemu postoji nekakva pogreška pa nije funkcionalan
- Daljinska kontrola – otvara backdoor na žrtvinom računalu
- Sakupljači podataka – većina ljudi na računalu na kojem rade imaju osjetljive podatke. Crv može pretražiti disk računala u potrazi za tim podacima i zatim ih poslati na prije određeno mjesto
- Brisači podataka
- Spam relays – dio crva Sobig kreira mail relay koji spameri mogu koristiti da bi slali neželjenu elektroničku poštu. Većina internet providera ima sigurnosne mehanizme koji blokiraju spam sa poznatih IP adresa, ali kod zaraze ovim crvom spam dolazi sa svih strana i nemoguće je na taj način kontrolirati njegovo širenje
- HTML-proxyji – još jedna osobina crva Sobig je distribucija HTML-proxyja. Preusmjerujući web zahtjeve preko mnogo proxyja web stranice sa zabranjenim sadržajem dobivaju na vremenu jer providerima treba puna vremena da otkriju na kojoj se adresi web stranica fizički nalazi. Ovo se koristi za razne nelegalne aktivnosti, uključujući prijevare sa upisivanjem financijskih podataka ili brojeva kartica

Tipovi računalnih crva:

- Bot crv- služi za pretvaranje računala u zombije. Tim računalima se može upravljati preko „botneta“ (skup uređaja povezanih internetom (računala, serveri, mobilni uređaji) koji su zaraženi i kontrolirani od strane nekog tipa zloćudnog softvera).
- IM (instant messaging) crv- razmnožavaju se putem usluga razmjene i iskorištavaju pristup popisu kontakata na računalima žrtava
- E-mail crv- šire se tako da su zakvačeni za obične e-mail poruke
- Etički crv- računalni crv koji je dizajniran za širenje preko mreže s ciljem isporuke zakrpa za poznate sigurnosne ranjivosti sustava



Slika 2. Prikaz računalnih sustava koji mogu biti zaraženi od strane računalnog crva (Preuzeto s https://www.brighthub.com/computing/smb-security/articles/69204.aspx#imgn_0)

2.1.3. Trojanski konj

„Trojanski konji su programi koje hakeri, računalni crvi ili virusi i korisnici trajno instaliraju na ciljane sisteme. Kada se instalira, trojanski konj vraća informacije hakeru ili nudi direktan pristup računalu.“ [Matthew Strebe, Charles Perkins, „Firewalls-zaštita od hakera“, 2003., prvo izdanje]

Trojanski konj je jedan od oblika zlonamjernih računalnih programa koji se korisniku računala predstavlja lažno kao neki koristan softver kako bi ga korisnik instalirao na svoje računalo. Termin trojanski konj je preuzet iz grčke mitologije te se odnosi na priču o osvajanju grada Troje. Većina trojanskih konja ima vrlo slične nazive nekim korisničkim programima ili primamljivim aplikacijama. Razlika između trojanskog konja i crva i virusa je u tome što se trojanski konj ne može sam umnožavati. Trojanski konji se uglavnom koriste za krađu osobnih podataka, širenje drugih virusa ili za remećenje rada računala. Uz to hakeri ih

koriste i za dobivanje neovlaštenog pristupa zaraženom računalu, inficiranje nekih datoteka te nanošenje štete računalnom sustavu. Čim se trojanac infiltrira u računalo on se počinje skrivati svojoj žrtvi, a kako su vrlo slični pravim virusima vrlo ih je teško detektirati.

U slučajevima kada trojanski konj omogući napadaču potpunu kontrolu nad zaraženim računalom napadač može poduzeti iduće korake:

- Koristiti zaraženo računalo kao dio „Botnet“ mreže
- Ukrasti povjerljive informacije
- Instalirati druge oblike zlonamjernog softvera
- Slati, primati i modificirati datoteke zaraženog računala
- Pratiti (špijunirati) aktivnosti žrtve
- Koristiti memoriju (prostor) tvrdog diska
- Rušiti zaraženo računalo

Napadač i ne mora biti taj koji je zarazio računalo trojanskim konjem, nego može skeniranjem portova otkriti zaraženo računalo i onda iskoristiti trojanskog konja za ostvarivanje kontrole nad zaraženim računalom.

Što se tiče širenja trojanskih konja na računalo tu postoji nekoliko načina kako se oni infiltriraju u neko računalo. Trojanski konj se može proširiti na neko računalo preuzimanjem zaraženog softvera, kao dio softvera, kao e-mail privitak, putem zlonamjernih web stranica s dinamičkim sadržajem ili pak preko ranjivosti softvera.

2.1.4. Špijunski programi (spyware)

Špijunski programi su još jedna vrsta zloćudnog softvera. To je softver koji se može sam instalirati na računalo bez da vas pita za vaše dopuštenje za instalaciju. On ne traži nikakvu vašu suglasnost ili kontrolu da bi se instalirao. Njihova glavna namjena je da presreće vaš rad na računalu ili da djelomično preuzme kontrolu nad radom računala bez vaše dozvole. Sam naziv „Špijunski programi“ nam daju do znanja da je riječ o programima čiji je cilj nadgledanje rada korisnika na svom računalu. Ovi štetni programi iskorištavaju korisnikovo

računalo kako bi stekli korist za osobu koja je taj zloćudni program ubacili u žrtvin računalni sustav.

Špijunski programi se od crva i virusa razlikuju u tome što se ne repliciraju sami na zaraženom sustavu. Kao i većini zloćudnih programa, špijunski programi su dizajnirani kako bi iskoristili zaražena računala za komercijalnu dobit. Tipične radnje koje šijunski program izvršava su prikazivanje pop-up reklama, krađa osobnih informacija, praćenje aktivnosti na internetu. Još neke od najčešćih radnji koje izvršava špijunski program su:

- Prikupljanje informacija o kreditnim karticama
- Otkrivanje lozinki
- Otkrivanje PIN-a za kreditnu karticu
- Otkrivanje identitea
- Prosljeđivanje povjerljivih datoteka i podataka
- Prikaz reklama i pop-up prozora
- Instalacija nepoželjnih programa na zaraženo računalo
- Usporavanje rada računala

Najčešća podjela špijunskih programa je podjela u četiri kategorije. Prva kategorija su oglašivački program („adware“), zatim imamo programe za praćenje rada sustava, kolačiči („cookies“) za praćenje rada na mreži te trojanci. Jedna od poznatijih vrsta špijunskih programa su također i „keyloggers“ programi koji prepoznaju što korisnik zaraženog računala upisuje na tipkovnici te tako mogu ukrasti razna korisnička imena i lozinke.

Špijunski programi najčešće na žrtvino računalo dolaze sa neke web lokacije, putem CD-a ili DVD-a koji su zaraženi, sa vanjskog tvrdog diska ili nekog drugog prijenosnog medija. Također špijunski programi mogu doći na računalo i instaliranjem nekih programa koji se predstavljaju kao korisni za korisnikovo računalo, ali je njihova stvarna namjena da to računalo zaraze.

2.1.5. Oglašivački programi („adware“)

Oglašivački programi („adware“) predstavljaju programe koji prikazuju oglase na korisnikovom računalu. To su neželjeni štetni programi koji su dizajnirani kako bi bacali razne oglase i reklame po ekranu zaraženog računala. Uglavnom se to događa kada korisnik pretražuje sadržaj na nekoj web lokaciji. Neki oglašivački programi se mogu svrstati i u kategoriju špijunskih programa iz razloga što narušavaju privatnost korisnika. Na računalo obično dolaze tako da se predstavljaju kao neka vrsta korisnog programa ili se prikače za neki drugi program kako bi vas prevarili da ih instalirate na vaše računalo. Oglašivački programi vrijednost za hakera koji ih je pustio na vaše računalo generiraju tako da automatski prikazuju oglase na vašem ekranu. Vi tako vidite reklamu koju je onaj koji je stavio ovaj zlćudni program na vaše računalo i htio da vidite te time on dobiva korist.

Slijedi prikaz nekih od najčešćih znakova koji prikazuju da se oglašivački program nalazi na vašem računalu:

- Reklame se prikazuju na mjestima gdje se ne bi smjele prikazivati
- Početna stranica vašeg web preglednika se promjenila bez vašeg znanja i odobrenja
- Web stranice koje ste uglavnom posjećivali se ne prikazuju konako kako bi trebale
- Linkovi na neke web stranice vas preusmjeravaju tamo kamo ne bi trebali
- Vaš web preglednik se znatno usporio
- Na vašem web pregledniku su se pojavile nove alatne trake, proširenja i dodaci
- Web preglednik vam se nenadano ruši

2.1.6. Ucjenjivački softver („ransomware“)

Ucjenjivačji softver („ransomware“) je još jedna vrsta zlćudnog softvera. Ova vrsta softvera korisniku uskraćuje pristup njegovom računalu te traži plaćanje „otkupnine“ kako bi korisnik tog računala mogao ponovo dobiti pristup svim dijelovima računalnog sustava. Jedan od oblika ucjenjivačkog softvera kriptira datoteke, dok drugi zaključaju sustav računala. Nakon što je sustav zaključan i korisnik računala nema pristup na ekranu se prikazuje poruka koja korisnika nagovara na plaćanje „otkupnine“.

Jedan od poznatijih primjera je „CryptoLocker“ koji se pojavio u rujnu 2013. godine. To je ustvari računalni crv koji generira par ključeva te kriptira sve datoteke određenog tipa (tekstualne datoteke, slike itd.). Nakon toga korisnik dobiva poruku da mora uplatiti određeni iznos novca na račun onoga koji je ubacio ucjenjivački softver na njegovo računalo ili će u suprotnom biti izbrisan privatni ključ bez kojeg se kriptirane datoteke neće moći koristiti.

Slika 3. Prikaz poruke koju šalje ucjenjivački softver nakon što zarazi žrtvin računalni sustav (Preuzeto s http://www.amchamvietnam.com/ctb-locker-crypto-malware-ransomware-in-vietnam/)

2.2. Denial of Service napadi (DoS napadi)

DoS napadi su napadi koji uskraćuju neku uslugu za korisnika na računalu kao što im i sam naziv govori. Ti napadi za cilj imaju učiniti računalo ili računalnu mrežu nedostupnima za korisnika nekog računalnog sustava. Tipičan oblik napada kod DoS napada na sustav je taj da napadači preplavljuju računalni sustav žrtve sa velikim brojem poruka, zahtjeva i informacija kako bi preopteretili sustav i prouzročili pad sustava. Time se onemogućava korisnika računala da koristi usluge tog računala kako ih je prije napada mogao koristiti.

DoS napadima se najčešće napadaju web serveri banaka, medijskih kuća, vladinih institucija ili internet trgovina. Također napadi se vrše na DNS („Domain Name System“) infrastrukturu i servise elektronske pošte. DoS napadi uglavnom uzrokuju probelme koji se odonose na to da usluge postanu neučinkovite, nedostupne, uzrokuju prekid mrežnog prometa ili probleme s konekcijom.

Ovi napadi predstavljaju pokušaje jedne osobe (napadača) da zrokuje napad na računalni sustav njegove žrtve s ciljem da mu onemogući pružanje usluga njegovog računalnog sustava. Ti napadi se izvršavaju s jedne lokacije. Također uz normalne DoS napade postoje i DDoS („Distributed Denial of Service) napadi. Za DDoS napade je karakteristično da se napadi izvršavaju sa više različitih lokacija. Dakle glavna razlika između DoS napada i DDoS napada je u tome što se DoS napadi na žrtvin sustav vrše s jedne lokacije dok se DDoS napadi vrše sa više različitih lokacija odjednom sinkronizirano kako bi se žrtvin računalni sustav što bolje opteretio napadima.

Tipične vrste DoS napada koje će biti detaljnije opisane su:

- Ping of Death („smrtonosni ping“)
- Teardrop („kap suze“)
- UDP flood
- SYN flood
- Prizemljenje
- Smurf
- Fraggle
- E-mail bombe
- Zlonamjerno formirane poruke

2.2.1. Ping of Death („smrtonosni ping“)

Ping of Death predstavlja jedan od poznatijih DoS napada. Kod ovog oblika napada iskorištava se greška u implementaciji TCP/IP protokola. Temelji se na nemogućnosti obrade ping paketa koji je veći od najveće dopuštene veličine paketa unutar IPv4 definicije. Ukoliko je došlo do primitka paketa većeg od dozvoljenog kod starijih operacijskih sustava to je uzrokovalo pojavu „Blue Screen of Death“ (plavi ekran smrti) zajedno s prijavom o

nemogućnosti nastavka rada. Kada veličina zaglavlja i dijela za podatke prekorači maksimum koji je dozvoljen i definiran u TCP/IP specifikaciji, tada implementacija TCP/IP-a može otkazati zbog grešaka nastalih u alociranju memorije.

Obrana od ovakve vrste napada je da se ne dozvoli paketima većima od dozvoljene veličine prolazak kroz vatrozid. Ova vrsta DoS napada je zastarjela i u današnje vrijeme svi operacijski sustavi imaju uključenu zaštitu od napada smrtonosnim pingom.

2.2.2. Teardrop (kap suze)

Kod slanja velikih IP paketa mrežom oni se dijele na fragmente koji se na kraju veze opet spajaju. U fragmente paketa upisuje se udaljenost od početka prvog paketa, što omogućuje ponovno sastavljanje paketa na drugoj strani. Teardrop napad predstavlja napad koji uključuje slanje oštećenih IP fragmenata s preklapanjem na ciljano računalo. Ukoliko napadač u neki od fragmenata postavi neodgovarajuću udaljenost to će dovesti do pada sustava.

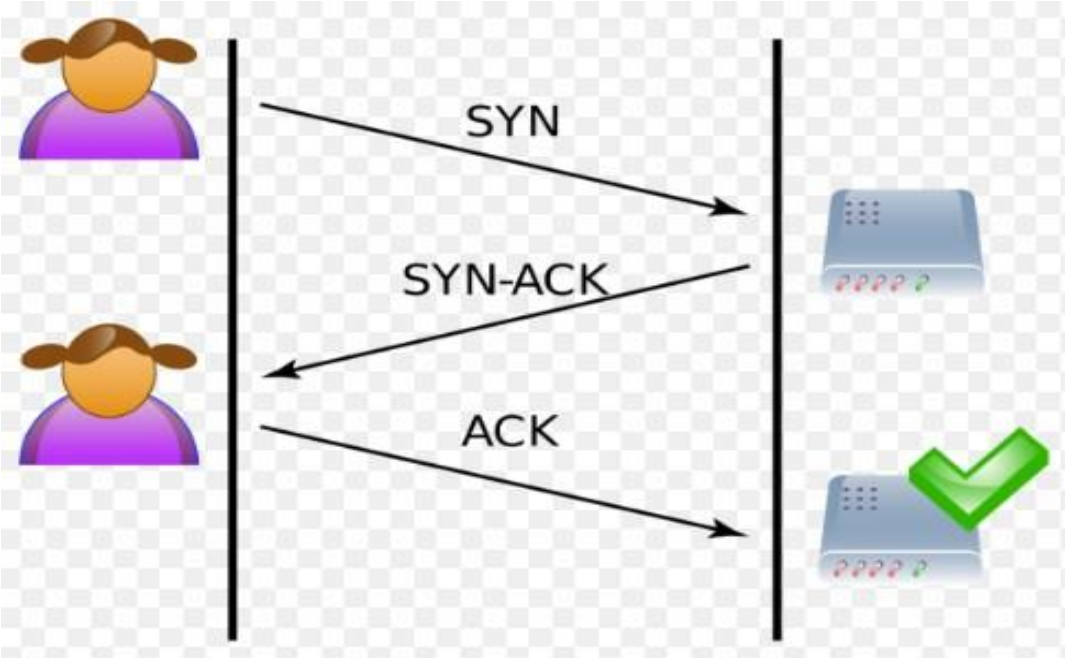
Kao obrana od ovakve vrste napada bitno je koristiti najažurnije zakrpe za sustav te postavljanje vatrozida tako da ponovo sasatavlja pakete.

2.2.3. SYN flood

Ovdje je prvo važno reći ćemu služi TCP protokol. TCP (Transmission Control Protocol) protokol se brine o razmjeni podataka mrežom koji osigurava pouzdanu isporuku od izvora podataka do odredišta. Klijent i poslužitelj razmjenjuju poruke prema idućem redosljedu:

1. Klijent šalje poslužitelju SYN (synchronize) poruku poslužitelju kojom zahtjeva vezu
2. Poslužitelj odgovara i potvrđuje vezu slanjem SYN-ACK (acknowledge) poruke klijentu
3. Klijent potvrđuje da je veza ostvarena slanjem povratne ACK poruke

Slijedi i grafički prikaz ostvarivanja veze.



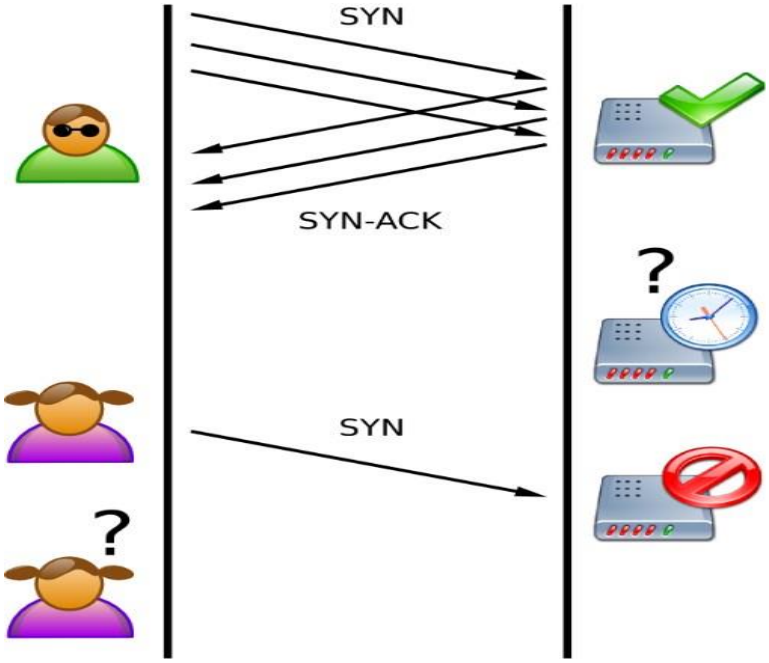
Slika 4. Uspostava veze između klijenta i poslužitelja

(Preuzeto s https://upload.wikimedia.org/wikipedia/commons/8/8c/Tcp_normal.png)

Ovakva vrsta uspostavljanja veze između poslužitelja i klijenta se naziva TCP „three-way handshake“.

Ranjivost se temelji na dužnosti poslužitelja da zadrži i registrira sve SYN zahtjeve te ih drži u memoriji dok se ne ispuni konekcija. Napadač koristi to saznanje tako da šalje, s lažirane adrese ili s drugih računala više SYN zahtjeva na koje dobiva odgovor u obliku SYN-ACK poruke, ali nikad ne odgovara na istu s ACK zahtjevom prisiljavajući poslužitelja da zadržava takve poluotvorene veze u memoriji. Kako poslužitelj ne zna razliku između legitimnih i lažnih SYN poruka, nakon što iskoristi sve memorijske resurse za poluotvorene veze kojima je pretrpan poslužitelj više nije u mogućnosti obraditi nove legitimne SYN poruke i time je uskraćeno davanje usluga legitimnim korisnicima.

Sljedeća slika daje prikaza kako napadač s lažnog izvora šalje SYN poruku prema poslužitelju te poslužitelj vraća SYN-ACK poruku no nikad ne dobiva ACK poruku natrag. Time legitimni klijenti ostaju uskraćeni za usluge od strane poslužitelja jer poslužitelj postane prenatrpan lažnim SYN porukama. Kada legitimni klijent pošalje poslužitelju SYN poruku u želji da uspostavi vezu sa poslužiteljem on ne dobije povratnu poruku.



Slika 5. Prikaz kako radi SYN flood napad

(Preuzeto s https://upload.wikimedia.org/wikipedia/commons/9/94/Tcp_synflood.png)

Obrana od ovakve vrste napada je dobar vatrozid koji može prepoznati karakteristike napada. Vatrozid može prepoznati identične pokušaje konekcije sa iste IP adrese te filtrirati sve sljedeće pokušaje konekcije na poslužitelj sa te IP adrese.

2.2.4. UDP flood

UDP protokol se nalazi u transportnoj razini OSI modela te uz TCP predstavlja jedan od temeljnih internet protokola. UDP je nekonekcijski orijentiran protokol. Nema kontrolu razmjene podataka, te je pogodan za komunikacije gdje su greške dozvoljene (prijenos video materijala). Također nema ni mogućnost provjere primitka poruke jer ne čuva informacije o stanju veze.

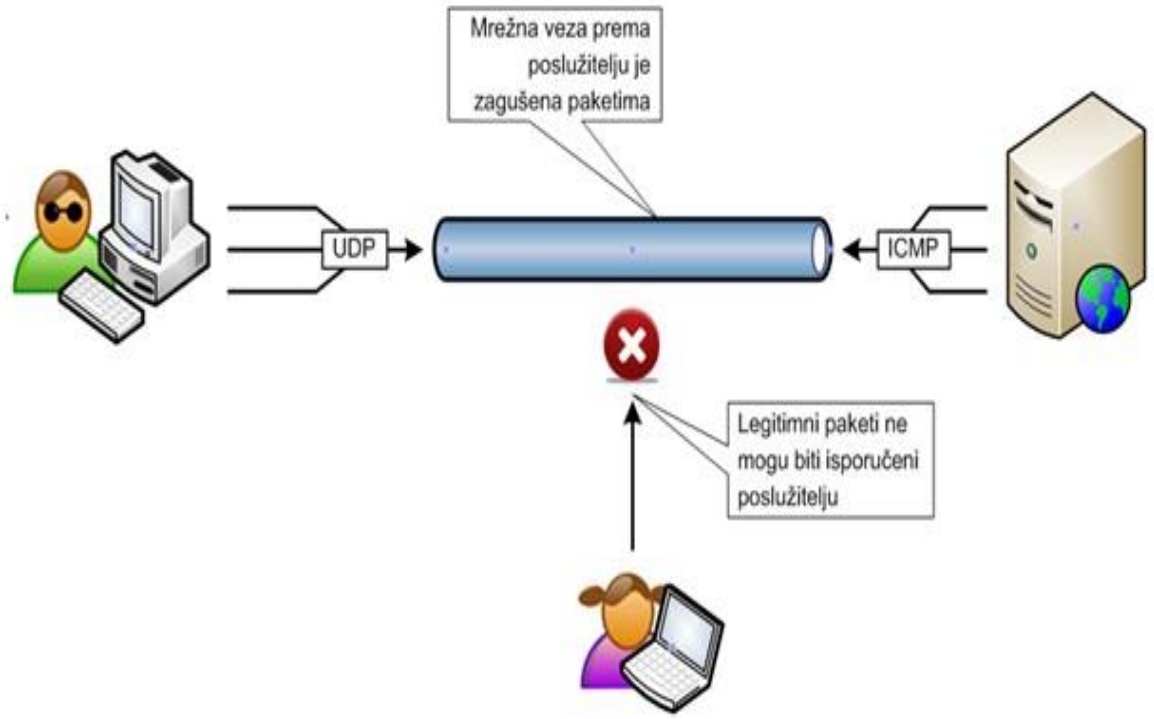
Kao što se može vidjeti UDP protokol ne osigurava nikakvu isporuku niti očekuje uspostavljanje veze putem potvrde (SYN, SYN-ACK, ACK), te iz toga proizlazi njegova ranjivost koju napadači koriste. Napadi se temelje na tome da napadači šalju velik broj UDP

paketa na slučajno odabrane portove računalnog sustava. Nakon što poslužitelj primi poruke on će uraditi sljedeće tri stvari:

1. Provjerit će koja aplikacija osluškuje na odabranom portu
2. Nakon toga poslužitelj shvaća da takve aplikacije nema
3. Na zahtjev koji je poslan odgovara ICMP (Internet Control Message Protocol) Destination Unreachable paketom - ovaj paket sadrži poruku da destinacija nije dostupna

Kako je na poslužitelj poslan velik broj lažnih UDP paketa, opisanim načinom obrade poslužitelj ustvari sam sebi zagušuje konekciju odgovaranjem na taj veliki broj lažnih UDP paketa.

Sljedeća slika će prikazati kako napadači šalju lažne UDP pakete, a poslužitelj na njih odgovara ICMP paketom da destinacija nije dostupna. Time se zagušuje konekcija te legitimni paketi od strane legitimnih korisnika ne mogu doći do poslužitelja.



Slika 6. Prikaz UDP flood napada

(Preuzeto s https://www.cis.hr/WikiIS/doku.php?id=dos_attacks)

2.2.5. Prizemljenje

Kod ove vrste DoS napada poslužitelju se šalje specijalno kreiran SYN paket. Radi se o tome da su izvorišna i destinacijska adresa tog SYN paketa ustvari IP adresa poslužitelja. Ovako poslan SYN paket na poslužitelja uzrokuje to da poslužitelj šalje SYN-ACK pakete na vlastitu IP adresu, kao i sljedeće ACK pakete što dovodi do uspostavljanja prazne konekcije. Svaka od konekcija će ostati uspostavljena dok je server ne prekine zbog neaktivnosti. Ovakva vrsta napada je poprilično zastarjela, a dovodila je do usporavanja operacijskog sustava ili do njegovog pada. Ipak u današnje vrijeme ovakvih napada više gotovo da i nema jer su proizvođači operacisjkih sustava ugradili obrane od ovakvih vrsta napada u sam sustav.

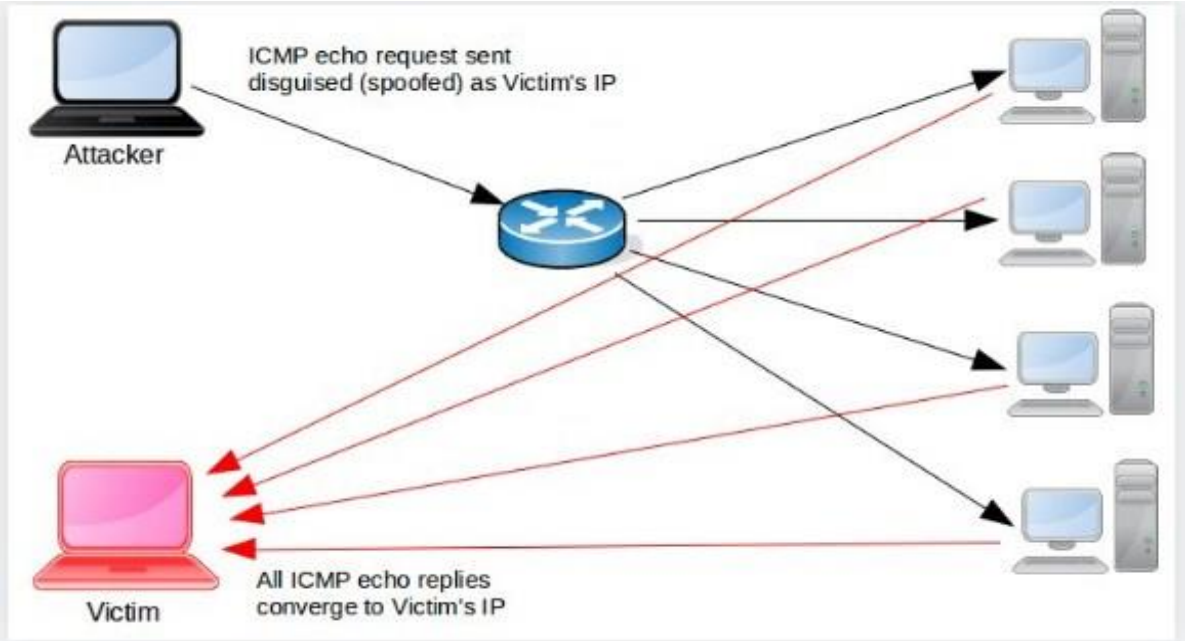
I dobra konfiguracija vatrozida također odbija ovakve vrste napada.

2.2.6. Smurf napad

Smurf napad se temelji na krivo postavljenim mrežnim uređajima. Ova vrsta napada započinje tako da napadač najprije šalje na usmjerivač velik broj ICMP echo zahtjeva (ping) s time da je adresa pošiljatelja izmijenjena tako da napadač umjesto svoje IP adrese postavi IP adresu žrtve koju napada. Nakon toga usmjerivač odašilje ICMP echo zahtjeve na cijelu podmrežu i sva računala na mreži odgovaraju na te zahtjeve. Time se zagušuje računalo žrtve i onemogućuje mu se normalan rad. U današnje vrijeme ovi napadi rijetko uspjevaju jer je zaštita od njih postala standardna postavka usmjerivača.

Također da bi se spriječila ovakva vrsta napada na mrežu moguće je isključiti na usmjerivaču ili vatrozidu osobine adresiranja javnog emitiranja. Vatrozid je potrebno konfigurirati tako da odbacuje ICMP pakete ukoliko ne želimo biti žrtva Smurf napada.

Na sljedećoj slici će biti prikazano kako funkcionira Smurf napada. Vidi se kako napadač šalje ICMP echo zahtjev sa žrtvinom IP adresom na usmjerivač te nakon toga ostala računala u mreži šalju odgovore na žrtvinu adresu i time zagušuju promet.



Slika 7. Prikaz Smurf napada

(Preuzeto s https://bobcares.com/blog/how-to-configure-firewall-in-linux-servers/4/)

2.2.7. Fraggle napad

Fraggle napad je u stvari jednostavna modifikacija Smurf napada. Kod Fraggle napada se umjesto IMPC echo poruka koriste UDP echo poruke. Koristi se UDP umjesto TCP protokola. Ovo mu dozvoljava to da napad prođe kroz vatrozidove koji filtriraju ICMP pakete.

Obrana od ovakve vrste napada je da se na vatrozidu postavi da se filtriraju UDP echo poruke.

2.2.8. E-mail bombe

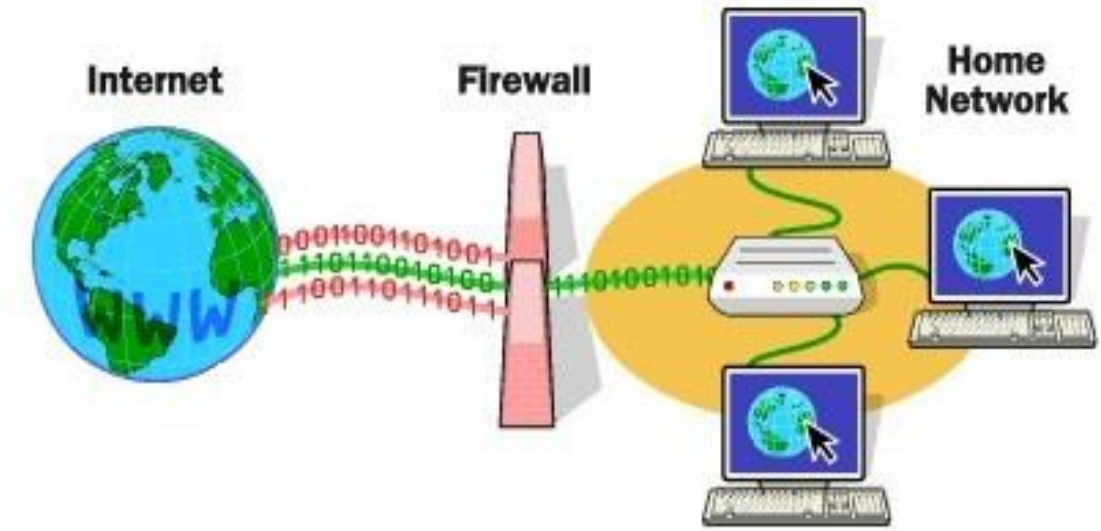
Osobina ove vrste napada je da napadač postavi računalo da neprestano šalje e-mail poruke na istu adresu. Time napadač može preopteretiti propusnost na mreži žrtve. Ova vrsta napada je dosta zastarjela i obrana od njega je laka. Ovakvi napadi gotovo da se više i ne koriste.

3. Vatrozid

Razvoj interneta je omogućio velikom broju korisnika da pristupaju mreži i time svoje podatke izlažu opasnostima koje prijete sa svih strana. U prethodnom dijelu rada opisane su razne vrste napada koje izvršavaju napadači od računalnih virusa i crva do raznih DoS napada. Kako bi se ti napadi izbjegli izrađen je sustav pod nazivom vatrozid koji spriječava razne vrste napada koji prijete na računalnoj mreži.

Vatrozid predstavlja kombinaciju hardvera i softvera koji kontrolira komunikaciju između računalnih mreža. To je sustav preko kojeg se odvija prijenos podataka u neku mrežu i iz te mreže. Vatrozid predstavlja sustav koji može biti postavljen na računalo koje ima ulogu vrata koja povezuju računalnu mrežu neke tvrtke ili institucije, sa globalnom mrežom Internet. U tom slučaju vatrozid ima ulogu vratara koji dozvoljava da se neki podaci prenose u mrežu ili iz nje dok druge podatke blokira. Vatrozid također može biti postavljen i na osobno računalo te u tom slučaju on ima zadatak propuštati podatke s Interneta na to računalo i s tog računala na Internet.

Na sljedećoj slici je prikazan grafički prikaz kako vatrozid funkcionira. Na slici se vidi kako sav promet između klijenta i Interneta kontrolira vatrozid.



Slika 8. Prikaz funkcije Vatrozida na mreži

(Preuzeto s https://www.comodo.com/resources/home/how-firewalls-work.php)

Možemo reći da vatrozidovi filtriraju tokove podataka koji ulaze u zaštićenu mreže i one koji izlaze iz te mreže. Mreža neke tvrtke uglavnom sadrži jedan usmjerivač koji se naziva vrata (gateway). Ta vrata povezuju mrežu tvrtke sa nekim rubnim usmjerivačem globalne mreže Internet. Tako sav promet koji ulazi i izlazi iz zaštićene mreže prolazi kroz vrata. Vatrozid kao softverski sustav se nalazi na tim vratima te izvodi filtriranje prometa kroz mrežu. Pod pojmom filtriranja misli se na to da vatrozid neke pakete pušta da uđu u mrežu ili izađu iz nje dok drugim paketima to ne dozvoljava. Na temelju pravila filtriranja koja definira administrator mreže i postavlja ih na vatrozidu, vatrozid odlučuje koje će pakete propustiti, a koje neće. Administrator pravila rada vatrozida određuje u skladu sa željama vlasnika mreže koju bi taj vatrozid trebao štititi.

Pravila definirana na vatrozidu bi trebala biti postavljena tako da vatrozid propušta ili odbacuje određene zahtjeve za uspostavu veze između vanjske mreže i klijenata na mreži koju taj vatrozid štiti. Također definirana pravila trebaju raditi i u obrnutom slučaju što znači da vatrozid treba propuštati i odbacivati zahtjeve za uspostavu veze koji dolaze od korisnika u zaštičenoj mreži prema adresama izvan te mreže.

Da bi vatrozid radio onako kako treba potrebno je dobro postaviti vrijednosti u tablicama vatrozida u kojima se zapisuju pravila prema kojima se određuje kako bi vatrozid trebao funkcionirati. Kao što se može vidjeti uloga vatrozida je da spriječava ili dopušta uspostavljanje određenih veza i određene tokove podataka prema pravilima koja su zapisana u njegovim tablicama. Posao oblikovanja pravila i njihov upis u tablice izvršava administrator mreže.

Za rad vatrozida postoji nekoliko karakterističnih stvari.

- Sav promet između štićene mreže i vanjske mreže treba prolaziti preko vatrozida. Da bi zaštita mreže bila uspješna bitno je da sav promet u nju i iz nje prolazi kroz barem jedan vatrozid koji ju štiti.
- Potrebno je postavljanje pravila na vatrozidu od strane administratora koja određuju adrese, vrste prijenosa i vrste sadržaja onih tokova podataka koji smiju ući u zaštičenu mrežu i onih koji smiju izaći iz zaštićene mreže. Sve ostale tokove podataka u štićenu mrežu i iz nje vatrozid treba spriječavati.
- Vatrozid bi trebao biti dobro zaštićen od svih vrsta napada. On je jedan od dijelova mreže te je time izložen svim vrstama mrežnih napada. Kako bi mogao štiti mrežu za

koju je postavljen da ju štiti vatrozid prvo treba zaštititi samog sebe od vanjskih napda koji mogu opteretiti njegov rad i tako ga učiniti beskorisnim ili čak štetnim.

- Vatrozid također ima ulogu zaštite bežične mreže. On blokira zločudne pokušaje upada na neko računalo žrtve putem bežične mreže. Kada napadač želi ući u žrtvin sustav, žrtvi iskače upozorenje i time joj omogućuje da reagira i blokira napad.
- Jedna od karakteristika vatrozida je da omogućava virtualno privatno umrežavanje (VPN). VPN se koristi kako bi se promet između dvije mreže odvijao sigurno, obično preko interneta. Iako VPN nije jedna od glavnih karakteristika vatrozida, vatrozidi nekih proizvođača nude VPN servise.
- Ovisno o postavkama neki vatrozidi pretražuju dolazne podatke kako bi otkrili viruse i ostale tipove zločudnih programa u njima.

3.1. Tipovi vatrozida

Kada govorimo o tipovima vatrozida oni se najčešće kategoriziraju u tri kategorije. To su tradicionalni filtri paketa (traditional packet filters), filtri paketa prema stanjima (stateful packet filters) i vrata aplikacija (application gateways).

3.1.1. Tradicionalni filtri paketa

Filtri ove vrste promatraju svaki IP paket zasebno. Na temelju pravila vatrozid odlučuje za svaki paket da li ga treba propustiti ili odbaciti. Svaki IP paket vatrozid procesira zasebno, neovisno od drugih paketa.

Odluka o tome kako će se filtrirati paketi određuje se na temelju sljedećih atributa IP paketa:

- IP adresa izvora ili odredišta – ukoliko postoji nepoželjna adresa izvora ili odredišta IP paketa na temelju toga se kreira pravilo prema kojem vatrozid ili propušta ili odbacuje pakete
- Sadržaj polja „Protokol“ koje se nalazi u zaglavlju IP paketa – sadržaj tog polja je broj koji označava neki od protokola (TCP, UDP, ICMP, OSPF). Kod ovakvog filtriranja

vatrozid može odbacivati neke pakete koji prenose segmente nekih protokola. To se radi zato što vlasnik štićene mreže ne želi komunikaciju ni uspostavu veza u kojima se određeni protokoli koriste.

- Ulazni i izlazni port u zaglavlju segmenta kojeg prenosi IP paket – kada se uspostavlja veza sa nekim serverom, segment koji sadrži zahtjev za uspostavu veze ima u zaglavlju zapisan port tog servera. Taj port obično pokazuje koja aplikacija hoće uspostaviti vezu. Kod ovakvog slučaja vatrozidom se može zabraniti nekim aplikacijama da pristupaju štićenoj mreži ili nekim njenim dijelovima.
- TCP bitovne oznake – to su SYN, ACK i druge bitovne oznake te se na temelju stanja tih bitovnih oznaka može spriječiti uspostava neke TCP veze uz pomoć vatrozida
- Tip ICMP poruke – kako IP protokol ne nudi ispravku greške koje nastaju kod prijenosa IP paketa uz IP protokol na mrežnoj razini se nalazi i ICMP protokol čija je uloga da evidentira gubitke IP paketa u prijenosu i šalje obavijest izvorima čiji su paketi izgubljeni. No bez obzira što postoje ove obavijesti IP protokol ne ispravlja greške u prijenosu paketa nego to radi TCP protokol. Međutim poruke ICMP protokola se mogu koristiti za neke vrste napada koji su navedeni ranije u radu. Iz tog razloga vatrozid bi trebao filtrirati poruke ove vrste.
- Različita pravila za datagrame koji ulaze ili napuštaju mrežu
- Razčičita pravila za različita sučelja usmjerivača

Na temelju gore navedenih atributa i drugih parametara te prema tome kakvi su stavovi organizacije administrator mreže postavlja pravila na vatrozidu. Ta pravila određuju koji će se paketi propuštati, a koji odbacivati. Kod postavljanja vatrozida u obzir se uzimaju produktivnost korisnika (radnika) i upotreba propusnosti kao i sigurnosna pitanja organizacije, dakle pravila na vatrozidu se formiraju prema stavovima tvrtke i njenim ciljevima. Stav tvrtke na primjer može biti da onemogući djelatnicima da igraju on-line igrice kojima bi gubili vrijeme, ili odlazak na stranice društvenih mreža. Također tvrtka želi visok stupanj zaštite svoje mreže od vanjskih napada. Može se zabraniti i slušanje radia preko interneta i slično. Ukoliko pak tvrtka ne želi da njezina interna mreža bude mapirana od strane „autsajdera“, može se blokirati sve ICMP TTL istekle poruke koje napuštaju mrežu organizacije. Prikaz koji pokazuje kako se postavlja vatrozid u odnosu na politiku tvrtke je prikazan u tablici Tablica 1. koja slijedi.

Politika tvrtke	Postavke vatrozida
Ne dopušta se pristup vanjskim Web sadržajima.	Odbaciti sve odlazne pakete na bilo koju IP adresu ako nose segment sa brojem porta 80 (port na kojem web serveri prihvaćaju dolazeće zahtjeve web preglednika).
Ne smiju se uspostavljati TCP veze koje dolaze izvana, osim onih koje vode na javni web server tvrtke.	Odbaciti sve dolazne TCP SYN pakete do bilo koje IP adrese osim na IP adresu 130.207.244.203., port 80.
Spriječavanje Web-radia da zaguši propusnost unutarnje mreže.	Treba odbaciti sve dolazne UDP pakete osim DNS paketa.
Treba zaštititi vlastitu mrežu da ne bi bila iskorištena za objašnjeni Smurf DoS napad.	Odbaciti sve ICMP ping pakete koji idu na „broadcast“ adresu (primjer 130.207.255.255).
Zaštititi vlastitu mrežu da ne bude mapirana (tracerouted).	Odbaciti sav odlazni ICMP TTL istekli promet.

Tablica 1. Prikaz postavki pravila na vatrozidu u odnosu na politiku tvrtke

Za filtiranje prometa na vatrozidu također su pogodne i bitovne oznake koje se nalaze u zaglavlju segmenata koji se prenose u IP paketima. To funkcionira tako da na temelju vrijednosti ACK bita u zaglavlju segmenta vatrozid može dopustiti uspostavu TCP veze sa serverom ili pak spriječiti uspostavu TCP veze. Kada se uspostavlja TCP veza u segementu sa kojim klijent traži uspostavljanje veze (prvi segment) vrijednost ACK bita je 0. Sa tim segmentom se nema što potvrditi jer je to segment sa kojim počinje uspostava veze. Što se tiče svih ostalih segmenata, vrijednost ACK bita je 1 čime se potvrđuje primitak segmenta. Ako se na vatrozidu postavi pravilo da odbacuje IP pakete koji dolaze izvana i nose TCP segment u kojem je ACK bit 0, tada nijedan vanjski klijent neće moći uspostaviti TCP vezu ni sa jednim serverom u štićenoj mreži. Ako se pak postavkama na vatrozidu dopusti korisnicima koji se nalaze u štićenoj mreži da šalju TCP segmente s ACK bitom 0 prema vanjskoj mreži time se unutarnjim korisnicima dopušta da šalju zahtjeve za uspostavu TCP veze prema vanjskim serverima. Vanjski serveri time mogu slati unutarnjim korisnicima željene podatke jer vatrozid odbacuje samo vanjske segmente koji imaju ACK bit s vrijednosti 0, a odgovori servera imaju uvijek ACK bit s vrijednosti 1.

Opisana pravila se vatrozidu zadaju pomoću tablica koje se zovu „lista za kontorlu pristupa za sučelje usmjerivača“ (An access control list for a router interface). U svakom retku tablice nalaze se zapisi pravila koja se postavljaju na vatrozidu. Slijedi tabelarni prikaz u tablici Tablica 2. s primjerima nekih pravila.

Akcija	Izvorišna adresa	Odredišna adresa	Protokol	Port izvora	Port odredišta	Bitovna oznaka
Propusti	222.22/16	Izvan 222.22/16	TCP	>1023	80	Bilo koja
Propusti	Izvan 222.22/16	222.22/16	TCP	80	>1023	ACK
Propusti	222.22/16	Izvan 222.22/16	UDP	>1023	53	-
Propusti	Izvan 222.22/16	222.22/16	UDP	53	>1023	-
Odbaci	Sve	Sve	Svi	Svi	Svi	Sve

Tablica 2. Lista za kontrolu pristupa za sučelje usmjerivača

(Podaci u tablici su preuzeti iz knjige Computer Networking: A Top-Down Approach, Kurose F. James i Ross W. Keith)

Ovakva tablica može imati mnogo redaka ovisno o tome kakva je politika tvrtke i što žele od strane vatrozida.

Prva dva pravila u ovoj tablici dopuštaju korisnicima koji se nalaze u štićenoj mreži da gledaju web stranice na cijelom internetu, dok pak sprječavaju one izvan štićene mreže da uspostavljaju TCP veze sa serverima unutar štićene mreže. Pravilo koje se odnosi na prvi redak tablice omogućava da se iz štićene mreže uspostavi TCP veza sa portom 80. Drugo pravilo vanjskom web serveru (port izvora 80) dopušta da šalje TCP segmente korisniku unutar štićene mreže s time da ti TCP segmenti moraju imati postavljen bit ACK na vrijednost 1 što znači da nose odgovor na neki zahtjev korisnika iz unutarnje mreže. Ovim pravilom se također ne dopušta da vanjski korisnici šalju zahtjeve za uspostavu TCP veze prema serverima u štićenoj mreži.

Druga dva retka u tablici se odnose na pravila koja dopuštaju DNS paketima (port 53) da ulaze u štićenu mrežu te da iz nje izlaze prema van.

Što se tiče primjene pravila prema datoj tablici ta pravila se primjenjuju odozgo prema dolje. Što se tiče IP paketa za koje prva četiri pravila ne vrijede njih se procesira prema petom pravilu što znači da ih se odbacuje. To znači da vatrozid sve te ostale iP pakete sprječava da uđu u štićenu mrežu ili da iz nje izađu.

Ovakav način rada ima i slabosti te dopušta neke jednostavne oblike napada. Ukoliko napadač pošalje IP paket sa TCP segmentom gdje je port izvorišta 80 i bit ACK je vrijednosti 1 tada vatrozid koji radi kao tradicionalni filter paketa propustiti taj paket jer prema navedenim pravilima u tablici ne postoji razlog da se taj paket odbaci. Time napadač u štićenu mrežu može učiniti štetu za unutarnju mrežu slanjem zločudnog programa u nju.

3.1.2. Filtri paketa prema stanjima

Što se tiče ove vrste vatrozida ona radi na sličan način kao i tradicionalni filtri paketa s time da imaju dodanu još jednu dimenziju u filtriranju paketa. Ovaj tip vatrozida održava i konzultira tablicu TCP veza koje se uspostavljaju i odvijaju preko njega. Kao što sam naziv ove vrste vatrozida govori oni pored tablice za kontrolu pristupa (Tablica 2.) promatraju i stanje TCP veza. Primjer jedne tablice sa stanjem veza je prikazan na slici slika 9. koja slijedi.

Source IP	Source Port	Destination IP	Destination Port	Connection State
10.1.1.100	1022	193.145.85.201	80	Established
10.1.1.102	1040	193.145.85.1	80	Established
10.1.1.110	1035	193.145.85.117	23	Established
192.145.85.20	1080	10.1.1.210	25	Established

Slika 9. Prikaz tablice stanja veza

(Preuzeto s https://www.slideshare.net/souviksantra/internetworking-with-pix-firewall)

Dakle ovaj tip vatrozida za svaki IP paket pojedinačno odlučuje što s njim učiniti, ali odluke ne donosi samo na temelju pravila danih u tablici sa listom za kontrolu pristupa (Tablica 2.) nego promatra i stanje TCP veza. Napad koji je opisan iznad, ova vrsta vatrozida može

spriječiti. Vatrozid koji radi kao filtar IP paketa s uvidom u stanje TCP veza, ne dopušta da u štićenu mrežu uđe IP paket koji nosi TCP segment sa ACK bitom 1, ako IP adresa odredišta toga paketa (u štićenoj mreži) nije ujedno adresa domaćina koji je pokrenuo proces uspostavljanja te TCP veze. Na ovaj način vatrozid ne dopušta da napadač šalje svoje TCP segmente na IP adrese u štićenoj mreži.

Kao što se može vidjeti ova vrsta vatrozida je slična kao i tradicionalni filtri paketa, ali je malo kvalitetnija u obrani mreže iz razloga što uz tablicu s listom pravila za kontrolu pristupa u obzir uzima i tablicu u kojoj se vodi evidencija o TCP vezama koje prolaze preko njega. Uvid u stanje veza olakšava vatrozidu da spriječi neke napade na štićenu mrežu koje pravila sa liste za kontrolu pristupa ne bi spriječila.

3.1.3. Vrata aplikacija (proxy server)

Treći tip vatrozida je vatrozid naziva vrata aplikacija koji omogućava da se filtriranje definira kvalitetnije i preciznije. Vatrozid ovog tipa nadzire i ograničava prijenos sadržaja u štićenu mrežu i iz nje na razini pojedinačnih aplikacija i pojedinačnih korisnika. Primjer bi bio da vatrozid ovog tipa dupušta korištenje usluge Telnet(*mrežni protokol koji se koristi da osigura korisniku jednog računala sesiju za korištenje sučelja komandne linije na drugom računalu*) preko granice štićene mreže samo određenim osobama iz te mreže. Ovaj tip vatrozida radi na sedmom sloju OSI modela (aplikacijski sloj) kao što mu i samo ime govori. Za svaku aplikaciju može se napraviti vatrozid tipa vrata aplikacije. Tako sav promet iz štićene mreže i u nju kojeg ostvaruje određena aplikacija prolazi kroz vrata te aplikacije. Vrata za razne aplikacije mogu raditi na istom računalu, ali svaka vrata aplikacije su zaseban vatrozid za jednu vrstu aplikacije. Ovakav tip vatrozid uglavnom je dopuna uz klasične vatrozide koji rade kao filtri paketa.

Ovaj tip vatrozida radi kao proxy server. To znači da se komunikacija između klijenta unutar štićene mreže i vanjskog web servera odvija u nekoliko korak, a sva komunikacija prolazi preko proxy servera. Ovaj proces komunikacije između klijenta u štićenoj mreži i vanjskog web servera će biti prikazana u četiri osnovna koraka prema kojima proxy server funkcionira:

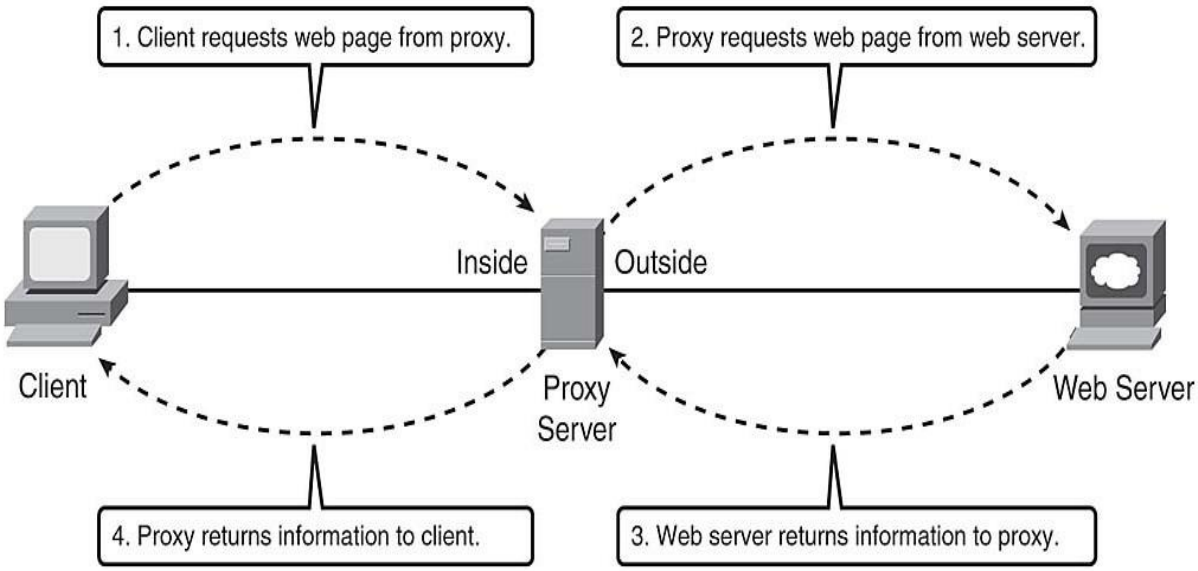
1. Klijent iz štićene mreže zatraži uspostavu veze sa web serverom koji se nalazi izvan te mreže.
2. Zatim proxy server prihvaća taj zahtjev i prosljeđuje ga prema odgovarajućem web sereveru.
3. Web server prima zahtjev od proxy servera i odgovara na taj zahtjev prema proxy serveru sa željenom informacijom.
4. Na kraju proxy server prihvaća tu informaciju i prosljeđuje je do izvorišnog klijenta koji je poslao početni zahtjev.

Ovakav tip komunikacije omogućava zaštitu klijenata unutar štićene mreže jer se promet odvija preko proxy servera, a ne direktno.

Vatrozid ovog tipa omogućava preciznu zaštitu mreže na razini pojedinačnih usluga i korisnika, ali čini proces uspostave veze složenijim i proces prijenosa podataka sporijim. Štićena mreža može imati više vrata aplikacije, po jedna vrata za svaku aplikaciju. Svaka od tih vrata predstavljaju jedan vatrozid, ali mogu raditi na istom domaćinu. Vatrozid koji radi kao vrata aplikacije omogućava precizno filtriranje, ali usporava komunikaciju između klijenta unutar štićene mreže i vanjskog web servera jer sve prolazi preko posrednika, a taj posrednik su vrata aplikacije. Zbog toga ova vrsta vatrozida može biti postavljena samo za neke aplikacije iz štićene mreže. Neki dijelovi štićene mreže mogu biti vezani na osnovni vatrozid bez da njihova komunikacija prolazi preko vrata aplikacija. Vrata aplikacija omogućuju bolju kontrolu prometa, ali se ta bolja kontrola može koristiti samo za neke aplikacije i samo za neke dijelove štićene mreže.

Prednost ove vrste vatrozida je da ukoliko napadač uspije naći ranjivost neke aplikacije u štićenoj mreži prvo bi morao napasti vatrozid koji radi kao vrata aplikacija (proxy) prije nego napadne uređaje koji se nalaze iza tog vatrozida.

Slijedi i grafički prikaz kako radi ova vrsta vatrozida s time da je na slici prikazana komunikacija između klijenta u štićenoj mreži i web servera preko proxy servera.



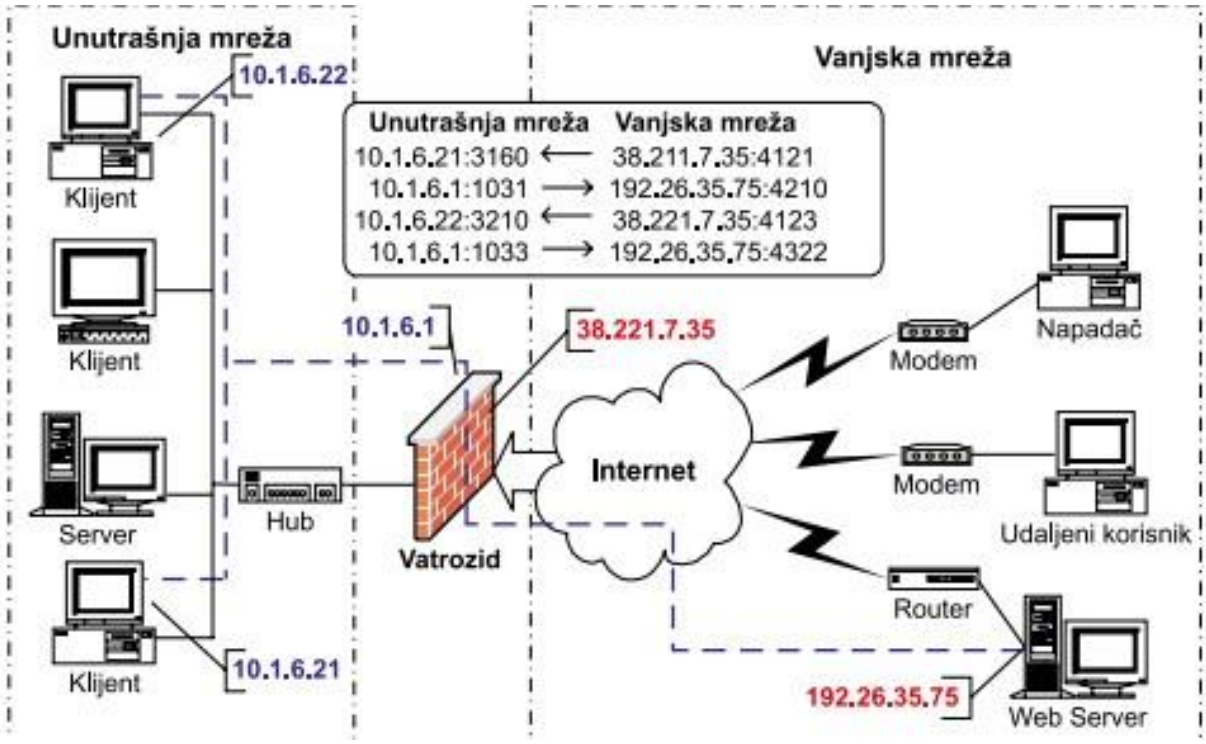
Slika 10. Prijenos podataka preko Proxy servera

(Preuzeto s https://www.networkworld.com/article/2255950/lan-wan/chapter-1--types-of-firewalls.html?page=2)

3.1.4. Prevođenje mrežnih adresa (NAT- „Network Address Translation“)

Prevođenje mrežnih adresa se izvodi tako da se pretvaraju mrežne adrese iz štićene mreže s ciljem da se stvori situacija u kojoj se čini da sav mrežni promet proizlazi iz jedne točke. Na ovaj način se omogučava korištenje jedne skupine mrežnih adresa interno i druge skupine za rad s vanjskim mrežama. To omogućava skrivanje identiteta klijenata unutar štićene mreže. Prevođenje mrežnih adresa ne pruža direktnu sigurnost sustavu, ali omogučava čuvanje tajnosti konfiguracije štićene mreže, što predstavlja značajnu sigurnosnu mjeru

Slijedi prikaz kako vatrozid koji se temelji na prevođenju mrežnih adresa funkcionira. Na slici Slika 11. se može vidjeti da kada se gleda od strane vanjske mreže čini se kao da cijeli promet proizlazi iz jedne točke te da se sustav za maskiranje adresa koristi TCP portovima kako bi sačuvao put spajanja vanjskog i unutarnjeg računala.[B. Svilčić, A. Kraš; Zaštita privatnosti računalnog sustava, 2005.].



Slika 11. Prevođenje mrežnih adresa

(Preuzeto od, B. Svilčić, A. Kraš; Zaštita privatnosti računalnog sustava, 2005.)

3.2. Prednosti i mane vatrozida

U najboljem slučaju vatrozid koji je postavljen između neke mreže i vanjskog prometa štiti tu mrežu od neželjenog pristupa iz ostatka interneta, ali ne može osigurati sigurnost za legitimnu komunikaciju između unutarnje i vanjske strane vatrozida. Temeljni razlog za uspostavu vatrozida je da oni obuhvaćaju sigurnost u centraliziranom sustavu štiteći sustav od ostatka računalne mreže. Administrator sustava u nekoj tvrtci može upravljati vatrozidom na željeni način (prema željama tvrtke) kako bi oslobodio korisnike i aplikacije unutar štićene mreže od sigurnosnih problema, barem od neke vrste tih problema.

Nažalost vatrozid ima i neka ograničenja koja su štetna za mrežu koju štiti. Kako vatrozid ne ograničava komunikaciju između korisnika unutar štićene mreže nego štiti mrežu od vanjskog prometa, napadač koji se uspije nekako ubaciti na jedno računalo unutar štićene mreže može

imati pristup i zaraziti sva računala u toj mreži. Primjer kako napadač može ući u štićenu mrežu je da je to neki nezadovoljni radnik koji ima pristup računalu u mreži ili pak putem zločudnog softvera koji se nalazi na CD-u ili skidanjem nekog softvera koji je zaražen putem interneta. Također vatrozid je u nekim situacijama moguće zaobići koristeći bežičnu komunikaciju.

Problem mogu biti i poslovni partneri ili vanjski zaposlenici koji imaju pristup štićenoj mreži. Ukoliko njihova sigurnost nije dobra kao sigurnost mreže koju vatrozid štiti, u tom slučaju je napadač može probiti i tako napasti i štićenu mrežu.

Jedan od glavnih problema za vatrozid je njihova ranjivost na bagove u računalima unutar štićene mreže. Bugovi se otkrivaju redovito te administrator sustava mora redovito pratiti njihove pojave.

3.2.1. Prednosti i nedostaci paketnog filtriranja

Prednosti:

- Jedan uređaj može štititi cijelu mrežu - Prednosti paketnog filtriranja su u tome da jedan dobro konfigurirani usmjerivač za filtriranje paketa može štititi cijelu mrežu. Ako se korisnici u štićenoj mreži spajaju na Internet preko samo jednog usmjerivača na kojem je postavljen vatrozid temeljen na filtriranju paketa povećava se sigurnost mreže.
- Velika efikasnost – kako filtriranje paketa zahtjeva pregled samo nekoliko zaglavlja paketa cijeli proces se odvija bez zakašnjenja.
- Široka dostupnost – postoji mnogobrojni hardverski i softverski proizvodi koji nude filtriranje paketa.

Nedostaci:

- Alati za paketno filtriranje nisu savršeni – kao što je u ranijem dijelu rada navedeno postoje neki nedostaci ovakve vrste vatrozida jer postoje neka ograničenja

(propuštanje paketa koji ne bi smjeli biti propušteni iz razloga što ih ni jedno pravilo postavljeno na vatrozidu ne zahvaća).

- Nemogućnost postavljanja nekih zabrana

3.2.2. Prednosti i nedostaci vrata aplikacija (proxy)

Prednosti:

- Pohrana upita – kako svi zahtjevi za komunikaciju između korisnika u štićenoj mreži i vanjskih mreža moraju prolaziti kroz proxy server postoji mogućnpst da proxy sprema česte upite. Time se povećavaju preformanse sustava.
- Pametno pročišćavanje sadržaja – proxy omogućava pročišćavanje sadržaja s ciljem otkrivanja i uklanjanja potencijalnih zlonamjernih programa
- Kontrola pristupa na razini korisnika – s obzirom da je proxy aktivno uključen u konekciju može se vršiti kontrola pristupa na razini korisnika i poduzeti određene akcije s obzirom na aktivnosti korisnika.

Nedostaci:

- Proxy za svaki pojedini protokol – postoji mogućnost da se dogodi situacija u kojoj je potrebno postaviti razne proxy servere za svaki pojedini protokol. To se događa jer proxy mora poznavati protokol kako bi uspješno radio. Ovo može biti vrlo zahtjevan postupak što predstavlja nedostatak.
- Dostupan samo za određene usluge
- Izmjena postavki klijenata i korisničkih programa – ako se uvodi proxy korisnici nisu uvijek u mogućnosti koristiti neke alate i programe prema standardnim uputama.

3.2.3. Prednosti i nedostaci prevođenja mrežnih adresa (NAT)

Prednosti:

- Prisila korištenja vatrozida – ako su na nekim računalima postavljene mrežne adrese koje se ne mogu koristiti na vanjskoj mreži potrebno je korištenje sustava za prevođenje mrežnih adresa. Ovako se postiže prisilna uspostava veze kroz vatrozid.
- Dodatna ograničenja ulaznog prometa – primjer za ovo je ukoliko neki napadač na štićenu mrežu ne reagira neko vrijeme, sustav za prevođenje mrežnih adresa poništava adresu ili je dodjeljuje nekom drugom računalu.

Nedostaci:

- Prepoznavanje mrežnih adresa – neki protokoli skrivaju adrese te je potrebno da sustav za prevođenje mrežnih adresa poznaje protokol vrlo dobro kako bi uspio promjeniti adresu. Većina tih sustava može to napraviti za neke protokole, ali ne za sve.
- Čuvanje statusa veze kod pretvorbe adrese – sustavom za prevođenje mrežnih adresa lako se može saznati da li je računalo preiknulo TCP vezu, no ne potoji način da se sazna da li je prekinuta UDP veza. To znači da bi u sustavu za prevođenje mrežnih adresa trebalo biti definirano koliko dugo će se čuvati trenutna pretvorba jer postoji opasnost od gubitka odgovora ili dostavljanja odgovora pogrešnom računalu.

4. Komercijalni vatrozidi

U ovom poglavlju će biti uspoređeni neki vatrozidovi koji se koriste na tržištu te će biti prikazane njihove glavne karakteristike. Na tržištu postoje mnogi proizvođaći vatrozidova te je nemoguće obuhvatiti sve proizvode tako da će ovdje biti prikazani samo neki.

4.1. Checkpoint Firewall - 1

Checkpoint Firewall – 1 je filter sa statusnom inspekcijom zasnovan na NAT-u i skupu filtera za Internet protokole. Jedan je od poznatijih vatrozida na tržištu. Checkpoint je razvio koncept statusne inspekcije kako bi se poboljšala sigurnost filtriranja paketa bez zahtjeva za dodatni rad proxy servera. Statusna inspekcija predstavlja pojam između jednostavnih filtera paketa i aplikacijskih proxya, zadržavaju se informacije o stanju svake konekcije pa provjeru stanja paketa čine uspješnom. Ovaj vatrozid omogućava filtriranje sadržaja za tri opća protokola: HTTP, SMTP, FTP.

Glavne osobine Checkpoint Firewall – 1 vatrozida:

- Filtriranje paketa prema stanju
- Transparentni proxy specifičnog protokola (HTTP, SMTP, FTP)
- Obrnuti proxy (HTTP, SMTP, FTP)
- NAT
- Redirekcija portova
- Dodatne komponente za VPN (Virtualna provatna mreža) tipa vatrozid-do-vatrozida i vatrozid-do-udaljenog klijenta.

Sporedne osobine:

- Filtriranje sadržaja (Java, skeniranje virusa i blokiranje URL-a)
- Detekcija spoofinga i automatsko blokiranje
- Zaštita od SYN flood napada
- Sigurnosni server proxy autentifikacije
- Dijagnostički alati
- Konfiguracija zasnovana na polititi tvrtke

- Integriranje LDAP-a (Lightweight Directory Access Protocol)
- Djeljenje DNS-a

Checkpoint Firewall - 1 ima klijent/server arhitekturu koja omogućuje da se centralno kontrolira proizvoljan broj vatrozid modula sa jedne upravljačke konzole. Grafičko korisničko sučelje je jednostavno i lako za razumjeti.

4.2. Symantec Enterprise Firewall

Symantec Enterprise Firewall je sigurnosni proxy vatrozid.

Glavne osobine su mu:

- Sigurnosni filter paketa za mrežni prolaz
- NAT
- Sigurnosni proxy
- Udaljena autentifikacija
- Podrška za VPN je omogućena kroz VPN i prenosivi VPN

Ovaj vatrozid ne dozovljava usmjeravanje na mrežnom sloju, pa tako ne uključuje klasično filtriranje paketa. Svi podaci i informacije nižih slojeva usmjeravaju se kroz proxy servise aplikacijskog sloja. Ovo je siguran način prijenosa informacija i garancija zaustavljanja zlonamjernih paketa kroz mrežni prolaz. Kao dodatak tome što ne upravlja usmjeravanjem, ovaj vatrozid automatski odbacuje pakete koji se pojavljuju na vanjskim „interfejsima“, a sadrže unutrašnje adrese.

Symantec Enterprise Firewall se pri ivođenju više adresa u jednu adresu primarno oslanja na svoj proxy servis. Također koristi i pravo i obrnuto prevođenje mrežnih adresa pomoću osobine koja se zove Virtual Clients.

Ovaj vatrozid je primarno sigurnosni proxy koji koristi odvojene sigurnosne proxye za svaki podržani protokol. Sadrži sigurnosne proxye za sljedeće servise: Telnet, FTP, SMTP, HTTP 1.1, HTTP-FTP, HTTPS, NDS, NTP.

Ostale osobine:

- Mime Sweeper skeniranje virusa- Koristi se za uklanjanje virusa s preuzetih podataka i priloga e-mail poruka.
- Blokiranje URL-a
- Ilegalni NAT- Koristeći Virtual Clients mogućnost, omogućava prevođenje klijentskih adresa kroz mrežni prolaz mreža koje koriste ilegalne IP adrese.
- Dvostruki DNS- Dozvoljava da različita DNS imena služe i javnim i privatnim stranama proxya.

Kod ovog vatrozida korisničko sučelje je nešto zahtjevnije od prethodno opisanog vatrozida, ali ne u mjeri da se ne bi dalo savladati.

4.3. Microsoft ISA (Internet Security and Acceleration) Server

Microsoft ISA Server je Microsoftov vatrozid koji izvodi obrnuti i transparentni proxy za brojne protokole. Glavne osobine ovog vatrozida su:

- Statusna inspekcija paketa
- Proxy
- Filtriranje dolazećeg i odlazećeg prometa na aplikacijskom sloju
- IPSec, PPTP, L2PT VPN
- Brojne metode autentifikacije

Statusna inspekcija paketa – osigurava da su odlazeći povratni kanali na vatrozidu zatvoreni kada se TCP veza zatvori ili joj istekne vrijeme.

Filtriranje aplikacisjog sloja – ISA server dolazi sa brojnim sigurnosnim filterima aplikacijskog sloja koji mogu procesiratipravila za specifične aplikacije. Konfiguracija filtera uključuje i SMTP, FTP, HTTP.

Za ISA server su raspoloživi brojni filteri sadržaja, skeneri virusa, i blokatori sadržaja.

Sporedne osobine ISA servera:

- Snažna detekcija upada
- Pokretanje odgovarajućih programa u slučaju reagiranja na napad
- Transparentno proksiranje
- Konfiguriranje vatrozida na temelju politike tvrtke
- Visoka raspoloživost i balansiranje učitavanja

4.4. Najbolje rangirani besplatni vatrozidi u 2018. godini

U ovom djelu će ukratko biti navedeni i opisani najbolje ocijenjeni vatrozidi u 2018. godini. Prema više izvora to su:

- ZoneAlarm Free Firewall 2018
- Comodo Free Firewall
- TinyWall
- AVS Firewall

4.4.1. ZoneAlarm Free Firewall 2018

Ova verzija vatrozida ZoneAlarm vatrozida nudi mogućnosti skrivanja otvorenih portova, identificira sumnjivi promet, zatim onemogućuje zloćudne programe i nudi povezivanje na DefenseNet što pruža sigurnosna ažuriranja u stvarnom vremenu (real-time) kada se otkriju neke nove prijetnje. Također ovaj vatrozid štiti vaše računalo na javnim Wi-Fi mrežama te nudi 5 GB sigurnosne kopije podataka preko Idrivea. ZoneAlarm vatrozid može zaustaviti datoteke s nekog drugog računala kako bi spriječio neke zlonamjerne promjene. Također može se i lozinkom zaštititi postavke vatrozida kako bi se spriječile neovlaštene promjene, a čak nudi i mogućnost za slanje E-maila koji vas izvještava o sigurnosnom stanju.

Kako bi ste aktivirali ovaj vatrozid potrebno ga je prvo pruzeti te se prijaviti putem E-mail adrese.

Ovaj vatrozid radi na Windows XP, Vista, Windows 7, Windows 7 64-bit, Windows 8, Windows 8 64-bit, Windows 10, Windows 10 64-bit operacijskim sustavim, a izradila ga je tvrtka Zone Labs.

4.4.2. Comodo Free Firewall

Comodo Free Firewall nudi virtualno pregledavanje sadržaja na internetu, sadrži bloker oglasa (ad blocker), prilagođene DNS poslužitelje, opciju „Virtual Kiosk“ te značajke koje lako blokiraju bilo koji program koji ulazi ili napušta mrežu. Opcija Virtual Kiosk je „sandbox“ radno okruženje unutar kojeg možete pokrenuti programe i pregledavati internet bez straha da će te aktivnosti učiniti štetu vašem računalu. (sandbox- u svijetu računalne sigurnosti ovaj pojam označava opciju koja omogućuje pokretanje aplikacija, preuzimanje datoteka i posjećivanje web stranica u sigurnom virtualnom okruženju izoliranom od ostatka računala).

Kod ovog vatrozida lako je upravljati dozvolama za različite mreže, a mogu se stvoriti i pravila za određene programe tako da se dopušta ili odbija dolazni i odlazni promet.

Viruscope opcija prati ponašanje svega što izgleda sumnjivo, a filtriranje web stranica omogućuje blokiranje određenih stranica.

Comodo vatrozid nudi mogućnost na vrlo jednostavan način dodati programe u listu za blokiranje programe i one koji su dopušteni. Umjesto dugog postavljanja putem čarobnjaka za definiranje portova i drugih opcija, ovdje možete samo naći određeni program i postaviti ga u željenu listu.

Ovaj vatrozid nudi opciju „Rating Scan“ koja služi za skeniranje svih pokrenutih procesa kako bi se pokazalo koliko su oni pouzdani. Ovo je korisno u slučaju ako sumnjate da se neka vrsta zloćudnog programa nalazi na vašem računalu.

Comodo KillSwitch je napredan dio Comodo vatrozida koji navodi sve pokrenute procese te omogućava lako prekidanje ili blokiranje svega šti ne želite. Kroz ovu opciju možete vidjeti i sve aplikacije i servise koji su pokrenuti na vašem računalu.

Comodo Free Firewall radi na Windows 10, Windows 8 i Windows 7 operacijskim sustavima.

4.4.3. TinyWall

TynyWall je još jedan besplatni vatrozid koji vas štiti bez prikazivanja velikog broja nepotrebnih obavijesti kao što to radi većina drugih vatrozida. U TinyWall vatrozid uključen je i skener aplikacija kako bi skenirao vaše računalo za programe koje možete dodati na listu sigurnih programa. Također kod ovog vatrozida moguće je ručno odabrati neki proces, datoteku ili servis i dati im dopuštenja na vatrozidu koja su trajna ili za određeni broj sati.

Ovaj vatrozid možete pokrenuti u načinu rada koji se naziva „Autolearn“ (automasko učenje) kako biste ga naučili o programima kojima želite dati mrežni pristup kako biste ih mogli otvoriti, a zatim isključiti ovaj način rada da biste brzo dodali sve svoje pouzdane programe na listu sigurnih programa.

Prozor „Connections“ prikazuje sve aktivne procese koji imaju vezu sa internetom, kao i sve otvorene portove. Desnom tipkom miša možete kliknuti na jednu od veza („Connections“) kako bi naglo prekinuli neki proces ili ga možete poslati u „VirusTotal“ opciju koja služi za skeniranje virusa.

Od ostalih opcija koje nudi TinyWall vrlo važno je napomenuti da on blokira poznate lokacije na mreži koje imaju viruse i crve, štiti promjene izvršene na Windows vatrozidu tako da te promjene mogu biti zaštićene lozinkom.

Ovaj vatrozid radi na operacijskim sustavima Windows Vista, Windows 10, Windows 8 i Windows 7 dok na Windows XP operacijskom sustavu ne radi.

4.4.4. AVS Firewall

Ovaj vatrozid ima vrlo „user-friendly“ sučelje i lako ga je svladati za korištenje.

AVS Firewall vatrozid vas štiti od zlonamjernih izmjena na vašem računalu, skočnih prozora, „flash“ banera, i većine reklama. Nudi vam i mogućnost da prilagodite URL-ove koji bi trebali biti blokirani za oglase i banere ako ih već niste naveli.

Dopuštanje i odbijanje određenih IP adresa, portova, i programa je vrlo jednostavno. Možete ih dodati ručno ili pregledati popis pokrenutih procesa kako bisre odabrali jedan od tamo navedenih.

AVS Firewall uključuje i „Parent Control“ (roditeljska zaštita) opciju koja predstavlja dio koji dopušta pristup eksplicitnim web stranicama. Ovaj odjeljak vatrozida možete zaštititi lozinkom kako biste spriječili neovlaštene izmjene.

Povijest mrežnih veza možete provjeriti putem odjeljka „Journal“ kako biste lako mogli pregledavati i vidjeti koje su veze uspostavljene u prošlosti.

AVS Firewall je moguće instalirati na Windows 8, Windows 7, Windows Vista i Windows XP operacijskim sustavima.

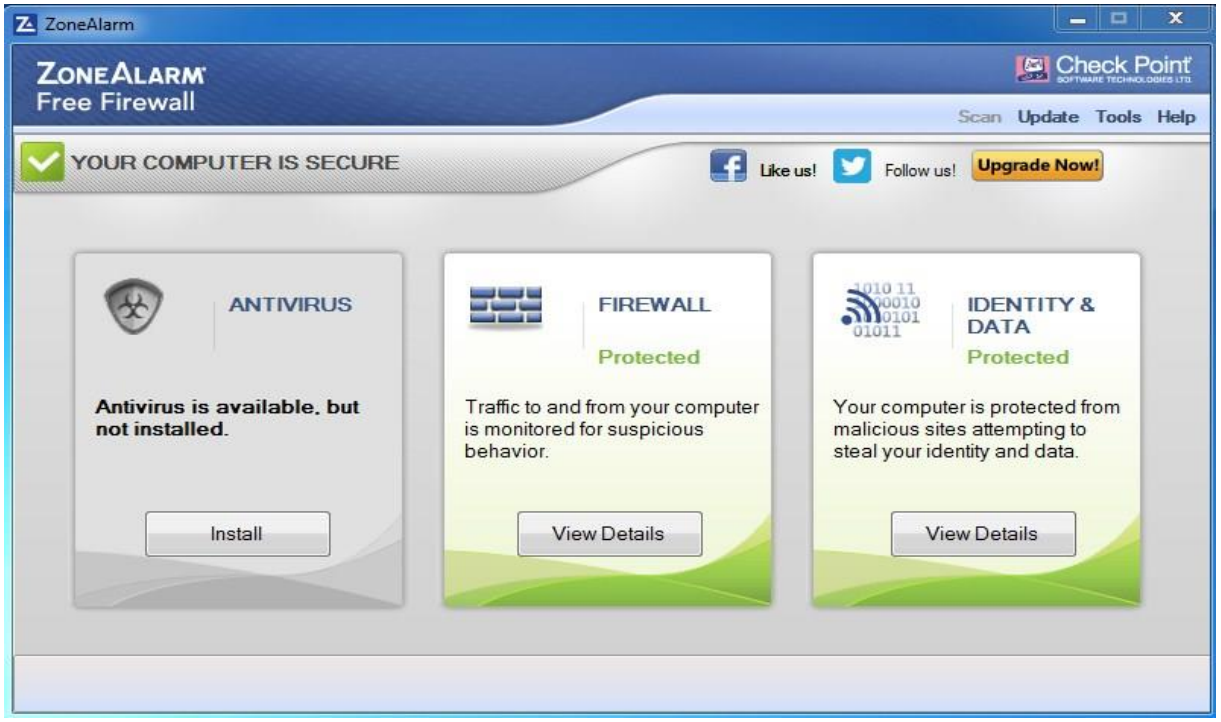
5. Postavljanje „ZoneAlarm Free Firewall 2018“ vatrozida

Za prikaz postavljanja vatrozida uzeo sam vatrozid ZoneAlarm Free Firewall 2018 iz razloga što je jednostavan za uporabu i svrstan je među najbolje besplatne vatrozide u ovoj godini. Ovaj vatrozid radi u dva smjera. Štiti računalo od dolaznih prijetnji s mreže kao što su napadi hakera, ali i zabranjuje odlaznim prijetnjama od strane šijunskih programa (spyware) i oglašivačkih programa (adware) da šalju informacije o tome što vi radite na računalu.

Prije postavljanja ovog vatrozida potrebmo ga je preuzeti sa službene ZoneAlarm web stranice (veza na stranicu: https://www.zonealarm.com/software/free-firewall). Kako bi ga pokretali možete pritisnuti na ZoneAlarm ikonicu u donjem desnom kutu vašeg računala, a to je prikazano na slici Slika 12.

Slika 12. ZoneAlarm ikona za okretanje vatrozida

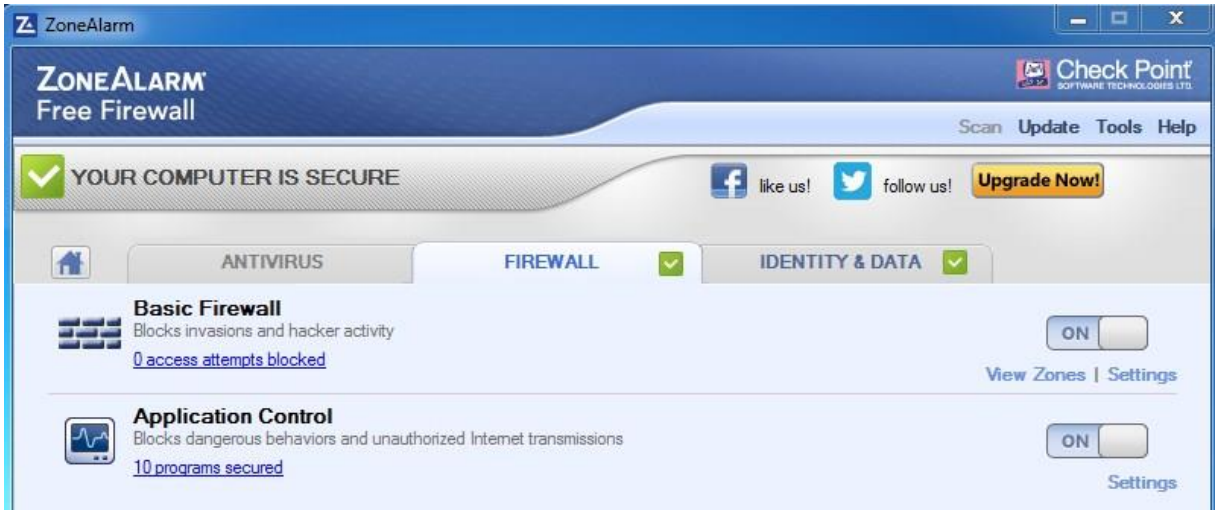
Glavni zaslon ZoneAlarm vatrozida vam prikazuje dva glavna područja u kojima vam vatrozid pruža sigurnost, a to su : „FIREWALL“ te „IDENTITY & DATA“ . Područje „ANTIVIRUS“ je isključeno te ga je potrebno dodatno instalirati.



Slika 13. Glavni zaslon ZoneAlarm vatrozida

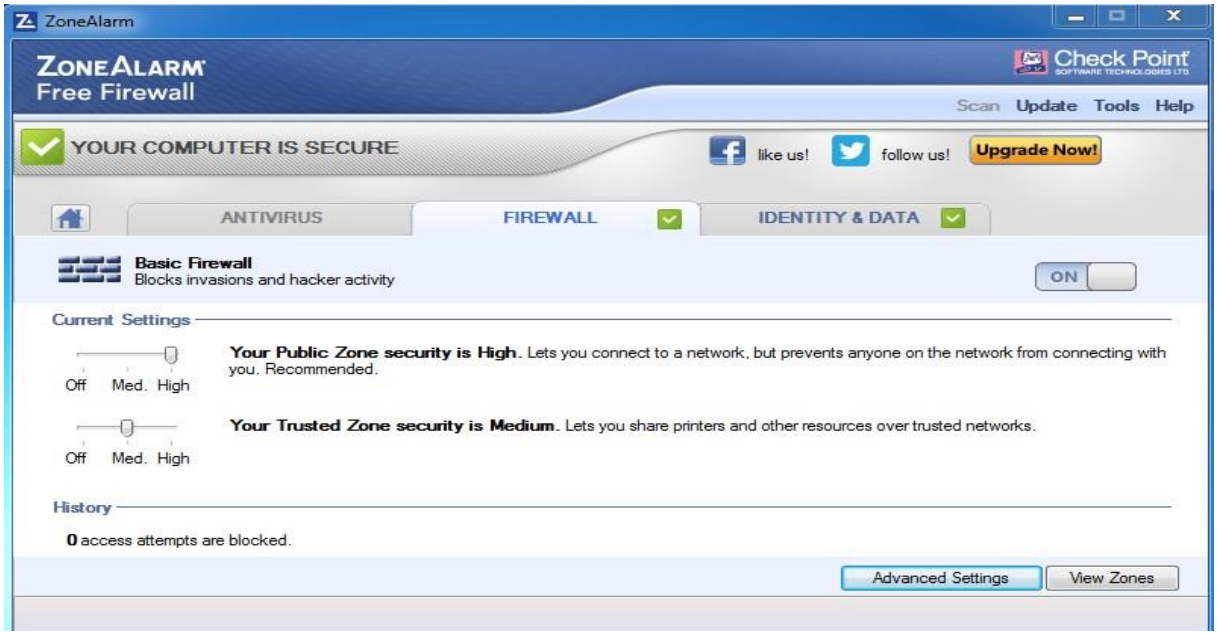
Kao što se može vidjeti sa slike Slika 13. u lijevom gornjem kutu vidimo zelenu kvačicu koja označava da je računalo sigurno od prijetnji.

Pritiskom na opciju „FIREWALL“ otvaraju se dvije mogućnosti: „Basic Firewall“ te „Aplication Control“.



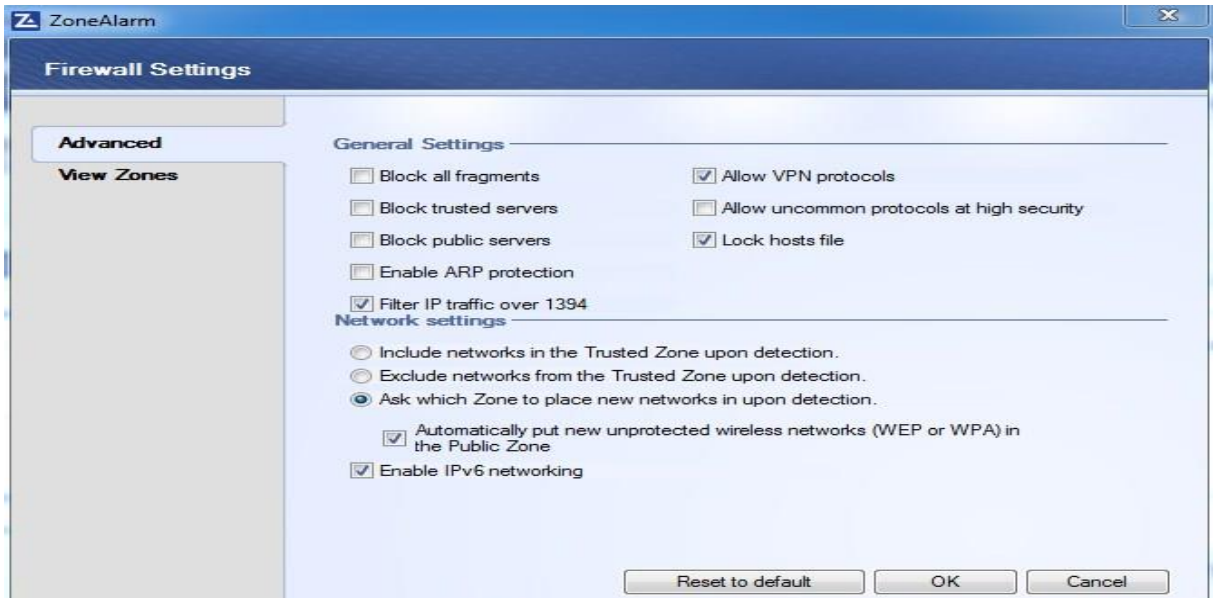
Slika 14. Opcija „FIREWALL“

Kod opcije „Basic Firewall“ možete kontrolirati razinu sigurnosti koju koristi vatrozid. Ako sumnjate da ste meta nekog napadača, što su postavke veće, više će te zaštite imati. Opcija „Advanced Settings“ tj. napredne postavke koritite u slučaju ako dovoljno dobro poznajete rad računala te kako će te postavke utjecati na funkcioniranje računalnog sustava.



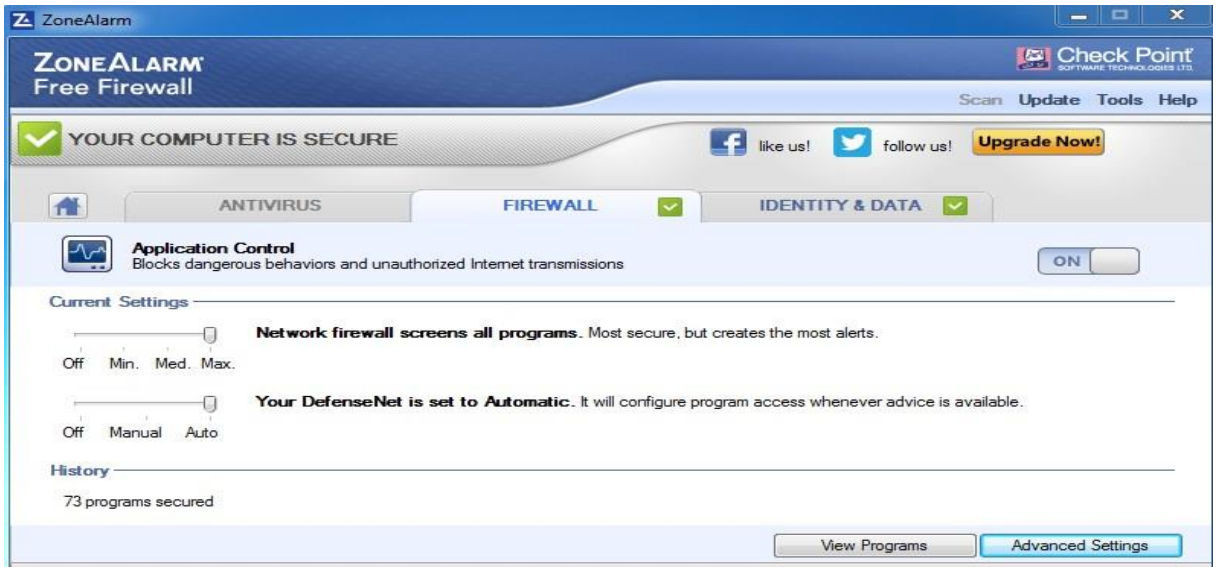
Slika 15. „Basic Firewall“

Slijedi prikaz naprednih postavki („Advanced Settings“) kod koje možete podešavati vaš vatrozid kako želite.



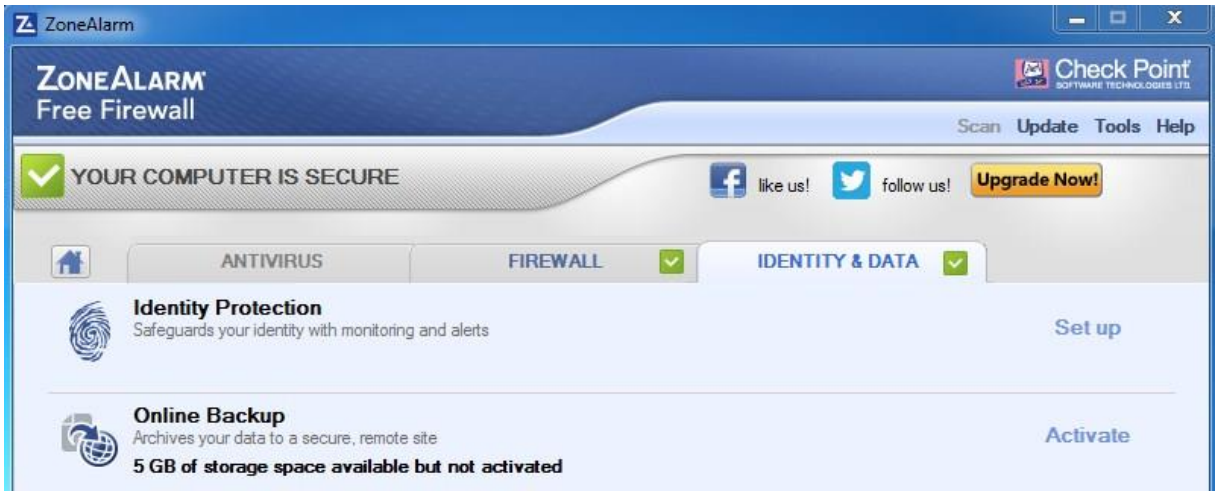
Slika 16. „Advanced Settings“

Slijedeća na redu je opcija „Application Control“. Ova opcija prati i omogućava rad s programima koji mogu naštetiti vašem računalu. Budući da hakeri koriste programe za infiltriranje u vaš sustav morate biti oprezni kada nešto instalirate i paziti gdje će te nešto preuzeti. Ova opcija nudi mogućnost zaštite računala ograničavanjem nekim programima da budu dostupni. Ovdje se također možete poigrati s postavkama („Advanced Settings“) kako bi pronašli najbolju ravnotežu tako da spriječiti štetne programe na vašem računalu.



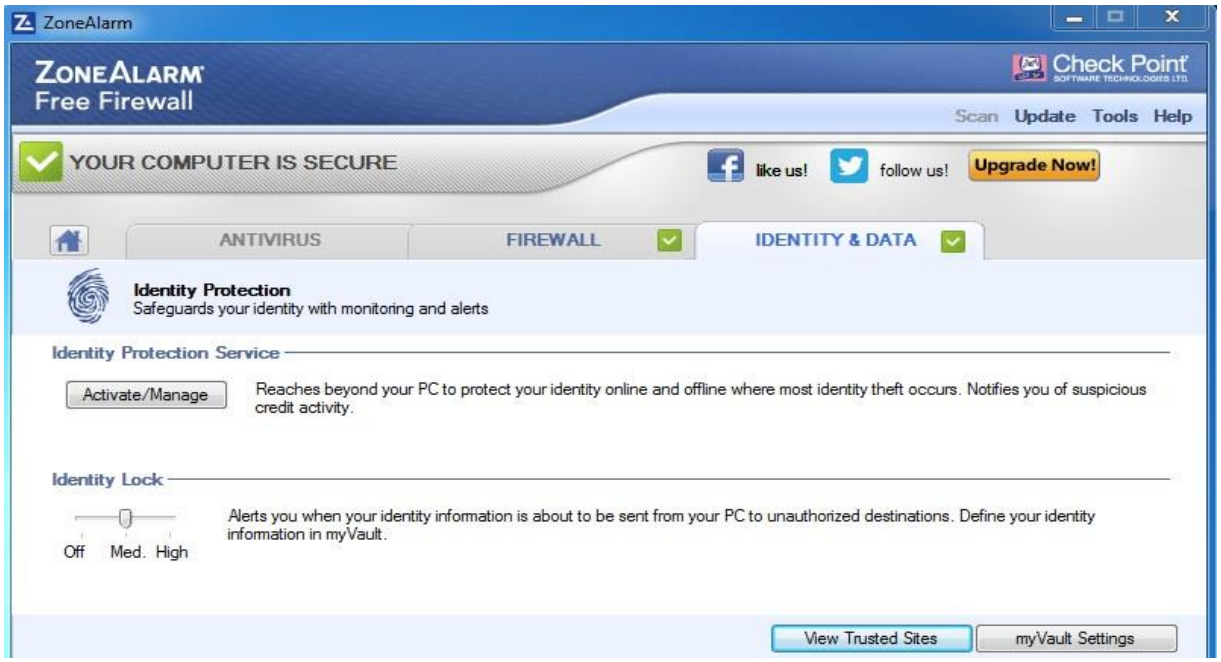
Slika 17. „Application Control“

Druga glavna opcija ZoneAlarm vatrozida je „IDENTITY & DATA“. Ova opcija nudi dvije mogućnosti, a to su: „Identity Protection“ i „Online Backup“.



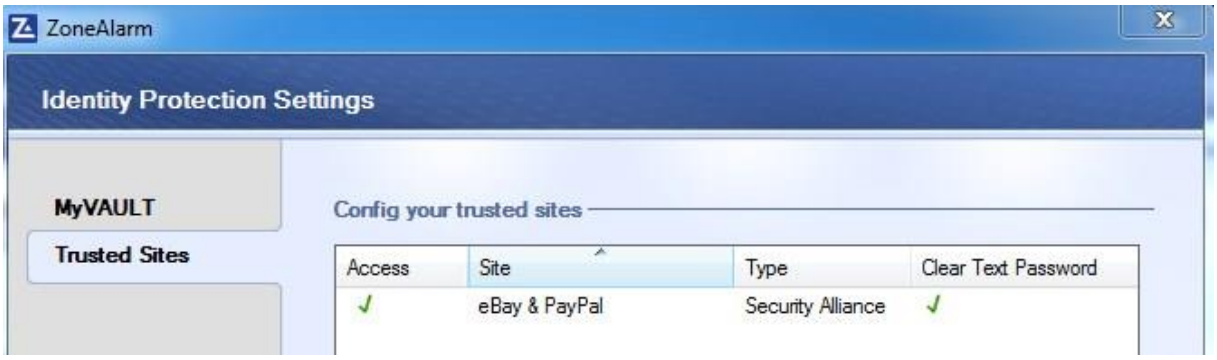
Slika 18. „IDENTITY & DATA“

„Identity Protection“ vam nudi zaštitu vašeg identiteta praćenjem i upozorenjima. Da biste pokrenuli ovu opciju morate ju aktivirati pritiskom na gumb „Activate/Manage“. Ova usluga ide izvan okvira vašeg računala kako bi se zaštitio vaš identitet on-line i offline gdje se događa većina krađe identiteta što može biti veoma opasno te vas obavještava o sumnjivoj kreditnoj aktivnosti. Ovdje možete vidjeti i neke sigurne stranice na kojima se vrše transakcije novčanih sredstava (navedene su „eBay“ i „PayPal“).



Slika 19. „Identity Protection“

Slijedi prikaz stranica koje su sigurne za kupnju putem njih koje se mogu vidjeti pritiskom na tipku „View Trusted Sites“.

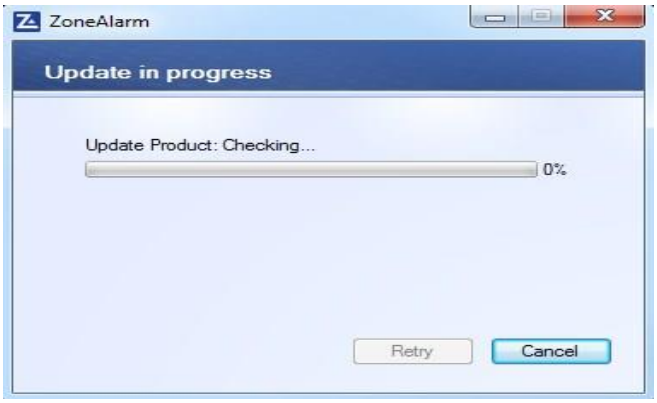


Slika 20. Sigurne stranice za kupnju

Otvaranjem opcije „Online Backup“ bit će te preusmjereni na stranicu ZoneAlarma gdje možete instalirati njihov softver za korištenje mrežnih usluga podrške. Ova usluga sprema vaše podatke na sigurno, udaljeno mjesto. ZoneAlaram kod besplatne verzije vatrozida vam nudi 5 GB prostora za spremanje podataka.

5.1. Ostale opcije ZoneAlarm Free Firewall vatrozida

U desnom gornjem kutu možete pronaći dodatne opcije vatrozida. To su „Update“ koja omogućuju ažuriranje vatrozida, opcija „Tools“ koja ima nekoliko mogućnosti te opcija „Help“ koja vam nudi pomoć i osnovne stavri o ovom vatrozidu.



Slika 21. Update opcija

Sada slijedi prikaz mogućnosti koje nudi opcija „Tools“

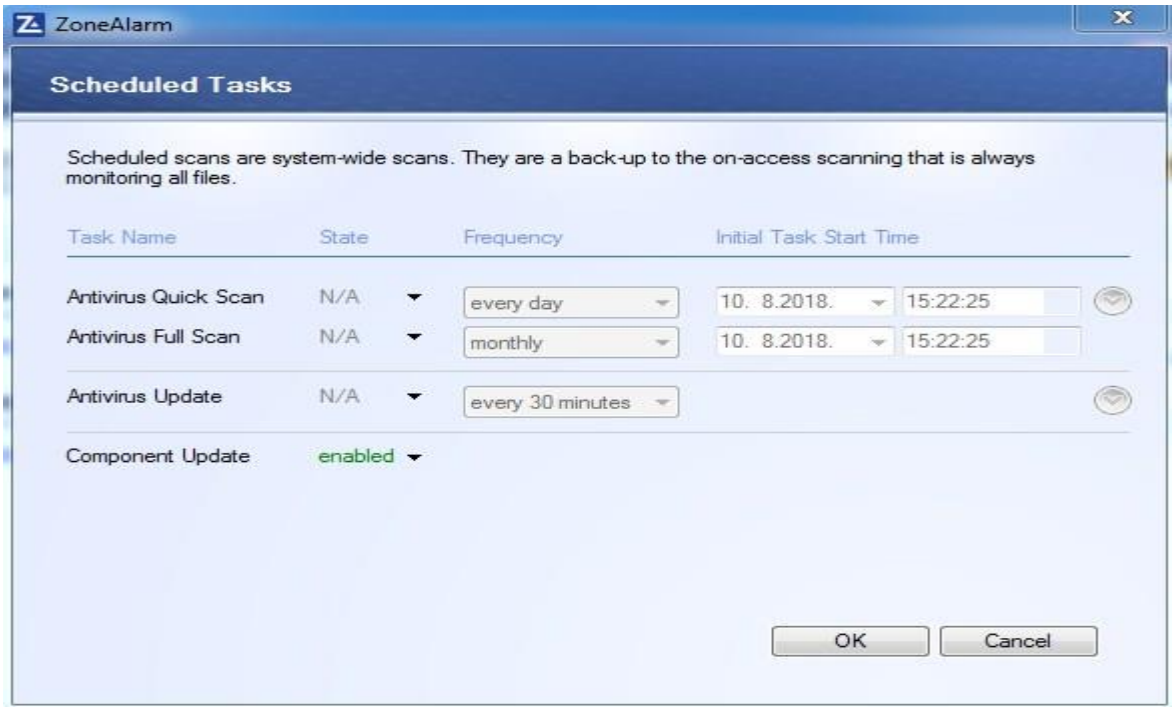
Slika 22. Opcija „Tools“

Ako kupujete ovaj vatrozid u mogućnosti ste upisati ključ koji vam omogućuje korištenje svih opcija ovog vatrozida (ne vrijedi za besplatnu varziju).

„Game Mode“ će vam omogućiti ograničavanje vatrozida tijekom igre, kao pto su online igre ili bilo koja igra koja bi mogla biti ometana od dolaznih i odlaznih podataka na vašem računalu. „Game Mode“ je poželjno isključiti nakon završetka igranja.

Slika 23. „Game Mode“

Opcija „Scheduled Tasks“ vam omogučava zakazivanje zadataka vatrozida ako instalirate i odgovarajući softver sa Zone Alarm sigurnosnim paketom.



Slika 24. „Scheduled Tasks“

ZoneAlarm Free Firewall vatrozid je jedan od najboljih besplatnih proizvoda ove vrste trenutno na tržištu te bih preporučio svakom da ga instalira na svoje računalo kako bi povećao sigurnost računala i zaštitio svoje podatke od neželjenih aktivnosti.

7. Zaključak

Kao što je navedeno u samom početku ovog diplomskog rada u današnje vrijeme sa svih strana prijete neke vrste prijetnji koje mogu naštetiti vašem računalnom sustavu bilo to u nekoj tvrtci ili na osobnom računalu kod kuće. Potrebno je biti vrlo oprezan prilikom pretraživanja i preuzimanja sadržaja s Interneta. Neki od najpoznatijih napada na vaš sustav su zloćudni softveri te DoS (Denial of Service“) napadi kao što je opisano u radu. Zloćudni softver („Malware“) prestavlja program koji je izrađen sa svrhom da se neprimjetno ubaci preko računalne mreže u sustav nekog računala i učini neku vrstu štete. Neke od najpoznatijih vrsta zloćudnih softvera su računalni virusi, računalni crvi, trojanski konj, špijunski programi („spyware“), oglašivački programi („adware“) te ucjenjivačji softver („ransomware“).

DoS napadi su napadi koji uskraćuju neku uslugu za korisnika na računalu kao što im i sam naziv govori. Tipičan oblik napada kod DoS napada na sustav je taj da napadači preplavljuju računalni sustav žrtve sa velikim brojem poruka, zahtjeva i informacija kako bi preopteretili sustav i prouzročili pad sustava. Time se onemogućava korisnika računala da koristi usluge tog računala kako ih je prije napada mogao koristiti. Najpoznatije vrste DoS napada koje su detaljno opisane u radu su Ping of Death („smrtonosni ping“),Teardrop („kap suze“), UDP flood, SYN flood, Prizemljenje, Smurf, Fraggle, E-mail bombe te zlonamjerno formirane poruke.

Kao što je vidljivo brojne su prijetnje koje se nalaze na mreži. Iz tog razloga izrađeni su vatrozidi, sustavi koji štite mrežu od vanjskih napada. Vatrozid predstavlja kombinaciju hardvera i softvera koji kontrolira komunikaciju između računalnih mreža. To je sustav preko kojeg se odvija prijenos podataka u neku mrežu i iz te mreže. U radu su navedene 4 osnovne vrste vatrozida.

Tradicionalni filtri paketa promatraju svaki IP paket zasebno. Na temelju pravila vatrozid odlučuje za svaki paket da li ga treba propustiti ili odbaciti. Svaki IP paket vatrozid procesira zasebno, neovisno od drugih paketa. Kod ove vrste vatrozida administrator mreže postavlja pravila na vatrozidu ovisno o stavovima tvrtke.

Filtri paketa prema stanjima su druga vrsta vatrozida. Rade na sličan način kao i tradicionalni filtri paketa s time da imaju dodanu još jednu dimenziju u filtriranju paketa. Ovaj tip vatrozida održava i konzultira tablicu TCP veza koje se uspostavljaju i odvijaju preko njega. Kao što

sam naziv ove vrste vatrozida govori oni pored tablice za kontrolu pristupa promatraju i stanje TCP veza. Dakle ovaj tip vatrozida za svaki IP paket pojedinačno odlučuje što s njim učiniti, ali odluke ne donosi samo na temelju pravila danih u tablici sa listom za kontrolu pristupa nego promatra i stanje TCP veza.

Treći tip vatrozida su Vrata aplikacija (proxy server). Ovaj tip vatrozida omogućava da se filtriranje definira kvalitetnije i preciznije. Vatrozid ovog tipa nadzire i ograničava prijenos sadržaja u štićenu mrežu i iz nje na razini pojedinačnih aplikacija i pojedinačnih korisnika. Proces komunikacije između klijenta u štićenoj mreži i vanjskog web servera prolazi preko proxy servera u četiri osnovna koraka. Klijent iz štićene mreže zatraži uspostavu veze sa web serverom koji se nalazi izvan te mreže. Zatim proxy server prihvaća taj zahtjev i prosljeđuje ga prema odgovarajućem web sereveru. Web server prima zahtjev od proxy servera i odgovara na taj zahtjev prema proxy serveru sa željenom informacijom. Na kraju proxy server prihvaća tu informaciju i prosljeđuje je do izvorišnog klijenta koji je poslao početni zahtjev.

Prevođenje mrežnih adresa (NAT) je četvri način rada vatrozida. Prevođenje mrežnih adresa se izvodi tako da se pretvaraju mrežne adrese iz štićene mreže s ciljem da se stvori situacija u kojoj se čini da sav mrežni promet proizlazi iz jedne točke. To omogućava skrivanje identiteta klijenata unutar štićene mreže.

Vidimo kako postoje različiti tipovi vatgrozida koji rade na različite načine i čine vašu mrežu sigurnom od napada. Svaki tip ima svoje prednosti i mane te se koriste ovisno o tome što se želi postići.

U sklopu rada navedeni su i opisani neki komercijalni vatrozid proizvodi koji se koriste. Također dan je prikaz najbolje ocijenjenih besplatnih vatrozida u ovoj godini te je opisano korištenje „ZoneAlarm Free Firewall 2018“ vatrozida. Ovaj vatrozid je uzet za prikaz iz razloga što je ocijenjen kao jedan od najboljih vatrozida trenutno te je jednostavan za korištenje i pruža vrlo dobru zaštitu.

8. Literatura

[1]. Mario Radovan: Računalne mreže (2): Prijenos, mrežne usluge i zaštita, DPT, Rijeka 2011.

[2]. Larry L. Peterson, Bruce S. Davie: Computer Networks: A systems approach (Fifth Edition), Morgan Kaufmann, San Francisco, 2011

[3]. James F. Kurose, Keith W. Ross: Computer Networking: A Top-Down Approach (Sixth edition), Addison-Wesley, 2009.

[4]. Brian Underdahl: Kućno umrežavanje:praktični vizualni vodič, Miš d.o.o. Zagreb, 2005.

[5]. Anonymous: Hakerski vodič za zaštitu-Maksimalna sigurnost, Kompjuter biblioteka, Čačak, 2004.

[6]. Matthew Strebe, Charles Perkins: Firewalls: zaštita od hakera, Kompjuter biblioteka, Čačak, 2003.

[7]. Boris Sviličić, Antun Kraš: Zaštita privatnosti računalnog sustava, Rijeka, 2005.,

[8]. IT4nextgen: What is a Firewall & Types of Firewall, 2017., preueto s: http://www.it4nextgen.com/types-of-firewall, (dostupno 20.7.2018.)

[9]. Ray Blair, Arvind Durai: Types of Firewalls, 2009., preuzeto s: https://www.networkworld.com/article/2255950/lan-wan/chapter-1--types-of-firewalls.html?page=2, (dostupno 21.7.2018.)

[10]. Wikipedia: Network security,preuzeto s: https://en.wikipedia.org/wiki/Network_securit, (dostupno 10.7.2018.)

[11]. Wikipedia: Malware, preuzeto s: https://en.wikipedia.org/wiki/Malware, (dostupno 12.7.2018.)

[12]. Securitywing: 7 Different Types of Firewalls, 2012., preuzeto s: https://securitywing.com/types-of-firewall, (dostupno 21.7.2018.)

[13]. Pina Chatralla: Types of Firewall, 2015., preuzeto s: https://www.slideshare.net/PinaChhatrala1/types-of-firewall-53269158, (dostupno 22.7.2018.)

[14]. Carrie Marshall, Cat Ellis, Jonas DeMuro: The best free firewall 2018, 2018., preuzeto s: https://www.techradar.com/news/the-best-free-firewall, (dostupno 5.8.2018.)

[15]. Kim Crawley: Explain How Firewalls Work to Me, 2017., preuzeto s: https://www.alienvault.com/blogs/security-essentials/explain-how-firewalls-work-to-me, (dostupno 15.7.2018.)

[16]. CERT: O virusima, 2018, preuzeto s: https://www.cert.hr/virusi/, (dostupno 20.7.2018.)

[17]. Lucia Denes: Što je to virus i kako ukloniti takav program, preuzeto s: http://virusi.hr/virusi, (dostupno 20.7.2018.)

[18]. Margaret Rouse: Computer worm, preuzeto s: https://searchsecurity.techtarget.com/definition/worm, (dostupno 21.7.2018.)

[19]. CERT: O crvima, preuzeto s: https://www.cert.hr/crvi/, (dostupno 21.7.2018.)

[20]. Malwarebytes: Adware, preuzeto s: https://www.malwarebytes.com/adware/, (dostupno 22.7.2018.)

[21]. WikiIS: DoS Napadi, preuzeto s: https://www.cis.hr/WikiIS/doku.php?id=dos_attacks, (dostupno 25.7.2018.)

Popis slika

Popis tablica