****

**Program: informatika**

**POŽARNI ZID**

**Seminarska naloga pri predmetu Varnost in zaščita**

**Študent: Dominik Dominko, 11150190092, INF-2**

**Mentor: Borut Bencak**

**Murska Sobota, februar 2014**

# 1 UVOD

Življenje v obdobju tehnološke in informacijske revolucije od posameznika zahteva nenehno dostopnost in povezanost kar pa seveda gre z roko v roki z ustrezno tehnologijo ki nam to omogoča. Odkar je internet postal stalnica v posameznikovem vsakdanjem življenju so se torej morale razviti tudi tehnologije, ki nam omogočajo da se na omrežje lahko priključimo. Ob razvoju tehnologije pa kot odgovorni uporabniki relativno novih tehnologij ne smemo pozabiti tudi na varnost ki je z njimi povezana in nujna. Požarni zid je eden izmed tistih sestavnih delov dobrega in varnega omrežja, ki omogoča hitro in produktivno delo preko svetovnega spleta a obenem zagotavlja njegovo varno uporabo ki se kaže kot vedno bolj ključna pri uporabi svetovnega spleta.

Opredelitev problema - predstaviti prednosti in slabosti požarnega zidu, kaj nam omogoča In onemogoča.

Cilj naloge je spoznati osnove delovanja požarnega zidu in njegove lastnosti.

Namen naloge je ukvarjati se s raziskovanjem delovanja požarnega zidu, navesti in opisati njegove sestavne komponente ter raziskati zakaj je temu tako. Prav tako je namen naloge postaviti določene hipoteze, ki jih s pomočjo raziskovalnega dela skozi nalogo preučimo in ob koncu potrdimo ali ovržemo.

Metode in oblike dela uporabljene pri izdelavi naloge so zajemale večinoma raziskovanje spletnih virov, kjer so informacije nekoliko bolj ažurne kot iz pisnih virov, v manjši meri pa so bili uporabljeni tudi pisni viri.

Hipoteza št.1 : Požarni zid je ob ustrezni uporabi protivirusnih programov odvečen oziroma nepotreben za varno delovanje sistema.

Hipoteza št.2: Programski požarni zidovi so bolj uporabni od strojnih požarnih zidov.

# 2 POŽARNI ZID

## 2.1 KAJ JE POŽARNI ZID IN KAKO DELUJE?

**Definicija**: predpisuje varnostno politiko med varnim notranjim in ne-varnim zunanjim omrežjem (npr. internetom). (Fister, 2009)

Požarni zíd je verjetno najpogostejši varnostni izdelek s področja omrežne varnosti. Potrebuje ga že skoraj vsaka naprava povezana v internet. Požarni zidovi so namenjeni ločevanju dveh odsekov omrežij, pogosto enemu odseku zaupamo, drugemu pa ne. Bistvo požarnega zidu je v zagotavljanju varnosti med dvema omrežjema. Požarni zid glede na določena pravila dovoli ali zavrne tok podatkov preko nje. (Fister, 2009)

Poznamo strojne in programske požarne zidove. Prednost programskih požarnih zidov je običajno v enostavnejši uporabi, predvsem pa je razlika v ceni. Medtem ko za domačo uporabo obstajajo brezplačni požarni zidovi, so strojni običajno precej dražji, prednost strojnega pa je pogosto v hitrosti, saj so normalno strojne rešitve precej hitrejše in tako omogočajo večjo prepustnost. (Fister, 2009)

Končno se uveljavlja tudi spoznanje, da končna točka povezave v internet ni samo požarni zid, ampak tudi posamezni računalniki, ki so za njim skriti. V večjih podjetjih hitro naraste možnost vdora in kraje informacij, saj je priključkov za dostop do omrežja veliko. Zato obstajajo npr. omejitve omrežnega priključka na strojni naslov omrežne kartice, ki pa vseeno ni dovolj, saj je mogoče strojni naslov omrežne kartice dokaj enostavno ponarediti. Zaradi tega so spisali standard 802.1x, ki omogoča dinamični vklop in izklop omrežnega priključka. Še večjo nevarnost za varnost omrežja predstavlja brezžična dostopna točka, saj je medij prenosa podatkov tu zrak in lahko vsak, ki ima prenosnik »prisluškuje« pogovoru med posameznimi brezžičnimi napravami, kar še posebej oteži zagotavljanje varnosti omrežja. (Fister, 2009; Parziale et al., 2010)

Med naprednejše funkcije požarnega zidu spadajo:

* preslikava (zasebnih) omrežnih naslovov (angl. oznaka NAT), ki omogoča skupno rabo internetne povezave
* demilitarizirana cona (angl. oznaka DMZ), ki omogoča ločen priklop bolj izpostavljenih naprav
* kontekstno odvisni nadzor dostopa, ki na podlagi protokolov dinamično dovoli dostop do storitev
* nudijo kriptirane tunelske povezave in tako omogočajo navidezna privatna omrežja (angl. oznaka VPN) (Vidmar, 2002)

Požarni zid je lahko osebni računalnik, usmerjevalnik, centralni računalnik (angl.mainframe), delovna postaja UNIX ali kombinacija teh in določa, katere informacije oz.storitve so dostopne od zunaj ter komu dovoljujemo njihovo uporabo. Običajno požarni zid namestimo v točki, kjer se srečata varno notranje omrežje in ne-varno zunanje omrežje. To točko imenujemo tudi točko dušenja (angl. choke point). Da bi laže razumeli,kako požarni zid deluje, si zamislimo omrežje kot zgradbo, ki jo nadzorujemo. Zgradba ima kot edino vstopno točko vežo, v kateri receptorji pozdravljajo obiskovalce, stražarjijih nadzorujejo, video kamere beležijo njihovo gibanje in obiskovalce, ki vstopijo vzgradbo, receptorji označijo z značkami. Čeprav te akcije lahko dobro nadzorujejo dostopdo zgradbe, pa v primeru, da se neavtorizirani osebi posreči vstop v zgradbo, ni načina,kako zgradbo zaščititi pred akcijami napadalca. Če njegovo premikanje nadzorujemo s kamero, lahko zaznamo njegove sumljive akcije. (Fister, 2009)

Pomembno je vedeti, da čeprav je požarni zid konstruiran tako, da dovoljuje prehod varnih podatkov preko omrežja, preprečuje ranljive storitve in ščiti notranje omrežje pred napadi od zunaj, ga lahko napadi, na katere ni pripravljen, npr. novi virusi, zlahka prebijejo. Da se lahko omrežni administrator uspešno pripravi na obrambo pred napadi od zunaj, mora preverjati vse loge in alarme, ki jih požarni zid generira. (Fister, 2009)

Vir: Fister, 2009



Slika 1: Primer požarnega zidu - požarni zid umestimo v točko dušenja, kjer se srečata dve omrežji

Vir: Fister, 2009



Slika 2: Primer požarnega zidu - požarni zid nadzoruje promet med varnim omrežjem in internetom

## 2.2 KOMPONENTE POŽARNEGA ZIDU

Komponente požarnega zidu v osnovi delimo na:

* + usmerjevalnik s filtriranjem paketov
	+ prehod proksi
	+ prehod na nivoju voda

Da bi bilo delovanje požarnega zidu kar se da produktivno je pomembno da vse tri komponente med seboj deluje komplementarno.

### 2.2.1 USMERJEVALNIK S FILTRIRANJEM PAKETOV

Prvi članek, ki je bil objavljen o požarnem zidu je bil izdan leta 1988, ko so inženirji iz DEC (Digital Equipment Corporation) razvili filterni sistem poznan kot »Packet Filter Firewall« ali požarni zid s filtriranjem paketov. (http://en.wikipedia.org)

Glavna prednost požarnega zidu s filtriranjem paketov je, da je to najcenejša vrsta požarnega zidu. Med varno in ne-varno omrežje postavimo usmerjevalnik, ki uporablja filtrirna pravila, ki dovoljujejo ali onemogočajo promet. (Vidmar, 2002)

Požarni zid ponavadi deluje na principu da prepovemo vse, kar ni eksplicitno dovoljeno, vsak gostitelj pa je neposredno dostopen iz zunanjega omrežja in mora iz tega razloga imeti lastni avtentikacijski mehanizem. (Vidmar, 2002)

Usmerjevalnik s filtriranjem paketov torej posreduje pakete glede na filtrirna pravila. Iz glave paketa lahko potegne naslednje informacije:

- Izvorni IP naslov,

- Ponorni IP naslov,

- TCP/UDP izvorna vrata,

- TCP/UDP ponorna vrata,

- ICMP tip sporočila.

Paketno filtriranje izvajamo z uporabo teh pravil kot vhodno informacijo. Pri določanju filtrirnih pravil moramo upoštevati zunanje napadalce, omejitve na nivoju storitve in omejitve na nivoju izvora oziroma ponora. (Parziale et al., 2010)

Vir: Fister, 2009



Slika 3: Primer topologije omrežja požarnega zidu

* + - 1. VRSTE FILTRIRANJA PAKETOV

**Filtriranje na nivoju storitve**

Dve glavni lastnosti filtriranja na nivoju storitve sta, da večina storitev uporablja splošno znane številke TCP/IP vrat, ter da storitve dovoljujemo z uporabo ustreznih informacij vrat v filtru. (Fister, 2009; Vidmar, 2002)

*Primer filtriranja na nivoju storitve:* strežnik FTP posluša zahteve za storitev po protokolu TCP na vratih 20 in 21. Če želimo dovoliti povezavam FTP pot skozi varno omrežje, mora usmerjevalnik omogočiti paketom, ki vsebujejo v glavi segmenta TCP vrata 20 in 21 prosto pot. (Parziale et al., 2010)

**Filtriranje na nivoju izvora/ponora**

Pravila filtriranja paketov usmerjevalnikom dovoljujejo ali prepovedujejo posredovanje paketov z oziroma na izvorne ali ponorne informacije v glavi datagrama. Če je v varnem omrežju na voljo neka storitev, običajno dovoljujemo zunanjim uporabnikom dostop samo na ta strežnik, t.j. vse pakete, ki imajo naslov IP različen od naslova IP tega strežnika zavržemo. (Fister, 2009)

**Napredno filtriranje**

Nekaterim izmed napadov, ki ogrožajo varnost v omrežju se lahko izognemo z uporabo pravil naprednega filtriranja kot je na primer preverjanje možnosti IP. Ob vseh možnostih filtriranja pa obstajajo tudi nekatere **omejitve** kot sta denimo to, da filtriranje poteka glede na informacije v različni poljih IP glave in se torej dogaja na IP plasti ter da lahko nadzor nad vsebino izvajamo le na aplikacijskem nivoju. (Fister, 2009; Vidmar, 2002)

Vir: Fister, 2009



Slika 4: Požarni zid s filtriranjem paketov

### PREHOD PROKSI (ANGL. PROXY GATEWAY)

V podjetju ki uporablja internet, je strežnik proksi posrednik med uporabniško delovno postajo in internetom. Strežnik proksi sprejema uporabniške zahteve po storitvah Interneta (npr. zahtevo po dokumentu HTML). Je del prehoda, ki ločuje zasebno omrežje od zunanjega omrežja in požarnega zidu ki varuje omrežje pred različnimi zunajimi vdori. Njegova glavna prednost je, da uporablja strogo avtentikacijo uporabnikov. (http://povezave.icrc.info)

Aplikacijski strežnik na požarnem zidu pogosto imenujemo tudi proksi. Proksi omogoča višje nivojski nadzor nad prometom med dvema omrežjema tako, da vsebine določene storitve nadzorujemo in filtriramo glede na našo varnostno politiko. Če želimo storitev nadzorovati, moramo na strežnik namestiti ustrezno aplikacijsko kodo proksi. (Fister, 2009; Vidmar, 2002)

Proksi deluje kot strežnik odjemalcu in kot odjemalec ponornemu strežniku. Vzpostavimo navidezno povezavo med odjemalcem in ponornim strežnikom. Čeprav je na prvi pogled proksi transparenten z vidika odjemalca in strežnika, je ta sposoben nadzora in filtriranja določenih vrst podatkov, kot npr. ukazov, preden jih pošlje na ponorni naslov. Namen strežnika proksi je nadzor izmenjave podatkov med dvema omrežjema na aplikacijski in ne na omrežni plati. V primerjavi s filtriranjem IP strežnik proksi omogoča več izčrpnejših poročil, ki temeljijo na aplikacijskih podatkih določene povezave. (Fister 2009)

*Primer uporabe prehoda proksi:* če uporabnik želi uporabljati storitve FTP ali Telnet iz ne-varnega omrežja, se mora najprej avtenticirati na strežniku proksi.

Vir: Fister, 2009



Slika 5: Aplikacijski strežnik proksi

Vir: Fister, 2009



Slika 6: Primer FTP proksi

### 2.2.3 PREHOD NA NIVOJU VODA

Najbolj znan primer prehoda na nivoju voda je socks. Ker pretok podatkov preko prehoda socks ne nadzorujemo ali filtriramo, lahko nastopi varnostni problem. Da zmanjšamo varnostne probleme morajo biti zaupne storitve in viri na zunanjem omrežju (ne-varnem omrežju). Razlike med PROXY in SOCKS:

-SOCKS ne omogoča procesiranja paketov in filtriranja,

-SOCKS uporabljamo za izhodne, PROXY pa vhodne in izhodne povezave,

-PROXY ne podpira UDP,

-SOCKS obdeluje več TCP in UDP aplikacij.

(Parziale et al., 2010)

Vir: Fister, 2009



Slika 7: Strežnik SOCKS

## 2.3 POŽARNI ZID Z DVODOMNIM GOSTITELJEM

Dvodomni gostitelj ima vsaj dva omrežna vmesnika in vsaj dva naslova IP. Ker posredovanje IP (angl. IP forwarding) ni aktivno, ves promet IP na požarnem zidu prekinemo.Tako paketi ne morejo skozi požarni zid, dokler na njem ne definiramo ustrezen prehod proksi oz. socks. Za razliko od požarnega zidu s filtriranjem paketov ta zagotavlja, da vsak napad, ki prihaja od neznane storitve, blokiramo. Požarni zid te vrste torej uporablja metodo, pri kateri prepovemo vse, kar ni eksplicitno dovoljeno. (Vidmar, 2002)

Vir: Fister, 2009



Slika 8: Primer požarnega zidu z dvodomnim gostiteljem

## 2.4 POŽARNI ZID Z ZASLONSKIM (PRIKRITIM) GOSTITELJEM

Ta tip požarnega zidu sestoji iz usmerjevalnika s filtriranjem paketov in aplikacijskega strežnika. Usmerjevalnik konfiguriramo tako, da ves promet posreduje aplikacijskemu strežniku v vlogi obrambnega zidu. Sestoji iz usmerjevalnika s filtriranjem paketov in aplikacijskega strežnika. (Fister, 2009; Vidmar, 2002)

Vir: Fister, 2009



Slika 9: Primer požarnega zidu z zaslonskim gostiteljem

## 2.5 POŽARNI ZID Z ZASLONSKIM (PRIKRITIM) PODOMREŽJEM

Ta tip požarnega zidu sestoji iz dveh usmerjevalnikov s filtriranjem paketov in branika. Požarni zid s prikritim omrežjem omogoča **najvišji nivo zaščite** med vsemi že omenjenimi primeri. Varnost dosežemo tako da ustvarimo demilitarizirane cone (angl. Demilitarized Zone, krajše DMZ) med zunanjim in notranjim omrežjem tako, da zunanji usmerjevalnik dovoljuje dostop iz zunanjega omrežja do branika in da notranji usmerjevalnik dovoljuje dostop iz notranjega omrežja do branika. (Vidmar, 2002; Parziale et al., 2010)

Takšna struktura omogoča močno varnost, saj se mora morebitni napadalec prebiti skozi tri ločene sisteme, da bi prišel na notranje omrežje.

# 3 ZAKLJUČEK

Dostop do svetovnega medmrežja je v današnjem nenehno razvijajočem se tehnološkem svetu nepogrešljiva dobrina. Morda je že celo pravica vsakega posameznika, da lahko svobodno dostopa do informacij zbranih na trenutno največjem in najbolj uporabljenim virom svetovnega znanja. Kakor se še vedno razvija in razširja nabor storitev ki jih internet ponuja, je ključno zagotoviti tudi možnost uporabe čim večjemu številu uporabnikov saj je od tega odvisen tudi njegov nadaljni razvoj.

A ob uporabi takšnega ogromnega vira podatkov se moramo zavedati tudi pasti, ki spremljajo vsako tehnologijo tovrstnih razsežnosti. Obstaja več vrst zaščite pred napadi nad omrežji uporabnikov, te so tako programske kot strojne. Požarni zid, protivirusni programi ter preventivne nastavitve omrežja so preproste rešitve, ki uporabniku zagotavljajo relativno visoko stopnjo zaščite.

 Spoznali smo delovanje požarnega zidu, njegovo natančno definicijo in lastnosti ter načine delitve komponent ki požarni zid sestavljajo. Ugotovili smo, da najvišji nivo zaščite predstavlja požarni zid z zaslonskim podomrežjem, medtem ko je najpomembnejša komponenta požarnega zidu usmerjevalnik s filtriranjem paketov čeprav je res da so vse tri posamezne komponente požarnega zidu pomembne in delujejo najbolje, ko so med seboj usklajene. Spoznali smo tudi, da je prehod proksi tisti, ki sprejema uporabniške zahteve po storitvah interneta in da je njegova glavna prednost uporaba stroge avtentikacije uporabnikov ter da ga uporabljamo za vhodne in izhodne povezave, medtem ko uporabljamo socks protokol za izhodne povezave.

Varnost na svetovnem medmrežju bo v prihodnosti vedno večjega pomena saj pisci zlonamerne kode izkoristijo vsako priložnost za trenutno precej preprosto pridobitev podatkov, ki so v nekaterih primerih lahko celo bistvenega pomena za posameznika. Zato je ključna uporaba požarnega zidu kot orodja, ki preprečuje napade na naše lastne podatke in na našo zasebnost, ki je kljub očitnemu nasprotnemu mnenju nekaterih svetovnih »agencij za varnost«, po mojem mnenju vedno bolj pomembna pravica posameznega uporabnika medmrežja a ironično tudi vedno bolj neupoštevana in kršena.

Prvo hipotezo, ki je trdila, da je požarni zid ob ustrezni uporabi protivirusnih programov odvečen oziroma nepotreben za varno delovanje sistema, smo ovrgli saj je protivirusni program omejen le na programsko raven, medtem ko je požarni zid del tudi strojne opreme in tako vendarle omogoča večjo stopnjo varnosti. Je pa potrebno poudarit, da so prav nastavitve požarnega zidu in protivirusnih programov ter njuno komplementarno delovanje tisti ključni dejavnik za uspešno vzdrževanje varnega sistema.

Drugo hipotezo, ki je trdila da so programski požarni zidovi bolj uporabni od strojnih programskih zidov zidov pa.lahko delno potrdimo saj smo spoznali, da so ponavadi strojne rešitve sicer res precej hitrejše in omogočajo večjo prepustnost ampak za precej višjo ceno in so ponavadi namenjene za komercialno uporabo. Za domačo uporabo, po drugi strani, pa so primerni in uporabni tudi brezplačni požarni zidovi.

# LITERATURA IN VIRI

Vidmar, T. *Informacijsko komunikacijski sistem.* Ljubljana: Pasadena 2002.

Parziale, I. et al. *Vedenje porabnikov*. Ljubljana: Ekonomska fakulteta, 2010.

Fister, I. *Vodnik v TCP/IP.* [Online]. 2009. Murska Sobota. [Citirano 26.februar 2014]. Dostopno na spletnem naslovu: ftp://ftp.scv.si/vss/ms/iztok\_fister/RKO-2/Vodnik%20v%20TCP-IP-II.pdf

*Požarni zidovi in proksi strežniki.* [Online]. 2009. [Citirano 27.februar 2014]. Dostopno na spletnem naslovu: http://povezave.ircr.info/omrezje/Pozarni%20zidovi%20in%20proxy%20 strezniki.htm

*Požarni zid.* [Online]. 2013. [Citirano 27. februar 2014]. Dostopno na spletnem naslovu: http://sl.wikipedia.org/wiki/Po%C5%BEarni\_zid

Firewall (computing). [Online]. 2013. [Citirano 26.februar 2014]. Dostopno na spletnem naslovu:http://en.wikipedia.org/wiki/

KAZALO SLIK

[Slika 1: Primer požarnega zidu - požarni zid umestimo v točko dušenja, kjer se srečata dve omrežji 4](#_Toc381388579)

[Slika 2: Primer požarnega zidu - požarni zid nadzoruje promet med varnim omrežjem in internetom 5](#_Toc381388580)

[Slika 3: Primer topologije omrežja požarnega zidu 6](#_Toc381388581)

[Slika 4: Požarni zid s filtriranjem paketov 7](#_Toc381388582)

[Slika 5: Aplikacijski strežnik proksi 8](#_Toc381388583)

[Slika 6: Primer FTP proksi 9](#_Toc381388584)

[Slika 7: Strežnik SOCKS 10](#_Toc381388585)

[Slika 8: Primer požarnega zidu z dvodomnim gostiteljem 10](#_Toc381388586)

[Slika 9: Primer požarnega zidu z zaslonskim gostiteljem 11](#_Toc381388587)

KAZALO VSEBINE

[1 UVOD 2](#_Toc381388531)

[2 POŽARNI ZID 3](#_Toc381388532)

[2.1 KAJ JE POŽARNI ZID IN KAKO DELUJE? 3](#_Toc381388533)

[2.2 KOMPONENTE POŽARNEGA ZIDU 5](#_Toc381388534)

[2.2.1 USMERJEVALNIK S FILTRIRANJEM PAKETOV 5](#_Toc381388535)

[2.2.2 PREHOD PROKSI (ANGL. PROXY GATEWAY) 8](#_Toc381388536)

[2.2.3 PREHOD NA NIVOJU VODA 9](#_Toc381388537)

[2.3 POŽARNI ZID Z DVODOMNIM GOSTITELJEM 10](#_Toc381388538)

[2.4 POŽARNI ZID Z ZASLONSKIM (PRIKRITIM) GOSTITELJEM 11](#_Toc381388539)

[2.5 POŽARNI ZID Z ZASLONSKIM (PRIKRITIM) PODOMREŽJEM 11](#_Toc381388540)

[3 ZAKLJUČEK 12](#_Toc381388541)

[LITERATURA IN VIRI 14](#_Toc381388542)