**FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA**
**UNSKA 3, ZAGREB**
**ZESOI**

# SUSTAVI ZA PRAĆENJE I VOĐENJE PROCESA

SEMINARSKI RAD

# *FIREWALLS*

Student: Slavko Šutić
JMBAG: 0036380367

Zagreb, svibanj 2004.

**SADRŽAJ:**

## 1. UVOD

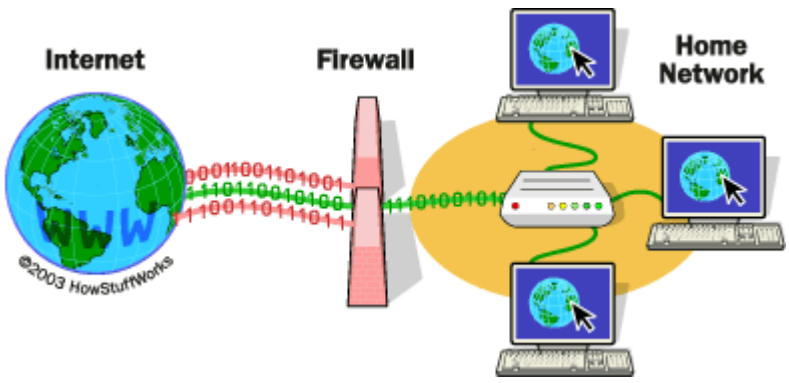
Generalno govoreći, računalne mreže su dizajnirane prvenstveno da obavljaju jednu glavnu funkciju, a to je da omoguće računalu spojenom u mrežu da slobodno izmjenjuje informacije i podatke s ostalim računalima koji su također spojeni u mrežu.

U idealnom svijetu, ovo je dobar način kako mreža funkcionira, upravo zahvaljujući univerzalnom načinu komunikacije između spojenih sustava. U tom slučaju pojedina računala mogu slobodno odlučivati s kim žele komunicirati, kojim informacijama će dopustiti pristup i koje će usluge pružati. Ovaj način rada se zove "*host based security"* jer pojedina računala ili domaćini (*hosts*) ugrađuju vlastiti sigurnosni mehanizam. Internet funkcionira na ovaj način kao i lokalna mreža u npr. nekoj tvrtki.

U praksi, pojedina računala nisu baš najpogodnija za pronalaženje i provođenje dosljedne sigurnosne zaštite. Razlog je tome što ona rade vrlo komleksno, česta je i pojava pogrešaka (*bugs*) u samim operacijskim sustavima koji tako onemogućavaju da se konstantno održi određena razina zaštite. Međutim, ovakav sustav zaštite se može primjeniti u slučajevima u kojima pojedini korisnici imaju povjerenja jedan prema drugome i gdje ne postoji motivacija da se naruši sigurnost ostalih korisnika kao što je to npr. u nekoj manjoj tvrtki.

Ali, ako je računalo ili mreža računala spojena na druge mreže i gdje više pojam povjerenja ne postoji u istom smislu, moraju se primjeniti neki drugi mehanizmi da bi se osigurala primjerena razina sigurnosne zaštite odgovarajućih podataka na lokalnoj mreži od potencijalnih napadača (*attackers*) s vanjske mreže.

Način na koji se ovo radi je djelomično kidanje veza u mreži tako da pojedine točke (računala, korisnici) na lokalnoj i vanjskoj mreži ne mogu više slobodno izmjenjivati podatke. Uređaji koji su zaduženi za to zovu se "Firewall" (vtreni zid, vatrozid, sigurnosna stijena). Pojam inače dolazi iz američke automobilske industrije gdje pojam *firewall* označava debelu čeličnu stijenku koja odvaja putničku kabinu od motora i tako sprečava da se vatra (toplina) širi od motora prema kabini.




**Slika 1.** Ideja firewalla

## 2. OPĆENITO O FIREWALL-u

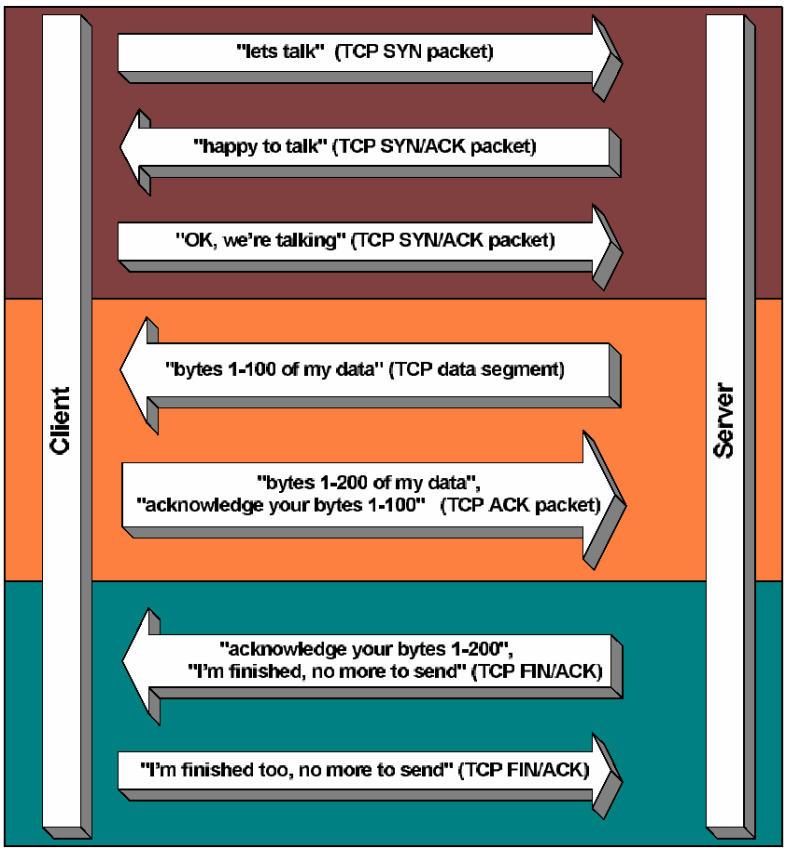
Firewall je uređaj koji spriječava zadobivanje pristupa korisnicima koji se nalaze izvan mreže koju nadgleda firewall. Ovaj uređaj je obično kombinacija softwarea i hardwarea. Firewallsi najčešće sadrže sheme i pravila koja sortiraju sav željen i neželjen promet.

Kao prvo, najjednostavnija autentikacijska procedura koristi IP adrese kao indekse. IP adresa je univerzalna identifikacijska "kartica" na Internetu a ta adresa može biti ili statična ili dinamička:

- Statična IP adresa je stalna, te je to adresa računala koje je uvijek spojeno na Internet. Postoji više klasa IP adresa. Jedna od klasa statičnih IP adresa može se otkriti zatraživanjem naredbe "whois". Ova klasa adresa predstavlja tzv. top-level računala u mreži, kao što su domain name serveri, Web serveri, i root-level računala. Druge klase IP adresa su adrese koje se pripisuju računalima drugog i trećeg razreda. Nad njima dominiraju domain name serveri, root serveri i Web serveri. Računala drugog i trećeg razreda također imaju stalnu fizičku adresu a između ostalog, ova računala mogu (ali i ne moraju) posjedovati registrirana imena (hostname).
- Dinamička IP adresa se pripisuje korisniku pri spajanju na mrežu. Dinamički IP se često koristi od strane ISP-ova za dial-up pristup - svaki put kada se korisnik spoji, pripisuje mu se druga IP adresa.

Bilo da je adresa korisnika statička ili dinamička, ona se koristi u svom mrežnom prometu u kojem sudjeluje korisnik. Kao primjer može se navesti snimanje korisnikove IP adrese na Web server prilikom zatraživanja određene Web stranice. Ovaj način se koristi ne kako bi narušio privatnost korisnika već kako bi server znao na koji način poslati zatražene podatke. Na sličan način svi mrežni servisi "hvataju" korisnikovu IP adresu (privremeno ili stalno) kako bi mogli vratiti podatke do korisnikove adrese. U biti, cijela procedura radi poput poštanskog ureda: svako pismo koje je poslano ima svog pošiljatelja koji ima svoju adresu i očekuje odgovor na svoj zahtjev. Kada je veza uspostavljena između korisnikovog računala i udaljenog računala, mogu se pojaviti razne informacije. Najčesća je tzv. "TCP/IP three-way handshake" (**Slika 2.**). Na bilo kojem stupnju takva informacija se pojavljuje tijekom koje korisnikov IP biva (pre)poznat računalu koje je zatražilo zahtjev. U normalnim okolnostima, gdje nema firewalla ili druge nadomjestne aplikacije (kao npr. TCP_Wrapper) instalirane, informacija između računala korisnika i udaljenog računala putuje direktno. Kada kažemo da informacija putuje direktno, time mislimo na ograničeni pojam jer je cjelokupni proces mnogo složeniji:

1. Podatak nastaje negdje unutar Korisnikove Mreže. U ovom slučaju, korisnik je spojen na mrežu svog providera. Takvim sagledavanjem, mreža providera se onda moze klasificirati i kao Korisnikova Mreža.




**Slika 2.** TCP/IP three-way handshake

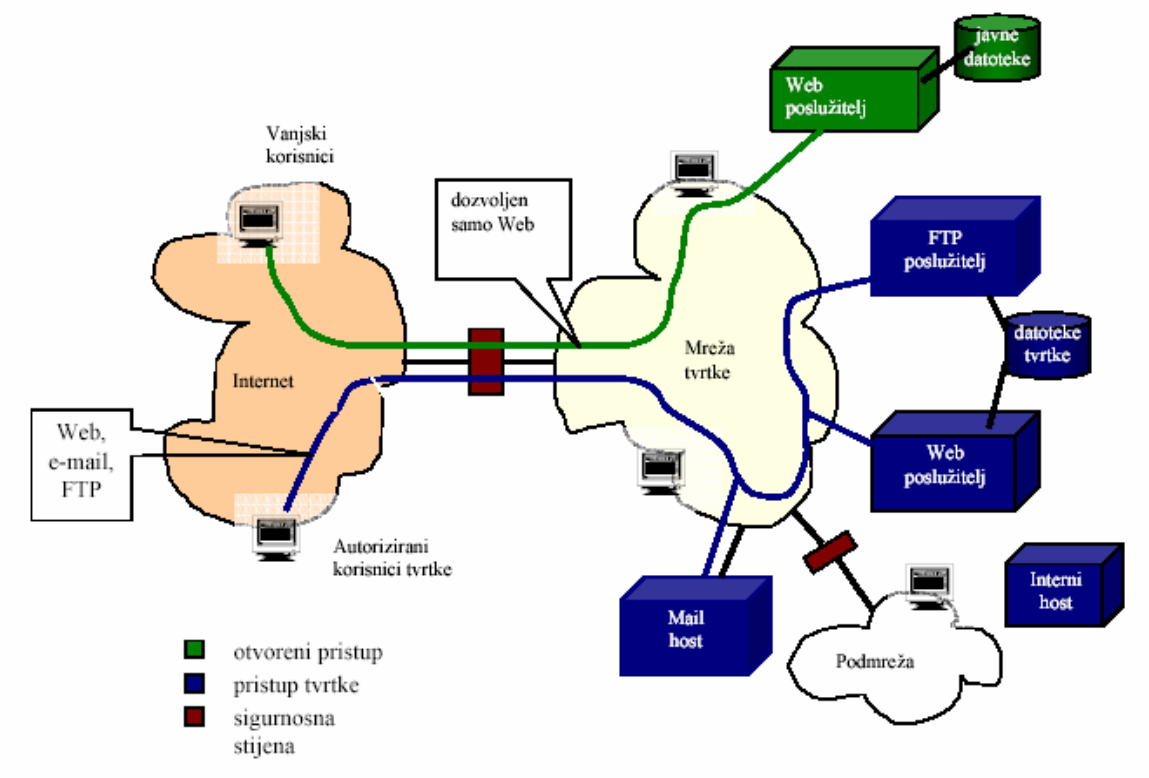
2. Informacija putuje od računala korisnika do računala u mreži providera. Zatim putuje putem Ethernet kabela (ili drugog oblika prijenosa) do glavnog servera Korisnikove Mreže.
3. Server Korisnikove Mreže predaje informaciju Routeru 1, koji promptno šalje informaciju kroz telefonsku liniju prema Internetu.
4. Informacija putuje preko Interneta (prolazi kroz mnogo routera i gatewaya putem), te dospijeva do Routera 2. Router 2 izručuje informaciju Serveru Providera a zatim se informacija šalje putem Etherneta ili drugog izvora prijenosa podataka do Mreže Providera.

Ako ni jedna ni druga strana nisu primjenile sigurnosne mjere, put informacije se smatra direktnim. Router 2, na primjer, propušta pakete sa bilo koje izvorisne (IP) adrese da putuje direktno do Servera Providera i tada do Mreže Providera. Prilikom

svog putovanja paketi ne nailaze na prepreku. Ovo je u potpunosti nesigurna situacija. Međutim, dugo godina ovaj način prijenosa podataka je bio standard. Tokom godina, mrežni inžinjeri počeli su primjenjivati širok spektar boljih riješenja, a među njima i firewall.

Vatrenim zidom (firewall, sigurnosna stijena), dakle, naziva se usmjerivač posebne namjene koji odvaja neku lokalnu mrežu (ili sustav lokalnih mreža) od ostatka Interneta. S obzirom da računalo nazvano vatrenim zidom, povezuje dvije različite mreže - tj. unutarnju/lokalnu i vanjsku - i prosljeđuje pakete iz jedne u drugu, to računalo možemo smatrati usmjerivačem, međutim, njegova osnovna funkcija nije prosljeđivanje, već **sprečavanje** da neki sadržaji budu prosljeđeni u lokalnu mrežu (koju štiti) i/ili iz te mreže.

Možemo reći da vatreni zid ima ulogu **filtra**. Naprimjer, vatreni zid može odbacivati sve one pakete/poruke (umjesto da ih proslijedi) koji dolaze iz vanjske mreže i koji su naslovljeni na neku IP adresu lokalne mreže, i/ili pak na neki TCP port. Vatreni zid može odbacivati pakete/poruke i na osnovu IP adrese pošiljatelja i time sprečavati da neki vanjski entiteti (čvorovi, procesi, komunikatori) uspostave komunikaciju sa domaćinima iz lokalne mreže koju taj vatreni zid štiti/odvaja od ostatka mreže (Slika 3.).




**Slika 3.** Položaj i uloga firewalls-a

Filtriranje komunikacije između domaćina iz lokalne mreže i ostatka mreže provodi se sa ciljem **kontrole pristupa računalima i sadržajima lokalne mreže**, kao i sa ciljem sprečavanja da se **iz lokalne mreže šalju van** neki sadržaji.

Najfundamentalnije komponente firewalla postoje unutar uma osobe koja ga konstruira a ne unutar softwarea ili hardwarea firewalla. Firewall je prije svega pojam a tek zatim produkt; firewall je ideja u umu stvaraoca koji odlučuje tko i što će biti omogućeno pristupanju mreži. TKO i ŠTO imaju veliki utjecaj na koji će način mrežni promet biti usmjeren. Zbog ovog razloga, konstruiranje firewalla je dijelom umjetnost, dijelom osjećaj, a prije svega logičko razmišljanje. Ako pretpostavimo da programer (arhitekt firewalla) zna da mora postojati Web server na mreži domaćina (host), onda je očito da će Web server prihvatiti spajanje sa bilo koje IP adrese. Zbog toga, mora biti stvoreno zabranjeno područje servera. Drugim riječima, u pružanju Web usluga od strane mreže domaćina, programer mora provjeriti ugrožava li Web server druge komponente mreže kako bi sve funkcioniralo u savršenom redu.

## 3. NAČIN RADA I VRSTE FIREWALLS-a

Firewallsi mogu biti sastavljeni od softwarea, hardwarea, ili, najčešće, od jednog i drugog. Softverske komponente mogu biti vlasnički - shareware ili besplatni - freeware. Hardware firewalla može predstavljati bilo koji hardware koji podržava upotrebu softwarea. Ako je hardverski, firewall se često sastoji samo od routera. Routeri su specifični po tome što imaju mogućnost da bilježe IP adrese. Ovaj proces bilježenja adresa omogućava nam da definiramo kojim je IP adresama dozvoljeno spajanje a kojima ne. Druge implementacije se sastoje od jednog i drugog, hardwarea i softwarea. U svakom slučaju, svi firewallsi dijele zajednički atribut: mogućnost da diskriminiraju ili mogućnost da odbiju pristup baziran na IP adresi.

### 3.1 FIREWALLS-i ZASNOVANI NA FILTRIRANJU

Postoje različite vrste firewallsa, i svaki tip ima svoje prednosti i mane. Najčešći tip firewalla odnosi se na takozvani "network-level" firewall. Network-level firewallsi su najčešće bazirani na routeru. To znači da se o pravilima tko i što može pristupiti mreži odlučuje na razini routera. Takav način obrađivanja podataka prihvaća se putem tehnike koja se zove "packet filtering". Packet filtering je proces koji proučava pakete koji dolaze do routera izvana. Firewallsi zasnovani na primjeni filtera sadrže **tablice adresa i portova**, na temlju kojih (tablica) odlučuju koje će pakete/poruke proslijediti a koje će odbaciti. Općenito, svaki redak takve tablice sadrži četiri osnovna parametra i to: **IP adresu i TCP (ili UDP) port izvora** i **IP adresu i TCP (ili UDP) port odredišta**, pritom, ti parametri mogu biti zapisani na način da označavaju cijele klase adresa ili portova (kako to ilustrira primjer koji slijedi). Takvi zapisi u tablicama mogu se koristiti za to da se **eksplicitno spriječi** komunikacija između navedenih adresa/čvorova i portova, ili pak da se **eksplicitno dozvoli** komunikacija (samo) između navedenih adresa/čvorova i portova, a da se spriječe sve druge komunikacije.

Naprimjer, redak takve tablice koji sadrži četvorku

< 192.12.13.14, 1234, 128.7.6.5, 80 >

može poslužiti vatrenom zidu kao osnova za to da odbaci ("filtrira") sve poruke/pakete koji dolaze sa porta 1234 na domaćinu čija IP adresa glasi 129.12.13.14, a koji su namijenjeni portu 80 na domaćinu čija IP adresa glasi 128.7.6.5.

Analogno, redak tablice koji sadrži četvorku

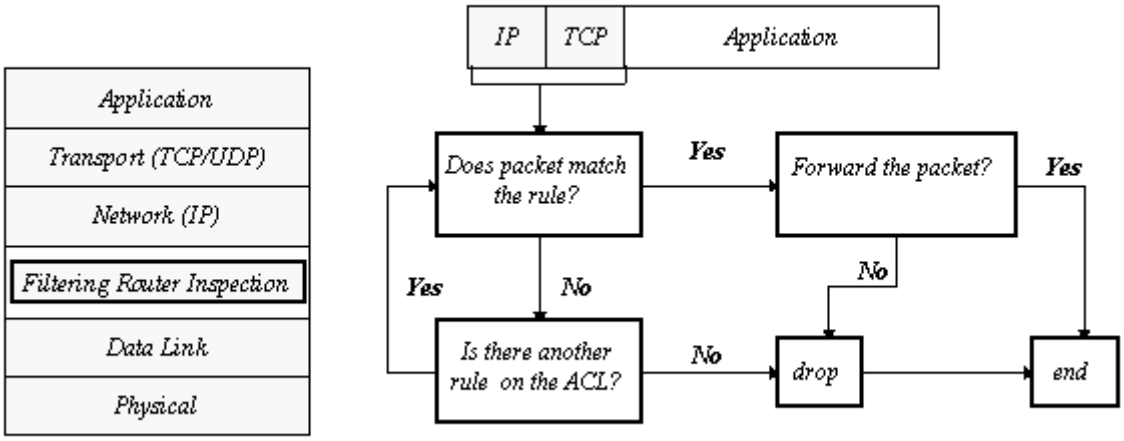
< , , 128.7.6.5, 80 >

može poslužiti kao osnova za to da vatreni zid odbaci **sve** pakete/poruke - to jest, pakete/poruke sa svih IP adresa - koji (paketi) su namijenjeni portu 80 na domaćinu čija

IP adresa glasi 128.7.6.5., tom portu na tom domaćinu ne može pristupiti nitko izvan lokalne mreže (koju taj vatreni zid štiti od ostatka mreže).

Kako je već spomenuto, zapisi iz tablica-filtera mogu biti interpretirani na "**negativan**" ili na "**pozitivan**" način. Negativnom interpretacijom nazvali smo onaj način korištenja (i definiranja) tablica-filtera kod kojeg vatreni zid **sprečava** komunikaciju između onih čvorova/procesa (tj. IP adresa i/ili portova) koji su navedeni (eksplicitno, ili implicitno, pomoću znaka "") u tablici-filteru. U gornjem primjeru uzeli smo da je tablica-filter definiran tako da sprečava komunikaciju između čvorova/procesa koji su navedeni u tablici-filteru, uzeli smo da vatreni zid radi uz negativnu interpretaciju zapisa iz tablice-filtera. Kod pozitivne interpretacije, filter **omogućava** komunikaciju samo između onih čvorova/procesa (tj. IP adresa i/ili portova) koji su navedeni u tablici-filteru, a onemogućava/sprečava (odbacivanjem paketa/poruka) svaku drugu komunikaciju između vanjske mreža i lokalne mreže.

Slika 4. zorno prikazuje na koji način firewall ispituje pojedine pakete i na osnovu postavljenih parametara odlučuje što s njima napraviti.




**Slika 4.** Koraci pri ispitivanju i filtriranju
(pristup temeljen na "oni koji nisu dopušteni su zabranjeni")

Firewallse koji su bazirani na routerima odlikuje brzina a jedan od glavnih razloga leži u činjenici da firewall vrši samo površnu provjeru adresa jer nije potrebno previše vremena da bi se identificirala loša ili zabranjena adresa. No takav firewall ima i neke mane. Samim time što dotični koriste izvorišnu adresu kao indeks, paketi koji se eventualno šalju sa lažne adrese mogu zadobiti pristup serveru.

U osnovi, mnoge tehnike filtriranja paketa mogu biti iskorištene sa ovom vrstom firewallsa a podupiru ovu ranjivost. Zaglavlje IP adrese nije jedino polje paketa koje moze biti "uhvaćeno" od strane routera. Pošto tehnologija filtriranja paketa postaje sve sofisticiranija isto se zahtjeva i sa pravilima pod kojima rade

firewallsi. Danas je tako sve češće korištenje pravila koje obuhvaćaju indekse koji se odnose na vrijeme, protokole i portove.

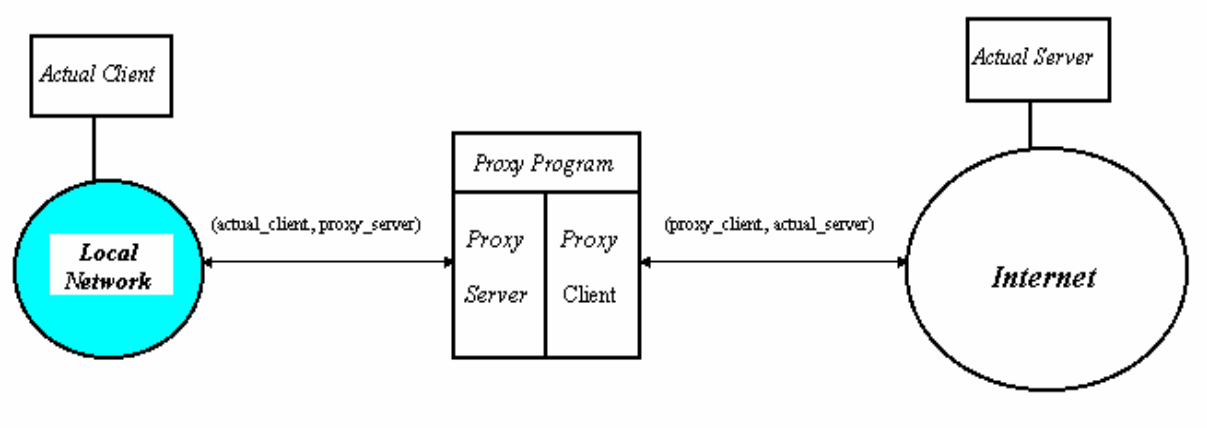
No, to nisu svi nedostatci koji pogađaju ovu vrstu firewalla pa se često spominje i broj RPC (Remote Procedure Call) usluga koji su vrlo zahtjevni za efikasno filtriranje zbog toga sto serveri "osluškuju" portove koji se dodjeljuju prilikom podizanja sistema. Pošto router ne može odrediti koji portovi se odnose na RPC usluge, nije u mogućnosti u potpunosti blokirati te usluge osim ako ne blokira u potpunosti sve UDP pakete (RPC usluge najcesce koriste UDP). Blokiranjem svih UDP-ova automatski bi se blokirale i neke vrlo važne usluge poput DNS-a tako da se danas vode brojne polemike o blokiranju RPC usluga.

### 3.2. FIREWALLS-i ZASNOVANI NA PRIMJENI PROXY-ja

Pogledajmo vatrene zidove koji se zasnivaju na primjeni proxy-je. Načelno govoreći, proxy je sustav koji se nalazi između klijenta i opslužitelja, pritom, gledano sa strane klijenta, proxy poprima ulogu opslužitelja, dok gledano sa strane opslužitelja, proxy poprima ulogu klijenta.

Proxy općenito pohranjuje u svojoj memoriji kopije raznih sadržaja (podataka, upita i odgovora) koji se često razmjenjuju u okviru komunikacije između klijenata i nekog opslužitelja. S obzirom da se ti upiti (i odgovori) često ponavljaju (od strane istog klijenta, ili pak od strane drugih klijenata), pohranjeni sadržaji ranijih upita i odgovora omogućavaju proxy-ju da **sam odgovara** na upite klijenata, bez da te upite prosljeđuje opslužitelju., gledano sa strane klijenta, proxy nastupa u ulozi opslužitelja. Ako/kada se dogodi da proxy nije u mogućnosti sam odgovoriti na neki upit klijenta, onda proxy **prosljeđuje taj upit opslužitelju**., gledano sa strane opslužitelja, proxy tada nastupa u ulozi klijenta.

Spomenimo da je jedan popularan oblik primjene proxy-ja vezan uz rad Web-opslužitelja. Proxy pohranjuje Web-stranice koje se donose na nekog domaćina sa nekog udaljenog domaćina, ako kasnije netko hoće pristupiti nekoj od tih stranica, onda mu ta stranica može biti dana izravno sa proxy-ja (na kojem je pohranjena), tako da ju nije potrebno ponovno donositi sa udaljenog domaćina. Naravno, proxy ima ograničen memorijski prostor (i odbacuje ono što je "zastarjelo"), nadalje, stranice sa proxy-ja nisu sasvim nove, njihovi vlasnici mogli su ih u međuvremenu izmijeniti. Konačno, čini se da neki Web-opslužitelji ne dopuštaju uporabu proxy-ja.




**Slika 5.** Primjena proxy-ja kod zaštite

Uzmimo da neka tvrtka ima svoje ispostave na udaljenim lokacijama, a da se njen Web-opslužitelj nalazi u sjedištu tvrtke. Uzmimo nadalje da tom Web-opslužitelju smiju pristupati svi domaćini i procesi koji pripadaju lokalnim mrežama te tvrtke (oni u sjedištu i oni na udaljenim lokacijama), ali ne smije mu pristupiti nitko drugi (nijedan čvor/proces izvan tvrtke). Takav zahtjev može se realizirati pomoću jednog vatrenog zida koji filtrira (tj. odbacuje) sve poruke osim onih koje dolaze sa IP adresa domaćina koji pripadaju toj tvrtki.

Međutim, ukoliko tvrtka ne želi zabraniti pristup svom Web-opslužitelju, već samo **nekim svojim Web-stranicama**, onda to ne može napraviti pomoću filtera, odnosno na osnovu tablica-filtera kako smo ih iznad definirali. Jer na osnovu svakog retka takve tablice može se zabraniti pristup domaćinu i/ili portu (npr. portu 80, HTTP protokola), ali ne i pristup pojedinačnim URL adresama. Zato se za realizaciju takvog zahtjeva koristi proxy, odnosno vatreni zid koji se zasniva na primjeni proxy-ja. Slika 5. ilustrira na koji način se to čini.

Poruke (upiti) koje dolaze iz vanjske mreže (tj. sa čvorova koji ne pripadaju toj tvrtki), a koje su su upućene Web-opslužitelju tvrtke, dospijevaju na proxy. Proxy uzima **URL-adresu izvora poruke/upita** te na osnovu svojih **tablica-filtera** odlučuje smije li se tom izvoru dopustiti pristup traženoj Web-stranici (tj. URL-adresi na Web-opslužitelju tvrtke), ili ne.

Ako smije, onda proxy uspostavlja HTTP/TCP vezu sa Web-opslužiteljem tvrtke i prosljeđuje mu primljeni upit, ako ne smije, onda proxy odbacuje taj upit. U slučaju prosljeđivanja upita, Web-opslužitelj vraća proxy-ju odgovor (tj. sadržaj tražene stranice), proxy zatim taj odgovor/sadržaj prosljeđuje izvoru koji je uputio dani upit. U slučaju kada proxy odbaci upit (i ne dopusti pristup trženoj URL-adresi), onda tražitelju može uputiti poruku o zabrani pristupa, ili jednostavno o greški.

Sudeći prema iznijetim prikazima, vatreni zid koji se zasniva na **primjeni proxy-ja** (proxy koji radi na opisani način, jest vatreni zid) i vatreni zid koji se zasniva

na **primjeni filtera** koriste istu osnovnu metodu rada. Proxy prvenstveno omogućava "finije filtriranje" utoliko što ne radi samo sa IP adresama i portovima, već u svojim tablicama vodi preciznu evidenciju o mogućnosti pristupa pojedinačnim URL-adresama. Međutim, u oba slučaja, filtriranje se zasniva na evidencijama entiteta (tj. na tablicama) kojima netko smije ili ne smije pristupiti.

Međutim, pored samog filtriranja, proxy obično obavlja i neke druge funkcije, naprimjer, proxy može usmjeravati promet na različite opslužitelje (unutar lokalne mreže koju štiti) i pohranjivati neke primljene poruke te ih naknadno prosljeđivati na odredišta, ili koristiti ih za vlastite potrebe.

Prednost application-gateway proxy modela je nedostatak IP proslijeđivanja te, što je važnije, više kontrola može biti primjenjeno na vezu udaljenog hosta. Naposlijetku, takvi alati često pružaju sofisticirane usluge logiranja. Iako ovakav oblik firewalla predstavlja odlično riješenje, ovakva shema "košta" firewall brzine. Zbog prihvaćanja svake veze i svih paketa, njihove provjere, prevođenja i proslijeđivanja, application gateway može biti i sporiji od router baziranog firewalla. IP proslijeđivanje pojavljuje se kada server primi zahtjev izvana i zatim proslijedi informaciju u IP formatu prema internoj mreži. Ostavljajući IP proslijeđivanje uključenim kompanije i korisnici koji koriste firewall često griješe jer se na taj način omogućava *crackeru* pristup izvana i otvara mu mogućnost pristupa internoj mreži. Druga negativna odlika ove sheme je u načinu upravljanja mrežnim servisima jer je za svaki servis potrebno napraviti posebnu proxy aplikaciju (za FTP, za Telnet, za HTTP, itd.). Ovaj problem je John Wack odlično objasnio u svom članku "Application Gateways":

"...Mana aplikacijskih gatewaya je ta, da u slučaju klijent - server protokola kao što je Telnet, su potrebna dva koraka za spajanje "inbound" ili "outbound". Neki aplikacijski gatewayi zahtjevaju modificirane klijente, koji se mogu gledati kao mana ili prednost, ovisno o tome smatra li korisnik da je na taj način lakše koristiti firewall. Telnet application gateway ne treba nužno modificiran Telnet klijent, ali zahtjeva modifikaciju u ponašanju korisnika: korisnik se mora spojiti (ali ne i logirati) na firewall kao što se spaja direktno na hosta. Ali modificirani Telnet klijent može učiniti firewall transparentnim zabranjujući korisniku specificiranjem odredišta sistema Telnet naredbom. Firewall bi tada služio kao put ka odredistu sistema i tako presreo vezu, i tada izveo dodatne korake ako je potrebno. Ponašanje korisnika ostaje isto, uz potrebu za modificiranim klijentom na pojedinom sistemu..."

## 4. IZGRADNJA FIREWALLS-a

U izgradnju firewalla ne može se upustiti bilo tko. Uobičajeno, u takve projekte ulaze sistemski administratori ili druge individue koji poznaju mrežna pravila i ustrojstvo mreže općenito, a i mrežu koju namjeravaju zaštiti firewallom. Ovaj proces nije jednostavan, a nekoliko glavnih koraka (kojih se treba pridržavati) su:

1. Poznavanje mreže i potrebnih protokola
2. Razvijanje primjerenih pravila
3. Posjedovanje adekvatnog alata
4. Korištenje alata na efektan način
5. Testiranje konfiguracije
6. Poznavanje mreže i ostala pravila

Prvi korak koji je potrebno znati u ovom složenom procesu je struktura, odnosno unutrašnjost mreže. Ovaj zadatak može uključivati i više nego puko nadgledanje mreža, logova, itd. Može uključivati i sporazumjevanje sa drugim organizacijama istog cilja. Na primjer, u većim mrežama, može postojati interakcija između određenog ureda u jednoj zgradi i određenog ureda u nekoj drugoj zgradi. Te zgrade mogu biti udaljene i stotine, pa i tisuće kilometara jedna od druge, no mora se znati koji tip odlaznog prometa korisnici zahtijevaju. Također dobar programer, i u ovom slučaju tvorac firewalla, često nailazi na korisnike koji ne vole promjene i vole raditi politikom tipa "Radimo ovako već deset godina, pa zašto ne bi i dalje tako." Iako programer u ovakvim slučajevima ima "odriješene ruke" (zbog važne uloge sigurnosti, a i rizika), on treba raditi sa ljudima koji nisu navikli na promjene kako bi zajedno pronašli adekvatno i prihvatljivo riješenje za obje strane kako ne bi u budućnosti došlo do eventualnih problema. Nadalje, njihova podrška je potrebna jer nakon što arhitekt firewalla završi svoj posao, morati će u suradnji sa korisnicima izdati i pravila pod kojima će se raditi. Što prisnije korisnici budu vezani za ta pravila to će sigurnost dotične mreže biti bolja. Na primjer, ako su neosigurani modemi smješteni u nekom od ureda, oni predstavljaju sigurnosnu rupu putem koje je moguće izvesti napad na mrežu. Pravilnim konzultiranjem lokalnih korisnika, neće biti razloga za strah jer će oni postupati po pravilima koja su prije utvrđena i na taj način kontrolirati svoj rad i rad tih modema. Dakle, prvi posao arhitekta firewalla je utvrđivanje što smije a što ne smije biti zabranjeno korisnicima. Utvrđivanjem pravila prelazi se na sljedeću točku izgradnje firewalla. Određivanje tko (ili što) ne smije dospijeti unutar mreže nije toliko kompleksni zadatak kao prije navedeni. Više nego vjerojatno, arhitekt će željeti blokirati pristup mreži prometu koji dolazi od strane mreža poznatih po eksplicitnim ili pornografskim materijalima, a i sličnih koji nisu u opisu posla koji je u opisu odredjene mreže. Također, moguća je i zabrana pristupa adresama koje su poznate po hakerskim ili crackerskim odlikama. Na primjer, dobro

poznata grupa hakera nedavno je provela veliko skeniranje američkih domena u potrazi za mogucim žrtvama, pod krinkom sigurnosnog istraživanja. Ovo je dovelo do neugodne situacije brojne u svijetu sigurnosti i zato je potrebno takve adrese filtrirati kako bi se odmah u početku spriječila zlonamjerna aktivnost i osiguralo od napada.

## 4.1 KOMERCIJALNI FIREWALLS-i

U ovom odjeljku bit će ukratko dat prikaz komercijalo dostupnih firewall programa.

**Zone Alarm / Zone Alarm Pro** je vrlo "prijateljski" raspoložen prema korisnicima. Upozorenja su opisna. Možda baš i nije najbolji za profesionalce, jer se čini vrlo jednostavan. Za početnike, nema boljeg programa. ZoneAlarm je jedini firewall koji osim pokušaja ulaska u korisnikovo računalo posmatra i programe koji šalju informacije sa korisnikovog računala. To je vrlo bitno ako slučajno imate trojanskog konja. Svaki program će biti blokiran ako se pokuša spojiti na internet. Onda korisnik može odlučiti da li da dozvoli vezu, da je dozvoli samo jedan put ili da nikada ne dozvoli da se taj program spoji na internet. Kasnije se korisnik može predomisliti i promjeniti odobrenja. Također, ZoneAlarm ima opciju koja kada se uključi, trenutno blokira svu vezu s internetom. Jedino bolje rješenje je da se isključi računalo. Provjerena zaštita,a plaća se ... ništa.

**BlackICE Defender** Ako ste lovac na glave, ovo je firewall koji morate imati. Ne zamara vas pitanjima šta da činite, nego sam od sebe pokušava da otkrije prijetnje vašem računalu. Najveći razlog slave ovoga programa je da ne samo da blokira napade, nego ih pamti i otkriva informacije o napadaču. Većina programa se oslanja na informacije koje se lako mogu otkriti, ali baš i nisu korisne, BlackICE pokušava (i vrlo često uspijeva) da otkrije IP adresu napadača. Nakon toga imate opciju da pošaljete te informacije napadačevom internet servisu. Poslje toga često usljedi isključenje korisnika. Loša osobina BlackICE_a je da ga je se teško riješiti ako ga više ne želite.

**McAfee.com Personal Firewall** je online servis sa malo opcija koje možete mjenjati, a koje bi služile vašim potrebama. Ipak, obavlja glavne dužnosti što i nije loše za 30 dolara. Svake godine, nakon plaćanja te cijene, možete završiti sa sve boljim programom, tako da se ne bi trebali žaliti. U drugu ruku, dobar program bi trebao trajati više od godinu dana. Najviše ga se preporučuje korisnicima ostalih McAfee proizvoda, kao i tvrtkama da bi lakše izlazili na kraj sa svim programima (firewall, anti-virus, system tools...).

**Norton Personal Firewall 2001 (2002)** Najnovija verzija je malo skupa ($50), ali s time dobijate mnoštvo funkcija koje možete "krojiti" po svojoj želji. Razni stupnjevi sigurnosti i sigurnosna pravila koja možete mjenajti su glavne karakteristike

ovog programa. Zaštita vaše privatnosti, koja ne dolazi sa ostalim programima koje spominjemo je vrlo dobra funkcija koju nebi trebali zanemariti. Na primjer, možete unjeti svoje ime, prezime, adresu ili broj telefona, i te informacije će biti spriječene da se šalju putem internet aplikacija (ali ne i e-mail).

**Sygate Personal Firewall** ima mogućnost "zatvaranja" portova ako programi koji obično koriste te izlaze nisu aktivni. Također ima i mogućnost postavljanja različitog stupnja sigurnosti za različito doba dana. Tako da kad odete na posao, a ne želite iskljuciti PC, mozete postaviti veću sigurnost kada niste tu. Slično BlackICE Defender-u, imate mogućnost otkrivanja uljeza kao i tehnike koju su koristili pri pokušaju ulaska u vaše računalo. Besplatan za osobnu upotrebu, 30 dolara za tvrtke.

**Tiny Presonal Firewall** lako se zove "tiny" (slob. prev. "maleni"/"sitni"), ovaj firewall ide ruku-pod-ruku sa ostalima na tržištu. "Free" za osobnu upotrebu, 40 dolara za komercijalne korisnike. Koristi manje resursa vašeg računala nego ostali programi. Nedostatak je da nije razumljiv početnicima. Upozorenja su "španska sela", koja čak i napredni korisnici ne mogu razumjeti. Također ima mogućnost "udaljene" administracije, tako da kompanije mogu imati centraliziran pristup svakom računalu u mreži i mjenjati nivo zaštite za svakog korisnika posebno.

Na kraju, odluka koji je program najbolji za vas će biti vaša. Tvrtke moraju uraditi "domaću zadaću" i dobro razmisliti što kupiti. Kupovinu hardware firewall-a ne treba isključiti ni u kom slučaju, ako ste imalo ozbiljnija tvrtka. Za kućnu upotrebu kao i za manje firme, ZoneAlarm je više nego dovoljan. Glavno pitanje je želite li da se vaše računalo sam suoči s legijama hakera i dječice koja žele postati "face", ili ćete ipak pomoći sami sebi i spriječiti četu luđaka da vam uđe u sustav.

## 5. ZAKLJUČAK

Jedna od glavnih ideja pri postavljanju firewalla kao zaštitnika mreže je u činjenici da bi mreža teoretski trebala biti nevidljiva ili u krajnjem slučaju nedostupna svima koji nemaju autorizirani pristup. No, mreža zaštićena firewallom ipak neće u popunosti biti imuna na sve vrste nedozvoljenog pristupa. Tako program (stealth scanner) pod nazivom Jakal, može skenirati domenu koja se nalazi iza firewalla bez ostavljanja tragova. Firewall također ne pruža adekvatnu zaštitu od virusa, već se za to preporuča upotreba posebnih anti-virusnih programa.

Sa teoretskog aspekta, firewall je najstroža sigurnosna mjera koja se može implementirati. No u svakom slučaju, rasprave o najstrožem sigurnosnom okruženju ostaju i danas. Prva stvar oko koje se vode diskusije je o sigurnosnim mjerama koje se provode putem firewalla za koje se smatra da "strogo" konfiguriranje može usporiti mrežne procese. Na primjer, neke studije pokazuju da je korištenje firewalla nepraktično u okruženjima gdje korisnici ovise o distribuiranim aplikacijama. Zbog primjene strogih sigurnosnih pravila, takva okruženja postaju sporija jer dobivanjem na sigurnosti, gubi se na funkcionalnosti. Sveučilišta su odličan primjer za ovaj tip okruženja. Istraživanja na sveučilištu se obično provode u suradnji dvaju ili više odjela u kojoj je potrebna konstantna razmjena podataka. U ovakvim okruženjima, rad pod navedenim sigurnosnim ograničenjima postaje gotovo nemoguć. Drugi problem je u tome sto firewallsi predstavljaju "usko grlo" mrežnog okruženja, zbog autorizacijskih procesa i ostalih sigurnosnih mjera. No i takvi uvjeti su prihvatljivi dok je firewall pouzdan u radu. Prije izgradnje firewalla treba provesti ozbiljna istraživanja kojima se treba upoznati mrežno okruženje jer je potrebno uskladiti brojne mrežne uređaje da komuniciraju međusobno bez problema. Takvo nešto postiže se automatiziranim procesima ili ljudskom interakcijom. Automatizirani procesi se mogu pokazati kao lako prilagodljivi dok se procesi koji nastaju ljudskim faktorom mogu u mnogome razlikovati...

Za neke organizacije, firewall je čisto nepraktičan. ISP-ovi se nalaze unutar ovog razreda. Glavni razlog je u novcu koji dolazi od korisnika, a strogim sigurnosnim mjerama stvorilo bi se okružje koje bi "otjeralo" korisnike svojim strogim pravilima. No postoje i drugi problemi prilikom postavljanja firewalla. Ako bi FTP, Telnet, Gopher, HTTP, RPC, rlogin, i NFS bili protokoli koji bi se koristili na Internetu, firewall bi se suočio samo sa ograničenim problemima pristupa mreži. Problem je u tome što se gotovo svaki mjesec pojavljuju novi protokoli i servisi. Kako bi se korisnicima pružio efektan Internet pristup, potrebno je ići u korak sa novim trendovima koje zahtjeva tržište. Proxiji za takve aplikacije/protokole će biti dostupni no tek neko vrijeme nakon izlaska protokola na tržiste. Naravno, neko vrijeme označava razdoblje i od nekoliko mjeseci, tijekom kojega će korisnici biti nezadovoljni.

## 6. LITERATURA


[1] "Internet Firewalls": uvod. NMI Internet Expert Services.
http://www.netmaine.com/netmaine/whitepaper.html

[2] "Features of the CentriTM Firewall". Centri.
http://www.gi.net/security/centrifirewall/features.html

[3] "Secure Computing Firewall for NT". Pregled.
http://www.sctc.com/NT/HTML/overview.html

[4] "How Firewalls Work"
http://www.howstuffworks.com