VISOKA POSLOVNA ŠKOLA
STRUKOVNIH STUDIJA
ČAČAK

SEMINARSKI RAD

Predmet: Raļunarske mreģe i mreģno programiranje

Zaģtita RM(Firewalls)

Mentor:_____
Profesor: _____

Student: _____
Br.Indeksa: _____

SADRŽAJ

POGLAVLJE I

POGLAVLJE II

POGLAVLJE III

POGLAVLJE I

1. UVOD

1.1.ŠTA SU FIREWALL-OLI?

Firewall je sigurnosni element smješten između neke lokalne mreže i javne mreže (Interneta), a koji je dizajniran kako bi zaštitio povjerljive, korporativne i korisničke podatke od neautoriziranih korisnika, (blokiranjem i zabranom prometa po pravilima koje definira usvojena sigurnosna politika). Nije nužno da svi korisnici u LAN-u imaju jednaka prava pristupa Internet mreži.Postavljanjem Firewall uređaja između dva ili više mrežnih segmenata može se kontrolirati i prava pristupa pojedinih korisnika pojedinim djelovima mreže. U takvom slučaju Firewall je dizajniran da dopušta pristup valjanim zahtijevima, a blokira sve ostale. Firewall ujedno predstavlja idealno rješenje za kreiranje Virtualne Privatne mreže jer stvarajući virtualni tunel kroz koji putuju kriptirani podaci.(omogućuje sigurnu razmjenu osjetljivih podataka među dislociranim korisnici)Firewall je servis (koji se tipično sastoji od firewall uređaja i Policy-a (pravilnika o zaštiti), koji omogućuje korisniku filtriranje određenih tipova mrežnog prometa sa ciljem da poveća sigurnost i pruži određeni nivo zaštite od provale.

Osnovna namjena Firewall-a je da spreči neautorizovani pristup sa jedne mreže na drugu. U suštini, ovo znači zaštitu unutrašnje mreže od Internet-a. Ako vaš sistem raspolaže Firewall-om, to znači da je odluka o tome šta je dozvoljeno, a šta nije - već donijeta. Ove odluke su u direktnoj vezi sa politikom sigurnosti vašeg informacionog sistema. Pri planiranju ponude informacionih servisa, politika sigurnosti određuje opcije konfiguracije servisa.
Osnova rada Firewall-a je u ispitivanju IP paketa koji putuju između klijenta i servera, čime se ostvaruje kontrola toka informacija za svaki servis po IP adresi i portu u oba smjera.Za Firewall je tipičan i kompromis između sigurnosti i lake upotrebe. Stav da "sve što nije dozvoljeno je zabranjeno" zahteva da se svaki novi servis individualno omogućava.

Firewall je odgovoran za više važnih stvari unutar informacionog sistema:

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

Firewall može biti softverski ili hardverski. Softverski firewall omogućuje zaštitu jednog računara , osim u slučaju kada je isti računar predodređen za zaštitu čitave mreže. Hardverski firewall omogućuje zaštitu čitave mreže ili određenog broja računara. Za ispravan rad firewall-a, potrebno je precizno odrediti niz pravila koja definiraju kakav mrežni promet je dopušten u pojedinom mrežnom segmentu. Takvom politikom se određuje nivo zaštite koji se želi postići implementacijom firewall usluge.

POGLAVLJE II

2. PODJELA POTENCIJALNIH 'NAPADAČA'

2.1. ZAŠTITA LOKALNE MREŽE OD ŠTETNOG DJELOVANJA 'NAPADAČA'

Firewalli koji nemaju čvrste i stroge politike prema dolaznim paketima podložni su različitim vrstama napada. Ukoliko firewall ne podržava kreiranje virtualnih privatnih mreža, a organizacija želi omogućiti pristup sa određenih IP adresa lokalnoj mreži, moguće je konfigurirati firewall da propušta pakete sa točno određenim izvorišnim IP adresama. Ali takav način postavljanja sadrži brojne nedostatke. Na primjer napadač se može domoći paketa te saznati logičku adresu sa kojom je dozvoljeno spajanje na lokalnu mrežu. Nakon toga napadač može kreirati pakete kojim kao izvorišnu stavlja logičku adresu računara kojem je dozvoljeno spajanje i tako pomoću posebno prilagođenih paketa nanijeti štetu lokalnoj mreži.

Firewall je potrebno konfigurisati tako da onemogućava različite postojeće napade. Većina današnjih proizvođača firewalla ponosno ističe na koje napade su njihovi firewalli otporni, ali nove vrste napada se svakodnevno razvijaju i sve su kompliciraniji i kompleksniji. Ipak svaki firewall bi trebao biti otporan na poznate napade kao što su sljedeći navedeni.

- ***Address Spoofing*** napad omogućava da paket bude proslijeđen sa vanjskog okruženja na neko od internih računara ukoliko napadač kao izvorišnu adresu uzme neku od adresa unutar lokalne mreže. U tom slučaju firewall je možda konfigurisan da omogućava prolazak paketa i time ciljni računar može primiti posebno prilagođeni paket. Da bi se ovakva vrsta napada onemogućila potrebno je onemogućiti prosljeđivanje paketa koji kao izvorišnu adresu imaju neku od lokalnih adresa, a kao ulazno okruženje ono okruženje koje je spojeno na Internet.

- ***Smurf*** **napad** spada u grupu napada koje imaju za cilj onemogućavanje rada pojedinih servera i računara, tzv. DoS napad (eng. *Denial of Service*). Napadač odašilje ICMP echo request paket na broadcast adresu cijele lokalne mreže. Time su adresirana svi računari unutar lokalne mreže. Kao odredište navodi se ciljni računar koji se želi onesposobiti velikim brojem odgovora. Za odbranu od ovakve vrste napada dovoljno je u konfiguracijskoj datoteci firewalla onemogućiti broadcast paket.

- ***Syn-Flood*** napad zasniva se na napadačevom slanju velikog broja početnih konekcijskih TCP paketa koji imaju postavljenu SYN zastavicu, i ignoriranjem TCP odgovora sa postavljenim SYN i ACK zastavicama. Time su resursi ciljanog računara zaokupljeni odgovaranjem na pakete. Da bi se spriječio ovakav oblik napada potrebno je ograničiti na firewallu broj dolazećih TCP paketa.

- ***Port-Scanner*** napad zasniva se na otkrivanju otvorenih TCP i UDP portova slanjem SYN ili FIN paketa na ciljane portove i čekanjem na RST odgovor. Potrebno je ograničiti broj takvih ispitivanja.

- ***Ping-of-Death*** napad može uzrokovati rušenje operativnog sistema, ukoliko se na računar usmjeri veliki broj ICMP echo zahtjeva. Najbolje rješenje je onemogućavanje echo-request paketa, a alternativo rješenje je ograničenje broja ICMP echo zahtjeva.

2.2.ZAŠTITA OD ŠTETNOG DJELOVANJA LOKALNIH KORISNIKA

Prilikom konfigurisanja firewalla najveća se pažnja posvećuje obradi dolaznih paketa. Danas sve više komercijalnih firewalla omogućava bolju kontrolu rada uposlenika. Oni su konfigurisani na način da ne dozvoljavaju lokalnim korisnicima pristup određenim materijalima. To mogu biti porno web stranice, web stranice koje propagiraju mržnju, web stranice za skidanje raznih video i audio zapisa itd... S obzirom na činjenicu da takve stranice sve češće nastaju potrebno je osvježavati podatke unutar firewalla, tj. imati pretplatu kod distributera takvih informacija.

Organizacijama je danas veoma bitno da ograniče svojim uposlenicima preveliku slobodu na Internetu kako zaposlenici ne bi nanijeli štetu ugledu organizacije posjećivanjem određenih web stranica (npr. dječja pornografija), ali i neobavljanjem posla za koji su zaduženi. Pri uvođenju restrikcija potrebno je paziti da se ne pretjera sa ograničenjima, što bi moglo imati kontraefekt kod uposlenika . Uposlenici bi u takvoj situaciji bili u nemogućnosti da pristupe materijalima koji im pomažu pri radu, ili bi takav tretman kod njih uzrokovao tzv. pasivni otpor prema radu.

Prilikom konfiguracije firewalla moguće je primijeniti različita pravila ograničenja spajanja lokalnih korisnika na Internet. Prvi koncept bio bi da se prema svim korisnicima lokalne mreže jednako odnosi, tj. da su svi u istom položaju. Isto tako moguće je lokalna računara svrstati u klase zavisno o njihovim IP adresama. Na taj način moguće je samo jednom sektoru unutar organizacije omogućiti nesmetani pristup Internetu, a ostalim ograničen ili nikakav.

Firewall može biti konfigurisan na način da propušta sve pakete osim paketa koji su usmjereni prema računarima sa određenim IP adresama u Internetu. Na tim se računarima nalaze materijali koji nisu potrebni uposlenicima (porno materijali, audio zapisi, itd...). Moguće je primijeniti i drugačiji princip filtriranja paketa. Propuštaju se paketi koji su namijenjeni samo računarima koji imaju točno određene IP adrese, a svi ostali paketi koji dolaze sa lokalne mreže ne prosljeđuju se. Takav koncept mogu primijeniti organizacije koje svojim uposlenicima dozvoljavaju pristup samo prema računarima na kojima se nalaze podaci bitni za rad uposlenika.

2.3. "NAPLATNA RAMPA"

Onog trenutka kada se poruka "Veryfing User Name and Password" ukloni sa ekrana i počne da odbrojava naše vrijeme na Internetu, naš provajder nam je dodijelio jedinstvenu adresu koju u tom trenutku imamo samo mi na Internetu i niko drugi - to je tzv. Ip adresa ili niz od 4 broja izmedju 0 i 255 razdvojenih tačkom (npr. 213.240.4.100).
Postoji mnogo računara na Internetu koji su prikačeni 24h i imaju svoju IP adresu koja se ne mijenja, ali većina nas, koji se prikačimo s vremena na vrijeme da razmijenimo poštu ili prosurfujemo Internetom dobijamo tzv. dinamicku IP adresu (svaki provajder ih ima nekoliko i kada se neko prikači dobije prvu slobodnu). Ove adrese (odnosno brojevi) nam mogu pomoći da identifikujemo sagovornika, jer se za one stalne tačno zna kome pripadaju dok se za dinamičke vodi evidencija kod provajdera kome su bile dodeljene u odredjenom trenutku.
Kada želimo da pristupimo nekom računaru, sve što je potrebno je da otkucamo njegovu adresu, ali da bi nam prekratili muke, uvedeni su tzv. DNS (Domain Name Server) računari koji prevode adrese u IP adresu i obrnuto. Sama adresa nije dovoljna, jer je potrebno obezbijediti posebne kanale za komunikaciju kako ne bi došlo do zabune.
Zbog toga su uvedeni portovi –zamislimo ih kao autoput na ulazu u grad sa 65536 traka (koliko god pomisao na puževske brzine u domaćim uslovima ometa sliku autoputa) i dva računara se uvek dogovoraju kojim će se trakama odvijati saobraćaj. Pošto je standardizacija uvek poželjna, portovi sa brojevima manjim od 1024 su rezervisani i imaju specijalnu namjenu (znači samo za posebna "vozila") dok su oni preostali namenjeni korisnicima. Tako npr. kada skidamo neke fajlove sa ftp servera, naš računar će dotičnom slati sve komande samo na port 21, a dotični će ih samo tamo i očekivati; fajlovi će pristizati na neki proizvoljni port na našem računaru (sa brojem većim od 1024) - ponekad i na više odjednom. To objašnjava kako je moguće istovremeno surfovati na tri stranice, skidati nekoliko fajlova, slati i primati poštu i čatovati.
Problem je što mi sa običnim Windowsom nemamo nikakvu kontrolu nad saobraćajem preko portova - podaci ulaze i izlaze a mi nemate pojma ni odakle su došli ni gdje idu . Zato je potrebno postaviti "**naplatnu rampu**" i "saobraćajce" - a to je upravo firewall.

Sve što stiže sa Interneta (ili lokalne mreze) ili odlazi sa našeg računara, prolazi preko firewalla i dotični program odlučuje (uz našu pomoć) da li će to smeti da prođe ili ne.
Nekima je opet najveća zabava u životu da takvim nepažljivim ljudima obrišu sve na računaru ili urade neku sličnu podlost. A kako oni znaju da li su neka vrata otvorena i koja su to od onih 65536? Jedan način je da u naš računar ubace virus ili trojanskog konja (preko e-maila, pomoću programa u koje je zamaskiran uljez ili lično instalirajući program na našem računaru) koji će otvoriti neki unaprijed odredjeni port. Sve što zatim preostaje dotičnom hakeru je da krene da adresira sve računare kod nekog provajdera (rekli smo da svaki provajder ima nekoliko IP adresa koje dodeljuje svojim korisnicima a hakeri znaju u kom se opsegu kreću te adrese) i da uz pomoć odgovarajućeg softwarea provjeri da li je taj port otvoren.

To se naziva TCP Port Scaning i uglavnom nije štetno po naš računar (naravno - ako nemamo trojanca i imamo firewall). Drugi način je da pokuša na silu da upadne kroz neki od portova - to se naziva Denial of Service attack (skraceno DoS attack). Radi se o tome da je neke programe moguće toliko zbuniti suviše velikim podatkom ili dovoljnim brojem ponavljanja neke instrukcije da se on jednostavno sruši i sa sobom povuče ceo Windows, ili da počne da izvršava neke instrukcije koje inače ne bi sproveo u "normalnom" stanju (poput hipnotisanog čoveka). U takve programe spadaju i naši browseri, programi za poštu, chat i mnogi drugi. I sam Windows često neće odoljeti napadima na neki port sa brojem ispod 1024 i tako će se naš računar, hteli mi to ili ne, pretvoriti u ftp, POP3, telnet ili neki drugi server koji je u službi dotičnog hakera. Svaki dobar firewall će prepoznati bilo koji od opisanih napada i spriječiti napadača da bilo šta preduzme (neće mu dozvoliti pristup preko odredjenog porta iako je ovaj otvoren). Glavni problem prilikom korišćenja firewalla je prepoznati da li je dotična IP adresa prijateljska ili ne, dali je port koji se upravo otvorio pod kontrolom nekog virusa ili to naš browser uspostavlja komunikaciju sa HTTP serverom i sl. Neki to odrade automatski i preduzmu odgovarajuće akcije ako se radi o napadu, a nama pošalju odgovarajuće obaveštenje (BlackICE), dok drugi rade poluautomatski i odmah prijave svaku sumnjivu stvar i od korisnika zahtevaju da odluči šta dalje (ATGuard). Nedostatak prvih je što prijavljuju dosta lažnih uzbuna (čak i samog korisnika okarakterišu kao napadača), a nedostatak drugih je što je korisnik glavni krivac kada bez razloga izblokira neki svoj program ili stvori suviše filtera pa ne moze da uspostavi vezu sa nekim serverom. Cijela umješnost rada sa ovim programima se dakle sastoji u razlikovanju normalne komunikacije od bezazlenih skeniranja portova, zaglupljivanja servera (kada pokušaju da nam pošalju podatke na neki drugi port pored onog dogovorenog), pokušaja upada u naš računar kada neki virus uspostavi vezu sa svojim gazdom i pokušaja nekog hakera da brutalnom silom uleti u naš računar.

2.4 OSNOVNE KONCEPCIJE FIREWALL SKENIRANJA PAKETA

2.4.1 Statičko filtriranje paketa (eng. stateless inspection)
Filtriranje paketa osnovni je dio svakog firewall. U tom se dijelu odlučuje da li mrežni paket treba biti proslijeđen na drugu mrežu ili ne. Pri tome se kod statičkog filtriranja pregledavaju različiti podaci:

Vrsta protokola:1.IP adrese odredišta i izvorišta
2.Odredišni tj. izvorišni port
3.Informacije o tablici usmjeravanja paketa
4.Broj fragmentiranog paketa

2.4.2 Filtriranje paketa zavisno o vrsti protokola

Protokolno filtriranje paketa zasniva se na sadržaju IP protokolnog polja. Protokol koji se koristi unutar paketa određuje da li paket treba proslijediti ili ne.
Neki od protokola su: 1.User Datagram Protocol (UDP)
2.Transmission Control Protocol (TCP)
3.Internet Control Message Protocol (ICMP)
4.Internet Group Management Protocol (IGMP)

2.4.3 Filtriranje paketa zavisno o IP adresama odredišta tj. izvorišta

Filtriranje zavisno o IP adresama omogućava zabranu konekcija od ili prema određenim računarima i/ili mrežama, zavisno o nihovim IP adresama. Ukoliko administrator želi zaštiti mrežu od neovlaštenih zlonamjernih napadača, on može zabraniti promet mrežnih paketa koje kao odredište imaju određene IP adrese. To je poprilično beskorisno jer napadači mogu promijeniti IP adrese. Zbog toga je puno bolje dozvoliti pristup mreži samo određenim paketima koji kao odredište imaju određene sigurne IP adrese. Normalno ukoliko se napadač domogne i tog popisa on može paketima pridružiti kao odredišnu IP adresu neku iz tog popisa.

2.4.4 Filtriranje paketa zavisno o odredišnim tj. izvorišnim portovima

Prilikom spajanja jednog računara na drugo i jedan I drugi koriste određene pristupne portove. Sve ukupni broj pristupnih portova je 65536. Prva 1024 porta su rezervirana za određene aplikacije i ne mogu se koristiti za neke druge. Primjerice HTTP koristi port 80, FTP port 20 i 21, DNS port 53 itd...

Administrator zavisno o aplikacijama može ograničiti pristup mrežnim paketima. Neki aplikacijski protokoli su izrazito osjetljivi na mrežne napade pa je potrebno onemogućiti pristup istima (Telnet, NetBIOS Session, POP, NFS, X Window, ...). Ti portovi su osobiti osjetljivi na napad zbog velikog nivoa kontrole koju pružaju napadaču. Neki drugi portovi mogu biti iskorišteni da bi se uništile određene bitne informacije. Takav port je DNS.

2.4.5 Filtriranje paketa zavisno o ruti usmjeravanja paketa (eng. Source Routing)

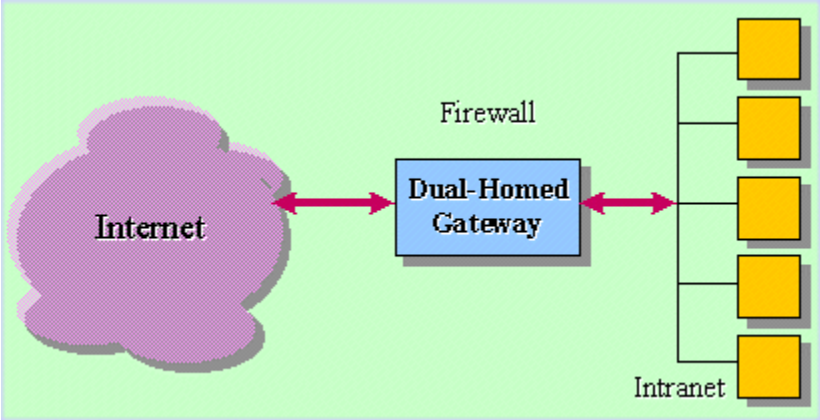
Source routing je proces određivanja točno određene rute kojom paket treba proći prilikom putovanja prema cilju odnosno prilikom povratnog putovanja. Source routing je originalno korišten za analiziranje i testiranje, ali se u današnje vrijeme koristi od strane napadača. Napadači postavljanjem bilo koje IP adrese u polje za izvorište mogu omogućiti da im se povratni paket vrati, stavljajući svoju vlastitu IP adresu. Pri tome oni mogu odrediti točnu stazu kojom paket treba proći, ili odrediti ciljna računala do kojih paket treba doći.

2.4.6 Filtriranje paketa zavisno o broju fragmentiranog paketa

U današnjim mrežama prevelike poruke se prenose raščlanjene (fragmentirane) u manje pakete. Veličina paketa za prijenos korištenjem ustaljenog IEEE 802.3 standarda jer ograničena sa maksimalnom veličinom od 1500 okteta. Početno fragmentirana poruka na izvorištu može se još dodatno fragmentirati na usmjerivačima preko kojih ta poruka prelazi. Tako raščlanjeni paketi se povezuju na odredištu u odaslanu poruku.
Moguće je na firewall-u izvesti filtriranje, na način da se odbacuje početni fragmentirani paket koji jedini sadrži port aplikacije,
i da se pretpostavi na osnovu te logike da će svi ostali paketi biti beskorisni jer neće niti doći do aplikacije. Takvo filtriranje je danas beskorisno jer napadači mogu prvom odaslanom fragmentiranom paketu umjesto rednog broja 0 dodijeliti redni broj 1. Na taj način bi poruka na kraju stigla do željene aplikacije.

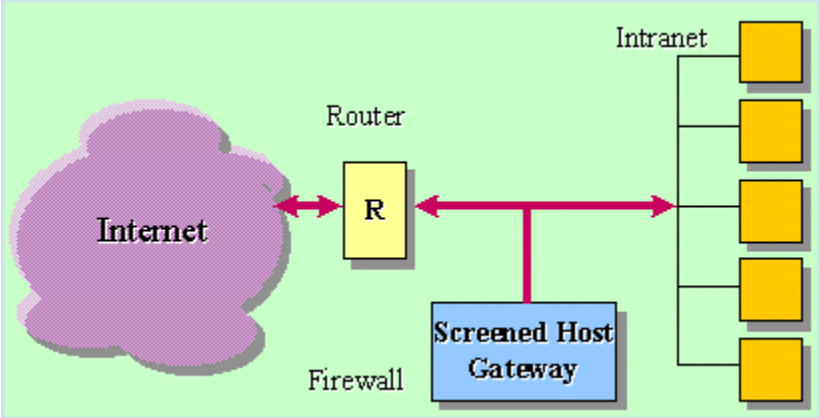
2.5 OSNOVNE FIREWALL KONFIGURACIJE

2.5.1 DUAL-HOMED GATEWAY



Dual-Homed Gateway ("među-sistemski") je Firewall koji se sastoji od računara sa najmanje dva mrežna adaptera. Ovakav sistem se normalno konfiguriše tako da se paketi ne rutiraju direktno sa jedne mreže (Internet) na drugu mrežu (Intranet). Računari na Internet-u mogu da komuniciraju sa Firewall-om, kao i računari sa unutrašnje mreže, ali je direktan saobraćaj blokiran.Glavna mana Dual-Homed Gateway-a je činjenica da blokira direktni IP saobraćaj u oba pravca. Ovo dovodi do ne mogućnosti rada svih programa koji zahtevaju direktnu putanju TCP/IP paketa. Da bi se rešio ovaj problem, Dual-Homed Gateway računari izvršavaju programe pod nazivom Proxy, da bi prosledili pakete između dve mreže. Umesto da direktno razgovaraju, klijent i server "pričaju" sa Proxy-jem, koji radi na bastion hostu. Poželjno je da Proxy bude transparentan za korisnike.

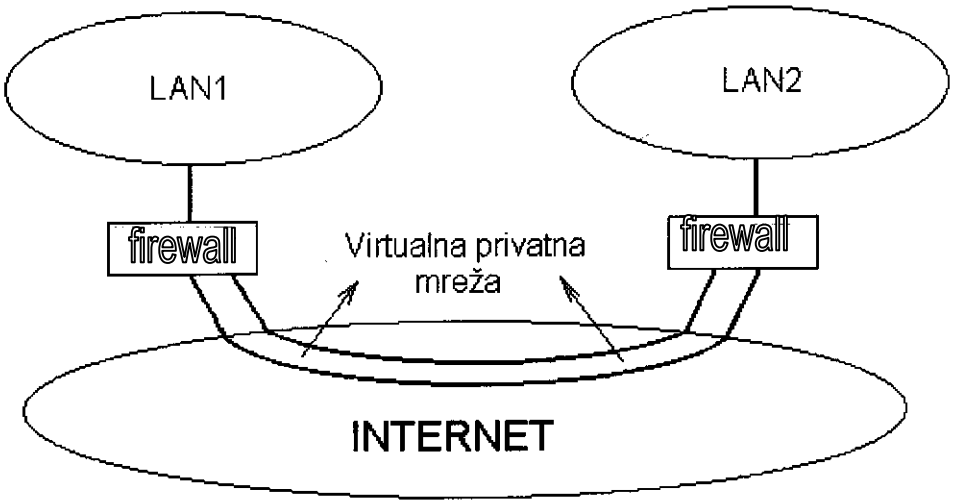
2.5.2 SCREENED HOST GATEWAY



Screened Host Gateway ("zaklonjeni") je Firewall koji se sastoji od bar jednog rutera i bastion hosta sa jednostrukim mrežnim interfejsom. Ruter se tipično konfiguriše da blokira sav saobraćaj do unutrašnje mreže tako da je bastion host jedini računar kome se može spolja pristupiti. Za razliku od Dual-Homed Gateway-a, Screened Host Gateway ne forsira sav saobraćaj kroz bastion host; pomoću konfiguracije rutera moguće je da se otvore "rupe" u Firewall-u, tako da postoji prolaz i do drugih računara u okviru unutrašnje mreže.Bastion host je zaštićen ruterom. Ruter se konfiguriše tako da dozvoli saobraćaj samo za određene portove na bastion hostu. Dalje, ruter se može konfigurisati tako da dozvoljava saobraćaj samo sa određenih spoljnih računara. Često je da se ruter konfiguriše tako da se dozvoljava prolaz svih konekcija koje su potekle sa unutrašnje mreže. Ovakva konfiguracija omogućava korisnicima da koriste sve standardne mrežne funkcije pri komunikaciji sa spoljnom mrežom bez korišćenja Proxy servisa.

2.5.3 VIRTUELNE PRIVATNE MREŽE (VPN – Virtual Private Networks)

Virtualne privatne mreže (tzv. enkripcijski tuneli) omogućavaju sigurno spajanje dvije fizički odvojene mreže preko Interneta bez izlaganja podataka neautoriziranim korisnicima. Zadatak vatrozida je da omogući sigurno stvaranje virtualne veze nekog udaljenog računala sa zaštićenom mrežom.



Primjer uspostavljanja VPN-a između dvije lokalne mreže

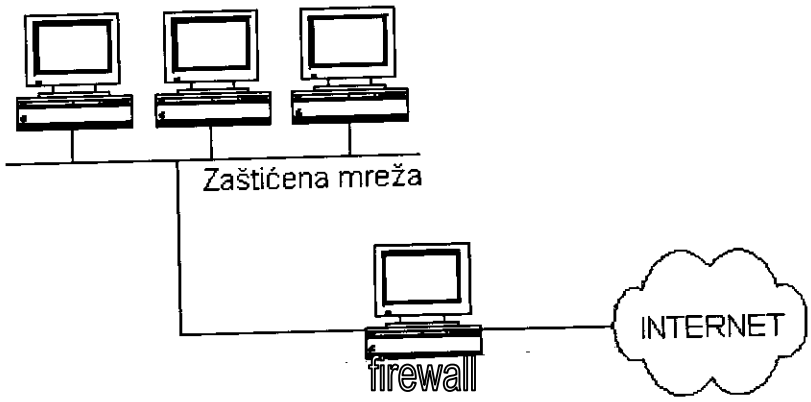
Nakon što je jednom uspješno uspostavljena, virtualna privatna mreža je zaštićena od neovlaštenih iskorištenja sve dok su enkripcijske tehnike sigurne.

Koncept VPN-a omogućava udaljenim korisnicima na nezaštićenoj strani da direktno adresiraju računala unutar lokalne mreže, što drugim korisnicima nije moguće zbog Network Address Translation-a i filtriranja paketa. Brzina kojom takvi udaljeni računri komuniciraju sa lokalnim računarima mnogo je sporija od one koju računari u lokalnoj mreži koriste. Razlog tome je njihova fizička udaljenost i oslonjenost na brzinu Interneta, ali i procesi enkripcije podataka, filtriranja paketa na firewall-u, i dekripcije originalnih podataka.

Kako bi udaljeni korisnici uspješno prošli fazu spajanja na lokalnu mrežu potrebno je da se uspješno obavi autentifikacija istih. Ta autentifikacija mora biti kriptirana da bi se spriječila krađa podataka od strane napadača i iskorištenje istih.

2.5.4 KONFIGURACIJA MREŽE BEZ SERVERA

U slučajevima kada organizacija koja koristi vatrozid ne pruža nikakve usluge korisnicima Interneta, vatrozid je dovoljno konfigurirati na način da propušta samo pakete koji napuštaju lokalnu mrežu, i pakete koji dolaze kao povratne informacije na temelju uspostavljenih veza.



Primjer konfiguracije mreže bez servera

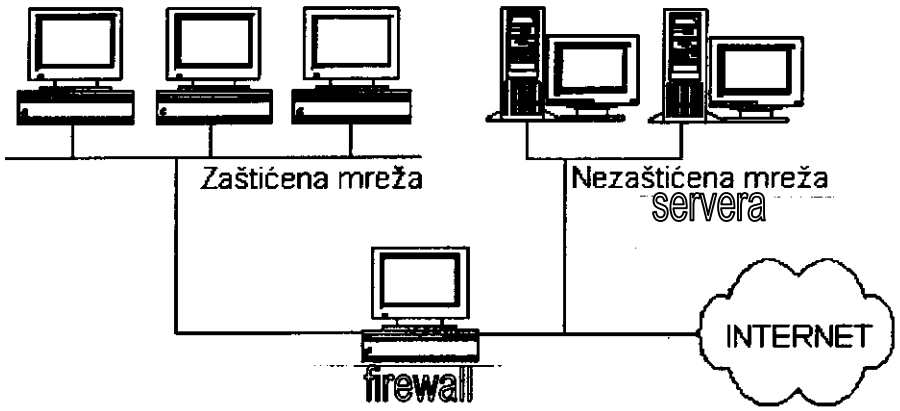
Ova konfiguracija u odnosu na konfiguracije mreža sa serveražiteljima je prvenstveno jednostavnija za konfigurirati, ali i sigurnija za lokalnu mrežu. Ali danas je takva mreža izrazito neučinkovita gledano sa poslovne i informacijske strane. Organizacije sve češće ne koncentriraju sve zaposlenike i rad na jednom mjestu, već ih raspoređuju po udaljenim lokacijama. U slučajevima kad je potrebno ostvariti vezu udaljenih lokacija, moguće je uz danu konfiguraciju jedino primijeniti fizičko povezivanje udaljenih LAN-ova što je za većinu organizacija ipak preskupo. Zbog toga je ovakva restriktivna konfiguracija rjeđa kod većih organizacija, ali češća kod kućnih ureda.

2.5.5 KONFIGURACIJA MREŽE SA JEDNIM SERVEROM I JEDNIM FIREWALLOM

Ukoliko organizacija treba imati servere onda je potrebno konfigurirati mrežu i firewall na kompleksniji način od prethodno opisanog. Lokalna mreža može biti konfigurisana na način da se koristi samo jedan firewall i serveri unutar lokalne mreže ili izvan lokalne mreže.

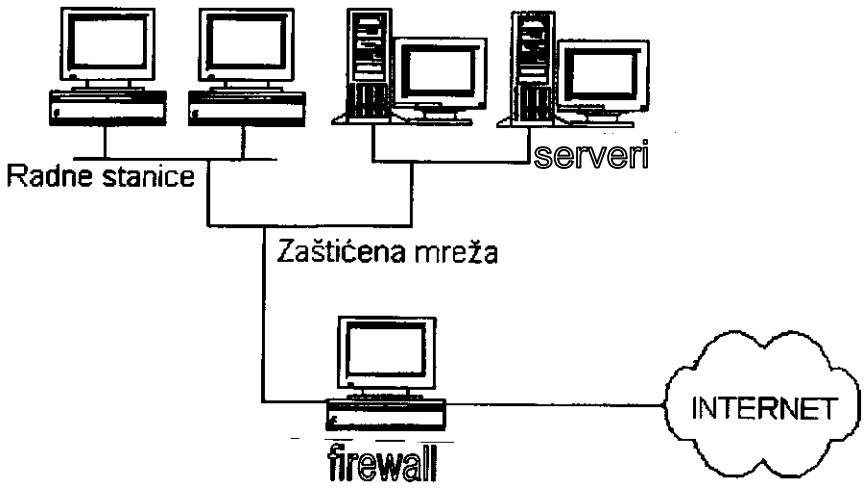
Ako je lokalna mreža konfigurisana na način da su serveri locirani izvan lokalne mreže, konfiguracija lokalne mreže i firewall-a može u potpunosti biti jednaka kao u slučaju mreže bez servera.

Takva konfiguracija koja ne dozvoljava prolazak paketa prema zaštićenoj mreži, ukoliko oni nisu dio neke prethodno uspostavljene veze, osigurava i dalje maksimalnu sigurnost za računare locirana u lokalnoj mreži. Ali računari locirani izvan lokalne mreže, koji rade kao serveri izložena su različitim napadima. Zlonamjerni napadači su u mogućnosti da izvedu DoS (eng. Denial of Service) napad, pri kojem se ostalim korisnicima Interneta, ali i lokalne mreže onemogućava korištenje usluga servera. Za organizaciju je čak puno gore od spomenutog napada ukoliko napadači modificiraju podatke koji se nalaze na serveru. Primjerice napadači mogu podvaljivati lažne obavijesti serveriima, ili čak programe koji su virusi. Time napadači mogu uvelike naštetiti ugledu organizacije.



Primjer konfiguracije mreže sa serverima lociranim izvan lokalne mreže

U slučaju kada je lokalna mreža konfigurisana na način da su serveri locirani unutar lokalne mreže, konfiguracija lokalne mreže i firewall-a je složenija. Osim dolaznih paketa koji su dio uspostavljene veze potrebno je omogućiti i prolazak početnih paketa samo prema serverima.

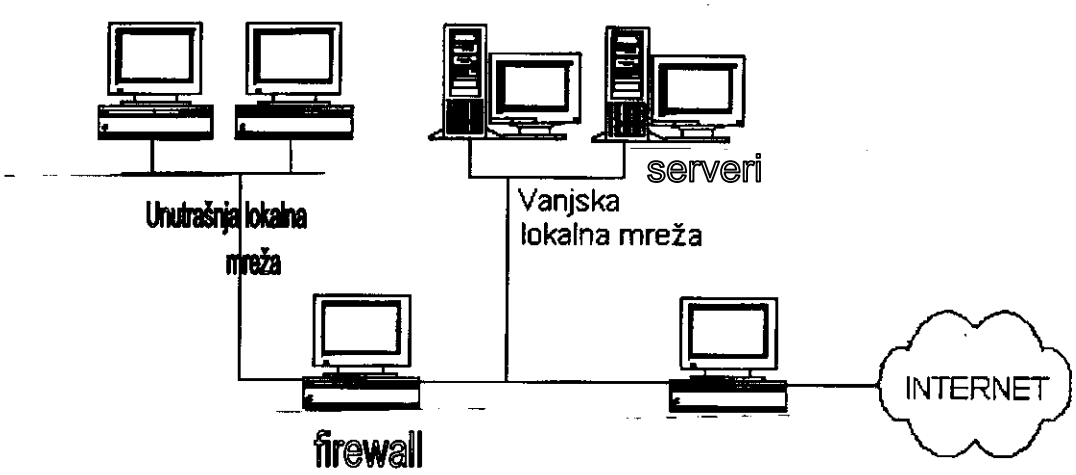


Primjer konfiguracije mreže sa serverima lociranim unutar lokalne mreže

Konfiguracija lokalne mreže sa serverima lociranim unutar lokalne mreže ostavlja brojne sigurnosne rupe koje vješti napadači mogu iskoristiti. Napadači mogu iskoristiti konfiguraciju firewalla koja propušta i početne pakete kako bi preko servera dospjeli do ostalih računala u mreži ili barem saznali određene informacije o njima.

2.5.6 KONFIGURACIJA MREŽE SA SERVERIMA I DVA FIREWALL-a

Ukoliko organizacija treba lokalnu mrežu sa serverima onda su prošla dva opisana rješenja neadekvatna jer omogućavaju različite napade. Korištenjem dva firewall-a, sprečavaju se različiti oblici napada koji bi inače bili mogući. Kao što je vidljivo sa slike , prvi firewall se spaja na Internet i mrežu servera, tzv. vanjska lokalna mreža. Između mreže servera i lokalne mreže smješta se drugi firewall.



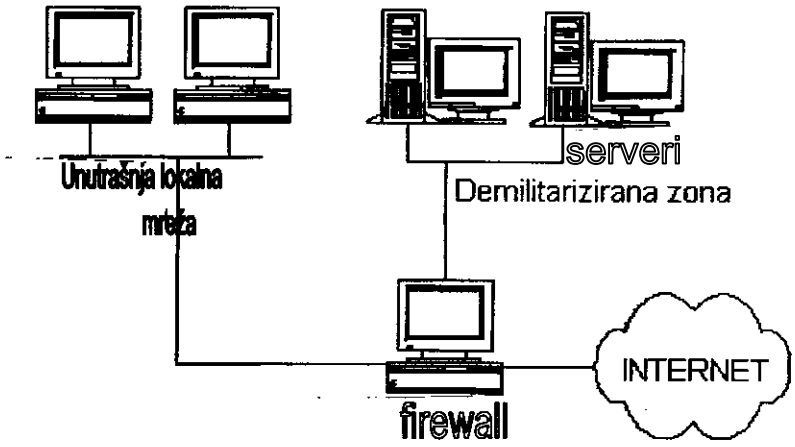
Primjer konfiguracije mreže sa serverom lociranim između dva firewalla

Politike propuštanja paketa koju firewalli primjenjuju su različite. Firewall koji štiti unutarnju lokalnu mrežu propušta samo one pakete prema unutrašnjoj lokalnoj mreži samo one pakete koji su dio neke uspostavljene veze. Firewall koji je spojen na Internet mora uz te pakete propuštati i pakete koji su namijenjeni serverima.

2.5.7 KONFIGURACIJA MREŽE SA DEMILITARIZOVANOM ZONOM

U prethodnom primjeru konfiguracije mreže potrebno je koristiti čak dva firewalla. Time se usporava brzina prenosa podataka jer podaci prolaze dvije obrade, ali i cijena cjele mreže jer je potrebno iskoristiti jedan računar kao firewall.

Rješenje za spomenuti problem je korištenje konfiguracije sa demilitariziranom zonom, koja pruža jednaku funcionalnost, ali bržu i jeftiniju od prethodno opisane. Firewallu pomoću kojeg se filtrira mrežni promet pridjeljena su dvije mreže: interna lokalna mreža i mreža servera, tzv. demilitarizirana zona.



Primjer konfiguracije mreže sa demilitariziranom zonom

Na firewallu je potrebno postaviti takvu konfiguraciju koja će propuštati na interfejs prema unutrašnjoj lokalnoj mreži samo pakete koji su dio uspostavljene veze. Prema serverima je potrebno omogućiti slanje početnih paketa i sa unutarnje lokalne mreže, i sa Interneta.

2.5.8 FIREWALL-I ZASNOVANI NA HOSTU

U ovom se slučaju koristi računar umjesto routera. To nudi mnogo više mogućnosti praćenja aktivnosti koje se odvijaju preko firewalla. Dok firewall zasnovan na routeru nadgleda pakete na IP razini, hostovi prenose kontrolu na nivou aplikacije. Da bi se osigurali od potencijalnih problema koji bi se mogli pojaviti zbog propusta u implementaciji sigurnosti u uobičajenoj programskoj podršci za mrežne usluge, firewalli zasnovani na hostovima obično koriste posebne verzije programe koji pružaju podršku potrebnim servisima. To su najčešće ogoljene verzije originalnih programa koje su zbog svoje kratkoće puno jednostavnije za održavanje, pa je i manja mogućnost za slučajne propuste (bugove) koji narušavaju sigurnost.

Osnovni nedostatak takvih firewalla je potreba za posebnom programskom podrškom za svaki od servisa koji treba podržati za mrežu "iza" firewalla. Kao dodatna mjera zaštite najčešće se koristi kombinacija zaštite na nivou aplikacije i filtrirajućeg routinga kojega također obavlja sam host ili vanjski router.

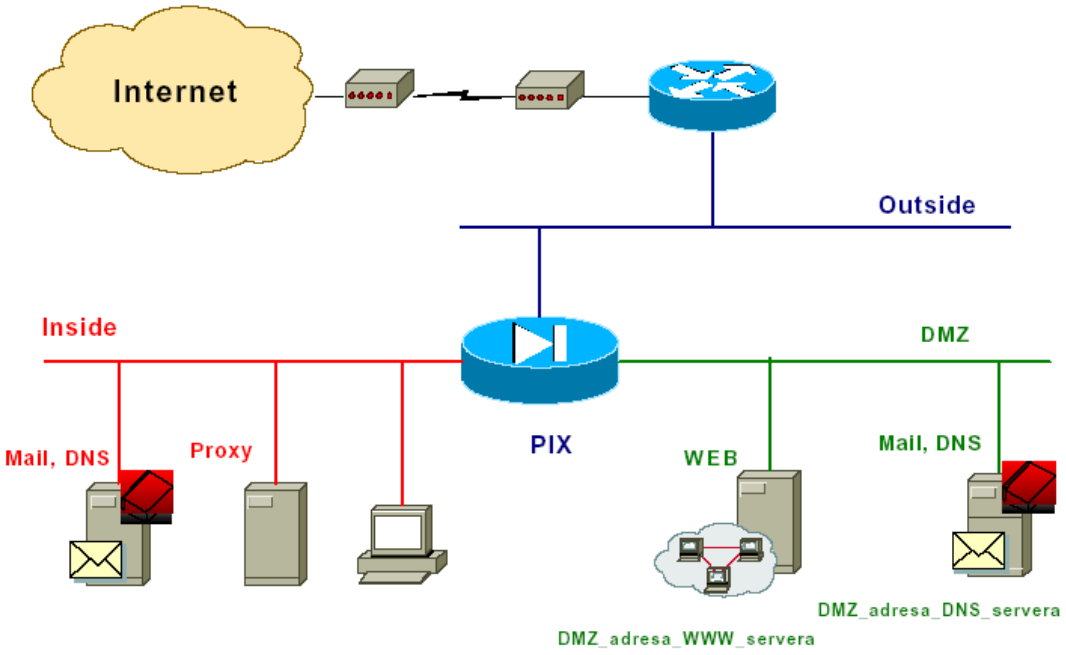
2.5.9 IZOLACIJSKE MREŽE

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

POGLAVLJE III

3.1 PRAKTIČIN PRIMJER REALNE KONFIGURACIJE Firewall-A

Bezjbedno povezivanje mreže na Internet je ostvareno korištenjem posvećenog uredaja za zaštitu Cisco 515 Firewall. Ovaj uredaj predstavlja Cisco-vo rešenje koje pruža veoma visok nivo sigurnosti za mala i srednja preduzeca. PIX platforma u potpunosti podržava implementaciju IPSec-a i formiranje VPN tunela izmedu dva PIX-a, izmedu PIX -a i Cisco VPN rutera kao i izmedu PIX -a i Cisco Secure VPNklijenta. PIX -515 sa softverom sa ogranicenom licencom ima dovoljno snage za više od 50000 istovremenih konekcija i propusni opseg do 170Mbps. Tri mrežna adaptera, koje uredaj posjeduje, omogućavaju kreirenje privatne zone u kojoj se nalazi lokalna računarska mreža kompanije, demilitarizovane zone u kojoj su smešteni javni web, mail i dns serveri i javne zone za vezu ka Internet provajderu.



Izmedu interfejsa se obavlja translacija adresa. Unutrašnja mreža ima privatne adrese, DMZ zona ima RFC 1918 adrese, a spoljna mreža ima legalne registrovane adrese (212.62.52.128/27).

Konfiguracija firewall-a je takva da je zabranjen sav saobracaj osim onog koji se eksplicitno dozvoli. Sa spoljne mreže mora biti propušten Web, DNS i Mail ka odgovarajucim javnim serverima koji su smešteni uDMZ-u.

To se postiže statickim mapiranjem adresa servera i upotrebom odgovarajucih access lista:
static (dmz,outside) 212.62.53.130 DMZ_adresa_DNS_servera netmask 255.255.255.255 0 0
static (dmz,outside) 212.62.53.132 DMZ_adresa_WWW_servera netmask 255.255.255.255 0 0
access-list outside-intf permit tcp any host 212.62.53.130 eq smtp
access-list outside-intf permit udp any host 212.62.53.130 eq domain
access-list outside-intf permit tcp any host 212.62.53.130 eq domain
access-list outside-intf permit tcp any host 212.62.53.132 eq www
access-group outside-intf in interface outside
Sav ostali saobracaj iz spoljašnje mreže ka DMZ-u je zabranjen. Iz DMZ-a ka spoljašnjoj mreži je propušten samo Mail i DNS sa Mail i DNS servera:
access-list dmz-intf permit tcp host DMZ_adresa_DNS_servera any eq smtp
access-list dmz-intf permit tcp host DMZ_adresa_DNS_servera any eq domain
access-list dmz-intf permit udp host DMZ_adresa_DNS_servera any eq domain
access-group dmz-intf in interface dmz
Što se tice komunikacije izmedu DMZ-a i privatne zone, iz DMZ-a je propušten jedinoMail sa javnog Mail servera ka internom kompanijskom serveru za elektronsku poštu. Iz privatnog dela, dozvoljen je DNS saobracaj sa Proxy servera ka DNS serveru I Mail konekcije od internog ka javnom Mail serveru. Ovim tehnickom rešenju, izlazak korisnika na Internet je predviden iskljucivo preko Proxy servera. Prema tome moraju biti propušteni odgovarajuci portovi sa Proxyservera ka javnoj zoni. U obrnutom smeru, od javne ka privatnoj zoni, zabranjen je sav saobracaj. Veoma korisna opciju koju PIX podržava je dodatna zaštita javnog SMTP servera podizanjem “Mail Guard”-a komandom: fixup protocol smtp Na ovoj nacin SMTP server može primiti samo RFC 821 komande: HELO, RCPT, DATA, RSET, NOOP i QUIT. Sve druge komande bivaju odbacene sa: “500 command unrecognized” odgovorom. Takode, svi karakteri u SMTP baneru, osim “0” i “2” se menjaju u “*”. Karakteristican baner izgleda ovako:

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

“Fixup protocol” komande koje mogu menjati servise i protokole na aplikativnom nivou primenju se i za ftp, http, h323, rsh, rtsp, sip i sqlnet protokole.

3.2 . HALTED FIREWALL-i

Halted firewall nije gotov proizvod, odnosno nije ga moguće nabaviti u obliku programskog paketa ili sklopovske konfiguracije. To je samo ideja kako poboljšati sigurnosne karakteristike firewalla baziranog na Linux alatima za filtriranje paketa (IP Chains i IP Tables).
Ideja *halted* firewalla bazira se na postupku gašenja računara s Linux operativnim sistemom. Na modernim operativnim sistemima nije moguće jednostavno ugasiti napajanje računara prilikom gašenja. U pravilu, računar prije samog prekidanja napajanja mora obaviti neke radnje kao što su spremanje zaostalih podataka na hard disk i sl., tako da se gašenje računara mora pokrenuti zadavanjem određene naredbe operativnom sistemu. U Linux-u se gašenje računara pokreće naredbama shutdown –h ili halt (ove naredbe su ekvivalentne). Nakon upisivanja jedne od ove dvije naredbe na računaru se pokreće *halt* sekvenca, tj. dešava se sljedeće:

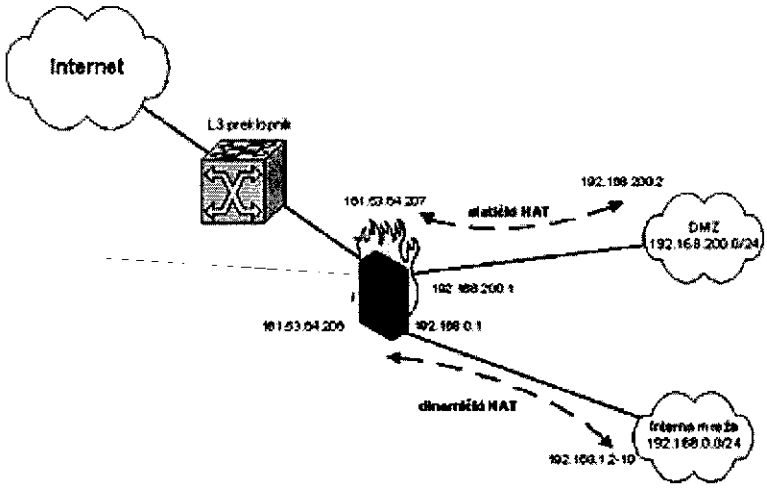
- računar prelazi u *runlevel* 0,
- izvršavaju se sve skripte iz /etc/rc0.d direktorija (ove skripte su zadužene za gašenje svih servisa i servera pokrenutih na računaru),
- gase se svi trenutno aktivni procesi,
- odspajaju (engl. *unmount*) se svi datotečni sustavi,
- gase se sva mrežna sučelja,
- miču se svi vanjski moduli iz jezgre (*kernel*) operativnog sistema.

Nakon što su napravljene sve navedene radnje, tj. nakon što je završila *halt* sekvenca, na računaru se može isključiti napajanje (kod računara s ATX kućištima se to radi automatski). Stanje u kojem se računar nalazi nakon završetka halt sekvence, a prije gašenja napajanja, naziva se *halted*. U *halted* stanju računar je, gledano od strane korisnika, "mrtvo", tj. na njemu se ne može ništa raditi jer su svi procesi, diskovi i mrežni iterfejsi ugašeni. Ali budući da su procesor i memorija još uvijek priključeni na napajanje, procesor i dalje izvršava instrukcije koje se nalaze u memoriji. U *halted* stanju u memoriji ostaje samo jezgra (*kernel*) operativnog sistema budući da su svi procesi ugašeni tokom *halt* sekvence.
Halted firewall je običan Linux firewall realiziran pomoću Linux alata za filtriranje paketa (IP Chains ili IP Tables) kod kojeg se modifikacijama *halt* sekvence postiglo zadržavanje funkcija za filtriranje paketa i u *halt* stanju. Nakon što je računar ušlo u *halt* stanje, sve njegove funkcije (osim funkcija za filtriranje paketa) su ugašene i računar radi isključivo kao firewall.

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

3.2.1 UOPŠTENO O HALTED FIREWALLU

Halted firewall je softverski firewall koji se može implementirati na klasičnom računaru i nije vezan za sklopovski specifična rješenja. Sklopovska konfiguracija računara na koje je firewall instaliran određuje performanse samog firewalla (to se najviše odnosi na brzinu rada i propusnost firewalla).
Firewall je realiziran pomoću Linux alata za filtriranje paketa (IP Tables) koji imaju ugrađenu podršku za NAT i *stateful inspection*, ali im nedostaje podrška za VPN tehnologiju i podrška za VLAN-ove.
Programska podrška pomoću koje je firewall realiziran je besplatna i dolazi standardno sa svim Linux distribucijama.
Minimalni sklopovski zahtjevi koji se preporučaju su sljedeći: procesor brzine 800 MHz, 1 GB HARD diska, 256 MB RAM memorije i dvije ili više mrežnih kartica. Zbog činjenice da firewall radi u *halted* stanju u kojem su hard diskovi isključeni, zahtjevi na veličinu hard diska nisu veliki. S druge strane, budući da u *halted* radu firewalla nema tvrdih diskova (nema ni *swap* diska), za veće mreže (više od 10 računara) potrebno je osigurati dovoljno RAM memorije kako bi firewall mogao obraditi cjelokupni mrežni promet. Isto tako, za veće mreže potrebno je koristiti i brže procesore.
Propusnost firewalla zavisi od korištenog sklopovlja. U slučaju da se koristi procesor brzine 500 MHz s 256Mb RAM memorije, firewall ima propusnost od 80Mbps.
Prilikom ispitivanja firewall je bio spojen na javnu računarsku mrežu, a iza njega su se nalazile dvije zone, interna i DMZ u kojima su postavljena računara s Linux Debian operacijskim sistemom . Testirani uređaj konfigurisan je sa tri Ethernet okruženja : vanjsko – spojeno na javnu mrežu, unutarašnje – spojeno na internu mrežu i DMZ – spojeno na štićenu DMZ zonu.
Kako je tokom testiranja simulirano stvarno pregledavanje mogućnosti uređaja, server koji se nalazi iza uređaja, a koji je spojen na DMZ okruženje između ostaloga je imao dignut Web server (Apache 1.3.24), prema kojem je s javne mreže bila uspostavljena statička ruta s pripadajućom javnom adresom. S druge strane na unutarnje sučelje spojeno je računar koje je predstavljalo internu mrežu.



Prikaz spajanja testiranog firewalla na Internet.

Osim opisane konfiguracije, za omogućavanje konekcije sa vanjske mreže na DMZ zonu korištene su i tehnika virtualnih adresa i *Proxy* ARP koji su u potpunosti podržani od strane IP Tables alata. Prilikom korištenja tehnike virtualnih adresa svi legitimni paketi pristigli na vanjskom okruženju , na port 80, preusmjeravali su se prema Web serveru na adresi 192.168.200.2.

3.2.2 PREDNOST HALTED FIREWALL-a

Osnovna prednost *halted* firewalla je činjenica da firewall radi na računaru koje je, gledano od strane korisnika, "mrtvo". Na firewallu u *halted* stanju nisu pokrenuti nikakvi servisi koji bi mogli poslužiti za neovlašteno dobivanje root ovlaštenja na samom firewallu.
Firewall je u cijelosti baziran na Linux operativnom sistemu i realiziran je pomoću standardnih Linux alata za filtriranje paketa (IP Tables) koji su standardno uključeni u sve distribucije Linux-a. Programska podrška kojom je firewall realiziran je besplatna i dolazi u sklopu distribucije tako da ju nije potrebno skidati s Interneta. IP tables programski paket se i dalje razvija, dodaju mu se nove funkcije tako da se očekuje da će mogućnosti firewalla realiziranog pomoću njega u budućnosti biti veće.
Osim navedenog, velika prednost *halted* firewalla je i njegova jednostavnost kao i cijena. Čak i neiskusniji korisnici mogu vrlo lako i brzo svladati cjeloukupnu sintaksu iptables programa. Na taj način mogu se kreirati firewalli koji u potpunosti odgovaraju korisnikovim potrebama. Također, *halted* firewall je besplatan i za njegovu izvedbu nije potrebno veliko novčano ulaganje.

3.2.3 NEDOSTACI HALTED FIREWALL-a

Nedostaci *halted* firewalla proizlaze iz same ideje rada firewalla na računaru koje je u *halted* stanju. Budući da na firewallu za vrijeme rada nije moguće pokrenuti nikakav korisnički program ili servis, logiranje događanja na firewallu nije moguće. Isto tako, administrator ne može pratiti događanja na firewallu u realnom vremenu i ne postoji mogućnost da se obavijesti administratora o neregularnim aktivnostima na firewallu. Isto tako nije moguća niti udaljena administracija i nadzor.
Administracija firewalla nije moguća za vrijeme normalnog rada. Da bi se unijele promjene u pravila za filtriranje paketa, računar je potrebno ponovno pokrenuti (za vrijeme pokretanja računara firewall je izvan funkcije) i nakon unosa promjena, ponovo vratiti u *halted* stanje.
Na firewallu su za vrijeme normalnog rada (u *halted* stanju) ugašeni hard diskovi tako da nema mogućnosti privremene pohrane podataka na *swap* disk. Ovo može biti veliki problem na mrežama s velikom prometom jer može doći do zagušenja firewalla ako u računaru nema dovoljno memorije. Preporuča se da se kod realizacije *halted* firewalla koristi računar s minimalno 256Mb RAM memorije (za mreže do 10 računara). Za veće mreže potrebno je koristiti računar s 512Mb RAM memorije ili više.

3.3 FIREWALL PROGRAMI ZA PERSONALNE RAČUNARE

Sa gledišta korisnika osobnog računara firewall ima zadatak da kontroliše i ograničava pristup RAČUNARU sa Interneta ili lokalne mreže. Njegova ideja je da na osobnom RAČUNARU mogu pristupiti samo oni kojima smo i dopustili da rade samo ono što smo im dopustili, a da svi ostali budu onemogućeni i da njihovi pokušaji budu zabilježeni.
Sad se postavlja pitanje kako sve to funkcioniše . Za razumijevanje rada firewall sistema potrebno je objasniti dva pojma, a to su IP adrese i TCP i UDP portovi. Sve što je povezano na Internet ima barem jednu jedinstvenu IP adresu. To može biti adresa našeg računara ili routera preko kojeg je naša lokalna mreža spojena na Internet. Svaki paket koji putuje Internetom u sebi nosi svoju izvorišnu i svoju odredišnu IP adresu, tako da se zna od koga je paket poslan i kome je poslan.
Drugi pojam su portovi TCP i UDP.
Korisnik putem mnogobrojnih programa (http, ftp, chat, ICQ, MSN, mail) koristi razne sadržaje na Internetu. Pitanja i odgovori prenose se u obliku TCP ili UDP paketa. Da bi se razlikovali paketi od različitih programa ,svaki program ima svoj "kanal" port po kojem šalje i prima pakete, pa tako npr. FTP koristi portove 20 i 21, Telnet port 23, HTPP port 80, ICQ portove 1508 i 1509.
Na ovaj način korisnik putem firewall sistema(programa) može dozvoliti/zabraniti promet sa određenih adresa i ograničiti rad određenih programa dozvoljavajući rad samo na određenim portovima.

- **ZoneAlarm/ZoneAlarmPro** je vrlo "prijateljski" raspoložen prema korisnicima. Upozorenja su opisna. Mozda baš i nije najbolji za profesionalce, jer se cini vrlo jednostavan. Za pocetnike, nema boljeg programa. ZoneAlarm je jedini firewall koji osim pokusaja ulaska u vas racunar posmatra i programe koji salje informacije sa našeg računara. To je vrlo bitno ako slučajno imamo trojanskog konja. Svaki program će da bude blokiran ako pokuša da se spoji na internet. Onda mi možemo odlučiti da li da dozvolite vezu, da je dozvolite samo jedan put ili da nikada ne dozvolite da se taj program spoji na internet. Kasnije se možemo predomisliti i promjenuti odobrenja. Takođe, ZoneAlarm ima dugme koje kada ga stisnemo, trenutno blokira svu vezu s internetom. Jedino bolje rješenje je da isključimo kompjuter.

- **BlackICE Defender** Najveci razlog zbog koga je na cijeni ovaj firwall je da ne samo da blokira napade, nego ih pamti i otkriva informacije o napadaču. Većina programa se oslanja na informacije koje se lako mogu otkriti, ali baš i nisu korisne, BlackICE pokušava (i vrlo često uspijeva) da otkrije IP adresu napadača. Nakon toga imamo opciju da pošaljemo te informacije napadečevom internet servisu. Poslje toga cesto usljedi iskljucenje korisnika. Losa osobina BlackICE_a je da ga je se teško riješiti ako ga više ne želimo.

- **McAfee.com Personal Firewall** je online servis sa malo opcija koje možemo mijenjati da služi našim potrebama. Ipak, obavlja glavne dužnosti što i nije loše za 30 dolara. Svake godine, nakon plaćanja te cijene, možemo završiti sa sve boljim programom, tako da se nebi trebali žaliti. U drugu ruku, dobar program bi trebao da traje više od godinu dana. Preporučuje se korisnicima ostalih McAfee proizvoda, kao i firmama da bi lakše izlazili na kraj sa svim programima (firewall, anti-virus, system tools...).

- **Norton Personal Firewall2001(2002)**Najnovija verzija je malo skupa ($50), ali s time dobijamo mnoštvo funkcija koje možemo "krojiti" po svojoj želji. Razni stepeni sigurnosti i sigurnosna pravila koja možemo mijenajti su glavne karakteristike ovog programa. Zaštita naše privatnosti, koja ne dolazi sa ostalim programima koje spominjemo je vrlo dobra funkcija koju nebi trebali zanemariti. Na primjer, možemo unijeti svoje ime, prezime, adresu ili broj telefona, i te informacije će biti sprečene 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. Takodje imamo i mogućnost postavljanja različitog stepena sigurnosti za različito doba dana. Tako da kad odemo na posao, a ne želimo isključiti PC, možemo postaviti veću sigurnost kada nismo tu . Slicno BlackICE Defender_u, imamo mogućnost otkrivanja uljeza kao i tehnike koju su koristili pri pokušaju ulaska u naš računar.

- **Tiny Personal Firewalll** iako se zove "tiny" (slob. prev. "maleni"/"sitni"), ovaj firewall ide ruku-pod-ruku sa ostalima na tržištu.. Koristi manje resursa našeg računara nego ostali programi. Nedostatak je da nije razumljiv početnicima. Upozorenja su veoma složena koja čak i napredni korisnici ne mogu razumjeti. Takodje ima mogućnost "udaljene" administracije, tako da kompanije mogu imati centralizovan pristup svakom racunaru u mrezi i mijenjati nivo zaštite za svakog korisnika posebno.

3.4 ZAKLJUČAK

U današnje vrijeme kada je Internet potreban i važan resurs u svim organizacijama veoma je bitno posvetiti određenu pažnju računarskoj sigurnosti. Pri tome firewall-i imaju veliku ulogu jer štite organizacije od brojnih zlonamjernih korisnika Interneta. Oni su prva brana koju napadač mora proći kako bi dospio do željenog cilja, zaštićenih računara.

Odabir željenog firewall-a sve je teži čemu pridonosi i sve veći broj nuđenih firewall-a. Ti firewall-i mogu biti komercijalni ili besplatni. Komercijalni obično nude lakše konfiguracije i veći broj mogućnosti. Besplatni su obično beskorisni bez stručnjaka koji bi ih konfigurisali i održavali. Osim podjele na komercijalne i besplatne vatrozidi se mogu podijeliti i na one zasnovane na Windows operativnim sistemima , te na firewall-e zasnovane na Unix/Linux operativnim sistemima . Perfomanse i mogućnosti su im u osnovi jednake i neki proizvođači firewall-a izrađuju firewall-e koji rade na oba operativna sistema .

Zavisno o potrebama organizacija ili korisnika moguće je konfigurisati lokalnu mrežu i firewall koji lokalnu mrežu štiti od neovlaštenih zlonamjernih korisnika na različite načine. Pri tome moguće je koristiti različita rješenja, bilo sklopovska ili programska.

LITERATURA

1.Andrew S. Tanenbaum, Computer Networks, Third edition, Prentice-Hall, Inc., 1996.
2.James F. Kurose, Keith W. Ross, Computer Networking: A Top-Down Approach Featuring the Internet, Addison Weslez, 2001
3. http://gislab.elfak.ni.ac.yu/
4. http://cs.elfak.ni.ac.yu/sr/postgraduates
5. http://www.google.com/