ZAVOD ZA ELEKTRONIKU, MIKROELEKTRONIKU, RAČUNALNE I INTELIGENTNE SUSTAVE
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
SVEUČILIŠTE U ZAGREBU

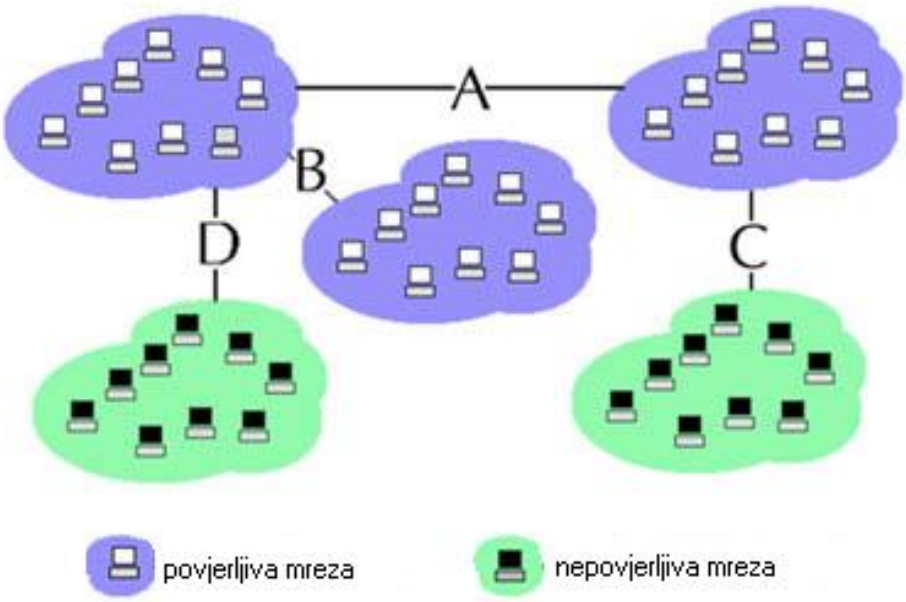
FIREWALL

IVICA KATIĆ
MREŽE RAČUNALA

Zagreb, 2003.

1. Uvod

Da bi računala mogla međusobno uspješno komunicirati, moraju koristiti standarde, pravila i protokole. TCP/IP je osnovni skup protokola koji se koristi na Internetu. Iako je razvoj TCP/IP protokola počeo za potrebe vlade SAD-a (Ministarstvo obrane), on je prvenstveno dizajniran da bude pouzdan, a ne siguran. Namjera je bila razviti protokol koji će biti dobar u dobavljanju informacija do njihove destinacije, čak i ako različiti djelovi tih informacija putuju različitim putevima. Zbog toga što se razvoj odvijao u okruženju u kojem je vladalo povjerenje, između relativno malog broja korisnika, sigurnost podataka u prometu, između korisnika, nije bila glavna briga.
Sada je Internet globalna mreža, sa više od 100 milijuna računala, gdje većina korisnika nema povjerenje prema drugima. Zato više nije mudro vjerovati drugim računalima ili korisnicima na Internetu. Ali Internet nije jedino mjesto gdje se mogu naći računala kojima se ne može vjerovati. To može biti bilo koja mreža nad kojom nemamo kontrolu.
Kada spajamo privatnu mrežu na Internet, u biti spajamo našu privatnu mrežu direktno na svaku mrežu koja je spojena na Internet. Ne postoji jedna centralna točka kontrole sigurnosti.
Firewall (prijevod na hrvatski jezik: sigurnosna stijena, vatrozid) koristimo kako bi stvorili sigurnosne kontolne točke na granicama privatnih mreža (slika 1). Na tim kontrolnim točkama, firewall ispituje sve pakete koji se razmjenjuju između privatne mreže i Interneta, te odlučuje da li će propustiti ili odbaciti paket. Ta odluka se temelji na pravilima koja su ugrađena u firewall.



slika 1. Mjesta ugradnje firewall-a

Na primjer (slika 1), postoje tri mreže u kojima se nalaze korisnici kojima se može vjerovati (ljubičasta boja), te dvije u kojima se nalaze korisnici u koje nepostoji povjerenje (zelena boja). Između tih mreža postoje točke na kojima želimo kontrolirati promet. Ideja je ne prekinuti komunikaciju na tim točkama nego je kontrolirati. To znači da bi na tim točkama trebalo postaviti uređaje koji bi provodili ispitivanje prometa (firewall). Na slici 1 mudro bi bilo postaviti firewall na točke C i D, jer se na tim točkama nalazi veza prema korisnicima u koje nemamo povjerenje, ali isto tako on (firewall) bi mogao biti potreban i na točkama A i B.

Firewall bi na tim točkama ispitivao koji korisnik ima pravo pristupa zaštićenoj lokalnoj mreži i ako ima pravo pristupa, kolike ovlasti ima taj korisnik. Nadalje trebao bi ispitivati koji tipovi paketa smiju proći kroz tu točku. Ti, ali i mnogi drugi, principi se trebaju primjenjivati na svim stupnjevima rada na Internetu, od malih ureda do ureda velikih tvrtki, od nekoliko povezanih LAN-ova do korporacijskih WAN-ova, od računala za pretraživanje Weba do servera za elektroničku trgovinu.
Postoje specifični napadi kojima cracker-i žele onesposobiti neko računalo u privatnoj lokalnoj mreži, pa čak i cijelu lokalnu mrežu, ili bilo koje računalo koje je spojeno na Internet. Recimo, cracker može zapisati u polje izvorišta neku IP adresu iz privatne zaštićene mreže te tako pokušati " prevariti " firewall (Address Spoofing napad). Ali zato firewall odbacuje sve TCP/IP pakete koji dolaze na sučelja prema javnim mrežama, prema nepovjerljivim računalima, a imaju u zaglavlju IP adresu iz privatne lokalne mreže. Isto tako, moguće je postavljanjem određenih zastavica u zaglavlju TCP/IP paketa zauzeti računalne resurse ili identificirati određene otvorene pristupe (Syn-Flood, Port-Scanner napad). Nadalje moguće onesposobiti operativne sustave šaljući velike i česte ping zahtijeve (Smurf, Ping-of-Depth napad). Svu moguću štetu, koju mogu uzrokovati ti napadi, je moguće spriječiti odgovarajućom upotrebom firewall-a. Ovi napadi, kao i načini zaštite, su detaljnije opisani u poglavlju 3.5.

2. Firewall

Firewall-i se nalaze na granicama privatne mreže, spojeni direktno na veze prema drugim mrežama. Koncept sigurnosti na granicama privatne mreže je vrlo važan, jer bez njega svako računalo u privatnoj mreži bi moralo izvoditi funkcije firewall-a trošeći resurse računala i povećavajući vrijeme potrebno za spajanje, autentifikaciju i dekodiranje podataka u LAN-ovima velikih brzina. Firewall-i dopuštaju da se centraliziraju svi sigurnosni servisi u računalu koje je optimizirano i posvećeno zadatku.
Po svojoj prirodi firewall-i stvaraju " usko grlo " između privatne mreže i vanjskih mreža, jer sav promet prolazeći između privatne mreže i vanjske mora proći kroz jednu kontrolnu točku. To je mala cijena koja se mora platiti zbog sigurnosti. Zbog toga što su veze između mreža relativno spore u odnosu na brzinu modernih računala, kašnjenje koje izaziva firewall može se zanemariti. Za većinu korisnika su i više nego dovoljni relativno jeftini firewall uređaji. Za tvtke i ISP-ove, čiji Internet promet je mnogo veći, razvijeni se novi firewall-i velikih brzina. Neke zemlje čak koriste firewall-e velikih brzina za cenzuriranje Interneta (Npr. Kina je prije nekog vremena cenzurirala pristup određenim sadržajima na Internetu).
Firewall-i funkcioniraju prvenstveno koristeći tri osnovne metode:

Packet Filtering Odbacuje TCP/IP pakete od neautoriziranih računala i pokušaje uspostavljanja veze sa neautoriziranim servisima.

Network Address Translation (NAT) Prevodi IP adresu internog računala da bi ga "sakrio" od vanjskog monitoringa.

Proxy Servises Stvara visoko-stupanjsku aplikacijsku vezu sa strane internog računala da bi kompletno prekinuo vezu mrežnog sloja između internog i vanjskog računala.

Većina firewall-a ima i dva ostala važna sigurnosna servisa:

Encrypted Authentication Dopušta korisnicima na javnoj mreži da dokažu svoj identitet firewall-u, da bi dobili pristup privatnoj mreži sa vanjskih lokacija.

Virtual Private Networking Uspostavlja sigurnu vezu između dvije privatne mreže preko javnog medija kao što je Internet.

2.1. Filtriranje paketa (Packet Filtering)

Packet filters (filteri paketa) su originalni firewall-i. Prvi pokušaji da se poboljša sigurnost TCP/IP-a su bili utemeljeni na ideji da je usmjeritelju veoma lako ispitati zaglavlje TCP/IP paketa i jednostavno odbaciti pakete koji ne zadovoljavaju specifikacije koje želimo prihvatiti.
Ipak filteri paketa imaju problema koji ih čine nedovoljnima da bi postigli potpunu zaštitu za privatnu mrežu. Zbog toga se oni upotrebljavaju sa proxy servisima i NAT-om (prevođenje mrežnih adresa).

Proxy servisi su prvenstveno dizajnirani da bi učinili World Wide Web bržim. NAT je pak prvenstveno dizajniran da bi povećao adresni prostor dostupan privatnim organizacijama i riješio problem spajanja privatnih mreža na Internet. A poslije su iskorištena njihova dobra svojstva, koja su spojena sa filtriranjem paketa i tehnologijom kodiranja/dekodiranja, da bi se stvorili moderni firewall-i.
Postoje dva primarna tipa filtriranja paketa:

- Filteri paketa bez pamćenja stanja (Stateless packet filtering), koji se upotrebljavaju u usmjeriteljima i operacijskim sustavima
- Filteri paketa sa pamćenjem stanja (Stateful packet filtering), koji se upotrebljavaju u modernim firewall-ima

2.1.1. Filteri paketa bez pamćenja stanja (Stateless packet filters)

Filteri paketa su granični usmjeritelji koji povećavaju sigurnost odlučujući da li da proslijede paket na osnovu informacija koje sadrži zaglavlje svakog paketa. Filteri teoretski mogu biti konfigurirani da tu odluku donesu na osnovu svakog dijela zaglavlja, ali najčešće se ta odluka donosi na osnovu:

- Izvor usmjeravanja (source routing)
- Tip protokola
- IP adresa
- TCP/UDP port
- Numeriranje fragmenata

Izvor usmjeravanja

Izvor usmjeravanja je lista u kojoj je definirana egzaktna ruta, kroz koju paket mora proći između računala koja su spojena preko IP veze. Izvor usmjeravanja je originalno bio korišten za otkrivanje pogrešaka i testiranje, ali sada ga često koriste cracker-i koji mogu staviti bilo koju adresu u polje odredišta i još osigurati da im se taj paket vrati navodeći svoje računalo (IP adresu) u ruti.
Dva tipa definiranja izvora usmjeravanja su:

- Neizričito definiranje izvora usmjeravanja (Loose source routing), koje određuje jedan ili više računala kroz koja paket mora proći, ali ne cijelu listu.
- Striktno definiranje izvora usmjeravanja (Strict source routing), koji određuje egzaktnu rutu kroz koju paket mora proći na putu između računala.

Neizričito definiranje izvora usmjeravanja cracker-i češće upotrebljavaju, jer jednostavno mogu staviti svoju IP adresu u zaglavlje paketa i tako osigurati da paket u svakom slučaju dođe do njihovih računala.

Filtriranje protokola

Polje u zaglavlju koje označava koji protokol je upotrebljen, može se iskoristiti da se diskriminira cijeli skup usluga, kao što su:

- User Datragram Protocol (UDP)
- Transmisson Control Protocol (TCP)
- Internet Control Mesage Protocol (ICMP)
- Internet Group Menagment Protocol (IGMP)

Na primjer, ako imamo server koji poslužuje koristeći uslugu temeljenu na TCP protokolu, onda možemo filtrirati sve UDP usluge. Ipak polje protokola je previše općenito da bi ga mogli koristiti za filtriranje.

Filtriranje IP adrese

Filtriranje IP adrese omogućuje da zabranimo vezu na (ili sa) određenog računala na temelju njegove IP adrese. Većina filtera dopuštaju da se zabrani pristup svim računalima osim onih koji su na listi prihvatljivih ili da se dopusti pristup svima osim onih koji su na listi neprihvatljivih.
Specifično odbijanje (računala koji su na listi neprihvatljivih) je skoro uvijek beskorisno, jer bi trebalo pratiti trag svakog cracker-a koji je ikad napao privatnu mrežu, pamtiti sve IP adrese sa kojih je on slao pakete, i pretpostaviti da on nije mogao prikupiti pakete sa neke druge IP adrese, koja ne postoji na popisu, te sa tim istim paketima napao privatnu mrežu. Kako oni uvijek to naprave ne treba se pouzdati na specifično odbijanje.
Specifično prihvaćanje adresa određenih računala pruža relativno dobru zaštitu. To je najjači način zaštite koji pružaju filteri paketa bez mogućnosti pamćenja stanja (stateless packet filters). Znači, odbijanjem pristupa za sva računala osim za ona koja se nalaze na listi znanih IP adresa, može se garantirati da će usmjeritelji biti dostupni samo računalima (njihovim IP adresama) za koja se zna. Odbijanjem pristupa svim drugim IP adresama znači da cracker ima vrlo malo mogućnosti da istraži vašu mrežu. Da bi cracker provalio u privatnu mrežu morao bi imati pristup listi znanih IP adresa.
Moguće je da cracker iskoristi izvor usmjeravanja (source routing) da bi ukrao IP adrese. Definirajući izvor usmjeravanja cracker može staviti dopuštenu adresu računala koje se nalazi u privatnoj mreži u paket i specificirajući IP adresu svog računala u listi dobit će povratni paket. Tako će cracker imati paket sa izvorišnom adresom iz privatne mreže. Zbog toga, filteri paketa bi se trebali uvijek konfigurirati tako da odbace paketa sa rutom usmjeravanja. Dobri filteri paketa dopuštaju da se specificiraju računala na osnovi protokola. Na primjer, može se dopustiti pristup svakom računalu na TCP port 80 za HTTP uslugu, ali samo računala iz privatne mreže mogu pristupiti TCP portu 23 (Telnet).

TCP/UDP portovi

Informacija o TCP/UDP portu je najčešće upotrebljavana za filtriranje jer ona točno označava koji protokol se koristi.
Kao i kod filtriranja IP adrese mogu se nabrojiti svi prihvatljivi ili svi neprihvatljivi protokoli. Za razliku od filtriranja IP adrese kod protokola je korisno i nabrojiti sve neprihvatljive, jer većina cracker-skih napada ciljaju na nekoliko određenih protokola.
Neki od tih protokola koji se mogu filtrirati na osnovi TCP ili UDP porta su:

Telnet (port 23) Ostavljajući ovaj port otvorenim računalo će dopustiti crackeru da otvori command prompt sa dopuštenjem za npr. brisanje nekih datoteka.

NetBIOS Session (port 139) Ostavljajući ovaj port otvorenim za Internet računalo server će dopustiti crackeru da se spoji na server kao da je lokalni klijent.

POP (port 110) Trebala bi se implementirati virtualna privatna mreža za udaljene klijente koji moraju provjeriti svoj mail, jer POP koristi lozinku korisnika u razgovijetnom obliku da dopusti pristup mail serveru. To dopušta cracker-u da ukrade korisnikovu lozinku.
Naravno isto tako se mogu filtrirati još neki protokoli: Echo, FTP, SMTP, DNS, HTTP, ...

Fragmentiranje

Fragmentiranje ja nastalo da bi poduprlo prolazak velikih IP paketa kroz data link. Tu nastaju problemi zbog činjenice da podatak o protokolu (o portu kojega on koristi) se nalazi samo na početku IP paketa i zbog toga će se on nalaziti samo u nultom fragmentu. Fragmenti broj 1 i viši neće sadržavati tu informaciju i zbog toga ne mogu biti filtrirani. Prvi filteri su, pod pretpostavkom da je nulti paket odbačen i da zbog toga će svi ostali biti bezvrijedni, jednostavno prosljeđivali ostale pakete. Ali ta pretpostavka nije točna u svakom slučaju. Neke starije verzije TCP/IP-a koje su se izvodile na računalima su svejedno pokušale ponovo spojiti paket i ako je svaki taj paket, od prvog do n-tog, bio ispravan TCP paket on ga je upotrijebio. To znači da je cracker mogao promijeniti svoj IP paket da kad započne njegovo fragmentiranje da prvi fragment ima oznaku 1 i tako dalje. Na taj način bi zaobišao filter.

Problemi sa filtriranjem paketa bez pamćenja stanja

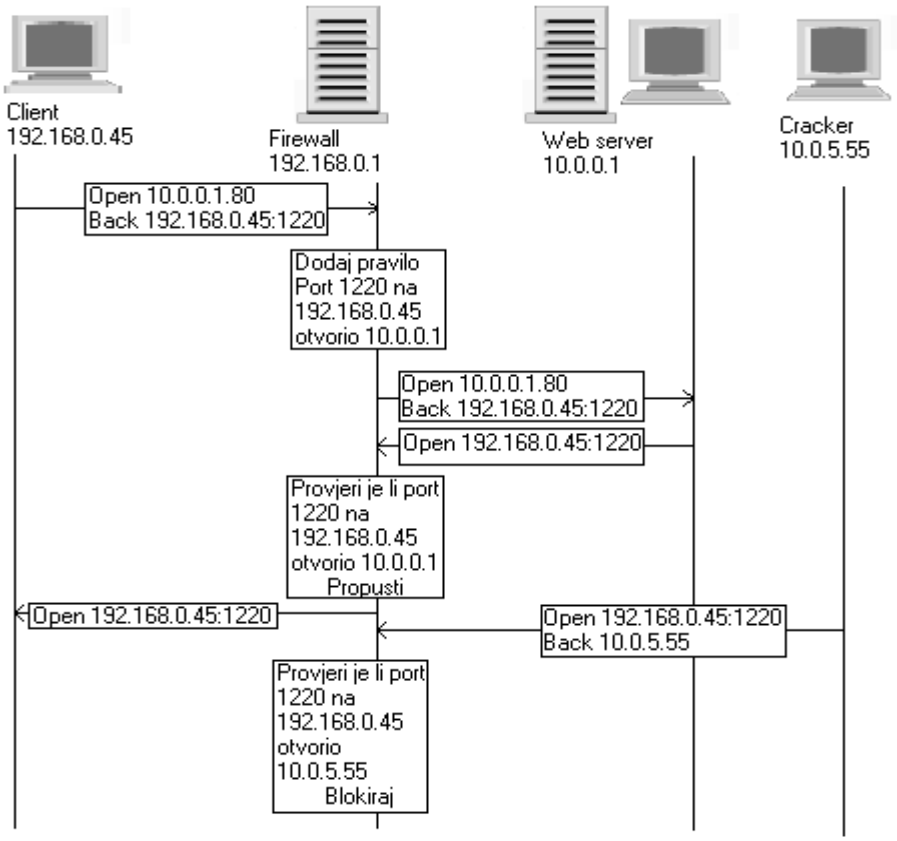
Filteri paketa imaju dva bitna problema:

- Ne mogu provjeriti sadržaj paketa
- Ne sadržavaju stanje veze

Većina filtera paketa su bez pamćenja stanja (stateless), što znači da oni ne sadrže informaciju o vezi kojoj pripadaju. Oni donose odluku o propuštanju/odbacivanju paketa na osnovi informacije koju taj paket sadrži. Isto tako, ne mogu odlučiti o odbacivanju fragmenata, jer fragmenti ne sadrže informaciju o portu koji se koristi. Filtera paketa bez pamćenja stanja ne mogu ustanoviti da li spojna veza odgovara vezi koja je uspostavljena unutar mreže, pa zbog toga moraju propustiti pakete na svim portovima iznad 1024.
Moderni filteri i firewall-i prate status veze i pamte to stanje, tako da mogu kontrolirati rutu paketa kroz privatnu mrežu.

2.1.2. Filteri paketa sa pamćenjem stanja (Statefull packet filters)

Standardni filteri paketa imaju određen broj mana, koje sve proizlaze iz činjenice da jedan paket u komunikaciji ne sadrži dovoljno informacija da bi se odlučilo da li ga treba odbaciti, jer je on dio veće komunikacije. To znači da jedan paket možda ne može nanijeti štetu računalu ili lokalnoj mreži, ali veći broj paketa koji dolaze na računalo bi već moglo biti opasno i zbog toga treba pratiti stanje te veze i na osnovi toga stanja odlučiti da li odbaciti pakete ili ne.
Filteri paketa sa pamćenjem stanja riješavaju ovaj problem, jer oni sadrže stanje cijelog prometa kroz firewall (spremljeno u memoriji) i na osnovu tog zapamćenog stanja odlučuju da li treba odbaciti pojedini paket.
Filteri paketa sa pamćenjem stanja pamte stanje veze na mrežnom i sesijskom sloju snimajući informacije o paketima koji prolaze kroz filter. Filteri tada koriste te informacije da bi razlikovali važeće pakete od nevažećih pokušaja uspostave veze.



Slika 2. Filteri paketa sa pamćenjem stanja

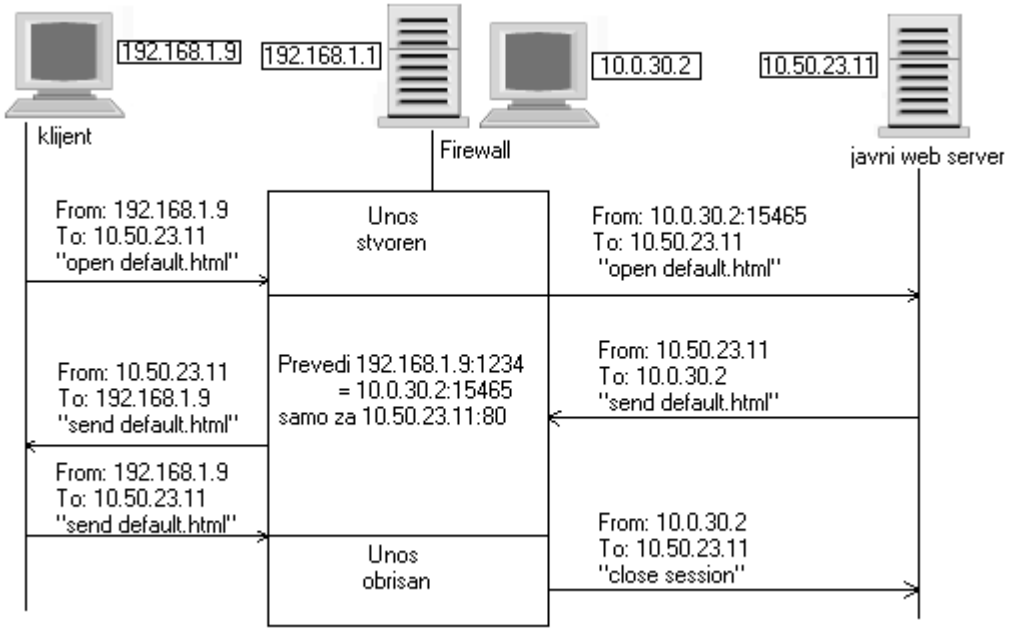
Kada se unutrašnje računalo, kojem se može vjerovati (Na slici 2: 192.168.0.45), spoji na TCP pristup na vanjskom računalu, kojem se ne može vjerovati (Na slici 2: 10.0.0.1), ono pošalje sinhronizacijski paket (IP adresu i port) na kojem očekuje odgovor. Kada taj SYN paket prođe kroz filter sa pamćenjem stanja veze, filter upiše u svoju tablicu stanja odredišni port i port na kojem očekuje odgovor. Kada dođe odgovor, filter jednostavno pogleda izvorište paketa i odredišne portove koji su zapisani u njegovoj tablici stanja, vidi da se oni poklapaju i propusti paket. Ako u tablici ne postoji takva informacija, paket se jednostavno odbaci, jer nije tražen iz unutrašnje mreže. Slika 2 pokazuje uspostavu filtera sa pamćenjem stanja veze. Na toj slici je cracker (10.0.5.55) pokušao pristupiti računalu 192.168.0.45 na port 1220. Filter paketa već ima zapisano u svojoj tablici da je port 1220 na 192.168.0.45 otvorio IP adresu 10.0.0.1. Dakle filter uspoređuje zapis u tablica sa sadržajem zaglavalja paketa koji šalje cracker. Utvrđuje da port 1220 ne pripada vezi sa 10.0.5.55 i blokira taj paket.

Filteri brišu unose u tablicu stanja kada kroz njih prođe TCP close paket. To osigurava da prekinute veze ne ostvaljaju sigurnosne rupe u tablicama stanja.

Filteri sa pamćenjem stanja veze su programirani pomoću pravila (policies), koja određuju njegovo ponašanje. Pravila su obično za pakete koje treba uvijek odbaciti, nikad odbaciti, usluge kojima je dopušten prolaz do određenih računala unutar mreže.

2.2. Network Address Translation (NAT)

NAT prevodi privatne IP adrese koja se nalazi u privatnoj lokalnoj mreži u globalno jedinstvene IP adrese za upotrebu na Internetu. Iako je NAT prvenstveno razvijen kao trik kojim se može povećati broj dostupnih IP adresa privatnim mrežama, ima sigurnosni aspekt koji je se pokazao važnim - skrivanje internih računala.
NAT skriva TCP/IP informacije o računalima unutar lokalne mreže od cracker-a na Internetu, prikazujući kao da sav promet iz privatne mreže dolazi sa jedne IP adrese.
Firewall-i sadržavaju tablicu pristupa lokalnoj mreži (računala unutar lokalne mreže) i odgovarajućih pristupa firewall-a prema Internetu. Kada unutrašnji klijent uspostavi vezu sa vanjskim računalom, firewall promijeni izvorišni pristup (klijent) u jedan od firewall-ovih pristupa prema Internetu i unese u tablicu prevođenja izvorišni, odredišni i odgovarajući pristup firewall-a, koji je upotrebljen kod tog prevođenja.
Kada vanjsko računalo(na Internetu) šalje podatke računalu u lokalnoj mreži, firewall provodi inverznu translaciju. Ako ne postoji unos u tablici prevođenja ili je paket došao sa IP adrese koju on ne očekuje, odbacuje paket.



Slika 3. Network address translation

Na slici 3 je primjer kako NAT prevodi adrese. Neka računalo u privatnoj mreži sa IP adresom 192.168.1.9 želi uspostaviti vezu sa javnim web serverom 10.50.23.11. Koristeći sljedeći slobodni port 192.168.1.9:1234 šalje TCP paket na 10.50.23.11:80.
Router/Firewall (192.168.1.1 adresa sučelja prema privatnoj mreži, 10.0.30.2 adresa sučelja prema Internetu) prima paket i kreira sljedeći unos u tablicu prevođenja:

Prevedi	192.168.1.9:1234
u	10.0.30.2:15465
samo za	10.50.23.11:80

Nakon toga šalje paket na odredište i 10.50.23.11:80 prima paket ali sa adrese 10.0.30.2:15465. Kada odredište želi odgovoriti onda on šalje odgovor na tu adresu misleći da je to originalno izvorište.
Kada primi paket firewall traži u svojoj tablici prevođenja odgovarajući pristup i nalazi ga. Tada ustanovi da je izvorište tog paketa isto kao i IP adresa javnog računala koja je unošena već prije. Ako ne postoji odgovarajući unos, paket se odbacuje.
Četiri primarne funkcije NAT firewall-a su:

- Dynamic Translation

  Dynamic translation (IP Masquerade) štiti unutarnja računala zamijenujući njihove IP adrese sa adresama koje vode do firewall-a. Individualna računala unutar firewall-a identificiraju se na osnovi broja porta u svakoj vezi koja prolazi kroz firewall.

  Zbog toga što informacija o prevođenju ne postoji dok unutrašnji klijent ne uspostavi vezu kroz firewall, vanjska računala ne mogu adresirati unutarnja koja su zaštićena sa dinamički prevedenom IP adresom.

  NAT ne čini ništa drugo da zaštiti klijenta, osim što sprečava vanjsko računalo da se spoji na njega. Ako je klijent zaveden da se spoji na maliciozno vanjsko računalo ili ako je trojan nekako instaliran na računalo koji se spaja na specifična vanjska računala, on (klijent) može biti komprimitiran. Zbog ovoga sam NAT nije dovoljan.

  Zavesti klijenta da se spoji na malicioznu stranicu je veoma jednostavno. Na primjer, ako vam prijatelj pošalje e-mail u kojem piše da provjerite određenu stranicu, vi ćete vjerojatno kliknuti na link. To je sve što cracker treba.

- Static Translation

  Static translation se koristi kada unutar firewall-a postoje resursi za koje želimo da budu dostupni javnosti ili kada se koristi protokol koji mora koristiti određeni port ili IP adresu.

  Static translation se može koristiti da bi se određeni skup IP adresa preveo u određeni skup privatnih adresa. Na primjer može se prevesti 128.110.121.0-128.110.121.255 u unutrašnji skup 10.1.2.0-10.1.2.255. Firewall može prevesti svaku IP adresu u tom skupu.

  Prosljeđivanje porta (Port forwarding) je tip statičkog prevođenja koji se odnosi na prosljeđivanja samo specifičnog porta. Recimo da je IP adresa vašeg e-mail servera 10.1.1.21, a vanjska adresa firewall-a je 10.0.30.2 . Onda se statički može spojiti pristup 10.0.30.2:25 na adresu 10.1.1.21:25. Ta statička veza će uzrokovati da firewall prevodi sve veze na SMTP port na e-mail server unutar firewall-a.

- Load Balancing Translation

  Jedna IP adresa i port su prevedeni na više identično konfiguriranih servera, tako da jedna javna IP adresa može biti na više servera.

- Network Redundancy Translation

  Višestruke Internet veze su spojene na NAT firewall. Firewall izabire i koristi mrežu na osnovu dostupnusti, propusnosti i zakrčenju prometa.

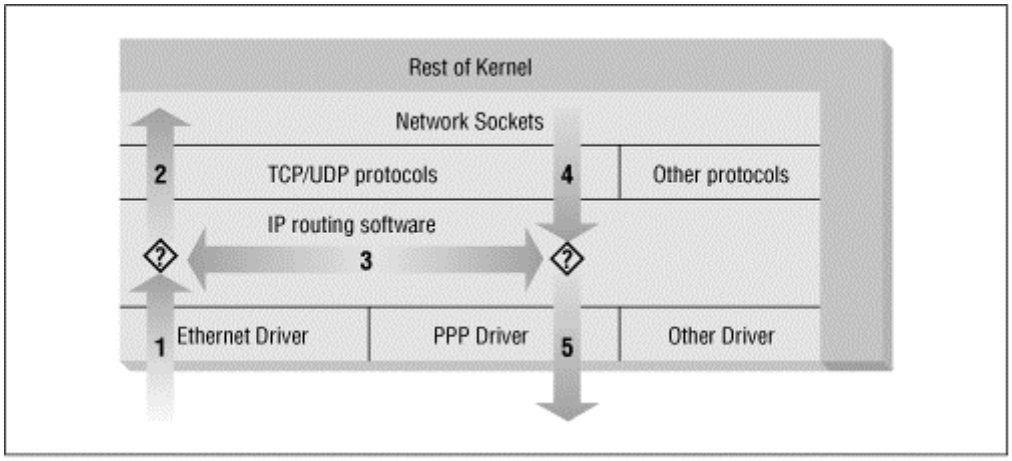
2.3. Proxy Services

NAT riješava mnoge probleme, ali ne ograničava dovoljno tok paketa kroz firewall. Moguće je da netko promatrajući mrežu nadgleda promet koji izlazi iz firewall-a i zaključi da firewall prevodi adrese drugih strojeva. Tada je moguće da cracker preuzme TCP vezu ili da je vrati nazad kroz firewall.
Proxy aplikacijskog sloja sprečavaju tako nešto. Proxy vam dopušta da prekinete protok protokola mrežnog sloja kroz firewall i ograničite promet samo na protokole viših slojeva kao što su HTTP, FTP i SMTP.
Proxy se ne mora izvršavati na firewall-u. Bilo koji server, unutar ili izvan privatne mreže može biti proxy. Ipak bez firewall-a ne postoji dovoljna sigurnost. Mora postojati barem neki filter paketa koji će štititi proxy.

3. Linux mrežni firewall

Da bi se napravio Linux IP firewall, potrebno je imati kernel sa podrškom za IP firewall i prikladna konfiguracijska biblioteka. U svim kernelima prije serije 2.2 koristio se ipfwadm. Kerneli 2.2.x su koristili IP firewall-e koji se zovu IP Chains. IP Chains koriste program koji je sličan ipfwadm i zove se ipchains. Linux kerneli 2.3.15 i kasniji podržavaju Linux IP firewall-e koji se zovu netfilter. Netfilter je rezultat velikog redizajniranja prometa kroz Linux. Netfilter ima kompatibilnu podršku za ipfwadm i ipchains, kao i za novu alternativu koja se zove iptables.

Prolazak paketa kroz kernel



Slika 4. Prolazak paketa kroz kernel

Na slici 4 je prikazan osnovni prolazak paketa kroz kernel.

- IP paket je primljen. (1)
- Primljeni IP paket je ispitan da bi se ustanovilo da li je namjenjen nekom procesu na ovom stroju.
- Ako je paket za ovaj stroj, onda je proslijeđen lokalno. (2)
- Ako njegovo odredište nije na ovom stroju, radi se pretraga tablice usmjeravanja da bi se našla prikladna ruta i paket se proslijedi na prikladno sučelje. Ako nije nađena prikladna ruta paket se onda odbaci. (3)
- Paketi lokalnih procesa su poslani software-u za usmjeravanje da ih on proslijedi prikladnom sučelju. (4)
- Odlazeći paketi su ispitani da bi se ustanovilo da li postoji ispravna ruta koja će se iskoristiti, ako ne postoji datagram se odbacuje.
- IP paket je poslan. (5)

Na slici 4 je prikazan prolazak paketa kroz kernel nekog stroja. Taj stroj (računalo) je spojen preko ethernet sučelja sa drugim računalima u lokalnu mrežu. Isto tako je spojen i na Intenet preko PPP (Point to Point) sučelja. Na ovom dijagramu put 1→3→5 predstavlja usmjeravanje podataka na stroju između lokalne ethernet mreže i računala na Internetu, koje je dostupno preko PPP linka. Put 1→2 i 4→5 predstavljaju izlaze i ulaze podataka mrežnog programa koji se izvodi na lokalnom računalu. Put 4→3→2 predstavlja promet podataka preko loopback veze. Mjesta gdje se nalaze upitnici predstavljaju odluku o usmjeravanju mrežnog sloja.

Linux kernel IP firewall je sposoban primjeniti filtriranje na različitim stupnjevima ovog procesa. To znači da se može filtrirati datagrame koji dolaze u stroj, koji se proslijeđuju preko stroja i one koji su spremni za slanje.

3.1. Iptables

Iptables biblioteka se koristi da bi se konfigurirala pravila filtriranja netfiltera. Sintaksa iptables-a je veoma slična sintaksi ipchains-a, ali ima mogućnost proširivanja. To znači da se njihova funkcionalnost može proširiti bez ponovnog prevođenja. To se može postići ako se koristi dinamička biblioteka.
Prije nego što se počne koristiti iptables mora se učitati netfilter kernel modul koji pruža podršku za iptables. Najlakši način je koristiti sljedeću naredbu:

```
modprobe ip_tables
```

Iptables naredbe se koriste da bi se konfiguriralo IP filtriranje i NAT. Postoje dvije tablice pravila koje se zovu *filter* i *nat*.Tablica filtera se pretpostavlja ako se koristi –t opcija. Isto tako je dostupno pet ugradbenih lanaca. INPUT i FORWARD lanci se koriste u tablici filtera, PREROUTING i POSTROUTING lanci se koriste u nat tablici i OUTPUT lanac se koristi u obje tablice.
Sintaksa većine iptables-a je:

```
iptables command rule-specification extensions
```

Neke osnovne naredbe (command) su:

-A *lanac*
: Dodaje jedno ili više pravila na kraj navedenog lanca.

-I *lanac*
: Dodaje jedno ili više pravila na početak navedenog lanca.

-D *lanac*
: Briše jedno ili više pravila, koji odgovaraju specifikaciji pravila, iz navedenog lanca.

-P *lanac sigurnosna politika*
: Postavlja sigurnosnu politiku specificiranog lanca. Sigurnosne politike lanca mogu biti: ACCEPT (dopušta prolaz paketima), DROP (Odbacuje pakete), QUEUE i RETURN.

-F [*lanac*]
: Briše sva pravila iz navedenog lanca ili iz svih lanaca, ako ni jedan lanac nije naveden.

Neka specifikacija pravila (rule-specification) su:

-p [!]*protocol*
: Specificira protokol paketa koji će odgovarati ovom pravilu. Imena protokola su tcp, udp, icmp ili broj protokola, ako se zna.

-s [!]*adresa*[/*maska*]
Specificira adresu izvorišta paketa, koja će odgovarati ovom pravilu.

-d [!]*adresa*[/*maska*]
Specificira adresu odredišta paketa, koja će odgovarati ovom pravilu.

-j *meta*
Specificira koja akcija će se poduzeti, ako ovo pravilo odgovara.

Sve naredbe (command), specifikacija pravila (rule-specification) i ekstenzije (extensions) su dostupne u Iptables Tutorial-u [3].

Jednostavan primjer

Pretpostavimo da postoji mreža u organizaciji i da se želi, koristeći firewall baziran na Linuxu, dopustiti korisnicima pristup WWW serverima na Internetu, ali da se ne dopusti nijedan drugi promet.Ako mreža ima 24-bitnu mrežnu masku i ima IP adresu 172.16.1.0, tada će se koristiti sljedeći niz iptables naredbi:

```
# modprobe ip_tables
# iptables –F FORWARD
# iptables –P FORWARD DROP
# iptables –A FORWARD –m tcp –p tcp –s 0/0 --sport 80 –d 172.16.1.0/24 /
    --syn –j DROP
# iptables –A FORWARD –m tcp –p tcp –s 172.16.1.0/24 --sport /
    80 –d 0/0 –j ACCEPT
# iptables –A FORWARD –m tcp –p tcp –d 172.16.1.0/24 --dport 80 –s 0/0
    –j / ACCEPT
```

Prva naredba učitava netfilter kernel modul koji pruža podršku za iptables. Druga naredba briše sva pravila iz forward lanca. Treća naredba definira da je podrazumijevajuća sigurnosna politika za forward pravilo DROP (odbaci). To znači da će firewall odbaciti sve pakete, osim one za koje se navede da ih mora prihvatiti. Četvrta naredba odbacuje sve pokušaje uspostave TCP veze koji dolaze sa porta 80. Zbog te naredbe se nijedno računalo na Webu neće moći spojiti niti na jedno računalo u lokalnoj mreži, koju želimo zaštiti. Jer čim dođe prvi SYN paket firewall će ga odbaciti i veza se neće uspostaviti. Konačno peta i šesta naredba omogućavaju korisnicima pristup WWW-u.

Manipulacija TOS bitovima

Type of service (TOS-tip usluge) bitovi su skup od četiri zastavice u IP zaglavlju. Kada je bilo koji od ovih bitova postavljen, usmjernik se može drugačije odnositi prema tom paketu nego kada nije postavljen. Svaki bit ima drugačiju svrhu i ne može istovremeno više od jednog biti postavljeno. Oni omogućuju aplikaciji koja šalje podatke da kaže mreži koji tip mrežne usluge zahtijeva.

Postavljanje TOS bitova koristeći iptables

Iptables alati dopuštaju da se prihvati samo paket s postavljenim TOS bitovima koji odgovaraju nekoj predefiniranoj vrijednosti koristeći opciju *–m* tos. Isto tako se mogu i postavljati TOS bitovi koristeći –j TOS target. TOS bitovi se mogu postavljati samo u forward i output lancima.

Klase dostupnih mrežnih usluga su:

Minimalno kašnjenje (Minimum delay)
Maksimalna propusnost (Maximum throughput)
Maksimalna pouzdanost (Maximum reliability)
Minimalni troškovi (Minimum cost)

Mnemonic	Hexadecimal
Normal-Service	0x00
Minimize-Cost	0x02
Maximize-Reliability	0x04
Maximize-Throughput	0x08
Minimize-Delay	0x10

Tablica 1. Klase mrežnih usluga

Sintaksa za provjeru poklapanja TOS bitova je:

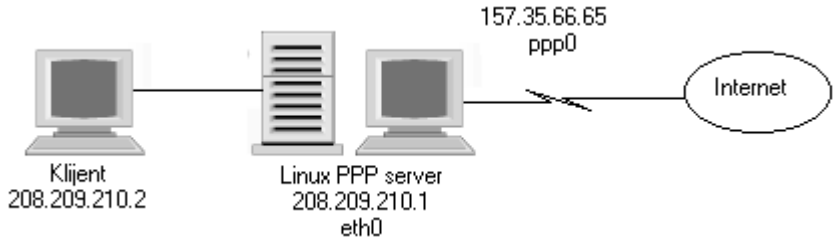
```
-m tos -tos mnemonic [other-args] -j target
```

Sintaksa za postavljanje TOS bitova je:

```
[other-args] -j TOS -set mnemonic
```

3.2. Firewall sa jednom zonom (Single-Homed Dial-up Server)

Većina malih tvrtki i ureda ima jednu vezu na Internet i ne žele da itko upada u njihovu mrežu. Mnoge od tih privremenih veza su broadband veze, gdje je medij dijeljen od strane pretplatnika koji su trenutno spojeni. To je savršeno za cracker-e.



Slika 5. Firewall sa jednom zonom

Sada možemo stvoriti iptables konfiguraciju za ovaj scenarij.

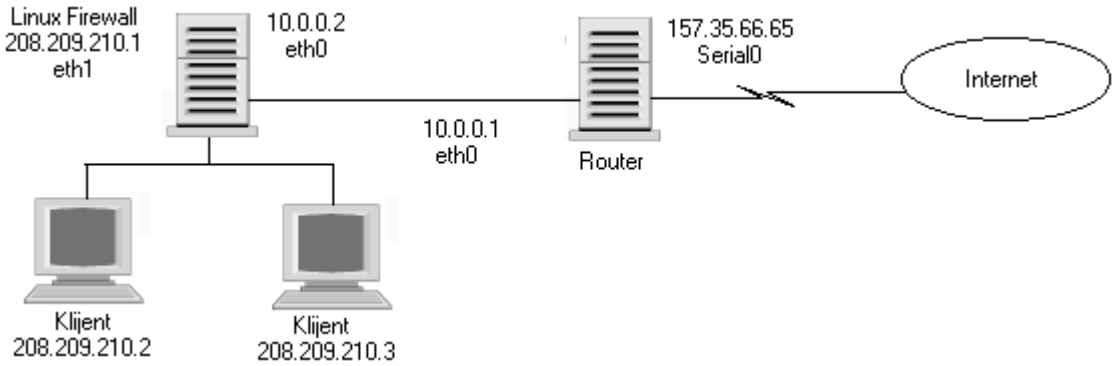
```
iptables -N protect
iptables -A protect --m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A protect --m state --state NEW -i ! ppp0 -j ACCEPT
iptables -A protect -j DROP
```

```
iptables -A INPUT -j protect
iptables -A FORWARD -j protect
```

Prva linija kreira novi lanac koji se zove protect. Druga linija osigurava propuštanje svih paketa koji dolaze sa Interneta, ako su oni odgovor na prije uspostavljenu vezu. Treća linija dopušta da se propusti nova veza, ali samo ako ne dolazi sa sučelja ppp0. Peta linija označava da sav promet koji ne odgovara prethodnim pravilima bude odbačen.

3.3. Firewall sa dvije zone (Dual-Homed Firewall)

Na jednoj centralnoj lokaciji u nekoj velikoj kompaniji se uvijek može naći usmjernik koji podržava stalnu vezu na Internet. To zahtijeva uključivanje firewall-a. Takav uređaj osigurava da je sav promet koji dolazi sa i odlazi na Internet ispitan. Takva konfiguracija je prikazana na slici 6.



Slika 6. Firewall sa dvije zone

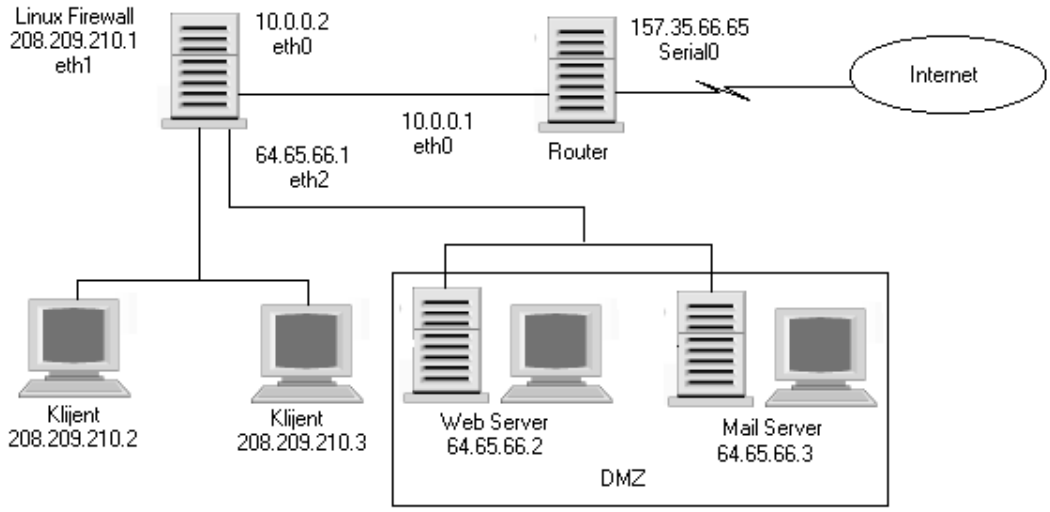
Pretpostavimo sigurnosnu politiku koja dopušta pristup Secure Shell-u(SSH), dok blokira druge tipove zahtijeva. Svi tipovi vanjskih TCP veza su dopušteni. ICMP unutrašnji promet je ograničen na echo request.
Sada možemo stvoriti iptables konfiguraciju za ovaj scenarij.

```
#Izbriši sva pravila iz lanaca
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD

#Podrazumijevajuća sigurnosna politika za Forward lanac je odbacivanje
iptables -P FORWARD deny

#Blokiraj sav dolazeći promet sa javnih sučelja (eth0)
iptables -A INPUT -i eth0 -j DROP

#Blokiraj sav odlazeći promet na javna sučelja (eth0)
iptables -A OUTPUT -o eth0 -j DROP

#Netfilter može prihvatiti fragmentirane pakete
iptables -A FORWARD -f -j ACCEPT

#Prihvati dolazeće TCP pakete od uspostavljenih veza
iptables -A FORWARD -m state -p tcp --state ESTABLISHED,RELATED -j
ACCEPT
```

```
#Prihvati dolazeće TCP veze (SSH) na eth0
iptables –A FORWARD –p tcp –i eth0 –d 208.209.210.0/24 --dport ssh –j
ACCEPT

#Prihvati sve odlazeće TCP veze koje dolaze na privatno sučelje (eth1)
iptables –A FORWARD –p tcp –i eth1 –j ACCEPT

#Prihvati sve odlazeće UDP veze koje dolaze na privatno sučelje (eth1)
iptables –A FORWARD –p udp –i eth1 –j ACCEPT

#Prihvati dolazeće ICMP pakete (ping odgovori)
iptables –A FORWARD –p icmp –i eth0 –d 208.209.210.0/24 --icmp –type 0 –
j ACCEPT

#Prihvati sve odlazeće ICMP veze koje dolaze na privatno sučelje (eth1)
iptables –A FORWARD –p icmp –i eth1 –j ACCEPT

#Odbaci sav ostali promet u Forward lancu
iptables –A FORWARD –j DROP
```

3.4. Firewall sa tri zone (Trihomed Firewall sa demilitariziranom zonom)

Neke mrežne arhitekture koriste trihomed firewall koji uključuje sučelje spojeno na javnu mrežu, sučelje spojeno na lokalnu mrežu i još jedno, treće sučelje koje poslužuje demilitariziranu zonu (DMZ). DMZ omugućuje ponudu javnih usluga sa nekim stupnjem kontrole, ali zabranjujući pristup anonimnim korisnicima sa Interneta u privatnu mrežu. Takva arhitektura je prikazana na slici 7.



Slika 7. Firewall sa tri zone

Proširit ćemo prijašnji scenarij tako da ćemo pristup Web serveru dopustiti samo udaljenim korisnicima iz mreže 208.209.210.0/24 , a pristup Mail serveru će biti dopušten korisnicima sa Interneta.
Sada možemo stvoriti iptables konfiguraciju za ovaj scenarij.

```
#Izbriši sva pravila iz lanaca
iptables –F INPUT
iptables –F OUTPUT
iptables –F FORWARD

#Podrazumijevajuća sigurnosna politika za Forward lanac je odbacivanje
iptables –P FORWARD deny

#Blokiraj sav dolazeći promet sa javnih sučelja (eth0)
iptables –A INPUT –i eth0 –j DROP


#Blokiraj sav odlazeći promet na javna sučelja (eth0)
iptables –A OUTPUT –o eth0 –j DROP

#Netfilter može prihvatiti fragmentirane pakete
iptables –A FORWARD –f –j ACCEPT

#Prihvati dolazeće TCP pakete od uspostavljenih veza
iptables –A FORWARD –m state –p tcp --state ESTABLISHED,RELATED –j
ACCEPT

#Prihvati dolazeće TCP veze (SSH) na eth0
iptables –A FORWARD –p tcp –i eth0 –d 208.209.210.0/24 --dport ssh –j
ACCEPT

#Prihvati dolazeće TCP veze na DMZ SMTP server (64.65.66.3)
iptables –A FORWARD –p tcp –i eth0 –d 64.65.66.3 --dport smtp –j ACCEPT

#Prihvati dolazeće TCP veze na web server od udaljenih korisnika
iptables –A FORWARD –p tcp –i eth0 –s 208.209.210.0/24 –d 64.65.66.2 --
dport www –j ACCEPT

#Prihvati sve odlazeće TCP veze koje dolaze na  sučelja eth1 i eth2
iptables –A FORWARD –p tcp –i eth1,eth2 –j ACCEPT

#Prihvati sve odlazeće UDP veze koje dolaze na  sučelja eth1 i eth2
iptables –A FORWARD –p udp –i eth1,eth2 –j ACCEPT

#Prihvati dolazeće ICMP pakete (ping odgovori)
iptables –A FORWARD –p icmp –i eth0 –d 208.209.210.0/24 --icmp –type 0 –
j ACCEPT

iptables –A FORWARD –p icmp –i eth0 –d 64.65.66.0/24 --icmp –type 0 –j
ACCEPT

#Prihvati sve odlazeće ICMP veze koje dolaze na sučelja eth1 i eth2
iptables –A FORWARD –p icmp –i eth1,eth2 –j ACCEPT

#Odbaci sav ostali promet u Forward lancu
iptables –A FORWARD –j DROP
```

Linije koje su otisnute masnim slovima su promjena u odnosu na prijašnji scenarij.

3.5. Zaštita od dobro znanih napada

Prvi veliki DoS (Denial of Service) napad se zbio 2. studenog 1988. Crv Morris, koji je napisao Robert Morris, student sveučilišta Cornell (Cornell University), je zarazio oko 5000 računala. Crv Morris je iskorištavao nekoliko čestih nedostataka u tadašnjim programima da bi se proširio Internetom velikom brzinom. Na primjer, crv je iskoristio nestandardnu naredbu dostupnu u programu Sendmail da bi se proširio sa jednog računala na drugo. Morris je pustio maliciozni program sa MIT-a i uskoro je spoznao da se crv širi većom brzinom nego što je on očekivao. Naravno uskoro su se mnoga računala diljem SAD-a bila zaražena. Kada je Morris shvatio što se dogadja, on je sa svojim prijateljom sa Harvarda poslao anonimni e-mail na Internet sa uputama kako da se ubije crv i spriječi daljne širenje. Ipak ta je poruka stigla prekasno. Mnoga računala na sveučilištima, medicinskim i vojnim ustanovama su bila zaražena. Robert Morris je osuđen na tri godine uvjetno, 400 sati dobrotvornog rada i $10,050 globe.
U daljnem tekstu su navedeni neki česti napadi. Iptables se mogu iskoristiti za zaštitu od specifičnih napada koji dolaze sa Interneta. Koristimo ih kao filtere prometa koji odgovara pojedinom napadu.

Address Spoofing

Mnoge firewall konfiguracije prihvaćaju pakete pošto utvrde da imaju neku adresu iz privatne mreže u polju izvorišta, u zaglavlju. Napadaču je jako lako stvoriti "spoof" paket generiran iz njegove mreže, ali sa adresom izvorišta iz privatne mreže. Može se zaštiti tako da se zahtijeva da paketi za adresom izvorišta iz privatne mreže moraju biti primljeni na sučelje koje je spojeno na privatnu mrežu. To se može postići koristeći iptables naredbu:

```
iptables –A FORWARD –s interna_mreža –i javno_sučelje –j DROP
```

Ova naredba dodaje pravilo u Forward lanac koje odgovara prometu, sa izvorištem u privatnoj mreži, ali ulazi na sučelje prema javnoj mreži. Netfilter onda mora odbaciti svaki paket koji odgovara tom pravilu.

Smurf napad

Smurf napad se zasniva na slanju ICMP echo request (ping) paketa na broadcast adresu vaše interne mreže. Izvorište paketa je adresa mete napadača. Tada meta postaje poplavljena ICMP echo odgovorima sa svih internih računala.
Sljedeća iptables naredba to sprečava:

```
iptables –A FORWARD –p icmp –d broadcat_adresa_interne_mreže –j DENY
```

Ova naredba dodaje pravilo u Forward lanac koje odgovara bilo kojem ICMP paketu koje dolazi na neko od sučelja, a čije je odredište broadcast adresa vašeg LAN-a. Kada paket odgovara ovom pravilu on se odbacuje.

Syn-Flood napad

Syn-Flood napad se zasniva na slanju velikog broja zahtijeva za TCP vezom (sa SYN zastavicom postavljenom) računalu, dok se potiskuju normalni SYN-ACK odgovori. Tada se može dogoditi da napadač zauzme sve resurse računala, tako da ono ne može poslije pružiti uslugu nekom običnom korisniku (Denial of Service).
Sljedeća iptables naredba to sprečava:

```
iptables -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT
```

Sa ovom naredbom se ograničava prihvaćanje TCP SYN zahtijeva na jedan po sekundi.

Port-Scanner napad

Mnoge port-scanner aplikacije pokušavaju identificirati otvorene TCP i UDP portove u sistemu šaljući SYN li FIN signal na određeni broj portova, očekujući RST signal za one portove koji nisu aktivni. Ova aktivnost se može ograničiti na jednu po sekundi sljedećom iptables naredbom:

```
iptables -A FORWARD -p tcp -tcp-flags SYN,ACK,FIN,RST RST -m limit --
limit 1/s -j ACCEPT
```

Ova naredba dodaje pravilo u Forward lanac koje odgovara TCP prometu koji dolazi u firewall sa postavljenim SYN, ACK i FIN zastavicama, i RST postavljenom zastavicom. Kada paket odgovara ovom pravilu prihvaća se, ali samo jedan u sekundi.

Ping-of-Death napad

Moguće je onesposobiti određene operativne sustave šaljući neobično velike i česte ICMP echo (ping) zahtijeve.
Sljedeća iptables naredba ograničava prihvat takvih pingova na jedan po sekundi.

```
iptables -A FORWARD -p icmp -icmp-type echo-request -m limit --limit 1/s
-j ACCEPT
```

Preporučljivo je blokirati sve skupa ICMP zahtijeve:

```
iptables -A FORWARD -p icmp -icmp-type echo-request -j DROP
```

osim ako ne postoji neki razlog da se računalo može pingati izvana.

4. T.Rex – besplatni firewall

T-Rex firewall je visoko integrirani sigurnosni paket koji kombinira funkcije, koje bi normalno zahtijevale instalaciju više proizvoda. Pruža organizacijama mogućnost definiranja jedne sigurnosne police na više firewall-a sa jedne radne stanice administratora.
T.Rex je napredni hibridni firewall dizajniran da bi spiječio sofisticirane napade od vještih i odlučnih napadača. Aplikacijski proxy blokira napade bazirane na aplikacijama, a koji su prošli neopaženo kroz statefull filter paketa.
T.Rex osigurava računala na zaštićenoj mreži provodeći striktnu kontrolu nad dostupnim funkcijama, tko ih može koristiti i kako ih smije koristiti. On sam se štiti od napada dizajnom njegovih funkcija i specijalnim kontrolama koje su ugrađene u uređaj.
T.Rex je dizajniran da bi odbacio sve poznate metode napada.

Programi sa poznatim sigurnosnim problemima su eliminirani.
Standardni demoni su zamijenjeni sa sigurnim proxy-jima
Prosljeđivanje IP paketa je onemogućeno. Zaštićene mreže nisu IP adresibilne iz nezaštićenih mreža
Jedini način da se dođe do informacije kroz firewall je koristeći sigurni proxy sa T.Rex-om

Svi nepotrebni programi su deaktivirani i uklonjeni. Jedino funkcije, koje su eksplicitno dopuštene, mogu proći kroz firewall. Ako IP paket stigne sa sigurne IP adrese na nesigurno mrežno sučelje , tada će veza biti prekinuta.
T.Rex podržava stotine aplikacijskih usluga i protokola. Podrška je pružena za sve glavne Internet usluge i protokole, kao što su:Web Browser, Web server, e-mail, sve TCP/IP aplikacije, kao i RPC i UDP aplikacije.

5. Cisco PIX Firewall v. 6.2

Cisco PIX firewall-i pružaju široki raspon naprednih firewall usluga, koje štite privatne lokalne mreže od pretnji koje kruže Internetom. Cisco Adaptive Security Algorithm (ASA) pruža ispitivanje paketa sa pamćenjem stanja (statefull). Administratori lako mogu kreirati sigurnosnu politiku koja će se provoditi na mrežnom prometu, koji prolazi kroz firewall.
Cicso PIX firewall-i pružaju zaštitu za brojne voice-over-IP (VoIP) standarde i druge multimedijalne standarde, uključujući H.323, Session Initiation Protocol (SIP), Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP) i Real-Time Transport Control Protocol (RTCP).
Koristeći standarde, temeljene na site-to-site VPN (Virtual Private Networking) mogućnostima, sa Cisco PIX firewall-ima, tvrtke mogu sigurno proširiti svoje mreže preko Internet veza do poslovnih partnera i udaljenih ureda diljem svijeta. Izgrađen na Internet Key Exchange (IKE) i IP Security (IPSec) VPN standardima, Cisco PIX firewall-i kodiraju podatke koristeći 56-bitni DES (Data Encryption Standard) ili napredni 168-bitni Triple DES (3DES). Isto tako se koristi i RSA, asimetrični algoritam kodiranja, te hash algoritmi MD5 i SHA-1. Javne ključeve razmjenjuju sa Diffie-Hellman-ovim postupkom. Time se sprečavaju pojedinci (napadači) da vide osjetljive poslovne podatke, koji putuju preko Interneta. Cisco PIX firewall-i, isto tako, mogu sudjelovati u Public Key Infrastructure (PKI – struktura javnog ključa) baziranoj na X.509 protokolu.
Integrirane mogućnosti zaštite lokalnih mreža od napadača sprečavaju mnoge popularne oblike današnjih napada, uključujući i DoS (Denial of Service) napade. Koristeći napredne zaštitne programe (DNSGuard, FloodGuard, MailGuard, …), Cisco PIX firewall-i nadgledaju promet. Ako dođe do napada firewall će ga blokirati i obavjestiti administratora u stvarnom vremenu. Cisco PIX firewall-i podržavaju fragmentiranje paketa, ali isto tako ispituju te fragmentirane pakete, da ne bi u njima bilo skrivenih napada.

6. Zaključak

Danas kada je Internet veoma nesigurno mjesto, puno potencijalnih napadača, mudro je koristi neke od sigurnosnih mjera koje su prikazane u ovom seminaru. Naravno da se mora razmisliti o riješenju koje najviše odgova. Da li se želi zaštiti osobno računalo u privatnom domu ili se želi zaštiti LAN neke velike tvrtke? Koliku razinu sigurnosti se mora zadovoljiti? Ta i mnoga ostala pitanja trebaju pomoći da se izabere da li će se kupiti neki gotovi firewall prozvod ili će se upustiti u taj zahtijevni posao - izgradnju sigurnosnog sustava.
Izgraditi Linux firewall je konceptualno lagan posao, ali je jako kompliciran zbog mnoštva detalja na koje treba obratiti pažnju. U ovom seminaru se pokušalo predočiti generalni koncept filtriranja paketa i njegovu implementaciju u Linuxov kernel. Može se saznati nešto i o tri osnovne firewall konfiguracije. Isto tako može se saznati nešto i o iptables-ima, alatu koji se koristi pri stvaranju filtera paketa. Prikazane su razne metode napada, te iptables naredbe kojima se oni sprečavaju. Na kraju su opisani i dva firewall-a, jedan besplatni i jedan komercijalni. Njima se može zaštiti privatnu mrežu od opasnosti koje "vrebaju" Internetom.

7. Literatura

1. Matthew Strebe, Charles Perkins, *Firewalls 24seven*, Sybex, 2nd Edition, ožujak 2002.
2. Iptables HOWTO, http://www.linuxguruz.org/iptables/howto/iptables-HOWTO.html , Rusty Russell, 1999.
3. Iptables tutorial, http://www.jollycom.ca/iptables-tutorial/iptables-tutorial.html , Oskar Andreasson, 2001.-2002.
4. http://2cobbs.com/firewalls/fwpg.htm
5. http://www.oreilly.com/catalog/linag2/book/index.html
6. http://www.opensourcefirewall.com/
7. http://www.pcflank.com/art18.htm
8. http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_data_sheets_list.html