Linux firewall – Netfilter je sastavni deo Linux kernela koji omogućuje filtriranje paketa, prevođenje mrežnih adresa ili skraćeno NAT (network address translation), kao i razne druge manipulacije paketima. Netfilter je unapređena verzija ipchains-a koji je bio aktuelan u starijim verzija Linux operativnog sistema.

**MALO O FIREWALL-U**

 Osnovna uloga firewall-a je zaštita sistema koju postižemo filtriranjem paketa.  U zavisnosti od toga da li je firewall namenjen zaštiti  računara na kome je aktivan ili čitave mrežu iza sebe, možemo ih podeliti na personalne i korporativne. Sama konfiguracija firewall-a takođe zavisi od većeg broja parametara. Kada govorimo o korporativnom firewall-u mislimo na uređaj koji se nalazi između interneta i lokalne mreže. U ovakvom scenariju firewall je zadužen za translaciju mrežnih adresa (NAT) i filtraciju paketa od interneta ka LAN-u i ako je potrebno obratno (od LAN-a ka internetu). Lokalna mreža opet može biti podeljena na više mrežnih segmenata, između kojih treba definisati bezbedonosnu politiku – za ovo je takođe zadužen firewall.

Često se iza firewall-a nalazi DMZ (Demilitarized zone), posebna zona čiji određeni segmenti trebaju biti izloženi internetu, ali koja ne treba biti vidljiva lokalnoj mreži

**Prevođenje mrežnih adresa (NAT)**

NAT je proces konverzije IP adresa privatne mreže u jedinstvenu IP adresu na internetu – javnu adresu koju koristi firewall. NAT nam unutar lokalne mreže dozvoljava korišćenje bilo kojeg opsega IP adresa, pa čak i onih javnih koje se već koriste na internetu.

NAT može biti SNAT (source network address translation) I DNAT (destination network address translation ). Kada neki računar iz lokalne mreže pošalje zahtev za određenim internet resursom, prilikom prolaska paketa kroz firewall, adresa iz lokalnog opsega zameniće se sa javnom adresom koju firewall koristi. To je SNAT i on omogućava računarima jedne lokalne mreže da koriste internet resurse i da na internetu budu vidljivi sa javnom adresom firewall-a.

Često korišćeni sinonim za DNAT je prosleđivanje portova (port forwarding). Kada neki računar preko interneta uputi zahtev firewall-u za nekim portom, firewall proverava NAT tabelu, tražeći unos za specifičan računaru iz privatne mreže koji je naznačen da prihvata zahteve po tom portu, pa ukoliko takav unos postoji, sledi zamena javne firewall adrese na koju je zahtev stigao, sa privatnom adresom računara kome je zahtev upućen.

## ****Filtriranje paketa****

Filtriranje paketa je fundamentalna funkcionalnost svakog firewall-a. Firewall analizira pakete i upoređuje ih sa utvrđenim pravilima i shodno tome primenjuje predefinisane akcije. Pakete firewall filtrira po tipu protokola, izvornoj (source) adresi ili informaciji o odredišnom portu. Na ovaj način pravimo izbor koje ćemo protokole (npr. TCP, UDP, ICMP, IGMP) propustitti, a koje ne, kao i sa kojih adresa je dozvoljen pristup određenim portovima. Moguće akcije koje firewall može primeniti su odbacivanje paketa (DROP), prihvatanje paketa (ACCEPT) ili odbijanje paketa uz obaveštenje pošiljaocu da njegov paket nije prihvaćen (REJECT).  U praksi se za odbacivanje paketa češće koristi DROP umesto REJECT, radi izbegavanja nepotrebnog mrežnog saobraćaja.

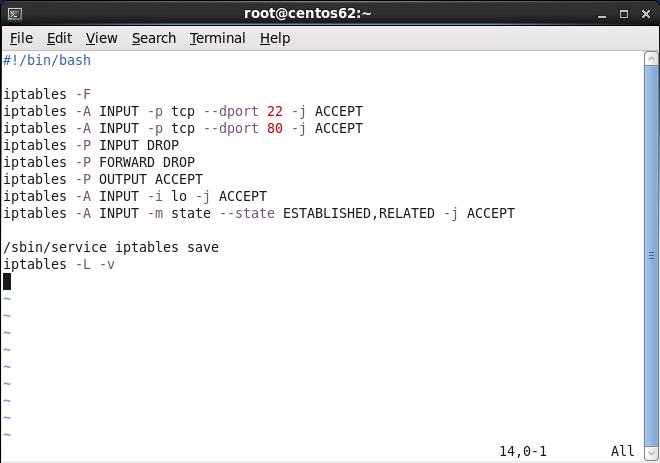
## ****Iptables struktura i konkretni primeri****

Iptables odaje utisak kompleksnosti na prvi pogled, međutim kada jednom razumete njegov koncept, shvatićete da je logičan i ne toliko nepristupačan za korišćenje. Struktura alata iptables je organizovana tako da se sastoji iz tabela (tables), lanaca (chains) i pravila (rules). Postoje četiri osnovne tabele: filter, nat, mangle i raw. Svaka od ovih tabela sadrži određene lance, pa tako recimo filter tabela sadrži INPUT, OUTPUT I FORWARD lance, a NAT tabela PREROUTING i POSTROUTING. Za svaki lanac se definišu određena pravila, koja predstavljaju predefinisane akcije koje ćemo primenti nad paketima.

Za filtriranje paketa, koristi se filter tabela. Ona se sastoji, kao što smo već napomenuli, iz INPUT, OUTPUT i FORWARD lanaca i svaki lanac sadrži listu pravila sa kojima upoređujemo pakete. Kada paket pristigne, na osnovu odredišne adrese se određuje da li je paket namenjen lokalnom računaru (firewall) i ako je tako prosleđuje se INPUT lancu. Ako pravila INPUT lanca dozvole da paket prođe, paket se prosleđuje odgovarajućem procesu kome je namenjen.

Ukoliko paket treba rutirati, onda ga prosleđujemo FORWARD lancu, pa ukoliko zadovolji sva pravila ovog lanca, prosleđuje se dalje interfejsu koji je zadužen za njega. OUTPUT lanac je zadužen za odlazne pakete. Ukoliko je paket prošao kroz lanac, a nijedno od pravila ga nije ni prihvatilo ni odbacilo, onda se na njega primenjuje predefinisana policija tog lanca.

**Jednostavni primer**



Slika demonstrira iptables konfiguraciju na računaru sa jednim mrežnim interfejsom. Sav dolazni saobraćaj je blokiran, osim ssh i http saobraća, a sav odlazni sabraćaj je dozvoljen. Takođe onemogućeno je rutiranje, jer postoji samo jedan mrežni interfejs.

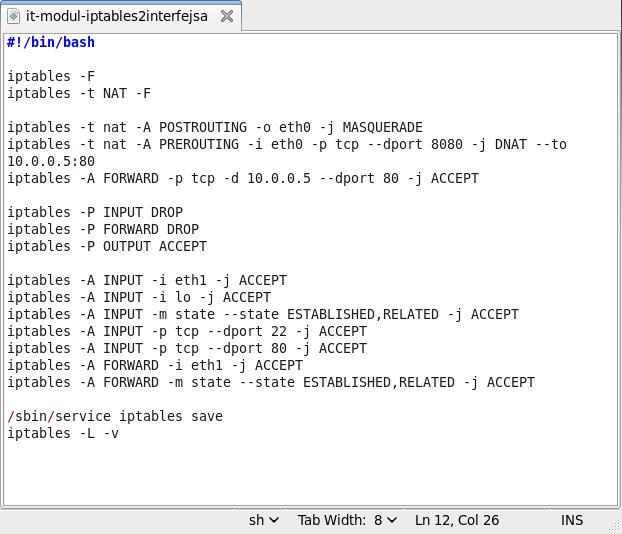
Prva linija „**iptables -F**“ obezbeđuje poništavanje (F – flush) trenutne iptables konfiguracije. Iduća dva reda obezbeđuju dodavanje (A – append) dva pravila u INPUT lanac, i dozvoljavaju tcp konekcije ka ssh i http portu na lokalnom računaru. P parametar označava predefinisanu policiju za odgovarajući lanac. To u našem primeru znači da svaki dolazni paket odbacujemo („iptables -P INPUT DROP“), dozvoljavamo odlazni saobraćaj („iptables -P OUTPUT ACCEPT“), kao i da onemogućavamo rutiranje („iptables -P FORWARD DROP“).

Već smo napomenuli da se prvo izvršavaju predefinisana pravila, pa ukoliko se nijedno od njih ne odnosi na paket, onda se primenjuje predefinisana policija datog lanca. „iptables -A INPUT -i lo -j ACCEPT“ – ovim naredbom smo dozvolili lokalni loopback saobraćaj (-i parametar znači interfejs). Sistem često prilazi određenim servisima po loklanom interfejsu (127.0.0.1), i bez ove komande rad sistema bi bio ugrožen, jer bi firewall odbacivao neke sistemske zahteve.

Sledeća linija je takođe zanimljiva. Parametar -m podrazumeva učitavanje dodatnog  modula – state modula u našem slučaju. State modul zadužen je za detekciju stanja paketa i on detektuje da li je dati paket deo neke već inicijalizovane konekcijie ili ne. Ukoliko jeste paket se propušta, u suprotnom biva odbačen.

Takođe možemo zaključiti da je iptables modularne strukture, i da je za dodavanje nekih funkcionalnosti potrebno učitavanje odgovarajućih modula. Predzadnja linija snima iptables konfiguraciju, kako bi bila aktuelna i nakon ponovnog podizanja sistema, a zadnja linija ekranski štampa trenutnu iptables konfiguraciju.

**Složeniji primer**



Slika demonstrira iptables konfiguraciju na računaru sa dva mrežna interfejsa – eth0 interfejs povezan sa internetom i eth1 lokalni LAN interfejs. Scenario je sledeći – lokalnoj mreži razrešavamo internet zahteve, radeći prevođenje mrežnih adresa (SNAT) na interfejsu eth0. Takođe svaki zahtev za lokalnim tcp portom 8080 firewall presleđuje na port 80 lokalnog računara sa IP adresom 10.0.0.5. Sam firewall izlaže web server i ssh server prema internetu, dok ka lokalnoj mreži nema restrikcija.

Prva linija je ista kao u prethodnom primeru, ali druga je već nešto drugačija. Naredba „iptables -t nat -F“ poništava sva pravila u NAT tabeli. Koristeći iptables podrazumevano radimo sa filter tabelom i tada parametar -t nije obavezan. Međutim, za rad sa drugim tabelama -t parametar je neophodan. Napomenuli smo već da u NAT tabeli postoje dva lanca PREROUTING I POSTROUTING. Prvi se koristi za razrešavanje mrežnih adresa ili SNAT, a drugi za prosleđivanje portova ili DNAT.

Naredba „iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE“ obezbeđuje prevođenje mrežnih adresa, a naredne dve su zadužene za DNAT ili prosleđivanje porta.

Naredba „iptables -t nat -A PREROUTING -i eth0 -p tcp –dport 8080 -j DNAT –to 10.0.0.5:80″ zamenjuje javnu odredišnu adresu interfejsa eth0 sa lokalnom adresom 10.0.0.5 i zamenjuje vrednost 8080 odredišnog porta sa vrednošću 80.

Naredba“iptables -A FORWARD -p tcp -d 10.0.0.5 –dport 80 -j ACCEPT“ prosleđuje dati paket FORWARD lancu koji ga dalje rutira do web servera sa loklanom IP adresom 10.0.0.5.

Sledi predefinisanje policije za sva tri lanca filter tabele. Vrednosti su identične kao i u prethodnom primeru, što znači da svaki dolazni paket odbacujemo („iptables -P INPUT DROP”), dozvoljavamo odlazni saobraćaj („iptables -P OUTPUT ACCEPT“), kao i da onemogućavamo rutiranje („iptables -P FORWARD DROP“).

C vcv bPolitika za dolazni saobraćaj je restriktivna, ali smo kao izuzetke postavili loopback interfejs (lo) i lokalni interfejs (eth1). Nastavak je sličan kao u prethodnom primeru. Dozvoljavamo pristup tcp portovima 22 i 80 na samom firewall-u. Definisali smo restriktivnu policiju FORWARD lanca, ali dodajemo lokalni eth1 interfejs kao izuzetak. Takođe propuštamo sve pakete koji su deo već ostvarenih konekcija, a treba ih dalje rutirati. Predzadnja linija snima trenutnu iptables konfiguraciju, a poslednja je ekranski štampa.

Napomenimo još nešto. Da bi rutiranje bilo omogućeno na Linux operativnom sistemu, moramo startovati sledeću naredbu „echo 1 > /proc/sys/net/ipv4/ip\_forward“. Data naredba dodeljuje vrednost „1“, fajlu ip\_forward, koji je sastavni deo proc pseudo fajl sistema, generisanog od strane Linux kernela. Isto kao i informacije u memoriji, svi podaci u proc fajl sistemu su tu do prvog ponovnog pokretanja sistema, zato je najednostavnije datu komandu ubaciti rc.local skriptu ili je startovati direktno iz iptables skripte.