Zaštita računarskih mreža v1.0
- Firewall –

Tehnički fakultet "Mihajlo Pupin" – Zrenjanin
Zrenjanin, april 2005.

Zaštita računarskih mreža - Firewall sistemi

U današnje vreme, sigurnost mreža i zaštita podataka predstavljaju veoma važan faktor. Povezivanje mreže na Internet i direktna veza sa svetom, predstavljaju stalnu pretnju za sistem i pružaju mogućnost napadačima, da koristeći različite bezbednosne propuste, provale u sistem.

Firewall predstavlja mehanizam zaštite u računarskim mrežama. To je softverski ili hardverski proizvod koji proverava pakete koji dolaze do njega i na osnovu unetih pravila, propušta ili odbija te pakete. Firewall se obično nalazi na ulazu u mrežu, tj. između unutrašnje i spoljašnje mreže, tako da se celokupan saobraćaj mora odvijati preko njega. On štiti mrežu na svim softverskim slojevima OSI modela – od sloja veze podataka, do aplikacionog sloja.

U firewall sistemima se koriste tri osnovna metoda zaštite:

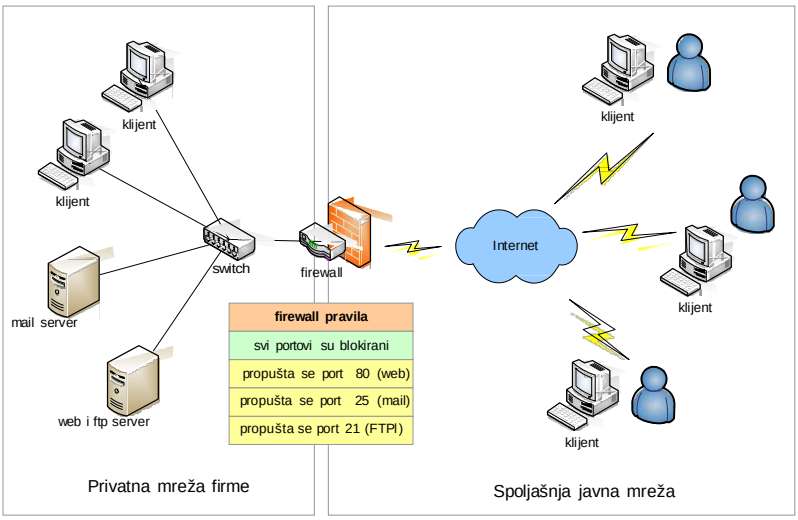
- filtriranje paketa (packet filtering) – metod pomoću koga se odbija pristup TCP/IP paketa koji dolaze sa neovlašćenih hostova i na neovlašćene servise.
- translacija adresa ili NAT (Network Address Translation) – metod koji prevodi IP adrese unutrašnjih hostova u neku od spoljašnjih (javnih) adresa i tako omogućava hostovima iz unutrašnje mreže pristup Internetu. Za ovaj metod se često koristi i termin IP masquerading.
- proxy servisi – metod koji radi pomoću aplikacija višeg sloja, koje omogućavaju hostovima iz interne mreže pristup servisima na javnim serverima.

Sve ove funkcije mogu se obavljati na jednom hostu, ali i na više njih. Ostale funkcije koje firewall system može da pruži su:

- kriptovana autentifikacija – omogućava korisnicima da sa spoljašnje, pristupe unutrašnjoj mreži, ako se identifikuju.
- podrška za virtualne privatne mreže ili VPN (Virtual Private Networking) – tehnologija koja pruža mogućnost uspostavljanja sigurne veze između dve privatne, preko javne mreže, npr. Interneta. VPN mreže se takođe nazivaju enkriptovani tuneli.
- skeniranje virusa – mogućnost da se vrši skeniranje dolaznih podataka da bi se otkrili i uklonili virusi.
- filtriranje sadržaja (content filtering) – mogućnost da se vrši blokiranje pristupa pojedinim servisima na osnovu sadržaja kojem se pristupa.

Filtriranje paketa

Prvi firewall sistemi su bili jednostavni filteri paketa. Filtriranje paketa (packet filtering) ostaje ključna i osnovna funkcija današnjih firewall sistema. Filtriranje je proces u kome se proveravaju paketi mrežnog protokola, kao što je IP, ili transportnog protokola, kao što je TCP. Paketi se upoređuju sa pravilima na osnovu kojih se vrši filtriranje. Pravila se nalaze u tabeli i mogu se naći na ruteru ili nekom od računara sa odgovarajućim softverom za filtriranje.



Filteri sprečavaju prolaz sumljivih paketa u unutrašnjost mreže. Upotreba *firewall* softvera na ruteru ima svojih prednosti. Ruteri se obično nalaze na ulazu u mrežu, kao čvorovi kroz koji mora da prođe ceo saobraćaj upućen na tu mrežu. Filteri koji su podignuti na njima mogu da kontrolišu pristup celoj mreži, delu mreže ili samo ka specifičnom hostu.

Filteri se mogu podići i na pojedinim hostovima. Ti filteri mogu obično da kontrolišu pristup samo onim hostovima na kojima se nalaze. Zbog toga se upotreba filtera na hostovima preporučuje samo kao dodatak i u kombinaciji sa filterima na ulaznim ruterima, a nikako kao jedinstveno rešenje.

Tipična pravila za filtriranje paketa mogu biti raznovrsna. Jedno od osnovnih je sprečavanje pokušaja uspostavljana dolazne konekcije na neki od hostova unutrašnje mreže. Takođe se može vršiti i sprečavanje pristupa određenom opsegu IP adresa, tj. većem broju hostova. Zatim postoji mogućnost dozvoljavanja ili zabrane uspostavljana izlazne konekcije.

Firewall može da vrši i sprečavanje pristupa onim portovima na unutrašnjim računarima, na kojima se nalaze servisi koji ne bi trebali da budu vidljivi na Internetu (npr. NetBIOS session port), a da dozvoli pristup za pakete upućene na portove na kojima se nalaze servisi koji treba da su dostupni sa spoljne mreže (SMTP za servis elektronske pošte ili HTTP za Web servis). Obično se dozvoljava pristup preko SMTP protokola (port 25) samo mail serveru, tj. samo onom hostu u mreži na kome se nalazi taj servis.

Unutrašnjim klijentima se obično dozvoljava izlaz sa mreže. Ako unutrašnji klijent inicira uspostavljanje veze sa spoljašnjim hostom, tada se spoljašnjim hostovima dozvoljava uspostavljanje povratne konekcije sa unutrašnjim hostom, koji je inicirao konekciju. Naime, kada host unutar mreže pokuša da uspostavi TCP konekciju, šalje TCP poruku na IP adresu odredišnog hosta i broj porta javnog servera na tom hostu. U inicijalnoj poruci se naznači IP adresa udaljenog servera i port koji će služiti za uspostavljanje povretne konekcije (npr. port 2050). Spoljašnji server šalje nazad podatke na naznačeni port. Pošto firewall proverava ceo saobraćaj između dva hosta, on zna da je konekcija inicirana sa hosta koji se nalazi unutar mreže, tj. hosta koji je priključen na njegov unutrašnji interfejs tako da taj saobraćaj propušta.

Internet serveri obično imaju otvorene određene portove. Tipični servisi potrebni za rad Internet servera su:

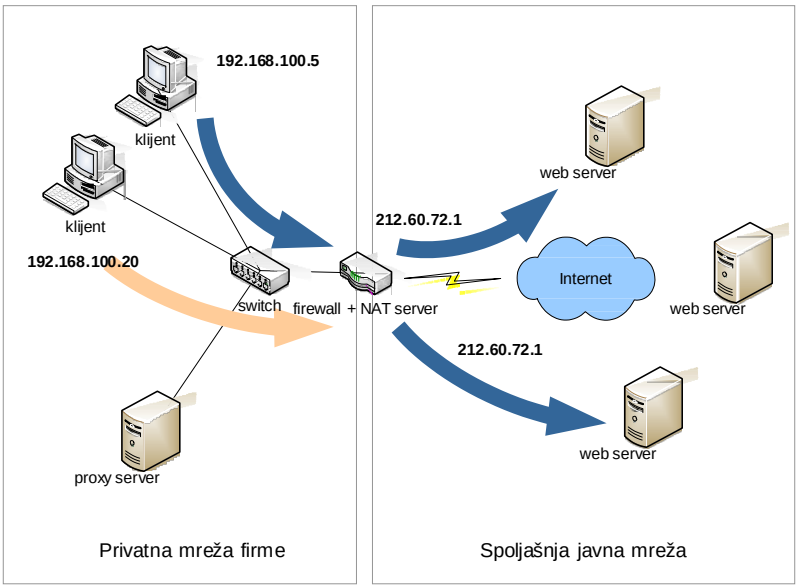
Port	Server
20	File Transfer Protocol (FTP-data)
21	File Transfer Protocol (FTP)
22	SSH - Secure Shell (Enkriptovani udaljeni pristup)
23	Telnet
25	Simple Mail Transfer Protocol (za međuserversku razmenu pošte)
53	Domain Name Service (DNS servis, ako postoji)
80	World Wide Web (HTTP)
110	Post Office Protocol version 3 (za preuzimanje pošte sa servera)
119	Net News (NNTP)
143	Internet Mail Access Protocol (za pristup klijenta mail serveru)
443	Secure HTTP (HTTPS)
8080	HTTP - proxy (squid)

Kada se postavljanju filteri, potrebno je zabraniti pristup svim protokolima i adresama. Nakon toga treba dozvoliti pristup pojedinim servisima i hostovima, ali samo onim za koje je to potrebno. Dalje je potrebno zabraniti sve pokušaje uspostavljanja konekcije u unutrašnjost mreže, jer dozvoljavanjem uspostavljana veze sa spoljne strane može se dozvoliti hakerima prolaz ka Trojan horse virusima ili bagovima u softveru.

NAT (Network Address Translation)

NAT predstavlja rešenje problema skrivanja internih hostova i informacija o njima od potencijalnih napadača. NAT je zastupnički servis mrežnog sloja. Suština ovog servisa je da jedan host, nazvan NAT server, ostvaruje konekcije iz unutrašnje, prema spoljašnjoj mreži i prema javnim serverima u ime ostalih hostova. Na taj način ih krije od ostatka sveta. Windows 2000, Windows XP, Linux i ostali UNIX operativni sistemi podržavaju NAT u sklopu distribucije operativnog sistema.

NAT krije unutrašnje IP adrese pretvaranjem njihovih adresa u adresu firewall sistema. Kada primi zahtev za uspostavljanje konekcije prema spoljašnjoj mreži, firewall to čini koristeći svoj broj TCP porta za uspostavljanje veze sa javnim hostom. Na Internetu, ovaj zahtev za uspostavljanje veze izgleda kao da saobraćaj dolazi sa jednog računara, u ovom slučaju NAT servera.



NAT efikasno krije sve informacije TCP/IP sloja o unutrašnjim hostovima. Adresna translacija takođe dozvoljava upotrebu privatnih IP adresa, koje bez tog servisa ne bi mogle da pristupe Internetu. To može da pomogne u slučajevima kada administrator ne raspolaže dovoljnim brojem javnih IP adresa i kada se ne bi moglo izvršiti adresiranje svih hostova koji treba da pristupaju Internetu.

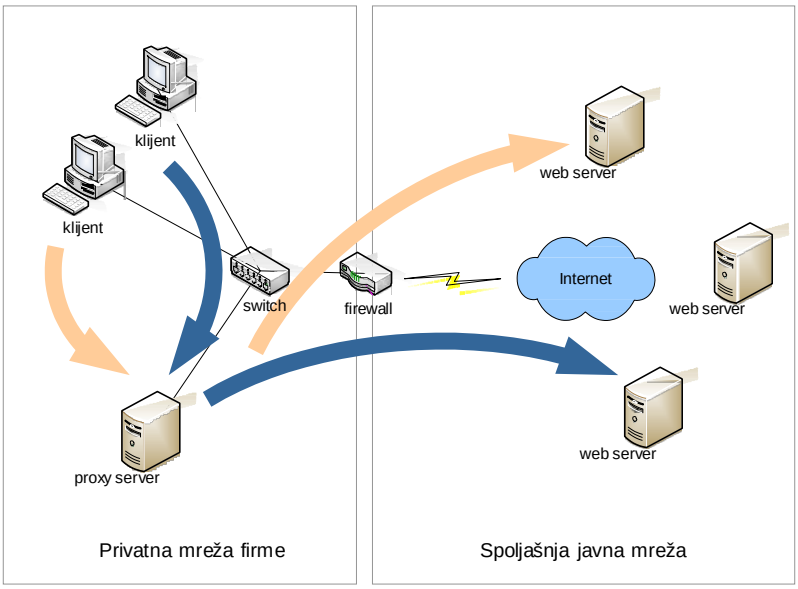
Hostovi unutar mreže se mogu adresirati sa bilo kojim IP adresama, ali to može dovesti do problema ako se neovlašteno dodele adrese koje već postoje na Internetu. Zbog toga se preporučuje upotreba privatnih IP adresa iz nekog, za tu svhu, preporučenih rezervisanih opsega (npr. 192.168.0.0 ili 10.0.0.0 adrese).

NAT takođe dozvoljava pristup Internetu sa većeg broja računara iz unutršanje mreže preko jedne javne IP adrese. To je veoma važno za kompanijske mreže koje ne raspolažu dovoljnim adresnim prostorom i u slučaju kada se deli jedna dial-up konekcija ili jedan pristup preko kablovskog modema.

Proxy servisi

Proxy softver radi na sloju aplikacije. On omogućava da se u potpunosti zabrani protok, na sloju mreže, kroz firewall i da se dozvoli saobraćaj samo sa protokolima višeg sloja kao što su HTTP, FTP i SMTP.

Proxy softver aplikacionog sloja je kombinacija servera i klijenta za specifični protokol. Na primer, Web proxy je kombinacija Web servera i Web klijenta. Serverska strana proxy servisa prima konekciju sa klijenta u unutrašnjoj mreži, klijentska strana proxy servera uspostavlja vezu ka Web serveru na javnoj mreži. Kada klijentski deo proxy servera primi podatke od javnog servera, serverska strana ga prosleđuje klijentu.



Proxy povezuje dve mreže između kojih je zabranjena komunikacija. Kada klijent na zaštićenom delu mreže uspostavi konekciju na javni server, proxy prima zahtev za tu konekciju i uspostavlja konekciju u ime zaštićenog klijenta. Proxy tada prosleđuje odgovor javnog servera na unutrašnju mrežu. Može se reći da proxy ima ulogu posrednika za hostove u unutrašnjoj mreži.

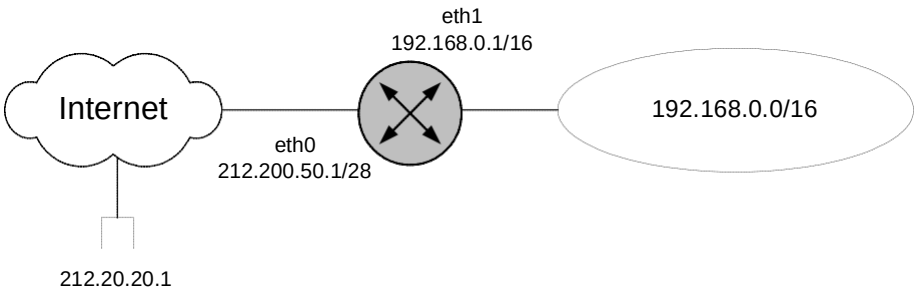
Aplikacioni proxy servisi (kao što Microsoft Proxy Server ili squid), za razliku od NAT servera i paketnih filtera, koriste se samo ako se u korisničkoj aplikaciji to navede. Na primer, u Internet Exploreru treba da se podesi upotreba proxy servera navođenjem njegove IP adrese (ili domenskog imena) i porta na kojem se servis nalazi (obično 8080). Tako Internet Explorer šaje sve svoje zahteve na proxy server, a ne direktno na Internet ka Web sajtovima.

Firewall sistemi - Zadaci

Zadatak 1.1.

Za mrežnu konfiguraciju prikazanu na slici izvršiti konfiguraciju firewall-a tako da se:

a) dozvoli pristup sa unutrašnje mreže (192.168.0.0/16) na pop3 server,
b) dozvoli pristup sa hosta 212.20.20.1 na pop3 server,
c) zabrani pristup sa svih ostalih hostova na isti pop3 server.



Napomena: pop3 server se nalazi na ruteru sa IP adresom 212.200.50.1

Rešenje

```
# brisanje svih pravila u Firewall-u #
iptables –F

# rešenje a) #
iptables -A INPUT -p tcp -s 192.168.0.0/16 --dport 110 -j ACCEPT

# rešenje b) #
iptables -A INPUT -p tcp -s 212.20.20.1/32 --dport 110 -j ACCEPT

# rešenje c) #
iptables -A INPUT -p tcp -s 0.0.0.0/0 --dport 110 -j REJECT
```

Zadatak 1.2.

Za mrežnu konfiguraciju prikazanu na prethodnoj slici izvršiti konfiguraciju firewall-a tako da se:

a) dozvoli pristup sa unutrašnje mreže (192.168.0.0/16) na ftp, ssh, telnet,
b) zabrani pristup sa svih ostalih hostova na iste servise.

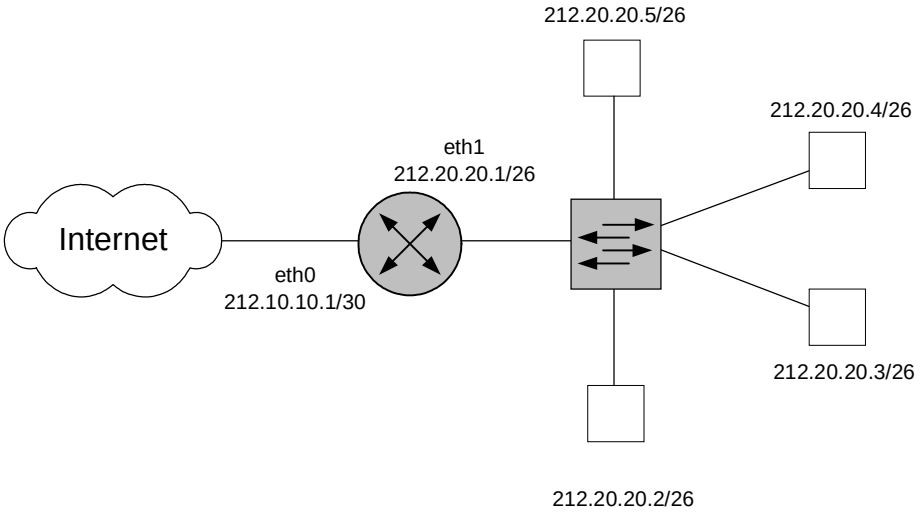
Napomena: navedeni servisi se nalaze na hostu sa IP adresom 212.200.50.1. FTP koristi portove 20 (ftp-data) i 21, ssh port 22, a telnet port 23.

Rešenje

```
# brisanje svih pravila u Firewall-u #
iptables –F

# rešenje a) #
iptables -A INPUT -p tcp -s 192.168.0.0/16 --dport 20:23 -j ACCEPT

# rešenje b) #
iptables -A INPUT -p tcp -s 0.0.0.0/0 --dport 20:23 -j REJECT
```

Zadatak 1.3.

Na slici je prikazana LAN mreža u kojoj su hostovima dodeljena javne IP adrese (212.20.20.0/26). Potrebno je konfigurisati firewall na ulaznom ruteru, tako da se zabrani pristup sa spoljne mreže računarima u LAN mreži.



Napomena: Da bi se računari efikasno zaštitli potrebno je zabraniti celokupan udp saobraćaj koji je sa spoljne mreže upućen na unutrašnju mrežu. Zatim je potrebno zabraniti sve dolazne tcp SYN konekcije koje su upućene sa spoljašne na unutrašnju mrežu. Sve ostale tcp konekcije ne treba zabranjivati da bi se saobraćaj koji su inicirali računari iz unutrašnje mreže mogao normalno odvijati. Za ovakvu konfiguraciju potrebno je koristiti FORWARD lanac, jer je potrebno filtrirati pakete koji nisu generisani na ruteru i koji su upućeni sa spoljne na unutrašnju mrežu, tj. pakete koji prolaze kroz ruter.

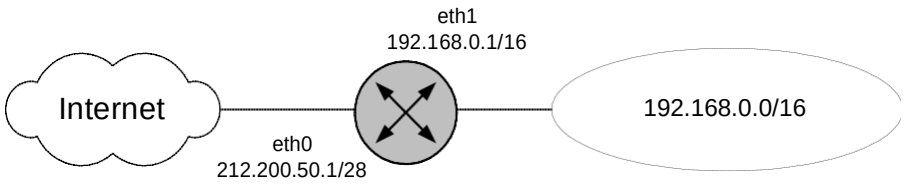
Rešenje

```
# brisanje svih pravila u Firewall-u #
iptables -F

# Zabrana pristupa unutrašnjoj mreži
iptables -A FORWARD -p tcp -s 0.0.0.0/0  -d 212.20.20.0/26  --syn -j REJECT
iptables -A FORWARD -p udp -s 0.0.0.0/0  -d 212.20.20.0/26  -j REJECT
```

Zadatak 1.4.

Za mrežnu konfiguraciju prikazanu na slici izvršiti konfiguraciju firewall-a tako da se omogući adresna translacija. Potrebno je dodeliti javnu IP adresu rutera (212.200.50.1) hostovima iz unutrašnje mreže (192.168.0.0/16).

Napomena: U ovom slučaju potrebno je koristiti nat tabelu i POSTROUTING lanac



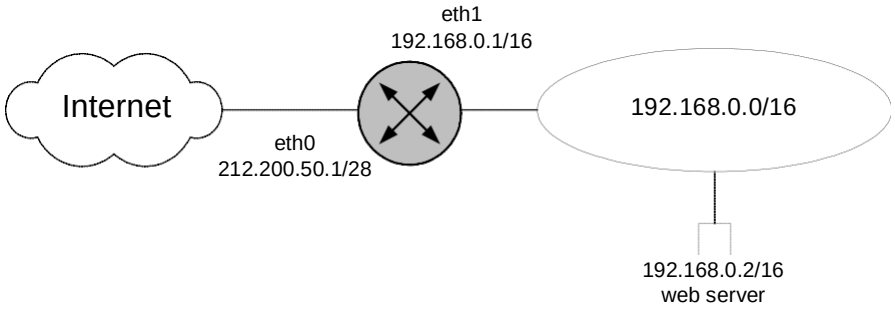
Rešenje

```
# brisanje nat tabele
iptables -F -t nat
```

```
# adresna translacija
iptables -A POSTROUTING -t nat -s 192.168.0.0/16 -o eth0 -j SNAT --to-source 212.200.50.1
```

Zadatak 1.5.

Na slici je predstavljlena mrežna konfiguracija u kojoj je web server postavljen u LAN mrežu. Web serveru je dodeljena privatna IP adresa. Ovo je učinjeno radi dodatne sigurnosti servera. Problem je što spoljni računari ne mogu da pristupe web serveru zbog privatne IP adrese. Da bi se omogućio pristup spoljnim računarima potrebno je izvršiti redirekciju web zahteva, koji dolaze sa spoljašnje mreže na ruter sa javnom IP adresom (212.200.50.1), na privatnu IP adresu web servera (192.168.0.2).



Napomena: redirekciju je moguće izvršiti na više načina. Prvi primer se odnosi na redirekciju celokupnog saobraćaja, a drugi samo na web saobraćaj

Rešenje

```
# brisanje nat tabele
iptables -F -t nat

# redirekcija na unutrašnju mrežu celokupnog saobraćaja
iptables -A PREROUTING -t nat -d 212.200.50.1 -j DNAT --to-destination 192.168.0.2
```

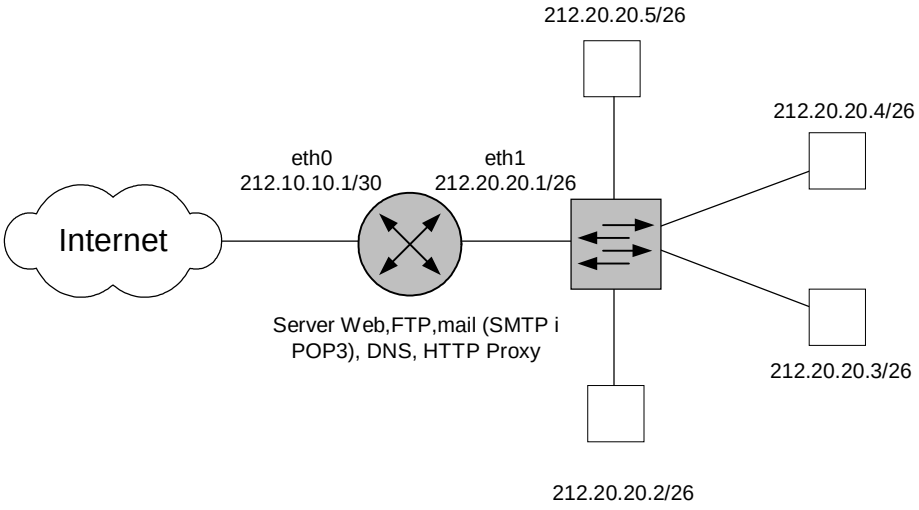
ili

```
# redirekcija na unutrašnju mrežu web saobraćaja
iptables -A PREROUTING -t nat –p tcp -d 212.200.50.1 -–dport 80 -j DNAT --to-destination
192.168.0.2
```

Zadatak 2.1.

Za mrežnu konfiguraciju prikazanu na slici izvršiti konfiguraciju firewall-a tako da se:

c) dozvoli pristup sa spoljne i unutrašnje mreže na DNS, Web, FTP i mail (SMTP) server – 212.10.10.1,
d) zabrane dolazne (SYN konekcije) sa spoljne na unutrašnju mrežu,
e) zabraniti direktan izlazak na Internet svim radnim stanicama osim radne stanice sa IP adresom 212.20.20.3
f) zabrani radnoj stanici 212.20.20.3 pristup mail (SMTP) serverima na spoljašnjoj mreži.



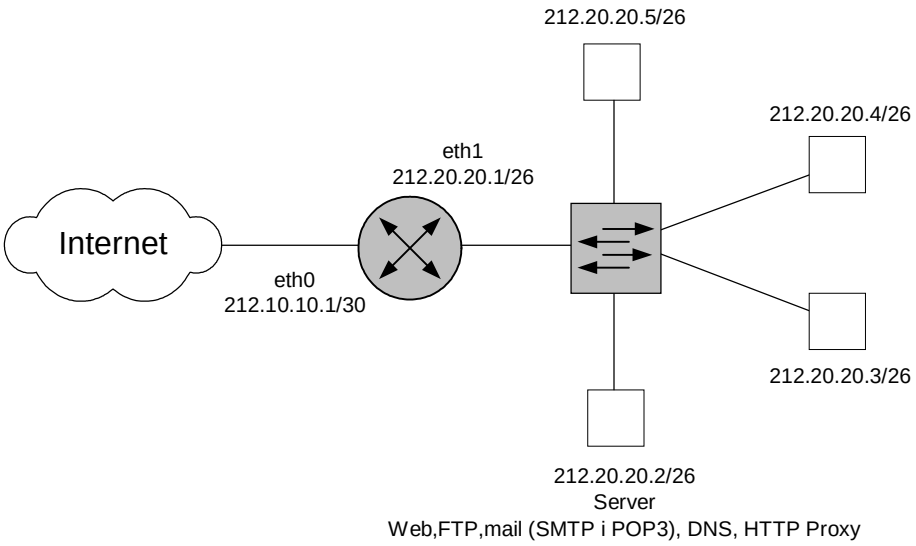
Rešenje

```
# brisanje svih pravila u Firewall-u #
iptables –F

# rešenje pod a) #
iptables -A INPUT -p tcp -d 212.10.10.1/32 --dport 53 -j ACCEPT
iptables -A INPUT -p udp -d 212.10.10.1/32 --dport 53 -j ACCEPT
iptables -A INPUT -p tcp -d 212.10.10.1/32 --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -d 212.10.10.1/32 --dport 21 -j ACCEPT
iptables -A INPUT -p tcp -d 212.10.10.1/32 --dport 20 -j ACCEPT
iptables -A INPUT -p tcp -d 212.10.10.1/32 --dport 25 -j ACCEPT
iptables -A INPUT -p udp -s 0.0.0.0/0 -d 212.20.20.0/26 -j REJECT
iptables -A INPUT -p tcp -s 0.0.0.0/0 -d 212.20.20.0/26 --syn -j REJECT

# rešenje pod b) #
iptables -A FORWARD -p tcp -s 0.0.0.0/0 -d 212.20.20.0/26 --syn -j REJECT
iptables -A FORWARD -p udp -s 0.0.0.0/0 -d 212.20.20.0/26 -j REJECT

# rešenje pod c) #
iptables -A FORWARD -s 212.20.20.3/32 -d 0.0.0.0-0 -j ACCEPT
iptables -A FORWARD -s 212.20.20.0/26 -d 0.0.0.0/0 -j REJECT

# rešenje pod d) #
iptables -A FORWARD –p tcp -s 212.20.20.3/32 -d 0.0.0.0-0 –dport 25 -j REJECT
```

Zadatak 2.2.

Za mrežnu konfiguraciju prikazanu na slici izvršiti konfiguraciju firewall-a tako da se:

a) dozvoli pristup sa spoljne mreže na DNS, Web, FTP i mail (SMTP) server – 212.10.10.1,
b) zabrane dolazne (SYN konekcije) sa spoljne na unutrašnju mrežu,
c) zabraniti direktan izlazak na Internet svim radnim stanicama osim na web servis

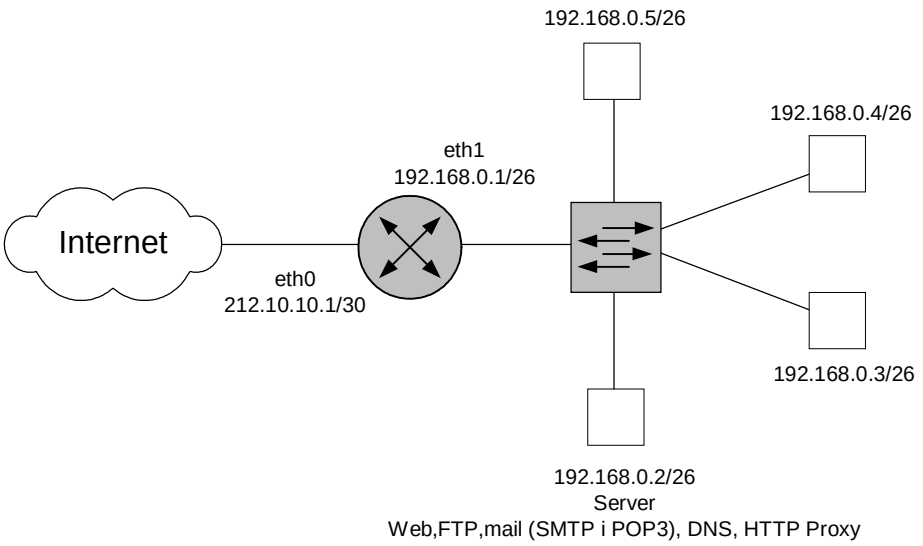



```
# brisanje svih pravila u Firewall-u #
iptables –F

# rešenje pod a) #
iptables -A INPUT -p tcp -d 212.10.10.1/32 --dport 53 -j ACCEPT
iptables -A INPUT -p udp -d 212.10.10.1/32 --dport 53 -j ACCEPT
iptables -A INPUT -p tcp -d 212.10.10.1/32 --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -d 212.10.10.1/32 --dport 21 -j ACCEPT
iptables -A INPUT -p tcp -d 212.10.10.1/32 --dport 20 -j ACCEPT
iptables -A INPUT -p tcp -d 212.10.10.1/32 --dport 25 -j ACCEPT
iptables -A INPUT -p udp -s 0.0.0.0/0 -d 212.20.20.0/26 -j REJECT
iptables -A INPUT -p tcp -s 0.0.0.0/0 -d 212.20.20.0/26 --syn -j REJECT

# rešenje pod b) #
iptables -A FORWARD -p tcp -s 0.0.0.0/0 -d 212.20.20.0/26 --syn -j REJECT
iptables -A FORWARD -p udp -s 0.0.0.0/0 -d 212.20.20.0/26 -j REJECT

# rešenje pod c) #
iptables -A FORWARD –p tcp -s 212.20.20.0/26 -d 0.0.0.0-0 –dport 80 -j ACCEPT
iptables -A FORWARD -s 212.20.20.0/26 -d 0.0.0.0/0 -j REJECT
```

Zadatak 2.3.

Za mrežnu konfiguraciju prikazanu na slici izvršiti konfiguraciju firewall-a tako da se:

a) dozvoli pristup sa spoljne mreže na DNS, Web, FTP i mail (SMTP) server – 192.168.0.2 (napomena: pošto se ovi servisi nalaze na računaru sa privatnom IP adresom, potrebno je izvšiti redirekciju na njih),
b) zabrane dolazne (SYN konekcije) sa spoljne na unutrašnju mrežu,
c) omogući izlazak na Internet mrežu hostovima 192.168.0.3 i 192.168.0.4 pomoću NAT servera



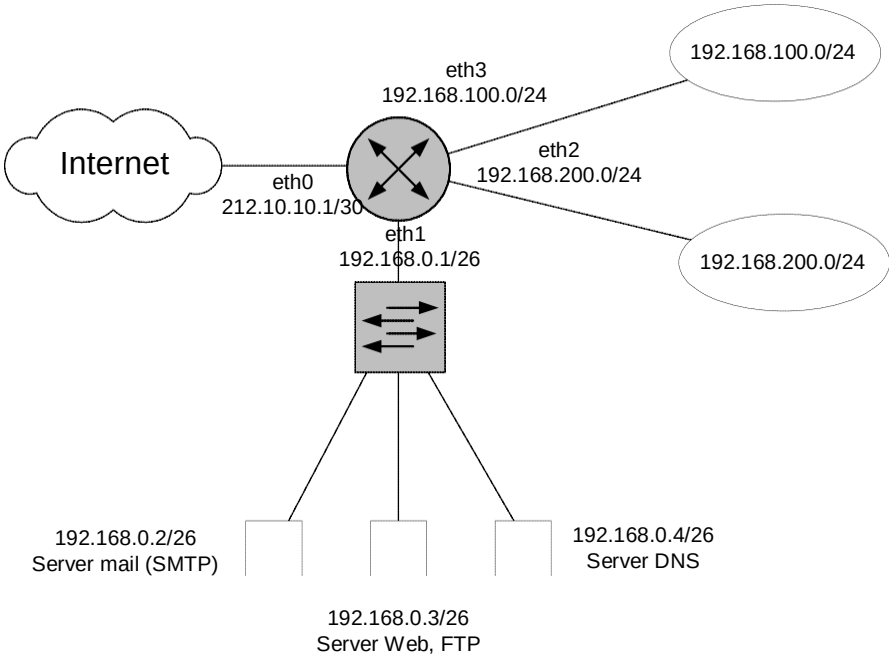
Rešenje

```
# brisanje svih pravila u Firewall-u #
iptables –F

# rešenje a) #
iptables -A PREROUTING -t nat –p tcp -d 212.10.10.1 -–dport 53 -j DNAT --to-destination
192.168.0.2
iptables -A PREROUTING -t nat –p udp -d 212.10.10.1 -–dport 53 -j DNAT --to-destination
192.168.0.2
iptables -A PREROUTING -t nat –p tcp -d 212.10.10.1 -–dport 80 -j DNAT --to-destination
192.168.0.2
iptables -A PREROUTING -t nat –p tcp -d 212.10.10.1 -–dport 20 -j DNAT --to-destination
192.168.0.2
iptables -A PREROUTING -t nat –p tcp -d 212.10.10.1 -–dport 21 -j DNAT --to-destination
192.168.0.2
iptables -A PREROUTING -t nat –p tcp -d 212.10.10.1 -–dport 25 -j DNAT --to-destination
192.168.0.2

# rešenje b) #
iptables -A FORWARD -p tcp -s 0.0.0.0/0 -d 192.168.0.2/26 --syn -j REJECT
iptables -A FORWARD -p udp -s 0.0.0.0/0 -d 192.168.0.2/26 -j REJECT

# adresna translacija – rešenje c)
iptables -A POSTROUTING -t nat -s 192.168.0.3/32 -o eth0 -j SNAT --to-source 212.10.10.1
iptables -A POSTROUTING -t nat -s 192.168.0.4/32 -o eth0 -j SNAT --to-source 212.10.10.1
```

Zadatak 2.4.

Za mrežnu konfiguraciju prikazanu na slici izvršiti konfiguraciju firewall-a tako da se:

a) dozvoli pristup sa spoljne mreže na DNS, Web, FTP i mail (SMTP) server (napomena: pošto se ovi servisi nalaze na računaru sa privatnom IP adresom, potrebno je izvšiti redirekciju na njih),
b) zabrane dolazne (SYN konekcije) sa spoljne na unutrašnju mrežu.



Rešenje

brisanje svih pravila u Firewall-u
iptables –F

rešenje a)
iptables -A PREROUTING -t nat –p tcp -d 212.10.10.1 -–dport 25 -j DNAT --to-destination 192.168.0.2
iptables -A PREROUTING -t nat –p tcp -d 212.10.10.1 -–dport 80 -j DNAT --to-destination 192.168.0.3
iptables -A PREROUTING -t nat –p tcp -d 212.10.10.1 -–dport 20 -j DNAT --to-destination 192.168.0.3
iptables -A PREROUTING -t nat –p tcp -d 212.10.10.1 -–dport 21 -j DNAT --to-destination 192.168.0.3
iptables -A PREROUTING -t nat –p tcp -d 212.10.10.1 -–dport 53 -j DNAT --to-destination 192.168.0.4
iptables -A PREROUTING -t nat –p udp -d 212.10.10.1 -–dport 53 -j DNAT --to-destination 192.168.0.4

rešenje b)
iptables -A FORWARD -p tcp -s 0.0.0.0/0 -d 192.168.0.2/26 --syn -j REJECT
iptables -A FORWARD -p udp -s 0.0.0.0/0 -d 192.168.0.2/26 -j REJECT

Zadatak 2.5.

U ovom primeru data je kompletna konfiguracija za tipičan firewall. Svako od pravila je ukratko objašnjeno.

Kreiranje default pravila (-P), tj. pravila koja se primenjuju ako nijedno drugo pravilo nije primenljivo

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

# Brisanje svih pravila
iptables -F
iptables -F -t nat

# Forward svih paketa sa eth1 (interna mreža) na eth0 (Internet).
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT

# Forward paketa koji su deo postojećih konekcija sa eth0 na eth1.
iptables -A FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Dozvola ulaska paketima u firewall ako su deo postojećih konekcija
iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Dozvola ulaska paketima u firewall sa unutrašnje mreže i lokalnog interfejsa
iptables -A INPUT -i eth1 -s 0/0 -d 0/0 -j ACCEPT
iptables -A INPUT -i lo -s 0/0 -d 0/0 -j ACCEPT

# Omogućavanje SNAT funkcionalnosti za unutrašnju mrežu na eth0
iptables -A POSTROUTING -t nat -s 192.168.0.0/24 -o eth0 -j SNAT --to-source 66.14.136.144

# Alternativno se umesto SNAT može korisititi MASQUERADE ako firewall koristi dinamičku IP adresu
# (uz pomoć DHCP protokola) pa se ne može predvideti koja će se javna adresa dodeliti firewall-u, tj.
# NAT serveru.
#
# iptables -A POSTROUTING -t nat -o eth0 -j MASQUERADE
#

# Zabrana pristupa svim IP paketima kojima je izvorišna adresa spoof-ovana, tj. dolaze sa izvorišnom IP
# adresom koja pripada unutrašnjoj mreži, a preko spoljašnjeg interfejsa eth0

iptables -A INPUT -i eth0 -s 66.14.136.144/32 -j DROP
iptables -A INPUT -i eth0 -s 66.14.136.145/32 -j DROP
iptables -A INPUT -i eth0 -s 66.14.136.146/32 -j DROP
iptables -A INPUT -i eth0 -s 66.14.136.147/32 -j DROP
iptables -A INPUT -i eth0 -s 66.14.136.148/32 -j DROP
iptables -A INPUT -i eth0 -s 192.168.0.0/24 -j DROP
iptables -A INPUT -i eth0 -s 127.0.0.0/8 -j DROP

# Prihvatanje svih dolaznih tcp SYN paketa za protokole SMTP, HTTP, HTTPS i SSH:
iptables -A INPUT -p tcp -s 0/0 -d 66.14.136.145/32 --destination-port 25 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 80 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 443 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 22 --syn -j ACCEPT

# Napomena: prethodni primer se odnosi na situaciju kada se servisi nalaze na firewall-u. Ako
```

```
# se servisi nalaze na hostu u unutrašnjoj mreži, tj. ako paketi upućeni na te servise prolaze kroz
# firewall, koristi se FORWARD lanac
#
# iptables -A FORWARD -p tcp -s 0/0 -d 66.14.136.145/32 --destination-port 25 --syn -j ACCEPT
# iptables -A FORWARD -p tcp -s 0/0 -d 0/0 --destination-port 80 --syn -j ACCEPT
# iptables -A FORWARD -p tcp -s 0/0 -d 0/0 --destination-port 443 --syn -j ACCEPT
# iptables -A FORWARD -p tcp -s 0/0 -d 0/0 --destination-port 22 --syn -j ACCEPT
#


# Dozvola prolaska paketa na DHCP server:
iptables -A INPUT -i eth1 -p tcp --sport 68 --dport 67 -j ACCEPT
iptables -A INPUT -i eth1 -p udp --sport 68 --dport 67 -j ACCEPT

# DNS upiti
# Dozvola UDP odgovora za određeni DNS server
iptables -A INPUT -p udp -s <IP adresa DNS servera> --source-port 53 -d 0/0 -j ACCEPT

# Dozvola postavljanja upita za DNS
iptables -A INPUT -p udp -s 0/0 -d 0/0 --destination-port 53 -j ACCEPT

# Za pristup FTP serveru sa određenih hostova
iptables -A INPUT -p tcp -s 66.14.136.144/32 -d 0/0 --destination-port 20 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 66.14.136.144/32 -d 0/0 --destination-port 21 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 66.14.136.145/32 -d 0/0 --destination-port 20 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 66.14.136.145/32 -d 0/0 --destination-port 21 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 66.14.136.146/32 -d 0/0 --destination-port 20 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 66.14.136.146/32 -d 0/0 --destination-port 21 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 66.14.136.147/32 -d 0/0 --destination-port 20 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 66.14.136.147/32 -d 0/0 --destination-port 21 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 66.14.136.148/32 -d 0/0 --destination-port 20 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 66.14.136.148/32 -d 0/0 --destination-port 21 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 127.0.0.1/8 -d 0/0 --destination-port 20 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 127.0.0.1/8 -d 0/0 --destination-port 21 --syn -j ACCEPT

# Na kraju, treba odbiti sve konekcije na bilo koji UDP i sve SYN konekcije na TCP portvor
# na koje nismo dizvolili ulazak. Mogu se korisiti DROP i REJECT direktive

iptables -A INPUT -s 0/0 -d 0/0 -p udp -j DROP
iptables -A INPUT -s 0/0 -d 0/0 -p tcp --syn -j DROP
```

Uspostavljanjem ovog projekta, zadovoljila se i veoma prisutna potreba za specijalizovanim timom, koji će na studente i omladinu pravovremeno i adekvatno delovati u edukativnom i pozitivno usmeravajućem pravcu, ali i predstavljati efikasnu podršku u pisanju sopstvenih radova (seminarskih, maturski, maturalnih, diplomskih, master, magistarskih, doktorskih, eseja …...)

TIM VRHUNSKIH PREVODILACA PREVODI ZA VAS SA I NA SLEDEĆE JEZIKE:

ENGLESKI, FRANCUSKI, ŠPANSKI, NEMAČKI, ITALIJANSKI