**IPTABLES ULERTZEKO ADIBIDEAK**



**Egilea:** Urko Zuñiga

**Zuzentzailea:** Amaia Erostarbe

Aurkibidea

[1 Aldez aurretiko urratsak 3](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857883)

[1.1 *Forwarding bit*a aktibatu 3](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857884)

[1.2 *Iptables* aktibatu sistemaren hasieran 3](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857885)

[2 Erregelak 3](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857886)

[3 Praktika 4](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857887)

[3.1 Sarea](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857888) 4

[3.2 *Script*a 4](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857889)

[3.2.1 Kontuan hartzekoak 4](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857890)

[3.2.2 *Script*a idatzi 4](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857891)

[3.2.3 *Script*a exekutatu 7](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857892)

3.2.3.1. *Filter* taula……………………………………………………………………………………………………….7

3.2.3.2. NAT taula…………………………………………………………………………………………………………8

[3.3 *Netfilter* 8](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857893)

[3.3.1 Eskema 8](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857894)

[3.3.2 Adibideak 9](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857895)

3.3.2.1. SSH eskaera LAN saretik suebakira………………………………………………………………....9

3.3.2.2. SSH eskaera Internetetik gure zerbitzarira…………………………………….………………10

3.3.2.3. PING DMZ saretik LAN sarerantz……………………………………………………………………11

3.3.2.4. Internetetik gure web-orrira nabigatu…………………………………………………………..12

3.3.2.5. DNS eskaera sare lokaletik Internetera………………………………………………………….12

3.3.2.6. Suebakitik Interneterako nabigazioa…………………………………………….……………….13

3.3.2.7. Internetera nabigatu LAN saretik……………………………………………………………….….14

[3.4 *Script*a hobetu 15](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857896)

[3.4.1 *Proxy* 15](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857897)

[4 Bibliografia .……………………………………………………………………………………………………………..…….16](file:///C:\Users\ir013360ae\Desktop\0.%20IPTABLES%20ulertzeko%20adibideak.docx#_Toc477857898)

# Aldez aurretiko urratsak

## *Forwarding bit*a aktibatu

*Forwarding bit*a aktibatu behar da, GNU/*Linux* ekipo batek routeatu dezan; aktibatzen ez bada, ez dute elkar ikusiko zuzenean suebakira konektatutako bi sareetako ekipoek. Aktibatzeko, honako lerro hau erantsiko dugu *script*ean:

echo "1">/proc/sys/net/ipv4/ip\_forward

## Sistemaren hasieran *Iptables* suebakia aktibatu

Sistemaren hasieran *Iptables* suebakia aktibatzeko, hauexek dira jarraibideak:

1. Sortu *script*a */etc* direktorioan.
2. Esleitu exekutatze-baimenak *script*ari.
3. Sartu lerro bat *script*aren ibilbide osoarekin */etc/rc.local* fitxategian.

# Erregelak

Honako hauek dira erregelak:

* iptables -I 🡪 \*insert\*. *Iptables*aren hasieran sartzen du erregela; azkar egiaztatzeko erabili ohi da erregela, eta, ondoren, ezabatu egiten da.
* iptables -A 🡪 \*append\*. Aukeratutako katearen bukaeran eransten du erregela; *script*etan erabili ohi da, erregelak s*cript*ean idatzitako ordenan gordetzea nahi dugulako.

Erregelan ataka bat idatzi nahi baldin badugu, bi era daude: ataka-zenbakia jartzea edo zerbitzuaren izena jartzea (*/etc/services* fitxategian zehaztutakoa):

Erregela sortzeko: iptables *-*I INPUT-m state -state NEW -j DROP

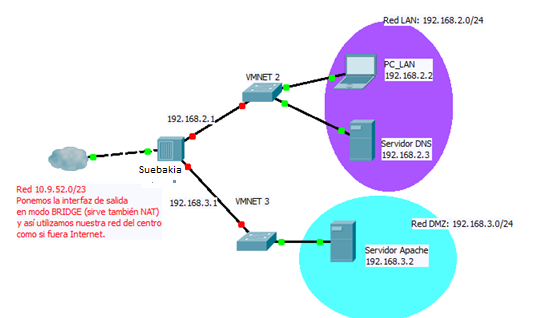
Erregela ezabatzeko: iptables *-*D INPUT -m state -state NEW -j DROP

# Praktika

## Sarea

Sareko egitura honetatik abiatuko gara:

**LAN sarea   
192.168.2.0/24**



eth1

eth0

eth2

DNS zerbitzaria  
192.168.2.3

**DMZ sarea   
192.168.3.0/24**

**10.9.52.0/23 sarea**eth2 irteera-interfazea BRIDGE moduan jarriko dugu (NATak ere balio du), eta, horrela, zentroko gure sarea Internet izango balitz bezala erabiliko dugu.

Apache zerbitzaria  
192.168.3.2

Kontuan izan ekipo batek, interfaze asko baldin baditu ere, sarbide-ate bakarra izan behar duela zehaztuta. Gure kasuan, interfaze bakarrari esleituko diogu sarbide-atea suebakian. Interfaze hori Internetera dago konektatuta.

## *Script*a

### Kontuan hartzekoak

Seguruago aritzeko, komenigarria da *DROP* izatea lehenetsitako politika *filter* taulako kate guztietan; horrela, trafiko guztia, berez, debekatuta egongo da. Zerbait baimendu nahi dugunean, unean egin beharko dugu. Zergatik erabili *DROP* eta ez *REJECT*? *REJECT*ekin erantzuna bidaltzen diogu igorleari, eta, hala, erasotzaileak arrastoa antzeman dezake.

### *Script*a idatzi

#Adi! Idazteko baimenak esleitu behar dizkiogu *script*ari.

#Hobetu daiteke: erregeletan, ahal denean, interfazeak erabili behar dira IPekin batera.

#Balizko IP publikoa 10.9.52.33.

#*Iptables*eko taula guztiak garbituko ditugu.

IPTABLES =/sbin/iptables

cat /proc/net/ip\_tables\_names | while read table; do

test "X$table" = "Xmangle" && continue

$IPTABLES -t $table -L -n | while read c chain rest; do

if test "X$c" = "XChain" ; then

$IPTABLES -t $table -F $chain

fi

done

$IPTABLES -t $table -X

done

#Honaino garbitzeko prozesua.

#Aldagaiak definitu.

LAN\_SAREA=192.168.2.0/24

DMZ\_SAREA=192.168.3.0/24

IP\_PUBLIKOA=10.9.52.33

#*Forward* aukera.

echo "1">/proc/sys/net/ipv4/ip\_forward

#*Filter* taulako kate guztietan *DROP* jarriko dugu (lehenetsitako politika).

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

#Irteerako NATa sare lokalerako. Suebakiaren IP publikoarekin irtengo da Internetera. *MASQUERADE* ere erabil daiteke.

iptables -t nat -A POSTROUTING -s 192.168.2.0/24 ! -d 192.168.3.0/24 -j SNAT --to-source $IP\_PUBLIKOA

#Irteerako NATa DMZ sarerako. Suebakiaren IP publikoarekin irtengo da

Internetera; *MASQUERADE* ere erabil daiteke.

iptables -t nat -A POSTROUTING -s 192.168.3.0/24 ! -d 192.168.2.0/24 -j SNAT --to-source $IP\_PUBLIKOA

#Sarrerako NATa Internetetik gure web-orrira nabigatzeko eskaerak DMZko zerbitzarira joan daitezen.

iptables -t nat -A PREROUTING -s 0/0 -d $IP\_PUBLIKOA -p tcp --dport 80 -j DNAT --to 192.168.3.2

#Sarrerako NATa Internetetik gure IP publikora heldutako SSH eskaerak DMZko zerbitzarira joan daitezen.

iptables -t nat -A PREROUTING -s 0/0 -d $IP\_PUBLIKOA -p tcp --dport 22 -j DNAT --to 192.168.3.2

# *Loopback* interfazetik edozein motatako *loppback* trafikoa baimenduko dugu. Hauxe da zergatia: batzuetan, aplikazio lokalek ordenagailuaren beraren sareko zerbitzuak erabili behar dituzte; X11rekin zerikusia dauka, adibidez.

iptables -A INPUT -i lo -j ACCEPT

iptables -A FORWARD -i lo -j ACCEPT

iptables -A OUTPUT -o lo -j ACCEPT

#Aldez aurretik ezarritako konexioak eta konexio erlazionatuak baimenduko ditugu *filter* taulako kate guztietan.

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# DMZko web-orrira nabigatzea baimenduko dugu.

iptables -A FORWARD -s 0/0 -d 192.168.3.2 -p tcp --dport 80 -m state --state NEW -j ACCEPT

#Sare lokaletik Internetera nabigatzea baimenduko dugu.

iptables -A FORWARD -s 192.168.2.0/24 ! -d 192.168.3.0/24 -p tcp --dport 80 -m state --state NEW -j ACCEPT

#DNS pribatuak "/etc/bind/named.conf.options" fitxategiko *forwarders* eremuan adierazitako DNSari eskaerak egitea baimenduko dugu.

iptables -A FORWARD -s 192.168.2.0/24 ! -d 192.168.3.0/24 -p udp --dport 53 -m state --state NEW -j ACCEPT

#DMZtik Internetera nabigatzea baimenduko dugu.

iptables -A FORWARD -s 192.168.3.0/24 ! -d 192.168.2.0/24 -p tcp --dport 80 -m state --state NEW -j ACCEPT

# Suebakia bera edonora konektatzea baimenduko dugu.

iptables -A OUTPUT -s $IP\_PUBLIKOA -d 0/0 -m state --state NEW -j ACCEPT

iptables -A OUTPUT -s 192.168.2.1 -d 0/0 -m state --state NEW -j ACCEPT

iptables -A OUTPUT -s 192.168.3.1 -d 0/0 -m state --state NEW -j ACCEPT

#Internetetik gure DMZko SSH zerbitzariarekin konektatzea baimenduko dugu.

iptables -A FORWARD -s 0/0 -d 192.168.3.2 -p tcp --dport 22 -m state --state NEW -j ACCEPT

#Suebakiaren SSH zerbitzuari egindako eskaerak baimenduko ditugu, sare lokaletik edo DMZtik baldin badatoz.

iptables -A INPUT -s $DMZ\_SAREA -d 192.168.3.1 -p tcp --dport 22 -m state --state NEW -j ACCEPT

iptables -A INPUT -s $SARE\_LOKALA -d 192.168.2.1 -p tcp --dport 22 -m state --state NEW -j ACCEPT

#Sare lokaletik edo DMZtik suebakira PING egitea baimenduko dugu

iptables -A INPUT -s $DMZ\_SAREA -d 192.168.3.1 -p icmp -m state --state NEW -j ACCEPT

iptables -A INPUT -s $SARE\_LOKALA -d 192.168.2.1 -p icmp -m state --state NEW -j ACCEPT

#Sare lokaletik suebakian DMZrekin lotutako interfazera PING egitea baimentzen dugu.

iptables -A INPUT -s $SARE\_LOKALA -d 192.168.3.1 -p icmp -m state --state NEW -j ACCEPT

#Internetetik gure IP publikora PING egitea baimenduko dugu.

iptables -A INPUT -s 0/0 -d $IP\_PUBLIKOA -p icmp -m state --state NEW -j ACCEPT

# Sare lokaletik eta DMZtik edonora PING egitea baimenduko dugu, baina ez DMZtik sare lokalera PING egitea.

iptables -A FORWARD -s $SARE\_LOKALA -d 0/0 -p icmp -m state --state NEW -j ACCEPT

iptables -A FORWARD -s $DMZ\_SAREA ! -d $SARE\_LOKALA -p icmp -m state --state NEW -j ACCEPT

### *Script*a exekutatu

Exekuzio-baimenak eman behar dizkiogu fitxategiari. Nahikoa da 750 ematea. Behin exekutatuta, kateak halaxe egongo dira ordenatuta:

#### Filter taula

*INPUT* katea

1. iptables -A INPUT -i lo -j ACCEPT
2. iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
3. iptables -A INPUT -s $DMZ\_SAREA -d 192.168.3.1 -p tcp --dport 22 -m state --state NEW -j ACCEPT
4. iptables -A INPUT -s $SARE\_LOKALA -d 192.168.2.1 -p tcp --dport 22 -m state --state NEW -j ACCEPT
5. iptables -A INPUT -s $DMZ\_SAREA -d 192.168.3.1 -p icmp -m state --state NEW -j ACCEPT
6. iptables -A INPUT -s $SARE\_LOKALA -d 192.168.2.1 -p icmp -m state --state NEW -j ACCEPT
7. iptables -A INPUT -s $SARE\_LOKALA -d 192.168.3.1 -p icmp -m state --state NEW -j ACCEPT
8. iptables -A INPUT -s 0/0 -d $IP\_PUBLIKOA -p icmp -m state --state NEW -j ACCEPT

*OUTPUT* katea

1. iptables -A OUTPUT -o lo -j ACCEPT
2. iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
3. iptables -A OUTPUT -s $IP\_PUBLIKOA -d 0/0 -m state --state NEW -j ACCEPT
4. iptables -A OUTPUT -s 192.168.2.1 -d 0/0 -m state --state NEW -j ACCEPT
5. iptables -A OUTPUT -s 192.168.3.1 -d 0/0 -m state --state NEW -j ACCEPT

*FORWARD* katea

1. iptables -A FORWARD -i lo -j ACCEPT
2. iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
3. iptables -A FORWARD -s 192.168.2.0/24 -d 192.168.3.2 -p tcp --dport 80 -m state --state NEW -j ACCEPT
4. iptables -A FORWARD -s 192.168.2.0/24 ! -d 192.168.3.0/24 -p tcp --dport 80 -m state --state NEW -j ACCEPT
5. iptables -A FORWARD -s 192.168.2.0/24 ! -d 192.168.3.0/24 -p udp --dport 53 -m state --state NEW -j ACCEPT
6. iptables -A FORWARD -s 192.168.3.0/24 ! -d 192.168.2.0/24 -p tcp --dport 80 -m state --state NEW -j ACCEPT
7. iptables -A FORWARD -s 0/0 -d 192.168.3.2 -p tcp --dport 22 -m state --state NEW -j ACCEPT
8. iptables -A FORWARD -s $SARE\_LOKALA -d 0/0 -p icmp -m state --state NEW -j ACCEPT
9. iptables -A FORWARD -s $DMZ\_SAREA ! -d $SARE\_LOKALA -p icmp -m state --state NEW -j ACCEPT

#### NAT taula

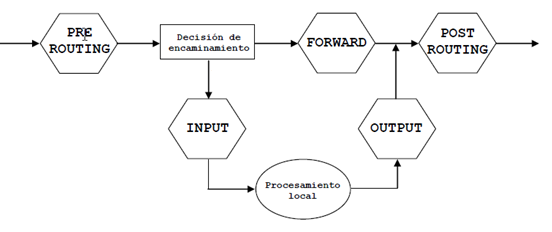
*PREROUTING* katea

1. iptables -t nat -A PREROUTING -s 0/0 -d $IP\_PUBLIKOA -p tcp --dport 80 -j DNAT --to 192.168.3.2
2. iptables -t nat -A PREROUTING -s 0/0 -d $IP\_PUBLIKOA -p tcp --dport 22 -j DNAT --to 192.168.3.2

*POSTROUTING* katea

1. iptables -t nat -A POSTROUTING -s 192.168.2.0/24 ! -d 192.168.3.0/24 -j SNAT --to-source $IP\_PUBLIKOA
2. iptables -t nat -A POSTROUTING -s 192.168.3.0/24 ! -d 192.168.2.0/24 -j SNAT --to-source $IP\_PUBLIKOA

* 1. ***Netfilter***
     1. **Eskema**

****

**EZ**

**BAI**

**BIDERATZE-ERABAKIA:**  
**Helburua FW makina bera da?**

Goiko eskemak suebakian gertatutakoari baino ez dio erreferentzia egiten. Prozesatze lokala esaten dugunean, zer esan nahi dugu? suebakian berak prozesatzen duela paketea, bai suebakian zuzendutakoa delako, bai suebakian sortutakoa delako. Prozesatze lokalak, hortaz, ez du esan nahi sare lokal osoan prozesatzen denik.

* + 1. **Adibideak**

Erregela baten ekintza gauzatzeko, erregela ostean dator horren baldintza guztiak bete behar dira: *eta*rekin elkartuta daude eta ez *edo*rekin. Ekintza, hala, -*j*ren.

Zerbitzariaren eta bezeroaren arteko konexioa ezartzeko, bezeroak zerbitzariari igorritako lehenengo paketea *NEW* izeneko egoeran dago; hau da, *syn* *flag*a aktibatuta dago. Konexio horretako beste pakete guztiak *ESTABLISHED* egoeran daude; alegia, *syn* eta *ack flag*ak aktibatuta daude.

*RELATED* egoera ere existitzen da, nahiz eta oso gutxitan agertu. Litekeena da protokolo jakin bat erabilita bidaltzea lehenengo paketea eta, erantzuteko, beste protokolo bat erabiltzea; hartara, azken pakete hori *RELATED* egoeran egongo da. Gure *script*eko 2, 10 eta 15 erregelek *ESTABLISHED* eta *RELATED* egoeretako pakete guztiak onartzen dituzte *filter* taulako kate guztietan. Horrela, zera saihestuko da: erantzunak banan-banan kontrolatu behar izatea *script*ean edozein trafiko mota zabaltzean.

**3.3.2.1.SSH eskaeraLANsaretik suebakira**

Suebakian *openssh* zerbitzua instalatuko dugu. Demagun LAN sareko 192.168.2.2 IP protokoloko PCan honako hau idatzi dugula: *“ssh* [*erabiltzailea@192.168.2.1*](mailto:erabiltzailea@192.168.2.1)”. Onartu egin behar da sortutako paketea. Ikusi taula:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Paketearen informazioa | **Protokoloa** | **Jatorrizko IPa** | **Helburu-IPa** | **Helburu-ataka** |
| TCP | 192.168.2.2 | 192.168.2.1 | 22 |

Hauexek dira paketeak eskeman jarraituko dituen urratsak:

1. Suebakian bertan sortutako paketea da?

Ez. Beraz, hasierara joango da paketea.

1. ***PREROUTING* katea**

23. erregela aztertuko da. Betetzen al dira baldintza hauek guztiak?

* 1. Paketea edonondik dator BAI
  2. Gure IP publikoa da helburua EZ
  3. TCP paketea da BAI
  4. Helburu-ataka 80 da? EZ

Baldintza guztiak betetzen ez direnez, kate horretako hurrengo erregelara joko du paketeak, eta 24. erregela aztertuko da. Betetzen al dira baldintza hauek guztiak?

1. Paketea edonondik dator BAI
2. Gure IP publikoa da helburua EZ
3. TCP paketea da BAI
4. Helburu-ataka 22 da? BAI

Baldintza guztiak betetzen ez direnez eta *PREROUTING* katean ez dagoenez beste erregelarik, paketeak aurrera egingo du eskeman. Bideratze-erabakia hartu beharko du orain: helburu-IPa (192.168.2.1) suebakiko bertako interfazeetako IPetako bat da? Bai. Orduan, *INPUT* katera joko du paketeak.

1. ***INPUT* katea**

1. erregelatik aurrerakoak aztertuko dira, ordenan. Ez dira betetzen 1., 2. eta 3. erregeletako baldintza guztiak; 4. erregelakoak, ordea, bai. Bada, 4. erregelako ekintza gauzatuko da: *ACCEPT*. Ondoren, paketeak aurrera jarraituko du eskeman, eta *POSTROUTING* katera iritsiko da.

1. ***POSTROUNTIG* katea**

Ez da 25. erregela betetzen, ezta 26. erregela ere. Paketea *Netfilter* eskematik joango da.

Beraz, nahi genuen bezala, paketea onartu, eta baimendu egin da komunikazioa.

**3.3.2.2.SSH eskaera internetetik gure zerbitzarira**

Demagun ikastetxeko LAN sareko (alegiazko Internet, guretzat) 10.9.53.201 IP protokolodun PCan norbaitek *“ssh* [*erabiltzaile@10.9.52.33*](mailto:erabiltzaile@10.9.52.33)*”* idatzi duela terminalean. Onartu egin behar da sortu den paketea. Ikusi taula:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Paketearen informazioa | **Protokoloa** | **Jatorrizko IPa** | **Helburu-IPa** | **Helburu-ataka** |
| TCP | 10.9.53.201 | 10.9.52.33 | 22 |

Hauexek dira paketeak eskeman jarraituko dituen urratsak:

1. Suebakian bertan sortutako paketea da?

Ez. Beraz, hasierara joango da paketea.

1. ***PREROUTING* katea**

23. erregela aztertuko da. Betetzen al dira baldintza hauek guztiak?

* 1. Paketea edonondik dator BAI
  2. Gure IP publikoa da helburua BAI
  3. TCP paketea da BAI
  4. Helburu-ataka 80 da? EZ

Baldintza guztiak betetzen ez direnez, kate horretako hurrengo erregelara joko du paketeak, eta 24. erregela aztertuko da. Betetzen al dira baldintza hauek guztiak?

1. Paketea edonondik dator BAI
2. Gure IP publikoa da helburua BAI
3. TCP paketea da BAI
4. Helburu-ataka 22 da? BAI

Baldintza guztiak betetzen direnez, 24. erregelako ekintza gauzatuko da: DNATa (Destination NATa). Hala, 192.168.3.2 jarriko da paketearen helburu-IParen eremuan, 10.9.52.33ren ordez. Ikusi taula:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Paketearen informazioa | **Protokoloa** | **Jatorrizko IPa** | **Helburu-IPa** | **Helburu-ataka** |
| TCP | 10.9.53.201 | 192.168.3.2 | 22 |

Ondoren, paketeak aurrera jarraituko du eskeman. Bideratze-erabakia hartu beharko du orain: helburu-IPa suebakiko bertako interfazeetako IPetako bat al da? Ez. Ondorioz, *FORWARD* katera joko du paketeak.

1. ***FORWARD* katea**

14. erregelatik aurrerakoak aztertuko dira, ordenan. Ez dira betetzen 14. erregelaren eta 19. erregelaren arteko baldintza guztiak; 20. erregelakoak, ordea, bai. Horrenbestez, 20. erregelako ekintza gauzatuko da: *ACCEPT* (onartu). Ondoren, paketeak aurrera jarraituko du eskeman, eta *POSTROUTING* katera iritsiko da.

1. ***POSTROUNTIG* katea**

Ez da 25. erregela betetzen; ezta 26. erregela ere. Paketea *Netfilter* eskematik joango da.

Beraz, nahi genuen bezala, paketea onartu, eta baimendu egin da komunikazioa.

**3.3.2.3.** **PING DMZ saretik LAN sarerantz**

Demagun DMZko *Apache* zerbitzariko (192.168.3.2 IPa) terminaletik norbaitek *“*ping *192.168.2.2”* idatzi duela. Ukatu egin behar da sortu den paketea. Ikusi taula:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Paketearen informazioa | **Protokoloa** | **Jatorrizko IPa** | **Helburu-IPa** | **Helburu-ataka** |
| ICMP | 192.168.3.2 | 192.168.2.2 |  |

Hauexek dira paketeak eskeman jarraituko dituen urratsak:

1. Suebakian bertan sortutako paketea da?

Ez. Beraz, hasierara joango da paketea.

1. ***PREROUTING* katea**

23. erregela aztertuko da. Betetzen al dira baldintza hauek guztiak?

* 1. Paketea edonondik dator BAI
  2. Gure IP publikoa da helburua EZ
  3. TCP paketea da EZ
  4. Helburu-ataka 80 da? EZ

Baldintza guztiak betetzen ez direnez, kateko hurrengo erregelara joko du paketeak, eta 24. erregela aztertuko da. Betetzen al dira baldintza hauek guztiak?

1. Paketea edonondik dator BAI
2. Gure IP publikoa da helburua EZ
3. TCP paketea da EZ
4. Helburu-ataka 22 da? EZ

Baldintza guztiak betetzen ez direnez eta *PREROUTING* katean beste erregelarik ez dagoenez, paketeak aurrera egingo du eskeman. Bideratze- erabakia hartu beharko du orain: helburu-IPa (192.168.2.2) suebakiko bertako interfazeetako IPetako bat da? Ez. Ondorioz, *FORWARD* katera joko du paketeak.

1. ***FORWARD* katea**

14. erregelatik aurrerakoak aztertuko dira, ordenan. Ez da erregelarik betetzen. Adi!, 22. erregelak DMZtik edonoranzko icmp trafikoa baimentzen du, LAN sareranzkoa izan ezik. Beraz, ez dagoenez baldintza guztiak bete dituen erregelarik, ez dago ekintzarik exekutatzeko. Zer egingo du paketeak, orduan? Lehenetsitako politikak dioena zera da: *DROP* (ezabatu). Ondoren, paketeak aurrera jarraituko du eskeman, eta *POSTROUTING* katera iritsiko da.

1. ***POSTROUNTIG* katea**

Ez da 25. erregela betetzen, ezta 26. erregela ere. Paketea *Netfilter* eskematik joango da.

Beraz, nahi genuen bezala, paketea ukatu, eta debekatu egin da komunikazioa.

**3.3.2.4.** **Internetetik gure web-orrira nabigatu**

Demagun ikastetxeko LAN sareko (alegiazko Internet, guretzat) 10.9.53.201 IP protokolodun PCan norbaitek *“*<http://10.9.52.33>*”* idatzi duela nabigatzailean. Onartu egin behar sortu den paketea, eta nabigazioa baimendu. Ikusi taula:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Paketearen informazioa | **Protokoloa** | **Jatorrizko IPa** | **Helburu-IPa** | **Helburu-ataka** |
| TCP | 10.9.53.201 | 10.9.52.33 | 80 |

Hauexek dira eskeman paketeak jarraituko dituen urratsak:

1. Suebakian bertan sortutako paketea da?

Ez. Beraz, hasierara joango da paketea.

2.***PREROUTING* katea**

23. erregela aztertuko da. Betetzen al dira baldintza hauek guztiak?

* 1. Paketea edonondik dator BAI
  2. Gure IP publikoa da helburua BAI
  3. TCP paketea da BAI
  4. Helburu-ataka 80 da? BAI

Baldintza guztiak betetzen direnez, 23. erregelako ekintza gauzatuko da: DNATa (Destination NATa). Horrenbestez, 192.168.3.2 jarriko da paketearen helburu-IParen eremuan, 10.9.52.33ren ordez. Ikusi taula:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Paketearen informazioa | **Protokoloa** | **Jatorrizko IPa** | **Helburu-IPa** | **Helburu-ataka** |
| TCP | 10.9.53.201 | 192.168.3.2 | 80 | |

Ondoren, paketeak aurrera jarraituko du eskeman. Bideratze-erabakia hartu beharko du orain: helburu-IPa suebakiko bertako interfazeetako IPetako bat da? Ez. Ondorioz, *FORWARD* katera joko du paketeak.

3.***FORWARD* katea**

14. erregelatik aurrerakoak aztertuko dira, ordenan. Ez dira betetzen 14. erregelaren eta 15. erregelaren arteko baldintza guztiak; 16. erregelakoak, ordea, bai. Hortaz, 16. erregelako ekintza gauzatuko da: *ACCEPT* (onartu). Ondoren, paketeak aurrera jarraituko du eskeman, eta *POSTROUTING* katera iritsiko da.

4.***POSTROUNTING* katea**

Ez da 25. erregela betetzen, ezta 26. erregela ere. Paketea *Netfilter* eskematik joango da.

Beraz, nahi genuen bezala, paketea onartu, eta baimendu egin da komunikazioa.

**3.3.2.5.** **DNSeskaera-sare lokaletik Internetera**

Demagun LANeko PC ordenagailuaren nabigatzailean “<http://www.google.es>” idatzi dugula. PC horrek 192.168.2.3 dauka DNS zerbitzari gisa; hala, DNS zerbitzariari eskatuko dio www.google.es URLaren IP publikoa. Zerbitzari horrek ez du izen publikorik ebazten, ordea. Horregatik, “/etc/bind/named.conf.options” fitxategian *forwarders* atalean adierazitako kanpoko DNSari eskatuko dizkio. Gure kasuan, 10.9.55.1 IP protokolodun ekipoari, hots, ikastetxeko DNS zerbitzariari; Interneteko zerbitzari publikotzat hartuko dugu DNS zerbitzaria. Ikusi taula:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Paketearen informazioa | **Protokoloa** | **Jatorrizko IPa** | **Helburu-IPa** | **Helburu-ataka** |
| UDP | 192.168.2.3 | 10.9.55.1 | 53 |

Onartu egin behar da sortutako paketea, eta nabigazioa baimendu.

Hauexek dira paketeak eskeman jarraituko dituen urratsak:

1. Suebakian bertan sortutako paketea da?

Ez. Beraz, hasierara joango da paketea.

2. ***PREROUTING* katea**

23. erregela aztertuko da. Betetzen al dira baldintza hauek guztiak?

1. Paketea edonondik dator BAI
2. Gure IP publikoa da helburua EZ
3. TCP paketea da EZ
4. Helburu-ataka 80 da? EZ

Baldintza guztiak betetzen ez direnez, kate horretako hurrengo erregelara joko du paketeak, eta 24. erregela aztertuko da. Betetzen al dira baldintza hauek guztiak?

1. Paketea edonondik dator BAI
2. Gure IP publikoa da helburua EZ
3. TCP paketea da EZ
4. Helburu-ataka 22 da? EZ

Baldintza guztiak betetzen ez direnez eta *PREROUTING* katean beste erregelarik ez dagoenez, paketeak aurrera egingo du eskeman. Bideratze-erabakia hartu beharko du orain: helburu-IPa (10.9.55.1) suebakiko bertako interfazeetako IPetako bat da? Ez. Ondorioz, *FORWARD* katera joko du paketeak. paketea.

3. ***FORWARD* katea**

14. erregelatik aurrerakoak aztertuko dira, ordenan. Ez dira betetzen 14. erregelaren eta 17. erregelaren arteko baldintza guztiak; 18. erregelakoak, ordea, bai. Hortaz, 18. erregelako ekintza gauzatuko da: *ACCEPT* (onartu). Ondoren, paketeak aurrera jarraituko du eskeman, eta *POSTROUTING* katera iritsiko da.

4.***POSTROUTING* katea**

25. erregela aztertuko da. Betetzen al dira baldintza hauek guztiak?

1. Paketea 192.168.2.0/24 saretik dator BAI
2. Helburua ez da DMZko IP bat BAI

Baldintza horiek guztiak betetzen direnez, 25. erregelako ekintza gauzatuko da: SNATa (Source NATa). Hartara, 10.9.52.33 jarriko da paketearen jatorrizko IParen eremuan, 192.168.2.3ren ordez. Ikusi taula:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Paketearen informazioa | **Protokoloa** | **Jatorrizko IPa** | **Helburu-IPa** | **Helburu-ataka** |
| UDP | 10.9.52.33 | 10.9.55.1 | 53 | |

Ondoren, paketea sistematik aterako da.

Beraz, nahi genuen bezala, paketea onartu, eta baimendu egin da komunikazioa.

**3.3.2.6.Suebakitik Interneterako nabigazioa**

Demagun suebakiaren beraren nabigatzailean (Google-ren IP publikoetako bat) “<http://173.194.34.88>” idatzi dugula. Onartu egin behar da sortu den paketea, eta nabigazioa baimendu. Ikusi taula:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Paketearen informazioa | **Protokoloa** | **Jatorrizko IPa** | **Helburu-IPa** | **Helburu-ataka** |
| TCP | 10.9.52.33 | 173.194.24.88 | 80 |

Hauexek dira paketeak eskeman jarraituko dituen urratsak:

1. Suebakian bertan sortutako paketea da?

Bai. Beraz, prozesatze lokala duen paketea da, eta *OUTPUT* katera joko du.

2. ***OUTPUT* katea**

9. erregelatik aurrerakoak aztertuko dira, ordenan. Ez dira betetzen 9. erregelako eta 10. erregelako baldintza guztiak; 11. erregelakoak, ordea, bai. Hortaz, 11. erregelako ekintza gauzatuko da: *ACCEPT* (onartu). Ondoren, paketeak aurrera jarraituko du eskeman, eta *POSTROUTING* katera iritsiko da.

3. ***POSTROUNTIG* katea**

Ez da 25. erregela betetzen; ezta 26. erregela ere. Paketea *Netfilter* eskematik joango da.

Beraz, nahi genuen bezala, paketea onartu, eta baimendu egin da komunikazioa.

**3.3.2.7.Internetera nabigatuLANsaretik**

Demagun LANeko PC ordenagailuko (192.168.2.2) nabigatzailean ´´<http://173.194.34.88>´´ (Google-ren IP publikoetako bat) idatzi dugula. Onartu egin behar da sortutako paketea, eta nabigazioa baimendu. Ikusi taula:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Paketearen informazioa | **Protokoloa** | **Jatorrizko IPa** | **Helburu-IPa** | **Helburu-ataka** |
| TCP | 192.168.2.2 | 173.194.24.88 | 80 |

Hauexek dira paketeak eskeman jarraituko dituen urratsak:

1.Suebakian bertan sortutako paketea da?

Ez. Beraz, hasierara joango da paketea.

2.***PREROUTING* katea**

23. erregela aztertuko da. Betetzen al dira baldintza hauek guztiak?

1. Paketea edonondik dator BAI
2. Gure IP publikoa da helburua EZ
3. TCP paketea da BAI
4. Helburu-ataka 80 da? BAI

Baldintza guztiak betetzen ez direnez, kateko hurrengo erregelara joko du paketeak, eta 24. erregela aztertuko da. Betetzen al dira baldintza hauek guztiak?

1. Paketea edonondik dator BAI
2. Gure IP publikoa da helburua EZ
3. TCP paketea da BAI
4. Helburu-ataka 22 da? EZ

Baldintza guztiak betetzen ez direnez eta *PREROUTING* katean beste erregelarik ez dagoenez, paketeak aurrera egingo du eskeman. Bideratze-erabakia hartu beharko du orain: helburu-IPa (173.194.34.88) suebakiko bertako interfazeetako IPetako bat da? Ez. Ondorioz, *FORWARD* katera joko du paketeak.

3.***FORWARD* katea**

14. erregelatik aurrerakoak aztertuko dira, ordenan. Ez dira betetzen 14. erregelaren eta 16. erregelaren arteko baldintza guztiak; 17. erregelakoak, ordea, bai. Hortaz, 17. erregelako ekintza gauzatuko da: *ACCEPT* (onartu). Ondoren, paketeak aurrera jarraituko du eskeman, eta *POSTROUTING* katera iritsiko da.

4.***POSTROUTING* katea**

25. erregela aztertuko da. Betetzen al dira baldintza hauek guztiak?

1. Paketea 192.168.2.0/24 saretik dator BAI
2. Helburua ez da DMZko IP helbide bat BAI

Baldintza guztiak betetzen direnez, 25. erregelako ekintza gauzatuko da: SNATa (Source NATa). 10.9.52.33 jarriko da paketearen jatorrizko IParen eremuan, 192.168.2.2ren ordez. Ikusi taula:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Paketearen informazioa | **Protokoloa** | **Jatorrizko IPa** | **Helburu-IPa** | **Helburu-ataka** |
| TCP | 10.9.52.33 | 173.194.24.88 | 80 | |

Ondoren, paketea sistematik aterako da.

Beraz, nahi genuen bezala, paketea onartu, eta baimendu egin da komunikazioa.

**3.4. *Script*a hobetu**

* + 1. ***Proxy***

Litekeena da suebakiak berak *proxy* zerbitzariaren lanak ere egin behar izatea, sare lokaletik zein DMZtik kontsultatutako web-orriak baimentzeko edo ukatzeko. Horretarako, *squid* zerbitzua konfiguratu genezake, 3128 atakan jarrita entzuten.

Horretarako, 3128 atakara berbideratu beharko ditugu DMZn edo sare lokalean egindako nabigazioak Interneterantz. Honako lerro hauek erantsiko ditugu *script*ean:

iptables -t nat -A PREROUTING –s 192.168.2.0 -p tcp --dport 80 -j REDIRECT --to-port 3128

iptables -t nat -A PREROUTING –s 192.168.3.0 -p tcp --dport 80 -j REDIRECT --to-port 3128

*REDIRECT* egitean, hauxe esaten ari gatzaizkio suebakiari: 80 atakara zuzendutako pakete bat datorkionean, bere 3128 atakara zuzentzeko. Baina, nola egiten da hori?

1. Honako informazio hau aldatu behar zaio paketeari:
   1. Helburu-IPa 10.9.52.33 izango da; ez da izango kontsultatu nahi den web-orriaren IP publikoa.
   2. Helburu-ataka 3128 izango da; ez da 80 izango.

Beraz, suebakira bertara zuzendutako paketea denez, *INPUT* katera pasatuko da; *FORWARD* katera, ez. Behin *INPUT* katean iragazita, prozesatze lokala egingo da.

1. Orduan, beste pakete bat sortuko da:
   1. Kontsultatu nahi den web-orriaren IP publikoa izango da helburu-IPa.
   2. Helburu-ataka 80 izango da.

Suebakian bertan sortutako paketea denez, *OUTPUT* katera joango da prozesatze lokala egin eta gero.

Beraz, honako erregela hauek ere erantsi behar dizkiogu *script*ari:

iptables –A INPUT –i eth0 –p tcp --dport 3128 -j ACCEPT

iptables –A INPUT –i eth1 --dport 3128 -j ACCEPT

iptables –A OUTPUT –o eth2 –p tcp --dport 80 -j ACCEPT

# Bibliografia

COSTAS, Jesús: *Seguridad y Alta Disponibilidad*, Editorial Ra-Ma, Madril, 2011.

GUERRA, Ander: *Sareko Zerbitzuak*, Lanbide Ekimena, Gasteiz, 2012.

MOLINA, Francisco José: *Servicios e Red*, Editorial Ra-Ma, Madril, 2010.