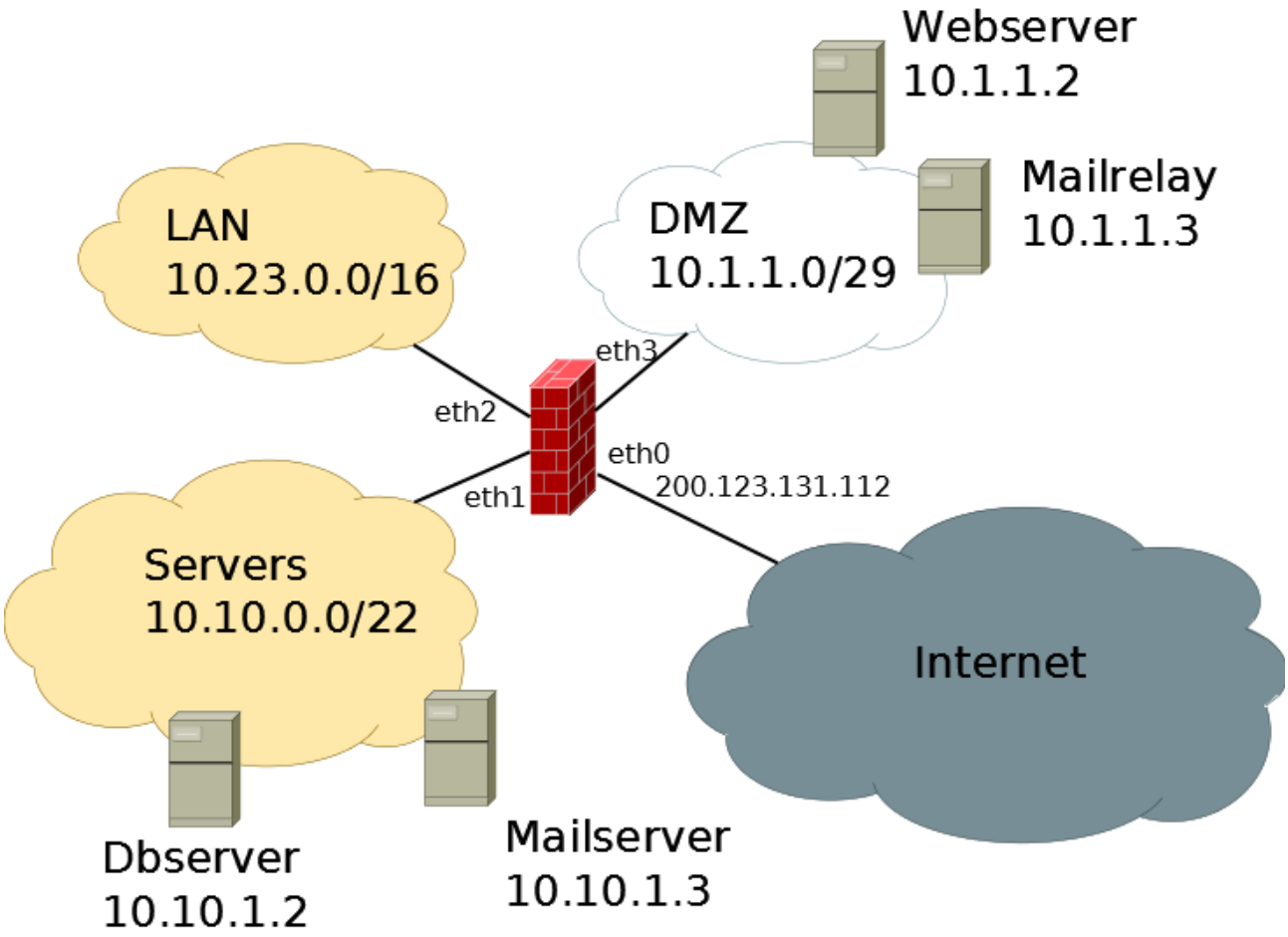
Ejercicio de Firewall –2017 – Comunicaciones - LCC

En la imagen se aprecia la red de una organización que tiene una red LAN separada de la de servidores, y una DMZ donde se ubican los equipos que tendrán presencia en Internet.Para mayor seguridad, se decidió que el servidor con las casillas de mail se encuentre en la red de servidores, sirviendo el "Mailrelay" como punto de paso de los email hacia y desde Internet. El servidor web de la DMZ ("Webserver") consulta al servidor de base de datos. El DNS maestro para la organizacion (autoritativo para el dominio y cache para los equipos internos) se encuentra en el servidor “Mailrelay”
En el servidor Dbserver también corre una aplicación web, que sólo es accesible para los equipos de la LAN.



Diseñar las reglas del firewall de tal manera de que se cumplan los siguientes enunciados.
1- Las PC de la LAN tienen acceso al correo electronico en la red de servidores (imap, imaps, pop, pop3s, smtp, smtp-ssl – tcp en todos los casos -) y a la aplicacion web de negocios en el dbserver por https. Asimismo pueden acceder al DNS de la DMZ, y a nada mas de las redes internas.
2- El servidor de mail de la red de servidores tiene acceso al dns y al puerto 465/tcp (smtps) del relay.
3- El relay tiene acceso al puerto 465/tcp del servidor de mail
4- el webserver de la dmz tiene acceso al puerto 3306/tcp (mysql) del dbserver.

5- Las pc pueden navegar libremente por internet.

6- Desde internet es posible acceder a los siguientes servicios de la DMZ: Mailrelay 53 udp y tcp (DNS) y 25 (SMTP), y a los puertos 80 y 443 del webserver, a través de la única IP pública.

7- Los servidores de la DMZ pueden consultar DNS a internet y el RELAY puede enviar correo a Internet a traves del puerto 25/tcp

8- En cuanto al firewall en si, sólo es posible ingresar desde la PC del administrador, 10.23.23.5 por ssh. Desde el firewall, solo se puede consultar dns en el servidor de la DMZ.

9- No hay más accesos que los especificados.

Solución

Creamos un script en shell que carga las reglas

```
#! /bin/sh
# Definicion de variables
F=/sbin/iptables
LAN=10.23.0.0/16
DMZ=10.1.1.0/29
WEBSRV=10.1.1.2
RELAY=10.1.1.3
MAILSRV=10.10.1.3
DBSRV=10.10.1.2
IF_LAN=eth2
IF_SRV=eth1
IF_DMZ=eth3
IF_EXT=eth0
IP_EXT=200.123.131.112
ADM_PC=10.23.23.5
# Valores por omision de las cadenas
# Deniego entrada y salida por omision.
# (no hace falta poner "-t filter" porque lo asume por omision)
$F -P INPUT DROP
$F -P OUTPUT DROP
# Enunciado 9
$F -P FORWARD DROP

######### TABLA filter #########
##### Cadenas INPUT y OUTPUT ####
# Rechazo "conexiones" inválidas y permito respuestas a conexiones
permitidas,
for i in INPUT OUTPUT ; do
$F -A $i -m state –state INVALID -j DROP
$F -A $i -m state –state RELATED,ESTABLISHED -j ACCEPT
done
# A partide de aqui, solo quedan las conexiones en estado "NEW" para las
cadenas INPUT y OUTPUT
# Enunciado 8
# Acceso SSH para el administrador. (utilizo -i para prevenir spoofing de
direcciones desde otra red)
$F -A INPUT -p tcp -i $IF_LAN -s $ADMIN_PC –dport 22 -j ACCEPT
# Como puse -P DROP, no sería necesario denegar todo el resto
explicitamente.
#$F -A INPUT -j DROP
```

```
# Consultas DNS
$F -A OUTPUT -p tcp -d $RELAY –dport 53 -j ACCEPT
$F -A OUTPUT -p udp -d $RELAY –dport 53 -j ACCEPT

# No se aceptan más paquetes en la cadena OUTPUT ( comando -P de más
arriba)

#### Cadena FORWARD ####
# Otra vez las reglas de estado. Conviene ponerlo al principio pues las
reglas que contienen ESTABLISHED y RELATED son las que más paquetes
matchearán.
$F -A FORWARD -m state –state INVALID -j DROP
$F -A FORWARD -m stat –state RELATED,ESTABLISHED -j ACCEPT


# Enunciado 1
# Nota: Los puertos se pueden poner usando la denominacion del
/etc/services ademas de numericas
$F -A FORWARD -m multiport -s $LAN -i $IF_LAN -p tcp -d $MAILSRV \
     –dports pop3,pop3s,domain,imap,imaps,smtp,smtps -j ACCEPT\
$F -A FORWARD -p udp -s $LAN -i $IF_LAN -d $RELAY –dport 53 -j ACCEPT
$F -A FORWARD -s $LAN -i $IF_LAN -p tcp -d $DBSRV --dport 443 -j ACCEPT


# el "y nada mas de las redes internas" del enunciado 1 queda cumplido
# con el -P.
# Enunciado 5 (ésto solo no alcanza, tambien hay que natear – ver abajo)
$F -A FORWARD -s $LAN -i $IF_LAN -o $IF_EXT -j ACCEPT
# Enunciado 2
# acceso a DNS por udp y tcp

$F -A FORWARD -s $MAILSRV -i $IF_SRV -p udp \
     -d $RELAY –dport 53 -j ACCEPT
$F -A FORWARD -s $MAILSRV -i $IF_SRV -m multiport -d $RELAY \
     -p tcp –dport 53,465 -j ACCEPT
# Enunciado 3
$F -A FORWARD -s $RELAY -i $IF_DMZ -p tcp -d $MAILSRV \
–dport 465 -j ACCEPT
# Enunciado 4
$F -A FORWARD -s $WEBSRV -i $IF_DMZ -p tcp -d $DBSRV \
     --dport 3306 -j ACCEPT
# Enunciado 6
# dns por udp desde el exterior
$F -A FORWARD -i $IF_EXT -p udp –dport 53 -d $RELAY -j ACCEPT
# acceso a mail y dns por tcp
$F -A FORWARD -m multiport -i $IF_EXT -p tcp –dports 53,25 \
-d $RELAY -j ACCEPT
# acceso a web
$F -A FORWARD -m multiport -i $IF_EXT -p tcp –dports 80,443 \
-d $WEBSRV -j ACCEPT

# Enunciado 7
for i in tcp udp ; do
$F -A FORWARD –i $IF_DMZ -o $IF_EXT -p $i –dport 53 -j ACCEPT
done
$F -A FORWARD -i $IF_DMZ -s $RELAY -p tcp -o $IF_EXT –dport 25 -j ACCEPT
```

```
########## TABLA nat #############
# Enunciado 6
$F -t nat -A PREROUTING -d $IP_EXT -p tcp –m multiport –dports 25,53 -j
DNAT ––to $RELAY
$F -t nat -A PREROUTING -p udp -d $IP_EXT -dport 53 -j DNAT ––to $RELAY
$F -t nat -A PREROUTING -p tcp -m multiport --dports 80,443 -j DNAT --to
$WEBSRV

# Para que se cumplan los Enunciados 5 y 7, además de permitir el acceso,
debemos natear.
#### Cadena POSTROUTING ####
# en ésta cadena no podemos usar -i ...
$F -t nat -A POSTROUTING -s $LAN -o $IF_EXT -j SNAT –to $IP_EXT
$F -t nat -A POSTROUTING -s $DMZ -o $IF_EXT -j SNAT –to $IP_EXT
```