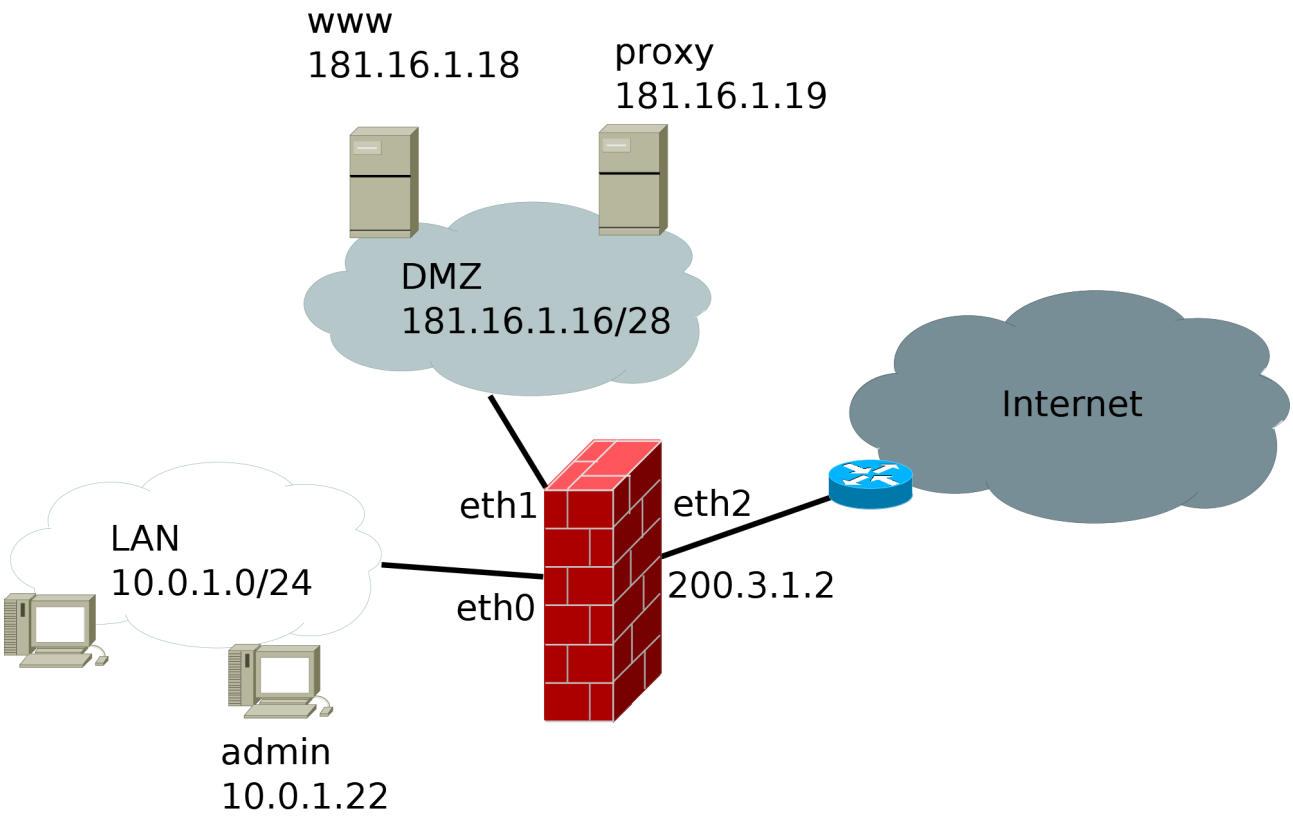
Comunicaciones – LCC

Ejercicio de Firewall 20181128



En la red de la figura, hay 2 servidores en la DMZ que tienen los siguientes servicios habilitados:

- Servidor “www”: Web (http y https), DNS y ssh
- Servidor “Proxy”: Proxy Web (puerto 3128), DNS, y ssh

El firewall tiene habilitado el servicio ssh en su interfaz LAN (eth0).

Diseñar las reglas de firewall/nat para que se cumplan los siguientes requerimientos:

1. La PC de administración es el único lugar desde donde se puede acceder al servicio ssh de los servidores y el firewall.
2. Las PC de la LAN pueden acceder a los servicios restantes de los servidores de la DMZ.
3. Las PC pueden acceder a Internet en forma directa, exceptuando la navegación web que debe realizarse exclusivamente a través del proxy. Para los servicios que no pasan por el proxy, es necesario realizar NAT, pues tienen direcciones privadas.
4. Los servidores de la DMZ solo pueden acceder a servicios DNS y web en Internet, y no tienen acceso alguno a la LAN.
5. Desde Internet, solo se puede acceder a los servicios DNS (ambos servers) y Web del “www”.
6. El firewall solo tiene acceso al proxy (para actualizaciones).

Solución

```
#! /bin/sh
# Ejercicio firewall/NAT – jkohan 20181128

case $1 in

start)

# Primero definimos algunas variables para que se lea más fácil
LAN=10.0.1.0/24
ADMIN=10.0.1.22
WWW=181.16.1.18
ILAN=eth0
IDMZ=eth1
INET=eth2
PROXY=181.16.1.19
I=/sbin/iptables

# Limpiamos reglas anteriores
$I -F -t nat
$I -F -t filter


# Tabla Filter
# Reglas de INPUT

# Descartamos cosas raras
$I -A INPUT -m state --state INVALID -j DROP

# Permitimos conexiones ya establecidas o relacionadas.
$I -A INPUT -m state --state RELATED, ESTABLISHED -j ACCEPT

# Regla 1: Se puede acceder por SSH desde la PC de administración
# (Especificamos interfaz de entrada para mejor protección ante spoofing)
$I -A INPUT -i $ILAN -p tcp -s $ADMIN --dport 22 -j ACCEPT

# Regla 1: No se permiten más accesos que los habilitados
# expresamente (se suele poner al principio, lo ponemos acá por legibilidad)
$I -P INPUT DROP

# Reglas de OUTPUT

# Si no tuviéramos restricciones de salida, no harían falta las reglas de
# estado tampoco.
$I -A OUTPUT -m state --state INVALID -j DROP
# La siguiente regla es necesaria para que funcione el ssh desde ADMIN
$I -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# Regla 6
$I -A OUTPUT -p tcp -d $PROXY --dport 3128 -j ACCEPT
$I -P OUTPUT DROP

# Reglas de FORWARD
$I -A FORWARD -m state --state INVALID -j DROP
$I -A FORWARD -m state --state RELATED, ESTABLISHED -j ACCEPT

# Accesos a la DMZ
# Regla 1 (acceso a servidores)
$I -A FORWARD -m iprange -s $ADMIN -i $ILAN --dst-range $WWW-$PROXY \
      -p tcp --dport 22 -j ACCEPT
```

```
# Regla 2 (acceso a servidores, resto de pcs)
# DNS por udp
$I -A FORWARD -m iprange -s $LAN -i $ILAN \
      --dst-range $WWW-$PROXY -p udp --dport 53 -j ACCEPT

# Puertos TCP a "www"
$I -A FORWARD -s $LAN -i $ILAN -m multiport -d $WWW --dports 53,80,443 \
      -j ACCEPT

# Puertos TCP a "proxy"
$I -A FORWARD -s $LAN -i $ILAN -m multiport -d $PROXY --dports 53,3128 \
       -j ACCEPT

# No se permiten mas accesos que los anteriores LAN->DMZ
# (REJECT en lugar de DROP para mejor diagnostico en la LAN)
$I -A FORWARD -i $ILAN -o $IDMZ -j REJECT

# Acceso de la LAN a Internet
# Regla 3.
# Ya no quedan mas destinos posibles que Internet y eso me permite simplificar.
$I -A FORWARD -i $ILAN -p tcp --dport 80,443 -j REJECT
$I -A FORWARD -i $ILAN -s $LAN -j ACCEPT

# Accesos a la DMZ desde el exterior
# Regla 5 (se podría combinar con la 2 y así optimizar?)
$I -A FORWARD -m iprange -p udp --dst-range $WWW-$PROXY --dport 53 -j ACCEPT
$I -A FORWARD -m iprange -p tcp --dst-range $WWW-$PROXY --dport 53 -j ACCEPT
$I -A FORWARD -m multiport -p tcp -d $WWW --dport 80,443 -j ACCEPT
# No mas accesos a la DMZ

# Accesos de la DMZ->*
# Regla 4
$I -A FORWARD -m iprange -i $IDMZ -p udp --src-range $WWW-$PROXY \
      -o $INET --dport 53 -j ACCEPT
$I -A FORWARD -m multiport -m iprange -i $IDMZ -p tcp \
      -o $INET --src-range $WWW-$PROXY --dports 53,443,80 -j ACCEPT

# No mas accesos (recordar, puede ir en cualquier lugar)
$I -P FORWARD DROP


# Tabla NAT
# Nateamos lo que viene de la DMZ y va a Internet
# (no se puede usar -i !)
$I -t nat -A POSTROUTING -o $INET -s $LAN -j SNAT --to 200.3.1.2


;;

stop)

$I -P INPUT ACCEPT
$I -P FORWARD DROP
$I -P OUTPUT ACCEPT
$I -F -t nat
$I -F

;;

*)
      echo "Sintaxis: $0 <start|stop>"
      exit 1
;;
```

```
esac
```