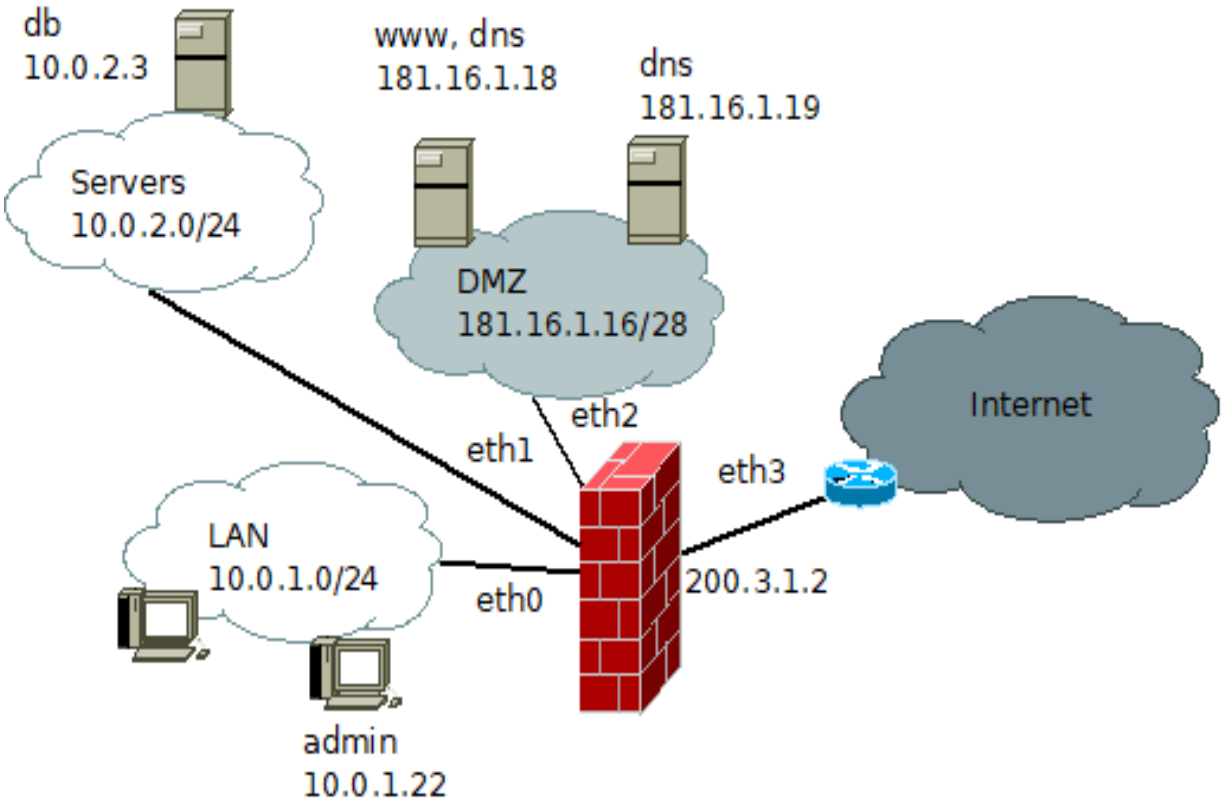
**Comunicaciones LCC - Ejercicio de Firewall  20201216**

(Última revisión: 20211115)




En la red de la figura, las PC de la LAN tienen libre acceso a cualquier lado menos a la red de servidores (de la cual solo se toma en cuenta el servidor de base de datos).  Para salir a Internet, deben ser nateadas, no asi a la DMZ donde además tienen acceso total.

Desde el exterior solo se puede tener acceso limitado a la DMZ: al dns (puertos tcp y udp 53 de ambos servidores) y puertos 80 y 443 del servidor Web. Desde la DMZ solo es posible hacer consultas DNS hacia el exterior y al al puerto 3306 del servidor de base de datos de la red de Servers. La red de servers no tiene ningún tipo de acceso (solo para responder al servidor web).

Realizar reglas del firewall. No es neceario escribir las reglas de INPUT para el firewall.

**(Una posible) Solución**
No tener en cuenta correccion ni sintaxis perfecta del script en sh, es admisible solo seccion start.

```
#! /bin/sh
LAN=10.0.1.0/24
I=/sbin/iptables

case $1 in
           start)

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

# Pcs de la LAN: NO tienen acceso a red de servidores, sí al resto del
universo.
$I -A FORWARD -i eth0 -o eth1 -j REJECT
$I -A FORWARD -i eth0 -s $LAN -j ACCEPT

# Hacia DMZ
# Permito acceso dns hacia toda la DMZ (supongo solo tengo esos dos
servers)
$I -A FORWARD -o eth2 -p udp --dport 53 -j ACCEPT
$I -A FORWARD -o eth2 -p tcp --dport 53 -j ACCEPT


# Permito accesos web al servidor correspondiente
$I -A FORWARD -m multiport -o eth2 -d 181.16.1.18 -p tcp \
     --dports 80,443 -j ACCEPT

# Desde DMZ, solo DNS saliente y accesos al db server
$I -A FORWARD -i eth2 -o eth3 -p udp --dport 53 -j ACCEPT
$I -A FORWARD -i eth2 -o eth3 -p tcp --dport 53 -j ACCEPT
$I -A FORWARD -i eth2 -o eth1 -d 10.0.2.3 -p tcp –dports 3306 -j ACCEPT

# No permito nada más.
$I -A FORWARD -j DROP

# Reglas de NAT

$I -t nat -A POSTROUTING -s $LAN -o eth3 -j SNAT –to 200.3.1.2
;;

stop)

     $I -F FORWARD
     $I -t nat -F POSTROUTING
;;

*)

echo Error de Sintaxis
exit 1
;;
esac
```