Guía Laboratorio

1.- Se tiene un servidor conectada a Internet y se requiere protegerla con un FW, este último posee servicios web, MySql y FTP

Aplicación de políticas por defecto para INPUT, OUPUT, FORWARD

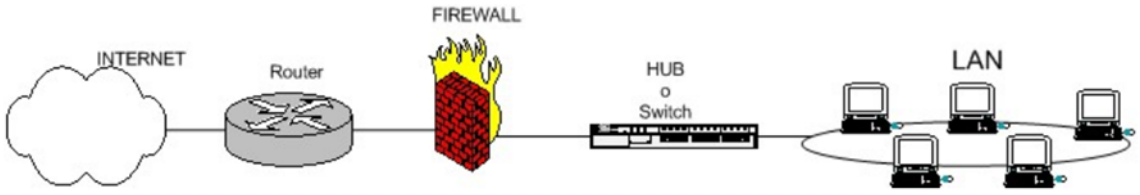
```
echo −n Aplicando Reglas de Firewall...
## FLUSH de reglas
iptables −F
iptables −X
iptables −Z
iptables −t nat −F

## Se establece la política por defecto (aceptamos todo)
iptables −P INPUT ACCEPT
iptables −P OUTPUT ACCEPT
iptables −P FORWARD ACCEPT
iptables −t nat −P PREROUTING ACCEPT
iptables −t nat −P POSTROUTING ACCEPT

# A nuestra IP le damos todos los permisos
# Al DBA le dejamos entrar al mysql para su administración
# A un operador le habilitamos FTP
# El puerto 80 de www debe estar abierto, es un servidor web.
```

¿Una vez establecido los filtros anteriores, que filtros cree ud que faltan para aumentar la seguridad?

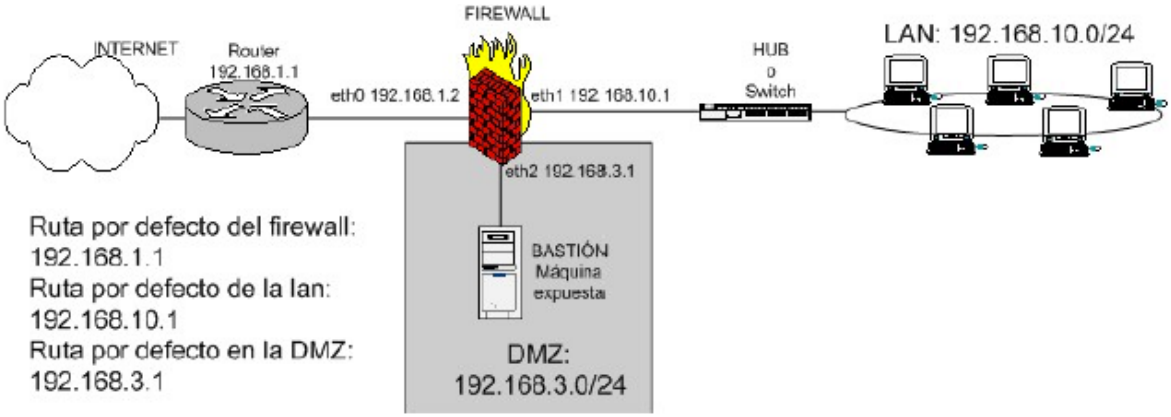
2.- Se debe configurar un FW para dar acceso a la red LAN



Se debe establecer una regla de NAT, en este caso se debe establecer un doble NAT, uno entre el router y el FW y otro entre este último y la red LAN. La LAN debe tener acceso a Internet, tanto a sitios hhtp como https, consulten a los DNS. Además, por razones presupuestarías el FW tendra servicios SMTP, pop3, y un PPTP. Por otro lado, se requiere compartir algún servicio pero de un servidor que se encuentra dentro de la red local, un servidor web, además se debe permitir la gestión remota por terminal server (telnet) para esta máquina por una externa.

¿cuáles son los problemas de este esquema?

3.- En el caso anterior, qué pasa si hackean el servidor web de la red local? Claramente no es la mejor opción, para evitarlo se debe pensar en un esquema con DMZ, como el siguiente:



En este caso el firewall debe permitir:
Acceso de la red local a internet.
Acceso público al puerto tcp/80 y tcp/443 del servidor de la DMZ
Acceso del servidor de la DMZ a una BBDD de la LAN
Obviamente bloquear el resto de acceso de la DMZ hacia la LAN.

¿Qué tipo de reglas son las que hay que usar para filtrar el tráfico entre la DMZ y la LAN?