Pauta guía de laboratorio

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

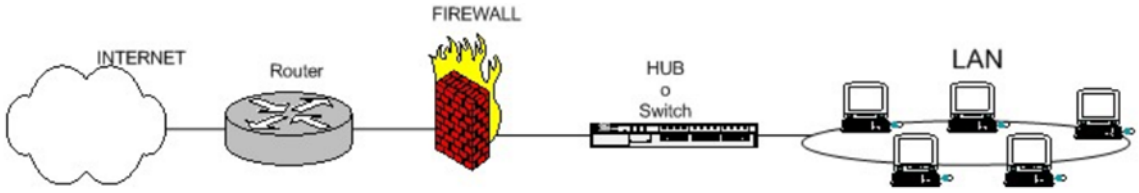
```
echo −n Aplicando Reglas de Firewall...
## FLUSH de reglas
iptables −F
iptables −X
iptables −Z
iptables −t nat −F

## Establecemos política por defecto (aceptamos todo)
## Establecemos politica por defecto
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
iptables −A INPUT −s 195.65.34.234 −j ACCEPT
# Al DBA le dejamos entrar al mysql para su administración
iptables −A INPUT −s 231.45.134.23 −p tcp −−dport 3306 −j ACCEPT
# A un operador le habilitamos FTP
iptables −A INPUT −s 80.37.45.194 −p tcp −dport 20:21 −j ACCEPT
# El puerto 80 de www debe estar abierto, es un servidor web.
iptables −A INPUT −p tcp −−dport 80 −j ACCEPT
# Cerramos al resto
iptables −A INPUT −p tcp −−dport 1:1024 −j DROP
iptables −A INPUT −p udp −−dport 1:1024 −j DROP
# Cerramos otros puertos que estan abiertos
iptables −A INPUT −p tcp −−dport 3306 −j DROP
```

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

Se deben filtrar también los protocolos UDP e ICMP. Es altamente probable que se algún sistema tiene abierto algún puerto UDP abierto y eso es tan peligroso como dejar abierto el SNMP.

Imaginemos que hemos dado un repaso a nuestro sistema y tenemos mejor identificados los puertos tcp y udp abiertos, por lo tanto se cierran, pero para aumentar la seguridad se deben cerrar también el rango de puertos reservados del 1 al 1024, tanto para tcp como udp.

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

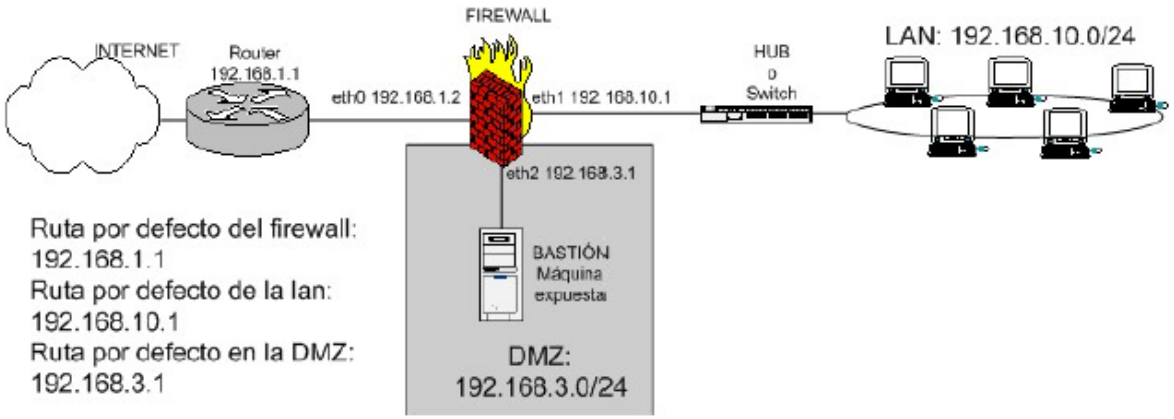


Se debe establecer una regla de NAT, en este caso se debe establecer un doble NAT, uno entre el router y el FW y otro entre este último y la red LAN. La LAN debe tener acceso a Internet, tanto a sitios hhtp como https, consulten a los DNS. Además, por razones presupuestarías el FW tendra servicios SMTP, pop3, y un PPTP. Ahora queremos compartir algún servicio pero de un servidor que tenemos dentro de la red local, por ejemplo el IIS de un servidor windows, y además permitir la gestión remota por terminal server para esta máquina para una externa. En este caso lo que hay que hacer es un redirección de puerto.

```
# Al firewall tenemos acceso desde la red local
iptables −A INPUT −s 192.168.10.0/24 −i eth1 −j ACCEPT

## REDIRECCIONES
# Todo lo que venga por el exterior y vaya al puerto 80 lo redirigimos
# a una maquina interna
iptables −t nat −A PREROUTING −i eth0 −p tcp −−dport 80 −j DNAT −−to 192.168.10.12:80
# Los accesos de un ip determinada a Terminal server se redirigen e esa
# maquina
iptables −t nat −A PREROUTING −s 221.23.124.181 −i eth0 −p tcp −−dport 3389 −j DNAT −−to
192.168.10.12:3389
## Abrimos el acceso a puertos de correo
# Abrimos el puerto 25, hay que configurar bien el relay del servidor SMTP
iptables −A INPUT −s 0.0.0.0/0 −p tcp −−dport 25 −j ACCEPT
# Abrimos el pop3
iptables −A INPUT −s 0.0.0.0/0 −p tcp −−dport 110 −j ACCEPT
# Y abrimos el puerto pptpd para la ip del adsl de casa del jefe
iptables −A INPUT −s 211.45.176.24 −p tcp −−dport 1723 −j ACCEPT

# Aceptamos que vayan a puertos 80
iptables −A FORWARD −s 192.168.10.0/24 −i eth1 −p tcp −−dport 80 −j ACCEPT
# Aceptamos que vayan a puertos https
iptables −A FORWARD −s 192.168.10.0/24 −i eth1 −p tcp −−dport 443 −j ACCEPT
# Aceptamos que consulten los DNS
iptables −A FORWARD −s 192.168.10.0/24 −i eth1 −p tcp −−dport 53 −j ACCEPT
iptables −A FORWARD −s 192.168.10.0/24 −i eth1 −p udp −−dport 53 −j ACCEPT
# Y denegamos el resto. Si se necesita alguno, ya avisaran
iptables −A FORWARD −s 192.168.10.0/24 −i eth1 −j DROP

# # Ahora hacemos enmascaramiento de la red local y activamos el BIT DE FORWARDING
iptables −t nat −A POSTROUTING −s 192.168.10.0/24 −o eth0 −j MASQUERADE
# Con esto permitimos hacer forward de paquetes en el firewall es decir que otras máquinas
puedan salir a través del firewall.
## Y ahora cerramos los accesos indeseados del exterior:
# Nota: 0.0.0.0/0 significa: cualquier red
# Cerramos el rango de puerto bien conocido
iptables −A INPUT −s 0.0.0.0/0 −p tcp −dport 1:1024 −j DROP
iptables −A INPUT −s 0.0.0.0/0 −p udp −dport 1:1024 −j DROP
```

Y cerramos el puerto del servicio PPTPD, solo abierto para el jefe.
iptables −A INPUT −s 0.0.0.0/0 −i eth0 −p tcp −−dport 1723 −j DROP

En esta última configuración las redirecciones y los servicios de correo funcionando en el firewall se torna bastante insegura. ¿Qué ocurre si hackean el servidor web de la red local? El firewall no sirve de mucho, lo poco que podría hacer una vez se ha ingresado en la red local es evitar escaneos hacia el exterior desde la máquina atacada, para esto último el firewall debería tener una buena configuración con denegación por defecto. Si necesitamos un servidor web, lo más recomendado armar un equipo con 2 tarjetas de red y crear una DMZ.



En este tipo de firewall hay que 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? Solo pueden ser las FORWARD, ya que estamos filtrando entre distintas redes, no son paquetes destinados al propio firewall.
FLUSH de reglas
iptables −F
iptables −X
iptables −Z
iptables −t nat −F
Establecemos politica por defecto
iptables −P INPUT ACCEPT
iptables −P OUTPUT ACCEPT
iptables −P FORWARD ACCEPT
iptables −t nat −P PREROUTING ACCEPT
iptables −t nat −P POSTROUTING ACCEPT
Empezamos a filtrar
Nota: eth0 es el interfaz conectado al router y eth1 a la LAN
Todo lo que venga por el exterior y vaya al puerto 80 lo redirigimos
a una maquina interna
iptables −t nat −A PREROUTING −i eth0 −p tcp −−dport 80 −j DNAT −−to 192.168.3.2:80
Los accesos de un ip determinada HTTPS se redirigen a esa máquina
iptables −t nat −A PREROUTING −i eth0 −p tcp −−dport 443 −j DNAT −−to 192.168.3.2:443
El localhost se deja (por ejemplo conexiones locales a mysql)
iptables −A INPUT −i lo −j ACCEPT
Al firewall tenemos acceso desde la red local
iptables −A INPUT −s 192.168.10.0/24 −i eth1 −j ACCEPT

Se realiza el enmascaramiento de la red local y de la DMZ para que puedan salir haca fuera y activamos el BIT DE FORWARDING
iptables −t nat −A POSTROUTING −s 192.168.10.0/24 −o eth0 −j MASQUERADE
iptables −t nat −A POSTROUTING −s 192.168.3.0/24 −o eth0 −j MASQUERADE
Con esto permitimos hacer forward de paquetes en el firewall, o sea que otras máquinas puedan salir a través del firewall.
Permitimos el paso de la DMZ a una BBDD de la LAN:
iptables −A FORWARD −s 192.168.3.2 −d 192.168.10.5 −p tcp −−dport 5432 −j ACCEPT
iptables −A FORWARD −s 192.168.10.5 −d 192.168.3.2 −p tcp −−sport 5432 −j ACCEPT
permitimos abrir el Terminal server de la DMZ desde la LAN
iptables −A FORWARD −s 192.168.10.0/24 −d 192.168.3.2 −p tcp −−sport 1024:65535 −−dport 3389 −j ACCEPT

Se debe hacer en uno y otro sentido …
iptables −A FORWARD −s 192.168.3.2 −d 192.168.10.0/24 −p tcp −−sport 3389 −−dport 1024:65535 −j ACCEPT
luego:
Cerramos el acceso de la DMZ a la LAN
iptables −A FORWARD −s 192.168.3.0/24 −d 192.168.10.0/24 −j DROP
Cerramos el acceso de la DMZ al propio firewall
iptables −A INPUT −s 192.168.3.0/24 −i eth2 −j DROP
Y ahora cerramos los accesos indeseados del exterior:
Nota: 0.0.0.0/0 significa: cualquier red
Cerramos el rango de puerto bien conocido
iptables −A INPUT −s 0.0.0.0/0 −p tcp −dport 1:1024 −j DROP
iptables −A INPUT −s 0.0.0.0/0 −p udp −dport 1:1024 −j DROP
Cerramos un puerto de gestión: webmin
iptables −A INPUT −s 0.0.0.0/0 −p tcp −dport 10000 −j DROP

Si las máquinas de la DMZ tienen una ip pública hay que tener muchísimo cuidado de no permitir el FORWARD por defecto. Si en la DMZ hay ip pública NO ES NECESARIO HACER REDIRECCIONES de puerto, sino que basta con rutar los paquetes para llegar hasta la DMZ.