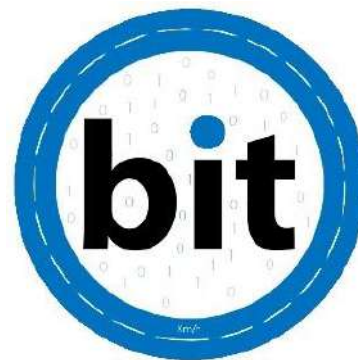


Fundamentación del Firewall y seguridad



Tercera entrega 1/11/2019

Ruta en GitLab: /Actividades/Taller03020/

Firewall:

Nuestra empresa tiene 2 firewalls con diferentes políticas, uno está ubicado entre la conexión del Router principal y el Switch principal, el cual es permisivo y va a controlar que entren y salgan del firewall y a la red interna todos los paquetes menos los que vengan por conexión de tipo FTP (puertos 20/21) y por SSH (22 o para el servidor 20022) excepto en el caso de los programadores, los cuales pueden salir de la red por SSH y pueden entrar paquetes por SSH que tengan una conexión previa establecida y tengan como destino la red de los programadores. También se encarga de redireccionar todos los paquetes que vengan por los puertos 80 y 443 hacia el servidor HTTP en la DMZ.

El otro firewall se ubica entre la conexión del Switch principal y el Switch de la sala de servidores, el cual es restrictivo y se encarga de bloquear todas las conexiones menos las realizadas por el puerto de Informix (9088) y las conexiones SSH (1112) realizadas por la red de los programadores.

REGLAS DEL FIREWALL PERMISIVO

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
```

##Nota: eth0 es la interfaz de red conectada al router

Con esto permitimos hacer forward de paquetes en el firewall, o sea
que otras máquinas puedan salir a traves del firewall.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

solo los programadores puedan salir por ssh

```
iptables -A FORWARD -s 192.168.14.0/26 -dport 22 -m state --state NEW, ESTABLISHED, RELATED -j ACCEPT
```

```
# solo permito entrar paquetes ssh si hay una conexion establecida y va hacia la red de los prog
iptables -A FORWARD -d 192.168.14.0/26 -dport 22 -m state --state ESTABLISHED, RELATED -j ACCEPT

# no puede entrar al firewall todo lo que venga por ssh (22)
iptables -A INPUT -p tcp -dport 22 -j DROP

# no puede salir del firewall todo lo que venga por ssh (22)
iptables -A OUTPUT -p tcp -dport 22 -j DROP

# no puede entrar a la red todo lo que venga por ssh (22)
iptables -A FORWARD -p tcp -dport 22 -j DROP

# no puede entrar al firewall todo lo que venga por ftp (20/21)
iptables -A INPUT -p tcp --dport 20:21 -j DROP

# no puede salir del firewall todo lo que venga por ftp (20/21)
iptables -A OUTPUT -p tcp --dport 20:21 -j DROP

# no puede entrar a la red todo lo que venga por ftp (20/21)
iptables -A FORWARD -p tcp --dport 20:21 -j DROP

# Todo lo que venga por el exterior y por el puerto 80 lo redirecciono al server http
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.1.200:80

# Todo lo que venga por el exterior y por el puerto 443 lo redirecciono al server http
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to 192.168.1.200:443
```

REGLAS DEL FIREWALL RESTRICTIVO

```
## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

## Establecemos politica por defecto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING DROP
iptables -t nat -P POSTROUTING DROP

# puede entrar a la red todo lo que venga por Informix (9088)
iptables -A FORWARD -p tcp -dport 9088 -j ACCEPT

# solo los prog pueden conectarse al servidor por ssh (1112)
iptables -A FORWARD -s 192.168.14.0/26 -p tcp -dport 20022 -j ACCEPT
```

```
# solo pueden salir paquetes del firewall por ssh si hay conexion establecida con los
prog
iptables -A FORWARD -d 192.168.14.0/26 -dport 1112 -m state --state ESTABLISHED, RELATED
-j ACCEPT
```

```
# Permitimos pasar toda conexcion de git que origine dl servidor (192.168.1.100)
iptables -A FORWARD -s 192.168.1.100 -dport 9418 -j ACCEPT
```

```
# solo permitimos entrar los paquetes git si ya había una conexión establecida
anteriormente
iptables -A FORWARD -d 192.168.1.100 -dport 9418 -m state --state ESTABLISHED, RELATED -j
ACCEPT
```

```
Permitimos pasar toda conexión de DNS utilizara por git. Esta debe originar del servidor
(192.168.1.100)
```

```
iptables -A FORWARD -s 192.168.1.100 -dport 53 -j ACCEPT
```

```
# solo permitimos entrar los paquetes DNS si ya había una conexión establecida
anteriormente
```

```
iptables -A FORWARD -d 192.168.1.100 -dport 53 -m state --state ESTABLISHED, RELATED -j
ACCEPT
```