FIREWALL ENTRE REDES

Victor Martinez Martinez

PRIMER PASO:

EQUIPO ROUTER

Crearemos un equipo, en mi caso un ubuntu server que actuara de router entre la red externa y a subred de la empresa

LIMPIANDO LAS IPTABLES:

```
iptables -F
iptables -t nat -F
```

HACER QUE TODAS LAS NORMAS ESTEN EN DROP:

```
iptables -p INPUT DROP
iptables -p OUTPUT DROP
iptables -p FORWARD DROP
```

PERMITIR TRAFICO DE RETORNO Y CONEXIONES ESTABLECIDAS:

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

ENRUTAMIENDO DE LA RED:

```
iptables -t nat -A POSTROUTING -s 192.168.222.0/24 -o enp0s3 -j MASQUERADE
```

SEGUNDO PASO:

Una vez limpiadas las iptables y habiendo hecho la configuracion inicial de estas editaremos el siguiente archivo: **/etc/sysctl.conf** y descomentaremos la siguiente linea:

```
net.ipv4.ip_forward=1
```

TERCER PASO:

Todos los equipos de la LAN deben poder realizar lo siguiente (únicamente, el resto debe estar denegado):

CONSULTAR PAGINAS WEB: Para el puerto **80**:

```
iptables -A FORWARD -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp --sport 80 -j ACCEPT
```

Para el puerto **443**:

```
iptables -A FORWARD -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -p tcp --sport 443 -j ACCEPT
```

Para permitir los **dns**:

```
iptables -A FORWARD -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -p udp --sport 53 -j ACCEPT
iptables -A FORWARD -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -p udp --sport 53 -j ACCEPT
```

Utlizar el correo electronico (POP3 y IMAP): Para POP3 y TLS POP3:

```
sudo iptables -A OUTPUT -p tcp --dport 110 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --dport 995 -j ACCEPT

sudo iptables -A FORWARD -p tcp --dport 110 -d *.*.*.* -j ACCEPT
sudo iptables -A FORWARD -p tcp --dport 995 -d *.*.*.* -j ACCEPT
```

Para IMAP y TLS IMAP:

```
sudo iptables -A OUTPUT -p tcp --dport 143 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --dport 993 -j ACCEPT

sudo iptables -A FORWARD -p tcp --dport 143 -d *.*.*.* -j ACCEPT
sudo iptables -A FORWARD -p tcp --dport 993 -d *.*.*.* -j ACCEPT
```

REALIZAR PINGS:

```

```

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

iptables -A FORWARD -p icmp --icmp-type echo-request -j ACCEPT
iptables -A FORWARD -p icmp --icmp-type echo-reply -j ACCEPT
```

CONSULTAR SERVIDORES DE TIEMPO NTP:

```
iptables -A OUTPUT -p udp --dport 123 -j ACCEPT
iptables -A FORWARD -p udp --dport 123 -d 130.206.3.166 -j ACCEPT
```

TERCER PASO:

El equipo interno del administrador debe ser el único que pueda conectarse al equipo que contiene el firewall. Se conectará por SSH.

```
iptables -A INPUT -p tcp --dport 22 -s 192.168.222.99 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -s 192.168.222.99 -j ACCEPT
```

CUARTO PASO:

El administrador (192.168.2.254) de la red debe poder acceder desde su casa por SSH al router, a su equipo dentro de la LAN y a los 3 servidores

ROUTER:

```
        iptables -A INPUT -p tcp --dport 22 -s 192.168.2.254 -j ACCEPT
        iptables -A OUTPUT -p tcp --dport 22 -s 192.168.2.254 -j ACCEPT
```

RED INTERNA:

ADMINISTRADOR:

```
iptables -A INPUT -p tcp --dport 22 -s 192.168.222.99 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -d 192.168.222.99 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 2222 -j DNAT --to-destination
192.168.222.99:22
```

MARIADB:

```
iptables -A INPUT -p tcp --dport 22 -s 192.168.222.200 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -d 192.168.222.200 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 2233 -j DNAT --to-destination
192.168.222.200:22
```

APACHE:

```
iptables -A INPUT -p tcp --dport 22 -s 192.168.222.88 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -d 192.168.222.88 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 2244 -j DNAT --to-destination
192.168.222.88:22
```

FTP:

```
iptables -A INPUT -p tcp --dport 22 -s 192.168.222.199 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -d 192.168.222.199 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 2255 -j DNAT --to-destination
192.168.222.254:22
```

QUINTO PASO:

El servidor web y el servidor ftp deben estar accesible desde cualquier equipo del exterior

SERVIDOR APACHE:

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination
192.168.222.88:80
iptables -t nat -A PREROUTING -p tcp --dport 443 -j DNAT --to-destination
192.168.222.88:443
iptables -A FORWARD -p tcp --dport 80 -d 192.168.222.88 -j ACCEPT
iptables -A FORWARD -p tcp --dport 443 -d 192.168.222.88 -j ACCEPT
```

SERVIDOR FTP:

```
iptables -t nat -A PREROUTING -p tcp --dport 20 -j DNAT --to-destination
192.168.222.199:20
iptables -t nat -A PREROUTING -p tcp --dport 21 -j DNAT --to-destination
192.168.222.199:21
iptables -A FORWARD -p tcp --dport 20 -d 192.168.222.199:20 -j ACCEPT
iptables -A FORWARD -p tcp --dport 21 -d 192.168.222.199:21 -j ACCEPT
```

SEXTO PASO:

El servidor web debe poder realizar consultas al servidor que tiene la base de datos.

No hay que hacer nada porque el servidor apache (web) y el servidor de mariadb(base de datos) ya estan en la misma red y se pueden comunicar sin ninguna necesidad de reglas de iptables

---

SEPTIMO PASO:

Si todas las normas fueran de tipo ACCEPT lo unico que habria que cambiar seria al principio, cuando hemos hecho iptables -F, despues de eso hacer:

```
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
```