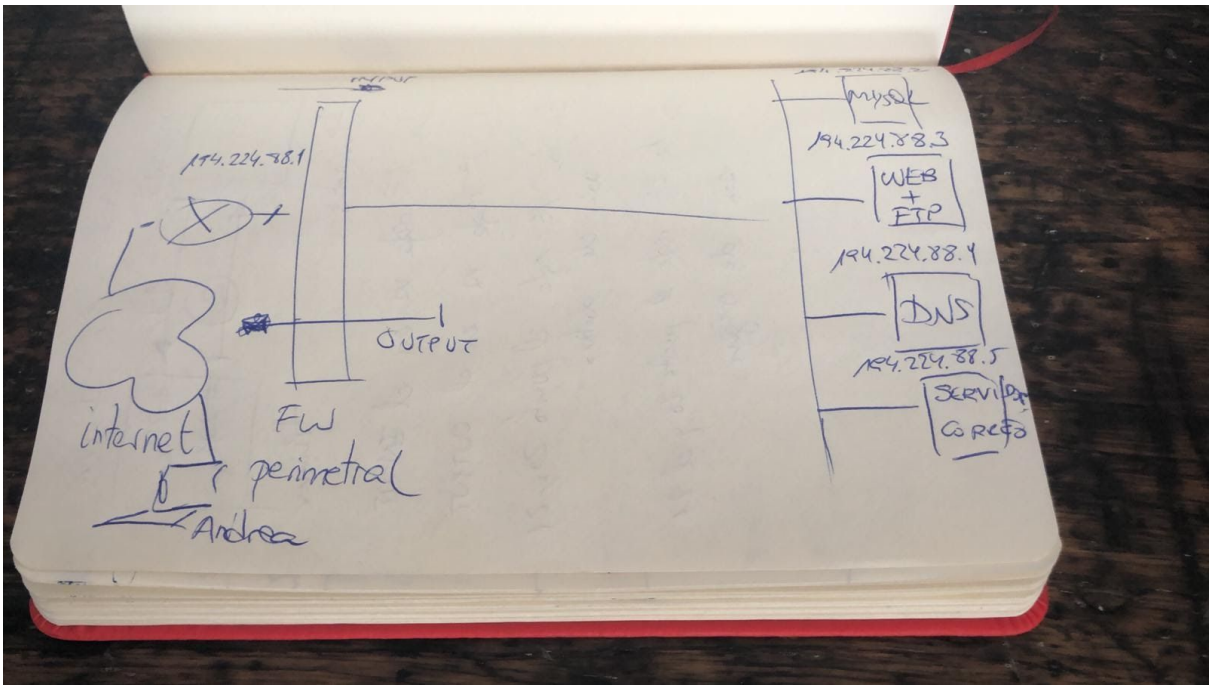
IPTABLES

By Kessusa

Vamos a configurar un firewall perimetral para la red de un hotel que tiene el siguiente esquema de red.



Vamos a configurar el input y el output de cada servicio,Andrea para la gestión a distancia tiene una VPN en el router y tiene la Ip fija dentro de la red 194.224.88.254.
IP Andrea 194.224.88.254 fija en la red.
También podemos contratar una ip fija con nuestra operadora directamente.

En primer lugar negamos todo el tráfico con las siguientes tres reglas.

iptables -A INPUT -P DROP
iptables -A OUTPUT -P DROP
iptables -A FORWARD -P DROP

Después vamos a crear las reglas para cada servicio recordando que tenemos que colocar las reglas encima de las tres anteriores para que puedan ejecutarse si no se hará caso a la más restrictiva y no funcionará.

Gestión desde el exterior para Andre por ssh -puerto 22,tendremos en todos los servidores instalado el servidor ssh para poder gestionarlos en remoto.

iptables -A INPUT -s 194.224.88.254 -p tcp --dport 22 -j ACCEPT
ip tables -A OUTPUT -d 194.224.88.254 -p tcp --sport 22 -j ACCEPT

MySql 194.224.88.2 no ponemos ninguna regla ya quewe no vamos a necesitar que nadie entre a la base de datos por el exterior y si hiciera falta andrea entraría por ssh y la gestionaría desde local.

FTP

iptables −A INPUT −s 194.224.88.3 −p tcp −−dport 20:21 −j ACCEPT
iptables −A OUTPUT −d 194.224.88.3 −p tcp −−sport 20:21 −j ACCEPT

Web para todo el mundo.

Para protocolo cifrado

iptables −A INPUT -d 194.224.88.3 −p tcp −−dport 443 −j ACCEPT
iptables −A OUTPUT -s 194.224.88.3 −p tcp −−sport 443 −j ACCEPT

En caso de tener el servidor sin usar http in cifrar.

iptables −A INPUT -d 194.224.88.3 -p tcp −−dport 80 −j ACCEPT
iptables −A OUTPUT -s 194.224.88.3 −p tcp −−sport 80 −j ACCEPT

Servidor DNS para que todo el mundo pueda acceder desde internet a nuestro servidor,recordamos que DNS usa tanto tcp como udp en el puerto 53 para resolver las peticiones de nombre.
Pero recordamos que un servidor DNS cuando no encuentra la solución en su registro porque no es autorizado para una zona , hace una consulta a otros servidores y debemos tenerlo en cuenta a la hora de configurar el firewall para que también permita ese tipo de tráfico.

iptables −A INPUT -d 194.224.88.4 −p tcp −−dport 53 −j ACCEPT
iptables −A INPUT -d 194.224.88.4 −p udp −−dport 53 −j ACCEPT
iptables −A OUTPUT -s 194.224.88.4 −p tcp −−sport 53 −j ACCEPT
iptables −A OUTPUT -s 194.224.88.4 −p udp −−sport 53 −j ACCEPT
iptables -A OUTPUT -s 194.224.88.4 -p tcp --dport 53 -j ACCEPT
iptables -A OUTPUT -s 194.224.88.4 -p udp --dport 53 -j ACCEPT
iptables -A INPUT -d 194.224.88.4 -p tcp --sport 53 -j ACCEPT
iptables -A INPUT -d 194.224.88.4 -p udp --sport 53 -j ACCEPT

Servidor de correo vamos a configurar smtp en el puerto 25,465,587 y luego entrega pops y imaps es decir con certificados ssl por tanto no voy a configurar los puertos 110 y 143. En este caso debemos permitir también tráficos con protocolo smtp desde el exterior por eso son necesarias las últimas reglas.

```
iptables -A INPUT -d  194.224.88.5  -p tcp -m tcp --dport 25 -j ACCEPT
iptables -A INPUT   -d  194.224.88.5 -p tcp -m tcp --dport 465 -j ACCEPT
iptables -A INPUT   -d  194.224.88.5 -p tcp -m tcp --dport 587 -j ACCEPT
iptables -A INPUT   -d  194.224.88.5 -p tcp -m tcp --dport 995 -j ACCEPT
iptables -A INPUT   -d  194.224.88.5 -p tcp -m tcp --dport 993 -j ACCEPT
```

```
iptables -A OUTPUT  -s 194.224.88.5 -p tcp -m tcp --sport 25 -j ACCEPT
iptables -A OUTPUT  -s 194.224.88.5 -p tcp -m tcp --dport 465 -j ACCEPT
iptables -A OUTPUT  -s 194.224.88.5 -p tcp -m tcp --sport 587 -j ACCEPT
iptables -A OUTPUT -s 194.224.88.5 -p tcp -m tcp --sport 995 -j ACCEPT
iptables -A OUTPUT -s 194.224.88.5 -p tcp -m tcp --sport 993 -j ACCEPT
iptables -A OUTPUT -s 194.224.88.5 -p tcp --dport 25 -j ACCEPT
iptables -A OUTPUT -s 194.224.88.5 -p tcp --dport 465 -j ACCEPT
iptables -A OUTPUT -s 194.224.88.5 -p tcp --dport 587 -j ACCEPT
iptables -A INPUT -d 194.224.88.5 -p tcp --sport 25 -j ACCEPT
iptables -A INPUT -d 194.224.88.5 -p tcp --sport 465 -j ACCEPT
iptables -A INPUT -d 194.224.88.5 -p tcp --sport 587  -j ACCEPT
```