#!/bin/bash #Habilitamos siempre el forwarding echo 1 > /proc/sys/net/ipv4/ip_forward

DMZIFACE=“eth1” LOCALIFACE=“eth2” INETIFACE=“eth0” VPNIFACE=“tun0”

DMZNET=“10.12.13.0/24” LOCALNET=“10.12.12.0/24”

VPNALLIFACE=“tun+”

case “$1” in

```
start)
echo "Iniciando Firewall... \n"
```

```
#Ponemos todo a cero
iptables -F
iptables -X
iptables -Z
```

```
#Politicas por defecto
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
```

```
      iptables -t nat -F
      iptables -t nat -P PREROUTING ACCEPT
      iptables -t nat -P POSTROUTING ACCEPT
      iptables -t nat -P OUTPUT ACCEPT
```

```
#Aceptamos las conexiones ya establecidas
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -i lo -m state --state NEW -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
##############################################
##  REGLAS PARA EL INPUT                    ##
##############################################
```

```
# Permitimos los pings
iptables -A INPUT -p icmp -m state --state NEW -j ACCEPT
```

```
#Abrimos en el INPUT el ssh desde cualquier interfaz
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

```
#Abrimos en el INPUT el openvpn desde cualquier interfaz
iptables -A INPUT -p udp --dport 1194 -j ACCEPT
```

```
#Abrimos en el INPUT dns para las vpn, la dmz y localnet
iptables -A INPUT -i $DMZIFACE  -p udp --dport 53 -j ACCEPT
iptables -A INPUT -i $VPNALLIFACE  -p udp --dport 53 -j ACCEPT
iptables -A INPUT -i $LOCALIFACE  -p udp --dport 53 -j ACCEPT
```

```
#Abrimos en el INPUT dhcp para las dmz y localnet
iptables -A INPUT -i $DMZIFACE  -p udp --dport 67 -j ACCEPT
iptables -A INPUT -i $LOCALIFACE  -p udp --dport 67 -j ACCEPT
```

```
##############################################
## REGLAS PARA TODOS LOS FORWARDS         ##
##############################################
```

```
# Permitimos los pings
iptables -A FORWARD -p icmp -m state --state NEW -j ACCEPT
```

```
##############################################
##  REGLAS PARA EL FORWARD desde la DMZ   ##
##############################################
```

```
#de la DMZ a Inet solo aceptamos web y ssh y enmascaramos. Aceptamos tb la
salida de rsync desde backup
iptables -A FORWARD -i $DMZIFACE -o $INETIFACE -p tcp -m multiport --
destination-ports www,ssh,https,sftp -m state --state NEW -j ACCEPT
iptables -A FORWARD -s srv-backup -i $DMZIFACE -p tcp --dport 873 -m state -
-state NEW -j ACCEPT
iptables -A FORWARD -s srv-backup -i $DMZIFACE -p tcp --dport 80 -m state --
state NEW -j ACCEPT
```

```
#abrimos el correo para srv-datos
iptables -A FORWARD -s srv-datos -i $DMZIFACE -o $INETIFACE -p tcp --dport
25 -m state --state NEW -j ACCEPT
iptables -A FORWARD -s srv-datos -i $DMZIFACE -o $INETIFACE -p udp --dport
25 -m state --state NEW -j ACCEPT
iptables -A FORWARD -s srv-datos -i $DMZIFACE -o $INETIFACE -p tcp --dport
21 -m state --state NEW -j ACCEPT
iptables -A FORWARD -s srv-datos -i $DMZIFACE -o $INETIFACE -p udp --dport
21 -m state --state NEW -j ACCEPT
iptables -A FORWARD -s srv-datos -i $DMZIFACE -o $INETIFACE -p tcp --dport
3306 -m state --state NEW -j ACCEPT
iptables -A FORWARD -s srv-datos -i $DMZIFACE -o $INETIFACE -p tcp --dport
161 -m state --state NEW -j ACCEPT
```

```
#abrimos el correo para srv-web
iptables -A FORWARD -s srv-web -i $DMZIFACE -o $INETIFACE -p tcp --dport 25
-m state --state NEW -j ACCEPT
iptables -A FORWARD -s srv-web -i $DMZIFACE -o $INETIFACE -p udp --dport 25
-m state --state NEW -j ACCEPT
```

```
#abrimos para el servidor de fechas
iptables -A FORWARD -s srv-web -i $DMZIFACE -o $INETIFACE -p udp --dport ntp
-m state --state NEW -j ACCEPT
```

```
#abrimos al as400 de salica
iptables -A FORWARD -s srv-web -d 194.30.40.94 -i $DMZIFACE -o $INETIFACE -m
```

```
state --state NEW -j ACCEPT

#abrimos al ENBOR de ingesit
iptables -A FORWARD -s srv-web -d 212.81.222.114 -i $DMZIFACE -o $INETIFACE
-m state --state NEW -j ACCEPT
```

```
      #abrimos al ENBOR de Basterra
iptables -A FORWARD -s srv-web -d 212.81.209.194 -i $DMZIFACE -o $INETIFACE
-m state --state NEW -j ACCEPT
```

```
      #abrimos al SQL SERVER de Gastrobaska
iptables -A FORWARD -s srv-web -d 212.8.98.176 -i $DMZIFACE -o $INETIFACE -m
state --state NEW -j ACCEPT
#iptables -A FORWARD -s 10.12.12.70 -d 212.8.98.176 -i $DMZIFACE -o
$INETIFACE -m state --state NEW -j ACCEPT

#abrimos el correo para el servidor de backup
iptables -A FORWARD -s srv-backup -i $DMZIFACE -o $INETIFACE -p tcp --dport
25 -m state --state NEW -j ACCEPT
iptables -A FORWARD -s srv-backup -i $DMZIFACE -o $INETIFACE -p udp --dport
25 -m state --state NEW -j ACCEPT

iptables -t nat -A POSTROUTING -s $DMZNET -o $INETIFACE -j MASQUERADE
```

```
##############################################
##  REGLAS PARA EL FORWARD desde la LOCAL ##
##############################################

#de la red local podemos acceder a los servicios de samba, http, https y ssh
de srv-datos. Y ftp
iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -d srv-datos -p tcp -m
multiport --destination-ports 999,www,ssh,https,139,445 -m state --state NEW
-j ACCEPT
iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -d srv-datos -p udp -m
multiport --destination-ports 137,138 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -d srv-datos -p tcp --dport
21 -m state --state NEW -j ACCEPT

#de la red local podemos acceder a los servicios de samba, http, https y ssh
de srv-web. Y ftp
iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -d srv-web -p tcp -m
multiport --destination-ports 999,www,ssh,https,139,445 -m state --state NEW
-j ACCEPT
iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -d srv-web -p udp -m
multiport --destination-ports 137,138 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -d srv-web -p tcp --dport 21
-m state --state NEW -j ACCEPT
iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -d srv-web -p tcp --dport 20
-m state --state NEW -j ACCEPT
```

```
#de la red local podemos acceder a toda la centralita
```

```
iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -d centralita -m state --
state NEW -j ACCEPT
iptables -A FORWARD -o $LOCALIFACE -i $DMZIFACE -s centralita -m state --
state NEW -j ACCEPT
```

```
#abrimos tambien el ldap
iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -d srv-datos -p tcp --dport
389 -m state --state NEW -j ACCEPT
#abrimos tambien el mysql
iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -d srv-datos -p tcp --dport
3306 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -d srv-web -p tcp --dport
3306 -m state --state NEW -j ACCEPT
```

```
#de la red local podemos acceder a los servicios de ssh y https de srv-
backup
iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -d srv-backup -p tcp -m
multiport --destination-ports ssh,https,www -m state --state NEW -j ACCEPT
```

```
#dejamos todo el trafico a internet y lo enmascaramos
#iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -p tcp --dport 20 -m state
--state NEW -j ACCEPT
      #iptables -A FORWARD -i $LOCALIFACE -o $DMZIFACE -p tcp --dport 21 -m
state --state NEW -j ACCEPT
      #iptables -A FORWARD -i $LOCALIFACE -o $INETIFACE -p tcp --dport 22 -m
state --state NEW -j ACCEPT
      #iptables -A FORWARD -i $LOCALIFACE -o $INETIFACE -p tcp --dport 2222
-m state --state NEW -j ACCEPT
      #iptables -A FORWARD -i $LOCALIFACE -o $INETIFACE -p tcp --dport 8443
-m state --state NEW -j ACCEPT
#iptables -A FORWARD -i $LOCALIFACE -o $INETIFACE -p tcp --dport 25 -m state
--state NEW -j ACCEPT
      #iptables -A FORWARD -i $LOCALIFACE -o $INETIFACE -p tcp --dport 80 -m
state --state NEW -j ACCEPT
      #iptables -A FORWARD -i $LOCALIFACE -o $INETIFACE -p tcp --dport 443 -
m state --state NEW -j ACCEPT
#iptables -A FORWARD -i $LOCALIFACE -o $INETIFACE -p tcp --dport 110 -m
state --state NEW -j ACCEPT
#iptables -A FORWARD -i $LOCALIFACE -o $INETIFACE -p tcp --dport 3306 -m
state --state NEW -j ACCEPT
iptables -A FORWARD -i $LOCALIFACE -o $INETIFACE -m state --state NEW -j
ACCEPT
iptables -t nat -A POSTROUTING -s $LOCALNET -o $INETIFACE -j MASQUERADE
```

```
#dejamos todo el trafico hacia los tuneles
iptables -A FORWARD -i $LOCALIFACE -o $VPNALLIFACE -m state --state NEW -j
ACCEPT
```

```
##############################################
##  REGLAS PARA EL FORWARD desde la VPN   ##
```

```
########################################
```

```
#Trafico abierto entre tuneles
iptables -A FORWARD -i $VPNALLIFACE -o $VPNALLIFACE -j ACCEPT
```

```
#de la VPN podemos acceder a los servicios de ssh y https de srv-backup
iptables -A FORWARD -i $VPNALLIFACE -o $DMZIFACE -d srv-backup -p tcp -m
multiport --destination-ports ssh,https -m state --state NEW -j ACCEPT

#de la VPN podemos acceder a los servicios de samba, http, https y ssh de
srv-datos
iptables -A FORWARD -i $VPNALLIFACE -o $DMZIFACE -d srv-datos -p tcp -m
multiport --destination-ports 999,www,ssh,https,139,445 -m state --state NEW
-j ACCEPT
iptables -A FORWARD -i $VPNALLIFACE -o $DMZIFACE -d srv-datos -p udp -m
multiport --destination-ports 137,138 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i $VPNALLIFACE -o $DMZIFACE -d srv-web -p tcp -m
multiport --destination-ports 999,www,ssh,https,139,445 -m state --state NEW
-j ACCEPT
iptables -A FORWARD -i $VPNALLIFACE -o $DMZIFACE -d srv-web -p udp -m
multiport --destination-ports 137,138 -m state --state NEW -j ACCEPT
```

```
echo "iniciado"
;;
```

```
stop)
#Ponemos todo a cero
iptables -F
iptables -X
iptables -Z

#Politicas por defecto
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
      iptables -t nat -F

iptables -t nat -A POSTROUTING -s $LOCALNET -o $INETIFACE -j MASQUERADE
iptables -t nat -A POSTROUTING -s $DMZNET -o $INETIFACE -j MASQUERADE
```

```
echo "Parando el Firewall... \n"
echo "Queda todo abierto \n"
;;
```

```
status)
echo "********************* Reglas de Filtrado ************************"
iptables -v -n --line-numbers -x -t filter -L
echo "*****************************************************************"
;;
```

-)

```
echo "Firewall: Script para la administracion de Firewall /n"
echo "Uso: Firewall {start|stop|status} /n"
;;
```

esac

exit 0

From:
https://wiki.merkatu.info/ - **Wiki de merkatu**

Permanent link:
https://wiki.merkatu.info/iptables?rev=1299515112

Last update: **2017/03/27 17:43**