Configuración escrita:

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

DMZIFACE=“eth1” LOCALIFACE=“eth2” INETIFACE=“eth0” VPNIFACE=“tun0” VPNALLIFACE=“tun+”

DMZNET=“10.12.13.0/24” LOCALNET=“10.12.12.0/24” VPNNET=“10.12.14.0/24”

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

# Permitimos snmp para todos - cacty
iptables -A INPUT -p snmp -m state --state NEW -j ACCEPT (DMZ)

#Abrimos en el INPUT el ssh desde cualquier red conocida
iptables -A INPUT -s 10.12.12.0/24 -i eth2 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -s 10.12.13.0/24 -i eth1 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -s 10.12.14.0/24 -i tun0 -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 eth1  -p udp --dport 53 -j ACCEPT
iptables -A INPUT -i tun0  -p udp --dport 53 -j ACCEPT
iptables -A INPUT -i eth2  -p udp --dport 53 -j ACCEPT

#Abrimos en el INPUT dhcp para la localnet
iptables -A INPUT -i eth2  -p udp --dport 67 -j ACCEPT
```

```
#Abrimos en el INPUT ntp para any
iptables -A INPUT -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   ##
##############################################
```

```
##DMZ(eth1) --> Internet(eth0)
#Tráfico desde DMZ a Internet por www,ssh/sftp,https enmascaramos.
iptables -A FORWARD -i eth1 -o eth0 -p tcp -m multiport --destination-ports
80,22,443 -m state --state NEW -j ACCEPT
```

```
#abrimos desde srv de DMZ (datos, web, backup)a internet para correo
#iptables -A FORWARD -i eth1 -o $INETIFACE --dport 25 -m state --state NEW -
j ACCEPT
iptables -A FORWARD -s 10.12.13.10 -i eth1 -o eth0 --dport 25 -m state --
state NEW -j ACCEPT
iptables -A FORWARD -s 10.12.13.12 -i eth1 -o eth0 --dport 25 -m state --
state NEW -j ACCEPT
iptables -A FORWARD -s 10.12.13.11 -i eth1 -o eth0 --dport 25 -m state --
state NEW -j ACCEPT
```

```
#Acceso desde srv-datos a MySql para????
#iptables -A FORWARD -s 10.12.13.10 -i eth1 -o eth0 -p tcp --dport 3306 -m
state --state NEW -j ACCEPT
```

```
#Conexión de srvweb a as400 de Salica puertos¿?
iptables -A FORWARD -s 10.12.13.12 -i eth1 -d 194.30.40.94 -o eth0 -m state
--state NEW -j ACCEPT
```

```
#Conexión de srvweb a ENBOR de ingesit puertos¿?
iptables -A FORWARD -s 10.12.13.12 -i eth1 -d 212.81.222.114 -o eth0 -m
state --state NEW -j ACCEPT
```

```
        #Conexión de srvweb a ENBOR de Basterra puertos¿?
```

```
iptables -A FORWARD -s 10.12.13.12 -i eth1 -d 212.81.209.194 -o eth0 -m
state --state NEW -j ACCEPT
```

```
     #Conexión de srvweb y ???? a SQL SERVER de Gastrobaska puertos¿?
iptables -A FORWARD -s 10.12.13.12 -i eth1 -d 212.8.98.176 -o eth0 -m state
--state NEW -j ACCEPT
#iptables -A FORWARD -s 10.12.12.70 -i eth2 -d 212.8.98.176 -o eth0 -m state
--state NEW -j ACCEPT
```

```
##DMZ --> Any
#Abrimos desde srv-backup a any (tb internet????) por servicios rsync
iptables -A FORWARD -s 10.12.13.11 -i eth1 -p tcp --dport 873 -m state --
state NEW -j ACCEPT ****
```

```
#Enrutado y enmascaramiento de la DMZ hacia internet
iptables -t nat -A POSTROUTING -s $DMZNET -i eth1 -o eth0 -j MASQUERADE
```

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

##LOCAL --> DMZ
#Tráfico desde local a en DMZ (datos, web, backup) por servicios samba,
http, https, ssh, netbios_tcp y 445
iptables -A FORWARD -i eth2 -d 10.12.13.10 -o eth1 -p tcp -m multiport --
destination-ports 999,80,22,443,139,445 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i eth2 -d 10.12.13.12 -o eth1 -p tcp -m multiport --
destination-ports 999,80,22,443,139,445 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i eth2 -d 10.12.13.11 -o eth1 -p tcp -m multiport --
destination-ports 80,22,443 -m state --state NEW -j ACCEPT
```

```
#habilitamos tráfico netbios_udp desde local a DMZ (datos, web, backup)
iptables -A FORWARD -i eth2 -o eth1 -p udp -m multiport --destination-ports
137,138 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i eth2 -d 10.12.13.10 -o eth1 -p udp -m multiport --
destination-ports 137,138 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i eth2 -d 10.12.13.12 -o eth1 -p udp -m multiport --
destination-ports 137,138 -m state --state NEW -j ACCEPT
```

```
#habilitamos tráfico desde local a la centralita todo y todos??
iptables -A FORWARD -i eth2 -d 10.12.13.100 -o eth1 -m state --state NEW -j
ACCEPT
iptables -A FORWARD -s 10.12.13.100 -i eth1 -o eth2 -m state --state NEW -j
ACCEPT
```

#abrimos desde local hacia srv-datos y srv-web el mysql

```
iptables -A FORWARD -i eth2 -d 10.12.13.10 -o eth1 -p tcp --dport 3306 -m
state --state NEW -j ACCEPT
iptables -A FORWARD -i eth2 -d 10.12.13.12 -o eth1 -p tcp --dport 3306 -m
```

```
state --state NEW -j ACCEPT
```

```
##LOCAL --> INTERNET
#abrimos trafico desde local hacia internet
iptables -A FORWARD -i eth2 -o eth0 -p tcp -m state --state NEW -j ACCEPT
```

```
#enrutado y enmascaramiento
iptables -t nat -A POSTROUTING -s $LOCALNET -i eth2 -o eth0 -j MASQUERADE
```

```
#dejamos todo el trafico desde local hacia el tun0????
#iptables -A FORWARD -i eth2 -o $VPNIFACE -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
```

```
#VPN --> DMZ
#Acceso desde VPN en DMZ (datos, web, backup) por servicios samba, http,
https, ssh, netbios_tcp y 445
iptables -A FORWARD -i $VPNALLIFACE -d 10.12.13.10 -o eth1 -p tcp -m
multiport --destination-ports 999, 80, 22,443,139, 445 -m state --state NEW
-j ACCEPT
iptables -A FORWARD -i $VPNALLIFACE -d 10.12.12.12 -o eth1 -p tcp -m
multiport --destination-ports 999, 80, 22,443,139, 445 -m state --state NEW
-j ACCEPT
iptables -A FORWARD -i $VPNALLIFACE -d 10.12.13.11 -o eth1 -p tcp -m
multiport --destination-ports 22,443,-m state --state NEW -j ACCEPT
```

```
#habilitamos tráfico netbios_udp desde VPN a DMZ (datos, web, backup)
iptables -A FORWARD -i $VPNALLIFACE -o eth1 -p udp -m multiport --
destination-ports 137,138 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i $VPNALLIFACE -d 10.12.13.10 -o eth1 -p udp -m
multiport --destination-ports 137,138 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i $VPNALLIFACE -d 10.12.13.12 -o eth1 -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=1303930330

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