#!/bin/bash

modprobe ip_conntrack modprobe ip_conntrack_ftp modprobe ip_nat_ftp

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

DMZIFACE="em1" LOCALIFACE="em3" INETIFACE="em2" VPNIFACE="tapm" VPNALLIFACE="tap+"

DMZNET="10.12.13.0/24" LOCALNET="10.12.12.0/24"

```
echo "FIREWALL 2.0, bloqueos a la carta."
      echo "Iniciando ........ "
```

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

```
      #Politicas por defecto
      iptables -P INPUT DROP
      iptables -P FORWARD ACCEPT
      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
      iptables -t nat -A POSTROUTING -s $LOCALNET -o $INETIFACE -j
MASQUERADE
      iptables -t nat -A POSTROUTING -s $DMZNET -o $INETIFACE -j MASQUERADE
```

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

```
      #Cerramos a atacantes
iptables -A INPUT -s 185.87.121.5 -j DROP
```

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

```
#Abrimos puertos apache para acceso desde el exterior
iptables -A INPUT -p tcp --dport 8080 -j ACCEPT
iptables -A INPUT -p tcp --dport 8888 -j ACCEPT # zabbix desde fuera
```

```
      #Abrimos en el INPUT el ssh desde cualquier interfaz
```

```
      iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --dport 2222 -j ACCEPT
```

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

```
#Abrimos en el INPUT el agente de Zabbix para cualquier interfaz
iptables -A INPUT -p tcp --dport 10050 -j ACCEPT
iptables -A INPUT -p tcp --dport 10051 -j ACCEPT
iptables -A INPUT -p udp --dport 10050 -j ACCEPT
iptables -A INPUT -p udp --dport 10051 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 10050 -j ACCEPT
      iptables -A OUTPUT -p tcp --dport 10051 -j ACCEPT
      iptables -A OUTPUT -p udp --dport 10050 -j ACCEPT
      iptables -A OUTPUT -p udp --dport 10051 -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, localnet y VNP
      iptables -A INPUT -i $DMZIFACE  -p udp --dport 67 -j ACCEPT
      iptables -A INPUT -i $LOCALIFACE  -p udp --dport 67 -j ACCEPT
      iptables -A INPUT -i $VPNALLIFACE  -p udp --dport 67 -j ACCEPT
```

```
      #Abrimos en el INPUT snmp para las dmz
      iptables -A INPUT -i $DMZIFACE  -p udp --dport 161 -j ACCEPT
      iptables -A INPUT -i $DMZIFACE  -p tcp --dport 161 -j ACCEPT
iptables -A INPUT -i $DMZIFACE  -p udp --dport 162 -j ACCEPT
      iptables -A INPUT -i $DMZIFACE  -p tcp --dport 162 -j ACCEPT
```

```
      ########################################################
      ##  Puertos y forward para el SVN y BBDD de Gureak   ##
      ########################################################
## 212.81.199.242
iptables -I OUTPUT -o $INETIFACE -d 0.0.0.0/0 -j ACCEPT
iptables -I INPUT -i $INETIFACE -m state --state ESTABLISHED,RELATED -j
ACCEPT
# MySQL
#iptables -A INPUT -s $OTXARKOAGA -i eth0 -p tcp --dport 3306 -j ACCEPT
      iptables -A INPUT -p tcp --dport 3306 -j ACCEPT
iptables -A PREROUTING -t nat -i $INETIFACE -p tcp --dport 3306 -j DNAT --to
10.12.13.11:3306
iptables -A FORWARD -p tcp -d 10.12.13.11 --dport 3306 -j ACCEPT
```

```
      # MySQL TIENDADONDE
#iptables -A INPUT -p tcp --dport 3307 -j ACCEPT
#iptables -A PREROUTING -t nat -i $INETIFACE -p tcp --dport 3307 -j DNAT --
to 10.12.13.20:3307
```

```
#iptables -A FORWARD -p tcp -d 10.12.13.20 --dport 3307 -j ACCEPT
```

```
# SVN
      iptables -A INPUT -p tcp --dport 8081 -j ACCEPT
iptables -A PREROUTING -t nat -i $INETIFACE -p tcp --dport 8081 -j DNAT --to
10.12.13.10:80
iptables -A FORWARD -p tcp -d 10.12.13.11 --dport 80 -j ACCEPT
```

```
# SVN (prueba Igor)
      iptables -A INPUT -s 0.0.0.0 -i $INETIFACE -p tcp --dport 8090 -j
ACCEPT
      iptables -A PREROUTING -t nat -i $INETIFACE -p tcp --dport 8090 -j
DNAT --to 10.12.13.18:8090
      iptables -A FORWARD -p tcp -d 10.12.13.18 --dport 8090 -j ACCEPT
```

SSH

```
iptables -A INPUT -s 0.0.0.0 -i $INETIFACE -p tcp --dport 22 -j ACCEPT
      iptables -A PREROUTING -t nat -i $INETIFACE -p tcp --dport 22 -j DNAT
--to 10.12.13.9:22
      iptables -A FORWARD -p tcp -d 10.12.13.9 --dport 22 -j ACCEPT
```

```
      # Apache y plesk en kokodrilo
      iptables -A INPUT -s 10.12.13.9 -i $INETIFACE -p tcp --dport 80 -j
ACCEPT
      iptables -A PREROUTING -t nat -i $INETIFACE -p tcp --dport 80 -j DNAT
--to 10.12.13.9:80
      iptables -A FORWARD -p tcp -d 10.12.13.9 --dport 80 -j ACCEPT
      iptables -A INPUT -s 10.12.13.9 -i $INETIFACE -p tcp --dport 443 -j
ACCEPT
      iptables -A PREROUTING -t nat -i $INETIFACE -p tcp --dport 443 -j DNAT
--to 10.12.13.9:443
      iptables -A FORWARD -p tcp -d 10.12.13.9 --dport 443 -j ACCEPT
      iptables -A INPUT -s 10.12.13.9 -i $INETIFACE -p tcp --dport 8443 -j
ACCEPT
      iptables -A PREROUTING -t nat -i $INETIFACE -p tcp --dport 8443 -j
DNAT --to 10.12.13.9:8443
      iptables -A FORWARD -p tcp -d 10.12.13.9 --dport 8443 -j ACCEPT
      iptables -A PREROUTING -t nat -i $INETIFACE -p tcp --dport 8447 -j
DNAT --to 10.12.13.9:8447
      iptables -A FORWARD -p tcp -d 10.12.13.9 --dport 8447 -j ACCEPT
```

```
      # Apache en ZABBIX
      iptables -A INPUT -s 0.0.0.0 -i $INETIFACE -p tcp --dport 8888 -j
ACCEPT
      iptables -A PREROUTING -t nat -i $INETIFACE -p tcp --dport 8888 -j
DNAT --to 10.12.13.16:80
iptables -A FORWARD -p tcp -d 10.12.13.16 --dport 80 -j ACCEPT
      iptables -A INPUT -s 10.12.13.16 -i $INETIFACE -p tcp --dport 443 -j
ACCEPT
      iptables -A PREROUTING -t nat -i $INETIFACE -p tcp --dport 443 -j DNAT
```

```
--to 10.12.13.16:443
      iptables -A FORWARD -p tcp -d 10.12.13.16 --dport 443 -j ACCEPT
```

```
# Acceso FTP
iptables -A INPUT -s 10.12.13.9 -i $INETIFACE -p tcp --dport 21 -j ACCEPT
iptables -A PREROUTING -t nat -i $INETIFACE -p tcp --dport 21 -j DNAT --to
10.12.13.9:21
iptables -A FORWARD -p tcp -d 10.12.13.9 --dport 21 -j ACCEPT
```

```
      # Acceso SSH FIELME VIEJO
      iptables -A INPUT -s 0.0.0.0 -i $INETIFACE -p tcp --dport 2222 -j
ACCEPT
      iptables -A PREROUTING -t nat -i $INETIFACE -p tcp --dport 2222 -j
DNAT --to 10.12.13.20:22
      iptables -A FORWARD -p tcp -d 10.12.13.20 --dport 22 -j ACCEPT
```

exit 0

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

Permanent link:
https://wiki.merkatu.info/script_iptables?rev=1496220674

Last update: **2017/05/31 10:51**