Practica 5

ZONAS DESMILITARIZADAS CON SHOREWALL (DOBLE FIREWALL)

JACOBO MARTÍNEZ GÓMEZ

Firewall exterior - Filtrado (Acceso)

1. Permitir desde exterior conexiones a puertos 80,443,25,110 de 10.20.20.22(web mail)
2. Permitir desde interior conexiones a puertos 80,443,22 de exterior (web, ssh)
3. Permitir desde 10.20.20.22 conexiones al puerto 25 de exterior (smtp)
4. Permitir desde interior y dmz conexiones al puerto 53 (tcp y udp) de exterior (dns)
5. Permitir desde interior conexiones al puerto 22 (ssh)

Firewall exterior - Configuración (Acceso)

ACCESO_jmgomez2 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Archivo Editar Pestañas Ayuda

```
root@acceso:/etc/shorewall# cat zones
#ZONE   TYPE    OPTIONS                 IN                      OUT
#                                       OPTIONS                 OPTIONS
fw      firewall
net     ipv4
loc     ipv4
dmz     ipv4
root@acceso:/etc/shorewall# cat interfaces
#ZONE   INTERFACE       OPTIONS
net     enp0s8
loc     enp0s3
dmz     enp0s3
root@acceso:/etc/shorewall# cat hosts
#ZONE       HOST(S)               OPTIONS
dmz         enp0s3:10.20.20.0/24        -
loc         enp0s3:10.10.10.0/24        -
root@acceso:/etc/shorewall# cat masq
#############################################################################
#INTERFACE              SOURCE          ADDRESS         PROTO   PORT(S) IPSEC   MARK
enp0s8                    10.10.10.0/24
enp0s8                    10.20.20.0/24
root@acceso:/etc/shorewall# cat policy
#############################################################################
#SOURCE         DEST            POLICY          LOG LEVEL       LIMIT:BURST
loc             all             DROP            info
net             all             DROP            info
dmz             all             DROP            info
```

ACCESO_jmgomez2 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

LXTerminal

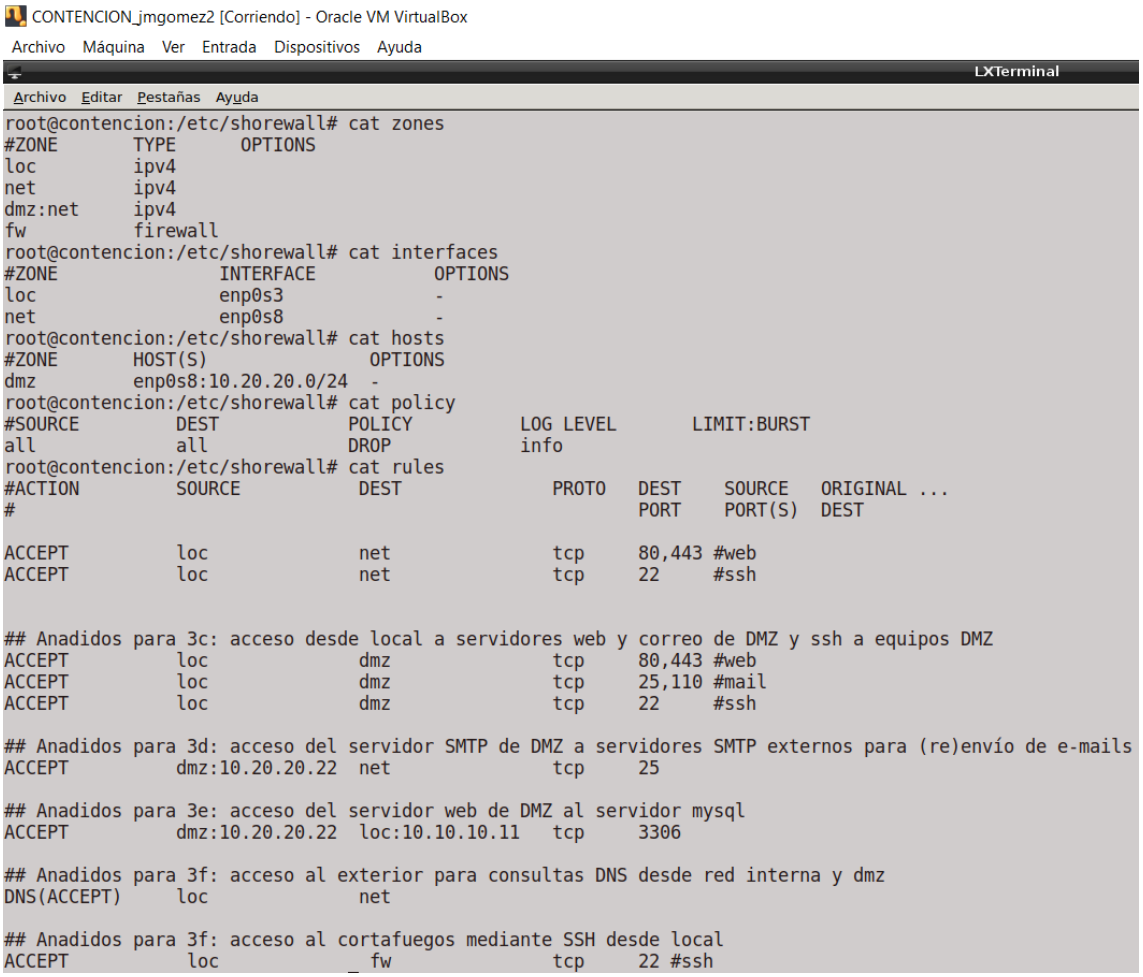
Archivo Editar Pestañas Ayuda

```
root@acceso:/etc/shorewall# cat rules
#############################################################################
#ACTION         SOURCE          DEST            PROTO   DEST    SOURCE   ORIGINAL ...
#                                                       PORT    PORT(S)  DEST
# Anadidos para 2a, 2b: redirec. puertos (servicios publicos: http, https, smtp, pop3) a DMZ
DNAT            net             dmz:10.20.20.22   tcp     80,443
DNAT            net             dmz:10.20.20.22   tcp     25,110
## Anadidos para 3b: acceso desde local a red externa (solo WEB y SSH)
ACCEPT          loc             dmz:10.20.20.22   tcp     80,443
ACCEPT          loc             dmz:10.20.20.22   tcp     25,10
# Anadidos para 3c: acceso desde local a servidores web y correo de DMZ y ssh a equipos DMZ
ACCEPT          loc             net             tcp     80,443
ACCEPT          loc             net             tcp     22
## Anadidos para 3d: acceso del servidor SMTP de DMZ a servidores SMTP externos para (re)envío de e-mails
ACCEPT          dmz:10.20.20.22  net             tcp     25
## Anadidos para 3f: acceso al exterior para consultas DNS desde red interna y dmz
DNS(ACCEPT)     loc             net
DNS(ACCEPT)     dmz             net
## Anadidos para 3f: acceso al cortafuegos mediante SSH desde local
ACCEPT           loc             fw              tcp     22
```

Firewall interior - Filtrado (Contención)

1. Permitir desde interior conexiones a puertos 80, 443, 22 de exterior (web, ssh)
2. Permitir desde interior conexiones a puertos 80,443,25,110,22 de dmz (web,mail ssh)
3. Permitir desde 10.20.20.22 conexiones al puerto 3306 de 10.10.10.11 (mysql)
4. Permitir desde interior conexiones al puerto 53 (tcp, udp) de exterior (dns)
5. Permitir desde interio conexión a puerto 22 (ssh)

Firewall interior - Filtrado (Contención)



Pruebas de funcionamiento realizadas

Desde exterior:

```
root@fuera:~# nmap -sT -Pn 193.147.87.47 10.20.20.22 10.20.20.2 10.10.10.11

Starting Nmap 7.40 ( http://nmap.org ) at 2019-12-15 15:03 CET
Nmap scan report for acceso.ssi.net (193.147.87.47)
Host is up (0.00064s latency).
Not shown: 996 filtered ports
PORT    STATE  SERVICE
25/tcp  open   smtp
80/tcp  open   http
110/tcp open   pop3
443/tcp closed https

Nmap scan report for 10.20.20.22
Host is up (0.029s latency).
All 1000 scanned ports on 10.20.20.22 are filtered

Nmap scan report for 10.20.20.2
Host is up (0.035s latency).
All 1000 scanned ports on 10.20.20.2 are filtered

Nmap scan report for 10.10.10.11
Host is up (0.026s latency).
All 1000 scanned ports on 10.10.10.11 are filtered

Nmap done: 4 IP addresses (4 hosts up) scanned in 21.41 seconds
```

Para el exterior la red interna y dmz están cerradas. Solo se puede acceder a los servicios web y mail de la maquina dmz a través de la ip del firewall exterior.

Desde interior:

```
root@dentro:~# nmap -sT -Pn  10.10.10.1 10.20.20.22 10.20.20.1 193.147.87.33

Starting Nmap 7.40 ( http://nmap.org ) at 2019-12-15 15:06 CET
Nmap scan report for contencion.ssi.net (10.10.10.1)
Host is up (0.0011s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for dmz.ssi.net (10.20.20.22)
Host is up (0.0044s latency).
Not shown: 995 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
25/tcp  open   smtp
80/tcp  open   http
110/tcp open   pop3
443/tcp closed https

Nmap scan report for acceso.ssi.net (10.20.20.1)
Host is up (0.0068s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for fuera (193.147.87.33)
Host is up (0.0011s latency).
Not shown: 996 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
53/tcp  closed domain
80/tcp  open   http
443/tcp closed https

Nmap done: 4 IP addresses (4 hosts up) scanned in 21.75 seconds
```

Para contención esta todo bloqueado menos ssh, para dmz todo bloqueado menos ssh, web y mail. En acceso todo bloqueado menos ssh y en la maquina fuera todo bloqueado menos ssh, dns y mail.

Desde DMZ:

```
root@dmz:~# nmap -sT -Pn 10.20.20.1 193.147.87.33 10.20.20.2 10.10.10.11

Starting Nmap 6.47 ( http://nmap.org ) at 2019-12-15 15:28 CET
Nmap scan report for acceso.ssi.net (10.20.20.1)
Host is up.
All 1000 scanned ports on acceso.ssi.net (10.20.20.1) are filtered

Nmap scan report for fuera (193.147.87.33)
Host is up (0.0081s latency).
Not shown: 998 filtered ports
PORT   STATE  SERVICE
25/tcp open   smtp
53/tcp closed domain

Nmap scan report for contencion.ssi.net (10.20.20.2)
Host is up.
All 1000 scanned ports on contencion.ssi.net (10.20.20.2) are filtered

Nmap scan report for dentro.ssi.net (10.10.10.11)
Host is up (0.015s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 4 IP addresses (4 hosts up) scanned in 19.89 seconds
```

Solo esta permitido el trafico dns y smtp al exterior y el trafico de mysql a dentro.