> Daniel Camba Lamas

Zonas desmilitarizadas: Doble firewall.

Los firewalls serán configurados con el esquema **two-interfaces** ubicado en `/usr/share/doc/shorewall/examples/two-interfaces`. La copia descomprimida del mismo, debe ser ubicada en `/etc/shorewall`.

Configuración del firewall *Acceso*.

La configuración se separa en base a los 6 archivos que es necesario modificar.

Zones.

> Zonas de la red y tipo de las mismas.

#ZONE	TYPE
externa	ipv4
fw	firewall
dmz	ipv4
interna	ipv4

Interfaces.

> Interfaces del firewall que se está configurando.

#ZONE	INTERFACE
-	eth0
externa	eth1

Hosts.

> Rangos de IP de las zonas de la red.

#ZONE	HOSTS	OPTIONS
interna	eth0:10.10.10.0/24	-
dmz	eth0:10.20.20.0/24	-

Masq.

> Redirecciones SNAT (privado -> público).

#INTERFACE:DEST	SOURCE
eth0	10.10.10.0/24
eth0	10.20.20.0/24

Rules.

> Restricciones explicitas que deben cumplirse.

Por defecto...

#ACTION	SOURCE	DEST	PROTO	PORTS
Invalid(DROP)	externa	all	tcp	
DNS(ACCEPT)	dmz	externa		

DNS(ACCEPT)	interna	externa		
SSH(ACCEPT)	interna	fw		
SSH(ACCEPT)	interna	externa		

Redirección para servicios públicos....

#ACTION	SOURCE	DEST	PROTO	PORTS
DNAT	externa	dmz:10.20.20.22	tcp	80,443 #http,https
DNAT	externa	dmz:10.20.20.22	tcp	25,110 #smtp,pop3

Servicios públicos desde el exterior, permitidos...

#ACTION	SOURCE	DEST	PROTO	PORTS
ACCEPT	externa	dmz:10.20.20.22	tcp	80,443 #http,https
ACCEPT	externa	dmz:10.20.20.22	tcp	25,110 #smtp,pop3

Servicio web y ssh al exterior desde la red interna....

#ACTION	SOURCE	DEST	PROTO	PORTS
ACCEPT	interna	externa	tcp	80,443 #http,https
ACCEPT	interna	externa	tcp	22 #ssh

Servicio ssh sobre el firewall desde la red interna....

#ACTION	SOURCE	DEST	PROTO	PORTS
ACCEPT	interna	fw	tcp	22 #ssh

Servicio smtp al exterior desde la dmz....

#ACTION	SOURCE	DEST	PROTO	PORTS
ACCEPT	dmz:10.20.20.22	externa	tcp	25 #smtp

Policy.

> Políticas de manejo de paquetes que no cumplan las especificaciones anteriores.

#SOURCE	DEST	POLICY	LOG LEVEL
all	all	REJECT	info
all	all	REJECT	info

Configuración del firewall *Contencion*.

La configuración se separa en base a los 5 archivos que es necesario modificar.

Zones.

> Zonas de la red y tipo de las mismas. En este caso hay la peculiaridad de que dmz será una subred de externa ya que no se puede delimitar un rango de direcciones para externa ya que puede ser cualquier IP pública.

#ZONE	TYPE
externa	ipv4
dmz:externa	ipv4

fw	firewall
interna	ipv4

Interfaces.

> Interfaces del firewall que se está configurando.

#ZONE	INTERFACE
interna	eth0
externa	eth1

Hosts.

> Rangos de IP de las zonas de la red.

#ZONE	HOSTS	OPTIONS
dmz	eth1:10.20.20.0/24	-

Rules.

> Restricciones explicitas que deben cumplirse.

Por defecto...

#ACTION	SOURCE	DEST	PROTO	PORTS
Invalid(DROP)	externa	all	tcp	
DNS(ACCEPT)	loc	externa		
SSH(ACCEPT)	interna	fw		
SSH(ACCEPT)	interna	dmz		

SSH(ACCEPT)	interna	externa		

Servicio web y ssh al exterior desde la red interna....

#ACTION	SOURCE	DEST	PROTO	PORTS
ACCEPT	interna	externa	tcp	80,443 #http,https
ACCEPT	interna	externa	tcp	22 #ssh

Servicios web, mail, ssh desde el interior a dmz...

#ACTION	SOURCE	DEST	PROTO	PORTS
ACCEPT	interna	dmz	tcp	80,443 #http,https
ACCEPT	interna	dmz	tcp	25,110 #smtp,pop3
ACCEPT	interna	dmz	tcp	22 #ssh

Servicio ssh sobre el firewall desde la red interna....

#ACTION	SOURCE	DEST	PROTO	PORTS
ACCEPT	interna	fw	tcp	22 #ssh

Servicio mysql desde la dmz a dentro....

#ACTION	SOURCE	DEST	PROTO	POI
ACCEPT	dmz:10.20.20.22	interna:10.10.10.11	tcp	33 #my

Policy.

> Políticas de manejo de paquetes que no cumplan las especificaciones anteriores.

#SOURCE	DEST	POLICY	LOG LEVEL
all	all	REJECT	info

Shorewall.conf

- `STARTUP_ENABLED = Yes`
- `IP_FORWARDING = On`

Pruebas: `namp -Pn`

DMZ hacia Fuera.

```
root@dmz:/etc/shorewall# nmap -Pn 193.147.87.33

Starting Nmap 6.47 ( http://nmap.org ) at 2016-12-
Nmap scan report for fuera (193.147.87.33)
Host is up (0.00067s latency).
Not shown: 998 closed ports
PORT   STATE    SERVICE
25/tcp filtered smtp
53/tcp filtered domain
```

Dentro hacia Fuera.

```
root@dentro:~# nmap -Pn 193.147.87.33

Starting Nmap 6.47 ( http://nmap.org ) at
Nmap scan report for fuera (193.147.87.33)
Host is up (0.00074s latency).
Not shown: 996 closed ports
PORT    STATE    SERVICE
22/tcp  filtered ssh
53/tcp  filtered domain
80/tcp  filtered http
443/tcp filtered https
```

DMZ hacia Dentro.

```
root@dmz:/etc/shorewall# nmap -Pn 10.10.10.11

Starting Nmap 6.47 ( http://nmap.org ) at 2016-12-
Nmap scan report for dentro.ssi.net (10.10.10.11)
Host is up (0.0015s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3306/tcp open  mysql
```

Dentro hacia DMZ.

```
root@dentro:~# nmap -Pn 10.20.20.22

Starting Nmap 6.47 ( http://nmap.org ) at 2016-
Nmap scan report for dmz.ssi.net (10.20.20.22)
Host is up (0.00019s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
```