Definición de zonas desmilitarizadas con Shorewall

$CDA \ 2021/22$

7 de octubre de 2021

Índice

1.	Descripción		1			
2.	Entorno de prácticas					
	2.1. Software de virtualización VIRTUALBOX		2			
	2.2. Imágenes a utilizar		2			
	2.3. Máquinas virtuales y redes creadas		3			
3.	Shorewall (Shoreline Firewall)		3			
	3.1. Funcionamiento		4			
	3.1.1. Comandos de control		4			
	3.2. Descripción de la red (zones, interfaces, hosts)		5			
	3.3. Definición del filtrado (policy, rules)		5			
	3.4. Configuración adicional (snat, tunnels, stoppedrules)		6			
4.	Configuración de una DMZ (<i>DeMilitarized Zone</i>) usando el generador de firewalls Shoreline Firewall (ShoreWall)	ip-tables	7			
	4.1. Descripción		7			
	4.2. Restriciones de acceso a implementar		7			
	4.3. Pasos previos (preparación del entorno)		8			
	4.4. Pasos a seguir		8			
	4.4.1. Pruebas a realizar		11			
5.	Documentación a entregar		12			

1. Descripción

Ejemplo de uso del generador de cortafuegos iptables/NETFILTER Shoreline Firewall (Shorewall)

• Definición de una DMZ con un firewall de 3 interfaces

2. Entorno de prácticas

2.1. Software de virtualización VIRTUALBOX

En estas prácticas se empleará el software de virtualización VIRTUALBOX para simular los equipos GNU/Linux sobre los que se realizarán las pruebas.

- Página principal: http://virtualbox.org
- Más información: http://es.wikipedia.org/wiki/Virtualbox

2.2. Imágenes a utilizar

- 1. Scripts de instalación
 - para GNU/Linux: ejercicio-dmz-openvpn.sh alumno@pc: \$ sh ejercicio-dmz-openvpn.sh
 - para MS windows: ejercicio-dmz-openvpn.ps1
 Powershell.exe -executionpolicy bypass -file ejercicio-dmz-openvpn.ps1

Notas:

- Se pedirá un identificador (sin espacios) para poder reutilizar las versiones personalizadas de las imágenes creadas (usad por ejemplo el nombre del grupo de prácticas o el login LDAP)
- En ambos scripts la variable \$DIR_BASE especifica donde se descargarán las imágenes y se crearán las MVs. Por defecto en GNU/Linux será en \$HOME/CDA2122 y en Windows en C:/CDA2122.
 Puede modificarse antes de lanzar los scripts para hacer la instalación en otro directorio más conveniente (disco externo, etc)
- Es posible descargar las imágenes comprimidas manualmente (o intercambiarlas con USB), basta descargar los archivos con extensión .vdi.zip de http://ccia.esei.uvigo.es/docencia/CDA/2122/practicas/ y copiarlos en el directorio anterior (\$DIR_BASE) para que el script haga el resto.
- Si no lo hacen desde el script anterior, se pueden arrancar las instancias VIRTUALBOX desde el interfaz gráfico de VirtualBOX o desde la línea de comandos con VBoxManage startvm <nombre MV>_<id>
- 2. Imágenes descargadas
 - base_cda.vdi (0,82 GB comprimida, 2,9 GB descomprimida): Imagen genérica (común a todas las MVs) que contiene las herramientas a utilizar

Contiene un sistema Debian 9 con herramientas gráficas y un entorno gráfico ligero LXDE (*Lighweight X11 Desktop Environment*) [LXDE].

- swap1GB.vdi: Disco de 1 GB formateado como espacio de intercambio (SWAP)
- 3. Usuarios configurados e inicio en el sistema
 - Usuarios disponibles

login	password
root	purple
usuario	usuario

- Acceso al entorno gráfico una vez logueado (necesario para poder copiar y pegar desde/hacia el anfitrión)

root@datos:~# startx

 Habilitar copiar y pegar desde/hacia el anfitrión en el menú Dispositivos -> Portapapeles compartido -> bidir de la ventana de la máquina virtual.

2.3. Máquinas virtuales y redes creadas

Una vez ejecutado el script se habrán definido las 3 redes y los 4 equipos virtualizados donde se realizarán los ejercicios:

- Red interna (10.10.10.0 ... 10.10.10.255): máquina dentro (enp0s3) + interfaz enp0s3 de firewall3
- Red DMZ (10.20.20.0 ... 10.20.20.255): máquina dmz (enp0s3) + interfaz enp0s8 de firewall3
- Red externa (193.147.87.0 ... 193.147.87.255): máquina fuera (enp0s3) + interfaz enp0s9 de firewall3



3. Shorewall (Shoreline Firewall)

Shorewall (Shoreline firewall) es un generador de reglas iptables a partir de una especificación expresada en un conjunto ficheros en formato texto (ubicados por defecto en /etc/shorewall).

- Shorewall organiza la red sobre la que se aplica el filtrado en zonas.
 - Una **zona** en Shorewall es una porción de la red (interna o externa) sobre la que se aplican una serie de restricciones de filtrado específicas
 - El objetivo es separar la descripción de la red y la definición del filtrado
 - El uso de **zonas** simplifica la configuración y permite reutilizar las definciones del filtrado, haciéndolas independientes de los detalles de la red (interfaces de red del cortafuegos, rangos de direcciones utilizados, etc).
- La definición de las zonas se detalla en los ficheros zones, interfaces, hosts
- La definición del filtrado se detalla en los ficheros policy y rules

• Otros aspectos complementarios de detallan en ficheros como **snat**, **tunnels**, etc.

Recursos complementarios

- Shorewall: http://www.shorewall.org/
 - Resumen: presentación Shorewall
 - DMZ (DeMilitarized Zone) con tres interfaces: Three interfaces firewall
- Netfilter/Iptables: Resumen iptables

3.1. Funcionamiento

Al compilar los ficheros de configuración, la información detallada en zones, interfaces y hosts permite a Shorewall identificar las zonas de origen y destino de cada paquete inspeccionado.

Internamente lo que hará Shorewall es crear una cadena iptables para cada par (zona origen, zona destino).

Con la información presente en interfaces y, opcionalmente, en hosts, se crearán reglas en las cadenas por defecto input, output y forward para capturar los paquetes con ese origen y ese destino y derivar el procesamiento de dichos paquetes a la correspondiente cadena (de nombre [origen]-[destino]).

La estructura de las cadenas [origen]-[destino] generadas es siempre la misma, por este orden:

- 1. Se permite el tráfico de conexiones ya abiertas
- 2. Reglas iptables resultado de traducir las entradas del fichero rules aplicables a las correspondientes zonas de origen y destino
- 3. Reglas iptables correspondientes al comportamiento por defecto entre las zonas origen y destino indicado en el fichero de configuración policy

Los ficheros de configuración complementarios (snat, tunnels, etc) son procesados y las respectivas reglas iptables son generadas conforme a su contenido y añadidas al script de Shell final generado por el compilador de configuraciones de Shorewall.

3.1.1. Comandos de control

Shorewall ofrece el comando shorewall con diferentes subcomandos (ver man shorewall ó https://shorewall.org/manpages/shorewall.html):

- shorewall start: Compila los ficheros de configuración de /etc/shorewall, genera en /var/lib/shorewall/.start el script de puesta en marcha del cortafuegos con los correspondientes comandos iptables y lo ejecuta para configurar Netfilter con las reglas de filtado creadas.
- shorewall clear: Deshabilita el cortafuegos, devolviendo Netfilter a su configuración por defecto (sin reglas y con una política ACCEPT por defecto en todas las cadenas)
- shorewall stop: Deshabilita el cortafuegos, estableciendo las reglas de filtrado generales indicadas en el fichero stoppedrules
- shorewall check: Comprueba la configuración de /etc/shorewall para verificar que es correcta, informando de los posibles errores en el caso contrario
- shorewall show: Muestra distintos tipos de informaciones relativas al cortafuegos y a su estado actual.

Por ejemplo shorewall show connections muestra la lista de conexiones sobre las que Netfilter hace "seguimiento de conexiones" (*connection tracking*) Adicionalmente, en entornos Debian, Ubuntu y derivados, se proporciona un script de arranque (/etc/init.d/shorewall) que activa y desactiva el cortafuegos durante el inicio del sistema (ver https://wiki.debian.org/HowTo/shorewall) o desde línea de comandos con systemctl [accion] shorewall.service.

 IMPORTANTE: para usar este script de arranque es preciso habilitarlo estableciendo la variable startup = 1 en /etc/default/shorewall

3.2. Descripción de la red (zones, interfaces, hosts)

zones (ver https://shorewall.org/manpages/shorewall-zones.html)

Formato: (una línea por cada zona declarada)

ZONE TYPE OPTIONS IN OPTIONS OUT OPTIONS

- Enumera las zonas que existen en la red e identifica el tipo de zona (firewall, ipv4,. ipv6, etc)
- Se requiere que al menos una de las zonas definidas sea de tipo firewall
- Es posible anidar unas zonas dentro de otras y vincular distintas opciones a cada zona

interfaces (ver https://shorewall.org/manpages/shorewall-interfaces.html)

Formato (versión 2, ?FORMAT 2): (una línea por cada interfaz de red [indicando - como zona si es necesario]) ZONE INTERFACE OPTIONS

- Vincula interfaces de red existentes en el cortafuegos con las zonas a las que dan acceso.
- Es necesario declarar todas las interfaces de red que el firewall deba manejar
- En caso de que una interfaz de red estuviera vinculada a más de una zona, se debe indicar su zona con (posteriormente se detallará en hosts cómo se vinculan sus IPs a las diferentes zonas)

hosts (opcional) (ver https://shorewall.org/manpages/shorewall-hosts.html)

Formato:

ZONE HOST(S) OPTIONS

- Complementa la información de interfaces, detallando la pertenencia a zonas concretas de IPs individuales o de subredes (rangos de IPs)
- La especificación de hosts y subredes debe indicar la interfaz y la dirección/rango separados por : (eth0:192.168.1.0/
- En casos sencillos, Shorewall será capaz de identificar la zona origen y la zona destino de cada paquete unicamente con la información de **interfaces**. Sólo en casos donde esto no posible se requerirá definir este fichero.

3.3. Definición del filtrado (policy, rules)

Shorewall hace uso del módulo conntrack de iptables que permite hacer seguimiento de las conexiones, usando Netfilter como un filtro de paquetes con estado.

- Por defecto, Shorewall generará reglas para permitir tráfico de conexiones ya abiertas, no siendo necesasio habilitarlo explícitamente.
- El control del tráfico que se configura en los ficheros **policy** y **rules** se refiere únicamente los mensajes de inicio de conexión (paquetes SYN en TCP o el primer paquete en UDP)

policy (ver https://shorewall.org/manpages/shorewall-policy.html)

Formato:	(una línea por combi	nación origen y de s	stino)	
SOURCE	DEST	POLICY	LOG	BURST:LIMIT

- Define la acción por defecto (comportamiento general) para las conexiones desde una zona origen a una zona destino (el valor all indica cualquier zona declarada).
- Algunas acciones posibles son:
 - ACCEPT: acepta el tráfico de la zona origen dejándolo pasar hacia la zona destino
 - DROP: descarta el tráfico procedente de la zona origen hacia la zona destino
 - **REJECT**: igual que **DROP** pero informando al origen del descarte del paquete con un mensaje del protocolo ICMP
- Opcionalmente, puede indicarse el nivel de log con el que se registrará el tráfico con las zonas origen y destino correspondientes.
- También se puede fijar la tasa de máxima (RATE) de paquetes permitidos para la combinación de tráfico indicada.

rules (ver https://shorewall.org/manpages/shorewall-rules.html)

Formato: (una línea por regla)

ACTION SOURCE DEST PROTO DPORT SPORT ORIGDEST ...

- Define el comportamiento específico para conexiones que cumplan los requisitos indicados (origen, destino, protocolos, puertos, etc) y que supongan excepciones al comportamiento general especificado en policy.
- Acciones posibles:
 - Mismas que en policy: ACCEPT, DROP, REJECT
 - Redirección de puertos (*Destination NAT*), con la acción DNAT e indicando el la columna DEST la nueva dirección destino
 - Redirección a un puerto del propio firewall, con la acción REDIRECT
- Aspectos configurables:
 - Origen (columna SOURCE) y destino (columna DEST) de las conexiones, bien forma de una zona o de una dirección IP o rango de direcciones dentro de una zona determinada (separando zona y dirección con :)
 - Protocolo (columna PROTO) usado en la conexión (tcp, udl, icpm, all, ...)
 - Puertos origen (columna SPORT) y destino (columna SPORT) de las conexiones
 - Tasas máximas de paquetes permitidas (RATE), máximo de conexiones (CONNLIMIT), puerto destino original de una redirección (ORIGDEST), etc
- Existe la posibilidad de abreviar las reglas usando *macros* parametrizables.
 - Macros disposibles declaradas en /usr/share/shorewall/ como ficheros macro.XXXX
 - Al usar una macro se debe indicar como parámetro la acción a aplicar
 - Como resultado, la macro se expandirá, reemplazándo su definición por el contenido del correspondiente fichero macro.XXXX reemplazando su parámetros (marcado con PARAM) y fijando los valores ajustables (marcados con -)
 - Se puede consultar la lista de macros disponibles con shorewall show macros

3.4. Configuración adicional (snat, tunnels, stoppedrules)

snat (ver https://shorewall.org/manpages/shorewall-snat.html)

Formato:

ACTION SOURCE DEST ...

- Define la traducción de direcciones origen (SNAT, *Source Network Addresss Translation*) en caso de que sea necesario utilizarla.
 - Si está presente, reemplaza al fichero masq de versiones anteriores de Shorewall
- La columna SOURCE indica el orgigen de los paquetes a enmascarar, puede indicarse un nombre de interfaz de red o un rango de direcciones IP

- La columna DEST indica el interfaz de red por donde pretenden "salir" los paquetes a enmascarar
- Las acciones pueden ser MASQUERADE (hace enmascaramiento/SNAT con la dirección establecida en la interfaz de red de salida) o SNAT(<direccion>) (hace enmascaramiento/SNAT con la dirección IP indicada)
- Pueden añadirse otras restriciones adicionales (protocolo, puertos origen y destino, etc)
- Al compilar este fichero, Shorewall añadirá las reglas iptables a la cadena POSTROUTTING de Netfilter con las acciones SNAT/MASQUERADE correspondientes.

tunnels (ver https://shorewall.org/manpages/shorewall-tunnels.html)

Formato:

TYPE ZONE GATEWAY GATEWAY ZONES

- Declara las conexiones VPN (*Virtual Private Network*) que debe gestionar el cortafuegos.
- Se debe indicar el tipo de VPN (ipsec, openvpn, pptp, ...), la zona del firewall donde se origina la conexión VPN e información de la/s pasarela/s VPN (gateways) desde las que llega esa conexión.

stoppedrules (ver https://shorewall.org/manpages/shorewall-stoppedrules.html)

Formato:

ACTION SOURCE DEST PROTO DPORT SPORT

- Fichero auxiliar, indica la configuración de cortafuegos a establecer cuando se ejecuta el comando shorewall stop
- Sintaxis similar a la de rules, aunque simplificada
- En SOURCE y DEST se usa el símbolo comodín para indicar "cualquier zona"

4. Configuración de una DMZ (*DeMilitarized Zone*) usando el generador de firewalls ip-tables Shoreline Firewall (ShoreWall)

4.1. Descripción

Se desarrollará un ejercicio de configuración básica de un firewall con DMZ empleando el generador de reglas iptables Shorewall. Se usará un equipo con tres interfaces para hacer el papel de firewall.

4.2. Restriciones de acceso a implementar

- 1. Enmascaramiento (SNAT) de la red interna (10.10.10.0/24) y de la DMZ (10.20.20.0/24)
- 2. Redireccionamiento (DNAT) de los servicios públicos que ofrecerá la red hacia la máquina **dentro (10.20.20.22)** de la DMZ
 - a) peticiones WEB (http y https)
 - b) tráfico de correo saliente (smtp) y entrante (pop3)
- 3. Control de tráfico con política "denegar por defecto" (DROP)
 - a) desde la red externa sólo se permiten las conexiones hacia la DMZ contempladas en las redirecciones del punto anterior (http, https, smtp, pop3)
 - b) des
de la red interna hacia la red externa sólo se permite tráfico de tipo
 WEB y SSH
 - c) desde la red interna hacia la DMZ sólo se permite tráfico WEB (http, https), e-mail (smtp, pop3), hacia los respectivos servidores, y tráfico SSH para tareas de administración en los equipos de la DMZ
 - d) desde el servidor SMTP de la red DMZ (máquina **dmz (10.20.20.22)**) hacia el exterior se permite la salida de conexiones SMTP (para el reenvío del e-mail saliente)

e) desde la máquina **dmz (10.20.20.22)** se permiten conexiones MySQL <u>única y exclusivamente</u> hacia la máquina **dentro (10.10.10.11)** de la red interna

Nota: Esta restricción va contra el principio general de las DMZ, que establece que se deben impedir conexiones desde la DMZ hacia la zona interna. En este caso se asume una excepción a este princpio, que debería ser limitada lo máximo posible y convenientemente monitorizada. Una solución más robusta a este caso sería plantear una DMZ de dos niveles.

- f) se permite la salida a la red externa de las consultas DNS originadas en la red interna y en la DMZ
- g) firewall sólo admite conexiones SSH desde la red interna para tareas de administración
- 4. Registro (log) de intentos de acceso no contemplados desde red externa a **firewall3 (193.147.87.47)** y a los equipos internos

4.3. Pasos previos (preparación del entorno)

1. PREVIO 1: Habilitar la redirección de tráfico en la máquina firewall3 [10.10.10.1, 10.20.20.1, 193.147.87.47]

```
firewall3:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Nota: Esta configuración no es permanente, se puede descomentar la línea #net.ipv4.ip_forward=1 en el fichero /etc/sysctl.conf para que se habilite la redirección de tráfico cada vez que arranque la máquina.

2. PREVIO 2: Tarea 1: (a incluir en la memoria entregable) Escaneo de las máquinas del ejercicio para verificar los servicios accesibles inicialmente

```
desde fuera:
  fuera: "# nmap -T4 193.147.87.47
                                      [escaneo de firewall3 (unica máquina visible desde fuera)]
  fuera: "# nmap -T4 10.10.10.11
                                      [escaneo de dentro (fallará)]
  fuera: "# nmap -T4 10.20.20.22
                                      [escaneo de dmz (fallará)]
desde dentro:
  dentro: "# nmap -T4 193.147.87.33
                                       [escaneo de fuera]
  dentro: "# nmap -T4 10.20.20.22
                                       [escaneo de dmz]
  dentro: "# nmap -T4 10.10.10.1
                                       [escaneo de firewall3]
desde dmz:
  dmz:~# nmap -T4 193.147.87.33
                                    [escaneo de fuera]
  dmz:~# nmap -T4 10.10.10.11
                                    [escaneo de dentro]
  dmz:~# nmap -T4 10.20.20.1
                                    [escaneo de firewall3]
desde firewall3:
  firewall3: "# nmap -T4 193.147.87.33
                                          [escaneo de fuera]
  firewall3:~ # nmap -T4 10.10.10.11
                                          [escaneo de dentro]
  firewall3:~# nmap -T4 10.20.20.22
                                          [escaneo de dmz]
```

Nota: En la imagen común a todas las máquinas virtuales fue habilitado el acceso exterior al servidor MySQL (en principio sólo será relevante para la máquina dentro(10.10.10.11)) [ya hecho en las MV de prácticas]

dentro~# nano /etc/mysql/mariadb.conf.d/50-server.cnf

```
(comentar la linea donde aparece bind-address 127.0.0.1)
...
# bind-address 127.0.0.1
...
```

4.4. Pasos a seguir

Se usará el esquema three-interfaces incluido en la distribución estándar de Shorewall y descrito en http://www.shorewall.net/three-interface.htm.

La plantilla para configurar el firewall está en el directorio /usr/share/doc/shorewall/examples/three-interfaces/

Todas las tareas de configuración de Shorewall se realizarán en la máquina firewall3.

1. Copiamos los ficheros de configuración en el directorio de configuración de Shorewall (/etc/shorewall/)

```
firewall3:~# cd /etc/shorewall
firewall3:/etc/shorewall# cp /usr/share/doc/shorewall/examples/three-interfaces/* .
```

2. Configurar las zonas (/etc/shorewall/zones) [lo dejaremos como está]

Tendremos 4 zonas:

- el propio firewall (fw)
- la red externa (net) [accesible a través de enp0s9]
- la red interna (loc) [accesible a través de enp0s3]
- la dmz (dmz) [accesible a través de enp0s8]

firewall3:/etc/shorewall# nano zones

#ZONE	TYPE	OPTIONS	IN	OUT			
#			OPTIONS	OPTIONS			
fw	firewall						
net	ipv4						
loc ipv4							
dmz	ipv4						

3. Configurar los interfaces (/etc/shorewall/interfaces)

Ajustar los interfaces de red de cada zona para que se ajusten a nuestra configuración (en columna INTERFACE)

firewall3:/etc/shorewall# nano interfaces

4. Definir el enmascaramiento (/etc/shorewall/snat)

En nuestro ejemplo enmascararemos (SNAT: source NAT) el tráfico saliente de nuestras 2 redes internas (loc y dmz) para salga a la red pública con la IP del cortafuegos.

firewall3:/etc/shorewall# nano snat

##############		****	+#######	+########	+#######	+########	+########	*#######	*****	****
#ACTION	SOURCE	DEST	PROTO	PORT	IPSEC	MARK	USER	SWITCH	ORIGDEST	PROBABILITY
#										
MASQUERADE	10.10.10.0/24	enp0s9								
MASQUERADE	10.20.20.0/24	enp0s9								

Indica que el tráfico de la red **10.10.10.0** y de **10.20.20.0** que pretenda salir a través del interface enp0s9 (red externa) se "reescribirá" su dirección origen con la dirección IP del interfaz enp0s9 (IP pública de **firewall3** (193.147.87.47))

5. Definir las políticas (/etc/shorewall/policy)

En nuestro caso fijaremos unas políticas restrictivas que descartarán por defecto todo el tráfico entre las zonas definidas. En el fichero /etc/shorewall/rules se ajustarán las excepciones pertinentes.

firewall3:/etc/shorewall# nano policy

#######################################	*################	#################	#################	#######################################
#SOURCE	DEST	POLICY	LOG LEVEL	LIMIT:BURST
#				
loc	all	DROP		

net	all	DROP	info
dmz	all	DROP	
# THE FOLLOWING	POLICY MUST B	E LAST	
all	all	REJECT	info

6. Incluir las excepciones y redirecciones en /etc/shorewall/rules

Mantendremos las excepciones (reglas) incluidas en el fichero rules de muestra.

 Definen el comportamiento para servicios básicos como DNS, SSH hacia dmz y firewall, mensajes ICMP de PING, etc

Nota: hace uso de macros como Ping(DROP), SSH(ACCEPT) (abrevian la notación ahorrando el escribir los puertos concretos)

Implementaremos las restricciones de tráfico descritas en la sección 4.2 y añadiremos al final del fichero las reglas correspondientes.

firewall3:/etc/shorewall# nano rules

```
******
#ACTION
            SOURCE
                          DEST
                                        PROTO
                                              DEST
                                                     SOURCE
                                                            ORIGINAL ...
                                               PORT
                                                     PORT(S) DEST
#
      Accept DNS connections from the firewall to the Internet
# DNS(ACCEPT)
               $FW
                            net
*******
      Accept SSH connections from the local network to the firewall and DMZ
SSH(ACCEPT)
                           $FW
                                # Cubre parte de las restricciones 3c
             loc
SSH(ACCEPT)
             loc
                           dmz
                                # Cubre parte de las restricciones 3c
. (sigue)
##
## ANADIDOS para implementar reglas de filtrado (AÑADIR al final del fichero "rules" DESDE AQUI)
##
## Anadidos para 2a, 2b: redirec. puertos (servicios publicos: http, https, smtp, pop3) a DMZ
                          dmz:10.20.20.22
DNAT
                                               80.443
            net
                                        tcp
DNAT
                          dmz:10.20.20.22
                                               25,110
            net
                                        tcp
## Anadidos para 3b: acceso desde local a red externa (solo WEB y SSH)
ACCEPT
                                               80,443
            loc
                          net
                                        tcp
ACCEPT
            loc
                                               22
                          net
                                        tcp
## Anadidos para 3c: acceso desde local a servidores web y correo de DMZ y ssh a equipos DMZ
ACCEPT
                          dmz:10.20.20.22
                                               80,443
            loc
                                        tcp
ACCEPT
            loc
                          dmz:10.20.20.22
                                        tcp
                                               25,110
ACCEPT
                                               22 # No sería necesario, cubierto por una regla anterior
            loc
                          dmz
                                        tcp
## 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 3e: acceso del servidor web de DMZ al servidor mysql
ACCEPT
            dmz:10.20.20.22 loc:10.10.10.11 tcp
                                               3306
## Anadidos para 3f: acceso al exterior para consultas DNS desde red interna y dmz
DNS(ACCEPT)
            loc
                          net
DNS(ACCEPT)
            dmz
                          net
####### NOTA: Reglas 3f equivalen a:
#ACCEPT
             loc
                                                53
                           net
                                         tcp
```

#ACCEPT	loc	net	udp	53			
#ACCEPT	dmz	net	tcp	53			
#ACCEPT	dmz	net	udp	53			
#######################################							

Anadidos para 3f: acceso al cortafuegos mediante SSH desde local
ACCEPT loc fw tcp 22

7. Ajustar el fichero de configuración de Shorewall (/etc/shorewall/shorewall.conf)

Como mínimo debe establecerse la variable STARTUP_ENABLED a yes, para que el compilador Shorewall procese los ficheros y genere las reglas iptables.

También debe habilitarse el *forwarding* de paquetes: Asegurar que la variable IP_FORWARDING está a on (o Keep si se garantiza que se habilita *ip forwarding* antes de iniciar el firewall)

```
firewall3:/etc/shorewall# nano shorewall.conf
```

8. Arrancar Shorewall

Nota: Se hará uso de Shorewall de forma manual con los subcomandos start, clear o compile.

 Previo: Editar el fichero stoppedrules usado por el subcomando shorewall stop con el siguiente contenido (permite todo el tráfico)

firewall3:/etc/shorewall# nano stoppedrules

#ACTION	SOURCE	DEST	PROTO	DEST	SOURCE	
#				PORT(S)	PORT(S)	
ACCEPT	-	-				

firewall3:/etc/shorewall# shorewall start

Más detalles sobre inicio, parada y deshabilitación de Shorewall

4.4.1. Pruebas a realizar

1. Comprobar la configuración actual de iptables en firewall3 (puede consultarse la configuración directamente con los comandos de iptables o analizando el script generado por Shorewall en /var/lib/shorewall/.start)

```
firewall3:~# iptables -L -n
firewall3:~# iptables -t nat -L -n
ó
firewall3:~# iptables-save > /tmp/volcado.txt
firewall3:~# leafpad /tmp/volcado.txt
ó
firewall3:~# leafpad /var/lib/shorewall/.start
```

Nota: También es posible ver el contenido a una cadena iptables concreta de las generadas por Shorewall (cadena [origen]-[destino], por ejemplo loc-net) [con shorewall show policies se pueden ver las cadenas generadas]

```
firewall3:~# iptables -L loc-net
ó
firewall3:~# shorewall show loc-net
```

- 2. Tarea 2: (a incluir en memoria entregable) revisar la configuración de Shorewall y estructura de las reglas generadas automáticamente a partir de ella.
 - a) Señalar las configuraciones de Shorewall (entradas en policy, rules, zones, interfaces, hosts, etc) que dan soporte al tráfico redireccionado hacia la DMZ
 - b) Identificar y describir las reglas iptables generadas por Shorewall para dar soporte al tráfico redireccionado hacia la DMZ
 - c) Señalar las configuraciones de Shorewall (entradas en policy, rules, zones, interfaces, host, etc) que habilitan el acceso desde la DMZ al servidor MySQL de la red interna
 - d) Identificar y describir las reglas iptables generadas por Shorewall que permiten el acceso desde la DMZ al servidor MySQL de la red interna
- 3. Tarea 3: (a incluir en memoria entregable) Comprobar que se verifican las redirecciones y restriciones de tráfico desde las distintas máquinas (fuera, dentro, dmz)
 - Puede hacerse empleando el escaner de puertos nmap, el generador de paquetes hping3, conexiones directas con telnet, nc ó socat, o conexiones directas empleando clientes de los propios protocolos implicados.

```
fuera:~# nmap -T4 193.147.87.47 10.10.10.11 10.20.20.22
dentro:~# nmap -T4 193.147.87.33 10.20.20.22 10.10.10.1
dmz:~# nmap -T4 193.147.87.33 10.10.10.11 10.20.20.1
firewall3:~# nmap -T4 193.147.87.33 10.10.10.11 10.20.20.22
```

Nota: El escaneo desde **firewall3** generará una serie de alertas por consola, dado que con las reglas de filtrado implementadas el cortafuegos no tiene permitido casi ningún tipo de tráfico de salida.

• Para el caso del servidor WEB redireccionado a la DMZ, puede comprobarse el "salto" adicional introducido por el firewall empleando la herramienta tcptraceroute.

```
fuera: "# tcptraceroute 193.147.87.47 80
```

• En el caso de la conexión SSH desde la red interna hacia el exterior (máquina **fuera**) puede realizarse la conexión SSH y, una vez conectado, verificar el origen de la conexión con los comandos who y netstat

dentro: "# ssh usuario@193.147.87.33 (con la contraseña usuario)

```
fuera:~# who
fuera:~# netstat -at
```

• En el caso del tráfico NAT a través de **firewall3** puede utilizarse el comando **netstat-nat** -a para ver las conexiones NAT establecidas actualmente.

```
firewall3:~# netstat-nat -n -N
```

 Documentar las pruebas realizadas, los resultados obtenidos y las posibles discrepancias con las políticas de filtrado previstas.

5. Documentación a entregar

Esquema propuesto

- Descripción **breve** del ejercicio realizado
- Detallar la situación inicial del la red del ejemplo (escaneo inicial de la Tarea 1 del punto PREVIO 2)
- Detallar las comprobaciones realizadas en el apartado 4.4.1 y documentar los resultados obtenidos (comentando, si es necesario, las discrepancias con el comportamiento deseado descrito en la sección 4.2).
 Incluir los resultados obtenidos en Tarea 2 (reglas iptables generadas) y Tarea 3 (escaneo final)
- Conclusiones (opcional): detallar los problemas encontrados, posibles mejoras o alternativas, impresiones sobre la idoneidad de las herramientas, etc

Entrega: MOOVI Fecha límite: 31/10/2021