Definición de zonas desmilitarizadas con Shorewall

CDA 2018/19

2 de noviembre de 2018

Índice

1. Descripción

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

- Definición de una DMZ con un firewall de 3 interfaces

Recursos complementarios

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

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/CDA1819` y en Windows en `C:/CDA1819`.
     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/1819/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** (0,65 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)

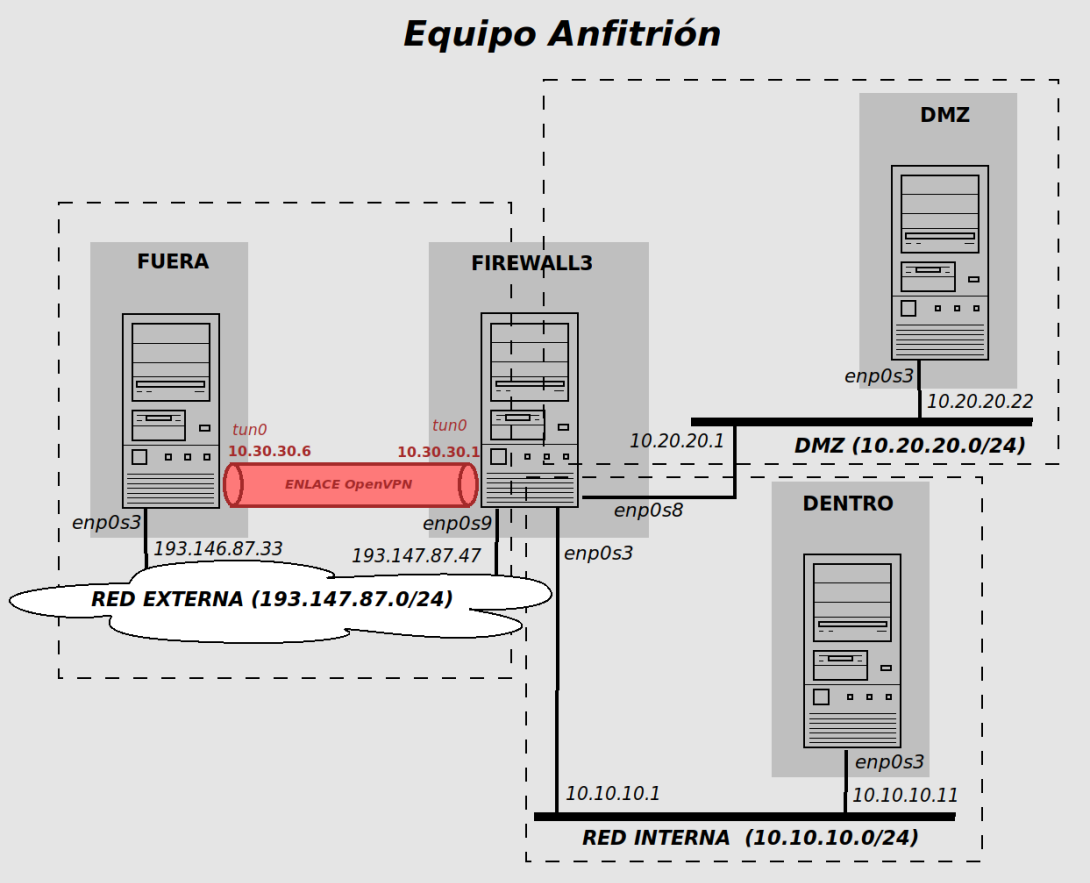
     `root@datos:~# startx`

   - 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**



2.4. 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: (Si no están iniciados) arrancar los servicios a utilizar [ya hecho]

   ```
   dentro:~# service mysql start                (ó   service mysql restart)
   dentro:~# service openbsd-inetd start        (ó   service openbsd-inetd restart)

   dmz:~# service apache2 start   (servidor web  [80])    (ó service apache2 restart)
   dmz:~# service postfix start   (servidor smtp [25])    (ó service postfix restart)
   dmz:~# service dovecot start   (servidor pop3 [110])   (ó service dovecot restart)
   ```

```
fuera:~# service apache2 start              (ó service apache2 restart)
fuera:~# service openbsd-inetd start        (ó service openbsd-inetd restart)
fuera:~# service postfix start              (ó service postfix restart)
```

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
    ...
```

3. **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]
     ```

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

3.1. 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.

3.2. 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) desde 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 única y exclusivamente hacia la máquina **dentro (10.10.10.11)** de la red interna

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

3.3. 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 y descomprimimos 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/* .
firewall3:/etc/shorewall# gunzip *.gz
```

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
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

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

################################################################################
?FORMAT 2
################################################################################
#ZONE   INTERFACE       OPTIONS
net     enp0s9            tcpflags,routefilter,norfc1918,nosmurfs,logmartians
loc     enp0s3            tcpflags,detectnets,nosmurfs
dmz     enp0s8            tcpflags,detectnets,nosmurfs
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

4. Definir las políticas (`/etc/shorewall/policy`)

   El fichero por defecto incluye todas las combinaciones posibles entre nuestras 3 zonas (`loc`, `dmz`, `net`) indicando una política ACCEPT para el tráfico de la zona `loc` y una política por defecto de rechazar (REJECT) y generando un LOG de los "rechazo" realizados.

   - Esta política sólo tiene utilidad para depuración
   - En nuestro caso fijaremos unas políticas restrictivas que descartarán por defecto todo el tráfico entre las zonas
   - 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            info
net             all             DROP            info
dmz             all             DROP            info

# THE FOLLOWING POLICY MUST BE LAST
all             all             REJECT          info

#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

5. Definir el enmascaramiento (`/etc/shorewall/masq`)

   En nuestro ejemplo enmascararemos (*SNAT: source NAT*) el tráfico saliente de nuestras 2 redes internas (`loc` y `dmz`).

```
firewall3:/etc/shorewall# nano masq

#############################################################################
#INTERFACE              SOURCE          ADDRESS         PROTO   PORT(S) IPSEC   MARK
enp0s9                   10.10.10.0/24
enp0s9                   10.20.20.0/24
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

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

6. Incluir las excepciones y redirecciones en `/etc/shorewall/rules` Mantendremos las excepciones (reglas) incluidas en el fichero `rules` de muestra.

   - Definen el comportamiento de servicios básico 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 parte de las restricciones de tráfico descrita en el ejercicio 1:

   - Se redireccionan todos los servicio públicos (`http, https, smtp` y `pop3`) que ofrecerá nuestra red hacia la DMZ (en nuestro caso a la máquina **10.20.20.22**)
   - Se permite acceso del servidor web de la DMZ (en **10.20.20.22**) al servidor MySQL de la red interna (en **10.10.10.11**)
   - Se permite el acceso desde la red interna a los servidores públicos (web y correo) alojados en la DMZ

   Añadiremos al final del fichero (antes de la línea `#LAST LINE ....`) las reglas que las implementan.

```
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
############### COMENTAR (no nos interesa) #################
# DNS(ACCEPT)      $FW              net
#############################################################

#       Accept SSH connections from the local network to the firewall and DMZ
SSH(ACCEPT)      loc              $FW    # Cubre parte de las restricciones 3c
SSH(ACCEPT)      loc              dmz    # Cubre parte de las restricciones 3c

... (sigue)


###############################################################################################
##
## ANADIDOS para implementar reglas de filtrado  (añadir al fichero "rules" desde aqui)
##
###############################################################################################

## 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              net               tcp     80,443
ACCEPT          loc              net               tcp     22


## Anadidos para 3c: acceso desde local a servidores web y correo de DMZ y ssh a equipos DMZ
ACCEPT          loc              dmz:10.20.20.22   tcp     80,443
ACCEPT          loc              dmz:10.20.20.22   tcp     25,110
ACCEPT          loc              dmz               tcp     22  # No sería necesario, cubierto por una regla anterior

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

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

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

#############################################################################
#                     S T A R T U P   E N A B L E D
#############################################################################
STARTUP_ENABLED=Yes
...

#############################################################################
#                      F I R E W A L L   O P T I O N S
#############################################################################
IP_FORWARDING=Yes
...
```

8. Arrancar Shorewall

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

   - **Previo:** Eliminar el fichero `stoppedrules` usado por el subcomando `stop`

     ```
     firewall3:~# rm stoppedrules
     ```

   ```
   firewall3:~# shorewall start
   ```

   Más detalles sobre inicio, parada y deshabilitación de Shorewall

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

2. **Tarea 2: (a incluir en memoria entregable)** revisar la estructura de las reglas generadas automáticamente por Shorewall.

   a) Identificar y describir las reglas iptables generadas que dan soporte al tráfico redireccionado hacia la DMZ

   b) Identificar y describir las reglas iptables generadas 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
     ```

   - 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.

4. Documentación a entregar

Esquema propuesto (hasta un máximo de 5-6 páginas)

- Descripción **breve** del ejercicio realizado
- Detallar la situación inicial del la red del ejemplo (escaneos de la **Tarea 1** del punto `PREVIO 3`)
- Detallar las comprobaciones realizadas en el apartado 3.3.1 y documentar los resultados obtenidos (comentando, si es necesario, las discrepancias con el comportamiento deseado descrito en la sección 3.2).

  Incluir los resultados obtenidos en **Tarea 2** y **Tarea 3**
- Conclusiones (opcional): detallar los problemas encontrados, posibles mejoras o alternativas, impresiones sobre la idoneidad de las herramientas, etc

Entrega: FAITIC

Fecha límite: 18/11/2018