Zonas desmilitarizadas (doble firewall)

SSI 2022/23

17 de noviembre de 2022

Índice

1. Entorno de prácticas

1.1. 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`

1.2. Imágenes a utilizar

1. Scripts de instalación
   - para GNU/Linux: ejercicio-doble-firewall.sh
     `alumno@pc: $ sh ejercicio-doble-firewall.sh`
   - para MS windows: ejercicio-doble-firewall.ps1
     `Powershell.exe -executionpolicy bypass -file ejercicio-doble-firewall.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/SSI2223` y en Windows en `C:/SSI2223`.
  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/SSI/2223/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
   - **parrot_ssi.vdi** (1,6 GB comprimida, 5,2 GB descomprimida): Imagen genérica (común a todas las MVs) que contiene las herramientas a utilizar
     Contiene un sistema Parrot Security OS (basado en Debian) 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

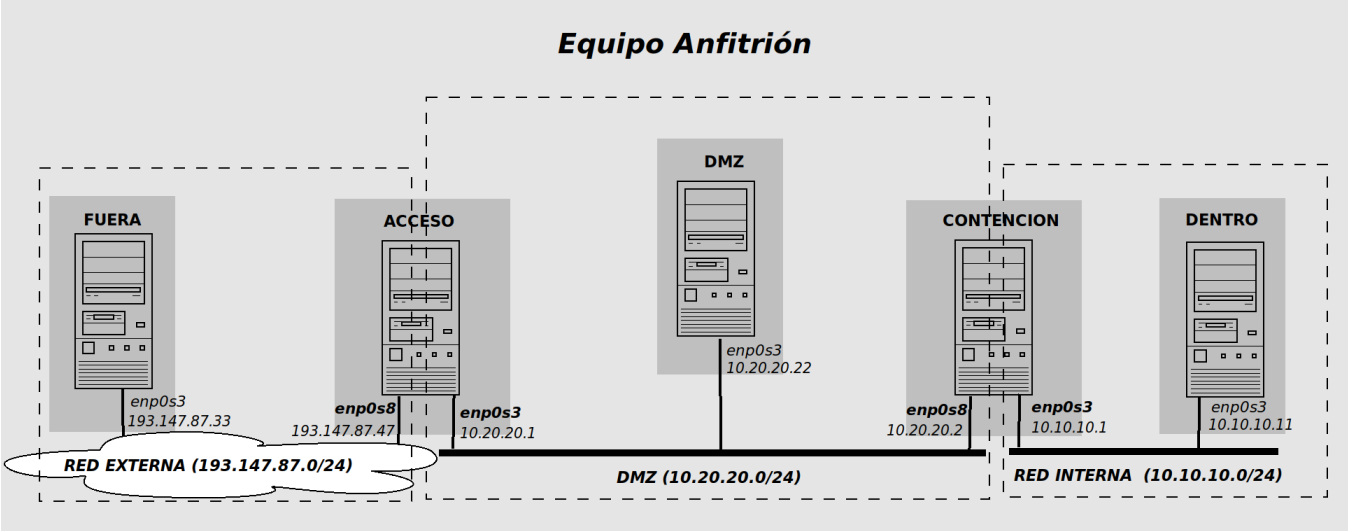
login	password
root	purple
usuario	usuario
(con privilegios sudo)	

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

     ```
     root@base:~# startx
     ```

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

1.3. Máquinas virtuales y redes creadas



- Redes donde se realizarán los ejercicios:

- Red interna (10.10.10.0 ... 10.10.10.255): máquina **dentro** (enp0s3) [10.10.10.11] + interfaz enp0s3 de **contencion** [10.10.10.1]
- Red DMZ (10.20.20.0 ... 10.20.20.255): máquina **dmz** (enp0s3) [10.20.20.22] + interfaz enp0s8 de **contencion** [10.20.20.2] + interfaz enp0s3 de **acceso** [10.10.10.1]
- Red externa (193.147.87.0 ... 193.147.87.255): máquina **fuera** (enp0s3) [193.147.87.33] + interfaz enp0s8 de **acceso** [193.147.87.47]

- Máquinas virtuales
  - Máquina **dentro**: equipo de la red interna
    - IP: 10.10.10.11
    - Puerta de enlace por defecto: 10.10.10.1
  - Máquina **contención**: cortafuegos de contención, separa la red interna de la DMZ
    - IP en la red interna: 10.10.10.11
    - IP en la DMZ: 10.20.20.2
    - Puerta de enlace por defecto: 10.20.20.1
  - Máquina **dmz**: equipo de la DMZ (con servidores públicos HTTP, HTTPS, SMTP, POP3)
    - IP: 10.20.20.22
    - Puerta de enlace por defecto: 10.20.20.1
  - Máquina **acceso**: cortafuegos de acceso, separa la DMZ de la red externa
    - IP en la DMZ: 10.20.20.1
    - IP en la red externa (pública): 193.147.87.47
  - Máquina **fuera**: equipo de la red externa
    - IP en la red externa (pública): 193.147.87.33

2. Preparación previa

1. Servicios arrancados por defecto en todas las máquinas (no es necesario iniciarlos manualmente)
   - servidor web (Apache 2) [**Nota:** puede ser necesario reiniciarlo manualmente con " `service apache2 restart` "]
   - servidor telnet (arrancado por `openbsd-inetd`)
   - servidor SSH (openSSH)
   - servidor ftp (arrancado por `openbsd-inetd`)
   - servidor finger (arrancado por `openbsd-inetd`)
   - servidor MySQL
   - servidor SMTP (postfix)
   - servidores POP3 e IMAP (dovecot)
2. Habilitar la redirección de tráfico en los dos cortafuegos: **acceso[10.20.20.1, 193.147.87.47]** y **contencion[10.10.10.1, 10.20.20.2]**

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

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

3. Ajustar las tablas de enrutado
   - La ruta por defecto (*default gateway*) de la máquina **contención**[10.10.10.1, 10.20.20.2] está establecida hacia la máquina **acceso** [10.20.20.1] para que el tráfico de la red interna pueda salir al exterior.
     - **Justificación:** Es necesario hacerlo así ya que en el cortafuegos **contención**[10.10.10.1, 10.20.20.2] no hacemos enmascaramiento (SNAT) de la red interna (10.10.10.0/24)

- En el cortafuegos **acceso**: añadir una ruta que encamine el tráfico hacia las IPs de la red interna (10.10.10.0/24) a través de la IP del cortafuegos **contención** en la DMZ (10.20.20.2)

  ```
  acceso:~# route add -net 10.10.10.0/24 gw 10.20.20.2
  acceso:~# route -n
  ```

  - **Justificación:** Es necesario hacerlo así para proporcionar al cortafuegos **acceso** una ruta para encaminar hacia la red interna (10.10.10.0/24) los paquetes de respuesta al tráfico saliente generado por los equipos de la propia red interna (10.10.10.0/24)
- En los equipos de la DMZ (**dmz** en el ejemplo): añadir una ruta que encamine el tráfico hacia las IPs de la red interna (10.10.10.0/24) a través de la IP del cortafuegos **contención** en la DMZ (10.20.20.2)

  ```
  dmz:~# route add -net 10.10.10.0/24 gw 10.20.20.2
  dmz:~# route -n
  ```

  Nota: Sin restricciones adicionales, esta ruta no sería estrictamente necesaria.
  - La ruta por defecto (*deafult gateway*) de **dmz**[10.20.20.22] encaminará el tráfico hacia la red 10.10.10.0/24 a la máquina 10.20.20.1 que a su vez, empleando la regla anterior, acabará por enviar esos paquetes a la máquina **contención**[10.20.20.2]
  - No obstante, puesto que en el cortafuegos `acceso`, *Shorewall* decidirá la aceptación o denegación de tráfico en el momento del inicio de conexión, y dado que dichos paquetes de inicio no llegarán a pasar por `acceso`, sino sólo por `contencion`, sí es **necesario establecer esta regla de enrutado** en las máquinas del DMZ.

3. Tarea 1: DMZ con doble firewall usando Shorewall

El ejercicio consiste en la configuración de los dos cortafuegos **acceso** y **contención** empleando el generador de reglas `iptables` Shorewall.

Material de partida:

- Web de Shoreline Firewall (Shorewall): http://www.shorewall.net/
- Resumen presentación Shorewall
- Práctica de CDA 2022/23: DMZ con firewall de 3 interfaces en Shorewall
  - Explicación de Shorewall y ficheros de configuración en Sección 3

Se pretende conseguir un comportamiento que cumpla las restricciones de filtrado descritas en la sección 3.1.

Una vez configurados los dos cortafuegos, se deberá comprobar su funcionamiento con escaneos `nmap` desde cada una de las máquinas del ejercicio hacia las restantes para verificar los puertos abiertos y cerrados en cada caso (incluir en el entregable la salida de estos escaneos)

3.1. Restricciones de filtrado a soportar

1. Enmascaramiento (SNAT) de la red interna (10.10.10.0/24) y de la DMZ (10.20.20.0/24) al salir hacia la red externa
2. Redireccionamiento (DNAT) de los servicios públicos que ofrecerá la red hacia la máquina **dmz (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 sus respectivos servidores, y SSH para la adminsitración de 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) los dos firewalls sólo admiten conexiones SSH desde la red interna

4. Registro (log) de los intentos de acceso no contemplados.

3.2. Detalles de configuración del cortafuegos de acceso

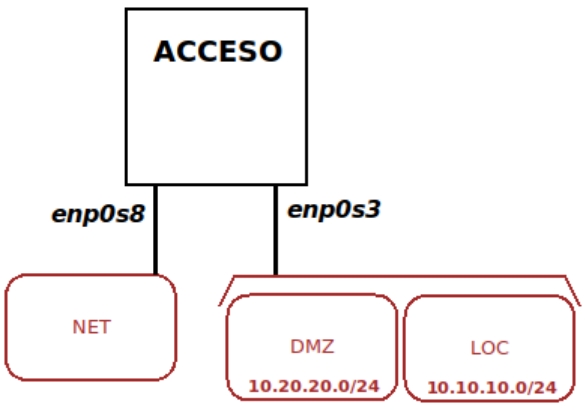
El cortafuegos de acceso regula el tráfico entre la red externa y los equipos de la DMZ y de la red interna.

En nuestro caso, además de las responsabilidades de filtrado del tráfico entrante y/o saliente se debe de encargar de la traducción de direcciones.

- Enmascaramiento (SNAT) de las direcciones de la DMZ (10.20.20.0/24) y de la red interna (10.10.10.0/24) en el tráfico saliente hacia la red externa.
- Redirección del tráfico procedente de la red externa hacia los servicios públicos de la DMZ (en este caso HTTP, HTTPS, SMTP y POP3 en la máquina **dmz**)

Existen varias alternativas para implementar este cortafuegos, pero la más sencilla es emplear un esquema con **tres zonas** basado en el esquema *"Parallel Zones"* del documento de Shorewall Multiple-Zones.html

- Dado que varias zonas (`dmz` y `loc`) "comparten" un interfaz (`enp0s3`), se declarará ese interfaz en el fichero `interfaces`, pero sin vincularlo a ninguna zona. Por lo que será necesario hacer uso del fichero `hosts` para distinguirlas en base a los rangos de direcciones IP empleados en cada caso.
- Más información: shorewall-zones, shorewall-interfaces, shorewall-hosts



3.3. Detalles de configuración del cortafuegos de contención

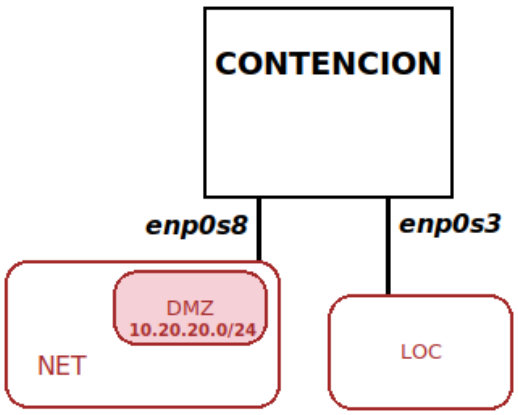
El cortafuegos de contención regula el tráfico entre la red interna y los equipo de la DMZ y de la red externa.

En nuestro caso no se contempla traducción de direcciones: el enmascaramiento (SNAT) de la red interna se delega en el cortafuegos de acceso y el acceso a la DMZ se realiza con las propias direcciones de la red interna [10.10.10.0/24] (requiere fijar adecuadamente las tablas de enrutado, como se hizo al inicio).

Existen varias alternativas para implementar este cortafuegos, pero la más sencilla es emplear un esquema con **tres zonas** basado en el esquema *"Nested Zones"* del documento de Shorewall Multiple-Zones.html

- Dado que varias zonas (`dmz` y `net`) "comparten" un interfaz (`enp0s8`) será necesario hacer uso del fichero `hosts` para distinguirlas en base a los rangos de direcciones IP empleados en cada caso.
- No obstante, en este caso no es posible separar las zonas `dmz` y `net` en base a rangos de direcciones IP (la zona `net` puede tener cualquier dirección IP pública).

  La estrategia a seguir consitirá a vincular el interfaz `enp0s8` a la zona `net` y especificar en el fichero `zones` qye `dmz:net` es una subzona dentro de `net`, empleando el fichero `hosts` para caracterizarla en base a sus direcciones.
- Más información: shorewall-nesting, shorewall-zones, shorewall-interfaces, shorewall-hosts



4. Detalles/problemas

- **Nota 1.**

  En caso de utilizar la plantilla *Three Interfaces Firewall* de Shorewall se incluye un fichero `stoppedrules` en `/etc/shorewall`

  - `stoppedrules` es un híbrido de `policy+rules` que define el tráfico permitido por el cortafuegos cuando se ejecuta el comando `shorewall stop`
  - En nuestro caso usaremos sólo `shorewall start` para iniciar el filtrado en los cortafuegos y `shorewall clear` para eliminar las reglas de filtrado, por lo que no es necesario y se puede eliminar.
  - En caso de no eliminarlo, deberá tener el siguiente contenido en ambos cortafuegos:

    ```
    acceso|contencion:/etc/shorewall# nano stoppedrules

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

- **Nota 2.** En las comprobaciones realizadas con `nmap` incluir la opción `-P0`

  - Esta opción omite la verificación de accesibilidad de los hosts escaneados empleando mensajes Ping
  - Con la configuración por defecto, en caso de que los cortafuegos bloquearan el tráfico ICMP, `nmap` omitiría el escaneo

5. Documentación y entrega

El material entregable de este ejercicio constará de una pequeña memoria cubriendo los siguientes puntos

- Tarea 1: DMZ con doble firewall

- Descripción del filtrado realizado por cada cortafuegos
- Detallar la configuración Shorewall empleada en el cortafuegos **acceso**
  - Explicar la definición de zonas empleada
  - Mostrar cada fichero de configuración (`zones`, `interfaces`, `hosts`, `policy`, `rules`, `snat`, etc), indicando los aspectos relevantes de cada uno.
- Detallar la configuración Shorewall empleada en el cortafuegos **contencion**
  - Explicar la definición de zonas empleada
  - Mostrar cada fichero de configuración (`zones`, `interfaces`, `hosts`, `policy`, `rules`, etc), indicando los aspectos relevantes de cada uno.
- Descripción de las pruebas de funcionamiento realizadas para verificar el cumplimiento de los requisitos indicados en la sección 3.1, incluir los resultados obtenidos.

Entrega (individual o en parejas): MOOVI (hasta 27/12/2022)