Actividad 1: Mecanismos de defensa en redes

Objetivos

Reforzar los conocimientos del estudiante relativos a topologías de defensa de redes, el uso de cortafuegos y arquitecturas DMZ.

Pautas de elaboración

Para facilitar la realización de esta actividad pueden hacer uso de la máquina virtual de NETinVM, a la que pueden acceder a través del escritorio virtual.

[NETinVM](https://informatica.uv.es/~carlos/docencia/netinvm/index.html) es una herramienta creada por Carlos y David Pérez (a los que agradecemos su amabilidad a la hora de permitirnos utilizarla en esta asignatura), que permite desplegar una topología de red completa dentro de una única máquina virtual tal y como se muestra en el gráfico.

Se recomienda la lectura de la [página de documentación de NETinVM](https://informatica.uv.es/~carlos/docencia/netinvm/netinvm.html) para una mejor comprensión de esta topología.

De cara a esta actividad lo importante es comprender que tenemos una red exterior (10.5.0.0/24) que simula ser **internet,** una **DMZ** (10.5.1.0/24) y una **red interna** (10.5.2.0/24). Las tres se encuentran unidas por un cortafuegos **fw** cuya configuración segura es el objeto de esta práctica. En el gráfico pueden verse los tres interfaces de fw y sus correspondientes direcciones IP **(eth0** con IP **10.5.0.254** interfaz con **internet, eth1** con IP **10.5.1.254** interfaz con **DMZ** y **eth2** con IP **10.5.2.254** interfaz con **red interna).**

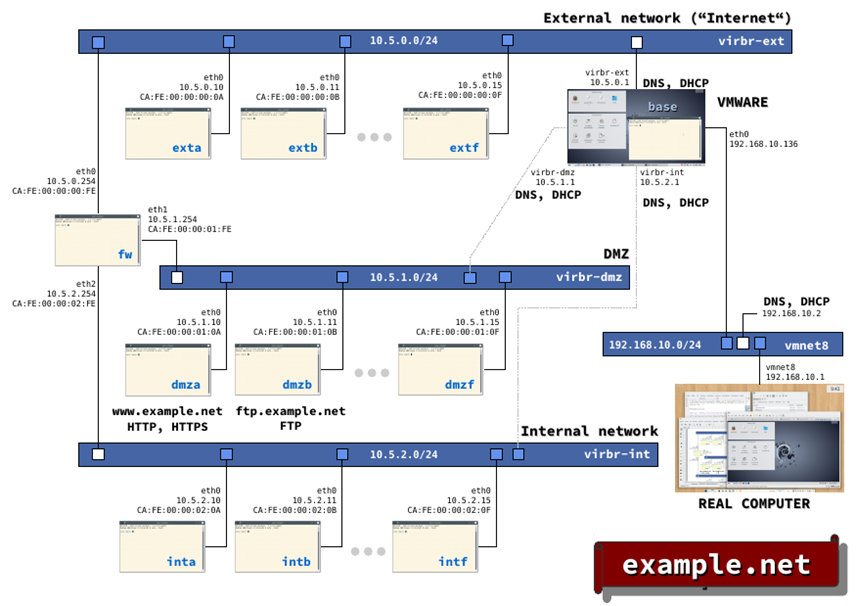


Figura 1. Arquitectura de NETinVM. Fuente: Pérez, C. y Pérez, D. (2018). *Seguridad informática - Introducción a NETinVM.* Universidad de Valencia. <https://informatica.uv.es/~carlos/docencia/netinvm/es/netinvm-intro/netinvm-intro.html>

Además, en cada uno de los segmentos pueden desplegarse diversas máquinas:

* En **internet** se pueden desplegar hasta un total de seis máquinas, que tomaran los nombres desde **exta** hasta **extf** y las IPs **10.5.0.10** hasta la **10.5.0.15.**
* En **DMZ** se pueden desplegar hasta un total de seis máquinas, que tomaran los nombres desde **dmza** hasta **dmzf** y las IPs **10.5.1.10** hasta la **10.5.1.15.** Siendo la primera, **dmza,** un servidor **WEB** y, la segunda, **dmzb,** un **servidor FTP.**
* En **red interna** se pueden desplegar hasta un total de seis máquinas, que tomaran los nombres desde **inta** hasta **intf** y las IPs **10.5.2.10** hasta la **10.5.2.15.**

En la topología que utilizaremos para la práctica desplegaremos cuatro máquinas:

* **fw:** cortafuegos que une todos los segmentos de red.
* **exta:** equipo en internet que nos permite tener una visión desde el exterior de nuestra arquitectura.
* **dmza:** servidor WEB en nuestra DMZ, cuyo acceso gestionaremos desde el cortafuegos.
* **inta:** equipo en la red interna que nos permite tener una visión desde el interior de nuestra arquitectura.

Para establecer esta topología deben asegurarse que la configuración de NETinVM es la adecuada, tal y como se muestra en la siguiente figura. Primero pulsan en el ícono «configure my machines» que tienen en el escritorio de NETinVM. Una vez que hayan pulsado en el ícono se les mostrará un fichero de configuración. En él, las líneas relativas a **fw, exta, inta** y **dmza** deben estar descomentadas para estar activadas (si no lo están deben descomentarlas). Si fuese necesario realizar algún cambio en el fichero, pulsan en «Save» para salvar los cambios y cierran el editor.

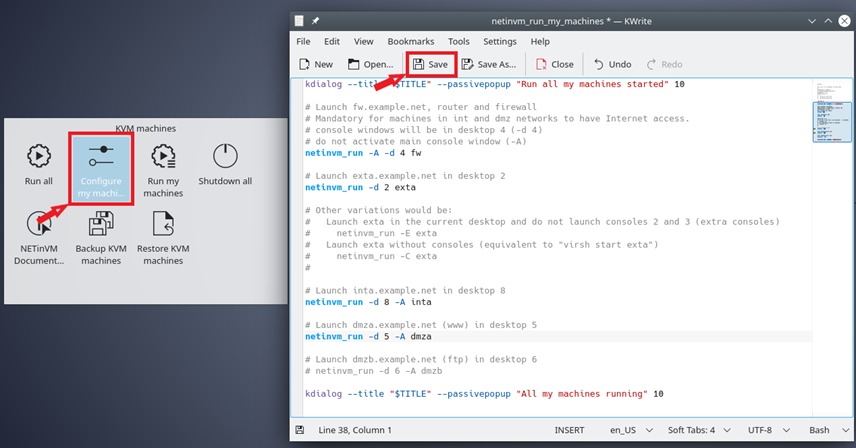


Figura 2. Configuración de NETinVM. Fuente: elaboración propia.

Una vez configurada la topología correctamente tienen que pulsar en el ícono «Run my machines» para crear la red virtual. Tras unos segundos de espera aparecerán diversos terminales que, al cabo de unos segundos más, les permitirán acceder a cada una de las máquinas creadas, tal y como puede verse en la siguiente figura.

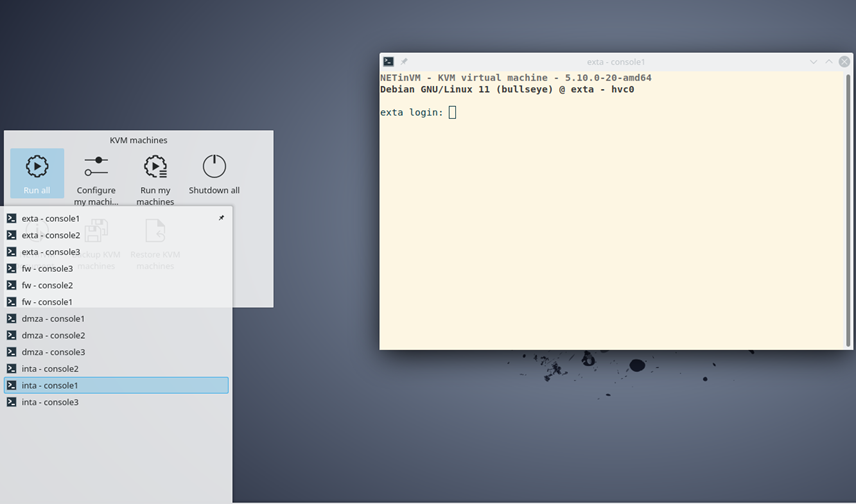


Figura 3. Terminales de acceso a las máquinas. Fuente: elaboración propia.

Las credenciales necesarias para acceder a las máquinas se encuentran en el fichero «passwords.txt» al que pueden acceder desde el escritorio.

Otras herramientas útiles:

Con el objetivo de comprobar que las reglas que les pediremos en la actividad son correctas, pueden hacer uso de algunas herramientas dentro del entorno de NETinVM.

La primera es utilizar el logging de Iptables. Para todas las reglas que crean que puedan crear justo antes una regla idéntica, pero cuya acción en vez de ser «ACCEPT» o «DROP» sea «LOG». De este modo, antes de aceptar o descartar un paquete, Iptables lo ingresara. Por ejemplo, si quisieran ingresar y aceptar todas las comunicaciones que atraviesen el cortafuegos, cuyo puerto destino sea el UDP 53, deberías introducir las siguientes reglas (el orden es importante ya que, si se ejecutase la regla «ACCEPT» primero, la «LOG» nunca llegaría a ejecutarse):

iptables -A FORWARD -p udp --dport 53 -j LOG

iptables -A FORWARD -p udp --dport 53 -j ACCEPT

Observando el fichero «/var/log/kern.log» verán los paquetes ingresados.

La segunda es utilizar el comando netcat, tanto para crear peticiones como para simular servicios (cuando estos no estén desplegados en la arquitectura). La sintaxis de netcat es muy sencilla. Por ejemplo:

* Para crear un servicio que escuche en el puerto 80 TCP: nc -l -p 80.
* Para crear un servicio que escuche en el puerto 53 UDP: nc -lu -p 53.
* Para comunicarse con un servicio que escucha en el puerto 80 TCP: nc [IP o nombre del host] 80.
* Para comunicarse con un servicio que escucha en el puerto 53 UDP: nc -u [IP o nombre del host] 53.

El siguiente gráfico muestra un ejemplo de una comunicación desde inta con el servidor WEB en dmza, y como ver en fw si las reglas que han introducido están siendo ejecutadas.

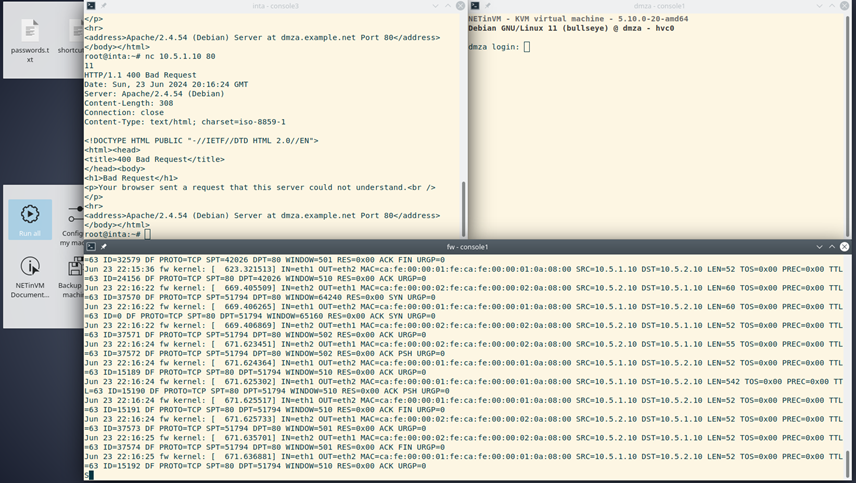


Figura 4. Comunicación con servidor WEB en DMZ desde red local. Fuente: elaboración propia.

En este caso, el servidor WEB ya está establecido en dmza, por lo cual no es necesario simularlo. Desde inta lanzamos netcat, escribimos cualquier secuencia de caracteres, pulsamos «Enter» y el servidor WEB responderá. Usando el comando tail en fw podemos ver cómo van ingresando los paquetes.

Para casos en los que sea necesario comunicarse hacia o desde internet pueden utilizar el equipo exta para recibir o generar tráfico. En el siguiente gráfico se simula un servicio de DNS (UDP) en dicho *host,* al cual se accede desde un equipo en la red local.

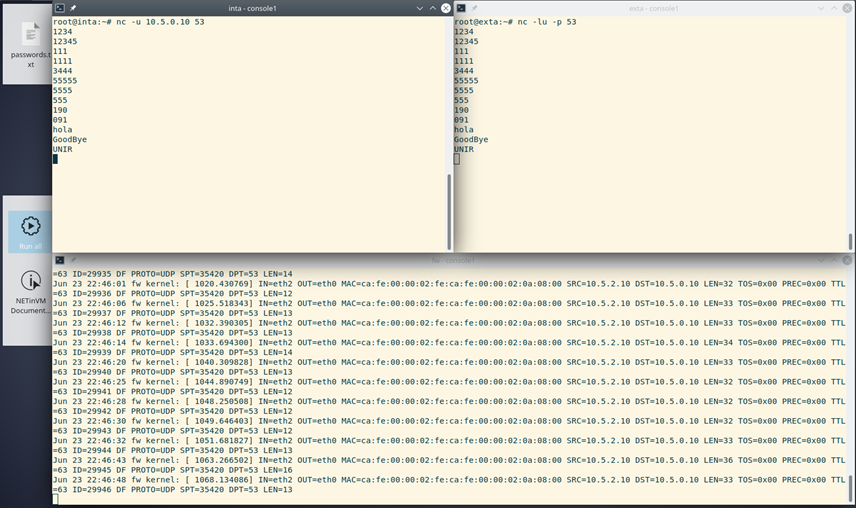


Figura 5. Comunicación con servidor DNS simulado en Internet desde red local. Fuente: elaboración propia.

Una vez tienen acceso a los cuatro equipos y dominan el uso de netcat, llega la hora de llevar a cabo la actividad.

Suena el teléfono y te despiertas sobresaltado. No son horas para recibir una llamada todavía, pero, aun así, el teléfono está sonando. Te acercas a mirar y ves una extensión empresarial. No sabes quién es, pero por la hora parece importante. Respondes.

La empresa Example ha sufrido una brecha de seguridad en su red. Por lo que te cuentan el ataque ya está bajo control, pero quieren evitar que les vuelva a ocurrir en el futuro. Para ello quieren contar con los servicios de un experto en seguridad en redes que les ayude a configurar su red de forma segura. Saben que tú sabes del tema, has estudiado el Máster en Seguridad Informática de la UNIR, y quieren contratarte. No lo dudas y aceptas el reto. Te pegas una ducha rápida y pones rumbo a sus oficinas.

Tras una reunión de apenas una hora tienes una idea clara de la arquitectura y dibujas un gráfico.

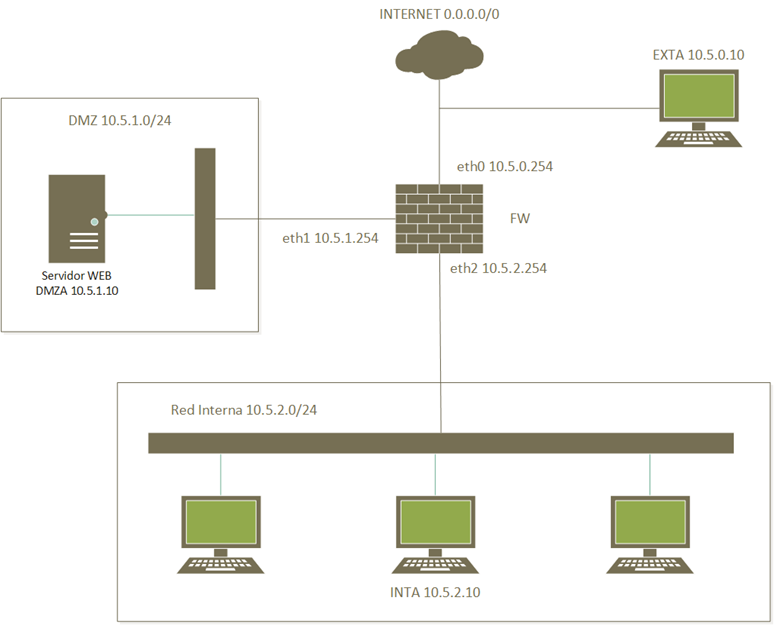


Figura 6. Gráfico de la arquitectura a proteger. Fuente: elaboración propia.

Un cortafuegos FW con tres interfaces interconecta tres segmentos de red: la red interna de la empresa, la DMZ y el acceso a internet. Dentro de la DMZ se encuentra un servidor WEB (DMZA). Además, tienes acceso a uno de los equipos de la red local (INTA) y a otro en internet (EXTA), que te permite tener una visión de la red desde el exterior.

Estudias la topología con calma y te pones manos a la obra:

1. Decides conectarte al cortafuegos como *root* y **listar las reglas de la tabla *filter* en modo «verbose».**
2. El listado te muestra que se permiten demasiadas conexiones. Decides que lo mejor es empezar desde cero y borrar todas las reglas de la tabla *filter.*
3. Además, no todas las cadenas de la tabla *filter* tienen una política restrictiva. Estableces una política restrictiva en la cadena que falta.
4. Una vez que has establecido una base segura, llega el momento de permitir las conexiones necesarias para Example. Lo primero es permitir el tráfico de las conexiones ya establecidas en todas las cadenas de la tabla *filter.*
5. A continuación, lo primero que necesitas es que la red local tenga capacidad de resolución de nombres. Desgraciadamente Example no cuenta con DNS propio, así que seleccionas uno que crees seguro en internet. Permites las nuevas conexiones salientes desde la red local a los servidores DNS (UDP) públicos de Cloudflare (IP: 1.1.1.1 y 1.0.0.1) que se encuentran en internet.
6. Los usuarios de la red local pueden acceder a páginas web de internet, pero de manera indirecta, a través del servidor WEB de la DMZ. Creas una regla que reasigne como destino al servidor WEB de la DMZ todas las nuevas conexiones desde la red local a servidores web seguros en internet.
7. Para completar el punto anterior el servidor WEB debe tener acceso a las webs de internet de forma segura. Creas una regla que permita las nuevas conexiones HTTPS desde el servidor WEB en la DMZ a servidores web de internet.
8. El servidor WEB puede ser administrado solo desde el equipo EXTA, a través de SSH. Creas una regla que permita las nuevas conexiones SSH desde el equipo EXTA al servidor WEB.
9. Example quiere que el cortafuegos pueda descargarse actualizaciones de seguridad de internet. Permites las nuevas conexiones HTTPS y SFTP desde el cortafuegos al servidor de actualizaciones de Debian en España (IP: 82.194.78.250), que se encuentra en internet.
10. Por último, Example quiere desplegar próximamente un servidor de virtualización que acepta peticiones por escritorio remoto (RDP) en su DMZ, con la IP 10.5.1.89, y te pide que dejes el acceso permitido en el cortafuegos para evitar volver a requerir tus servicios. Permites las nuevas conexiones desde la red local al futuro servidor de escritorio remoto (RDP) que se encontrará en la DMZ (10.5.1.89).

Extensión y formato

Ya has configurado el cortafuegos de forma segura, has comprobado que todo sea correcto y crees que has terminado el trabajo, pero no es así. El responsable de seguridad de Example es de la vieja escuela y quiere todas las reglas documentadas.

Además, es muy quisquilloso y solo aceptará la documentación si se la entregas en un formato concreto. Debes rellenar la Tabla 1 solo con las reglas de Iptables que deberían aplicarse en el cortafuegos FW para llevar a cabo las acciones solicitadas, generar un PDF y hacer entrega de este a través de la plataforma facilitada dentro del plazo establecido. ¡Suerte!

Notas:

* Las reglas, siempre que sea posible, deben determinar acción, interfaz, protocolo, dirección IP origen y destino, puertos origen y destino, y el estado de la conexión.
* A pesar de que en el cortafuegos bloqueen todas las conexiones entrantes, todavía pueden acceder a él y al resto de los equipos a través de los terminales provistos ya que estos simulan acceso local, no por red.
* La evaluación de la práctica se llevará a cabo únicamente evaluando la tabla de reglas que entreguen.
* Utilicen los [puertos](https://es.wikipedia.org/wiki/Anexo:Puertos_de_red) conocidos asociados a los protocolos utilizados.

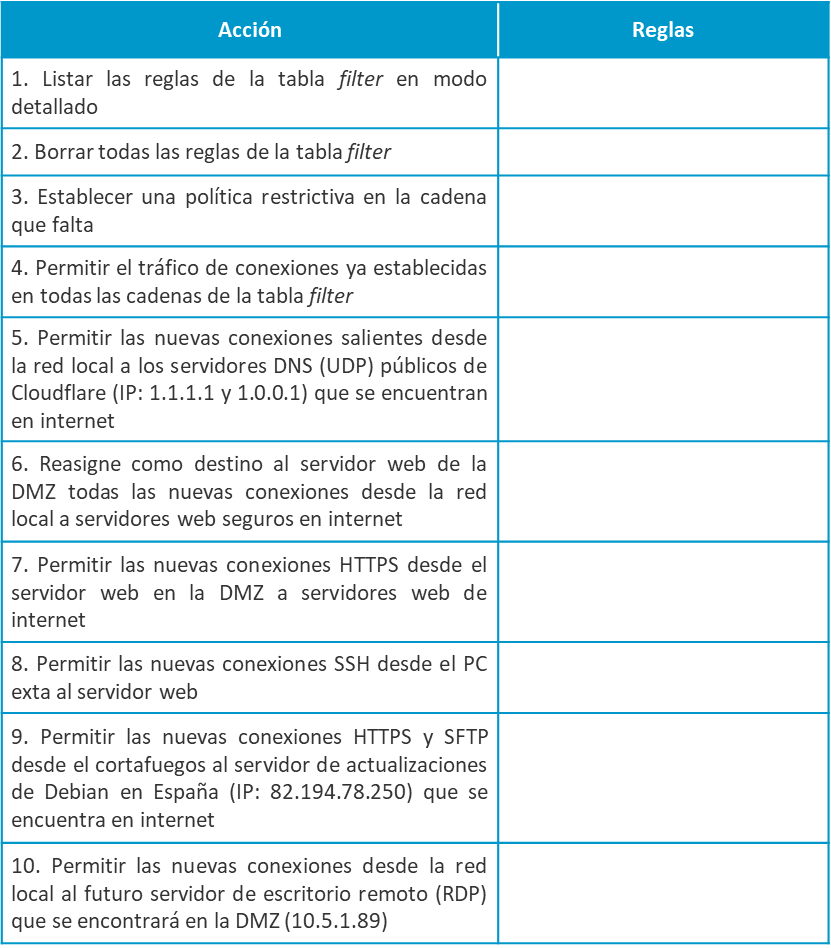


Tabla 1. Reglas Iptables. Fuente: elaboración propia.

Rúbrica

|  |  |  |  |
| --- | --- | --- | --- |
| Mecanismos de defensa en redes | Descripción | Puntuación máxima  (puntos) | Peso  % |
| Criterio 1 | Cada acción vale 1 punto. | 10 | 100 % |
| Criterio 2 | Se resta 0,5 por los fallos en las cadenas y 0,25 por el resto de los fallos u omisiones. |  |  |
| Criterio 3 | Tres o más fallos en una acción hacen que esa acción puntúe 0. |  |  |
|  |  | **10** | **100 %** |