

# Configuración de una DMZ

Sistemas Confiables  
Máster Universitario en Investigación en Ciberseguridad

Octubre 2022

Distributed under: Creative Commons Attribution-ShareAlike 4.0 International



Se pretende construir una DMZ (utilizando contenedores Docker para simular las máquinas) siguiendo la topología de red de la figura 1 y atendiendo los siguientes criterios:

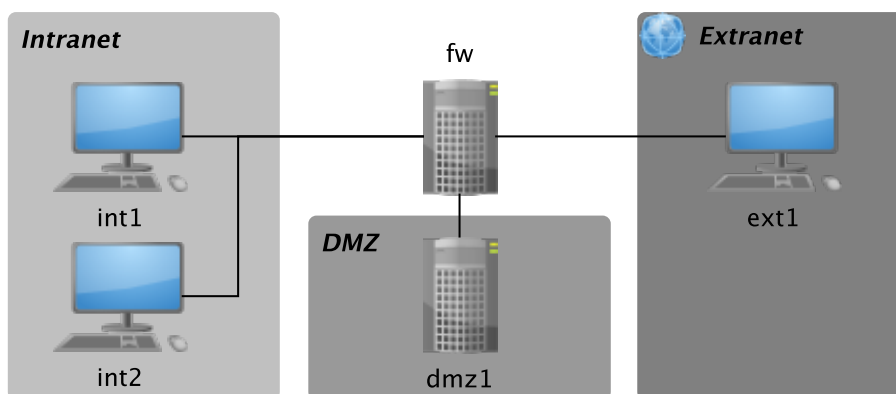


Figura 1: Arquitectura propuesta.

## Entregables

Con respecto a la entrega, han de tenerse en cuenta las siguientes indicaciones generales:

- Es **obligatorio** grabar uno o varios vídeos que permitan visualizar el funcionamiento global del sistema en los términos descritos en cada ejercicio. Las pruebas a realizar están descritas en el guión (etiquetas desde  $T_1$  a  $T_{14}$ ). La duración acumulada de los vídeos no debe exceder los 5 minutos. Si el tamaño del vídeo excede los 50MB será necesario compartirlo con el profesor indicando en el fichero de manifiesto explicado más adelante la url para acceder al mismo.
- La entrega debe contener todos los scripts, ficheros Dockerfile y docker-compose.yml, otros ficheros de configuración, etc., creados o editados en cada ejercicio debidamente etiquetados.
- También se incluirá un fichero de manifiesto (README) indicando los ficheros que conforman la entrega y su contenido. También debe incluir en este archivo la salida de los comandos `ip address` e `ip route` en todas las máquinas. Si es necesario, también pueden incluirse indicaciones para probar la práctica (orden de las mismas, cambios entre pruebas, etc.). En cualquier caso, estas indicaciones deben de ser breves y concisas, se trata de un fichero de manifiesto, **no de una memoria**.

## Pautas generales

Ten en cuenta las siguientes pautas generales antes de empezar a trabajar:

- Para poder ejecutar reglas iptables en el contenedor es necesario instalar los paquetes `iptables`, `iptables-dev` (sólo en Ubuntu 18 o anterior), y `pkg-config`. Además, es necesario iniciar el contenedor con permisos especiales (`--privileged`, o `--cap-add=NET_ADMIN` y `--cap-add=NET_RAW`).
- Para poder ejecutar ping y otros comandos para chequear las comunicaciones es necesario instalar los siguientes paquetes en el contenedor: `net-tools`, `iputils-ping`, `traceroute`, `iproute2`, `tcpdump` y `nmap`.
- La ejecución de las pruebas es secuencial de la  $T_1$  a la  $T_{13}$ . A medida que se ejecutan, hay que ir introduciendo reglas iptables. Para simplificar la ejecución de las pruebas, lo más sencillo es escribir las reglas iptables en scripts y guardarlos en los contenedores que correspondan. Así podrán ser ejecutados en el orden adecuado (desde el propio contenedor con `docker-compose exec`) sin tener que parar, re-build e iniciar de nuevo el contenedor.

## 1. Configuración de *fw*

*fw* contará con tres interfaces de red. Una, con conexión a la red externa (extranet); otra, con conexión a la DMZ; y la última, con conexión a la red interna (intranet).

- La dirección de la toma de red externa será 10.5.0.1. La red externa, que simulará una red WAN, será la subred 10.5.0.0/24.
- La dirección de la toma de red hacia la DMZ será 10.5.1.1. La DMZ será la subred 10.5.1.0/24.
- La dirección de la toma de red interna será 10.5.2.1. La Intranet será la subred 10.5.2.0/24.

### Configuración inicial de las comunicaciones a través de *fw*

*fw* tiene que encaminar todo el tráfico procedente de la Intranet e impedir que cualquier otro tráfico penetre en ella. A su vez, deber permitir conexiones hacia *dmz1* desde cualquier sitio, incluida la intranet. Configura las comunicaciones en *fw* siguiendo las siguientes consideraciones:

- *fw* debe ser capaz de encaminar tráfico, por tanto, es necesario activar el bit de forwarding.
- Cambiar la política por defecto de las cadenas INPUT y FORWARD para que descarten los paquetes.
- Cambiar la política de OUTPUT para que permita pasar todos los paquetes.
- Permitir el tráfico entrante a través de la interfaz de loopback.
- Permitir el tráfico entrante correspondiente a cualquier conexión previamente establecida.
- Permitir consultas entrantes de tipo ICMP ECHO REQUEST.
- Asegúrate que los cambios anteriores persisten en caso de parar y arrancar *fw*. Puedes guardar las reglas en un script que se ejecute al iniciar el contenedor y el valor del bit de forwarding mandado la salida del comando `echo 1` a `/proc/sys/net/ipv4/ip_forward` también al iniciar el contenedor<sup>1</sup>.

Para probar la configuración anterior realiza las siguientes pruebas:

$T_1$  Usando `nmap`<sup>2</sup> en *ext1*, *dmz1* y *int1*, comprueba que *fw* no ofrece ningún acceso desde ninguna de las tres redes (`nmap -sS fw`).

```
1 $ nmap -sS fw
```

$T_2$  Comprobar que *fw* responde a las peticiones ICMP ECHO REQUEST desde las tres redes (ping fw).

```
1 $ ping 10.5.0.1 # desde ext1
2 $ ping 10.5.1.1 # desde DMZ
3 $ ping 10.5.2.1 # desde int1 e int2
```

<sup>1</sup>En realidad, en Docker el bit está activo por defecto, pero para tomar conciencia se pide activarlo explícitamente.

<sup>2</sup>Lo vamos a usar mucho, sería una buena idea que estuviera en las imagenes Docker. Para ello basta añadirlo a la lista de paquetes que se instalan en el Dockerfile.

## 2. Configuración de *ext1*

*ext1* contará con una única interfaz de red conectada a la Extranet. Debe tener instalado un servidor web (apache2) que debe ser accesible desde la Intranet. La dirección de la interfaz de red será fija; en concreto, 10.5.0.20.

## 3. Configuración de *int1* y *int2*

*int1* y *int2* contarán con una única interfaz de red conectada a la Intranet. La dirección de las interfaces de red será fija; en concreto, 10.5.2.20 para *int1*, y 10.5.2.21 para *int2*.

### Comunicaciones desde la red interna

El primer paso es configurar el acceso desde la red interna a la red externa y al resto del mundo. Suponiendo que no se desea restringir demasiado este acceso, se debe permitir el siguiente tráfico a través de la cadena FORWARD:

- Todo el tráfico de conexiones establecidas o relacionadas para los protocolos TCP, UDP e ICMP.
- Todo el tráfico que entre en *fw* a través de la interfaz con la red interna, con protocolo TCP, UDP o ICMP, con dirección IP origen en el rango 10.5.20.0/24, y que vaya a salir a través de la interfaz con la red externa.

Para comprobar la configuración anterior realiza las siguientes pruebas:

*T*<sub>3</sub> Comprueba la conectividad de *int1* con *ext1* mediante ping.

*T*<sub>4</sub> Usando wireshark, tshark, tcpdump o similar<sup>3</sup>; identifica los paquetes intercambiados.

*T*<sub>5</sub> Comprueba la conectividad de *int1* con *ext1* usando SSH.

A continuación, utilizaremos SNAT para ocultar la estructura interna de la red interna. La configuración de SNAT debe cumplir los siguientes requisitos:

- Todos los paquetes que abandonen *fw* por la interfaz externa y que provengan de la red interna (10.5.2.0/24) deben cambiar su IP de origen para que sea la de *fw* en esa interfaz (10.5.0.1).
- Puesto que la IP 10.5.0.1 es fija, es conveniente usar SNAT y no MASQUERADE. El motivo es que así es más eficiente, ya que MASQUERADE debe consultar la IP de la interfaz cada vez que procesa un paquete.

Después de realizar los cambios anteriores, realiza las siguientes pruebas:

*T*<sub>6</sub> Comprueba la conectividad de *int1* con *ext1* usando ping.

*T*<sub>7</sub> Usando Usando wireshark, tshark, tcpdump o similar; identifica los paquetes intercambiados, comprobando que la IP de origen del paquete que llega a *ext1* es la de la interfaz externa de *fw*.

*T*<sub>8</sub> Comprueba la conectividad de *int1* con *ext1* usando SSH.

*T*<sub>9</sub> Comprueba la conectividad HTTP de *int1* con *ext1*:

```
1 $ wget 10.5.0.20
```

## 4. Configuración de *dmz1*

*dmz1* contará con una única interfaz de red conectada a la DMZ. Debe tener instalado un servidor web (apache2) accesible tanto desde la DMZ, como desde la Intranet y la red externa. La dirección de la interfaz de red será fija; en concreto, 10.5.1.20.

---

<sup>3</sup>Puedes instalarlo en las propias máquinas –editando el Dockerfile– o capturar los paquetes desde el sistema anfitrión en la interfaz adecuada

## Comunicaciones en la DMZ

Es necesario agregar reglas para permitir el acceso desde y hacia la DMZ. En particular, es necesario tener en cuenta las siguientes indicaciones generales:

- Los nodos de esta red actúan como nodos bastión y debe limitarse el acceso a ellos tanto desde Internet como desde la red interna. Es necesario permitir el acceso solamente a los servicios que ofrecen y, en su caso, permitir el acceso desde las máquinas de la red interna que tengan tareas administrativas.
- Estos nodos están necesariamente expuestos a ataques desde Internet (pues tienen que ofrecer servicios), por tanto, es necesario proteger a los nodos de la red interna de cualquier tipo de acceso no deseado desde los nodos bastión. De esta forma, en caso de que un nodo bastión sea comprometido, se podrá detectar y tratar el incidente antes de que afecte a la red corporativa.

En nuestro caso, hay que modificar la configuración de *fw* para que permita los siguientes tipos de acceso:

- Acceso TCP desde cualquier máquina (interna o externa) a la máquina *dmz1* (IP 10.5.1.20), exclusivamente al servicio HTTP (puerto 80).
- Acceso SSH desde *int1* (10.5.2.20) a *dmz1*.

Después de realizar los cambios anteriores, realiza las siguientes pruebas:

*T*<sub>10</sub> Comprueba que es posible acceder al servicio HTTP tanto desde la red interna como desde la externa:

```
1 $ wget 10.5.1.20
```

*T*<sub>11</sub> Comprueba, con nmap, que no es posible acceder a ningún puerto más, tanto desde la red interna como desde la externa. En la red interna, prueba desde *int1* e *int2*, ya que desde *int1* sí está permitido el acceso SSH:

```
1 $ nmap -sS 10.5.1.20
```

*T*<sub>12</sub> Comprueba que es posible conectarse por SSH desde *int1* a *dmz1*.

*T*<sub>13</sub> Comprueba que desde *dmz1* no es posible acceder a ningún puerto ni de *int1*, ni de *int2*.

## A. Nuevos servicios (opcional)

Se pide introducir nuevos servicios en la DMZ: primero, habrá que bastionar las conexiones SSH con los equipos de la DMZ; después, habrá que adaptar *dmz1* para que además de servir HTTP, sirva HTTPS; además, se instalara un servidor VPN en una nueva máquina para establecer conexiones con la red interna.

Se recomienda trabajar en dos fases:

1. Para cada uno de los servicios crea una imagen Docker basada en Ubuntu o similar que permita desplegar un contenedor para dar el servicio correspondiente. Puedes probarlo desde el host.
2. Una vez tengas el servicio funcionando, intégralo en el entorno creado con Docker Compose.

### A.1. Hardening de OpenSSH Server

Los servidores OpenSSH de la DMZ tienen que soportar las siguientes funcionalidades:

- El servidor debe escuchar peticiones en el puerto 2222.
- No debe permitirse la conexión con el usuario root. Habrá que crear al menos usuario sin privilegios en el contenedor para establecer las conexiones.
- Se permitirá la autenticación mediante contraseña siempre y cuando esta no sea vacía.
- También se permitirá el login sin contraseña mediante clave pública. Habrá que cargar las claves del usuario/s en el propio contenedor.
- El número máximo de intentos de autenticación será 2.
- Debe mostrarse un banner personalizado con los datos del alumno cuando se establezca una conexión.
- Es necesario implementar al las siguientes medidas de seguridad adicionales.
  - Usar *fail2ban* para detectar ataques de fuerza bruta y bloquear direcciones IP.
  - Se instalará y sistema de autenticación multifactor.

Realiza las pruebas que consideres necesarias para poder visualizar la nueva funcionalidad en el/los vídeo/s.

## A.2. Servicio HTTPS

Modifica la configuración de Apache para poder servir HTTPS. Para probar, crearemos un sitio web de prueba que contenga un fichero html estático con un mensaje, e.g. “¡Hola mundo desde la primera práctica Sistemas Confiables!”.

Realiza la pruebas que consideres necesarias para poder visualizar la nueva funcionalidad en el/los vídeo/s.

## A.3. Servidor VPN

El nuevo servidor se llamará *dmz2* y dará servicios de conexión a una VPN a ext1. Para ello instalaremos un servidor VPN (OpenVPN) atendiendo a las siguientes pautas:

- Los nodos de la red externa podrán establecer conexiones con *dmz1* para conectarse a la misma red que los nodos de la red interna.

Realiza la pruebas que consideres necesarias para poder visualizar la nueva funcionalidad en el/los vídeo/s.