

U-TAD

Redes de Ordenadores

Entrega 2 | v2

Firewall

Autor
Gerardo Escudero López
Ekaitz Arriola Garcia

Asignatura supervisada por
Rafael Socas Gutierrez

December 14, 2020

Índice

Introducción	2
Creación del diseño de la solución mediante un diagrama de red	3
(a) Diseño del diagrama de red	3
Creación de Firewall con iptables	4
(b) Creación de la red	4
(b).1 Descarga de archivos y configuración	4
(b).2 Cambio de hostname	5
(b).3 Configuración manual de los elementos la red	5
(c) Configuración del firewall	7
Conclusiones	7
(d) HTTPS	7
(e) Adaptador de Red	7
(f) UFW	7
(g) IPTABLES	7
Bibliografía	8

Introducción

El objetivo de esta practica es montar la infraestructura de seguridad necesaria por medio de un firewall basado en Linux. Para ello instalaremos un equipo con Linux y se usaran reglas con iptables. Los requisitos son:

- La red local, la Intranet, el direccionamiento debe ser 192.168.20/24.
Los integrantes de esta red deben poder navegar por Internet (tanto http, https, DNS).
Tambien deben acceder a la web de la intranet, aunque para este caso no hace falta usar resolución de nombres por DNS. Esto es, se podrá acceder introduciendo la IP del servidor web en el navegador.
- LA DMZ, con un direccionamiento tal que 192.168.30/24 debe que albergar un servidor Linux con los servicios descritos en el apartado anterior.
Basicamente es un servidor web donde tendremos nuestra página web y que será la web de la empresa, además de un servidor SSH para poder administrar este servidor de forma remota.
- El Firewall hará de frontera entre Internet, la DMZ y nuestra Intranet.
El direccionamiento de Internet puede ser cualquiera. En esta maqueta se simulara una red de Internet con un direccionamiento 192.168.10/24.

Creación del diseño de la solución mediante un diagrama de red

Lo siguiente es un diagrama con la arquitectura física de la red. Para crear dicho diagrama se deberá usar para ello algún programa de diseño de redes y diagramas como puede ser el Visio (o mejor alguna alternativa de software libre).

NOTA

Se deberá indicar en el diagrama los equipos, redes, servicios y direcciones IP, que servirá de guía para implementarlo. Es importante conocer todos los apartados y cuestiones de la implementación para conocer todos los equipos, redes, etc. que tendrá la maqueta.

(a) Diseño del diagrama de red

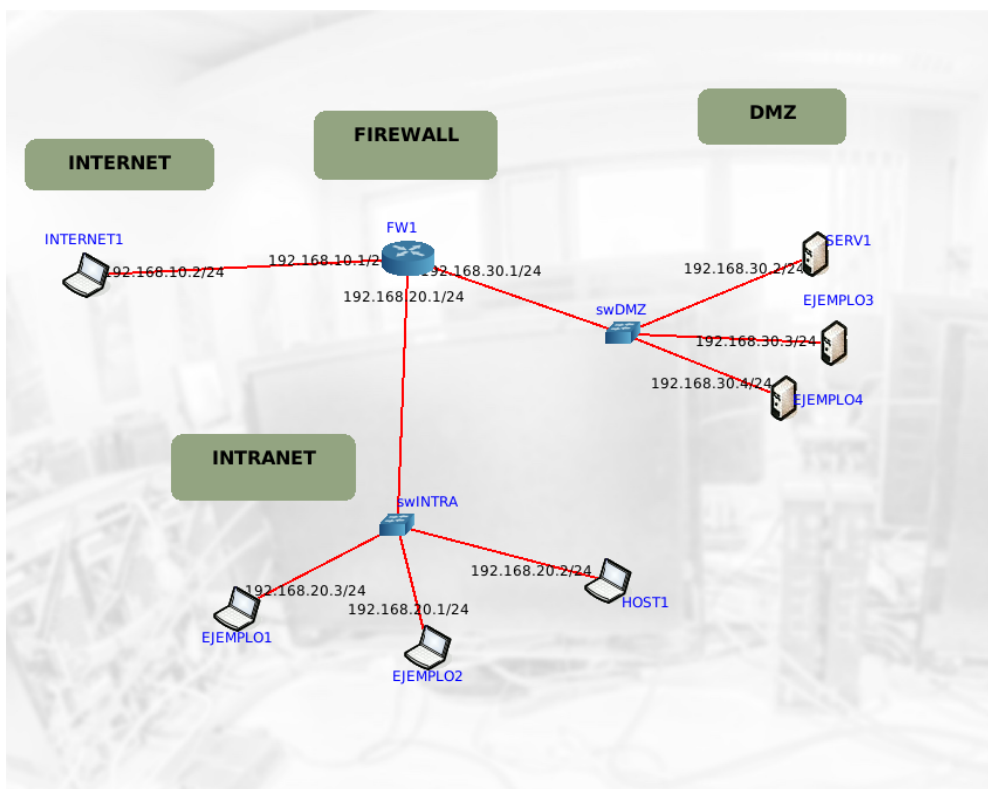


Figure 1: Diagrama Red

La red que se va a crear contiene 2 subredes, ambas conectadas a internet, y entre ellas a través de un firewall. Esto se simulará con 4 máquinas:

1. SERV1

Será donde esté un servidor web, siendo accesible desde cualquier equipo mediante **http** y **https** —los puertos 80 y 443—.

También se podrá gestionar a través de **SSH** desde la INTRANET. Estará en la subred DMZ.

2. HOST-1

Simulará a un empleado de la compañía, por lo tanto, estará en la Intranet. Podrá acceder a cualquier página de internet, así como a la gestión de la DMZ (**SERV1**) mediante SSH.

3. INTERNET-1

Simulará ser una salida a internet. También alojará un servidor **DNS** y web. En cuanto a la conexión con la DMZ, tal como se menciona en la especificación de **SERV1**, solo podrá acceder a ella mediante http y https.

4. FW1

FireWall. Se usará para interconectar dichas redes. Actuará tanto de router como de firewall con sus respectivas iptables, estas con un protocolo de **whitelisting**. Tendrá 3 interfaces de red, dado que se conecta con cada una de las máquinas anteriormente mencionadas.

NOTA

Las máquinas llamadas "EJEMPLO" no serán implementadas, y solo existen para dar a entender que en la red podría haber otros ordenadores sin cambiar el funcionamiento ni el firewall de la misma

Creación de Firewall con iptables

(b) Creación de la red**(b).1 Descarga de archivos y configuración**

Para facilitar el trabajo, se empieza teniendo acceso a internet a través de un adaptador puente para descargar los paquetes/servidores necesarios: SSH, DNS y apache2 (http y https). Después de descargar lo necesario cambiamos la configuración de las máquinas en VirtualBox a red interna.

```
veranono29@INTERNET-1:/etc/bind$ ls
bind.keys  db.255  db.madrid.org  named.conf.default-zones  rndc.key
db.0       db.empty db.Proyecto2.com  named.conf.local          zones.rfc1918
db.127    db.local named.conf      named.conf.options
```

(a) Archivos del DNS

```
veranono29@INTERNET-1:~$ nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-12 19:35 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000053s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
631/tcp   open  ipp
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
veranono29@INTERNET-1:~$
```

(b) Servicios de la máquina **INTERNET-1**

```
veranono29@SERV1:~$ nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-12 19:28 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000061s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
631/tcp   open  ipp
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
veranono29@SERV1:~$
```

(c) Servicios del servidor web **SERV1**

Figure 2: Archivos/servicios necesarios

OTRO MODO DE DESCARGA

Este paso se podría hacer de otra manera para no tener que darle acceso a internet a las máquinas de la DMZ, Este consistiría en separar el disco de esos ordenadores sin internet y asociarlo a algún ordenador que sí que tenga internet. Descargar en ese momento lo que se quiera y volver a asociarlo con la máquina sin internet.

Las instalaciones y posteriores configuraciones (DNS, SSH, apache2...) se cubrieron en las anteriores entregas (DNS, Demonios en Linux), así como en los pdf proporcionados.

Todos los enlaces se encuentran en la bibliografía.

En el DNS se definirá un dominio con dos registros de tipo A.

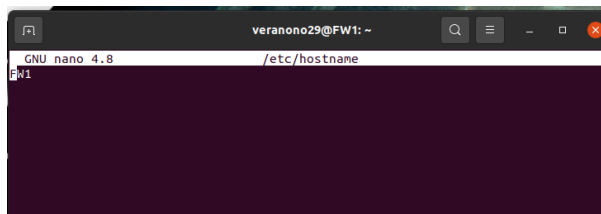
Uno devolverá la IP de la máquina virtual **INTERNET1** y otro la IP del **SERV1**.

(b).2 Cambio de hostname

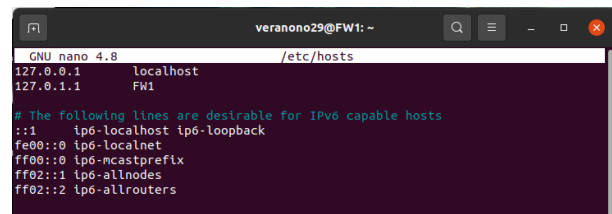
Editando los siguientes archivos subrayados en la imagen (en modo usuario) y reiniciando el dispositivo se cambia el nombre de la máquina.

```
veranono29@INTERNET-1:~$ sudo nano /etc/host
host.conf  hostid  hostname  hosts  hosts.allow  hosts.deny
```

(a) Archivos a editar



(b) Archivo Hostname



(c) Archivo Hosts

Figure 3: Cambio de hostname

(b).3 Configuración manual de los elementos la red

Las **interfaces de red** de la maquina se configuran desde VirtualBox.

En el caso de **FW1**, tendrá 3 interfaces, las cuales tambien serán red interna.

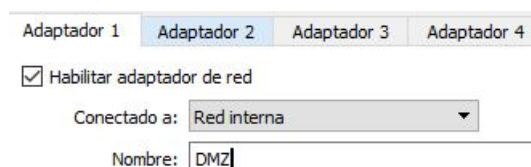


Figure 4: Interfaz de red

Cancelar

Cableada

Aplicar

Detalles

Identidad

IPv4

IPv6

Seguridad

Velocidad de conexión

1000 Mb/s

Dirección IPv4

192.168.10.1

Dirección IPv6

fe80::358a:2d7:2565:e84f

Dirección física

08:00:27:A5:B3:4B

Ruta predeterminada

192.168.20.1

DNS

192.168.10.2

☒ Conectar automáticamente

☒ Hacer disponible para otros usuarios

☐ Conexión medida: tiene límite de datos o puede incurrir en cargos

Las actualizaciones de software y otras descargas grandes no se iniciarán automáticamente.

Eliminar perfil de conexión

Cancelar

Cableada

Aplicar

Detalles

Identidad

IPv4

IPv6

Seguridad

Velocidad de conexión

1000 Mb/s

Dirección IPv4

192.168.20.1

Dirección IPv6

fe80::9fe0:a3b3:88ae:df6

Dirección física

08:00:27:01:8D:DA

Ruta predeterminada

192.168.30.1

DNS

192.168.10.2

☒ Conectar automáticamente

☒ Hacer disponible para otros usuarios

☐ Conexión medida: tiene límite de datos o puede incurrir en cargos

Las actualizaciones de software y otras descargas grandes no se iniciarán automáticamente.

Eliminar perfil de conexión

(a) Firewall (I)

(b) Máquina 1(INTERNET-1)

Cancelar

Cableada

Aplicar

Detalles

Identidad

IPv4

IPv6

Seguridad

Velocidad de conexión

1000 Mb/s

Dirección IPv4

192.168.20.1

Dirección IPv6

fe80::9fe0:a3b3:88ae:df6

Dirección física

08:00:27:01:8D:DA

Ruta predeterminada

192.168.30.1

DNS

192.168.10.2

☒ Conectar automáticamente

☒ Hacer disponible para otros usuarios

☐ Conexión medida: tiene límite de datos o puede incurrir en cargos

Las actualizaciones de software y otras descargas grandes no se iniciarán automáticamente.

Eliminar perfil de conexión

Cancelar

Cableada

Aplicar

Detalles

Identidad

IPv4

IPv6

Seguridad

Velocidad de conexión

1000 Mb/s

Dirección IPv4

192.168.10.2

Dirección IPv6

fe80::8a57:b8e6:1879:17d8

Dirección física

08:00:27:9B:3A:70

Ruta predeterminada

192.168.10.1

DNS

192.168.10.2

☒ Conectar automáticamente

☒ Hacer disponible para otros usuarios

☐ Conexión medida: tiene límite de datos o puede incurrir en cargos

Las actualizaciones de software y otras descargas grandes no se iniciarán automáticamente.

Eliminar perfil de conexión

(c) Firewall (II)

(d) Máquina 2(HOST-1)

Cancelar

Cableada

Aplicar

Detalles

Identidad

IPv4

IPv6

Seguridad

Velocidad de conexión

1000 Mb/s

Dirección IPv4

192.168.20.2

Dirección IPv6

fe80::4a93:3bd6:d119:7569

Dirección física

08:00:27:1B:63:04

Ruta predeterminada

192.168.20.1

DNS

192.168.10.2

☒ Conectar automáticamente

☒ Hacer disponible para otros usuarios

☐ Conexión medida: tiene límite de datos o puede incurrir en cargos

Las actualizaciones de software y otras descargas grandes no se iniciarán automáticamente.

Eliminar perfil de conexión

Cancelar

Cableada

Aplicar

Detalles

Identidad

IPv4

IPv6

Seguridad

Velocidad de conexión

1000 Mb/s

Dirección IPv4

192.168.30.2

Dirección IPv6

fe80::45a8:c47f:1ffa:d590

Dirección física

08:00:27:23:D3:08

Ruta predeterminada

192.168.30.1

DNS

192.168.10.2

☒ Conectar automáticamente

☒ Hacer disponible para otros usuarios

☐ Conexión medida: tiene límite de datos o puede incurrir en cargos

Las actualizaciones de software y otras descargas grandes no se iniciarán automáticamente.

Eliminar perfil de conexión

(e) Firewall (III)

(f) Máquina 3(SERV1)

Figure 5: Configuración manuales

Las IP terminadas en ".1" y ".2" son las que se enlazan entre sí, siendo estas primeras pertenecientes al **FW1** (Firewall), y las segundas a los distintos ordenadores de la red.

La puerta de enlace (Gateway) será la dirección IP correspondiente a la interfaz de **FW1** que esté en esa red. Es la IP del adaptador a través del cual se podrá acceder a otras redes que no son la propia: 192.168.*.1, siendo * el número correspondiente, esto es, 10 para la **salida a internet**, 20 para la **Intranet** y 30 para la **DMZ**.

El DNS está definido en la salida a internet (192.168.10.2). En ella se definió un dominio con dos registros de tipo A. Uno devolverá la IP de la máquina virtual **INTERNET1** y otro la IP del **SERV1**.

La máscara de red será 255.255.255.0 al ser solo los últimos 4 bits para los ordenadores.

(c) Configuración del firewall

Para configurar el firewall utilizamos un modelo basado en iptables, creamos 2 scripts, uno que configura el firewall (firewall.sh) y otro que lo deshabilita (firewallLimpio.sh).

También se incluye en el script el comando para habilitar el firewall como router con el comando **sysctl net.ipv4.ip_forward=1**.

Los scripts están comentados, y la información sobre el funcionamiento de estos se encuentran en los pdf proporcionados.

Los scripts están en el repositorio github.

Conclusiones

(d) HTTPS

Los permisos. Cuando se descarga la clave de https, pide introducir la IP, pero no hay que poner la actual, sino la que tendrá una vez se le quite el acceso a internet y se introduzca en la DMZ

(e) Adaptador de Red

Una vez que configuras todo tienes que apagar el adaptador y volver a encenderlo para actualizar la configuración. Esto nos lió un rato ya que no se conectaba con el FW y pensábamos que el problema estaba en el firewall.

(f) UFW

En un punto estuvimos mirando que era y al ser una capa de abstracción por encima de las iptables, entraba en conflicto con las modificaciones que hacíamos en las iptables a mano. AL final, usamos el comando "sudo ufw disable" para que se apagase y no se mantuvieran las reglas al encender el ordenador. Después de reiniciarlo, volvimos a ejecutar el script y todo volvió a ir bien.

(g) IPTABLES

Mientras configurábamos las reglas, creamos también un script para limpiar todas las reglas.

Índice de figuras

1	Diagrama Red	3
2	Archivos/servicios necesarios	4
3	Cambio de hostname	5
4	Interfaz de red	5
5	Configuración manuales	6

Bibliografía

- [1] Configurar https
- [2] Primera practica | DNS
- [3] Primera practica | Demonios en linux
- [4] Instalacion y configuracion de bind9
- [5] PDF informativos sobre el funcionamiento de los iptables y otras configuraciones