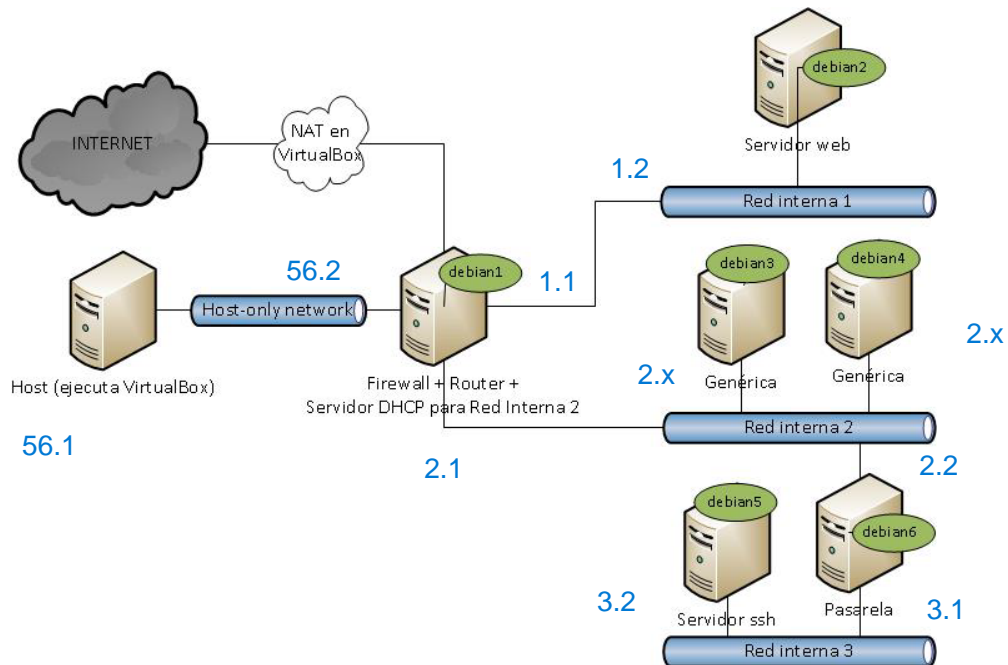


Grado en Ingeniería Informática. Administración de sistemas 2022/2023

Trabajo práctico final

El objetivo del trabajo es la instalación y configuración del sistema cuyo esquema se muestra a continuación, todo ello virtualizado en el entorno VirtualBox:



Especificaciones:

- 1) Todas las máquinas deben correr el sistema operativo que se indica en el anexo. **MUY IMPORTANTE: ES OBLIGATORIO QUE LAS MAQUINAS DERIVEN DE LA ESPECIFICADA. EN CASO CONTRARIO LA PRACTICA NO SE EVALUARÁ (NO PRESENTADO).**
- 2) En la máquina *debian1* se debe conservar el interface por defecto (*enp0s3*) de tipo *NAT*. Esta conexión se utilizará para acceder a Internet, y así poder descargar el software necesario para las máquinas. Su uso será ese exclusivamente. En el resto de máquinas no deben usarse interfaces tipo *NAT* de VirtualBox; deben tener solamente definidos en VirtualBox los interfaces necesarios en cada caso, de acuerdo con el esquema mostrado.
- 3) Todas las máquinas deben tener IPs estáticas, excepto *debian3* y *debian4*.
- 4) En la máquina *debian1* se debe instalar y configurar adecuadamente un servidor DHCP para la "Red Interna 2". Dicho servidor será utilizado por las máquinas *debian3* y *debian4*.
- 5) Se debe configurar la máquina *debian1* para actuar como router (con rutas estáticas), de forma que se pueda alcanzar la "Red interna 3" desde cualquier punto del sistema.
- 6) En la máquina *debian5* se debe instalar y configurar adecuadamente un servidor *ssh*.
- 7) En la máquina *debian2* se debe instalar y configurar adecuadamente un servidor web (*nginx* o *apache*). No es necesario poner contenido, simplemente que se muestre la página principal por defecto de la instalación, para comprobar su correcto funcionamiento.

- 8) La máquina *debian1* actuará como firewall. Consideraremos que separa nuestra intranet (que estará formada por las tres redes internas) de la extranet (la red "*Host only network*", el host e Internet en general). El firewall debe:
 - a. Permitir todo el tráfico intranet, y todo el tráfico de salida (hacia el *Host* e Internet).
 - b. Debe prohibir todo el tráfico desde la extranet a la intranet salvo el generado por las conexiones al servidor web en *debian2* y al servidor ssh en *debian5*. Es decir, las páginas web del servidor deben ser accesibles desde la máquina *Host*, y se debe poder conectar vía *ssh* al servidor *debian5* desde *Host*.
 - c. La máquina *debian1* (el firewall) debe contestar a los pings generados en la intranet, pero no a los generados desde la máquina *Host*.
- 9) Todo el tráfico hacia la extranet (hacia la red "*Host only network*") desde la intranet tiene que utilizar como IP origen la dirección pública del firewall (la del interface de *Debian1* a "*Host only network*") con independencia del nodo de origen.
- 10) Todo el tráfico desde la extranet (desde la red "*Host only network*") hacia la intranet tiene que utilizar como IP destino la dirección pública del firewall (la del interface de *Debian1* a "*Host only network*") con independencia del nodo de destino.
- 11) Todo debe ponerse en funcionamiento automáticamente al rebotar las máquinas; es decir, los servicios deben arrancar automáticamente, las reglas del firewall deben aplicarse en el arranque, las rutas estáticas ídem, etc.

Se debe realizar una **breve** memoria de lo realizado (en texto, no pdf, no Word...), que se entregará siguiendo el procedimiento habitual, incluyendo aspectos tales como:

- Software instalado y como se ha instalado
- Configuración del software: cambios en los ficheros de configuración...
- Decisiones de administrador que se han tomado: direcciones de las subredes y equipos, decisiones en la configuración del servidor DHCP...
- Cualquier cosa adicional que consideréis oportuna.
- **Pensad que la memoria debería ser como una guía paso a paso de lo que debe hacer para lograr el mismo resultado partiendo de cero, con comentarios y aclaraciones adicionales cuando sea necesario.**

En la evaluación de la práctica, que será presencial, se requerirá el sistema diseñado funcionando. Su no presentación supone la no presentación de la práctica. Se permitirá la presentación utilizando un portátil propio, o bien en una máquina del laboratorio.

Autoevaluación:

- Todas las máquinas *debianX* deben verse entre sí mediante ping, y deben ver a *Host* (pero *Host* no las verá mediante ping).
- Todas las máquinas *debianX* se deben poder conectar a Internet (a través de *debian1*).
- Todas las máquinas (incluida *Host*) deben poder conectarse al servidor *ssh* en *debian5*.
- Desde *Host*, con un navegador se debe poder conectar al servidor web en *debian1*, y verse la página web que se instala por defecto, o la que se ponga.

Notas:

- Resulta útil cambiar el nombre de las máquinas, para distinguirlas mejor (el nombre sale en el prompt). Nombrarlas como en el enunciado.
- Buscar el software necesario, leer la documentación de configuración.
- La máquina debian1 debe realizar labores de *firewall*, *NAT* y *port forwarding*. Utilizar *iptables* para implementar dicha funcionalidad.
- El orden en el que se han escrito las especificaciones anteriores no es necesariamente el que se ha de seguir, ni siquiera tiene por ser el mejor.
- Es objetivo del trabajo ser capaz de buscar, estudiar e interpretar correctamente la documentación técnica necesaria. Esto es especialmente importante en el caso de *iptables*.

ANEXO

Las máquinas utilizadas deben derivar de la imagen:

<https://cloud.unizar.es/index.php/s/KiiX7H2QJQfbk44>

ATENCIÓN: Es una versión modificada de debian 11, que sustituye nftables por iptables.

La máquina virtual cuenta con dos usuarios definidos: root (password toor) y as (password as). Este último dispone de privilegios de administración mediante sudo.

Para realizar este trabajo práctico, y ya que se deben ejecutar simultáneamente 6 máquinas virtuales, hay que tener en cuenta que el espacio de disco necesario será muy grande si se crean máquinas virtuales completas. Para evitarlo, se pueden emplear dos aproximaciones distintas:

- 1) **[Opción preferida]** Utilizar un disco multiconexión. Para ello se crea una máquina completa (importar el fichero as_base.ova), y a continuación, estando parada, se ejecuta el “administrador de medios virtuales” del menú archivo, desde el que se debe **liberar el disco** de dicha máquina, y **modificarlo a tipo “multiconexión”**. A partir de este momento tenemos un disco base que podemos usar para crear muchas máquinas virtuales usando poco espacio, ya que solo se guardan los cambios de cada máquina respecto a ese disco base que es “inmutable”, nunca cambia. Al crear las máquinas (debian1 a debian6), elegir la opción “Usar un archivo de disco duro virtual existente”, y seleccionar el archivo .vdi de la máquina base. (La “máquina base” ya no funcionará porque ya no tiene disco asociado, la podéis borrar del entorno VirtualBox, pero solo la máquina, no los archivos).
- 2) Crear una máquina completa como en el caso anterior, y a partir de esa primera máquina virtual completa crear clones diferenciales (la opción al clonar es “clonación enlazada”). En esta aproximación lo ideal sería no ejecutar nunca esa máquina originaria, y crear 6 clones diferenciales (máquinas debian1 a debian6).