**Topologia de red Corporativa, Configuracion de Servicios y Seguridad**

**Laboratorio: Cisco GNS3, Virtual Box, DNS, Firewall, Oracle DB, Serv Aplicaiones, Apache Proxy Inverso con Balanceo, DHCP**

Contenido

[Objetivos 2](#_Toc127580871)

[Dudas abiertas 3](#_Toc127580872)

[Topología deseada 4](#_Toc127580873)

[Instalación entorno GNS3 4](#_Toc127580874)

[Instalación Virtual Box 4](#_Toc127580875)

[Instalación de máquinas virtuales 4](#_Toc127580876)

[Construcción de la topología sobre GNS3 5](#_Toc127580877)

[Configuración lógica red - IPv4 5](#_Toc127580878)

[Configuración del servicio DHCP para la intranet 7](#_Toc127580879)

[Configuración del enrutamiento 7](#_Toc127580880)

[Configuración de servicios públicos 7](#_Toc127580881)

[Configuración de servicios MZ 7](#_Toc127580882)

[Configuración de servicios privados 7](#_Toc127580883)

[Configuración de seguridad 7](#_Toc127580884)

[Configuración vigilancia 7](#_Toc127580885)

[Comprobación seguridad 8](#_Toc127580886)

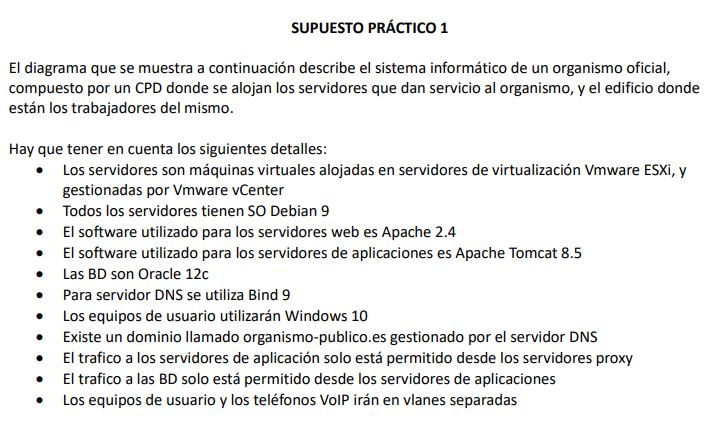
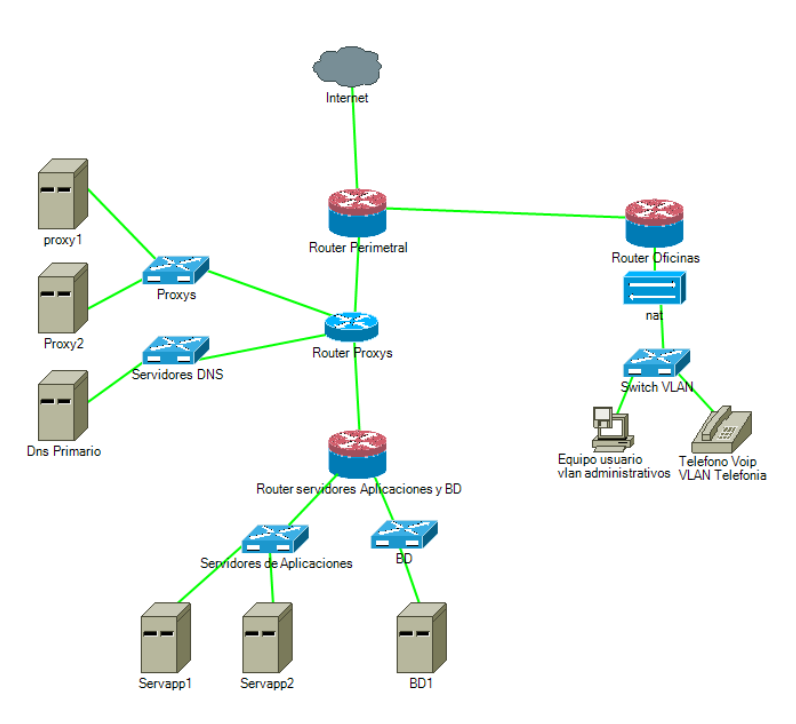
[Referencias: 8](#_Toc127580887)

# Objetivos

El objetivo del laboratorio surge del supuesto práctico 1 del proceso de oposición y examen Analista Aplicaciones CARM 2021.

El objetivo es construir mediante virtualización un escenario, en el que poder probar, configurar y experimentar con los objetivos propuestos, problemas de configuración que pudieran aparecer, problemas de seguridad, aclarar conceptos teóricos y prácticos sobre el laboratorio de formación.

Una vez guardado el laboratorio, podrá ser almacenado e importado en futuros periodos de prueba, entrenamiento o ensayo partiendo de un escenario ya montado en el que poder practicar con las distintas distribuciones de sistemas y diferentes ‘dialectos’ o mecanismos de configuración en IT.



# Dudas abiertas

Tras un primer esbozo de la solución, me surgen algunas dudas:

* ¿Tiene sentido exponer tanto la DMZ y los servicios con direccionamiento público? Aunque dispongamos de FW1 para filtrar que puertos y tipos de conexiones se dejar pasar y en los servidores destino que conexiones aceptar.
  + Se están exponiendo los servicios de HTTPs Apache Proxy Inverso – Balanceo (redirección internamente a los servidores de aplicaciones en la MZ)
  + Se está exponiendo también el DNS, entiendo que no sería nuestro AD corporativo.
  + Se están exponiendo las IPs de los routers y equipos de la DMZ. Todo esto estaría filtrado por IP destino y todos los puertos, ping/tracert incluido.
* En caso de tener un dominio de correo corporativo, ¿Quién es el responsable de su gestión?
  + En los DNS bajo la INNA existirá el registro MX para el dominio ‘@miorg.es’ que apunte a la IP publica de nuestro DNS para la resolución recursiva.
  + Los users ‘pepe@miorg.es’ seremos los responsables de resolverlos.
  + A nivel de infraestructura de correo, donde esta nuestro MDA (Mail Delivery Agent). Sería una instalación de un servidor exchange interno, al que se apunta. ¿La tendencia actual es delegarlo en la nube como un SAAS y que se encargue Microsoft de nuestro correo?
* En nuestro PEER de internet el enrutamiento que deben configurar para todo nuestro trafico seria:
  + Todo tráfico con destino a 220.15.10.0/24 llegara por la dirección 220.15.10.209 (es la IP exterior de nuestra organización y la que he elegido para el mejor aprovechamiento de direcciones y subredes del rango publico C).

# Hardware

Laptop:

CPU:

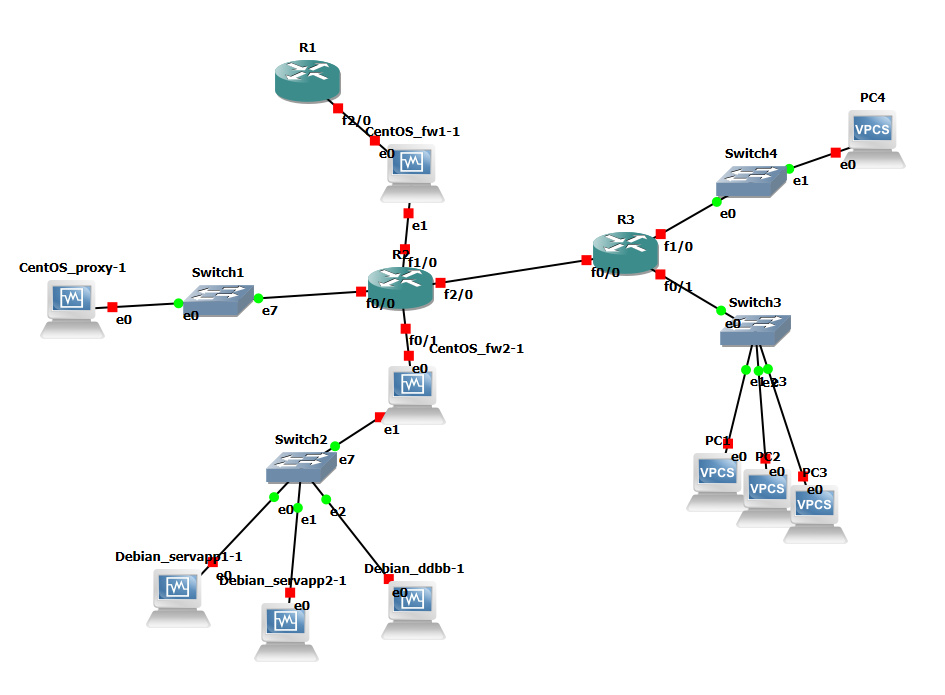
Memoria:

Monitor adicional:

USB 3.0 Externo SSD 480GB

# Topología deseada

Se desea recrear una topología como la figura, con la implementación de red, seguridad y servicios.



# Instalación GNS3

* Importar imágenes de routers cisco
  + Configurar el IDLE-PC para cada modelo de router configurado (para asi minimizar de consumo de CPU de los routers virtualizados).
  + Instalar los paquetes de red: ncap, … ¿?

# Instalación Virtual Box

Para correr los servidores

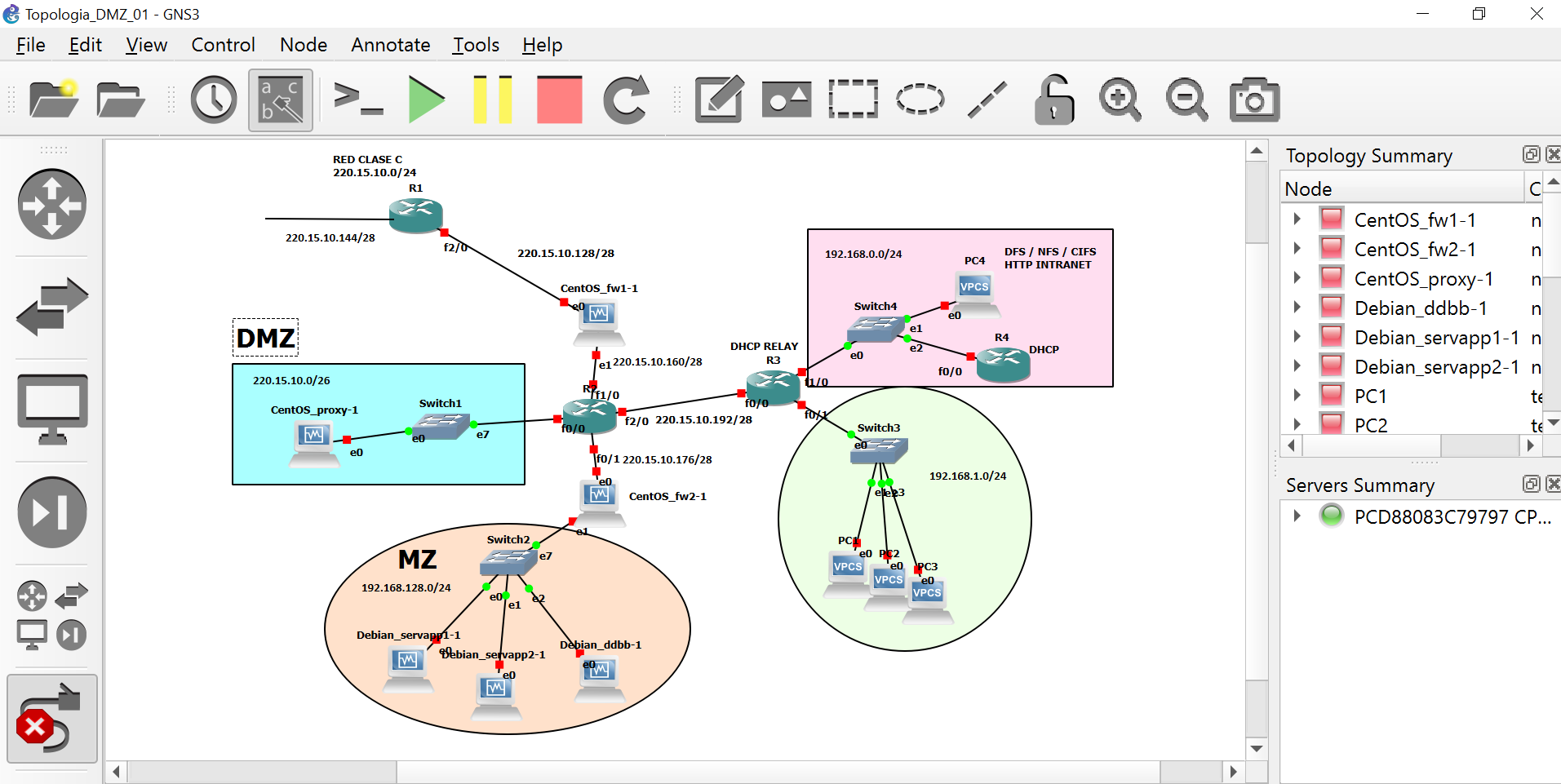
# Instalación Máquinas Virtuales

Usamos esta distribución de máquinas con estos objetivos.

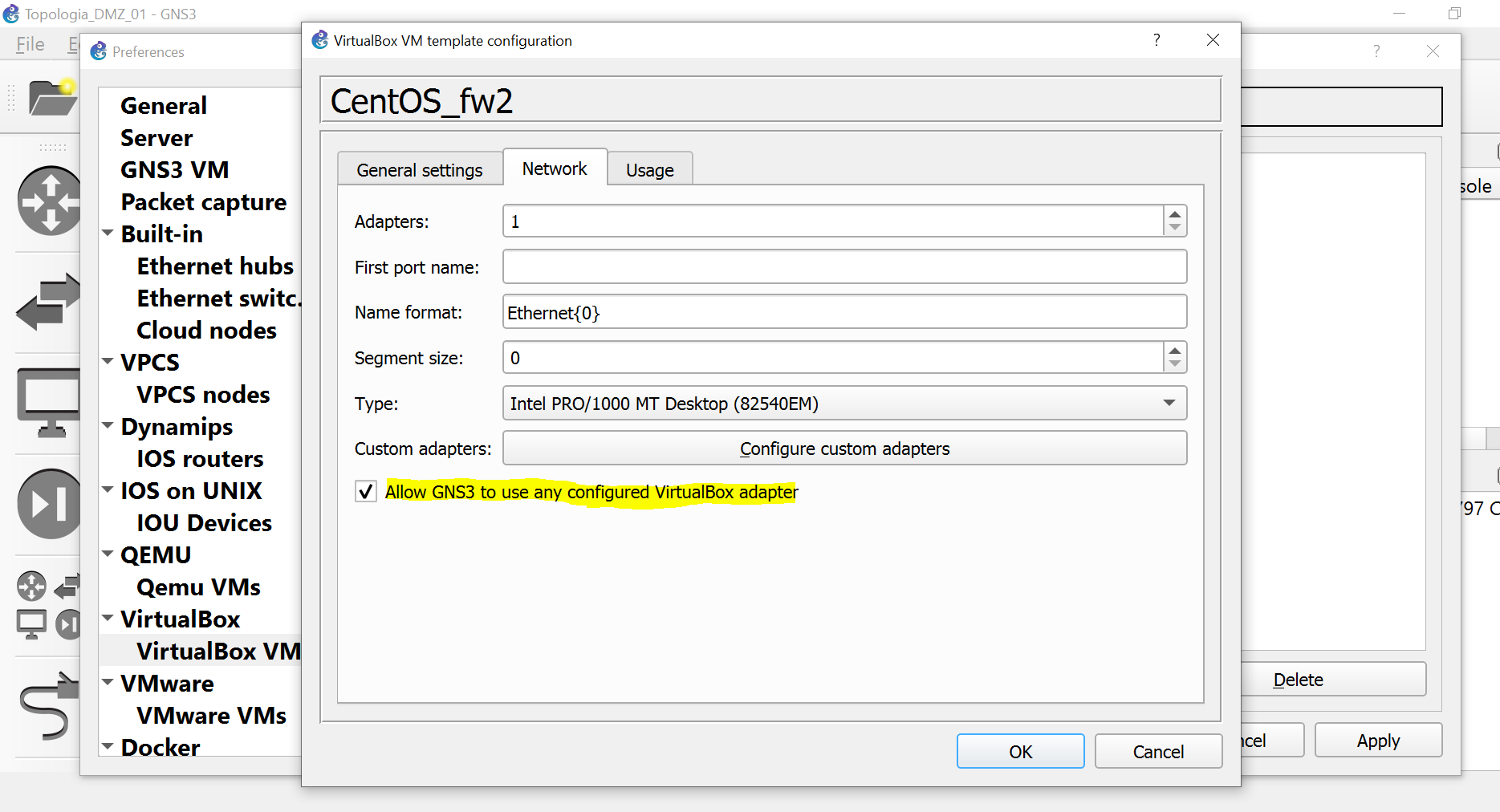
* CentOS\_proxy: apache Proxy Inverso APACHE
* CentOS\_fw1: firewall
* CentOS\_fw2: firewall
* Debian\_servapp1: servidor aplicaciones TOMCAT
* Debian\_servapp2: servidor aplicaciones TOMCAT (HA – respaldo)
* CentOS\_ddbb: Oracle DB
* Win2019\_dns: DNS
* VirtualPC: equipos terminal de usuarios
* **CentOS**: distribución basada en REDHAT una de las grandes familias de distribuciones Linux. Fedora, RedHAT, son distribuciones compatibles.
* **Debían**: otra de las distribuciones más propagadas de Linux. Ubuntu,
* Instalar las maquina reservando los adaptadores de red que vayan a utilizarse en la topología, y añadir un interfaz de red extra en modo NAT contra el equipo anfitrión, para que pueda descargarse software de internet a través de esta interfaz.
* Instalar versiones en modo texto para minimizar el consumo de recurso, disco, memoria, cpu, I/O, sobre el equipo anfitrión.

# Topología Física sobre GNS3

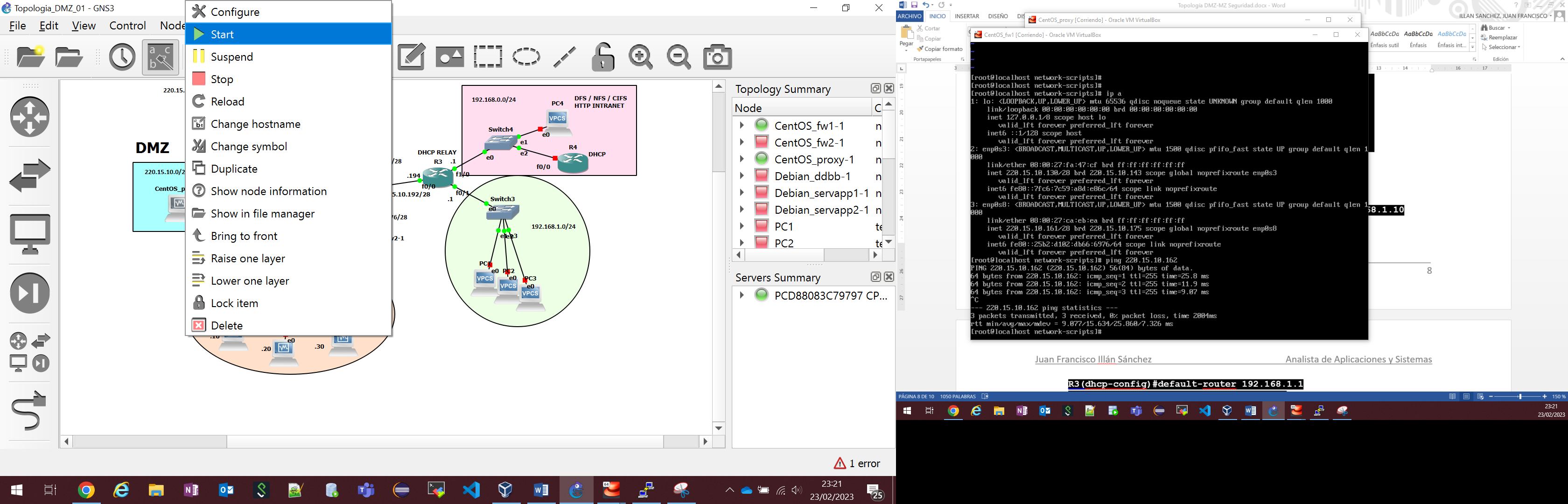
Construimos sobre GNS3 la topología de red y vinculamos con las máquinas de VirtualBox para que estén dentro de la misma topología.



Importar las maquinas en GNS3 y permitir que GNS3 configure el adaptador de red de las maquinas VirtualBox que van a utilizar en la topología (los que hemos reservado). Si la maquina tiene más de 1 interfaz, hacerlo para todos los adaptadores.



Arrancamos los servidores y los routers de uno en uno para un arranque “suave” de al infraestructura sobre el host anfitrión.



# Configuración Lógica de la red - IPv4

Tenemos una **Clase C Publica 220.15.10.0/24** sobre la que ofreceremos servicios públicos y enrutables desde internet sin redirección de puertos en el router frontera del ISP.

Creamos las subredes 220.15.10.0/24 aplicando VLSM:

60 IPs para DMZ de servicios públicos en internet 🡪 2^6 = 64 IPs

**220.15.10.00HHHHHH**

**220.15.10.0/26**

**255.255.255.192**

60 IPs Reservadas 🡪 2^6 = 64 IPs

**220.15.10.01HHHHHH**

**220.15.10.64/26**

**255.255.255.240**

10 IPs para Enlace entre R1 y FW1 🡪 2^4 = 16 IPs

**220.15.10.1000HHHH**

**220.15.10.128/28**

10 IPs para Enlace entre R1 e ISP 🡪 2^4 = 16 IPs

**220.15.10.1001HHHH**

**220.15.10.144/28**

10 IPs para Enlace entre FW1 y R2 🡪 2^4 = 16 IPs

**220.15.10.1010HHHH**

**220.15.10.160/28**

10 IPs para Enlace entre R2 y Fw2 🡪 2^4 = 16 IPs

**220.15.10.1011HHHH**

**220.15.10.176/28**

10 IPs para Enlace entre R2 y R3 🡪 2^4 = 16 IPs

**220.15.10.1100HHHH**

**220.15.10.192/28**

Para el resto de subredes utilizaremos direccionamiento privado IPv4 de clase C

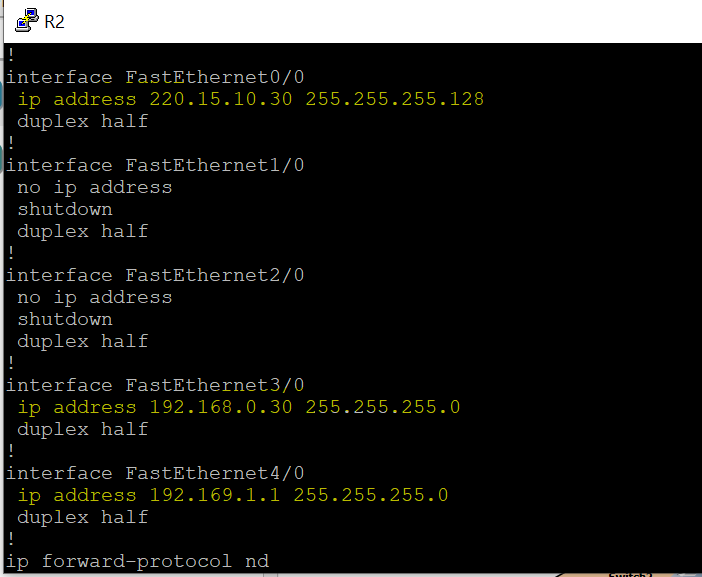
192.168.0.0/24 para la red de servicios de la intranet

192.168.1.0/24 para intranet de usuarios

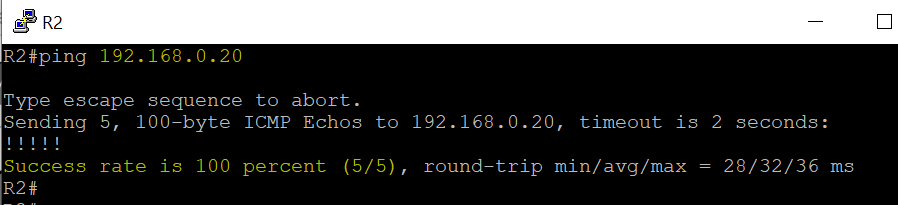
192.168.128.0/24 para la MZ de servicios y bbdd

## Configuración Equipos de RED (Routers)

Configuramos en todos los equipos router y terminales las direcciones asignadas de forma estática.



Comprobamos algunos ping entre interfaces directamente conectadas.



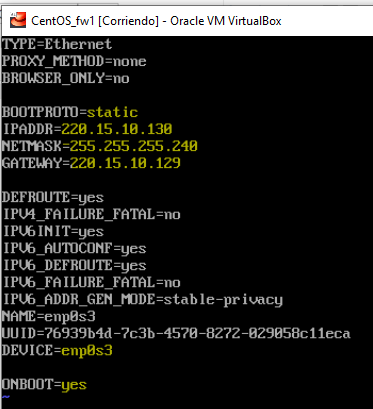
## Configuración Equipos CentOS

Configuramos los equipos de la familia RedHAT configuran las interfaces de red en scripts de configuración:

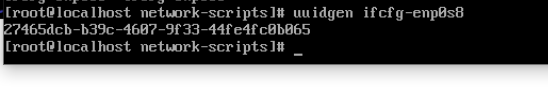
/etc/sysconfig/network-script/ifcfg-enp0s3

/etc/sysconfig/network-script/ifcfg-enp0s8

Realizamos la configuración con IPs staticas.



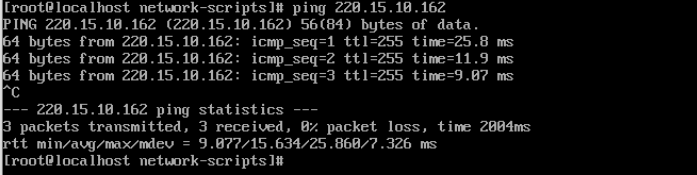
Si tenemos que instalar un nuevo adaptador y no nos ha generado los ficheros de configuración en la instalación del sistema, copiamos uno y modificamos los datos de conexión, el nombre DEVICE/NAME del adaptador, y le generamos un nuevo UUID de dispositivo.



Reiniciamos el servicio de red:

systemctl restart network (gestión servicios SystemD)

Según vamos configurando equipos y redes vamos comprobando la conectividad



## Configuración Equipos Debían

# Configuración del servicio DHCP para la intranet de usuarios

Configuramos en R3

**R3(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10**

**R3(config)#ip dhcp pool DHCP\_INTRANET\_USERS**

**R3(dhcp-config)#network 192.168.1.0 255.255.255.0**

**R3(dhcp-config)#default-router 192.168.1.1**

**R3(dhcp-config)#dns-server 220.15.10.50**

[**https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/**](https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/)

[**http://librosnetworking.blogspot.com/2013/02/configuracion-de-dhcp-relay.html**](http://librosnetworking.blogspot.com/2013/02/configuracion-de-dhcp-relay.html)

# Configuración del enrutamiento

To make the route permament, you need to create a static route configuration file. Create a file with the name route-interface in /etc/sysconfig/network-scripts, such as:

/etc/sysconfig/network-scripts/route-eth0

Then, add the same line you would with ip route add:

172.16.5.0/24 via 10.0.0.101 dev eth0

Make sure to restart your network settings so they take effect:

service network restart

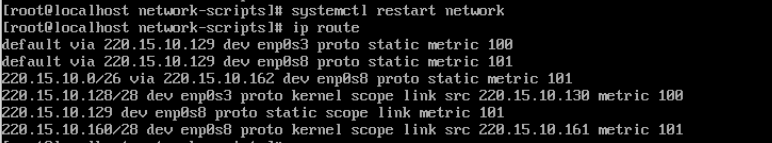
If you lose your internet connection

If you suddenly cannot connect to the internet after adding a static route and are using static IPs (as opposed to DHCP), you may not have your default gateway configured correctly. Add it to your /etc/sysconfig/network file:

nano /etc/sysconfig/network

GATEWAY=10.0.0.1





# Configuración de servicios públicos

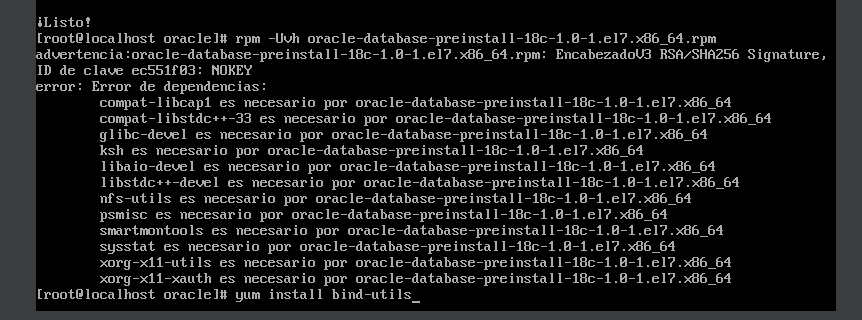
## Apache ProxyBalancer

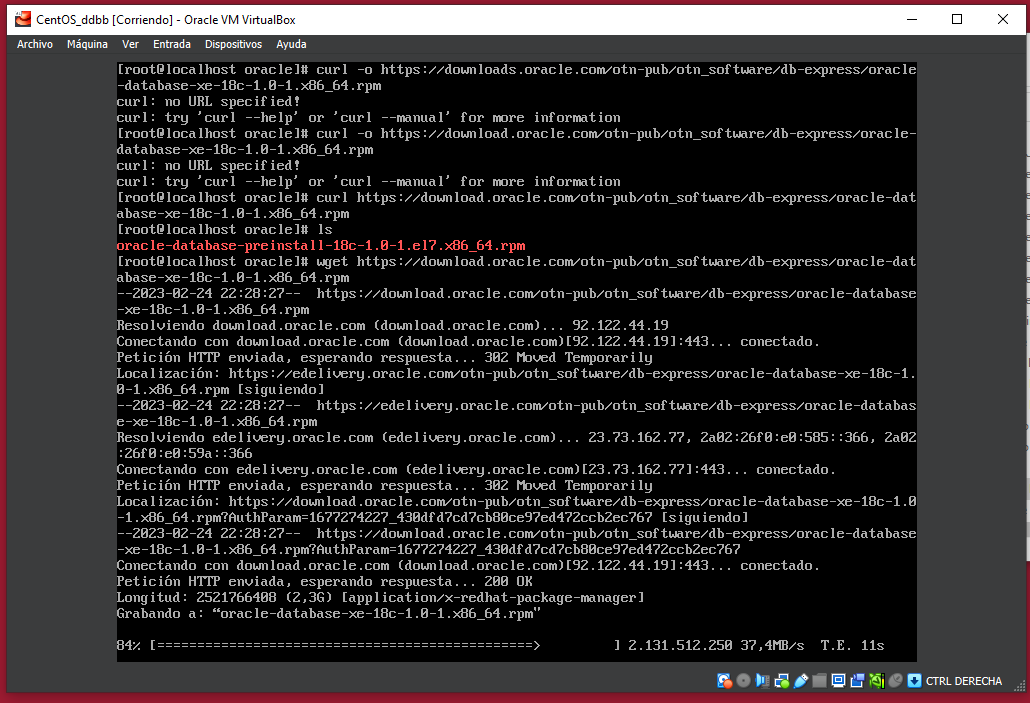
## DNS

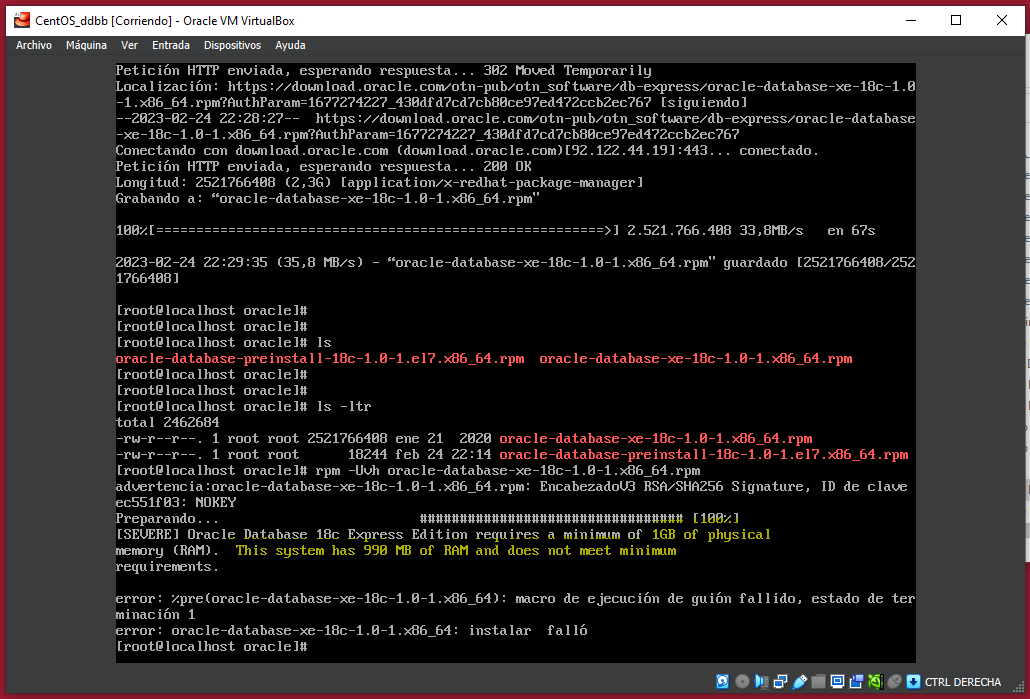
# Configuración de servicios MZ

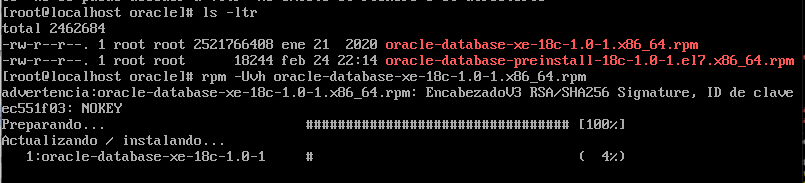
## Oracle DB

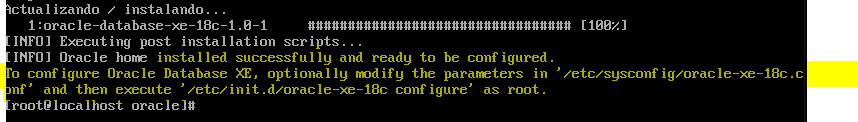
<https://tutorialesit.com/linux-instalacion-oracle-18c-xe-en-centos-8-mediante-consola/>







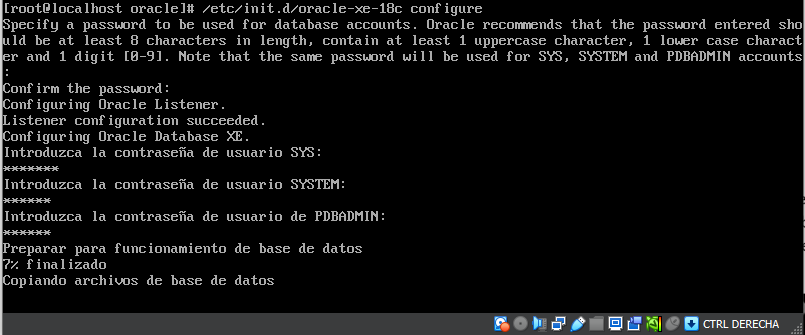


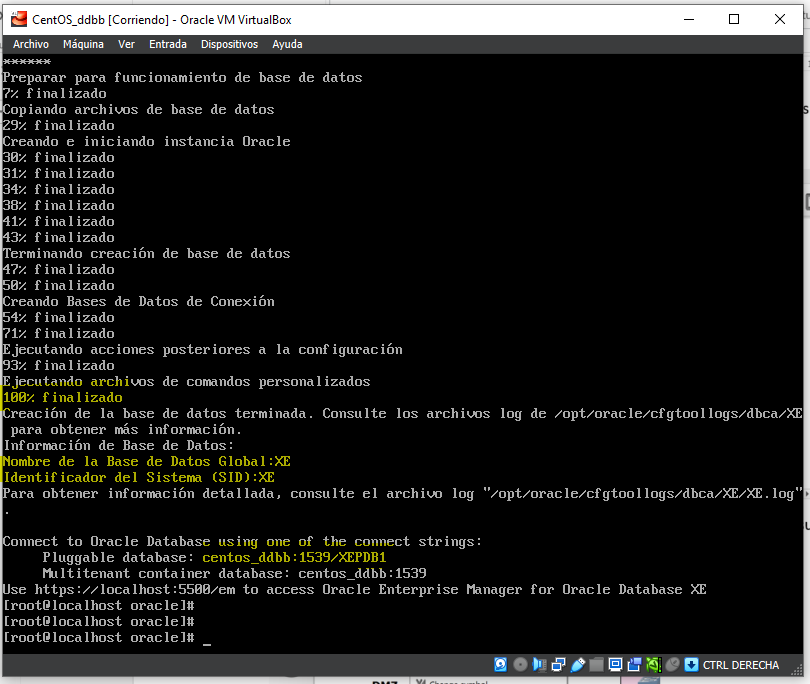


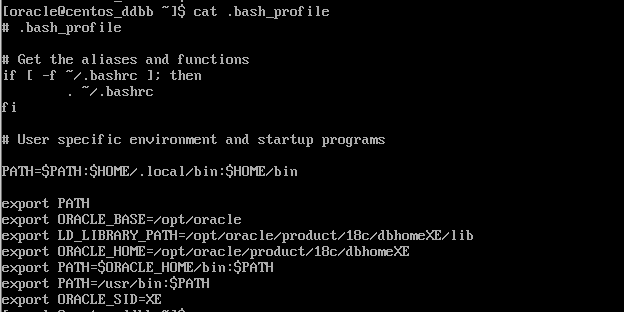
Configuramos el hostname

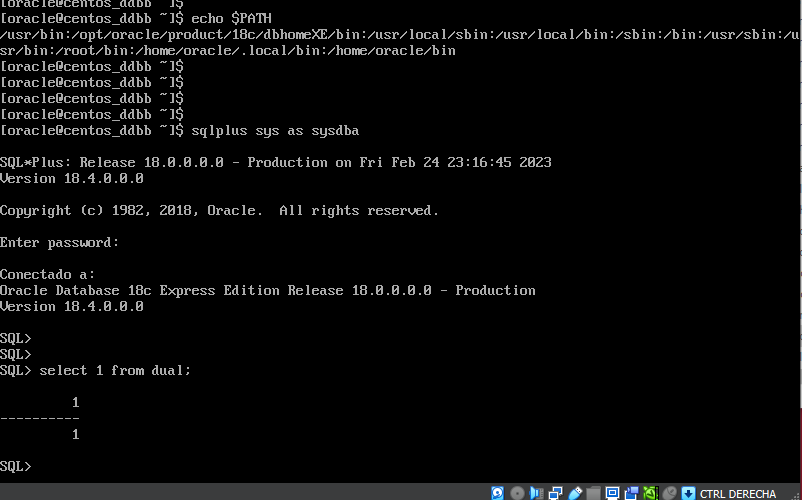
Configuramos el adaptardor de red para la topología

Configuramos el fichero /etc/hosts para resolver el nomnbre









## Servidor Tomcat

# Configuración de servicios privados

## NFS/DFS

## HTTP Intranet

# Configuración de seguridad

ZeroTrust

En los equipos no permitir conexiones habilitadas explícitamente.

## Firewall (iptables)

## Wrappers TCP

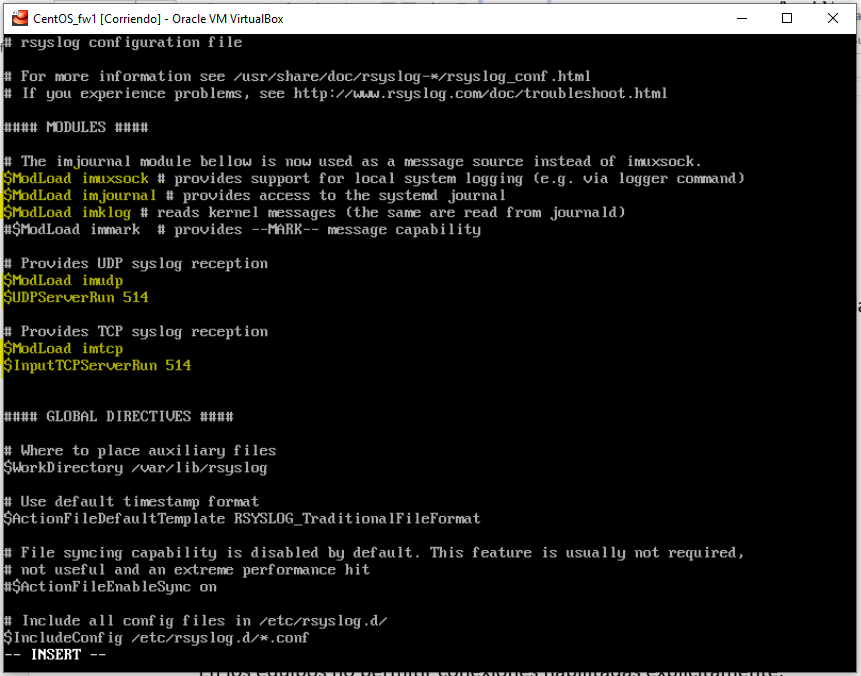
# Configuración de vigilancia

## IDS: PSAD - SNORT

## Gestión centralizada de LOGs

La máquina FW1 va a recolectar los logs de todas las máquinas de la red DMZ.

Configuramos el servicio rsyslog (rsyslog.conf) de FW1



Configurar reglas de distribución de logs

Configurar para que cada máquina que mande sus logs, se archiven en un directorio concreto.



Configuramos el servicio rsyslog (rsyslog.conf) de PROXY, FW2, simplemente indicando que debe enviar los logs de forma remota a servidor FW1 por el puerto 514.

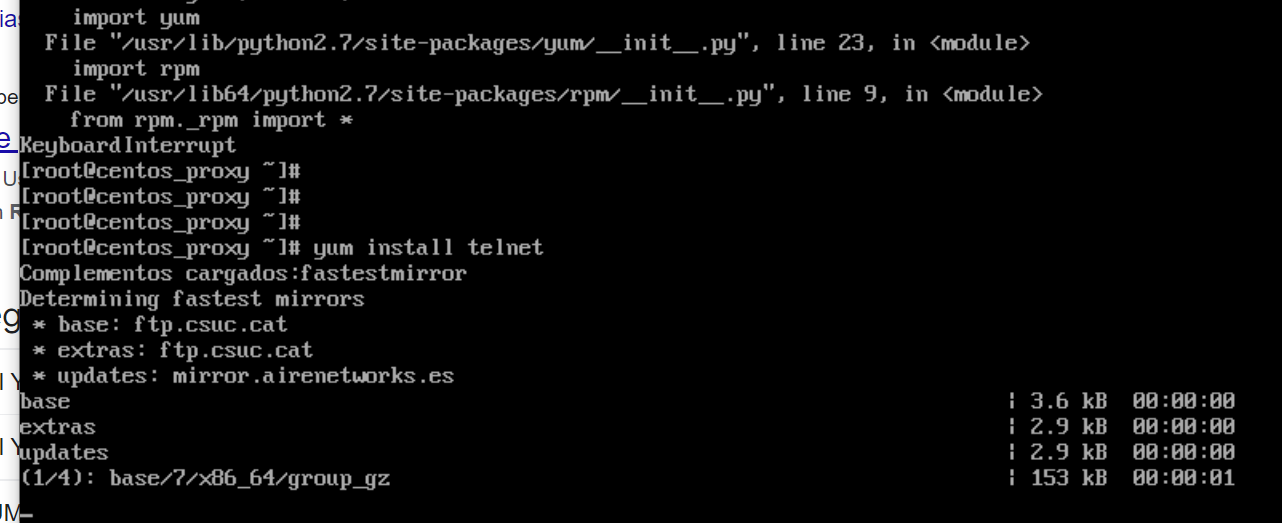


# ANEXO I: Conectividad a Internet en una maquina

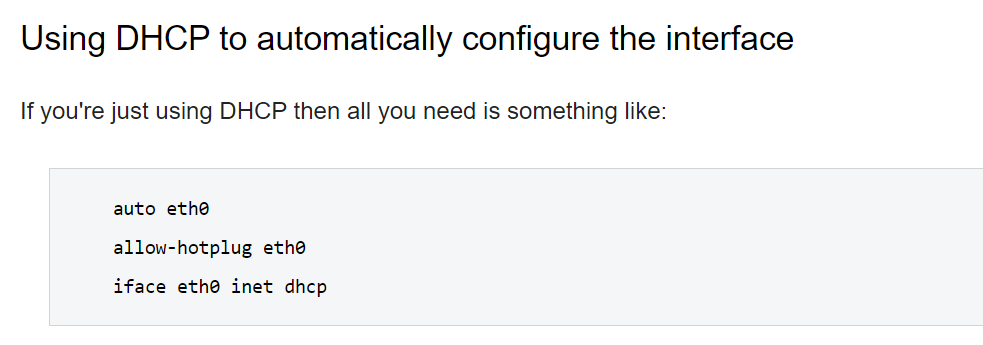
Podremos tener un adaptador extra configurado en VirtualBox como adaptador NAT o PUENTE con el equipo anfitrión para tener conectividad a internet.

Apagando las otras interfaces o poniéndola temporalmente como ruta por defecto, tomara esta salida y tendremos acceso a internet y resolución de nombres con los datos de DNS tomados del DHCP doméstico.

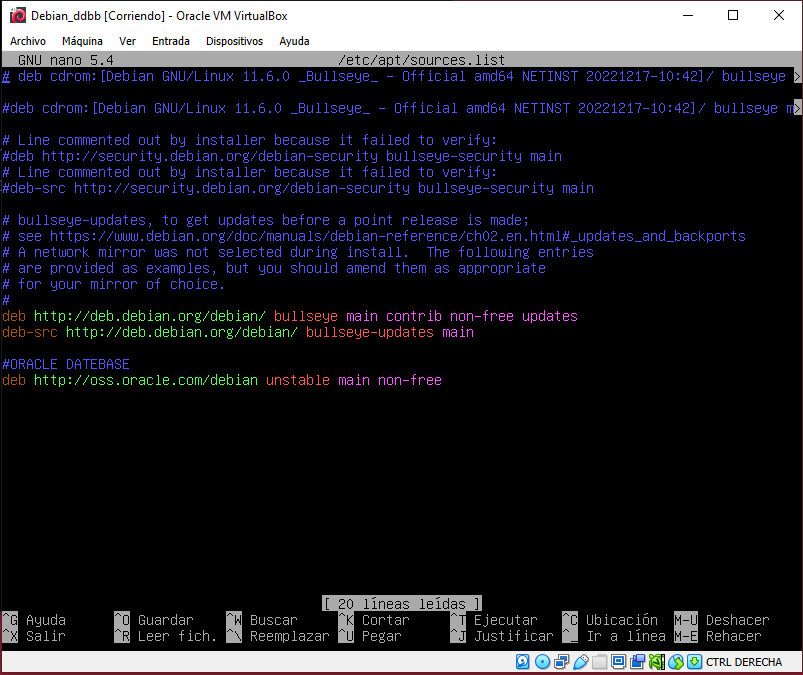
**CentOS**



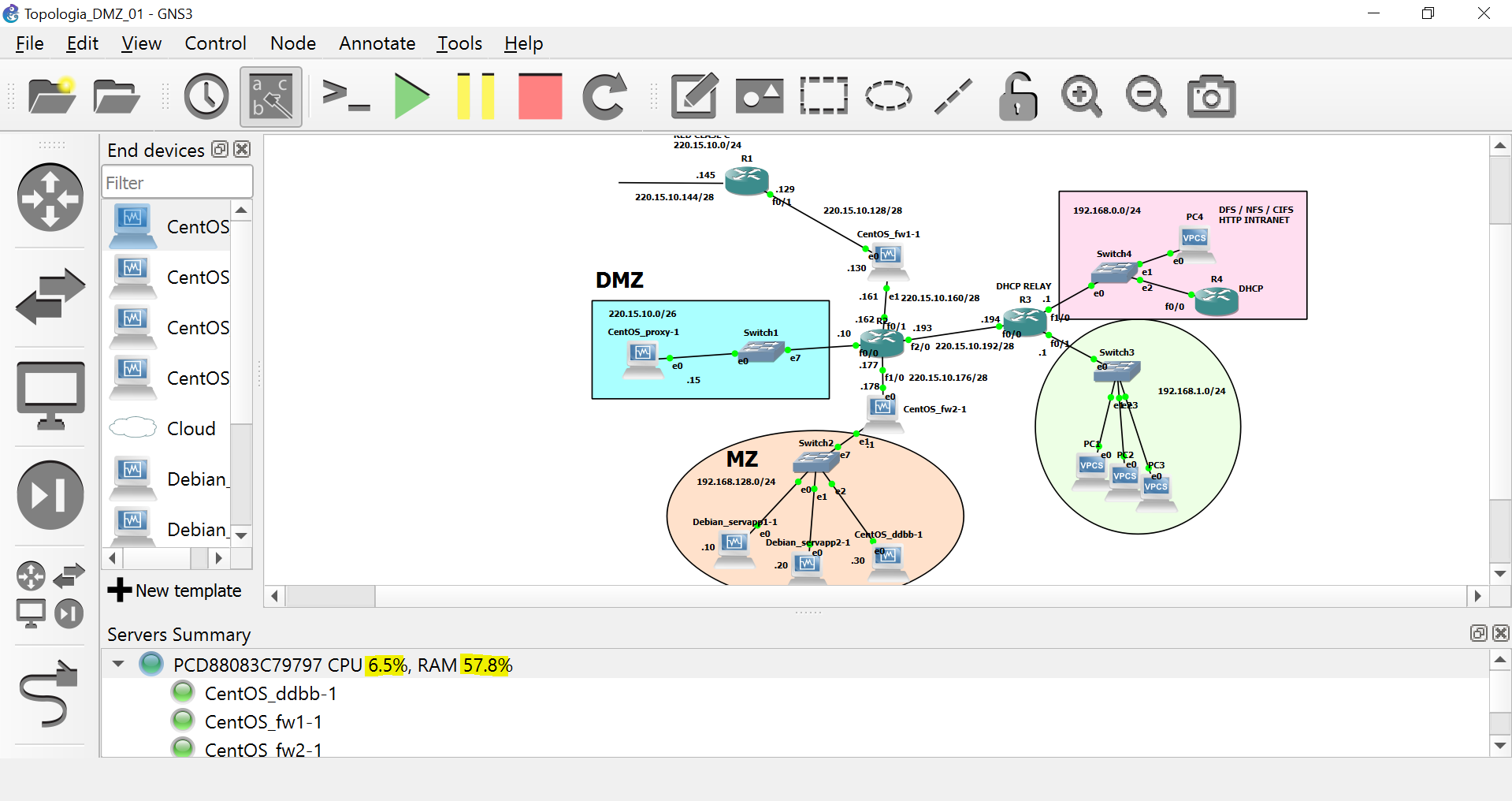
**Debian:**



# ANEXO II: Lista de repositorios debían



# ANAXOIII: Consumo de recursos PC Anfitrión



# REFERENCIAS:

http://librosnetworking.blogspot.com/2013/02/configuracion-de-dhcp-relay.html

# BIBLIOGRAFIA:

CISCO

GNS

VirtualBox