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

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.

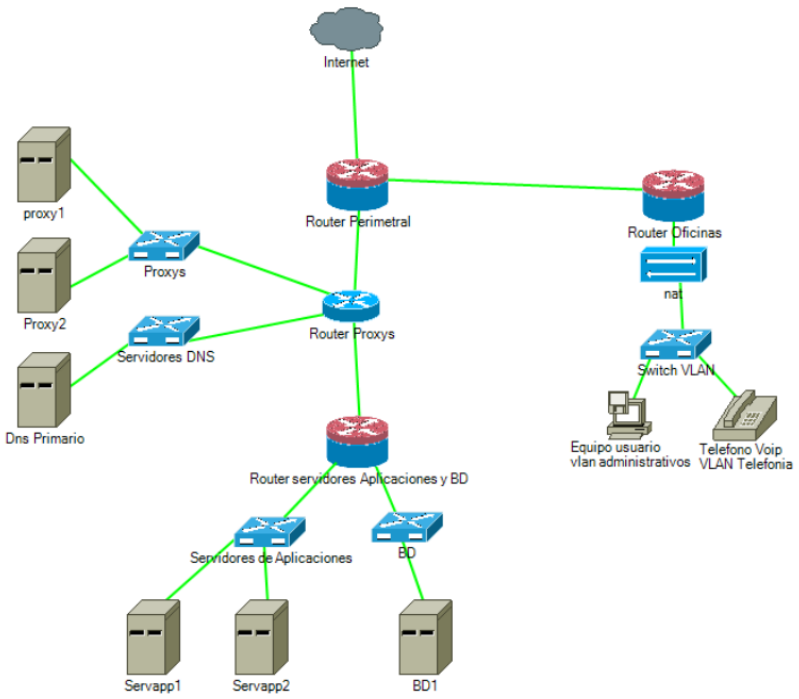
Una vez guardado el laboratorio, podrá ser almacenado e importado en futuros periodos de prueba, entrenamiento o ensayo partiendo de un escenario ya montado en el que poder practicar con las distintas distribuciones de sistemas y diferentes 'dialectos' o mecanismos de configuración en IT.

SUPUESTO PRÁCTICO 1

El diagrama que se muestra a continuación describe el sistema informático de un organismo oficial, compuesto por un CPD donde se alojan los servidores que dan servicio al organismo, y el edificio donde están los trabajadores del mismo.

Hay que tener en cuenta los siguientes detalles:

- Los servidores son máquinas virtuales alojadas en servidores de virtualización Vmware ESXi, y gestionadas por Vmware vCenter
- Todos los servidores tienen SO Debian 9
- El software utilizado para los servidores web es Apache 2.4
- El software utilizado para los servidores de aplicaciones es Apache Tomcat 8.5
- Las BD son Oracle 12c
- Para servidor DNS se utiliza Bind 9
- Los equipos de usuario utilizarán Windows 10
- Existe un dominio llamado organismo-publico.es gestionado por el servidor DNS
- El trafico a los servidores de aplicación solo está permitido desde los servidores proxy
- El trafico a las BD solo está permitido desde los servidores de aplicaciones
- Los equipos de usuario y los teléfonos VoIP irán en vlanes separadas

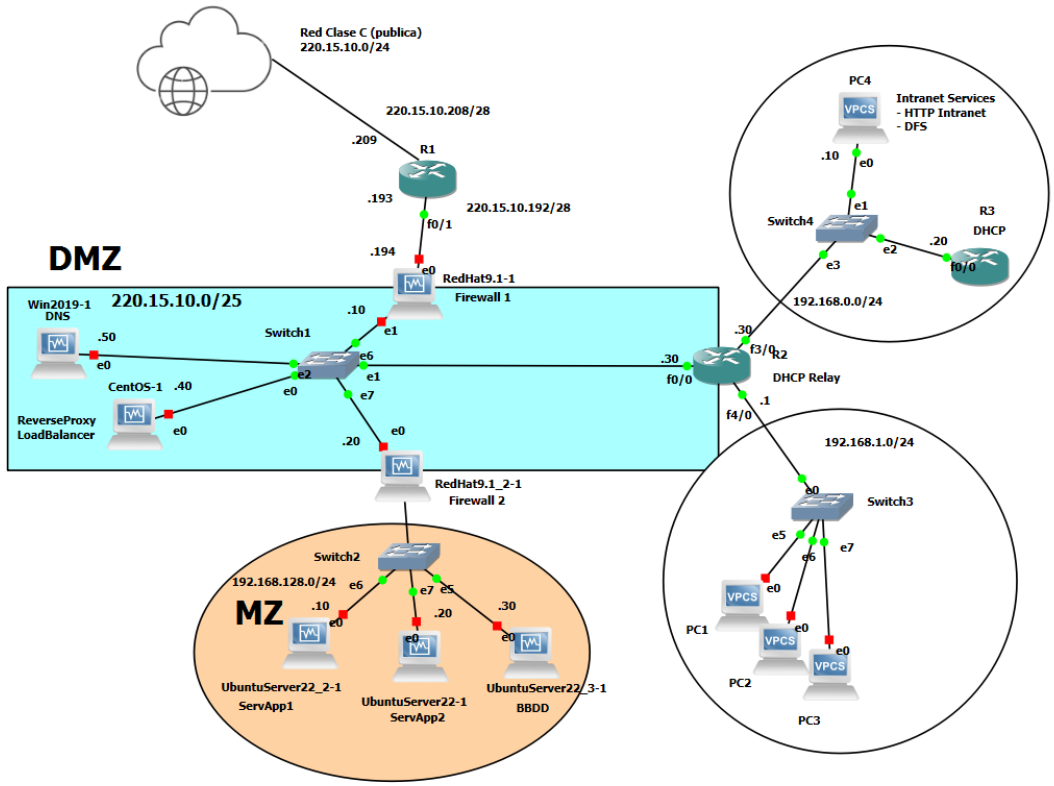


Dudas abiertas

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).

Topología deseada



Instalación entorno GNS3

- Importar imágenes de routers cisco
  - Configurar el IDLE-PC (minimizar consumo de CPU de los routers virtualizados)

Instalación Virtual Box

Para correr los servidores

Instalación de las máquinas virtuales en Virtual Box

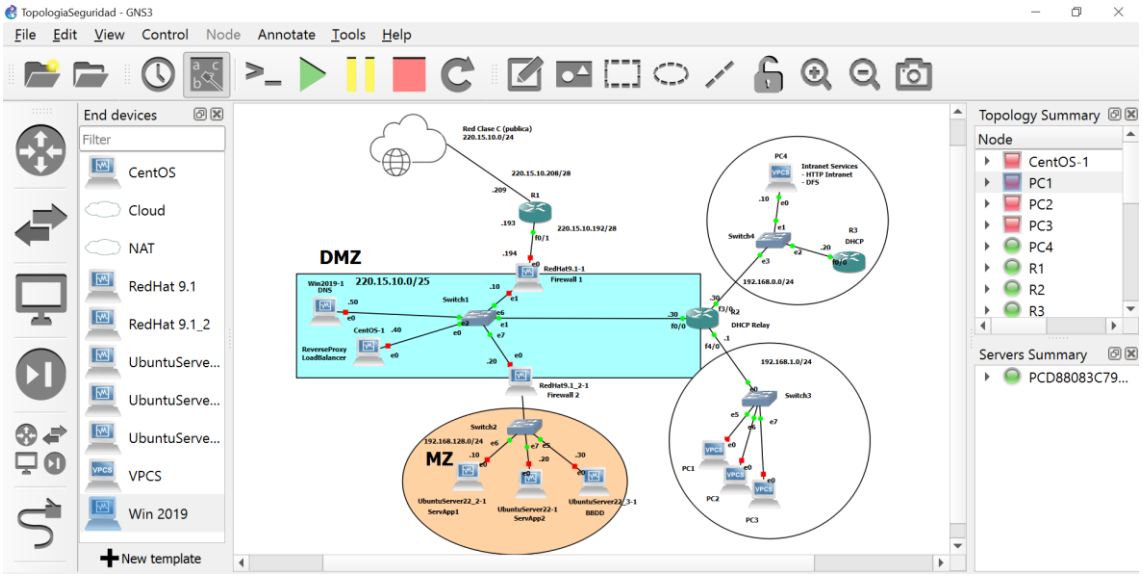
Usamos estas distribuciones con estos objetivos.

- CentOS: apache Proxy Inverso
- RedHat 9.1: firewall
- RedHat 9.1: firewall
- Ubuntu 22: servidor aplicaciones
- Ubuntu 22: servidor aplicaciones (HA – respaldo)
- Ubuntu 22 (only terminal): Oracle DB
- Windows 2019: DNS
- VirtualPC: equipos terminal de usuarios

- Kali: equipo con software para análisis de vulnerabilidades en la red y servicios.

Construcción de la topología sobre GNS3

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



Configuración lógica 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:

100 IPs para DMZ de servicios públicos en internet → 2^7 = 128 IPs

220.15.10.0HHHHHHH

220.15.10.0/25

60 IPs Reservadas → 2^6 = 64 IPs

220.15.10.10HHHHHH

220.15.10.128/26

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

220.15.10.1100HHHH

220.15.10.192/28

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

220.15.10.1101HHHH

220.15.10.208/28

10 IPs Reservadas → 2^4 = 16 IPs

220.15.10.1110HHHH

220.15.10.224/28

10 IPs Reservadas → 2^4 = 16 IPs

220.15.10.1111HHHH

220.15.10.240/28

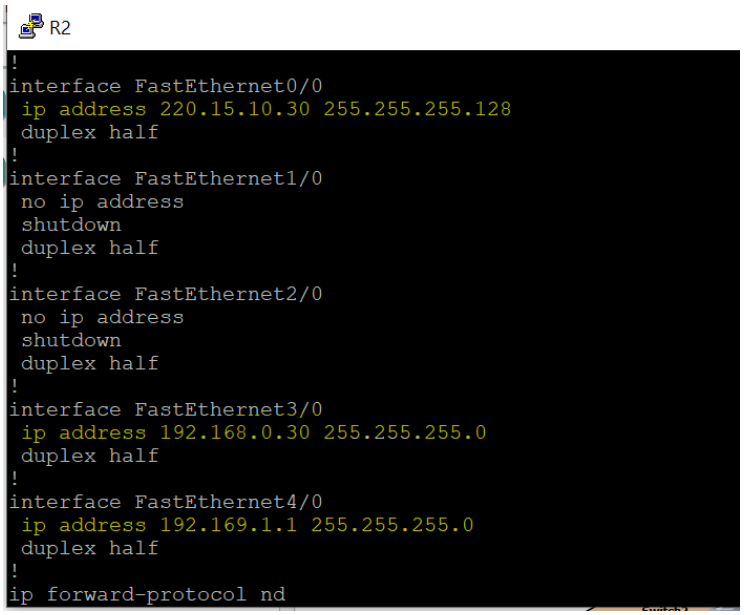
Para el resto de subredes utilizaremos direccionamiento privado IPv4 de clase C

192.168.0.0/24 para la red de servicios de la intranet

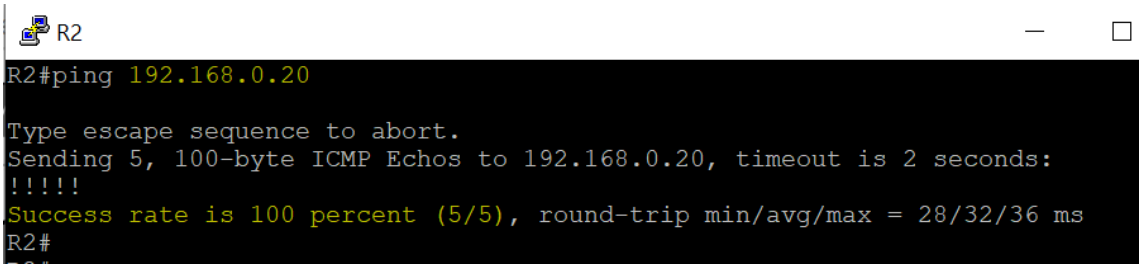
192.168.1.0/24 para intranet de usuarios

192.168.128.0/24 para la MZ de servicios y bbdd

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



Comprobamos algunos ping entre interfaces directamente conectadas.



Configuración del servicio DHCP para la intranet

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
```

Configuración del enrutamiento

static route

Configuración de servicios públicos

Apache ProxyBalancer

DNS

Configuración de servicios MZ

Oracle DB

Servidor Tomcat

Configuración de servicios privados

DFS

HTTP Intranet

Configuración de seguridad

Firewall (iptables)

IDS: SNORT

Configuración de vigilancia

PSAD / SNORT

Comprobación seguridad

Pentesting con Kali distro

Referencias:

CISCO

GNS

VirtualBox

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