

Pasos realizados

Paso 1. Instalar paquetes en servidor2

* sudo apt update
* sudo apt install -y vsftpd openssl lftp

Paso 2. Generar certificados SSL

* sudo mkdir -p /etc/ssl/localcerts
* sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \

-keyout /etc/ssl/localcerts/vsftpd.key \

-out /etc/ssl/localcerts/vsftpd.crt \

-subj "/C=CO/ST=Valle del Cauca/L=Cali/O=UAO/OU=Servicios [Telematicos/CN=ftp.servicios.com/emailAddress=admin@servicios.com](mailto:Telematicos/CN=ftp.servicios.com/emailAddress=admin@servicios.com)"

* sudo chmod 600 /etc/ssl/localcerts/vsftpd.key

Paso 3. Configurar vsftpd

* sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.bak
* sudo vim /etc/vsftpd.conf

ASEGURARSE QUE ESTE ESTO ALMENOS

listen=YES

listen\_ipv6=NO

anonymous\_enable=NO

local\_enable=YES

write\_enable=YES

local\_umask=022

dirmessage\_enable=YES

use\_localtime=YES

xferlog\_enable=YES

connect\_from\_port\_20=YES

ftpd\_banner=Bienvenido al FTP Seguro de la práctica

chroot\_local\_user=YES

allow\_writeable\_chroot=YES

secure\_chroot\_dir=/var/run/vsftpd/empty

pam\_service\_name=vsftpd

# --- SSL ---

rsa\_cert\_file=/etc/ssl/localcerts/vsftpd.crt

rsa\_private\_key\_file=/etc/ssl/localcerts/vsftpd.key

ssl\_enable=YES

force\_local\_logins\_ssl=YES

force\_local\_data\_ssl=YES

ssl\_tlsv1=YES

require\_ssl\_reuse=NO

# --- Pasivo ---

pasv\_enable=YES

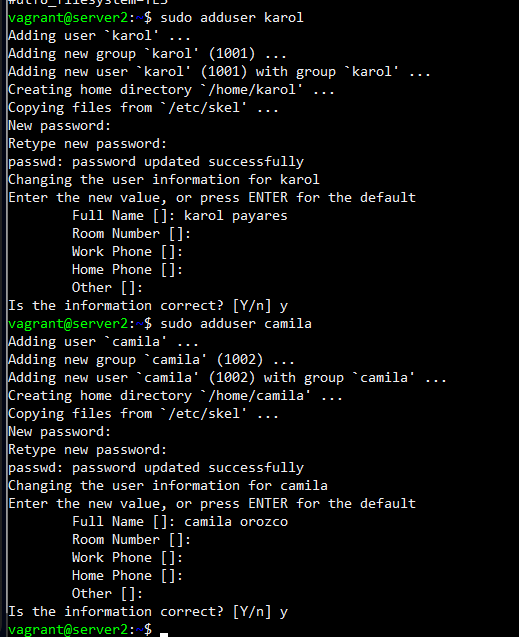
pasv\_min\_port=40000

pasv\_max\_port=40100

pasv\_address=192.168.50.3

pasv\_addr\_resolve=NO

Paso 4. Crear usuarios locales de prueba



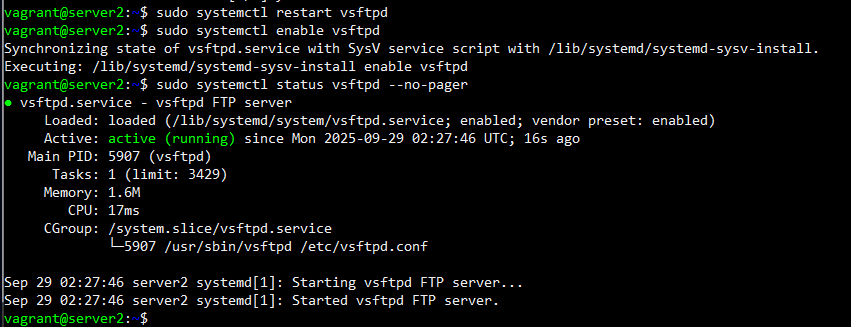
Contraseña

Karol 🡪 karol1

Camila 🡪camila1

Paso 5. Reiniciar y habilitar el servicio

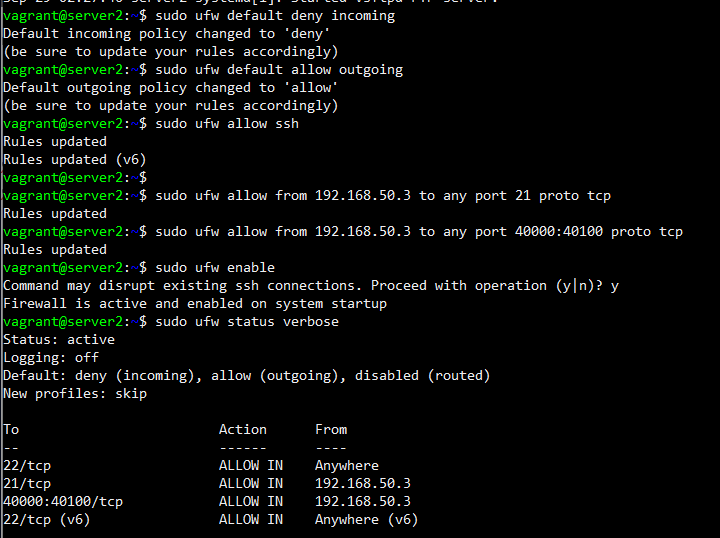
* sudo systemctl restart vsftpd
* sudo systemctl enable vsftpd
* sudo systemctl status vsftpd --no-pager

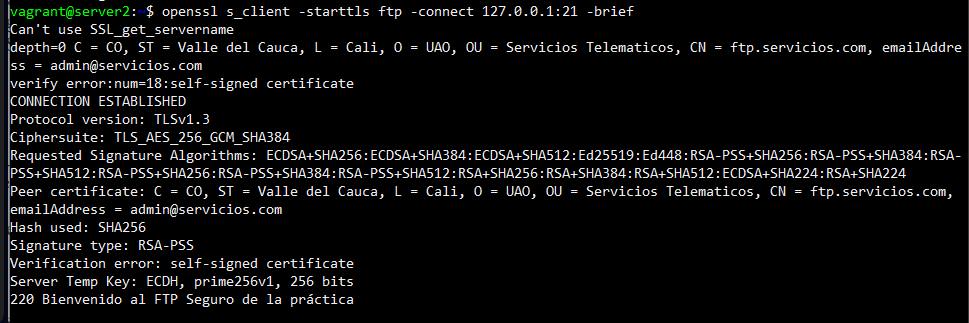


Paso 6. Configurar UFW en servidor2 por protección (buenas practicas)

Política por defecto + permitir solo tráfico desde servidor1 (192.168.50.3):

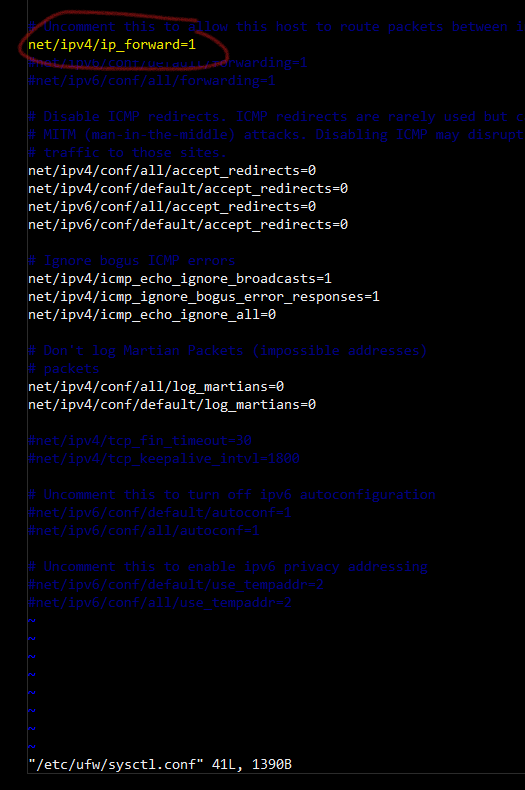
* sudo ufw default deny incoming
* sudo ufw default allow outgoing
* sudo ufw allow ssh
* sudo ufw allow from 192.168.50.3 to any port 21 proto tcp
* sudo ufw allow from 192.168.50.3 to any port 40000:40100 proto tcp
* sudo ufw enable
* sudo ufw status verbose





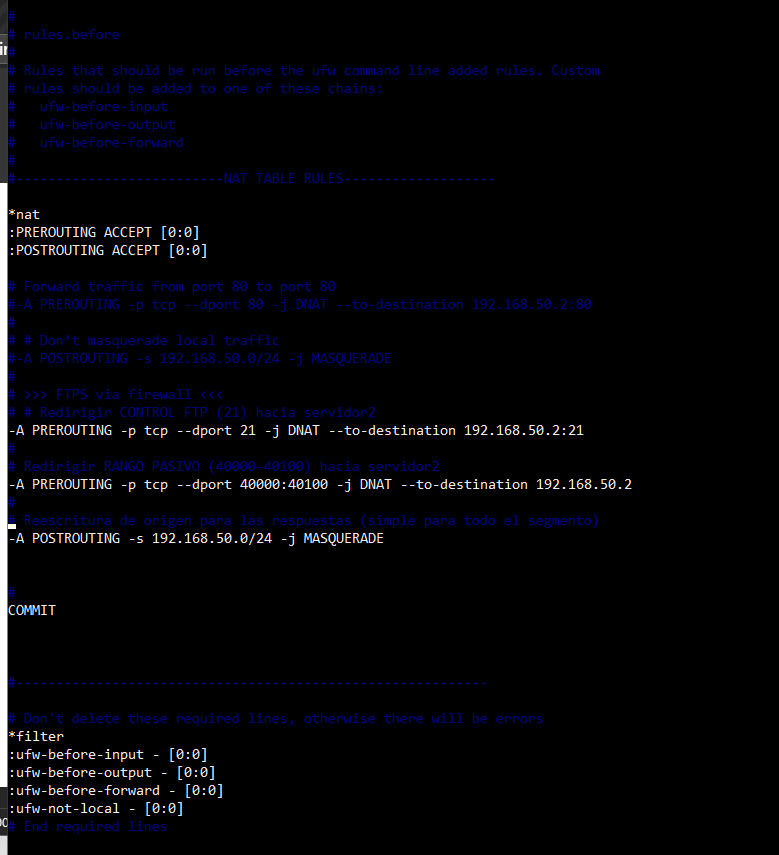
Servidor1

Paso 1: ver que este habilitado en sudo vim /etc/ufw/sysctl.conf el:



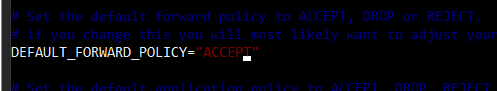
Paso 2: Editar reglas de UFW para NAT y DNAT

* sudo vim /etc/ufw/before.rules



Paso 3: Habilitar forwarding en UFW

* Sudo vim /etc/default/ufw



Paso 4: Reglas UFW en **servidor1**

* sudo ufw default deny incoming
* sudo ufw default allow outgoing
* sudo ufw allow ssh

# Abrimos el punto de entrada para el cliente:

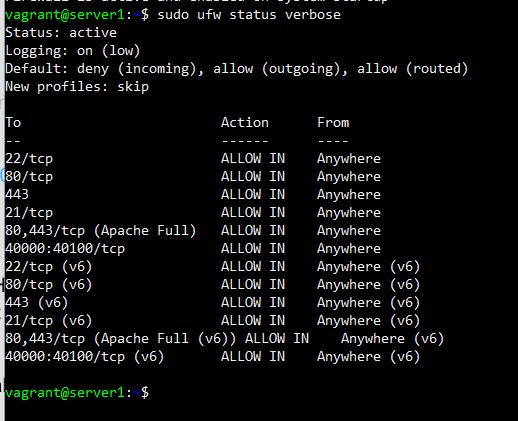
* sudo ufw allow 21/tcp
* sudo ufw allow 40000:40100/tcp

# Reaplicar UFW para que cargue las reglas de before.rules

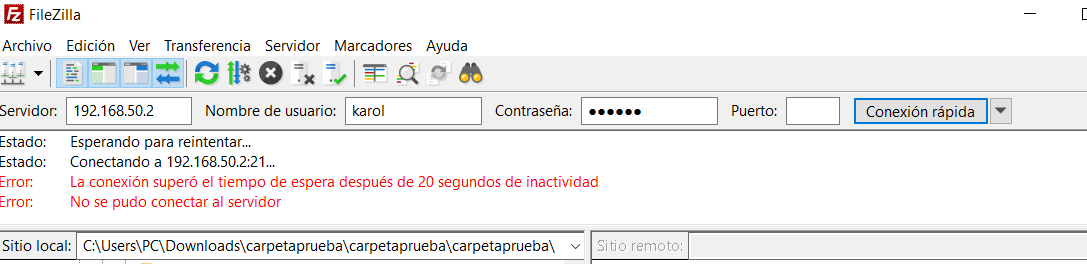
* sudo ufw disable && sudo ufw enable

# Verificación

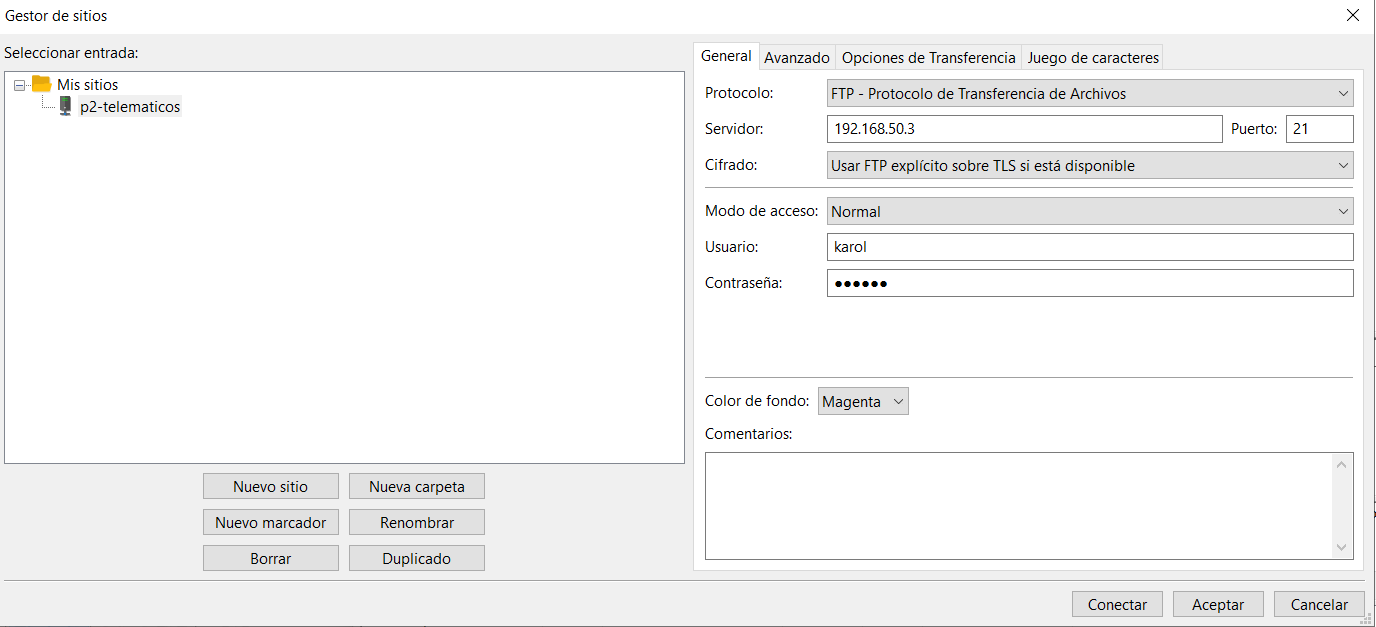
* sudo ufw status verbose

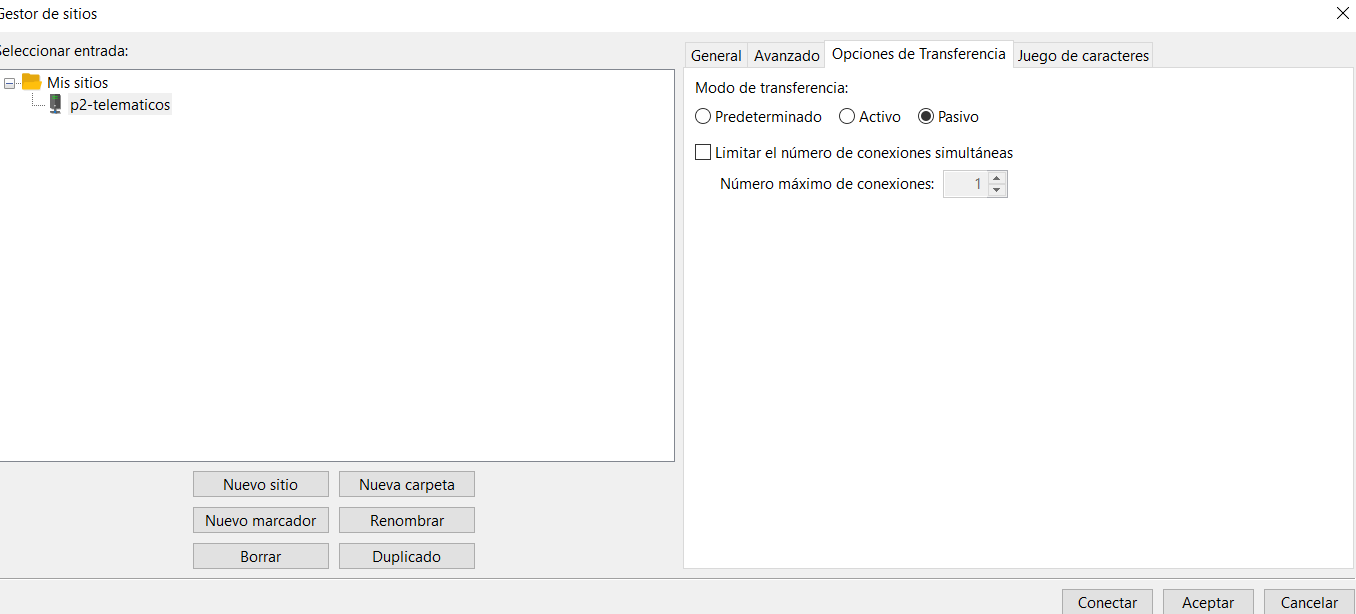


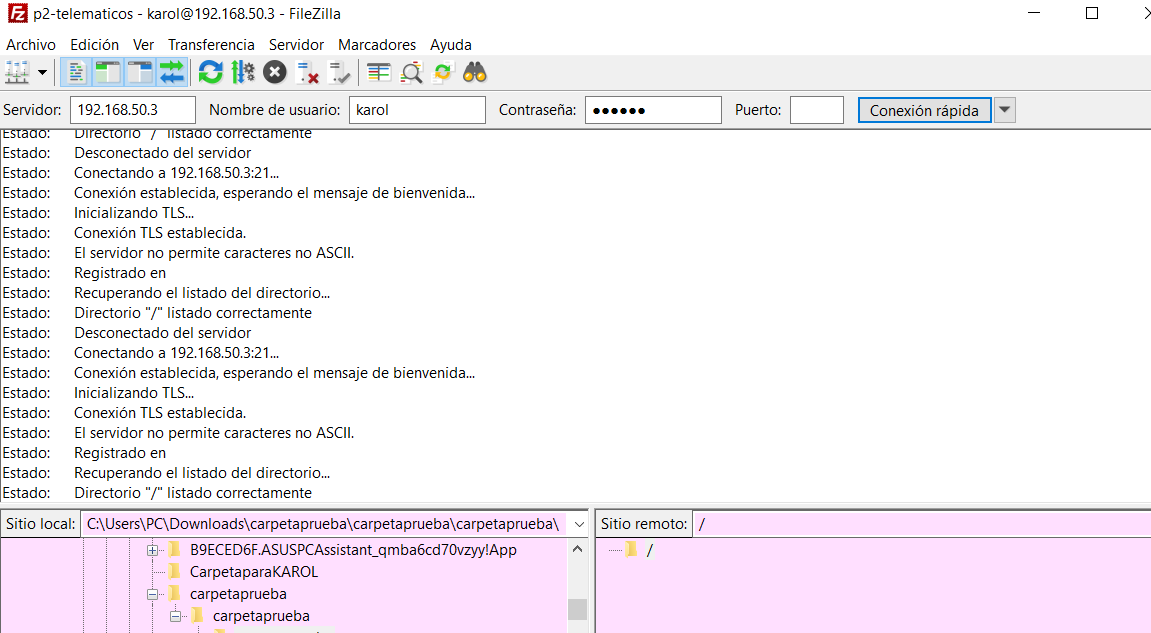
PRUEBAS



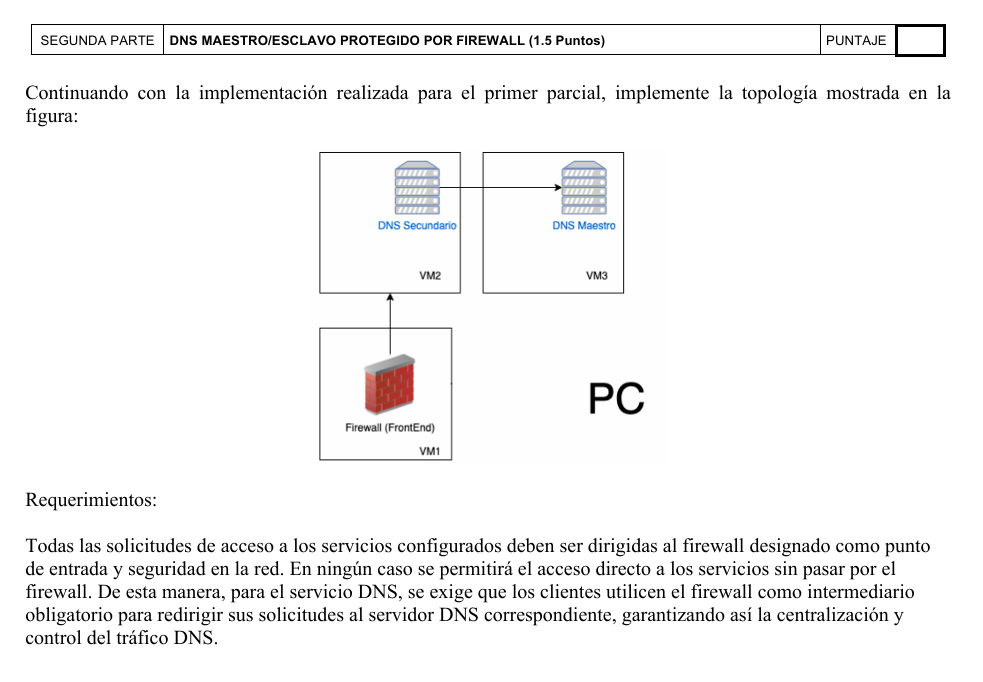
Debe salir eso ósea que esta bien, ahora configurar el sitio







PARTE 2 DEL PARCIAL



CONFIGURACION SERVIDOR1-🡪esto pasa a servidor 3 que será el dns maestro

**TOPOLOGÍA FINAL**

CLIENTE EXTERNO → SERVIDOR 1 (Firewall: 192.168.50.3) → SERVIDOR 2 (Esclavo+Web: 192.168.50.2)

↘ SERVIDOR 3 (Maestro: 192.168.50.4)

**SERVIDOR 3 (DNS MAESTRO - 192.168.50.4)**

**1. INSTALACIÓN BIND9**

* sudo apt update
* sudo apt install -y bind9 bind9utils bind9-doc

**2. CONFIGURACIÓN ZONAS**

**Archivo:** /etc/bind/named.conf.local

sudo vim /etc/bind/named.conf.local

Contenido:

zone "ejercicio.com" {

type master;

file "/etc/bind/db.ejercicio.com";

allow-transfer { 192.168.50.2; };

};

zone "50.168.192.in-addr.arpa" {

type master;

file "/etc/bind/db.192";

allow-transfer { 192.168.50.2; };

};

**3. CONFIGURACIÓN ZONA DIRECTA**

**Archivo:** /etc/bind/db.ejercicio.com

* sudo cp /etc/bind/db.local /etc/bind/db.ejercicio.com
* sudo vim /etc/bind/db.ejercicio.com

Contenido:

$TTL 604800

@ IN SOA ns1.ejercicio.com. admin.ejercicio.com. (

2025093001 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

@ IN NS ns1.ejercicio.com.

@ IN NS ns2.ejercicio.com.

ns1 IN A 192.168.50.4

ns2 IN A 192.168.50.2

www IN A 192.168.50.2

ftp IN A 192.168.50.2

**4. CONFIGURACIÓN ZONA INVERSA**

**Archivo:** /etc/bind/db.192

* sudo cp /etc/bind/db.127 /etc/bind/db.192
* sudo vim /etc/bind/db.192

Contenido:

$TTL 604800

@ IN SOA ns1.ejercicio.com. admin.ejercicio.com. (

2025093001 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

@ IN NS ns1.ejercicio.com.

@ IN NS ns2.ejercicio.com.

4 IN PTR ns1.ejercicio.com.

2 IN PTR ns2.ejercicio.com.

2 IN PTR www.ejercicio.com.

2 IN PTR ftp.ejercicio.com.

**5. VERIFICACIÓN Y REINICIO**

* sudo named-checkconf
* sudo named-checkzone ejercicio.com /etc/bind/db.ejercicio.com
* sudo named-checkzone 50.168.192.in-addr.arpa /etc/bind/db.192
* sudo systemctl restart bind9
* sudo systemctl enable bind9

**6. CONFIGURACIÓN FIREWALL**

* sudo ufw default deny incoming
* sudo ufw default allow outgoing
* sudo ufw allow ssh
* sudo ufw allow from 192.168.50.3 to any port 53
* sudo ufw enable

**SERVIDOR 2 (DNS ESCLAVO + WEB - 192.168.50.2)**

**1. INSTALACIÓN BIND9**

* sudo apt update
* sudo apt install -y bind9 bind9utils

**2. CONFIGURACIÓN ZONAS ESCLAVAS**

**Archivo:** /etc/bind/named.conf.local

* sudo vim /etc/bind/named.conf.local

Contenido:

zone "ejercicio.com" {

type slave;

file "/var/lib/bind/db.ejercicio.com";

masters { 192.168.50.4; };

};

zone "50.168.192.in-addr.arpa" {

type slave;

file "/var/lib/bind/db.192";

masters { 192.168.50.4; };

};

**3. VERIFICACIÓN Y REINICIO**

* sudo named-checkconf
* sudo systemctl restart bind9
* sudo systemctl enable bind9

**4. INSTALACIÓN Y CONFIGURACIÓN APACHE**

* sudo apt install -y apache2
* sudo systemctl start apache2
* sudo systemctl enable apache2

**5. CONFIGURACIÓN PÁGINA WEB**

**Archivo:** /var/www/html/index.html

* sudo vim /var/www/html/index.html

Contenido HTML

**6. CONFIGURACIÓN FIREWALL (INCLUYENDO PUERTO 80)**

sudo ufw default deny incoming

sudo ufw default allow outgoing

sudo ufw allow ssh

sudo ufw allow from 192.168.50.3 to any port 21

sudo ufw allow from 192.168.50.3 to any port 40000:40100

sudo ufw allow from 192.168.50.3 to any port 53

sudo ufw allow from 192.168.50.4 to any port 53

sudo ufw allow from 192.168.50.3 to any port 80 proto tcp *# ← REGLA CLAVE QUE FALTABA*

sudo ufw enable

**SERVIDOR 1 (FIREWALL - 192.168.50.3)**

**1. CONFIGURACIÓN REGLAS NAT**

**Archivo:** /etc/ufw/before.rules

* sudo vim /etc/ufw/before.rules

En la sección \*nat agregar:

*# >>> FTP via firewall <<<*

-A PREROUTING -p tcp --dport 21 -j DNAT --to-destination 192.168.50.2:21

-A PREROUTING -p tcp --dport 40000:40100 -j DNAT --to-destination 192.168.50.2

*# >>> DNS via firewall <<<*

-A PREROUTING -p udp --dport 53 -j DNAT --to-destination 192.168.50.4:53

-A PREROUTING -p tcp --dport 53 -j DNAT --to-destination 192.168.50.4:53

*# >>> HTTP via firewall <<<*

-A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.50.2:80

*# MASQUERADE*

-A POSTROUTING -s 192.168.50.0/24 -j MASQUERADE

**2. CONFIGURACIÓN FIREWALL UFW**

* sudo ufw default deny incoming
* sudo ufw default allow outgoing
* sudo ufw allow ssh
* sudo ufw allow 21/tcp
* sudo ufw allow 40000:40100/tcp
* sudo ufw allow 53/udp
* sudo ufw allow 53/tcp
* sudo ufw allow 80/tcp *# ← HABILITAR PUERTO WEB*
* sudo ufw disable && sudo ufw enable

**3. HABILITAR FORWARDING**

**Archivo:** /etc/default/ufw

* sudo vim /etc/default/ufw

Asegurar que tenga:

DEFAULT\_FORWARD\_POLICY="ACCEPT"

**VERIFICACIONES FINALES**

**VERIFICAR DNS**

nslookup www.ejercicio.com 192.168.50.3

nslookup ftp.ejercicio.com 192.168.50.3

nslookup 192.168.50.2 192.168.50.3

**VERIFICAR SERVICIO WEB**

*# Desde navegador o línea de comandos:*

curl http://192.168.50.3

**VERIFICAR TRANSFERENCIA ZONAS**

*# En Server2:*

ls -la /var/lib/bind/

*# Deben aparecer db.ejercicio.com y db.192*

**PROBLEMA IDENTIFICADO**

**Configuración incorrecta de firewall en Servidor 2 (Esclavo)** causaba que el servicio DNS no respondiera a consultas externas.

**CONFIGURACIÓN INCORRECTA ORIGINAL**

En Servidor 2, UFW tenía reglas conflictivas:

53/tcp ALLOW 192.168.50.3 ← SÓLO permitía del firewall

53/udp ALLOW 192.168.50.3 ← SÓLO permitía del firewall

53 ALLOW 192.168.50.0/24 ← Permitía de toda la red (CORRECTO)

**Las reglas específicas tenían prioridad**, bloqueando consultas de otros equipos.

**SOLUCIÓN APLICADA**

**En Servidor 2 (192.168.50.2):**

*# Eliminar reglas específicas conflictivas*

sudo ufw delete allow from 192.168.50.3 to any port 53 proto tcp

sudo ufw delete allow from 192.168.50.3 to any port 53 proto udp

*# Configuración final correcta:*

sudo ufw status | grep 53

*# 53 ALLOW 192.168.50.0/24*

**CONFIGURACIÓN FINAL CORRECTA - SERVIDOR 2**

22/tcp ALLOW Anywhere

21/tcp ALLOW 192.168.50.3

40000:40100/tcp ALLOW 192.168.50.3

80/tcp ALLOW 192.168.50.3

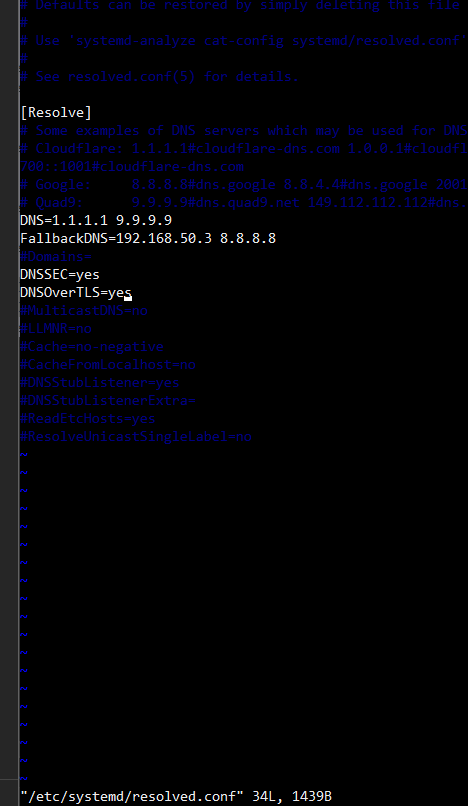
53 ALLOW 192.168.50.0/24 # ← Permite consultas DNS de toda la red

PARCIAL PARTE 3

Implementación de DNS sobre TLS en una máquina Cliente Linux utilizando systemd en una distribución CentOS o Ubuntu, y verificación del funcionamiento a través de Wireshark.

EN CLIENTE 192.168.50.12

* sudo apt update
* sudo apt install -y network-manager
* sudo systemctl status NetworkManager --no-pager
* sudo systemctl status systemd-resolved --no-pager
* sudo vim /etc/systemd/resolved.conf



* sudo vim /etc/NetworkManager/conf.d/10-dns-systemd-resolved.conf
* ls -l /etc/resolv.conf
* sudo systemctl enable systemd-resolved
* sudo systemctl start systemd-resolved
* sudo systemctl status systemd-resolved
* sudo systemctl restart NetworkManager
* ip a
* resolvectl status
* cat /etc/resolv.conf
* sudo vim /etc/systemd/resolved.conf
* sudo systemctl restart systemd-resolved
* sudo resolvectl flush-caches
* nslookup drivemeca.com

