



Parcial 2

Servicios telemáticos

Jhon Sebastian Cortes Vásquez - 2205199

Informe Parcial2

Oscar Hernán Mondragón Martínez

Docente Académico

Universidad Autónoma de Occidente

Santiago de Cali

2023

Paso 1: Configuración del firewall (VM1)

Para este paso, me centraré en utilizar `firewalld`, que es un administrador de firewall dinámico con soporte para zonas de red o firewall. Es más fácil de usar que `iptables` y es el predeterminado en muchas distribuciones modernas de Linux.

1.1. Instalación y configuración inicial de `firewalld` en VM1 (firewall):

Si no está instalado, instale `firewalld` con:

```
root@firewall:~  
C:\Users\Jhon\Documents\UAO\Servicios Telematicos\Practicas\1\Prueba>vagrant ssh firewall  
[vagrant@firewall ~]$ sudo -i  
[root@firewall ~]# sudo yum install -y firewalld  
CentOS Stream 9 - BaseOS                               854 kB/s | 7.8 MB    00:09  
CentOS Stream 9 - AppStream                             3.3 MB/s | 18 MB    00:05  
CentOS Stream 9 - Extras packages                       3.1 kB/s | 14 kB    00:04  
Extra Packages for Enterprise Linux 9 - x86_64          13 MB/s | 19 MB    00:01  
Extra Packages for Enterprise Linux 9 - Next - x86_64   444 kB/s | 1.4 MB   00:03  
Package firewalld-1.2.5-1.el9.noarch is already installed.  
Dependencies resolved.  


| Package               | Architecture | Version     | Repository | Size  |
|-----------------------|--------------|-------------|------------|-------|
| Upgrading:            |              |             |            |       |
| firewalld             | noarch       | 1.2.5-1.el9 | baseos     | 525 k |
| firewalld-filessystem | noarch       | 1.2.5-1.el9 | baseos     | 9.6 k |
| python3-firewall      | noarch       | 1.2.5-1.el9 | baseos     | 387 k |

  
Transaction Summary  
-----  
Upgrade 3 Packages  
  
Total download size: 922 k  
Downloading Packages:  
(1/3): firewalld-filessystem-1.2.5-1.el9.noarch.rpm          15 kB/s | 9.6 kB    00:00  
(2-3/3): python3-firewall-1.2.5-1.el9.no 46% [=====] 1.6 MB/s | 431 kB    00:00 ETA
```

Una vez instalado, inicie el servicio y habilítelo para que se inicie automáticamente en el arranque:

```
root@firewall:~  
[root@firewall ~]# sudo systemctl start firewalld  
[root@firewall ~]# sudo systemctl enable firewalld  
[root@firewall ~]#
```

1.2. Asegurar que todas las solicitudes al servidor FTP pasen a través del firewall:

Para hacerlo, necesitamos configurar las zonas y las reglas de reenvío de puertos adecuadas. Asumiendo que el puerto FTPS es el 990 (este es el puerto predeterminado para FTPS):

```
[root@firewall ~]# sudo firewall-cmd --set-default-zone=public
Warning: ZONE_ALREADY_SET: public
success
[root@firewall ~]# sudo firewall-cmd --zone=public --add-forward-port=port=990:proto=tcp:toaddr=192.168.50.3:toport=990
--permanent
success
[root@firewall ~]# sudo firewall-cmd --reload
success
[root@firewall ~]#
```

Estos comandos aseguran que cualquier solicitud al firewall en el puerto 990 sea reenviada al servidor FTP en la dirección IP 192.168.50.3 en el mismo puerto.

Con esto, hemos completado la configuración básica del firewall para nuestro escenario. Sin embargo, es posible que necesitemos más ajustes una vez que el servidor FTP esté en marcha y queramos hacer pruebas.

Zonas

1. Crear las zonas DMZ e Internal (si aún no existen):

```
[root@firewall ~]# sudo firewall-cmd --new-zone=dmz --permanent
Error: NAME_CONFLICT: new_zone(): 'dmz'
[root@firewall ~]# sudo firewall-cmd --new-zone=internal --permanent
Error: NAME_CONFLICT: new_zone(): 'internal'
[root@firewall ~]#
```

2. Asignar las interfaces a sus respectivas zonas:

```
root@firewall:~
[root@firewall ~]# sudo firewall-cmd --zone=public --change-interface=eth0 --permanent
The interface is under control of NetworkManager, setting zone to 'public'.
success
[root@firewall ~]# sudo firewall-cmd --zone=dmz --change-interface=eth1 --permanent
The interface is under control of NetworkManager, setting zone to 'dmz'.
success
[root@firewall ~]# sudo firewall-cmd --zone=internal --change-interface=eth2 --permanent
Error: [Errno 13] Permission denied: '/etc/sysconfig/network-scripts/ifcfg-eth1'
[root@firewall ~]# sudo firewall-cmd --zone=internal --change-interface=eth2 --permanent
success
[root@firewall ~]#
```

3. Asegurarse de que las reglas de reenvío de puertos están en la zona DMZ y de que los puertos requeridos están abiertos en la zona DMZ:

```
root@firewall:~  
[root@firewall ~]# sudo firewall-cmd --zone=dmz --add-forward-port=port=21:proto=tcp:toaddr=172.16.0.3:toport=21 --permanent  
success  
[root@firewall ~]# sudo firewall-cmd --zone=dmz --add-forward-port=port=990:proto=tcp:toaddr=192.168.50.3:toport=990 --permanent  
success  
[root@firewall ~]# sudo firewall-cmd --zone=dmz --add-port=20-21/tcp --permanent  
success  
[root@firewall ~]# sudo firewall-cmd --zone=dmz --add-port=31500-32500/tcp --permanent  
success  
[root@firewall ~]#
```

Recargar las reglas del firewall y Verificar las zonas y sus interfaces:

```
[root@firewall ~]# sudo firewall-cmd --reload  
success  
[root@firewall ~]# sudo firewall-cmd --get-active-zones  
dmz  
    interfaces: eth1  
internal  
    interfaces: eth2  
public  
    interfaces: eth0  
[root@firewall ~]#
```

Tienes razón, el servicio `ftp` debería estar permitido en la zona `dmz` y el `masquerade` debería estar habilitado para que el reenvío de paquetes funcione correctamente.

Vamos a realizar esos ajustes:

1. **Agregar el servicio FTP a la zona DMZ y Habilitar el masquerade en la zona DMZ:**

Esto es necesario para que las máquinas detrás del firewall (como tu servidor FTP) puedan comunicarse correctamente con el mundo exterior, y viceversa.

2. **Recargar las reglas del firewall y verificar los cambios:**

```

root@firewall:~
[root@firewall ~]# [root@firewall ~]# sudo firewall-cmd --zone=dmz --add-service=ftp --permanent
success
[root@firewall ~]# sudo firewall-cmd --zone=dmz --add-masquerade --permanent
success
[root@firewall ~]# sudo firewall-cmd --reload
success
[root@firewall ~]# sudo firewall-cmd --zone=dmz --list-all
dmz (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth1
  sources:
  services: ftp ssh
  ports: 20-21/tcp 31500-32500/tcp
  protocols:
  forward: yes
  masquerade: yes
  forward-ports:
    port=21:proto=tcp:toport=21:toaddr=172.16.0.3
    port=990:proto=tcp:toport=990:toaddr=192.168.50.3
  source-ports:
  icmp-blocks:
  rich rules:
[root@firewall ~]#

```

Usar IPTABLES directamente para el reenvío de paquetes:

El uso directo de `iptables` nos dará un control más detallado sobre el reenvío de paquetes.

Paso 1: Asegúrate de que la IP forwarding esté habilitada:

Paso 2: Limpia cualquier regla existente en `iptables` (esto eliminará todas las reglas existentes, así que ten cuidado):

Paso 3: Establece reglas de reenvío para el FTP:

Paso 4: Habilita el masquerading para que las respuestas del servidor se envíen de nuevo al cliente:

```

root@firewall:~
[root@firewall ~]# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@firewall ~]# sudo iptables -F
[root@firewall ~]# sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 21 -j DNAT --to-destination 172.16.0.3:21
[root@firewall ~]# sudo iptables -A FORWARD -p tcp -d 172.16.0.3 --dport 21 -j ACCEPT
[root@firewall ~]# sudo iptables -t nat -A POSTROUTING -j MASQUERADE
[root@firewall ~]#

```

Estas reglas de `iptables` reenviarán el tráfico entrante en el puerto 21 de `eth0` (la interfaz externa) al servidor FTP en `172.16.0.3`.

estos cambios en `iptables` no persistirán después de reiniciar la máquina. Si quieres que persistan, tendrías que instalar y configurar un servicio como `iptables-persistent` o recrear las reglas en cada inicio.

Paso 2: Configuración del servidor FTP seguro (VM2) con enfoque en seguridad

2.1. Instalación de vsftpd en VM2 (servidor):

```
[root@servidor ~]# sudo systemctl start vsftpd
[root@servidor ~]# sudo systemctl enable vsftpd --now
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/systemd/system/vsftpd.service.
[root@servidor ~]#
```

2.2. Crear un usuario y directorio:

```
root@servidor:~
[root@servidor ~]# sudo useradd -m -c "Usuario para vsftpd" -d "/home/ftpusuario" ftpusuario
[root@servidor ~]# sudo mkdir -p /home/ftpusuario/carpeta_ftp
[root@servidor ~]# sudo chmod -R 750 /home/ftpusuario/carpeta_ftp
[root@servidor ~]# sudo chown ftpusuario: /home/ftpusuario/carpeta_ftp
[root@servidor ~]# sudo passwd ftpusuario
Changing password for user ftpusuario.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@servidor ~]# echo ftpusuario >> /etc/vsftpd/user_list
[root@servidor ~]#
```

2.3. Configuración de vsftpd:

Abrir el archivo de configuración:

```
[root@servidor ~]# sudo vim /etc/vsftpd/vsftpd.conf
[root@servidor ~]#
```

```
root@servidor:~  
# capabilities.  
#  
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).  
anonymous_enable=NO  
#  
# Uncomment this to allow local users to log in.  
local_enable=YES  
#  
# Uncomment this to enable any form of FTP write command.  
write_enable=YES  
#  
# Default umask for local users is 077. You may wish to change this to 022,  
# if your users expect that (022 is used by most other ftpd's)  
local_umask=022  
  
dirmessage_enable=YES  
xferlog_enable=YES  
ftpd_banner=Bienvenido al Servicio FTP de JHON  
chroot_local_user=YES  
allow_writeable_chroot=YES  
anon_root=/var/anonymous/publico  
  
pasv_min_port=31500  
pasv_max_port=32500  
userlist_file=/etc/vsftpd/user_list  
userlist_deny=NO  
  
#  
# Uncomment this to allow the anonymous FTP user to upload files. This only  
# has an effect if the above global write enable is activated. Also, you will  
# obviously need to create a directory writable by the FTP user.  
# When SELinux is enforcing check for SE bool allow_ftpd_anon_write, allow_ftpd_full_access  
#anon_upload_enable=YES  
-- INSERT --
```

2.4. Configuración de SSL/TLS en vsftpd:

Generar el certificado:


```
root@servidor:~  
[root@servidor ~]# [root@servidor ~]# sudo systemctl restart vsftpd  
[root@servidor ~]#
```

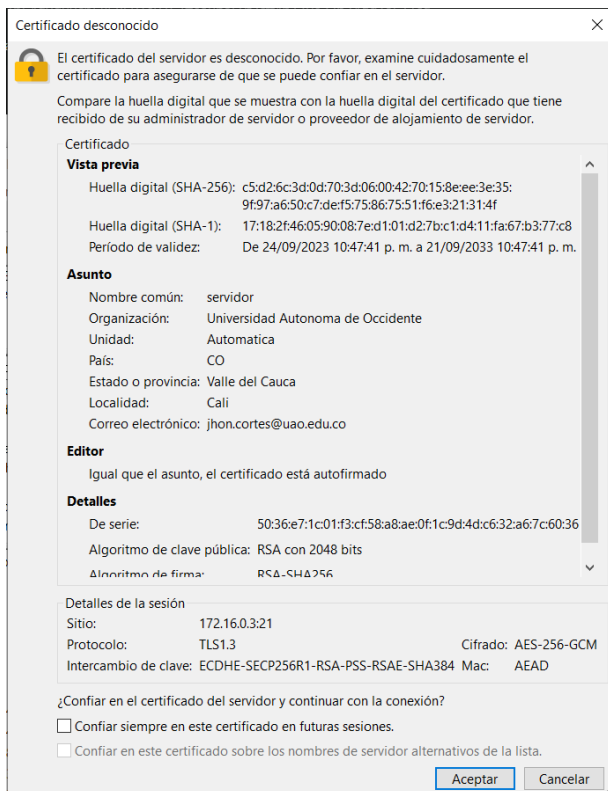
2.5. Configuración del firewall para vsftpd:

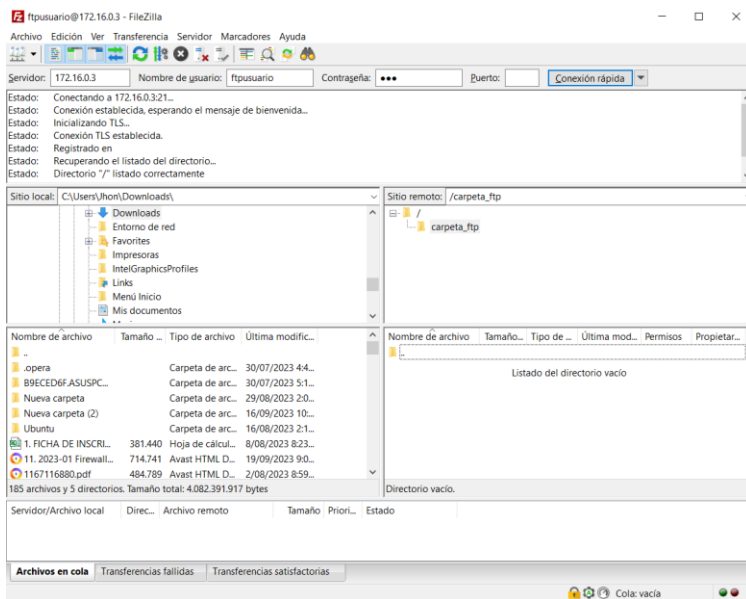
Si estás utilizando firewalld:

```
[root@servidor ~]# sudo systemctl start firewalld  
[root@servidor ~]# sudo firewall-cmd --permanent --add-port=20-21/tcp  
success  
[root@servidor ~]# sudo firewall-cmd --permanent --add-port=31500-32500/tcp  
success  
[root@servidor ~]# sudo firewall-cmd --reload  
success  
[root@servidor ~]#
```


Con esto, hemos configurado el servidor FTP seguro de acuerdo con la guía proporcionada. El siguiente paso será configurar el cliente Filezilla en el PC anfitrión y realizar pruebas.

Pruebas:





Certificado desconocido

 El certificado del servidor es desconocido. Por favor, examine cuidadosamente el certificado para asegurarse de que se puede confiar en el servidor.

Compare la huella digital que se muestra con la huella digital del certificado que tiene recibido de su administrador de servidor o proveedor de alojamiento de servidor.

Certificado

Vista previa

Huella digital (SHA-256): c5:d2:6c:3d:0d:70:3d:06:00:42:70:15:8e:ee:3e:35:9f:97:a6:50:c7:de:f5:75:86:75:51:f6:e3:21:31:4f

Huella digital (SHA-1): 17:18:2f:46:05:90:08:7e:d1:01:d2:7b:c1:d4:11:fa:67:b3:77:c8

Período de validez: De 24/09/2023 10:47:41 p. m. a 21/09/2033 10:47:41 p. m.

Asunto

Nombre común: servidor

Organización: Universidad Autonoma de Occidente

Unidad: Automatica

País: CO

Estado o provincia: Valle del Cauca

Localidad: Cali

Correo electrónico: jhon.cortes@uao.edu.co

Editor

Igual que el asunto, el certificado está autofirmado

Detalles

De serie: 50:36:e7:1c:01:f3:cf:58:a8:ae:0f:1c:9d:4d:c6:32:a6:7c:60:36

Algoritmo de clave pública: RSA con 2048 bits

Algoritmo de firma: RSA-SHA256

Detalles de la sesión

Sitio: 192.168.50.3:21

Protocolo: TLS1.3

Cifrado: AES-256-GCM

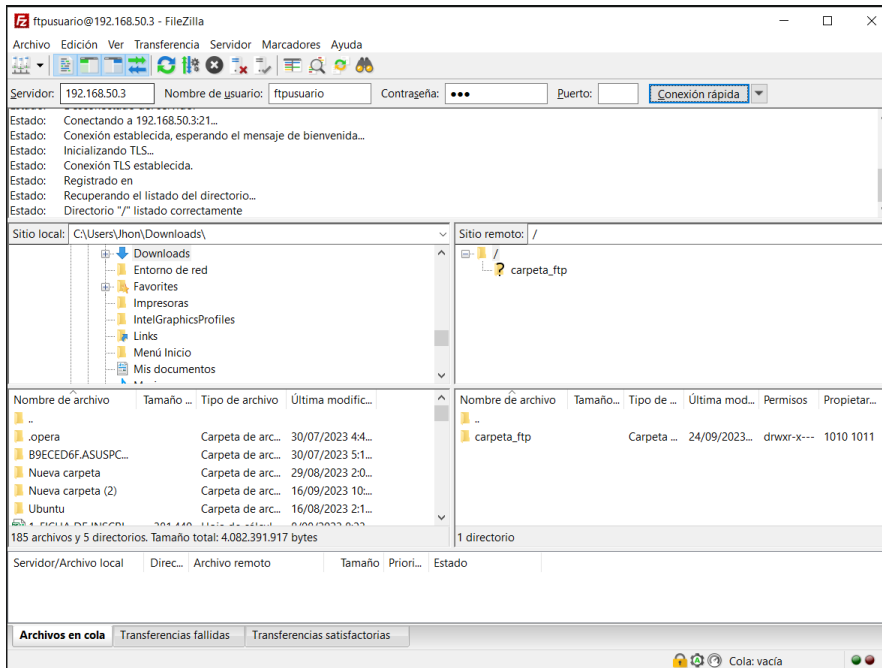
Intercambio de clave: ECDHE-SECP256R1-RSA-PSS-RSAE-SHA384

Mac: AEAD

¿Confiar en el certificado del servidor y continuar con la conexión?

☐ Confiar siempre en este certificado en futuras sesiones.

☐ Confiar en este certificado sobre los nombres de servidor alternativos de la lista.



Parte 2

Evaluación del Vagrantfile actual:

Podemos reutilizar estas VMs para nuestra topología actual, aunque el nombre "servidor" puede ser confuso en este contexto, ya que ahora tendrás dos servidores DNS. Sin embargo, para no alterar demasiado el Vagrantfile, mantendremos los nombres.

Configuración del Firewall (VM1):

Asignación de roles:

- VM1 (firewall): `firewall.servicios.com` - Punto de entrada y seguridad para toda la red.
- VM2 (servidor): `servidor2.servicios.com` - Servidor DNS secundario (esclavo).
- VM3 (cliente): `servidor3.servicios.com` - Servidor DNS maestro.

Paso a paso:

1. Configuración de DNS Maestro (VM3 - cliente):

1. Instalación de BIND:

```

[root@cliente ~]# sudo yum install bind bind-utils -y
CentOS Stream 9 - BaseOS                                27 kB/s | 17 kB    00:00
CentOS Stream 9 - AppStream                              42 kB/s | 18 kB    00:00
CentOS Stream 9 - Extras packages                        33 kB/s | 20 kB    00:00
Extra Packages for Enterprise Linux 9 - x86_64           43 kB/s | 47 kB    00:01
Extra Packages for Enterprise Linux 9 - x86_64           6.8 MB/s | 19 MB    00:02

```

1. Configuración de la zona en named.conf:

Edita el archivo /etc/named.conf:

```

[root@cliente ~]# sudo vim /etc/named.conf
[root@cliente ~]#

```

```

zone "servicios.com" IN {
    type master;
    file "/var/named/servicios.com.zone";
    allow-transfer {192.168.50.3; 172.16.0.3;}; // IP del servidor esclavo
};

```

1. Creación del archivo de zona:

Crea el archivo /var/named/servicios.com.zone:

```

[root@cliente ~]# sudo vim /var/named/servicios.com.zone
[root@cliente ~]#

```

```

root@cliente:~
$TTL 86400
@ IN SOA  servidor3.servicios.com. root.servicios.com. (
    2023092401 ;Serial
    3600      ;Refresh
    1800      ;Retry
    604800    ;Expire
    86400     ;Minimum TTL
)
@ IN NS   servidor3.servicios.com.
@ IN A    172.16.0.3
servidor3 IN A    172.16.0.3
servidor2 IN A    192.168.50.3
firewall  IN A    192.168.50.4

```

2. Configuración de DNS Secundario (VM2 - servidor):

1. Instalación de BIND:

```
[root@servidor parcial2]# sudo yum install bind bind-utils -y
CentOS Stream 9 - BaseOS                               33 kB/s | 17 kB   00:00
CentOS Stream 9 - BaseOS                               1.2 MB/s | 7.8 MB 00:06
CentOS Stream 9 - AppStream                             42 kB/s | 18 kB   00:00
CentOS Stream 9 - AppStream                             302 kB/s | 18 MB  01:00
CentOS Stream 9 - Extras packages                       30 kB/s | 20 kB   00:00
Extra Packages for Enterprise Linux 9 - x86_64          87 kB/s | 47 kB   00:00
Extra Packages for Enterprise Linux 9 - x86_64          13 MB/s | 19 MB   00:01
Extra Packages for Enterprise Linux 9 - Next - x86_64   109 kB/s | 62 kB  00:00
Package bind-32:9.16.23-13.el9.x86_64 is already installed.
Package bind-utils-32:9.16.23-13.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@servidor parcial2]#
```

1. Configuración de la zona en named.conf:

Edita el archivo `/etc/named.conf`:

```
zone "servicios.com" IN {
    type slave;
    file "/var/named/slaves/servicios.com.zone";
    masters { 172.16.0.3; };
};
```

Creación del directorio de zonas esclavas:

```
[root@servidor parcial2]# sudo mkdir /var/named/slaves
mkdir: cannot create directory '/var/named/slaves': File exists
[root@servidor parcial2]# sudo chown named:named /var/named/slaves
[root@servidor parcial2]#
```

3. Configuración del Firewall (VM1):

El tráfico DNS utiliza el puerto 53, así que asegúrate de que esté abierto en el firewall. Si no lo está, puedes abrirlo usando:

```
[root@firewall ~]# sudo firewall-cmd --add-service=dns --permanent
success
[root@firewall ~]# sudo firewall-cmd --reload
success
[root@firewall ~]#
```

3. Inicia y habilita el servicio BIND en ambas VMs:

```
sudo systemctl start named
```

```
sudo systemctl enable named
```

5. Pruebas:

Desde cualquier VM:

Ambas consultas deben devolver respuestas válidas.

Con todo lo anterior, tendrías un DNS maestro en VM3 (cliente) y un DNS esclavo en VM2 (servidor), con VM1 (firewall) actuando como firewall de la red.

```
[root@cliente ~]# dig @192.168.50.3 servicios.com

; <<>> DiG 9.16.23-RH <<>> @192.168.50.3 servicios.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 51204
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;; udp: 1232
; COOKIE: 7de8995dfe84425601000000651306292e2dc1dc8aea85b0 (good)
;; QUESTION SECTION:
;servicios.com.                IN      A

;; Query time: 4 msec
;; SERVER: 192.168.50.3#53(192.168.50.3)
;; WHEN: Tue Sep 26 16:26:17 UTC 2023
;; MSG SIZE rcvd: 70

[root@cliente ~]#
r parcial2]#
Query time: 5 msec
SERVER: 192.168.50.3#53(192.168.50.3)
WHEN: Tue Sep 26 16:26:06 UTC 2023
MSG SIZE rcvd: 70
```

```
[root@firewall ~]# [root@firewall ~]# dig @172.16.0.3 servicios.com
```

```
; <<>> DiG 9.16.23-RH <<>> @172.16.0.3 servicios.com  
; (1 server found)  
;; global options: +cmd  
;; connection timed out; no servers could be reached
```

```
[root@firewall ~]# dig @192.168.50.3 servicios.com
```

```
; <<>> DiG 9.16.23-RH <<>> @192.168.50.3 servicios.com  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 49353  
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1232  
; COOKIE: ca8ccd0c96a4a92c010000006513061ef4f28e604eb09568 (good)  
;; QUESTION SECTION:  
servicios.com.                IN      A  
  
;; Query time: 5 msec  
;; SERVER: 192.168.50.3#53(192.168.50.3)  
;; WHEN: Tue Sep 26 16:26:06 UTC 2023  
;; MSG SIZE rcvd: 70
```

```
[root@firewall ~]#
```