Nombre: Victor Manuel Gomez Zarama
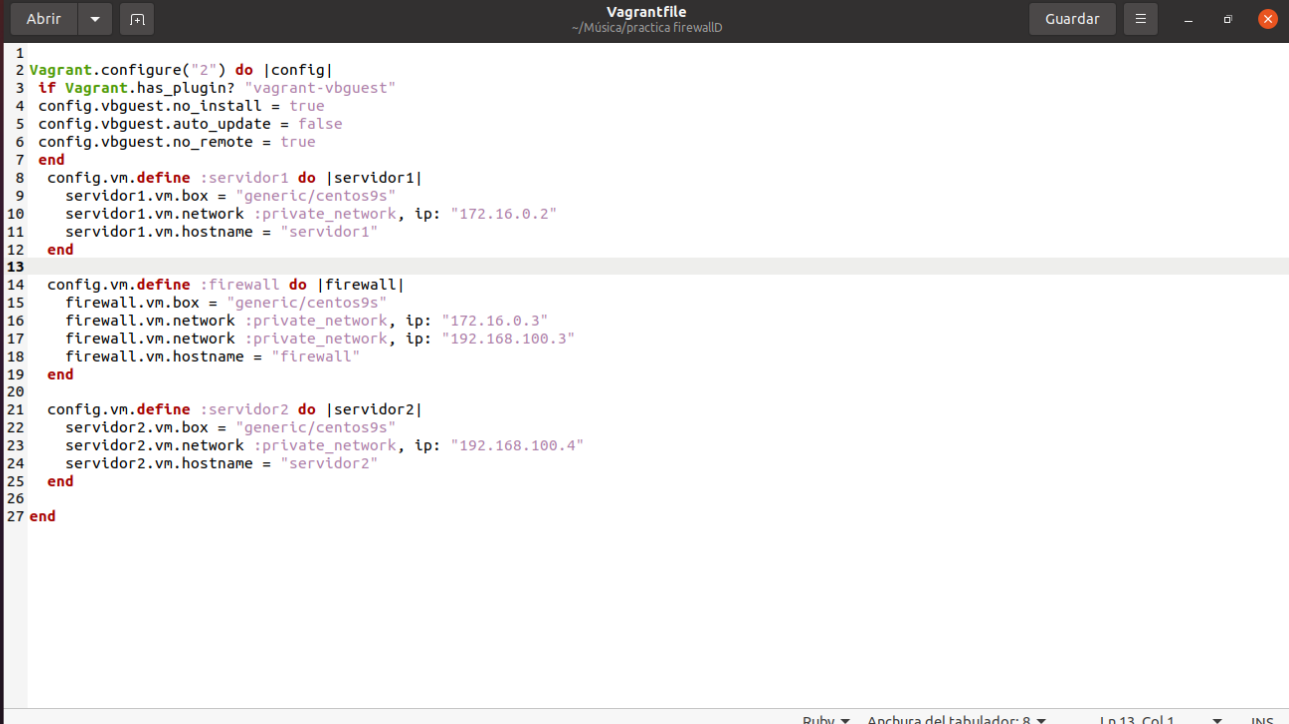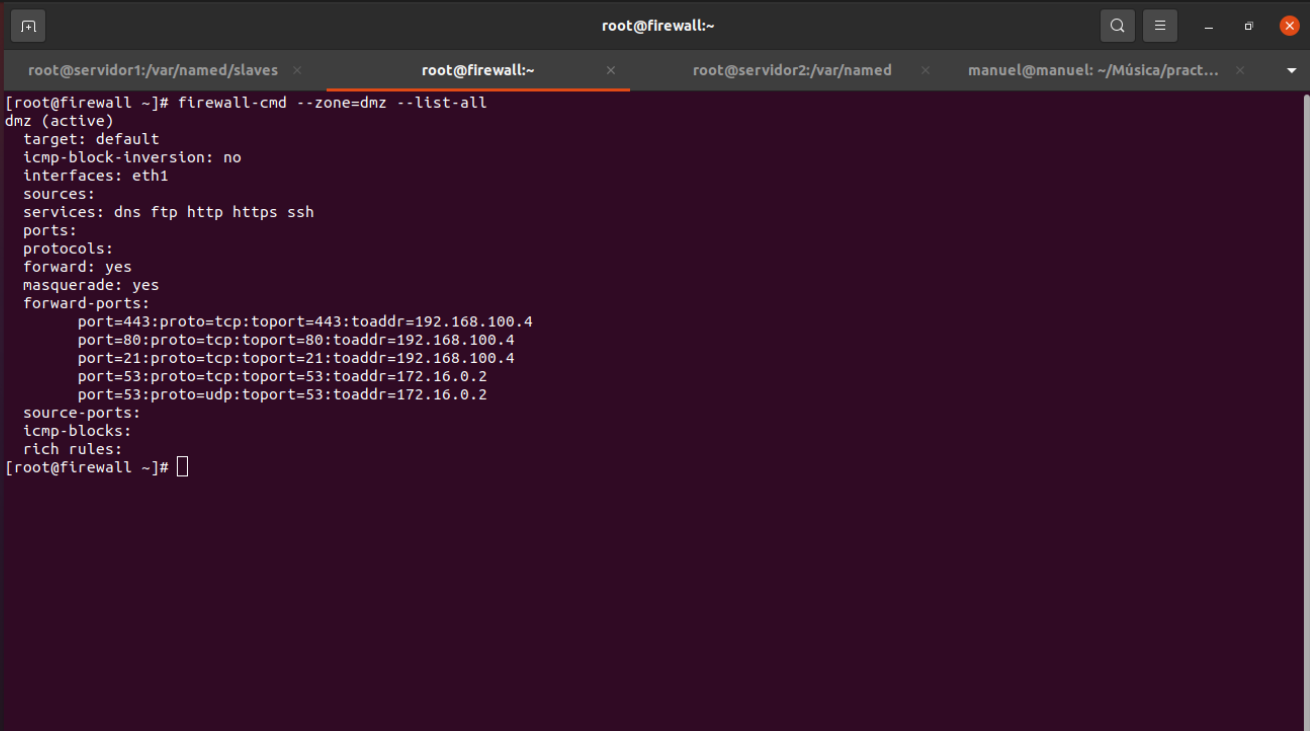


```ruby
Vagrant.configure("2") do |config|
  if Vagrant.has_plugin? "vagrant-vbguest"
    config.vbguest.no_install = true
    config.vbguest.auto_update = false
    config.vbguest.no_remote = true
  end
  config.vm.define :servidor1 do |servidor1|
    servidor1.vm.box = "generic/centos9s"
    servidor1.vm.network :private_network, ip: "172.16.0.2"
    servidor1.vm.hostname = "servidor1"
  end

  config.vm.define :firewall do |firewall|
    firewall.vm.box = "generic/centos9s"
    firewall.vm.network :private_network, ip: "172.16.0.3"
    firewall.vm.network :private_network, ip: "192.168.100.3"
    firewall.vm.hostname = "firewall"
  end

  config.vm.define :servidor2 do |servidor2|
    servidor2.vm.box = "generic/centos9s"
    servidor2.vm.network :private_network, ip: "192.168.100.4"
    servidor2.vm.hostname = "servidor2"
  end
end
```

PARTE 1:


```
[root@firewall ~]# firewall-cmd --zone=dmz --list-all
dmz (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth1
  sources:
  services: dns ftp http https ssh
  ports:
  protocols:
  forward: yes
  masquerade: yes
  forward-ports:
        port=443:proto=tcp:toport=443:toaddr=192.168.100.4
        port=80:proto=tcp:toport=80:toaddr=192.168.100.4
        port=21:proto=tcp:toport=21:toaddr=192.168.100.4
        port=53:proto=tcp:toport=53:toaddr=172.16.0.2
        port=53:proto=udp:toport=53:toaddr=172.16.0.2
  source-ports:
  icmp-blocks:
  rich rules:
[root@firewall ~]#
```

Nombre: Victor Manuel Gomez Zarama


```
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/xferlog
#
# If you want, you can have your log file in standard ftpd xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
                                                                    69,1         38%
```



```
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# 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
#
# 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
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
                                                                    1,1          Top
```

Nombre: Victor Manuel Gomez Zarama


```
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
# Make sure, that one of the listen options is commented !!
listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
allow_writeable_chroot=YES
ssl_enable=YES
rsa_cert_file=/etc/pki/tls/certs/ca.crt
rsa_private_key_file=/etc/pki/tls/private/ca.key

                                                              131,0-1          Bot
```

PARTE 2:


```
//

options {
        listen-on port 53 { 127.0.0.1;192.168.100.4;};
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        secroots-file   "/var/named/data/named.secroots";
        recursing-file  "/var/named/data/named.recursing";
        allow-query     { localhost;172.16.0.0/24;192.168.100.0/24;};

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-validation yes;

        managed-keys-directory "/var/named/dynamic";
        geoip-directory "/usr/share/GeoIP";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";

        /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
        include "/etc/crypto-policies/back-ends/bind.config";
};

logging {
                                                              39,0-1          21%
```

Nombre: Victor Manuel Gomez Zarama


```
        managed-keys-directory "/var/named/dynamic";
        geoip-directory "/usr/share/GeoIP";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";

        /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
        include "/etc/crypto-policies/back-ends/bind.config";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

/* zona hacia adelante*/
zone "techcraft.com" IN {
 type master;
 file "techcraft.com.fwd";
};
/* Zona reversa*/
zone "0.16.172.in-addr.arpa" IN {
 type master;
 file "techcraft.com.rev";

};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

                                                    70,0-1        Bot
```



```
        include "/etc/crypto-policies/back-ends/bind.config";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};




/* zona hacia adelante*/
zone "techcraft.com" IN {
 type slave;
 file "slaves/techcraft.com.fwd";
 masters {192.168.100.4; };
};

zone "0.16.172.in-addr.arpa" IN {
 type slave;
 file "slaves/techcraft.com.rev";
 masters {192.168.100.4; };
};




include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

"/etc/named.conf" 78L, 1994B                       78,0-1        Bot
```

Nombre: Victor Manuel Gomez Zarama


```
root@servidor2:/var/named

$ORIGIN 0.16.172.in-addr.arpa.
$TTL 3H
@       IN      SOA     servidor3.techcraft.com. root@techcraft.com. (
                                0       ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H      ; minimum TTL
                                )
@       IN      NS      servidor3.techcraft.com.

;host en la zona
2 IN PTR servidor3.techcraft.com.
3 IN PTR servidor2.techcraft.com.
4 IN PTR firewall.techcraft.com.
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"techcraft.com.rev" 16L, 358B                                    3,30-40        All
```



```
root@servidor2:/var/named

$ORIGIN techcraft.com.
$TTL 3H
@       IN SOA      servidor3.techcraft.com. root@techcraft.com. (
                                0       ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H      ; minimum TTL
                                )
@       IN      NS      servidor3.techcraft.com.

;host en la zona
servidor3 IN    A       192.168.100.4
servidor2 IN    A       172.16.0.2
firewall  IN    A       172.16.0.3
~
~
~
~
~
~
~
~
~
~
~
~
~
"techcraft.com.fwd" 16L, 350B                                    14,32          All
```