**Paso 1: Configurar el Servidor FTP Seguro**

**Instalamos un servidor FTP seguro vsftpd y nos asegúrate de configurarlo para que funcione de manera segura con SSL/TLS.**

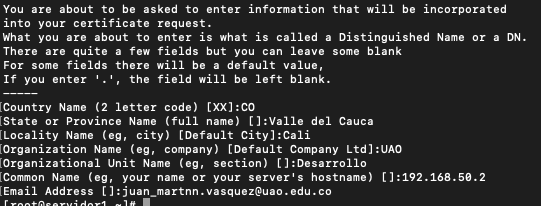
yum install vsftpd

**Generamos el certificado:**

mkdir -p /etc/ssl/vsftpd

openssl req -x509 -nodes -keyout /etc/ssl/vsftpd/vsftpd.pem -out /etc/ssl/vsftpd/vsftpd.pem -days 365 -newkey rsa:2048

**Configuramos el certificado:**



**Paso 2: Configurar VSFTPD para usar SSL/TLS**

vim /etc/vsftpd/vsftpd.conf

**# Configuración FTP SEGURO**

**anonymous\_enable=NO**

**local\_enable=YES**

**write\_enable=YES**

**local\_umask=022**

**anon\_upload\_enable=YES**

**dirmessage\_enable=YES**

**xferlog\_enable=YES**

**connect\_from\_port\_20=YES**

**xferlog\_std\_format=YES**

**ftpd\_banner=Bienvenidos al parcial**

**chroot\_local\_user=YES**

**allow\_writeable\_chroot=YES**

**listen=YES**

**listen\_ipv6=NO**

**pam\_service\_name=vsftpd**

**userlist\_enable=YES**

**userlist\_deny=NO**

**# Configuración FTP SEGURO**

**ssl\_enable=YES**

**ssl\_tlsv1\_2=YES**

**ssl\_sslv2=NO**

**ssl\_sslv3=NO**

**rsa\_cert\_file=/etc/ssl/vsftpd/vsftpd.pem**

**rsa\_private\_key\_file=/etc/ssl/vsftpd/vsftpd.pem**

**allow\_anon\_ssl=NO**

**force\_local\_data\_ssl=YES**

**force\_local\_logins\_ssl=YES**

**require\_ssl\_reuse=NO**

**ssl\_ciphers=HIGH**

**debug\_ssl=YES**

**pasv\_enable=YES**

**pasv\_min\_port=40000**

**pasv\_max\_port=50000**

**pasv\_promiscuous=YES**

**Reiniciamos**

systemctl restart vsftpd

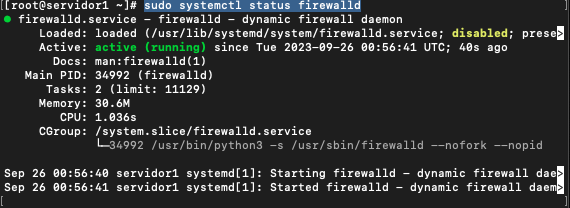
**CONFIGURACION DEL FIREWALL**

sudo systemctl stop firewalld

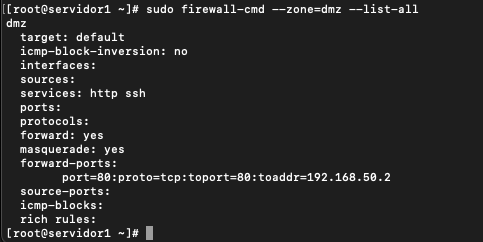
sudo systemctl restart firewalld

sudo systemctl start firewalld

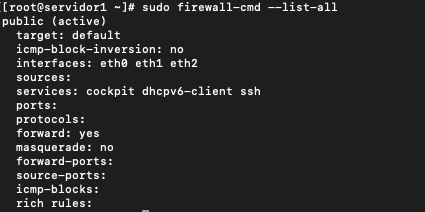
sudo systemctl status firewalld

****

sudo firewall-cmd --zone=dmz --list-all

****

sudo firewall-cmd --list-all

****

firewall-cmd --get-active-zones

****

sudo firewall-cmd --zone=dmz --add-port=990/tcp –permanent

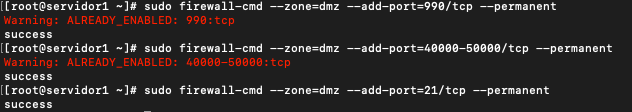
****

**Abre el puerto 990 (control) y el rango de puertos pasivos en la zona dmz (ajusta según tu configuración)**

sudo firewall-cmd --zone=dmz --add-port=990/tcp –permanent

sudo firewall-cmd --zone=dmz --add-port=40000-50000/tcp –permanent

sudo firewall-cmd --zone=dmz --add-port=21/tcp –permanent

****

sudo firewall-cmd –reload

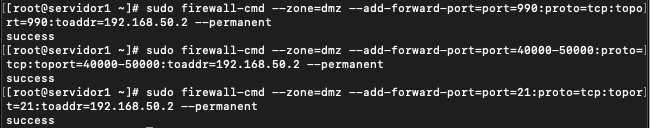
**Redirige las solicitudes de FTP seguro al servidor FTP seguro (192.168.50.2) en la zona**

**Redirige el tráfico de los puertos 990 y 40000-50000 hacia el servidor FTP seguro en la zona dmz (ajusta la dirección IP según tu configuración)**

sudo firewall-cmd --zone=dmz --add-forward-port=port=990:proto=tcp:toport=990:toaddr=192.168.50.2 –permanent

sudo firewall-cmd --zone=dmz --add-forward-port=port=40000-50000:proto=tcp:toport=40000-50000:toaddr=192.168.50.2 –permanent

sudo firewall-cmd --zone=dmz --add-forward-port=port=21:proto=tcp:toport=21:toaddr=192.168.50.2 –permanent

****

**Habilitar ftp a zona dmz**

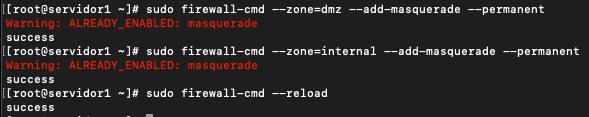
sudo firewall-cmd --permanent --zone=dmz --add-service=ftp

**Masquerade zona dmz y internal**

sudo firewall-cmd --zone=dmz --add-masquerade –permanent

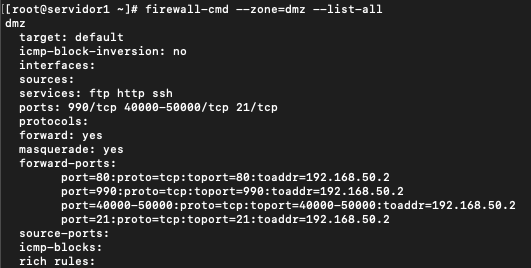
sudo firewall-cmd --zone=internal --add-masquerade –permanent

sudo firewall-cmd –reload

****

**Validar con el siguiente comando**

firewall-cmd --zone=dmz --list-all

****

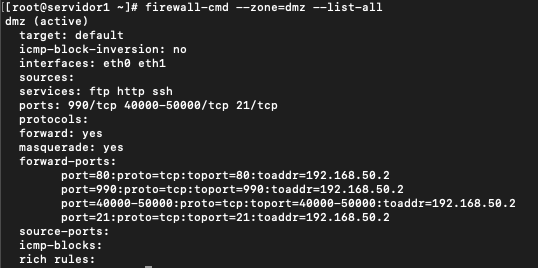
**La zona por default debe ser la dmz**

sudo firewall-cmd --set-default-zone=dmz

****

**Configuración actual**

firewall-cmd --zone=dmz --list-all

****

firewall-cmd --get-default-zone



**Si no esta dmz a la zona default**

**asignarla**

**La zona por default debe ser la dmz**

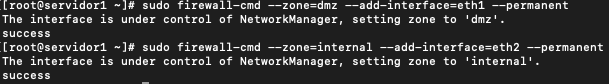
sudo firewall-cmd --set-default-zone=dmz

****

**Agregar a la zona dmz e internal**

sudo firewall-cmd --zone=dmz --add-interface=eth1 –permanent

sudo firewall-cmd --zone=internal --add-interface=eth2 –permanent

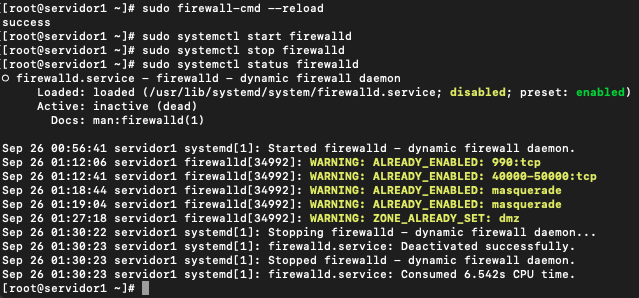
****

sudo firewall-cmd –reload

sudo systemctl start firewalld

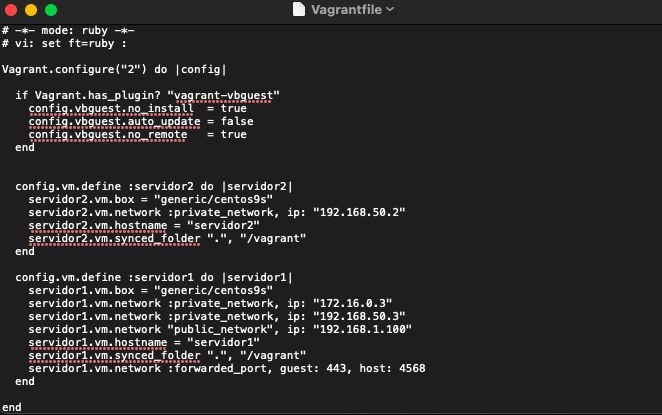
sudo systemctl stop firewalld

sudo systemctl status firewalld

****

**Agregar ip publica al vagrantfile y darle vagrant reload servidor**

vm.network "public\_network", ip: "192.168.1.100"



sudo firewall-cmd --zone=dmz --add-rich-rule='rule family="ipv4" source address="192.168.1.100" port protocol="tcp" port="21" accept'

sudo firewall-cmd --zone=dmz --add-rich-rule='rule family="ipv4" source address="192.168.1.100" port protocol="tcp" port="40000-50000" accept'

sudo firewall-cmd --zone=dmz --add-rich-rule='rule family="ipv4" source address="192.168.1.100" port protocol="tcp" port="21" accept'

sudo firewall-cmd --zone=dmz --add-rich-rule='rule family="ipv4" source address="192.168.1.100" port protocol="tcp" port="40000-50000" accept'

sudo firewall-cmd --zone=dmz --add-rich-rule='rule family="ipv4" source address="192.168.1.100" port protocol="tcp" port="21" accept'

sudo firewall-cmd --zone=dmz --add-rich-rule='rule family="ipv4" source address="192.168.1.100" port protocol="tcp" port="40000-50000" accept'

sudo firewall-cmd --reload