PARCIAL 2

Angie Feligrana

Jose Daniel Cruz

Punto 1. FTP Seguro

Vagranfile utilizado

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 :cliente do |cliente|

cliente.vm.box = "generic/centos9s"

cliente.vm.network :private\_network, ip: "192.168.50.2"

cliente.vm.hostname = "cliente"

cliente.vm.synced\_folder ".", "/vagrant"

end

config.vm.define :servidor do |servidor|

servidor.vm.box = "generic/centos9s"

servidor.vm.network :private\_network, ip: "192.168.50.3"

servidor.vm.network :private\_network, ip: "172.16.0.3"

servidor.vm.network :forwarded\_port, host: 5567, guest:80

servidor.vm.network :forwarded\_port, host: 5568, guest:443

servidor.vm.hostname = "servidor"

servidor.vm.synced\_folder ".", "/vagrant"

end

config.vm.define :firewall do |firewall|

firewall.vm.box = "generic/centos9s"

firewall.vm.network :private\_network, ip: "192.168.50.4"

firewall.vm.hostname = "firewall"

firewall.vm.synced\_folder ".", "/vagrant"

end

end

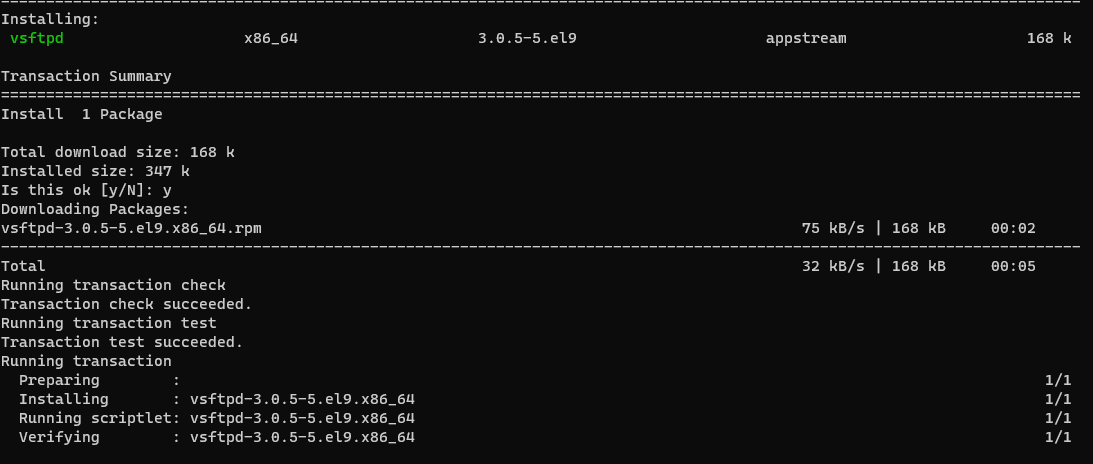
Configuración del ftp

Instalamos el vsftpd

sudo dnf install vsftpd

sudo systemctl start vsftpd

sudo systemctl enable vsftpd –now





Creamos usuario y Directorio con superusuario

useradd -m -c "Usuario para vsftpd" -d "/home/ ftpuserparcial " ftpuserparcial

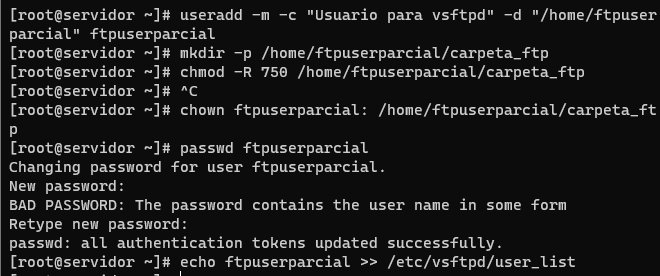
mkdir -p /home/ftpus ftpuserparcial ario/carpeta\_ftp

chmod -R 750 /home/ ftpuserparcial /carpeta\_ftp

chown ftpuserparcial: /home/ ftpuserparcial /carpeta\_ftp

passwd ftpuserparcial

ftpuserparcial >> /etc/vsftpd/user\_list



Configuracion vsftpd

Vim /etc/vsftpd/vsftpd.conf

Se agregaron las siguientes líneas:

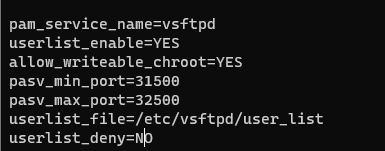
allow\_writeable\_chroot=YES

pasv\_min\_port=31500

pasv\_max\_port=32500

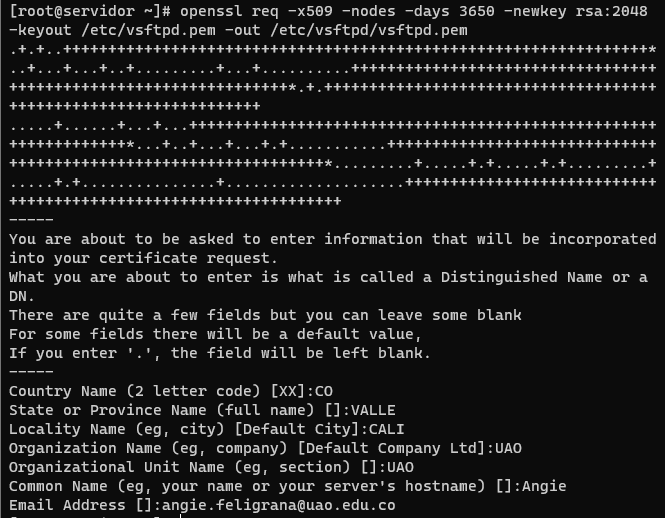
userlist\_file=/etc/vsftpd/user\_list

userlist\_deny=NO



Configuracion SSL para generar certificado

openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout /etc/vsftpd.pem -out /etc/vsftpd/vsftpd.pem



Se agregan las lineas de certificación a la configuración

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

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

ssl\_enable=YES

Texto

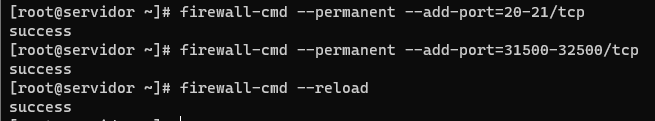
Descripción generada automáticamente

Reiniciamos el vsftpd

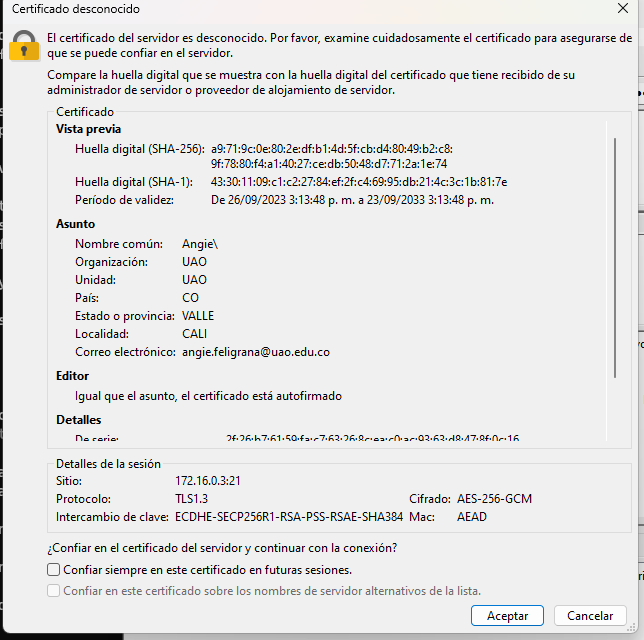
Service vstpd restart



Configuración del firewalld con el vsftpd



Prueba



Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Configuración desde firewalld

Instalación

Yum install firewalld

Texto

Descripción generada automáticamente

Iniciamos el servicio firewalld



Configuramos el aseguramiento de los solicitudes

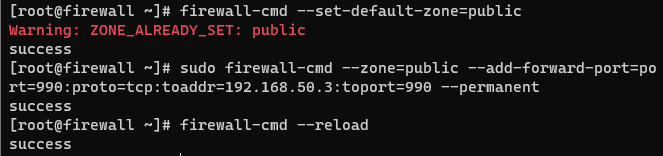
# Configuramos la zona por defecto a "public"

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

# Reenviamos el puerto 990 (FTPS) a través del firewall al servidor FTP sudo firewall-cmd --zone=public --add-forward-port=port=990:proto=tcp:toaddr=192.168.50.3:toport=990 --permanent

# Recargamos las reglas del firewall para que los cambios tengan efecto

sudo firewall-cmd –reload



Configuramos las zonas public,internal y dmz

firewall-cmd --zone=public --change-interface=eth0 –permanent

firewall-cmd --zone=dmz --change-interface=eth1 --permanent

firewall-cmd --zone=internal --change-interface=eth2 –permanent

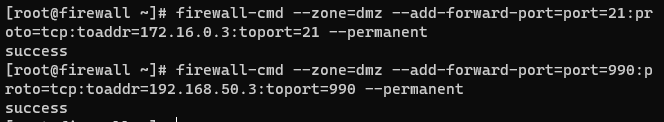
Texto

Descripción generada automáticamente

**Asegurarse de que las reglas de reenvío de puertos están en la zona DMZ:**

firewall-cmd --zone=dmz --add-forward-port=port=21:proto=tcp:toaddr=172.16.0.3:toport=21 --permanent

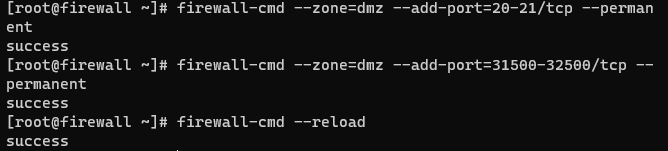
firewall-cmd --zone=dmz --add-forward-port=port=990:proto=tcp:toaddr=192.168.50.3:toport=990 –permanent



**Asegurarse de que los puertos requeridos están abiertos en la zona DMZ:**

firewall-cmd --zone=dmz --add-port=20-21/tcp --permanent

firewall-cmd --zone=dmz --add-port=31500-32500/tcp –permanent



Verificacion de las zonas y las interfaces

Texto

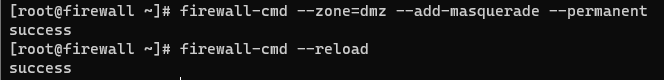
Descripción generada automáticamente

Agregar el servicio ftp a la zona dmz

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



Habilitar masquerada y habilitar las reglas



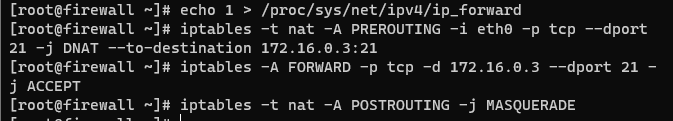
Verificacion

Texto

Descripción generada automáticamente

**Usar IPTABLES directamente para el reenvío de paquetes**:

echo 1 > /proc/sys/net/ipv4/ip\_forward



Prueba desde filezilla

