**Presentacion parcial**

**En servidor2 (192.168.50.2) - bloquear acceso directo**

**• Denegar todo incoming por defecto**

**• Permitir 192.168.50.3 entrar a los puertos de servicio**

**• SSH solo desde el firewall**

**sudo ufw status numbered**

**#Para probarlo interaremos acceder a un servicio apuntando directamente al servidor2**

**Debe fallar**

**curl -I http://192.168.50.2**

**Debe responde**

**curl -I http://192.168.50.2**

**#Validamos ftps desde C:\Users\Juan>ftp 192.168.50.3**

**#No nos permite usuarios anonimos**

**ftp 192.168.50.3**

**Usuario: anonymous**

**------------------------------------------------**

**#Los usuarios locales solo los permite con ftps**

**C:\Users\Juan>ftp 192.168.50.3**

**Conectado a 192.168.50.3.**

**220 (vsFTPd 3.0.5)**

**200 Always in UTF8 mode.**

**Usuario (192.168.50.3:(none)): fptuser**

**530 Non-anonymous sessions must use encryption.**

**Conexión cerrada por el host remoto.**

**-----------------------------------------------------------------------**

**#Configuracion del servidor1 Firewall para que enrute al servidor2**

**Servidor1 192.168.50.3**

**Habilitamos SHH (puerto 22)**

**Habilitamos ufw**

**Aqui se agregan las reglas**

**/etc/default/ufw**

**habilita a tu firewall (servidor1) para reenviar paquetes a otras máquinas, permitiendo el port forwarding hacia tu servidor2.**

**DEFAULT\_FORWARD\_POLICY="ACCEPT"**

**vim /etc/ufw/sysctl.conf**

**DEscomentacmos esta linea para permitir el ip\_forward en ipv4**

**net/ipv4/ip\_forward=1**

**vim /etc/ufw/before.rules (Redireccionamiento)**

**definimos a donde se van a enviar las peticiones que llegan a ese servidor1**

**21 FTp - para conexion de control**

**443 Https**

**80 Http**

**990 Cifrado TLS para FTP implicito**

**---------------------------**

**Paso 1 — Endurecer servidor2 (bloquear acceso directo)**

En servidor2 (192.168.50.2)

* Denegar todo **incoming** por defecto
* Permitir 192.168.50.3 entrar a los puertos de servicio
* SSH solo desde el firewall

En servidor2:

# Políticas base

sudo ufw default deny incoming

sudo ufw default allow outgoing

# Permitir SOLO desde el firewall (192.168.50.3)

sudo ufw allow from 192.168.50.3 to any port 80 proto tcp

sudo ufw allow from 192.168.50.3 to any port 443 proto tcp

# Dejamos listos los puertos de FTPS (los usarás en el punto de FTPS)

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 990 proto tcp

sudo ufw allow from 192.168.50.3 to any port 30000:30100 proto tcp

# (Opcional pero recomendado) SSH solo desde el firewall

sudo ufw allow from 192.168.50.3 to any port 22 proto tcp

# Activar y revisar

sudo ufw enable

sudo ufw status numbered

Resultado esperado: si curl -I http://192.168.50.2 desde **host**, debe fallar (bloqueado). Solo el firewall podrá entrar a 80/443/21/990/30000-30100.

Paso 2

 **DNAT**: cambia el **destino** del paquete (redirige al servidor interno).

 **MASQUERADE**: cambia el **origen** del paquete (para que parezca que todo viene del firewall).

 **IP forwarding** → servidor1 puede reenviar tráfico.

 **UFW en servidor1** → define qué puertos del mundo exterior están abiertos.

 **DNAT + MASQUERADE** → hace que el tráfico de esos puertos se redirija a servidor2, pero siempre pasando por servidor1.

Paso 3

Servidor2

listen=YES

listen\_ipv6=NO

ssl\_enable=YES

allow\_anon\_ssl=NO

force\_local\_data\_ssl=YES

force\_local\_logins\_ssl=YES

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

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

pasv\_enable=YES

pasv\_min\_port=30000

pasv\_max\_port=30100

# --- Habilitar usuarios locales y desactivar anónimo ---

anonymous\_enable=NO

local\_enable=YES

write\_enable=YES

# (Opcional recomendado) Enjaular al usuario en su $HOME

chroot\_local\_user=YES

# Si el HOME del usuario es escribible, vsftpd lo bloquea por seguridad.

# Habilita esta excepción o crea un subdirectorio para subir archivos.

allow\_writeable\_chroot=YES

# Asegura que PAM esté activo para autenticar usuarios del sistema

pam\_service\_name=vsftpd

# Anunciar la IP del FIREWALL (punto de entrada)

pasv\_address=192.168.50.3

~ "/etc/vsftpd.conf" 31L, 796B   
  
  
Pruebas:

Entra al usuario ftpuser del servidor2

vagrant@servidor2:~$ su – ftpuser