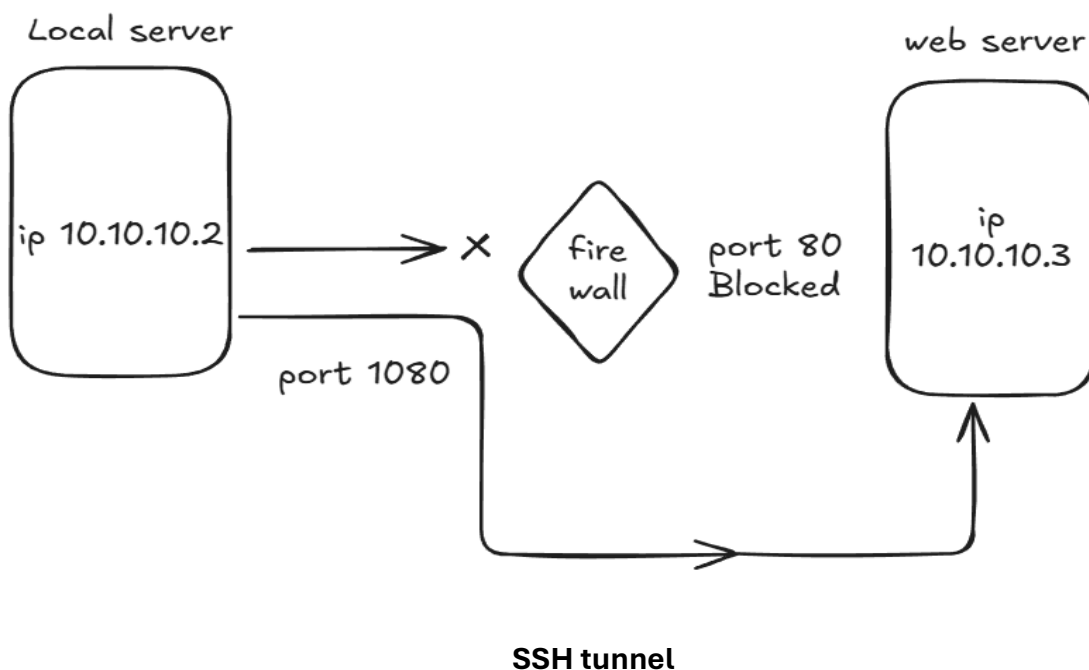


Dynamic Port Forwarding with SSH

Purpose:

Create a SOCKS proxy using SSH to allow applications (Browser, Curl) to route traffic dynamically to any destination through an encrypted SSH tunnel.

Lab



Components

Component	Description
VM1	Local server (Client)
VM2	Remote Web server
Nginx	Web service on port 80
SSH	Service on port 22
Firewall	Port 80 blocked on Web server

Prerequisites

- SSH access to remote server
- Web service running on remote server
- SSH service running
- Port 80 blocked on Web server

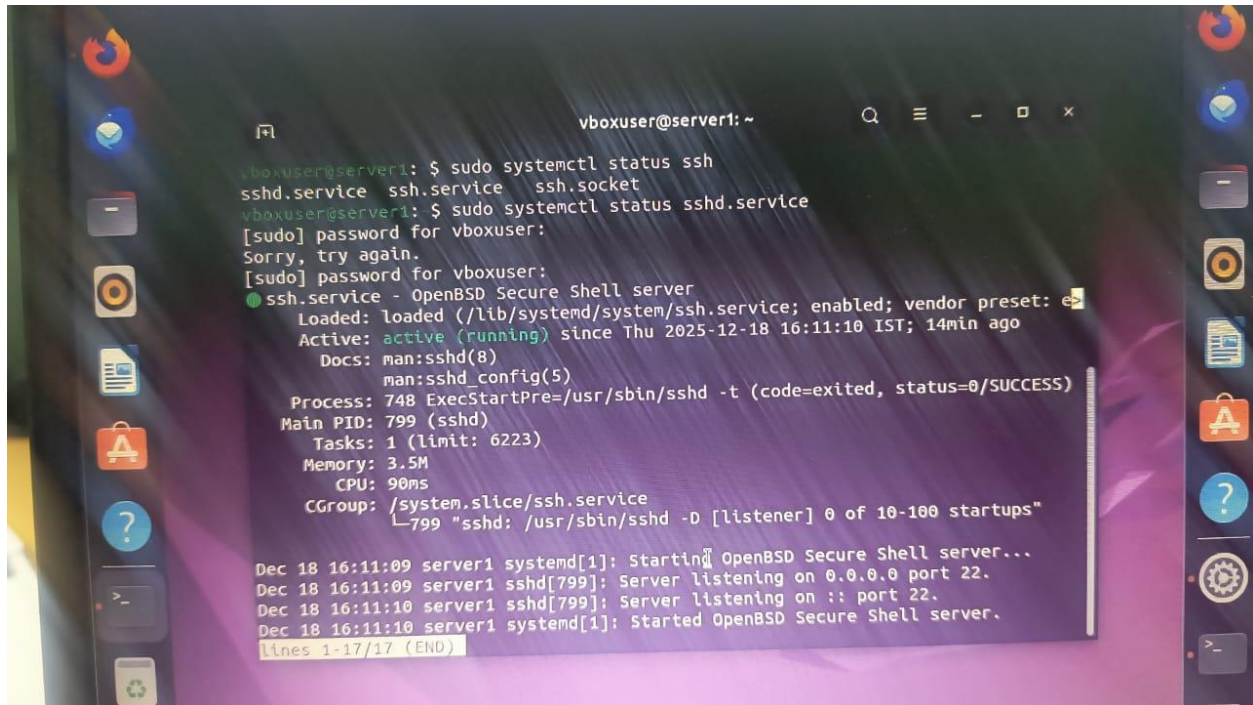
Step 1: Verify Web Service on Client VM (10.10.1.3)

```
vboxuser@server2: ~  
vboxuser@server2: $ sudo systemctl status nginx.service  
[sudo] password for vboxuser:  
● nginx.service - A high performance web server and a reverse proxy server  
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: en  
   Active: active (running) since Thu 2025-12-18 16:15:41 IST; 3min 23s ago  
     Docs: man:nginx(8)  
    Process: 639 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process  
    Process: 703 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (co  
 Main PID: 712 (nginx)  
    Tasks: 2 (limit: 2268)  
   Memory: 8.1M  
      CPU: 176ms  
   CGroup: /system.slice/nginx.service  
           └─712 "nginx: master process /usr/sbin/nginx -g daemon on; master  
             719 "nginx: worker process" "" "" "" "" "" "" "" "" "" "" "" "" ""  
  
Dec 18 16:15:39 server2 systemd[1]: Starting A high performance web server and  
Dec 18 16:15:41 server2 systemd[1]: Started A high performance web server and ap  
lines 1-16/16 (END)
```

```
sudo systemctl status nginx
# OR
sudo systemctl status apache2
```

Check that the web service is running.

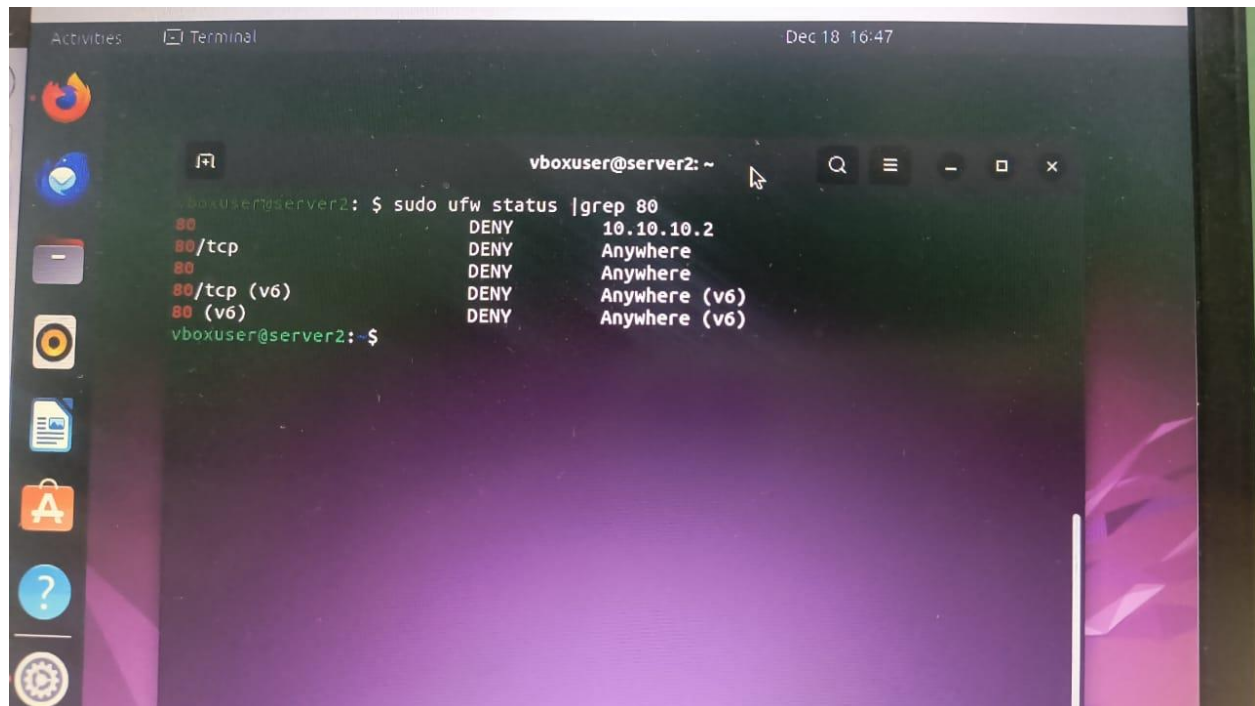
Step 2: Verify SSH Service on VM (10.10.10.2)

A screenshot of a terminal window on a Linux desktop. The terminal shows the user 'vboxuser' at 'server1' running the command 'sudo systemctl status ssh'. The output shows that the 'ssh.service' is loaded and active (running) since Thursday, 2025-12-18 at 16:11:10 IST. It also shows the process details for 'sshd' and the log messages indicating the service started successfully. The desktop background is dark with various application icons on the left and right sides.

```
vboxuser@server1: ~  
vboxuser@server1: $ sudo systemctl status ssh  
ssh.service ssh.service ssh.socket  
vboxuser@server1: $ sudo systemctl status sshd.service  
[sudo] password for vboxuser:  
Sorry, try again.  
[sudo] password for vboxuser:  
● ssh.service - OpenBSD Secure Shell server  
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: en  
   Active: active (running) since Thu 2025-12-18 16:11:10 IST; 14min ago  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
   Process: 748 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)  
    Main PID: 799 (sshd)  
      Tasks: 1 (limit: 6223)  
     Memory: 3.5M  
        CPU: 90ms  
   CGroup: /system.slice/ssh.service  
           └─799 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"  
  
Dec 18 16:11:09 server1 systemd[1]: Starting OpenBSD Secure Shell server...  
Dec 18 16:11:09 server1 sshd[799]: Server listening on 0.0.0.0 port 22.  
Dec 18 16:11:10 server1 sshd[799]: Server listening on :: port 22.  
Dec 18 16:11:10 server1 systemd[1]: Started OpenBSD Secure Shell server.  
lines 1-17/17 (END)
```

```
sudo systemctl status ssh  
# Check listening port  
sudo ss -tln | grep :22
```

Step 3: Verify Port 80 Blocked on Web Server

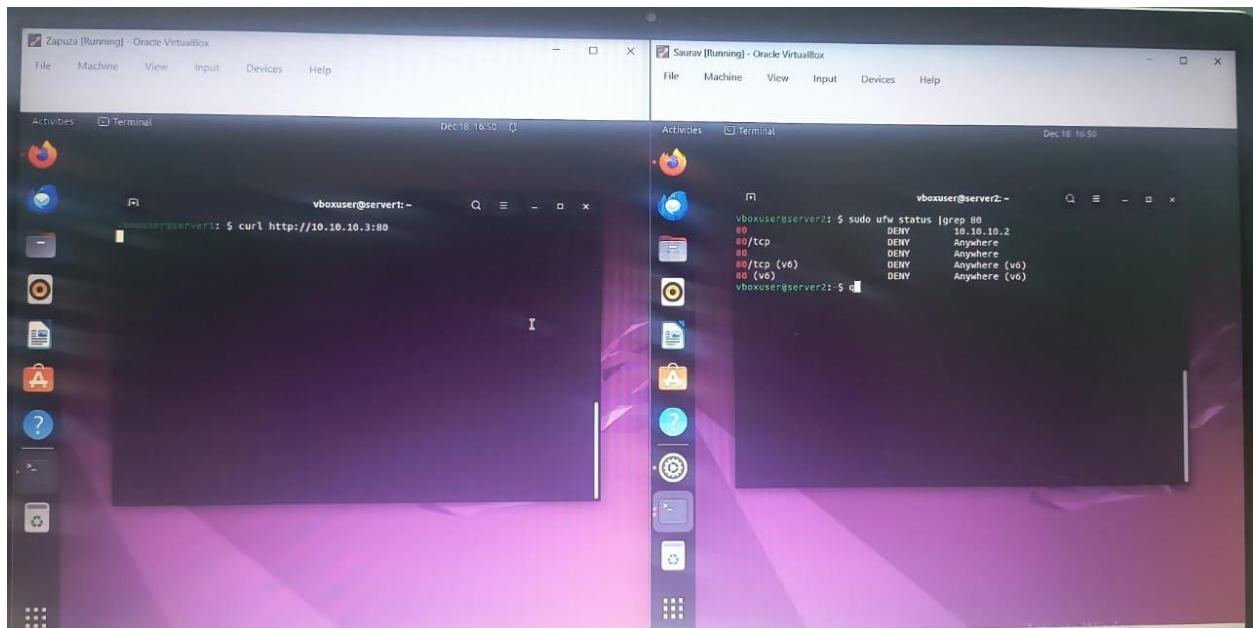
A screenshot of a Linux terminal window. The terminal title bar shows 'Activities', 'Terminal', and the date/time 'Dec 18 16:47'. The prompt is 'vboxuser@server2: ~'. The command 'sudo ufw status | grep 80' has been executed, resulting in the following output:

```
vboxuser@server2: $ sudo ufw status | grep 80
80 DENY 10.10.10.2
80/tcp DENY Anywhere
80 DENY Anywhere
80/tcp (v6) DENY Anywhere (v6)
80 (v6) DENY Anywhere (v6)
vboxuser@server2:~$
```

The terminal output shows that port 80 is blocked (DENY) for the IP 10.10.10.2 and for all incoming traffic (Anywhere) on both IPv4 and IPv6.

```
sudo ufw status | grep 80
```

Step 4: Direct Access Test (Expected to Fail)

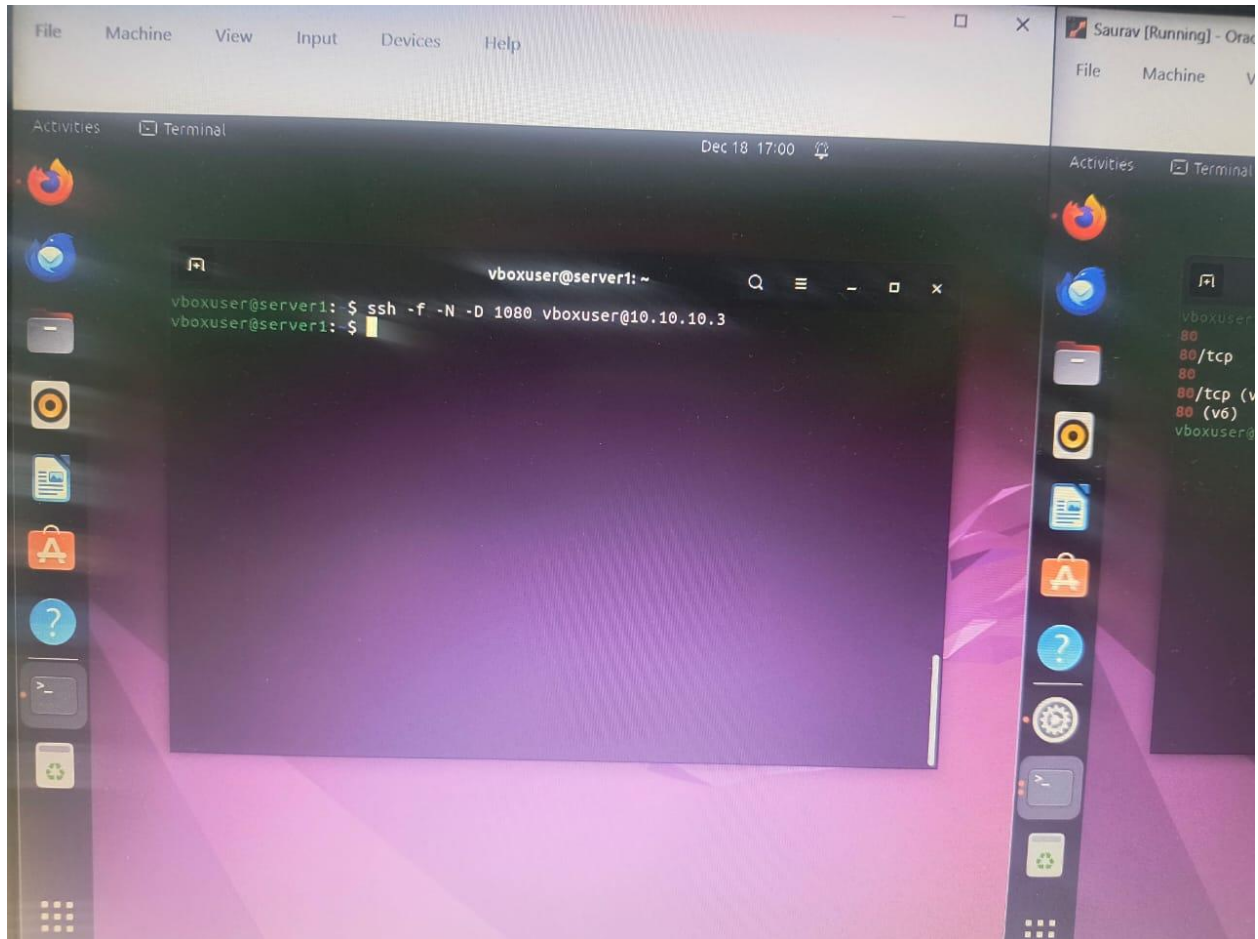


From Server VM (10.10.10.2):

`curl http://10.10.10.3:80`

Fails due to firewall restrictions or localhost binding.

Step 5: Create SSH Dynamic Port Forwarding



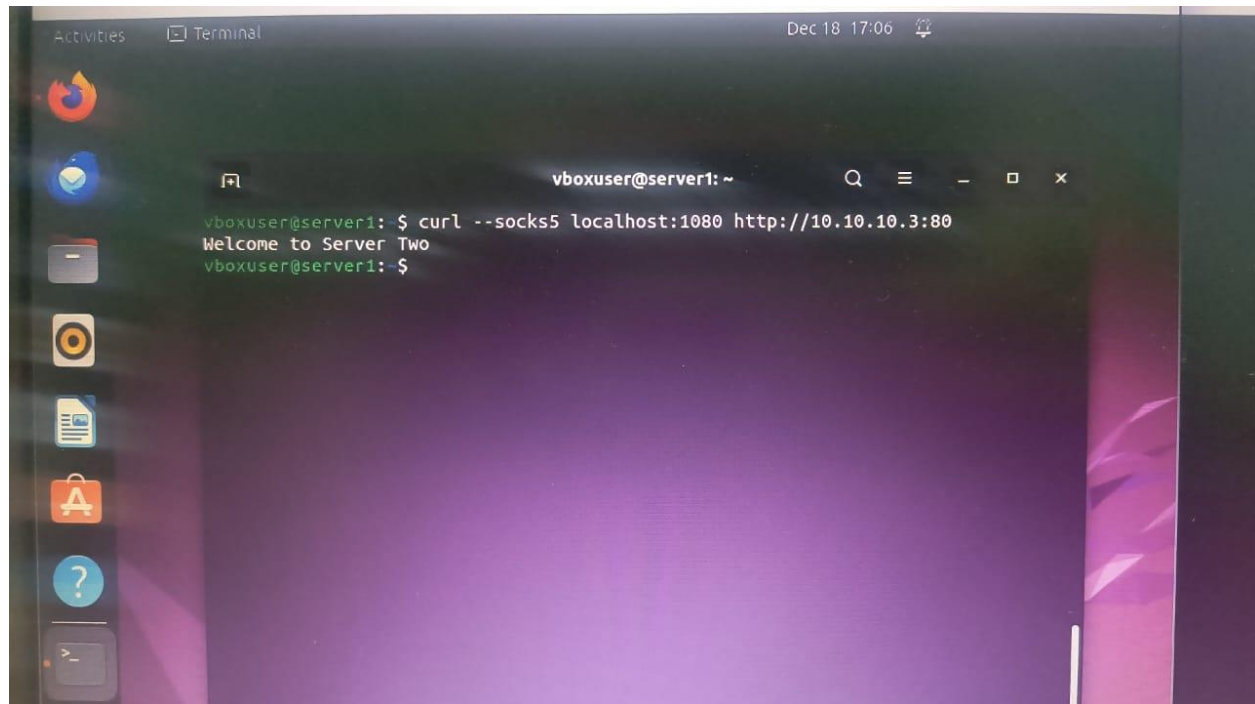
On Client VM (10.10.10.2):

```
ssh -f -N -D 1080 username@Server_IP
```

Flags Explained:

- -D → Dynamic port forwarding
- -f → Run SSH in background
- -N → Do not open remote shell

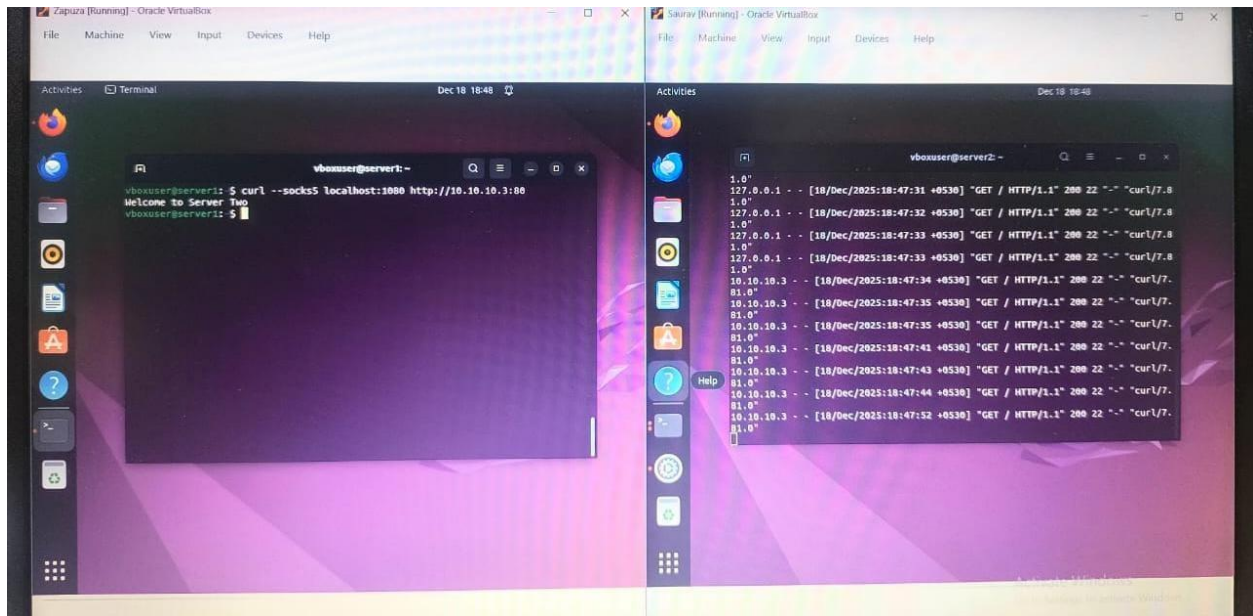
Step 6: Access the Service via Proxy



`curl --socks5 localhost:1080 http://10.10.10.3:80`

Or open the browser and set SOCKS5 proxy to `localhost:1080`.

Step 7: Check Web Server Logs on Client VM



```
sudo tail -f /var/log/nginx/access.log
```

Why 127.0.0.1?

Traffic reaches Nginx through the SSH tunnel, which forwards requests locally on the client VM.