VPN Setup and Samba Access Between Two Linux Virtual Machines

ITC3013 System Administration

Name : Dhanuka Gunasekara

Contents

1 Objective

The objective of this assignment is to establish a secure Virtual Private Network (VPN) between two Linux virtual machines named Sri Lanka Client and US Server using an opensource VPN solution (OpenVPN). The VPN ensures confidential communication between the two locations. In addition, a Samba file server is configured on the US virtual machine and securely accessed from the Sri Lanka virtual machine only through the VPN tunnel.

1.1 Key Goals

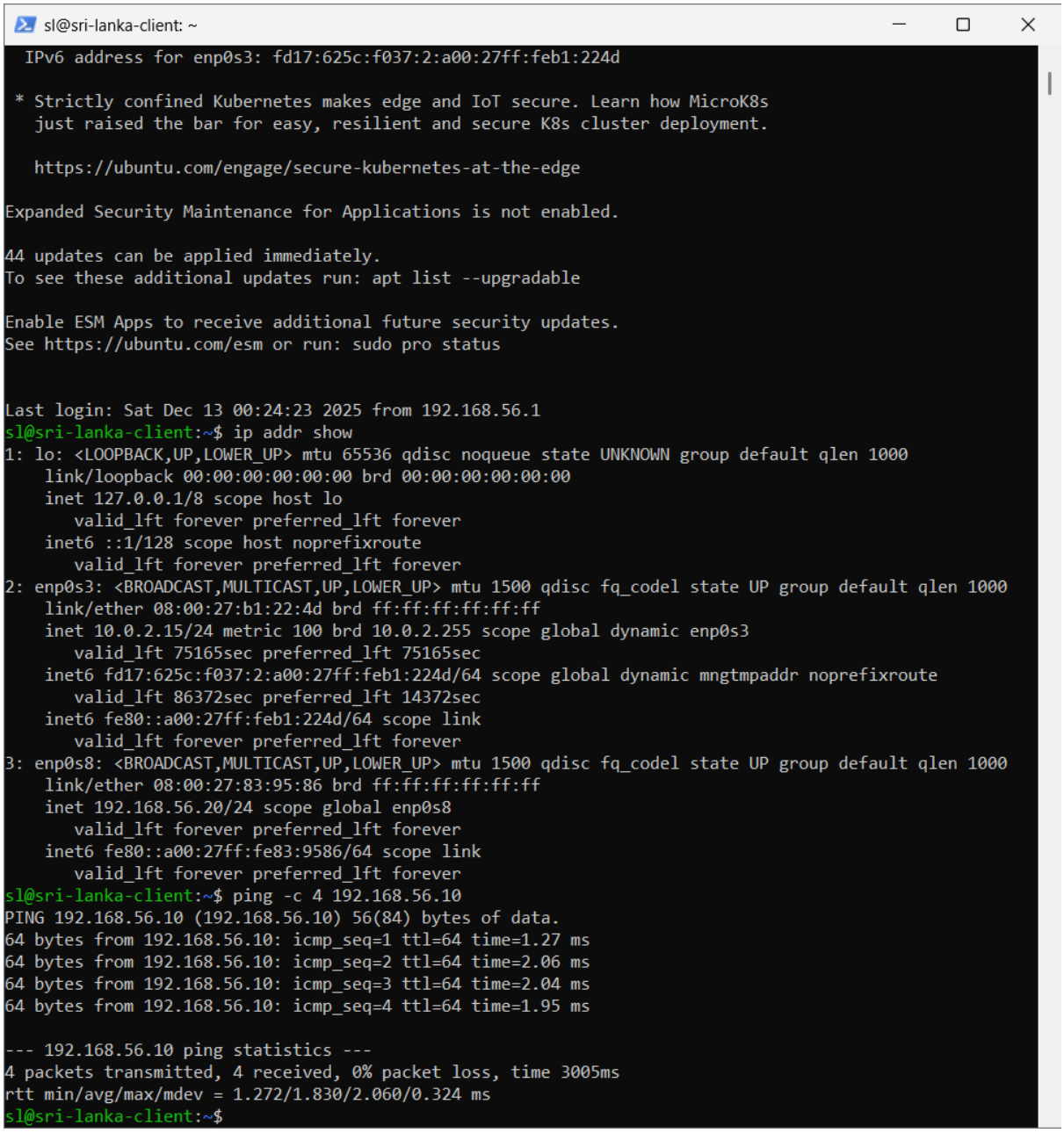
- Create a secure OpenVPN tunnel between two Linux VMs
- Verify VPN connectivity with 100% successful ping
- Configure a Samba server on the US VM
- Access and transfer files from the Sri Lanka VM through the VPN

2 Environment / Platforms Used

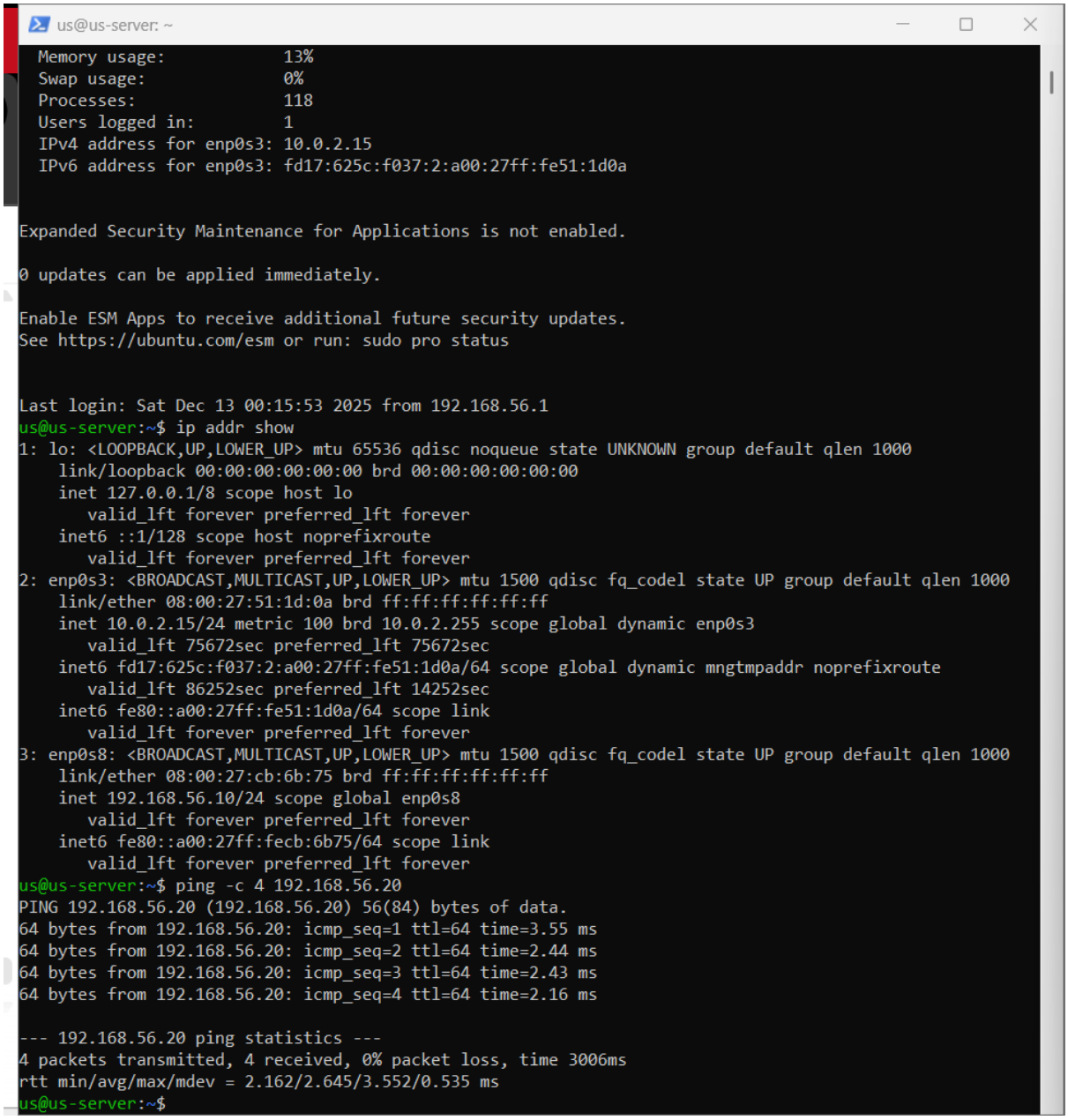
Component	Details
Virtualization	Oracle VirtualBox
Operating System	Ubuntu 22.04 LTS
VPN Software	OpenVPN (Easy-RSA)
File Sharing	Samba
Networking Mode	NAT + Host-Only Adapter
VPN Subnet	10.8.0.0/24
Server VM Name	US Server
Client VM Name	Sri Lanka Client

Host-only IP addresses are used for initial connectivity, SSH access, and VPN endpoint communication. All secure communication and file sharing occur over the VPN subnet (10.8.0.0/24).

2.1 Sri Lanka Client Server Configuration



2.2 US Server Configuration



3 Network Configuration

3.1 Static IP Assignment

US-Server:

- Host-only IP: 192.168.56.10/24
- VPN IP: 10.8.0.1

SriLanka Client:

- Host-only IP: 192.168.56.20/24

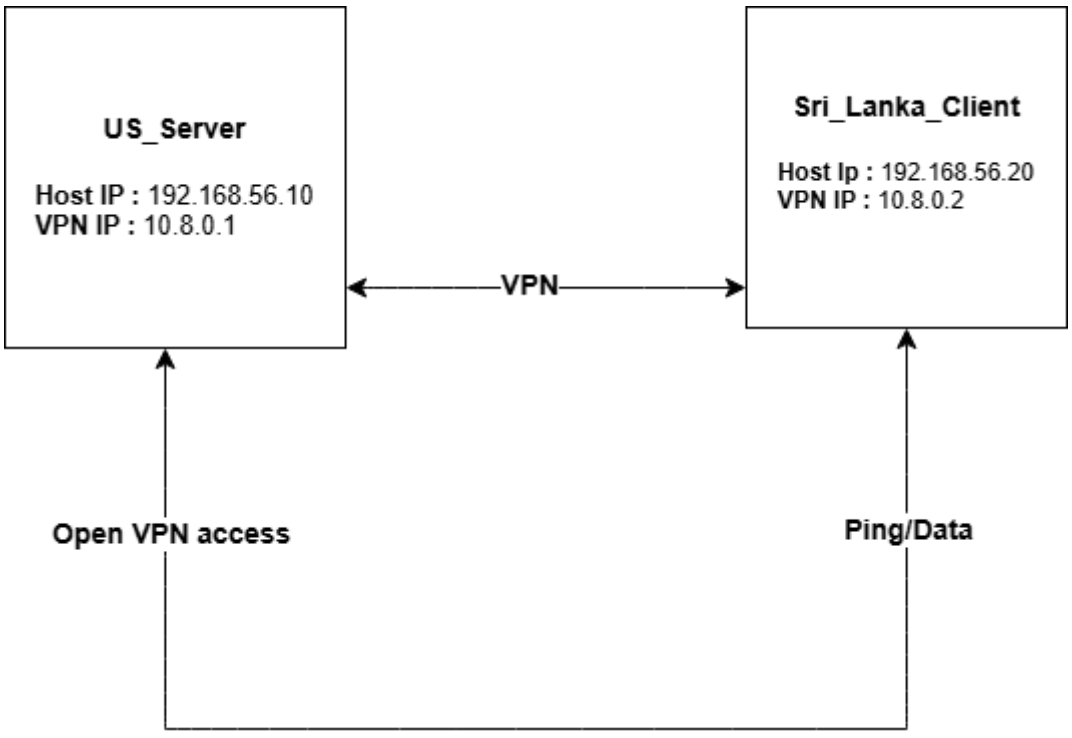
- VPN IP: 10.8.0.

Static IPs were configured using Netplan on both virtual machines to ensure consistent addressing.

4 Network Diagram

The following diagram illustrates the complete setup:

- VM names (SriLanka-Client, US-Server)
- Host-only IP addresses
- VPN IP addresses
- OpenVPN tunnel
- Samba service location on US-Server



5 OpenVPN Setup

5.1 Installing OpenVPN

OpenVPN and Easy-RSA were installed on the US-Server to act as the VPN server and certificate authority. The OpenVPN client package was installed on the SriLanka-Client.

```
Selecting previously unselected package opensc-pkcs11:amd64.
Preparing to unpack .../5-opensc-pkcs11_0.25.0~rc1-1build2_amd64.deb ...
Unpacking opensc-pkcs11:amd64 (0.25.0~rc1-1build2) ...
Selecting previously unselected package opensc.
Preparing to unpack .../6-opensc_0.25.0~rc1-1build2_amd64.deb ...
Unpacking opensc (0.25.0~rc1-1build2) ...
Selecting previously unselected package openvpn.
Preparing to unpack .../7-openvpn_2.6.14-0ubuntu0.24.04.3_amd64.deb ...
Unpacking openvpn (2.6.14-0ubuntu0.24.04.3) ...
Selecting previously unselected package easy-rsa.
Preparing to unpack .../8-easy-rsa_3.1.7-2_all.deb ...
Unpacking easy-rsa (3.1.7-2) ...
Setting up libccid (1.5.5-1) ...
Setting up libeac3:amd64 (1.1.2+ds+git20220117+453c3d6b03a0-1.1build2) ...
Setting up opensc-pkcs11:amd64 (0.25.0~rc1-1build2) ...
Setting up libpcsclite1:amd64 (2.0.3-1build1) ...
Setting up libpkcs11-helper1t64:amd64 (1.29.0-2.1build2) ...
Setting up easy-rsa (3.1.7-2) ...
Setting up openvpn (2.6.14-0ubuntu0.24.04.3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn.service → /usr/lib/systemd/system/ope
nvpn.service.
Setting up opensc (0.25.0~rc1-1build2) ...
Setting up pcscd (2.0.3-1build1) ...
Created symlink /etc/systemd/system/sockets.target.wants/pcscd.socket → /usr/lib/systemd/system/pcscd.soc
ket.
pcscd.service is a disabled or a static unit, not starting it.
Processing triggers for libc-bin (2.39-0ubuntu8.6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...

Service restarts being deferred:
 /etc/needrestart/restart.d/dbus.service
 systemctl restart systemd-logind.service
 systemctl restart unattended-upgrades.service

No containers need to be restarted.

User sessions running outdated binaries:
 us @ session #1: login[929]
 us @ user manager service: systemd[1144]

No VM guests are running outdated hypervisor (qemu) binaries on this host.
us@us-server:~$ make-cadir ~/easy-rsa
```

5.2 Certificate Authority and Key Management

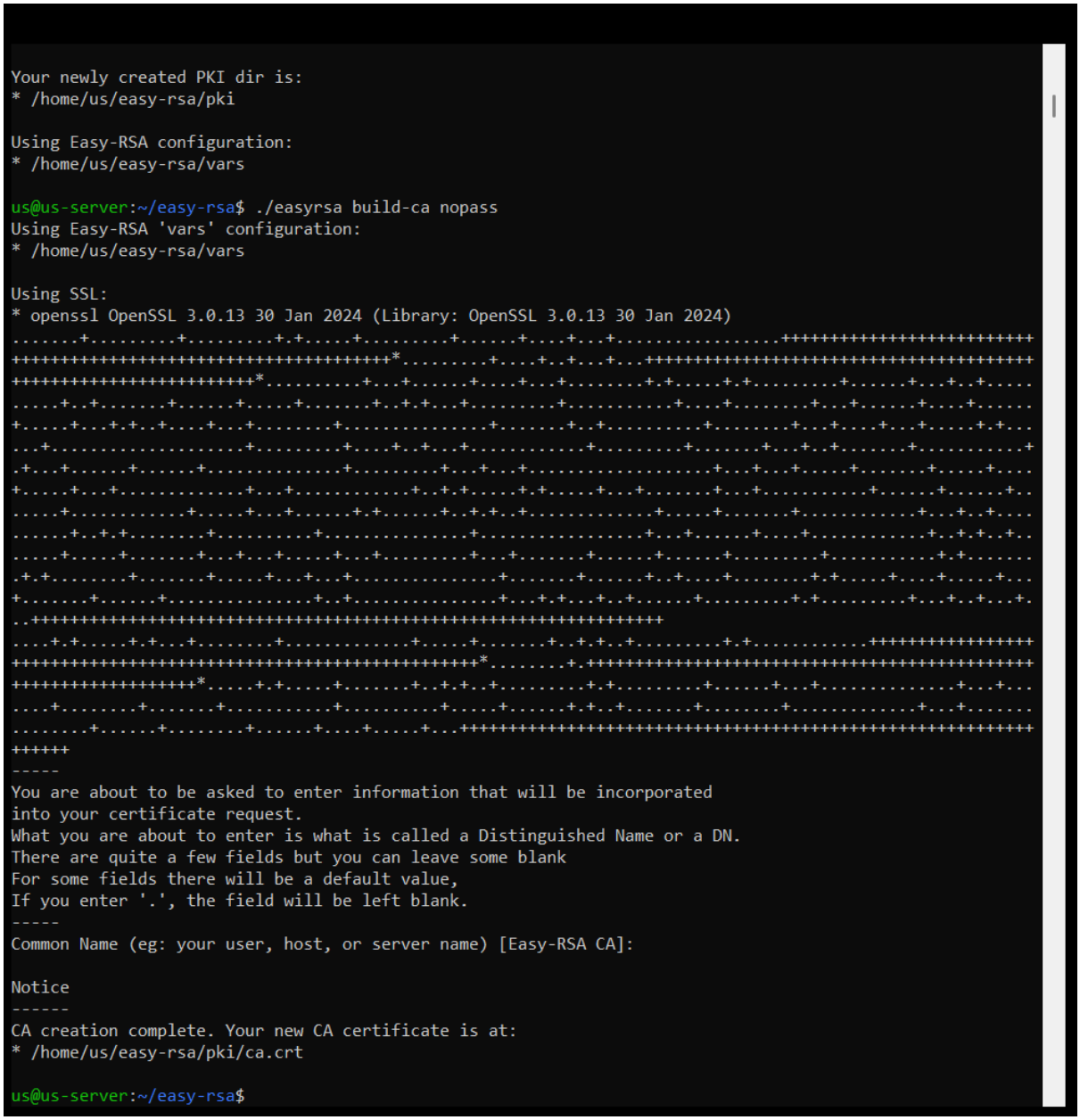
Easy-RSA was used to create a Public Key Infrastructure (PKI). A Certificate Authority (CA) was initialized, followed by the generation and signing of:

- Server certificate (us-server)
- Client certificate (srilanka-client)

- Diffie-Hellman parameters
- TLS authentication key

Private keys were securely stored with restricted permissions, and only public certificates were exchanged.

5.2.1 CA Creation



5.2.2 Server and Client Certificates

```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [srilanka-client]:

Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: /home/us/easy-rsa/pki/reqs/srilanka-client.req
* key: /home/us/easy-rsa/pki/private/srilanka-client.key

us@us-server:~/easy-rsa$ ./easyrsa sign-req client srilanka-client
Using Easy-RSA 'vars' configuration:
* /home/us/easy-rsa/vars

Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
You are about to sign the following certificate:
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.
Request subject, to be signed as a client certificate
for '825' days:

subject=
    commonName                = srilanka-client

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes

Using configuration from /home/us/easy-rsa/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'srilanka-client'
Certificate is to be certified until Mar 17 06:26:32 2028 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* /home/us/easy-rsa/pki/issued/srilanka-client.crt

us@us-server:~/easy-rsa$
```

5.3 OpenVPN Server Configuration (US-Server)

The OpenVPN server configuration file (/etc/openvpn/server/server.conf) defines:

- UDP port 1194
- TUN virtual interface
- VPN subnet 10.8.0.0/24
- Encryption algorithms (AES-256-GCM, SHA256)
- TLS authentication

IP forwarding was enabled to allow VPN traffic routing.

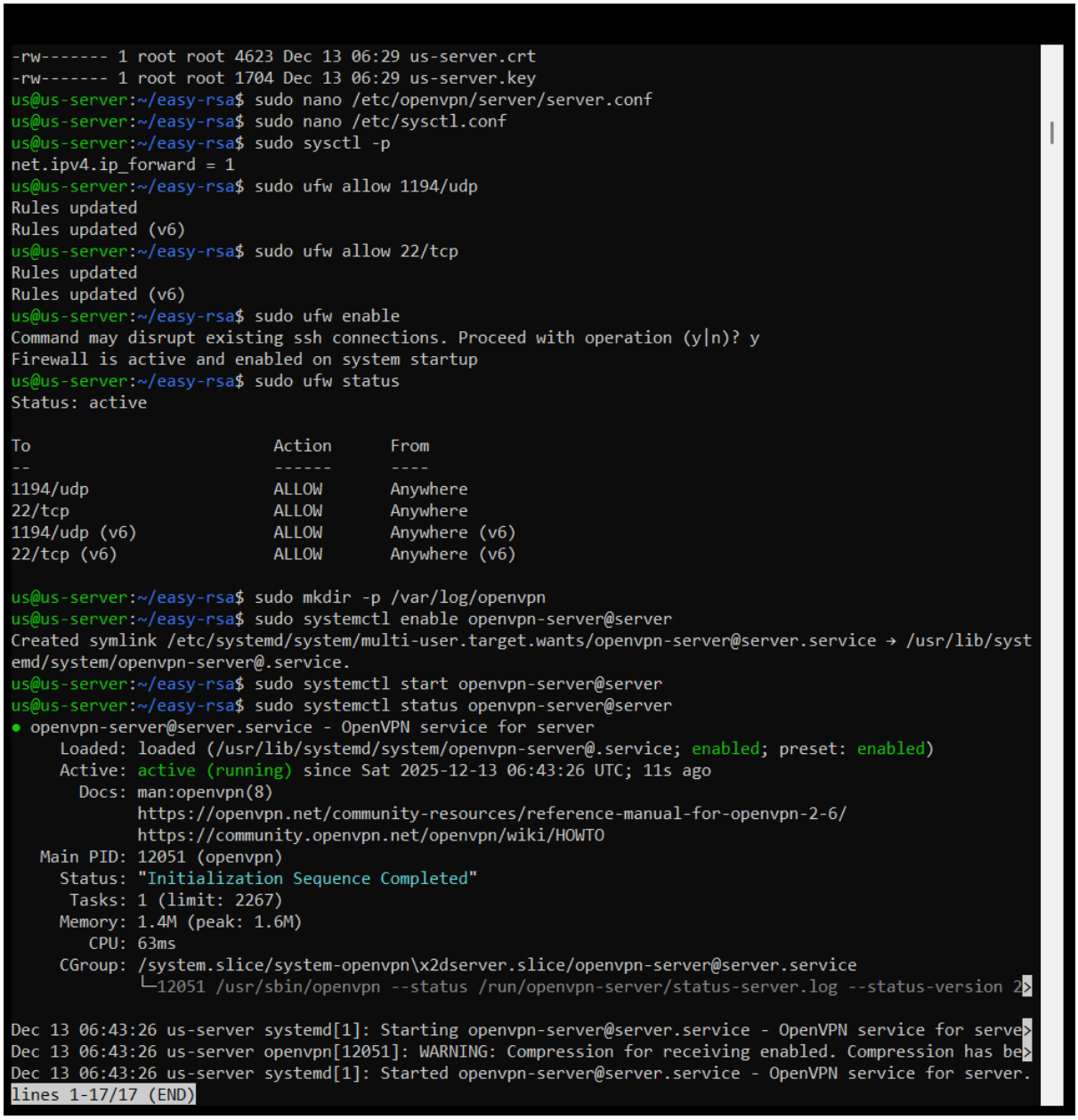
5.3.1 IP Forwarding Configuration

```
You are about to sign the following certificate:
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.
Request subject, to be signed as a client certificate
for '825' days:

subject=
    commonName                = srilanka-client

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes

Using configuration from /home/us/easy-rsa/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'srilanka-client'
Certificate is to be certified until Mar 17 06:26:32 2028 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* /home/us/easy-rsa/pki/issued/srilanka-client.crt

us@us-server:~/easy-rsa$
us@us-server:~/easy-rsa$
us@us-server:~/easy-rsa$ sudo mkdir -p /etc/openvpn/server
us@us-server:~/easy-rsa$ sudo cp ~/easy-rsa/pki/ca.crt /etc/openvpn/server/
us@us-server:~/easy-rsa$ sudo cp ~/easy-rsa/pki/issued/us-server.crt /etc/openvpn/server/
us@us-server:~/easy-rsa$ sudo cp ~/easy-rsa/pki/private/us-server.key /etc/openvpn/server/
us@us-server:~/easy-rsa$ sudo cp ~/easy-rsa/pki/dh.pem /etc/openvpn/server/
us@us-server:~/easy-rsa$ sudo cp ~/easy-rsa/pki/ta.key /etc/openvpn/server/
us@us-server:~/easy-rsa$ sudo chmod 600 /etc/openvpn/server/us-server.key
us@us-server:~/easy-rsa$ ls -l /etc/openvpn/server/
total 24
-rw------- 1 root root 1204 Dec 13 06:29 ca.crt
-rw------- 1 root root  424 Dec 13 06:29 dh.pem
-rw------- 1 root root  636 Dec 13 06:30 ta.key
-rw------- 1 root root 4623 Dec 13 06:29 us-server.crt
-rw------- 1 root root 1704 Dec 13 06:29 us-server.key
us@us-server:~/easy-rsa$ sudo nano /etc/openvpn/server/server.conf
us@us-server:~/easy-rsa$ sudo nano /etc/sysctl.conf
us@us-server:~/easy-rsa$ sudo sysctl -p
net.ipv4.ip_forward = 1
us@us-server:~/easy-rsa$
```

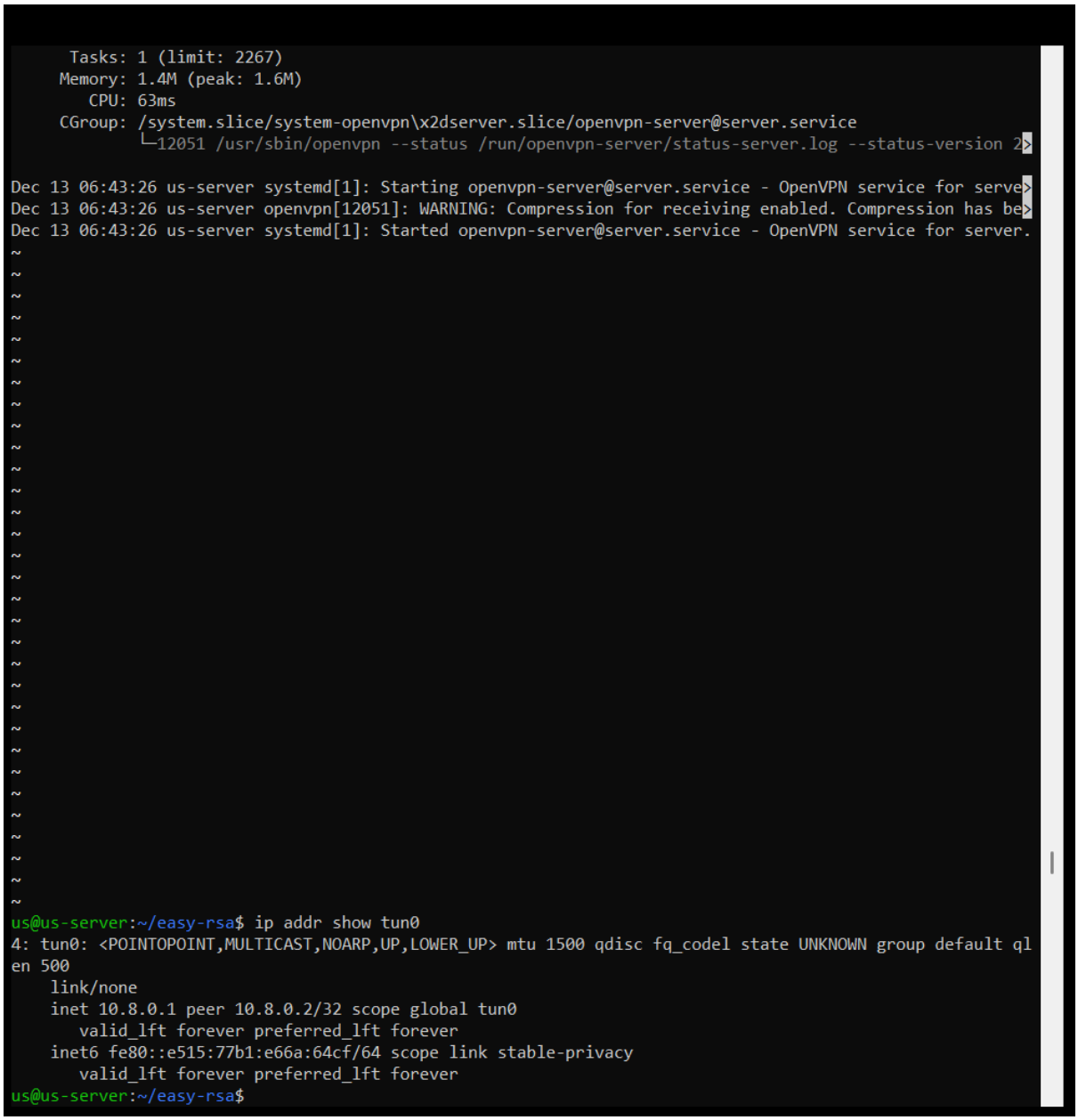
5.3.2 Firewall Configuration (UFW)

```
Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* /home/us/easy-rsa/pki/issued/srilanka-client.crt

us@us-server:~/easy-rsa$
us@us-server:~/easy-rsa$
us@us-server:~/easy-rsa$ sudo mkdir -p /etc/openvpn/server
us@us-server:~/easy-rsa$ sudo cp ~/easy-rsa/pki/ca.crt /etc/openvpn/server/
us@us-server:~/easy-rsa$ sudo cp ~/easy-rsa/pki/issued/us-server.crt /etc/openvpn/server/
us@us-server:~/easy-rsa$ sudo cp ~/easy-rsa/pki/private/us-server.key /etc/openvpn/server/
us@us-server:~/easy-rsa$ sudo cp ~/easy-rsa/pki/dh.pem /etc/openvpn/server/
us@us-server:~/easy-rsa$ sudo cp ~/easy-rsa/pki/ta.key /etc/openvpn/server/
us@us-server:~/easy-rsa$ sudo chmod 600 /etc/openvpn/server/us-server.key
us@us-server:~/easy-rsa$ ls -l /etc/openvpn/server/
total 24
-rw------- 1 root root 1204 Dec 13 06:29 ca.crt
-rw------- 1 root root  424 Dec 13 06:29 dh.pem
-rw------- 1 root root  636 Dec 13 06:30 ta.key
-rw------- 1 root root 4623 Dec 13 06:29 us-server.crt
-rw------- 1 root root 1704 Dec 13 06:29 us-server.key
us@us-server:~/easy-rsa$ sudo nano /etc/openvpn/server/server.conf
us@us-server:~/easy-rsa$ sudo nano /etc/sysctl.conf
us@us-server:~/easy-rsa$ sudo sysctl -p
net.ipv4.ip_forward = 1
us@us-server:~/easy-rsa$ sudo ufw allow 1194/udp
Rules updated
Rules updated (v6)
us@us-server:~/easy-rsa$ sudo ufw allow 22/tcp
Rules updated
Rules updated (v6)
us@us-server:~/easy-rsa$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
us@us-server:~/easy-rsa$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
1194/udp                   ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
1194/udp (v6)              ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)

us@us-server:~/easy-rsa$
```

5.3.3 OpenVPN Server Service Running



5.3.4 TUN0 Interface with IP 10.8.0.1

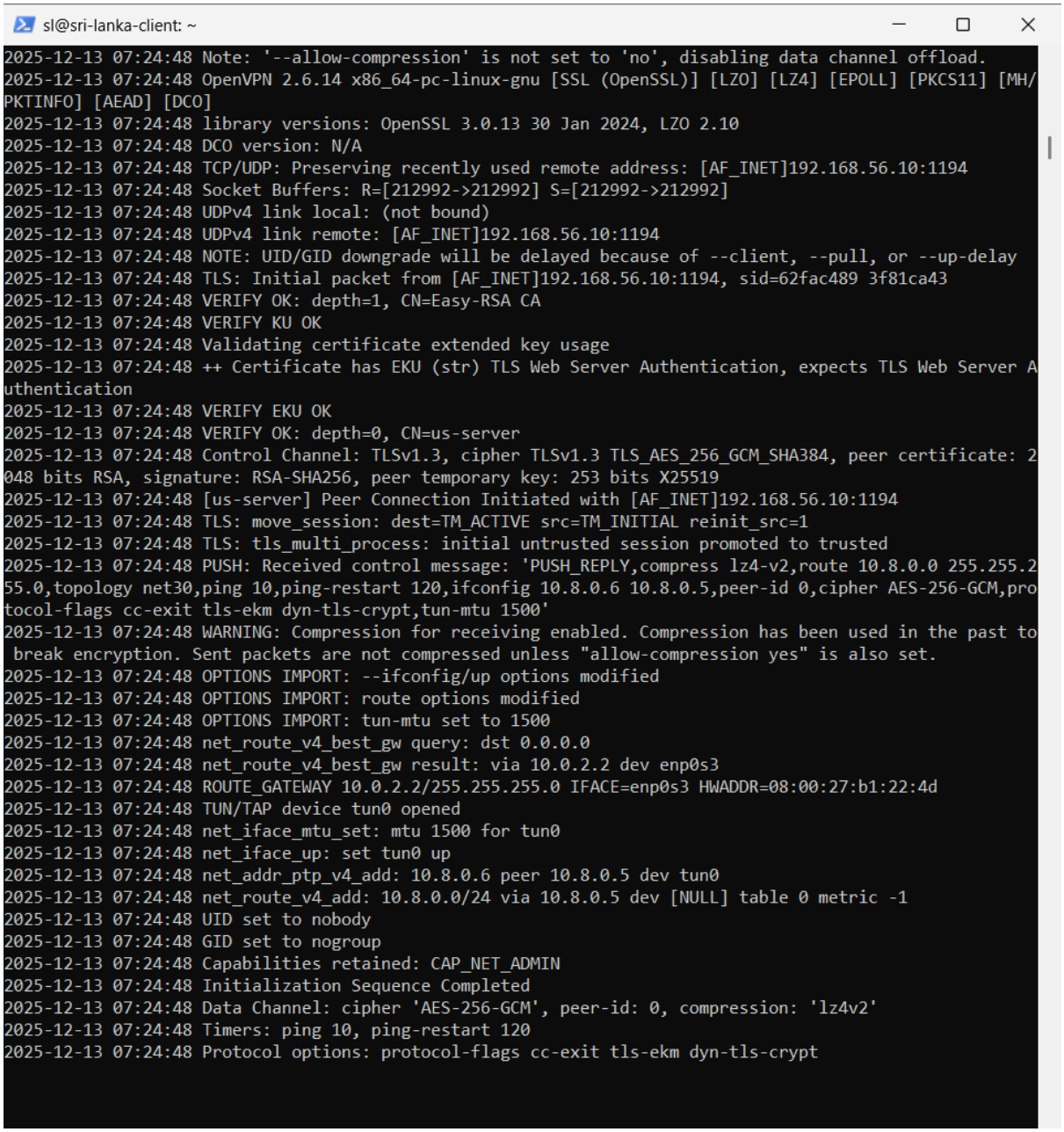


5.4 OpenVPN Client Configuration (SriLanka-Client)

The client configuration file includes:

- Server endpoint 192.168.56.10:1194
- Client certificates and keys
- Encryption and authentication settings

The VPN connection was established using the OpenVPN client command.



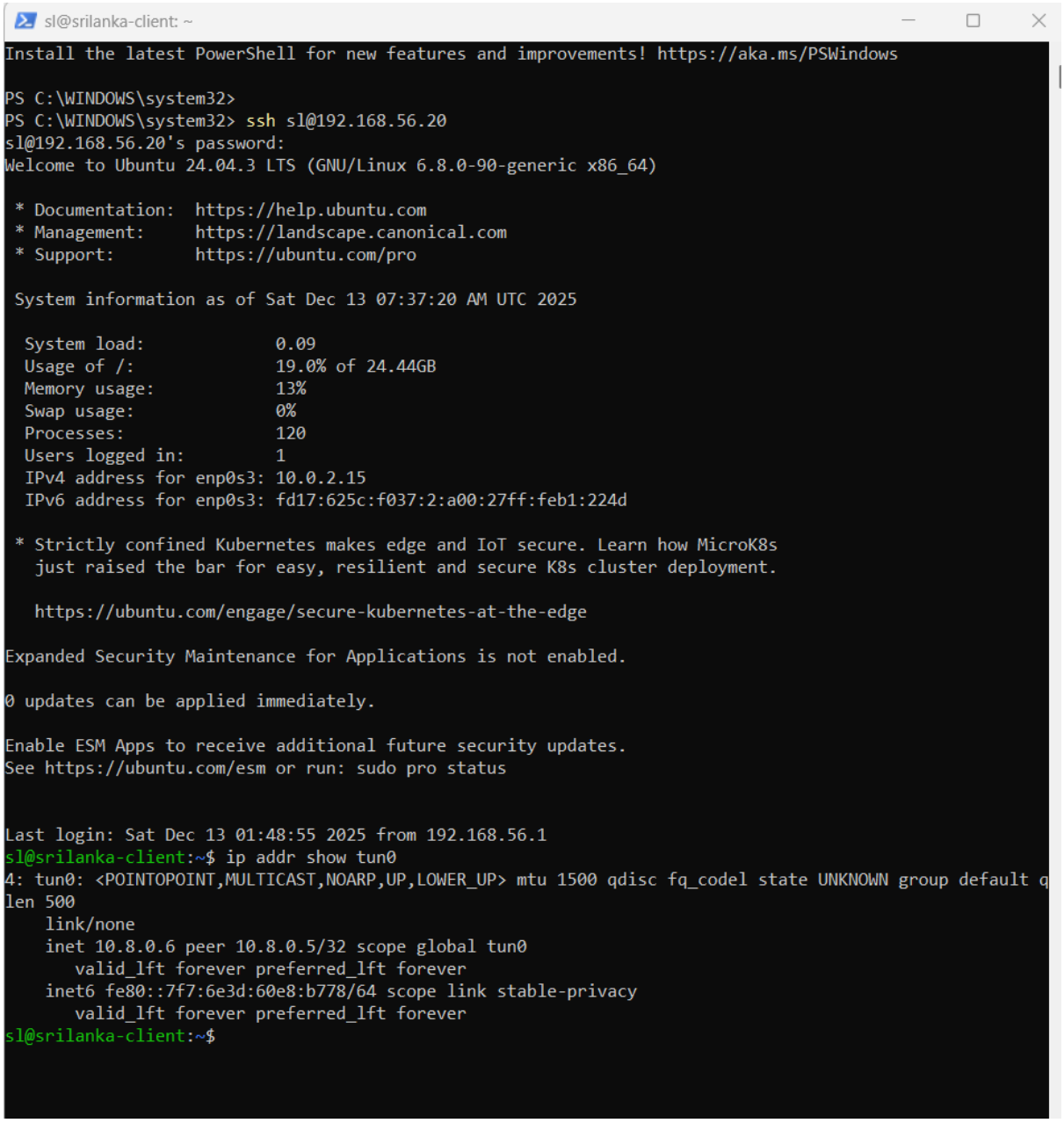
6 VPN Verification

VPN connectivity was verified using the following tests:

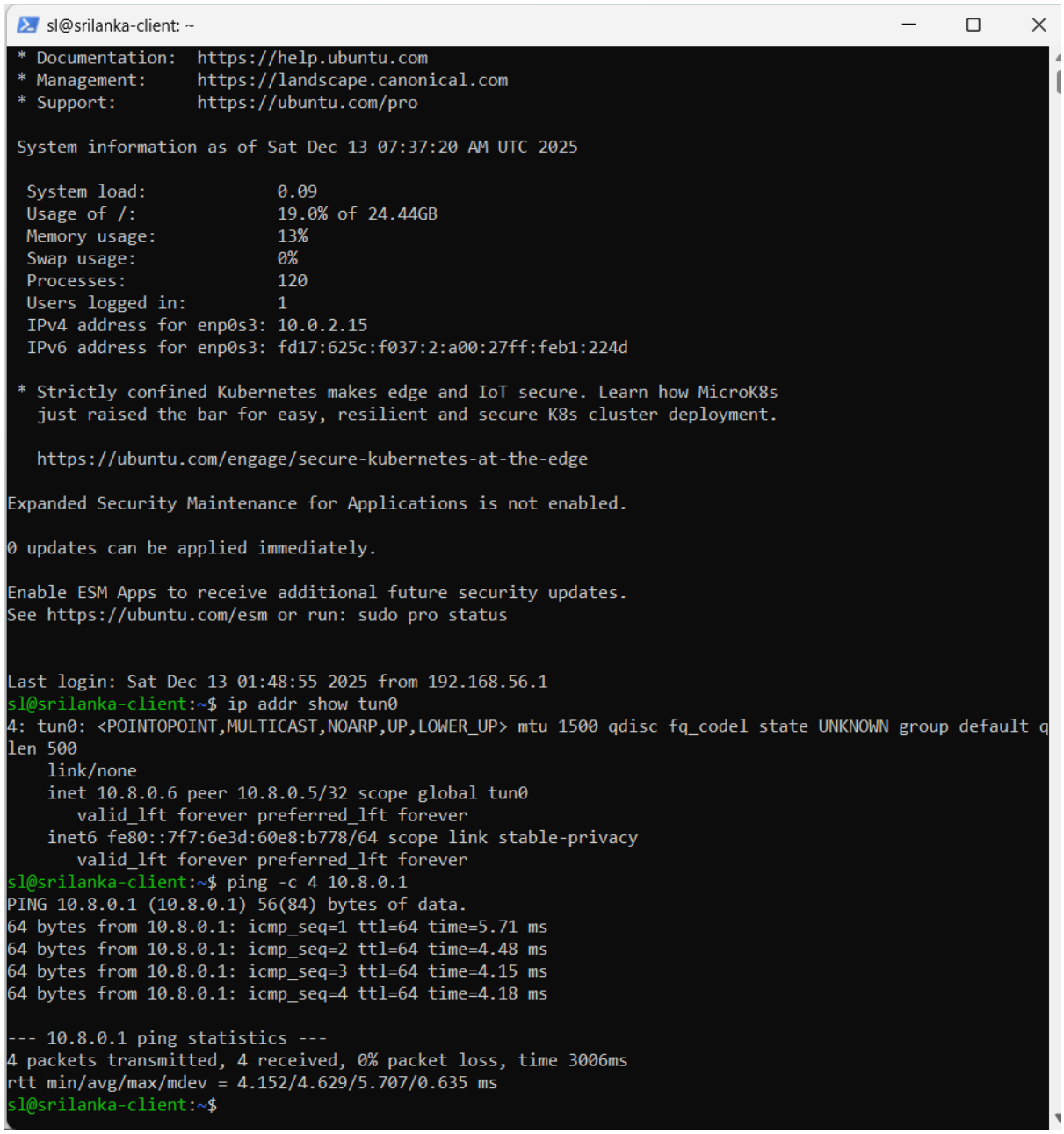
- ip addr show tun0 to confirm VPN interface
- ping 10.8.0.1 from SriLanka-Client

All ping tests showed 0% packet loss, confirming a stable and secure VPN tunnel.

6.1 TUN0 Interface on Client



6.2 Successful Ping to 10.8.0.1



7 Samba Server Setup (US-Server)

7.1 Installing Samba

Samba was installed to provide a network file-sharing service for the project data.

7.2 Creating Shared Directory

A directory /srv/samba/biomed-share was created and configured with appropriate permissions. A test file was added to verify access.

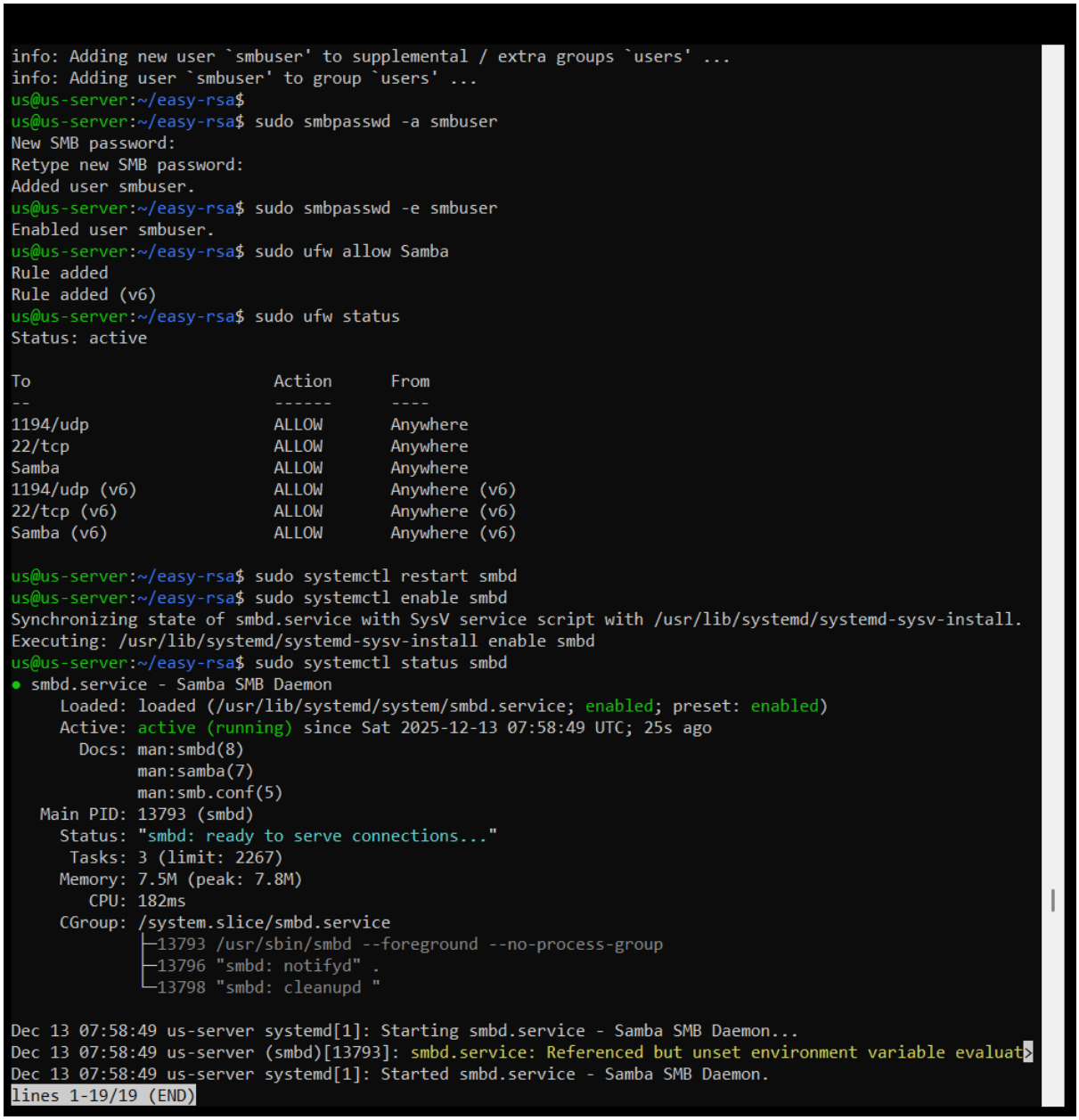
7.3 Samba Configuration

A secure Samba share named biomed-share was configured with:

- Authenticated user access only
- Read and write permissions
- Restricted to the Samba user smbuser

The Samba service was restarted and verified to be running.

7.3.1 Samba Service Active



7.3.2 Testparm Output

```
SMB1 disabled -- no workgroup available
us@us-server:~/easy-rsa$ testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions

# Global parameters
[global]
        log file = /var/log/samba/log.%m
        logging = file
        map to guest = Bad User
        max log size = 1000
        obey pam restrictions = Yes
        pam password change = Yes
        panic action = /usr/share/samba/panic-action %d
        passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n *password\supdated
\ssuccessfully* .
        passwd program = /usr/bin/passwd %u
        server role = standalone server
        server string = %h server (Samba, Ubuntu)
        unix password sync = Yes
        usershare allow guests = Yes
        idmap config * : backend = tdb


[printers]
        browseable = No
        comment = All Printers
        create mask = 0700
        path = /var/tmp
        printable = Yes


[print$]
        comment = Printer Drivers
        path = /var/lib/samba/printers


[biomed-share]
        comment = BioMed Confidential Project Share
        create mask = 0755
        path = /srv/samba/biomed-share
        read only = No
        valid users = smbuser
us@us-server:~/easy-rsa$ sudo apt install smbclient -y
```

7.3.3 Local Share Listing

```
        panic action = /usr/share/samba/panic-action %d
        passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n *password\supdated
\ssuccessfully* .
        passwd program = /usr/bin/passwd %u
        server role = standalone server
        server string = %h server (Samba, Ubuntu)
        unix password sync = Yes
        usershare allow guests = Yes
        idmap config * : backend = tdb


[printers]
        browseable = No
        comment = All Printers
        create mask = 0700
        path = /var/tmp
        printable = Yes


[print$]
        comment = Printer Drivers
        path = /var/lib/samba/printers


[biomed-share]
        comment = BioMed Confidential Project Share
        create mask = 0755
        path = /srv/samba/biomed-share
        read only = No
        valid users = smbuser
us@us-server:~/easy-rsa$ sudo apt install smbclient -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
smbclient is already the newest version (2:4.19.5+dfsg-4ubuntu9.4).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
us@us-server:~/easy-rsa$ smbclient -L localhost -U smbuser
Password for [WORKGROUP\smbuser]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        biomed-share    Disk      BioMed Confidential Project Share
        IPC$            IPC       IPC Service (us-server server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
us@us-server:~/easy-rsa$
```

8 Accessing Samba from SriLanka-Client via VPN

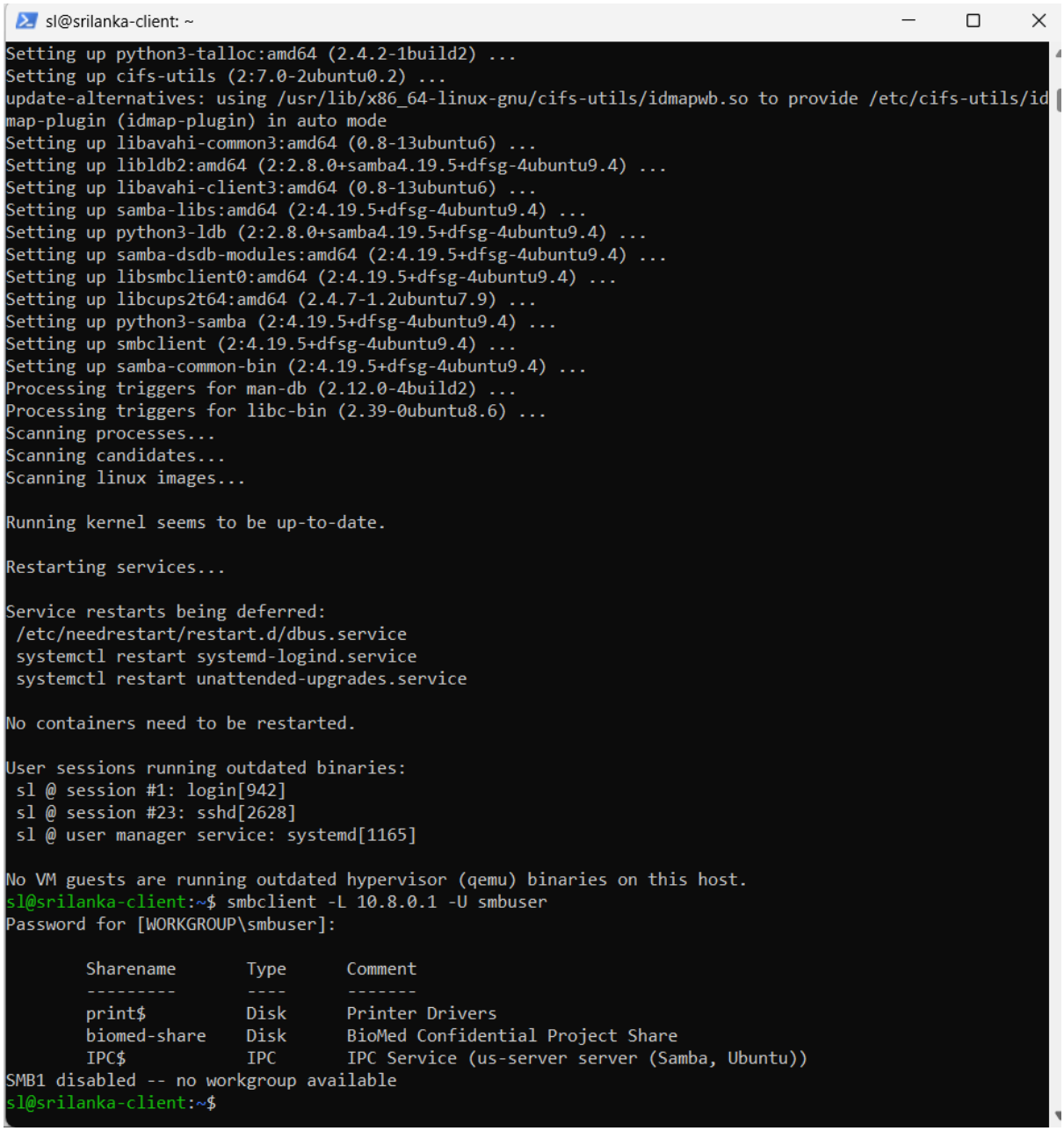
Samba client tools were installed on the SriLanka-Client. The Samba share was accessed using the VPN IP address (10.8.0.1) to ensure all traffic passed through the encrypted tunnel.

The share was:

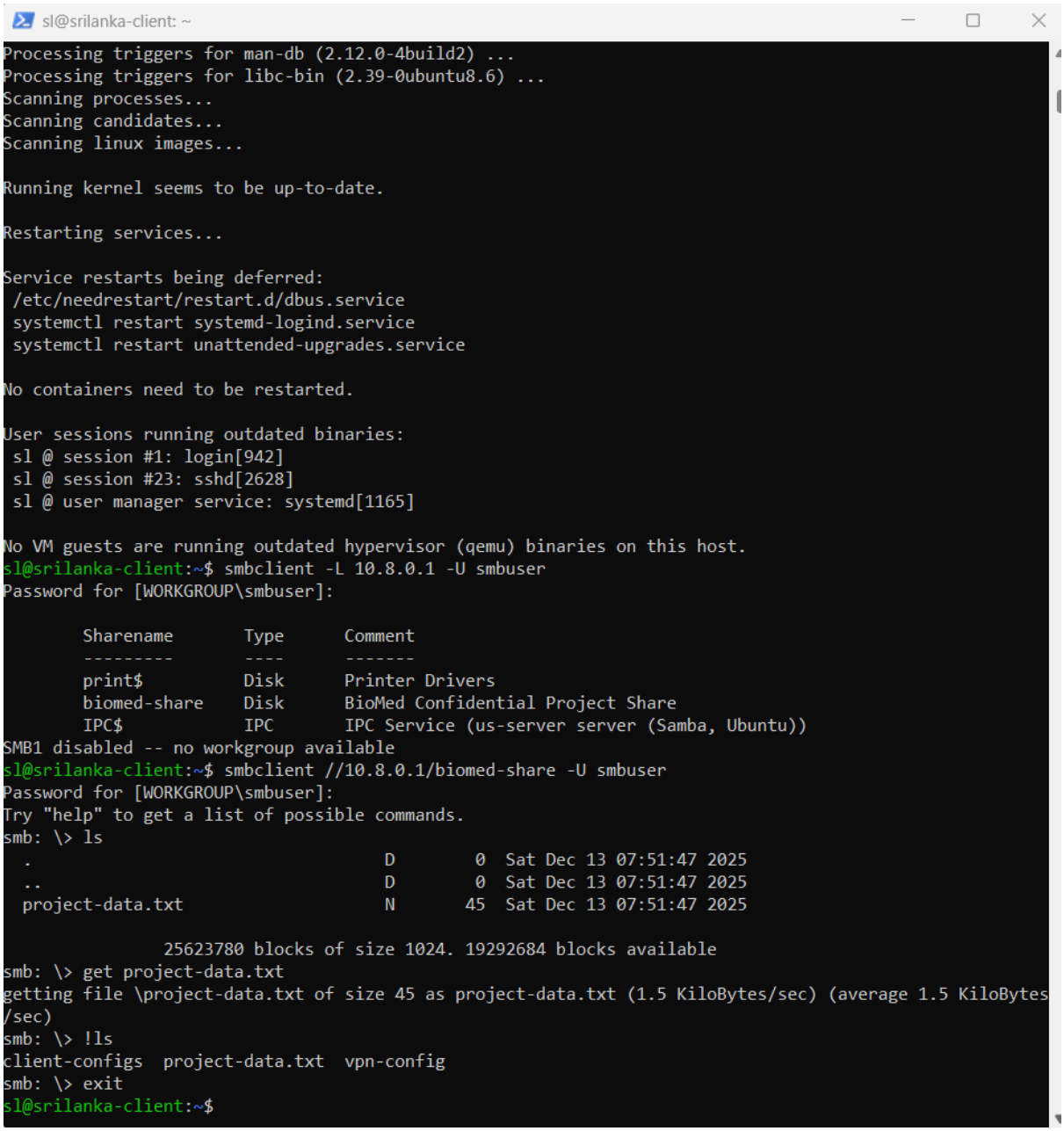
- Listed using smbclient
- Accessed interactively
- Mounted locally using CIFS

File read and write operations were tested successfully.

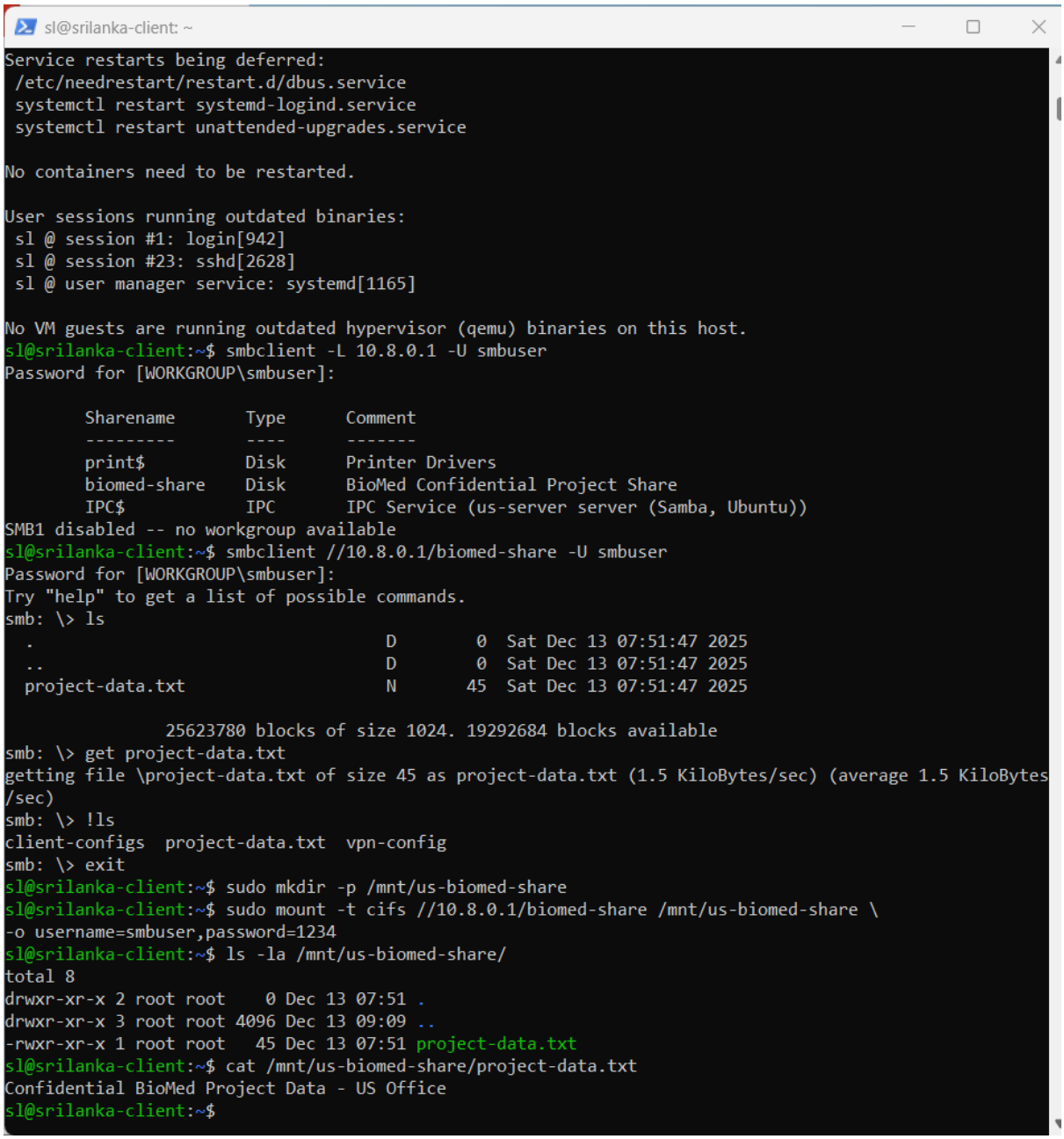
8.1 Samba Shares Listed Over VPN



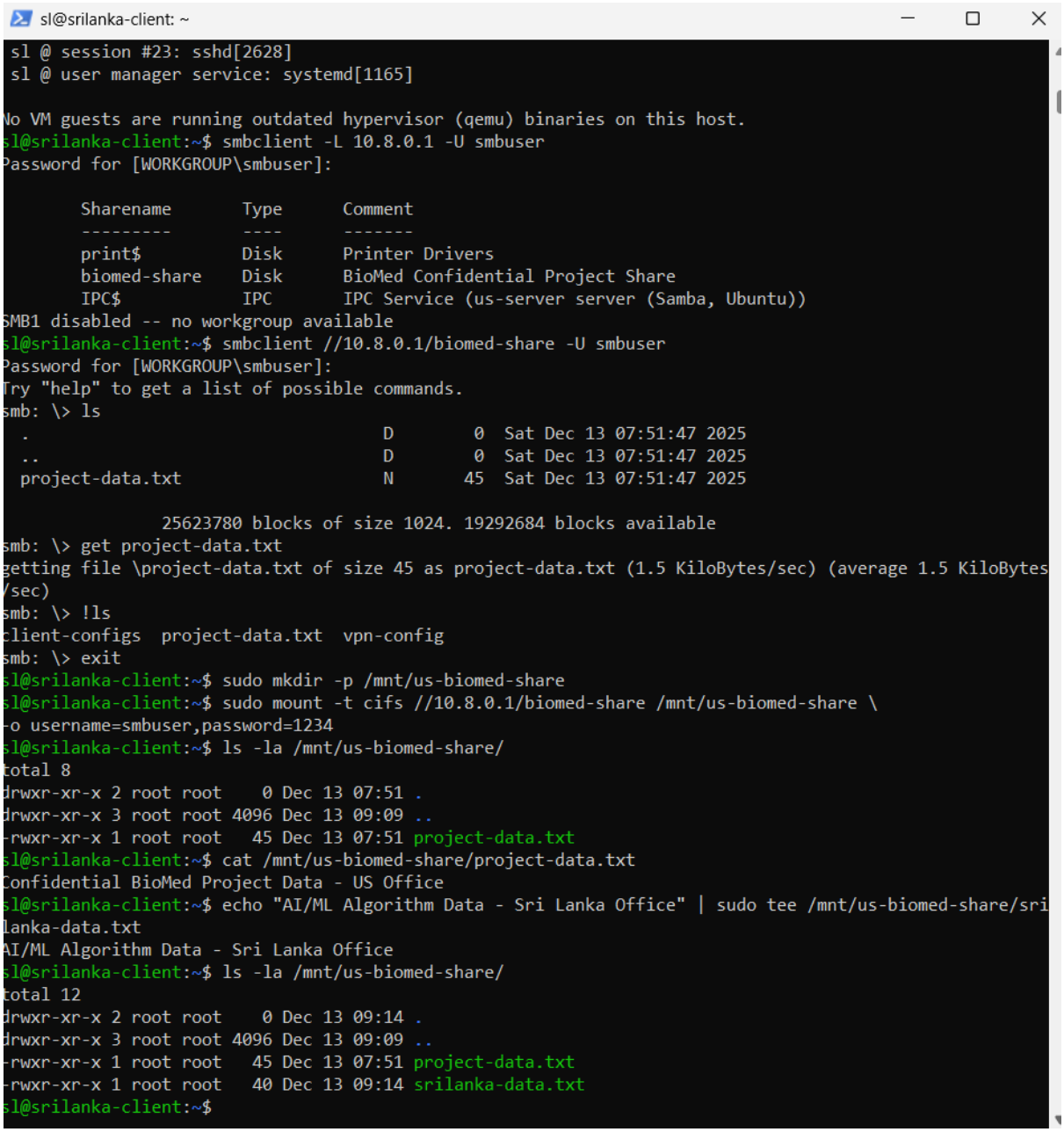
8.2 File Listing Inside Share



8.3 Mounted Share with Files



8.4 File Created on Client Visible on Server



9 Final Verification and Testing

This phase verifies that the VPN tunnel between the US Server and the Sri Lanka Client is successfully established and that secure file sharing via Samba is functioning correctly over the VPN.

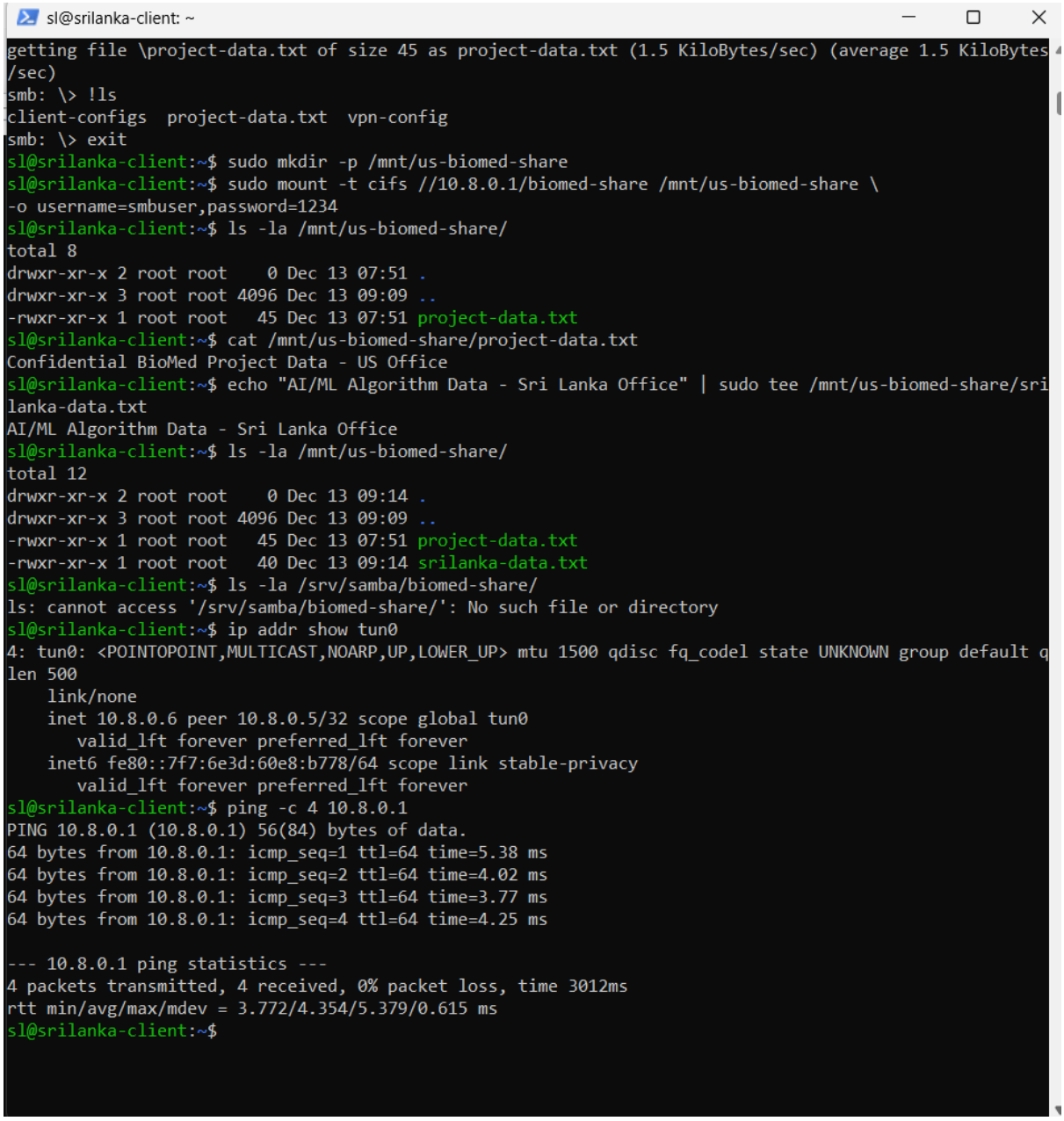
9.1 VPN Tunnel Verification (Sri Lanka Client)

Commands executed:

```
ip addr show tun0 ping -c 4 10.8.0.1
```

Expected Outcome:

- tun0 interface is active with an IP address in the 10.8.0.0/24 range
- Successful ping responses confirm VPN connectivity with the US Server



9.2 Samba Share Mount Verification

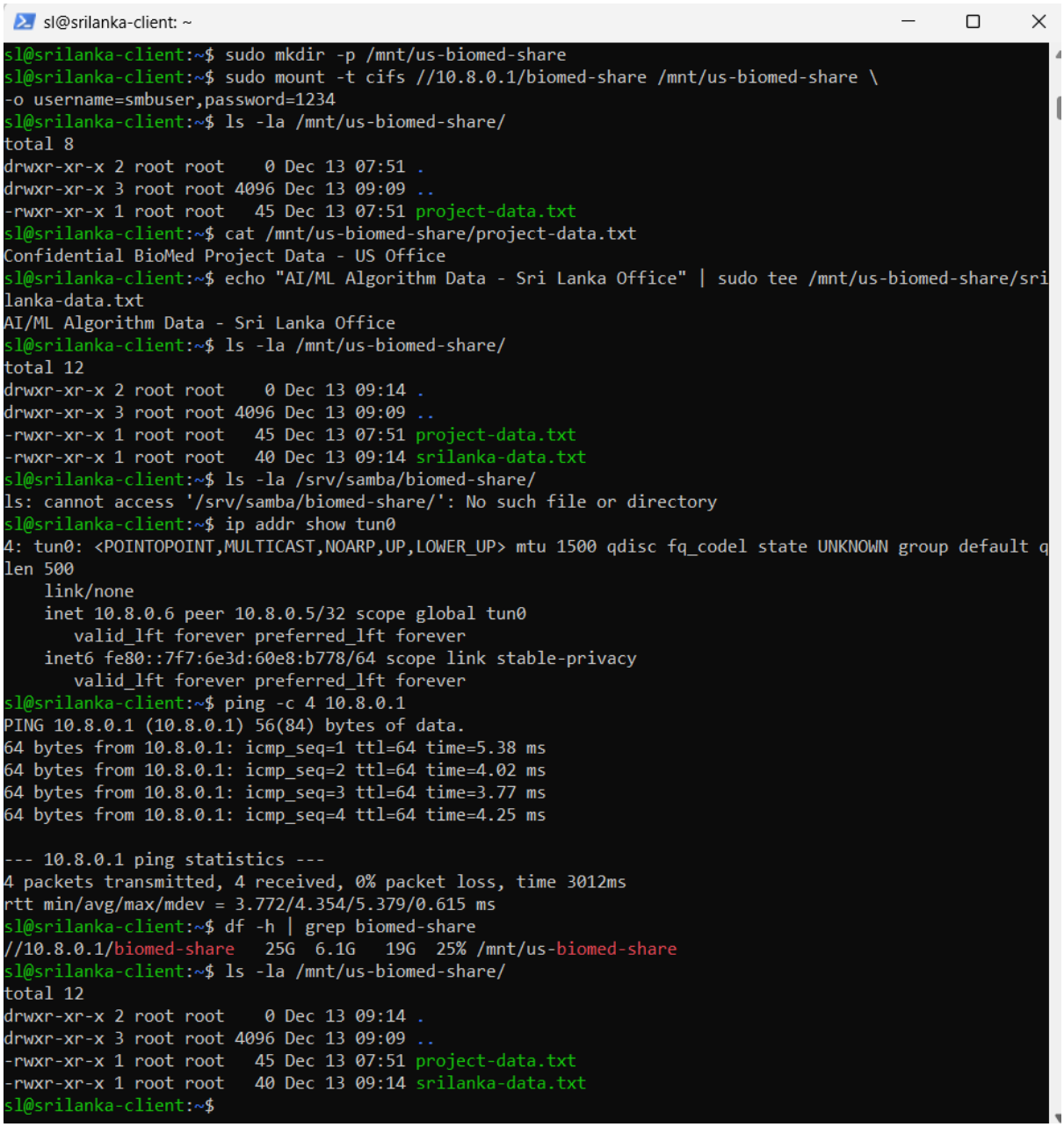
Commands executed:

```
df -h | grep biomed-share ls -la /mnt/us-
biomed-share/
```

Expected Outcome:

- Samba share is mounted successfully

- Files inside the shared directory are visible



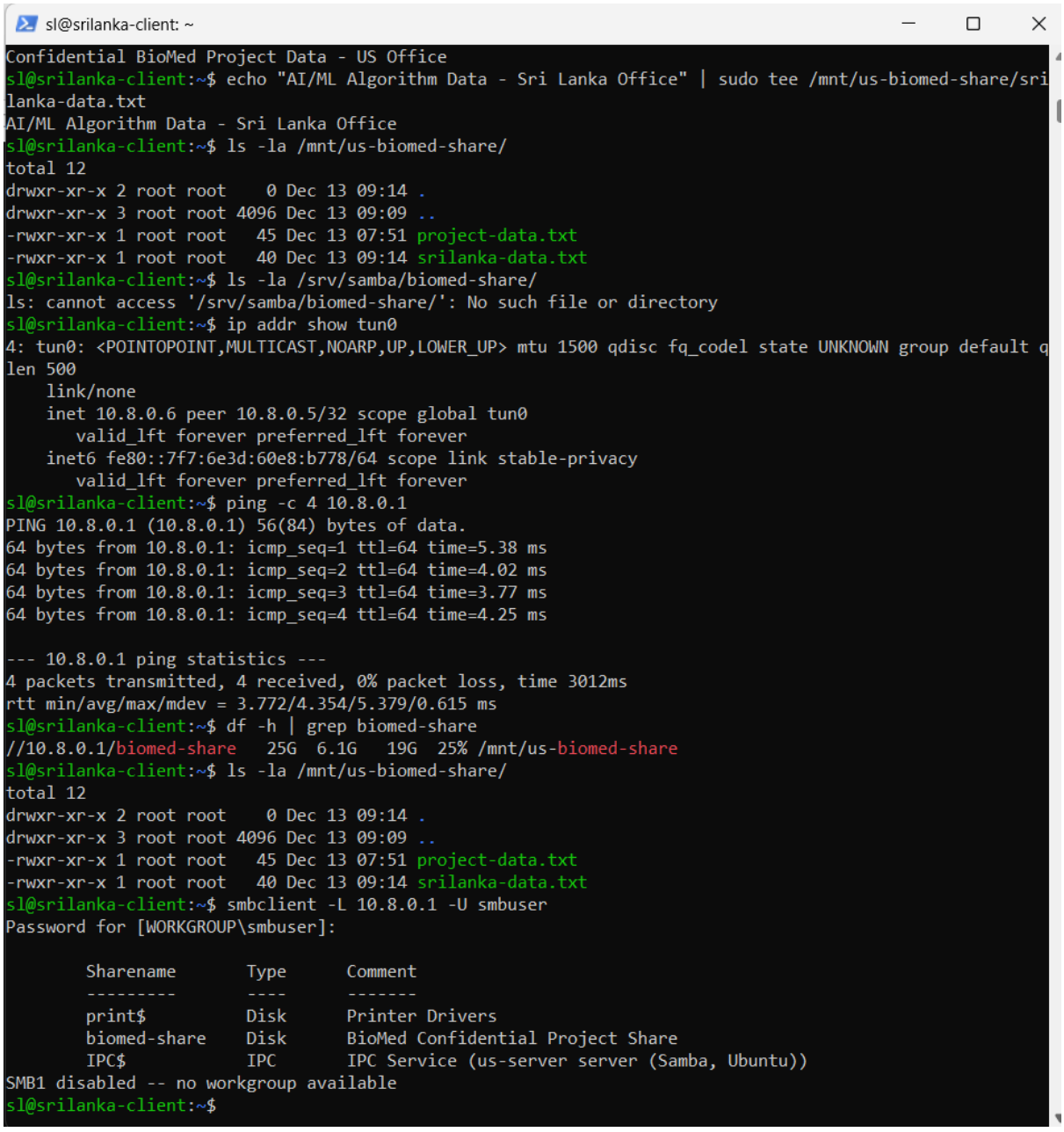
9.3 Samba Server Accessibility Test

Command executed:

```
smbclient -L 10.8.0.1 -U smbuser
```

Expected Outcome:

- Samba shares hosted on the US Server are listed successfully
- Confirms Samba access over VPN



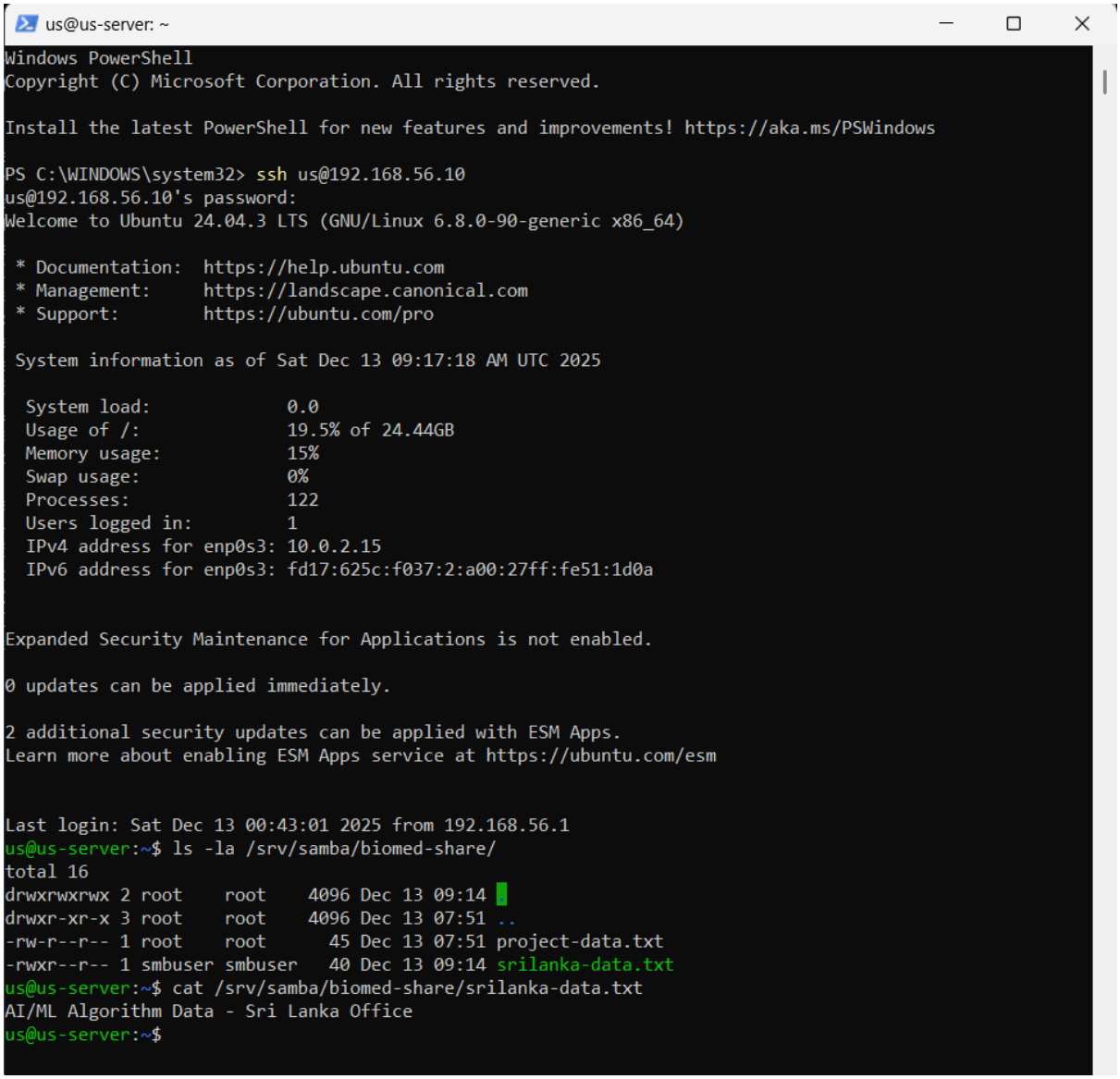
9.4 Two-Way File Sharing Confirmation

To confirm bidirectional file sharing, the US Server was used to verify files created from the Sri Lanka Client.

```
ls -la /srv/samba/biomed-share/
cat /srv/samba/biomed-share/srilanka-data.txt
```

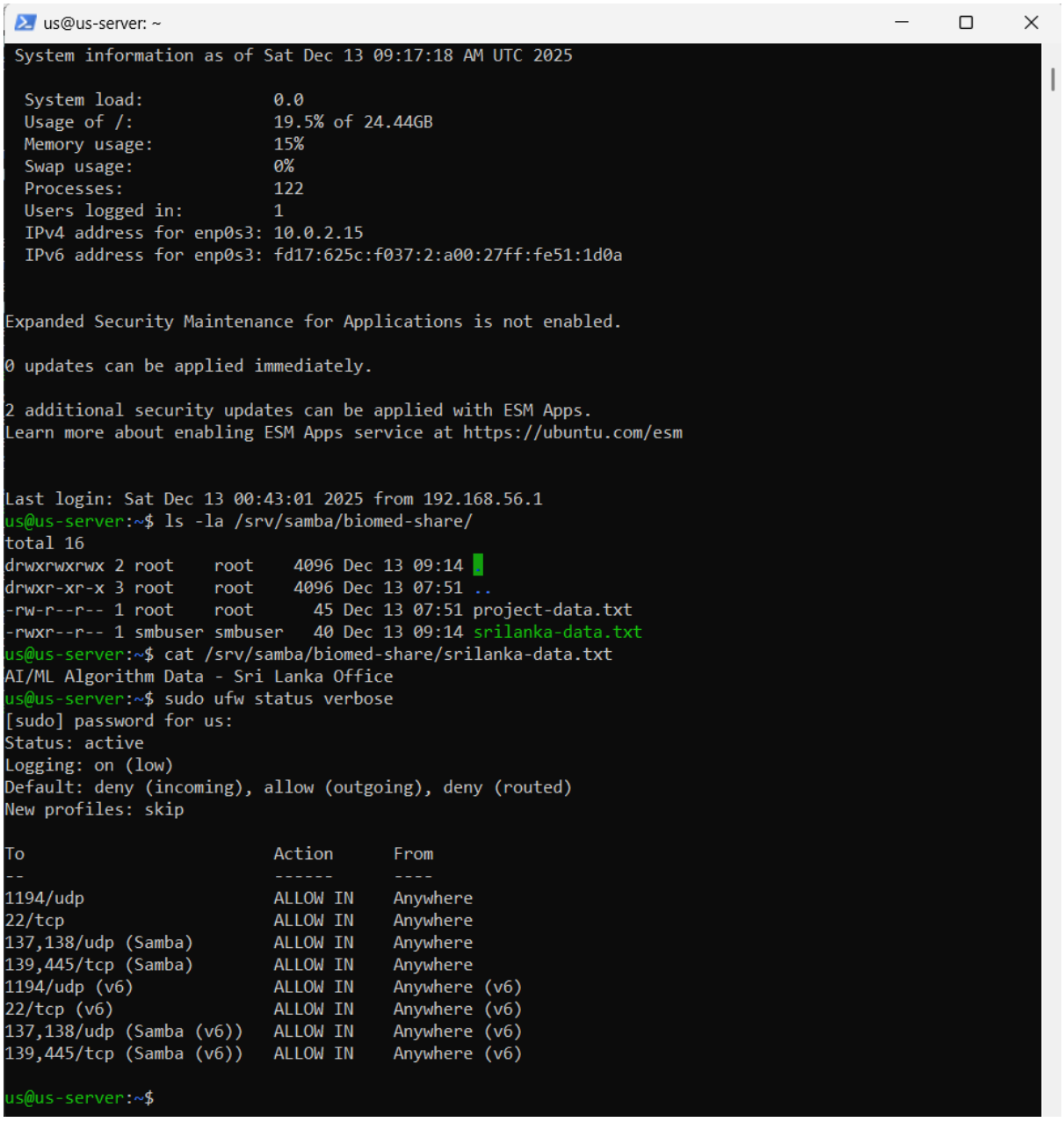
Expected Outcome:

- Files created on the Sri Lanka Client are visible on the US Server
- File contents can be read successfully


us@us-server: ~
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\WINDOWS\system32> ssh us@192.168.56.10
us@192.168.56.10's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Sat Dec 13 09:17:18 AM UTC 2025
System load: 0.0
Usage of /: 19.5% of 24.44GB
Memory usage: 15%
Swap usage: 0%
Processes: 122
Users logged in: 1
IPv4 address for enp0s3: 10.0.2.15
IPv6 address for enp0s3: fd17:625c:f037:2:a00:27ff:fe51:1d0a
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
2 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm
Last login: Sat Dec 13 00:43:01 2025 from 192.168.56.1
us@us-server:~$ ls -la /srv/samba/biomed-share/
total 16
drwxrwxrwx 2 root root 4096 Dec 13 09:14 .
drwxr-xr-x 3 root root 4096 Dec 13 07:51 ..
-rw-r--r-- 1 root root 45 Dec 13 07:51 project-data.txt
-rwxr--r-- 1 smbuser smbuser 40 Dec 13 09:14 srilanka-data.txt
us@us-server:~$ cat /srv/samba/biomed-share/srilanka-data.txt
AI/ML Algorithm Data - Sri Lanka Office
us@us-server:~$

10 Security Considerations

- OpenVPN encrypts all traffic between Sri Lanka and US
- Samba is accessible only through the VPN subnet
- UFW firewall allows only required services (OpenVPN, SSH, Samba)
- Private keys are masked in screenshots



11 Troubleshooting

- **VPN connection issues:** Check OpenVPN logs and firewall rules
- **Ping failure:** Verify IP forwarding and VPN interface
- **Samba access issues:** Verify service status and user credentials

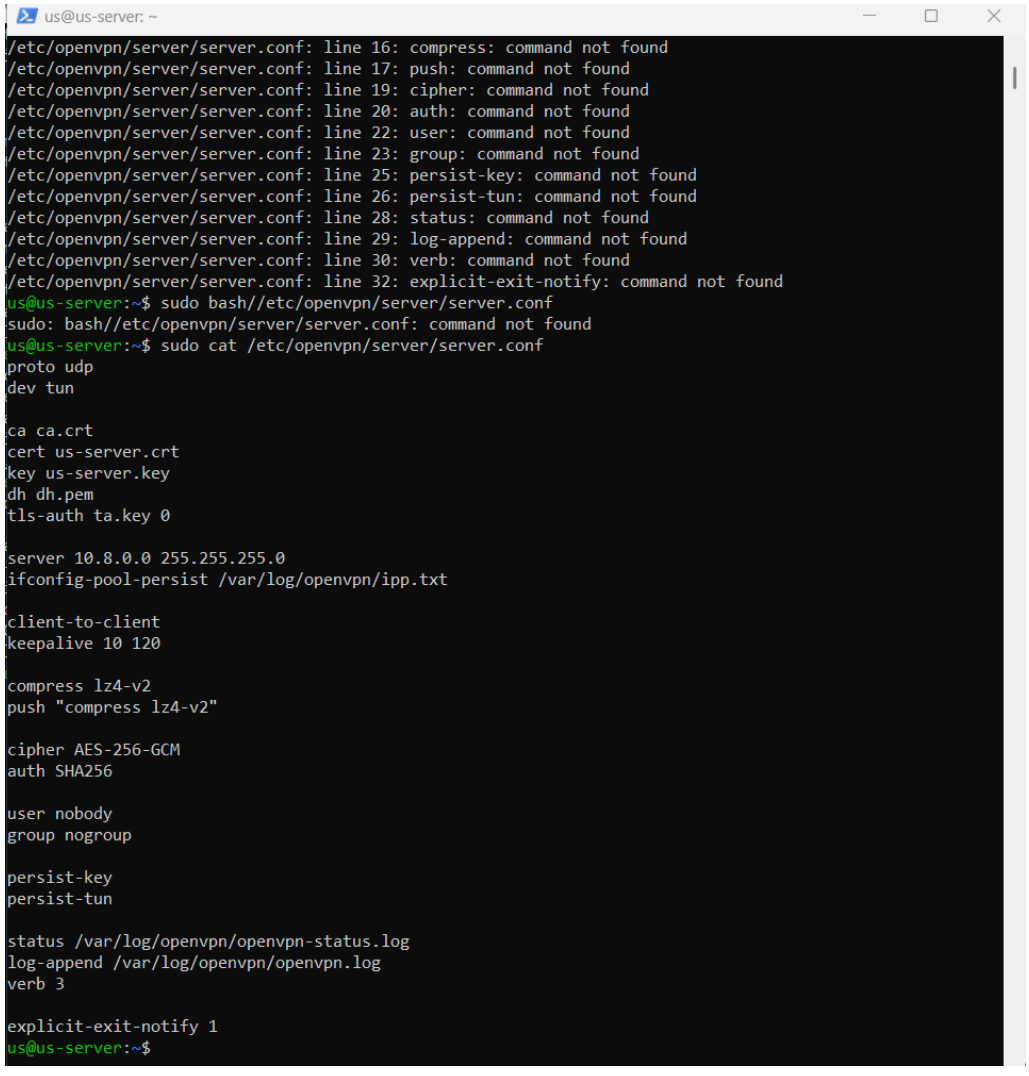
12 Conclusion

A secure OpenVPN tunnel was successfully established between SriLanka-Client and USServer. VPN connectivity was verified with 100% successful ping tests. A Samba server hosted on the US-Server was securely accessed from the SriLanka-Client through the VPN, demonstrating confidential file sharing in a Linux environment.

13 Appendix

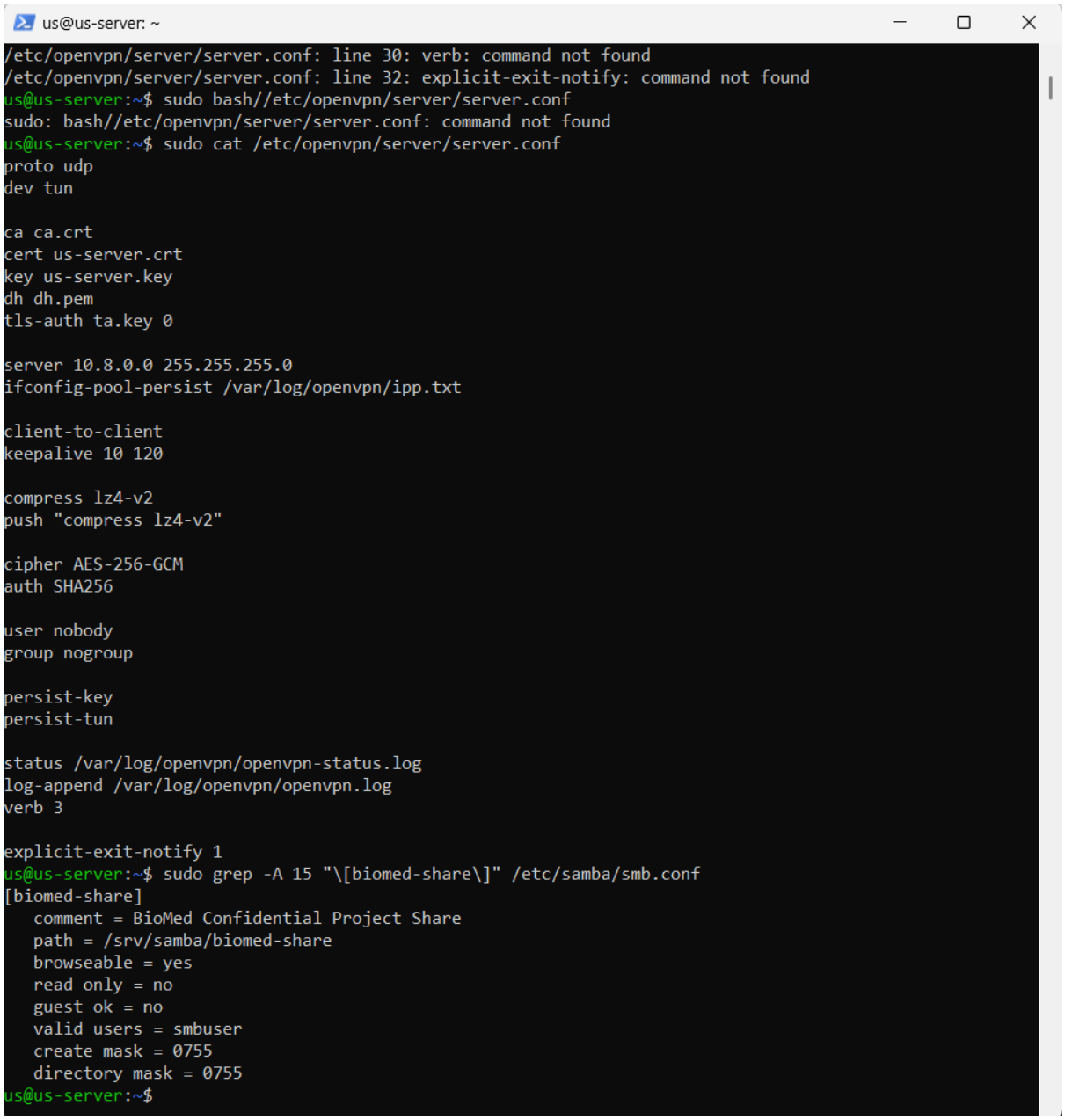
13.1 Server Configuration File

/etc/openvpn/server/server.conf - Shows how the VPN server was configured on the US Server



13.2 Client Configuration File

/etc/openvpn/client/client.conf - Shows how the Sri Lanka client connects securely to the VPN server



13.3 Samba Configuration File

/etc/samba/smb.conf - Shows the Samba share used for confidential file sharing