COSC2733 - UNIX SYSTEM ADMINISTRATION AND PROGRAMMING

OPENVPN Access Server

Group 6

Lecture: Dr. Jonathan Crellin
Dr. Jeff Nijsse

Nguyen Tu Quoc Thai (s3957050)
Nguyen Dinh Lam (s3990403)
Pham Dang Khoa (s3884419)

Date: 22 August 2024

Table of Contents

Introduction

This project aims to establish a secure and accessible Virtual Private Network (VPN) using the OpenVPN software on an Ubuntu-based system. The VPN will enable remote users to securely connect to a private network over the public internet, providing access to resources as if they were physically connected to the local network. This project will configure the OpenVPN server to support various client devices, including desktop computers, laptops, iOS, and Android devices. Furthermore, comprehensive user documentation will be provided to facilitate easy setup and connection.

By successfully implementing this OpenVPN server, our team will gain hands-on experience in network administration, security, and system configuration. Through collaboration in establishment, and testing the application, this assignment cultivates critical problem-solving abilities and enhances the technical skills of the whole team.

I. Planning

1. Requirements Specification

Functional Requirements

The OpenVPN server must provide secure and reliable remote access to a private network. Core functionalities include:

1. **User Authentication**: Implementing robust authentication mechanisms to verify user identities before granting VPN access. This will involve secure password storage or integration with external authentication systems.
2. **Data Encryption**: Employing strong encryption protocols to safeguard data transmitted over the VPN. This includes protecting both data confidentiality and integrity during transit.

3. **Multi-device Support**: Ensuring compatibility with a wide range of devices, including desktop, laptop, iOS, and Android platforms. This requires configuring OpenVPN clients and providing clear setup instructions for each platform.
4. **Access Control**: Implementing granular access controls to restrict user permissions based on roles or groups. This involves creating different user profiles with varying levels of network access.
5. **User Activity Logging:** Maintaining detailed logs of VPN connections, including connection times, data usage, and IP addresses. This information is essential for troubleshooting, security audits, and performance analysis.
6. **Split Tunneling:** Allowing users to selectively route specific traffic through the VPN while bypassing others. This provides flexibility and optimizes network performance.
7. **Bandwidth Management:** Implementing traffic shaping techniques to manage network congestion and ensure fair resource allocation among users.

Non-Functional Requirements

The VPN server must meet specific performance, scalability, reliability, security, and usability criteria:

1. **Performance**: Maintaining low latency and high-speed connections to provide a seamless user experience. This involves optimizing network configurations and hardware resources.
2. **Scalability**: Supporting a growing number of concurrent users without compromising performance. The system should be designed to handle increasing user loads efficiently.
3. **Reliability**: Ensuring high availability through redundant components and automated failover mechanisms. This includes regular system monitoring and backup strategies.

4. **Security**: Implementing robust security measures to protect the VPN infrastructure and user data. This entails using strong encryption, firewalls, intrusion detection systems, and regular security audits.
5. **Usability:** Providing user-friendly client software and clear documentation for easy setup and configuration. The VPN system should be intuitive for users with varying technical expertise.

2. System Requirements

a. Server Specifications:

To accommodate the expected workload and ensure optimal performance, the OpenVPN server requires the following minimum hardware (OpenVPN n.d) and software resources:

- **CPU:** At least 4 vCPUs for efficient handling of multiple concurrent connections.
- **RAM:**
    i. **Base requirement:** Minimum 1 GB of memory to support the OpenVPN server and client processes.
    ii. **Additional memory:** Approximately 1GB for every 150 connected devices.
- **Storage:** 16GB is sufficient for logs, certificates, and configuration files.
- **Bandwidth:** 1 Gbps network interface, 2 TB monthly transfer
- **Operating System:** Ubuntu 20.04 LTS and above.

b. Software Requirements:

The following software components are essential for building and operating the OpenVPN server:

- **OpenVPN 2.5.x:** A widely used and secure open-source VPN software that provides the core functionality for creating and managing VPN tunnels.
- **Easy-RSA 3.x:** A tool for generating and managing digital certificates required for OpenVPN authentication.
- **UFW (Uncomplicated Firewall):** A user-friendly firewall configuration tool to protect the server from unauthorized access.

Technology Choices

Based on thorough evaluation, the following technologies were selected for the OpenVPN project:

1. **Operating System: Ubuntu 24.04 LTS:** Chosen for its long-term support, stability, and robust package management system.
2. **VPN Software: OpenVPN 2.6.9:** Selected for its open-source nature, strong security features, cross-platform compatibility, and extensive community support.
3. **Certificate Management: Easy-RSA 3.2.0:** Adopted for its user-friendly interface and ability to generate and manage certificates efficiently.
4. **Firewall: UFW:** Chosen for its simplicity and ease of use in configuring firewall rules.

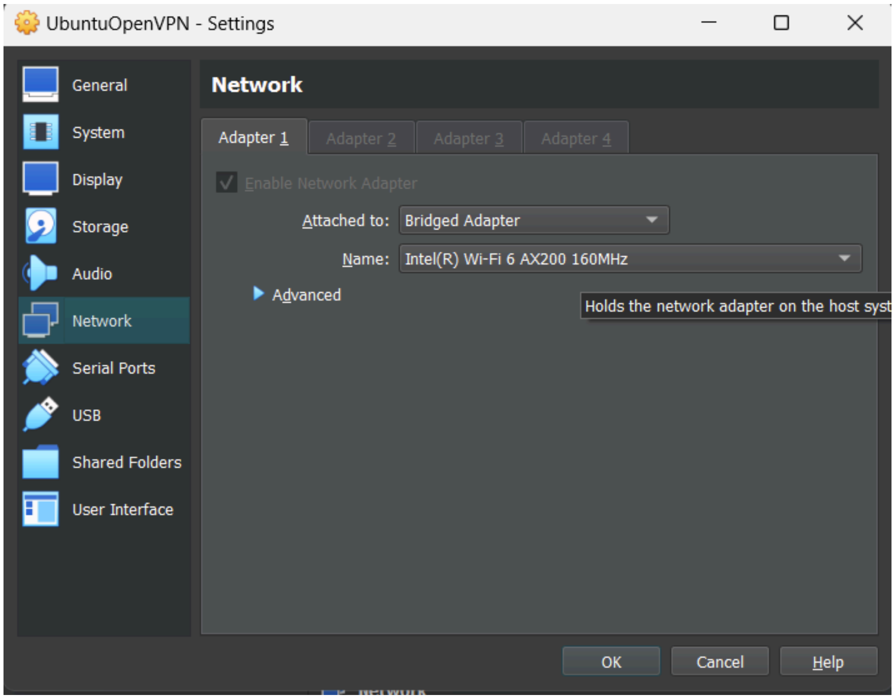
II. Implementation

● *Installation Process*

Below is the installation process of OpenVPN Access server on the Ubuntu VM. Since the server package was already set up, the need of manually setting up each one such as RSA, UFW, server keys, and Diffie-Hellman parameters, is not required.

A. VMs setup:

Step 1: Setting up one Ubuntu Virtual Machine to host the VPN server.



☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Intel(R) Wi-Fi 6 AX200 160MHz

Holds the network adapter on the host syst

Figure 1: VM's network setting

- Before installing the server, go to **Settings** ↠ **Network**, and change the "**Attached to:**" field to Bridged Adapter. After that, Ubuntu shows your Ipv4 address and other information in the system Settings (Figure 2).

Step 2: Create another Ubuntu VM for a Linux client to connect to the server with the **same** Network setting.

B. Installation:

Step 1: Go to **https://openvpn.net/** and sign up. After logging in, the OpenVPN console will appear in the user interface (Figure 3).

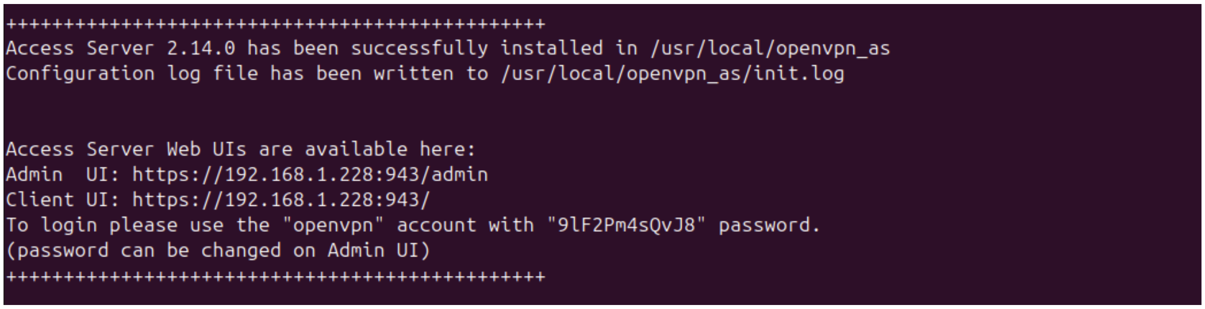
Step 2: Click on "Install Access Server" on the sidebar to find the command to install on Linux.

Step 3: Open the **Terminal** and type **sudo -s** to gain root privilege. Enter the command below to the terminal.

```
bash <(curl -fsS https://as-repository.openvpn.net/as/install.sh)
```

- Within the **.sh** file is a series of pre-made commands to download all necessary packages. Below are the notable parts of it:
    - Firstly, the system created the **keyrings** in the **apt** directory with the **wget** command to install the key rings from the https link (Figure 5).
    - Secondly, the OpenVPN needs to be updated with **apt update** command and also the installation of ca-certificates and net-tools happening in this phase (Figure 6).
    - In the next phase, “openvpn-as” ($PLIST) is installed (Figure 7).
    - Finally, after running the command line in the beginning of Step 4, the terminal console will show the completed installation process of the OpenVPN application in Ubuntu's user-interface (Figure 8).

Step 4: After the installation, OpenVPN will provide an address for Admin UI, and another for the Client UI. It is also included in the admin’s username and password (Figure 9).



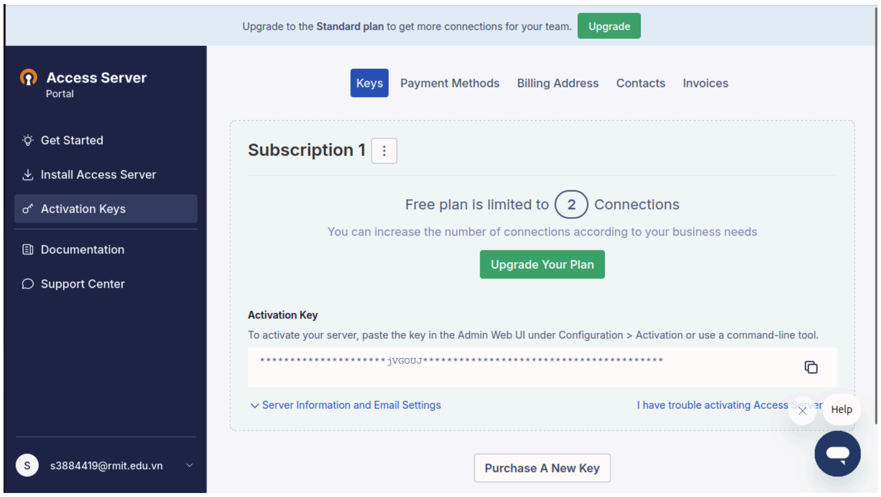
```
+++++++++++++++++++++++++++++++++++++++++++++++
Access Server 2.14.0 has been successfully installed in /usr/local/openvpn_as
Configuration log file has been written to /usr/local/openvpn_as/init.log


Access Server Web UIs are available here:
Admin  UI: https://192.168.1.228:943/admin
Client UI: https://192.168.1.228:943/
To login please use the "openvpn" account with "9lF2Pm4sQvJ8" password.
(password can be changed on Admin UI)
+++++++++++++++++++++++++++++++++++++++++++++++
```

Figure 9: Admin and Client UI’s information.

C. Activation:

<u>Step 1</u>: Sign in to the Admin UI using the provided username and password in the last step (Figure 10).

<u>Step 2</u>: Return to the Access server portal, and click on “Activation Keys” (Figure 11). Here, copy the provided key for Subscription 1.



Subscription 1

Free plan is limited to 2 Connections

You can increase the number of connections according to your business needs

Activation Key

To activate your server, paste the key in the Admin Web UI under Configuration > Activation or use a command-line tool.

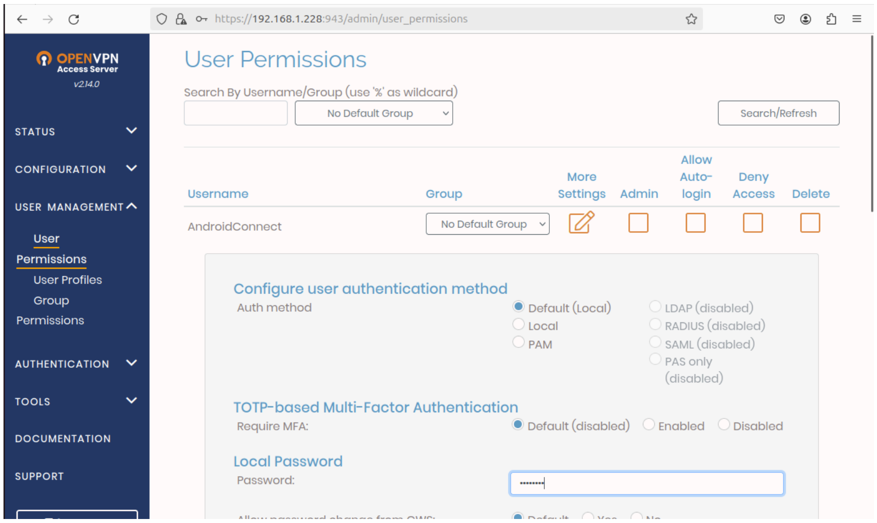
```
********************jVGOUJ***************************************
```

Figure 11: Activation Keys page.

<u>Step 3</u>: Go back to the Admin UI. Go to **Configuration** ↠ **Activation**, and activate the subscription using the key (Figure 12).

- ## ***User management***

1. <u>Create a new user</u>: To create a new user, go to **User Management** ↠ **User Permissions**, and enter a new username and click on More settings to add a password (Figure 13).



User Permissions

Search By Username/Group (use '%' as wildcard)

No Default Group

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
AndroidConnect	No Default Group	✎	□	□	□	□

Configure user authentication method

Auth method: ● Default (Local) ○ Local ○ PAM ○ LDAP (disabled) ○ RADIUS (disabled) ○ SAML (disabled) ○ PAS only (disabled)

TOTP-based Multi-Factor Authentication

Require MFA: ● Default (disabled) ○ Enabled ○ Disabled

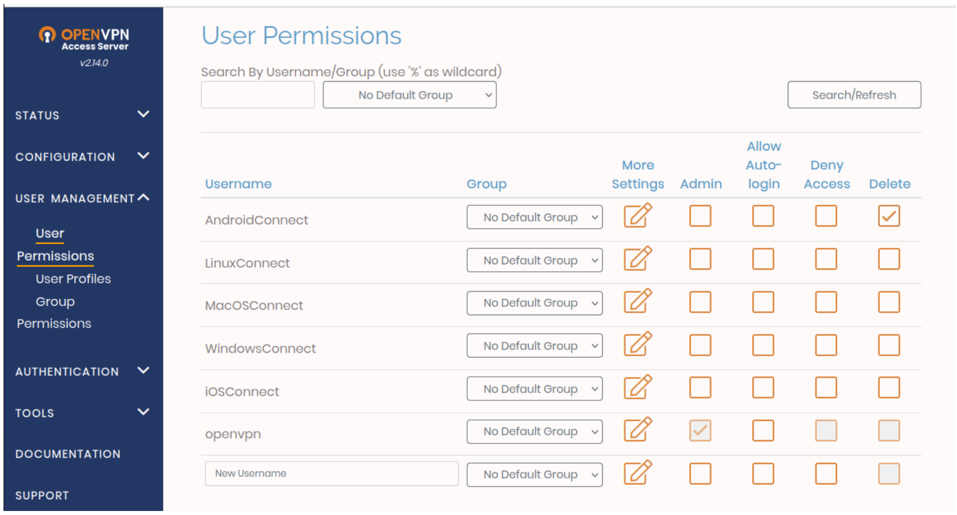
Local Password

Password: ••••••••

Figure 13: User permissions page.

- Then, hit **Save Settings** ↠ **Update Running Server**.

2. <u>Change user's password</u>: To change a user's password, open the More settings tab of that user, then enter a new password. Hit **Save Settings** ↠ **Update Running Server** to update that user. (similar to creating a new user)
3. <u>Delete an existing user</u>: To delete a user, check the delete box, then hit **Save Settings** ↠ **Update Running Server** (Figure 14).



User Permissions

Search By Username/Group (use '%' as wildcard)

No Default Group

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
AndroidConnect	No Default Group	✎	□	□	□	☑
LinuxConnect	No Default Group	✎	□	□	□	□
MacOSConnect	No Default Group	✎	□	□	□	□
WindowsConnect	No Default Group	✎	□	□	□	□
iOSConnect	No Default Group	✎	□	□	□	□
openvpn	No Default Group	✎	☑	□	□	□
New Username	No Default Group	✎	□	□	□	□

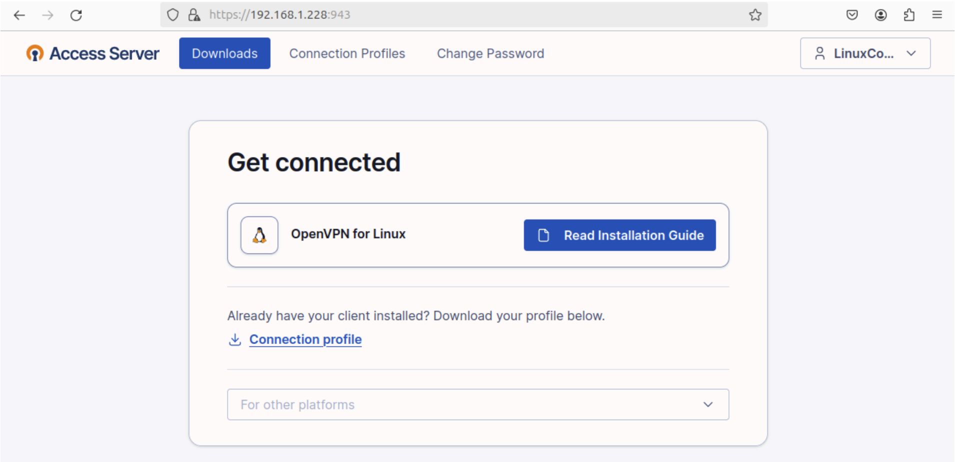
Figure 14: Delete a user.

Connection

Below are instructions on how to connect to the VPN server on Ubuntu Linux. For other platforms, see *User Documentation*.

Step 1: On server VM, go to the Client UI (in figure 15) and log in using the username and password created earlier in *User management*.

Step 2: When logged in, click on Connection profile (.ovpn) to download it (Figure 16).



Already have your client installed? Download your profile below.

Figure 16: Connection profile can be found when logged in.

Step 3: Transfer the profile to your Client VM using SCP or any other preferred methods.

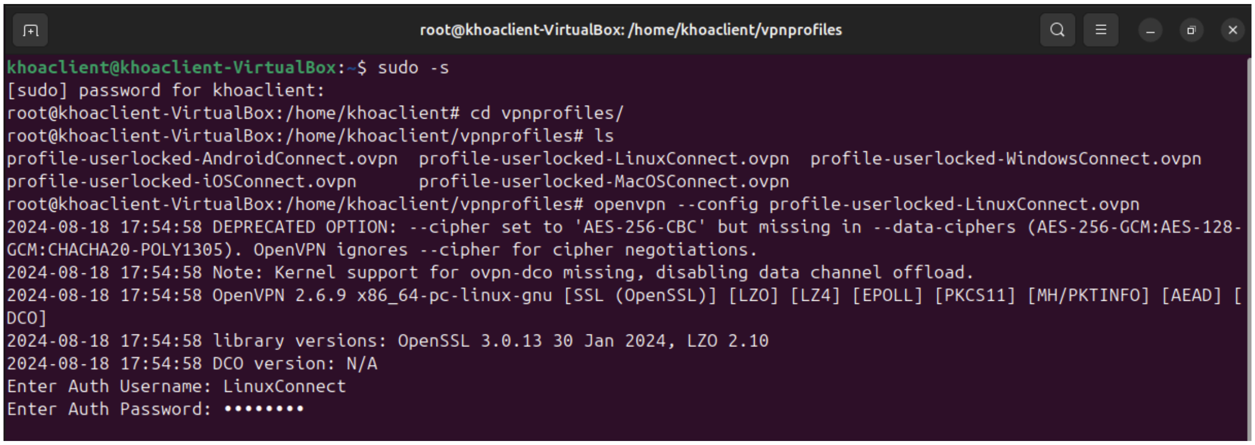
Step 4: Install OpenVPN on client side using the following command:

```
sudo apt install openvpn
```

Step 5: Enter the following command on your **Client VM's Terminal**:

```
openvpn –config {your_connection_profile_path}
```

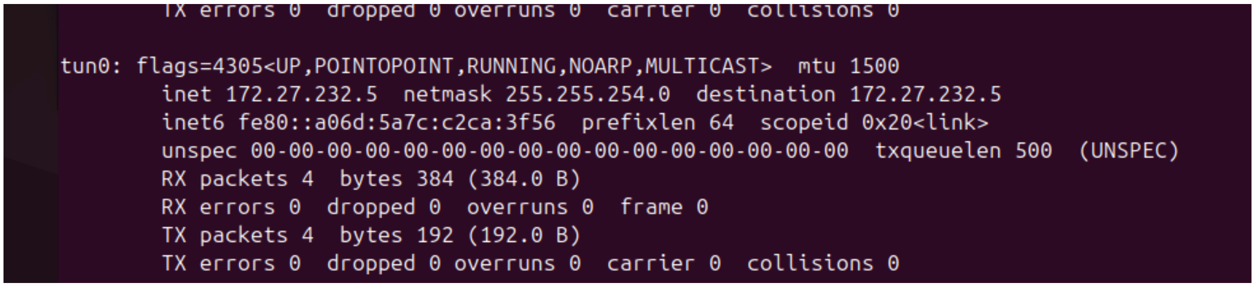
Step 6: Enter the username and password of that profile.



```
khoaclient@khoaclient-VirtualBox:~$ sudo -s
[sudo] password for khoaclient:
root@khoaclient-VirtualBox:/home/khoaclient# cd vpnprofiles/
root@khoaclient-VirtualBox:/home/khoaclient/vpnprofiles# ls
profile-userlocked-AndroidConnect.ovpn  profile-userlocked-LinuxConnect.ovpn  profile-userlocked-WindowsConnect.ovpn
profile-userlocked-iOSConnect.ovpn      profile-userlocked-MacOSConnect.ovpn
root@khoaclient-VirtualBox:/home/khoaclient/vpnprofiles# openvpn --config profile-userlocked-LinuxConnect.ovpn
2024-08-18 17:54:58 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-
GCM:CHACHA20-POLY1305). OpenVPN ignores --cipher for cipher negotiations.
2024-08-18 17:54:58 Note: Kernel support for ovpn-dco missing, disabling data channel offload.
2024-08-18 17:54:58 OpenVPN 2.6.9 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [
DCO]
2024-08-18 17:54:58 library versions: OpenSSL 3.0.13 30 Jan 2024, LZO 2.10
2024-08-18 17:54:58 DCO version: N/A
Enter Auth Username: LinuxConnect
Enter Auth Password: ••••••••
```

Figure 17: Connecting to VPN server.

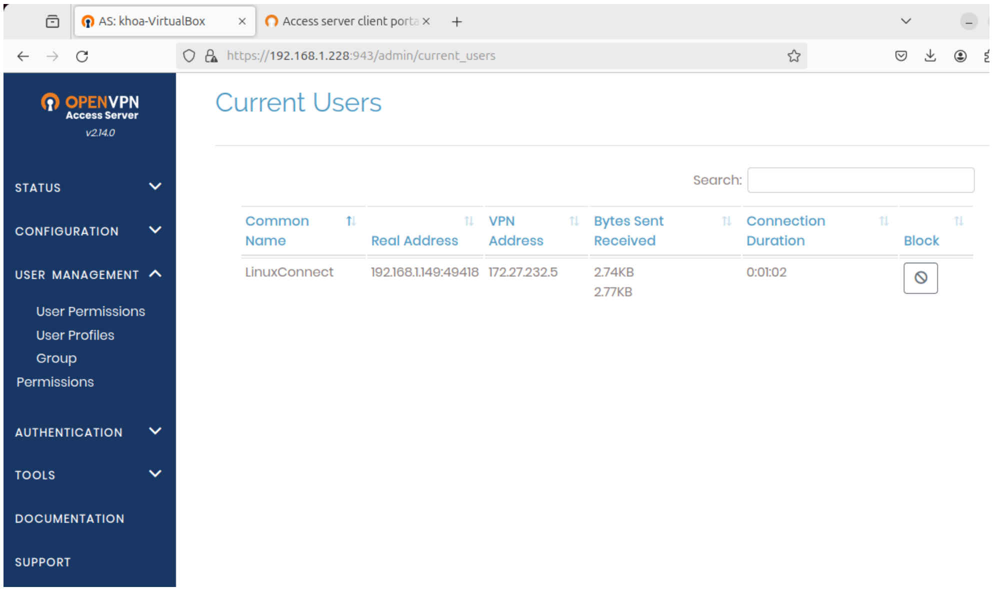
Step 7: To verify the connection, open another Terminal window and type in **ifconfig**. Look for the appearance of **tun0**, and your VPN address next to **inet**.



```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 172.27.232.5  netmask 255.255.254.0  destination 172.27.232.5
        inet6 fe80::a06d:5a7c:c2ca:3f56  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 4  bytes 384 (384.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 192 (192.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 18: tun0 appears when connecting to the VPN server.

- On server VM, go to the Admin UI, and go to **Status** ↠ **Current Users** to see a list of all current users that are connecting to the VPN (Figure 19).



Current Users

Common Name	Real Address	VPN Address	Bytes Sent Received	Connection Duration	Block
LinuxConnect	192.168.1.149:49418	172.27.232.5	2.74KB 2.77KB	0:01:02	⃠

Figure 19: List of all current users. (Admin UI)

III. Testing

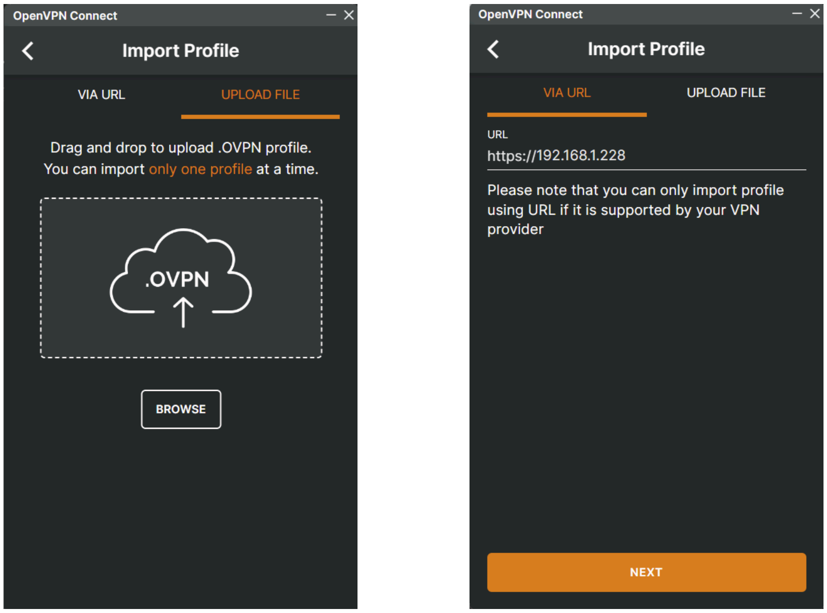
1. Objective

Testing the OpenVPN application with the provided **.ovpn** file from the host to access to the private IP on **Windows** platform.

2. Steps

Step 1: Go to https://openvpn.net/client/client-connect-vpn-for-windows/ to download the application (Figure 20).

Step 2: After the installation, the OpenVPN application for Windows will appear on the user-interface. Now, import the **.ovpn** file to the system or use the provided IP address from the host to connect to the OpenVPN server (Figure 21 a, b).



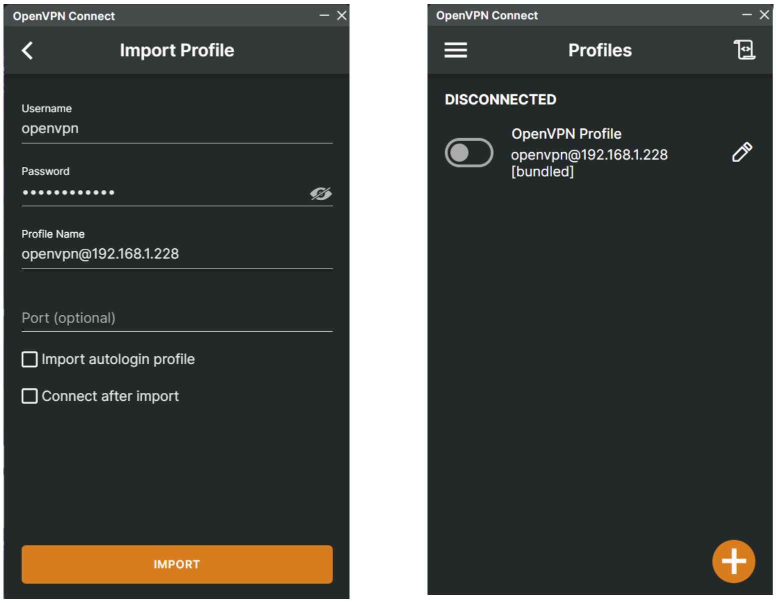
Drag and drop to upload .OVPN profile.
You can import only one profile at a time.

URL
https://192.168.1.228

Please note that you can only import profile using URL if it is supported by your VPN provider

Figure 21 a, b: Access to application with two methods.

Step 3: The application displays an imported profile with username and password (Figure 22 a, b).



Username
openvpn

Password
••••••••••••

Profile Name
openvpn@192.168.1.228

Port (optional)

□ Import autologin profile

□ Connect after import

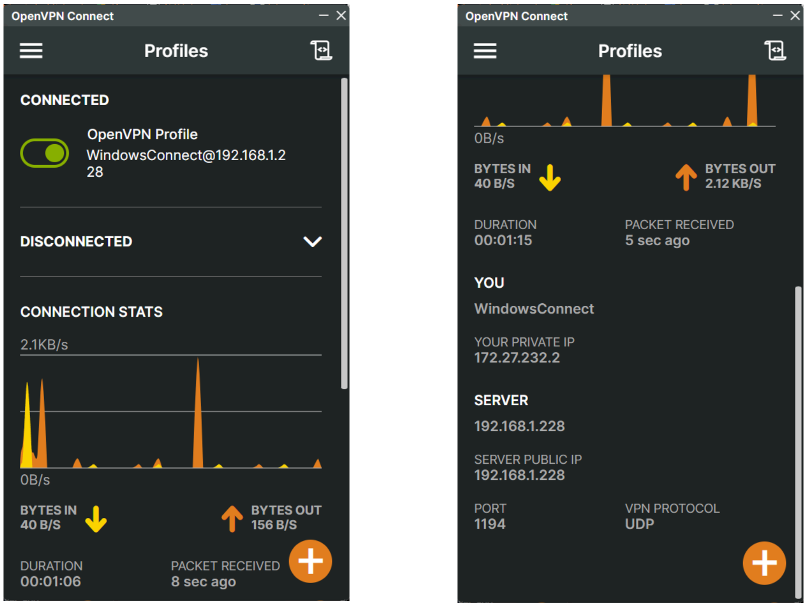
DISCONNECTED

OpenVPN Profile
openvpn@192.168.1.228
[bundled]

Figure 22 a, b: Imported **.ovpn** file process.

3. Expected Outcome

Following the imported process, the OpenVPN should show all the data of the user profile including: Connection Stats, Duration and the private IP.



CONNECTED

OpenVPN Profile
WindowsConnect@192.168.1.228

DISCONNECTED

CONNECTION STATS

BYTES IN 40 B/S
BYTES OUT 156 B/S
DURATION 00:01:06
PACKET RECEIVED 8 sec ago

BYTES IN 40 B/S
BYTES OUT 2.12 KB/S
DURATION 00:01:15
PACKET RECEIVED 5 sec ago

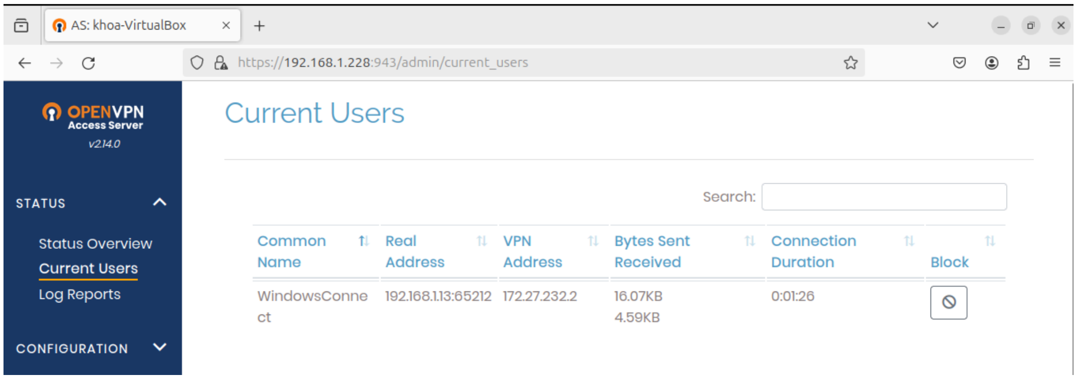
YOU
WindowsConnect
YOUR PRIVATE IP 172.27.232.2

SERVER
192.168.1.228
SERVER PUBLIC IP 192.168.1.228
PORT 1194
VPN PROTOCOL UDP

Figure 23 a, b: Connecting process.

4. Actual Result

The administrator can observe the current clients on the OpenVPN management interface following the connection process (Figure 24).



https://192.168.1.228:943/admin/current_users

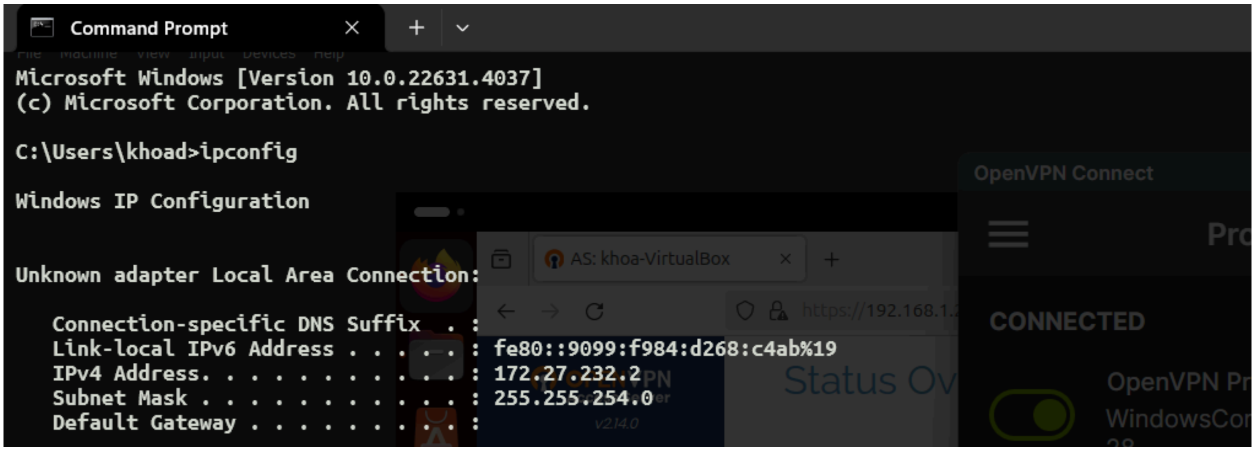
Current Users

Search:

Common Name	Real Address	VPN Address	Bytes Sent Received	Connection Duration	Block
WindowsConnect	192.168.1.13:65212	172.27.232.2	16.07KB 4.59KB	0:01:26	⊘

Figure 24: Connected Windows user on management interface.

In the Windows cmd, the user runs the command **“ipconfig”** to overlook the specific information of connected data (Figure 25).



```
Microsoft Windows [Version 10.0.22631.4037]
(c) Microsoft Corporation. All rights reserved.

C:\Users\khoad>ipconfig

Windows IP Configuration


Unknown adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9099:f984:d268:c4ab%19
   IPv4 Address. . . . . . . . . . . : 172.27.232.2
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . :
```

Figure 25: Connected user’s data in Windows cmd.

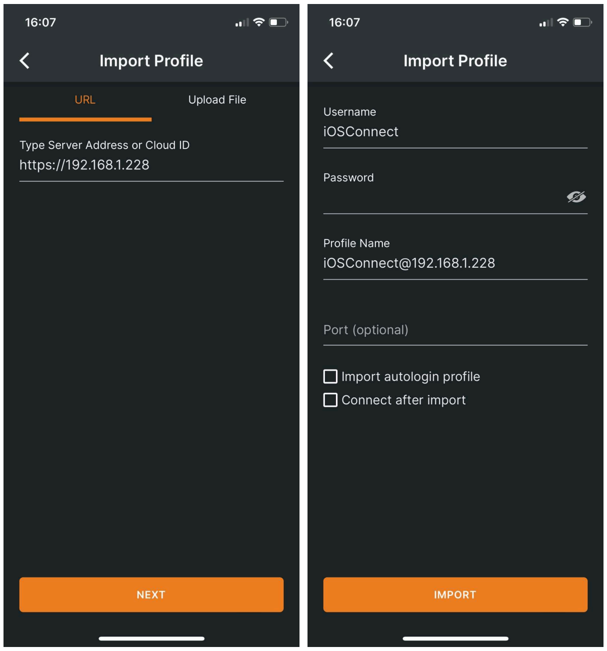
IV. User Documentation

- The steps for connecting to the VPN server on iOS and Android devices are similar, so users of both platforms can follow the instructions below.

  Step 1. Download the OpenVPN Connect app from the App Store or CH Play.

  Step 2. Connect to the server.

- The OpenVPN Connect application offers 2 ways to connect to the VPN server:
  - ➢ Option 1: Using the server address.
    - Enter the provided IP address of the VPN server. Then, enter the username and password.


16:07

Import Profile

URL | Upload File

Type Server Address or Cloud ID
https://192.168.1.228

NEXT

16:07

Import Profile

Username
iOSConnect

Password

Profile Name
iOSConnect@192.168.1.228

Port (optional)

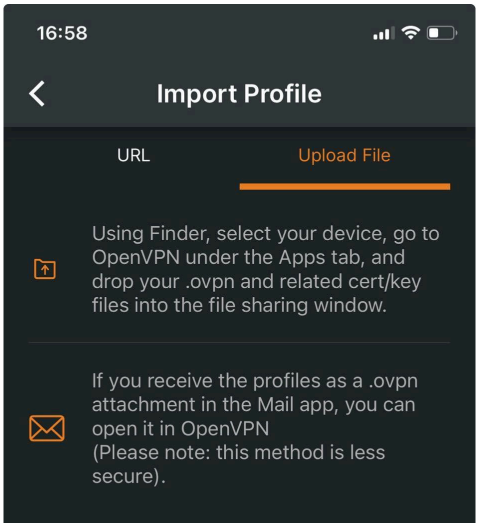
□ Import autologin profile
□ Connect after import

IMPORT

Figure 26 a, b: Connect via server IP address.

➢ Option 2: Using a connection profile (.opvn)

- A profile can be imported via email (i.e., Gmail) or cloud storage (i.e., Google Drive), as noted in the application below.


16:58

Import Profile

URL | Upload File

Using Finder, select your device, go to OpenVPN under the Apps tab, and drop your .ovpn and related cert/key files into the file sharing window.

If you receive the profiles as a .ovpn attachment in the Mail app, you can open it in OpenVPN
(Please note: this method is less secure).

Figure 27: Instructions on importing connection profile.

V. Group and individual reflections

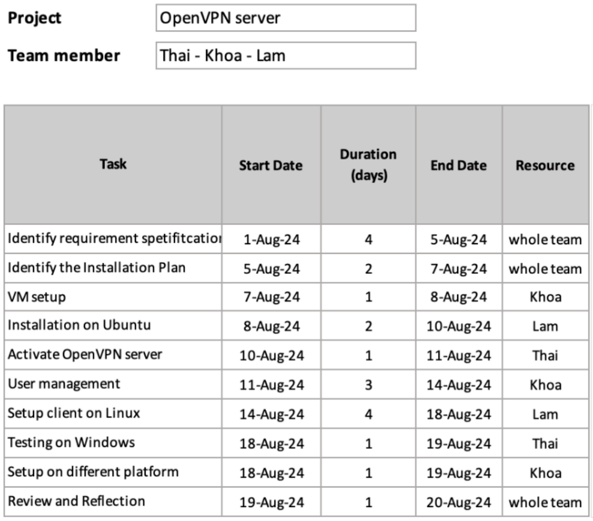
1. Group reflection

Our team's experience implementing the OpenVPN Access Server project was both challenging and enlightening. This assignment provided us with practical experience in network administration, security, and system configuration within the Unix environment. In addition, collaboration was crucial to our success. We effectively managed our time and coordinated efforts using tools like the Gantt Chart and regular team meetings. This approach helped us meet deadlines and leverage each member's strengths. The diverse tasks involved - from VM setup and server installation to user management and cross-platform testing - allowed each of us to develop a range of skills and share our expertise.

One of the most significant learning outcomes was the improvement in our problem-solving abilities. We faced various challenges, particularly during the setup and debugging phases, which required critical thinking and teamwork to overcome. This process not only enhanced our technical skills but also improved our ability to communicate complex ideas clearly within the team. Consequently, it deepened our understanding of cybersecurity principles, emphasizing the importance of robust user authentication, data encryption, and access control. Creating user documentation further challenged us to explain technical concepts accessibly, improving our technical writing skills.

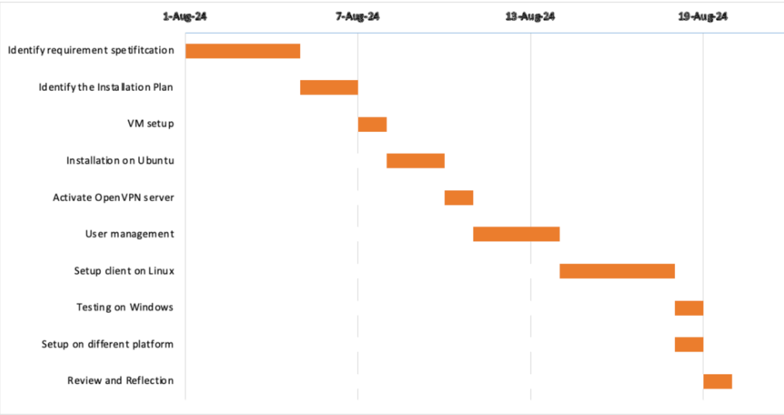
Overall, this project provided a comprehensive learning experience that will be invaluable in our future IT and cybersecurity careers, while also demonstrating our ability to work effectively in a small team - a key component of this assessment.

The Gantt Chart tool



Project	OpenVPN server
Team member	Thai - Khoa - Lam

Task	Start Date	Duration (days)	End Date	Resource
Identify requirement spetifitcatio	1-Aug-24	4	5-Aug-24	whole team
Identify the Installation Plan	5-Aug-24	2	7-Aug-24	whole team
VM setup	7-Aug-24	1	8-Aug-24	Khoa
Installation on Ubuntu	8-Aug-24	2	10-Aug-24	Lam
Activate OpenVPN server	10-Aug-24	1	11-Aug-24	Thai
User management	11-Aug-24	3	14-Aug-24	Khoa
Setup client on Linux	14-Aug-24	4	18-Aug-24	Lam
Testing on Windows	18-Aug-24	1	19-Aug-24	Thai
Setup on different platform	18-Aug-24	1	19-Aug-24	Khoa
Review and Reflection	19-Aug-24	1	20-Aug-24	whole team



2. Individual reflections

★ Nguyen Dinh Lam (s3990403)

After working on this project with my Team, I know exactly how to create a Server by using OpenVPN. I have gained much experience in hosting servers and greatly improved my technical abilities in network management and security. Using OpenVPN, Easy-RSA, and UFW in practice has given me practical knowledge that enhances my theoretical comprehension. My problem-solving abilities were put to the test during the project, particularly when it came to setting different system components and debugging server issues. Working with my team helped me become a better communicator and taught me the importance of utilizing the different qualities that exist within a group. I gained the ability to communicate technical ideas clearly and actively listen to the opinions and worries of my teammates. My technical writing abilities were sharpened by producing user documentation and adding to the project report, which challenged me to communicate difficult ideas in an understandable way.

The project's deadlines and breadth forced me to hone my time management abilities. I gained knowledge on how to successfully prioritize activities, make reasonable goals, and adjust to unforeseen difficulties without sacrificing the project's deadline. This experience has increased my confidence in my ability to manage several tasks at once.

Possibly above all, this endeavor fostered a greater understanding of cybersecurity. It affected my approach to system configuration and user administration, causing me to constantly prioritize security when making decisions. I now have a more comprehensive grasp of network security and how different parts work together to provide a safe environment.

By investigating more complex VPN ideas, concentrating on performance optimization, and honing my ability to foresee possible security flaws, I hope to build on this basis going ahead.

★ Nguyen Tu Quoc Thai (s3957050)

For this project, by successfully creating the OpenVPN server on the VMs led me to gain more knowledge from setting up the network port to apply the security layer of VPN on many different platforms. Also, it is essential to deeply understand the command lines on Ubuntu's terminal, such as assisting me in making the bridge connection between the host server and users through OpenVPN on remote devices. Moreover, the whole team consistently collaborates together to identify the key goals of the projects and utilizes the Gantt Chart and Teams Meeting tools to create the schedule of deadlines for each part. Therefore, I have the opportunity to effectively strengthen my problem-solving skills by testing on numerous platforms, and showing how to execute the completed version of this project in the most convenient way for our developer team and users.

After all, this assignment provided me with the key concept of Linux systems and practical cases in reality environments.

★ Pham Dang Khoa (s3884419)

Through this assignment, I gained foundational knowledge in setting up an OpenVPN server on an Ubuntu virtual machine. Alongside this, I learned essential tasks such as preparing a VM, remotely accessing another VM, and transferring files between machines. Additionally, I developed skills in creating user documentation and collaborating within a small team to approach the project effectively. Overall, this assessment significantly expanded my understanding of Linux-based systems and network management, especially considering my lack of prior experience in this area.

VI. Video demo link

YouTube link for demo: *https://youtu.be/beyDJldXj2g*

VI. References

[1] OpenVPN. (n.d.). “Easy-RSA 3 Quickstart README”, Github. Available at: *https://github.com/OpenVPN/easy-rsa/blob/master/README.quickstart.md (Accessed: 20 August 2024).*

[2] *Business VPN for secure networking* (2023) *OpenVPN*. Available at: https://openvpn.net/ (Accessed: 20 August 2024).

[3] Inc., O. (2013) *OpenVPN connect – openvpn app*, *App Store*. Available at: https://apps.apple.com/us/app/openvpn-connect-openvpn-app/id590379981(Accessed: 20 August 2024).

[4] *OpenVPN connect – openvpn app - apps on Google Play* (no date a) *Google*. Available at: https://play.google.com/store/apps/details?id=net.openvpn.openvpn(Accessed: 20 August 2024).

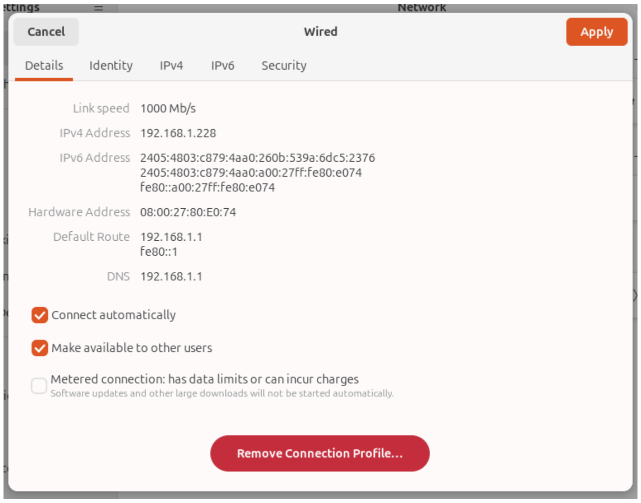
[5] *OpenVPN connect - client software for Windows* (2024) *OpenVPN*. Available at: https://openvpn.net/client/client-connect-vpn-for-windows/(Accessed: 20 August 2024).

[6] OpenVPN - *Linux*. Available at: https://openvpn.net/as-docs/linux.html (Accessed: 20 August 2024).

[7] *Enterprise open source and linux* (n.d) *Ubuntu*. Available at: https://ubuntu.com/(Accessed: 20 August 2024).

[8] *Security - firewall | ubuntu (n.d)*. Available at: https://ubuntu.com/server/docs/security-firewall(Accessed: 20 August 2024).

VII. Appendices



Link speed 1000 Mb/s

IPv4 Address 192.168.1.228

IPv6 Address 2405:4803:c879:4aa0:260b:539a:6dc5:2376
2405:4803:c879:4aa0:a00:27ff:fe80:e074
fe80::a00:27ff:fe80:e074

Hardware Address 08:00:27:80:E0:74

Default Route 192.168.1.1
fe80::1

DNS 192.168.1.1

☑ Connect automatically

☑ Make available to other users

□ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.

Figure 2: VM’s Network information.

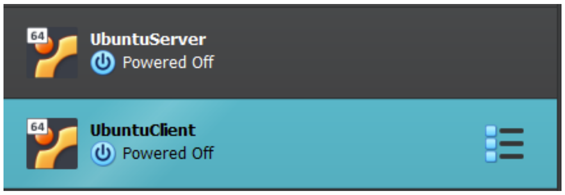
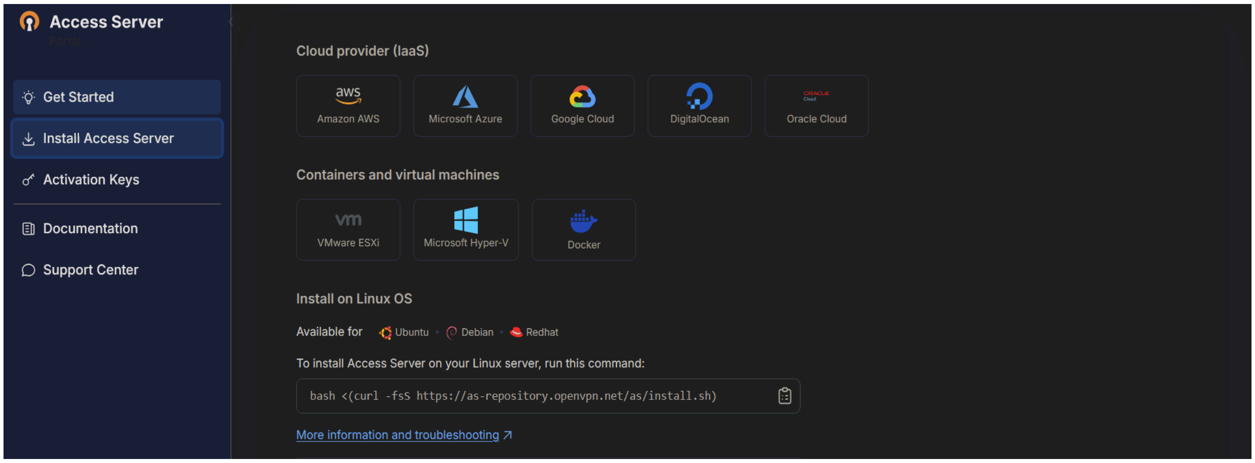


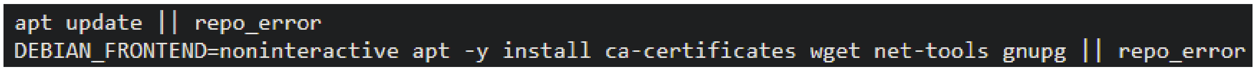
Figure 3: List of VMs that need to be created



To install Access Server on your Linux server, run this command:

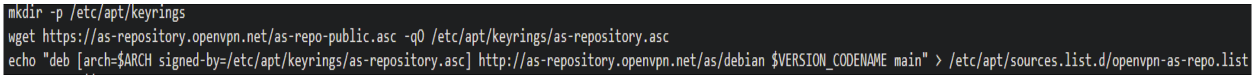
```
bash <(curl -fsS https://as-repository.openvpn.net/as/install.sh)
```

Figure 4: Command to install on Linux



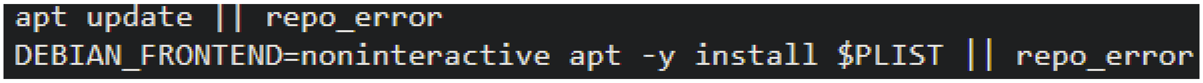
```
apt update || repo_error
DEBIAN_FRONTEND=noninteractive apt -y install ca-certificates wget net-tools gnupg || repo_error
```

Figure 5: Create and Install files in “keyrings” directory.



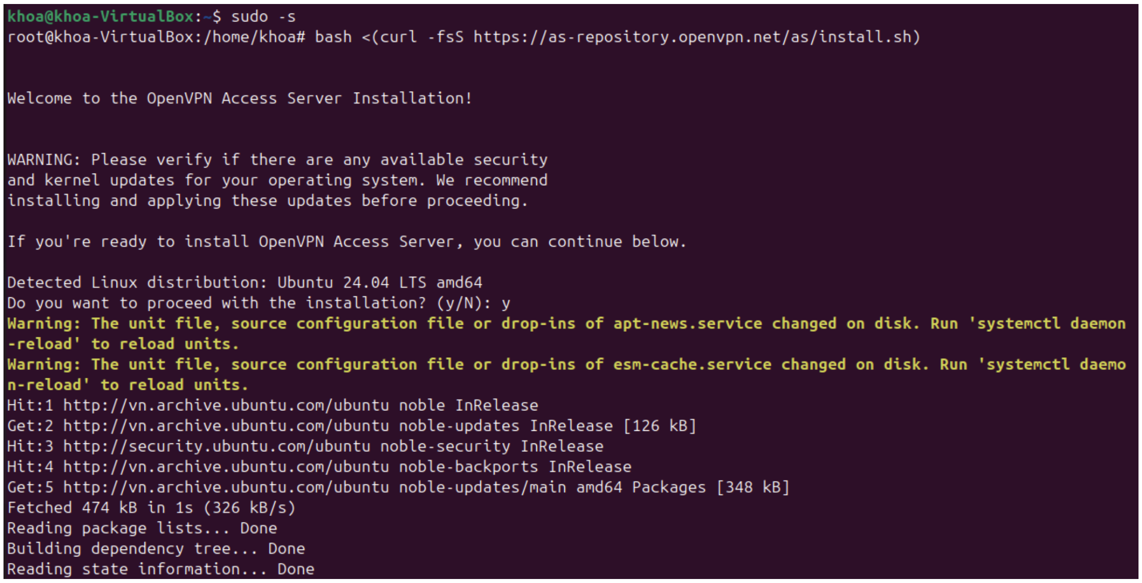
```
mkdir -p /etc/apt/keyrings
wget https://as-repository.openvpn.net/as-repo-public.asc -qO /etc/apt/keyrings/as-repository.asc
echo "deb [arch=$ARCH signed-by=/etc/apt/keyrings/as-repository.asc] http://as-repository.openvpn.net/as/debian $VERSION_CODENAME main" > /etc/apt/sources.list.d/openvpn-as-repo.list
```

Figure 6: Installing keyrings.



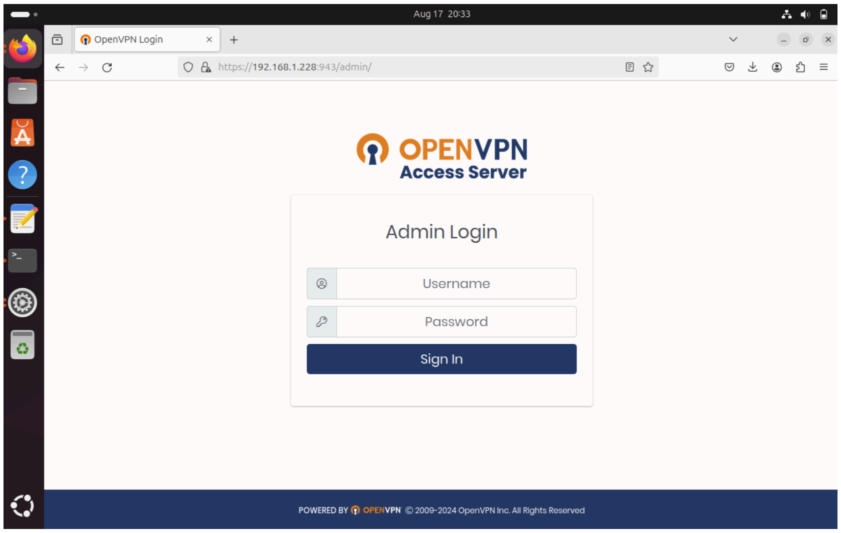
```
apt update || repo_error
DEBIAN_FRONTEND=noninteractive apt -y install $PLIST || repo_error
```

Figure 7: Installing the ca-certificates and net-tools.



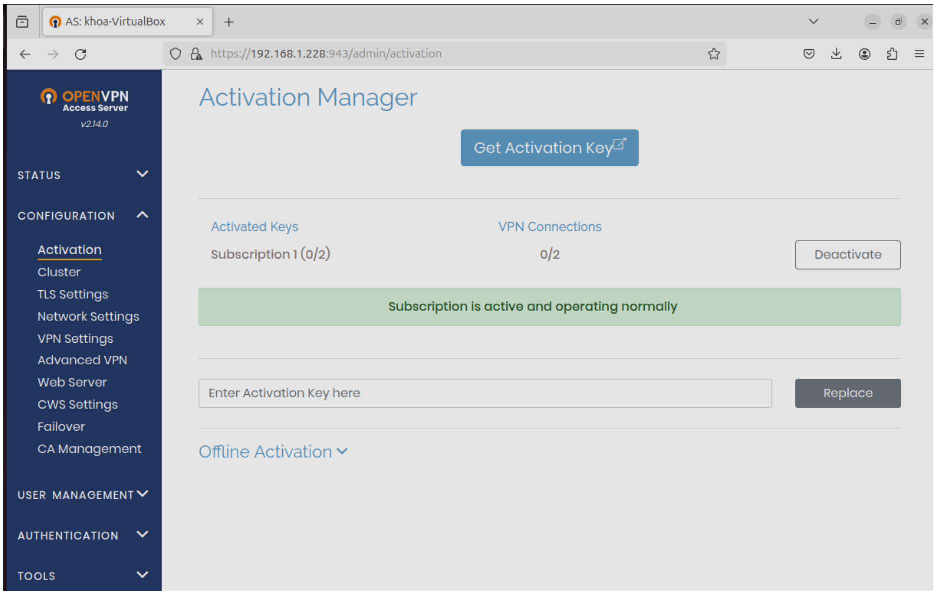
```
khoa@khoa-VirtualBox:~$ sudo -s
root@khoa-VirtualBox:/home/khoa# bash <(curl -fsS https://as-repository.openvpn.net/as/install.sh)


Welcome to the OpenVPN Access Server Installation!


WARNING: Please verify if there are any available security
and kernel updates for your operating system. We recommend
installing and applying these updates before proceeding.

If you're ready to install OpenVPN Access Server, you can continue below.

Detected Linux distribution: Ubuntu 24.04 LTS amd64
Do you want to proceed with the installation? (y/N): y
Warning: The unit file, source configuration file or drop-ins of apt-news.service changed on disk. Run 'systemctl daemon
-reload' to reload units.
Warning: The unit file, source configuration file or drop-ins of esm-cache.service changed on disk. Run 'systemctl daemo
n-reload' to reload units.
Hit:1 http://vn.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://vn.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:3 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:4 http://vn.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:5 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [348 kB]
Fetched 474 kB in 1s (326 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Figure 8: Completed installation process.



Aug 17 20:33
OpenVPN Login
https://192.168.1.228:943/admin/
OPENVPN
Access Server
Admin Login
Username
Password
Sign In
POWERED BY OPENVPN © 2009-2024 OpenVPN Inc. All Rights Reserved

Figure 10: OpenVPN Admin UI login interface.

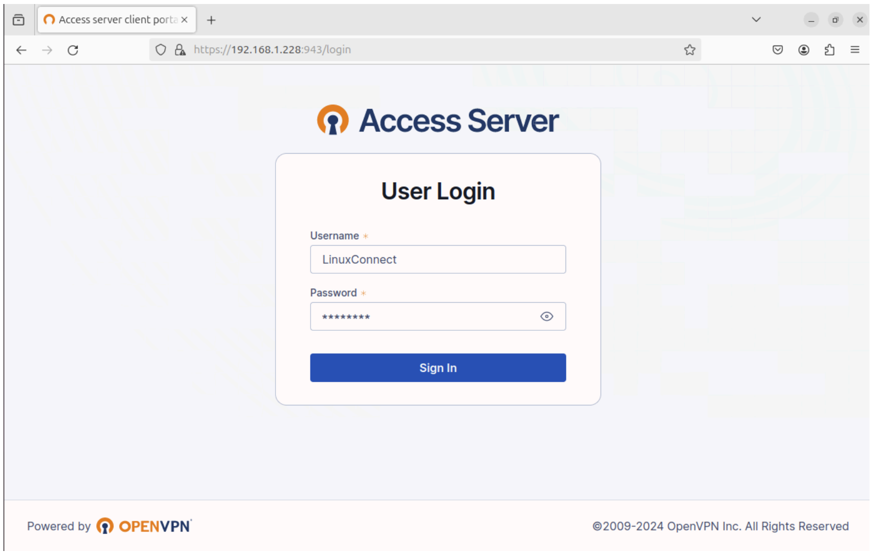


Activation Manager

Activated Keys	VPN Connections
Subscription 1 (0/2)	0/2

Subscription is active and operating normally

Figure 12: Activation page to enter the key.



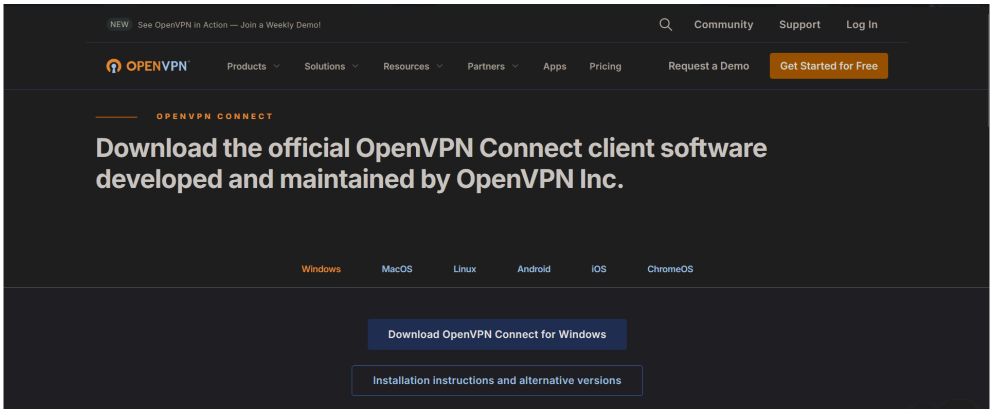
User Login

Username *
LinuxConnect

Password *
****

©2009-2024 OpenVPN Inc. All Rights Reserved

Figure 15: Client UI log in.



OPENVPN CONNECT

Download the official OpenVPN Connect client software developed and maintained by OpenVPN Inc.

Figure 20: OpenVPN Connect for Windows