Secure Virtualized Home Lab Environment

Simulating enterprise-grade cybersecurity infrastructure through hands-on virtualization.

Neer Patel

Table of Content

Introduction

This document outlines the design and implementation of a secure, multi-VM home lab environment using Oracle VirtualBox. It aims to simulate a corporate IT infrastructure with core services like Active Directory, secure VPN access, and security monitoring tools such as Nessus and Splunk. The lab provides a comprehensive platform to gain hands-on experience in network administration, cybersecurity, and system integration.

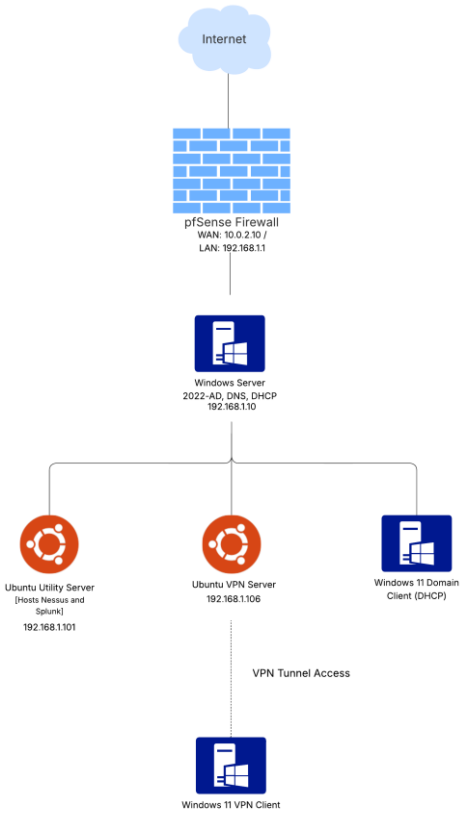
Lab Overview

The lab consists of six VMs, each serving a specific function:

- **pfSense**: Firewall and gateway
- **Windows Server 2022**: AD DS, DNS, and DHCP
- **Ubuntu Utility Server**: Hosts Nessus and Splunk
- **Ubuntu VPN Server**: Provides OpenVPN access
- **Windows 11 Domain Client**: Joins the AD domain
- **Windows 11 VPN Client**: Connects remotely via VPN

These machines are interconnected to emulate a functional and secure enterprise network.

Network Topology Diagram



Explanation of the Diagram

- **Internet**: Represents the external network.
- **VirtualBox NAT**: Simulates the internet on the host system.
- **pfSense Firewall**: Secures and segments the internal lab environment.
- **Windows Server 2022**: Provides core infrastructure services.
- **Ubuntu Utility Server**: Hosts Nessus and Splunk.
- **Ubuntu VPN Server**: Offers remote VPN access.
- **Windows 11 Domain Client**: Internal domain-joined machine.
- **Windows 11 VPN Client**: Connects remotely via VPN and receives internal IP.

Component Summary Table

Component	Role/Function	IP Address	Hostname	Key Services
pfSense Firewall	Firewall and gateway	WAN: 10.0.2.10	pfSense	NAT, Routing
Windows Server 2022	AD, DNS, DHCP	192.168.1.10	Winserver 22	AD DS, DNS, DHCP
Windows 11 Domain PC	Internal domain client	DHCP-assigned	win11-domain	AD Authentication
Windows 11 VPN Client	Remote access client via VPN	VPN-assigned	win11-vpn	Secure Remote Access
Ubuntu Utility Server	Security monitoring	192.168.1.101	utility-server	Nessus, Splunk
Ubuntu VPN Server	VPN endpoint	192.168.1.106	vpn-server	OpenVPN

Virtual Environment Setup Details

6.1. pfSense Firewall

What is it: pfSense is an open-source firewall and router solution that manages network traffic and security.

Why it's necessary: It acts as the primary gateway in the lab, securing internal VMs from external threats and managing LAN/WAN segmentation.

- **WAN IP**: 10.0.2.10/24
- **LAN IP**: 192.168.1.1/24

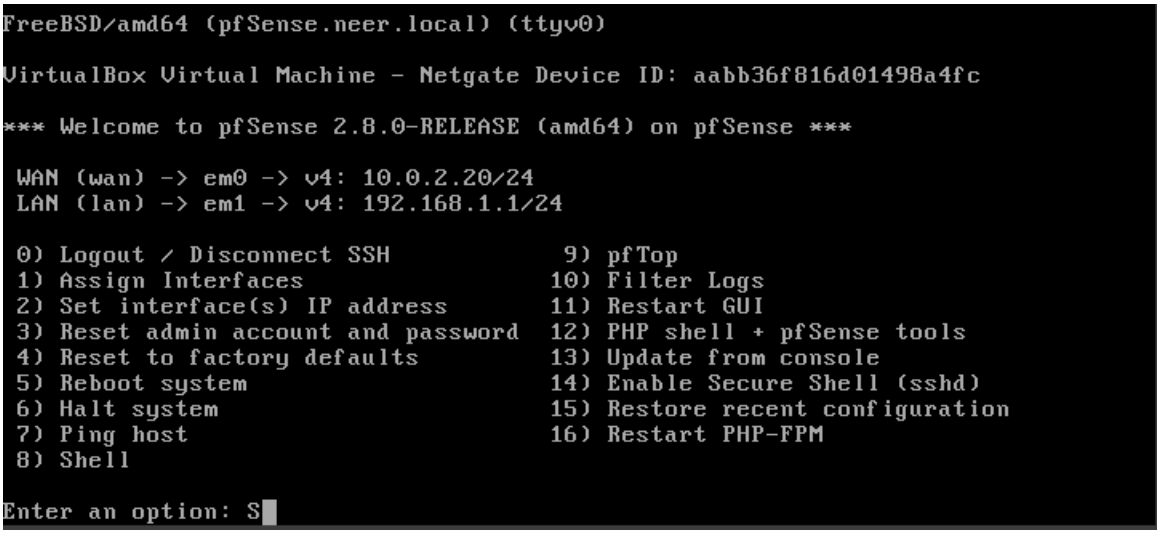


Figure 6.1: Pfsense configuration

6.2. Windows Server 2022 (Winserver22)

What is it: A Microsoft server OS that provides core infrastructure services like Active Directory, DNS, and DHCP.

Why it's necessary: It manages user authentication, IP assignment, and internal name resolution for all domain-connected machines.

- **IP Address**: 192.168.1.10
- **Domain**: neer.local

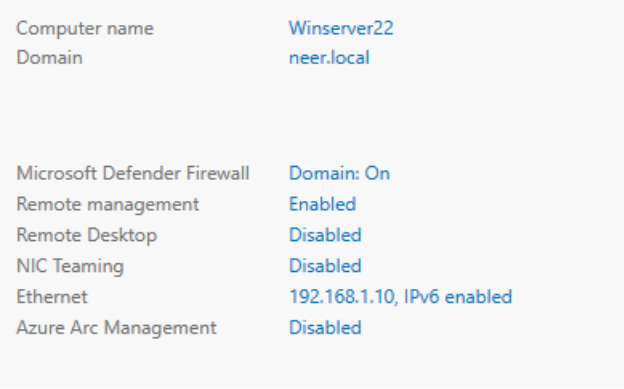


Figure 6.2.1: Winserver22 and domain.

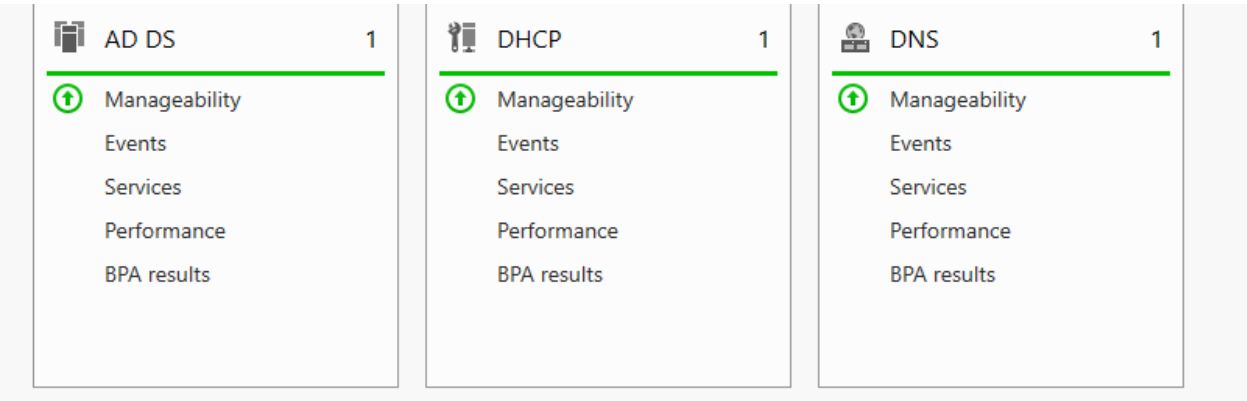


Figure 6.2.2: AD, DHCP, DNS install and configured

6.3. Windows 11 (Domain Client)

What is it: A Windows 11 VM joined to the neer.local domain for user login and group policy testing.

Why it's necessary: It simulates a corporate user system, allowing for testing of AD authentication, GPOs, and user access.

- **IP Address**: DHCP assigned

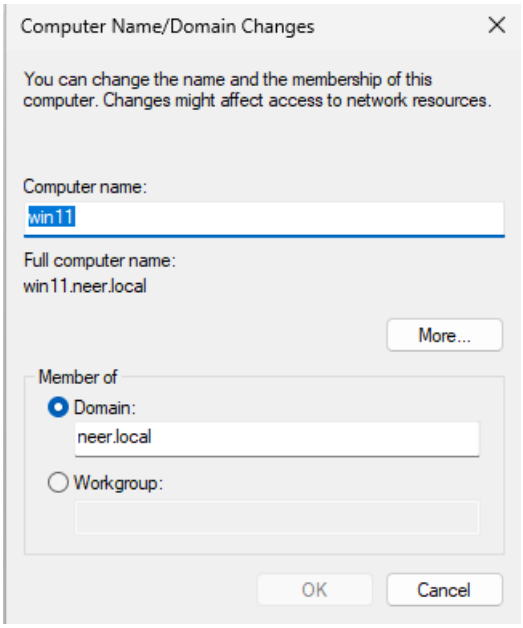


Figure 6.3.1: Domain configured in win 11.

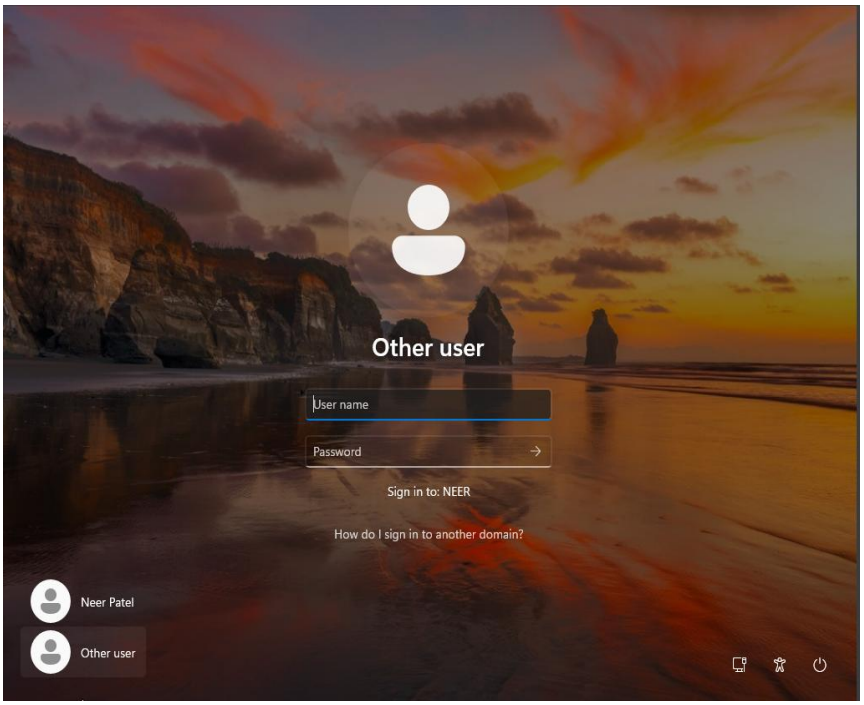


Figure 6.3.2: After domain configured login using Ad users.

6.4. Ubuntu Server (Utility Server)

What is it: A Linux VM running Nessus for vulnerability scanning and Splunk for log analysis.

Why it's necessary: It enables real-time monitoring, threat detection, and security analysis across the lab environment.

- **IP Address**: 192.168.1.101
- **Tools**: Nessus, Splunk

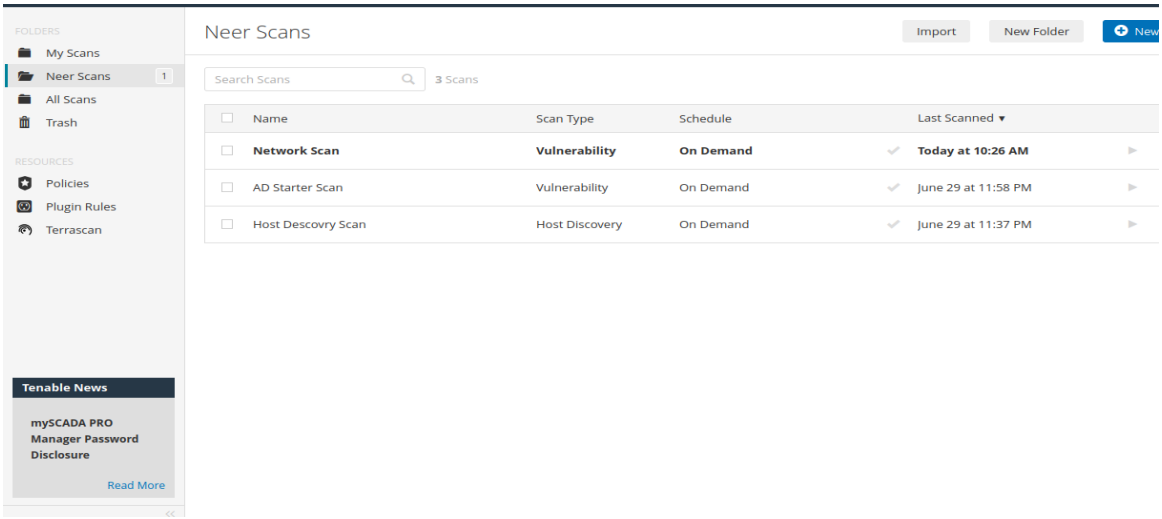


Figure 6.4.1: Nessus setup and perform different scans.

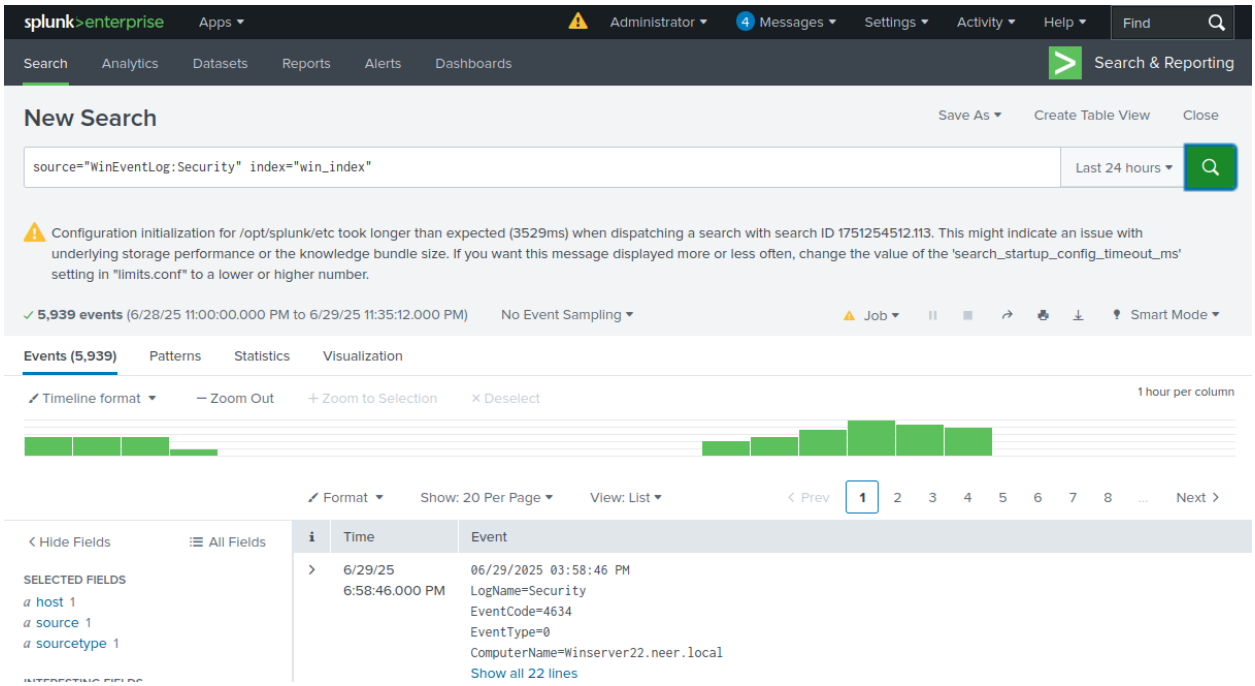


Figure 6.4.2: Splunk enterprise setup and get logs of winserver22.

6.5. Ubuntu Server (VPN Server)

What is it: A Linux-based OpenVPN server used to provide secure remote access into the lab network.

Why it's necessary: It allows the VPN Client VM to connect securely from outside, simulating remote access in enterprise setups.

- **IP Address**: 192.168.1.106

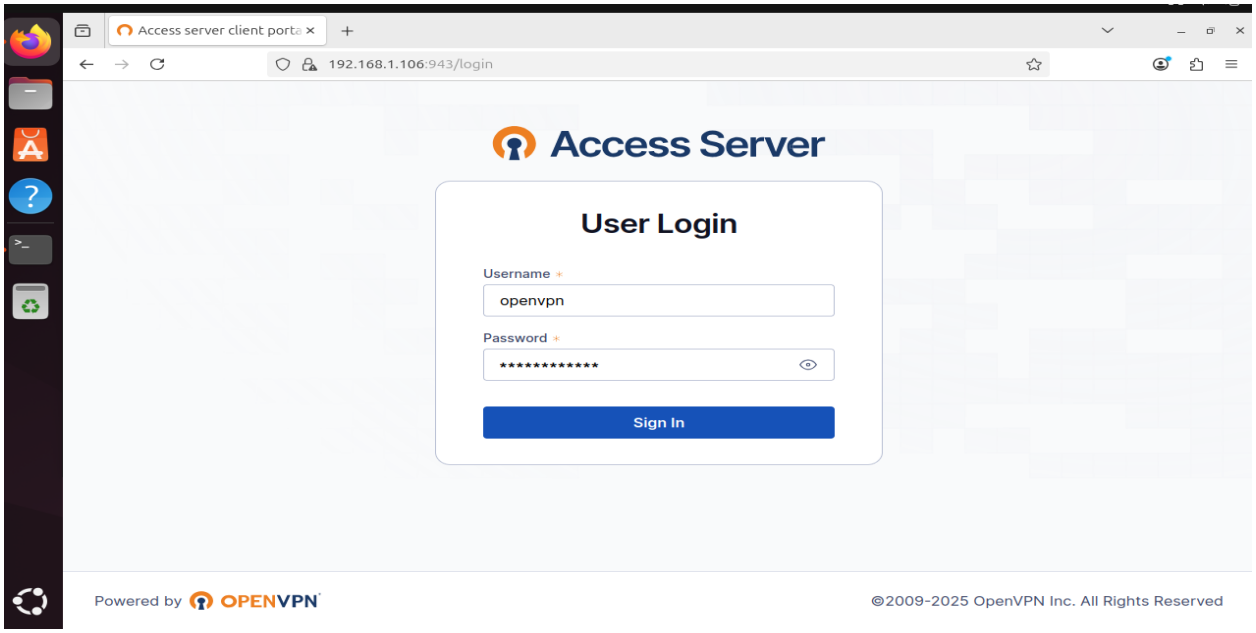


Figure 6.5.1: OpenVPN server deploy and setup successfully.

6.6. Windows 11 (VPN Client)

What is it: A Windows 11 VM configured to connect securely to the lab network via VPN.

Why it's necessary: It simulates remote access, testing encrypted connectivity and external access to internal resources.

- **IP Address**: Assigned via VPN (192.168.1.x)

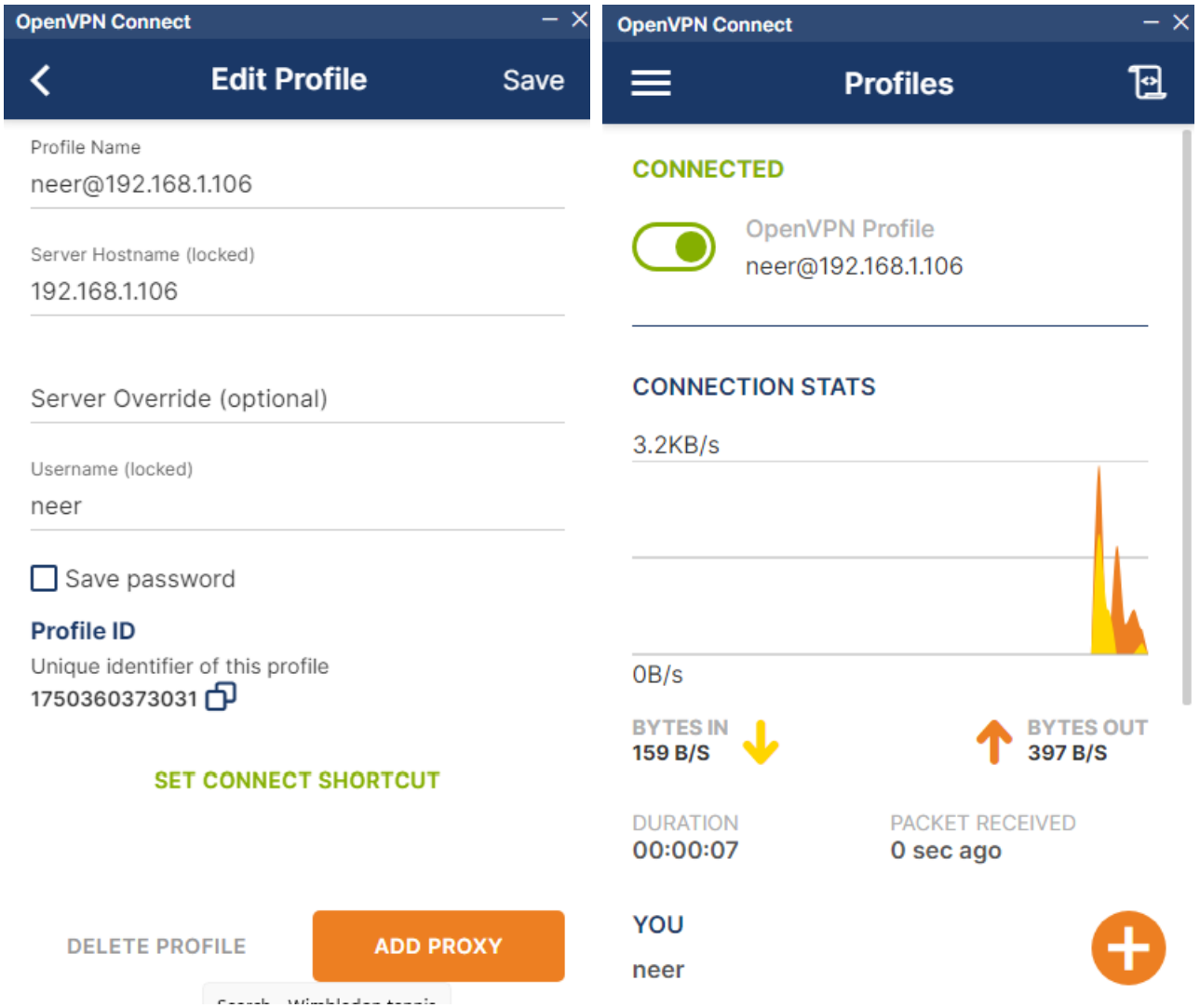


Figure 6.6.1: OpenVPN client setup and connected.

Key Features and Technologies Used

- **pfSense**: Enterprise-grade firewall and routing.
- **AD DS**: Centralized identity and access control.
- **OpenVPN**: Encrypted remote access.
- **DHCP & DNS**: Automated IP and name resolution.

- **Nessus**: Vulnerability assessment.
- **Splunk**: SIEM log aggregation and alerting.
- **VirtualBox**: Isolated multi-VM testing environment.

Learning Outcomes

- Designed a segmented network with secure firewall rules.
- Deployed AD with real-world features like DNS and DHCP.
- Established secure VPN connectivity.
- Performed vulnerability scanning and SIEM configuration.
- Practiced cross-platform system administration.

Conclusion

This home lab replicates a real-world IT infrastructure, offering a sandbox to learn and practice security, administration, and network design. It's a valuable tool for certification prep, interviews, and hands-on upskilling.

Future Enhancements

- Add SNORT/Suricata for IDS/IPS.
- Join Linux clients to AD domain.
- Simulate phishing and incident response.
- Automate SIEM alerting.
- Schedule Nessus scans and reporting.

References

- https://www.microsoft.com/en-us/evalcenter/download-windows-server-2022 (Server 2022 download)
- https://www.youtube.com/watch?v=I4pG29mT-oI&list=PLErQ2qAXz3rp1rqHIdSx8QmW3n7Zqi9UL&index=1 (DHCP configuration)
- https://www.youtube.com/watch?v=FDhndiAEyxs&t=16s (AD DS configuration)
- https://www.youtube.com/watch?v=OtdOEiTozUE&list=PLErQ2qAXz3rp1rqHIdSx8QmW3n7Zqi9UL&index=2 (DNS configuration)
- https://www.youtube.com/watch?v=K7thNKB7v5c&list=PLErQ2qAXz3rp1rqHIdSx8QmW3n7Zqi9UL&index=4 (Join windows 11 pc with domin server)
- https://www.youtube.com/watch?v=x87gbgQD4eg (Nessus setup)
- https://www.youtube.com/watch?v=wd4BLsJThQY (Splunk Universal Forwarder setup)

- https://www.youtube.com/watch?v=IvpUvqYq4cE (Splunk setup)
- https://www.youtube.com/watch?v=TW4I7X6G6Ak&list=PLYoFyx6U4T4DLZbm9btYzjv69jAiy72ol (Splunk setup)
- https://davidf.io/2024/07/16/setup-ubuntu-server-as-vpn-server-on-active-directory-via-ldap/ (VPN server setup)
- https://mattglass-it.com/ubuntu-domain-join/ (Join Ubuntu machine with AD)