

NETWORK LONDON - SWANSEA PART2

**Implementing:
ROUTING
DHCP
Active Directory
Secure VPN**

David Lopez Rodriguez
id: 2336542



David Lopez Rodriguez id:2336542

Networking operating systems and services ACA5023LON

Table of contents

1. Introduction	1
2. Network Topology and IP Addressing.....	1
Screenshots of a successful connection between clients using static IP:	1
3. Routing and Inter-Site Connectivity	4
4. Firewall Configuration and Troubleshooting.....	4
Screenshots of PING with and without firewall rule:	4
5. Active Directory, DNS and DHCP Services	5
Screenshots of Active Directory setup:	5
Screenshots of DHCP and Relay setup:	6
6. VPN Configuration (Partial Implementation)	6
VPN Partial setup:	6
7. Conclusion	6

Enterprise Network Design and Implementation

1. Introduction

This report documents the implementation of a multi-site enterprise network connecting two locations, Swansea and London. The objective was to configure core network infrastructure services, including IP addressing, routing, Active Directory, DNS, DHCP, and secure connectivity, following enterprise networking best practices.

2. Network Topology and IP Addressing

Two local area networks were configured:

SwanseaLAN: 192.168.1.0/24

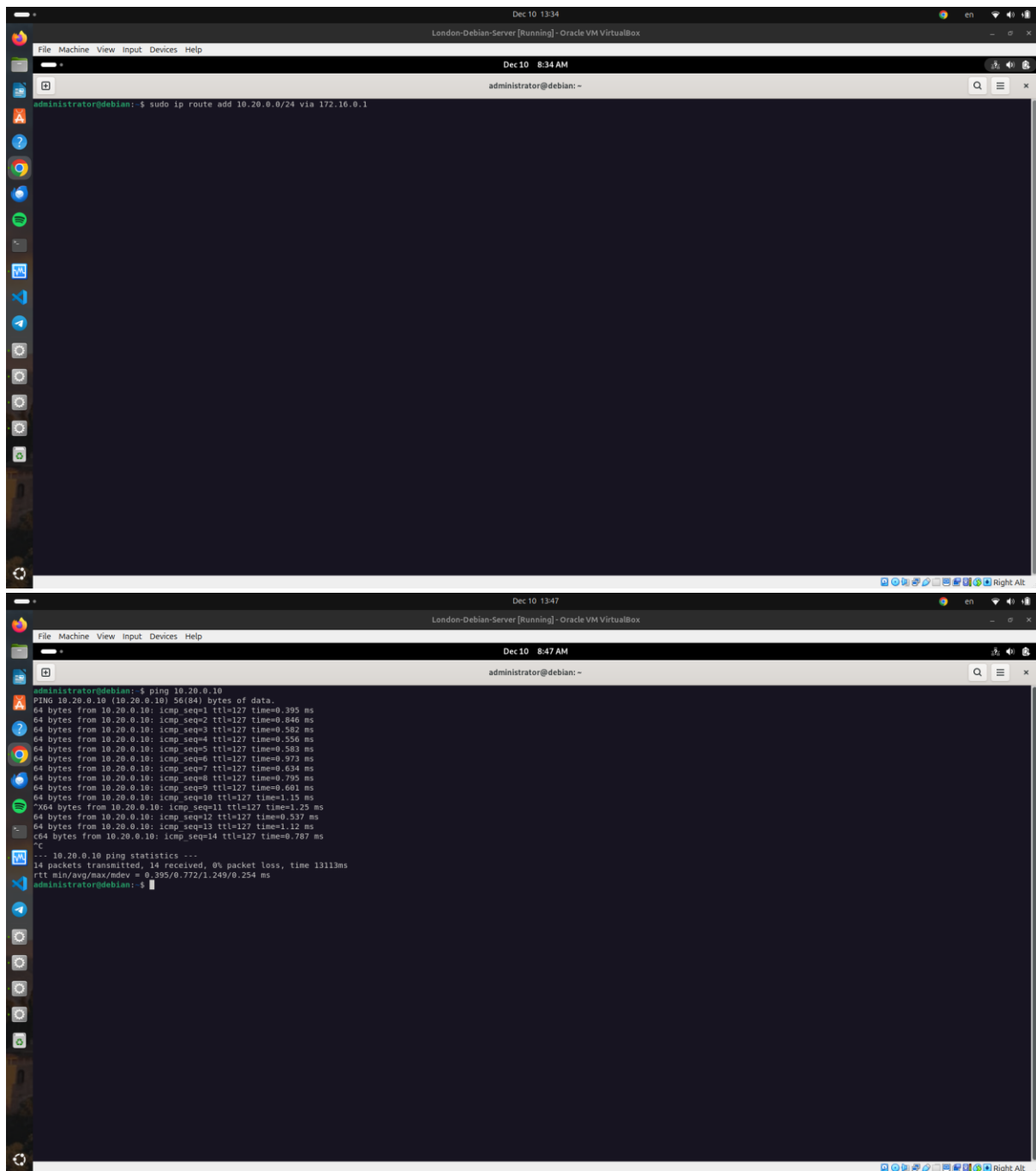
LondonLAN: 192.168.2.0/24

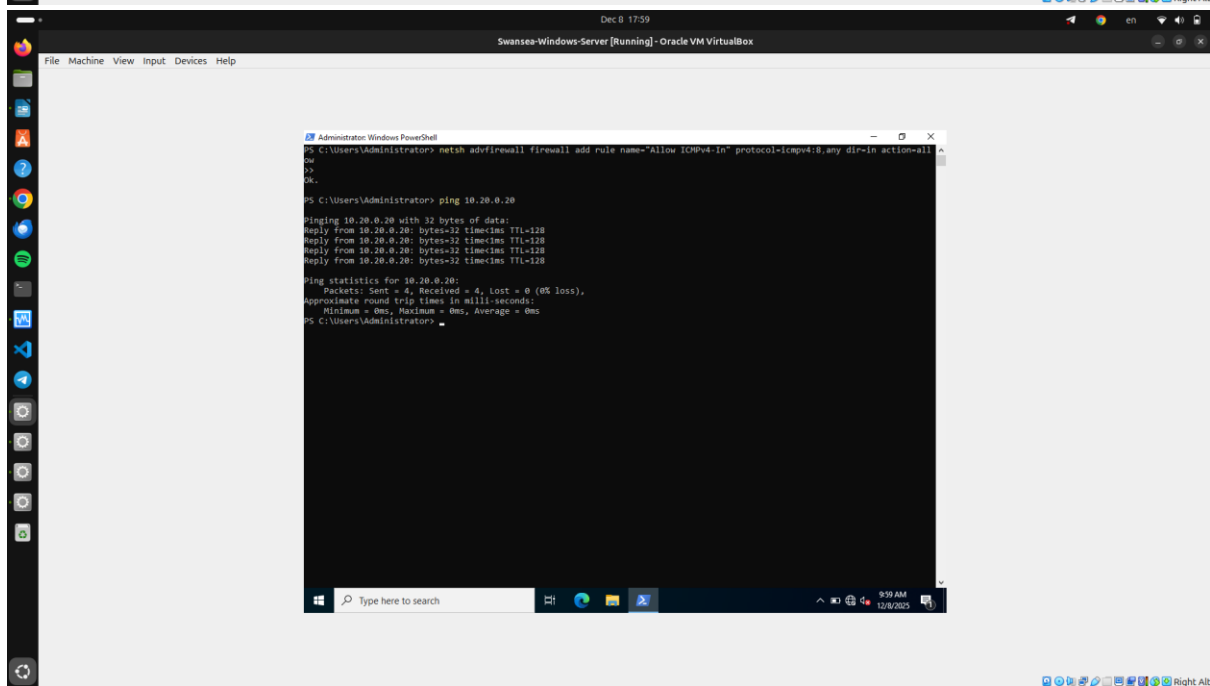
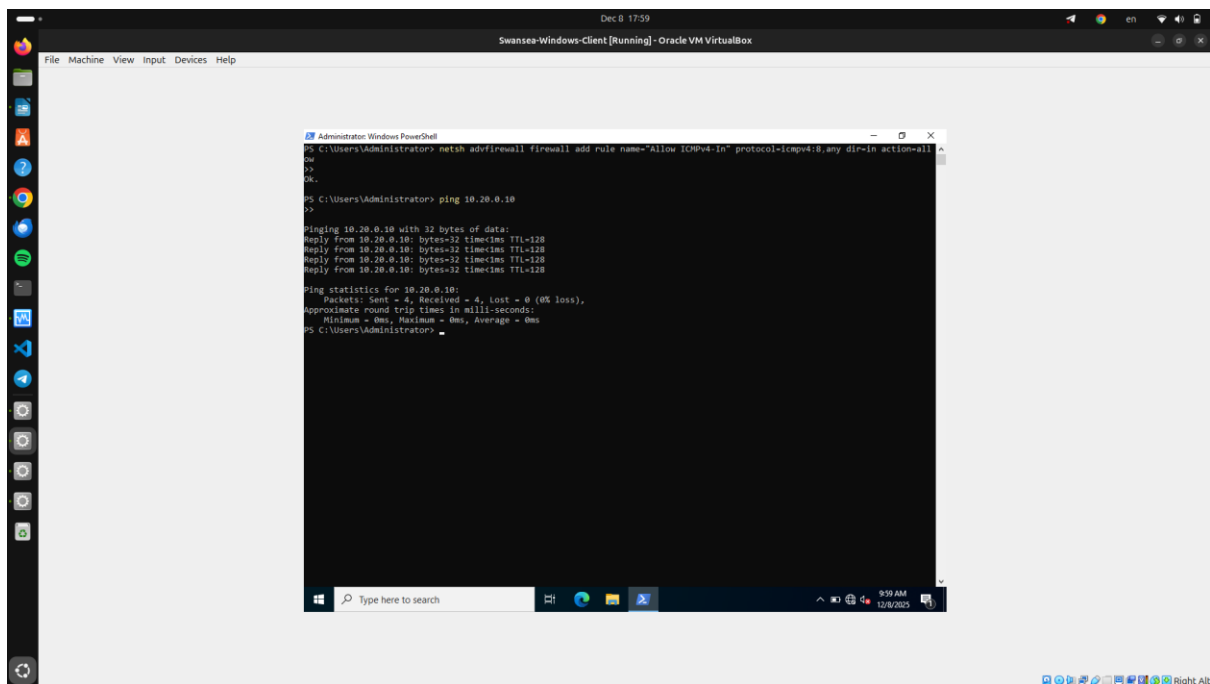
Both sites are interconnected via a dedicated point-to-point **Interlink network (172.16.0.0/30)**.

Device	Location	IP Address
S-DC (Windows Server)	Swansea	192.168.1.1
ClientS1	Swansea	192.168.1.10
L-CD (Debian Server)	London	192.168.2.1
ClientL1	London	192.168.2.10
Interlink	WAN	172.16.0.1 / 172.16.0.2

Static IP addressing was applied to servers, while DHCP was later introduced for automated client configuration.

Screenshots of a successful connection between clients using static IP:





3. Routing and Inter-Site Connectivity

Routing between the two sites was achieved using:

RRAS (LAN Routing) on the Windows Server

IP forwarding enabled on the Debian Server

Static routes configured on both systems

Connectivity was verified using ICMP testing between:

Clients and servers within each LAN

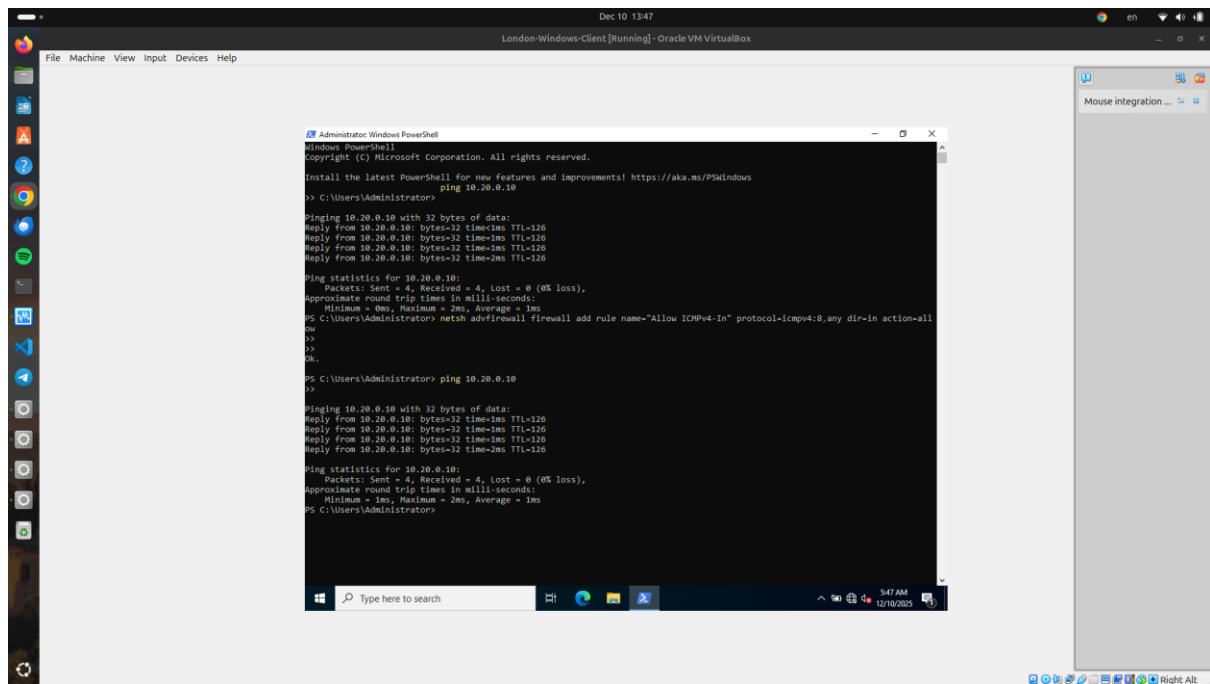
Servers across the Interlink network

Clients across sites

4. Firewall Configuration and Troubleshooting

Testing found that default firewall policies blocked ICMP. Inbound firewall rules were configured for the server and clients for specific ICMP rules to allow troubleshooting. Network profiles were set to Private.

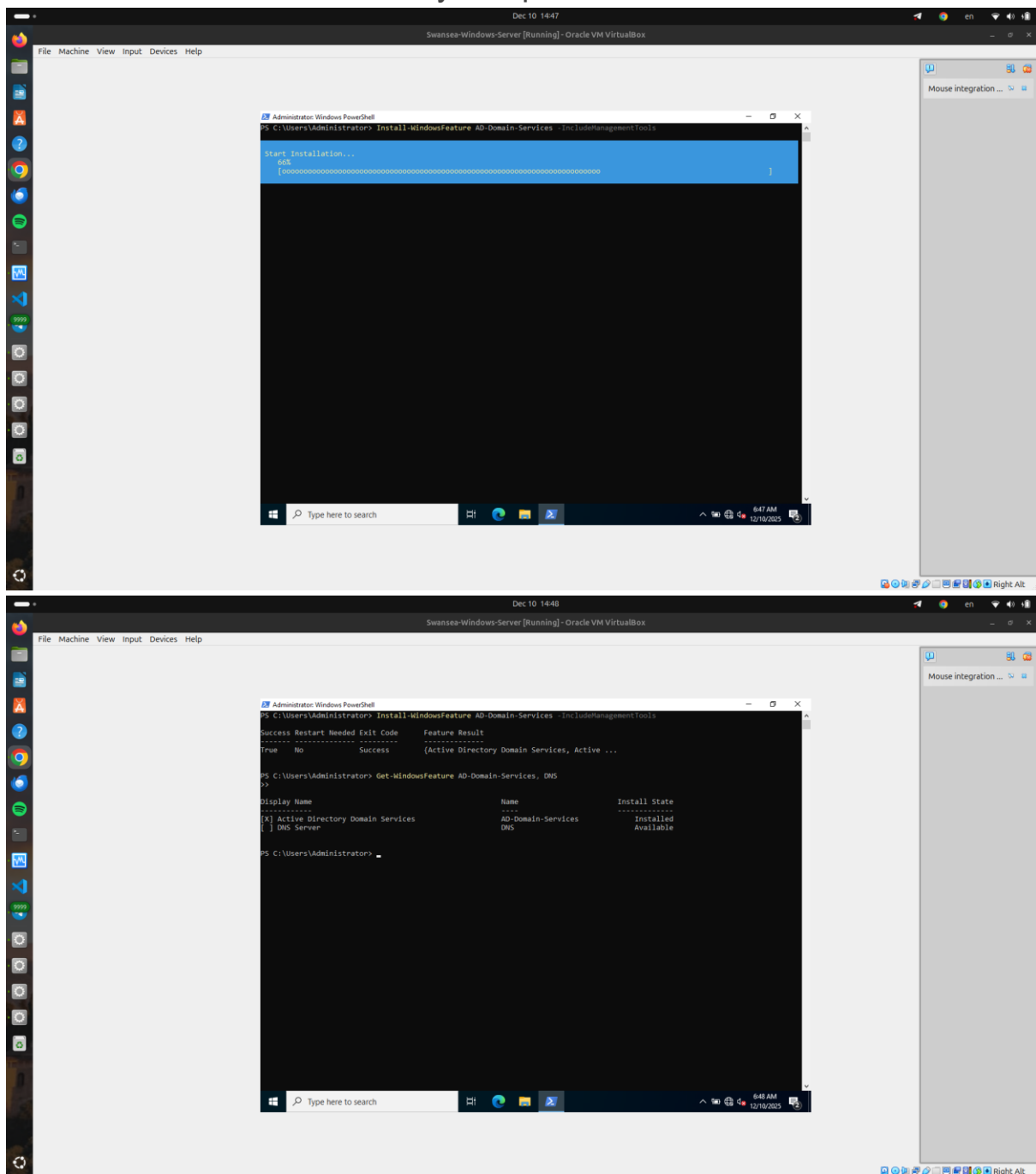
Screenshots of PING with and without firewall rule:

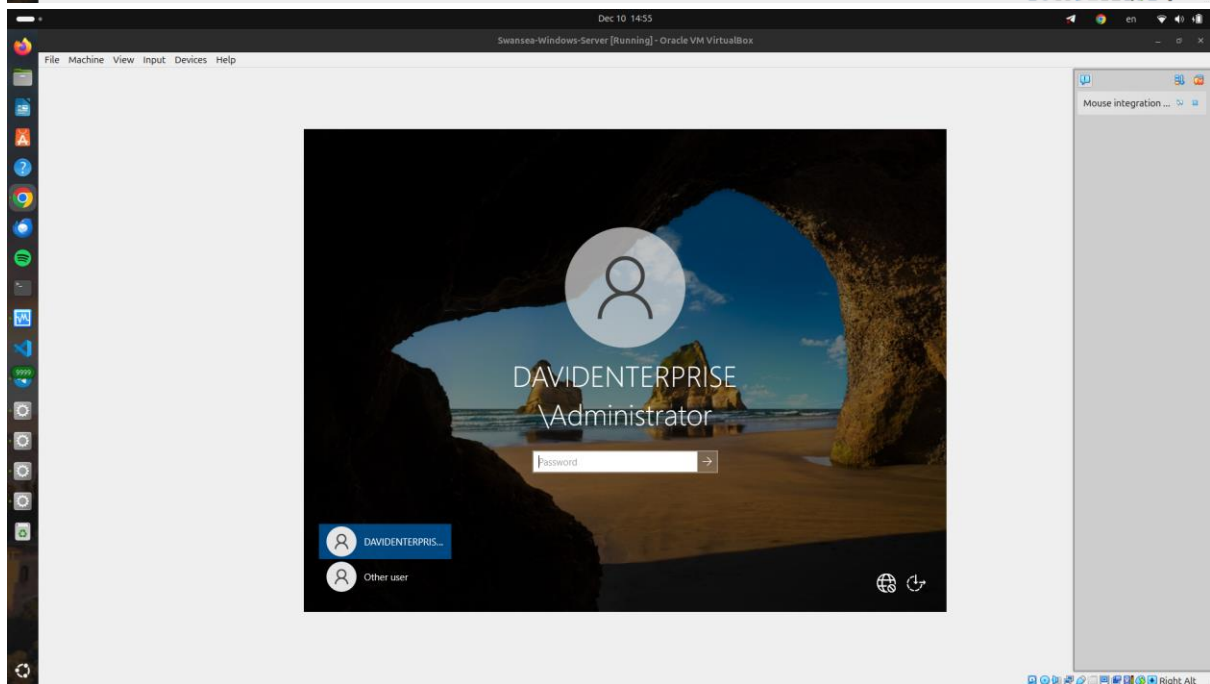
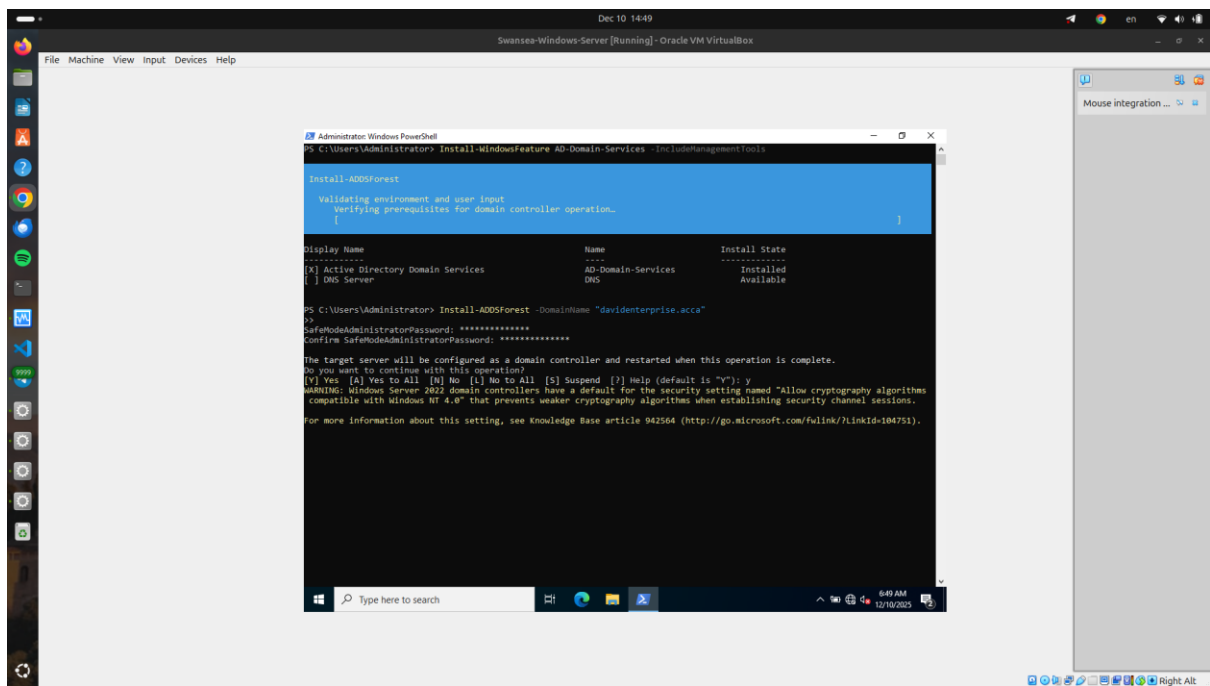


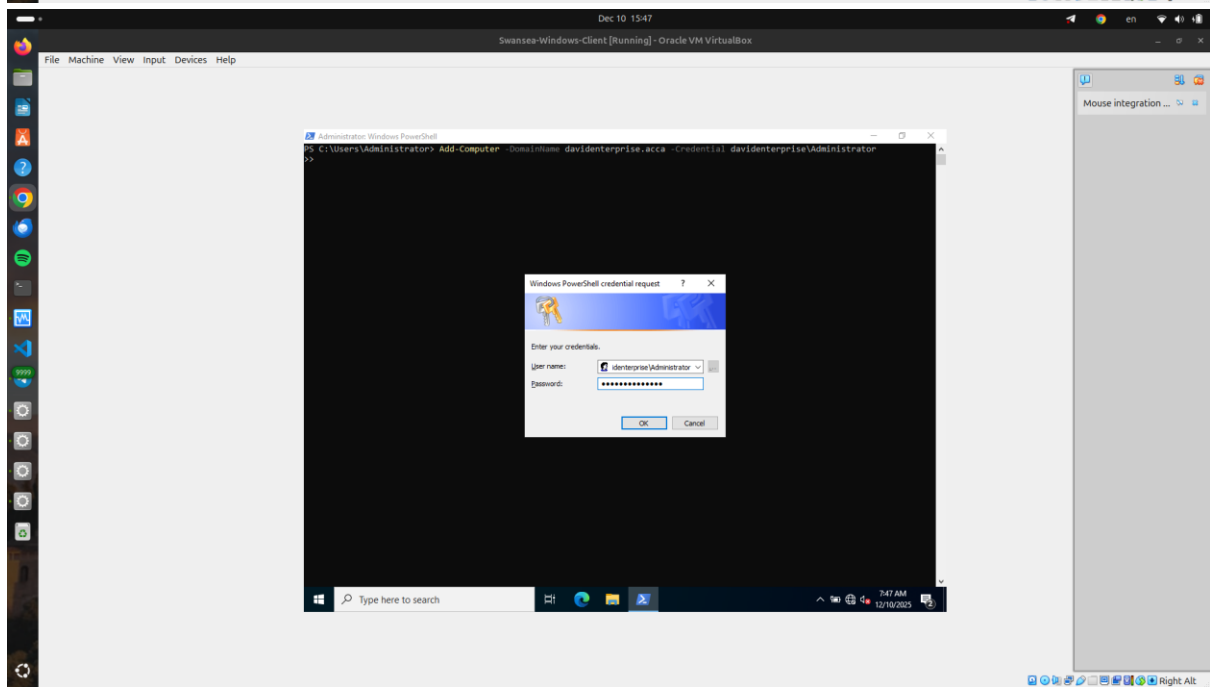
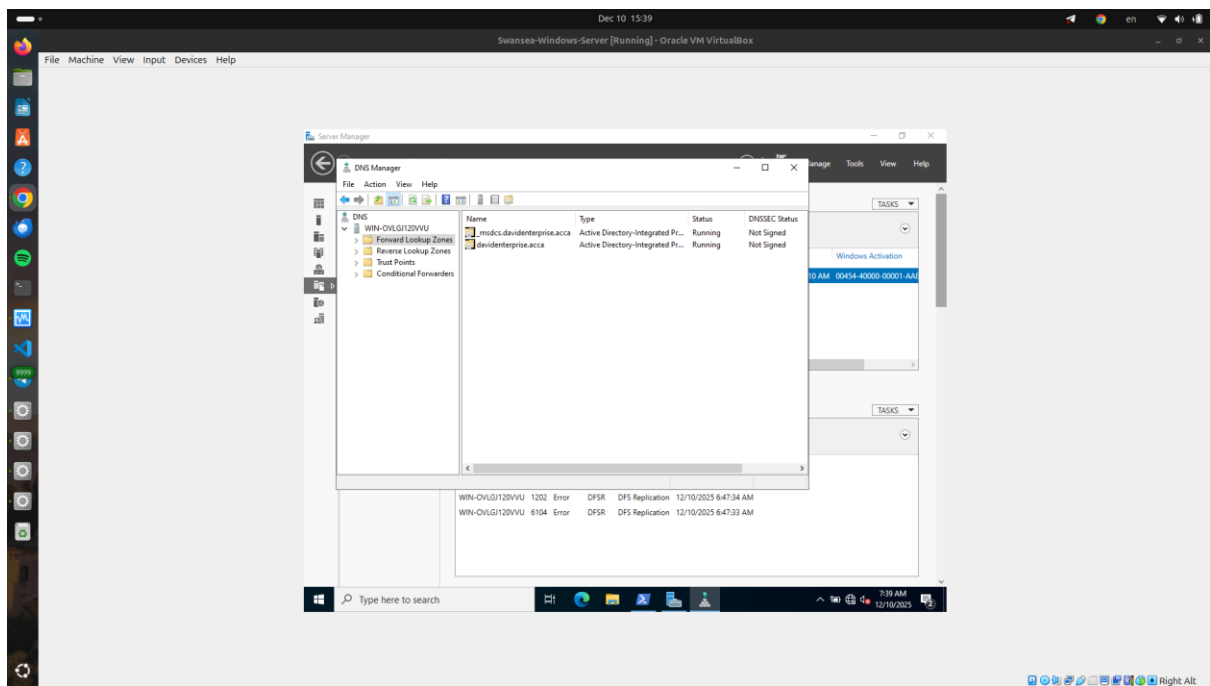
5. Active Directory, DNS and DHCP Services

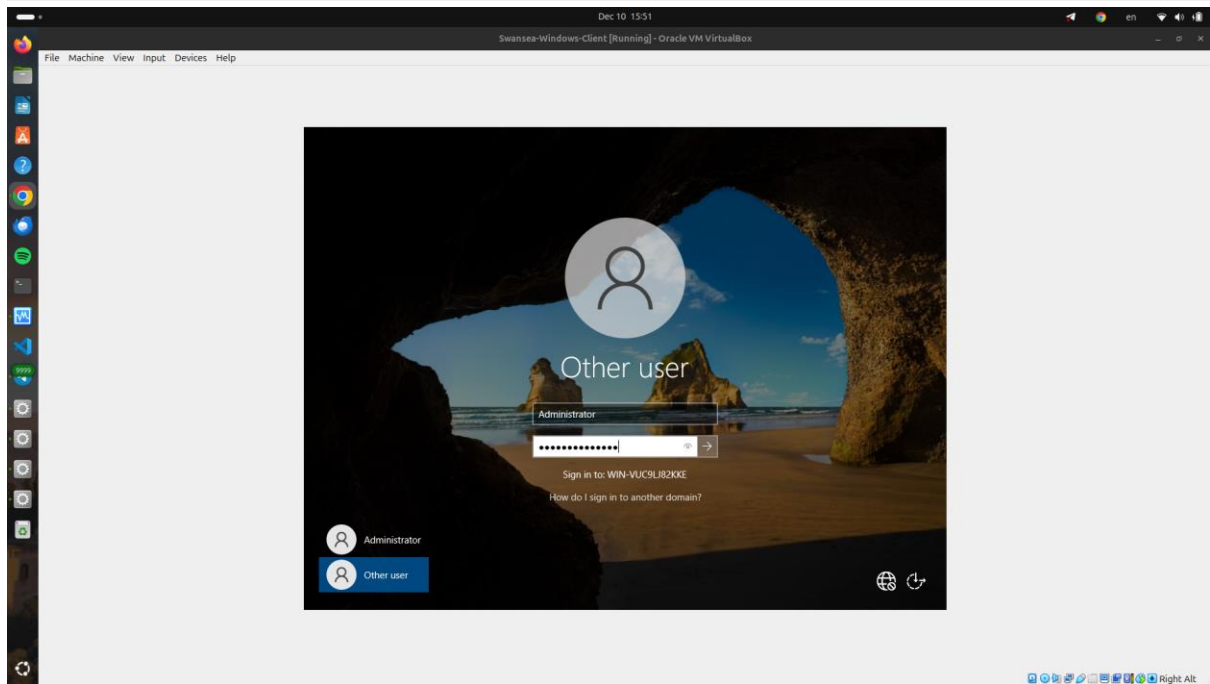
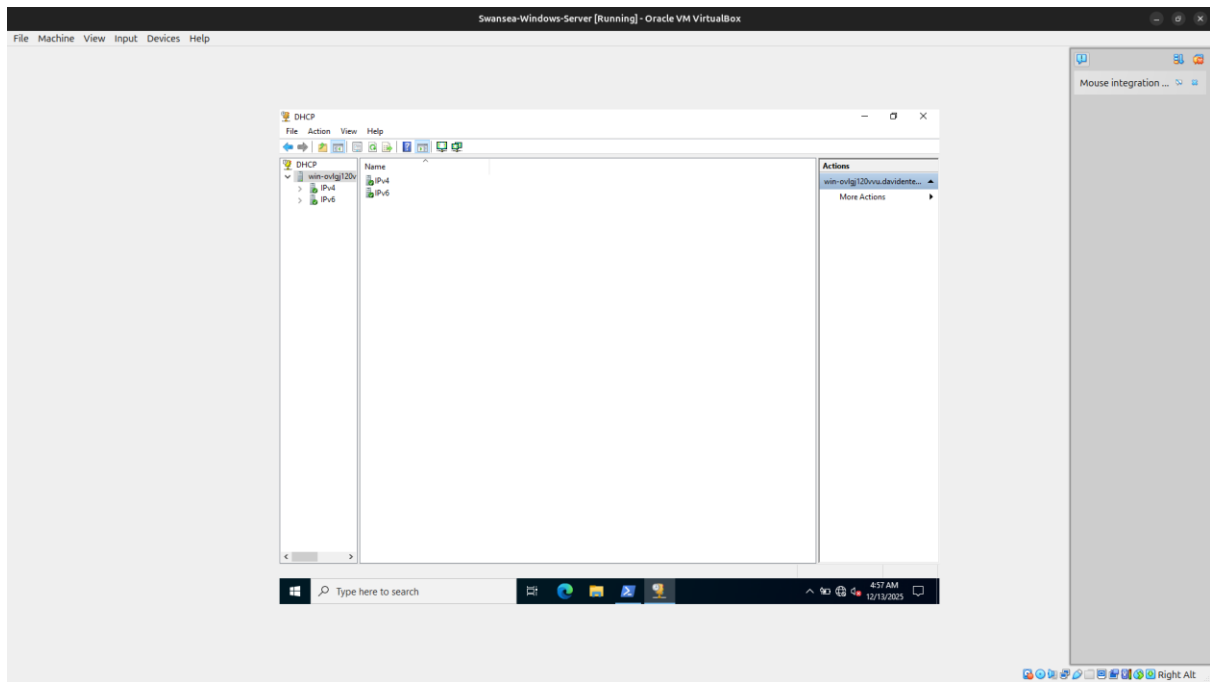
The Active Directory domain (davidenterprise) was installed on the Swansea server. The DNS services were installed and integrated with Active Directory which provides name resolution between the two sites. Both clients were joined to the domain and domain-based authentication worked at login. DHCP services was configured to allow for dynamic allocation of IP addresses to clients for ease of management and to provide a consistent enterprise network configuration.

Screenshots of Active Directory setup:

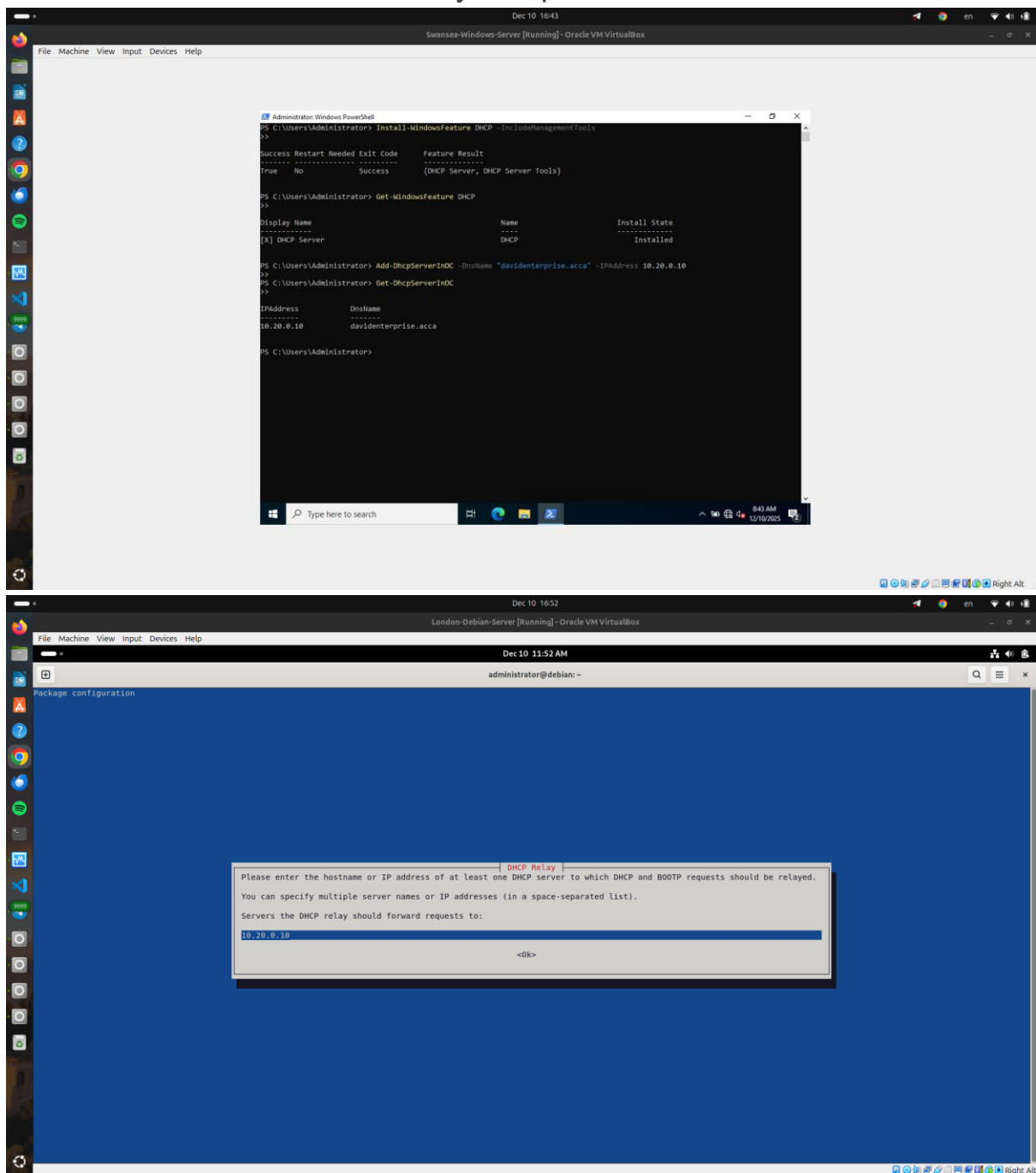








Screenshots of DHCP and Relay setup:



```
Dec 10 16:53
London-Debian-Server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Dec 10 11:53 AM
administrator@debian: ~$

sudo apt install isc-dhcp-relay -y
[sudo] password for administrator:
Hit:1 http://security.debian.org/debian-security trixie-security InRelease
Hit:2 http://deb.debian.org/debian trixie InRelease
Hit:3 http://deb.debian.org/debian trixie-updates InRelease
7 packages can be upgraded. Run 'apt list --upgradable' to see them.
Installing:
isc-dhcp-relay
Installing dependencies:
isc-dhcp-common
Summary:
Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 7
Download size: 0 B / 1,289 kB
Space needed: 3,086 kB / 13.6 GB available

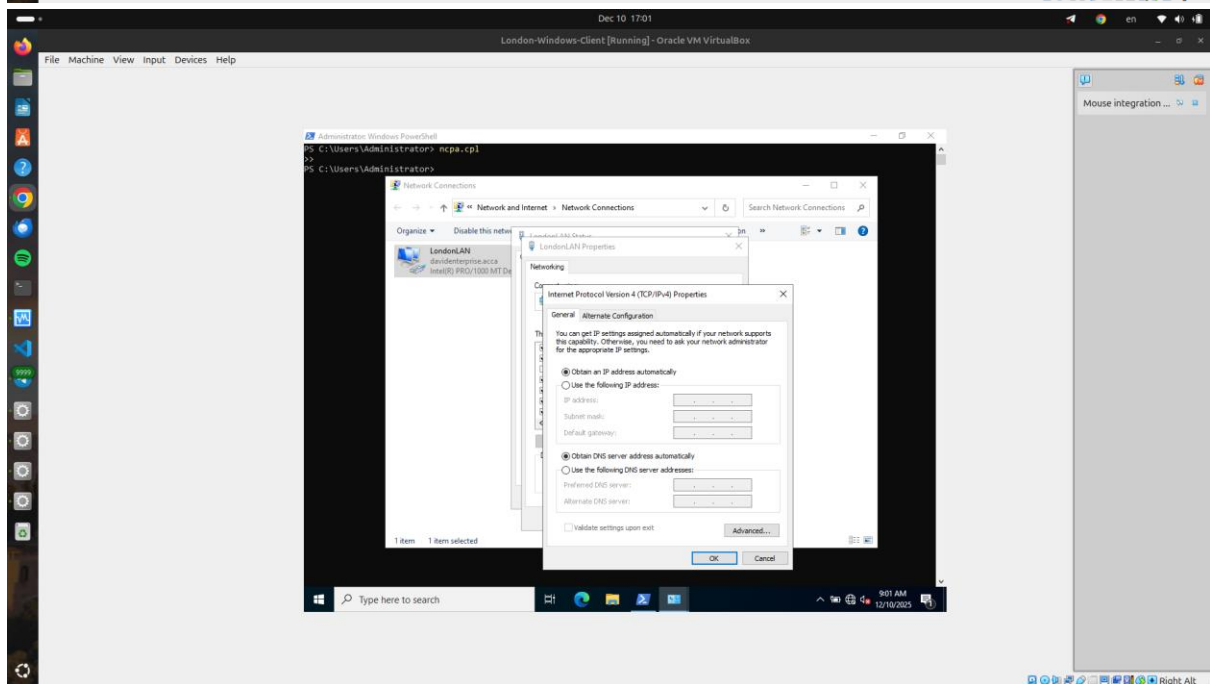
Preconfiguring packages ...
Selecting previously unselected package isc-dhcp-common.
(Reading database ... 135356 files and directories currently installed.)
Preparing to unpack .../isc-dhcp-common_4.4.3-P1-8_amd64.deb ...
Unpacking isc-dhcp-common (4.4.3-P1-8) ...
Selecting previously unselected package isc-dhcp-relay.
Preparing to unpack .../isc-dhcp-relay_4.4.3-P1-8_amd64.deb ...
Unpacking isc-dhcp-relay (4.4.3-P1-8) ...
Setting up isc-dhcp-relay (4.4.3-P1-8) ...
Generating /etc/default/isc-dhcp-relay...
Setting up isc-dhcp-common (4.4.3-P1-8) ...
Processing triggers for man-db (2.13.1-1) ...
administrator@debian:~$ sudo nano /etc/default/isc-dhcp-relay
administrator@debian:~$ cat nano /etc/default/isc-dhcp-relay
cat: nano: No such file or directory
# Defaults for isc-dhcp-relay initscript
# sourced by /etc/init.d/isc-dhcp-relay
# installed at /etc/default/isc-dhcp-relay by the maintainer scripts

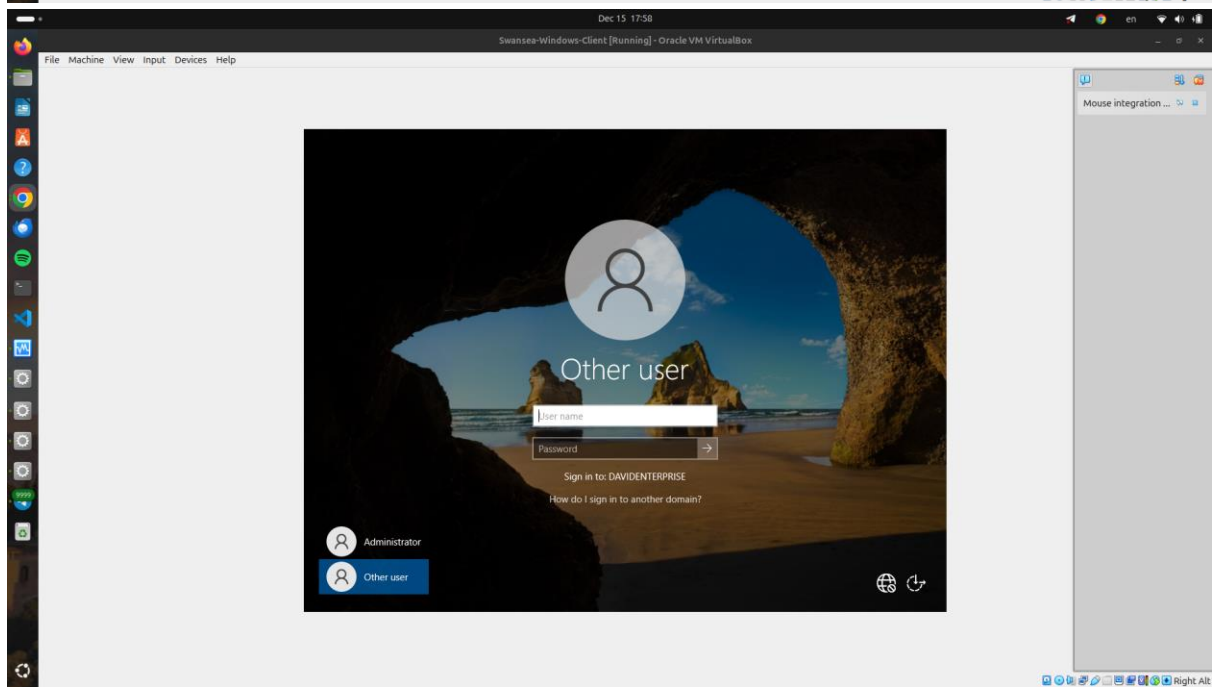
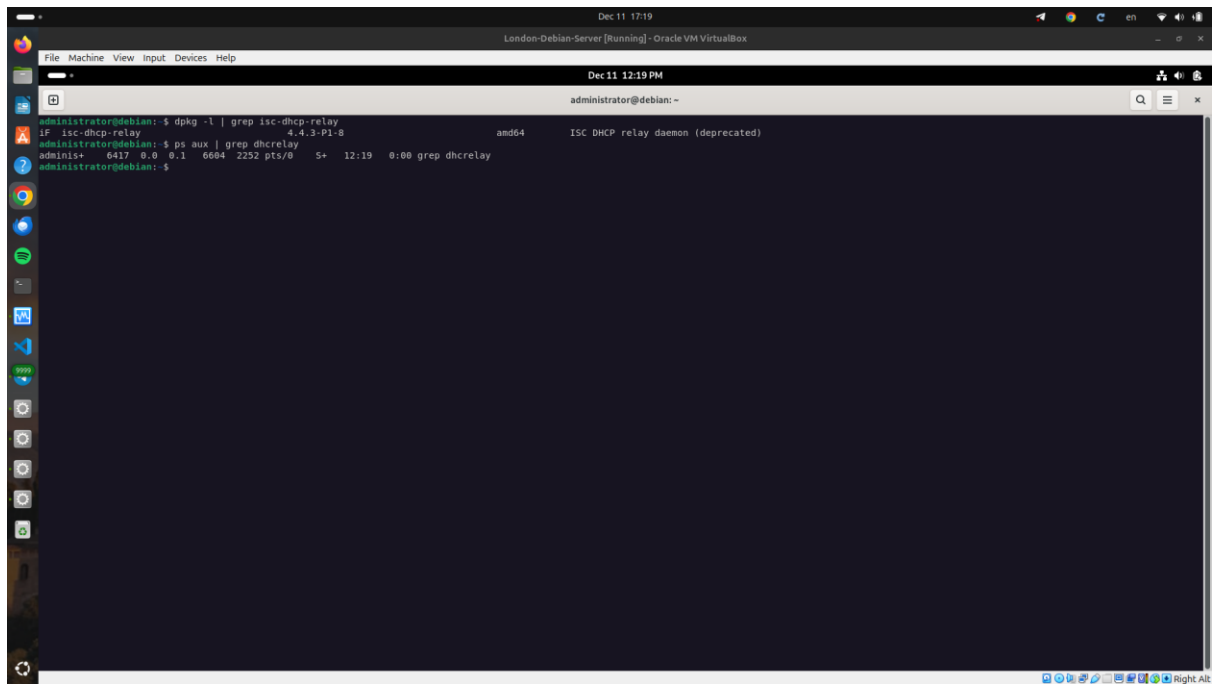
#
# This is a POSIX shell fragment

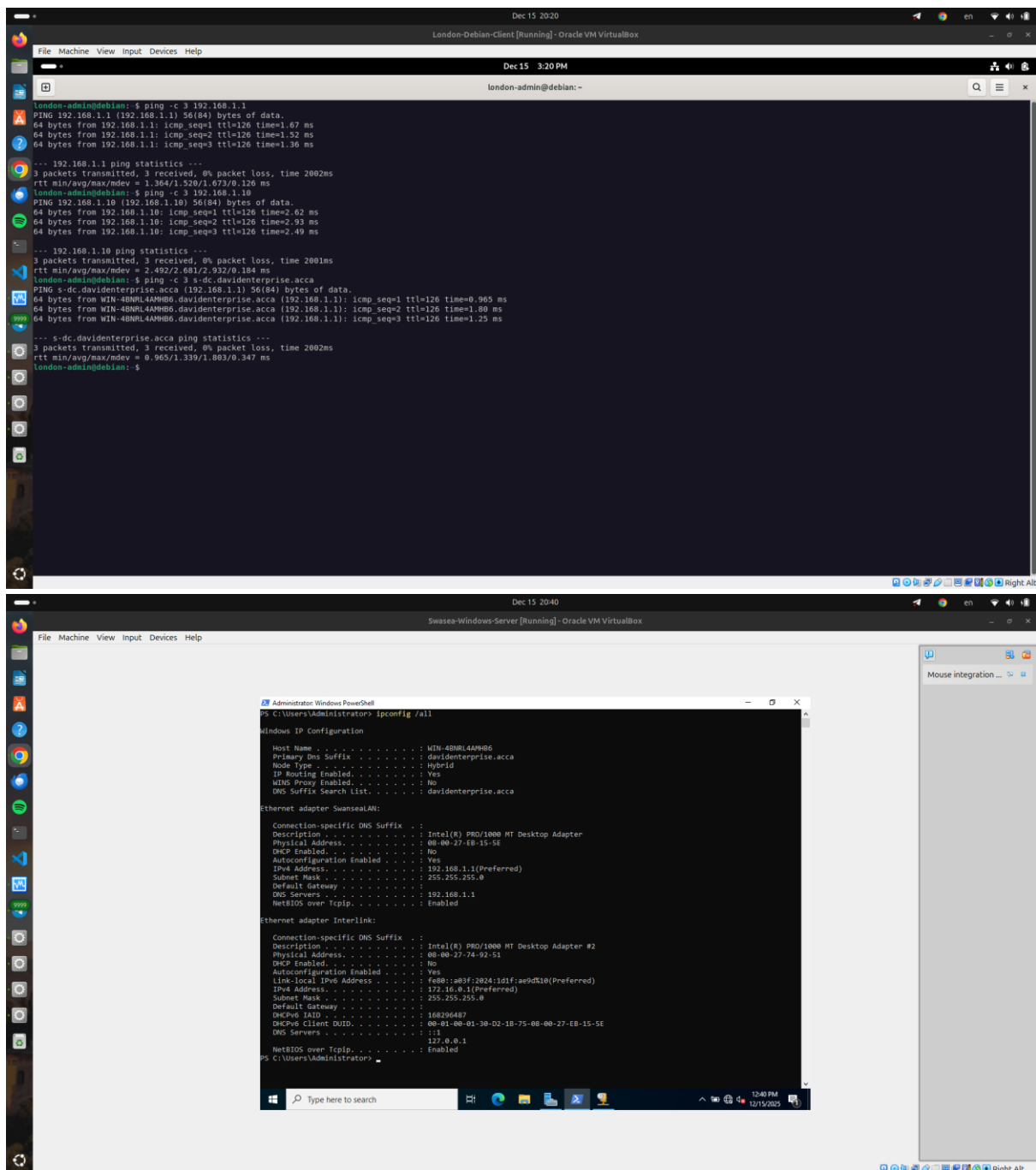
#
# What servers should the DHCP relay forward requests to?
SERVERS="19.28.0.10"

# On what interfaces should the DHCP relay (dhrelay) serve DHCP requests?
INTERFACES="enp0s3 enp0s8"

# Additional options that are passed to the DHCP relay daemon?
OPTIONS=""
administrator@debian:~$
```







6. VPN Configuration (Partial Implementation)

A site-to-site VPN was planned to provide encrypted communication between Swansea and London. While the VPN service was partially configured, full validation could not be completed within the available timeframe.

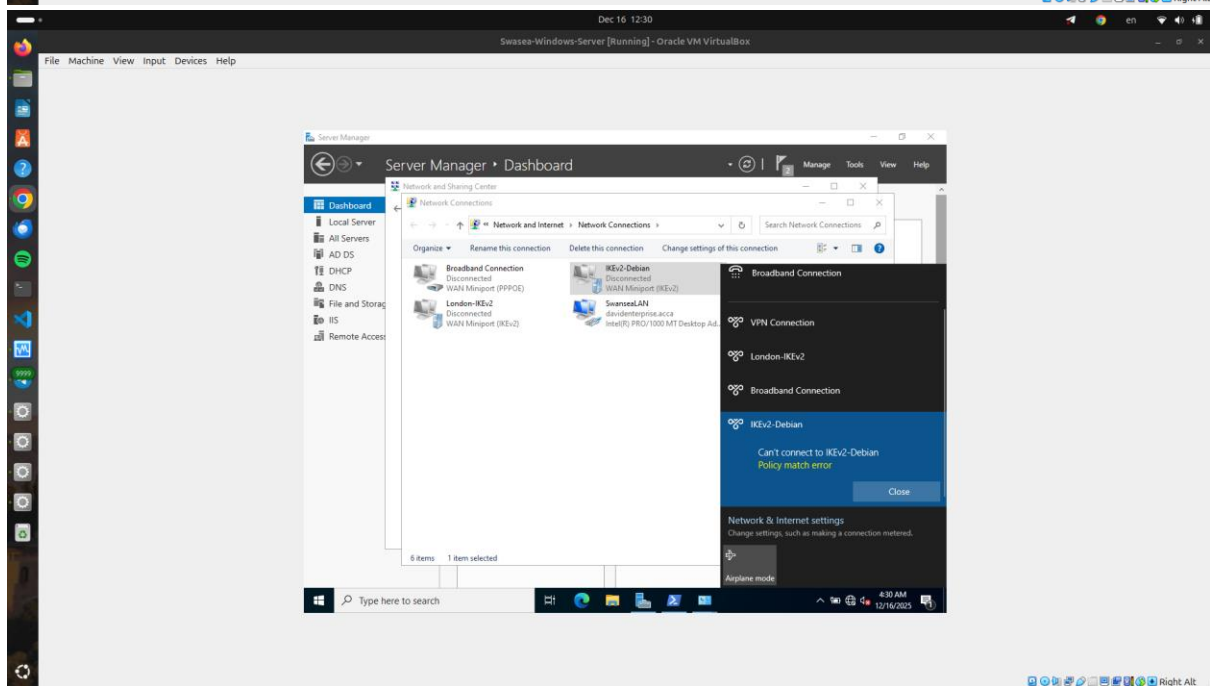
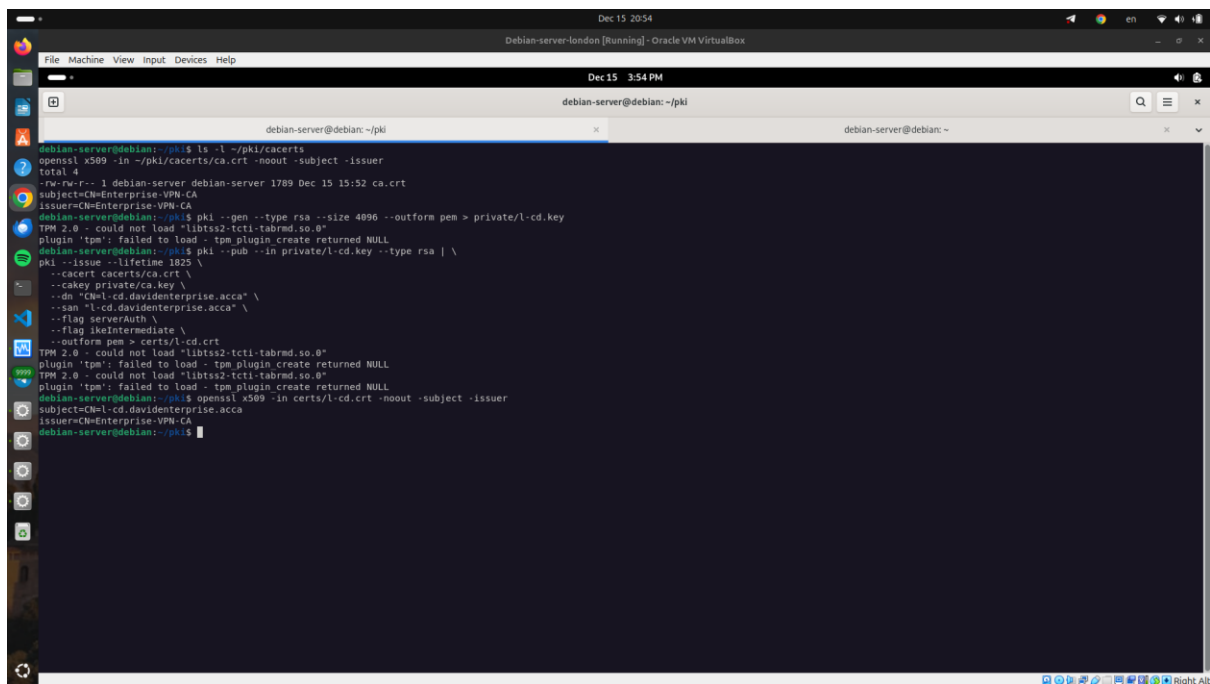
However, the required prerequisites for VPN operation, such as routing, firewall configuration, and inter-site connectivity, were successfully implemented. This demonstrates an understanding of secure network design principles and VPN deployment requirements.

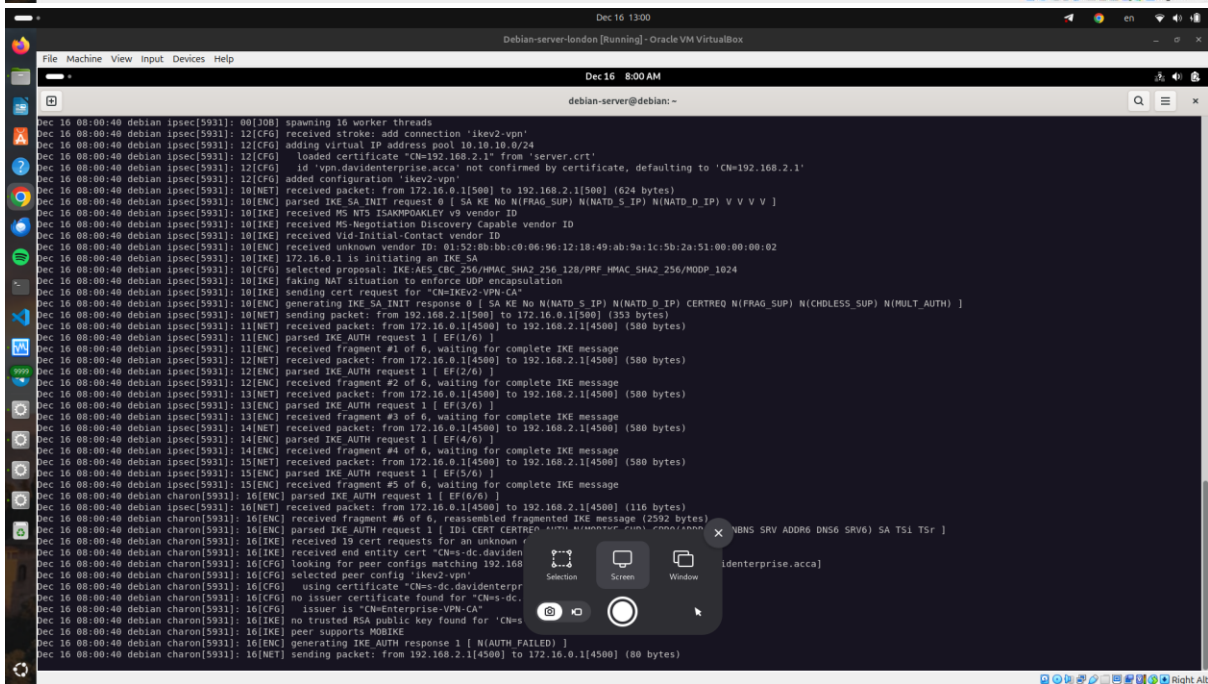
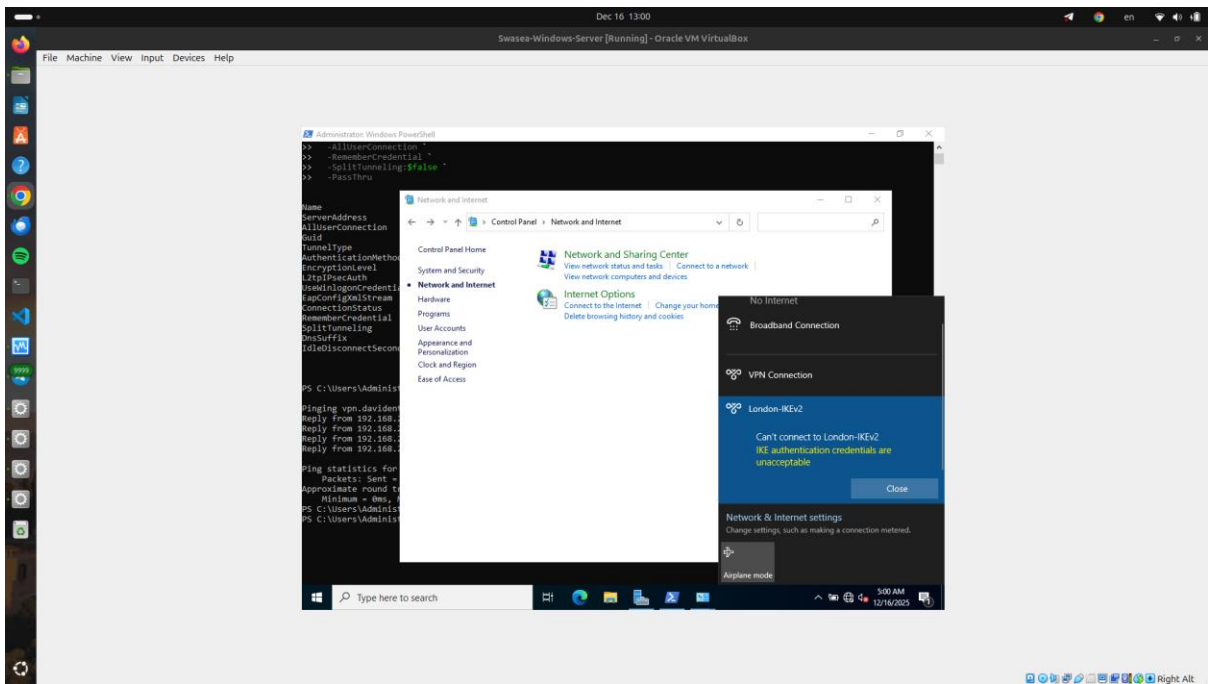
VPN Partial setup:

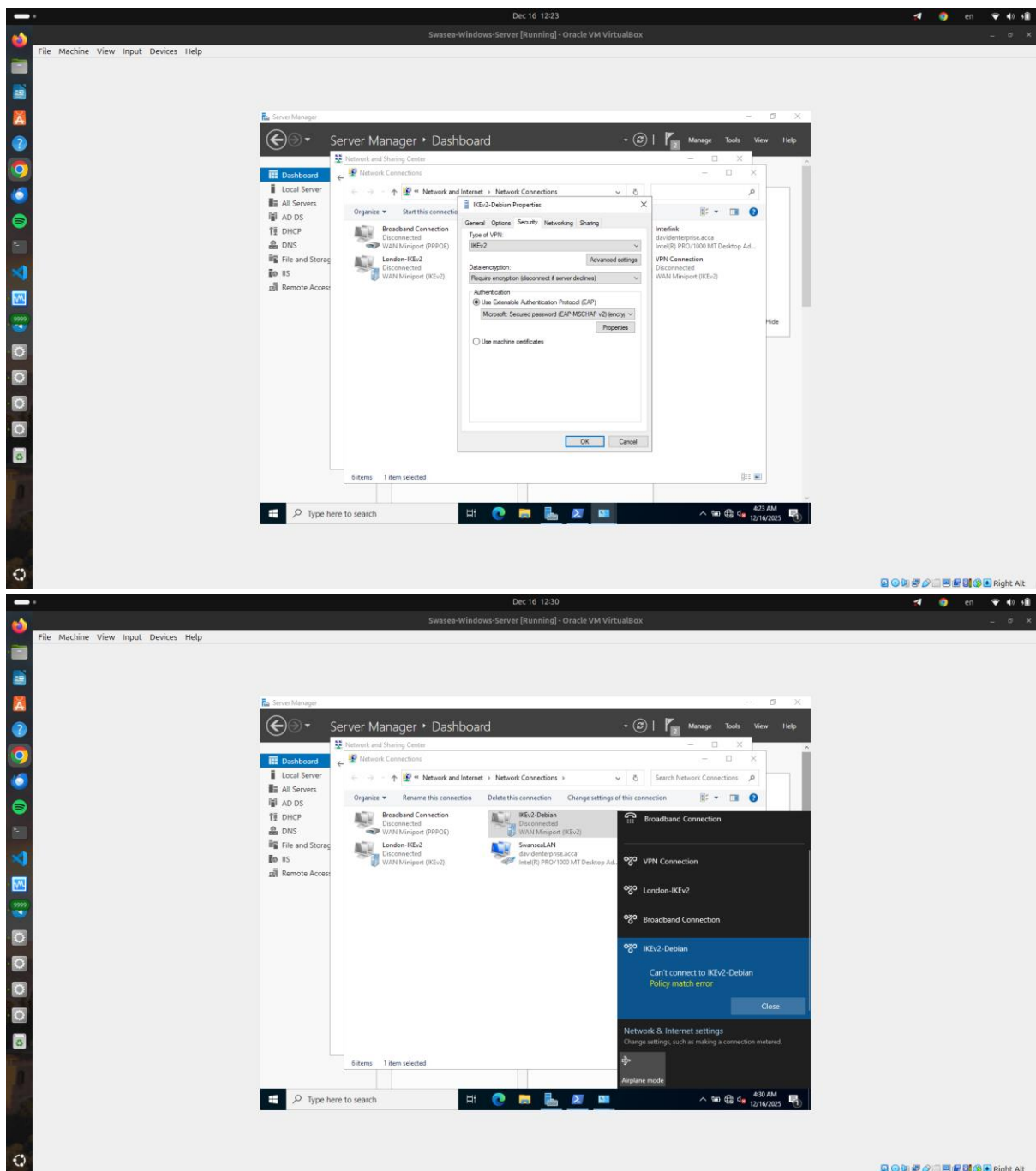
The image consists of two screenshots of a terminal window running on a Debian server within an Oracle VM VirtualBox. The top screenshot, dated Dec 15 20:48, shows the generation of a CA key and certificate using the 'ipsec pki' command. The bottom screenshot, dated Dec 15 20:53, shows the listing of the generated certificates and the creation of a certificate for the VPN server using 'openssl x509'.

```
debian-server@debian:~/pki$ ipsec pki --gen --type rsa --size 4096 --outform pem > private/ca.key
ipsec pki --self --ca --lifetime 3650 \
--in private/ca.key \
--type rsa \
--dn "CN=Enterprise-VPN-CA" \
--outform pem > cacerts/ca.crt

debian-server@debian:~/pki$ ls -l ~/pki/cacerts
total 4
-rw-rw-r-- 1 debian-server debian-server 1789 Dec 15 15:52 ca.crt
subject=CN=Enterprise-VPN-CA
issuer=CN=Enterprise-VPN-CA
debian-server@debian:~/pki$
```







7. Conclusion

The project successfully delivered a functional enterprise network with structured IP addressing, inter-site routing, domain services, DNS resolution, and DHCP automation. Although the VPN configuration was not fully finalised, the core infrastructure demonstrates practical understanding of network operating systems, troubleshooting methodologies, and enterprise networking concepts.

