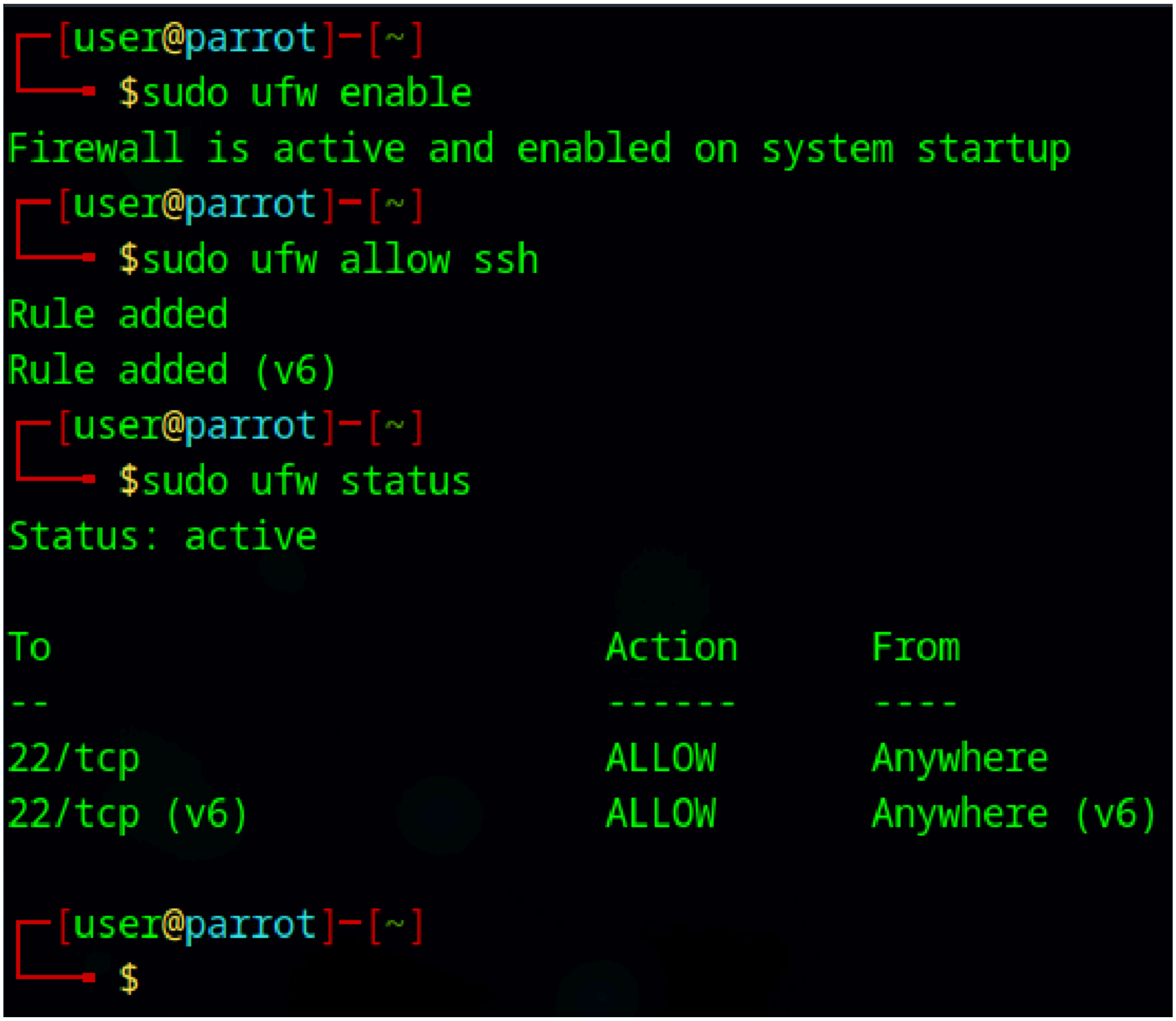
Network Access & Authentication

Overview

This document outlines the implementation of Network Access Control, identity-based access, a site-to-site VPN (or SSH tunnel as a substitute), and role-based access control.

A. Implement Network Access Control

Step 1: Enable UFW (Uncomplicated Firewall)

1. Enable UFW:
   sudo ufw enable
2. Allow SSH access:
   sudo ufw allow ssh
3. Verify UFW status:
   sudo ufw status
4. **Screenshot:** UFW status output.
5. 

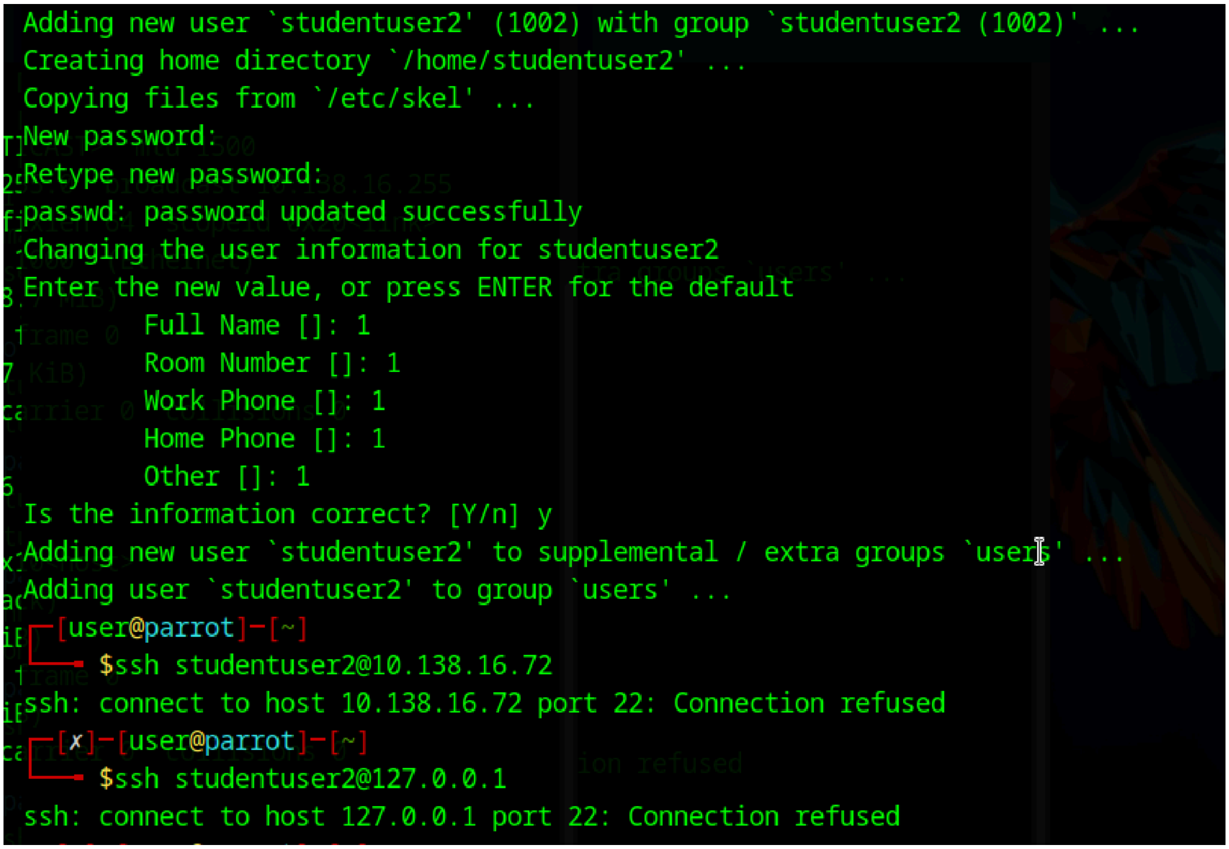
```
┌─[user@parrot]─[~]
└──╼ $sudo ufw enable
Firewall is active and enabled on system startup
┌─[user@parrot]─[~]
└──╼ $sudo ufw allow ssh
Rule added
Rule added (v6)
┌─[user@parrot]─[~]
└──╼ $sudo ufw status
Status: active

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

┌─[user@parrot]─[~]
└──╼ $
```

B. Identity-Based Access

Step 2: Create a New User

1. Add a new user named studentuser:
   sudo adduser studentuser
2. Follow the prompts to set a password.
3. **Screenshot:** Confirmation of user creation.

Step 3: Test SSH Login

1. From another terminal or VM, log in to studentuser:
   ssh studentuser@10.138.16.72
2. **Screenshot:** Successful SSH login.
3. 

```
Adding new user `studentuser2' (1002) with group `studentuser2 (1002)' ...
Creating home directory `/home/studentuser2' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for studentuser2
Enter the new value, or press ENTER for the default
        Full Name []: 1
        Room Number []: 1
        Work Phone []: 1
        Home Phone []: 1
        Other []: 1
Is the information correct? [Y/n] y
Adding new user `studentuser2' to supplemental / extra groups `users' ...
Adding user `studentuser2' to group `users' ...
┌─[user@parrot]─[~]
└──╼ $ssh studentuser2@10.138.16.72
ssh: connect to host 10.138.16.72 port 22: Connection refused
┌─[✗]─[user@parrot]─[~]
└──╼ $ssh studentuser2@127.0.0.1
ssh: connect to host 127.0.0.1 port 22: Connection refused
```

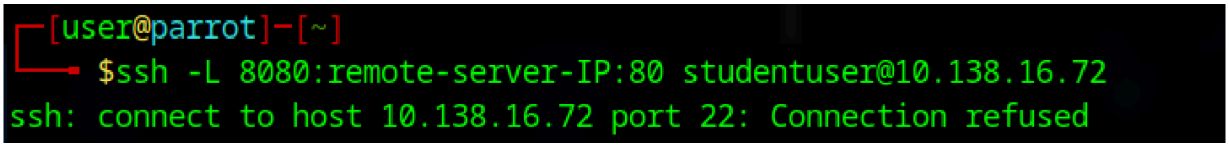
C. Set Up a Simple Site-to-Site VPN (or SSH Tunnel)

Option 1: Install OpenVPN

1. Install OpenVPN:
   sudo apt install openvpn -y
2. Use OpenVPN documentation to configure a basic connection.

Option 2: Create an SSH Tunnel

1. Forward a local port to a remote service:
   ssh -L 8080:remote-server-IP:80 studentuser@10.138.16.72
2. **Screenshot:** Terminal showing the tunnel running.

3. 

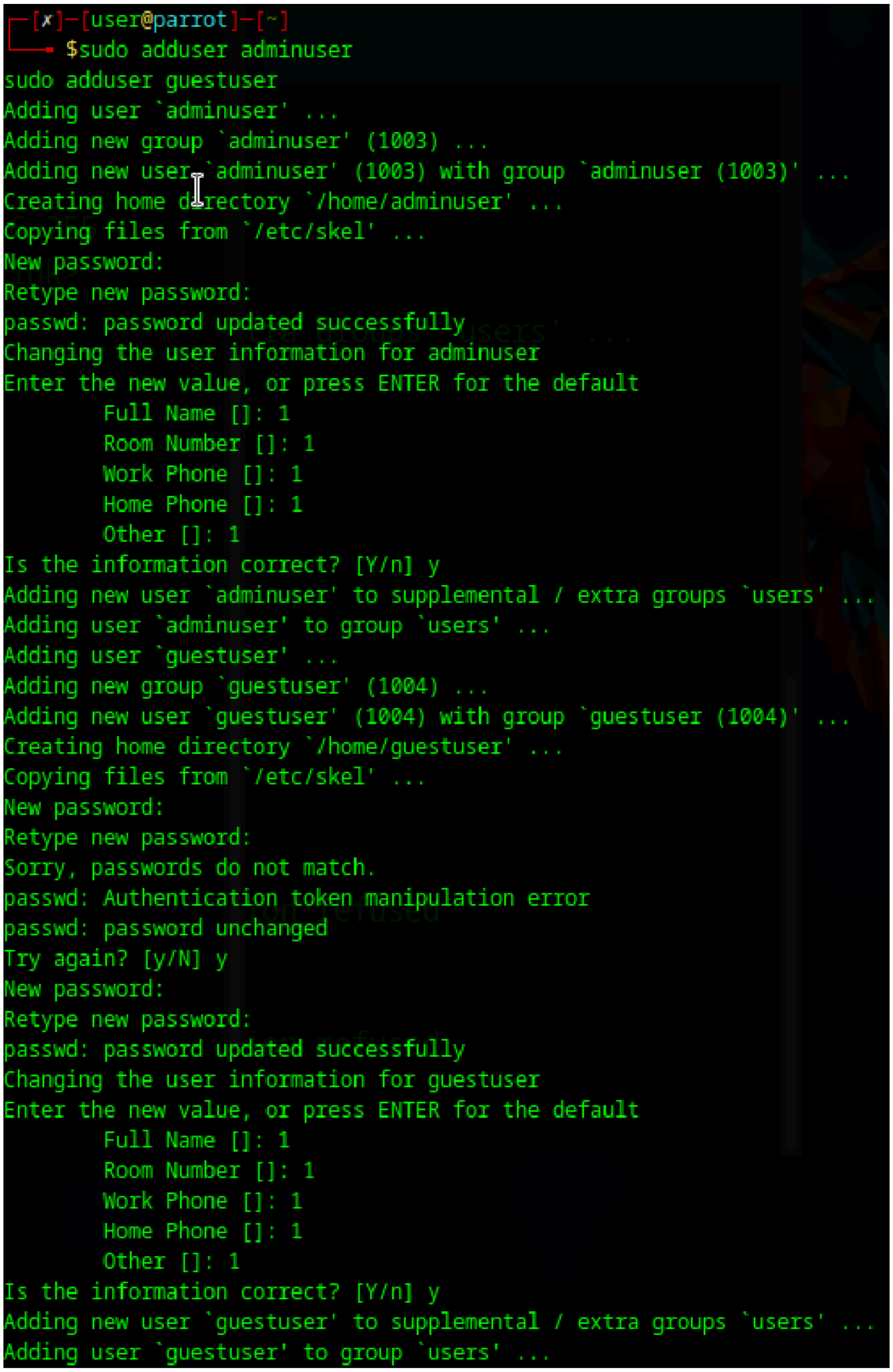
```
┌─[user@parrot]─[~]
└──╼ $ssh -L 8080:remote-server-IP:80 studentuser@10.138.16.72
ssh: connect to host 10.138.16.72 port 22: Connection refused
```

Documentation:

"The tunnel/VPN securely connects two networks, allowing safe communication."

D. Role-Based Access Control (RBAC)

Step 1: Create Users with Different Roles

1. Add two users:
   sudo adduser 1
2. sudo adduser 1
3. **Screenshot:** User creation confirmation.
4. 

```
┌─[✗]─[user@parrot]─[~]
└──╼ $sudo adduser adminuser
sudo adduser guestuser
Adding user `adminuser' ...
Adding new group `adminuser' (1003) ...
Adding new user `adminuser' (1003) with group `adminuser (1003)' ...
Creating home directory `/home/adminuser' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for adminuser
Enter the new value, or press ENTER for the default
        Full Name []: 1
        Room Number []: 1
        Work Phone []: 1
        Home Phone []: 1
        Other []: 1
Is the information correct? [Y/n] y
Adding new user `adminuser' to supplemental / extra groups `users' ...
Adding user `adminuser' to group `users' ...
Adding user `guestuser' ...
Adding new group `guestuser' (1004) ...
Adding new user `guestuser' (1004) with group `guestuser (1004)' ...
Creating home directory `/home/guestuser' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for guestuser
Enter the new value, or press ENTER for the default
        Full Name []: 1
        Room Number []: 1
        Work Phone []: 1
        Home Phone []: 1
        Other []: 1
Is the information correct? [Y/n] y
Adding new user `guestuser' to supplemental / extra groups `users' ...
Adding user `guestuser' to group `users' ...
```

Step 2: Restrict Access to a Sensitive File

1. Create a secure file:
   sudo touch /secure-data.txt
2. sudo chown adminuser /secure-data.txt
3. sudo chmod 700 /secure-data.txt
4. **Screenshot:** File permissions and user details.

Documentation:

"Only **adminuser** can access **/secure-data.txt**, demonstrating Role-Based Access Control (RBAC)."