Building a VPN Server with OpenVPN

Objectives:

At the end of this episode, I will be able to:

1. Describe the OpenVPN networking server.
2. Install and configure OpenVPN on a Linux server.

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- Building a VPN Server with OpenVPN

    - Introduction to OpenVPN
    - Installing OpenVPN
    - OpenVPN Configuration Files

- Introduction to OpenVPN

    - Open source project
    - Designed to provide a simple, yet flexible, VPN server/client infrastructure
    - Uses OpenSSL (TLS) for encryption/decryption
    - Relies upon private/public key pairs for authentication

        - Also supports username/password

- OpenVPN Infrastructure

    - Install the OpenVPN package on the VPN server

        - `sudo apt install openvpn`

    - Issue a trusted certificate for the server
    - Generate client profiles using that certificate
    - Transmit the client profiles to the remote users

- OpenVPN Installation Script

    1. Download and review the script

        - `wget https://git.io/vpn -O openvpn.sh`

    2. Mark the script executable

        - `chmod +x ./openvpn.sh`

    3. Run the script and answer the configuration questions

        - `sudo ./openvpn.sh`

- Firewall rules

    - Script based install

        - Automatically configured in *iptables*
        - `sudo iptables-save | grep 1194`

    - Mannual install

        - Open up the appropriate port
        - `sudo ufw allow 1194/udp`
        - `sudo ufw allow 1194/tcp`

- Verifying OpenVPN

    - Check for service errors

        - `sudo systemctl status openvpn-server@server`

    - Verify the tunnel interface is present

- ip -br addr | less -S
  - Review the server config
    - less /etc/openvpn/server/server.conf