4 - Connecting to Firewall production networks

1. **Create Layer 3 Network Interfaces**
    1. Account for each user's IP address & CDR
    2. `Network > Interfaces > Ethernet
    3. Select an Ethernet interface to configure
    4. Set the `Interface Type` to `Layer 3`
        - Assign Interface to `none`
    5. Set IPv4 settings
        1. Type: `Static`
        2. Add ip address under heading
    6. Repeat steps for the next ip address using the next ethernet interface in line.
2. **Create a Virtual Router**
   This allows the virtual router to obtain routes to other subnets using the static routes defined previously.
    1. `Network > virtual routers> default`
    2. Name the virtual router `CCDC`; Add the previously configured `ethernet interfaces`
    3. Static Routes > IPv4 > Add
    4. Configure Virtual Router
    - Name: `CCDC default gateway`
    - Destination: `0.0.0.0./0`
    - Interface: `ethernet1/1`
    - Next Hop: IP Address
        - `203.0.113.1`
3. **Segment production using Security Zones**

    1. `Network > Zones > Add`
    2. Add Ethernet interface `ethernet1/1` naming it `internet`
    3. Repeat for `ethernet1/2` naming it `Users Net`
    4. Repeat for `ethernet1/3` naming it `Extra Net`
4. Commit all changes
5. Test each connectivity
    1. On the desktop, open `Remmina`
    2. Check the `Firewall` entry to log in to the CLI
    3. Use the following command to check connection of the ethernet interfaces to the host:
        1. `ping source [ethernet1/1 IP] host 8.8.8.8`
        2. `ping source [ethernet1/2 IP] host 192.1.20`
        3. `ping source [ethernet1/3 IP] host 192.1.20`
            1. Exit with ctrl + c after at least 3 successful pings
6. Define Interface Management Profiles
   You will define two interface profiles.
   One to allow ping profile to internet interface
   One to allow ping and secure network traffic
    1. Using Palo Alto: `Network > Network Profiles > Interface Management > Add`
    2. Name: `Allow Ping`
       Network Services: `Ping'
    3. Add another profile:
        - Name: `Allow-mgt`
        - Under Administrative Management Services Check the following:
            - `HTTPS`
            - `SSH`
        - Network Services
            - `ping`

        - `SNMP`
        - `Response Pages`
        - `User-ID`
    4. `Network > Interfaces > Ethernet > Ethernet 1/1`
    5. Advanced tab > other info
    6. Management profile: `Allow-Ping`
       Note: This action applied allow ping interface management to an internet-facing interface.
       This is NOT recommended in a real production environment.
    7. `Network > Interfaces > Ethernet > Ethernet 1/2`
        1. Advanced tab > other info
        2. Management profile: `Allow-mgt`
    8. `Network > Interfaces > Ethernet > Ethernet 1/3`
        1. Advanced tab > other info
        2. Management profile: `Allow-mgt`
    9. Commit all changes
7. Test interface access
    1. Open `Terminal Emulator` on desktop
    2. Use the following commands to test the interfaces
        1. `ping 192.168.1.1`
    3. Attempt an ssh connection to the firewall through this ip
        1. `sudo su`
        2. `ssh admin@192.168.1.1`
        3. `Accept the RSA fingerprint`