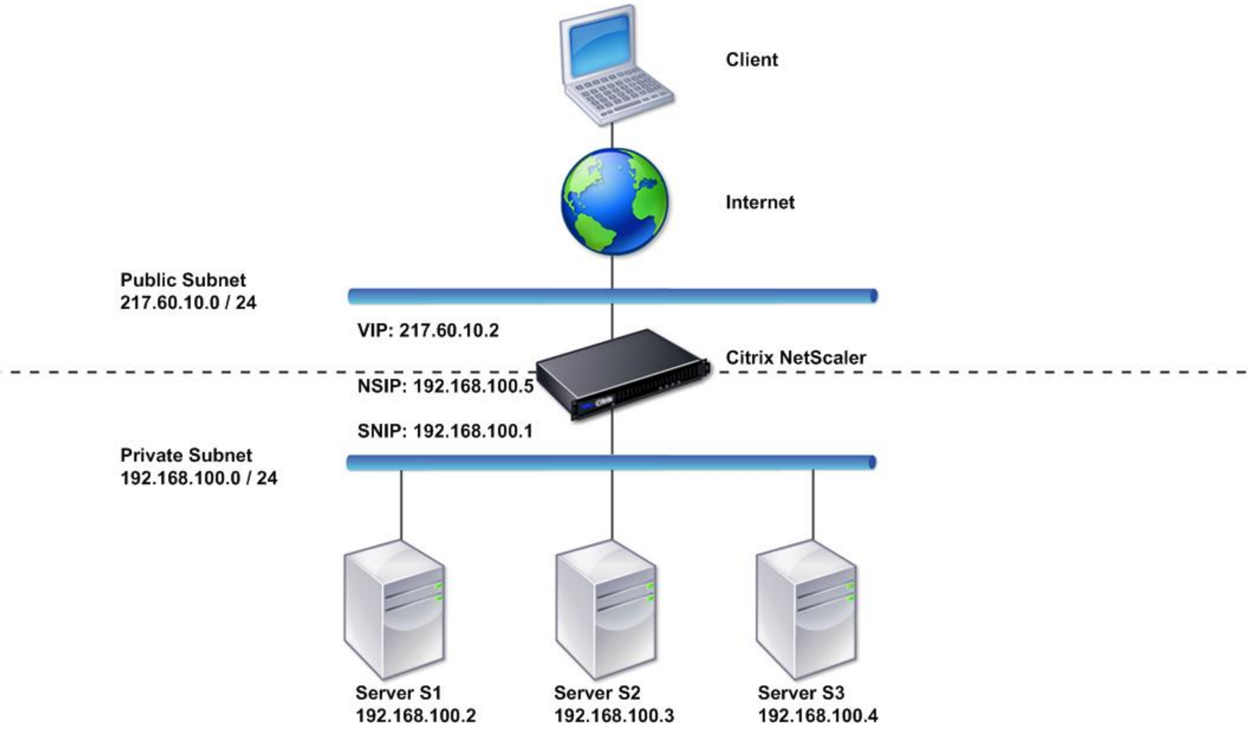

- **Firewall/VPN Appliance:** The core device responsible for establishing and managing the SSL VPN tunnel.
- **Remote Client Devices:** Various devices (laptops, smartphones, tablets) used by remote users to connect to the SSL VPN.

Components Used:

- **Firewall/VPN Appliance:** A network security device capable of supporting SSL VPN, such as a FortiGate, Cisco ASA, or Palo Alto Networks firewall.
- **Client Devices:** Devices running compatible SSL VPN client software (e.g., FortiClient, Cisco AnyConnect, Palo Alto Networks GlobalProtect).

Steps of the Lab:

1. **Configure SSL VPN Settings:**
   - **Create a VPN Portal:** Define the portal settings, including authentication methods (e.g., username/password, certificate), access policies, and permitted network resources.
   - **Configure SSL VPN Tunneling:** Set up the SSL VPN tunnel parameters, such as the listening interface, port number, and encryption algorithms.
   - **Define Client Access Policies:** Specify which users or groups can access the VPN and the resources they can access.
2. **Install and Configure Client Software:**
   - **Install Client Software:** Deploy the appropriate SSL VPN client software on remote devices.
   - **Configure Client Settings:** Configure the client software with the VPN server address, portal name, and user credentials.
3. **Test the VPN Connection:**
   - **Establish a VPN Connection:** Attempt to connect to the VPN server using the client software.
   - **Verify Connectivity:** Once connected, test network connectivity to internal resources (e.g., file servers, applications) to ensure proper tunnel functionality.

Testing the Lab:

- **Successful Connection:** Remote users should be able to establish secure VPN connections to the corporate network.
- **Access to Resources:** Once connected, users should be able to access authorized network resources, such as file servers, email, and internal applications.
- **Secure Communication:** All data transmitted over the VPN tunnel should be encrypted to protect sensitive information.

Results:

- **Enhanced Security:** SSL VPN provides a secure and encrypted connection, protecting sensitive data from unauthorized access.
- **Remote Access:** Remote workers can access network resources from anywhere with an internet connection.
- **Improved Productivity:** Remote users can work efficiently, as if they were in the office.

Configuration Example (FortiGate):

```
config vpn ssl-vpn
    edit vpn1
        set interface port1
        set listen-port 443
        set authentication-server internal
        set authentication-method user-password
        set client-ip-assignment pool
            edit pool1
                set start 192.168.100.100
                set end 192.168.100.200
            next
        next
    next
config firewall policy
    edit 1
        set src-intf ssl.vpn1
        set dst-intf port1
        set src-addr all
        set dst-addr all
        set service all
        set action accept
    next
```