VPN

This guide will help you to configure a point2point VPN, between 2 hosts, using SSH protocol.

Server Side

1. Firewalling
   a. Drop all forward packet

      -
        ```
        $ sudo iptables -P FORWARD DROP
        ```
   b. Accept all packets from interface ens3

      -
        ```
        $ sudo iptables -I FORWARD -i ens3 -j ACCEPT
        ```
   c. Accept all packets with state ESTABLISHED, RELATED

      -
        ```
        $ sudo iptables -I FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
        ```
   d. Accept all packet with input and output interface ens3:0

      -
        ```
        $ sudo iptables -I FORWARD -i ens3:0 -j ACCEPT
        ```

      -
        ```
        $ sudo iptables -I FORWARD -o ens3:0 -j ACCEPT
        ```
2. Configuring Server
   a. Starting server

      -
        ```
        $ sudo service ssh start
        ```
   b. Verify that port 22 is listening

      -
        ```
        $ sudo apt install net-tools
        ```

      -
        ```
        $ netstat -tpln
        ```
   c. For check what happens with incoming connections you can monitor the auth.log file

      -
        ```
        $ sudo tail -f /var/log/auth.log
        ```
   d. Enable SSH Tunneling in the configuration file

      -
        ```
        $ sudo nano /etc/ssh/sshd_config
        ```
      - Add the line “PermitTunnel yes” or modify it, if any
   e. Restart SSH server

      -
        ```
        $ sudo service ssh restart
        ```
   f. Enabling virtual interface

      -
        ```
        $ sudo ifconfig ens3:0 10.1.0.131
        ```

Client Side

1. Configure interface
   a. ```
      $ sudo ifconfig ens3:0 10.1.0.132 pointopoint 10.1.0.131 up
      ```
2. Verify if other end of tunnel is reachable
   a. ```
      $ ping 10.1.0.131
      ```
3. Adding ARP public entry on ens3
   a. ```
      $ sudo arp -sD 10.1.0.131 ens3 pub
      ```
4. Check arp table
   a. ```
      $ arp -a
      ```
5. Start VPN connection
   a. ```
      $ sudo ssh ubuntu@10.1.0.131 -w 0:0
      ```

To check if  everything works you must check connection on client side, if everything works you should be connected on SSH to server and all data are encapsulated into a tunnel. With wireshark you
      ```

can check tunneling between the two hosts and also check what happens after the tunnel. To check the last point you can navigate using ssh tunnel an check data that server gives in output.