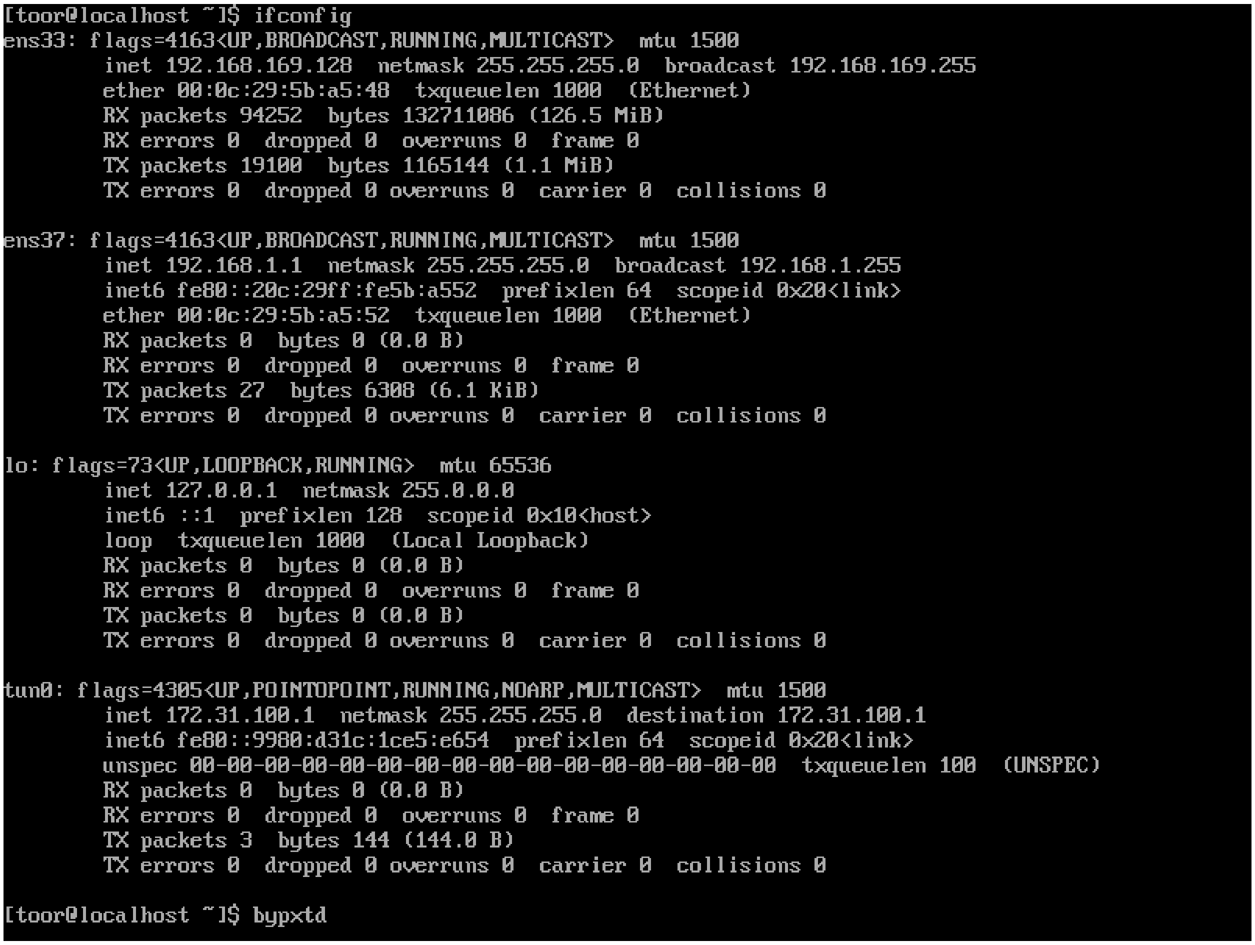
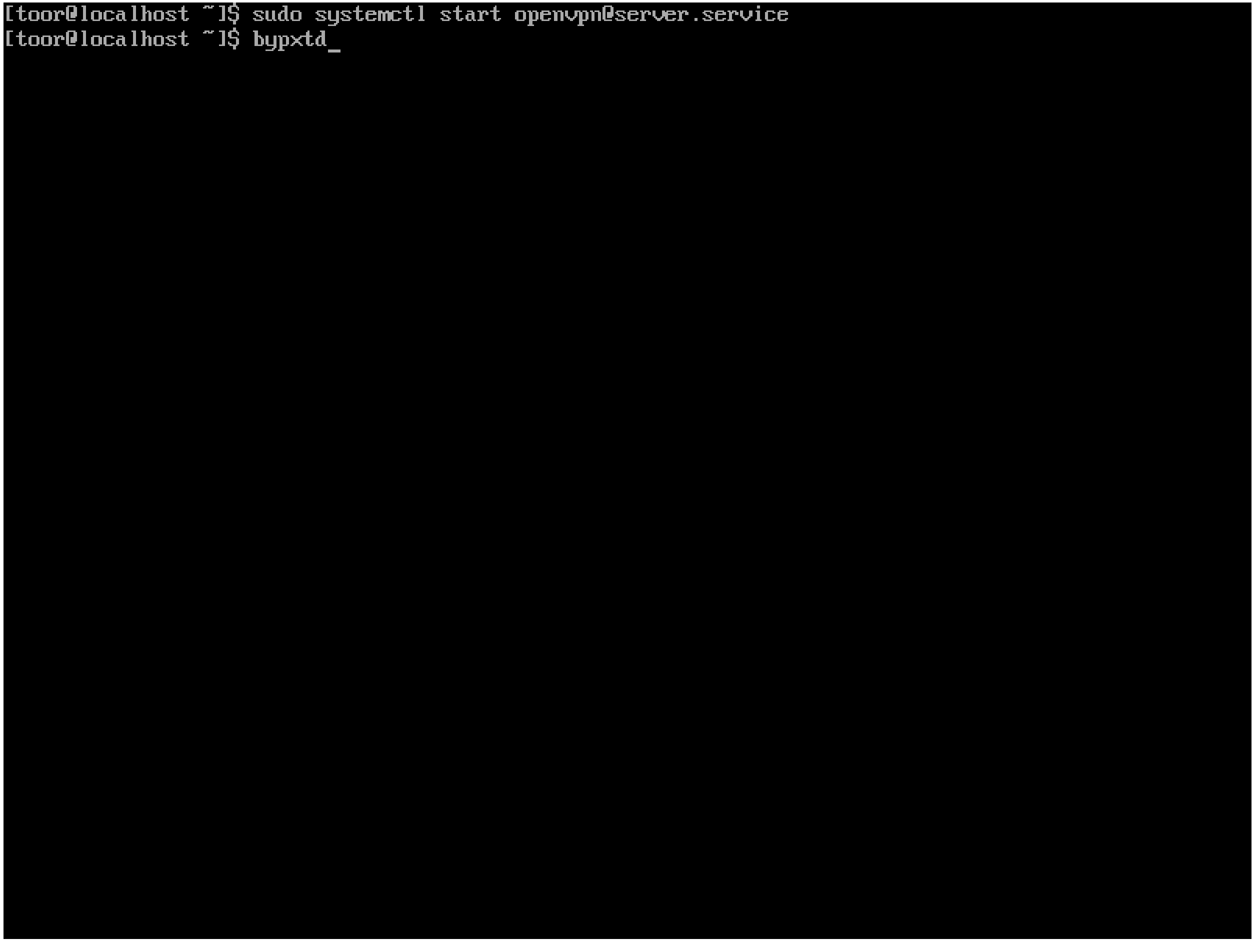
1. After the OpenVPN is installed and configured in the SERVER succesfully execute the $sudo systemctl start openvpn@server.service command, type your pawprint in the command line and take a screenshot.



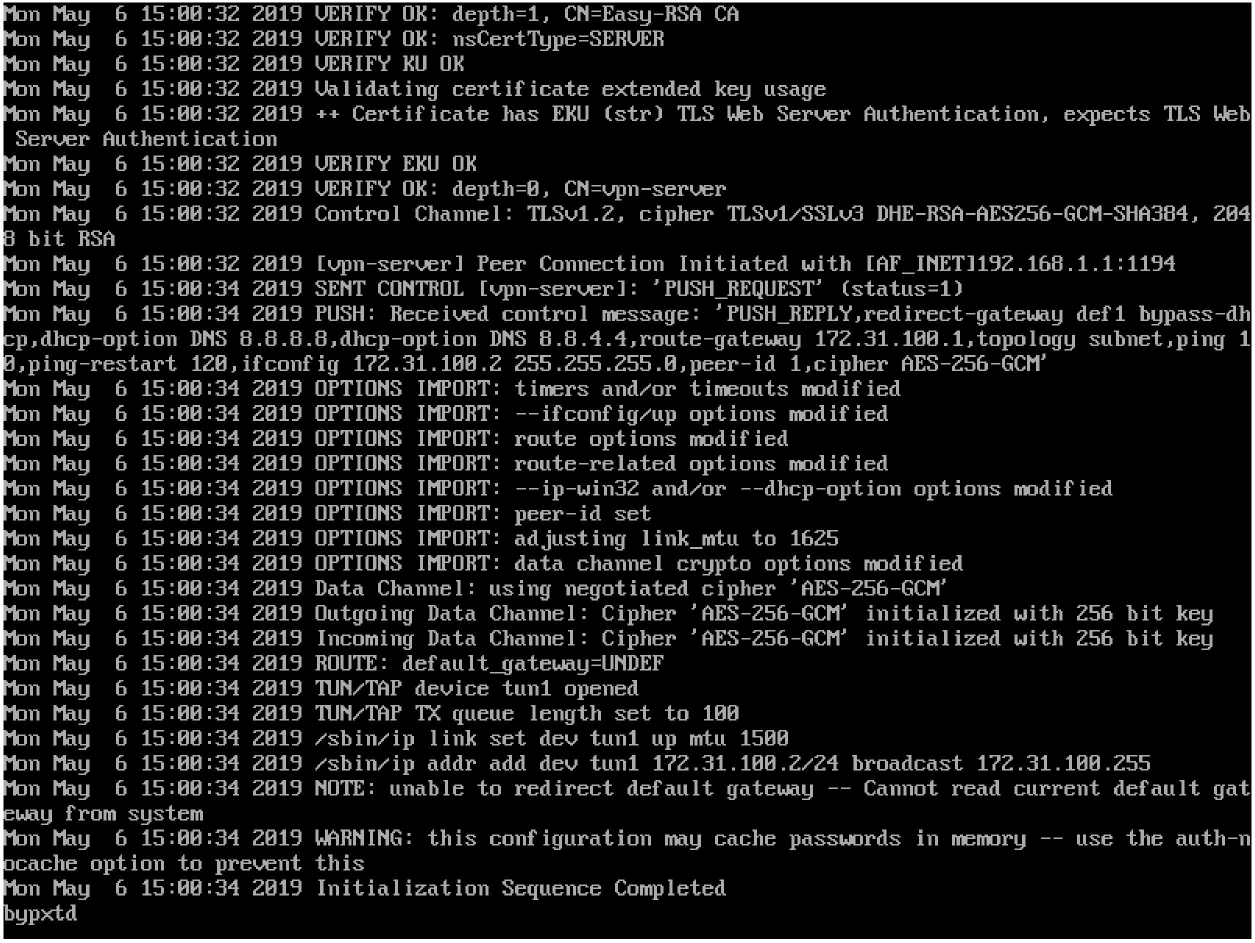
```
[toor@localhost ~]$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.169.128  netmask 255.255.255.0  broadcast 192.168.169.255
        ether 00:0c:29:5b:a5:48  txqueuelen 1000  (Ethernet)
        RX packets 94252  bytes 132711086 (126.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19100  bytes 1165144 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.1  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe5b:a552  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:5b:a5:52  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27  bytes 6308 (6.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 172.31.100.1  netmask 255.255.255.0  destination 172.31.100.1
        inet6 fe80::9980:d31c:1ce5:e654  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3  bytes 144 (144.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[toor@localhost ~]$ bypxtd
```

2. In the SERVER type ifconfig showing the new virtual network interface created by the VPN, type your pawprint and take a screenshot.



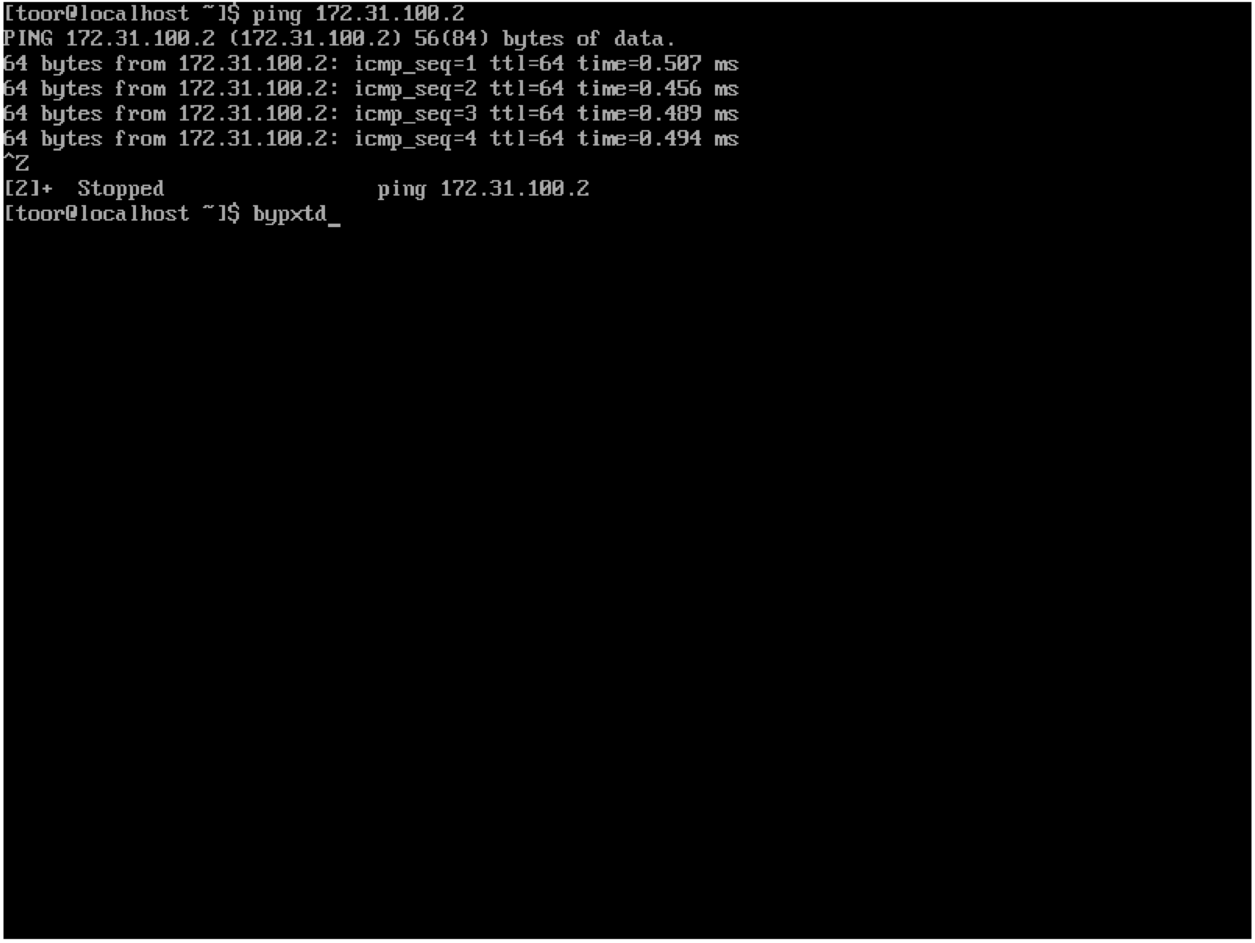
```
[toor@localhost ~]$ sudo systemctl start openvpn@server.service
[toor@localhost ~]$ bypxtd_
```

3. After the OpenVPN is installed and configured in the CLIENT succesfully, execute $sudo openvpn --config client.ovpn (take a screenshot).



```
Mon May  6 15:00:32 2019 VERIFY OK: depth=1, CN=Easy-RSA CA
Mon May  6 15:00:32 2019 VERIFY OK: nsCertType=SERVER
Mon May  6 15:00:32 2019 VERIFY KU OK
Mon May  6 15:00:32 2019 Validating certificate extended key usage
Mon May  6 15:00:32 2019 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web
 Server Authentication
Mon May  6 15:00:32 2019 VERIFY EKU OK
Mon May  6 15:00:32 2019 VERIFY OK: depth=0, CN=vpn-server
Mon May  6 15:00:32 2019 Control Channel: TLSv1.2, cipher TLSv1/SSLv3 DHE-RSA-AES256-GCM-SHA384, 204
8 bit RSA
Mon May  6 15:00:32 2019 [vpn-server] Peer Connection Initiated with [AF_INET]192.168.1.1:1194
Mon May  6 15:00:34 2019 SENT CONTROL [vpn-server]: 'PUSH_REQUEST' (status=1)
Mon May  6 15:00:34 2019 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway def1 bypass-dh
cp,dhcp-option DNS 8.8.8.8,dhcp-option DNS 8.8.4.4,route-gateway 172.31.100.1,topology subnet,ping 1
0,ping-restart 120,ifconfig 172.31.100.2 255.255.255.0,peer-id 1,cipher AES-256-GCM'
Mon May  6 15:00:34 2019 OPTIONS IMPORT: timers and/or timeouts modified
Mon May  6 15:00:34 2019 OPTIONS IMPORT: --ifconfig/up options modified
Mon May  6 15:00:34 2019 OPTIONS IMPORT: route options modified
Mon May  6 15:00:34 2019 OPTIONS IMPORT: route-related options modified
Mon May  6 15:00:34 2019 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Mon May  6 15:00:34 2019 OPTIONS IMPORT: peer-id set
Mon May  6 15:00:34 2019 OPTIONS IMPORT: adjusting link_mtu to 1625
Mon May  6 15:00:34 2019 OPTIONS IMPORT: data channel crypto options modified
Mon May  6 15:00:34 2019 Data Channel: using negotiated cipher 'AES-256-GCM'
Mon May  6 15:00:34 2019 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Mon May  6 15:00:34 2019 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Mon May  6 15:00:34 2019 ROUTE: default_gateway=UNDEF
Mon May  6 15:00:34 2019 TUN/TAP device tun1 opened
Mon May  6 15:00:34 2019 TUN/TAP TX queue length set to 100
Mon May  6 15:00:34 2019 /sbin/ip link set dev tun1 up mtu 1500
Mon May  6 15:00:34 2019 /sbin/ip addr add dev tun1 172.31.100.2/24 broadcast 172.31.100.255
Mon May  6 15:00:34 2019 NOTE: unable to redirect default gateway -- Cannot read current default gat
eway from system
Mon May  6 15:00:34 2019 WARNING: this configuration may cache passwords in memory -- use the auth-n
ocache option to prevent this
Mon May  6 15:00:34 2019 Initialization Sequence Completed
bypxtd
```

4. From VPN SERVER ping the VPN CLIENT using the VPN IP addresses.



```
[toor@localhost ~]$ ping 172.31.100.2
PING 172.31.100.2 (172.31.100.2) 56(84) bytes of data.
64 bytes from 172.31.100.2: icmp_seq=1 ttl=64 time=0.507 ms
64 bytes from 172.31.100.2: icmp_seq=2 ttl=64 time=0.456 ms
64 bytes from 172.31.100.2: icmp_seq=3 ttl=64 time=0.489 ms
64 bytes from 172.31.100.2: icmp_seq=4 ttl=64 time=0.494 ms
^Z
[2]+  Stopped                 ping 172.31.100.2
[toor@localhost ~]$ bypxtd
```