We support VPN (virtual private network) for connecting to the IITD internal LAN from outside IITD. We use OpenVPN , and run an OpenVPN server on *ssh2.iitd.ernet.in (for faculty/retfaculty/emeritus) and vpn.iitd.ernet.in (for part-time msr/ part-time phd students)* . VPN access is granted only to faculty/retfaculty/emeritus and part-time msr/part-time phd students.
(They can request from https://ldap1.iitd.ac.in/usermanage/services.php .)
VPN users are advised to set up their VPN in IITD before going out of the campus to try to use it. The certificate-key pairs will not be sent by email under any circumstances.

The VPN feature may be required by users while traveling outside IITD for a variety of reasons:

1. for accessing software license servers (e.g. MATLAB)
2. for accessing internal *SVN* repositories.
3. for accessing online journals and conference proceedings through the IITD library site (through IITD Proxy Servers).
4. for accessing IITD internal web servers like internal.iitd.ernet.in , the IRD internal webpage, the ACSS webpage etc. for accessing forms, software repositories and other information.
5. for accessing the internal DNS, proxy and mail servers in case there is a need (though note that the IITD mail server can be securedly accessed directly from outside; see the CSC web-page).
6. for accessing files, IITD homes (CIFS) , HPC facility and other resources from an internal machine.

In what follows, we briefly describe the configuration details:

1. The OpenVPN server runs on the *UDP port 1194* on *ssh2.iitd.ernet.in (for faculty/retfaculty/emeritus) and vpn.iitd.ernet.in (for part time msr/part-time phd students)*

2. Check out the OpenVPN howto for details on how to setup and start an OpenVPN client on your Windows, Linux or Mac laptops. In particular, check out the *Linux/Windows/Mac notes*

in the section called
Installing OpenVPN
. See the
Screen Shots for Windows OS
.

3. On successful connection the client will be automatically assigned an IP addess in the range 10.50.2.x or 10.52.2.x with routes set to the IITD internal VLANs. Your *default route* will not be altered from what has been set to connect to your ISP. On internal network the IP range 10.50.2.x gets one-to-one mapping to 10.51.2.x, and 10.52.2.x gets one-to-one mapping to 10.53.2.x

The VPN connection will be *point-to-point* and the broadcast traffic of the 10.50.2.x or 10.52.2.x VLAN will not be available to the client.

We require three independent mechanisms of secure authentication (all three are required):

1. SSL/TLS key exchange. For this you will need to obtain your own RSA private/public key-pairs duly signed by the IITD Certificate Authority . You will also need the CCIITD-CA.crt on your laptop. You can obtain your RSA key-pairs, and CCIITD-CA.crt files from
https://ldap1.iitd.ernet.in/usermanage/usercert.html
. Please request VPN
here
. Please request while still on campus. This cannot be done from outside. For part time msr/part time phd students, approval of faculty advisor is required.

2. For extra security beyond what is provided by SSL/TLS, we use a *pre-shared TLS key* to create an "HMAC firewall" to help block DoS attacks and UDP port flooding. This key can also be obtained from
https://ldap1.iitd.ernet.in/usermanage/usercert.html

3. You can also download client configuration file from https://ldap1.iitd.ernet.in/usermanage/usercert.html .

4. Finally, you will also need to authenticate using your IITD *username/passwd* for setting up a VPN connection. The exchange with the VPN server will be over a secured channel.

5. The certificates and keys mentioned above, and the sample client.opvn are all that are required for the client side configuration. Install the
client.opvn
file in the

openvpn directory
(
/etc/openvpn
in Linux) and edit the location paths for theÂ
certificates
and the
keys
. The comments in the
client.opvn
file should be self explanatory. On starting
openvpn
you will be prompted for the username and passwd.

6. After successfully establishing an *OpenVPN* connection, you may have to manually add the internal DNS servers, 10.10.1.2/10.10.2.2, in you connection settings so that you may access the internal machines by their names. Normally your client should set this up automatically; the openvpn server provides these parameters.