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.ac.in (for faculty/retfaculty/emeritus/adjunct/vfaculty) and vpn[123].iitd.ac.in (for all students and all staff including contractual/project staff)*
. VPN access is granted to all faculty, staff and students.
They can request from
https://ldap1.iitd.ac.in/usermanage/services.php
within the IITD campus.
The users are advised to set up their VPN as prescribed
here
.

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.ac.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 C SC 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/adjunct/vfaculty
) and vpn.iitd.ernet.in (for
all students and all staff including contractual staff
)*

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 10.50.8.x/21 or 10.52.8.x/21 , 10.54.8.x/21 or 10.54.16.x/21 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 10.50.8.x/21 gets one-to-one mapping to 10.51.8.x/21 , 10.52.8.x/21 gets one-to-one mapping to 10.53.8.x/21 , 10.54.8.x/21 gets one-to-one mapping to.10.55.8.x/21 and 10.54.16.x/21 gets one-to-one mapping to.10.55.16.x/21

The VPN connection will be *point-to-point* and the broadcast traffic of the 10.50.8.x/21 or 10.52.8.x/21 or 10.54.8.x/21 or 10.54.16 .x/21 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 NEWCCIITD-CA.crt on your laptop / any computing device. You can obtain your RSA key-pairs, and NEWCCIITD-CA.crt files from https://newcert.iitd.ac.in/usermanage/usercert.html .. Please request VPN here. Please note request/approval can be made within the IITD campus. This cannot be done from outside. For students/staff, approval of faculty advisor or Project PI is required. The users (student or staff) can request by email to their faculty mentor /supervisor/PI. Faculty then approve the VPN access through the link ( ). The faculty who don't have VPN acces and are not inthe campus can send their request by email to sysadm @ cc.iitd.ac.in.

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://newcert.iitd.ac.in/usermanage/usercert.html
.

3. You can also download client configuration file from https://newcert.iitd.ac.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. Please note the certificate-key pairs will not be sent by email under any circumstances but can be downloaded.
Install the
client.opvn
file in the
openvpn directory
(
/etc/openvpn
in Linux) and edit the location paths for the CÂ
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, your client's DNS search domains iitd.ac.in and iitd.ernet.in as well as DNS Servers 10.10.1.2 and 10.10.2.2 are automatically set. In case they are not, you may have to manually set up these after making the connection.