VPN Frequently Asked Questions

What is a VPN?

A Virtual Private Network (VPN) is a “tunnel” connection created to allow secure communications over public networks. Essentially, VPNs encrypt the traffic from your computer to the CSU network allowing you to work remotely without worry of someone intercepting your communications. It uses extra authentication technology which will let you access data and applications not accessible to the general Internet population.

Why are we changing?

In order to better secure access to university electronic assets from off-campus, it is in the best interest of the institution to adopt a single standard method for remote access. Currently, anyone on the internet can access the CSU network remotely. By just enabling Remote Desktop to your work computer, you are opening it up for anybody to get into. VPN adds another layer of security by using both encryption and extra authentication technology.

Starting January 1, 2011, off-campus users will be required to use the OpenVPN client to access the University network remotely. Remote access will be limited to individuals who have been approved for VPN access.

How does it work?

OpenVPN uses Secured Sockets Layer (SSL) to encrypt your traffic. This is the same underlying technology that is used in web browsers to secure online shopping/banking.

Can I still continue to use what I am using today?

You can continue to use Remote Desktop or pcAnywhere to connect to your office Windows computer or Virtual Network Computing (VNC) for Macs. You will need to enable the VPN client first.

How do I get a VPN account?

All tenured and tenure track faculty are automatically set-up for VPN access, as well as other faculty and staff who are currently authorized to have remote access.

Other faculty and staff who need VPN access must fill out the VPN Authorization form found in http://mycsu.csuohio.edu/offices/ist/security/vpn.html and obtain approval from their supervisor and the Human Resources department.

Can I still use the Internet while I'm connected?

Yes. This technology uses a technique called ‘split tunneling’, where only specific network traffic destined for University resources is routed via the VPN client.

Will it work anywhere?

OpenVPN has two modes:

- UDP - The default, uses DTLS (datagram TLS). This is more efficient, but is sometimes blocked by Internet Service Providers (ISP).
- TCP - Uses the standard SSL port (TCP/443). Hardly anyone blocks this, but breaks UDP applications.

The ISP that you are using at the time of connection may block specific types of TCP/IP traffic, thereby preventing VPN connectivity. Contact your ISP for further assistance.

How many workstations can I set-up?

You can install the VPN client on as many workstations you have off-site, but you can only have one VPN connection active at any time.

We advise against installing the VPN client on a shared computer.

Will it work on my Mac?

Yes. Connecting to a Mac desktop is different from a Windows desktop. Mac connection requires separate software.   Please refer the Installation instructions or call IS&T for assistance.