

Virtual Private Network (VPN) Policy

Participation in a remote access program may not be possible for every employee. Remote access is meant to be an alternative method of meeting Office of Research needs. The Office of Research may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

1.0 Purpose

The purpose of this policy is to provide guidelines for Remote Access IPSec or Virtual Private Network (VPN) connections to the UCSF Office of Research network.

2.0 Scope

This policy applies to all UCSF Office of Research employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the UCSF Office of Research network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

3.0 Policy

Approved UCSF Office of Research employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to UCSF Office of Research internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the UCSF network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by UCSF Office of Research network operational groups.
6. All computers connected to UCSF Office of Research internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the UCSF standard (provide URL to this software); this includes personal computers.
7. VPN users will be automatically disconnected from UCSF Office of Research's network after TWENTY (20) minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 12 hours.
9. Users of computers that are not UCSF Office of Research -owned equipment must configure the equipment to comply with UCSF Office of Research's VPN and Network policies.
10. Only UCSF approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of UCSF Office of Research's network, and as such are subject to the same rules and regulations that apply to UCSF Office of Research-owned equipment, i.e., their machines must be configured to comply with UCSF's Security Policies.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
IPSec Concentrator	A device in which VPN connections are termin
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the UCSF network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a UCSF Office of Research-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into UCSF Office of Research and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Remote Access	Any access to UCSF Office of Research's UCSF network through a non-UCSF Office of Research controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-UCSF Office of Research network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into UCSF Office of Research's UCSF network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.