



Virtual Private Network Policy

CS Department Virtual Private Network (VPN) Policy

1.0 Purpose

The purpose of this policy is to provide guidelines for Remote Access IPsec or L2TP Virtual Private Network (VPN) connections to the SUNY Stony Brook CS department network.

2.0 Scope

This policy applies to all SUNY Stony Brook CS department users, employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the SUNY Stony Brook CS department network. This policy applies to implementations of VPN that are directed through an IPsec Concentrator.

3.0 Policy

Approved SUNY Stony Brook CS department users 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 users with VPN privileges to ensure that unauthorized users are not allowed access to SUNY Stony Brook CS department 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 such as SSH.
3. When actively connected to the CS department 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 SUNY Stony Brook CS department network operational group.
6. All computers connected to SUNY Stony Brook CS department internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the department standard (available from the CS department web site); this includes personal computers.
7. VPN users will be automatically disconnected from SUNY Stony Brook CS department's network after thirty 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 24 hours.
9. Users of computers that are not SUNY Stony Brook CS department-owned equipment must configure the equipment to comply with SUNY Stony Brook CS department's VPN and Network policies.
10. Only CS department systems staff-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are de facto extension of SUNY Stony Brook CS department's network, and as such are subject to the same rules and regulations that apply to SUNY Stony Brook CS department-owned equipment, i.e., their machines must be configured to comply with CS department Security Policies.

4.0 Enforcement

Any users found to have violated this policy may be subject to disciplinary action.

5.0 Definitions

| Term | Definition |
|--------------------|---|
| IPsec Concentrator | A device in which VPN connections are terminated. |

6.0 Revision History