Purpose

This policy prohibits network activities undertaken within a UCSF unit that may result in security risks or inappropriate use of the campus network and online resources. Examples of this type of activity include installation of modem pools, proxy servers or VPN gateways. This policy does not cover the installation of routers, switches, and other network devices that extend the internal network without providing external access.

Definitions

Router

A networking device that forwards data packets between computer networks.

Open Proxy

A proxy server that does not require users to be identified or authorized to use the proxy, although it does make them appear to be authorized users of the network hosting the proxy server.

Proxy Server

Also called a ?proxy? or ?application level gateway,? it is an application that breaks the connection between sender and receiver. All input is forwarded out a different port, closing a straight path between two networks and preventing someone from obtaining internal addresses and details of a private network.

Switch
A network device that selects a path or circuit for sending a unit of data to its next destination. A switch also may include the function of the router, a device or program that can determine the route specifying to which adjacent network point the data should be sent.

Policy

Units shall not install devices that allow access to the network if those devices compromise network security or otherwise allow inappropriate use of UCSF network resources. Units may install the following or similar devices to meet departmental operational requirements only after providing indicated basic registration information to IT Network Engineering:

- Proxy Servers other than Open Proxy Servers? Proxy servers must not be deployed to circumvent UCSF network and systems security policies. Units implementing proxy servers must describe their purpose and constituency to IT and provide a contact phone number.
- Remote Access Gateways (virtual private networking [VPN] or dial-up access)? Remote access to university systems for purposes such as system maintenance and monitoring must be password-protected and use multifactor authentication. Remote access gateways must not be deployed to circumvent UCSF network and systems security policies. Campus departments implementing remote access gateways must describe their purpose and constituency to IT and provide a contact phone number and email address.
- Other Gateways (NAT, T-1, etc.)? Gateways must not be deployed to circumvent UCSF network and systems security policies. Campus departments implementing network gateways must describe their purpose and constituency to IT Network Engineering and provide a contact phone number.
- Unsecured Wireless Access Points? Any access device on the campus network must be appropriately installed and configured to prevent unauthorized use of the campus network or computing resources.
- When UCSF IT Governance establishes policies for network border security through the IT Governance process, all entry points to the network must comply with those policies through implementation of firewalls or other access control methodologies.

Open proxy servers are not allowed on campus. IT will regularly monitor the campus for open proxies and notify the appropriate administrator if one is found.

Responsibilities

Contact Responsible Office (see above) with any questions.

References

- Wireless Networking and Security Standards [3]
- UCSF Information Technology [4]