SCinet 2005 Network Security Policy

The annual challenge for the SCinet committee is to provide a robust, scalable, production-quality network that meets the bandwidth requirements for a Conference devoted to showcasing leading-edge research. SCinet provides very high bandwidth connectivity between the show floor network and high-speed Agency and experimental Wide Area Networks. Due to the high bandwidth and large scale of the SC2005 network, SCinet does not provide firewall services.

There is no firewall at SC2005.

The SC2005 network is a logical extension of the open Internet. Any host on the Internet can connect to any machine on the show floor unless the machine's owners take the necessary steps to prevent unauthorized access. The Internet is a hostile environment where security is a collective responsibility.

Each Exhibitor is responsible for ensuring that their *systems* are configured in accordance with their security requirements.

Experience has shown that many of the systems used by Exhibitors at previous SCxy Conferences were configured in a default or standard manner. These default configurations often have well-known vulnerabilities for which freely available exploits exist. Exhibitors should ensure that the equipment they use at SC2005 has been patched and configured in accordance with the Original Equipment Manufacturer's (OEM) recommendations and the Exhibitor's security requirements.

Each Exhibitor is responsible for ensuring that their *communication sessions* are protected in accordance with their security requirements.

Exhibitors who use insecure communication methods are exposing their networks and systems to compromise. The use of insecure applications including TELNET and FTP is *strongly discouraged*. TELNET and FTP are subject to compromise because they send passwords to remote hosts in human readable cleartext. Exhibitors are *strongly encouraged* to protect their communication sessions through a mechanism such as Secure Shell (SSH) where all communication is encrypted. SSH implementations are widely available for little or no cost, and are straightforward to implement and use. Consult your system and network administration staff for more information on configuration and use of SSH.

SCinet will passively monitor traffic on most external network connections as part of their network performance monitoring activities. In addition, SCinet has a restricted capability to monitor Exhibit floor and external network traffic for evidence of security-related activity including compromise or abuse. However, by no means should this coverage be considered a substitute for safe security practices. Please do your part by being cognizant of network security risks and protecting your systems and sessions.