Windows Security
Port Blocking at the Campus Border

November 3, 2009

To address growing security concerns, certain types of Internet traffic into campus are only be allowed through a "Virtual Private Network" (VPN) connection. This requirement started Tuesday, November 18, 2003. The traffic being blocked is exploited by hackers to compromise Windows machines on ports 135-139, 445, and 593. These ports handle Windows DCOM "Remote Procedure Calls" (DCOM RPC), NetBIOS "Name", "Datagram", and "Session" services, Directory Services (Active Directory), and HTTP RPC services.

The traffic block affects Windows file and print sharing and any other program or process that uses Windows authentication. If you need to use these functions to connect to a campus computer from home or elsewhere off-campus, you need to install client software on your off-campus computer to make the connection. If you are simply browsing the ISU Web site, checking mail, or using most Telnet or FTP software programs you will not need to use a VPN connection.

Windows VPN client software (to create a VPN connection from an off-campus computer) is available (free of charge) to people with an ISU NetID. This software must be used in combination with your ISU NetID and password to connect to the on-campus network. Once a VPN connection is made your off-campus computer appears to be "on-campus". Traffic to and from campus is encrypted in a secure manner.

To acquire the Windows VPN client software go the Windows software download page at http://tech.its.iastate.edu/win2000/downloads/downloads.shtml