

## Summer IT Clean-Up and Security Improvement Controlling University Network Access

By Mitchell Ashley  
June 2006

Summer break is the busy season. Not for college students but for campus network administrators and security staff as most major network or security improvement projects are scheduled to occur over the summer months. Increasingly, implementing network access control, or NAC, is a major project initiative on campus networks.

NAC projects are occurring with such frequency because of previous costly experiences when students and sometimes faculty computers introduce an infection that compromises the network. Other intruders pose the threat of great loss of student and financial data. *The Houston Chronicle* reported in April 2006 that 106,000 University of Texas students, alumni and others had their names and Social Security number data stolen. Similarly, the University of Colorado suffered network break-ins at three campuses in 2005.

Gartner analyst Avivah Litan says, "Universities are the target of 30 to 35 percent of all data theft activity in the U.S." Litan cited that it is not unusual for universities to get attacked because of their open access policies and low security budgets.

With such an open network footprint and diverse user base, many campus security and network administrators are adding NAC to their security architecture.

### NAC History

Early 2004 and 2005 efforts to implement NAC achieved mixed results largely due to the shortage of experience in implementing fledgling NAC solutions and also the immaturity of many NAC technologies and products. Many early NAC products were originally vulnerability scanners, wireless gateways or network management systems. While these technologies continue to mature, many NAC solutions, as well as products that have been re-branded as NAC solutions, still rely on vulnerability scanners and overburdened personal firewall client technologies that were utilized in early NAC products.

**It's not practical to require every student, faculty and administrative staff computer to install and support a heavy agent such as a personal firewall.**

Today's state-of-the-art NAC solutions have changed significantly in the short time the NAC marketplace has been around. The mega-vendor NAC architectures, such as Cisco NAC

and Microsoft NAP, are still in the early maturation stages but a few of the well rounded, seasoned NAC solutions are easy-to-deploy, viable options in a campus network. Early education campus NAC implementations have taught us a lot. The freedom and flexibility desired in an educational environment, limited security staff, budget, the wide range of unmanaged end user devices, and the propensity of students' less than desirable network activity on a campus network can surpass the security challenges of many corporate networks.

So what are the key ingredients to a successful campus NAC implementation and how should network security staff go about selecting the appropriate NAC solution? Let's apply the lessons learned over the past few years.

---

### Agentless and Non-persistent Agents

It's not practical to require every student, faculty and administrative staff computer to install and support a heavy agent such as a personal firewall. IT network support staff resources are limited and supporting agents on students' computers adds a very heavy burden to this already scarce resource. Frankly, not all computers arriving on campus this Fall are created equal. Newly purchased machines may be able to run an agent but that fourth & fifth

year student's laptop may buckle under the weight of yet another startup memory resident application. The Windows Personal Firewall is now enabled by default beginning with Windows XP SP2 and installing a second firewall can cause compatibility issues or further burden the device.

Agentless NAC technologies, which performs a direct network connection to user's computer, are a very attractive option since no software is downloaded or installed. It also makes frequent re-testing of computers very easy. Non-persistent agents, such as ActiveX or Java based plug-ins, can also be an attractive option as the agent is downloaded at connection time and does not install or remain running on the user's computer.

If using an agent is an option, consider using a lightweight security posture agent (SPA), one whose primary function is to quickly assess the security posture of the computer. SPAs tend to be much smaller in size and don't entangle themselves in the TCP network stack or system software, reducing the frequency of compatibility issues, performance problems and system crashes.

### Typical Security Requirements

There are typical key requirements campus security staff want most end user computers to comply with. These include: Anti-virus, operating system (OS) updates, automatic update, and restricted software. It's usually

mandated that anti-virus software, school or student supplied, be updated with the latest virus definitions. Ensuring computers have all the latest operating system and security patches is important as well. For computers to continue to stay-up-to date with patches, Windows Automatic Update must be enabled. There may be restrictions on music, file sharing and peer-to-peer applications. Don't forget about that rogue piece of software developed by some enterprising computer science student during the mid-year that you would like banned from the network.

Windows Vista and its many retail and business configurations is available for download as beta and is scheduled to be available sometime during late 2006, early 2007. This will introduce a new OS platform with new security wrinkles that should be ironed out by any implemented NAC solution.

### Residential, Faculty and Administrative Networks

Implementing NAC isn't just for students. A threat to the network can just as easily come from a faculty or administrative staff member who unknowingly introduces a worm or piece of malware into the network from behind the firewall. The implemented NAC solution will need to meet the requirements of the residential, faculty and administrative networks and their respective unique architectures and technologies. This may require that the NAC solution support multiple deployment options.

### Achieving NAC Success

Keeping these factors in mind when planning and implementing a NAC solution will make a significant difference in the resulting effectiveness. NAC by its very nature is about

improving the security not of just one element of the network but a very large number of end user devices across multiple networks. Putting programs and processes in place to bring end user devices into compliance will significantly ease the transition to a more secure network.

Also consider phasing in the requirements over a period of time. Begin by requiring anti-virus software and up-to-date OS patches during the first week students arrive on campus. Phase in other security requirements over time as you have the support processes, documentation and remove tools in place. Use NAC not only to enforce network security policies but also to examine device compliance against new security policies you are considering.

NAC offers very significant benefits to education campus networks which can be the most challenging to secure. The past few years of experience with NAC provides everyone a larger experience base to help ensure its successful implementation.

---

*Mitchell Ashley is CTO and VP of Customer Experience at StillSecure where he is responsible for the product strategy and development of the StillSecure suite of network security products. Mr. Ashley has more than 20 years of industry experience holding leading positions in data networking, network security, and software product and services development. Mr. Ashley can be reached at [mashley@stillsecure.com](mailto:mashley@stillsecure.com) or 303-381-3830.*