Network Access Control (NAC) is the process of controlling users’ and device access to the network. Because of increased employee mobility and the growing number of end-user network-capable devices, tracking and controlling network access has become essential to maintaining data security in corporate networks.

In January 2006, Infonetics Research released the results of a study suggesting a significant growth of the NAC market (an 11-fold increase predicted from 2005 to 2008). Their press release describes NAC as follows: “Network access control, or NAC, is considered the holy grail of network security, as it is an intelligent network infrastructure that can identify users, identify and do integrity checks on the computers they are using, and then grant them access to specific locations and/or resources and set policies based on user and machine identity.”

Tim Greene wrote in _Network World_ at the beginning of May that NAC products would be highly visible at Interop Las Vegas. Greene wrote, “Infonetics breaks NAC designs into three components: clients that check end devices for compliance, enforcement points that impose policies and back-end servers that dictate policies to the enforcement points. NAC identifies and authenticates users and machines, ensures machines meet security policies, sets policies based on user and machine status, and grants access to specified resources. An Infonetics survey recognizes Cisco's Network Admission Control, Microsoft's Network Access Protection (NAP) and the Trusted Computing Group (TCG) consortium's Trusted Network Connect as the three NAC schemes best known among IT executives.”

Richard Kagan is Vice President of Marketing at Infoblox, a firm that delivers network infrastructure essential for any NAC deployment scheme; he recently sent me a brief summary of key issues underlying NAC for network architects and security personnel. The following is a lightly-edited version of his comments.

---

What NAC solution is best for your organization? Stand-alone security applications? 802.1x? Cisco? Microsoft? End-point security is critically important and must take into account the following requirements:

- Networks are largely operating anonymously, with IT departments having limited awareness or control over how the network is being used or by whom.
- Increasingly strict regulatory pressures and security concerns are forcing organizations to establish identity-driven networks which require more control over user access and devices, and in turn, better monitoring of network data.
NAC solutions must be able to interact with gear from multiple vendors and systems. Ideally, NAC solutions should not require an infrastructure overhaul.

Network identity services such as Dynamic Host Configuration Protocol (DHCP) are essential to any NAC solution.

DHCP is the method used in all Internet Protocol (IP) networks for automatically assigning the IP address for networked devices. Address acquisition is the first step for access over IP, so DHCP is a must for any NAC implementation. NAC solutions must link the DHCP server to the network to enable authorized access; otherwise, IP addresses would be provided to all requesting devices. Consequently, the NAC solution you deploy must have a robust DHCP infrastructure that enables today’s advanced services such as voice over IP (VoIP) and wireless applications to support an increasingly mobile workforce.

It is not yet clear which NAC solutions will be the most widely accepted; however, it is clear that all solutions will require a solid DHCP foundation. Here is what to look for:

- Out-of-the-box support for basic device and user authentication;
- Easy integration with client-based and clientless end-point scanning, remediation and threat mitigation systems;
- Ability to link users, device Media Access Control (MAC) addresses, IP addresses and host names;
- Ubiquitous networking equipment vendor support;
- Using existing directory stores and user credentials without additional provisioning.

For more information about essential network identity services, including DHCP, Domain Name Service (DNS) and Remote Authentication Dial-In User Service (RADIUS), visit <http://www.infoblox.com/library/whitepapers_confirm.cfm>.

[Disclaimer from MK: I have no financial relations whatever with any of the vendors named in the article above and mentioning their products or services implies no endorsement.]

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www2.norwich.edu/mkabay/www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay & Richard Kagan. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.