



Fast Brief:

Is It Time for NAC 2.0?

Why the way NAC was being implemented could never work, and a more effective solution for system protection.

August, 2009 saw the closure of NAC pioneer ConSentry Networks. This announcement came on the heels of a difficult year for the industry which saw closures and/or major restructuring for a number of vendors in the industry including Nevis Networks, Autonomic Networks and Lockdown Networks. We believe that at this point it is worth looking at what NAC was meant to accomplish, critique the approaches used, and ask whether there might be a better way.

What is NAC?

Analyst firm Gartner has defined Network Access Control (NAC) as a process and an architecture for implementing three critical security functions. These include:

1. Noticing whenever something is connected to your network, determining if it is one of your devices or not, and if it is one of your users or not.
2. Determining the security status of the device connecting to your network.
3. Given (1) and (2) deciding what to do.

Clearly, the value of being able to reliably execute these functions on an enterprise network provides value for securing critical systems and data. In fact, despite an abysmal year for technology, Gartner estimated that NAC spending was \$220M in 2008, over a 50% increase over spending in the previous year.

What are the problems with NAC?

Many early NAC implementations were effectively guest networking solutions, designed to provide access to limited segments of the enterprise network to visitors, contractors, or students. Network protection was introduced as a simple “scan and block” approach, where a system with unauthorized or outdated software would not be allowed on the network. This effectively penalized users who haven’t received the latest build from central IT. On the management side, NAC implementations lacked the necessary management tools for baselining, determining which applications were in use, and formulating appropriate security policies. This “all or nothing” approach to managing access allowed little room for allowing enterprises to balance network risks with productivity.

The need for a better approach

Ironically, the need for what NAC promised to provide

has never been greater. Extended enterprises, remote access and regulatory compliance have contributed to the urgency for a system protection solution which can work with existing networks and applications. Security concerns around virtualization and cloud computing will only add to this. In this regard, one question planners should ask themselves is, “If NAC did not work on the real network, why is it going to work now on the virtual network?”

So how can this security vision be realized? Layer 2 approaches to network security have been tried for decades and have failed to live up to their early hype. Protocols at layers 3 and 4 (where TCP/IP resides) are too well established to warrant a wide-scale upgrade. Layer 7 (Application Layer) solutions require reengineering existing systems and applications.

Time for NAC 2.0

At Applied Identity, we believe it is time to define NAC 2.0, where the network has evolved to include **user identity and application trust in the packet**. To that end, Applied Identity’s Identisphere provides the only non-intrusive solution for system protection based on packet water marking at the network edge. The Identisphere solution effectively works between layers 2 and 3 to transparently apply access policies independent of user access mode, network infrastructure or the applications being accessed.

Identisphere solves the problem of the “all-or-nothing” approach to network admission presented by traditional NAC implementations. With Identisphere, managers have the ability to define and enforce granular policies based on which users are accessing networked applications, the clients they are using to access them, and the degree of trust they associate with each access request. The result is more effective risk management without disrupting the business.