From: www.cio.com

Network Access Control: Deploy Now or Wait?

– Karen D. Schwartz, CIO

August 13, 2008

Network Access Control (NAC) sounds like something of a panacea—: technology that can not only authenticate who is using your company's network, but also ensure that users' methods of access are virus-free and fully comply with your company's corporate security policies. And NAC has been getting a lot of press lately—proponents tout its ability to keep corporate networks clean and healthy in ways that technologies of the past couldn't.

As technologies like virtual private networks (VPNs), Ppersonal Digital digital Assistants assistants (PDAs) and wireless technologies proliferate, the situation at many companies has become untenable.

Enter NAC. Many companies are beginning to see the technology as an answer to the network access problem, especially for guest or contractor access, but also for remote and wireless users.

"If you have a business partner visiting who needs Internet access to do a demo or a contractor temporarily working in your offices, you want to be able to provide them with network access, but without potentially introducing malicious programs they might have running on their systems to the network or giving them access to the entire network," explains Paul Roberts, senior analyst for enterprise security at The 451 Group of New York. "NAC provides a way to ensure that when they connect to your company's network, they are who they say they are, their systems are up to date, and they aren't infected with anything."

But it's far from a perfect technology. Not only is it still maturing, but there are several competing factions and little in the way of industry standards, leading some to wonder if it might make sense to wait.

Every company doesn't need it today, says Joel Snyder, senior partner at Opus One, a consulting firm in Tucson, Ariz. However, you should strongly consider it if you are worried about the authentication of people using your network, if you are concerned about the status of endpoint security on your systems, or if you need stronger, more granular access controls at the user level.

But there are signs that companies are ready to adopt the technology. According to a February, 2008 report from The 451 Group, enterprises are now ready to deploy NAC technology due to compliance issues, the need to lock down guest access and threat of data loss.

"It's definitely maturing," says Andrew Braunberg, research director for enterprise software and security at Current Analysis of Sterling, Va. "Major players like Cisco and Trusted Computing Group have realized that they have to play nice with Microsoft, so they now have interoperability agreements with Microsoft. That's just one example of how interoperability issues are being worked out. But it will take

some more time.

A Confusing Proposition

NAC technology has grown in fits and starts since around 2001. Cisco was first out of the gate with technology that allowed companies to vet systems prior to admitting them to a network. Its technology resides in the switching and routing infrastructure. Others soon followed. One of those was Microsoft, which took a different approach by adding the technology to the operating system layer, via its Network Access Protection (NAP) offering. Other pureplay vendors have since joined the fray, including Forescout, Mirage Networks, Bradford Networks and Vernier Networks.

To make matters more confusing, each of these vendors comes at NAC in different ways. But to boil it down, there are basically two options: Inin-Band band and Outout-of-Bandband. In-Band band (sometimes called Inin-Lineline) systems are installed between users and the rest of the network; that is, between access layer switches and core switches. This method prevents systems that don't comply with company policies from entering the network. Examples include Edgewall from Vernier Networks, LANenforcer from Nevis Networks and LANShield Controller from ConSentry Networks.

In-Band band systems are good choice when companies are forced to allow machines of unknown origin to connect to their network, says John Pescatore, a vice president at Gartner.

"When a contractor machine connects, he might have software you don't like, but you can't tell the contractor to delete the software from his company PC. But if you had something in-line between the contractor and the network and the contractor started sending out dangerous things, you could just block it."

The other option is out-of-band NAC. These products, which use the existing network architecture, allow networks to communicate with the switching infrastructure and block things anywhere on the network. That's especially useful for complicated network architectures, Pescatore says. Vendors with out-of-band NAC options include Mirage Networks and Bradford Networks.

Which way you go, and which vendor you settle on, will depend on several factors. The first step, Roberts says, is determining your immediate needs. Based on the answer, you'll know whether you need to deploy NAC now or later, and you'll know whether to consider an in-line or out-of-band solution.

The next step is looking at your existing vendors to see if that vendor has a compatible NAC solution. If you're a pure Cisco shop, for example, it would make sense to go with Cisco's Network Admission Control (C-NAC). Similarly, if you are planning to upgrade to Microsoft Vista or Longhorn soon, you should strongly consider Microsoft's NAS solution.

Heterogeneous environments are probably better off with a pureplay vendor, Pescatore says. Yet another option might be Trusted Computing Group's Trusted Network Connect (TNC), which was developed using open standards.

But whether you choose to wait or move forward, chances are that your company will be using some type of NAC solution before too long. According to Gartner, the NAC market reached $225 million last year and is expected to grow to $440 million by the end of 2008. Growth will continue until 2010, when it is expected to reach $700 million, and flatten after that as NAC becomes more of a standard offering in all types of technology.