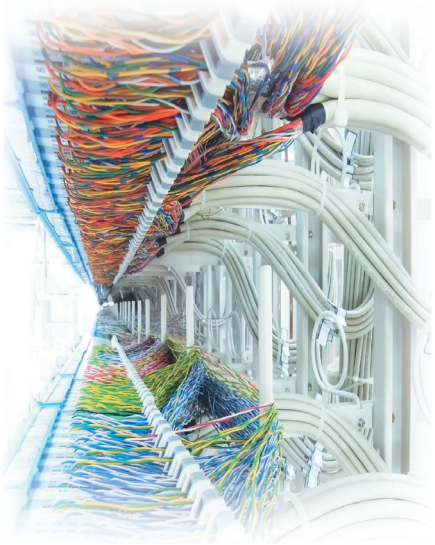
Whatever Happened to Network-Access-Control Technology?



David Geer

Although vendors developed network-access-control technology to cope with the threats organizations face from within their networks, NAC has not been as widely adopted as experts predicted.

Organizations face complex threats while providing network access for customers, vendors, mobile employees, contractors, and others.

Many organizations see these inside threats as a top network-security challenge, one unmet by products such as firewalls and antivirus software.

In response, security vendors developed network-access-control technology.

NAC systems authenticate devices trying to connect to a network and evaluate whether they have updated security software, patches, and other safety measures in place, explained University of Tulsa associate professor Mauricio Papa.

They then dynamically provision or don't provision network access to users based on the host organization's security policies.

Not long ago, experts said the need was so great that NAC would sweep the market. However, that hasn't happened. Vendors aren't seeing the revenue or growth that was predicted, according to analyst Chris Rodriguez with the Frost & Sullivan market research firm.

"Agreement on what NAC even means and the right approach remains as elusive today as in 2006, when the first products burst on the scene," said Alan Shimel, CEO of The CISO Group, which offers security consulting and management, on-site support, and regulatory-compliance services.

Also, some NAC vendors emphasize their security strengths or target corporate or other specific types of customers, said Alan White, director for information-security consulting with service provider SecureWorks. This causes the various NAC products to look and act differently, creating confusion over what NAC is.

Vendors are using their own technologies to differentiate themselves from competitors, hoping their proprietary approaches will become de facto standards, White explained.

With all these differences, said Cisco Systems security solutions manager Bill McGee, "you [often] can't get two systems to communicate with each other."

Despite the challenges, proponents contend that vendors and standards bodies eventually will solve the problems NAC faces and that the technology's future will be bright.

A LOOK AT NAC

The first NAC product was Bradford Networks' Campus Manager, released in 2003.

Products

Today's products include Avenda System's eTIPS, Black Box's VeriNAC appliance, Bradford Networks' Network Sentry, Check Point Software Technologies' NAC, Cisco's Clean Access appliance, Enterasys Networks' Network Access Control, ForeScout Technologies' CounterACT, Hewlett-Packard's ProCurve Identity Driven Manager, Impulse Point's Safe Connect NAC, InfoExpress' CyberGateKeeper, Insightix's BSA Network Access Control, Juniper Networks' Unified Access Control, McAfee's N-450 NAC Appliance, Microsoft's Network Access Protection, NetClarity's NACwall, Sophos' NAC Advanced, StillSecure's Safe Access, Symantec's Network Access Control, and Trustwave's NAC.

0018-9162/10/$26.00 © 2010 IEEE Published by the IEEE Computer Society

Frameworks

There are four NAC frameworks, which are sets of standards and/or technical requirements that let collections of compliant components, products, and software interoperate to provide NAC services.

Cisco calls its framework Trusted Security or TrustSec. TrustSec works within an organization's existing Cisco-based network infrastructure, said Frost & Sullivan's Rodriguez.

The Internet Engineering Task Force (IETF) has developed its Network Endpoint Assessment framework, which enables NEA-compliant equipment from different vendors to interoperate.

Microsoft's Network Access Protection is a software framework that hardware vendors can implement. NAP works with different types of hardware, software, or operating systems.

"It is both a set of embedded tools [in Windows] and a … framework capable of interrogating an end-point device for varying levels of [security-policy] compliance and communicating that information to a centralized policy server," explained Avaya product manager Dale O'Grady.

The Trusted Computing Group (TCG)—an organization that develops and promotes open, vendor-neutral standards—has developed the Trusted Network Connect (TNC) framework. This cross-platform approach—which can be implemented in software, hardware, firmware, or a combination of these elements—provides end-point analysis, user authentication, network-activity monitoring, and the implementation of network-access rules.

The IETF and TCG have designed their frameworks to work with each other, which enables equipment compliant with either approach to interoperate.

Threats

For several years, a growing number of organizations have let employees use their personal laptops or smart phones at work or use their company-supplied mobile devices outside the office, noted Steve Hanna, a Juniper Networks Distinguished Engineer and cochair of both the TCG's TNC Working Group and the IETF's NEA Working Group.

Devices' security-related problems can enable hackers to break into systems or let malware move onto an organization's network, said Arthur Hedge, president of Castle Ventures, which provides security and other IT-related services.

Organizations sometimes give employees remote access to the corporate network, or they give contractors or some guests limited access. This creates potentially serious threats to network security.

NAC provides authentication, end-point security checking, access control, and behavior monitoring.

How NACs work

NAC provides authentication, end-point security checking, access control, and behavior monitoring, according to Hanna.

The technology also provides user-access tracking services, noted Hedge.

In essence, NAC systems determine who is trying to connect to a corporate network and whether a user can be admitted safely. The products then deny or limit admittance when necessary, and discontinue access for policy violations.

Policy decision points, the brains of the system, are located at a central node such as an authentication server, as Figure 1 shows. A PDP can be hardware or software. It uses authentication and security-assessment information to decide which users and devices should get what level of network access, based on an organization's policies.

The PDPs work with the Remote Authentication Dial-In User Service standard, said Eric Stinson, Enterasys' director for NAC product management. RADIUS provides centralized authentication and authorization for computers trying to connect to and use network services.

Devices request access to a network via *policy enforcement points*, the switches, firewalls, and other parts of the network that prevent or allow access based on decisions made by the PDPs.

To work with NAC systems, the connecting devices must have either installed agent software or temporary agents that the system pushes through the network to them upon connection, according to Jason Nadeau, director of product management for Symantec's end point security business.

The agents analyze the connecting device and tell the NAC system whether it has the appropriate security software installed and updated.

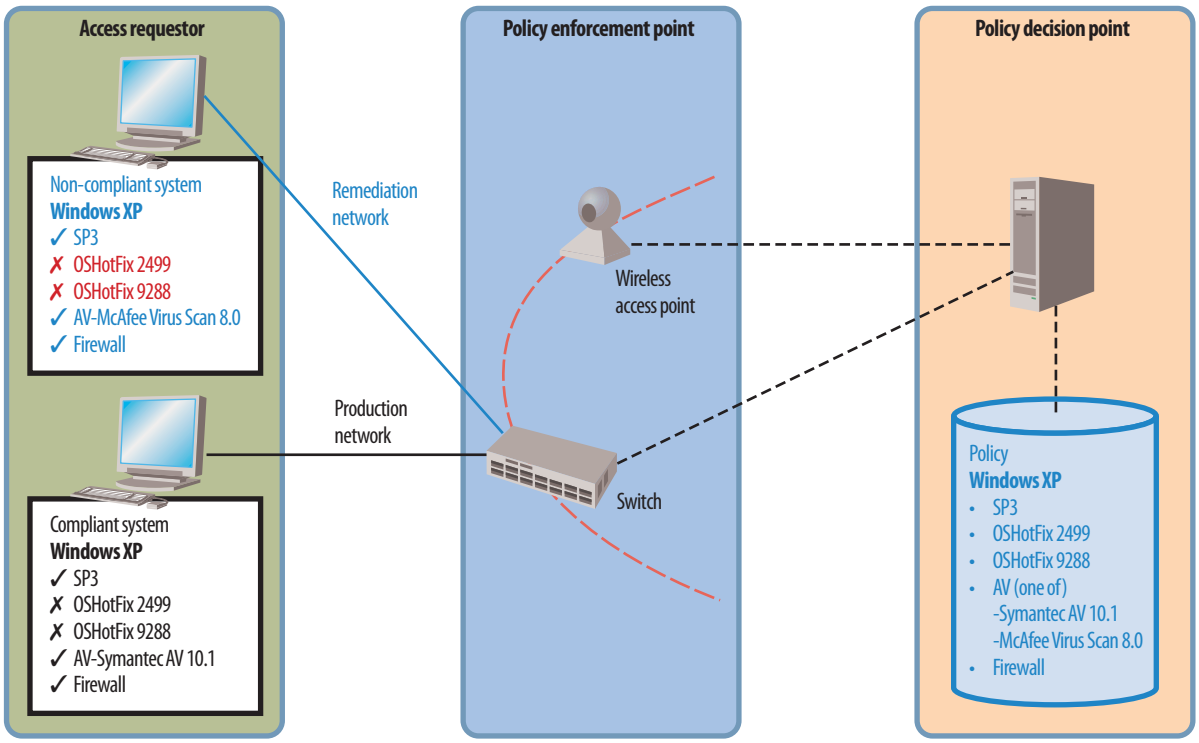
The NAC system then decides to which of the network's virtual LANs it will direct the end point, based on whether the device needs security remediation, Internet access only, or limited corporate-network access.

Many of today's systems can use agents to monitor connected devices on an ongoing basis, to determine whether they incur problems that justify changing their access rights.

Implementation

Initially, most NAC systems were implemented as appliances that attached to the network. Typically, the appliances were hardened PCs using network interface cards and proprietary NAC-related software.

During the past two years, vendors have integrated NAC functionality within the network and security



Source: Trusted Computing Group

Figure 1. In this highly simplified network-access-control system, the access requestor (AR) is a device trying to connect to the network. The policy enforcement point (PEP) enforces network-access policies, which the policy decision point manages. The host organization's network-access policy—which states what security-related characteristics the AR must have—is stored in the PDP. The PDP analyzes the AR and determines whether it complies with the policy. If so, the PEP grants access. If not, it sends the device for remediation.

infrastructures.

Appliances offer quicker implementation but don't scale as well as the embedded approach.

Some organizations are starting their NAC adoption by implementing the technology in limited deployments, such as just for wireless or guest access to networks, which represent particularly difficult security challenges.

NO KNACK FOR NAC

For several reasons, NAC deployment has been considerably lower than many vendors hoped for and many industry observers expected.

Noted the University of Tulsa's Papa, the IETF is still working on the adoption of some of its NEA-related standards. If the IETF had ratified standards sooner, he said, more vendors would be adopting the standards and more products would be interoperable, encouraging greater NAC deployment.

Reasons for not adopting NAC

Customer confusion about NAC has contributed to lower-than-expected adoption. "Vendors try to offer all kinds of solutions to meet real and perceived customer needs. The result is that no one knows what NAC is, and NAC vendors are clearly not offering the same set of functionality in their products," said Alan DeKok, cofounder and chief technical officer of vendor Mancala Networks and chair of the IETF's Extensible Authentication Protocol Working Group.

NAC frequently requires organizations to buy new hardware—such as appliances, servers, or switches—and perform costly and time-consuming system configurations, he noted.

"Organizations haven't adopted NAC because managing the new systems is too complicated," he added.

For example, some companies create network-access policies but don't update them as applications are added, new protocols are implemented, or other conditions change. This leaves them vulnerable despite having NAC systems.

Regular updates could require ongoing rewriting and reapplication of policies, which could be time-consuming and expensive.

NAC products can also be complex to deploy and operate. Some systems are inflexible, requiring all network elements to change radically to accommodate them, according to Juniper Networks' Hanna.

"The biggest issue making NAC products difficult to deploy is that everybody's network is unique. Deploying NAC with best practices from one network does not [necessar-

ily] work on the next network," said The CISO Group's Shimel.

When elements that network-access control relies on—such as authentication servers and antivirus software—experience problems, this affects NAC systems.

For the systems to work, many hardware components must interoperate. If even some of them don't, the NAC system might fail.

NAC products change regularly, as do the network components they work with, noted Jennifer Jabbusch, network security engineer and consultant with Carolina Advanced Digital, an IT service provider. The failure to update NAC systems promptly can cause stability problems, she explained.

Interoperability issues

Interoperability among NAC-related network elements would encourage greater adoption and enable users to choose the components they want in their systems.

Products from the same vendor or that work within the same framework already interoperate.

"The TCG just announced a TNC certification program, certifying products that are compatible with TNC," said Juniper's Hanna.

However, stated Frost & Sullivan's Rodriguez, "There are stand-alone products that are not based on the various NAC frameworks, and they don't interoperate with one another."

"If you have a Cisco-only network, Cisco NAC probably works well there. But if you start introducing other vendors' [products], Cisco NAC doesn't work so well," noted The CISO Group's Shimel.

Some vendors build their NAC systems to work with only certain security products. This can cause interoperability problems in networks that don't use those products.

And some NAC and network infrastructures don't interoperate. For example, NAC systems that rely on RADIUS won't operate with network components that don't work with the technology.

According to Eric Cole, a senior vice president and chief technology officer for the Americas with security vendor McAfee, "High cost is becoming less of a factor in NAC deployment. In the past, organizations didn't understand NAC's return on investment. Now, they are seeing a benefit to justify costs."

As NAC becomes more embedded in the network infrastructure and integrated into network-management products, the technology will seem less like an additional expense and its purchase will become easier to justify, stated Seth Goldhammer, Hewlett-Packard Tipping Point's product manager.

NAC will become more widely adopted because of the emergence and increasing vendor implementation of the IEEE 802.1X authentication standard, with which network-access-control systems work, said Symantec's Nadeau.

"Cisco and Juniper have bought [NAC-related companies] and integrated them into their product portfolios, so there are now more integrated solutions from vendors that customers already do business with," said principal analyst Ted Julian with the Yankee Group, a market research firm.

NAC will also benefit from its new constant-monitoring capabilities, which will catch problems before they have time to cause damage, said Cole.

Increased governmental network-security regulation will encourage NAC adoption, added Cisco's McGee.

However, said Mancala Networks' DeKok, "NAC's future is still uncertain. Vendors and customers need to agree on a clear and consistent definition of NAC. Until then, customers don't understand what the vendors are selling, so they don't know what to buy."

"Perhaps the greatest risk to NAC adoption is that the buzz is gone," stated Julian. "Enterprising security pros are likely to get far greater exposure with projects involving compliance, cloud security, mobile security, and application security."

Nonetheless, said Cole, "as things progress, NAC will become the true traffic cop on your network."

David Geer *is a freelance technology writer based in Ashtabula, Ohio. Contact him at david@geercom.com*

Editor: Lee Garber, *Computer*; l.garber@computer.org

Engineering and Applying the Internet

IEEE Internet Computing

IEEE Internet Computing reports emerging tools, technologies, and applications implemented through the Internet to support a worldwide computing environment.

For submission information and author guidelines, please visit www.computer.org/internet/author.htm