Understanding Network Access Control (NAC) Standards
Before you select a NAC solution, it’s important to understand the strengths and weaknesses of the top emerging NAC frameworks.

Network access control (NAC) is currently receiving a great deal of attention in the network security arena. Organizations are deploying NAC solutions in increasing numbers, with manufacturer revenue for NAC enforcement expected to more than double between 2008 and 2011, from US$1.8 billion to US$3.8 billion.† To bring a degree of control and interoperability to this dynamic and rapidly evolving market, a number of high-profile players are developing and promoting various NAC standards.

Making sense of these standards—and choosing the best NAC approach for your organization—can be a difficult and confusing process in today’s marketplace. The recent development of new NAC technologies has made it challenging to understand the NAC landscape and make sound decisions. To make matters even more complicated, several new software companies have joined the fray and attempted to redefine the space, making it difficult to even find an accurate working definition for NAC. As a result, solutions marketed under the NAC banner can include everything from repurposed personal firewalls and dressed up vulnerability scanners, to purpose-built solutions that are designed from the ground up to solve network access control challenges.

In the simplest terms, NAC solutions deny or limit access to the network if a device violates a policy. These policies can be based on a user’s identity, a preconnect endpoint health check or post-connect behavior. Endpoints that pass the tests and prove their compliance are given access, while potentially harmful endpoints—those that do not comply with established security policies—are denied access or quarantined to segments of the network where they cannot inflict harm.

NAC is an efficient, highly effective way to protect the network, given that endpoints and their often unwitting owners have become primary targets for exploitation by hackers and others with malicious intentions. In fact, according to PricewaterhouseCoopers, a full 61 percent of security incidents originate inside corporate networks.

NAC systems tend to be more complex than other security tools. They must be embedded and function within the network infrastructure. On the endpoint testing side, they have to accommodate a range of different managed and unmanaged devices, operating systems and connections. And on the enforcement side, a variety of interactions need to occur among user directories, domains, policy servers, posture assessment servers, routers, switches and other network infrastructure components.

Leading NAC Frameworks

In response to the complexity and variety of today’s NAC solutions and approaches, vendors such as Microsoft and Cisco—along with a number of industry consortiums—are promoting specific NAC “frameworks.” These are essentially interoperable standards that attempt to bring a level of uniformity and conformity to the landscape. In theory, these efforts should allow vendors of NAC and NAC-related solutions to develop products that are interoperable. However, some believe that moving toward a single standard may lock organizations into a big-company, single-vendor model that stifles innovation and limits functionality.

Before you select a NAC solution, it’s important to understand the strengths and weaknesses of the top emerging NAC frameworks. Today, these include Cisco’s CNAC architecture, Microsoft’s NAP initiative and the...
None of these standards has emerged as a clear industry leader, and there is evidence that two or more of them may actually inter-operate with each other. Given this lack of a single leading framework, which one—if any—should you choose? And how can you make sure the NAC solution you deploy today will work with tomorrow’s framework-compliant infrastructure components? To help answer these questions, this paper will take a closer look at all frameworks and summarize the pros and cons of each one.

Cisco* NAC

The Cisco Network Admission Control (CNAC) framework is a hardware-centric approach that leverages Cisco networking components to test and enforce compliance. The biggest drawback of the CNAC framework is that it requires a homogeneous Cisco environment to work effectively. With CNAC, each endpoint must have the Cisco Trust Agent (CTA) installed. This agent reports the endpoint’s health posture to Cisco’s Access Control Server, which integrates with other Cisco components (such as routers, VPNs and switches) to allow, deny or limit the endpoint’s access.

While CNAC is a viable option for an all-Cisco environment, implementation can be quite complex. Furthermore, CNAC is not supported on older Cisco infrastructure components, so additional hardware upgrades may be required to fully implement CNAC functionality. Non-supported devices that do not have the CTA installed also present a problem for a CNAC framework. It’s possible to perform some limited vulnerability scanning on unmanaged devices, but it’s a less than optimal solution. This weakness, combined with the Cisco-only requirement, has forced Cisco to adopt a dual NAC strategy in the form of a separate NAC appliance that is based on acquired technology. However, this separate appliance is not necessarily CNAC compliant.

Cisco has an extensive CNAC partner program that includes dozens of security software vendors. The purpose of these partnerships is to enable CNAC to compile data from a wide range of security tools when determining an endpoint’s health posture. For example, CNAC is capable of working with any of about two dozen antivirus solutions. Thorough testing requires that the Cisco Trust Agent be able to “poll” each of these antivirus tools, depending on which is installed on a given endpoint. Cisco has chosen to make partner vendors responsible for ensuring that their products integrate with the appropriate CNAC components. Cisco seeks to use its position in the market to dictate terms to partners, but this leaves them vulnerable to vendors who may not want to march to the beat of the Cisco drum. As a result, CNAC users could find themselves vulnerable if their current antivirus, antispyware or firewall vendors are not CNAC compliant. In these situations, organizations are left with the unenviable choice of either moving to a security tool that supports CNAC or living with holes in their NAC coverage.

Microsoft* NAP

While CNAC is a hardware-based NAC framework, Microsoft NAP (which stands for Network Access Protection) is primarily an infrastructure-neutral, software-based solution that can provide NAC functionality across heterogeneous network infrastructures. The Microsoft NAP framework provides native support for Windows Vista*, XP and Windows Server*, which means any endpoint running Vista or XP will automatically be NAP enabled.

On the network side, NAP consists of network policy servers that integrate with Active Directory*. The NAP system then leverages existing infrastructure components (such as 802.1X switches, firewalls, VPN and IPsec) to keep noncompliant endpoints off the network. Like Cisco, Microsoft has an extensive partner program to facilitate thorough endpoint testing and health checks, but it’s
On paper, this collaboration seems to hold a great deal of potential, but industry watchers are withholding judgment until the architecture is proven in production environments.

the same double-edged sword—there may be holes in coverage if security vendors choose not to become NAP partners. Like Cisco, Microsoft—because of its dominant position—will likely succeed in getting security vendors to tow the NAP line.

NAC and NAP Interoperability Architecture

In September 2006, Cisco and Microsoft announced a working demonstration of their previously announced joint effort to support each other’s NAC frameworks. The joint NAC and NAP interoperability architecture combines Cisco’s hardware enforcement and support with Microsoft’s Windows and common identity management systems. Interoperability between the two frameworks eliminates certain redundancies. For example, the Microsoft NAP agent, which is natively embedded in the Vista OS, eliminates the need for the Cisco Trust Agent. Also, partner integration will occur through the NAP APIs.

On paper, this collaboration seems to hold a great deal of potential, but industry watchers are withholding judgment until the architecture is proven in production environments. Getting two companies of this stature, both of which are used to doing things their own way, to collaborate effectively on a relatively complex technology like NAC presents obvious challenges.

Trusted Computing Group’s Trusted Network Connect (TNC)

Trusted Network Connect, or TNC, is the NAC framework being developed by the Trusted Computing Group. Trusted Computing Group is a consortium of security software developers dedicated to creating vendor-neutral industry standards for NAC components and communications. More than 70 vendors are participating in the TNC effort, including IBM, HP, Extreme Networks, Juniper, Nortel, Symantec and even Microsoft. Cisco is conspicuously absent from this collection of industry powerhouses.

The TNC’s goal is to create a vendor-neutral set of NAC standards and APIs. The standard will specify the data formats and communication protocols for a complete, end-to-end NAC system. In theory, any vendor that develops to the standard can integrate its product with any other compliant product. It would then be feasible to implement a multi-vendor NAC solution, where each component is provided by a different vendor. For example, company A’s endpoint testing agent would work with company B’s policy server, and company C’s antispyware product would integrate easily with company D’s posture server.

The TNC standard offers organizations considerable flexibility as technology evolves over time. If, down the road, a vendor develops a policy server that’s ideal for your environment, you’ll be able to deploy it without having to replace the entire NAC system.

TNC’s vendor-neutral approach has considerable appeal. Widespread adoption of the TNC standard will depend on deployments in actual production environments, where interoperability among NAC components from multiple vendors can be proven. With competing frameworks from heavyweights Microsoft and Cisco, TNC will face challenges as it works to build confidence and awareness in the marketplace. TNC will also face competition from the NAC standard development effort recently launched by the Internet Engineering Task Force (IETF) Network Endpoint Assessment Group (NEA), which is jumping into the game a bit late, but which has a high level of vendor participation, including support from Cisco and Microsoft.
Purchasing NAC Today

If you are planning to deploy a NAC solution in the near future, it’s important to decide how you will approach these competing frameworks. How big a factor should framework support be in your decision? Can you safely select a NAC solution today without having it become obsolete two, three or five years from now?

The right framework—and choosing the right vendor—is largely dependent on your environment and security needs. Some of the questions you’ll need to consider include:

- Are you an all-Cisco environment?
- Is your infrastructure up to date, or do you have a patchwork of vendors and technologies?
- Is your network environment heterogeneous or homogeneous?
- Who are your end users? Do you frequently provide access to visitors, contractors and other “untrusted” endpoints?
- Are your endpoints all Windows devices, or do you have to accommodate Mac* and Linux* machines as well?
- How thoroughly do you need to test endpoints? Is checking for OS service packs and current antivirus data files sufficient, or do you want to perform a more in-depth endpoint evaluation?
- Will the answers to these questions change over time? Is your environment static—or will your NAC solution need the flexibility to function in a dynamic environment?

Answering these questions may point you in the direction of a particular NAC framework. The dozen or so primary NAC vendors typically advertise which framework(s) they support.

A logical approach would be to consider a solution, such as Novell® ZENworks® Network Access Control, that has been developed to interoperate with all of the primary frameworks. This essentially allows you to hedge your bets. You benefit today from the improved security a NAC solution provides, but you’re assured that if and when one of the frameworks emerges as the leader, your NAC system will fully support it.

Novell ZENworks Network Access Control: A Framework Neutral Solution

Novell ZENworks Network Access Control is designed for flexibility, and it offers the widest possible range of endpoint testing, enforcement and interoperability options by embracing all of the emerging NAC standards.

Novell is a member of the TNC, and ZENworks Network Access Control fully supports the TNC framework. The similarities between the ZENworks Network Access Control and TNC architectures actually make it easier for Novell to implement the TNC specification.

Novell is also a Microsoft NAP partner. The support that ZENworks Network Access Control has for NAP expands your enforcement options by providing expanded support for DHCP, VPN, 802.1X and IPsec.

Finally, Novell ZENworks Network Access Control supports Cisco’s CNAC framework. The flexible ZENworks architecture allows it to function seamlessly in Cisco environments and extend CNAC’s endpoint testing capabilities by providing deeper policy definition and multiple testing and enforcement options. Using ZENworks Network Access Control in conjunction with the NAC/NAP framework can also maximize protection in mixed environments.

Unlike solutions that only function in specific environments and architectures, ZENworks Network Access Control doesn’t require expensive network infrastructure upgrades or architectural changes. It works in your environment regardless of which network vendors or infrastructure models you choose.
Novell ZENworks Network Access Control provides five enforcement options for quarantining endpoints, which makes it possible to enforce policy compliance across complex, heterogeneous networks. Enforcement options include:

- 802.1X enforcement
- DHCP enforcement
- Endpoint-based enforcement
- Inline enforcement for VPN and RAS connections
- Cisco NAC enforcement

You can also choose to blend enforcement options within a Novell ZENworks Network Access Control implementation and manage the whole solution from a single Web-based console. Additionally, ZENworks Network Access Control offers three endpoint testing options:

- Agentless testing
- ActiveX-based testing
- Agent-based testing

Collectively, these testing options allow ZENworks Network Access Control to evaluate a wide range of endpoints, including managed, unmanaged, remote, wireless, LAN-based and visitor devices.

Novell ZENworks Network Access Control includes hundreds of off-the-shelf tests that fully assess endpoint security posture. It also includes native support for testing dozens of security products from third-party vendors. Unlike the NAP and Cisco NAC approaches, ZENworks Network Access Control does not require individual integrations with these products to determine an endpoint’s health posture. Categories of ZENworks Network Access Control endpoint tests include:

- OS service packs and hotfixes
- Browser and OS security settings
- Antivirus, installed and up to date
- Personal firewall, installed and up to date
- Antispyware, installed and up to date
- Spyware (presence of)
- Peer-to-peer applications (presence of)
- Worms, viruses and Trojans (presence of)
- Required software, administrator defined
- Prohibited software, administrator defined

**Conclusion**

The emergence of NAC standards—or frameworks—is a natural progression of NAC technology. Consumers of NAC systems are ultimately the beneficiaries of these efforts, because they advance interoperability in the network environment and allow organizations greater flexibility in deploying NAC solutions. If you are considering a NAC solution, it’s important to confirm that the NAC vendor you select will operate within the framework that’s most appropriate for your environment and security needs.

The award-winning Novell ZENworks Network Access Control addresses this issue by fully supporting all the leading standards and expanding the NAC testing capabilities of each. Whether you embrace a particular framework or choose a framework-neutral approach, ZENworks Network Access Control is a NAC solution that will work with your network environment today and accommodate tomorrow’s standards-based systems.