Gartner Research

Publication Date: 23 January 2009 ID Number: G00164599

Simplify the NAC Vendor Selection Process

Lawrence Orans, John Pescatore

Defining your use case for network access control (NAC) is key to selecting the best solution. Here, we provide network managers with a set of criteria for evaluating vendors for each NAC usage case.

Key Findings

- NAC is a broad process that can be used in multiple ways to enhance network security. The four most common uses for NAC are: guest network services, endpoint baselining, identity-aware networking and monitoring/containment.
- Each of the four usage cases requires a different set of criteria. A common problem, which adds confusion during the vendor selection process, is for network managers to mix and match vendors across multiple usage cases.

Recommendations

- Identify your primary NAC usage case. Of the four NAC usage cases, which is the best fit for your environment?
- Limit your vendor analysis to a subset of vendors that have strong solutions for your primary usage case. Avoid evaluating vendors that have strong solutions for other usage cases, but weak solutions for your primary usage case.
- Plan ahead by evaluating solutions that not only are strong for your primary usage case, but also provide a good foundation for adding other usage cases so that you can achieve the benefits of a full NAC solution.

WHAT YOU NEED TO KNOW

Focus on vendors that can best meet the criteria for your primary NAC usage case. Avoid the common mistake of building a shortlist that mixes and matches vendors across multiple usage cases. For example, some vendors are stronger for the endpoint compliance usage case (based on device policies); others are stronger for the identity-aware networking usage case (based on user policies). Very few vendors are strong in multiple usage cases, so a good shortlist should not randomly mix vendors from multiple categories.

ANALYSIS

Overview

The adoption of NAC has been slowed by confusion and misunderstanding. Enterprises embarking on NAC projects face two main challenges:

- The term "NAC" is often interpreted differently by various people in the IT organization. For example, a network manager is likely to view NAC as a solution for keeping guests and visitors off the corporate network; a desktop manager is likely to view NAC as a tool for enforcing endpoint compliance (ensuring that patches and antivirus signatures are up-to-date).
- Choosing an NAC vendor is difficult. Numerous vendors claim to be NAC vendors (Gartner's "MarketScope for Network Access Control, 2008" lists 17 vendors), and many other vendors have latched on to the market hype and claim to have NAC functionality.

Analysis

"Network Access Control in 2009 and Beyond" addresses the first issue. It clarifies NAC by restating Gartner's NAC definition and outlining the four most common usage cases for NAC. Here, we address the second issue by providing guidelines for simplifying the vendor selection process and highlighting the key criteria for each of the four usage cases.

As highlighted in "Network Access Control in 2009 and Beyond," the four most common uses for NAC are:

- Guest Network Services — To isolate guests and visitors from the corporate network, providing them with limited connectivity, typically Internet access only.
- Endpoint Baselining — Determining if endpoints on the corporate network are compliant with device configuration policies and providing support for remediation efforts.
- Identity-Aware Networking — Providing greater visibility and control over user behavior on the network. Add identity-awareness to the network to monitor user traffic and enforce access to critical resources.
- Monitoring/Containment — Monitoring endpoints or network traffic to detect and quickly contain endpoints that begin to exhibit dangerous behavior.

Each of these usage cases requires a different mix of network and security processes (for example, device authentication, user authentication, policy enforcement). There are multiple technology options for each process (for example, in-line versus out-of-band enforcement). The multiple possibilities, and the multiple vendor choices, often lead to a confusing and unfocused

vendor selection process. A common mistake is for an NAC project team to assemble an "apples and oranges" shortlist of vendors, where some vendors are strong for one usage case and other vendors are strong for a different usage case.

For example, vendors that have strong solutions for endpoint baselining are typically not the best choice for identity-aware networking (and vice versa). A more focused approach is to decide first on your primary NAC usage case, and then build a shortlist of vendors that can best satisfy that usage case. Figure 1 highlights the criteria that are important for each of the four NAC usage cases.

Figure 1. NAC Usage Cases/Criteria

Use Case / Criteria	Guest Network Services	Endpoint Baselining	Identity-Aware Networking	Monitoring/ Containment
User Authentication	●	○	●	○
Device Authentication	● *	●	○	◐
Baseline	○	●	○	◐
Access Control/Enforcement	●	●	●	◐
Policy Configuration and Reporting	◐	◐	●	◐
Directory Integration	●	○	●	○
Monitoring	○	○	○	●
Containment	○	○	○	●

Level of Importance: High ● Medium ◐ Low ○

*Device authentication may also be used in the guest network usage case to determine if a user is an employee or a guest.

Source: Gartner (January 2009)

Network Access Control Criteria

Authentication — The ability to authenticate devices or users is the key requirement of a guest networking solution. If you choose to authenticate devices, you are making the guest versus employee decision based on the user's endpoint. For example, if a visitor attempts to connect a laptop to your network, it will fail authentication, and it will be moved to the guest network. If you authenticate users, the guest versus employee decision is based on the user's role as defined in a directory (users not defined in the directory are quarantined or treated as guests). Network managers that plan to extend guest networking to endpoint baselining NAC should start with device authentication. Those that plan to extend guest networking to identity-aware networking should start with user authentication.

- *Device Authentication* — There are multiple approaches for device-based authentication. MAC address tables, 802.1X (machine certificates), cookielike approaches and agentless scanning (where a scanner with administrative access "walks" through the Windows registry to identify a device) are the most common device-based authentication methods. Vendor support varies widely for these approaches.

- *User Authentication* — There are multiple approaches to authenticating users and determining if a user is a guest or not (see "Introducing the Identity-Aware Network"). Captive portal, 802.1X (user credentials) and snooping the authentication process are all approaches for the network to gain a user's identity and determine if the user gains access to the main network or to the guest network.

Baselining — As its name implies, this is the most important criterion for the endpoint baselining usage case (determining if an endpoint is compliant with device configuration policies). Ideally, the endpoint baselining process should also attempt to determine if the endpoint is "dangerous" (that is, it is capable of infecting other network endpoints with malware), but most NAC offerings are not capable of this level of assessment. Baselining can be achieved with permanent endpoint agents, dissolvable agents or agentless solutions. There is a wide range of vendor support for baselining technology. Some vendors support all three approaches; others support only one approach.

Access Control/Enforcement — Access control applies to devices or to users, depending on the usage case. In many cases, the same policy enforcement points (PEPs; for example, switches and NAC appliances) can be used to enforce access for multiple usage cases. NAC solutions can enforce access via in-line techniques (for example, drop/filter packets and access control lists [ACLs]), out-of-band techniques (such as virtual LAN [VLAN] steering and TCP resets), via 802.1X-enabled PEPs, or other approaches (for example, Address Resolution Protocol [ARP] spoofing, Dynamic Host Configuration Protocol [DHCP] and agent-based self-enforcement). Access control differs for these usage cases:

- *Guest Network* — Access control is a critical component of a guest network. Some endpoint protection (EPP) solutions have the ability to detect rogue devices (endpoints without an EPP agent), but lack enforcement capability. Look for guest solutions that can detect guests (via authentication) and provide enforcement across wired and wireless LANs.

- *Endpoint Baselining* — While most organizations are not yet quarantining noncompliant endpoints, enforcing access control is still an important criterion. Endpoint compliance NAC implementations should include the option to quarantine endpoints, particularly as a response to a malware outbreak, botnet compromise or other crisis. Look for solutions that can baseline endpoints in LAN, wireless LAN and virtual private network (VPN) environments.

- *Identity-Aware Networking* — The "identity firewall" is a common enforcement mechanism for this usage case. Identity firewalls are in-line PEPs that allow/deny packets based on deep packet inspection, packet tagging or access control lists. Other PEP approaches include proxy servers, IPsec (using certificates to create trusted domains), and Secure Sockets Layer (SSL) gateways. VLAN steering (out-of-band) may be used, although it has scalability issues.

- *Policy Configuration and Reporting* — NAC solutions vary widely in their ability to create policies and to produce meaningful reports. This criterion is important for all four NAC usage cases, but it has the most relevance for identity-aware networking, where audit trail reports are needed to monitor user behavior and satisfy regulatory auditors. Some advanced guest networking solutions include a specific guest management application that provides provisioning, management (for example, revoking guest privileges) and reporting (such as how many guests are on the network).

- *Directory Integration* — Identity-aware networks build policies based on role and user information stored in directories. Many NAC solutions integrate with Microsoft's Active Directory and most Lightweight Directory Access Protocol (LDAP)-based directories, and they provide Remote Authentication Dial-In User Service (RADIUS) support. Many guest networking implementations will need to integrate with the organization's main directory to determine if the user is an employee or a guest. Some solutions include a small database of guest users on a purpose-built guest networking appliance.

- *Monitoring* — Signature-based and anomaly-based detection are the two main technologies for monitoring traffic to detect malware and network-based attacks. Some NAC solutions support both approaches; others support only anomaly detection. The depth of signature support and anomaly detection also varies widely between vendors. In-band and out-of-band architectures are valid approaches for malware detection, although in-band approaches are superior for containing outbreaks, and more intrusion prevention system (IPS) vendors are entering the NAC space.

- *Containment* — In-line solutions are better than out-of-band solutions for containing malware and network attacks, because they can respond more quickly and more precisely (by dropping/filtering packets). Out-of-band solutions can also contain many attacks, but not as effectively. ARP spoofing solutions (available on some out-of-band NAC appliances) can also be used to contain some attacks by directing malicious traffic to an NAC appliance and preventing it from spreading.

The Path to Full NAC

While it is important to choose a vendor that satisfies your primary NAC usage case, remember that you will likely adopt other usage cases to achieve the benefits of full NAC. For example, after starting with guest network services, many network managers move on to implement endpoint baselining or, less commonly, identity-aware networking. Look for solutions that not only meet the requirements of your primary usage case, but also provide a good foundation for follow-on usage cases. As noted, the choice of an authentication mechanism is a critical decision for guest network services, because device-based authentication provides a good platform for endpoint compliance; user-based authentication provides a good platform for identity-aware networking. NAC is maturing, and many early NAC implementations have expanded to include additional usage cases.

RECOMMENDED READING

"Introducing the Identity-Aware Network"

"Findings: Wired 802.1X Adoption on the Rise"

"Network Access Control in 2009 and Beyond"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner