

Network Access Control Decision Framework

Gartner RAS Core Research Note G00143551, John Pescatore, Mark Nicolett, Lawrence Orans, 5 October 2006 R2052 1/25/2007

Business, technology and market realities have driven many enterprises to implement subsets of network access control. Choosing the best initial approach is the key to eventually reaching full NAC.

ANALYSIS

Dealing with the damage caused by dangerous and vulnerable PCs and servers after they connect to corporate networks has made network access control (NAC) a critical security process for enterprises. As many vendors, both large and small, have jumped on the NAC hype bandwagon, a confusing array of implementations has arisen. Following a structured decision framework is the key to selecting the best short-term and long-term approaches for your organization.

Gartner defined three approaches to implementing network access control functionality:

- **Infrastructure-based** – Primarily driven by Cisco and Microsoft, this approach involves upgrading your network or client/server operating system infrastructure to provide integrated (and generally proprietary) NAC functionality. An emerging infrastructure NAC approach utilizes Dynamic Host Configuration Protocol (DHCP) as a mechanism for enforcing NAC policies.
- **Endpoint software-based** – NAC can also be accomplished by installing, both permanently and as part of a temporary download to unmanaged devices, endpoint software that implements NAC baselining and access-control functionality.
- **Network security appliance-based** – The above approaches can be expensive and complex, or require waiting for an incumbent vendor to provide NAC support. Network-based NAC appliances can be used to implement NAC functionality (or subsets of full NAC). Often, these appliances are the simplest solutions to derive some of the key benefits of NAC if the first two approaches are not feasible or are too expensive.

The following provides a decision framework for making the best decision for your organization across the three major approaches to NAC. The first step is to ensure you are ready to implement NAC. For NAC to provide business value, you must have defined security configuration policies for both managed and unmanaged computers. You must also have carefully considered if, when and how to quarantine machines that are infected or vulnerable. Quarantining must work hand in hand with remediation – you must have patching and malicious software removal capabilities that can deal with noncompliant or dangerous configurations. Finally, you need automated methods to undo quarantining when a machine has been successfully remediated.

Decision Framework

1. Time frame for infrastructure upgrade –

Heterogeneous environments (more than just one network vendor, or more than just Windows desktops and servers) are obviously not candidates for infrastructure-based solutions from the large network vendors or Microsoft. If your environment is more homogeneous, and you have actively planned and budgeted to upgrade your network infrastructure to have 802.1x capabilities in 2006 or early 2007, or will be aggressively moving to Microsoft Vista during that time (and some adoption of Longhorn in 2007), the infrastructure-based NAC approach should be the first choice. For Cisco networks, the primary barriers to Cisco Network Admission Control (CNAC) have been the cost of upgrading routers and switches and the expense of deploying Cisco software to all endpoints (particularly PCs and laptops). Both of those barriers will be removed by 2007 for enterprises that have reached the natural refresh points for network equipment and desktop/laptops. The other network vendors will have competitive approaches with some degree of Microsoft's Network Access Protection (MNAP) integration by 2007 as well (see Note 1).

If your network will not be 802.1x-capable before 2007, or if you are not planning to deploy Vista before then, another infrastructure approach involves integrating NAC functionality into DHCP services. If you are upgrading DHCP capabilities with Blue Cat, Infoblox, Metainfo or some others, many of these vendors have begun to integrate with NAC appliance vendors. This approach generally requires deeper technical expertise, but by 2007, integration of NAC capabilities with DHCP offerings will simplify this approach and afford a mainstream alternative.

If none of these infrastructure upgrades is in your budget before 2008, Gartner believes that NAC is too valuable a capability to ignore in the interim. The key is to deploy one of the other two NAC approaches without entering into dead-end investments that will not lead to integrated NAC capabilities in the future.

2. How does your current endpoint security or configuration management software vendor support NAC? Most enterprises have deployed some combination of configuration management, antiviral and personal firewall software on their managed endpoints. The NAC capabilities of installed endpoint agents must be weighed in any NAC decision, regardless of the specific network control functions under consideration, because of the potential for automating the baseline and mitigation functions on managed endpoints.

The use of existing endpoint agents for NAC baseline and mitigation functions requires integration with the specific access control method that an organization is implementing for NAC. Most major desktop security and management vendors support

Note 1 Infrastructure-Based Approach

Vendors that have infrastructure-based approaches for NAC include Cisco, Extreme Networks, Microsoft and Nortel. The Trusted Computing Group/TNC consortium is working toward an open infrastructure-based NAC architecture, but adoption there has been limited.

Note 2 Client-Software Based Approach

Client software-based approaches include McAfee, Symantec, Trend Micro, Checkpoint, Infoexpress, Altiris, BigFix, Citadel, Landesk, Tivoli, Patchlink and Enforce.

CNAC and have announced plans to support MNAP (see Note 2). Many antivirus/personal firewall vendors also provide their own network control appliances, and a growing number of configuration management vendors have completed specific integrations with other NAC solutions beyond CNAC and MNAP. Integration with the major frameworks should be a minimum requirement for all client software-based approaches.

NAC-specific endpoint solutions can be installed on PCs and servers to add NAC functionality where existing endpoint software does not support NAC. This approach adds the additional cost and complexity of installing software and deploying another management console but can provide the advantages of client-side NAC where existing software agents cannot be upgraded. NAC endpoint vendors may also have more NAC-dedicated control and reporting capabilities than the mainstream vendors, but those additional capabilities may not be worth the added cost.

The leading client software NAC vendors have on-the-fly download solutions (temporary installation of ActiveX controls or Java applets) to deal with the major weakness of the client-side software approach – dealing with unmanaged PCs that do not have the permanently installed client software. However, if unmanaged devices represent a large portion of the security gain of NAC, the client-side software approach will not be the best choice. In addition, if you do not have NAC-capable client-side software installed on managed endpoints, or if the complexity of using this approach is too great, appliance-based approaches that implement a subset of full NAC capability will be a better starting point.

3. Are network security appliance-based approaches sufficient to meet your current needs? For enterprises in which infrastructure or client-software-based approaches are not feasible, are not affordable or are just overkill, appliance-based approaches that provide subsets of NAC capabilities have proved to be viable solutions. These approaches either monitor network behavior of connected devices or attempt to make a vulnerability assessment of devices after connection. Even using in-line network intrusion prevention to filter dangerous packets and identify a dangerous computer can provide some NAC functions. Some approaches can then take direct action to disconnect or quarantine devices, or they can be integrated with network devices to limit connectivity (see Note 3).

Vendors that offer solutions that could be binned in any of the three areas have been placed in the category we think is most applicable (see Note 4).

These approaches do not provide the same level of NAC capabilities as the infrastructure or client-

Note 3 Appliance-Based Approach

Appliance-based approaches include Cisco Clean Access, Consentry, Forescout, Lockdown Networks, Mirage Networks, Nevis Networks, StillSecure and Vernier.

Note 4 All Three Areas

Some vendors offer solutions that could be binned in all three areas. Gartner has placed them in the category we think is most appropriate.

software-based approaches. However, for many enterprises, guest or contractor unmanaged machine access is driving the near-term need for NAC, and these products can effectively limit that exposure with a low level of investment. They are often the best choice for universities and other loosely managed, highly distributed, heterogeneous, budget-constrained environments.

To avoid making dead-end investments in NAC appliances, query vendors on how their appliance can integrate to a full NAC framework, such as CNAC and MNAP, and the status of their certification by the framework vendor. Evaluation criteria should also include support for the Trusted Computing Group's Trusted Network Connect standard. While vendor proprietary frameworks, such as CNAC and MNAP, have detracted from the adoption of TNC standards, Gartner believes support for open standards is important in order to have both price competition and alternatives for heterogeneous network and operating system environments.