



Microsoft NAP and Network Access Control

NAC Picks Up Where NAP Leaves Off

A Mirage Networks White Paper
May 2008

EXECUTIVE SUMMARY

While Microsoft NAP is often perceived to be a solution with which Network Access Control (NAC) vendors will have to do battle, that's actually not the case at all. Microsoft NAP offers more powerful features in several cases, but it only addresses a subset of most NAC solutions' functionality. The NAP-NAC battle will never happen because the two heavyweight acronyms turn out to be quite complementary.

NETWORK ACCESS CONTROL OVERVIEW

The term Network Access Control (NAC) has been given different meanings by different parties with different interests, and there are a number of solutions available with completely different approaches. These approaches can generally be broken down into network appliances, software-based solutions, and infrastructure solutions. A network appliance solution would include a hardware platform that (typically) plugs into a network switch. These can be inline appliances, out-of-band appliances, or virtually inline appliances. Software-based solutions typically consist of endpoint agents and some central management platform. Infrastructure-based solutions vary but typically attempt to roll NAC functionality into switches, firewalls, IPS devices, etc. Each approach has its strengths and weaknesses, and from a technical standpoint the deployment environment usually dictates which approach is best.

Regardless of approach, there are also categories of functionality that must be considered. It should be noted that within each category there are different levels of functionality, but most solutions can be cleanly categorized with respect to these four categories. The four categories include:

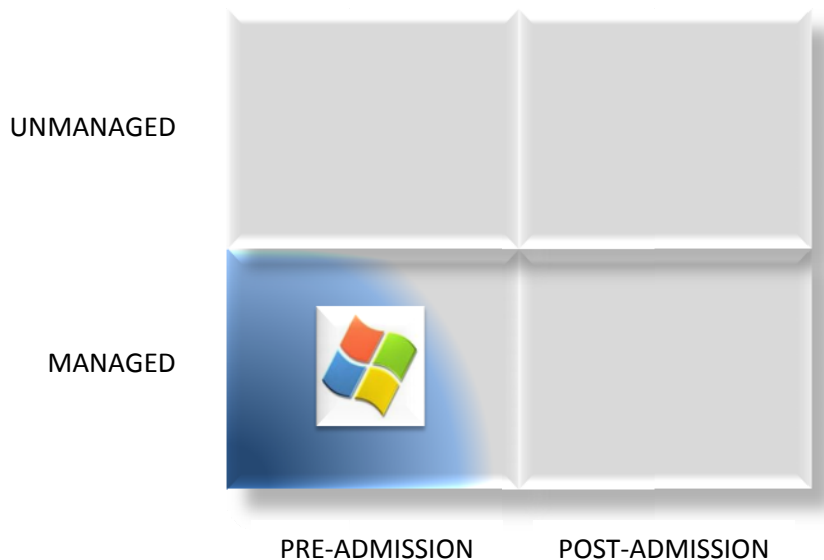
- **Pre-Admission** – This term refers to requiring endpoints to meet some requirements before they are given access to the network. Common examples include identity checks and endpoint health checks. Based on a policy decision, endpoints are either given or denied access.
- **Post-Admission** – This term refers to monitoring endpoints once they have network access. After the Pre-Admission screening is complete and endpoints are given partial or full network access, some NAC solutions continue to monitor endpoint network activity and enforce behavioral policies to isolate threats or simply stop unauthorized behavior.
- **Managed** – This term refers to endpoints that are owned and managed by the organization implementing NAC. If the IT staff has administrative rights to an endpoint, and thus can install an endpoint agent, the endpoint is considered managed.
- **Unmanaged** – This refers to every endpoint that is not managed. It can include mobile computers that move from location to location and cannot be completely controlled by the IT staff. It can also include guests, contractors, and any other endpoints on which an organization does not have the authority to install agents. Endpoints that are owned and controlled by the IT staff, but still cannot be controlled with agent software (i.e. IP phones, printers, gaming consoles, etc.) are sometimes referred to as unmanageable devices. In this white paper, unmanageable devices are included in the unmanaged category.

Note: There are several important capabilities of NAC solutions that are not dissected in this paper, including enforcement, remediation, and centralized management. These factors are critical in choosing an access control solution but are not pertinent to the scope of this document, which is focused on coverage.

MICROSOFT NAP OVERVIEW

Microsoft NAP is a software-based solution that, at a very high level, includes endpoint agents called system health agents (SHA's) and a policy server. The SHA's are available (by default) with the Windows Vista and Windows XP SP3 operating systems. The policy server is a component of Windows Server 2008. In a nutshell, Microsoft NAP offers system health checks for environments with Windows Vista or Windows XP SP3 endpoints and a back-end Windows 2008 server.

So, how does Microsoft NAP equate to NAC? In the context of NAC as described above, for the most part Microsoft NAP covers the categories of Pre-Admission and Managed. This means it provides pre-admission checks for managed endpoints, specifically the endpoints that have a SHA installed and configured properly. It allows for policy decisions to be made based on endpoint health information and can potentially combine that with user identity information. The graphic below illustrates Microsoft NAP's coverage in the four-element NAC grid. **Note:** The gradient indicates NAP provides pre-admission coverage for managed devices, but not all managed devices (only Vista and XP SP3).



Microsoft conducted an internal deployment of NAP on a reasonably large scale, and the Microsoft NAP Internal Case Study describing that deployment can be found [here](#). The case study explains how NAP policies were deployed and to some extent shares the results of the deployment. Nowhere in the case study or in any other Microsoft literature does Microsoft claim to cover unmanaged endpoints or perform post-admission endpoint monitoring.

NAP AND NAC

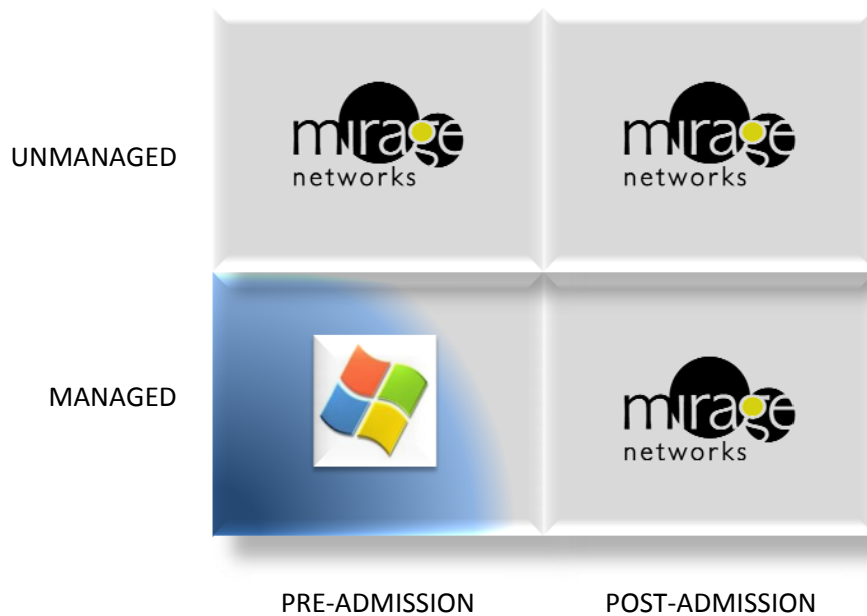
So while Microsoft NAP is perceived to be directly competitive to other NAC solutions, the technologies offered by many NAC vendors are in fact quite complementary. Vendors such as Mirage Networks offer full-cycle NAC, a term commonly used to refer to solutions that have pre-admission and post-admission capabilities, for both managed and unmanaged endpoints. These solutions can not only exist in a NAP environment, but can provide complete coverage throughout the life-cycle of an endpoint and offer more robust policy enforcement when combined with NAP. And while NAP provides complete pre-admission health checks for managed devices, there is a huge swath of unmanaged devices that should also be subjected to pre-admission checks to mitigate the risk of allowing them on the network. It is certainly the case that in higher education and similar environments there is a preponderance of unmanaged devices. But there are also many large enterprises who report ratios as high as 60:40 of unmanaged to managed devices. This can be attributed to mobility, outsourcing, an explosion of IP-enabled devices, and a number of other influencers. The coverage chart below indicates where NAP and Mirage NAC offer access control coverage.

Endpoint Type	MS NAP		Mirage NAC	
	Pre-Admission	Post-Admission	Pre-Admission	Post-Admission
Windows Vista (Managed)	X		X	X
Windows XP SP3 (Managed)	X		X	X
Windows Vista (Unmanaged)			X	X
Windows XP (Unmanaged)			X	X
Windows 2000			X	X
Windows 98			X	X
Windows 95			X	X
Macintosh			X	X
Linux			X	X
Printers			X	X
VoIP Phones			X	X
Windows Mobile Handhelds			X	X
iPhones			X	X
Gaming Consoles			X	X
IP-enabled Healthcare Devices			X	X
IP-enabled Mfg. Devices			X	X

Although the chart appears to minimize NAP’s coverage, it should be noted that Microsoft NAP is included with current operating systems, so organizations that already have Windows Server 2008 and endpoints running Windows Vista and/or Windows XP SP3 have the components needed to leverage NAP without additional capital expenditures. As pointed out in the Microsoft white paper, NAP policy management also inherently ties together a framework of separate network protection policies - update management, virus protection, a domain isolation environment, and so on –in a single solution that provides a centralized means of understanding our policy definitions, compliance, and remediation.

Microsoft NAP and Network Access Control

So while the strengths of NAP cannot be discounted, there is clearly an opportunity for other technologies to offer complementary solutions that bring a more complete view of the environment and allow for the creation and enforcement of a more complete set of policies. Instead of competing with Microsoft NAP, vendors such as Mirage Networks are embracing the presence of Microsoft in the space and are delivering solutions that will have a long-term presence in a NAP environment. The graphic below illustrates a combined NAP – Mirage environment in the four-element NAC grid.



Note: Mirage offer pre-admission coverage for managed devices as well, but the graphic above is intended to represent a combined NAP - Mirage environment, where NAP would presumably be the technology for pre-admission coverage of managed Windows endpoints.

CONCLUSION

Microsoft NAP is an excellent validation of the market need for controlling access to an organization's network(s). The approach is sound, but leaves a great opportunity for other technology vendors to fill in the gaps, some of which are quite large. Vendors who focus on unmanaged endpoints and post-admission policy enforcement have a long-term place co-existing with Microsoft NAP.