**Challenges and Opportunities**

Administrators face the time-consuming challenge of ensuring computers that connect to private network assets are up-to-date and meet network health policy requirements. Failure to keep computers current jeopardizes the integrity of a network. Key challenges include:

* Update Management: Organizations spend increased time and resources to ensure required software and updates are installed on desktop computers
* Remote Workers: Employees working from their home computers do not update with the latest antivirus signatures
* Roaming and visiting laptops: Employees returning from trips, consultants or guests plugging into the network, or employees VPN-ing in may be using machines that are not regularly updated
* Targeted Attacks: Malware may target and attack out-of-date, vulnerable machines in the network

To address these challenges, IT Administrators are looking for tools to:

* Detect and manage threats
* Establish health policies and require baseline compliance
* Keep the network resilient
* Remediate vulnerabilities
* Manage the policy enforcement and remediation system

**Solution Overview**

**Network Access Protection (NAP)** is a policy enforcement platform built into the Microsoft® Windows Vista and Windows Server 2008 operating systems that allows better protection of network assets by enforcing compliance with system health requirements. With Network Access Protection, administrators can create customized health policies to validate computer health before allowing access or communication, automatically update compliant computers to ensure ongoing compliance, or limit the access of noncompliant computers to a restricted network until they become compliant.

Network Access Protection has four important and distinct aspects:

* **Policy Validation:** Determines whether the computers are compliant with the company’s security policy. Compliant computers are deemed “healthy.”
* **Network Access Limitation:** Restricts network access to computers based on their health.
* **Automatic Remediation:** Provides necessary updates to allow the computer to “get healthy.” Once healthy, the network restrictions are removed.
* **Ongoing Compliance:** Automatically updates compliant computers so that they adhere to ongoing changes in health policy requirements.

Network Access Protection requires servers to run Windows Server 2008 and clients to run Windows Vista or Windows Server 2008. Microsoft is investigating an update for clients running Windows® XP with Service Pack 2 (SP2).

**Note:** The Network Access Protection platform is not the same as Network Access Quarantine Control, which is a capability provided with Windows Server 2003 to provide additional protection for remote access (dial-up and virtual private network [VPN]) connections. For more information, see [Network Access Quarantine Control in Windows Server 2003](http://www.microsoft.com/windowsserver2003/techinfo/overview/quarantine.mspx).

**Key Benefits and Differentiators**

With Network Access Protection, IT administrators are able to **monitor and update the health of desktops and laptops** connecting to the private network. Benefits include:

* ***Enhanced security*** – Communications are authenticated, authorized and healthier. IT administrators can cover most network protocols including DHCP, VPN, IPsec, 802.1X. Network Access Protection provides policy-based access that administrators can set and control.
* ***Increased business value and return-on-investment (ROI)*** – Up-to-date protection from malware preserves user productivity. This solution extends existing investments in Microsoft and third-party infrastructure, and leverages a broad industry partnership to accommodate many network architectures.
* ***Decreased risk level*** – By maintaining computer health and validating network policies, administrators can lower the risk of attack and software problems. This solution provides network defense at multiple layers.

**Solution Architecture**



Network Access Protection is a platform that includes a client and server architecture. NAP provides limited access enforcement components for the following technologies. Administrators can configure these technologies separately or together, depending on specific network needs:

* Internet Protocol security (IPsec)
* IEEE 802.1X authenticated network connections
* Virtual private networks (VPNs)
* Dynamic Host Configuration Protocol (DHCP)

Components that can be configured as part of Network Access Protection include:

*Platform Components*

* Quarantine Agent (QA) = Reports client health status, coordinates between SHA and QEC.
* Network Access Devices = Provide network access to healthy endpoints.
* Quarantine Server (QS) = Restricts client’s network access based on what SHV certifies.

*Health Components*

* System Health Validators (SHV) = Certify declarations made by health agents.
* Health Registration Authority = Issues certificates to clients that pass health checks.
* System Health Servers = Define health requirements for system components on the client.
* System Health Agents (SHA) = Declare health (patch state, virus signature, system configuration, etc.).

*Enforcement Components*

* Quarantine Enforcement Clients (QEC) = Negotiate access with network access device(s); DHCP, VPN, 1X, IPsec QECs.
* Remediation Servers = Install necessary patches, configurations, applications. Bring clients to healthy state.

**Competitive Landscape**

A large number of vendors fall into the “Network Access Control” category:

* Networking equipment providers
* End-point security software solutions
* “Bump in the wire” appliances

**Go to Market and Partners**

Network Access Protection shipped as a core Windows component in Windows Vista and will be included in Windows Server 2008, offering several opportunities for vendors and ecosystem partners:

* **Vendor and Developer Opportunities:** Designed to be flexible, Network Access Protection provides an infrastructure and a published API set for extending Network Access Protection functionality. It can interoperate with any vendor’s software that provides SHAs and SHVs or that recognizes its API set. Vendors and software developers can build their own network policy validation, ongoing network policy compliance, and network isolation components that are compatible with Network Access Protection.
* **Ecosystem Partners:** (<http://www.microsoft.com/windowsserver2003/partners/nappartners.mspx>)
	+ Networking
	+ Anti-Virus Systems
	+ Integrators
	+ Endpoint Security
	+ Update/Management
* **Interoperability with Cisco:** Cisco and Microsoft have been collaborating for over two years to enable rich interoperability between the Cisco Network Admission Control (NAC) and Microsoft Network Access Protection (NAP) solutions. This coordinated approach will allow customers to take advantage of the benefits of both NAC and NAP while still being able to implement a single, coordinated solution. Interoperability will be supported with the release of NAP in the future version of Windows Server 2008.

The NAC-NAP architecture consists of:

1. Client
	* System Health Agent (SHA)
	* NAP Agent (QA)
	* EAP Host Quarantine Enforcement Agent (QEC) – For plugging in additional supplicants
	* 802.1x supplicant
2. Network Discovery and Enforcement Component – Switches, routers, access points
3. Policy Infrastructure Components
	* Cisco Access Control Server (ACS)
	* Microsoft Network Policy Server (NPS)
	* Health Registration Authority (HRA) in case of “out-of-band” scenario
	* Third-party policy servers – as required

**F**or further details, see the white paper: [Cisco Network Admission Control and Microsoft Network Access Protection Interoperability Architecture](http://download.microsoft.com/download/d/0/8/d08df717-d752-4fa2-a77a-ab29f0b29266/NAC-NAP_Whitepaper.pdf).

* **Interoperability with Trusted Computing Group (TCG):** Trusted Computing Group (TCG), an industry standards body focused on security technologies, and Microsoft Corporation, a TCG member and an active participant in the development of TCG standards, announced they will provide customers and partners with interoperability of TCG Trusted Network Connect (TNC) and Microsoft Network Access Protection (NAP) via a shared statement of health. For further details of this interoperability, read the whitepaper [Standardizing Network Access Control: Microsoft NAP and TNC to interoperate](http://download.microsoft.com/download/c/1/2/c12b5d9b-b5c5-4ead-a335-d9a13692abbb/tnc_nap_white_paper.pdf).

**Roadmap**

Windows Server 2008

* NPS, HRA, Enforcement Servers
* Windows XP SP3 NAP Client
Windows Vista SP1 (Vista released with a NAP Client and EAP Host)
* NAP/NAC integration

**Resources**

* For more information about Network Access Protection, please visit:

**TechNet site (Public):** Network Access Protection

<http://www.microsoft.com/nap>

* **Windows Server System site (Public):** For the latest information about Windows Server System <http://www.microsoft.com/windowsserversystem>
* **Network Access Protection Blog (Public)**: For ongoing discussions of NAP from members of the NAP product team at Microsoft, <http://blogs.technet.com/nap/default.aspx>
* **White Paper**: Introduction to Network Access Protection

<http://www.microsoft.com/technet/network/nap/napoverview.mspx>

* **White Paper** Network Access Protection Platform Architecture

<http://www.microsoft.com/technet/network/nap/naparch.mspx>

* **FAQ:** Frequently Asked Questions about Network Access Protectio

<http://www.microsoft.com/technet/network/nap/napfaq.mspx>

* **Webcast**: “Introduction to Network Access Protection” white paper webcast

<http://support.microsoft.com/kb/921070>

* **Web Forum:**

<http://forums.microsoft.com/TechNet/ShowForum.aspx?ForumID=576&SiteID=17>