



# Network Access Protection

Ensuring network health through policy-based access enforcement

## What is Network Access Protection?

Network Access Protection (NAP) is a policy enforcement platform built into Windows Vista® and Windows Server® 2008. It is designed to inspect, assess, ensure compliance to policy, and remediate, where necessary, endpoints (e.g. laptops or other devices) attempting to access networked resources, such as applications, data, and information.

Network Access Protection is designed to protect both remote and local users from viruses, worms, and malicious software by helping to verify and directly update any computer attempting to access the network while restricting the network access of non-compliant clients. This set of technologies allows an IT administrator to keep the endpoints healthy and provides flexible control to set the policy of what is considered healthy enough to connect to the network.

## How does it work?

When a client tries to access the network, it must present its system health state. If a client cannot prove it is compliant with the system health policy, its access to the network can be restricted to a special network segment containing access to server resources so compliance issues can be remedied. After the updates are installed, the client again requests access to the network, presenting updated health credentials. Now compliant, the client is granted full access to the network based on the associated access policy. For greater control and better user experience, health credentials are reusable for immediate access to the network until there is a change in client health state or system health policy.

## Solution Overview

### Policy Validation

Determines whether endpoints are compliant with health and security policy. Compliant endpoints are deemed healthy.

### Network Restriction

Restricts network access based on validated endpoint health state.

### Remediation

Provides necessary updates to enable endpoints to get to a healthy state. Once healthy, network restrictions are removed.

### Ongoing Compliance

Changes to the health/security policy or to the endpoint's health state may dynamically result in network restriction and remediation.

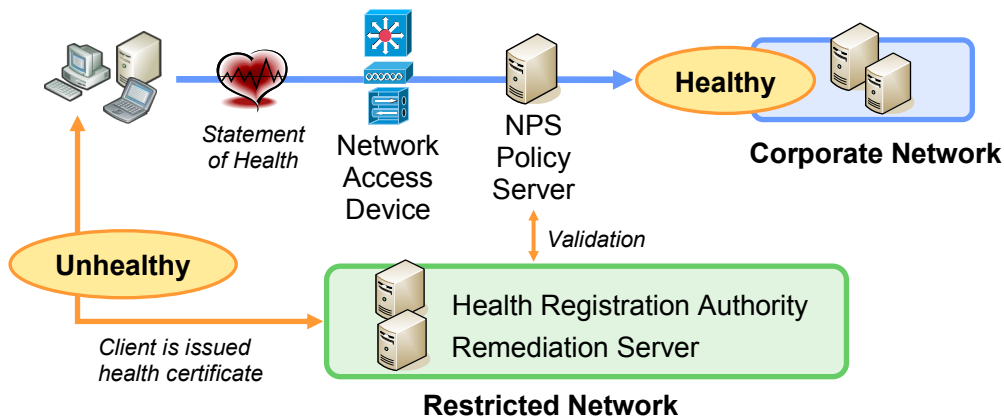
## Flexibility of Enforcement Options

Network Access Protection is about defense in depth and customer choice. A customer can implement Network Access Protection using the enforcement mechanism best suited to the company's business needs, threat model, existing infrastructure, and infrastructure upgrade schedule.

Enforcement Option	Healthy Client	Unhealthy Client
IPsec	Can communicate with any trusted peer	Connection requests rejected by healthy peers
802.1X	Full access	Restricted VLAN
SSL application proxy	Full application access	Access to restricted set of resources
VPN	Full access	IP filters enforced at VPN servers
DHCP	Full IP address given, full access	Restricted set of routes

*Protect network access, host access, application access in any combination, as needed, where appropriate.*

## Network Access Protection Process



# Network Access Protection

## System Requirements

- Windows Server® 2008
- DHCP Server service
- Routing and Remote Access service
- Network Policy Server (NPS)
- Health Registration Authority Server
- Health Registration Authority Server Management

## Client Support

- Windows Vista®
- Windows® XP Service Pack 3 (SP3)
- Licensable APIs for third party vendors to write support for Windows 2000, UNIX, Linux, or Mac clients
- NAP agents for Mac and Linux clients available through partners

## Features List

- DHCP NAP
- RRAS/VPN NAP
- IPsec NAP
- Health Registration Authority Server
- Vulnerability Assessment System Health Agent/Validator
- NAP Audit Only Mode
- NAP Enforcement Mode
- 802.1X NAP
- Improved NPS UI
- Health Registration Authority Server Management
- Integration with multiple Antivirus vendors
- Interoperability with Systems Center Configuration Manager and Operations Manager
- Interoperability with Forefront Client Security
- NAP Statement of Health (SOH) adopted by the Trusted Computing Group's TNC.

## Resources & Contacts

- **Web site and Whitepapers**  
[www.microsoft.com/nap](http://www.microsoft.com/nap)
- **FAQ**  
<http://www.microsoft.com/windowsserver2003/techinfo/overview/napfaq.mspx>
- **SDK Distribution**  
[napsdk@microsoft.com](mailto:napsdk@microsoft.com)
- **Partners**  
<http://www.microsoft.com/windowsserver2003/partners/nappartners.mspx>
- **Questions and Feedback**  
[asknap@microsoft.com](mailto:asknap@microsoft.com)

## Industry Support

A broad array of networking vendors have plans to innovate on top of the extensible architecture. This means investments you have already made in your infrastructure can be readily leveraged and plugged in interchangeably. To view a list of partners, please visit <http://www.microsoft.com/nap>.