Windows Server 2008

Windows Vista

Introduction to Network Access Protection

Abstract

Network Access Protection (NAP) is one of the most desired and highly anticipated features of Microsoft® Windows Server® 2008. NAP is a new platform and solution that controls access to network resources based on a client computer's identity and compliance with corporate governance policy. NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access. NAP includes an application programming interface (API) for developers and vendors to create complete solutions for health state validation, limitation of network access or communication, and ongoing compliance. This paper describes the scenarios for NAP, the components of NAP, and how NAP works for the enforcement methods included with Windows Server 2008, Windows Vista™, and Windows® XP Service Pack 3.

Contents

Introduction

One of the most time-consuming challenges that network administrators face is ensuring that computers that connect to private networks are up to date and meet health policy requirements. This complex task is commonly referred to as maintaining computer health. Enforcing requirements is even more difficult when the computers, such as home computers or traveling laptops, are not under the administrator's control. Yet failure to keep computers that connect to the network up to date is one of the most common ways to jeopardize the integrity of a network. For example, attackers create malicious software that targets out-of-date computers. Users who do not update their computers with the most recent operating system updates or antivirus signatures risk exposing private network assets to attacks and viruses. Administrators frequently lack the time or resources to ensure that all the software they would like to require is, in fact, installed and up to date. Additionally, administrators cannot easily manage or change requirements as often as they want.

Network Access Protection (NAP) for Windows Server 2008, Windows Vista, and Windows XP Service Pack 3 provides components and an application programming interface (API) that help administrators enforce compliance with health requirement policies for network access or communication. With NAP, developers and administrators can create solutions for validating computers that connect to their networks, provide needed updates or access to needed health update resources, and limit the access or communication of noncompliant computers. The enforcement features of NAP can be integrated with software from other vendors or with custom programs. Administrators can customize the health maintenance solution they develop and deploy, whether for monitoring the computers accessing the network for health policy compliance, automatically updating computers with software updates to meet health policy requirements, or limiting the access of computers that do not meet health policy requirements to a restricted network.

NAP is not designed to protect a network from malicious users. It is designed to help administrators automatically maintain the health of the computers on the network, which in turn helps maintain the network's overall integrity. For example, if a computer has all the software and configuration settings that the health policy requires, the computer is compliant and will be allowed unlimited access to the network. NAP does not prevent an authorized user with a compliant computer from uploading a malicious program to the network or engaging in other inappropriate behavior.

Aspects of NAP

NAP has three important and distinct aspects:

- **Health state validation** When a computer attempts to connect to the network, the computer's health state is validated against the health requirement policies as defined by the administrator. Administrators can also define what to do if a computer is not compliant. In a monitoring-only environment, all computers have their health state evaluated and the compliance state of each computer is logged for analysis. In a limited access environment, computers that comply with the health requirement policies are allowed unlimited access to the network. Computers that do not comply with health requirement policies can have their access limited to a restricted network.

- **Health policy compliance** Administrators can help ensure compliance with health requirement policies by choosing to automatically update noncompliant computers with missing software updates or configuration changes through management software, such as Microsoft Systems Management Server.

In a monitoring-only environment, computers will have access to the network before they are updated with required updates or configuration changes. In a limited access environment, noncompliant computers have limited access until the updates and configuration changes are completed. In both environments, computers that are compatible with NAP can automatically become compliant and administrators can define exceptions for computers that are not compatible with NAP.

- **Limited access** Administrators can protect their networks by limiting the access of noncompliant computers, as defined by the administrator. Limited network access can be based on a specific amount of time or on what the noncompliant computer can access. In the latter case, administrators define a restricted network containing health update resources and the limited access will last until the noncompliant computer is brought into compliance. Administrators can also configure exceptions so that computers that are not compatible with NAP do not have their network access limited.

Note The NAP 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](#) at http://www.microsoft.com/technet/network/vpn/quarantine.mspx.

The NAP platform requires servers running Windows Server 2008 and clients running Windows Vista, Windows Server 2008, or Windows XP with Service Pack 3.

Scenarios for NAP

NAP helps provide a solution for the following common scenarios:

- Verifying the health state of roaming laptops

  Portability and flexibility are two primary advantages of laptops, but these features also present a health threat. Company laptops frequently leave and return to the company network. While laptops are away from the company, they might not receive the most recent software updates or configuration changes. Laptops might also become infected while they are exposed to unprotected networks such as the Internet. By using NAP, network administrators can check the health state of any laptop when it reconnects to the company network, whether by creating a VPN connection to the company network or by physically returning to the office.

- Verifying the health state of desktop computers

  Although desktop computers do not usually leave the premises, they still can present a threat to a network. To minimize this threat, administrators must maintain these computers with the most recent updates and required software. Otherwise, these computers are at risk of infection from Web sites, e-mail, files from shared folders, and other publicly accessible resources. By using NAP, network administrators can automate health state checks to verify each desktop computer's compliance with health requirement policies. Administrators can check log files to determine which computers do not comply. With the addition of management software, administrators can generate automatic reports and automatically update noncompliant computers. When administrators change health requirement policies, computers can be automatically provisioned with the most recent updates.

- Verifying the health state of visiting laptops

Organizations frequently need to allow consultants, business partners, and guests to connect to their private networks. The laptops that these visitors bring might not meet system health requirements and can present health risks. By using NAP, administrators can determine that the visiting laptops are not compliant and limit their access to a restricted network. Typically, administrators would not require or provide any updates or configuration changes to the visiting laptops. The administrator could configure Internet access for visiting laptops, but not for other organization computers whose access is limited.

- Verifying the health state of unmanaged home computers

Unmanaged home computers that are not a member of the company's Active Directory® Domain Services domain can connect to a managed company network through a VPN connection. Unmanaged home computers provide an additional challenge to administrators because they do not have physical access to these computers. Lack of physical access makes enforcing compliance with health requirements, such as the use of antivirus software, even more difficult. However, with NAP, network administrators can verify the health state of a home computer every time it makes a VPN connection to the company network and limit the access to a restricted network until system health requirements are met.

Depending on their needs, administrators can configure a solution to address any or all of these scenarios for their networks.

Components of NAP

NAP is an extensible platform that provides infrastructure components and an API for adding components that verify and amend a computer's health and enforce various types of network access or communication. The following sections describe some of the components of the NAP infrastructure to facilitate a basic understanding of NAP processes. For a more detailed explanation of NAP components and architecture, see Network Access Protection Platform Architecture at http://go.microsoft.com/fwlink/?LinkId=49885.

System Health Agents and System Health Validators

Components of the NAP infrastructure known as system health agents (SHAs) and system health validators (SHVs) provide health state tracking and validation. Windows Vista and Windows XP Service Pack 3 include a Windows Security Health Validator SHA that monitors the settings of the Windows Security Center. Windows Server 2008 includes a corresponding Windows Security Health Validator SHV. NAP is designed to be flexible and extensible. It can interoperate with any vendor's software that provides SHAs and SHVs that use the NAP API.

Enforcement Components and Methods

Components of the NAP infrastructure known as enforcement clients (ECs) and enforcement servers (ESs) require health state validation and enforce limited network access for noncompliant computers for specific types of network access or communication. Windows Vista, Windows XP Service Pack 3, and Windows Server 2008 include NAP support for the following types of network access or communication:

- Internet Protocol security (IPsec)-protected traffic

- IEEE 802.1X-authenticated network connections

- Remote access VPN connections

- Dynamic Host Configuration Protocol (DHCP) address configurations

- Terminal Server (TS) Gateway connections

These types of network access or communication are known as NAP enforcement methods. Administrators can use them separately or together to limit the access or communication of noncompliant computers. Network Policy Server (NPS) in Windows Server 2008, the replacement for Internet Authentication Service (IAS) in Windows Server 2003, acts as a health policy server for all of these NAP enforcement methods.

The following sections describe the IPsec, 802.1X, VPN, and DHCP enforcement methods.

IPsec Enforcement

With IPsec enforcement, a computer must be compliant to initiate communications with other compliant computers. Because IPsec enforcement is leveraging IPsec, you can define requirements for protected communications with compliant computers on a per-IP address or per-TCP/UDP port number basis. IPsec enforcement confines communication to compliant computers after they have successfully connected and obtained a valid IP address configuration. IPsec enforcement is the strongest form of limited network access or communication in NAP.

The components of IPsec enforcement consist of a Health Registration Authority (HRA) running Windows Server 2008 and an IPsec Relying Party EC in Windows Vista, Windows XP Service Pack 3, and Windows Server 2008. The HRA obtains X.509 certificates for NAP clients when they prove that they are compliant. These health certificates are then used to authenticate NAP clients when they initiate IPsec-protected communications with other NAP clients on an intranet.

802.1X Enforcement

With 802.1X enforcement, a computer must be compliant to obtain unlimited network access through an 802.1X-authenticated network connection, such as to an authenticating Ethernet switch or an IEEE 802.11 wireless access point (AP). For noncompliant computers, network access is limited through a restricted access profile placed on the connection by the Ethernet switch or wireless AP. The restricted access profile can specify IP packet filters or a virtual LAN (VLAN) identifier (ID) that corresponds to the restricted network. 802.1X enforcement enforces health policy requirements every time a computer attempts an 802.1X-authenticated network connection. 802.1X enforcement also actively monitors the health status of the connected NAP client and applies the restricted access profile to the connection if the client becomes noncompliant.

The components of 802.1X enforcement consist of NPS in Windows Server 2008 and an EAP Quarantine EC in Windows Vista and Windows Server 2008. For Windows XP with Service Pack 3, there are separate ECs for wired and wireless connections. 802.1X enforcement provides strong limited network access for all computers accessing the network through an 802.1X-authenticated connection.

VPN Enforcement

With VPN enforcement, a computer must be compliant to obtain unlimited network access through a remote access VPN connection. For noncompliant computers, network access is limited through a set of IP packet filters that are applied to the VPN connection by the VPN server. VPN enforcement enforces health policy requirements every time a computer attempts to obtain a remote access VPN connection to the network. VPN enforcement also actively monitors the health status of the NAP client and applies the IP packet filters for the restricted network to the VPN connection if the client becomes noncompliant.

The components of VPN enforcement consist of NPS in Windows Server 2008 and a Remote Access Quarantine EC in Windows Vista, Windows XP Service Pack 3, and Windows Server 2008. VPN enforcement provides strong limited network access for all computers accessing the network through a remote access VPN connection.

Note VPN enforcement with NAP is different than Network Access Quarantine Control, a feature in Windows Server 2003. Network Access Quarantine Control relies on the creation of customized scripts and manual configuration of two tools (RQS.exe and RQC.exe) from the Windows Server 2003 Resource Kit Tools or included with Windows Server 2003 Service Pack 1 and later. Using Network Access Quarantine Control, administrators can create customized VPN connections for their users. These connections can check for required programs, and administrators can isolate a VPN connection until these checks have been performed. Network Access Quarantine Control is not part of NAP. It is compatible with VPN servers using NAP, although administrators might need to adjust some scripts. Administrators can use Network Access Quarantine Control and NAP simultaneously.

DHCP Enforcement

With DHCP enforcement, a computer must be compliant to obtain an unlimited access IPv4 address configuration from a DHCP server. For noncompliant computers, network access is limited by an IPv4 address configuration that allows access only to the restricted network. DHCP enforcement enforces health policy requirements every time a DHCP client attempts to lease or renew an IP address configuration. DHCP enforcement also actively monitors the health status of the NAP client and renews the IPv4 address configuration for access only to the restricted network if the client becomes noncompliant.

The components of DHCP enforcement consist of a DHCP ES that is part of the DHCP Server service in Windows Server 2008 and a DHCP Quarantine EC in Windows Vista, Windows Server 2008, and Windows XP Service Pack 3. Because DHCP enforcement relies on a limited IPv4 address configuration that can be overridden by a user with administrator-level access, it is the weakest form of limited network access in NAP.

NPS

NPS is a Remote Authentication Dial-In User Service (RADIUS) server and proxy in Windows Server 2008. As a RADIUS server, NPS provides authentication, authorization, and accounting (AAA) services for various types of network access. For authentication and authorization, NPS uses Active Directory to verify user or computer credentials and obtain user or computer account properties when a computer attempts an 802.1X-authenticated connection or a VPN connection.

NPS also acts as a NAP health policy server. Administrators define system health requirements in the form of health policies on the NPS server. NPS servers evaluate health state information provided by NAP clients to determine health compliance, and for non-compliance, the set of remediation actions that must be done by the NAP client to become compliant.

The role of NPS as a AAA server is independent from its role as a NAP health policy server. These roles can used separately or combined as needed. For example:

- NPS can be a AAA server on an intranet that has not yet deployed NAP.

- NPS can be a combination of AAA server and a NAP health policy server for 802.1X-authenticated connections on an intranet that has deployed NAP and 802.1X enforcement.

- NPS can be a NAP health policy server for DHCP configuration on an intranet that has deployed NAP and DHCP enforcement.

Remediation Servers

Remediation servers consist of servers, services, or other resources that a noncompliant computer that has been placed on the restricted network can access. These resources might perform name resolution or store the most recent software updates or components needed to make a noncompliant computer meet system health requirements. For example, a Domain Name System (DNS) server, an antivirus signature file server, and a software update server could all be remediation servers. An SHA can communicate with a remediation server directly or use the facilities of installed client software.

How NAP Works

NAP is designed so that administrators can configure it to meet the individual needs of their networks. Therefore, the actual configuration of NAP will vary according to the administrator's preferences and requirements. However, the underlying operation of NAP remains the same. This section describes how NAP works on an example intranet.

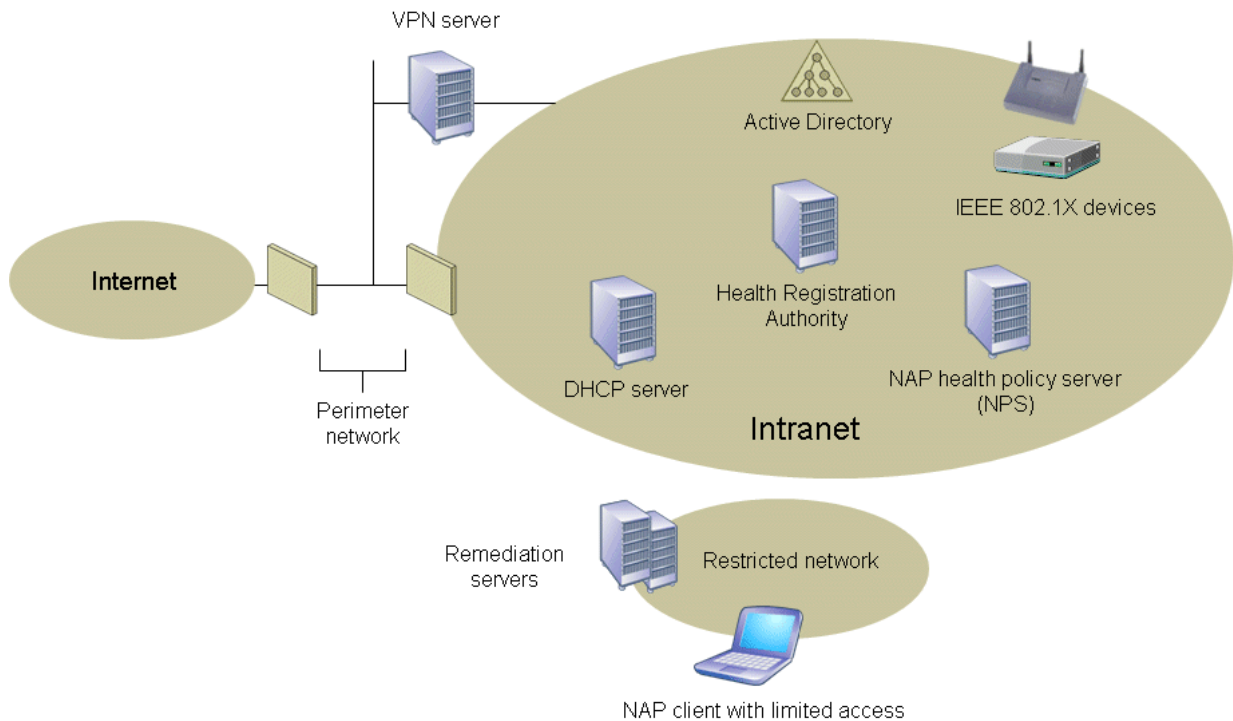Figure 1 shows an example intranet that has deployed NAP.

Figure 1: Example intranet that has deployed NAP

This example intranet is configured for the following:

- Health state validation, health policy compliance, and limited network access for noncompliant NAP clients

- IPsec enforcement, 802.1X enforcement, VPN enforcement, and DHCP enforcement

When obtaining a health certificate, making an 802.1X-authenticated or VPN connection to the intranet, or leasing or renewing an IPv4 address configuration from the DHCP server, each NAP client is classified in one of the following ways:

- NAP clients that meet the health policy requirements are classified as compliant and allowed unlimited access or normal communication on the intranet.

- NAP clients that do not meet the health policy requirements are classified as noncompliant and have their access limited to the restricted network until they meet the requirements. A noncompliant NAP client does not necessarily have a virus or some other active threat to the intranet, but it does not have the software updates or configuration settings as required by health policy. Therefore, noncompliant

NAP client pose health risks to the rest of the intranet. The SHAs on NAP clients can automatically update computers with limited access with the software or configuration settings required for unlimited access.

The example intranet in Figure 1 contains a restricted network. A restricted network can be defined logically or physically. IP filters, static routes, or a VLAN identifier are placed on the connection of NAP clients with limited access to define the remediation servers with which they can communicate.

Because most intranets contain a heterogeneous mixture of computers and devices, an administrator might choose to exempt some computers or devices from health policy requirements. For example, computers running versions of Windows prior to Windows XP and operating systems other than Windows do not support NAP. In a limited access environment, these computers will always have limited access. To prevent limited access for these computers, the administrator can configure an exception health policy on the NAP health policy server; exempted computers are not checked for compliance and have unlimited access to the intranet.

The following sections describe the basic processes for IPsec enforcement, 802.1X enforcement, VPN enforcement, and DHCP enforcement for a NAP client. For a more detailed explanation of these processes, see Network Access Protection Platform Architecture at http://go.microsoft.com/fwlink/?LinkId=49885.

How IPsec Enforcement Works

The following process describes how IPsec enforcement works for a NAP client that is starting on the example intranet shown in Figure 1:

1. The IPsec Relying Party EC component sends its current health state to the HRA.

2. The HRA sends the NAP client's health state information to the NAP health policy server.

3. The NAP health policy server evaluates the health state information of the NAP client, determines whether the NAP client is compliant, and sends the results to the HRA. If the NAP client is not compliant, the results include health remediation instructions. The HRA sends the NAP client the health evaluation results.

4. If the health state is compliant, the HRA obtains a health certificate for the NAP client. The NAP client can now initiate IPsec-protected communication with other compliant computers using its health certificate for IPsec authentication, and respond to communications initiated from other compliant computers that authenticate using their own health certificate.

5. If the health state is not compliant, the HRA does not issue a health certificate. The NAP client cannot initiate communication with other computers that require a health certificate for IPsec authentication. However, the NAP client can initiate communications with remediation servers to correct its health state.

6. The NAP client sends update requests to the appropriate remediation servers.

7. The remediation servers provision the NAP client with the required updates for compliance with health requirements. The NAP client updates its health state information.

8. The NAP client sends its updated health state information to the HRA and the HRA sends the updated health state information to the NAP health policy server.

9. Assuming that all the required updates were made, the NAP health policy server determines that the

NAP client is compliant and sends that result to the HRA.

10. The HRA obtains a health certificate for the NAP client. The NAP client can now initiate IPsec-protected communication with other compliant computers.

How 802.1X Enforcement Works

The following process describes how 802.1X enforcement works for a NAP client that is initiating an 802.1X-authenticated connection on the example intranet shown in Figure 1:

1. The NAP client and the Ethernet switch or wireless AP begin 802.1X authentication.

2. The NAP client sends its user or computer authentication credentials to the NAP health policy server, which is also acting as a AAA server.

3. If the authentication credentials are not valid, the connection attempt is terminated.

4. If the authentication credentials are valid, the NAP health policy server requests the health state from the NAP client.

5. The NAP client sends its health state information to the NAP health policy server.

6. The NAP health policy server evaluates the health state information of the NAP client, determines whether the NAP client is compliant, and sends the results to the NAP client and the Ethernet switch or wireless AP. If the NAP client is not compliant, the results include a limited access profile for the Ethernet switch or wireless AP and health remediation instructions for the NAP client.

7. If the health state is compliant, the Ethernet switch or wireless AP completes the 802.1X authentication and the NAP client has unlimited access to the intranet.

8. If the health state is not compliant, the Ethernet switch or wireless AP completes the 802.1X authentication but limits the access of the NAP client to the restricted network. The NAP client can send traffic only to the remediation servers on the restricted network.

9. The NAP client sends update requests to the remediation servers.

10. The remediation servers provision the NAP client with the required updates for compliance with health policy. The NAP client updates its health state information.

11. The NAP client restarts 802.1X authentication and sends its updated health state information to the NAP health policy server.

12. Assuming that all the required updates were made, the NAP health policy server determines that the NAP client is compliant and instructs the Ethernet switch or wireless AP to allow unlimited access.

13. The Ethernet switch or wireless AP completes the 802.1X authentication and the NAP client has unlimited access to the intranet.

How VPN Enforcement Works

The following process describes how VPN enforcement works for a NAP client that is initiating a remote access VPN connection to the example intranet shown in Figure 1:

1. The NAP client initiates a remote access connection to the VPN server.

2. The NAP client sends its user authentication credentials to the NAP health policy server, which is also acting as a AAA server.

3. If the authentication credentials are not valid, the VPN connection attempt is terminated.

4. If the authentication credentials are valid, the NAP health policy server requests the health state from the NAP client.

5. The NAP client sends its health state information to the NAP health policy server.

6. The NAP health policy server evaluates the health state information of the NAP client, determines whether the NAP client is compliant, and sends the results to the NAP client and the VPN server. If the NAP client is not compliant, the results include a set of packet filters for the VPN server and health remediation instructions for the NAP client.

7. If the health state is compliant, the VPN server completes the VPN connection and the NAP client has unlimited access to the intranet.

8. If the health state is not compliant, the VPN server completes the VPN connection but, based on the packet filters, limits the access of the NAP client to the restricted network. The NAP client can send traffic only to the remediation servers on the restricted network.

9. The NAP client sends update requests to the remediation servers.

10. The remediation servers provision the NAP client with the required updates for compliance with health policy. The NAP client updates its health state information.

11. The NAP client restarts authentication with the VPN server and sends its updated health state information to the NAP health policy server.

12. Assuming that all the required updates were made, the NAP health policy server determines that the NAP client is compliant and instructs the VPN server to allow unlimited access.

13. The VPN server completes the VPN connection and the NAP client has unlimited access to the intranet.

How DHCP Enforcement Works

The following process describes how DHCP enforcement works for a NAP client that is attempting an initial DHCP configuration on the example intranet shown in Figure 1:

1. The NAP client sends a DHCP request message containing its health state information to the DHCP server.

2. The DHCP server sends the health state information of the NAP client to the NAP health policy server.

3. The NAP health policy server evaluates the health state information of the NAP client, determines whether the NAP client is compliant, and sends the results to the NAP client and the DHCP server. If the NAP client is not compliant, the results include a limited access configuration for the DHCP server and health remediation instructions for the NAP client.

4. If the health state is compliant, the DHCP server assigns an IPv4 address configuration for unlimited access to the NAP client and completes the DHCP message exchange.

5. If the health state is not compliant, the DHCP server assigns an IPv4 address configuration for limited access to the restricted network to the NAP client and completes the DHCP message exchange. The NAP client can send traffic only to the remediation servers on the restricted network.

6. The NAP client sends update requests to the remediation servers.

7. The remediation servers provision the NAP client with the required updates for compliance with health policy. The NAP client updates its health state information.

8. The NAP client sends a new DHCP request message containing its updated health state information to the DHCP server.

9. The DHCP server sends the updated health state information of the NAP client to the NAP health policy server.

10. Assuming that all the required updates were made, the NAP health policy server determines that the NAP client is compliant and instructs the DHCP server to assign an IPv4 address configuration for unlimited access to the intranet.

11. The DHCP server assigns an IPv4 address configuration for unlimited access to the NAP client and completes the DHCP message exchange.

Summary

NAP is a key feature of Windows Server 2008 that includes client and server components to control access to network resources based on a client's identity and compliance with corporate governance policy. Administrators can configure IPsec enforcement, 802.1X enforcement, VPN enforcement, DHCP enforcement, or all of them, depending on their needs. NAP provides an infrastructure and an API, which vendors and software developers can use to build their own health validation and limited network access or communication components.

Related Links

For additional information, see the following resources:

- [Microsoft Network Access Protection Web page](#) at http://www.microsoft.com/nap

- [Network Access Protection Platform Architecture](#) at http://go.microsoft.com/fwlink/?LinkId=49885

- [Network Accesss Protection: Frequently Asked Questions](#) at http://go.microsoft.com/fwlink/?LinkId=49886

- [Network Access Protection (NAP) blog](#) at http://blogs.technet.com/nap/default.aspx