Introduction to Network Access Protection

Microsoft Corporation

Published: June 2004, Updated: May 2006

Abstract

Network Access Protection, a platform for Microsoft® Windows Server® "Longhorn" (now in beta testing) and Windows Vista™ (now in beta testing), provides policy enforcement components that help ensure that computers connecting to a network or communicating on a network meet administrator-defined requirements for system health. Administrators can use a combination of policy validation and network access limitation components to control network access or communication. Administrators can also choose to temporarily limit the access of computers that do not meet requirements to a restricted network. Depending on the configuration chosen, the restricted network might contain resources required to update the computers so that they then meet the health requirements for unlimited network access and normal communication. Network Access Protection includes an application programming interface (API) set for developers and vendors to create complete solutions for health policy validation, network access limitation, and ongoing health compliance. This document describes the components of Network Access Protection, shows how they work, and provides a theoretical configuration using Windows Server "Longhorn" and Windows Vista.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Contents

Introduction

One of the most time-consuming challenges that administrators face is ensuring that computers that connect to private network assets 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 software that targets out-of-date computers. Users who do not update their home computers with the most recent antivirus signatures risk exposing private network assets to 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 for Windows Server "Longhorn" and Windows Vista provides components and an application programming interface (API) set that help administrators enforce compliance with health policies for network access or communication. Developers and administrators can create solutions for validating computers that connect to their networks, can provide needed updates or access to needed resources (called health update resources), and can limit the access of noncompliant computers. The enforcement features of Network Access Protection can be integrated with software from other vendors or with custom programs. Administrators can customize the systems 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.

Network Access Protection is not designed to secure a network from malicious users. It is designed to help administrators maintain the health of the computers on the network, which in turns helps maintain the network's overall integrity. For example, if a computer has all the software and configurations that the health policy requires, the computer is considered compliant, and it will be granted the appropriate access to the network. Network Access Protection does not prevent an authorized user with a compliant computer from uploading a malicious program to the network or engaging in other inappropriate behavior.

Network Access Protection has three important and distinct aspects:

- **Health Policy Validation** When a user attempts to connect to the network, the computer's health state is validated against the health policies as defined by the administrator. Administrators can then choose what to do if a computer is not compliant. In a monitoring-only environment, all authorized computers are granted access to the network even if some do not comply with health policies, but the compliance state of each computer is logged. In a restricted access environment, computers that comply with the health policies are allowed unlimited access to the network, but computers that do not comply with health policies or that are not compatible with Network Access Protection have their access limited to a restricted network. In both environments, computers that are compatible with Network Access Protection can automatically become compliant and administrators can define exceptions to the validation process. Network Access Protection will also include migration tools to make it easier for administrators to define exceptions that best suit their network needs.

- **Health Policy Compliance** Administrators can help ensure compliance with health policies by choosing to automatically update noncompliant computers with the missing requirements through management software, such as Microsoft Systems Management Server. In a monitoring-only environment, computers will have access to the network even before they are updated with required software or configuration changes. In a restricted access environment, computers that do not comply with health policies have limited access until the software and configuration updates are completed. Again, in both environments, computers that are compatible with Network Access Protection can automatically become compliant and the administrator can define policy exceptions.
- **Limited Access** Administrators can protect network assets by limiting the access of computers that do not comply with health policy requirements. Non-compliant computers will have their access limited as defined by the administrator. Network access limits can be based on a specific amount of time or whether the network access is limited to a restricted network, to a single resource, or to no internal resources at all. If an administrator does not configure health update resources, the limited access will last for the duration of the connection. If an administrator configures health update resources, the limited access will last only until the computer is brought into compliance. Administrators might use both monitoring and health policy compliance in their networks and configure exceptions.

Network Access Protection is an extensible platform that provides an infrastructure and an API set for adding components that verify and amend a computer's health and that enforce existing policy systems. By itself, Network Access Protection does not provide components to verify or amend a computer's health. Other components, known as system health agents (SHAs) and system health validators (SHVs), will provide health policy validation and health policy compliance. Windows Vista and Windows Server "Longhorn" include an SHA and an SHV that provides health policy validation and health policy compliance for health attributes monitored by the Windows Security Center.

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.

Scenarios for Network Access Protection

Network Access Protection is designed to be flexible. It can interoperate with any vendor's software that provides SHAs and SHVs or that recognizes its published API set. Network Access Protection helps provide a solution for the following common scenarios.

Check the health and status 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 be infected while exposed to unsecured networks, such as the Internet. By using Network Access Protection, network administrators can check the health of any laptop when it reconnects to the company network, whether by creating a VPN connection back to the company network or by physically returning to the office.

Ensure the health of desktop computers

Although desktop computers do not usually leave the premises, they still can present a health threat to a network. To minimize this threat, administrators must maintain these computers with the most recent updates and software the company wants to require. Otherwise, those computers are at higher risk of infection from Web sites, e-mail, files from shared folders, and other publicly accessible resources. By using Network Access Protection, network administrators can automate system checks to verify each desktop computer's compliance with the health policies. Administrators can check log files to review what computers do not comply. With the addition of management software, automatic reports can be generated, updates can be made automatically to noncompliant computers, and when administrators change health policies, computers can be automatically provided with the most recent updates.

Determine the health of visiting laptops

Organizations frequently need to allow consultants and guests access to their private networks. The laptops that these visitors bring might not meet network requirements and can present health risks. By using Network Access Protection, administrators can determine that the visiting laptops are not authorized to access the network and limit their access to a restricted network. Generally, administrators would not require or provide any updates or configuration changes to the visiting laptops. The administrator might configure Internet access for visiting laptops in the restricted network, but not for other computers whose access is limited.

Verify the compliance and health of unmanaged home computers

Unmanaged home computers provide an additional challenge to network administrators because they do not have physical access to these computers. Lack of physical access makes enforcing compliance with network requirements (such as the use of antivirus software) even more difficult. Verifying the health of these computers is similarly challenging. By using Network Access Protection, network administrators can check for required programs, registry settings, files, or combinations of these every time a home computer makes a VPN connection to the network, and they can limit the connection 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 Network Access Protection

Network Access Protection provides limited access enforcement components for the following technologies:

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

Administrators can use these technologies separately or together to limit noncompliant computers. Network Policy Server (NPS), the replacement for Internet Authentication Service (IAS) in Windows Server 2003 in Windows Server "Longhorn," acts as a health policy server for all of these technologies.

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

IPsec Enforcement

IPsec Enforcement comprises a health certificate server and an IPsec NAP Enforcement Client (EC). The health certificate server issues X.509 certificates to quarantine clients when they are determined to be compliant. These certificates are then used to authenticate NAP clients when they initiate IPsec-secured communications with other NAP clients on an intranet.

IPsec Enforcement confines the communication on your network to those nodes that are considered compliant and because it is leveraging IPsec, you can define requirements for secure communications with compliant clients 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 in Network Access Protection.

802.1X Enforcement

802.1X Enforcement comprises an NPS server and an EAPHost NAP EC component. Using 802.1X Enforcement, an NPS server instructs an 802.1X access point (an Ethernet switch or a wireless access point) to place a restricted access profile on the 802.1X client until it performs a set of remediation functions. A restricted access profile can consist of a set of IP packet filters or a virtual LAN (VLAN) identifier to confine the traffic of an 802.1X client. 802.1X Enforcement provides strong limited network access for all computers accessing the network through an 802.1X connection.

VPN Enforcement

VPN Enforcement comprises a VPN NAP Enforcement Server (ES) component and a VPN NAP EC component. Using VPN Enforcement, VPN servers can enforce health policy requirements any time a computer attempts to make a VPN connection to the network. VPN Enforcement provides strong limited network access for all computers accessing the network through a VPN connection.

Note VPN Enforcement with NAP is different than Network Access Quarantine Control, a feature in Windows Server 2003[1].

DHCP Enforcement

DHCP Enforcement comprises a DHCP NAP ES component and a DHCP NAP EC component. Using DHCP Enforcement, DHCP servers can enforce health policy requirements any time a computer attempts to lease or renew an IP address configuration on the network. DHCP Enforcement is the easiest enforcement to deploy because all DHCP client computers must lease IP addresses. Because DHCP Enforcement relies on entries in the IP routing table, it is the weakest form of limited network access in Network Access Protection.

NPS/RADIUS

The Remote Authentication Dial-In User Service (RADIUS) component of Windows Server "Longhorn", NPS, does not have a NAP ES or NAP EC component. Instead, it works as a policy server in conjunction with NAP ES and NAP EC components. Administrators must define system health requirements in the form of policies on the NPS server. NPS servers provide health policy checks and coordinate with the Active Directory® directory service any time a computer attempts to obtain a health certificate or to connect to an 802.1X access point, a VPN server, or a DHCP server.

For information about how to configure NPS for system health requirements, see Configuring Network Access Protection Policies in Windows Server "Longhorn".

Additional Components and Resources for Network Access Protection

Network Access Protection consists of additional server components, additional client components, remediation servers, and policy servers. Administrators can configure some or all of the following components when they implement Network Access Protection.

Client Components for Network Access Protection

NAP Agent

The NAP Agent is client software that coordinates information between the various system health agents (SHAs) and NAP enforcement clients (ECs).

[1] 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 (now in beta testing). 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 Network Access Protection. It is compatible with VPN servers using Network Access Protection, although administrators might need to adjust some scripts. Administrators can use Network Access Quarantine Control and Network Access Protection simultaneously.

System Health Agent

A system health agent (SHA) is client software that integrates with the NAP Agent to provide system policy checks and to indicate system health. An SHA uses a Statement of Health (SoH) to define its health state.

Server Components for Network Access Protection

NAP Administration Server

The NAP Administration Server is component of an NPS server that coordinates the output from all the system health validators (SHVs) and determines whether NAP Enforcement Server (NAP ES) components should limit the access of a client based on the configured health policy requirements.

System Health Validator

A system health validator (SHV) is server software that validates whether the Statement of Health (SoH) submitted by an SHA complies with the required health state. SHVs run on the NPS server, which must coordinate the output from all of the SHVs. An SHV uses a Statement of Health Response (SoHR) to indicate either compliance with the required health state or noncompliance with the required health state and remediation instructions.

Health Policy

A health policy specifies the required conditions for unlimited access. Health policies are configured on the NPS server. A network might have more than one health policy. For example, VPN Enforcement and DHCP Enforcement might use different health policies.

Accounts Database

An accounts database stores user and computer accounts and their network access properties. For Windows Server "Longhorn" domains, Active Directory functions as the accounts database.

Health Certificate Server

A health certificate server is the combination of a Health Registration Authority (HRA)—a computer running Windows Server "Longhorn" and Internet Information Services (IIS)—and a certification authority (CA). The CA can be installed on the computer running Windows Server “Longhorn” or it can be installed on a separate computer. The health certificate server obtains health certificates for compliant computers. A health certificate can be used instead of Statements of Health (SoHs) to prove that a client is compliant with system health requirements.

Remediation Server

Remediation servers consist of servers, services, or other resources that a noncompliant computer on the restricted network can access. These resources might perform name resolution or store the most recent software updates or components needed to make the computer comply with health requirements. For example, a secondary 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.

Policy Server

SHVs communicate with policy servers to validate the SoH from a corresponding SHA.

How Network Access Protection Works

Network Access Protection is designed so that administrators can configure it to meet the needs of individual networks. Therefore, the actual configuration of Network Access Protection will vary according to the administrator's preferences and requirements. However, the underlying operation of Network Access Protection remains the same. The following diagram and steps illustrate how Network Access Protection works in an example network.

When evaluating the following, keep in mind that Network Access Protection is not a security solution. It is designed to help prevent computers with unsafe configurations from connecting to a network, not to protect networks from malicious users who have valid sets of credentials and computers that meet current health requirements.

Figure 1 shows an example network for Network Access Protection.

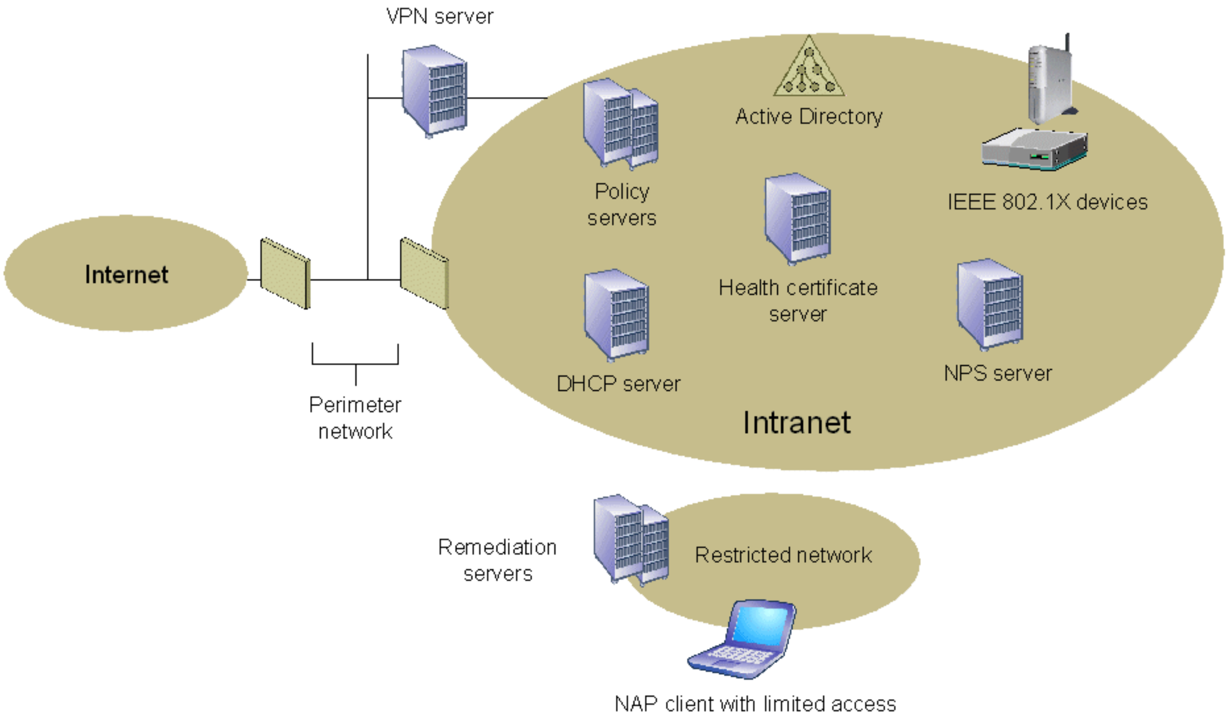

Figure 1 Example network in which Network Access Protection has been deployed

The example network is configured for IPsec Enforcement, 802.1X Enforcement, VPN Enforcement, and DHCP Enforcement. NPS is installed on a separate server. The NPS server acts as health policy server. This example network is configured for health policy validation, health policy compliance, and limited network access for noncompliant computers.

When obtaining a health certificate, making an 802.1X or VPN connection to the network, or leasing or renewing an IP address from the DHCP server, each computer is classified in one of the following ways:

- Computers that meet the health policy requirements are classified as compliant and allowed unlimited access to the network.

- Computers 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 computer does not necessarily have a virus or some other active threat to the network, but it does not have the software and configuration required by network health policy. Therefore, noncompliant computers pose health risks to the rest of the network. SHAs automatically update computers with limited access with the software required for unlimited access.

The example network contains a restricted network. A restricted network can be defined logically or physically. Restrictions can be placed on computers with limited access—such as IP filters, static routes, or a VLAN identifier—to define the remediation servers with which they can communicate.

IPsec Enforcement

The following process describes how IPsec Enforcement works for a NAP client that has only a single SHA on a network configured similarly to the network in Figure 1:

1. When the NAP client starts, it sends its current SoH to the health certificate server.
2. The health certificate server passes the SoH information to the NPS server. The NPS server communicates with the policy server to determine whether the SoH is valid.
   A. If the SoH is valid, the health certificate server issues the NAP client a health certificate. The NAP client can now initiate IPsec-based communication with secure resources using the issued health certificate for IPsec authentication, and respond to communications initiated from other NAP clients that can authenticate using their own health certificate.

   B. If the SoH is not valid, the health certificate server informs the NAP client how to correct its health state and 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 the remediation server to bring itself back into compliance.
3. The NAP Agent on the restricted NAP client sends update requests to the remediation server.
4. The remediation server provisions the NAP client with the required updates to bring it into compliance with health policy. The NAP client's SoH is updated.
5. The NAP client sends its updated SoH to the health certificate server. When the NPS server validates the updated SoH, the health certificate server issues a health certificate to the NAP client.

Depending on network needs, an administrator might choose to make some computers, devices, and users exempt from health policy requirements. For example, some versions of Windows do not support Network Access Protection, so computers running these versions of Windows always have limited access by default. However, the network administrator can configure an exception for these computers. Excepted computers are not checked for compliance, and they will have unlimited access to the network.

802.1X Enforcement

The following process describes how 802.1X Enforcement works for an 802.1X client that has only a single SHA on a network configured similarly to the network in Figure 1:

1. The 802.1X client initiates a connection to the 802.1X access point.

2. The 802.1X client passes its authentication credentials to the 802.1X access point using PEAP and a PEAP method such as MS-CHAP v2.
3. If the authentication credentials are valid, the NPS server requests an SoH from the 802.1X client.
4. If the 802.1X client has an SoH, the client passes the SoH to the NPS server. The NPS server communicates with the policy server to determine whether the SoH is valid.
   A. If the SoH is valid, the 802.1X access point completes the connection and grants the 802.1X client unlimited access to the network, as defined by policy.
   B. If the SoH is not valid, the 802.1X access point completes the connection but limits the access of the 802.1X client to the restricted network. The 802.1X client can successfully send traffic only to the restricted network, the 802.1X access point, and the software update remediation server.
5. If the 802.1X client does not have an SoH, it is not compliant. The 802.1X access point completes the connection but limits the access of the 802.1X client to the restricted network.
6. The NAP Agent on the noncompliant 802.1X client sends update requests to the remediation server.
7. The remediation server provisions the 802.1X client with the required updates to bring it into compliance with health policy. The 802.1X client's SoH is updated.
8. The 802.1X client restarts 802.1X authentication and sends its updated SoH to the NPS server. When the NPS server validates the updated SoH, the 802.1X access point grants the 802.1X client unlimited access to the network, as defined by policy.

An 802.1X NAP client can also use a health certificate, rather than its SoH, to indicate its health status to an NPS server.

VPN Enforcement

The following process describes how VPN Enforcement works for a VPN client that has only a single SHA on a network configured similarly to the network in Figure 1:

1. The VPN client initiates a connection to the VPN server.
2. The VPN client passes its authentication credentials to the VPN server using Protected Extensible Authentication Protocol (PEAP) and Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2).
3. If the authentication credentials are valid, the VPN server requests an SoH from the VPN client.
4. If the VPN client has an SoH, the client passes the SoH to the VPN server, which passes the SoH to the NPS server. The NPS server communicates with the policy server to determine whether the SoH is valid.
   A. If the SoH is valid, the VPN server completes the connection and grants the VPN client unlimited access to the network, as defined by policy.
   B. If the SoH is not valid, the VPN server completes the connection but limits the access of the VPN client to the restricted network. The VPN client can successfully send traffic only to the restricted network, the VPN server, and the remediation server.
5. If the VPN client does not have an SoH, it is not compliant. The VPN server completes the

connection but limits the access of the VPN client to the restricted network.

6. The NAP Agent on the noncompliant VPN client sends update requests to the remediation server.
7. The remediation server provisions the VPN client with the required updates to bring it into compliance with health policy. The VPN client’s SoH is updated.
8. The VPN client sends its updated SoH to the NPS server. When the NPS server validates the updated SoH, the VPN server grants the VPN client unlimited access to the network, as defined by policy.

DHCP Enforcement

The following process describes how DHCP Enforcement works on a network configured similarly to the network in Figure 1 when a DHCP client that has only a single SHA must lease or renew a lease on an IP address:

1. The DHCP client sends a DHCP request message to the DHCP server.
   A. If the DHCP client has an SoH, the DHCP request message includes it. The SoH contains information about the health of the client. The DHCP server passes the SoH to the NPS server. The NPS server communicates with the policy server to determine whether the SoH is valid.
      I. If the SoH is valid, the DHCP server assigns the DHCP client a complete IP address configuration. The DHCP client has unlimited access to the network, as defined by policy.
      II. If the SoH is not valid, the DHCP server limits the access of the DHCP client to the restricted network and assigns it a limited access subnet mask and static routes, as defined by policy.
   B. If the DHCP client does not have an SoH, it is not compliant. The DHCP server limits the access of the DHCP client to the restricted network, as the network administrator has defined.
2. The NAP Agent on the DHCP client sends update requests to the remediation server.
3. The remediation server provisions the DHCP client with the required updates to bring it into compliance with health policy. The DHCP client’s SoH is updated.
4. The DHCP client sends a DHCP request message, including the updated SoH, to the DHCP server. When the NPS server validates the updated SoH, the DHCP server grants the DHCP client unlimited access to the network, as defined by policy.

Assumptions and Limitations

Some of the assumptions and limitations of Network Access Protection include:

- To configure a network with Network Access Protection, administrators must understand Windows components and technologies such as IPsec, 802.1X authentication, VPNs, DHCP, NPS, Active Directory, Certificate Services, and Group Policy.
- Computers that are not compliant do not have to have their access limited. Administrators can choose what level of action to take.
- Network Access Protection does not protect against malicious users whose computers meet network health requirements.

- Computers have their access limited to a restricted network only if they connect to the network through an enforcement mechanism that supports Network Access Protection, such as 802.1X authentication, a VPN connection, or DHCP configuration.
- The DHCP, DNS, and remediation servers must be accessible to all computers, whether or not they have unlimited access. Active Directory domain controllers might or might not be accessible to computers that have limited access.
- DNS servers that are on the restricted network do not have to be primary DNS servers. They can be secondary servers or even simple forwarders that can forward queries to DNS servers outside the restricted network.
- SHAs and SHVs can be matched to a corresponding policy server and remediation server. For example, an antivirus SHA, an antivirus SHV, an antivirus policy server, and an antivirus remediation server are matched for a specific antivirus software vendor.

Summary

Network Access Protection is a new platform to limit the access of connecting computers until they are compliant with system health requirements. Network Access Protection includes client and server components. Administrators can configure IPsec Enforcement, 802.1X Enforcement, VPN Enforcement, DHCP Enforcement, or all of them, depending on their network needs. Network Access Protection provides an infrastructure and an API, which vendors and software developers can use to build their own health requirements validation and network access limitation components that are compatible with Network Access Protection.

Related Links

See the following resources for further information:

- Network Access Protection Web site at http://www.microsoft.com/nap
- Network Access Protection Platform Architecture at http://www.microsoft.com/technet/itsolutions/network/nap/naparch.mspx
- Network Access Protection Frequently Asked Questions at http://www.microsoft.com/technet/itsolutions/network/nap/napfaq.mspx

For the latest information about Windows Server System, see the Windows Server System Web site at http://www.microsoft.com/windowsserversystem.