Network Access Protection: New Ways To Keep Your Network Healthy
Network Access Protection: New Ways To Keep Your Network Healthy

Mark Mizrahi, Global Knowledge Instructor, MCSE, MCT

What It Is

Network Access Protection (NAP) is a security-policy enforcement technology built into Windows Server Longhorn, Windows Vista, and WindowsXP-sp2 that allow a computer administrator to develop and enforce compliance with health policies for network access and communication. NAP provides administrator-defined requirements for system health policy enforcement that help ensure computers connecting to a network or communicates on a network meet these policy requirements. NAP also provides an Application Programming Interface (API) to help administrators, developers and vendors enforce compliance with health policies for network access and communication.

Network Access Protection is also known as a network quarantine platform from Microsoft that isolates a computer that might be a danger to your network until they are patched or until it gets updated with antivirus software, the firewall is enabled, or it complies with whatever measures your company’s security policies dictate. NAP supports IPsec, DHCP, VPN 802.1X, and a Terminal Server quarantine enforcement client.

One of the most time-consuming, resource-intensive duties a network administrator faces is ensuring that computers are kept up-to-date with health policy requirements, also known as computer health, before they access their private networks or communicate with network resources. Some of the challenges are the traveling laptops, home computers, and even the internal desktop machines, all of which might not meet the health policies that a private network is trying to maintain. NAP provides a mechanism to ensure ongoing compliance as the security policies change.

Health policies requirements are put in place to protect the private network’s overall integrity from clients, who might have out-of-date or no virus protection, malicious programming code installed, out-of-date software updates, improper vendor specific and custom programs, and miss configured configurations, connect to resources. These health policies are required to maintain the integrity and security of the private network and can be easily managed and changed at any time.

How It Works

When a user attempts to connect to the network, either remotely or internally, the computer sends a Statement of Health (SoH) to the NAP server, a Longhorn Server system configured as a Network Policy Server (NPS). The NPS communicates with policy servers, such as antivirus and patch-management servers, to determine whether the PC meets the predetermined health policy. NAP can be used simply as a tracking tool to monitor all computers and grant them access to the network even if they don’t comply with health policies. The computers compliance state is logged for review at any time.
For more restrictive access to the network, NAP can be set up to restrict or limit access to the private network, while permitting access to a restricted area of the network, and automatically update computers with software updates to meet health policy requirements. If a computer has all the software and configurations that the health policy requires, the computer is considered compliant and will be allowed in to access the network. Noncompliant computers are quarantined and can be redirected to a remediation server to receive the proper updates and configurations that will make the machine compliant with the health policy. Then, private network access will be granted.

Four Features of Network Access Protection

1. Health Policy Validation
   When a user attempts to connect to a network, the computer’s SoH is validated against the health policies of the private network. The NPS communicates with a System Health Verifier (SHV) such as an anti-virus server or a path-management server to check the SoH of client machines running NAP client software. The client machine accessing the network is known as a System Health Agent (SHA). Based on the SoH by the SHA, the SHV verifies health compliance and can redirect the client to the proper remediation server to obtain the proper items necessary to become compliant.

2. Isolation
   NAP can be configured to limit, redirect, or restrict traffic of noncompliant computers. Restrictions can be set for a specific amount of time, redirecting to a quarantined part of the private network or restrictions to specific resources. Exceptions might be placed on specific health policy requirements by allowing customized limited access.

3. Remediation
   Noncompliant computers can be automatically updated with the required software, updates, and configuration necessary to conform to the current health policy. When compliance is reached, the computer is granted access to the private network. Microsoft Systems Management Server or a Remediation Server can provide the missing requirements needed by the noncompliant computer to be compliant for network access.

4. Ongoing Compliance
   Automatic remediation is built into Network Access Protection within the SHA. If your machine is out of compliance, you will be notified of the consequence (e.g., limited network connectivity). The SHA will do its best to automatically remediate. If your machine is out of compliance, it will follow the SHA’s instructions, such as turning on the firewall, etc., to get out of quarantine. You can also specify deferred enforcement. If, for example, a service pack is needed, you won’t be quarantined, but you will have 30 days to comply with the health policy, after which time NAP will download it automatically.

Four Enforcement Technologies

1. Internet Protocol Security (IPsec)
   IPsec enforcement is the strongest form of limited network access for Network Access Protection. It consists of a health certificate server and an IPsec NAP Enforcement Client (EC). The health certificates server issues a X.509 certificate to a client that has been quarantined to allow access after they are determined to be compliant. The certificate is then used to authenticate NAP clients when they initiate IPsec-secured communications. With IPsec, you can define requirements for secure communications with compliant clients based on IP address or TCP/UDP port numbers.
2. 802.1X Authentication

802.1X enforcement provides strong limited network access for computers. It consists of a NPS and an Extensible Authentication Protocol (EAP) Host running NAP EC software. If a client is non-conforming, the NPS server instructs the 802.1X wireless access point or Ethernet switch to place a restricted access profile on the 802.1X client until it performs a remediation. A restricted access profile can consist of IP packet filters or a Virtual LAN (VLAN) identifier to quarantine the traffic of an 802.1X client.

3. Virtual Private Network (VPN) Enforcement

When a VPN client initiates a connection to the VPN Server using Protected Extensible Authentication (PEAP) and Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2), the VPN server requests a SoH from the client. The VPN server passes the SoH to the NPS. The NPS communicates with the policy server to determine whether the SoH is valid. The client is granted full access or restricted access, depending on the validity of the client's SoH. The NAP agent on the client computer sends an update request to the remediation server and gives the VPN client the required updates to conform to the health policy. The VPN client sends its updated SoH to the NPS. The VPN server now grants the client access to the network.

4. DHCP Enforcement

The DHCP client sends a DHCP request that includes the SoH. The DHCP server passes the SoH to the NPS, which communicates with the policy server to determine the validity of the SoH. If the SoH is valid, the DHCP server assigns the DHCP client a complete IP address configuration for full access to the network. If the SoH is not valid, the DHCP server assigns the client an IP address configuration that will limit the client to a restricted part of the network. The NAP agent on the client sends an update request to the remediation server that updates the client with the current health policy. Then the client sends a DHCP request with updated SoH to the DHCP server and when the NPS validates the SoH, the DHCP server assigns a complete full access IP configuration to the network.

![Figure 1. Diagram of Components of a NAP-enabled network infrastructure](Image)
Defining the Components of a NAP-enabled Network Infrastructure

**NAP clients:** Computers that support the NAP platform for protected communication using IPsec, IEEE 802.1X authentication, remote access VPN connections, and DHCP configuration.

**NAP servers:** Computers running Windows Server Longhorn that use a NPS to determine the health state of NAP clients, whether network access or communication is allowed, and the set of remediation actions that a noncompliant client must perform. Examples of NAP servers are the following:

- **Health certificate server:** 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 (HCS) obtains health certificates for compliant NAP clients.

- **VPN server:** Routing and Remote Access on a computer running Windows Server Longhorn allows VPN-based remote access connections to an intranet.

- **DHCP server:** The DHCP Server service on a computer running Windows Server Longhorn provides automatic IP address configuration to intranet clients.

**NPS servers:** The NPS runs on a computer running Windows Server Longhorn and provides network access and health policy requirement validation. NPS is the replacement for the Internet Authentication Service (IAS) provided with Windows Server 2003. NPS can run on an HCS, a VPN server, a DHCP server or, more commonly, as shown in Figure 1, on a separate server for centralized configuration of network access and health requirement policies.

**Policy servers:** Policy servers are computers that provide current system health state for NPS servers.

**Active Directory® directory service:** Active Directory is the Windows directory service that stores credentials for VPN and 802.1X-based connections and Group Policy settings for IPsec-based communication.

**Restricted network:** A separate logical or physical network that contains:

- **Remediation servers:** These are computers that contain health update resources, such as the necessary updates, configurations, and applications that NAP clients can access to remediate their noncompliant state. Examples include antivirus signature distribution servers and software update servers.

- **NAP clients with limited access:** These are computers that are placed on the restricted network when the clients do not comply with health requirement policies.
The Different Methods of Contacting a NAP-enabled Network

Between a NAP client and an HCS
The NAP client uses HyperText Transfer Protocol (HTTP) over Secure Sockets Layer (SSL) (HTTPS) to create a secure session with the HCS to indicate its current system health state and request a health certificate. The HCS uses the secure HTTPS session to send remediation instructions (if the NAP client is noncompliant) or a health certificate (if the NAP is compliant).

Between a NAP client and an 802.1X access point
The NAP client, acting as an 802.1X client, uses PEAP messages sent over EAP over LAN (EAPOL) to perform authentication of the 802.1X connection and to indicate its current system health state to the NPS server. The NPS server uses PEAP messages to indicate either remediation instructions (because the 802.1X client is noncompliant) or that the 802.1X client has unlimited access to the intranet. PEAP messages between the 802.1X client and NPS server are routed through the 802.1X access point (an Ethernet switch or a wireless access point).

Between a NAP client and a VPN server
The NAP client acting as a VPN client uses Point-to-Point Protocol (PPP) messages to establish a VPN connection and PEAP messages over the PPP connection to indicate its current system health state to the NPS server. The NPS server uses PEAP messages to indicate either remediation instructions (because the VPN client is noncompliant) or that the VPN client has unlimited access to the intranet. PEAP messages between the VPN client and NPS server are routed through the VPN server.

Between a NAP client and a DHCP server
The NAP client acting as a DHCP client uses DHCP messages to obtain a valid IPv4 address configuration and to indicate its current system health state. The NAP server uses DHCP messages to allocate either an IPv4 address configuration for the restricted network and indicate remediation instructions (if the DHCP client is noncompliant), or an IPv4 address configuration for unlimited access (if the DHCP client is compliant).

Between a NAP client and a remediation server
While the NAP client has unlimited access to the intranet, it accesses the remediation server to ensure that it remains compliant. For example, the NAP client periodically checks an antivirus server to ensure that it has the latest antivirus signature file or a software update server, such as Windows Update Services, to ensure that it has the latest operating system updates.

If the NAP client has limited access, it communicates with the remediation server to become compliant, based on instructions from the NPS server. For example, if during the health validation process the NPS server determined that the NAP client does not have the most current antivirus signature file, the NPS server instructs the NAP client to update its local signature file with the latest file that is stored on a specified antivirus server.

Between an HCS and an NPS server
The HCS sends Remote Authentication Dial-In User Service (RADIUS) messages containing the settings of the NAP client’s system health state to the NPS server.
The NPS server sends RADIUS messages to:

- Indicate that the NAP client has unlimited access because it is compliant. Based on this response, the HCS obtains a health certificate and sends it to the NAP client.

- Indicate that the NAP client has limited access until it performs a set of remediation functions. Based on this response, the HCS does not issue a health certificate to the NAP client.

**Between an 802.1X access point and an NPS server**
The 802.1X access point sends RADIUS messages to transfer PEAP messages sent by an 802.1X NAP client.

The NPS server sends RADIUS messages to:

- Indicate that the 802.1X client has unlimited access because it is compliant.

- Indicate a limited access profile to place the 802.1X client on the restricted network until it performs a set of remediation functions. A limited access profile can consist of a set of IP packet filters or a virtual LAN identifier to confine the traffic of a noncompliant 802.1X client.

- Send PEAP messages to an 802.1X NAP client.

**Between a VPN server and an NPS server**
The VPN server sends RADIUS messages to transfer PEAP messages sent by a VPN-based NAP client. The NPS server sends RADIUS messages to:

- Indicate that the VPN client has unlimited access because it is compliant.

- Indicate that the VPN client has limited access until it performs a set of remediation functions.

- Send PEAP messages to a VPN-based NAP client.

**Between a DHCP server and an NPS server**
The DHCP server sends RADIUS messages to the NPS server that contains the DHCP client's system health state.

The NPS server sends RADIUS messages to the DHCP server to:

- Indicate that the DHCP client has unlimited access because it is compliant.

- Indicate that the DHCP client has limited access until it performs a set of remediation functions.

**Between an NPS server and a policy server**
When performing network access validation for a NAP client, the NPS server might have to contact a policy server to obtain information about the current requirements for system health. For example, the NPS server might have to contact an antivirus server to check for the version of the latest signature file or to contact a software update server to obtain the date of the last set of operating system updates and patches.
Summary

Network Access Protection is a new platform available with Windows Longhorn Server, Windows Vista, and Windows XPsp2 to limit network access by computers until they are compliant with the system health policies. NAP includes client and server components. Administrator can configure enforcement policies with technologies using IPsec Enforcement, 802.1X Enforcement, VPN Enforcement, and DHCP Enforcement. Any one or combinations of enforcement policies can be used and customized for various access needs. NAP provides an API for vendors and software developers to build their own health requirements, validation, and network access limitations that are compatible with NAP. NAP also reduces the administrative task of maintaining the integrity of client computers accessing their networks by using this centralized management, quarantine, and remediation technology.

About the Author

Mark Mizrahi has been an MCSE since NT3.51 with a specialty in Security. He is an MCT and currently teaches Microsoft curriculum for Global Knowledge. He is President of Standard Computer Services and consults for various Fortune 500 companies. He designs and implements web-based Internet security and video surveillance systems for a diversified customer base. Keeping up with the new technologies of Windows Vista and Longhorn platforms is part of his daily intake of information, and he loves sharing it with his clients and students.
Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out our complete list of Microsoft courses at www.globalknowledge.com/microsoft or call 1-800-COURSES to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.