Module 8

Configuring Network Access Protection

Contents:
Lesson 1: Overview of Network Access Protection 8-3
Lesson 2: How NAP Works 8-18
Lesson 3: Configuring NAP 8-27
Lesson 4: Monitoring and Troubleshooting NAP 8-34
Lab: Configuring NAP for DHCP and VPN 8-38
Module Overview

- Overview of Network Access Protection
- How NAP Works
- Configuring NAP
- Monitoring and Troubleshooting NAP

Network Access Protection (NAP) ensures compliance with specific health policies for systems accessing the network. NAP assists administrators in achieving and maintaining a specific health policy. This module provides information about how NAP works, and how to configure, monitor, and troubleshoot NAP.
Lesson 1
Overview of Network Access Protection

- What is Network Access Protection?
- NAP Scenarios
- NAP Enforcement Methods
- NAP Platform Architecture
- NAP Architecture Interactions
- NAP Client Infrastructure
- NAP Server-Side Infrastructure
- Communication Between NAP Platform Components

NAP is a system health policy enforcement platform built into Windows Server 2008, Windows Vista™, and Windows® XP Service Pack 3 (which includes the NAP Client for Windows XP, now in beta testing), that allows you to better protect private network assets by enforcing compliance with system health requirements. With NAP, you can create customized health requirement policies to validate computer health before allowing access or communication, automatically update compliant computers to ensure ongoing compliance, and limit the access of noncompliant computers to a restricted network until they become compliant.
What is 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.

NAP has three important and distinct aspects:

- Health state validation
- Health policy compliance
- Limited access

**Question:** How would you use NAP enforcement in your environment, considering home users, roaming laptops and outside business partners?
Additional Reading

- Introduction to Network Access Protection
NAP Scenarios

NAP benefits the network infrastructure by verifying the health state of:

- Roaming laptops
- Desktop computers
- Visiting laptops
- Unmanaged home computers

NAP helps provide a solution for the following common scenarios:

- Verifying the health state of roaming laptops
- Verifying the health state of desktop computers
- Verifying the health state of visiting laptops
- Verifying the health state of unmanaged home computer

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

**Question:** Have you ever had an issue with non-secure, unmanaged laptops causing harm to the network? Do you think NAP would have addressed this issue?

**Additional Reading**

- Network Access Protection
## NAP Enforcement Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Key Points</th>
</tr>
</thead>
</table>
| IPSec enforcement for IPSec-protected communications | • Computer must be compliant to communicate with other compliant computers  
• The strongest NAP enforcement type and can be per-IP address or per protocol port number |
| 802.1X enforcement for IEEE 802.1X-authenticated wired or wireless connections | • Computer must be compliant to obtain unlimited access through an 802.1X connection (authentication switch or access point) |
| VPN enforcement for remote access connections | • Computer must be compliant to obtain unlimited access through a RAS connection |
| DHCP enforcement for DHCP-based address configuration | • Computer must be compliant to receive an unlimited access IPv4 address configuration from DHCP  
• This is the weakest form of NAP enforcement |

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
- Institute of Electrical and Electronics Engineers (IEEE) 802.1X-authenticated network connections
- Remote access VPN connections
- Dynamic Host Configuration Protocol (DHCP) address configurations

Windows Vista and Windows Server 2008 also include NAP support for Terminal Services Gateway (TS Gateway) connections.
The following sections describe the IPSec, 802.1X, VPN, DHCP and TS Gateway enforcement methods.

- IPSec Enforcement
- 802.1X Enforcement
- VPN Enforcement
- DHCP Enforcement
- Terminal Services Gateway

**Question:** Which of the NAP enforcement types would best suit your company? Can you see your organization using multiple NAP enforcement types? If so, which ones?

**Additional Reading**
- Terminal Services
- Network Access Protection
NAP Platform Architecture

The components of a NAP-enabled network infrastructure consist of the following:

- NAP clients
- NAP enforcement points

Examples of NAP enforcement points are the following:

- Health Registration Authority (HRA)
- VPN server
- DHCP server
- Network access devices
- NAP health policy servers
- Health requirement servers
• Active Directory® Domain Service
• Restricted network, which includes:
  • Remediation servers
  • NAP clients with limited access

**Question:** Does your environment presently use 802.1x authentication at the switch level? If so, would 802.1x NAP be beneficial considering remediation VLANs can be configured to offer limited access?

**Additional Reading**
• Network Access Protection Platform Architecture
The interactions for the computers and devices of a NAP-enabled network infrastructure are as follows:

- Between a NAP client and an HRA
- Between a NAP client and an 802.1X network access device (an Ethernet switch or a wireless access point)
- Between a NAP client and a VPN server
- Between a NAP client and a DHCP server
- Between a NAP client and a remediation server
- Between an HRA and a NAP health policy server
- Between an 802.1X network access device and a NAP health policy server
- Between a VPN server and a NAP health policy server
- Between a DHCP server and a NAP health policy server
- Between a NAP health policy server and a health requirement server
Additional Reading

- Network Access Protection Platform Architecture
The NAP client architecture consists of the following:

- A layer of NAP enforcement client (EC) components
- A layer of system health agent (SHA) components
- NAP Agent
- SHA application programming interface (API)
- NAP EC API

The NAP ECs for the NAP platform supplied in Windows Vista, Windows Server 2008, and Windows XP with SP2 (with the NAP Client for Windows XP) are the following:

- An IPSec NAP EC for IPSec-protected communications
- An EAPHost NAP EC for 802.1X-authenticated connections
• A VPN NAP EC for remote access VPN connections
• A DHCP NAP EC for DHCP-based IPv4 address configuration

**Question:** How would your organization deal with enabling the appropriate enforcement client (EC) on non-domain computers outside of the management scope?

**Additional Reading**
• Network Access Protection Platform Architecture
• Network Access Protection Platform Software Development Kit (SDK)
NAP Server-Side Infrastructure

A Windows-based NAP enforcement point has a layer of NAP Enforcement Server (ES) components. Each NAP ES is defined for a different type of network access or communication. For example, there is a NAP ES for remote access VPN connections and a NAP ES for DHCP configuration. The NAP ES is typically matched to a specific type of NAP-capable client. For example, the DHCP NAP ES is designed to work with a DHCP-based NAP client. Third-party software vendors or Microsoft can provide additional NAP ESs for the NAP platform.

Additional Reading
• Network Access Protection Platform Architecture
Communication Between NAP Platform Components

The NAP Agent component can communicate with the NAP Administration Server component through the following process:

1. The NAP Agent passes the SSoH to the NAP EC.
2. The NAP EC passes the SSoH to the NAP ES.
3. The NAP ES passes the SSoH to the NPS service.
4. The NPS service passes the SSoH to the NAP Administration Server.

The NAP Administration Server can communicate with the NAP Agent through the following process:

1. The NAP Administration Server passes the SoHRs to the NPS service.
2. The NPS service passes the SSoHR to the NAP ES.
3. The NAP ES passes the SSoHR to the NAP EC.
4. The NAP EC passes the SSoHR to the NAP Agent.
An SHA can communicate with its corresponding SHV through the following process:

1. The SHA passes its SoH to the NAP Agent.
2. The NAP Agent passes the SoH, contained within the SSoH, to the NAP EC.
3. The NAP EC passes the SoH to the NAP ES.
4. The NAP ES passes the SoH to the NAP Administration Server.
5. The NAP Administration Server passes the SoH to the SHV.

The SHV can communicate with its corresponding SHA through the following process:

1. The SHV passes its SoHR to the NAP Administration Server.
2. The NAP Administration Server passes the SoHR to the NPS service.
3. The NPS service passes the SoHR, contained within the SSoHR, to the NAP ES.
4. The NAP ES passes the SoHR to the NAP EC.
5. The NAP EC passes the SoHR to the NAP Agent.
6. The NAP Agent passes the SoHR to the SHA.

**Additional Reading**
- Network Access Protection Platform Architecture
Lesson 2: How NAP Works

- NAP Enforcement Processes
- How IPSec Enforcement Works
- How 802.1X Enforcement Works
- How VPN Enforcement Works
- How DHCP Enforcement 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.

When a client attempts to access the network or communicate on the network, it must present its system health state or proof of health compliance. If a client cannot prove it is compliant with system health requirements (for example, that it has the latest operating system and antivirus updates installed), its access to the network or communication on the network can be limited to a restricted network containing server resources so that health compliance issues can be remedied. After the updates are installed, the client requests access to the network or attempts the communication again. If compliant, the client is granted unlimited access to the network or the communication is allowed.
Network Access Protection (NAP) is a policy enforcement platform built into the Windows Vista, the Microsoft Windows XP, and the Windows Server 2008 operating systems that allows you to better protect network assets by enforcing compliance with system health requirements.

To validate access to a network based on system health, a network infrastructure needs to provide the following areas of functionality:

- **Health policy validation**: Determines whether the computers are compliant with health policy requirements.
- **Network access limitation**: Limits access for noncompliant computers.
- **Automatic remediation**: Provides necessary updates to allow a noncompliant computer to become compliant.
- **Ongoing compliance**: Automatically updates compliant computers so that they adhere to ongoing changes in health policy requirements.
Additional Reading

- Network Access Protection (NAP) for Windows Server 2008
How IPSec Enforcement Works

IPSec enforcement limits communication for IPSec-protected NAP clients by dropping incoming communication attempts that are sent from computers that cannot negotiate IPSec protection using health certificates. Unlike 802.1X and VPN enforcement, IPSec enforcement is performed by each individual computer, rather than at the point of entry into the network. Because you can take advantage of IPSec policy settings, the enforcement of health certificates can be done for all the computers in a domain, specific computers on a subnet, a specific computer, a specific set of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports, or for a set of TCP or UDP ports on a specific computer.

IPSec enforcement defines the following logical networks:

- Secure network
- Boundary network
- Restricted network
Based on the definition of the three logical networks, the following types of initiated communications are possible:

- Computers in the secure network can initiate communications with computers in all three logical networks.
- Computers in the boundary network can initiate communications with computers in the secure or boundary networks that are authenticated with IPSec and health certificates or with computers in the restricted network that are not authenticated with IPSec.
- Computers in the restricted network can initiate communications with computers in the restricted and boundary networks.

**Question:** What types of computers in the secure network would you allow unsecure communication from computers in the restricted network to succeed?

**Answer:** IP filters can be created to allow certain communications to not be

**Additional Reading**

- Network Access Protection
How 802.1x Enforcement Works

IEEE 802.1X enforcement instructs an 802.1X-capable access point to use a limited access profile, either a set of IP packet filters or a VLAN ID, to limit the traffic of the noncompliant computer so that it can reach only resources on the restricted network. For IP packet filtering, the 802.1X-capable access point applies the IP packet filters to the IP traffic that is exchanged with the 802.1X client and silently discards all packets that do not correspond to a configured packet filter. For VLAN IDs, the 802.1X-capable access point applies the VLAN ID to all of the packets exchanged with the 802.1X client and the traffic does not leave the VLAN corresponding to the restricted network.

If the NAP client is noncompliant, the 802.1X connection has the limited access profile applied and the NAP client can only reach the resources on the restricted network.

**Question:** What must the network devices support to be able to implement 802.1x NAP?
Additional Reading

- Network Access Protection Platform Architecture
- Network Access Protection
How VPN Enforcement Works

VPN enforcement uses a set of remote access IP packet filters to limit the traffic of the VPN client so that it can only reach the resources on the restricted network. The VPN server applies the IP packet filters to the IP traffic that is received from the VPN client and silently discards all packets that do not correspond to a configured packet filter.

If the VPN client is noncompliant, the VPN connection has the packet filters applied, and the VPN client can only reach the resources on the restricted network.

Question: How does the VPN NAP enforcement method respond to non-compliant computers that make connection attempts?

Additional Reading
- Network Access Protection Platform Architecture
How DHCP Enforcement Works

DHCP address configuration limits network access for the DHCP client through its IPv4 routing table. DHCP enforcement sets the DHCP Router option value to 0.0.0.0, so the noncompliant computer does not have a configured default gateway. DHCP enforcement also sets the subnet mask for the allocated IPv4 address to 255.255.255.255, so that there is no route to the attached subnet.

To allow the noncompliant computer to access the remediation servers on the restricted network, the DHCP server assigns the Classless Static Routes DHCP option, which contains a set of host routes to the computers on the restricted network, such as the DNS and remediation servers.

**Question:** Does the DHCP NAP enforcement type work on IPv6 networks?

**Additional Reading**
- Network Access Protection Platform Architecture
Lesson 3: Configuring NAP

- What Are System Health Validators?
- What is a Health Policy?
- What are Remediation Server Groups?
- NAP Client Configuration
- Demonstration: Using the Configure NAP Wizard to Apply Network Access Policies

This lesson provides information about configuring the client to interoperate with the server-side infrastructure of a NAP enforced environment.
What are 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.

**Question:** Does NAP only work with Microsoft-supplied System Health Validators?

**Additional Reading**
- Network Access Protection Platform Architecture
- Introduction to Network Access Protection
What is a Health Policy?

Health policies consist of one or more system health validators (SHVs) and other settings that allow you to define client computer configuration requirements for the NAP-capable computers that attempt to connect to your network.

Question: Can you only use one System Health Validator (SHV) in a health policy?

Additional Reading
- Help Topic: Health Policies
What are Remediation Server Groups?

A remediation server group is a list of servers on the restricted network that provide resources required to bring noncompliant NAP-capable clients into compliance with administrator-defined client health policy.

**Question:** What services might a remediation server offer to update anti-virus signatures?

**Additional Reading**
- Help Topic: Remediation Server Groups
NAP Client Configuration

- Some NAP deployments that use Windows Security Health Validator require that Security Center is enabled.
- The Network Access Protection service is required when you deploy NAP to NAP-capable client computers.
- You must also configure the NAP enforcement clients on the NAP-capable computers.

Use the following basic guidelines when performing NAP client configuration:

- Some NAP deployments that use Windows Security Health Validator require that Security Center is enabled.
- The Network Access Protection service is required when you deploy NAP to NAP-capable client computers.
- You must also configure the NAP enforcement clients on the NAP-capable computers.

Question: What Windows groups have the rights to enable Security Center in Group Policy, enable NAP service on clients and enable/disable NAP enforcement clients?
Additional Reading

- Help Topic: Enable Security Center in Group Policy
- Help Topic: Enable the Network Access Protection Service on Clients
- Help Topic: Configure NAP Enforcement Clients
Demonstration: Using the Configure NAP Wizard to Apply Network Access Policies

**In this demonstration, you will see how to:**
- Create DHCP NAP policies
- Configure DHCP enforcement on the DHCP server
- Use the NAP Client Management snap-in to enable EC

Additional Reading
- Help Topic: Create NAP Policies with a Wizard
- Help Topic: Checklist: Configure NAP Enforcement for DHCP
Lesson 4: Monitoring and Troubleshooting NAP

- What is NAP Tracing?
- Configuring NAP Tracing
- Demonstration: Configuring Tracing

Because of the differing levels of technology and the expertise and prerequisites for each of the NAP enforcement methods, troubleshooting and monitoring the NAP structure is an important administrative task. Trace logs are available for NAP, but are disabled by default. These logs serve two purposes: troubleshooting and evaluating the health and security of the network.
What is NAP Tracing?

- **NAP tracing identifies NAP events and records them to a log file based on the one of the following tracing levels:**
  - Basic
  - Advanced
  - Debug

- **You can use tracing logs to:**
  - Evaluate the health and security of your network
  - For troubleshooting and maintenance

- **NAP tracing is disabled by default, which means that no NAP events are recorded in the trace logs**

You can use NAP Client Configuration snap-in to configure NAP tracing. Tracing records NAP events in a log file and is useful for troubleshooting and maintenance. You can also use tracing logs to evaluate the health and security of your network. You can configure three levels of tracing: Basic, Advanced and Debug.

You should enable NAP tracing when:

- You are troubleshooting NAP problems.
- You want to evaluate the overall health and security of the computers in your organization.

**Additional Reading**

- Help and Support Topic: NAP tracing
Configuring NAP Tracing

- You can configure NAP tracing by using one of the following tools:
  - The NAP Client Management console
  - The `netsh` command-line tool

- To enable logging functionality, you must be a member of the Local Administrators group

- Trace logs are located in the following directory: `%systemroot%\tracing\nap`

There are two tools that are available for configuring NAP tracing. The NAP Client Configuration console is part of the Windows user interface, and `netsh` is a command-line tool.

To view the log files, navigate to the `%systemroot%\tracing\nap` directory and open the particular trace log that you want to view.

**Question:** What is the `netsh` command for enabling debug logging levels for NAP?

**Additional Reading**
- Help Topic: Enable and Disable NAP Tracing
- Help Topic: Specify Level of Detail in the NAP Trace Log
Demonstration: Configuring Tracing

In this demonstration, you will see how to:

- Configure tracing from the GUI
- Configure tracing from the command line
- View the log files

Question: What group must you be a member of to enable tracing for NAP?

Additional Reading

- Help Topic: Enable and Disable NAP Tracing
- Help Topic: Specify Level of Detail in the NAP Trace Log
Lab: Configuring NAP for DHCP and VPN

- Exercise 1: Configuring NAP for DHCP Clients
- Exercise 2: Configuring NAP for VPN Clients

Logon information

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>NYC-DC1, NYC-SVR1 and NYC-CL1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 120 minutes

Objectives
- Configure NAP for DHCP clients
- Configure NAP for VPN clients

Logon Information
- Virtual Machines: 6421A-NYC-DC1, 6421A-NYC-SVR1, and 6421A-NYC-CL1
- User Name: WoodgroveBank\Administrator
- Password: Pa$$w0rd

Scenario
As the Woodgrove Bank Technology Specialist, you have been tasked with automatically bringing client computers into compliance by using Network Policy Server, creating client compliance policies and configuring a NAP server to check computers’ current health.
Exercise 1: Configuring NAP for DHCP Clients
In this exercise, you will configure and test NAP for DHCP clients.
The main tasks are as follows:
1. Ensure that you have completed the steps in the Lab Setup.
2. Open the Server Manager tool on 6421A-NYC-SVR1.
3. Install the DHCP and NPS server roles.
4. Configure NYC-SVR1 as a NAP health policy server.
5. Configure DHCP service for NAP enforcement.
6. Configure NYC-CL1 as a DHCP and NAP client.
7. Test NAP enforcement.
8. Shut down the virtual machines and do not save changes.

▶ Task 1: Ensure that you have completed the steps in the Lab Setup
  • Review the Lab Setup section and ensure you have completed the steps before you continue with this lab.

▶ Task 2: Open the Server Manager tool on 6421A-NYC-SVR1
  • On 6421A-NYC-SVR1, open Server Manager from the Administrative Tools menu.
Task 3: Install the NPS and DHCP server roles

1. On NYC-SVR1, open Server Manager.
2. Right-click Roles, and then click Add Roles.
4. On the Select Role Services page, select the Network Policy Server.
5. On the Select Network Connection Bindings page, verify that 10.10.0.24 is selected. Remove the check mark next to 192.168.1.10.
6. On the Specify DNS Server Settings page, verify that woodgrovebank.com is listed under Parent domain.
7. Type 10.10.0.10 under Preferred DNS server IP address, and click Validate. Verify that the result returned is Valid.
8. On the Specify WINS Server Settings page, accept the default setting.
9. On the Add or Edit DHCP Scopes page, click Add.
10. In the Add Scope dialog box, type NAP Scope next to Scope Name. Next to Starting IP Address, type 10.10.0.50, next to Ending IP Address type 10.10.0.199, and next to Subnet Mask type 255.255.0.0.
11. Select the Activate this scope check box, and then click OK.
12. On the Configure DHCPv6 Stateless Mode page, select Disable DHCPv6 stateless mode for this server.
13. On the Authorize DHCP Server page, select Use current credentials. Verify that Woodgrovebank\administrator is displayed next to Username, and then click Next.
15. Verify the installation was successful, and then click Close.
Task 4: Configure NYC-SVR1 as a NAP health policy server

1. Open the Network Policy Server administrative tool from the Start Menu, Administrative Tools location.

2. Configure SHVs:
   a. Expand Network Access Protection, and then click System Health Validators.
   b. Configure the System Health Validator. Clear all check boxes except A firewall is enabled for all network connections. You do not have to clear the Windows Update check box.

3. Configure remediation server groups:
   a. In the console tree, under Network Access Protection, right-click Remediation Server Groups, and then click New.
   b. Create a new remediation group with a group name of Rem1 and add the IP address of 10.10.0.10.

4. Configure health policies:
   a. Expand Policies.
   b. Right-click Health Policies, and then click New.
   c. Create a new health policy called Compliant that specifies the Client passes all SHV checks and uses the Windows Security Health Validator.
   d. Right-click Health Policies, and then click New.
   e. Create a new health policy called NonCompliant that specifies the Client fails one or more SHV checks and uses the Windows Security Health Validator.

5. Configure a network policy for compliant computers:
   a. In the console tree, under Policies, click Network Policies.
   b. Disable the two default policies under Policy Name.
   c. Create a new Network Policy called Compliant-Full-Access.
   d. In the Specify Conditions window, click Add.
   e. In the Select condition dialog box, double-click Health Policies, select Compliant, and then click OK.
f. In the **Specify Access Permission** window, verify that **Access granted** is selected.

g. In the **Configure Authentication Methods** window, select the **Perform machine health check only** check box. Clear all other check boxes.

h. In the **Configure Settings** window, click **NAP Enforcement**. Verify that **Allow full network access** is selected.

i. In the **Completing New Network Policy** window, click **Finish** to complete configuration of your network policy for compliant client computers.

6. Configure a network policy for Noncompliant computers:

   a. Right-click **Network Policies**, and then click **New**.

   b. Create a new **Network Policy** called **NonCompliant-Restricted**.

   c. In the **Specify Conditions** window, click **Add**.

   d. In the **Select condition** dialog box, double-click **Health Policies**, select **Noncompliant**, and then click **OK**.

   e. In the **Specify Access Permission** window, verify that **Access granted** is selected, and then click **Next**.

   **Important:** A setting of **Access granted** does not mean that noncompliant clients are granted full network access. It specifies that clients matching these conditions will be granted an access level determined by the policy.

f. In the **Configure Authentication Methods** window, select the **Perform machine health check only** check box. Clear all other check boxes.

  g. In the **Configure Constraints** window, click **Next**.

  h. In the **Configure Settings** window, click **NAP Enforcement**. Select **Allow limited access** and verify that **Enable auto-remediation of client computers** is selected.

  i. Click **Next**, and then click **Finish**. This completes configuration of your NAP network policies. Close the Network Policy Server console.
Task 5: Configure DHCP service for NAP enforcement

1. On NYC-SVR1, open the DHCP Management console by typing `dhcpmgmt.msc` in the Run box, and then pressing ENTER.

2. In the DHCP Management console, expand `NYC-SVR1.woodgrovebank.com`, and then expand IPv4.

3. Open the Properties for the Scope. On the Network Access Protection tab, verify Use default Network Access Protection profile is selected, and then click OK.

4. In the DHCP Management console, configure Scope Options.

5. On the Advanced tab, verify that Default User Class is chosen next to User class.

6. Under Available Options, select the 003 Router check box, type `10.10.0.1` in IP Address, select the 015 DNS Domain Name check box, type `Woodgrovebank.com` in String value, and then click OK. The `Woodgrovebank.com` domain is a full-access network assigned to compliant NAP clients.

7. In the DHCP Management console, configure Scope Options.

8. On the Advanced tab, next to User class, choose Default Network Access Protection Class.

9. Select the 006 DNS Servers check box, type `10.10.0.10` in IP Address, select the 015 DNS Domain Name check box, type `restricted.Woodgrovebank.com` in String value, and then click OK. The restricted.woodgrovebank.com domain is a restricted-access network assigned to noncompliant NAP clients.
Task 6: Configure NYC-CL1 as a DHCP and NAP client

1. On NYC-CL1, enable Security Center:
   a. Click Start, point to All Programs, click Accessories, and then click Run.
   b. Type gpedit.msc, and then press ENTER.
   d. Double-click Turn on Security Center (Domain PCs only), click Enabled, and then click OK.
   e. Close the console window. When prompted to save settings, click No.

2. Enable the DHCP enforcement client:
   a. Click Start, click All Programs, click Accessories, and then click Run.
   b. Type napclcfg.msc, and then press ENTER.
   c. In the console tree, click Enforcement Clients.
   d. Enable the DHCP Quarantine Enforcement Client.
   e. Close the NAP Client Configuration console.

3. Enable and start the NAP agent service:
   a. Click Start, point to All Programs, click Accessories, and then click Run.
   b. Type services.msc, and then press ENTER.
   c. In the services list, set Network Access Protection Agent Startup type to Automatic and start the service.
   d. Wait for the NAP agent service to start, and then click OK.
   e. Close the Services console.
4. Configure NYC-CL1 for DHCP address assignment:
   a. Click **Start**, and then click **Control Panel**.
   b. Click **Network and Internet**, click **Network and Sharing Center**, and then click **Manage network connections**.
   c. Configure **Local Area Connection** properties with the following:
      - Clear the **Internet Protocol Version 6 (TCP/IPv6)** check box.
      - Set properties of **Internet Protocol Version 4 (TCP/IPv4)** to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
   d. Click **OK**, and then click **Close** to close the **Local Area Connection Properties** dialog box.

5. Close the **Network Connections** and **Network and Sharing Center** windows.

**Task 7: Test NAP Enforcement**

1. Verify the DHCP assigned address and current Quarantine State:
   a. On NYC-CL1, open an administrative command prompt using the **Run As Administrator** command.
   b. At the command prompt, type `ipconfig /all`.
   c. Verify that the connection-specific DNS suffix is **Woodgrovebank.com** and the Quarantine State is **Not Restricted**.

2. Configure the System Health Validator policy to require antivirus software:
   a. On NYC-SVR1, in the Network Policy Server console, open **NPS (Local)**, open **Network Access Protection**, and then open **System Health Validators**.
   b. Configure Windows Security Health Validator so that **Virus Protection** is set to **An antivirus application is on**.
   c. Click **OK**, and then click **OK** again to close the **Windows Security Health Validator Properties** window.
3. Verify the restricted network on NYC-CL1:
   a. On NYC-CL1, open an administrative command prompt using the Run As Administrator command.
   b. At the command prompt, type `ipconfig /release`.
   c. At the command prompt, type `ipconfig /renew`.
   d. Verify the connection-specific DNS suffix is now `restricted.woodgrovebank.com`.
   e. Close the command window and double-click the Network Access Protection icon in the system tray. Notice it tells you the computer is not compliant with requirements of the network.
   f. Click Close.

▶ Task 8: Shutdown virtual machines and do not save changes
   • Close all open windows, turn off all virtual machines and discard undo disks.
   • For Exercise 2, start NYC-DC1, NYC-SVR1 and NYC-CL1.
   • Log on to each as WoodgroveBank\administrator with a password of Pa$$w0rd.
Exercise 2: Configuring NAP for VPN Clients

In this exercise, you will configure NAP for VPN Clients. This exercise uses the Windows Security Health Agent and Windows Security Health Validator to require that client computers have Windows Firewall enabled and have an antivirus application installed.

You will create two network policies in this exercise. A compliant policy grants full network access to an intranet network segment. A noncompliant policy demonstrates network restriction by applying IP filters to the VPN tunnel interface that only allow client access to a single remediation server.

The main tasks are as follows:

1. Configure NYC-DC1 as an Enterprise Root CA
2. Configure NYC-SVR1 with NPS functioning as a health policy server
3. Configure NYC-SVR1 with the Routing and Remote Access service configured as a VPN server
4. Allow ping on NYC-SVR1
5. Configure NYC-CL1 as a VPN client and a NAP client
6. Close all virtual machines and discard undo disks.

▶ Task 1: Configure NYC-DC1 as an Enterprise Root CA

1. On NYC-DC1, click Start, point to Administrative Tools, and then click Server Manager.
2. Under Roles Summary, click Add Roles, and then click Next.
3. On the Before you Begin page, click Next.
4. Select the Active Directory Certificate Services check box and configure the wizard with the following:
   a. On the Specify Setup Type page, select Enterprise.
   b. On the Configure CA Name page, specify a name of Root CA.
   c. On the Confirm Installation Selections page, click Install.
5. On the Installation Results page, verify the installation succeeded, and then click Close.
6. Close the Server Manager window.

7. From the Administrative Tools menu, open the Certification Authority management tool.

8. Right-click Certificate Templates, and then choose Manage from the context menu.

9. Change the security on the Computer template to allow Authenticated Users the Enroll permission.


Task 2: Configure NYC-SVR1 with NPS functioning as a health policy server

1. On NYC-SVR1, restart the server. After the computer restarts, log on as Woodgrovebank\administrator with a password of Pa$$w0rd.

2. Obtain a computer certificate on NYC-SVR1 for server-side PEAP authentication:
   a. Create a custom MMC console that includes the Certificates snap-in for Computer Account.
   b. In the console tree, double-click Certificates, right-click Personal, point to All Tasks, and then click Request New Certificate.
   c. The Certificate Enrollment dialog box opens. Click Next.
   d. Select the Computer check box, and then click Enroll.
   e. Verify the status of certificate installation as Succeeded, and then click Finish.
   f. Close the Console1 window.
   g. Click No when prompted to save console settings.

3. Install the NPS Server role:
   a. On NYC-SVR1, click Start, click Administrative Tools, and then click Server Manager.
   c. Verify the installation was successful, and then click Close.
   d. Close the Server Manager window.
4. Configure NPS as a NAP health policy server:
   a. Click Start, click Run, type nps.msc, and then press ENTER.
   b. Expand Network Access Protection, and then click System Health Validators.
   c. In the middle pane under Name, double-click Windows Security Health Validator.
   d. Configure the Windows Security Health Validator properties so all check boxes except A firewall is enabled for all network connections are cleared.
   e. Click OK to close the Windows Security Health Validator dialog box, and then click OK to close the Windows Security Health Validator Properties dialog box.

5. Configure health policies:
   a. Expand Policies.
   b. Create a new health policy called Compliant.
   c. Under Client SHV checks, verify that the Client passes all SHV checks check box is selected.
   d. Under SHVs used in this health policy, select the Windows Security Health Validator check box.
   e. Click OK.
   f. Create a new health policy called Noncompliant.
   g. Under Client SHV checks, select Client fails one or more SHV checks.
   h. Under SHVs used in this health policy, select the Windows Security Health Validator check box.
   i. Click OK.

6. Configure network policies for compliant computers:
   a. Expand Policies.
   b. Click Network Policies.
   c. Disable the two default policies under Policy Name.
   d. Create a new network policy called Compliant-Full-Access.
   e. In the Specify Conditions window, click Add.
f. In the Select condition dialog box, double-click Health Policies.

g. In the Health Policies dialog box, under Health policies, select Compliant.

h. In the Specify Access Permission window, verify that Access granted is selected.

i. In the Configure Settings window, click NAP Enforcement. Verify that Allow full network access is selected.

j. In the Completing New Network Policy window, click Finish.

7. Configure network policies for noncompliant computers:

a. Create a new network policy called Noncompliant-Restricted.

b. In the Specify Conditions window, click Add.

c. In the Select condition dialog box, double-click Health Policies.

d. In the Health Policies dialog box, under Health policies, select Noncompliant, and then click OK.

e. In the Specify Conditions window, verify that Health Policy is specified under Conditions with a value of Noncompliant, and then click Next.

f. In the Specify Access Permission window, verify that Access granted is selected.

Important: A setting of Access granted does not mean that noncompliant clients are granted full network access. It specifies that clients matching these conditions should continue to be evaluated by the policy.

g. In the Configure Settings window, click NAP Enforcement. Select Allow limited access and select Enable auto-remediation of client computers.

h. In the Configure Settings window, click IP Filters.

i. Under IPv4, create a new input filter for Destination network with the following values:
   - IP address: 10.10.0.10
   - Subnet mask: 255.255.255.255

This step ensures that traffic from noncompliant clients can only reach DC1.
j. Click **OK** to close the **Add IP Filter** dialog box, and then select **Permit only the packets listed below** in the **Inbound Filters** dialog box.

k. Under **IPv4**, create a new outbound filter with the following source network values:
   - **IP address**: 10.10.0.10
   - **Subnet mask**: 255.255.255.255

l. Click **OK** to close the **Add IP Filter** dialog box, and then select **Permit only the packets listed below** in the **Outbound Filters** dialog box. This step ensures that only traffic from DC1 can be sent to noncompliant clients.

m. In the **Completing New Network Policy** window, click **Finish**.

8. Configure connection request policies:
   a. Click **Connection Request Policies**.
   b. Disable the default CRP found under **Policy Name**.
   c. Create a new Connection Request policy called **VPN connections**.
   d. Under **Type of network access server**, select **Remote Access Server (VPN-Dial up)**.
   e. In the **Specify Conditions** window, click **Add**.
   f. In the **Select Condition** window, double-click **Tunnel Type**, select **PPTP** and **L2TP**, and then click **OK**.
   g. In the **Specify Connection Request Forwarding** window, verify that **Authenticate requests on this server** is selected.
   h. In the **Specify Authentication Methods** window, select **Override network policy authentication settings**.
   i. Under **EAP Types**, click **Add**. In the **Add EAP** dialog box, under **Authentication methods**, click **Microsoft: Protected EAP (PEAP)**.
   j. Under **EAP Types**, click **Add**. In the **Add EAP** dialog box, under **Authentication methods**, click **Microsoft: Secured password (EAP-MSCHAP v2)**.
   k. Under **EAP Types**, click **Microsoft: Protected EAP (PEAP)**, and then click **Edit**.
1. Verify that Enable Quarantine checks is selected, and then click OK.

m. Click Next twice, and then click Finish.

▶ Task 3: Configure NYC-SVR1 with the Routing and Remote Access service configured as a VPN server

1. Click Start, click Run, type rrasmgmt.msc, and then press ENTER.

2. In the Routing and Remote Access management console, configure and enable Routing and Remote Access with the role Remote access (dial-up or VPN).

3. Select the VPN check box, and then click Next.

4. Click the network interface with an IP address of 192.168.1.10. Clear the Enable security on the selected interface by setting up static packet filters check box, and then click Next. This ensures that NYC-SVR1 will be able to ping NYC-DC1 when attached to the Internet subnet without having to configure additional packet filters for ICMP traffic.

5. On the IP Address Assignment page, select From a specified range of addresses, and on the Address Range Assignment page, specify a range of 10.10.0.100 to 10.10.0.110.


7. Click Next, and then click Finish.

8. Click OK, and wait for the Routing and Remote Access service to start.

9. Open the Network Policy Server console from the Administrative Tools menu, expand Policies, select Connection Request Policies, and then disable the Microsoft Routing and Remote Access Service Policy by right-clicking the policy and choosing Disable.

Task 4: Allow ping on NYC-SVR1
1. Click Start, click Administrative Tools, and then click Windows Firewall with Advanced Security.
2. Create a custom inbound rule for All Programs with the protocol type of ICMPv4 and ICMP type of Echo Request for the default scope options.
3. In the Action window, verify that Allow the connection is selected, and then click Next.
4. Click Next to accept the default profile.
5. In the Name window, under Name, type ICMPv4 echo request, and then click Finish.

Task 5: Configure NYC-CL1 as a VPN client and a NAP client
1. Configure NYC-CL1 so that Security Center is always enabled:
   a. Open the Local Group Policy Object Editor using the Run command with gpedit.msc.
   c. Double-click Turn on Security Center (Domain PCs only), click Enabled, and then click OK.
   d. Close the Local Group Policy Object Editor console.
2. Enable the remote access quarantine enforcement client:
   a. Launch the NAP Client Configuration tool using the Run command with napclcfg.msc.
   b. Enable the Remote Access Quarantine Enforcement Client.
   c. Close the NAP Client Configuration window.
3. Enable and start the NAP agent service:
   a. Open the Services console using `services.msc` in the Run command.
   b. In the Services list, double-click Network Access Protection Agent.
   c. Change the startup type to Automatic, and then click Start.
   d. Wait for the NAP agent service to start, and then click OK.
   e. Close the Services console.

4. Configure NYC-CL1 for the Internet network segment:
   a. Configure Local Area Connection Properties with Internet Protocol Version 4 (TCP/IPv4) set for the following:
      - IP address: 192.168.1.20
      - Subnet mask: 255.255.255.0
      - Remove Preferred DNS server setting of 10.10.0.10
   b. Click OK, and then click Close to close the Local Area Connection Properties dialog box.
   c. Close the Network Connections window.

5. Verify network connectivity for NYC-CL1:
   a. Open a command prompt and type `ping 192.168.1.10`.
   b. Verify that the response reads “Reply from 192.168.1.10.”
   c. Close the command window.

6. Configure a VPN connection:
   a. Using the Network and Sharing Center, create a new Connect to a workplace with the Use my Internet Connection (VPN) option.
   b. Click I’ll set up an Internet connection later.
   c. On the Type the Internet address to connect to page, next to Internet address, type 192.168.1.10. Next to Destination name, type Woodgrovebank. Select the Allow other people to use this connection check box, and then click Next.
   d. On the Type your user name and password page, type administrator next to User name, and type the password for the administrator account next to Password. Select the Remember this password check box, type Woodgrovebank next to Domain (optional), and then click Create.
e. In the **Network and Sharing Center** window, click **Manage Network Connections**.

f. Under **Virtual Private Network**, right-click the **Contoso** connection, click **Properties**, and then click the **Security** tab.

g. Select **Advanced (custom settings)**, and then click **Settings**.

h. Under **Logon security**, select **Use Extensible Authentication Protocol (EAP)**, and then choose **Protected EAP (PEAP) (encryption enabled)**.

i. Click **Properties**.

j. Select the **Validate server certificate** check box. Clear the **Connect to these servers** check box, and then select **Secured Password (EAP-MSCHAP v2)** under **Select Authentication Method**. Clear the **Enable Fast Reconnect** check box, and then select the **Enable Quarantine checks** check box.

k. Click **OK** three times to accept these settings.

7. Test the VPN connection:

   a. In the **Network Connections** window, use the **Woodgrovebank** connection object to initiate the VPN connection.

   b. Verify that administrator account credentials are entered and that the **Save this user name and password for future use** check box is selected, and then click **OK**.

   c. You are presented with a **Validate Server Certificate** window the first time this VPN connection is used. Click **View Server Certificate**, and verify **Certificate Information** states that the certificate was issued to **NYC-SVR1.Woodgrovebank.com** by **Root CA**. Click **OK** to close the **Certificate** window, and then click **OK** again.

   d. Wait for the VPN connection to be made. Because NYC-CL1 is compliant, it should have unlimited access to the intranet subnet.

   e. Open a command prompt and type **ipconfig /all** to view the configuration.

   f. View the IP configuration. **System Quarantine State** should be **Not Restricted**.

      The client now meets the requirement for VPN full connectivity.

   g. Disconnect from the **Woodgrovebank** VPN.
8. Configure Windows Security Health Validator to require an antivirus application:
   b. Expand Network Access Protection, and then click System Health Validators.
   c. Configure the Windows Security Health Validator to require virus protection by selecting the check box next to An antivirus application is on.
   d. Click OK, and then click OK again to close the Windows Security Health Validator Properties window.

9. Verify the client is placed on the restricted network:
   a. On NYC-CL1, in the Network Connections window, right-click the Woodgrovebank connection, and then click Connect.
   b. Wait for the VPN connection to be made. You might see a message in the notification area that indicates the computer does not meet health requirements. This message is displayed because antivirus software has not been installed.
   c. Open a command prompt and type `ipconfig /all` to view the IP Configuration. System Quarantine State should be Restricted.
      The client does not meet the requirements for the network and therefore is put on the restricted network.
      Try to ping 10.10.0.24. This should be unsuccessful.
      Try to ping 10.10.0.10. This is the only server that the policy allows access to.
   d. Disconnect from Woodgrovebank VPN.

▶ Task 6: Close all virtual machines and discard undo disks
1. On the host computer, click Start, point to All Programs, point to Microsoft Virtual Server, and then click Virtual Server Administration Website.
2. Under Navigation, click Master Status. For each virtual machine that is running, click the virtual machine name, and in the context menu, click Turn off Virtual Machine and Discard Undo Disks. Click OK.
Module Review and Takeaways

<table>
<thead>
<tr>
<th>Module Review and Takeaways</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Review Questions</td>
</tr>
<tr>
<td>• Best Practices</td>
</tr>
<tr>
<td>• Tools</td>
</tr>
</tbody>
</table>

**Review Questions**

1. What are the three main client configurations that need to be configured for most NAP deployments?

2. You want to evaluate the overall health and security of the NAP enforced network. What do you need to do to start recording NAP events?
Best Practices

Consider the following best practices when implementing NAP:

- Use strong enforcement methods (IPSec, 802.1x and VPN). Strong enforcement methods provide the most secure and effective NAP deployment.

- Do not rely on NAP to secure a network from malicious users. NAP is designed to help administrators maintain the health of the computers on the network, which in turn helps maintain the network’s overall integrity. NAP does not prevent an authorized user with a compliant computer from uploading a malicious program to the network or disabling the NAP agent.

- Use consistent NAP policies throughout the site hierarchy to minimize confusion. Configuring a NAP policy incorrectly may result in clients accessing the network when they should be restricted or valid clients being erroneously restricted. The more complicated your NAP policy design, the higher the risk of incorrect configuration.

- Do not rely on NAP as an instantaneous or real-time enforcement mechanism. There are inherent delays in the NAP enforcement mechanism. While NAP helps keep computers compliant over the long run, typical enforcement delays may be several hours or more due to a variety of factors, including the settings of various configuration parameters.
Tools
The following table describes the tools that you can use to configure NAP.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Use For</th>
<th>Where to find it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>Enable and configure the NAP service on client computers</td>
<td>Click Start, click Control Panel, click System and Maintenance, click Administrative Tools, and then click double-click Services.</td>
</tr>
<tr>
<td>Netsh nap</td>
<td>Using netsh, you can create scripts to automatically configure a set of Windows Firewall with Advanced Security settings, create rules and rules, monitor connections, and display the configuration and status of Windows Firewall with Advanced Security.</td>
<td>Open a command window with administrative rights and type netsh nap. You can type help to get a full list of available commands.</td>
</tr>
<tr>
<td>Group policy</td>
<td>Some NAP deployments that use Windows Security Health Validator require that Security Center is enabled.</td>
<td>Enable the Turn on Security Center (Domain PCs only) setting in the Computer Configuration, Administrative Templates, Windows Components, and Security Center sections of Group Policy.</td>
</tr>
<tr>
<td>Configure NAP with a wizard</td>
<td>Used to create the health policies, connection request policies, and Network Access Protection (NAP) with Network Policy Server.</td>
<td>Open the NPS (Local) console. In Getting Started and Standard Configuration, select Network Access Protection (NAP) policy server. The text and links below the text change to reflect your selection. Click Configure NAP with a wizard.</td>
</tr>
</tbody>
</table>