

Infrastructure Planning   
and Design

Selecting the Right NAP Architecture

Version 1.1

Published: June 2008

Updated: November 2011

For the latest information, please see [www.microsoft.com/ipd](http://www.microsoft.com/ipd)

Copyright © 2011 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility.  By using or providing feedback on this documentation, you agree to the license agreement below.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/2.5/> or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS".  Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation.  Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, Microsoft Press, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries and regions.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose.  You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback.  You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[The Planning and Design Series Approach 1](#_Toc305756163)

[Introduction to the Selecting the Right NAP Architecture Guide 2](#_Toc305756164)

[Components of NAP 4](#_Toc305756165)

[NAP Enforcement Options 6](#_Toc305756166)

[Step 1: Determine Client Connectivity 8](#_Toc305756167)

[Step 2: Determine the VPN Platform 9](#_Toc305756168)

[Step 3: Determine the Enforcement Layer 11](#_Toc305756169)

[Step 4: Select Between 802.1X and DHCP 14](#_Toc305756170)

[Additional Considerations 16](#_Toc305756171)

[Conclusion 18](#_Toc305756172)

[Appendix A: IPD in Microsoft Operations Framework 4.0 20](#_Toc305756173)

[Appendix B: Selecting the Right NAP Architecture in Microsoft Infrastructure Optimization 21](#_Toc305756174)

[Version History 22](#_Toc305756175)

[Acknowledgments 23](#_Toc305756176)

# 

# The Planning and Design Series Approach

This guide is one in a series of planning and design guides that clarify and streamline the planning and design process for Microsoft® infrastructure technologies.

Each guide in the series addresses a unique infrastructure technology or scenario. These guides include the following topics:

* Defining the technical decision flow (flow chart) through the planning process.
* Describing the decisions to be made and the commonly available options to consider in making the decisions.
* Relating the decisions and options to the business in terms of cost, complexity, and other characteristics.
* Framing the decision in terms of additional questions to the business to ensure a comprehensive understanding of the appropriate business landscape.

The guides in this series are intended to complement and augment the product documentation.

## Benefits of Using This Guide

Using this guide will help an organization to plan the best architecture for the business and to deliver the most cost-effective enterprise messaging technology.

Benefits for Business Stakeholders/Decision Makers:

* Most cost-effective design solution for an implementation. Infrastructure Planning and Design (IPD) eliminates over-architecting and overspending by precisely matching the technology solution to the business needs.
* Alignment between the business and IT from the beginning of the design process to the end.

Benefits for Infrastructure Stakeholders/Decision Makers:

* Authoritative guidance. Microsoft is the best source for guidance about the design of Microsoft products.
* Business validation questions to ensure the solution meets the requirements of both business and infrastructure stakeholders.
* High-integrity design criteria that includes product limitations.
* Fault-tolerant infrastructure, where necessary.
* Proportionate system and network availability to meet business requirements.
* Infrastructure that is sized appropriately to meet business requirements.

**Benefits for** Consultants or Partners:

* Rapid readiness for consulting engagements.
* Planning and design template to standardize design and peer reviews.
* A “leave-behind” for pre- and post-sales visits to customer sites.
* General classroom instruction/preparation.

Benefits for the Entire Organization:

Using this guide should result in a design that will be sized, configured, and appropriately placed to deliver a solution for achieving stated business requirements, while considering the performance, capacity, manageability, and fault tolerance of the system.

# Introduction to the Selecting the Right NAP Architecture Guide

There are several specific questions to answer when designing a Network Access Protection (NAP) architecture, and they can be put into three categories:

* What are the current capabilities of the network infrastructure and computers?
* Which is more important: the cost or the robustness of the solution?
* How do the client computers connect to the network: directly, or through a virtual private network (VPN)?

NAP is a new platform and solution that controls access to network resources based on a client computer’s identity and compliance with corporate governance policy. NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

## NAP Design Process

The goal of this guide is to ensure that the reader understands the fundamental architectural choices that NAP supports so that decisions can be made that most effectively meet the organization’s requirements and capabilities. Although this document can help an organization make the best architectural decisions, more tactical guidance is available from other resources, including online documents and books referred to throughout the rest of this guide. In addition, certified Microsoft partners, Microsoft Consulting Services, and Microsoft Support Services can provide seasoned experts to validate designs and assist with the deployment process.

This guide addresses the following decisions and activities that must occur in preparing for NAP planning. The steps below represent the most critical design elements in a well-planned NAP design:

* Step 1: Determine Client Connectivity
* Step 2: Determine the VPN Platform
* Step 3: Determine the Enforcement Layer
* Step 4: Select Between 802.1X and DHCP

Some of these items represent decisions that must be made. Where this is the case, a corresponding list of common response options is presented.

Other items in this list represent tasks that must be carried out. These types of items are addressed, because their presence is significant for completing the infrastructure design.

Figure 1 provides a graphical overview of the steps involved in designing a NAP infrastructure.

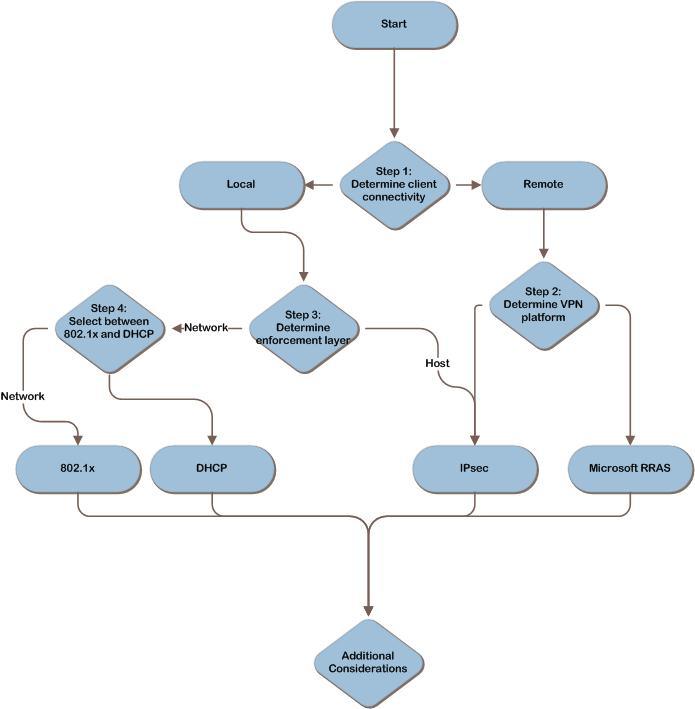


Figure 1. The NAP infrastructure decision flow

# Components of NAP

Figure 2 illustrates all the possible components of the NAP infrastructure. The rest of this section briefly describes the purpose of each component.

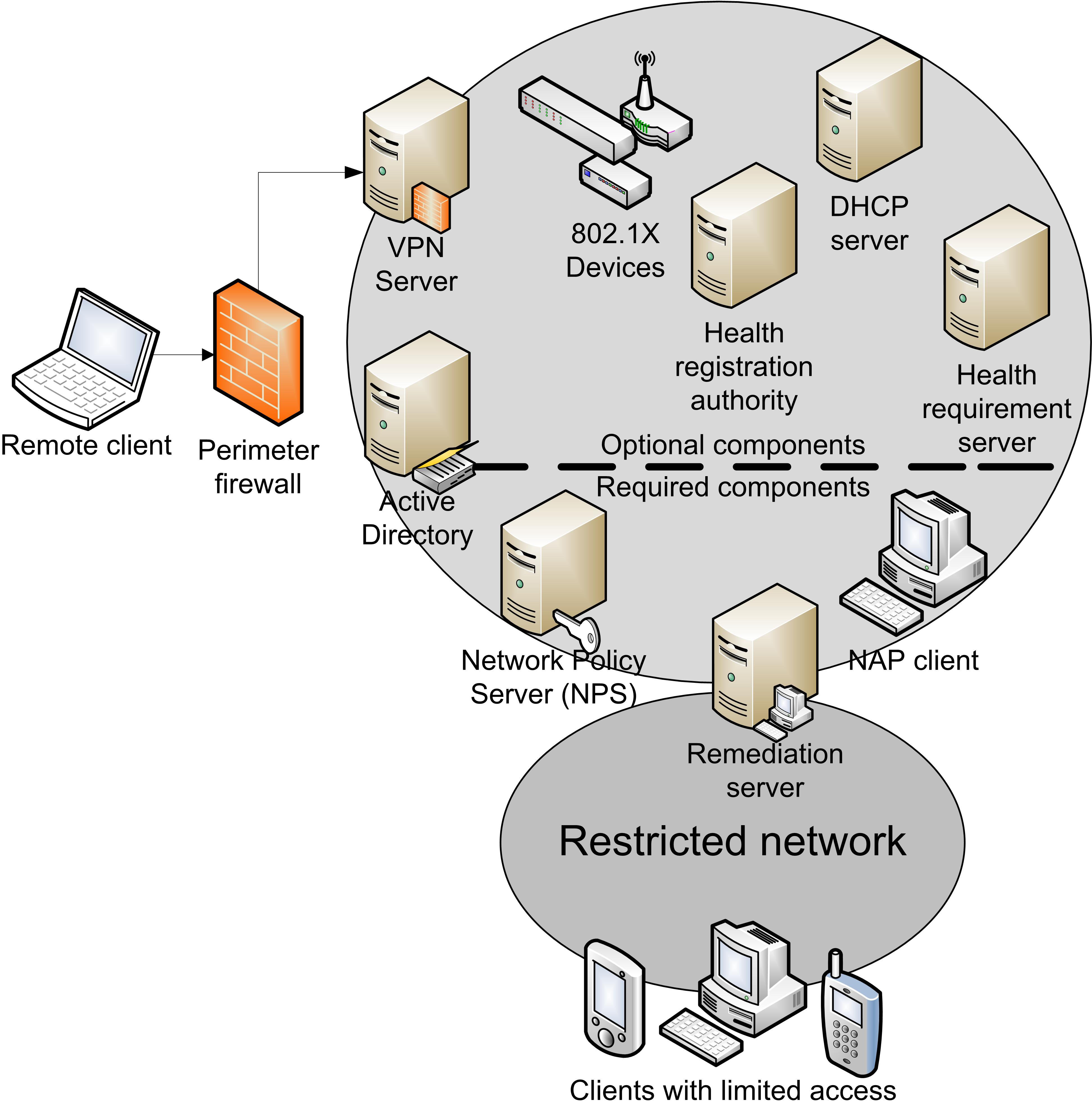


Figure 2. Example NAP architecture

The components are:

* **NAP enforcement points.** These points are devices that use NAP or can be used in conjunction with NAP to control access until clients prove that their compliance state meets the organization’s policies. Such enforcement points include:
* **Health Registration Authority (HRA).** An HRA is a server running Windows Server® 2008 and Internet Information Services (IIS). It receives health certificates from a certification authority (CA) for client devices that have demonstrated their compliance.
* **VPN server.** A virtual private network (VPN) server is a computer running Windows Server 2008 and Routing and Remote Access service (RRAS) that provides access to the internal network for remote client devices.
* **Network access devices.** Such devices include wired ethernet switches or wireless access points that support 802.1X authentication.
* **Dynamic Host Configuration Protocol (DHCP) server.** This is a computer running Windows Server 2008 and a DHCP service that dynamically issues IP address information to internal client devices.
* **Network policy servers.** These servers are computers running Windows Server 2008 and the Network Policy Server (NPS) service. NPS is the Windows Server 2008 implementation of Remote Authentication Dial-In User Service (RADIUS). NPS replaces Internet Authentication Service (IAS), the version of RADIUS included in Windows Server 2003. In a NAP deployment, NPS acts as the health policy server regardless of enforcement method; it also provides authentication, authorization, and accounting services when 802.1X is the enforcement method.
* **Health requirement servers.** These computers define the current compliance state for health policy servers—for example, an antivirus server that tracks the latest version of the software’s antivirus signature file. Some examples of health requirement servers are Microsoft System Center Configuration Manager, Microsoft Windows Server Update Services, and Microsoft System Center Operations Manager.
* **Active Directory® Domain Services (AD DS).** AD DS stores account credentials and other information. It is required for Internet Protocol security (IPsec), 802.1X authentication, and VPN connections.
* **NAP clients.** These computers include NAP agent software. The Windows Vista®, Windows Server 2008, and Windows® XP with Service Pack 3 (SP3) operating systems all include the necessary software; third-party agents are available for other platforms.
* **Restricted network.** This logically or physically separate network includes:
* Remediation servers. These servers—such as those hosting software updates and antivirus signature updates—can update NAP client devices to help them become compliant with the organization’s health policies.
* NAP client devices with limited access. These computers have not yet met the health policy requirements.
* Clients that are not NAP-capable. These devices do not support NAP. They can be placed on the restricted network or granted exemptions that allow them to access the internal network. Client computers and servers that are not NAP-capable can be exempted from the NAP restrictions so that they can continue to use the network. This compromise can ease the transition until the older client computers are upgraded to a NAP-capable version of the Windows operating system or a third-party agent is acquired. It is likely that some hosts will never become NAP capable; in such cases, IT may consider granting permanent exemptions to certain classes of hosts, such as IP phones, network printers, and handheld devices.

# NAP Enforcement Options

NAP allows IT to enforce organizational policies when client computers attempt to connect to the corporate network. These policies are referred to as health policies. When a client device meets the health policy requirements, it is considered compliant. Four methods are available for restricting client devices until they have demonstrated that they meet the policy requirements. IT pros can implement a single method or combine several methods to increase the robustness of the solution.

## IPsec Enforcement

When IPsec is used, the client device is able to communicate with only a limited number of servers until it has demonstrated its compliance. Other managed systems will ignore network traffic from these client devices unless they prove their compliance or are exempted from compliance checks. When compliance has been confirmed, the client device achieves unrestricted access, because the managed systems are able to recognize that its compliance status has been established. IPsec enforcement can be complex to deploy, because it relies on IPsec and certificates issued from a public key infrastructure (PKI). However, it is robust and does not involve upgrading infrastructure components such as Ethernet switches or DHCP servers.

## 802.1X Enforcement

When 802.1X is used—over either wired or wireless networks—the client device’s access is restricted by network infrastructure devices such as wireless connection points and switches. Until the device has demonstrated its compliance, client access is restricted. Restriction is enforced on the network access device using an access control list (ACL) or by placing the client device on restricted virtual local area networks (VLANs). The 802.1X standard is more complex to deploy than DHCP, but it provides a high degree of protection.

## VPN Enforcement

When VPN enforcement is used, the VPN server itself restricts the client device’s access by using IP filters until the client device has demonstrated its compliance. When compliance has been proven, the VPN server lifts the restrictions and grants the client device full access. VPN enforcement is less complex than either IPsec or 802.1X, but it can restrict only remote client devices and is not appropriate for controlling access to client devices that connect locally. VPN enforcement requires the RRAS service in Windows Server 2008 and the Microsoft VPN client included with Windows XP with SP3, Windows Server 2008, and Windows Vista.

## DHCP Enforcement

When DHCP is used, the DHCP server assigns an IPv4 address configuration to client devices that allows them limited access to the network until they have demonstrated compliance with the organization’s health policies. When a client device has proven its compliance, it receives a new configuration that grants it unrestricted access. Although DHCP enforcement is the simplest to deploy, it is also the easiest for malicious users to bypass if they have administrative privileges on their computer, because they can manually configure their computer with a static IP address, which avoids all DHCP enforcement capabilities.

## Applicable Scenarios

This guide addresses the following considerations related to planning and designing the necessary components for a successful NAP infrastructure:

* Planning a limited proof-of-concept deployment of NAP.
* Planning a broad test deployment of NAP using the reporting-only mode.
* Planning production deployments of NAP using one of four enforcement methods:
* IPsec
* 802.1X
* VPN
* DHCP

## Out of Scope

Another potential enforcement method is to leverage Terminal Services Gateway connections. When this approach is used, client devices can only connect to shared resources and other network services through Terminal Services in Windows Server 2008; noncompliant hosts are restricted at the TS Gateway. This enforcement method is beyond the scope of this guide; however, for more information, see “Configuring the TS Gateway NAP Scenario” at <http://technet2.microsoft.com/WindowsServer2008/en/library/b3c07483-a9e1-4dc6-8465-0a7900900a551033.mspx>.

# Step 1: Determine Client Connectivity

Client devices connect to a corporate network in either of two ways: locally, through a wired or wireless interface; or using a remote connection such as a VPN. The type of network connectivity dictates which enforcement methods are appropriate for consideration.

## Task 1: Select the Scope of NAP Clients

If the NAP clients in scope for this project will be local to the network, proceed to Step 3. If the NAP clients will be remote to the network, proceed to Step 2. This option could serve as an intermediate NAP deployment. An organization could initially deploy NAP to enforce compliance requirements for managed VPN clients. IT may need to grant exemptions if staff members are allowed to connect to the VPN using unmanaged systems (for example, their own personal computers). When the IT team has become more familiar and the system health policies have been tuned appropriately, local enforcement can be put into effect.

Some organizations will initially deploy NAP for managing locally connected computers; others will use NAP for both local and remote clients. In the latter case, proceed to Step 2. When that step is complete, go on to Step 3.

# Step 2: Determine the VPN Platform

In the previous step, it was determined that NAP clients connect to the network remotely. Now, the VPN platform must be identified. With regard to NAP, there are two options for defining the organization’s VPN platform: Microsoft or third-party. It is important to make this selection, because if IT uses RRAS to provide remote access to the corporate network, packet filtering can be used at the VPN server to control client device access until devices have proven that they meet the organization’s compliance requirement policies. If another technology is used for the VPN, IPsec must be used as the enforcement method.

## Option 1: Microsoft VPN

If RRAS provides remote clients with VPN access to the corporate network, NAP enforcement can be implemented using packet filters on the VPN server—a simple process. To support NAP with VPN enforcement, IT pros must update the VPN server to run Windows Server 2008. If Microsoft VPN is chosen and there will be no enforcement for locally connected computers, the decision-making process is complete. If locally connected computers will also be managed by NAP, proceed to Step 3.

## Option 2: Third-Party VPN

If a third-party VPN solution is used, IPsec must be used to restrict access for client devices that have not proven that they meet the organization’s health policies. Procedures for implementing IPsec are well documented, and the Windows operating system includes tools for managing IPsec, but IPsec is still challenging for some organizations because of lack of knowledge and experience. If a third-party VPN is chosen and there will be no enforcement for locally connecting computers, the decision-making process is complete. If locally connected computers will also be managed by NAP, proceed to Step 3.

## Evaluating the Characteristics

Technical criteria are not the only factors IT must consider when making an infrastructure design decision. The decision should also be mapped to appropriate operational criteria or characteristics. The following tables compare each option according to the characteristics that are applicable to this decision-making topic.

|  |  |  |
| --- | --- | --- |
| Complexity | | |
| RRAS | Using RRAS to enforce NAP restrictions is not complex. | Low |
| Third-party VPN | Maintaining IPsec rules is greatly eased by the management tools available with Windows. Nevertheless, it may seem complex to organizations with little IPsec expertise. | High |

|  |  |  |
| --- | --- | --- |
| Cost | | |
| RRAS | RRAS is a low-cost means of enforcing NAP restrictions. | Low |
| Third-party VPN | Although the cost of acquiring the IPsec technology is low, the costs of designing, implementing, and managing IPsec are moderate. | Medium |

## Step Summary

In this step, the VPN platform was decided.

## Additional Reading

* “Network Access Protection Platform Architecture”: [www.microsoft.com/technet/network/nap/naparch.mspx](http://www.microsoft.com/technet/network/nap/naparch.mspx)
* Chapter 15, “Preparing for Network Access Protection,” of *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press®, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.
* Chapter 18, “VPN Enforcement” in *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.

# Step 3: Determine the Enforcement Layer

In previous steps, it was determined that clients connect to the network locally. The purpose of this step is to determine whether to enforce NAP restrictions at each host using IPsec or to enforce it on the network. Each approach has unique strengths and weaknesses.

## Option 1: Enforce Restrictions at the Hosts

With IPsec enforcement, hosts on the network will ignore traffic from client devices that have not proven that they meet the organization’s health policies. This is a powerful method of protecting compliant computers from other computers. Additionally, it can be combined with server and domain isolation to ensure that when a system has demonstrated its compliance, it will still be restricted to communicating only with authorized hosts. IPsec provides other benefits, as well. For example, network packets are digitally signed, which reduces the risk of man-in-the-middle and replay attacks. Also, traffic can be encrypted with IPsec, which provides a high degree of protection from eavesdropping attacks.

Windows Server includes tools for managing and monitoring IPsec that eliminate much of the associated complexity. Nevertheless, IPsec enforcement is more complex than DHCP enforcement. The cost of acquiring IPsec technology is low, however, because support for it is built into all versions of the Windows operating system that support NAP.

## Option 2: Enforce Restrictions on the Network

Enforcing restrictions on the network means that either 802.1X or DHCP will be used to prevent clients that do not meet the organization’s health policies from accessing the network. The pros and cons of each of these technologies are discussed in the next step. One advantage they both have over IPsec, however, is that noncompliant devices are able to communicate only with hosts on the remediation network, because they are unable to send traffic to any other segments of the network.

## Evaluating the Characteristics

Technical criteria are not the only factors to be considered during an infrastructure design decision. The decision should also be mapped to appropriate operational criteria or characteristics. The following tables compare each option according to the characteristics that are applicable to choosing a method for enforcing NAP.

|  |  |  |
| --- | --- | --- |
| Security | | |
| Host using IPsec | IPsec can isolate individual hosts and entire segments of the network from potentially noncompliant hosts. In addition, the IPsec policies continue to protect portable computers, regardless of where they may travel. IPsec provides robust defense-in-depth protection by digitally signing and encrypting network traffic. | ↑ |
| Network | Depending on the specific network-based enforcement method, the level of security can be good, but not quite as robust as IPsec. | ↑ |

|  |  |  |
| --- | --- | --- |
| Complexity | | |
| Host using IPsec | For many organizations, IPsec would be the most complex approach. However, for those organizations that are already using IPsec for server and domain isolation or other purposes, the level of complexity will seem much lower. | High |
| Network | The level of complexity varies depending on the specific network-enforcement method, but it tends to be lower than that of IPsec. | Medium |

|  |  |  |
| --- | --- | --- |
| Cost | | |
| Host using IPsec | Acquiring IPsec technology costs little because it is built into Windows operating systems. But the overall project costs can be somewhat more expensive than DHCP due to greater complexity. | Medium |
| Network | The cost varies depending on the size of the network and on whether existing resources can be used or upgraded (versus new technology purchased). For example, if new network equipment must be deployed to use 802.1X, the cost will be high, but if existing servers can be used to enforce the restrictions through DHCP, the cost will be low. | High |

## Validating with the Business

In addition to evaluating the decision in this step against IT-related criteria, planners should validate the effect of the decision on the business. The following questions have been known to affect NAP design decisions:

* **What level of risk is acceptable regarding noncompliant devices gaining access to the network?** Although IPsec provides very strong protection for managed hosts, it cannot protect unmanaged hosts from noncompliant devices. For example, if someone establishes an internal web server that the IT team does not manage, that server will have no protection from a mobile user who reconnects a noncompliant computer to the network. Is this a risk that the business can tolerate?
* **Are there other compelling reasons to consider enforcement at the hosts?** Using IPsec enforcement enables other possibilities. When IPsec is deployed across the enterprise, an organization can also use IPsec policies to protect critical business assets from unauthorized access. For example, IPsec policies could be created that allow only members of the legal department to directly access the file server on which documents concerning litigation are stored. All other employees could be prevented from even seeing the server on the network.

## Step Summary

If IPsec enforcement at the hosts is chosen, the decision-making process is complete unless a hybrid solution is required as outlined in “Combining NAP Technologies” later in this guide. If network enforcement is chosen, continue to Step 4.

## Additional Reading

* “Network Access Protection Platform Architecture”: [www.microsoft.com/technet/network/nap/naparch.mspx](http://www.microsoft.com/technet/network/nap/naparch.mspx)
* Chapter 15, “Preparing for Network Access Protection,” in *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.
* Chapter 16, “IPsec Enforcement,” in *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.
* Chapter 17, “802.1X Enforcement” in *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.
* Chapter 19, “DHCP Enforcement,” in *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.

# Step 4: Select Between 802.1X and DHCP

If IT decides to enforce NAP restrictions at the network layer, the organization must choose between two methods: 802.1X and DHCP. Both methods are viable, and each has pros and cons that must be carefully considered. The 802.1X standard can be more complex and expensive, but DHCP provides less security. To use 802.1X as the enforcement method, the switches and wireless access points must support the 802.1X authentication protocol, which means that the devices support Extensible Authentication Protocol (EAP) authentication pass-through to RADIUS, 802.1X authentication, traffic segmentation, and/or dynamic VLAN switching over RADIUS. Many vendors now offer hardware with these capabilities, but it is likely that organizations will have older hardware that must be upgraded or replaced if 802.1X is going to be used in conjunction with NAP. If such hardware is only partially deployed or not deployed at all, the cost of using 802.1X will rise—perhaps considerably, depending on the size of the network.

## Option 1: 802.1X Enforcement

Like IPsec, 802.1X is a robust choice that offers a high degree of protection. Until a client device has demonstrated that it meets the organization’s compliance requirements, the network switches and wireless access points will restrict its access to the network. These restrictions will be difficult to bypass, even by a determined malicious user.

The potential drawback of using 802.1X for enforcement is that it may be more complex and costly to implement than DHCP. The potential cost will vary from one organization to the next, depending on the size of the network and whether the infrastructure devices are capable of supporting 802.1X and NAP. If the network switches and wireless access points do not fully support 802.1X, the organization will have to weigh the expense of upgrading or replacing these network devices versus the benefits of using 802.1X for enforcement. It may be necessary to purchase additional hardware or software, or it may be as simple as downloading and installing new firmware.

## Option 2: DHCP Enforcement

DHCP is the simplest and least-expensive enforcement option. Until a computer has been proven to meet the organization’s health policies, the DHCP server assigns it an IPv4 address configuration that restricts its access to a portion of the network. DHCP enforcement requires that Windows Server 2008 be used to provide DHCP services on the network. Many organizations begin their testing and pilot deployments of NAP using DHCP enforcement, because it can be deployed quickly.

There is one significant drawback to using DHCP with NAP: It is easily bypassed by a user who has administrative privileges on his or her computer. This means that it is trivial for a malicious user and relatively easy for a technically savvy one.

## Evaluating the Characteristics

Technical criteria are not the only factors that should be considered during an infrastructure design decision. The decision should also be mapped to appropriate operational criteria or characteristics. The following tables compare each option according to the characteristics applicable to choosing a method for enforcing NAP.

|  |  |  |
| --- | --- | --- |
| Security | | |
| 802.1X | 802.1X adds defense-in-depth protection by helping to isolate VLANs from one another. | ↑ |
| DHCP | DHCP offers little defense-in-depth protection. | ↓ |

|  |  |  |
| --- | --- | --- |
| Complexity | | |
| 802.1X | Deployment of 802.1X is moderately complex in most situations. | Medium |
| DHCP | DHCP is the simplest enforcement method to implement. | Low |

|  |  |  |
| --- | --- | --- |
| Cost | | |
| 802.1X | The cost of using 802.1X varies depending on two factors: the size of the network, and whether existing hardware can be used or upgraded (versus new hardware purchased). | High |
| DHCP | DHCP tends to be less expensive, especially if the DHCP service in Windows Server 2008 is already deployed. | Low |

## Validating with the Business

In addition to evaluating the decision in this step against IT-related criteria, planners should validate the effect of the decision on the business. The following questions have been known to affect NAP design decisions:

* **Which is more important: implementation cost or security?** Although DHCP is less expensive to deploy, it offers a much lower level of protection than 802.1X.
* **How important is it to minimize the risk of malicious users accessing the network?** Malicious users can easily bypass restrictions that DHCP enforce, but 802.1X is much more robust and difficult for attackers to overcome.

## Step Summary

If either 802.1X enforcement or DHCP enforcement is chosen, the decision-making process is complete.

## Additional Reading

* “Network Access Protection Platform Architecture”: [www.microsoft.com/technet/network/nap/naparch.mspx](http://www.microsoft.com/technet/network/nap/naparch.mspx)
* Chapter 15, “Preparing for Network Access Protection,” in *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.
* Chapter 17, “802.1X Enforcement,” in *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.
* Chapter 19, “DHCP Enforcement,” in *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.

# Additional Considerations

This section presents other factors that should be taken into account when creating plans for deploying NAP.

## Determining System Compliance Requirements

The organization must consider which characteristics will be checked on the client devices for them to be considered compliant. It may decide to use only what is already present on the client devices; conversely, it may find merit in the idea of rolling out additional technologies for system health checks and remediation in conjunction with the NAP deployment. The NAP client is able to verify a range of items when conducting the system compliance check:

* Are malware-prevention technologies, such as antivirus and antispyware software, enabled and up to date?
* Are automatic updates for Windows-based computers enabled?
* Are all current security updates installed?
* Is a host-based firewall enabled and configured correctly?

### Additional Reading

* “Network Access Protection Policies in Windows Server 2008”: [www.microsoft.com/downloads/details.aspx?FamilyID=8e47649e-962c-42f8-9e6f-21c5ccdcf490&displaylang=en](http://www.microsoft.com/downloads/details.aspx?FamilyID=8e47649e-962c-42f8-9e6f-21c5ccdcf490&displaylang=en)
* Chapter 15, “Preparing for Network Access Protection,” in *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.

## Combining NAP Technologies

The steps presented in this guide may imply that each enforcement technology will be implemented alone, but it is possible to use multiple enforcement methods simultaneously. An organization might invest additional resources into combining these enforcement technologies, because they have complementary strengths and weaknesses. RRAS can be used to enforce organizational compliance policies on remote client devices; IPsec could be used for local client devices. The 802.1X protocol and IPsec offer a particularly robust combination, because together they can restrict network connectivity at multiple layers of the network protocol stack. Keep in mind, however, that the complexity of the NAP deployment can increase when combining enforcement methods.

Table 1 illustrates potential ways to combine enforcement methods. The rows represent the primary NAP enforcement method, and the columns represent other methods that can be combined with it.

Table 1. Potential NAP Technology Combinations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | IPsec | 802.1X | VPN | DHCP |
| IPsec |  | ✓ | ✓ | ✓ |
| 802.1X | ✓ |  | X | ✓ |
| VPN | ✓ | X |  | X |
| DHCP | ✓ | ✓ | X |  |

## Dependencies

All NAP enforcement methods rely on NPS in Windows Server 2008 to validate the compliance status of NAP clients. Using DHCP enforcement requires the DHCP service in Windows Server 2008. Using IPsec enforcement requires HRA service in Windows Server 2008. When 802.1X is used, the network devices must be capable of supporting NAP and 802.1X. Using VPN enforcement requires RRAS in Windows Server 2008.

# Conclusion

Organizations can choose from several enforcement methods when deploying NAP. Each has its own strengths and drawbacks with regard to complexity, ease of deployment, and cost, as have been discussed in this guide. After selecting the best NAP enforcement technology and client compliance requirements, the planning process can continue.

If the organization’s analyses lead it to choose IPsec, refer to the following sources for additional planning and implementation guidance:

* Chapter 16, “IPsec Enforcement,” Windows Server 2008 Networking and Network Access Protection (NAP). Microsoft Press, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.
* “Internet Protocol Security Enforcement in the Network Access Protection Platform”: [www.microsoft.com/technet/network/nap/napipsec.mspx](http://www.microsoft.com/technet/network/nap/napipsec.mspx)
* “TechNet Virtual Lab: Network Access Protection with IPSec Enforcement”: <http://go.microsoft.com/?linkid=7032267>
* *Step-by-Step Guide: Demonstrate NAP IPsec Enforcement in a Test Lab*: <http://go.microsoft.com/fwlink/?Linkid=85894>

If the organization’s analyses lead it to choose 802.1x, refer to the following sources for additional planning and implementation guidance:

* Chapter 17, “802.1X Enforcement,” in *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.
* *Step-by-Step Guide: Demonstrate NAP 802.1X Enforcement in a Test Lab*: <http://go.microsoft.com/fwlink/?Linkid=86036>

If the organization’s analyses lead it to choose RRAS, refer to the following sources for additional planning and implementation guidance:

* Chapter 18, “VPN Enforcement,” in *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.
* *Step-by-Step Guide: Demonstrate NAP VPN Enforcement in a Test Lab*: <http://go.microsoft.com/fwlink/?Linkid=85896>

If the organization’s analyses lead it to choose DHCP, refer to the following sources for additional planning and implementation guidance:

* Chapter 19, “DHCP Enforcement,” in *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008. This information is also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.
* *Step-by-Step Guide: Demonstrate NAP DHCP Enforcement in a Test Lab*: <http://go.microsoft.com/fwlink/?Linkid=85897>

## Additional Reading

* Windows Server 2008 R2 Network Access Protection (NAP): [www.microsoft.com/nap](http://www.microsoft.com/nap)
* Microsoft NAP team’s blog: [http://blogs.technet.com/nap](http://blogs.technet.com/nap%20)
* TechNet NAP discussion forum: <http://forums.technet.microsoft.com/en-US/winserverNAP/threads>
* “Introduction to Network Access Protection”: [www.microsoft.com/technet/network/nap/napoverview.mspx](http://www.microsoft.com/technet/network/nap/napoverview.mspx)
* “Network Access Protection Platform Architecture”: [www.microsoft.com/technet/network/nap/naparch.mspx](http://www.microsoft.com/technet/network/nap/naparch.mspx)
* Chapter 14, “Network Access Protection Overview,” *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008; also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.
* Chapter 15, “Preparing for Network Access Protection,” *Windows Server 2008 Networking and Network Access Protection (NAP).* Microsoft Press, 2008; also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.
* Chapter 5, “Firewall and Network Access Protection,” Windows Server 2008 Security Resource Kit. Microsoft Press, 2008; also available as part of the Windows Server 2008 Resource Kit. Microsoft Press, 2008.

# Appendix A: IPD in Microsoft Operations Framework 4.0

Microsoft Operations Framework (MOF) 4.0 offers integrated best practices, principles, and activities to assist an organization in achieving reliable solutions and services. MOF provides guidance to help individuals and organizations create, operate, and support technology services, while helping to ensure the investment in technology delivers expected business value at an acceptable level of risk. MOF’s question-based guidance helps to determine what is needed for an organization now, as well as providing activities that will keep the organization running efficiently and effectively in the future.

Use MOF with IPD guides to ensure that people and process considerations are addressed when changes to an organization’s technology services are being planned.

* Use the Plan Phase to maintain focus on meeting business needs, consider business requirements and constraints, and align business strategy with the technology strategy. IPD helps to define an architecture that delivers the right solution as determined in the Plan Phase.
* Use the Deliver Phase to build solutions and deploy updated technology. In this phase, IPD helps IT pros design their technology infrastructures.
* Use the Operate Phase to plan for operations, service monitoring and control, as well as troubleshooting. The appropriate infrastructure, built with the help of IPD guides, can increase the efficiency and effectiveness of operating activities.
* Use the Manage Layer to work effectively and efficiently to make decisions that are in compliance with management objectives. The full value of sound architectural practices embodied in IPD will help deliver value to the top levels of a business.



Figure A-1. The architecture of Microsoft Operations Framework (MOF) 4.0

# Appendix B: Selecting the Right NAP Architecture in Microsoft Infrastructure Optimization

The Infrastructure Optimization (IO) Model at Microsoft groups IT processes and technologies across a continuum of organizational maturity. (For more information, see <http://go.microsoft.com/fwlink/?LinkId=229236>.) The model was developed by industry analysts, the Massachusetts Institute of Technology (MIT) Center for Information Systems Research and Microsoft's own experiences with its enterprise customers. A key goal for Microsoft in creating the Infrastructure Optimization Model was to develop a simple way to use a maturity framework that is flexible and can easily be applied as the benchmark for technical capability and business value.

IO is structured around three IO models: the Core IO Model, the Application Platform IO Model, and the Business Productivity IO Model. According to the Core IO Model**,** controlling which client computers can access network resources based on their current compliance status helps move an organization toward the Dynamic level (Figure B-1). NAP gives administrators control over which client computers are allowed full access to the internal network by enforcing organizational policies such as required patch levels or the use of antivirus software. This guide assists IT pros in planning and designing the infrastructure for a NAP implementation.

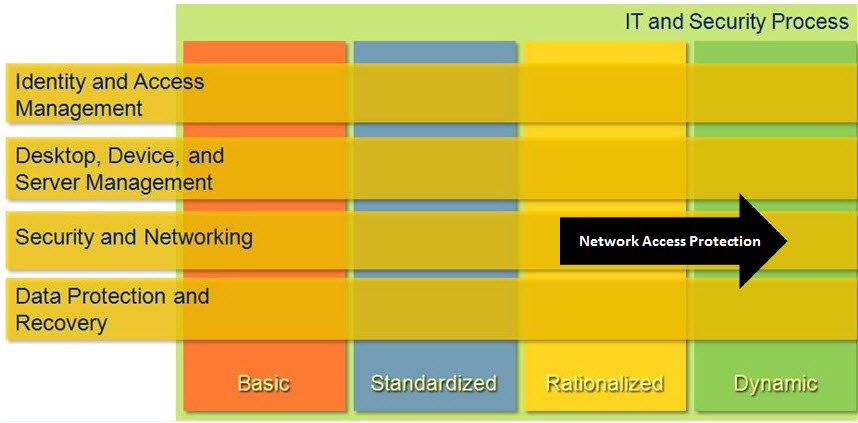


Figure B-1. Mapping of NAP technology into the Core Infrastructure Optimization Model

# Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Description** | **Date** |
| 1.1 | Put guide in current template. | November 2011 |
| 1.0 | First release. | June 2008 |

# Acknowledgments

The Solution Accelerators–Management and Infrastructure (SA-MI) team acknowledges and thanks the people who produced the Infrastructure Planning and Design Guide for Selecting the Right NAP Architecture. The following people were either directly responsible for or made a substantial contribution to the writing, development, and testing of this guide.

**Contributors:**

* Kurt Dillard – *Studio B Productions*
* Greg Lindsay – *Microsoft*
* Frank Simorjay – *Microsoft*

**Reviewers:**

* Tom Cloward – *Microsoft*
* Dave Field – *Studio B Productions*
* Michael Kaczmarek – *Microsoft*
* Robin Maher – *Microsoft*
* Jeff Sigman – *Microsoft*
* Melissa Stowe – *Microsoft*

**Editors:**

* Michelle Anderson – *Studio B Productions*
* Laurie Dunham – *Xtreme Consulting Group*
* Ruth Preston – *Volt Technical Services*

## Feedback

Please direct questions and comments about this guide to [ipdfdbk@microsoft.com](mailto:ipdfdbk@microsoft.com?subject=IPD%20-%20Selecting%20the%20Right%20NAP%20Architecture).