



# Security Architecture for SharePoint Products and Technologies

**Date published:** June 9, 2004

**Summary:**

This is a sample chapter from the Microsoft SharePoint Products and Technologies Resource Kit. You can obtain the complete resource kit (ISBN 0-7356-1881-X), which includes a companion CD-ROM, from [Microsoft Press](#).

Microsoft SharePoint Products and Technologies security is layered on top of, and depends on, the security of underlying products and technologies such as ASP.NET, Internet Information Services (IIS), SQL Server 2000, and Windows Server 2003. It is vital to implement a layered approach to security, often referred to as *defense-in-depth*. Use of defense-in-depth means that security is addressed at a number of levels, including organizational security policies, Windows Server 2003 configuration, IIS configuration, ASP.NET configuration, SharePoint Product and Technologies configuration, communication security, firewall configuration, and so on. In this chapter, we will focus on authentication, authorization, code access security, and communication security in SharePoint Products and Technologies.

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

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

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2007 Microsoft Corporation. All rights reserved.

Microsoft, SharePoint, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

# Security Architecture for SharePoint Products and Technologies

This is a sample chapter from the Microsoft SharePoint Products and Technologies Resource Kit. You can obtain the complete resource kit (ISBN 0-7356-1881-X), which includes a companion CD-ROM, from [Microsoft Press](#).

Microsoft SharePoint Products and Technologies security is layered on top of, and depends on, the security of underlying products and technologies such as ASP.NET, Internet Information Services (IIS), SQL Server 2000, and Windows Server 2003. Needless to say, communication security and firewall configuration are vital as well. As with any Web application, your SharePoint site is only as secure as its weakest link; security is a concern across all components of your SharePoint Products and Technologies deployment. Because SharePoint Products and Technologies security spans many technologies, you need to have an understanding of security in these technologies to make all parts of your SharePoint Products and Technologies deployment work together in a secure fashion.

It is vital to implement a layered approach to security, often referred to as *defense-in-depth*. Use of defense-in-depth means that security is addressed at a number of levels, including organizational security policies, Windows Server 2003 configuration, IIS configuration, ASP.NET configuration, SharePoint Product and Technologies configuration, communication security, firewall configuration, and so on.

SharePoint Products and Technologies make use of a number of technologies that reduce the risk of security being compromised. These technologies include:

- Authentication that uses Windows principals and therefore can make use of strong authentication methods, password policies, account lockout policies, and encryption
- Authorization that is based on the permissions model to ensure a high degree of granular control over access to contents of a site
- Code access security in .NET Framework that allows you to control code access to protected resources and operations
- Security techniques such as Secure Sockets Layer (SSL) and IPsec that allow you to protect your communications inside and outside the firewall
- Firewall protection of external sites

In this chapter, we will focus on authentication, authorization, code access security, and communication security in SharePoint Products and Technologies. Research has shown that early design of authentication and authorization eliminates a high percentage of vulnerabilities. Code access security allows code to be trusted to varying degrees, depending on where the code originates from and on other aspects of the code's identity. Communication security is an integral part of securing your deployment to protect data passed between users and your site, and between the servers in your deployment. For discussion on security policies for SharePoint Products and Technologies refer to Chapter 24, "Information Security Policies for SharePoint Products and Technologies."

## ***Authentication***

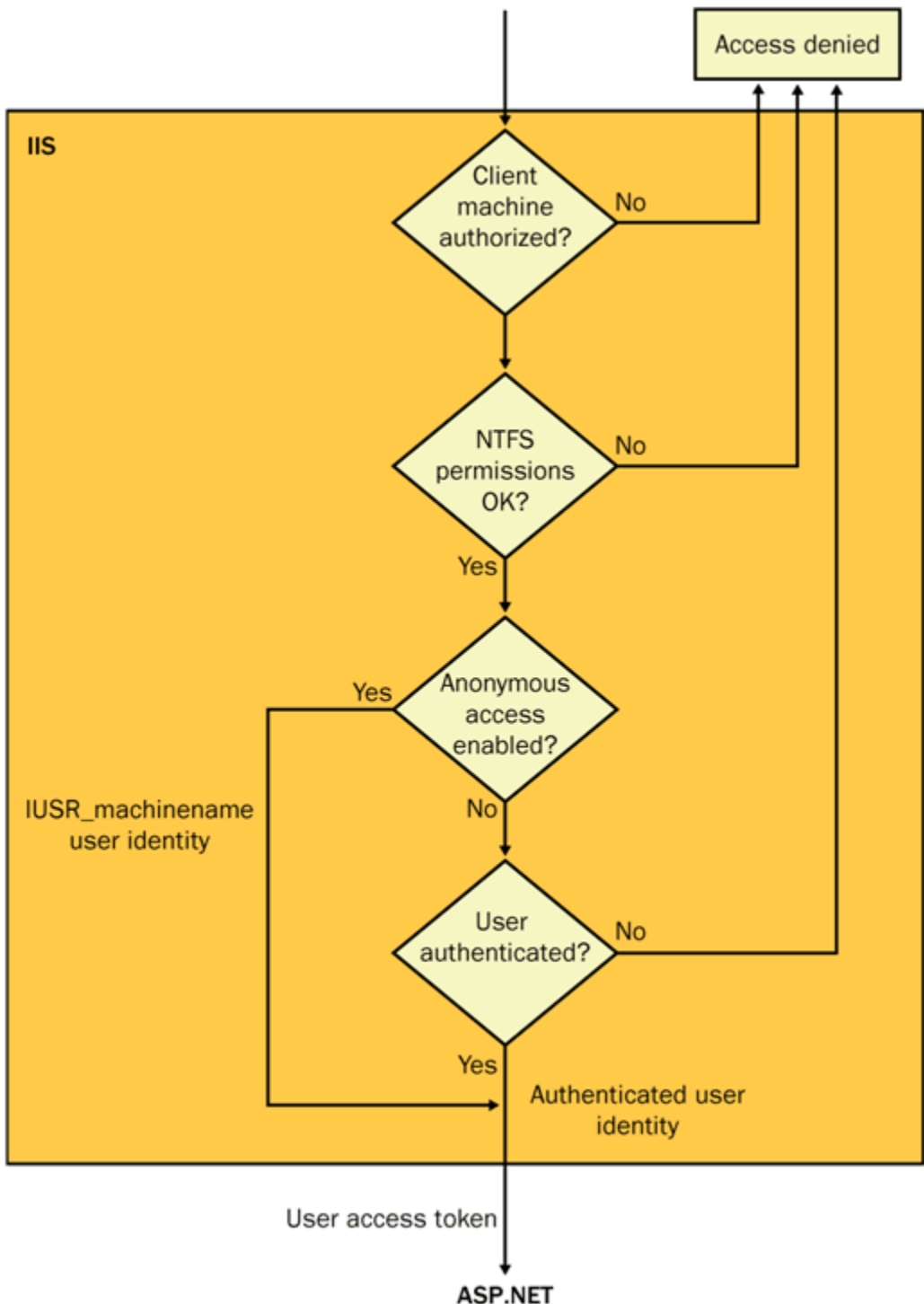
Authentication is the process of positively identifying the users of your site. Authentication ensures that the users are who they claim to be. Authenticated clients are referred to as *principals*.

In SharePoint Products and Technologies, authentication is based on Windows security accounts.

For SharePoint sites, ASP.NET is configured to use Windows authentication. In web.config files, the authentication section is as follows:

```
<system.web>  
  <authentication mode="windows" >  
</system.web>
```

With Windows authentication mode, ASP.NET relies on IIS to perform the required authentication of a client. IIS authenticates the requesting user against Windows security accounts. After IIS authenticates a client, it passes a user identity to ASP.NET. (See Figure 6-1.)



**Figure 6-1 Passing user identity in Windows authentication mode**

You can use a variety of IIS authentication schemes for SharePoint Products and Technologies user authentication, as follows:

**Basic.**

- Basic authentication is part of the HTTP 1.1 protocol that is supported by virtually all browsers. With SharePoint Products and Technologies, it can be used in the extranet environment. The

credentials are transmitted unencrypted. You should use basic authentication only over SSL; otherwise, basic authentication is not secure.

### **Integrated Windows.**

- Integrated Windows authentication is a secure authentication method that is most suitable for your intranet SharePoint sites. It does not work over proxy servers. It is implemented as either Kerberos or NTLM. Kerberos requires Windows 2000 or later operating systems on the client and server computers.


### **Client Certificates Mapping.**

- Clients require X.509 certificates. This is an optional authentication mechanism that can be used when SSL is enabled between the client and the server. For example, it can be used on the extranets when your security policy requires two-level authentication—a system in which clients are required to provide something they have (a certificate) and users are asked to provide something they know (authentication credentials). For configuration details, refer to Chapter 27, “Securing an Extranet Using SSL and Certificates.”

### **Anonymous.**

- Anonymous authentication allows anonymous access to the website. The default user identity used for anonymous access is IUSR\_machinename. When IIS receives an anonymous request, it impersonates the IUSR\_machinename account. In this case, the identity passed to ASP.NET is IUSR\_machinename.

User access in SharePoint Products and Technologies is based on Windows security principals such as individual user accounts and security group accounts (DOMAIN\user and DOMAIN\security group).

 You cannot use distribution lists to control access to content in Windows SharePoint Services because distribution lists are not Windows security principals.

In addition to authenticating users for the SharePoint sites access, SharePoint Portal Server provides a single sign-on (SSO) functionality that allows you to authenticate users to a portal site, and then to retrieve a user’s stored credentials for other user-aware enterprise business applications from an SSO database when required. The SSO functionality is implemented by the Microsoft Single Sign-On service (SSOSrv). SSOSrv provides storage and mapping of credentials such as account names and passwords so that the portal-based applications can retrieve information from the third-party applications and back-end systems. This prevents users from having to authenticate themselves again when the portal-based applications need to obtain information from other business applications and systems. For details on how you can enable and configure SSO in SharePoint Portal Server, refer to Chapter 26, “Single Sign-On in SharePoint Portal Server 2003.”

## **Authorization**

Authorization defines which resources and operations the authenticated user is allowed to access. In Windows SharePoint Services and SharePoint Portal Server, access to sites is controlled through a role-based membership system by which each user is associated directly or indirectly with a permission that controls the specific actions that the user can perform. This membership system is based on *site groups*. Using a site group is a way to configure rights for users based on the kinds of tasks they perform.


Site groups specify what rights the users have on a site. The rights determine what specific actions the users can perform on the site. Although the concepts of using site groups are the same in Windows SharePoint Services and SharePoint Portal Server, because of the additional feature set in the SharePoint Portal Server there are differences in the user rights and corresponding permissions, as well as the default site groups. Because of these differences, we

will look into authorization in Windows SharePoint Services and SharePoint Portal Server separately.

## Authorization in Windows SharePoint Services

In this section, we will look into user authorization to access Windows SharePoint Services sites as well as administrative tasks related to setting up authorization. Windows SharePoint Services uses site groups to manage site-wide security. Rights specify the actions that users can perform; in essence, each site group is a collection of rights.

If you want all users to be able to browse your site, you can enable anonymous access to the site. Anonymous access is disabled by default.

 With anonymous access enabled, users can browse the site without authentication, but they cannot perform any administrative tasks on the site. The administration pages require authentication.

To run custom code that uses the Windows SharePoint Services object model, users must have the appropriate permissions assigned to them, just as when they interact with a site or list through the user interface.

To be authorized to perform administrative tasks that affect settings for all websites and virtual servers on the server computer, a user must be a member of the local administrators group on the server machine or a member of the SharePoint administrators group.

## Site Groups

Windows SharePoint Services includes 21 rights, which are used in the five default user site groups. The five default user rights groups are Guest, Reader, Contributor, Web Designer, and Administrator. Table 6-1 shows user rights that are included in each site group by default.

The rights assigned to the Guest and Administrator site groups cannot be changed. However, you can customize the rights available in Reader, Contributor, and Web Designer site groups to include only the rights you want.

You can add new site groups to combine different sets of rights, edit the rights assigned to a site group, or delete an unused site group.

You cannot assign users directly to the Guest site group, rather users who are given access to lists or document libraries by way of per-list permissions are automatically added to the Guest site group. The Guest site group cannot be customized or deleted.

You can manage site groups and permissions by using HTML administration pages or the command-line administration tool Stsadm.exe. For a detailed description of specific tasks, refer to Chapter 16, "Windows SharePoint Services Site Administration."

You can also use the Windows SharePoint Services object model to perform the management tasks in code. For details, refer to the SharePoint Products and Technologies Software Development Kit (SDK) at <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/spptsdk/html/SPSDKWelcome.asp>.

**Table 6-1. Default Windows SharePoint Services Site Groups and their Rights**

Site group name	User rights included by default
Guest	None
Reader	Use Self-Service Site Creation View Pages

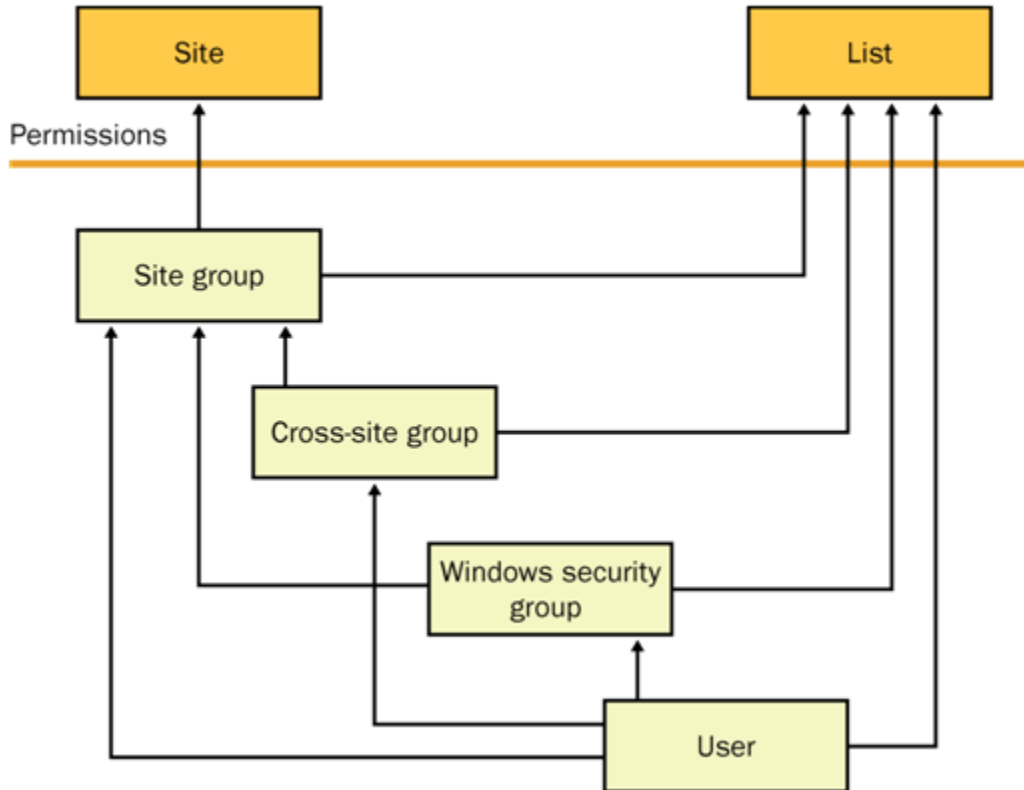
Site group name	User rights included by default
	View Items
Contributor	All rights included in the Reader site group, plus: <ul style="list-style-type: none"> <li>• Add Items</li> <li>• Add/Remove Private Web Parts</li> <li>• Browse Directories</li> <li>• Create Cross-Site Groups</li> <li>• Delete Items</li> <li>• Edit Items</li> <li>• Manage Personal Views</li> <li>• Update Personal Web Parts</li> </ul>
Web Designer	All rights included in the Contributor site group, plus: <ul style="list-style-type: none"> <li>• Add and Customize Pages</li> <li>• Apply Themes and Borders</li> <li>• Apply Style Sheets</li> <li>• Cancel Check-out</li> <li>• Manage Lists</li> </ul>
Administrator	All rights included in the Web Designer site group, plus: <ul style="list-style-type: none"> <li>• Create Subsites</li> <li>• Manage List Permissions</li> <li>• Manage Site Groups</li> <li>• View Usage Data</li> </ul>

In addition to defining the site groups, you can define your own cross-site groups. Cross-site groups consist of users and can be assigned to a site group on any website in a site collection. There are no cross-site groups defined by default.

Site groups are defined per website. Subsites can either use the same permissions as the parent website (inheriting both the site groups and users available on the parent website) or use unique permissions. When you create a subsite, you can choose whether to inherit the permissions from the parent website or to create unique permissions for your subsite.


You can specify unique permissions on a per-list basis. Unlike for sites, you can add users together with specified permissions directly to a list, in which case the users are automatically assigned to the Guest site group on the current site if the site is unique and does not inherit permissions from a parent site. If the current site inherits permissions, the users are added to the Guest site group on the most recent unique ancestor site.

The users are granted permissions to a site or list through direct or indirect membership in a site group. They can be added directly to a site group or added to a cross-site group that is a member of a site group, or they can be members of a Windows domain group that is added to a site group. In addition, an individual user can be directly added to a list in association with a specified permission. Figure 6-2 shows the means by which users are granted permissions to a site or a list.



**Figure 6-2 Granting user permissions to a site or list in Windows SharePoint Services**

Most user rights are dependent on other user rights. For example, you must be able to view items before you can edit items. If a right is deleted from a site group, any rights dependent on that right are also deleted. For detailed information about dependencies on user rights, refer to Table 6-2.

 In the Windows SharePoint Services object model, unlike the user interface, rights are not dependent on other rights. To run custom code that uses types and members in the SharePoint Products and Technologies object model, users and groups must be assigned the appropriate permissions, just as when interacting with a site or list by using the user interface. However, in this case there are no dependencies: rights can be assigned individually without including dependent rights, and they can be assigned to users and groups in any combination.

**Table 6-2. Windows SharePoint Services Rights Dependencies**

Right	Permissions	Groups included by default	Dependent rights
-------	-------------	----------------------------	------------------


<b>Right</b>	<b>Permissions</b>	<b>Groups included by default</b>	<b>Dependent rights</b>
Add and Customize Pages	Create ASP.NET, ASP, and HTML pages for a website	Web Designer, Administrator	Browse Directories, View Pages
Add Items	Add items to lists or add documents to document libraries	Contributor, Web Designer, Administrator	View Items, View Pages
Add/Remove Private Web Parts	Add and remove Web Parts to personalize Web Part Pages	Contributor, Web Designer, Administrator	Update Personal Web Parts, View Items, View Pages
Apply Style Sheets	Apply a style sheet to the entire website	Web Designer, Administrator	View Pages
Apply Themes and Borders	Apply a theme or border to an entire website	Web Designer, Administrator	View Pages
Browse Directories	Browse the directory structure of a website	Contributor, Web Designer, Administrator	View Pages
Cancel Check-Out	Cancel the check-out action performed by another user	Web Designer, Administrator	View Pages
Create Cross-Site Groups	Create or delete cross-site groups, or change membership of a cross-site group	Contributor, Web Designer, Administrator	View Pages
Create Subsites	Create a new subsite or workspace site, such as a Document Workspace site or Meeting Workspace site	Reader, Contributor, Web Designer, Administrator	View Pages
Delete Items	Delete list items and documents from the website	Contributor, Web Designer, Administrator	View Items, View Pages
Edit Items	Edit existing list items and documents in the website	Contributor, Web Designer, Administrator	View Items, View Pages
Manage Lists	Create, edit, or delete lists and change their settings	Web Designer, Administrator	View Items, View Pages, Manage Personal Views
Manage List Permissions	Change permissions for a list or document library	Administrator	Manage Lists, View Items, View Pages, Manage Personal Views

<b>Right</b>	<b>Permissions</b>	<b>Groups included by default</b>	<b>Dependent rights</b>
Manage Personal Views	Create, edit, or delete personal views on lists	Contributor, Web Designer, Administrator	View Items, View Pages
Manage Site Groups	Create, delete, and edit site groups, both by changing the rights assigned to the site group and by changing which users are members of the site group	Administrator	View Pages
Manage Web Site	Perform administration tasks for a particular site or subsite	Administrator	View Pages
Update Personal Web Parts	Update Web Parts to display personalized information	Contributor, Web Designer, Administrator	View Items, View Pages
Use Self-Service Site Creation	Use the Self-Service Site Creation tool to create a top-level website.	Reader, Contributor, Web Designer, Administrator	View Pages
View Items	View items in lists, documents in document libraries, and Web discussion comments	Reader, Contributor, Web Designer, Administrator	View Pages
View Pages	Browse pages in the website	Reader, Contributor, Web Designer, Administrator	None
View Usage Data	View reports on website usage	Administrator	View Pages


## Site Creation Rights

Site creation rights (Use Self-Service Site Creation and Create Subsites) control whether users can create top-level websites, subsites, or workspaces.

Members of the Administrator site group can create subsites from their websites. However, Self-Service Site Creation is different: it is a feature that is enabled by administrators and allows users to create their own top-level websites. Users do not need administrator permissions on the server or virtual server, only permissions on the website where Self-Service Site Creation is hosted. By default, the Use Self-Service Site Creation right is included in all site groups except the Guest site group, and it gives users access to the signup page and the ability to use Self-Service Site Creation.

 The Self-Service Site Creation right is available only on a top-level website in a site collection.

Self-Service Site Creation allows users to create and manage their own top-level websites automatically. Self-Service Site Creation is disabled by default—you must turn on the feature to use it. You enable Self-Service Site Creation for a single virtual server at a time from the Configure Self-Service Site Creation page for the virtual server that you want to enable. If you want to use it on all virtual servers in your server farm, you must enable it for every virtual server individually.


 You can use either HTML administration pages or the command-line tools `enablescc.exe` and `disablescc.exe` to turn on and configure Self-Service Site Creation. Either method allows you to turn on or turn off Self-Service Site Creation and specify the type of information to require when creating a site. For details, refer to Chapter 15, “Configuring Windows SharePoint Services.”

## Anonymous Access

Anonymous access allows users to view pages anonymously or to contribute anonymously to lists and surveys. When you enable anonymous access in Windows SharePoint Services, you are enabling access to your site for the IIS anonymous account `IUSR_machinename`.

Anonymous access is disabled by default and is controlled at the site level. To enable anonymous access, you must first verify that IIS is configured to allow anonymous access, and then enable anonymous access for your website by using the Site Settings. Anonymous access for specific lists is controlled using the per-list permissions. If anonymous access is disabled for your site, it cannot be enabled for a particular list in the site.

You can also grant access to “all authenticated users” to allow all members of your domain to access a website without having to enable anonymous access.

 For detailed description of configuration steps for enabling anonymous access, refer to Chapter 16.

## Performing Administration Tasks

Users assigned to the Administrator site group are administrators only for a particular website. To perform any administrative tasks that affect settings for all websites and virtual servers on the server computer, a user must be an administrator for the server computer (also known as a *local administrator*) or a member of the SharePoint administrators group, rather than a member of the Administrator site group for the site.


The virtual server administration pages can be accessed only by local computer administrators or the members of the SharePoint administrators group. This is configured using URL authorization in the `web.config` file for the Central Administration pages that is located in the folder `<Local Drive>:\Program Files\Common Files\Microsoft Shared\web server extensions\60\TEMPLATE\ADMIN\1033`. The `<authorization>` element is defined as follows:

```
<authorization>
  <allow roles="BUILTIN\Administrators" />
  <allow users="Domain\SharePoint Administrators account name" />
  <deny users="*" />
</authorization>
```

The SharePoint administrators group is a Windows domain group that has administrative access to Windows SharePoint Services in addition to the local administrators group. Members of this local administrators group configure the name of a Windows group to become the SharePoint

Administrators group using Central Administration pages. The name specified in Central Administration pages is the name in web.config file; when you change the SharePoint administrators group, the name is changed in the <authorization> element in web.config file.

You can add users to the SharePoint administrators groups, rather than to the local administrators group, to separate administrative access to Windows SharePoint Services from administrative access to the local server computer. Members of both the SharePoint administrators group and the local administrators group have rights to view and manage all sites created on their servers.

 The SharePoint administrators group members do not have access to the IIS metabase, so they cannot perform the following actions for Windows SharePoint Services: extend virtual servers, manage paths, change the SharePoint administrators group, change the configuration database settings, and use the Stsadm.exe command-line tool. They can perform any other administrative action using the HTML Administration pages or the Windows SharePoint Services object model.

## Authorization in SharePoint Portal Server

In this section, we will look into user authorization access to SharePoint Portal Server sites, backward-compatible document libraries, and search results.

Similar to Windows SharePoint Services, SharePoint Portal Server uses site groups to manage site-wide security. Each user is a member of at least one site group, and access to portal sites is controlled through a site group membership system. After you create a portal site, you can give users access to it by assigning them to site groups. A user who is not assigned to a site group won't be able to access the portal site.

In addition to providing authorization based on the site groups membership, SharePoint Portal Server provides role-based security for backward-compatible document libraries.

## Site Groups

SharePoint Portal Server uses six default site groups to group users with a specific set of customizable rights. You can also create a custom site group for a specific area or list and assign a specific set of rights to it. You can edit the rights assigned to a site group, create a new site group, or delete an unused site group.

The six default SharePoint Server groups are as follows:

- Reader site group allows users to search, view, and browse content in the site.
- Member site group allows users to submit listings and create personal sites.
- Contributor site group allows users to submit content to areas in the site to which they are granted rights.
- Web Designer site group allows users to change layout and settings on a Web page to which they are granted rights.
- Administrator site group allows users full control of the website.
- Content Manager site group allows users to manage all settings and content in an area to which they are granted rights.

You can use site groups to control general access to the portal site as well as to control access to specific areas in the portal site.

Although the site groups in SharePoint Portal Server and Windows SharePoint Services are similar in many respects, there are a number of differences:

- There are two default site groups in SharePoint Portal Server that are not available with

Windows SharePoint Services: Member and Content Manager. Both site groups allow users access to the features that are defined only in the SharePoint Portal Server: Member site group allows you to create personal sites, and Content Manager allows you to manage areas for grouping content by user-defined criteria.

- There is no default Guest site group in SharePoint Portal Server. This is because the Guest group is used automatically in Windows SharePoint Services when you assign per-list permissions.
- The user rights and the corresponding permissions differ between SharePoint Portal Server and the Windows SharePoint Services. This is because of the differences in the functionality and feature set of these two products. Some rights are the same—for example, View Pages. However, the rights that relate to managing areas, alerts, user profiles, audiences, and search are distinctly different because these features are present only in SharePoint Portal Server.

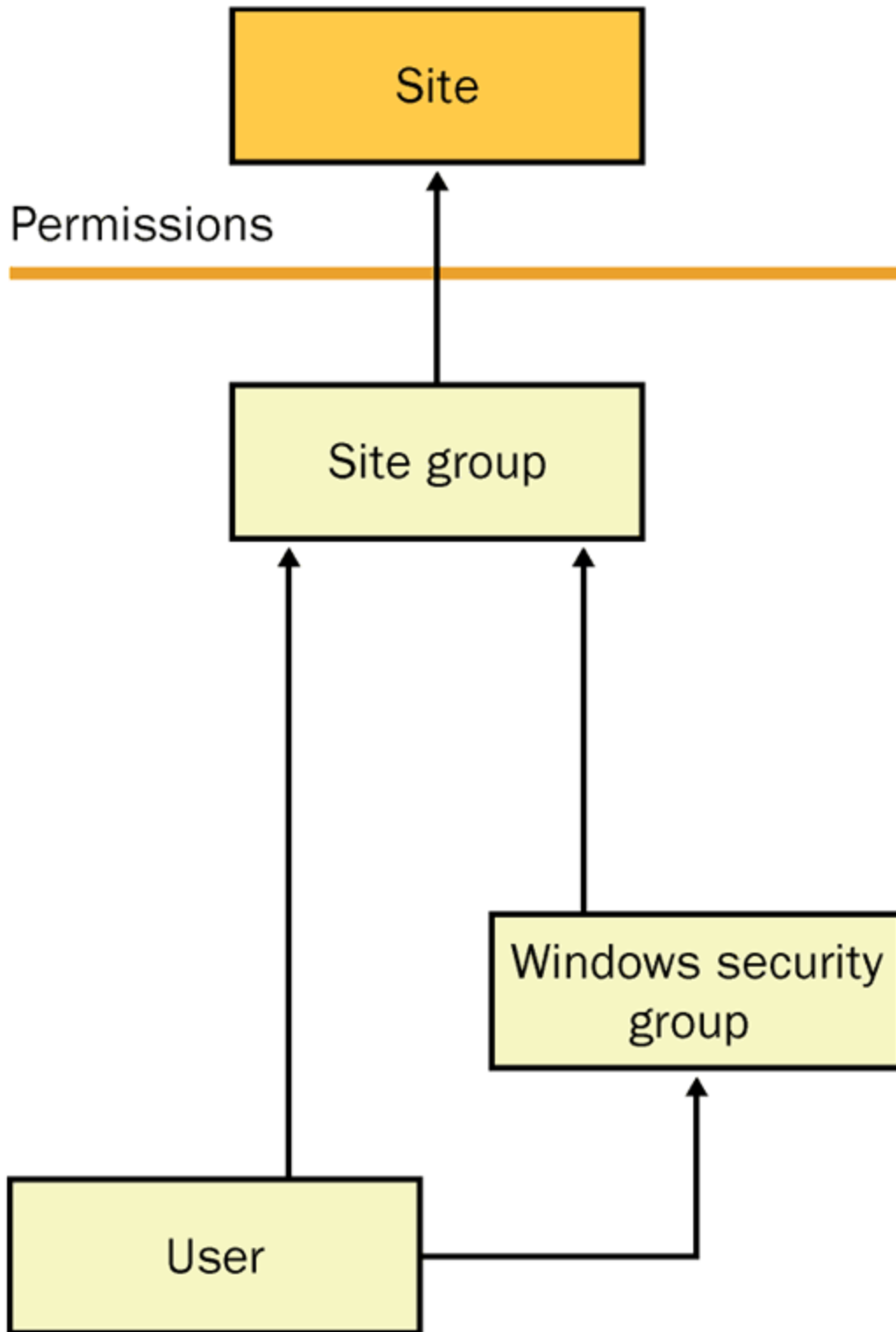
The SharePoint Portal Server user rights and corresponding permissions are listed in Table 6-3.

**Table 6-3. SharePoint Portal Server User Rights and Corresponding Permissions**

<b>Right</b>	<b>Permissions</b>
Add and Customize Pages	Add, change, or delete HTML pages or Web Part Pages, and edit the portal site by using a Windows SharePoint Services-compatible editor
Add Items	Add items to lists, add documents to SharePoint document libraries, add Web Discussion comments
Add/Remove Personal Web Parts	Add or remove Web Parts on a personalized Web Part Page
Apply Style Sheets	Apply a style sheet (.CSS file) to an area or the portal site
Browse Directories	Browse directories in an area
Cancel Check-Out	Check in a document without saving the current changes
Create Area	Create an area on the portal site
Create Personal Site	Create a personal SharePoint site
Create Sites	Create SharePoint sites by using Self-Service Site Creation
Delete Items	Delete items from a list, documents from a document library, and Web discussion comments in documents
Edit Items	Edit items in lists, edit documents in SharePoint document libraries, and customize Web Part Pages in SharePoint document libraries
Manage Alerts	Change alert settings for the portal site and manage alerts for users
Manage Area	Delete or edit the properties for an area on the portal site
Manage Area Permissions	Add, remove, or change user rights for an area
Manage Audiences	Add, change, or delete audiences

<b>Right</b>	<b>Permissions</b>
Manage Personal Views	Create, change, and delete personal views of lists
Manage Portal Site	Specify portal site properties and manage site settings
Manage Search	Add, change, or delete index and search settings in the portal site
Manage User Profiles	Add, change, or delete user profile information and properties
Search	Search the portal site and all related content
Update Personal Web Parts	Update Web Parts to display personalized information
Use Personal Features	Use alerts and personal sites
View Area	View an area and its contents
View Pages	View pages in an area

As in Windows SharePoint Services, users are granted permissions to a portal site through direct or indirect membership in a site group. However, the difference in assigning rights is that cross-site groups are not supported in SharePoint Portal Server; cross-site groups are supported only in Windows SharePoint Services. In SharePoint Portal Server, users can be added directly to a site group or they can be members of a Windows domain group that is added to a site group. Figure 6-3 shows the means by which users are granted permissions to a portal site.



**Figure 6-3 Granting user permissions to a portal site**

You can adjust access to areas of the portal site by assigning users to a site group for a specific area. You can customize security for each area in the portal by adding, editing, or removing users or site groups.

By default, security settings on a parent area will be applied automatically to all its subareas. Adding users or groups to a specific area will break the inheritance of security settings: if you customize the security on a subarea, the subarea will no longer inherit changes made to the parent area.

## Site Creation Rights

Site creation rights (Create Sites and Create Personal Site) control whether users can create portal sites and personal sites.

The Create Sites right allows users to create portal sites by using Self-Service Site Creation. As in Windows SharePoint Services, the Self-Service Site Creation is disabled by default in SharePoint Portal Server—you must turn on the feature to use it. By default, the new sites are created using the default content database; you can configure the alternate content database. For details, refer to Chapter 18, “Managing SharePoint Portal Server 2003.”


The Create Personal Sites right allows users to create a personal site by clicking My Site on the title bar on the portal home page. Site administrators control the location and site naming format for the personal sites on the portal by using the Manage Personal Sites page.

## Anonymous Access


Anonymous access allows users to view pages on your portal site anonymously or to perform searches anonymously. When you enable anonymous access in SharePoint Portal Server, you are enabling access to your site for the IIS anonymous account IUSR\_machinename.

Anonymous access is disabled by default and is controlled at the portal-site level. To enable anonymous access, you must first verify that IIS is configured to allow anonymous access, and then enable anonymous access for your portal site by using SharePoint Portal Server Central Administration pages.

If you need to retain the ability to authenticate users as well as provide anonymous access, you can create a new virtual server, extend this virtual server, and then enable anonymous access for this virtual server by using SharePoint Portal Server Central Administration. In this case, users who access the original portal site will require authentication while users who access the new virtual server will have anonymous access.

 To create and extend a virtual server, you must be a member of the local administrators group. To enable anonymous access or manage anonymous access settings, you must be an Administrator on the portal site, a member of the SharePoint Administrators group, or a member of the local administrators group.

After you have enabled anonymous access for your portal site, you can allow anonymous users to access and view pages and to perform searches on your portal site. If anonymous access is disabled for your site, it cannot be enabled for viewing areas or performing searches.

 For detailed instruction on configuration steps for setting up anonymous access for a portal site, refer to Chapter 18, “Managing SharePoint Portal Server 2003.”

## Performing Administration Tasks

SharePoint Portal Server is built on Windows SharePoint Services, so it comes as no surprise that as far as performing administration tasks are concerned, the permissions remain essentially the same:

- To perform any administrative tasks that affect settings for all portal sites and virtual servers on the server computer, a user must be an administrator for the server computer or a member of the SharePoint administrators group.

- Users assigned to the Administrator site group are administrators only for a particular portal site.

## **Security for Backward-Compatible Document Libraries**

It is a frequent requirement to restrict access to information in the backward-compatible document library (Web Storage System–based). In some cases, it is required to restrict the viewing of a document to users who edit or approve it, until it is ready for a larger audience.

In the backward-compatible document library, SharePoint Portal Server roles add actions such as check-in, check-out, publish, and approve to traditional file-access permissions such as Read, Write, and Change. There are three fixed roles; each role identifies a specific set of permissions, as follows:

- Coordinators handle management tasks.
- Authors add and update files.
- Readers have read-only access to published documents.

Access permissions for the three roles are fixed and cannot be modified. SharePoint Portal Server also offers the option of denying users access to specific documents. Roles are usually specified at the folder level, although you can add coordinators at the document-library level for management tasks.

## **Search Results**

SharePoint Portal Server recognizes security policies in use on your organization's servers, file shares, and databases during searches. This authorization is important, as it prevents users from finding documents to which they have no access when they perform searches in the portal site. For detailed discussion on the search architecture, functionality, and configuration, refer to Chapter 21, "The Architecture of the Gatherer," and Chapter 22, "Managing External Content in Microsoft Office SharePoint Portal Server 2003."

## ***Code Access Security***

SharePoint Products and Technologies Services use code access security to control access to protected resources. Code access security is a security mechanism that lets you assign to a SharePoint Products and Technologies application a configurable level of trust that corresponds to a predefined set of permissions. Code access security allows code to be trusted to varying degrees, depending on where the code originates and on other aspects of the code's identity. Code access security provides the following functionality:

- Defines permissions and permission sets that represent the right to access various system resources
- Enables administrators to configure security policy by associating sets of permissions with groups of code (code groups)
- Enables code to request the permissions it requires to run, as well as the permissions that would be useful to have, and specifies which permissions the code must never have
- Grants permissions to each assembly that is loaded, based on the permissions requested by the code and on the operations permitted by security policy
- Enables code to demand that its callers have specific permissions
- Enables code to demand that its callers possess a digital signature, thus allowing only callers from a particular organization or site to call the protected code
- Enforces restrictions on code at run time by comparing the granted permissions of every caller

on the call stack to the permissions that callers must have

To determine whether code is authorized to access a resource or perform an operation, the runtime's security system walks the call stack, comparing the granted permissions of each caller to the permission being demanded. If any caller in the call stack does not have the demanded permission, a security exception is thrown and access is refused.

To allow the administrator to switch levels of trust assigned to an application, in addition to the ASP.NET default security policy files Windows SharePoint Services provides two policy files of its own: Windows SharePoint Services Minimal (WSS\_Minimal) and Windows SharePoint Services Medium (WSS\_Medium). When a virtual server is extended to host Windows SharePoint Services, the WSS\_Minimal policy is applied to it by default.

## SharePoint Products and Technologies Code Access Security Policies

The WSS\_Minimal and WSS\_Medium policy files are located by default in the folder <Local Drive>:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\60\config. The files are named wss\_minimaltrust.config and wss\_mediumtrust.config, respectively. Permissions in WSS\_Minimal and WSS\_Medium policy files are listed in Table 6-4.

**Table 6-4. Permissions Defined in WSS\_Minimal and WSS\_Medium Policies**

Permission	WSS_Medium	WSS_Minimal
AspNetHostingPermission	Medium	Minimal
Environment	Read: TEMP, TMP, OS, USERNAME, COMPUTERNAME	
FileIO	Read, Write, Append, PathDiscovery:Application Directory	
IsolatedStorage	AssemblyIsolationByUser, UserQuota specified	
Security	Execution, Assertion, ControlPrincipal, ControlThread, RemotingConfiguration	Execution
WebPermission	Connect to origin host (if configured)	
DNS	Unrestricted or all subpermissions granted	
SqlClientPermission	Unrestricted or all subpermissions granted	
SharePointPermission	SharePointPermission.ObjectModel	
WebPartPermission	WebPartPermission.Connections	WebPartPermission.Connections


Both WSS\_Minimal and WSS\_Medium policies extend ASP.NET default policy files. These policies grant Full trust to assemblies in the global assembly cache (GAC) and \$CodeGen, but they only partially trust the assemblies installed in the /bin directory of the virtual server.

In addition to the default set of permissions defined by ASP.NET and the common language runtime, SharePoint Products and Technologies has defined two custom permissions, `SharePointPermission` and `WebPartPermission`, as part of the `Microsoft.SharePoint.Security` namespace located in the `Microsoft.SharePoint.Security.dll`. All code that tries to access the SharePoint Products and Technologies class libraries needs the `SharePointPermission` with the `ObjectModel` property set to true. For a full list of `SharePointPermission` and `WebPartPermission` attributes, refer to the “Microsoft Windows SharePoint Services and Code Access Security” whitepaper located at [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/odc\\_sp2003\\_ta/html/sharepoint\\_wsscodeaccesssecurity.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/odc_sp2003_ta/html/sharepoint_wsscodeaccesssecurity.asp).

Based on the requirements and the trust associated with assemblies installed in the `/bin` directory of the virtual server extended with SharePoint Products and Technologies, administrators can choose to change the permissions associated with these assemblies. An easy approach is to change the policy applied to the virtual server by changing the trust level attribute in the `web.config` file of the specific virtual server. The default levels of trust, listed in permissions order, are as follows:

- Full
- High (This is an ASP.NET default level, so the `SharePointPermission` and `WebPartPermission` will not be granted.)
- WSS\_Medium
- Medium (This is an ASP.NET default level, so the `SharePointPermission` and `WebPartPermission` will not be granted.)
- Low (This is an ASP.NET default level, so the `SharePointPermission` and `WebPartPermission` will not be granted.)
- WSS\_Minimal
- Minimal (This is an ASP.NET default level, so the `SharePointPermission` and `WebPartPermission` will not be granted.)

If your code tries to perform an action or access a resource that is protected by the common language runtime, the default permissions might be insufficient and your code might need one or more of the default ASP.NET permissions.

 If you want to use the classes and members in the `Microsoft.SharePoint.Portal.SingleSignOn` namespace, your code will need an additional permission, `SingleSignonPermission.Access`. Refer to Chapter 26 for detailed instructions.

There are several ways to make sure your code has the required permissions to access the SharePoint Products and Technologies class libraries, as follows:

- Create a custom security policy and assign the `SharePointPermission` with the `ObjectModel` property set to true to the specific assembly or set of assemblies. Refer to Chapter 39, “Using Microsoft Office InfoPath with SharePoint Products and Technologies,” for detailed instructions.
- Install the assembly in the global assembly cache, as the code in it always has Full trust. Although installing your Web Part assembly in the GAC is a viable option, it is recommended that you install Web Part assemblies in the `/bin` directory for a more secure deployment. For the full list of pros and cons of installing an assembly into the GAC, refer to [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/odc\\_sp2003\\_ta/html/sharepoint\\_wsscodeaccesssecurity.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/odc_sp2003_ta/html/sharepoint_wsscodeaccesssecurity.asp).
- Raise the trust level for the virtual server extended with SharePoint Products and Technologies by changing the trust level attribute in the `web.config` file. For example, to change the policy level of a virtual server from `WSS_Minimal` to `WSS_Medium`, perform the following steps:
  1. Open the `web.config` file of the virtual server in a text editor such as Notepad.

2. Search for `<trust level="WSS_Minimal" originUrl="" />`.
3. Change the level to the following: `<trust level="WSS_Medium" originUrl="" />`
4. Save the web.config file.
5. Reset Internet Information Services (IIS) by using `iisreset` in the command prompt.

## **Communication Security**

Secure communication between the components of a SharePoint Products and Technologies deployment is a vital element of an in-depth security architecture. In SharePoint Products and Technologies deployments, it's important to apply secure communication techniques for both inside and outside the firewall. Secure communication provides privacy and integrity of data.

Privacy ensures that data remains private and confidential, and that it cannot be viewed by eavesdroppers armed with network-monitoring software. Privacy is usually provided by means of encryption.

Integrity ensures that data is protected from accidental or deliberate (malicious) modification while in transit. Secure communication channels must provide integrity of data. Integrity is usually provided by using Message Authentication Codes (MACs).

To provide security of communication, you can use the following technologies:

### **Secure Sockets Layer/Transport Layer Security (SSL/TLS).**

- Secure Sockets Layer (SSL) is a public key–based security protocol that comprises a set of cryptographic technologies that provides authentication, confidentiality, and data integrity. It is most commonly used to secure the channel between a browser and a Web server. However, it can also be used to secure communications to and from a database server running Microsoft SQL Server 2000.

### **Internet Protocol Security (IPSec).**

- IPSec provides a transport-level secure communication solution and can be used to secure the data sent between two computers. IPSec is a transport-layer mechanism through which you can ensure the confidentiality and integrity of TCP/IP-based communications between computers. IPSec is completely transparent to applications because encryption, integrity, and authentication services are implemented at the transport level.

In this section, we will look into communication security for SharePoint Products and Technologies, including the following topics:


- Communication with Microsoft SQL Server
- Communication between index and search servers in the SharePoint Portal Server server farm deployments
- Using firewalls to protect SharePoint sites
- Using SSL for extranet sites

## **Communication with Microsoft SQL Server**

In SharePoint Products and Technologies deployments, connections between the front-end Web server and the computer running SQL Server are not encrypted. It is recommended that you implement Secure Sockets Layer (SSL) or otherwise encrypt server-to-server communications—for example, by using IPSec.


If you decide to use SSL to secure communication with SQL Server 2000, you need to perform the following steps:

1. On a computer running SQL Server, obtain and install a server certificate.
2. The certificate authority (CA) that issued the certificate must be trusted by connecting clients. To achieve this, on the client computers, such as front-end Web servers, install the certificate of the issuing CA.
3. On the computer running SQL Server, use Server Network Utility to configure whether to force all clients to use SSL or to allow clients to choose whether or not to use SSL.

 For more information, refer to Microsoft Knowledge Base article 276553, "HOW TO: Enable SSL Encryption for SQL Server 2000 with Certificate Server" at <http://support.microsoft.com/default.aspx?scid=276553>.

If you decide to use IPsec to secure communication with SQL Server 2000, you need to perform the following steps:

1. Create an IP Security policy on the database server computer.
2. Export the IPsec policy that you have created, and copy it to the front-end server computer.
3. On both the database server and the remote server computers, assign the IPsec policy. An IPsec policy must be assigned before it becomes active.

 For more information about IPsec, refer to TechNet at <http://www.microsoft.com/technet/prodtechnol/windows2000serv/howto/ispstep.mspx>.

## Communication Between Index and Search Servers

In a server farm running SharePoint Portal Server, when indexes are propagated from an index management server to a search server, the transmission is not encrypted and therefore might not be secure. It is recommended that you implement IPsec to secure the communication between the index server and the search servers.

To use IPsec to secure the propagation of indexes, do the following:

1. Create an IP Security policy on the index management server computer.
2. Export the IPsec policy to each of the search server computers.
3. On index server and search server computers, assign the IPsec policy to activate it.

## Using Firewalls to Protect the SharePoint Sites

When a SharePoint site provides services across an extranet or is accessible from the Internet by the general public, it is essential that external access to the site occurs through a firewall. The firewall inspects all incoming and outgoing traffic, and then allows or disallows the traffic based on the preconfigured policies.

On a simple level, firewalls perform packet filtering: when traffic comes to the firewall, it compares the data in the IP header with the preconfigured rules to determine whether to allow or deny access. However, to protect SharePoint Portal Server deployments from external attacks, it is also necessary to check and verify the payload inside the HTTP header. Microsoft Internet Security and Acceleration (ISA) Server 2000 firewall is an application-layer firewall that, in addition to packet filtering, provides the ability to examine the content contained in the application-level protocols such as HTTP. Refer to Chapter 25, "Firewall Considerations for SharePoint Portal Server Deployments," for detailed information on the ISA server configuration for making your SharePoint sites available to external users without compromising the security of your internal network.

## **Using SSL for Extranet Deployments**

In the Web environment, SSL is commonly used between Web browsers and front-end Web servers to create a secure communication channel. In SharePoint Products and Technologies deployments, SSL provides a secure way of establishing an encrypted communication link with users who connect to the SharePoint sites from outside the firewall.

For a detailed discussion of SSL and instructions on how to enable it in your environment, refer to Chapter 27, “Securing an Extranet Using SSL and Certificates.”

### ***Summary***

In this chapter, we looked at the security mechanisms SharePoint Products and Technologies uses to provide secure access for users and reduce the threat of security compromise. User authentication is built on underlying technologies such as IIS and ASP.NET and uses Windows security principals, while access authorization is based on a site group membership that associates each user directly or indirectly with a permission that controls the specific actions that the user can perform. Code access security allows you to configure granular access for the SharePoint Products and Technologies application code. Communication security is vital for making sure that the data is transmitted securely both inside and outside the firewall. Because SharePoint Products and Technologies security is layered on top of the security of many underlying technologies, it is important to implement a defense-in-depth approach that addresses security across all components of your SharePoint Products and Technologies deployment.