

Module 4: Securing a Web Content Management System

Date published:

February 2009

Summary:

This paper describes the security considerations that apply to Web Content Management (WCM) solutions in Microsoft® Office SharePoint® Server 2007.

See [Web Content Management Training Modules](http://go.microsoft.com/fwlink/?LinkId=141931) (http://go.microsoft.com/fwlink/?LinkId=141931) for a complete list of the available downloads.

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.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Excel, Forefront, InfoPath, SharePoint, SQL Server, Windows, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Table of Contents

Module 4: Securing a Web Content Management System 1

Module 4 Overview 1

Objectives 1

Lesson 1: Securing Servers 1

Protecting Servers with Firewalls 1

Using Perimeter Networks 1

Important Ports 2

Server Hardening for Web Content Management 4

Domain Trust Relationships 4

File and Printer Sharing Service 4

Database Communication 4

Securing the Web.config File 5

Microsoft Security Products 6

ISA Server and Office SharePoint Technologies 6

Microsoft Forefront Security for SharePoint and Office SharePoint Technologies 6

Lesson 2: Network Security 7

Objectives 7

Using Secure Sockets Layer 7

Digital Certificates 8

SSL Sessions 8

Implementation Options 9

Using IP Security 9

IP Security Policies 10

IP Filter Lists 10

Filter Actions 10

Typical IP Security Policy 11

Service Requirements for Session State 12

Session State and Office SharePoint Server 2007 12

Security Measures and Session State 12

Secure Authentication 12

Selecting Authentication Methods 13

Supporting Multiple Authentication Methods 14

Supporting the Indexing Service 14

Locking Down Forms Pages 14

Undesirable Anonymous Access 15

The Lockdown Feature 15

Review of Module 4 15

Module 4 Overview

When you publish content to an anonymous, Internet-facing environment, you must take particular care to ensure that your servers and your network are secure. This module describes the security considerations that apply to Web Content Management (WCM) solutions in Microsoft® Office SharePoint® Server 2007.

Objectives

After completing this module, you will be able to:

* Describe techniques to secure servers in an Office SharePoint Server 2007 WCM solution ([Lesson 1](#Lesson1))
* Describe techniques to secure network communications in a WCM server farm ([Lesson 2](#Lesson2))

Lesson 1: Securing Servers

When you deploy a WCM solution, you must often isolate your production server farm both from the Internet and from your internal network. This lesson describes some of the measures you can take to protect your servers while still enabling legitimate anonymous users to access your content.

Objectives

After completing this lesson, you will be able to:

* [Plan firewall configurations for a SharePoint Server 2007 WCM deployment](#ProtectingServerswithFirewalls)
* [Describe how standard server-hardening guidelines differ for WCM solutions](#ServerHardeningforWCM)
* [Describe how you can use Microsoft security products to provide edge security, virus protection, and content filtering](#MicrosoftSecurityProducts)

Protecting Servers with Firewalls

Firewalls are devices that regulate connections between different networks, such as between the Internet and a corporate network. A properly configured firewall only permits network connections that have been explicitly allowed, based on the source and destination address, protocol, port number, and target application of a request. To protect an Internet-facing WCM solution with firewalls, you must understand the port numbers and protocols that Office SharePoint Server 2007 uses to communicate with clients and servers.

* [Using Perimeter Networks](#UsingPerimeterNetworks)
* [Important Ports](#ImportantPorts)

Using Perimeter Networks

A perimeter network (also known as demilitarized zone, DMZ, and screened subnet) sits between an organization's internal network and the Internet. The perimeter network typically contains servers such as Web servers and Mail servers that you want to expose to external users. Conceptually, a perimeter network includes two firewalls: an outer firewall between the Internet and the perimeter network, and an inner firewall between the perimeter network and the internal network. In practice, you are likely to use Microsoft Internet Security and Acceleration Server (ISA Server) or a similar product to manage the perimeter network and provide firewall functionality.

The outer firewall is configured to allow external users to connect to specific servers in the perimeter network on specific ports. For example, your outer firewall might allow connections to your Web servers on port 80 and port 443, and connections to your Mail server on port 110. Similarly, the inner firewall is configured to allow internal users to connect to specific servers in the perimeter network on specific ports. It also regulates any necessary network traffic from the perimeter network to the internal network. Together, the outer firewall and the inner firewall prevent external users from gaining access to servers in your internal network.

If you use multiple Office SharePoint Server 2007 farms for a WCM solution, only your production environment is typically exposed to external users. As such, you usually install the entire production server farm in your perimeter network. Your staging environment, together with development and test environments if you use them, are normally not exposed to external users. For this reason, you should install staging, test, and development server farms in your internal network. To deploy content from your staging environment to your production environment, you must configure your inner firewall to permit communication from the Central Administration server in your staging environment to the Central Administration server in your production environment. If you share a Shared Services Provider (SSP) across a firewall, you must configure the firewall to permit communication on various ports for different services.

Finally, you should note that the recommended server farm layouts described here for WCM solutions differ from recommended server farm layouts for other Office SharePoint Server 2007 solutions, where you are more likely to deploy Web servers in a perimeter network with Application servers and Database servers in an internal network.

Important Ports

The servers in an Office SharePoint Server 2007 server farm communicate on several different ports. If this communication occurs across a firewall, you must configure the firewall to permit communication on that particular port. The following table lists the ports that Office SharePoint Server 2007 requires for various functions.

|  |  |  |
| --- | --- | --- |
| **Function** | **From/To** | **Ports** |
| Client access | * External users to Web servers * Internal users to Web servers | * TCP port 80 * TCP port 443 (SSL) |
| Remote administration | * Terminal Services jump point to all servers | * RDP (TCP 3389) |
| Administrator access to Central Administration | * Internal users to Web server that hosts the Central Administration Web site | * Configured on installation |
| File and printer sharing service | * Web servers to Query servers (search requests) * Index servers to Query servers (index propagation) | * TCP/UDP port 445 (SMB) (recommended) or * TCP/UDP ports 137, 138, and 139 (NetBIOS) |
| Office Server Web services | * Web servers to Query servers * Web servers to Index server * Web servers to Excel Calculation Services host * Index server to Query servers * Query servers to Index server | * TCP port 56737 or * TCP port 56738 (SSL) * (configured per SSP) |
| Database communication | * All Office SharePoint servers (regardless of role) to Database servers | * TCP port 1433 * UDP port 1434 * Note: You should reassign these ports. This is described in the next section, “Server Hardening for Web Content Management.” |
| SSO service | * From any server role that hosts the single sign-on (SSO) service to the encryption key server | * TCP port 135 * Restricted high ports (for static RPC) or random high ports (for dynamic RPC) |
| Document conversions | * Web servers to document conversions services host | * TCP port 8082 (Document Conversions Launcher Service) * TCP port 8093 (Document Conversions Load Balancer Service) |
| Index crawls | * Index server to web servers (or dedicated crawl server * Index server to other content sources | * TCP port 80 * TCP port 443 (SSL) * Other content source-appropriate ports |
| Authentication and DNS | * ALL Office SharePoint servers to DC and DNS servers | * DS (TCP 445) * RPC (TCP 135) * DNS (UDP 53) * Kerberos (UDP 88) |
| Outbound Email | * Web servers to SMTP and Exchange | * SMTP (TCP 25) |
| Inbound Email (if applicable) | * SMTP to Web servers | * SMTP (TCP 25) |
| LDAP Authentication (optional) | * Web servers to LDAP hosts * Central Administration site host(s) to LDAP host(s) * Index Server to LDAP hosts (profile imports) | * LDAP (TCP 389 * LDAPS (TCP 636) |

The File and Printer Sharing Service and database communication issues are discussed in more detail in [Server Hardening for Web Content Management](#ServerHardeningforWCM).

Note: You might also need to understand additional port numbers that are used by infrastructure server roles such as Microsoft® Active Directory® directory service domain controllers. For more information, see [Plan security hardening for extranet environments](http://go.microsoft.com/fwlink/?LinkID=140059&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=140059&clcid=0x409).

Server Hardening for Web Content Management

In an Internet-facing Office SharePoint Server 2007 solution, it is particularly important to protect your servers from malicious users and content. You can substantially reduce your exposure to attack by carefully configuring network topology and firewalls, installing virus protection, and disabling unnecessary services.

Note: Your starting point for server-hardening recommendations should be the patterns and practices guidance. See [Improving Web Application Security: Threats and Countermeasures](http://go.microsoft.com/fwlink/?LinkId=140080&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=140080&clcid=0x409).

This topic contains the following topics:

* [Domain Trust Relationships](#DomainTrustRelationships)
* [File and Printer Sharing Service](#FileandPrinterSharingService)
* [Database Communication](#DatabaseCommunication)
* [Securing the Web.config File](#SecuringtheWebconfigFile)

Domain Trust Relationships

If you install your production server farm in the perimeter network and install your staging server farm in the internal network, each farm typically runs in an isolated domain with a separate domain controller. You do not need to configure a domain trust relationship between the networks to migrate content from the staging farm to the production farm. Instead, you must specify an account from the production farm domain when you create migration jobs.

However, if you want to authenticate users in the production environment by using their Windows® credentials, you must configure a one-way trust relationship in which the perimeter network trusts the internal network. If you authenticate users by using Forms authentication or Web single sign on (SSO), this does not apply.

File and Printer Sharing Service

Many Office SharePoint Server 2007 services require the protocols and ports of the File and Printer Sharing Service to provide functionality. The search service requires the File and Printer Sharing Service for crawling, indexing, and querying. Microsoft® Office Excel® Services uses the File and Printer Sharing Service to retrieve workbooks over Universal Naming Convention (UNC) paths. The Setup process uses the File and Printer Sharing Service to create databases and copy installer files.

The File and Printer Sharing Service can use either NetBIOS over TCP/IP or direct-hosted server message blocks (SMBs) to communicate. The direct-hosted SMB protocol is more secure. It is recommended that you disable NetBIOS over TCP/IP. However, if you do so, you must permit the File and Printer Sharing Service to use the direct-hosted SMB port (TCP/UDP port 445).

Database Communication

By default, a standard instance of Microsoft® SQL Server® 2005 listens for connections on TCP port 1433, and broadcasts the listening port number on UDP port 1434. A named instance of SQL Server 2005 listens for connections on a randomly assigned TCP port, and broadcasts the listening port number on UDP port 1434.

When a client computer contacts a database server, it attempts to initiate communication on port 1433. If it is unable to do so, it queries the SQL Server Resolution Service on port 1434. The SQL Server Resolution Service broadcasts the listening port number, and the client retries to initiate communication on the correct listening port number.

These standard port numbers are well-known and have been targeted by malicious users. Reassigning the listening port number in itself is not enough, as malicious software can simply query the SQL Server Resolution Service to obtain the new listening port number.

The following procedure shows you how to protect your database server more effectively.

► Protect the database server

1. Block TCP port 1433 and UDP port 1434 on the database server. These ports should also remain blocked by default on any network firewalls.
2. Reassign the listening port to a nonstandard TCP port.
3. Disable the SQL Server Resolution Service.

To enable your Web servers and application servers to contact your database servers on a nonstandard port, without using the SQL Server Resolution Service, you must configure a SQL client alias on each computer. This enables you to specify a database name and a listening port number for a specific database instance.

Securing the Web.config File

Microsoft recommends that you make the following checks and amendments to the Web.config file for each Web application in your deployment. You should only make these changes after you have run setup:

* Ensure that the customErrors attribute is set to **On**.
* In the PageParserPaths element, ensure that you do not permit compilation or scripting of database pages. PageParserPath elements are used to permit inline code in Web pages to execute.
* In the SafeMode element, ensure that the CallStack attribute is set to **false** and the AllowPageLevelTrace attribute is set to **false**.
* In the WebPartLimits element, ensure that the MaxZoneParts attribute is set to as low a value as possible. The MaxZoneParts attribute specifies the maximum permissible number of controls per Web Part zone.
* Ensure that you delete any unused SafeControl elements.
* Ensure that you delete any authorizedType elements that relate to unused workflows.

For more recommendations about server hardening, see [Plan security hardening for server roles within a server farm](http://go.microsoft.com/fwlink/?LinkId=140083&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=140083&clcid=0x409) and [Plan security hardening for extranet environments](http://go.microsoft.com/fwlink/?LinkId=140059&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=140059&clcid=0x409).

Microsoft Security Products

Microsoft provides various security products that can help you to protect your Office SharePoint Server 2007 deployment. This section describes how these products relate to WCM solutions.

|  |  |
| --- | --- |
| [ISA Server](#ISAServerandSharePointTechnologies) | Provides edge security to protect networks |
| [Microsoft® Forefront™ Security for SharePoint®](#ForefrontSecurityforSharePoint) | Provides virus protection and filtering |

ISA Server and Office SharePoint Technologies

ISA Server 2006 performs a variety of network gateway and edge security functions. ISA Server provides advanced firewall functionality. For example, you configure ISA Server with three network adapters to define and isolate an internal network, a perimeter network, and an external network (the Internet). Communication traffic between any of these networks is monitored and regulated by ISA Server. This deployment strategy is often used for WCM scenarios, to isolate Web publishing servers from both the Internet and the internal network.

ISA Server also performs several other tasks such as applying publishing rules to map public URLs to internal URLs. This is known as reverse proxy server functionality. This is particularly useful for WCM solutions in Office SharePoint Server 2007 because you are likely to define at least two zones (anonymous Internet access and authenticated internal access) for each Web application. You can combine publishing rules on ISA Server with alternate access mappings in Office SharePoint Server 2007 to provide a consistent experience for all users.

You can also relieve the burden on your Web servers by using ISA Server to cache content in some circumstances. This is known as reverse caching, when ISA Server caches content hosted on internal servers to serve requests from external users. You should only use ISA Server caching, in addition to Office SharePoint Server 2007 caching, if all the following criteria are met:

* The production environment is configured entirely for anonymous access.
* Content is largely static (changes infrequently).
* Post-cache substitution is not used. In post-cache substitution, parts of a page are cached, and then the page is reassembled before being rendered to the user.
* URLs are not modified (pages are rendered under the URL that the user requested).

Note: For more information about ISA Server, see [Forefront Edge Security](http://go.microsoft.com/fwlink/?LinkId=140261&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=140261&clcid=0x409).

Microsoft Forefront Security for SharePoint and Office SharePoint Technologies

Microsoft Forefront Security for SharePoint provides virus protection and content filtering services that are specifically tailored to Office SharePoint Server 2007 and Windows® SharePoint® Services 3.0. You can use Forefront Security for SharePoint to protect your Office SharePoint Server 2007 deployment from malicious code, undesirable content, and disclosure of confidential information.

In a WCM solution, you are less likely to be concerned about the propagation of viruses through content upload and download when compared to a collaboration solution. However, you are more likely to require measures to prevent the publication of inappropriate content, such as the inadvertent disclosure of confidential information. You can use Forefront Security for SharePoint to create keyword-based filter policies that prevent any such disclosure.

You deploy Forefront Security for SharePoint on each Web server in your server farm. If you use separate server farms for your staging and production environments, you should deploy Forefront Security for SharePoint in your staging farm to identify any policy breaches before your content is deployed to the Internet-facing production environment.

Forefront Security for SharePoint is covered in greater depth in the Advanced IT Professional Course for SharePoint Server 2007 and Windows SharePoint Services 3.0. You can also find additional information in the Office SharePoint Server Server Farm Architecture and Operations and Management white papers in [Advanced lectures and whitepapers](http://go.microsoft.com/fwlink/?LinkId=140087&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=140087&clcid=0x409).

Lesson 2: Network Security

In addition to protecting your servers, you must also protect any sensitive network traffic between your servers and between users and servers. Requirements for network security in a WCM solution differ from other Office SharePoint Server 2007 solutions because you will typically expose the WCM solution to the Internet and probably permit some level of anonymous access. This lesson describes the network security issues raised by WCM solutions and explains how you can mitigate these issues.

Objectives

After completing this lesson, you will be able to:

* [Explain how Secure Sockets Layer (SSL) encryption works](#UsingSecureSocketsLayer)
* [Describe how you can use IP Security (IPSec) to protect server-server network traffic](#UsingIPSecurity)
* [Describe how Session state affects service requirements](#ServiceRequirementsforSessionState)
* [Explain how to select authentication methods](#SecureAuthentication)
* [Describe how to lock down Forms pages](#LockingDownFormsPages)

Using Secure Sockets Layer

Many Web publishing environments have member areas, or require you to sign in to access certain resources. To prevent user credentials or sensitive materials from being intercepted, you should consider using SSL encryption to protect network traffic between clients and servers.

Always use SSL to encrypt communications with the Central Administration and SSP administration web sites — administrators enter service accounts and passwords on various pages in both of these sites, so it is important to encrypt communication that carries these credentials. Also, always use SSL for Web applications that use Forms or Basic authentication, to encrypt the credentials being passed via these methods. Keep in mind that data that is not considered sensitive in an internal network might be considered sensitive if it is published on authenticated sites to external networks: If you are exchanging sensitive data, you should consider using SSL on the Web application zone that is used to publish that data in your WCM solution.

This section contains the following topics:

[Digital Certificates](#DigitalCertificates)

[SSL Session](#SSLSessions)

[Implementation Options](#ImplementationOptions)

Digital Certificates

To enable users to connect to your WCM solution over an SSL-encrypted channel, you must install a digital certificate (X.509 certificate) in your server farm. In commercial scenarios, certificates are typically issued by a trusted third-party Certification Authority (CA) and effectively guarantee the identity of your organization to external users. Windows Server® 2003 uses the Certificate Services component to manage certificates.

A digital certificate consists of two parts: a public key and a private key. The public key is used to encrypt data, and the private key is used to decrypt data. The public key is freely distributed to Internet browsers on client machines, while the private key is retained securely on your server farm. This means that anyone can use your certificate to encrypt information, but only your Web server can decrypt it. This enables client browsers to verify that they have connected to your server farm rather than to a malicious intercept. For example, the browser could use your certificate to encrypt some random text, and the Web server can prove its identity by decrypting the text.

However, in itself the digital certificate can only provide one-way (client to server) encryption. SSL uses the digital certificate to establish a two-way encryption channel.

SSL Sessions

The Web server and the client browser use the following process to establish a two-way encryption channel.

► Establish two-way encryption channel

1. The browser uses the public key component of your digital certificate to verify the identity of your Web server.
2. The browser and the Web server establish mutually compatible encryption methods.
3. The browser sends the Web server a random secret key (symmetric key) that both parties can use to encrypt and decrypt data. The browser uses the public key component of your digital certificate to encrypt the secret key.
4. The browser and the Web server use the secret key to encrypt and exchange information.

Notice that SSL does not authenticate users. When the SSL session has been established, you must authenticate the user in the same way that you would authenticate a user for an unencrypted session, by using Windows, Forms, or Web SSO authentication.

Note: If you are using SSL in a load-balancing environment, you must configure your load-balancing solution to use sticky sessions (also known as bidirectional affinity). With sticky sessions, every request from a particular user is directed to the same Web server over the course of a session. This means that only one server needs to establish an SSL connection with the client computer. Without sticky sessions, the user can get "Underlying connection was closed" error messages if subsequent requests are processed by a different Web server.

Implementation Options

SSL is configured at the IIS Web site level. If you have established a requirement for encrypted sessions for some of the content on your WCM solution, you can deploy the solution in two different ways:

* Add the sensitive content to a separate site collection in a new Web application. Configure the IIS Web site for the new Web application to require SSL encryption.
* Add a new zone (effectively an extranet zone) to the existing Web application. Configure the IIS Web site for the new zone to require SSL encryption. Use authentication and authorization to control access to the sensitive content.

Note that if you are using SSL with host headers and IIS6, you’ll need to use wildcard certificates.

You should also be aware that SSL sessions can create a substantial processing burden on your Web servers. Avoid using SSL sessions unless there is a clear business need to encrypt client-server network traffic. If your organization uses ISA Server, you can configure ISA Server to establish and terminate SSL sessions to reduce the burden on your Web servers. ISA Server 2006 provides load-balancing functionality that can automatically configure sticky sessions for your users.

Finally, you should place authenticated sites or areas below the root site in the URL hierarchy. This will simplify your caching strategy because output caching creates separate caches for each unique security group setting.

Using IP Security

IPSec is a suite of networking protocols. In Windows® Server® 2003, IPSec is implemented by the IPSec Services service and is managed through Group Policy and firewalls, such as monitoring and filtering network traffic and restricting communication to specific ports and protocols.

However, although you use firewalls to restrict and monitor communication between separate networks, you configure IPSec to protect the communication between individual servers in a domain.

The IPSec suite includes facilities to encrypt the traffic between servers in a domain. This can help you to provide defense in depth for your server farm: If a malicious user manages to bypass your outer firewall and intercept network traffic, you nevertheless prevent that user from retrieving any user credentials or other sensitive information that can be passed between your servers.

In most circumstances, you should use SSL to encrypt client-server traffic and IPSec to encrypt server-server traffic.

Following are some terms defined in this section.

|  |  |
| --- | --- |
| [IP security policy](#IPSecurityPolicies) | A security policy that consists of IP filter lists and filter actions |
| [IP filter list](#IPFilterLists) | A set of rules that identify and classify network traffic between servers |
| [Filter action](#FilterActions) | The action that is applied to network traffic that matches the IP filter list |

IP Security Policies

Before you configure IPSec for your server farm, you must group the servers in your server farm into Active Directory Organizational Units, based on their security requirements. You can then create a new Group Policy object and associate it with an Organizational Unit. Within the Group Policy object, you create a new IPSec Policy.

An IPSec Policy consists of one or more IPSec rules. Each security rule consists of two major parts:

* An IP filter list that specifies the criteria that are used to identify particular communication types.
* A collection of filter actions that can be applied when a communication matches the filter list criteria. Although the security rule can contain many filter actions, you can only activate a single filter action at any one time.

IP Filter Lists

Each IP filter list contains one or more IP filters. An individual IP filter identifies a specific communication by specifying the following properties:

* **The source address**: This could be a specific IP address, a specific DNS name, a specific subnet, the default gateway, or various other parameters.
* **The destination address**: This is selected in the same way as the source address. You can also specify that the filter is mirrored, so that the filter identifies communication in either direction (source-destination or destination-source).
* **The protocol type**: Examples include TCP, UDP, ICMP, and any other protocol at the Internet layer of the TCP/IP model. If you select TCP or UDP, you can also specify particular source and destination ports.

Filter Actions

Each security rule can apply one filter action to communications that match the criteria specified by the filter list. A filter action has three basic types of behavior, as shown in the following table.

|  |  |
| --- | --- |
| **Filter Action Behavior** | **Details** |
| Permit | Permits all communications that match the IP filter list. |
| Block | Blocks all communications that match the IP filter list. |
| Negotiate Security | Imposes authentication and encryption constraints on all communications that match the IP filter list. |

If you set the filter action behavior to Negotiate Security, you can specify security methods that must be applied to all communications that match the IP filter list. You can select from three different security methods, as shown in the following table.

|  |  |
| --- | --- |
| **Filter Action Behavior** | **Details** |
| Integrity and encryption | All communications that match the IP filter list are hashed and signed to guarantee that they are unmodified and encrypted. |
| Integrity only | All communications that match the IP filter list are hashed and signed to guarantee that they are unmodified, but they are not encrypted. |
| Custom | Enables you to specify which cryptographic algorithms to use for integrity and encryption. |

Typical IP Security Policy

A typical IPSec Policy for an Office SharePoint Server 2007 WCM deployment might consist of two security rules. The first security rule specifies that all legitimate communication within the server farm must be encrypted, as shown in the following table.

|  |  |
| --- | --- |
| **Rule Component** | **Details** |
| IP Filter Lists | * All legitimate communication paths within the server farm * Further constrained by port numbers |
| Filter Actions | * Negotiate Security * Security method set to Integrity and Encryption |

The second security rule specifies that any communication that does not match the first security rule is blocked, as shown in the following table.

|  |  |
| --- | --- |
| **Rule Component** | **Details** |
| IP Filter Lists | * All inbound traffic |
| Filter Actions | * Block |

The IPSec Services service gives precedence to security rules according to their specificity. In this case, the second security rule is the more general; it specifies that all inbound traffic should be blocked. This provides the default behavior for the security policy. The first security rule is more specific and takes precedence over the second security rule. When the IPSec Services service identifies traffic that matches the first security rule, the second security rule is ignored and the communication is permitted and encrypted.

Service Requirements for Session State

When a user browses to a Web site, the client browser and the Web server use the Hypertext Transfer Protocol (HTTP) to exchange information. HTTP is a stateless protocol that consists of client requests and server responses. As such, the Web server treats every request as an independent request and responds accordingly. The Web server cannot track which user sent a particular request or what the user was doing beforehand.

Although this behavior works well for basic Web sites, many Web applications must track users and retain a history of their actions until they have completed a particular task. For example, if a user is populating a Web page with information, the Web server must retain that information between postbacks. ASP.NET Web applications use Session state to store variable values for the duration of each user's session. A particular session starts when the user browses to the Web site and ends when the user browses away from the site, closes the browser window, or the session time limit expires.

Session State and Office SharePoint Server 2007

Office SharePoint Server 2007 includes a Session State Service that uses the underlying ASP.NET Session state implementation. The Session State Service for a particular Web application is operated by the primary SSP. Office SharePoint Server 2007 automatically enables session state when you create an SSP. If a Web application does not have an SSP, you cannot enable Session state.

Many Office SharePoint Server 2007 services rely on Session state. If you use multiple load-balanced Web servers, the load balancer allocates user sessions to a specific Web server to ensure that the user gets a consistent experience for the duration of their session. Microsoft® Office InfoPath® 2007 Forms Services, Office Excel Services, and Microsoft Office Project Server all rely on Session state to provide interactivity.

Security Measures and Session State

Web server-hardening guidelines recommend that you disable the ASP.NET State service and the View State service if these are not required. If you use any services or components that require Session state (such as Office Project Server 2007 and Microsoft® Office Forms Server 2007), do not disable the ASP.NET State service. In addition, if you use Office InfoPath Forms Services, do not disable the View State service.

Secure Authentication

When you plan authentication for an Office SharePoint Server 2007 WCM deployment, you must choose the most appropriate authentication method for your existing infrastructure and the planned reach of your solution. There are three principal types of authentication that you can use with Office SharePoint Server 2007:

* **Integrated Windows authentication (IWA)** uses your existing Active Directory infrastructure to authenticate users. This can be either NTLM authentication or Kerberos authentication, depending on how your infrastructure is configured.
* **ASP.NET forms authentication** (also known as forms-based authentication) uses the membership providers and role managers provided by ASP.NET. This enables you to use custom or external authentication systems to authenticate users.
* **Web SSO authentication** enables users who are managed by an external Active Directory infrastructure to access your site without providing credentials when they are authenticated against their own Active Directory credentials.

Note: Web SSO authentication is unrelated to the SharePoint SSO service.

The implementation details for each of these authentication types are covered in the Advanced IT Professional Course for Microsoft Office SharePoint Server 2007 and Windows SharePoint Services 3.0, Module 3, "Securing Microsoft SharePoint Products and Technologies Server Farms."

This section focuses on how to select the most appropriate authentication methods for your WCM environment, as shown in the following table.

|  |  |
| --- | --- |
| **Aspect** | **Details** |
| [Selecting authentication methods](#SelectingAuthenticationMethods) | * Implement IWA to use your Active Directory credentials. * Implement ASP.NET Forms to use a custom solution. * Implement Web SSO to use external Active Directory credentials |
| [Multiple authentication methods](#SupportingMultipleAuthenticationMethods) | One authentication method for each Web application zone |
| [Indexing Service](#SupportingtheIndexingService) | Web application must include an IWA zone to support the indexing service |

Selecting Authentication Methods

The following table shows when each authentication type might be the appropriate choice for your organization.

|  |  |
| --- | --- |
| **Authentication Type** | **When to Use** |
| Integrated Windows authentication | Use IWA if you manage your user credentials in Active Directory. |
| ASP.NET Forms | Use ASP.NET forms authentication if you use a custom authentication solution to manage your user credentials, or if you want to create a simple database to manage credentials. |
| Web SSO | Use Web SSO authentication if you manage your user credentials in Active Directory, and you need to extend access to your site to a partner organization that also uses Active Directory to manage user credentials. To use Web SSO, each organization must participate in a federated authentication system, such as Active Directory Federation Services (AD FS). |

In a WCM environment, you are likely to require some degree of anonymous access. You can choose to permit anonymous access with any of these authentication methods. You must first configure the Web application to permit anonymous access, and then configure each site collection to permit anonymous access as required.

If you use IWA, you can also permit Basic authentication as a secondary authentication method. This can be useful if you need to authenticate employees against their Active Directory credentials when they access the site remotely. IIS will first attempt to authenticate the user by using IWA. If this fails, the user is prompted to enter credentials and IIS uses Basic authentication to validate the credentials against Active Directory. However, you must only permit Basic authentication over a secure channel such as SSL because credentials are sent in clear text.

Supporting Multiple Authentication Methods

In many circumstances, you might want to allow access to your WCM solution through more than one authentication method. For example, you might want to authenticate your internal users through IWA, but authenticate users from outside your organization through FBA. Alternatively, you might want to enable users to access most areas of your site anonymously over HTTP, but sign in over HTTPS to access sensitive content. To use multiple authentication methods, you extend your Office SharePoint Web application to additional zones.

Each IIS Web site has a single authentication method associated with it, and can use either HTTP or HTTPS. When you first create an Office SharePoint Web application, there is a one-to-one mapping between the Office SharePoint Web application and the IIS Web site. If you extend your Office SharePoint Web application to additional zones, each zone corresponds to an IIS Web site. Each zone also corresponds to a base URL, so you can create multiple access paths to the same content.

Supporting the Indexing Service

The indexing service can only use IWA to access content. Even if you authenticate all your users through forms-based authentication or Web SSO, you must still configure a Web application zone to use IWA so that the indexing service can function properly.

Note: This section refers to the release-to-manufacturing (RTM) version of Office SharePoint Server 2007. Microsoft® Search Server 2008 and Office SharePoint Server 2007 SP1 and later can log on to crawl content with forms-based authentication.

However, when crawling a forms-based authentication site, the indexer does a simple crawl of the content only, and does not capture security information or the kind of rich metadata that the crawler can gather when using the native SharePoint protocol handler. For those reasons, whether or not you have applied Service Pack 1, it is recommended that you crawl SharePoint sites protected by forms authentication by using the native SharePoint protocol handler. See more details on this subject at [Forms Authentication in SharePoint Products and Technologies (Part 3): Forms Authentication vs. Windows Authentication](http://go.microsoft.com/fwlink/?LinkId=140095&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=140095&clcid=0x409 ).

Locking Down Forms Pages

Office SharePoint Server 2007 automatically grants the Limited Access permission set to users to enable them to access specific lists, document libraries, list items, folders, or documents. The Limited Access permission set is granted to ensure that users can get to the resources that you have explicitly granted them access to. For example, if you grant a user read permissions on a specific document, Office SharePoint Server 2007 grants that user the following permissions through the Limited Access permission set:

* Minimal access to the folder that contains the document
* Minimal access to the document library that contains the folder
* Minimal access to the site that contains the document library

Without these additional permissions, the user cannot access the document to which you have granted them read permissions.

Undesirable Anonymous Access

In a WCM environment, you are likely to grant anonymous users access to at least some of your content. As a result, Office SharePoint Server 2007 applies the Limited Access permission set as necessary to ensure that anonymous users can reach those resources to which you have granted them access. However, the Limited Access permission set can have the undesirable secondary effect of granting anonymous users access to Office SharePoint Forms pages. For example, anonymous users can inadvertently be granted access to the http://<server>/Pages/Forms/AllItems.aspx page. This contains the Pages library that stores all the pages in a publishing site.

The Lockdown Feature

You cannot modify the permissions in the Limited Access permission set directly. However, Office SharePoint Server 2007 includes a feature that you can use to remove undesirable permissions. The ViewFormPagesLockdown feature (usually referred to as the Lockdown feature) removes the following permissions from the Limited Access permission set:

* The View Application Pages permission
* The Use Remote Interfaces permission

To activate the Lockdown feature, use the following **stsadm** command.

stsadm –o activatefeature –url <site URL> -filename ViewFormPagesLockdown\feature.xml

The Lockdown feature is activated by default on sites based on the Publishing Portal template because publishing sites are far more likely to require anonymous access. If you are using an alternative site template, you must manually activate the feature.

If you have enabled anonymous access to your site before you run the Lockdown feature, you must disable and reenable anonymous access after running the Lockdown feature before the changes will take effect.

Review of Module 4

* Securing Servers
* Network Security

References

The following videos provide supplemental information to these modules. There is no one-to-one correspondence between the modules and the videos:

* [Video 1](http://go.microsoft.com/fwlink/?LinkId=140097&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=140097&clcid=0x409)
* [Video 2](http://officecpub/Teams/itpro/Documents/White%20paper%20library/WCM%20modules/Video%202) (http://go.microsoft.com/fwlink/?LinkID=140063&clcid=0x409)
* [Video 3](http://officecpub/Teams/itpro/Documents/White%20paper%20library/WCM%20modules/Video%203) (http://go.microsoft.com/fwlink/?LinkID=140068&clcid=0x409)
* [Video 4](http://officecpub/Teams/itpro/Documents/White%20paper%20library/WCM%20modules/Video%204) (http://go.microsoft.com/fwlink/?LinkId=140101&clcid=0x409)