Chapter 7

MCTS/MCITP Exam 649

Configuring Web Infrastructure Services

Exam objectives in this chapter:

- **Installing and Configuring FTP Publishing Services**
- **Installing and Configuring SMTP Services**

Exam objectives review:

- ☑ **Summary of Exam Objectives**
- ☑ **Exam Objectives Fast Track**
- ☑ **Exam Objectives Frequently Asked Questions**
- ☑ **Self Test**
- ☑ **Self Test Quick Answer Key**

Introduction

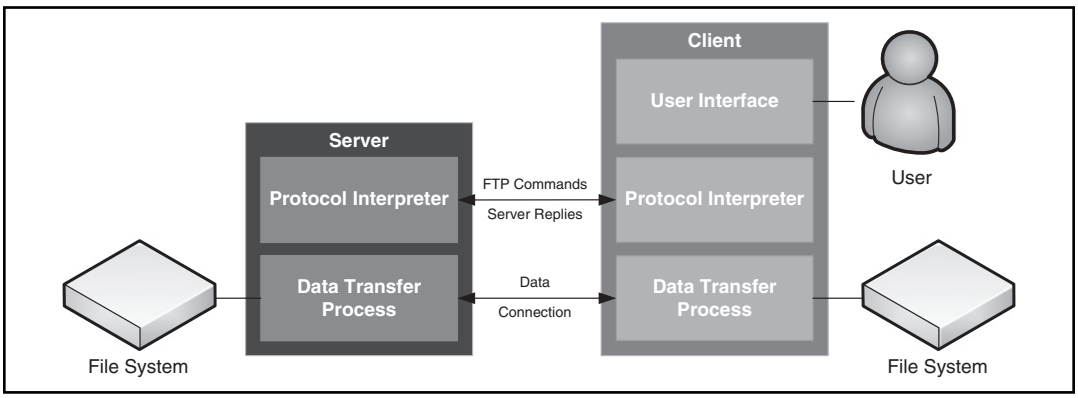
It's easy to think of Internet Information Server (IIS) as a mechanism for hosting Web sites or Web applications. However, IIS provides several optional components that can either be used by themselves, or as a complement to an existing site. One such component is the File Transfer Publishing Service (FTP). FTP provides a mechanism for allowing users to upload and download files from your Web server.

Another optional component is the Simple Message Transfer Protocol (SMTP) service. You can use the SMTP service to turn your IIS server into an e-mail server, although the capabilities provided by the SMTP service are very crude when you compare them to those found in a full-blown mail server product, such as Microsoft Exchange. In this chapter, you will learn how to deploy, configure, and secure the FTP and the SMTP services.

Installing and Configuring FTP Publishing Services

File transfer services based on the File Transfer Protocol (FTP) have been around since 1971. As a protocol it has become a standard method for transferring files between remote systems running on various operating systems (see Figure 7.1). The protocol and surrounding services were designed to give the user a simple interface while handling the complexities of the differences among file systems under the covers. In addition to FTP you can use other protocols such as HTTP, WebDAV (based on HTTP), BITS, SMB/CIFS, and others. FTP delivers advantages when handling data exchange among remote systems and those with disparate system architectures.

Figure 7.1 FTP Service Model as Outlined in RFC 959



When you connect to an FTP server a control connection is established between the client and server's protocol interpreter. This process typically occurs on port 21 using TCP. Over this control connection the client sends commands and receives replies from the server acknowledging the commands in a fashion similar to a Telnet session. When a data transfer is requested, a data connection is established between the client and server. At this layer all of the translation occurs between the two file systems. Data transfer happens using either active or passive transfer modes. Each mode has a different method for establishing the data connection. In the active mode the server establishes the data connection with the client using a random TCP port 1024 and higher. In passive mode the client establishes the data connection with the server using a random TCP port 1024 and higher. For most security professionals the challenge of opening up ports 1024 and higher on either the client or the server is perplexing. Many firewalls deal with this scenario by listening to the control connection for the PORT command and dynamically opening the port needed to establish the data connection.

In 1997 an extension was proposed in the form of RFC 2228. This extension deals with the fact that FTP as defined back in 1971 uses an unencrypted control and data connection. Prior to RFC 2228 authentication credentials and files were transmitted without any privacy controls. The RFC describes the use of SSL to secure the control and data channels to address this problem and is known as FTPS. This release of IIS ships the FTP Publishing Service with support for SSL encryption. This provides a viable alternative to the recommendations for using WebDAV over HTTPS in past releases for secure file transfer.

Exam Warning

There is another variation of secure FTP transfer—SSH File Transfer Protocol (SFTP). This binary protocol based on RFC 4253 is not compatible with FTPS clients and servers. It does benefit from using a single connection as opposed to the split control and data connections; however it presents challenges such as the management of SSH keys and the changing standards and implementations.

In addition to security, this release also adds support for Unicode characters and IPv6 addressing, and taps into the rich architecture of IIS as part of a major rewrite. The tight integration allows you to leverage custom authentication modules, rich logging and tracing capabilities, and integration with the Web server for publishing scenarios.

Installing the FTP Publishing Service

With the amount of work undertaken by the IIS product group, the major enhancements to the FTP Publishing Service did not make it into this release. Microsoft shipped the IIS 6 FTP Publishing Service with some compatibility fixes in its place. To gain access to all of the new FTP Publishing Service features you will need to download the out-of-band release from the IIS Download Center (www.iis.net/downloads).

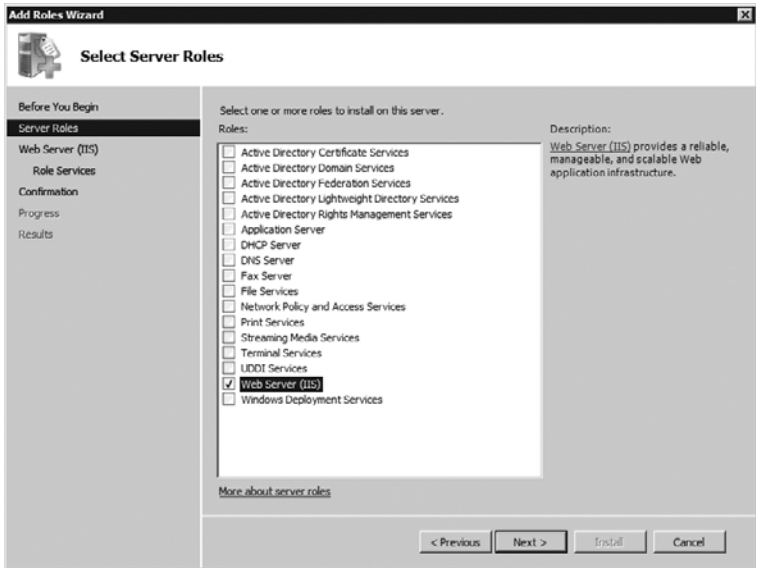
The Web release is a full installation; however it does require that the Web Server (IIS) role be installed, as it integrates in with the IIS Management functionality. If you have previously installed the Web Server role with the FTP Publishing Service you will need to uninstall it before using the Web release.

EXERCISE 7.1

Installing FTP Server

1. From the Start Menu select **Server Manager.**
2. In Server Manager, scroll the right-hand pane to the **Roles Summary** section and click **Add Roles.**
3. In the Add Roles Wizard on the Before You Begin page, click **Next**.
4. On the Select Server Roles page, select the **Web Server (IIS)** role and click **Next** (see Figure 7.2).

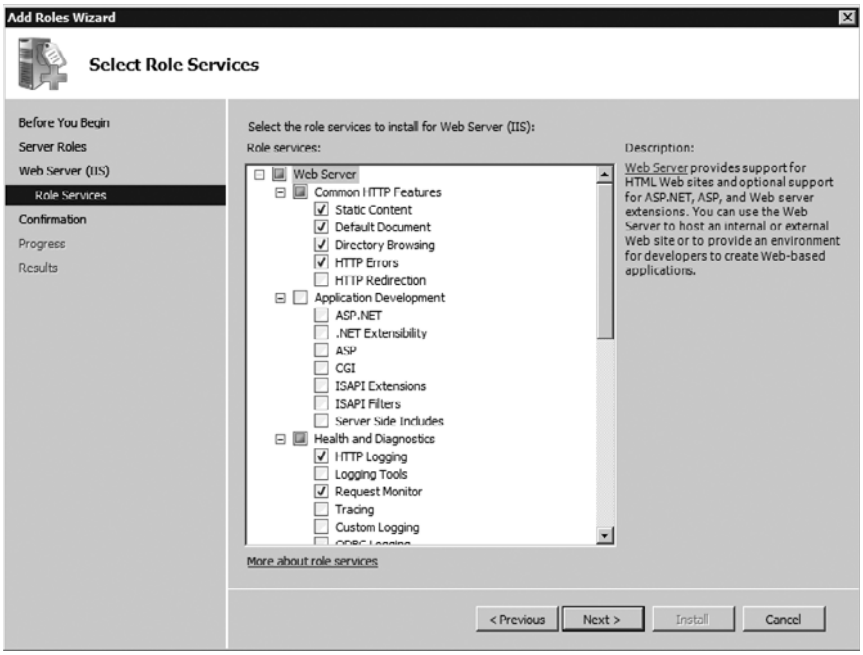
Figure 7.2 Select Server Roles Page



5. The Web Server (IIS) page gives you a brief description of the role along with some important notes and links to more information on the role (see Figure 7.3). Click **Next.**

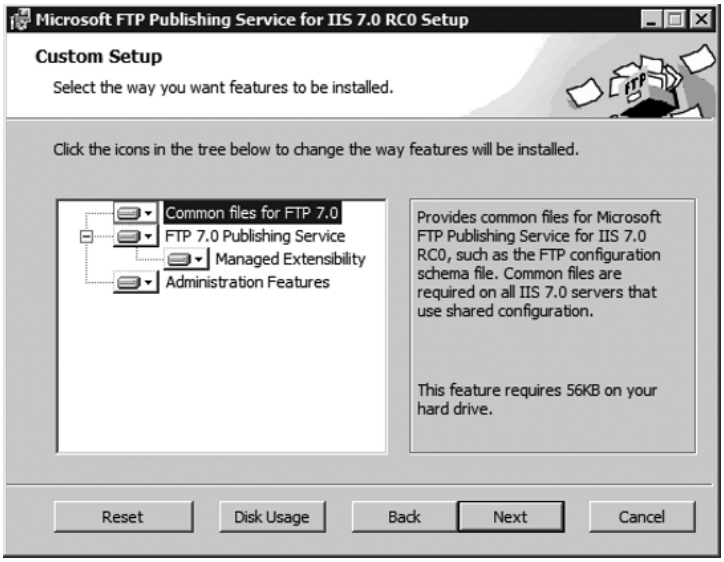
   If this is your first time setting up the Web Server (IIS) role, you should read these notes, as they cover common issues that you will encounter.

Figure 7.3 Select Web Server (IIS) Role Services Page



6. On the Role Services page you are prompted to install several groups of services to the role; leave the default values for the purposes of the upcoming exercises, and click **Next.**
7. On the Confirmation page review your choices and click **Install.**
8. On the Results page, review the success or failure of the installation and click **Close.**
9. Double-click the **FTP Server installation package**, follow the prompts for the update process to acknowledge the package, then read and accept the license agreement.
10. On the Custom Setup page, accept the defaults and click **Next** (see Figure 7.4).

Figure 7.4 Custom Setup Page



11. On the Ready to Install page click **Install.**
12. On the Completed page click **Finish.** Figure 7.5 shows the IIS Manager with the FTP server installed.

Figure 7.5 IIS Manager with the FTP Server Installed

With the installation complete you will see the Web Server role appear in Server Manager. From here you can get an overview of related event log entries, Windows services, and the Role Services you have chosen to install. In addition the Resources and Support section gives you at-your-fingertips access to resources that go in-depth on common issues and best practices to consider. The FTP Server will not appear in Server Manager. You will administer the FTP server through the IIS Manager.

Server Core installations of Windows Server 2008 allow you to install FTP Services in its entirety. The only functionality that will not be available is the graphical administrative interface and managed authentication modules.

EXERCISE 7.2

INSTALLING THE FTP SERVER ON SERVER CORE

1. Execute the following command to install the Web Server (IIS) role and the basic set of the role on a Server Core installation:

```
Start /W PkgMgr /IU:IIS-WebServerRole;IIS-WebServer;IIS-
CommonHttpFeatures;IIS-StaticContent;IIS-DefaultDocument;IIS-
DirectoryBrowsing;IIS-HttpErrors;IIS-HealthAndDiagnostics;IIS-
HttpLogging;IIS-RequestMonitor;IIS-Security;IIS-RequestFiltering; IIS-
Performance;IIS-HttpCompressionStatic;IIS-WebServerManagementTools;IIS-
IIS6ManagementCompatibility;IIS-Metabase;WAS-WindowsActivationService;WAS-
ProcessModel
```

2. Execute the following command to start installation of the FTP Server, follow the prompts for the update process to acknowledge the package, and read and accept the license agreement:

```
MSIEXEC /I FTP7_X86.msi
```

3. On the Custom Setup page, accept the defaults and click **Next.**
4. On the Ready to Install page click **Install.**
5. On the Completed page click **Finish.**
6. If you have enabled Windows Firewall and intend on using only non-secure FTP connections you will need to enable communication using the following commands:

```
NetSh AdvFirewall Set Global StatefulFTP Enable

NetSh AdvFirewall Firewall Add Rule Name="File Transfer Protocol (In)" Dir=In
Action=Allow Program="C:\WINDOWS\SYSTEM32\SvcHost.exe"
Protocol=TCP Service=ftpsvc
```

7. If you have enabled Windows Firewall and intend on using secure FTP (FTPS) connections you will need to disable stateful FTP inspection:

```
NetSh AdvFirewall Set Global StatefulFTP Disable
```

8. If you have enabled Windows Firewall and intend on using passive FTP connections, enable the FTP Publishing Service to communicate outwards as well:

```
NetSh AdvFirewall Firewall Add Rule Name="File Transfer Protocol (Out)"
Dir=Out Action=Allow Program="C:\WINDOWS\SYSTEM32\SvcHost.exe"
Protocol=TCP Service=ftpsvc
```

9. If you have enabled Windows Firewall on your server you will need to add the following exceptions:

   Remote Administration Service Exception

```
NetSh Firewall Set Service Type=RemoteAdmin Mode=Enable
```

   Windows Management Instrumentation Exception

```
NetSh AdvFirewall Firewall Set Rule Group="Windows Management
Instrumentation (WMI)" New Enable=Yes
```

   Lockdown the AHAdmin DCOM Endpoint to Port 49494

```
Reg Add "HKCR\AppId\{9FA5C497-F46D-447F-8011-05D03D7D7DDC}" /v
Endpoints /t REG_MULTI_SZ /d "ncacn_ip_tcp,0,49494"
```

   Remote Web Server Management Exception

```
NetSh AdvFirewall Firewall Add Rule Name="Remote Web Server Management
(RPC)" Dir=In Action=Allow
Program="C:\WINDOWS\SYSTEM32\dllhost.exe" Protocol=TCP LocalPort=49494

NetSh AdvFirewall Firewall Add Rule Name="Remote Web Server Management
(RPC-EPMap)" Dir=In Action=Allow
Program="C:\Windows\system32\svchost.exe" Service=RPCSS Protocol=TCP
LocalPort=RPC-EPMap
```

   If your security policy requires a more strict security setting you can use port exceptions on all or specific interfaces.

10. If you want to use Windows Remote Shell you will need to enable it:

```
WinRM QuickConfig
```

A word of warning—the graphical tools cannot connect to a Server Core installation. This is because the graphical tools have a dependency on the IIS Management Service which is built on the .NET Framework and cannot be run on Server Core because of that. There are a few ways to remotely administer IIS on Server Core:

- **Command-line Tools** Using WinRS you can make calls to AppCmd.exe. Note that WinRM does not allow for interact sessions, instead outputting the results of your command.

```
WinRS.exe -Remote:FTPSERVER %SYSTEMROOT%\SYSTEM32\INETSRV\AppCmd.exe
LIST SITE
```

TEST DAY TIP

AppCmd uses a verb-noun combination. Open Command Prompt, type in AppCmd /? and get to know the list of objects which you can take an action upon. The verb list will generally follow a common sense approach (e.g., you Create Backup, not Add Backup).

- **Windows Management Instrumentation** Scripting, programming languages, Windows PowerShell, WMIC, WinRM, and WinRS can all administer IIS on Server Core through WMI.

```
WMIC.exe /Output:Sites.txt /Node:FTPSERVER
/Namespace:\root\WebAdministration Path Site Get
```

- **COM and .NET Programming Interfaces** In addition to WMI you can use the Microsoft.ApplicationHost.AdminManager DCOM object in VBScript/JScript or the Microsoft.Web.Administration assembly through Windows PowerShell scripts and .NET applications.

```
[Reflection.Assembly]::LoadFrom("C:\WINDOWS\SYSTEM32\inetsrv\Microsoft.
Web.Administration.dll");
$WebServer =
[Microsoft.Web.Administration.ServerManager]::OpenRemote("FTPSERVER");
$WebServer.Sites | Format-Table Id, Name;
```

With our server setup, you can now configure your server's features to fit your deployment scenario's needs. If you need to uninstall the FTP Publishing Service make sure that you remove it before removing the Web Server role. The following sections will take you through basic configuration steps for each of the functional areas.

EXAM WARNING

Know the differences between Server Core and full installations of Windows Server 2008 with Internet Information Services. There is a small subset of features that are not available on Server Core and they happen to be fairly important in the Microsoft Web application eco-system.

Provisioning FTP Sites

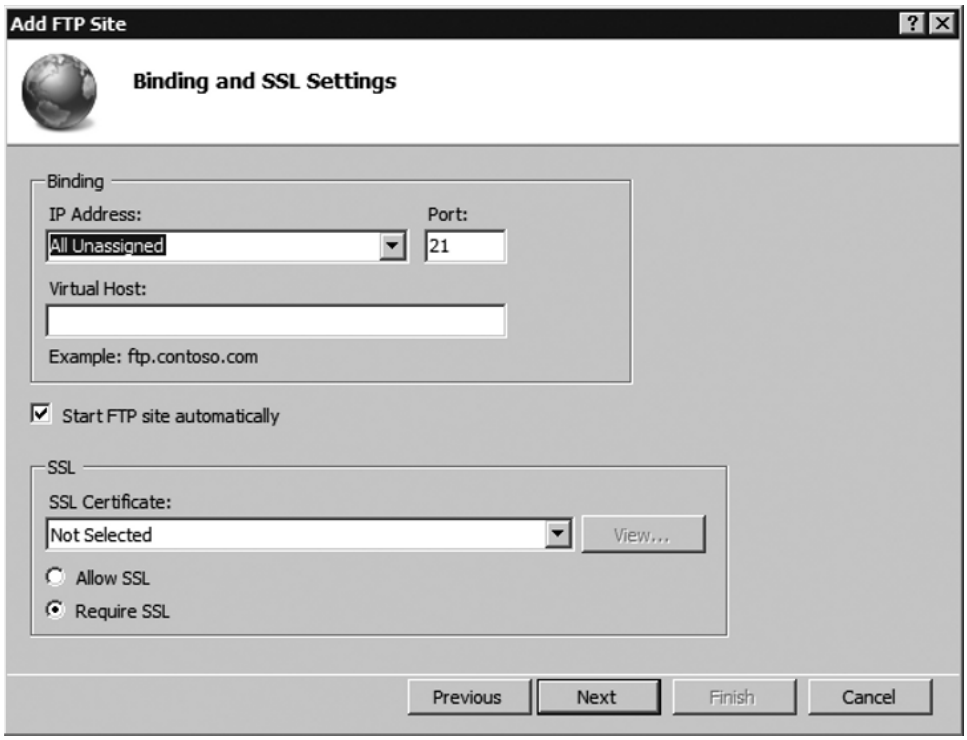
With the FTP Server installed the first step is to provision a new FTP site. You can setup independent FTP sites or bind them with a Web site on the server in this release. The latter is particularly useful in shared hosting environments to provide access to hosted sites.

EXERCISE 7.3

CREATING AN FTP SITE

1. Open **Control Panel** and under System and Maintenance | Administration Tools, double-click the **Internet Information Services (IIS) Manager** shortcut.
2. In the Internet Information Services (IIS) Manager management console, expand the server node in the left-hand pane, right-click **Sites**, and select **Add FTP Site.**
3. In the **Add FTP Site** dialog, provide a descriptive **FTP Site Name** and a **Physical Path** to the content and click **Next.**
4. On the Binding and SSL Settings page, select an **IP Address** and optionally an **SSL certificate** and click **Next** (see Figure 7.6).

Figure 7.6 Binding and SSL Settings Page



New & Noteworthy…

Host Headers and FTP

The ability to support virtual hosts is new to IIS 7. If you have used FTP in the past you may be asking yourself how exactly this works. It's a great question and one that deserves some investigation. FTP traditionally has worked without any reliance on DNS for resolution. You could just as easily FTP into an IP address as you could a host name. With this release of IIS the product group implemented two methods for supporting FTP virtual hosts: one is a band-aid solution, and another is part of a draft proposal from the Internet Engineering Task Force.

Continued

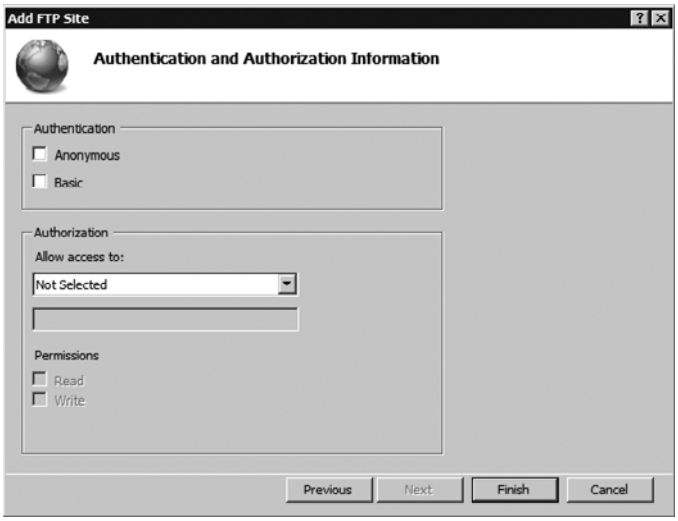
The band-aid approach is to prefix the username with the host name and a pipe symbol. The syntax for <hostname>|<username> means that if you want to login to the ftp.contoso.com virtual host as jsmith you would use ftp.contoso.com|jsmith as your username. This will tell the FTP server that the user is being authenticated in the context of the ftp.contoso.com virtual host. This approach allows you to use your favorite FTP client without worrying if it will support the proposed extensions.

The proposed draft outlines the addition of a new HOST command to be used by FTP clients and servers. Upon the connection to a site the FTP client sends a FEAT command to determine if the server supports the HOST command. If it does then it will send a HOST <hostname> command before the USER and PASS commands to authenticate the connection. The HOST command provides the necessary information for the server to determine which virtual host to connect to.

5. On the Authentication and Authorization Information page, select the **Authentication** module you want to use and the default site **Authorization** rules, and click **Finish** (see Figure 7.7).

   Unlike previous versions there is no site-wide Read / Write authorization. In this release you define a set of authorization rules that are applied to all users, all anonymous users, or a specific group of users or roles.

Figure 7.7 Authentication and Authorization Information Page



In addition to creating a standalone FTP site you can also enable an existing Web site with FTP access. This will allow users to work with their site content using the FTP protocol while keeping the configuration information tied to the Web site.

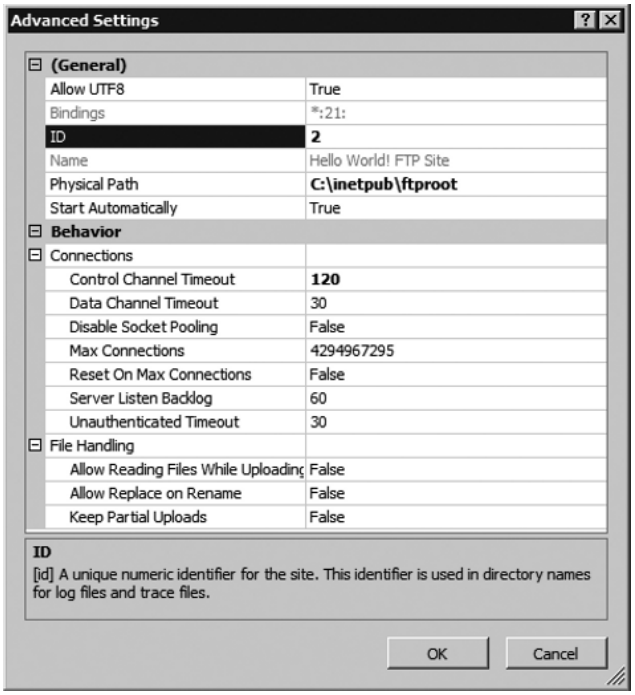
EXERCISE 7.4

CREATING A WEB SITE-BOUND FTP SITE

1. Open **Control Panel** and under System and Maintenance | Administration Tools double-click the **Internet Information Services (IIS) Manager** shortcut.
2. In the Internet Information Services (IIS) Manager management console, expand the server and sites node in the left-hand pane, right-click the Web site you wish to publish, and select **Add FTP Publishing.**
3. At the Add FTP Site Publishing screen, select an **IP Address** and optionally an **SSL certificate** and click **Next.**
4. On the Authentication and Authorization Information page, select the **Authentication** module you want to use and the default site **Authorization** rules, and click **Finish.**

With the site created there are a set of advanced settings available to help you fine tune the behavior of your FTP Site. They can be found by selecting the site from the left-hand pane, and in the right-hand Actions pane under Manage FTP site clicking **Advanced Settings** (see Figure 7.8).

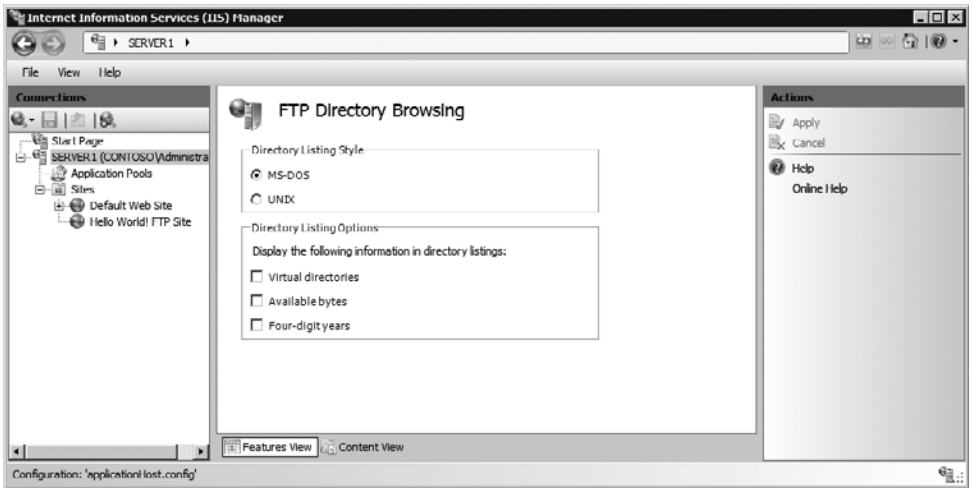
Figure 7.8 FTP Site Advanced Settings



Directory Browsing

When using the FTP service clients will often browse the various folders to locate the content that they want to retrieve. You have the option of configuring several options that will affect how the items within a folder are listed, as shown in Figure 7.9.

Figure 7.9 FTP Directory Browsing Module Configuration



The first option group is a style preference between MS-DOS and UNIX directory listings:

- Listing 7.1 MS-DOS Directory Listings

```
02-01-08 08:33PM     0 default.txt
11-02-06 04:39AM     15821312 imageres.dll
```

- Listing 7.2 UNIX Directory Listings

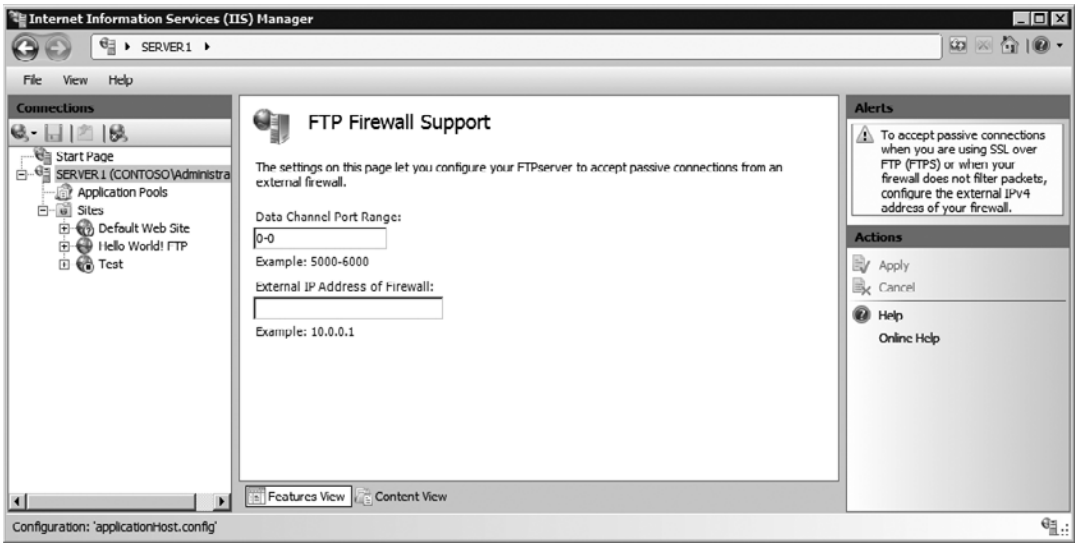
```
-rwxrwxrwx 1 owner group             0 Feb     1     20:33     default.txt
-rwxrwxrwx 1 owner group      15821312 Nov     2      2006     imageres.dll
```

The second option group focuses on the information included within the directory listings. The first option enables or disables showing virtual directories in the listings. In previous releases this was disabled by default, creating the effect of "hidden" folders. With the industry shying away from the security-by-obscurity approach this option was exposed to give you the choice depending on your business needs. The second option determines if the remaining bytes are reflected in the directory listings. Typically this will show the remaining bytes left on the disk; however, if a folder-level quota has been enabled then it will reflect the remaining bytes based on the quota. The final option determines if the last modified date should reflect a two or four digit year.

Firewall Support

The Firewall Support feature allows you to facilitate passive connections to the FTP server when it is behind a firewall (see Figure 7.10). When the FTP server provides a port number for the client to establish a data connection, the IP address is embedded within the response. This feature allows you to both limit the port range and specify the appropriate external IP address. Once this feature is configured you will need to forward the specified port range from your firewall.

Figure 7.10 FTP Firewall Support Module Configuration



Configuring & Implementing…

Active versus Passive Mode

The key difference between active and passive FTP mode is the designation of who opens the port for the data connection. In active mode the client is responsible for opening the port. In passive mode it is the server which is responsible. In most deployments you will see passive mode as the preferred method because it represents the least amount of configuration and confusion across the spectrum of users that you will service. To enforce an even more secure approach look to add Windows Firewall with Advanced Security to your deployment using the service filtering options that ship with Windows Server 2008 to lock it down further to the FtpSvc service identifier.

Messages

When FTP sessions are established, authenticated, ended, or denied connection you can include a message for the user. The Messages feature gives you a chance to

configure the default message at the server and specific site messages as shown in Figure 7.11. The first option group allows you to suppress the FTP service banner, enable the use of variables in the message, and show detailed error messages when connecting from the local machine. The variables available include:

- **%BytesReceived%** Total number of bytes sent to the client in the current session
- **%BytesSent%** Total number of bytes received from the client in the current session
- **%SessionID%** Unique identifier for the current session
- **%SiteName%** Site Name for the FTP Site being accessed
- **%UserName%** Username of the currently logged in user

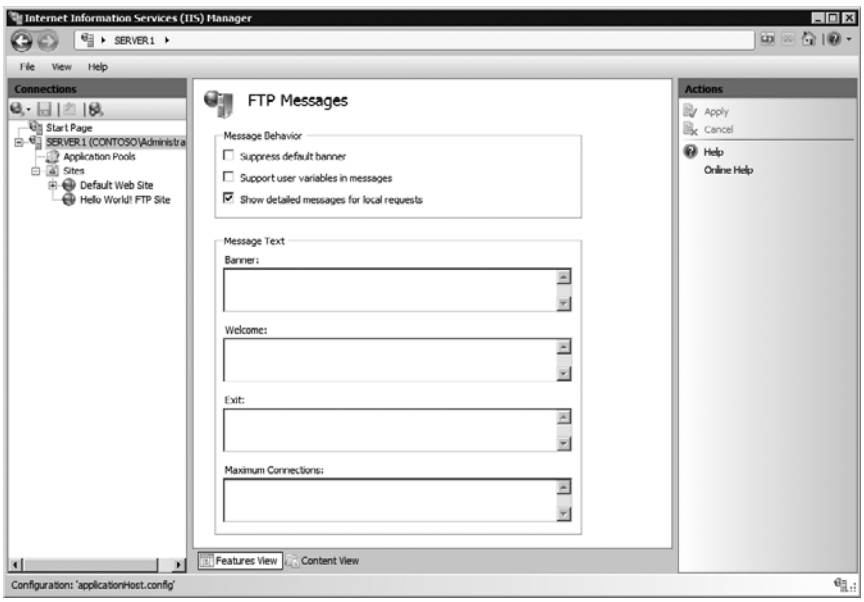
The following is an example of the variables in action:

```
Thank you for visiting %SiteName%, during your session %SessionID% we
sent %BytesReceived% bytes to you and we received %BytesSent% from you.
We look forward to seeing you again %UserName%!
```

The preceding message would generate output similar to this:

```
Thank you for visiting Hello World! FTP Site, during your session 1 we
sent 5,729 bytes to you and we received 5,828,640 from you. We look
forward to seeing you again CONTOSO\Colin!
```

Figure 7.11 FTP Messages Module Configuration



Virtual Directories

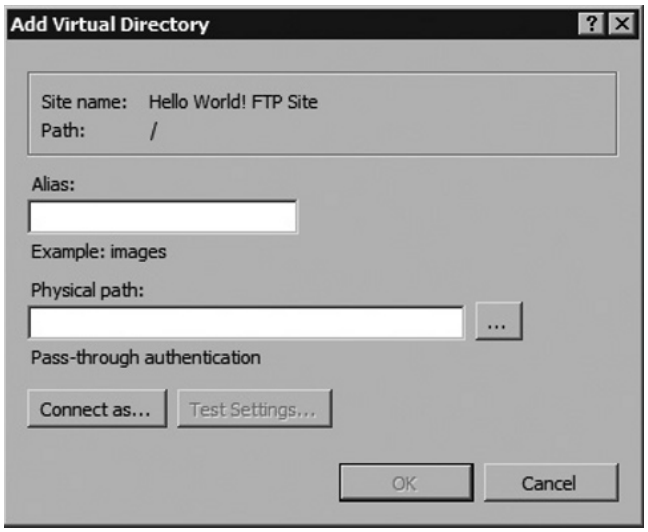
With FTP sites being used for more than managing Web content, it was quite common to see virtual directories being used to link to different folders within the system. A virtual directory works by creating a reference in the site configuration to where the content resides. The FTP service will parse the link and allow users to navigate to the folders as if they were another regular folder within the structure.

EXERCISE 7.5

Creating a Virtual Directory

1. Open **Control Panel** and under System and Maintenance | Administration Tools double-click the **Internet Information Services (IIS) Manager** shortcut.
2. In the Internet Information Services (IIS) Manager management console, expand the server and sites nodes in the left-hand pane, right-click your FTP site, and select **Add Virtual Directory.**
3. In the **Add Virtual Directory** dialog, provide the **Alias** of the virtual directory to be used by requests and a **Physical Path** to the content, and click **OK** (see Figure 7.12).

Figure 7.12 Add Virtual Directory Dialog



Application Pools

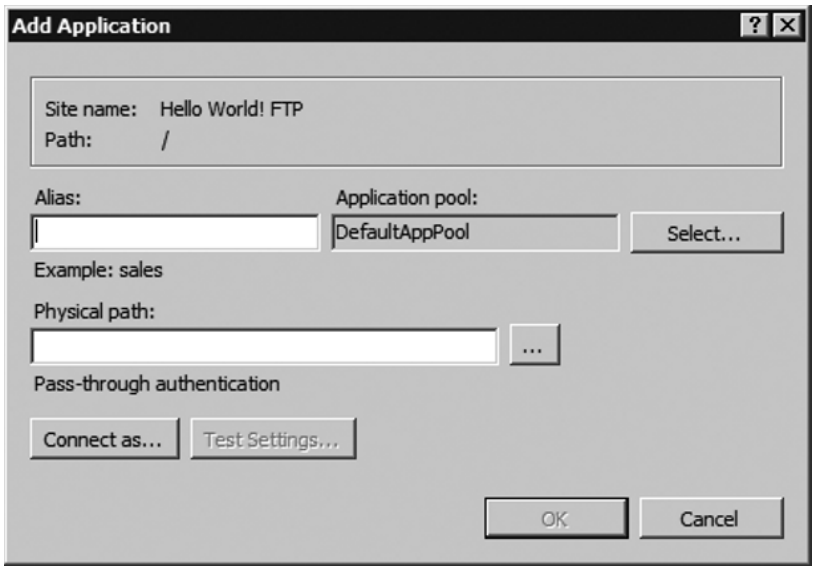
With the changes in architecture in this release, FTP sites have been shifted to use application pools for processing requests. This allows you to separate out the sites into individual worker processes and control their process identity and resource utilization as you would with a Web site.

EXERCISE 7.6

Converting a Folder to an Application

1. Open **Control Panel** and under System and Maintenance | Administration Tools double-click the **Internet Information Services (IIS) Manager** shortcut.
2. In the Internet Information Services (IIS) Manager management console, expand the server and sites nodes in the left-hand pane, right-click a folder within a FTP site, and select **Convert to Application.**
3. In the **Add Application** dialog select the application pool you want your application to run under, if desired set a content access identity, and click **OK** (see Figure 7.13).

Figure 7.13 Add Application Dialog



Securing Your FTP Site

Protecting your FTP site may require one or more tactics to ensure that the content is only accessed by authorized users:

- **Transport Security** Focused on privacy of data being transmitted between the user and the server
- **Authentication** Provides a method for determining the user's identity
- **Authorization** Evaluates a set of rules to determine if the user is allowed to make the request

This section will take you further into each tactic and the details behind them. The most notable changes in these sections for this release are the support of SSL and the ability to use custom authentication modules.

Transport Security

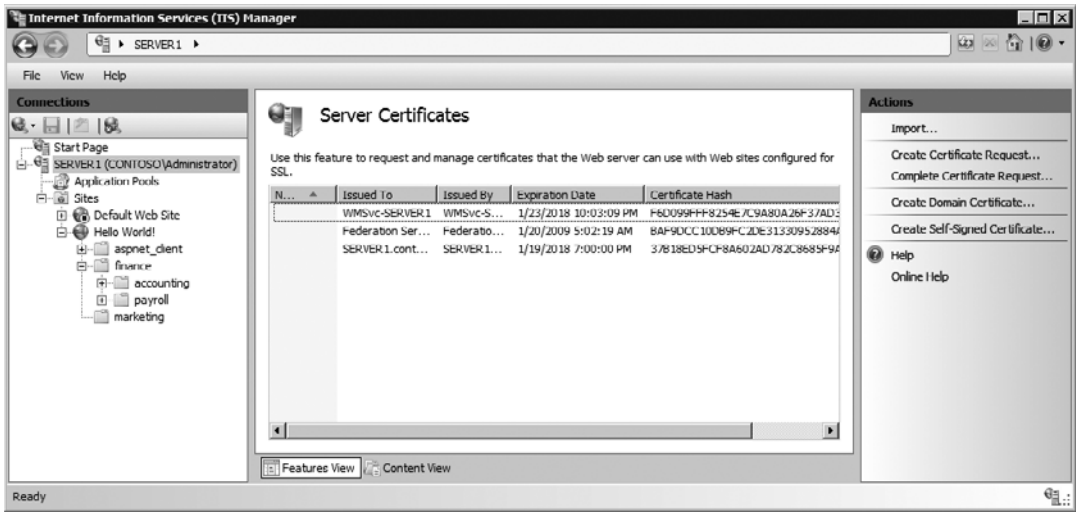
Protecting the privacy of the data being transmitted is the primary focus of transport security. There are a number of options within the Windows Server 2008 infrastructure to protect the privacy. You may want to wrap all data being transmitted, for example, through a virtual private network or IPSec tunnel. With this as the extreme at one end, IIS provides a more moderate and widely used method for protecting data using Secure Socket Layers (SSL). SSL uses digital certificates to encrypt the communication. There are two approaches to engaging SSL: implicit, where SSL is used for communication upon the initial connection, and explicit SSL, where SSL is enabled for the session after the initial connection is made. FTP Services was built to support explicit SSL, which is the method documented in RFC 2228. The implicit method has been documented in several drafts, but never formally adopted by the IETF. At a high level the explicit FTP SSL process works as follows:

1. The client connects to the server (typically through TCP port 21).
2. The client requests a secure session.
3. The server sends back its public encryption key.
4. The client checks the key to ensure:
   - The name of the host being requested matches the key,
   - The key is within the valid date range, and
   - The key's issuer is trusted by the client.

5. If the client determines that it can trust the server's public key, it will send its public key to the server.
6. The server will generate a password and encrypt it using both the client's public key and the server's private key and send it back to the client.
7. The client will decrypt the password as evidence that the server is the one who sent the password, thereby establishing that only the server and the client will be capable of reading the encrypted information.
8. The client will send the request to the server encrypted with the password that the server sent to it.
9. With the secure channel established, the FTP client continues on to authenticate the user and begin the session.

Before you can enable your FTP site for secure communication you will need to register a security certificate. IIS 7 introduces a new management interface for security certificates used by all protocols it handles. This new interface, as shown in Figure 7.14, gives you a single point to review all of the certificates installed on your server along with exposing the ability to generate a self-signed certificate from within the interface. Previously self-signed certificates were only available through the command-line SelfSSL tool that shipped with the IIS 6.0 Resource Kit tools.

Figure 7.14 Server Certificates Module Configuration



The first step to enabling a secure FTP site is to import or create a new certificate into the server. When creating a certificate you can create one from an online

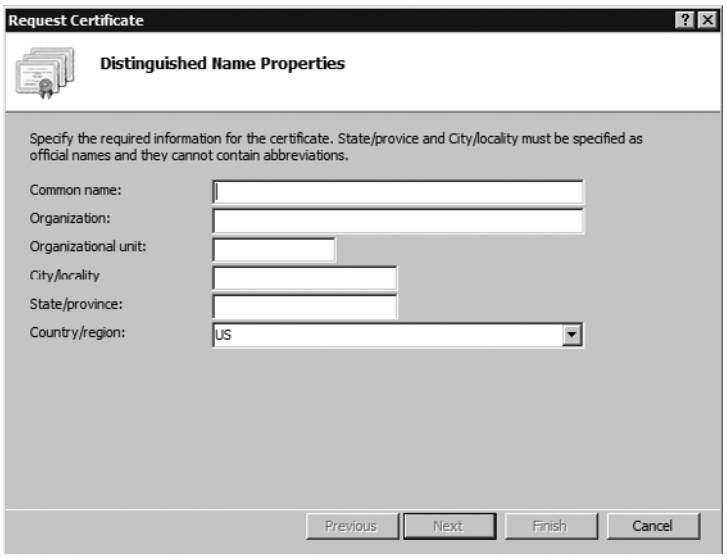
connected certificate authority (CA) like the Certificate Services role that ships with Windows Server 2008, a third-party CA (e.g., Comodo, Thwarte, Verisign), or generate a self-signed certificate. Whichever path you choose the one thing to remember is that the client will need to trust the certificate's issuer in order to trust the certificate. When using a self-signed certificate no one will trust it unless they take steps to specifically add it to their trusted certificates list.

EXERCISE 7.7

ADDING A NEW SECURITY CERTIFICATE

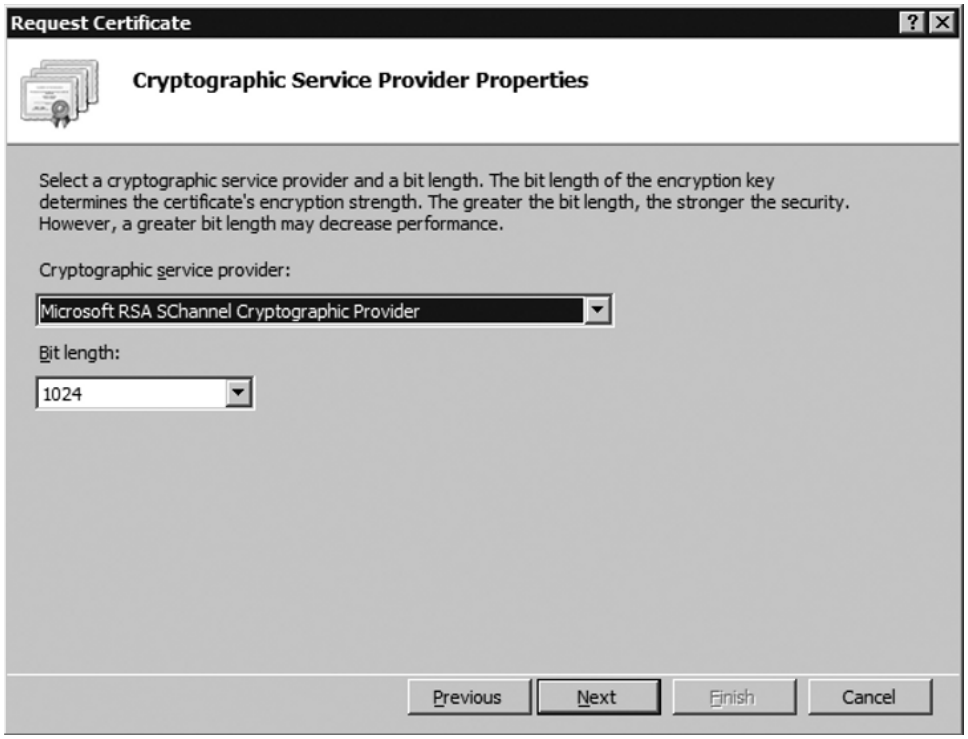
1. Open **Control Panel** and under System and Maintenance | Administration Tools double-click the **Internet Information Services (IIS) Manager** shortcut.
2. In the Internet Information Services (IIS) Manager management console, click the server node, and in the middle pane click **Server Certificates.**
3. In the right-hand actions pane click **Create Certificate Request.**
4. In the **Request Certificate** dialog on the Distinguished Name Properties page, provide the host name that will be used to access your site (e.g., ftp.contoso.com) along with your company information and click **Next** (see Figure 7.15).

Figure 7.15 Distinguished Name Properties Page



5. On the Cryptographic Service Provider Properties page, shown in Figure 7.16, choose a **Cryptographic Server Provider** and a minimum of 1,024 **Bit Length** for the key, and click **Next.**
   - **RSA SChannel Cryptographic Provider** Uses an MD5 hash with an SHA hash, signed with an RSA private key. It supports SSL2, PCT1, SSL3, and TLS1 protocols.
   - **DH SChannel Cryptographic Provider** Uses the Diffie-Hellman algorithm and supports SSL3 and TLS1 protocols. Use this algorithm when you must exchange a secret key over an insecure network without prior communication with the client.
   - **Bit Length** The default length supported by most browsers and certificate authorities is 1,024 bits. With processors becoming more powerful expect to see a move towards 2,048 bit length certificates past the year 2010. Be sure to check with your chosen certificate authority to ensure they will support bit lengths larger than 1,024 before increasing this value.

Figure 7.16 Cryptographic Service Provider Page



6. On the File Name page provide a path and name of a file for sorting the certificate request and click **Next.**
7. Contact your preferred certificate authority to obtain the response file for your request.

   If you are looking to test out the SSL functionality, there are a number of providers, such as Comodo and GeoTrust, that will give you a free trial SSL certificate that lasts anywhere from 15 to 60 days. This is handy because they have all of the trust features of regular certificates with no cost.
8. When you obtain the response file open IIS Manager and return to the Server Certificates section.
9. In the right-hand actions pane click **Complete Certificate Request.**
10. In the **Complete Certificate Request** dialog on the Specify Certificate Authority Response page, locate the **Certificate Authority's Response** file, provide a **Friendly Name** for the certificate, and click **Next** to complete the process.

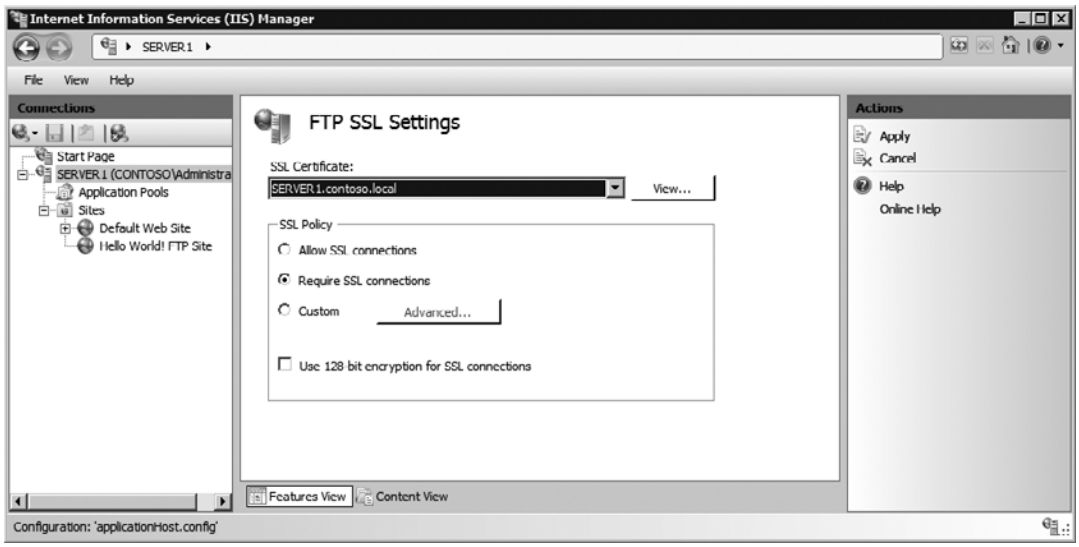
With the certificate in place you can now bind the certificate to your FTP site. Once the certificate is bound you can choose to allow or force the use of SSL for the control channel, data channel, or both.

EXERCISE 7.8

ENABLING SECURE COMMUNICATIONS ON YOUR FTP SITE

1. Open **Control Panel** and under System and Maintenance | Administration Tools double-click the **Internet Information Services (IIS) Manager** shortcut.
2. In the Internet Information Services (IIS) Manager management console, expand the server node and sites node and select your FTP site.
3. In the middle pane under Features view, double-click **FTP SSL Settings** (see Figure 7.17).

Figure 7.17 FTP SSL Settings Module Configuration

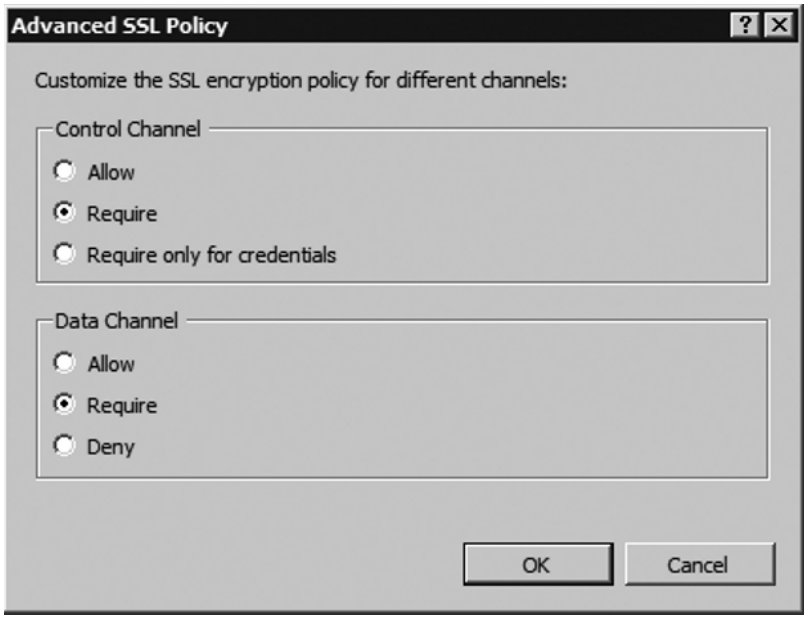


4. On the FTP SSL Settings page, select an **SSL Certificate**, choose whether to **Allow** or **Require SSL connections**, and in the actions pane click **Apply.**

   As with\Web connections you can force a minimum of 128-bit encryption.

Any form of encryption will add overhead to the processing. If you have an FTP server that is heavily used or needs to coexist with other applications, you can also customize the behavior of SSL to protect one of the channels or just the login process. The choice will depend on your data privacy policies. At a minimum you will generally want to protect user credentials. If the FTP clients are unable to support FTP over SSL, you will need to leave these settings at *Allow*. Otherwise, you can use the "Require Only for Credentials" option to minimize overhead and protect what is traditionally a clear text exchange (see Figure 7.18). If you need to protect what the user is doing from anyone who may be monitoring the network traffic the encryption of the control channel as a whole is best. Finally if you are exchanging sensitive data such as customer information you may want to protect the data channel using the *Require* option. Specifically for the data channel, you can also deny the encryption which may be required for certain compliance monitoring scenarios.

Figure 7.18 Advanced SSL Policy Dialog

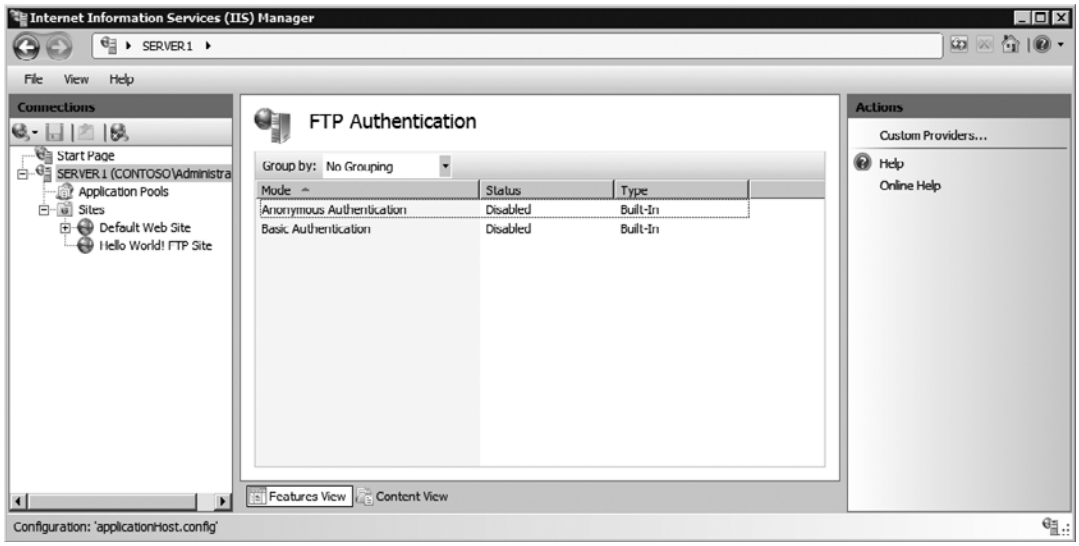


Authentication

Authentication is the process of asserting the identity of the user when they are establishing a session with the FTP site. With this identity we can track who is doing what and evaluate rules to determine if they are authorized to interact with content and folders. IIS ships with two types of authentication modules that can be used to determine a user's identity (see Figure 7.19):

- **Anonymous** Enabled by default to allow any user to access public content without a username and password. Anonymous connections use the username "anonymous" and prompt the user to enter their e-mail address as a password for logging purposes.
- **Basic** Requires the user to provide a username and password. This authentication protocol is a standard across all platforms. It does not perform any sort of encryption with the information provided by the user. As such you should use it with SSL to ensure that the credentials are sent over a secure connection.

Figure 7.19 FTP Authentication Module Configuration



EXERCISE 7.9

ENABLING BASIC AUTHENTICATION

1. Open **Control Panel** and under System and Maintenance | Administration Tools double-click the **Internet Information Services (IIS) Manager** shortcut.
2. In the Internet Information Services (IIS) Manager management console, expand the server and select an FTP Site on which you want to enable authentication.
3. In the middle pane under Features view double-click **FTP Authentication.**
4. Right-click the **Basic Authentication** module and select **Enable.**

Authorization

With the user's identity established the next step is to determine if the user can perform the action that is being requested. Actions on an FTP site include downloading and uploading of content. They can also perform basic file management functions if authorized. The authorization module evaluates the action based on a set of rules that decide if the user should be allowed, based on the user's identity

and if they are attempting to read or write data. IIS provides two modules focused on authorization and supporting services: URL authorization and IP authorization.

URL Authorization

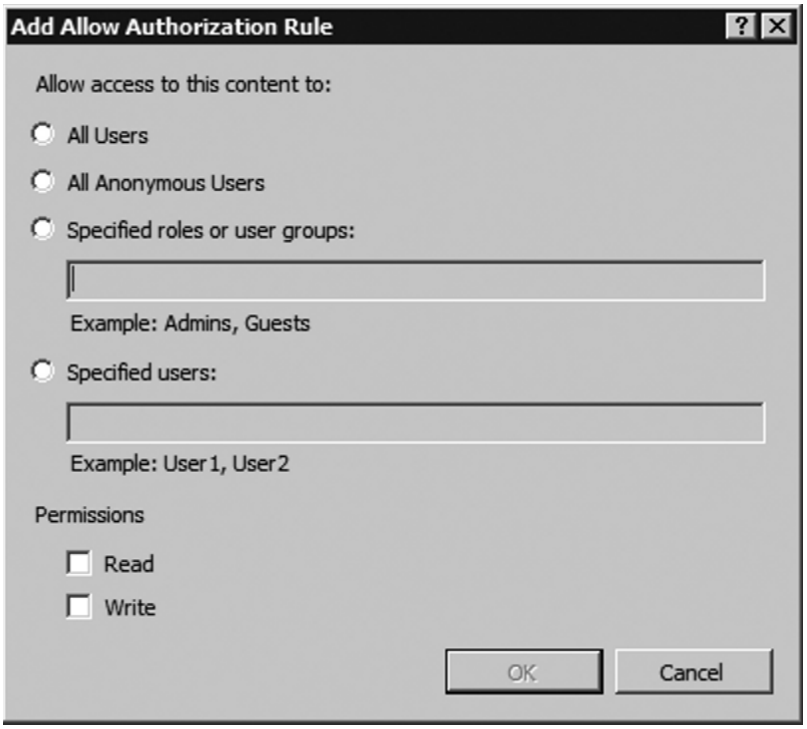
In previous releases the authorization to perform actions was decided at the site level and enforced further down through NTFS permissions. In this release the URL authorization capabilities typically enjoyed by the Web site have been extended for the FTP server scenarios. This module allows administrators the ability to control read or write access to files and folders in addition to the NTFS permissions on the content. Unlike NTFS permissions, you do not need file system access to the server to apply permissions, since everything is managed through the web.config file stored at the root of the site or within a given folder. This allows you to easily carry the permissions with the site as it moves environments.

EXERCISE 7.10

RESTRICTING ACCESS TO A FOLDER

1. Open **Control Panel** and under System and Maintenance | Administration Tools double-click the **Internet Information Services (IIS) Manager** shortcut.
2. In the Internet Information Services (IIS) Manager management console, expand the server and site node, locate a folder to secure (or choose the site as a whole), and click your selection.
3. In the middle pane under Features View double-click **Authentication.**
4. On the Authentication page, ensure that the Anonymous Authentication module is **Disabled**, select one of the other authentication modules, and click **Enable** in the right-hand Actions pane.
5. Click the **Back** arrow in the top left-hand corner.
6. On the folder page in the middle pane under Features view, double-click **Authorization Rules.**
7. On the Authorization Rules page, click **Add Allow Rule** in the right-hand actions pane.
8. Select the **Specified Users** radio button, provide a username, and click **OK** (see Figure 7.20).

Figure 7.20 Add Allow Authorization Rule Dialog



IP Authorization

The ability to restrict access to specific IP addresses has existed for quite some time across both servers and networking devices such as firewalls. In the past this function, like file permissions, was only available through IIS Manager and was tough to replicate across to other servers as it was stored in the metabase. This setting, along with all other configuration options, has been moved to the new XML-based configuration files. This allows you to centralize, copy, and manipulate the settings using new programming interfaces and command-line tools as well as the traditional graphical user interface.

EXERCISE 7.11

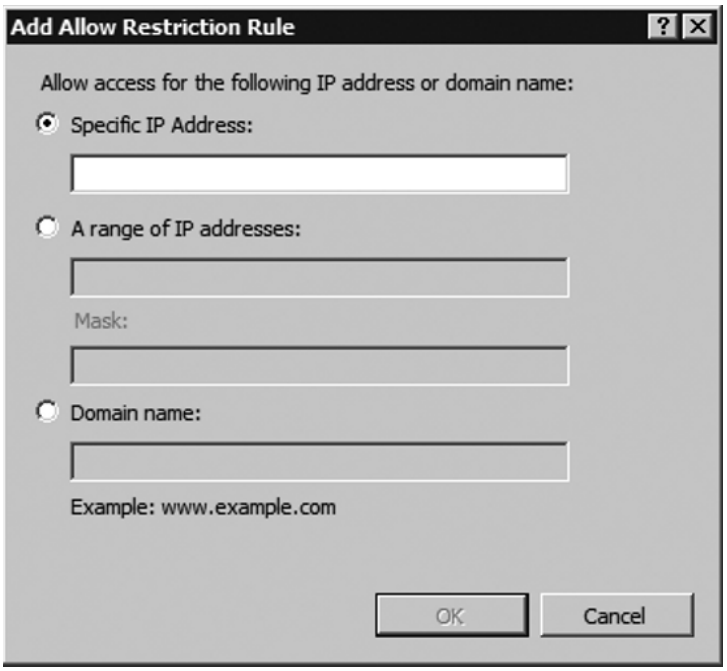
RESTRICTING ACCESS TO USERS BASED ON THEIR IP ADDRESS

1. Open **Control Panel** and under System and Maintenance | Administration Tools double-click the **Internet Information Services (IIS) Manager** shortcut.

2. In the Internet Information Services (IIS) Manager management console, expand the server and sites node, locate a folder to secure (or choose the site as a whole), and click your selection.
3. In the middle pane under Features view double-click **FTP IPv4 Address and Domain Restrictions.**
4. In the right-hand actions pane click **Add Deny Entry.**
5. In the **Add Deny Restriction Rule** dialog, select the **Specific IPv4 Address** radio button, provide an IP address (e.g., 127.0.0.1 if you want to test ftp access from the server), and click **OK.**

When users attempt to access a file or folder to which they have been denied they will receive a forbidden error. Another option is to restrict users based on their domain name. You will need to enable this through the *Edit Feature Settings* link in the module page on IIS. Be aware that the added overhead of DNS resolution for each IP address could negatively affect the performance of your FTP site. Just as you can restrict specific users, you can also deny all and only allow specific users. This process is similar to adding deny rules with the dialog, shown in Figure 7.21, looking very similar to that of adding deny restriction rules.

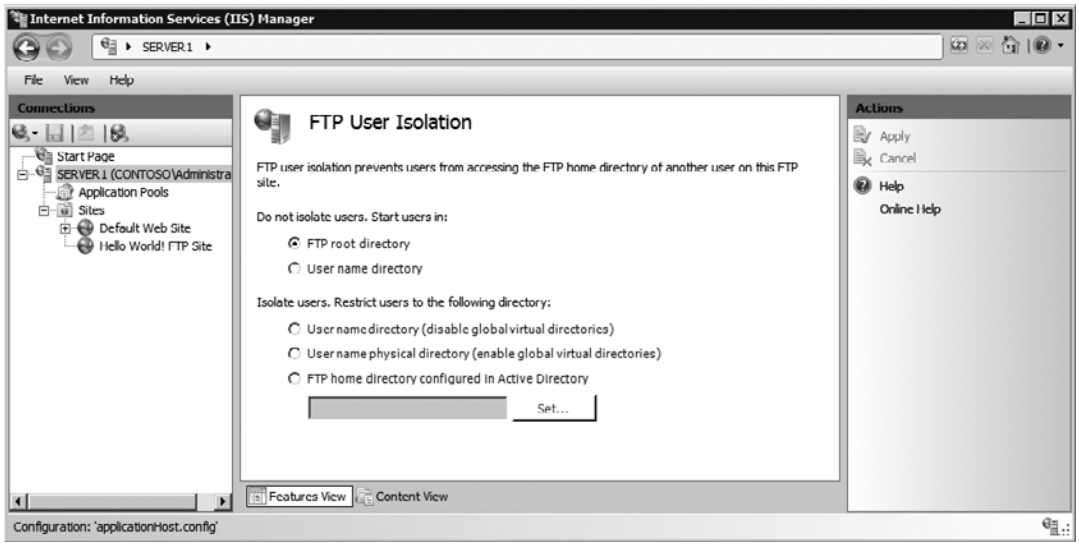
Figure 7.21 Add Allow Restriction Rule with Domain Restrictions Enabled



User Isolation

The User Isolation feature will place users into their own home folder when they login, while preventing them from viewing or overwriting other users' content (see Figure 7.22). This feature is most commonly used in shared hosting scenarios. Inside their home folder users can create, modify, and remove files and folders as they wish.

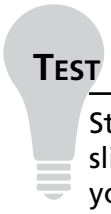
Figure 7.22 FTP User Isolation Module Configuration



There are five isolation options to choose from:

- **Do Not Isolate Users: FTP Root Directory** This is the default option that places everyone in the FTP root folder upon logon.
- **Do Not Isolate Users: User Name Directory** Users will start in a folder that bears their username if it exists; otherwise they will be placed in the FTP root folder. The user can navigate to the root of the FTP site.
- **Isolate Users: User Name Directory** Isolate users to a physical or virtual directory that bears their username. The user cannot navigate to the root of the FTP site.
- **Isolate Users: User Name Physical Directory** Isolates users to the physical directory that bears their username. The user cannot navigate to the root of the FTP site.

- **Isolate Users: FTP Home Directory Configured in Active Directory** Isolates users to the directory specified in their Active Directory account. The user cannot navigate to the root of the FTP site.



Test Day Tip

Study the different user isolation options carefully—the differences are slight, but they have a big impact on the security of the solution that you propose.

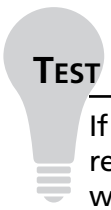
In all cases the folder needs to be created for the user before they login. The syntax for folder names depends on how the user account is stored:

- **Anonymous Users for Non-Isolated User Name Directory Mode** (FTP Site Root)\Default
- **Anonymous Users when using an Isolation Mode** (FTP Site Root)\LocalUser\Public
- **Windows Local Users** (FTP Site Root)\LocalUser\(Username)
- **Windows Domain Users** (FTP Site Root)\(Domain Name)\(Username)
- **IIS Manager or Custom Authentication Module Users** (FTP Site Root)\Local User\(Username)

To specify the starting directory for anonymous access, create a physical or virtual directory folder named *default* in the root directory of the FTP site.

Installing and Configuring SMTP Services

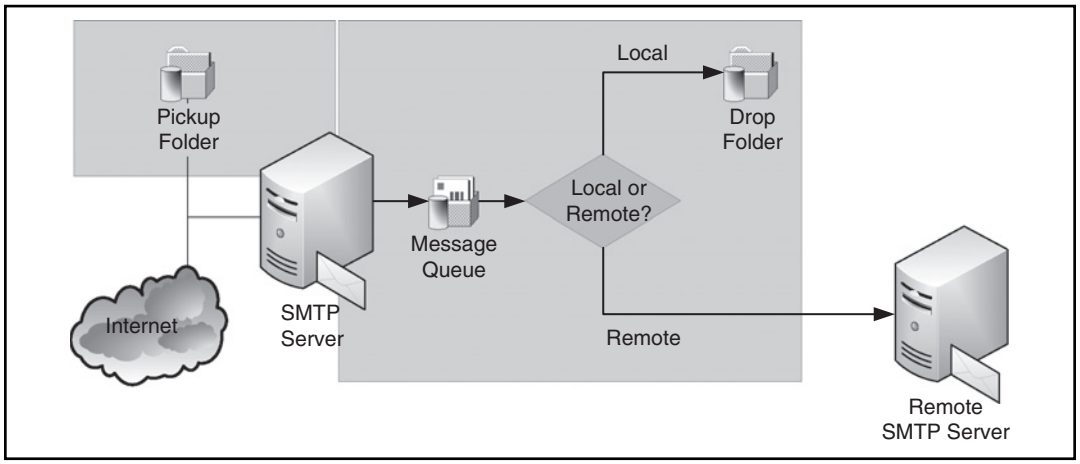
Many applications use e-mail delivery to support the functionality that they offer. The Simple Mail Transfer (SMTP) Service is a basic mail relay that ships with Windows Server 2008 and provides local and remote delivery of messages, as shown in Figure 7.23.



Test Day Tip

If you have used the IIS 6 SMTP Service you will find the differences in this release to be very minimal. Knowledge and skills attained through working with the previous release will apply to this release and as such to the exam.

Figure 7.23 SMTP Relay Process



When you receive messages locally, they are received through the Drop folder. When you receive messages remotely, they are received through a TCP connection, by default port 25. Messages are placed into a message queue for processing. The SMTP server reviews the message destination and compares it with the list of domains that it maintains. If it contains explicit instructions on how to handle a message then it acts upon those. If the SMTP server is considered the local domain SMTP server, then it will place the message in a local Drop folder for another application to pickup and process. If it has explicit instructions to route to a remote SMTP server then it will follow those instructions. If it does not have any corresponding record for the domain and the caller has relay privileges then it will locate the remote SMTP server and send the message as well.

Configuring & Implementing…

Real-World Use of SMTP Server

Over the past few generations of Windows Server, the use of SMTP Server has started to dwindle. The major product group relying on SMTP Server was the Exchange Server team. With the recent Exchange Server 2007

Continued

release, the Exchange Server team chose to write a new SMTP Server for use within the product. The SMTP Server today, as it exists in Windows Server 2008, now resides there primarily for backwards compatibility. This release saw very little development and no discussion of the future of the SMTP Server. To prepare your environment for future Windows Server releases, you should be aware of where the dependencies for this service exist (e.g., Windows SharePoint Services, third-party applications), and possible alternatives.

Installing SMTP Services

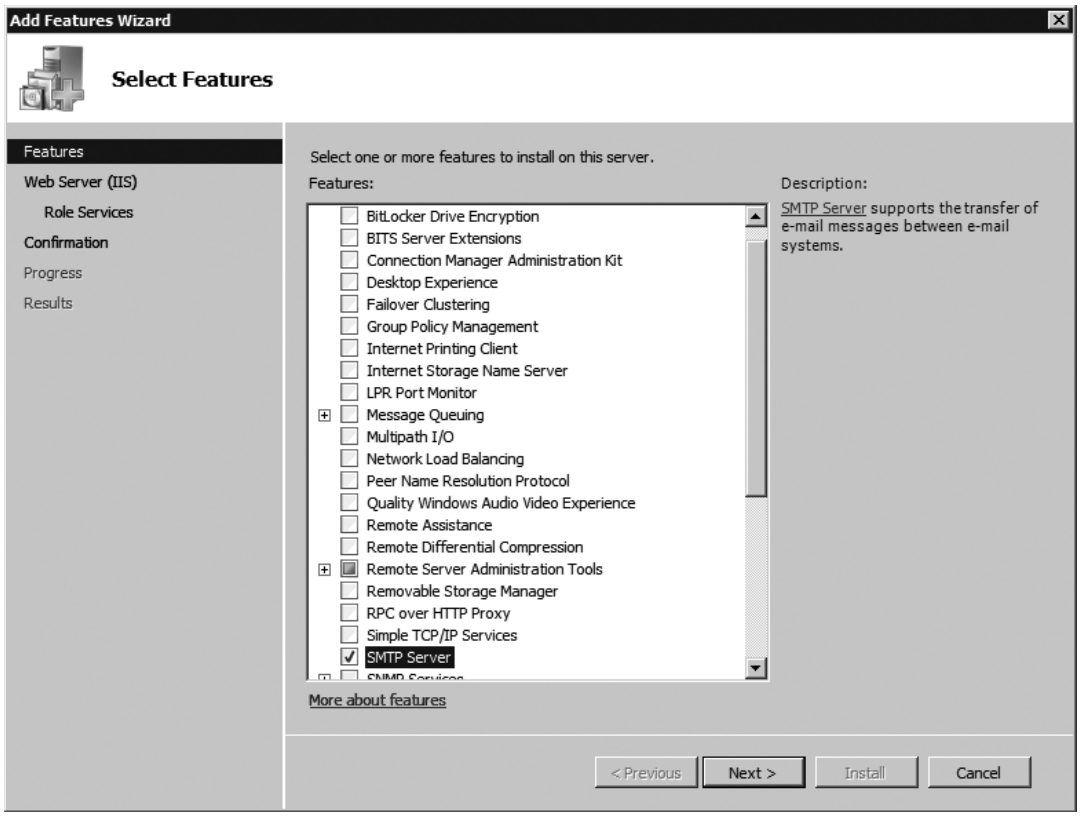
The Simple Mail Transfer Protocol (SMTP) Server is listed as a server-level Feature and not a part of any specific role. It has dependencies on the IIS 6 Management Compatibility and IIS 6 Management Console role server which is available in the Web Server role.

EXERCISE 7.12

INSTALLING SMTP SERVER

1. From the Start Menu select **Server Manager.**
2. In Server Manager, click the root node, scroll the right-hand pane to the **Features Summary** section, and click **Add Features.**
3. In the Add Features Wizard on the Before You Begin page, click **Next.**
4. On the Select Features page, select the **SMTP Server** role and click **Next**, as shown in Figure 7.24.

Figure 7.24 Select Features Page

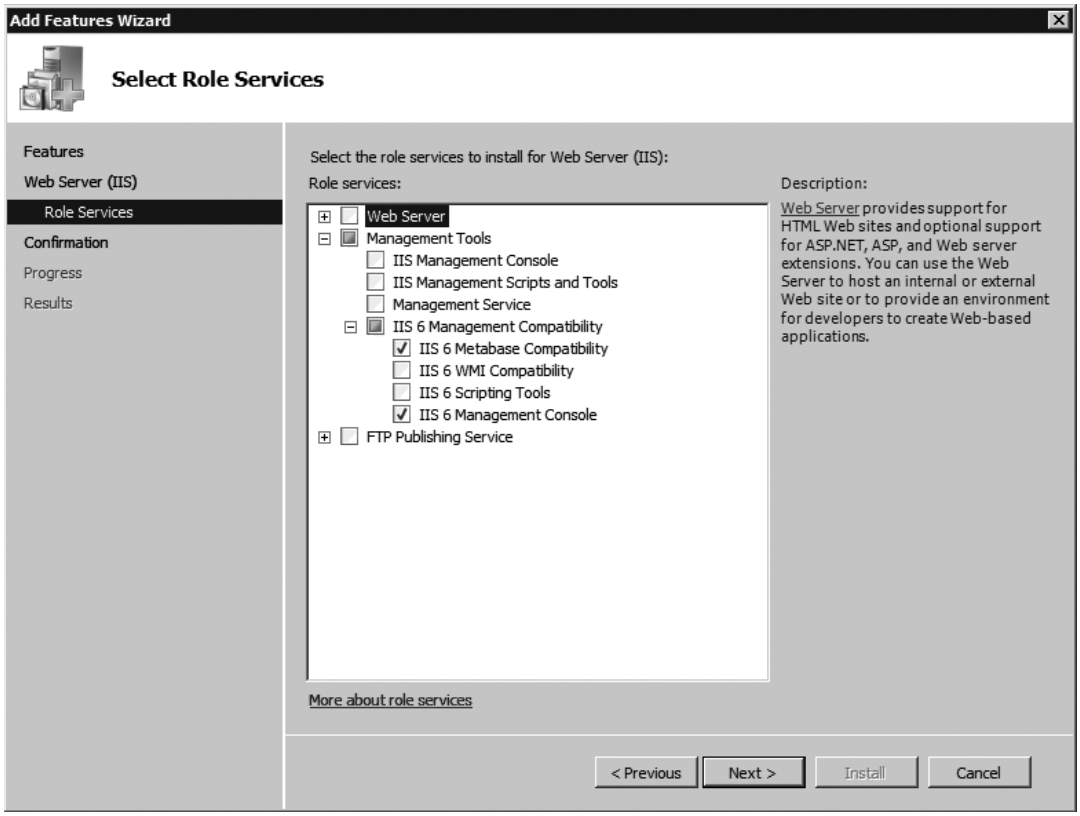


5. The Web Server (IIS) page gives you a brief description of the role along with some important notes and links to more information on the role. Click **Next.**

   If this is your first time setting up the Web Server (IIS) role, you should read these notes as they will cover common issues that you will encounter

6. On the Role Services page you are prompted to install several groups of services to the role (see Figure 7.25). Leave the default values and click **Next.**

Figure 7.25 Select Web Server (IIS) Role Services Page



7. On the Confirmation page, review your choices and click **Install.**
8. On the Results page, review the success or failure of the installation, then click **Close.**

With the SMTP Server installed you can manage it through the Internet Information Services (IIS) 6.0 Manager console located in the Administrative Tools group on the server.

EXAM WARNING

With Windows Server 2008 there is a split installation of IIS 6 and IIS 7 components. Be sure to understand which services have a specific reliance on IIS 6 components as they are managed in two different interfaces.

Provisioning Virtual Servers

A virtual server is the container under which receive and delivery rules are configured. You can have multiple virtual servers on a server, but they cannot be bound to the same IP address and port combination.

EXERCISE 7.13

Creating a New Virtual Server

1. Open **Control Panel** and under System and Maintenance | Administration Tools double-click the **Internet Information Services (IIS) 6.0 Manager** shortcut.
2. In the Internet Information Services (IIS) 6.0 Manager management console, right-click the server node and select **New | SMTP Virtual Server.**
3. In the New SMTP Virtual Server Wizard on the Welcome page, provide a descriptive **Name** and click **Next.**
4. On the Select IP Address page, select an **IP Address** and click **Next.**
5. On the Select Home Directory page, set a root **Home Directory** for your virtual server working folders and click **Next.**
6. On the Default Domain page, provide a **Default Domain** for the virtual server (which serves as the local domain) and click **Finish.**

With your virtual server set up to receive mail, you will need to add a list of domains for which it can receive mail. By default, anonymous connections will only be able to send mail to the domains that you have configured. When you configure the domain using domain routing instructions you can choose whether mail should be delivered to the local drop folder or to a remote server.

EXERCISE 7.14

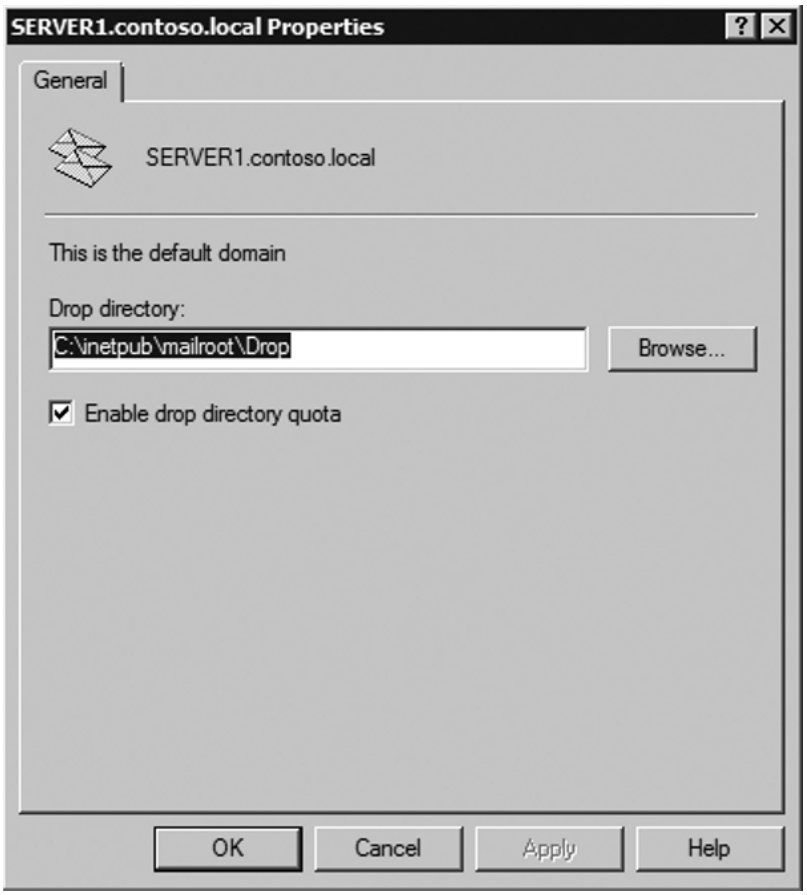
Adding Domain Routing Instructions

1. Open **Control Panel** and under System and Maintenance | Administration Tools double-click the **Internet Information Services (IIS) 6.0 Manager** shortcut.

2. In the Internet Information Services (IIS) 6.0 Manager management console, expand the server and virtual server node.
3. Right-click **Domains** and choose **New | Domain.**
4. In the New SMTP Domain Wizard on the Welcome page, select **Alias** or **Remote** depending on your needs.
5. On the Domain Name page enter a valid domain **Name** (e.g., contoso.com) and click **Finish.**

If you setup an alias domain there are no other properties available. The alias domains are an alternative name for the default local domain. The folder where the mail will be delivered is configured in the Properties of the default local domain, as shown in Figure 7.26.

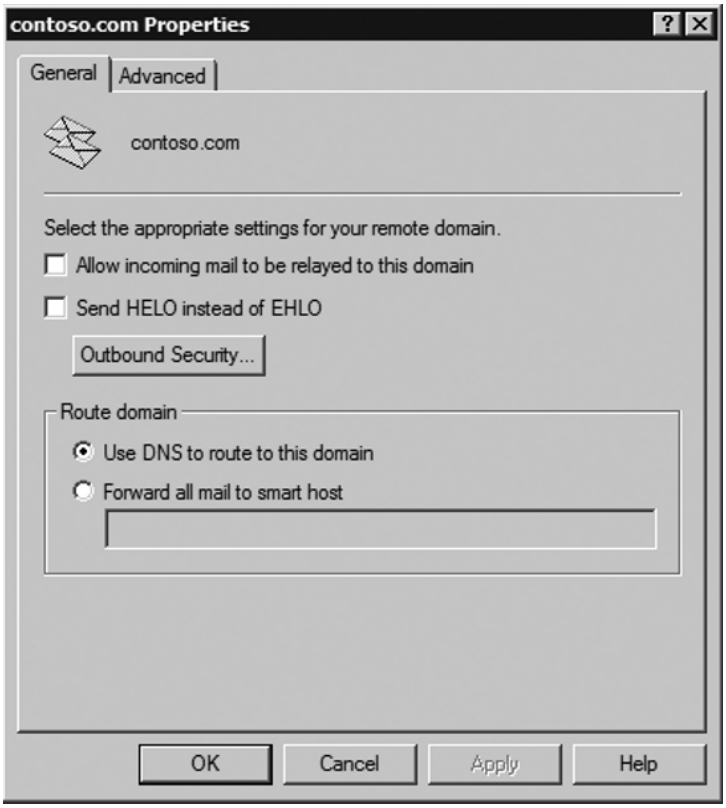
Figure 7.26 Default Local Domain Properties Dialog



For remote domains you will need to select the **Allow incoming mail to be relayed to this domain** checkbox to enable the server to accept mail. This option is disabled by default. This was done specifically to force you to knowingly allow the SMTP to receive and process mail for this domain. Much of the early unsolicited email problems were due to "open relays." This meant the SMTP servers would accept mail for any domain and attempt to deliver the message. Spammers would take advantage of these open relays as a way to obscure the source of their annoyances.

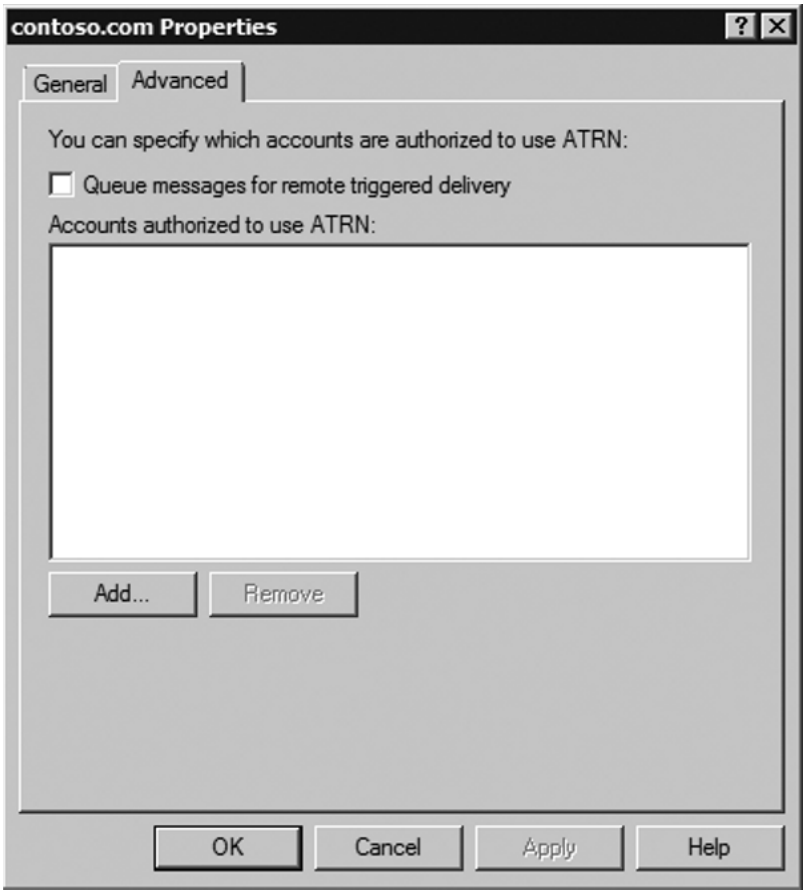
The rest of the dialog box has domain-specific delivery instructions (see Figure 7.27). In the **General** tab you can tell the server to use HELO for older SMTP servers that do not support EHLO. The **Outbound Security** button allows you to specify a set of credentials to use when connecting to the remote server where the message will be delivered. The Route Domain group gives you the option of trying to look up the mail exchanger (MX) records for the domain or forward directly to a specific host (smart host).

Figure 7.27 Remote Domain Properties Dialog



Under the **Advanced** tab, shown in Figure 7.28, you have the server queue the incoming messages until a client connects and issues the Authenticated TURN (ATRN) command. When this command is issued the messages will then be sent for delivery based on the configuration options specified under the **General** tab. If you need to secure this further you can specify that the ATRN command can only be executed by clients that connect and authenticate under specific accounts.

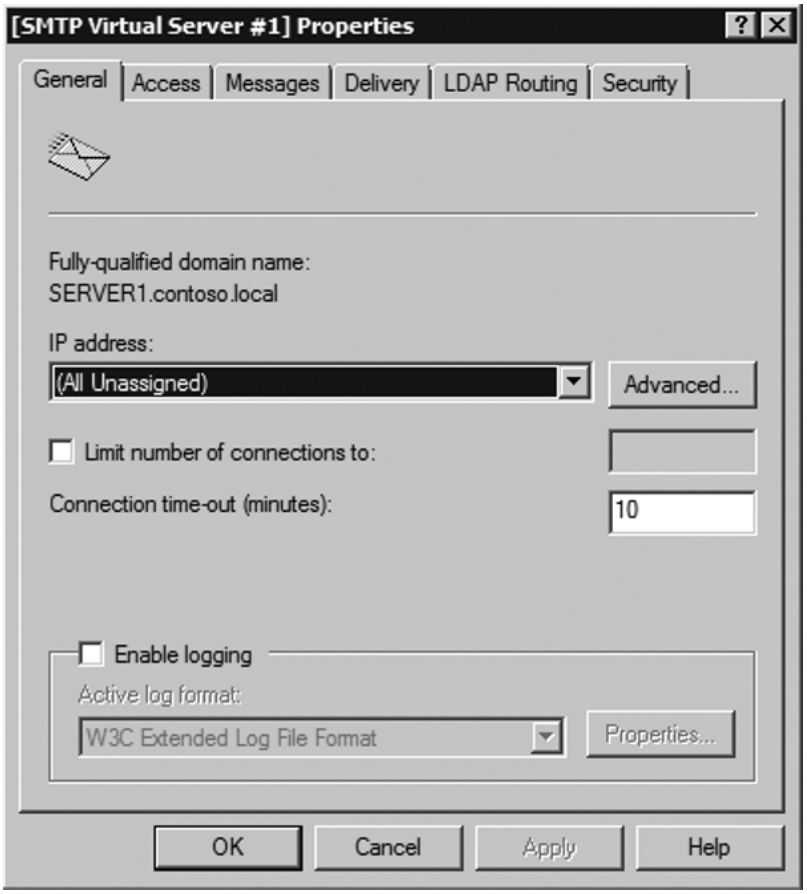
Figure 7.28 Advanced Tab



Configuring a Virtual Server

The default configuration for an SMTP virtual server requires little adjustment for most environments. Even so you should be aware of the various settings available (see Figure 7.29). In this section we will review each group of settings.

Figure 7.29 Virtual Server Properties Dialog



Server Bindings

By default the SMTP virtual server will look to bind to all IP addresses on the server using TCP port 25. There are scenarios where you might want to change this behavior to bind only to a specific network on a multi-homed server, or offer an alternative port for clients who are on a network that blocks port 25. If you are requiring users to use SSL/TLS (discussed later in this chapter) you will want to use port 465. In 1998 the Internet Engineering Task Force (IETF) published RFC 2476, which attempted to shift mail submission from port 25 to 587 for authenticated mail submission. In 2004 several major mail service providers echoed this push as part of the Anti-Spam Technical Alliance Technology and Policy Proposal (see www.microsoft.com/downloads/details.aspx?FamilyId=EF4A02D4-12AB-46A3-A4EC-9AADBED0ABB8 for a copy of the proposal).

EXERCISE 7.15

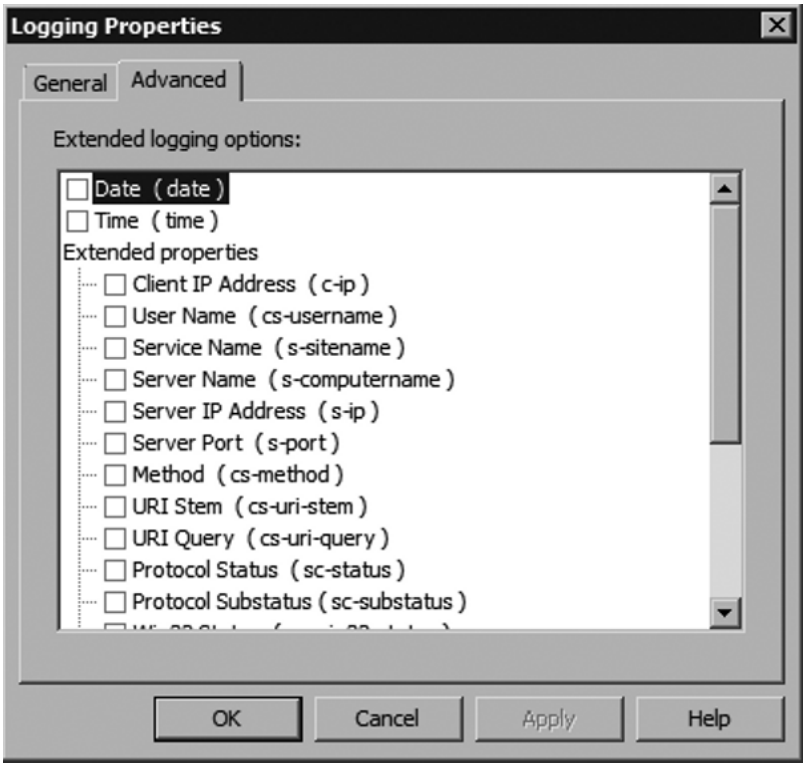
ADDING A NEW PORT BINDING

1. Open **Control Panel** and under System and Maintenance | Administration Tools double-click the **Internet Information Services (IIS) 6.0 Manager** shortcut.
2. In the Internet Information Services (IIS) 6.0 Manager management console expand the server node, right-click your virtual server, and select **Properties.**
3. In the **SMTP Virtual Server Properties** dialog under the **General** tab, click the **Advanced** button.
4. In the **Advanced** dialog click the **Add** button.
5. In the **Identification** dialog select the appropriate **IP Address**, provide the **TCP Port** number that you want to bind on, and click **OK** until all of the dialogs are closed.

Logging

Activity logging gives you a detailed picture of what your SMTP server is doing. For each request made to the server the log records particular properties of both the request and response for later analysis. Using log analysis tools you can review aggregate statistics to determine the number of messages passing through your server, where they are going, and when they are doing it (see Figure 7.30). You can also use activity logs as a tool in troubleshooting. IIS ships with logging disabled by default. You can enable logging by simply checking the **Enable Logging** checkbox in the **General** tab of the **Virtual Server Properties** dialog. The logs are written to the WINDOWS\SYSTEM32\LogFiles folder by default. The logs can be written using IIS, NCSA, and W3C formats. Alternatively you can log directly to any ODBC-compliant database.

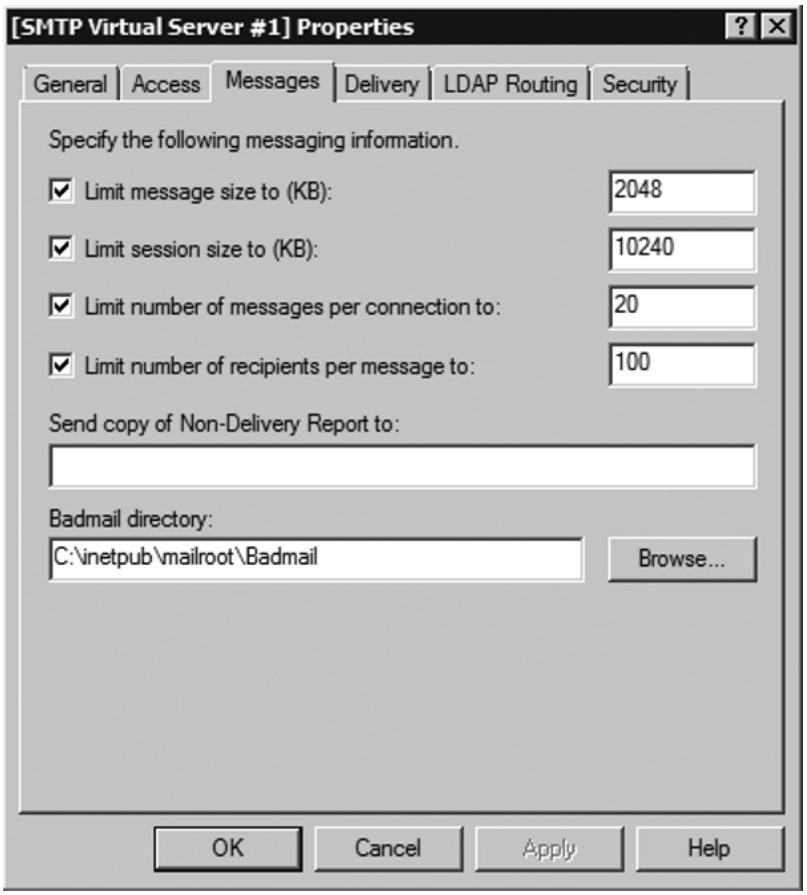
Figure 7.30 W3C Extended Logging Options



Message Limits

The message limits for a virtual server allow you to set various limits on incoming messages. This prevents people from overloading the server or downstream mail servers. If a message cannot be received or routed for any specific reason it will result in a non-delivery report being generated. You can specify to store a copy of the message in a local folder and send a copy of the non-delivery report to another address as well for troubleshooting purposes. The most common scenario for which you will visit this dialog is to adjust message size limits, as in Figure 7.31.

Figure 7.31 Messages Tab



EXERCISE 7.16

Increasing the Message Size Limit

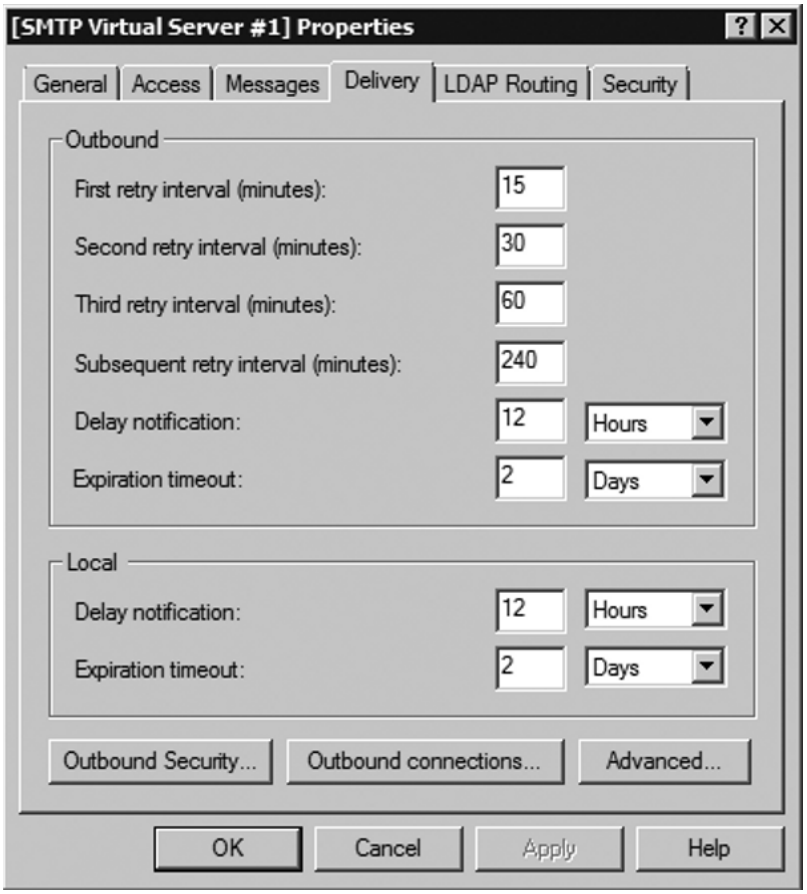
1. Open **Control Panel** and under System and Maintenance | Administration Tools double-click the **Internet Information Services (IIS) 6.0 Manager** shortcut.
2. In the Internet Information Services (IIS) 6.0 Manager management console expand the server node, right-click your virtual server, and select **Properties.**
3. In the **SMTP Virtual Server Properties** dialog select the **Messages** tab.

4. Set the value of **Limit Message Size** to the largest size of a message that you want to support and click **OK.**

Delivery Options

Once a message has been accepted the server needs to deliver the message. The SMTP protocol uses a store-and-forward approach to delivery, meaning that it does not require all mail servers to be online. The **Delivery** tab in the virtual server settings (see Figure 7.32) exposes the configuration options that control how long the server will wait to retry the delivery of a message. In most cases the default values are sufficient.

Figure 7.32 Delivery Tab

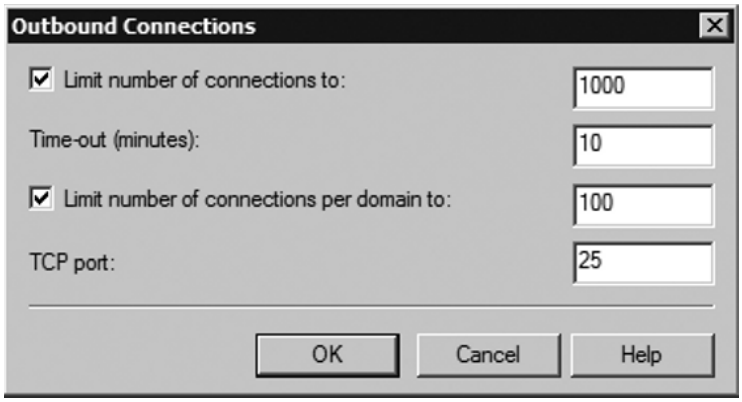


In the **Outbound Security** section you can specify the method and credentials used for delivery of messages, as shown in Figure 7.33. When set at the server level the selected method is used for delivery of all outbound messages.

Figure 7.33 Outbound Security Dialog

In the **Outbound Connections** section you can configure several options to throttle the number of concurrent outbound connections at the server and domain level, as shown in Figure 7.34. The TCP port can be changed for all outbound delivers. Unless you have a specific reason to change this port you should leave it at the default value since all Internet SMTP servers receive mail on port 25 by default.

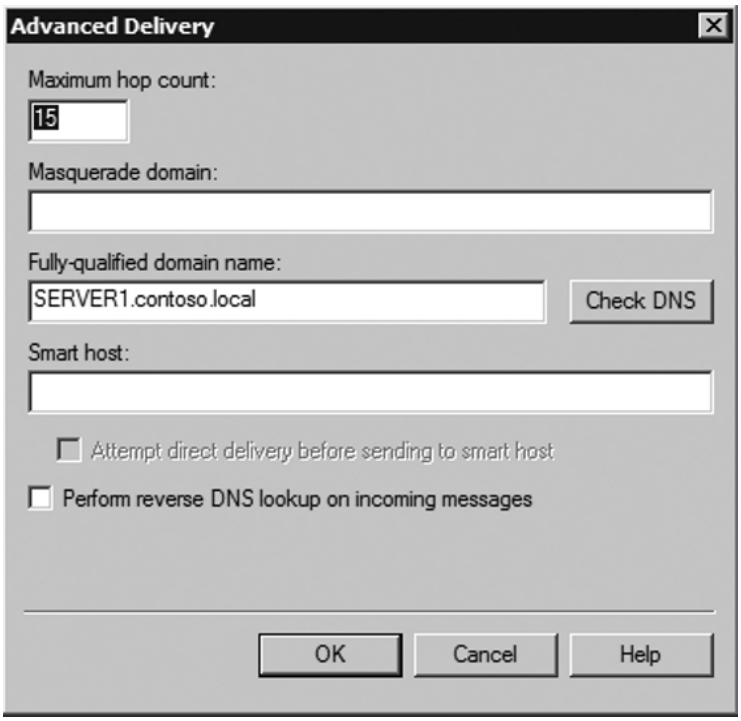
Figure 7.34 Outbound Connections Dialog



In the **Advanced** Delivery section you are presented with some advanced server behavior options (see Figure 7.35):

- **Maximum Hop Count** Stops messages from passing through this server if they have been through a certain number of servers already. This is useful to stop messages that may be stuck in a continuous loop.
- **Masquerade Domain** Replaces the domain name in the Mail From line with the specified value
- **Fully Qualified Domain Name** Server identifier added to message headers when a message passes through the SMTP gateway
- **Smart Host** Force all outbound messages to be routed to this server
- **Perform Reverse DNS Lookup on Incoming Messages** Will check all incoming messages to ensure that the domain that the server claims to be matches the reverse DNS record of the IP address. If no match can be made then an unverified message is added to the message header.

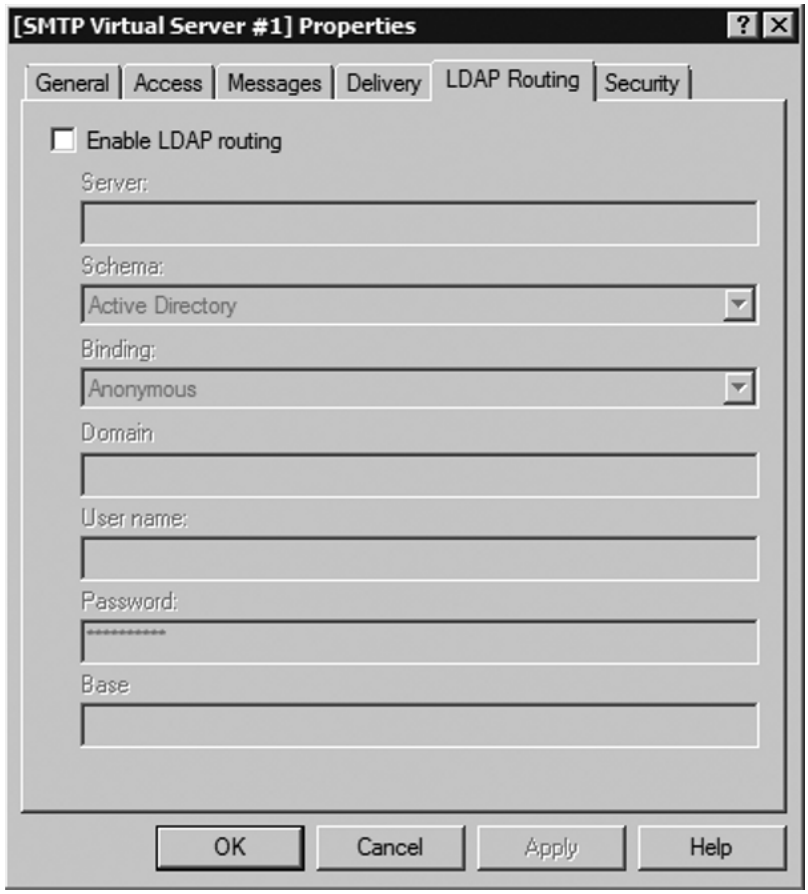
Figure 7.35 Advanced Delivery Dialog



LDAP Routing

You can configure the SMTP Server to resolve recipients using Active Directory, Site Server Membership Directory (version 3.0 and earlier), and the Exchange LDAP Service (version 5.5 and earlier). When a message is received, SMTP will look up the email address in the directory and if it is a group it will send the message to all members in the group. The options in the **LDAP Routing** tab specify the name of the server and account to use for binding (see Figure 7.36). The account will require browse, read, and search permissions within the directory to function properly.

Figure 7.36 LDAP Routing Tab



Securing Your SMTP Virtual Server

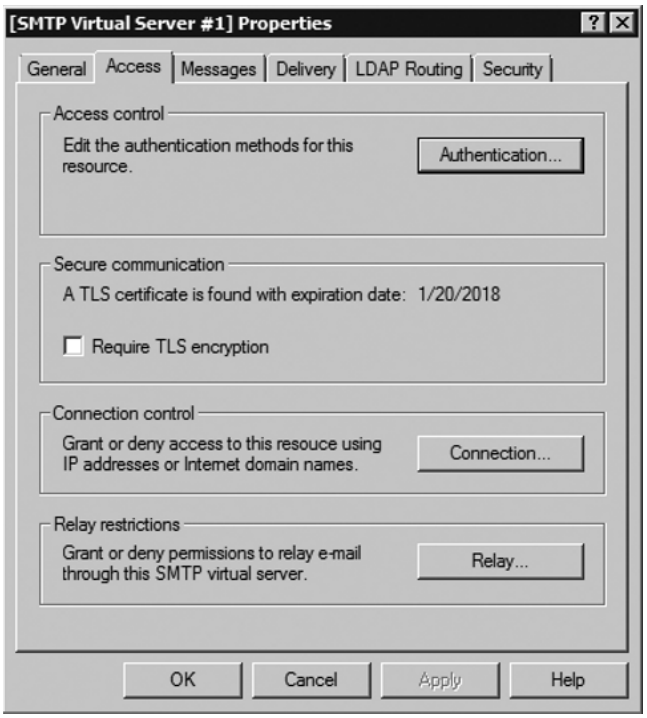
To secure your SMTP virtual server, you need to understand the Transport Layer Security (TLS) protocol, the three types of authentication that an SMTP Server supports for determining a user's identity, connection control, and relay restrictions. We'll now discuss each of these areas.

Transport Security

SMTP Server supports securing message communication using Transport Layer Security (TLS). The TLS protocol is known as the successor to Secure Socket Layers (SSL). It shares many of the same characteristics as SSL, including how the connection is set up, but it is not compatible. Under this release of the SMTP Server you

cannot choose the server certificate that will be used for TLS encryption. The service will automatically look for a certificate that matches the full qualified domain name of the computer. The Access options tab is shown in Figure 7.37.

Figure 7.37 Access Tab



New & Noteworthy…

Certificate Creation Changes

If you have used the IIS 6 SMTP Server then you might notice that the Secure Communication section in the Windows Server 2008 release has changed. No longer do you have the ability to create and manage certificates from this interface. Instead that functionality has been moved over to the IIS 7 management tools. Another behavioral change to be aware of is the automatic choice of using a certificate that matches the machine's full qualified domain name.

Authentication

Authentication is the process of asserting the identity of the user or service that is sending a message through your virtual server. The SMTP Server supports three types of authentication to determine a user's identity:

- **Anonymous** Enabled by default to allow any user to send messages to authorized domains without a username and password
- **Basic** Requires the user to provide a username and password. This authentication protocol is standard across all platforms.

  Just as you can require TLS for the incoming communication as a whole, you can require TLS for any connection that tries to authenticate using Basic authentication. Using TLS will protect the otherwise clear text username and password.
- **Integrated Windows Authentication** Used mainly in intranet scenarios, it allows SMTP to use the current user's Windows domain credentials to authenticate the connection.

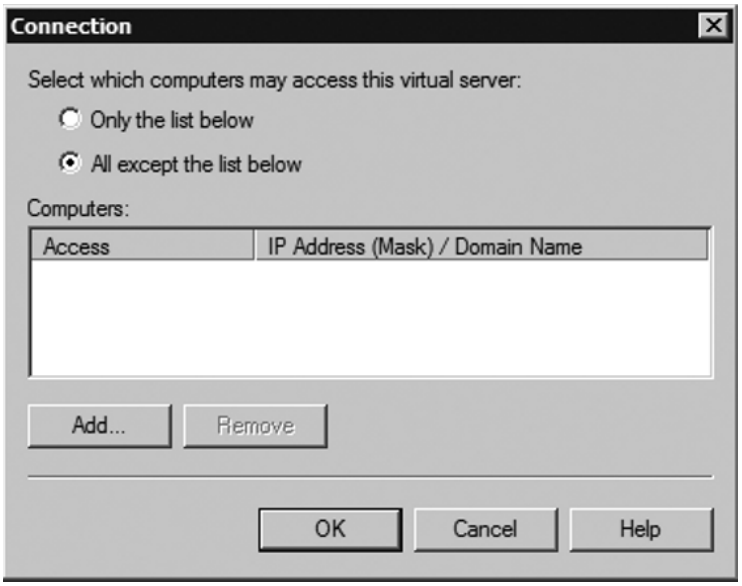
In public-facing scenarios where you are setting up SMTP Server to be an incoming mail relay, you will select **Anonymous access** authentication, as shown in Figure 7.38. For internal applications or to allow users to relay through the server to any domain, you will need to use either **Basic** or **Integrated Windows Authentication**.

Figure 7.38 Authentication Dialog

Connection Control

Connection Control allows you to limit the devices that can connect to the SMTP Server, as demonstrated in Figure 7.39. This can be useful if you are using the service as a relay for locally installed applications by restricting connections to that of the local host. You can alternatively prevent specific computers from connecting to the server. Connections can be evaluated based on a single IP address, a masked IP range, or a domain name. If you choose domain name the server will perform a reverse DNS lookup on all incoming connections, which may adversely affect performance.

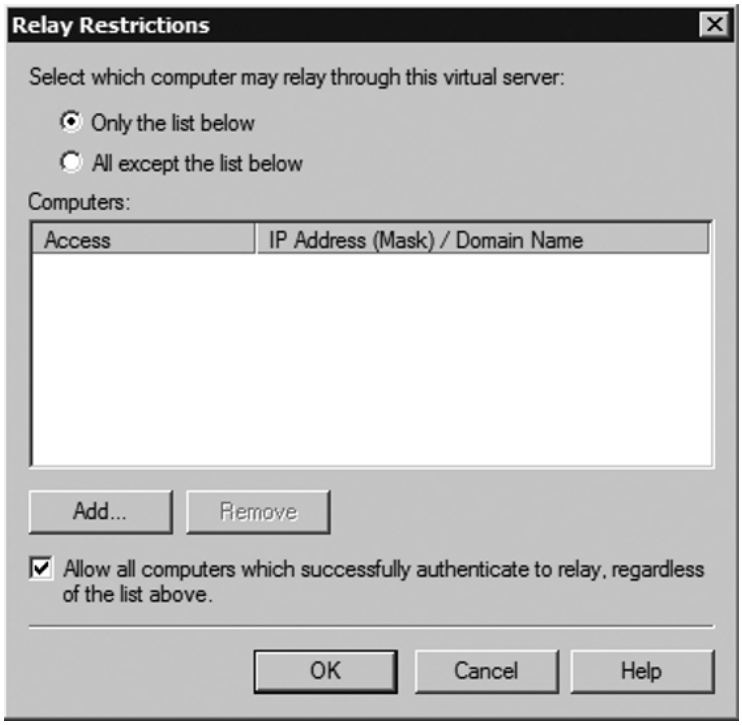
Figure 7.39 Connection Control Dialog



Relay Restrictions

By default the SMTP service will only allow users who authenticate to your server to relay. If you have applications that do not support SMTP authentication and need to relay you can add them to the relay restrictions list to allow them the ability to use the server as a relay (see Figure 7.40). This restriction provides you with another method to control who can relay through your SMTP server.

Figure 7.40 Relay Restrictions Dialog



EXERCISE 7.17

ENABLING CLIENTS TO RELAY MAIL

1. Open **Control Panel** and under System and Maintenance | Administration Tools double-click the **Internet Information Services (IIS) 6.0 Manager** shortcut.
2. In the Internet Information Services (IIS) 6.0 Manager management console expand the server node, right-click your virtual server, and select **Properties.**
3. In the **SMTP Virtual Server Properties** dialog select the **Access** tab and click the **Relay** button.
4. In the **Relay Restrictions** dialog click **Add.**
5. In the **Computer** dialog select the **Single Computer** radio button, provide the **IP Address** of the client computer, and click **OK** until all of the dialogs are closed.

Summary of Exam Objectives

This chapter focused on configuration of the File Transfer (FTP) Publishing and Simple Mail Transfer (SMTP) Services. The major investments in this release focused on the FTP support by providing a re-written, integrated FTP service that takes advantage of the advancements brought forth in Internet Information Services. While Windows Server 2008 ships with the older IIS 6 FTP Publishing Service, you should use this new release, as it was the version intended to ship with Windows Server 2008, but missed the cutoff for inclusion. The SMTP Server, on the other hand, remains similar to the older IIS 6 SMTP Server with very little change.

With the FTP Server we discussed the installation of the service. It requires the Web Server role be installed and that the old IIS 6 FTP Publishing Service be removed. After installing the new FTP Publishing Service, you manage it through the wide array of tools provided by the IIS infrastructure, including IIS Manager, AppCmd, and the various programmatic interfaces (Windows Management Instrumentation, Microsoft.Web.Administration Assembly, and so on).

The new FTP Publishing Service supports both full and Server Core installations. When you are ready to create your first FTP site you can create a standalone or bound FTP site. The standalone version works much like a typical FTP site where you point it to a folder that may or may not contain content for users to download and upload. In the bound FTP site the functionality is tied into an existing Web site setup in IIS. This allows you to give users alternative means of managing the content and Web applications on their site. Combined with the IIS Management Service and the new XML-based configuration files this is a complete and powerful set of tools available to users.

When you have configured your FTP site, you will need to consider whether you want the user or your server to be responsible for opening up a port to receive the data connection. If you choose the server to be responsible for establishing a port for the data connection (active mode), then you can establish a pre-defined range for the security administrators to forward from the firewall. If you choose for the user to establish that port then no further configuration is required.

The new FTP Publishing Service shares a number of other concepts with the Web side, including virtual directories and hosting the request processing inside an application pool. Virtual directories allow you to link in content folders from several locations into a single easy-to-navigate tree for users. The application pool gives you added isolation and resiliency in that if your FTP site were to fail, it would not impact other sites within the server. In a standard configuration FTP will send your

credentials and content over a clear text connection. Enabling FTP over SSL will give you the option to protect the authentication, control, and/or data conversations occurring. IIS implements an explicit SSL connection per RFC 2228 which means that the client connects over port 21 and explicitly asks the server for a secure conversation. With a secure connection in place you can further apply URL and IP restrictions to prevent groups of users from accessing the site as a whole or a specific section within. If you have users who need to access a personal home directory, user isolation gives you a chance to enforce the user's session to be isolated to that folder.

The SMTP Server enables you to receive mail from local Web applications or remote senders and forward them to other remote servers or keep them local for applications to process. Installation of the SMTP Server requires a full installation and depends on the IIS 6 backwards compatibility components of the Web Server role to function. After installing the SMTP Server it has a default virtual server created, however you can create others. A virtual server is a container for limits, authentication, authorization, and handling settings. It is bound to one or more IP address and port combinations. Each virtual server can be configured with specific instructions for handling mail destined to a particular domain, or with either authorization or being granted rights through the relay restrictions can relay mail to other mail exchangers (MX) in the network. If the SMTP server is being used as a local spool and you have an outbound SMTP gateway already in place through products like Exchange Server, you can configure the virtual server or specific domains to use that gateway as a default next point-of-contact (smart host). Incoming connections can be authenticated using Anonymous, Basic, or Integrated Windows Authentication modules. Likewise outbound connections can use the same three modules on a server or per-domain basis to ensure mail is transmitted in a secure manner. Privacy for mail is handled through TLS encryption. TLS draws upon the SSL family through the use of security certificates.

Exam Objectives Fast Track

Installing and Configuring FTP Publishing Service

- ☑ Windows Server 2008 ships with the older IIS 6 FTP Publishing Service. You should grab the Web release as it was the version that was meant to ship with Windows Server 2008 (but missed the deadline for inclusion by a few weeks).
- ☑ The new FTP Publishing Service is a major rewrite that adds a much

tighter integration into the IIS 7 framework and several important security enhancements. It works on both full and Server Core installations.

- ☑ Sites can be either standalone or bound to a Web site to provide greater options for users who need to manage their Web site or Web application content.
- ☑ From a transport security perspective the support of Explicit SSL connections allows you to protect the control, authentication, and/or data conversations between the client and the server.
- ☑ The rules around security (SSL) certificates follow the same rules as the Web sites in terms of the types of certificates and how they are validated.
- ☑ Out-of-the-box authentication modules include anonymous and basic authentication. Building on the IIS Framework allows you to open that up to a number of custom authentication modules.
- ☑ The built-in authorization mechanisms include a URL and IP restriction based on a set of rules. Within the URL side you assign allow/deny access to one or more users (including user groups/roles). Alternatively you can control which devices can connect to the site through IP restrictions.
- ☑ Once into the site you can apply a set of user isolation policies to restrict users to their personal home directory, or you can let them navigate the structure you have created using a set of physical and virtual folders.

Installing and Configuring SMTP Services

- ☑ Windows Server 2008 ships with the older IIS 6 SMTP Server with a few minor compatibility fixes. It depends on the Web Server role for IIS 6 backwards compatibility components. It can only be installed on a full server installation.
- ☑ Virtual servers are bound to combination IP address and port to represent the container for authentication, limits, and domain handling instructions.
- ☑ Within the virtual server you can specify handling instructions for a domain including allowing the server to accept anonymous relays, the method of delivery (lookup via DNS or to a smart host), the outbound authentication method, and whether to queue the messages until triggered.
- ☑ Inbound and outbound communication can be protected using TLS, which is related to the SSL family of communication encryption protocols.

Exam Objectives Frequently Asked Questions

Q: I need to set up an FTP site so our business partner can send us purchase orders. Where should I create their account so they can authenticate into the FTP site?

A: The new FTP Publishing Service supports basic authentication out-of-the-box, which looks to the IIS Users data store, local Windows security account manager, and, if a domain member, to Active Directory for authentication credentials. Using the IIS framework you can also implement a custom authentication module if needed.

Q: A user is trying to access the server using FTPS; however, they are being told that the certificate name does not match the host name. Where should I look?

A: The same rules for SSL on the Web apply to FTP—the certificate is bound to the IP address and port that the FTP site runs on. The certificate should reflect the name of the FTP site, use a wildcard sub-domain, or take advantage of the subjectAltName field to list several host names. If the client cannot match the host name, the user connected to it should show the warning about the certificate. In most clients the user can acknowledge the difference and continue to connect.

Q: We have set up the FTP Publishing Service in a shared hosting scenario. I need to isolate users to their own personal home directory in a way that they are unable to see others. Should I set up individual URL authorization rules to do this?

A: No, take a look at the user isolation feature in the FTP Publishing Service and choose between the three isolation modes to find one that matches your needs.

Q: I have set up an SMTP Server in our DMZ to receive mail from the Internet. I want it to forward to our internal mail server. What should I be doing to get it to forward the mail?

A: In the virtual server, set up a domain routing entry to allow it to receive mail for your domain and set it to forward to the specific IP address of your internal mail server (smart host) rather than look up how to deliver the messages.

Q: Our remote branch office has an unreliable connection. I have an Exchange Server there and I want to queue up the mail to be received by the remote server when it reconnects. What should I configure with SMTP Server to allow it to queue mail on behalf of this server?

A: You should set up your Exchange Server to issue an ATRN command to the SMTP server when it connects. This will cause the SMTP server to attempt to deliver all of the mail destined for that domain that resides in the queue.

Q: I think the SMTP server isn't processing mail it receives from the outside, but I'm not sure. Where can I look to determine that it is not working?

A: The first step is to send a message to the server. This can be done using a Telnet client and the steps outlined in Microsoft Support KB 323350 (http://support.microsoft.com/?id=323350). Once the message has been received you should check the Queue folder to see if you can see your message. The electronic mail (.eml file extension) files can be opened up with a text editor to view the contents of the message. From there you can turn on logging on the virtual server to see the outbound connection attempts to deliver the message. If all else fails use Network Monitor to ensure that SMTP is able to make an outbound connection.

Self Test

1. You have been asked to set up a secure FTP connection to receive confidential data from a business partner using FTP and SSL. After installing IIS with the FTP Publishing Service, you cannot find how to enable secure communications on the FTP site in IIS 6 Manager. What should you do?
   A. Obtain a new SSL certificate and add it using IIS Manager
   B. Ensure port 21 is not being used by another Web site or ftp site
   C. Install the Web version of the FTP Publishing Service
   D. You can't secure FTP communications
2. You need to set up several FTP sites on a single IP address. Using the FTP Publishing Service support for virtual hosts you have configured ftp.contoso.com, ftp.fabrikam.com, and ftp.woodgrove.com. When users attempt to log in, their account is not being recognized. How should you approach the problem?
   A. Reset the user's password
   B. Ask the users to try a different FTP client
   C. Ask the users to use the hostname|username format to ensure that they are connecting to the appropriate host
   D. Restart the application pool hosting each of the virtual hosts
3. You received a support call from a user trying to upload a file to the site. They are able to connect, authenticate using their network account, and browse the folder structure, but unable to upload a file. Where should you look?
   A. Ensure the FTP authorization rule includes Write permissions
   B. Ensure the anonymous module is disabled
   C. Change the port number the site is bound on
   D. Ensure that the passive data connection ports are accessible from the user's computer
4. You have recently set up an FTP site with a virtual directory that links to a network share where video journalists can upload their video. The authorization rules have been configured to allow only write access to this folder. When you logged in to the FTP site and attempted to change to the folder the server said that it was unable to change to the folder. How should you resolve the problem?

A. Remove and re-create the authorization rule

B. Write a batch file to copy the content to the network share on a regular basis

C. Configure the virtual directory to use a set of credentials to connect to the remote share

D. Turn on FTP Site logging and review the logs

5. An ISP has contacted you for guidance on enabling their Web hosting clients' access to their content using FTP. After reviewing their plans you have determined that they want an easy-to-maintain solution that minimizes the maintenance involved with maintaining the FTP access. What solution should you recommend?

   A. Set up the FTP Site to use a User Name Directory

   B. Set up User Isolation using Virtual Directories that link to the Web site

   C. Bind the FTP Site to the Web Site in IIS Manager

   D. Create a standalone FTP Site for each client that points to the location of the Web content

6. After setting up your new FTP site you need to enable FTP access to the server. The computer runs Windows Firewall and you are using the Passive FTP mode. What ports should you open up?

   A. 21/tcp and 1024-65535/tcp

   B. 21/udp and 1024-65535/tcp

   C. 21/tcp and the range specified in the Firewall Settings module

   D. Add a Program Exception for SvcHost.exe using FtpSvc as the service identified

7. Users accessing your FTP site have reported that they cannot see the virtual directory that you recently created. You can see that the virtual directory does exist and is set to the proper path through IIS Manager. What should you do to enable users to see the virtual directory?

   A. Disable the Anonymous Authentication Module

   B. Enable UNIX Directory Listing Style in the Directory Browsing module

   C. Enable Virtual Directories in the Directory Browsing module

   D. Change the incoming connections to require SSL

8. The new FTP Publishing Service introduces the ability to use SSL to protect the privacy of the connection. Where can SSL not be applied on an FTP session?

   A. SSL on the Control Channel

   B. SSL on the Control Channel during Authentication

   C. SSL on the Data Channel

   D. SSL on the Data Channel during Authentication

9. After a recent security audit you have been asked to disable anonymous authentication on your FTP site. What is the most secure option available using the authentication modules that are shipped with the FTP Publishing Service?

   A. Basic

   B. Windows

   C. Digest

   D. Client Certificate

10. You have installed SMTP Server to receive mail from outside users as well as let remote users authenticate and relay through. A user calls you telling you that their ISP has blocked port 25 and recommends using port 465 instead. What should you do to enable the user to connect?

    A. Create a new virtual server bound to port 465

    B. Add a port binding to the existing virtual server

    C. Add the user's IP address to the relay restrictions allow list

    D. Ask the user to use another SMTP Server

Self Test Quick Answer Key

1. **C**
2. **C**
3. **A**
4. **C**
5. **C**
6. **D**
7. **C**
8. **D**
9. **A**
10. **B**