Security

8

IN THIS CHAPTER

What's New

Security has always been a concern for Exchange administrators. Since the introduction of Exchange 5.5, the tools for securing the Exchange platform have grown with every release of Exchange and the Windows Server operating system in general.

In Exchange 2003, security is a vital concern, and much time and effort have been placed on getting the security right from the start.

From the "secure by design" operating system to full support for Kerberos authentication for both servers and clients, Exchange 2003 provides a tough set of security features to crack. The most-read section of this chapter is the section on configuring RPC over HTTP, which allows users to access Exchange from Outlook 2003 without using a virtual private network (VPN) or other network.

As you read this chapter, you will learn about these and other security features that are new to Exchange 2003, as well as some security aspects you might have overlooked with Exchange 2000 implementations. If you are serious about providing a secure messaging and collaboration platform, this is a good place to start.

Server Security Enhancements

One of the key areas where security administrators can really make a difference when working with Exchange is with the security of the servers. Aside from the normal security concerns (physical access, passwords, and so on), several security concerns are specific to deploying

Exchange servers. The following sections examine some of the enhancements in Exchange 2003 that make it easier to secure your messaging and collaboration platform.

Operating System

A good place to start looking at server security is with the underlying operating system. Although Exchange 2003 can run on Windows 2000 servers, security enhancements have been made in Windows 2003 Server that benefit Exchange administrators. These benefits aren't necessarily specific to Exchange, but Exchange administrators will leverage them to provide a secure server platform.

When you're installing Exchange 2003 on Windows 2003 Server, you can be assured that all the security enhancements made with this operating system release are filtered through to Exchange. By default, Windows 2003 Server provides a secure, scalable platform for Exchange through Microsoft's new mantra of "secure by design." Microsoft's mantra ensures that only required features are enabled when you first install and configure the operating system.

For Exchange administrators, this means less avenues for attack or exploitation of Exchange servers. This includes direct attacks against the servers as well as attacks using applications that run on the servers, including Outlook Web Access (OWA).

SECURITY FEATURES IN WINDOWS 2003 SERVER
For more information on the security features in Windows 2003 Server, pick up a copy of the *Windows Server 2003 Delta Guide* (ISBN 0-7897-2849-4), also from Sams Publishing.

SSL Security

With previous versions of Exchange, administrators had a decision to make when it came to deploying OWA, the Web-based client for Exchange. Although the ability to access email remotely was appealing, the functionality that was provided was far below what was offered in the full Outlook client, and there were serious security concerns about deploying a Web-based client for Exchange.

With the introduction of a newly updated version of OWA that is on a rough parity with the full Outlook 2003 client, mail administrators will want to take a second look at deploying this Web-based client for Exchange.

OWA
Because this chapter is dedicated to Exchange security, it doesn't cover the features included in OWA. For more information on that, check out **Chapter 10, "Other Exchange Clients," page 127.**

Because OWA is installed and configured by default with Exchange 2003, administrators now have a robust Web client for Exchange that is easy to deploy and use. Although the updated OWA provides a host of new features for Exchange users, some of the same security concerns have persisted from previous versions.

If you are thinking about deploying OWA, the configuration and use of Secure Sockets Layer (SSL) encryption should be at the top of your security checklist. This security measure was also available for Exchange 2000 and its implementation of OWA; however, if you chose not to deploy OWA within your organization, you probably haven't run across it as an administrator.

As a user, you have probably been to numerous Web sites or e-commerce sites that were secured using SSL, where the padlock appears in the bottom-right corner of your browser or the address is prefixed by `HTTPS://` (instead of `HTTP://`), indicating that the Web site or store is secure.

Because OWA is installed by default with Exchange 2003, you will want to configure SSL to provide a secure interface to OWA and secure communications between front-end servers that connect to the other servers in your Exchange topology. This section looks at some of the steps required to use SSL in your Exchange implementation.

First, you need to have a Server Certificate to enable SSL. A Server Certificate is a virtual document that is available from a Certification Authority (CA). You can use a commercial CA, such as Thawte or VeriSign, or you can use an internal CA that your company maintains. This CA collects information from you, including details about your organization, and issues a certificate that serves as verification that you are who you say you are. This same certificate makes it possible to create a secure connection between two computers, using encryption keys to ensure that the information being sent across the wire is confidential and hasn't been tampered with.

To obtain a certificate, it's easiest to request one from a commercial CA. You could create your own certificate, but most browsers are already programmed to trust certificates that are issued by commercial CAs, eliminating those annoying pop-up messages every time you want to access a Web site.

Luckily, the process of requesting a server certificate from a CA has been streamlined through the use of a wizard. This wizard collects information about your organization and submits it to the CA. To obtain a server certificate, follow these steps:

1. On the server, open the Internet Services Manager from the Administrative Tools group.
2. Locate the EXCHWEB Web site beneath the Default Web Site node. Then right-click on the Web site and select its properties.
3. Click on the Directory Services tab and click the button marked Server Certificate to open the Server Certificate Wizard. Then click Next to open the dialog box shown in Figure 8.1.

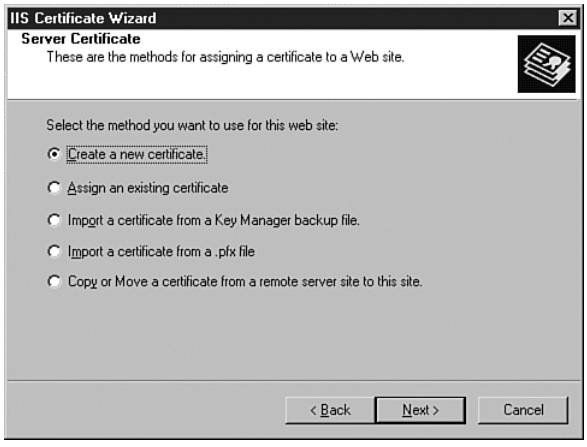

FIGURE 8.1 Server Certificate Wizard.

4. Select the option Create a New Certificate and click Next to proceed to the next step of the wizard.
5. Select the option Prepare Request Now But Send Later and click Next to proceed.
6. Using the dialog box shown in Figure 8.2, enter a name for your certificate, as well as `1024` for the bit length. Click Next to proceed.

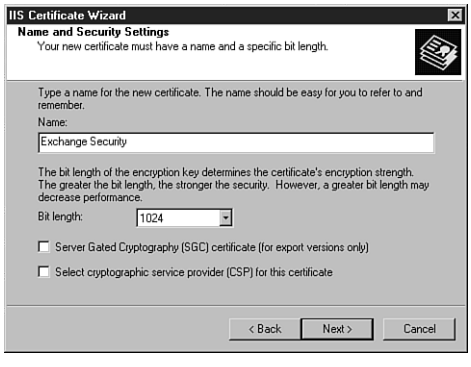

FIGURE 8.2 Certificate name.

7. Enter the name of your organization and organizational unit. The organization name should be your legal trading name (that is, “Orion Mining, LLC”), and the organizational unit should be something that describes your particular area within that organization (that is, “Mining Operations.”)
8. Enter the DNS name for your server. This should be the name of the front-end server that you are using for Exchange OWA that is exposed to the Internet.

ISA SERVER
If you are using ISA Server with Exchange in a firewall/DMZ setup, this should be the name of the ISA server. Check your ISA Server documentation for how to request and implement a server certificate on this platform. For more information on implementing ISA server, including different deployment scenarios you can use with Exchange 2003, visit `http://www.microsoft.com/isa`.

9. Enter your geographical information, including your country, state, city, and so on. Then click Next to proceed.
10. Finally, enter a filename and location for your certificate request.

After you have created this request, you can send it on to a CA (`http://www.verisign.com`, `http://www.thawte.com`, and so on), who will then check your credentials and, upon the payment of a fee, issue you a server certificate. (The timeframe for this could be anywhere from the same day to a few weeks' time.) With your certificate in hand, it is time to do a little more configuration work to make Exchange secure.

To use your Server Certificate to secure Exchange, follow these steps:

1. On the server, open the Certificate Manager from the Administrative Tools program group.
2. Install and configure your Server Certificate using the instructions that your Certificate Authority provides.
3. Open the Internet Services Manager from Administrative Tools and select the Web server you want to secure.

INDIVIDUAL WEB SITES
You could also use this same process to secure specific virtual folders within your Web site. However, Exchange provides several different access methods (OWA, Outlook Mobile Access [OMA], and so on) that are exposed through IIS, so it is best to secure the entire Web site using SSL.

4. Click on the Directory Services tab and click the button marked Edit under Secure Communications. Then select the option Require Secure Channel (SSL).

Now whenever users want to access OWA or other Exchange client applications that are exposed through IIS, they will use the `HTTPS://` prefix, which provides a secure SSL connection.

Kerberos Authentication

Exchange 2003 now also supports Kerberos authentication, which allows information sent between Exchange servers to be secured. If you worked with a multiserver architecture in previous versions of Exchange, you are probably already aware of the inherent security issues, including the passing of user credentials between front-end and back-end servers using Basic authentication.

This authentication method posed a severe security risk for Exchange. Hackers could "sniff" the connection between the servers and work out the credentials from there. This meant that for previous Exchange implementations, you also had to apply IPSec security to the communications between servers to encrypt the information being sent between them. Often, administrators overlooked this security concern, leaving many organizations unaware that there was a potential security risk.

With the introduction of Exchange 2000, NTLM was used as the default authentication protocol between servers. The primary reason for not using Kerberos was the lack of support for the protocol when using clustered servers.

Since Windows 2000 Server SP3, Kerberos authentication is now fully supported for single and clustered servers, meaning that any information or credentials that are passed between servers are secure. This eliminates the vulnerability of "sniffing" or "listening" in on the traffic between the two servers. By default, Kerberos is enabled whenever you add multiple servers to your Exchange topology.

KERBEROS AUTHENTICATION
For more information on how Kerberos authentication works, check out `http://www.microsoft.com/security`.

RPC Over HTTP

As email has grown to be one of the primary methods of business communication, enabling users to access their email remotely has become a priority. With an updated version of OWA, users have a rich email client that is approaching the full set of features and functionality found in Outlook 2003. However, some features are available only in the full Outlook client.

The good news is that with Exchange 2003 and RPC over HTTP, you can allow remote users to use the full Outlook 2003 client to access their email without setting up a VPN or other facility.

Remote Procedure Call (RPC) is one of the protocols that Exchange supports for client connections. To use RPC over HTTP, you need to configure one of your Exchange front-end servers to act as an RPC proxy server.

You can then expose this server to the outside world and allow users to connect through it. Alternatively, you can use Microsoft ISA Server to route requests through your firewall or perimeter network.

> **MICROSOFT ISA SERVER**
> For more information on installing and configuring Microsoft ISA Server, check out `http://www.microsoft.com/isa`.

Outlook 2003 supports RPC over HTTP. However, you need to upgrade your user's operating system to Windows XP, SP1 and apply Windows Update 331320 (available from `http://windowsupdate.microsoft.com`) to use this feature.

To configure RPC over HTTP using your existing Exchange front-end servers, follow these steps:

1. From the Control Panel, select Add/Remove Programs and then Add/Remove Windows Components. From Networking Services, install the RPC over HTTP protocol.
2. In the IIS Manager, locate the RPC virtual directory and select its properties from the shortcut menu, shown in Figure 8.3.

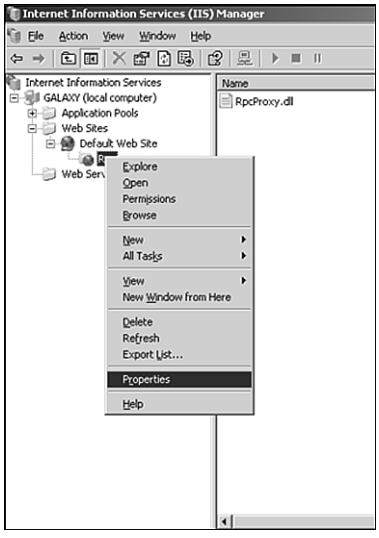

FIGURE 8.3 Virtual directory properties.

3. Open the Directory Security property page and edit the Authentication and Access Control settings to select Basic Authentication.

4. Edit the registry and locate the HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\RpcProxy key.
5. Modify the ValidPorts key and add the following identifiers and ports, separated by a semicolon as shown here:

   ExchangeServer:593;
   ExchangeServerFQDN:593;
   ExchangeServer:6001-6002;
   ExchangeServerFQDN:6001-6002;
   ExchangeServer:6004;
   ExchangeServerFQDN:6004;
   GlobalCatalogServers:593;
   GlobalCatalogServersFQDN:593;
   GlobalCatalogServer:6004;
   GlobalCatalogServerFQDN:6004

   CONFIGURING PORTS
   Replace the previous placeholders with the name and fully qualified domain name of the servers in your Exchange topology.

6. On your Global Catalog Server, edit the registry and locate the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters key.
7. Add a new key (multistring) and name it `NSPI interface Protocol Sequences`.
8. Modify the key you have just created and add the value **ncacn_http:6004**.

To configure Outlook 2003 to communicate via RPC over HTTP, follow these steps:

1. From the Control Panel, open the Mail control panel. Then create a new profile.
2. Add a new email account, selecting Exchange as your server type. Enter the name of your Exchange back-end server (*not* your Exchange front-end server).
3. Click the More Settings button and select the Connection property page shown in Figure 8.4. Then select the option Connect to My Exchange Mailbox Using HTTP.
4. Select the Exchange Proxy Settings property page, shown in Figure 8.5. Under Connection Settings, enter the name of your Exchange front-end server in the text box marked Use This URL.
5. Check the options for Connect Using SSL Only and Mutually Authenticate.

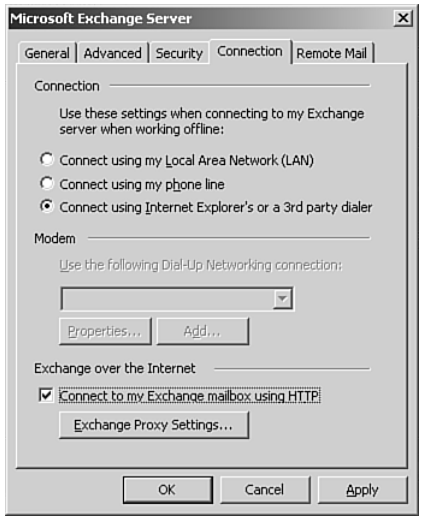

FIGURE 8.4 Outlook connection settings.

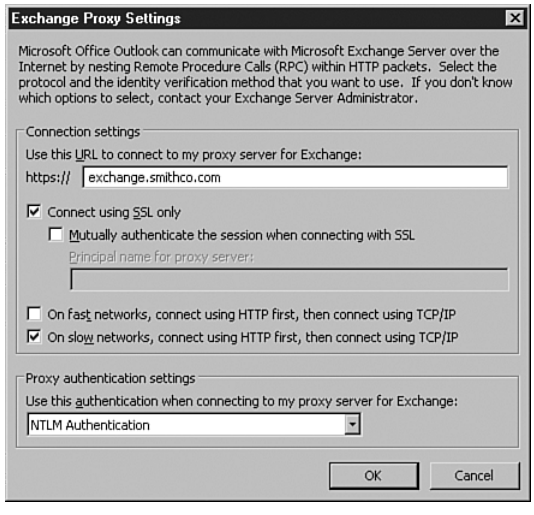

FIGURE 8.5 Proxy settings.

6. In the text box marked Principle Name for Proxy Server, enter the fully qualified domain name of your Exchange front-end server, prefixed by **msstd:** (that is, msstd:exch.orion.com).
7. Change the Proxy Authentication Settings to use basic authentication.

Your Outlook client is now ready to communicate with Exchange using RPC over HTTP.

WORKING WITH MICROSOFT ISA SERVER

There are two critical areas where Microsoft ISA Server can be implemented alongside Exchange to increase security. The first is RPC over HTTP, which was already examined. You can place an ISA Server within the demilitarized zone (DMZ) or outside your firewall to handle RPC requests and route these requests back to your Exchange front-end servers.

Second, for securing OWA implementations, you can configure ISA as a proxy to an Exchange front-end server, eliminating the need to expose a front-end server to the rest of the world. Using ISA Server, you can use a special publishing wizard for OWA to configure a proxy to your Exchange front-end servers. This eliminates the need to open multiple ports to the outside world and provides a more secure implementation method for OWA.

Cross-Forest SMTP Authentication

Another real security concern is the process called *spoofing*, in which a hacker or other user who has malicious intent pretends to be a valid Exchange user and sends email messages as if they were from that user. Identity theft is on the rise, and spoofing provides an easy method for hackers to obtain sensitive information from users within and outside of your organization.

Most people don't look at the email address when they reply to a message. If the email appears to have come from a trusted source, users are likely to use the Reply button to respond to it. This address is usually not the correct reply email address either.

To ensure that malicious users do not spoof emails or send emails that appear to be from someone within your organization, Exchange 2003 provides tools and methods for combating this security risk.

First, Exchange 2003 requires authentication before it verifies a sender's name. In this scenario, a malicious user could try to send an email with a fake From address, but this email message would not go through until the user had been authenticated on Exchange and the name presented was checked against the global address list.

Although this provides an end to spoofed email messages, it can also cause problems when you have an Exchange topology that spans multiple forests. Remember from the architecture discussions in Chapter 2, "Architecture," that an Exchange organization can only span a single forest. If you have multiple Exchange organizations running in multiple forests, there is no authentication of the user and no way to check the sender address before sending an email message.

To make this particular security feature work in a multiple-forest topology, you need to configure all the forests involved so that you can authenticate the user and check the sender address before sending an email message. This works through *cross-forest SMTP authentication*.

The basic premise behind this setup is that you will configure an SMTP connector between each of the forests that is used to authenticate and check the user that is sending the email message against the appropriate global address list.

WEB RESOURCE

For detailed instructions on configuring cross-forest SMTP authentication, go to the Delta Guide series Web site at `http://www.deltaguideseries.com` and enter article ID A030801.

Client Security Enhancements

In addition to security improvements for Exchange servers, enhancements have been made to security of the clients that access Exchange, including Outlook 2003, OWA, OMA, and so on.

Although this book examines the functionality included in these different clients in Chapter 10, this chapter also looks at some of the new security features so that you can understand some of the new security features and functionality as you are thinking about deploying these clients.

Windows Rights Management

One of the most exciting enhancements to Outlook 2003 and the Microsoft Office System 2003 in general is the introduction of rights management, through Windows Rights Management Service. This feature is new with Office 2003 and requires Windows Server 2003 to work.

Rights management is based on the concept that you can assign a security policy to a particular document, which includes emails and attachements. This policy can restrict how the document can be used, including settings to allow/disallow viewing the document, copying, printing, saving, and forwarding.

In addition to internal users who might be using Office 2003, the rights management policies can be enforced with external users. A plug-in has been provided for Internet Explorer so that you can view rights-managed documents.

WINDOWS RIGHTS MANAGEMENT SERVER

For more information on rights management within Outlook 2003 or the Windows Rights Management Server, check out `http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/rmenterprise.mspx`.

Kerberos

The "Server Security Enhancements" section of this chapter looked briefly at how the Kerberos protocol was being used to make secure connections between servers. You can also use the Kerberos protocol to make a secure connection between Outlook 2003 and Exchange 2003. In addition to providing a secure connection, Kerberos enables cross-forest authentication in forests that are running their domain controllers using Windows Server 2003, allowing the separation of Exchange users and Exchange servers.

This separation has a significant impact on the configuration of your Exchange topology and could be used to provide a "hosted" email solution to other organizations or to simplify or effectively outsource Exchange administration.

S/MIME

Finally, one of the most commonly requested security features for Exchange has been implemented in this release for OWA and OMA. Secure/Mime (S/MIME) has been the industry standard for sending secure email messages. S/MIME was originally based on the RSA public-key encryption technology.

With the release of Exchange 2003 and Outlook 2003, you can now send secure email messages using S/MIME from the full Outlook client, OWA and OMA, eliminating the need for a special add-in or third-party tool and making secure messaging with other platforms and clients a reality.

WEB RESOURCE

For configuring S/MIME with Exchange 2003, go to the Delta Guide series Web site at `http://www.deltaguideseries.com` and enter article ID A030802.