

Microsoft®

Using ISA Server 2000 with Exchange Server 2003



Product Version: Exchange Server 2003
Reviewed by: Exchange Product Development
Latest Content: www.microsoft.com/exchange/library
Author: Exchange Documentation Team

 **Windows Server System**

Microsoft®

Using ISA Server 2000 with Exchange Server 2003

Joey Masterson

Published: October 2003

Applies to: Exchange Server 2003

Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

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

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, ActiveSync, MSDN, Outlook, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

Acknowledgments

Project Editor: Cathy Anderson

Contributing Editors: Alison Hirsch

Technical Reviewers: Brendan Power, Jim Harrison, Allen Atwood, Nathan Bigman

Graphic Design: Kristie Smith

Production: Joe Orzech, Sean Pohtilla

Table of Contents

Introduction.....	1
ISA Server 2000 and Exchange Server 2003.....	1
Permissions for Deploying ISA Server	3
Configuring ISA Server and Exchange.....	4
Test Prior to Deploying in Your Production Environment	4
Step 1: Deploy ISA Server 2000.....	5
Step 2: Move the ISA Server into the Perimeter Network.....	10
Step 3: Configure Inbound and Outbound Internet Mail Through ISA Server.....	12
Step 4: Configure Your Server Architecture and SSL.....	20
Step 5: Configure ISA Server for Outlook Web Access.....	26
Step 6: Configure RPC over HTTP for Outlook 2003.....	33
Step 7: Configure Outlook Mobile Access.....	36
Step 8: Configure Exchange ActiveSync	38
Step 9: Configure Access for IMAP4 and POP3 Clients	41
Additional Resources.....	43
Websites	43
Exchange Server 2003 Books.....	44
Microsoft Knowledge Base Articles.....	44

Introduction

Microsoft® Internet Security and Acceleration (ISA) Server 2000 and Microsoft Exchange Server 2003 are designed to work closely together in your network environment to provide a more secure messaging environment than previous versions of Exchange. When you use ISA Server to handle all inbound requests from client applications such as Microsoft Office Outlook® 2003 and Outlook Web Access, your Exchange front-end servers no longer need to be located in the perimeter network.

This article describes how to deploy ISA Server 2000 with Service Pack 1 (SP1) and Feature Pack 1 as your advanced firewall server to protect your messaging environment. This article does not explain how ISA Server functions or its underlying technologies. Additionally, you must familiarize yourself with ISA Server and fully test ISA Server in a test environment before deploying ISA Server in your corporate infrastructure.

ISA Server 2000 and Exchange Server 2003

ISA Server acts as an advanced firewall that controls Internet traffic entering your internal corporate network and outbound communication from your messaging environment. When you use ISA Server in place of an Exchange front-end server, you can locate all your Exchange Server 2003 servers within your corporate network, and use ISA Server as the advanced firewall server exposed to Internet traffic in your perimeter network.

Note

Although you remove your Exchange front-end servers from the perimeter network, they still act as front-end servers in your corporate network.

All inbound Internet traffic bound to your Exchange servers, such as Microsoft Office Outlook® Web Access, RPC over HTTP communication from Microsoft Office Outlook 2003 clients, Outlook Mobile Access, Post Office Protocol version 3 (POP3), Internet Message Access Protocol version 4rev1 (IMAP4), and so on are processed by ISA Server. When ISA Server receives a request from a client application such as Outlook 2003 to access information on an Exchange server, ISA Server routes the request to the appropriate Exchange servers on your internal network. The internal Exchange servers return the requested data to ISA Server, and then ISA Server sends the information to the client through the Internet. Figure 1 shows an example of this type of deployment.

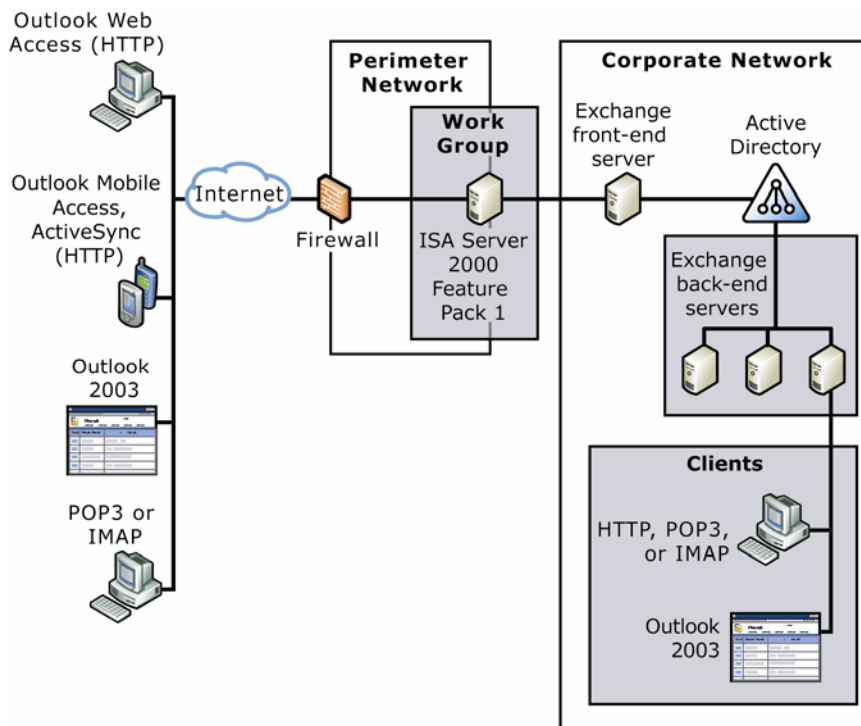


Figure 1. Deploying ISA Server as your advanced firewall server

Permissions for Deploying ISA Server

Table 1 lists the necessary permissions to complete the procedures in this article.

Table 1 Procedures and required permissions or roles

Procedure	Required permissions or roles
Deploy ISA Server 2000	Local administrator
Move the ISA Server into the perimeter network	Not applicable
Configure inbound and outbound Internet mail through ISA Server	Local administrator
Configure your server architecture and Secure Sockets Layer (SSL)	Local administrator
Configure ISA Server for Outlook Web Access	Local administrator
Configure RPC over HTTP for Outlook 2003	Local administrator
Configure Outlook Mobile Access	Local administrator
Configure Exchange ActiveSync®	Local administrator
Configure access for IMAP4 and POP3 clients	Local administrator

Configuring ISA Server and Exchange

This section focuses on the necessary steps to configure ISA Server 2000 and Exchange Server 2003. Although information about how to configure ISA Server is provided, this article assumes you are familiar with ISA Server and that you understand the basic ISA Server concepts, including planning, deployment, and administration.

- Step 1: Deploy ISA Server 2000
- Step 2: Move the ISA Server computer into the perimeter network
- Step 3: Configure inbound and outbound Internet mail through ISA Server
- Step 4: Configure your server architecture and SSL
- Step 5: Configure Outlook Web Access
- Step 6: Configure RPC over HTTP for Outlook 2003
- Step 7: Configure Outlook Mobile Access
- Step 8: Configure Exchange ActiveSync
- Step 9: Configure access for IMAP4 and POP3 clients

You should complete these steps in the order provided; however, if you do not require a specific configuration, skip that step. For example if you do not plan to allow POP3 access from the Internet, you can skip the step that discusses allowing POP3 traffic.

Test Prior to Deploying in Your Production Environment

The steps in the following sections describe what you do when you deploy ISA Server in your production environment. However, before deploying ISA Server in production, you should thoroughly test it in a non-production, test lab environment. In addition to lab testing, and to minimize service disruption to users, you may want to stage your production rollout so that you do not move servers out of the perimeter network until you verify that ISA Server is working properly.

If you decide on a phased rollout, the overall approach you will take is to deploy ISA Server in the perimeter network, and then add support for specific Exchange functionality one at a time, testing as you go. After you verify that a specific service is working through ISA Server, move the current Internet-facing server handling that service out of the perimeter network and switch to using ISA Server to route the relevant traffic to servers on your internal network.

For example, after you configure ISA Server as the proxy server for inbound Simple Mail Transfer Protocol (SMTP) traffic, test the inbound mail traffic through ISA Server and make sure

it is getting to the back-end Exchange servers. Then, bring up a temporary inbound SMTP server on the internal network, create a mail exchanger (MX) resource record for a new test address space (such as @test.example.com) in your external Domain Name System (DNS) to point to the ISA Server computer, and create a Recipient Policy for the test address space in Exchange. After you verify that inbound mail to users is working with the test address, you can move your current SMTP front-end server out of the perimeter network and point your primary MX record to the Internet Protocol (IP) address of your ISA Server computer.

Note

The following steps are for your production rollout of ISA Server. Modify them as needed to thoroughly test the functionality in your test environment.

Step 1: Deploy ISA Server 2000

Before you deploy ISA Server in the perimeter network and start moving other servers back into your internal network, you need to install ISA Server on a dual-homed server (a server with two network cards). Review your ISA Server documentation for specific installation steps. There are a few guidelines to be aware of when installing ISA Server for Exchange 2003 support. Install ISA Server using the configuration detailed in the following sections.

Important

After you install ISA Server, and before you deploy ISA Server as the advanced firewall server for your messaging environment, make sure you install all updates and security patches.

Moving the Server to a Workgroup

Before you install ISA Server on your server, remove the server from any domains that it is a member of and place it in a workgroup. Install ISA Server as a stand-alone firewall server and not as part of an ISA Server array (which requires domain membership). You do not want ISA Server to run on a member server in your Microsoft Windows® forest because, if the server is compromised by attacks from the Internet, the attackers can gain access to domain resources. In addition, minimize the number of ports open to your internal network. Member servers require additional ports for activities such as talking to domain controllers.

Installing ISA Server in Firewall Mode

When you use ISA Server with Exchange, you do not need to use the caching features in ISA Server because the data that users access through their Web browser, such as mail using Outlook Web Access, is dynamic and constantly changing. Therefore, install ISA Server in firewall mode. Note that, if you do want to use the caching features in ISA Server (for example, if you will also be publishing an e-commerce site through ISA Server), you can install ISA Server in integrated mode. However, the data compression feature in Outlook Web Access cannot be used if you are using the caching features in ISA Server. If you want to use data compression, and your ISA Server is using caching, you must specify a routing rule to disable caching for Outlook Web Access. Figure 2 shows the modes you can use to install ISA Server.

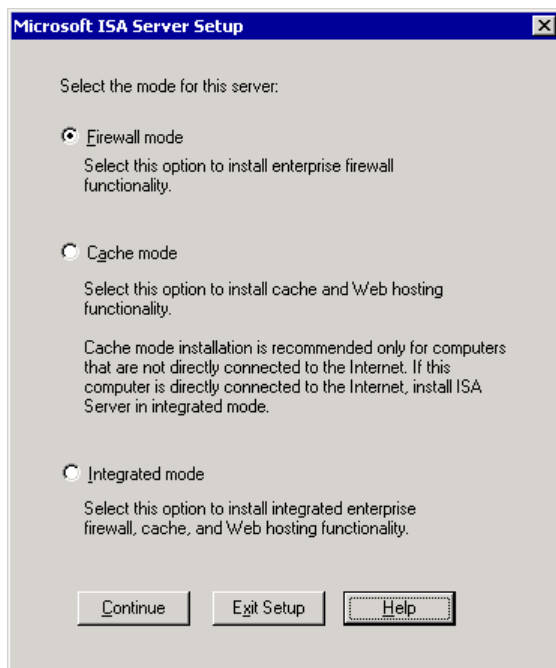


Figure 2 Installing ISA Server in firewall mode

Constructing the Local Address Table

During the ISA Server setup, make sure to enter the full range of IP addresses for your internal network and to construct the local address table (LAT) (Figure 3). The LAT provides ISA Server with the IP addresses that are external to your network and that should be processed by the ISA Server.

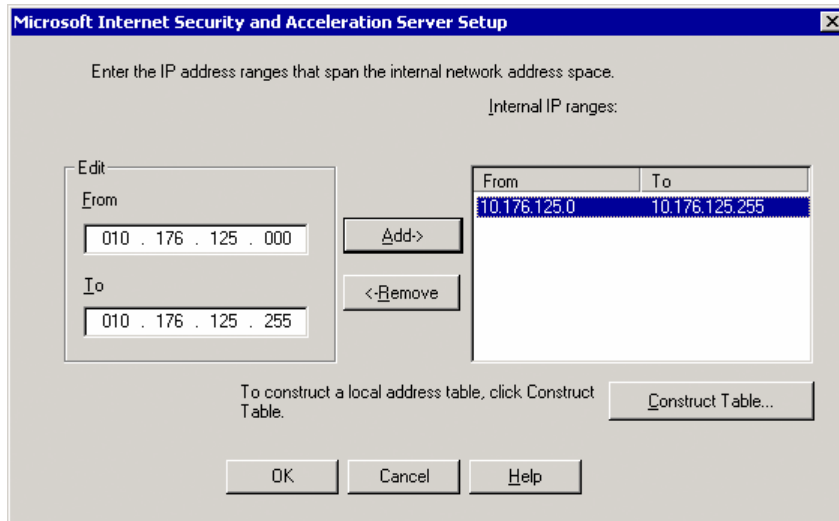


Figure 3 Constructing the local address table (LAT) during ISA Server setup

Selecting the Network Interface Card

When you construct the LAT during setup, make sure you select the internal network interface card (NIC) and not the external NIC (Figure 4). If you select the external NIC, ISA Server treats your Internet IP address as part of your internal network and ignores any traffic coming in from the Internet on that IP address.

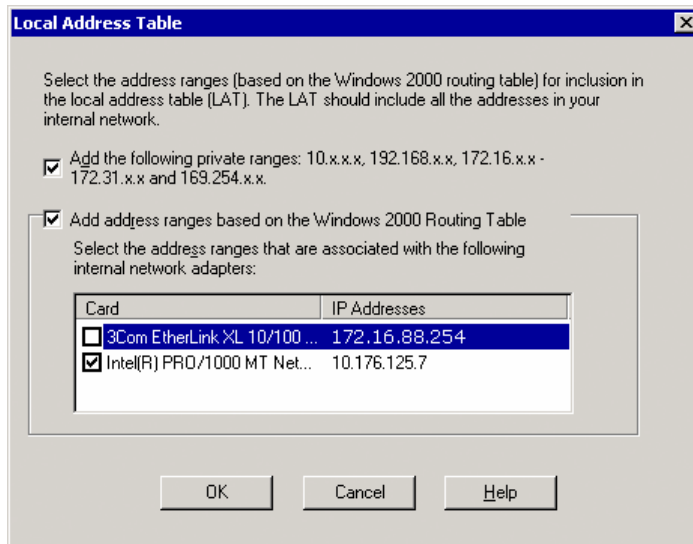


Figure 4 Selecting NICs in the local address table (LAT)

Installing Updates

Before you connect ISA Server to your corporate network, make sure you install the updates and security patches listed in Table 2.

Table 2 Download locations of updates and security patches for ISA Server

Type of download	Download location
ISA Server 2000 Service Pack 1	<ul style="list-style-type: none"> • http://go.microsoft.com/fwlink/?LinkID=18918
ISA Server 2000 Feature Pack 1	<ul style="list-style-type: none"> • http://go.microsoft.com/fwlink/?LinkID=18917
ISA Server 2000 downloads website	<ul style="list-style-type: none"> • http://go.microsoft.com/fwlink/?LinkID=18919
Microsoft security information	<ul style="list-style-type: none"> • Microsoft security website (http://www.microsoft.com/security) • TechNet security website (http://go.microsoft.com/fwlink/?LinkID=5936)

Install Service Pack 1 for ISA Server

After you finish installing ISA Server, install ISA Server 2000 Service Pack 1 (SP1). Note that this update is different from Feature Pack 1.

For more information about obtaining ISA Server 2000 SP1, see the ISA Server Downloads page (<http://www.microsoft.com/fwlink/?LinkID=18918>). Download the Isasp1.exe file to your server, and run it on the ISA Server computer.

Install ISA Server Updates for Windows Server 2003

If you install ISA Server on a computer running Microsoft Windows Server™ 2003, you need to apply a set of required updates to ISA Server after you install ISA Server SP1.

For more information about these updates and the download location, see Microsoft Knowledge Base article 331062, "Running ISA Server on Windows Server 2003" (<http://go.microsoft.com/fwlink/?linkid=3052&kbid=331062>).

Install ISA Server Feature Pack 1

ISA Server 2000 Feature Pack 1 provides many enhanced features to help secure your messaging environment. The following features are included with ISA Server Feature Pack 1:

- Enhanced SMTP filter
- Enhanced Exchange remote procedure call (RPC) filter
- URLScan 2.5 for ISA Server
- Web authentication for RSA SecurID
- Delegation for RSA SecurID and basic authentication
- Outlook Web Access Wizard
- RPC Filter Configuration Wizard
- Link Translator
- Scenarios and troubleshooting documentation

Install ISA Server Feature Pack 1 to obtain these features for your ISA Server. After you finish installing ISA Server Feature Pack 1, you can proceed with deploying ISA Server to secure your messaging environment.

Install ISA Server Security Patches

To protect your ISA Server from potential security risks, download and install the ISA Server security updates and patches. For information about the latest security updates and patches, see the Microsoft TechNet security website (<http://www.microsoft.com/fwlink/?LinkID=5936>).

Step 2: Move the ISA Server into the Perimeter Network

After you install ISA Server 2000 SP1, Feature Pack 1, and the security updates on a server, you are ready to move it into your perimeter network and connect the server to both the Internet and your internal network.

Obtaining an External IP Address for ISA Server

Your external NIC needs an Internet IP address to which Internet traffic can connect. Obtain an Internet IP for the external NIC, and configure it in the TCP/IP settings.

If you already manage your own external DNS, consider using the IP address assigned to your Internet domain's name server. Using this IP address allows you to move your external DNS server back to the internal network and to use ISA Server to forward DNS requests from the Internet. If you obtain a separate IP address for ISA Server and then move your external DNS servers back to the internal network, you need to update your name server records at your Internet registrar to point to the new ISA Server IP address.

Configuring Incoming Web Page Requests to Use an External IP Address

After you set the external NIC on the ISA Server computer to use an Internet IP address, you need to configure ISA Server to listen on that IP address for incoming Web requests. This configuration is necessary for ISA Server to respond to Web page requests such as Outlook Web Access or Outlook Mobile Access traffic.

To configure ISA Server to listen for incoming Web requests

1. Open the ISA Server management console: Click **Start**, point to **All Programs**, and then click **ISA Management Console**.
2. In the ISA Server management console, open the ISA Server properties page.

3. On the **Incoming Web Requests** tab, select **Configure listeners individually per IP address** and verify that the IP address listed is your external IP address (Figure 5).

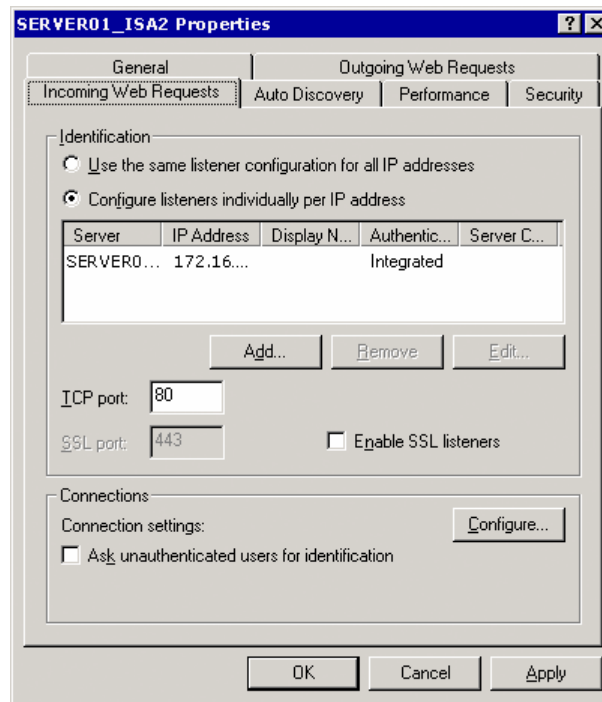


Figure 5 Configuring ISA Server to listen for Web requests on the Internet IP address

Note

After you add an incoming Web request listener, you need to restart the Web proxy service for ISA Server.

Using a Static Internal IP Address

Make sure the IP address of the ISA Server computer's internal NIC is static. This configuration is necessary because you need to configure secure network address translation (SecureNAT) clients, such as your inbound SMTP server, and point them to the internal IP address of your ISA Server. If the IP address on your internal NIC changes, you need to manually update those clients. When you use a static IP address, you avoid this problem.

After your ISA Server computer is connected to both the Internet and your internal network, it can start regulating inbound and outbound Internet traffic.

Step 3: Configure Inbound and Outbound Internet Mail Through ISA Server

After you place your ISA Server computer in the perimeter network and configure your internal and external NICs, ISA Server is ready to start acting as the gatekeeper for inbound and outbound Internet traffic. To do this, you need to configure inbound and outbound e-mail traffic to go through ISA Server.

Configuring Inbound Internet Mail

When you configure inbound Internet mail, you configure ISA Server to manage mail from the Internet to your internal users. Instead of your SMTP gateway server receiving inbound mail in the perimeter network, you configure ISA Server to receive the incoming SMTP traffic and forward it to the SMTP server on your internal network.

Update Your MX Record to Point to ISA Server

Most likely, your organization's external MX record points to a host record, which in turn points to the Internet IP address of your SMTP gateway in your perimeter network. You must update the host record in external DNS to point to the external IP address of your ISA Server. You can continue to use the same MX record and host name, but you need to point to a different IP address.

For example, consider the following DNS entry:

```
Mail Exchanger (MX)    [10]    smtp.contoso.com.  
smtp Host (A)        192.168.0.2
```

The MX record points to the host record named **smtp**, which resolves to IP address 192.168.0.2. In this case, you update the IP address of the smtp host record with the new external IP address of the ISA Server .

Move SMTP and DNS Servers out of the Perimeter Network

ISA Server handles all inbound traffic from the Internet. Any existing servers you have connected directly to the Internet or in the perimeter network should be moved to the internal network.

For messaging purposes, the servers that are important are your SMTP gateway and external DNS server. Move these servers out of the perimeter network, and locate them within the internal corporate network. These servers no longer need to be dual-homed servers.

Important

Make sure the IP addresses are static for any server that ISA Server will forward requests for. Because ISA Server is configured to route incoming traffic to specific IP addresses, if the IP address for your SMTP or DNS servers change, inbound mail could stop flowing.

If you are not managing your own external DNS, but instead have it managed by a third party, you do not need to do anything with your external DNS servers.

If you do move your external DNS server into the internal network, update your name server record for your Internet domain to point to the external IP address of the ISA Server computer.

Create Server Publishing Rule for Inbound DNS Traffic

After you move your external DNS server into the corporate network and update the name server record for your domain to point to the ISA Server, you need to configure ISA Server to forward inbound DNS queries from the Internet to your external DNS server, which is now located on your internal network.

In the ISA Server management console, create a new server publishing rule with the settings described in Table 3.

Table 3 Server publishing rule settings for inbound DNS

Setting	Value
Server publishing rule name	Inbound DNS
IP address of internal server	IP address of your external DNS server
External IP address on ISA Server	Internet IP address of external ISA Server NIC
Apply the rule to this protocol	DNS Query Server
Client type	Any request
Apply the rule to requests from	Any request

Figure 6 shows an example server publishing rule for inbound DNS queries.

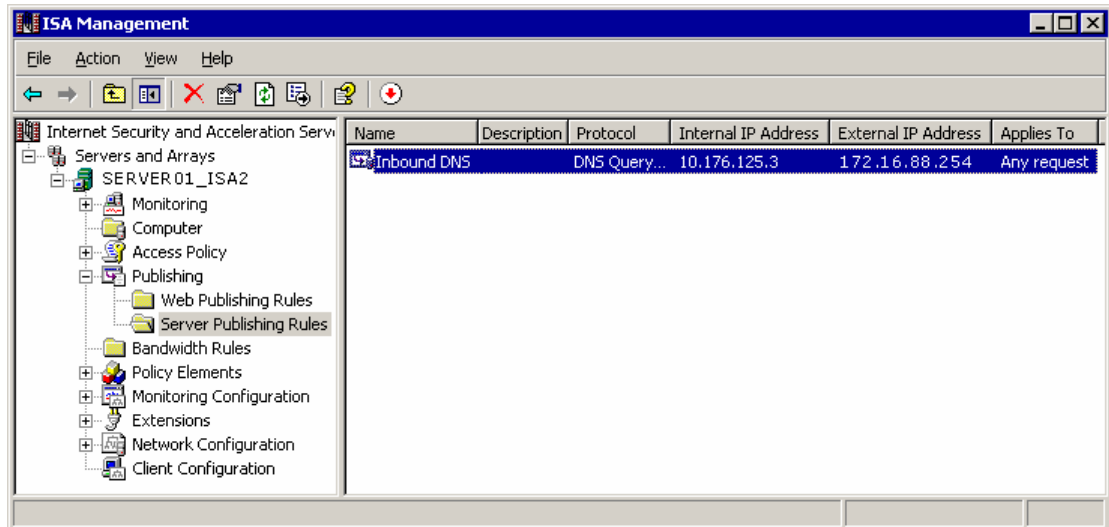


Figure 6 Server publishing rule settings for inbound DNS queries

Configure External DNS Server to Be a SecureNAT Client

If you manage your external DNS server, you need to configure the server as a secure network address translation (SecureNAT) client. SecureNAT clients are computers with a default TCP/IP route to the Internet that goes through the ISA Server. When ISA Server forwards the incoming DNS request from the Internet to your external DNS server, the DNS server needs to be configured as a SecureNAT client to successfully route the response back to the Internet through ISA Server. For the DNS server to be able to route the response, you must set the default gateway on the SecureNAT client to use the IP address of the ISA Server internal NIC.

To configure your DNS server as a SecureNAT client, open the TCP/IP properties page on the server's NIC, and set the default gateway IP address to the IP address of the ISA Server internal NIC.

Note

Pointing to your ISA Server computer internal NIC assumes that your DNS server is on the same network segment as your ISA Server. If you have a routed network and your DNS server is on a different network segment, point the default gateway to a router, and configure the router to route Internet-bound packets to the ISA Server internal IP address.

Figure 7 shows the TPC/IP settings that you need on your external DNS server to configure it as a SecureNAT client.

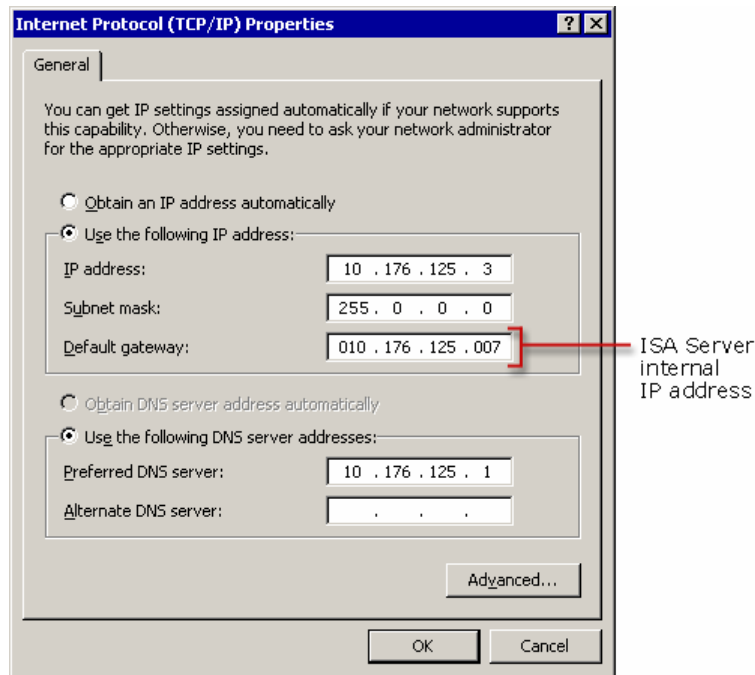


Figure 7 Configuring an external DNS server as a SecureNAT client

Test External DNS from the Internet

Computers with Internet access should now be able to query your external DNS server, even if it is located on the internal network. Test that external DNS queries are working. First, create a new host record on your external DNS server to use for testing (call it dnstest). Next, from a computer connected to the Internet, use a tool such as NSLOOKUP to query dnstest.example.com (where *example* is the name of your domain) and make sure that the query is successful. Remember that the name server IP address you use for the NSLOOKUP query should be the IP address of the ISA Server external NIC.

Create Server Publishing Rule for Inbound SMTP Traffic

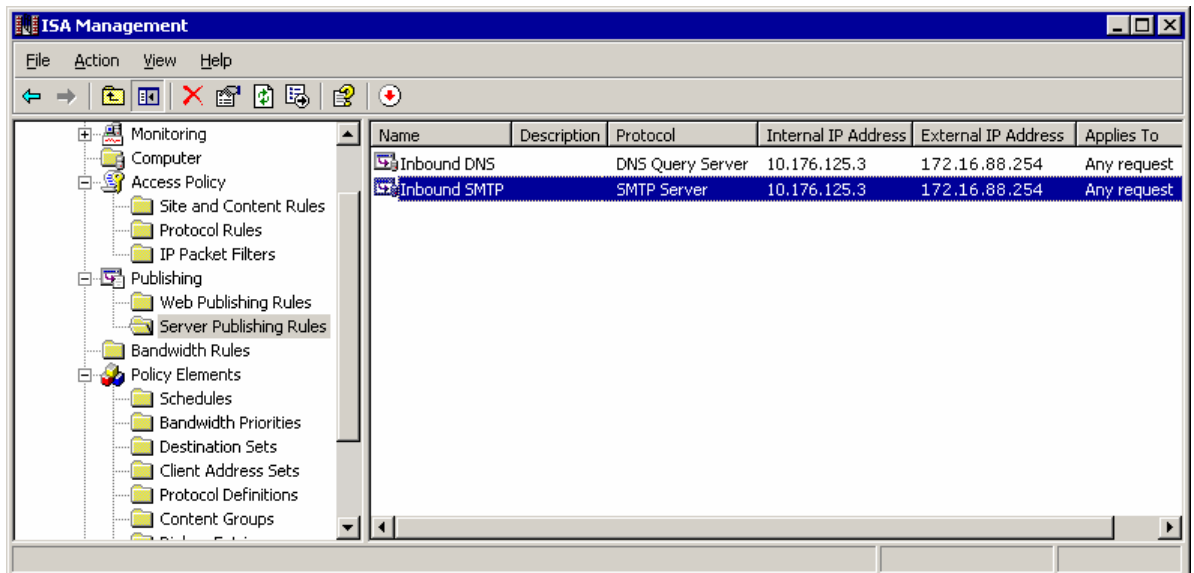
In the same way you created a server publishing rule for incoming DNS requests, you need to create a server publishing rule that instructs ISA Server to forward incoming SMTP requests to your SMTP gateway.

In the ISA Server management console, create a new server publishing rule with the settings described in Table 4.

Table 4 Server publishing rule settings for inbound SMTP traffic

Setting	Value
Server publishing rule name	Inbound SMTP
IP address of internal server	IP address of your inbound SMTP gateway server
External IP address on ISA Server	Internet IP address of external ISA Server NIC
Apply the rule to this protocol	SMTP Server
Apply the rule to requests from	Any request

Figure 8 shows an example server publishing rule for inbound SMTP traffic.

**Figure 8 Server publishing rule settings for inbound SMTP traffic**

Configure SMTP Server to Be a SecureNAT Client

As with DNS, by default your inbound SMTP server needs to route Internet traffic through the ISA Server. Configure your SMTP server to be a SecureNAT client as described in the section "Configure External DNS Server to Be a SecureNAT Client." If your SMTP gateway is the same as your external DNS server, no further configuration is required.

Test Inbound SMTP Traffic Using Telnet

Mail servers on the Internet should now be able to connect on port 25 to your inbound SMTP server to send mail to your organization. You should test that this connectivity is working. From a computer connected to the Internet, use telnet to access your external MX record host on port 25.

For example, if an MX record in external DNS lists smtp.contoso.com as the host, you would type the following at a command prompt:

```
telnet smtp.contoso.com 25
```

In this example, you would see a response similar to the following:

```
220 smtp.contoso.com Microsoft ESMTP MAIL Service, Version:  
6.0.3790.0 ready at Wed, 25 Jun 2003 09:08:58 -0700
```

If you do not see a response from your SMTP server, try connecting to the ISA Server computer's IP address directly. If that works, it is possible that you have a DNS configuration problem.

Send a Test Message from the Internet

After you confirm that you can use telnet to access the SMTP server through ISA Server, you should be ready to receive inbound SMTP mail from the Internet. Send a test message from the Internet to someone in your organization, and make sure it arrives.

Configuring Outbound Internet Mail

After you configure inbound Internet mail, the next step is to configure outbound mail traffic from your organization to be routed to the Internet through ISA Server. Your SMTP bridgehead server responsible for Internet mail needs to be able to create SMTP sessions to mail servers on the Internet. Additionally, computers on your network must be able to query DNS servers on the Internet.

Enable Outbound SMTP Traffic

To enable outbound SMTP connections from your network, create a protocol rule on ISA Server that allows outbound SMTP traffic.

In the ISA Server management console, create a new protocol rule with the settings listed in Table 5.

Table 5 Protocol rule settings for outbound SMTP traffic

Setting	Value
Protocol rule name	SMTP Outbound
Response to client requests to use protocol	Allow
Apply this rule to	Selected protocols
Protocols	SMTP
Use this schedule	Always
Apply the rule to requests from	Any request

Figure 9 shows an example protocol rule for outbound SMTP traffic.

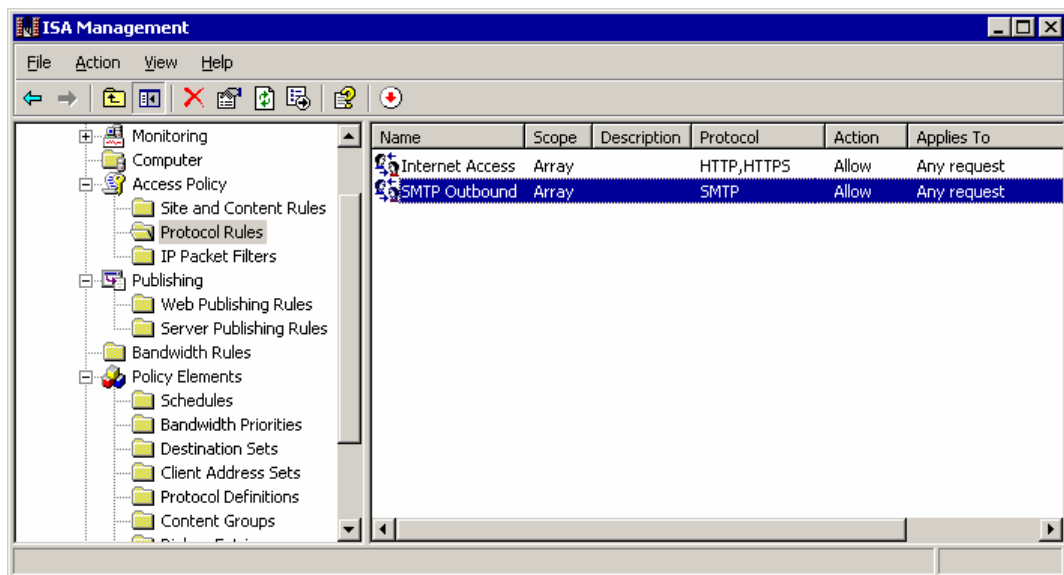


Figure 9 Protocol rule settings for outbound SMTP traffic

Enable Outbound DNS Traffic

To allow Exchange to send mail to Internet addresses, it needs to be able to resolve DNS names on the Internet. If the server responsible for external DNS resolution is located on your internal network, you must create a protocol rule on ISA Server that allows outbound DNS queries.

In the ISA Server management console, create a new protocol rule with the settings listed in Table 6.

Table 6 Protocol rule settings for outbound DNS traffic

Setting	Value
Protocol rule name	DNS Outbound
Response to client requests to use protocol	Allow
Apply this rule to	Selected protocols
Protocols	DNS Query
Use this schedule	Always
Apply the rule to requests from	Any request

Figure 10 shows an example protocol rule for outbound DNS traffic.

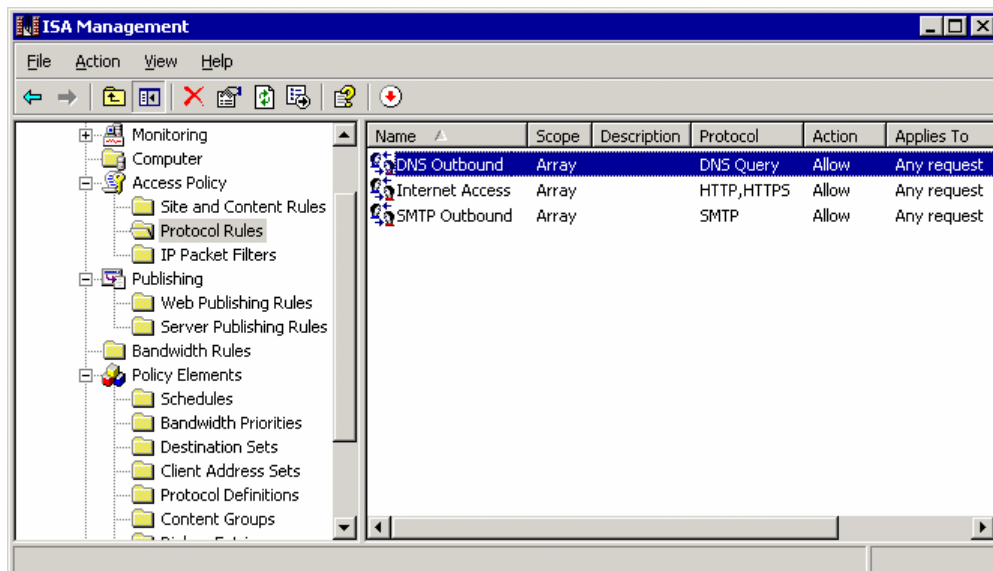


Figure 10 Protocol rule settings for outbound DNS traffic

Configure the SMTP Bridgehead Server As a SecureNAT Client

If your SMTP connector for outbound Internet mail is configured to use DNS, the Exchange server on which it is homed must be configured as a SecureNAT client. If, instead of using DNS, the connector is configured to route to a smart host, the smart host (which is itself configured to use DNS to route outbound mail) needs to be a SecureNAT client.

To configure your SMTP bridgehead server to be a SecureNAT client, use the information described in the previous section "Configure External DNS Server to Be a SecureNAT Client."

Send a Test Message to a User on the Internet

Users should now be able to send mail to recipients with Internet mail addresses. Verify that outbound mail is working by sending a test message to a user on the Internet.

Step 4: Configure Your Server Architecture and SSL

After you have outbound and inbound Internet mail working through ISA Server, you can start configuring client access to Exchange from the Internet through ISA Server. Outlook Web Access users on the Internet normally connect to a front-end server in the perimeter network, which looks up the user's mail server and then sends the Outlook Web Access request back to the user's Exchange server.

With ISA Server, Outlook Web Access requests are received by the ISA Server in the perimeter network, which forwards the requests to the front-end server on the internal network.

Moving Front-End Servers out of the Perimeter Network

When you use ISA Server, Outlook Web Access users no longer access your front-end Outlook Web Access servers directly from the Internet. You can move these Exchange front-end servers out of the perimeter network and back into the internal network. These servers no longer need to be dual-homed servers. Additionally, make sure the IP addresses are static because ISA Server will be configured to route incoming Outlook Web Access traffic to the specific IP addresses of your front-end servers. If the IP addresses for your front-end servers change, Outlook Web Access could stop working.

Closing Internal Firewall Ports

Your Exchange front-end server requires that numerous ports be open on your internal firewall. For example, the front-end server uses ports 389 and 3268 for Lightweight Directory Access Protocol (LDAP) to query Microsoft Active Directory® directory service when looking up a user's mailbox server. If you maintain your internal firewall, you can close these ports when you deploy ISA Server.

Note

You still need to keep ports open for traffic that ISA Server sends to the internal network, such as those listed in Table 7. Close any ports that are no longer required on your internal firewall.

Table 7 Protocols and ports required by ISA Server

Protocol	Port
HTTP	80
HTTPS	443
SMTP	25
DNS	53
IMAP4	114
POP3	110

Updating External DNS

Outlook Web Access users connect over the Internet to an Internet address such as <http://mail.contoso.com/exchange>. In a typical front-end and back-end Exchange deployment, the external DNS for your domain includes a host record that resolves to the IP address of your front-end server. In this example, the contoso.com domain would have an existing host record called "mail" that points to the IP address of the front-end server.

Because ISA Server will now handle the incoming Outlook Web Access traffic, the IP address of the host record is updated to point to the external IP address of the ISA Server. Users continue to use the same URL to connect to Outlook Web Access, but DNS resolves the request to the ISA Server instead of the front-end server.

Update your external DNS record for Outlook Web Access to point to the external IP address of the ISA Server.

Configuring SSL on ISA Server

If you use Secure Sockets Layer (SSL) to encrypt Outlook Web Access communications, you must configure ISA Server to support SSL traffic. In general, you should always use SSL for Outlook Web Access traffic. Otherwise, users' mail data will be sent over the Internet without a secure channel. Unless you use an encryption method for the mail itself, such as S/MIME, malicious users on the Internet could intercept the e-mail messages as they traverse the Internet.

To configure ISA Server to handle SSL traffic for Outlook Web Access, you need to install the SSL certificate on ISA Server.

Export Your SSL Certificate

The first step to installing your existing SSL certificate on ISA Server is to export it from your front-end server.

To export the SSL certificate

1. Open the Certificates Microsoft Management Console (MMC) snap-in for the front-end server computer account.
2. Locate the personal certificates store (Figure 11).

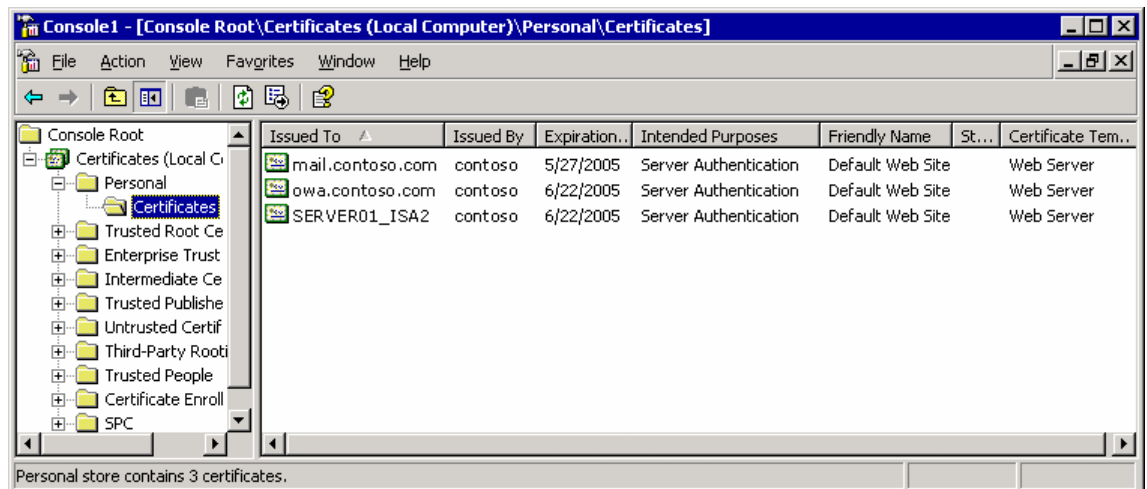


Figure 11 The personal certificates store

- Use the Certificate Export Wizard to export the existing certificate used for Outlook Web Access. Use the settings in Table 8 to export the certificate.

Table 8 Export certificate settings

Setting	Value
Export Private Key	Yes, export the private key
Export File Format	Personal Information Exchange PKCS #12 (.pfx) <ul style="list-style-type: none"> • Include all certificates in the certification path if possible • Enable strong protection

Important

Unless you terminate SSL traffic on the ISA Server, you must export the private key. Without the private key, ISA Server cannot decrypt the SSL traffic from the Internet.

You must include all the certificates in the certification path because you may need to add the root certification authority for the certificate to the trusted certification authority store in ISA Server, especially if you use your own internal certification authority. Otherwise, ISA Server may not be able to validate that the SSL certificate is from a trusted source.

Import Your SSL Certificate

After you export the SSL certificate, you must import it to the ISA Server certificate store.

To import the SSL certificate

- On the ISA Server, open the Certificates MMC snap-in for the ISA Server computer account.
- Locate the personal certificates store.
- Use the Certificate Import Wizard to import the certificate that you exported from the front-end server into the personal certificates store. Use the default settings in the Wizard.

After you import the certificate, you will see all the certificates in the certification path in the personal certificates store (Figure 12).

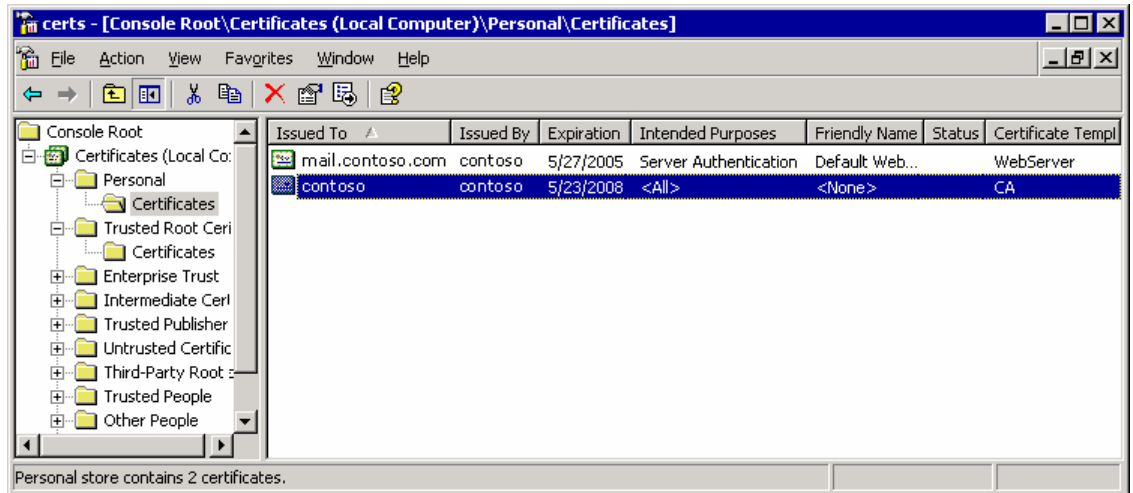


Figure 12 Imported certificates

Note

If you use your own certification authority (CA) or a CA that is not in the Trusted Root Certification Authorities certificate store, the SSL certificate will not be trusted by ISA Server and you will see errors when you view it.

4. Move the root CA certificate that you imported into the Trusted Root Certification Authorities certificate store. ISA Server will now trust the SSL certificate you imported into the personal store.

5. View the SSL certificate in the personal store, and make sure there are no errors (Figure 13).

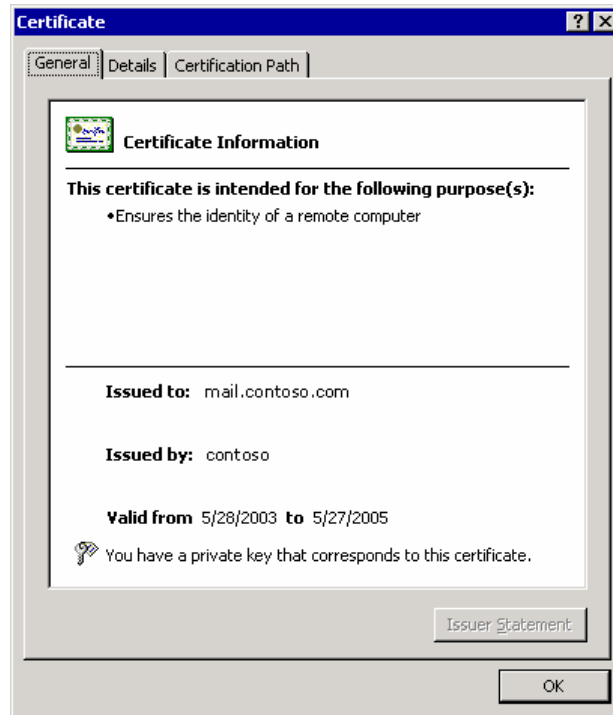


Figure 13 SSL certificate on the ISA Server with no errors

Modify Hosts File to Allow SSL for External Clients

SSL Web certificates are issued for a particular address. The address on the SSL certificate must match the address of the URL to which users connect. For example, if your Outlook Web Access users connect to `http://mail.contoso.com/exchange`, the SSL certificate must be issued for the address `mail.contoso.com`.

Because the SSL certificate rejects any URLs that do not use the address on the certificate, a problem may occur when ISA Server sends requests to the front-end server. In this case, SSL is used in two instances: between the Outlook Web Access client and ISA Server, and between ISA Server and the Exchange front-end server. Both ISA Server and the front-end server have the same SSL certificate, and the SSL certificate in both cases requires that the URL it is responding to matches the address on the certificate. Therefore, ISA Server needs to send the incoming request to the address on the SSL certificate (for example, `mail.contoso.com`). If ISA Server sends the request to the IP address of the front-end server, the SSL certificate on the front-end server will reject the request, because the URL (for example, `http://10.176.125.3/exchange`) does not match the address on the SSL certificate (`http://mail.contoso.com/exchange`).

Because the address on the SSL certificate resolves in DNS to the ISA Server, ISA Server cannot use DNS to forward the request to the Internet address. Instead, you must modify the hosts file on the ISA Server to map the Internet address to the IP address of the front-end server. Modifying the file allows you to have ISA Server send requests to the Internet address (for example, mail.contoso.com) and still send them to the IP address of the front-end server.

To modify the hosts file

1. Locate the hosts file found in \WINNT\system32\drivers\etc\hosts.
2. Open the hosts file on the ISA Server in a text editor such as Notepad.
3. Add an entry for the Outlook Web Access Internet address.

In this example, the hosts file entry would look similar to the following:

```
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host
# name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       192.168.0.2       rhino.example.com           # source server
#       192.168.0.9       x.example.com             # x client host
#
172.16.0.1       localhost
10.176.125.3     mail.contoso.com
```

Step 5: Configure ISA Server for Outlook Web Access

After you locate your ISA Server computer in the perimeter network and move your Exchange front-end servers within your internal network, you can configure ISA Server to provide access to Outlook Web Access. To provide this access, you need to create a destination set.

Creating an Outlook Web Access Destination Set

Outlook Web Access URLs use three different virtual directories:

- Exchange
- Public
- Exchweb

You need to create a destination set in ISA Server that includes these three directories.

To create an Outlook Web Access destination set

1. In the ISA Server management console, create a new destination set called **Outlook Web Access**.
2. Configure the three destinations using the information in Table 9.

Table 9 Outlook Web Access destination set settings

Name/IP range	Path
mail.example.com	/exchange/*
mail.example.com	/public/*
mail.example.com	/exchweb/*

3. Replace mail.example.com with the address that your users use to connect to Outlook Web Access. For example, if users enter the URL <http://mail.contoso.com/exchange> to log on to Outlook Web Access, set the **Name/IP Range** value for each entry in the destination set to mail.contoso.com.

Figure 14 shows an example Outlook Web Access destination set created for the address mail.contoso.com.

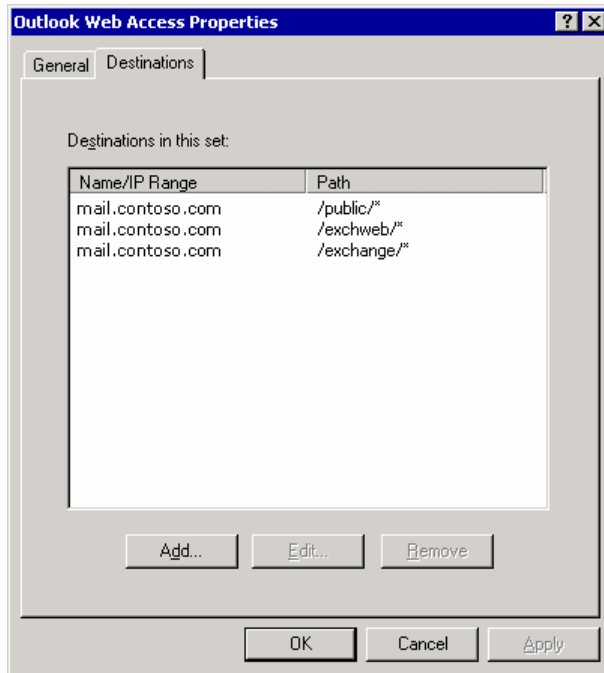


Figure 14 Outlook Web Access destination set

Creating Web Publishing Rule for Outlook Web Access

After you configure the Outlook Web Access destination set, you can publish your Exchange front-end server through ISA Server, using a Web publishing rule.

Although you can use server publishing rules to send HTTPS traffic to the front-end server for Outlook Web Access requests, Web publishing rules are a better choice for performance and manageability.

In the ISA Server management console, create a new Web publishing rule for Outlook Web Access using the settings listed in Table 10.

Table 10 Outlook Web Access Web publishing rule settings

Setting	Value
Web publishing rule name	Outlook Web Access
Apply this rule to	Specified destination set
Name	Outlook Web Access (the destination set previously created)
Apply this rule to requests from	Any request
Redirect the request to this internal Web server (name or IP address)	address.example.com (your Internet address for Outlook Web Access)
Send the original host header to the publishing server instead of the actual one (specified above)	Check box selected

Figure 15 shows the Rule Action page in the wizard.

Figure 15 Configuring the Web publishing rule for Outlook Web Access**Important**

Make sure to select the check box for sending the original host header. If ISA Server does not send the original host header to the front-end server, Outlook Web Access will not function correctly.

Note

Use the address you entered in the hosts file on the ISA Server for the Web server address (the address of the Exchange front-end server). If you do not use SSL, you enter the IP address of the front-end server instead of the Outlook Web Access Internet address.

Activating SSL on the Web Publishing Rule

After you have created the Web publishing rule for Outlook Web Access, you must activate SSL on the rule.

To activate SSL

- In the ISA Server management console, on the **Bridging** tab, select the **Require secure channel (SSL) for published site** check box (Figure 16).

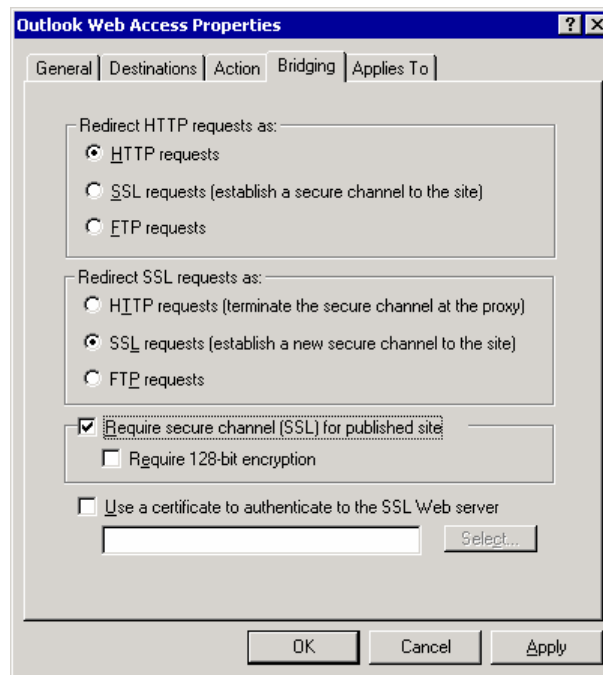


Figure 16 Activating SSL on the Web publishing rule

Enabling SSL Listeners

The final step to configuring Outlook Web Access is to enable SSL listeners on the ISA Server external IP address. These SSL listeners listen for incoming Web requests.

To enable SSL listeners

1. In the ISA Management console, open the ISA Server **Add/Edit Listeners** page.
2. Edit the IP address that you configured in the section "Configuring Incoming Web Requests to Use External IP."
3. Select the Use a server certificate to authenticate to web clients check box.
4. Click **Select**, and then select the SSL certificate installed on the ISA Server (Figure 17).

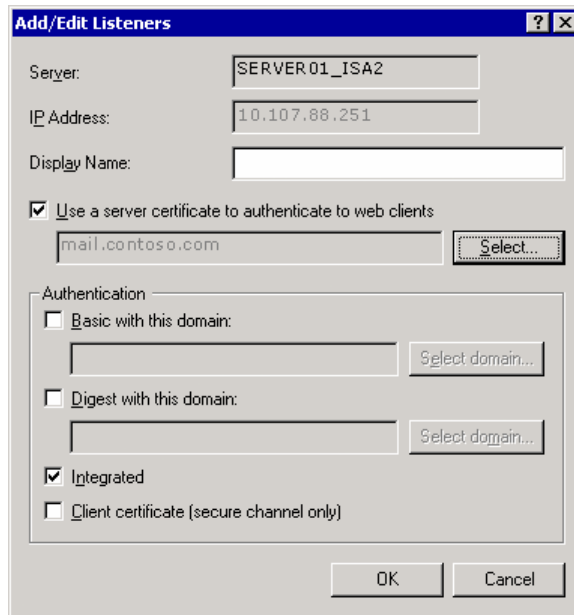


Figure 17 Selecting the SSL certificate for incoming Web requests

5. After you select the SSL certificate to use, on the **Incoming Web Requests** tab on the server property page, select the **Enable SSL listeners** check box (Figure 18).

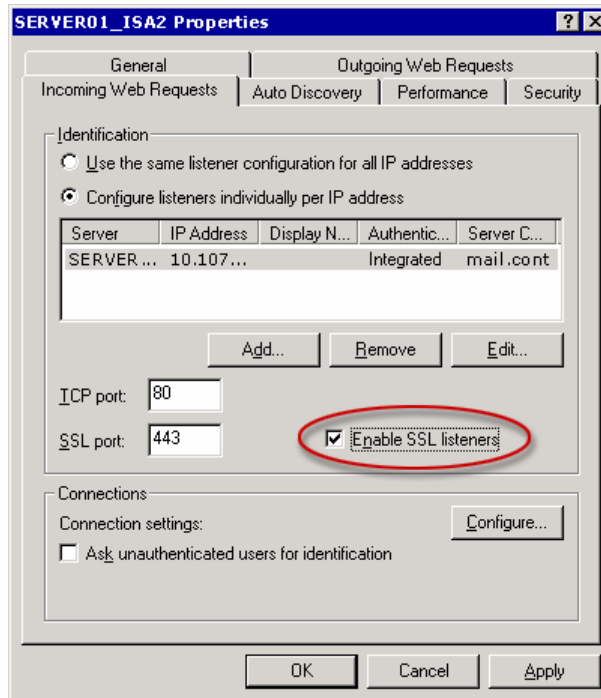


Figure 18 Enabling SSL listeners

Testing Outlook Web Access

Outlook Web Access is now configured to work through ISA Server. From a computer with Internet access, connect to your Outlook Web Access DNS address and make sure that Outlook Web Access works properly.

Step 6: Configure RPC over HTTP for Outlook 2003

To provide RPC over HTTP access to your Exchange servers for your Outlook 2003 users, you need to publish the \rpc virtual directory on your RPC Proxy server through ISA Server. You can publish this directory by using a Web publishing rule to specify the \rpc virtual directory on the RPC Proxy server. In this example, the RPC Proxy server is located on the Exchange front-end server, but you can also locate your RPC Proxy server on another Web server. For ease of maintenance, it is recommended that you use your Exchange front-end server as your RPC Proxy server.

Creating an RPC over HTTP Destination Set

RPC over HTTP uses the \rpc virtual directory located on your RPC Proxy server. You need to create a destination set in ISA Server that includes this directory.

To create an RPC over HTTP destination set

1. In the ISA Server management console, create a new destination set called **RPC over HTTP**.
2. Configure the destination set using the information in Table 11.

Table 11 RPC over HTTP destination set settings

Name/IP range	Path
mail.example.com	/rpc/*

3. Replace mail.example.com with the address of your RPC Proxy server.

Figure 19 shows an example RPC over HTTP destination set created for the address mail.contoso.com.

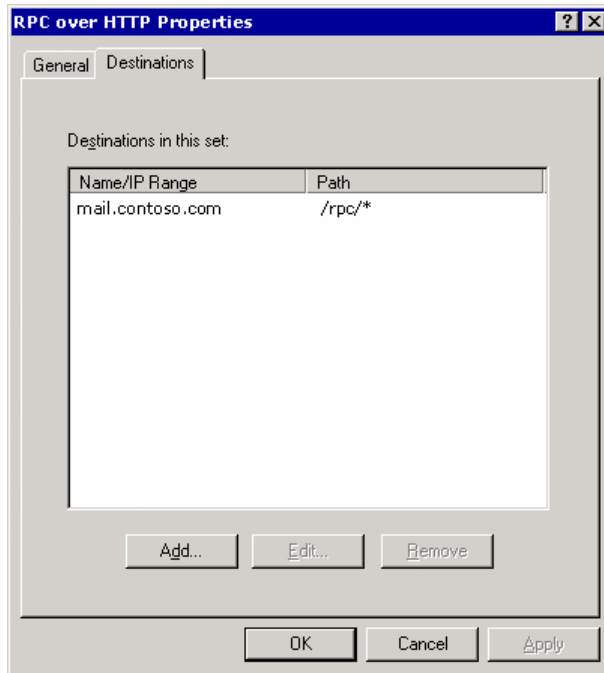


Figure 19 RPC over HTTP destination set

Creating Web Publishing Rule for RPC over HTTP

After you configure the RPC over HTTP destination set, you can publish your RPC Proxy server through ISA Server using a Web publishing rule.

In the ISA Server management console, create a new Web publishing rule for RPC over HTTP using the settings listed in Table 12.

Table 12 RPC over HTTP Web publishing rule settings

Setting	Value
Web publishing rule name	RPC over HTTP
Apply this rule to	Specified destination set
Name	RPC over HTTP (the destination set previously created)

Setting	Value
Apply this rule to requests from	Any request
Redirect the request to this internal Web server (name or IP address)	address.example.com (your Internet address for your RPC Proxy server)
Send the original host header to the publishing server instead of the actual one (specified above)	Check box selected

Note

Use the address you entered in the hosts file on the ISA Server computer for the Web server address (the address of the Exchange front-end server). If you do not use SSL, you enter the IP address of the front-end server instead of the RPC Proxy server Internet address.

Activating SSL on the Web Publishing Rule

After you create the Web publishing rule for RPC over HTTP, you must activate SSL on the rule.

To activate SSL

- On the **Bridging** tab, select the **Require secure channel (SSL) for published site** check box.

Enabling SSL Listeners

The final step to configuring RPC over HTTP is to enable SSL listeners on the ISA Server external IP address. These SSL listeners listen for incoming Web requests. For information about how to configure the SSL listeners, see the procedure "To enable SSL listeners" in "Enabling SSL Listeners" in "Step 5: Configure ISA Server for Outlook Web Access."

Setting the Default Connection Timeout for Incoming Web Requests

When you use RPC over HTTP with ISA Server as your front-end server, you need to set the default connection timeout for incoming Web requests to a value greater than the default value of 120 seconds.

To set the default timeout value

1. In the ISA Server management console, open the **Properties** page, and then click the **Incoming Web Requests** tab.
2. In **Connections**, click **Settings**, and then change the **Connection timeout value** to a value of 900 seconds or greater.

Testing RPC over HTTP

RPC over HTTP for Outlook 2003 clients is now configured to work through ISA Server. From a computer with Internet access, connect to your Outlook 2003 client and make sure that RPC over HTTP connectivity is working properly.

Step 7: Configure Outlook Mobile Access

To publish Outlook Mobile Access with ISA Server, you need to create a destination set for the \oma virtual directory on your Exchange front-end server, and then create a Web publishing rule for the destination set.

Creating an Outlook Mobile Access Destination Set

Outlook Mobile Access uses the \oma virtual directory. You need to create a destination set in ISA Server that includes this directory.

To create an Outlook Mobile Access destination set

1. In the ISA Server management console, create a destination set called **Outlook Mobile Access**.
2. Configure the destination set using the settings in Table 13.

Table 13 Outlook Mobile Access destination set

Name/IP range	Path
mail.example.com	/oma/*

3. Replace mail.example.com with the address of your Exchange front-end server.

Creating Web Publishing Rule for Outlook Mobile Access

After you create the Outlook Mobile Access destination, you can publish your Outlook Mobile Access \oma virtual directory on your Exchange front-end server through ISA Server, using a Web publishing rule.

In the ISA Server management console, create a new Web publishing rule for Outlook Mobile Access using the settings in Table 14.

Table 14 Outlook Mobile Access Web publishing rule settings

Setting	Value
Web publishing rule name	Outlook Mobile Access
Apply this rule to	Specified destination set
Name	Outlook Mobile Access (the destination set created in the previous step)
Apply this rule to requests from	Any request
Redirect the request to this internal Web server (name or IP address)	address.example.com (your Internet address for your Exchange front-end server)
Send the original host header to the publishing server instead of the actual one (specified above)	Check box selected

Activating SSL on the Web Publishing Rule

After you have created the Web publishing rule for Outlook Mobile Access, you must activate SSL on the rule.

To activate SSL

- On the **Bridging** tab, select the **Require secure channel (SSL) for published site** check box.

Enabling SSL Listeners

The final step to configuring Outlook Mobile Access is to enable SSL listeners on the ISA Server external IP address. These SSL listeners listen for incoming Web requests. For information about how to configure the SSL listeners, see the procedure "To enable SSL listeners" in "Enabling SSL Listeners" in "Step 5: Configure ISA Server for Outlook Web Access."

Testing Outlook Mobile Access

Outlook Mobile Access is now configured to work through ISA Server. From a computer with Internet access, use Internet Explorer to connect to your Outlook Mobile Access DNS address and make sure that Outlook Mobile Access is working properly.

Note

Although Internet Explorer is not a supported client for Outlook Mobile Access, it is useful to test whether you can communicate with your Exchange front-end server.

After you successfully connect to your Exchange front-end server using Outlook Mobile Access, verify that you can connect to your Exchange servers using a supported mobile device with Internet connectivity.

Step 8: Configure Exchange ActiveSync

To publish Exchange ActiveSync with ISA Server, you need to create a destination set for the \Microsoft-Server-ActiveSync virtual directory on your Exchange front-end server, and then create a Web publishing rule for the destination set.

Creating an Exchange ActiveSync Destination Set

Exchange ActiveSync uses the \Microsoft-Server-ActiveSync virtual directory. You need to create a destination set in ISA Server that includes this directory.

To create an Exchange ActiveSync destination set

1. In the ISA Server management console, create a destination set called **Exchange ActiveSync**.

2. Configure the destination set using the settings shown in Table 15.

Table 15 Exchange ActiveSync destination set

Name/IP range	Path
mail.example.com	/Microsoft-Server-ActiveSync/*

3. Replace mail.example.com with the address of your Exchange front-end server.

Creating Web Publishing Rule for Exchange ActiveSync

After you configure the Exchange ActiveSync destination set, you can publish your Exchange front-end server through ISA Server, using a Web publishing rule.

In the ISA Server management console, create a new Web publishing rule for Exchange ActiveSync using the settings listed in Table 16.

Table 16 Exchange ActiveSync Web publishing rule settings

Setting	Value
Web publishing rule name	Exchange ActiveSync
Apply this rule to	Specified destination set
Name	Exchange ActiveSync (the destination set created in the previous step)
Apply this rule to requests from	Any request
Redirect the request to this internal Web server (name or IP address)	address.example.com (your Internet address for Outlook Web Access)
Send the original host header to the publishing server instead of the actual one (specified above)	Check box selected

Activating SSL on the Web Publishing Rule

After you create the Web publishing rule for Exchange ActiveSync, you must activate SSL on the rule.

To activate SSL

- On the **Bridging** tab, select the **Require secure channel (SSL) for published site** check box.

Enabling SSL Listeners

The final step to configuring Exchange ActiveSync is to enable SSL listeners on the ISA Server external IP address. These SSL listeners listen for incoming Web requests. For information about how to configure the SSL listeners, see the procedure "To enable SSL listeners" in "Enabling SSL Listeners" in "Step 5: Configure ISA Server for Outlook Web Access."

Testing Exchange ActiveSync

ISA Server is now configured to support Windows-powered mobile devices that can use Exchange ActiveSync. Configure a mobile device to connect to your Exchange server using Exchange ActiveSync, and make sure that ISA Server and Exchange ActiveSync are working properly.

Configuring Up-to-Date Notifications for Exchange ActiveSync

To allow the Up-to-Date Notifications feature to work properly, you must add a registry value to ISA Server. The following procedure describes how to add the necessary registry value for Up-to-Date Notifications.

Caution

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

To add the registry value for Up-to-Date Notifications

1. On the ISA Server computer, start Registry Editor.
2. In the console tree, navigate to the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\
Services\W3Proxy\Parameters
```

3. Add the values listed in Table 17.

Table 17 Registry values for Up-to-Date Notifications

Item type	Value
Name	PassOPTIONSToPublishedServer
Data type	REG_DWORD
Data	1
Default	0

4. Click **File**, and then click **Exit** to save your changes.

Step 9: Configure Access for IMAP4 and POP3 Clients

To support client access with IMAP4 and POP3 clients to Exchange, you need to configure server publishing rules in ISA Server.

Creating Server Publishing Rules for IMAP4 Server and POP3 Server Traffic

Open the ISA Server management console, and create the appropriate server publishing rule with its respective properties. Table 18 shows the settings for a server publishing rule to support IMAP4 clients, and Table 19 shows the settings for a server publishing rule to support POP3 clients.

Table 18 IMAP4 server publishing rule settings

Setting	Value
Server publishing rule name	IMAP4
IP address of the internal server	Specify the IP address of the Exchange front-end server
IP address of the internal server	Specify the IP address of the external NIC on the ISA Server
Apply this rule to this protocol	IMAP4 Server

Setting	Value
Apply this rule to requests from	Any request

Table 19 POP3 Server publishing rule settings

Setting	Value
Server publishing rule name	POP3
IP address of the internal server	Specify the IP address of the Exchange front-end server
IP address of the internal server	Specify the IP address of the external NIC on the ISA Server
Apply this rule to this protocol	POP3 Server
Apply this rule to requests from	Any request

Testing IMAP4 or POP3 Mail

To test if IMAP4 or POP3 is working through ISA Server, use an IMAP4 or POP3 client to verify that you can send and receive mail through your ISA Server.

Additional Resources

For information about Microsoft Exchange Server, see <http://www.microsoft.com/exchange>.

Note

To download a self-extracting executable of all Exchange Product Team technical articles and online books for Exchange 2000 Server, see <http://go.microsoft.com/fwlink/?LinkId=10687>

Websites

- Exchange Server 2003 Technical Library (<http://www.microsoft.com/exchange/library>)
- Exchange Server 2003 Tools and Updates (<http://www.microsoft.com/exchange/2003/updates>)
- Microsoft Developer Network (MSDN®) (<http://msdn.microsoft.com/>)
- ISA Server 2000 Service Pack 1 (<http://go.microsoft.com/fwlink/?LinkID=18918>)
- ISA Server 2000 Feature Pack 1 (<http://go.microsoft.com/fwlink/?LinkID=18917>)
- ISA Server 2000 downloads website (<http://go.microsoft.com/fwlink/?LinkID=18919>)
- Microsoft security website (<http://www.microsoft.com/security>)
- TechNet security website (<http://go.microsoft.com/fwlink/?LinkID=5936>)

Exchange Server 2003 Books

- *What's New in Exchange Server 2003*
(<http://www.microsoft.com/exchange/library>)
- *Planning an Exchange Server 2003 Messaging System*
(<http://www.microsoft.com/exchange/library>)
- *Exchange Server 2003 Deployment Guide*
(<http://www.microsoft.com/exchange/library>)
- *Exchange Server 2003 Administration Guide*
(<http://www.microsoft.com/exchange/library>)

Microsoft Knowledge Base Articles

The following Microsoft Knowledge Base article is available at <http://support.microsoft.com/>:

- 331062, "Running ISA Server on Windows Server 2003"
(<http://go.microsoft.com/fwlink/?linkid=3052&kbid=331062>)

Does this book help you? Give us your feedback. On a scale of 1 (poor) to 5 (excellent), how do you rate this article?

Mail feedback to exchdocs@microsoft.com.