

# Using ISA Server 2004 with Exchange Server 2003

## Microsoft Internet Security and Acceleration Server 2004

---

### Introduction

Microsoft® Internet Security and Acceleration (ISA) Server 2004 and Microsoft Exchange Server 2003 are designed to work closely together in your network environment to provide a secure messaging environment.

This article describes how to deploy ISA Server 2004 as your advanced firewall server to protect your messaging environment.

---

### ISA Server 2004 and Exchange Server 2003



#### Note

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

ISA Server acts as an advanced firewall that controls Internet traffic between any number of networks that are connected to it, through its multinetworking feature. In the Exchange scenario, ISA Server will control traffic entering your internal corporate network and outbound communication from your messaging environment. 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, and your Exchange resources are protected from attack.

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), and Internet Message Access Protocol version 4rev1 (IMAP4) 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.

---

## ISA Server Features

ISA Server 2004 includes several features that complement and ease the publishing of Exchange servers.

### New Mail Server Publishing Wizard

The New Mail Publishing Wizard allows you to easily configure access rules that publish:

- Web client access
- Client access
- Server-to-server communication: Simple Mail Transfer Protocol (SMTP) and Network News Transfer Protocol (NNTP)

#### Web client access

Web client access includes:

- Outlook Web Access. Outlook Web access gives users SSL-secured access through a Web browser to their e-mail, calendar, group scheduling, and public folder information on computers running Exchange Server.
- Outlook Mobile Access. Outlook Mobile Access provides users with access to Outlook from mobile devices.
- Exchange ActiveSync. Exchange ActiveSync® allows you to synchronize directly and with high levels of security to your Exchange mailboxes from Microsoft Windows®-powered devices such as Pocket PC 2002, the Pocket PC Phone, and Windows Powered Smartphone.

Publication of Web client access services is described in the document "[OWA Server Publishing in ISA Server 2004](http://www.microsoft.com)" (<http://www.microsoft.com>).

ISA Server also enables you to publish an RPC Proxy server so that Microsoft Office Outlook 2003 clients can access their mailboxes using RPC over HTTP.

#### Client access

ISA Server enables you to publish Exchange to allow direct client access on these protocols:

- RPC
- IMAP

- POP3
- SMTP (to allow sending of e-mail)

**Server-to-server communication**

The New Mail Server Publishing Wizard enables you to publish a server on the SMTP, Secure SMTP, and NNTP protocols so that other servers can send mail to it.

**SMTP Filter and Message Screener**

ISA Server includes components that help prevent mail relaying, the entry of viruses, and unwanted attachments on the network: the SMTP filter and Message Screener.

The purpose of the SMTP filter is to allow the filtering of SMTP command verbs and to prevent users or domains from accessing the network by intercepting all SMTP traffic that arrives on port 25. The SMTP application filter is installed with ISA Server. The SMTP filter is always located on the ISA Server computer. When SMTP traffic arrives at the ISA Server computer, the traffic is analyzed against the rules configured, and forwarded if allowed by the rules and the filter.

**Important**

We do not recommend that you use Message Screener with Exchange Server 2003, because Message Screener will interfere with the functioning of the Exchange Server Connection and Recipient Filtering feature.

The SMTP filter can be used with Exchange Server 2003.

The purpose of Message Screener is to filter keywords and attachments indicated on the other tabs in the SMTP filter properties. Message Screener must be installed on an Internet Information Services (IIS) 6.0 or IIS 5.0 SMTP server. This server does not have to be the ISA Server computer. For example, Message Screener could be installed on the ISA Server computer, on the Exchange Server computer, or on any other IIS 6.0 or IIS 5.0 SMTP server in the Internal network or in a perimeter network.

Installation and configuration of the SMTP filter and Message Screener are described in the document "[Using the ISA Server 2004 SMTP Filter and Message Screener](http://www.microsoft.com)" (<http://www.microsoft.com>).

---

# Scenarios

There are two common scenarios that are considered in this document:

- You have an Exchange Server 2003 deployment, consisting of Exchange front-end servers in a perimeter network, and back-end servers in the Internal network. You want to secure this deployment with ISA Server.

- You have an Exchange Server 2003 deployment, consisting of Exchange front-end and back-end servers in the Internal network. You want to secure this deployment with ISA Server.

---

## Solutions

If your Exchange front-end servers are in a perimeter network, the solution is to move the front-end servers to the Internal network, and allow ISA Server to handle the requests from outside the corporate network, such as requests from the Internet. There will be no direct access to the Exchange servers from outside the corporate network, so they will remain secure.

If your front-end servers are already in the Internal network, you can deploy ISA Server in front of the front-end servers to secure them.

The procedures provided later in this document address both solutions. If your front-end servers are already in the Internal network, skip the procedures related to moving the servers.

---

## Deployment Recommendations

The walk-through procedures describe deployment of ISA Server in a 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 your configuration.

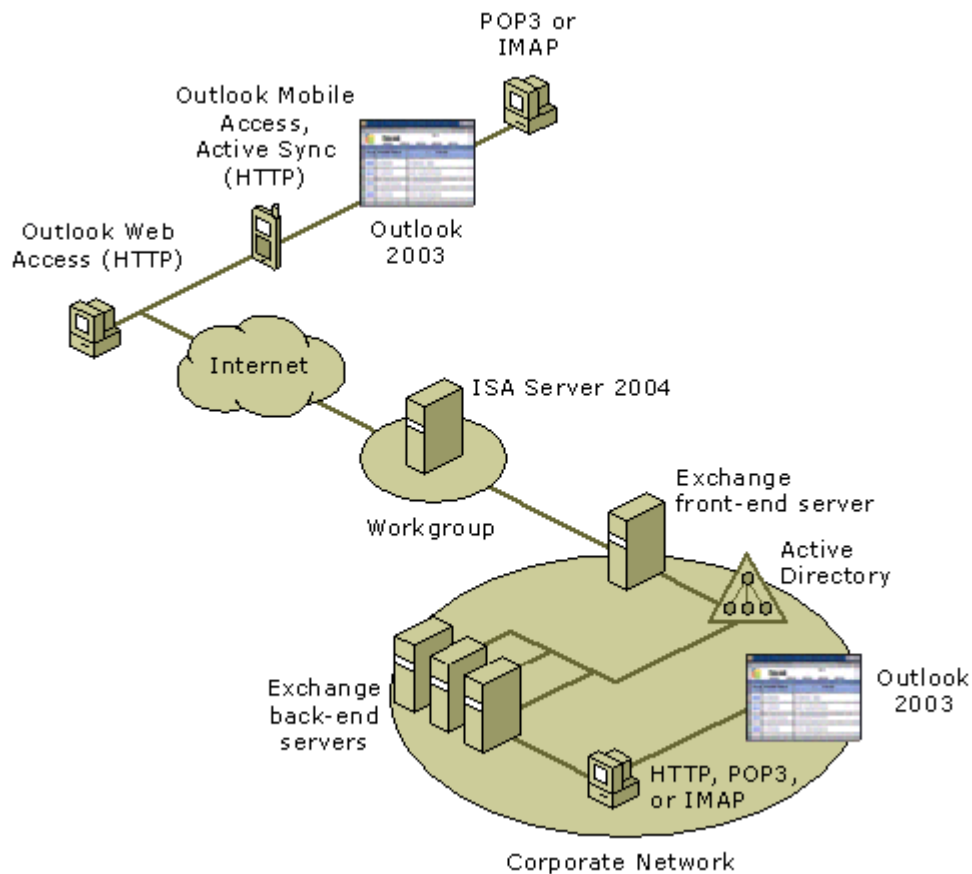
---

## Network Topology

To deploy this solution, you will require the following computers (these are minimal requirements for a laboratory configuration):

- Computer to serve as the Exchange front-end server. This computer must run Windows Server™ 2003 or Windows® 2000 Server and Exchange 2003. For more information about system requirements for Exchange, see "[System Requirements for Exchange Server 2003](http://www.microsoft.com)" (<http://www.microsoft.com>).
- Computer to serve as an Exchange back-end server. This computer must run Windows Server 2003 or Windows 2000 Server and Exchange 2003. For more information about system requirements for Exchange, see "[System Requirements for Exchange Server 2003](http://www.microsoft.com)" (<http://www.microsoft.com>).
- Domain controller on the Internal network.
- At least one internal client computer.
- ISA Server 2004 computer, with at least two network adapters.
- At least one external client computer.

The network topology (after moving servers out of the perimeter network) is shown in the following figure.



### Important

Do not use your ISA Server computer as a front-end server. An Exchange front-end server includes functionality that cannot be provided by an ISA Server computer such as providing a unified namespace for external access. We recommend that you deploy ISA Server in front of your Exchange front-end server.

## Using ISA Server with Exchange Server 2003—Walk-through

This walk-through contains the following procedures:

- Procedure 1: Deploy ISA Server 2004

- Procedure 2: Move Exchange Front-End Server to the Internal Network
- Procedure 3: Configure Corporate DNS Servers
- Procedure 4: Configure SMTP Servers
- Procedure 5: Configure ISA Server for Inbound Mail
- Procedure 6: Configure ISA Server for Outbound Mail
- Procedure 7: Enable External Client Access to the Exchange Server
- Procedure 8: Configure RPC over HTTP for Outlook 2003

---

## Using ISA Server with Exchange Server 2003 Walk-through

### Procedure 1: Deploy ISA Server 2004

Before you deploy ISA Server in the perimeter network and start moving Exchange servers into the Internal network, you must install ISA Server on a computer with at least two network adapters.

#### Placing the ISA Server Computer

Before you install ISA Server, consider where the ISA Server computer should be placed. You may place the ISA Server computer in your corporate domain. In some topologies, you may require that the ISA Server computer not be a member of the corporate domain. In that scenario, ISA Server can either be added to a separate domain with a trust relationship to the corporate domain through which authentication requests are supported, or placed in a workgroup and use RADIUS authentication if needed.

#### Using a Static Internal IP Address

Make sure the IP address of the ISA Server computer's internal network adapter is static. This configuration is necessary because you must configure SecureNAT clients, such as your inbound SMTP server, and point them to the internal IP address of your ISA Server computer. If the IP address on your internal network adapter changes, you must 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.

#### Obtaining an External IP Address for ISA Server

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

If you already manage your own corporate DNS server for external name resolution, consider using the IP address assigned to your Internet domain's name server. Using this IP address allows you to move the DNS server into 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

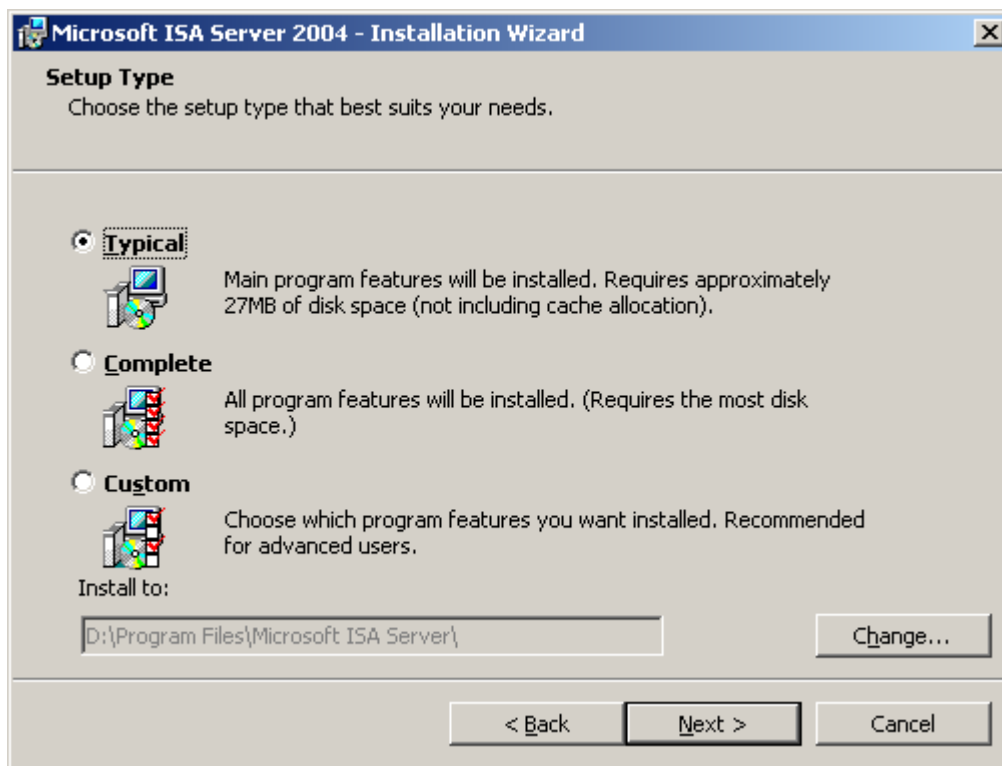
DNS server back to the Internal network, you must update your name server records at your Internet registrar to point to the new ISA Server IP address.



### Install ISA Server 2004

To install ISA Server on the designated computer, follow these steps.

1. Insert the ISA Server CD into the CD drive, or run ISAautorun.exe from the shared network drive.
2. In Microsoft ISA Server Setup, click **Install ISA Server**.
3. After the setup program prompts that it has completed determining the system configuration, on the **Welcome** page, click **Next**.
4. If you accept the terms and conditions stated in the end-user license agreement, click **I accept the terms in the license agreement**, and then click **Next**.
5. Type your customer details, and then click **Next**.
6. Click **Typical Installation**.





### Note

There are four components that can be installed:

- ISA Server Services. The services that comprise ISA Server.
- ISA Server Management. The ISA Server management user interface.
- Firewall Client Installation Share. A location from which client computers can install the Firewall Client software. This is typically installed on a computer other than the ISA Server computer, so it is not part of the Typical Installation option. The Firewall Client Share can be installed on computers running Windows Server 2003, Windows 2000 Server or Windows XP.
- Message Screener. A component that you configure to screen e-mail messages for keywords and attachments. This component must be installed on an SMTP server, which is typically not your ISA Server computer.

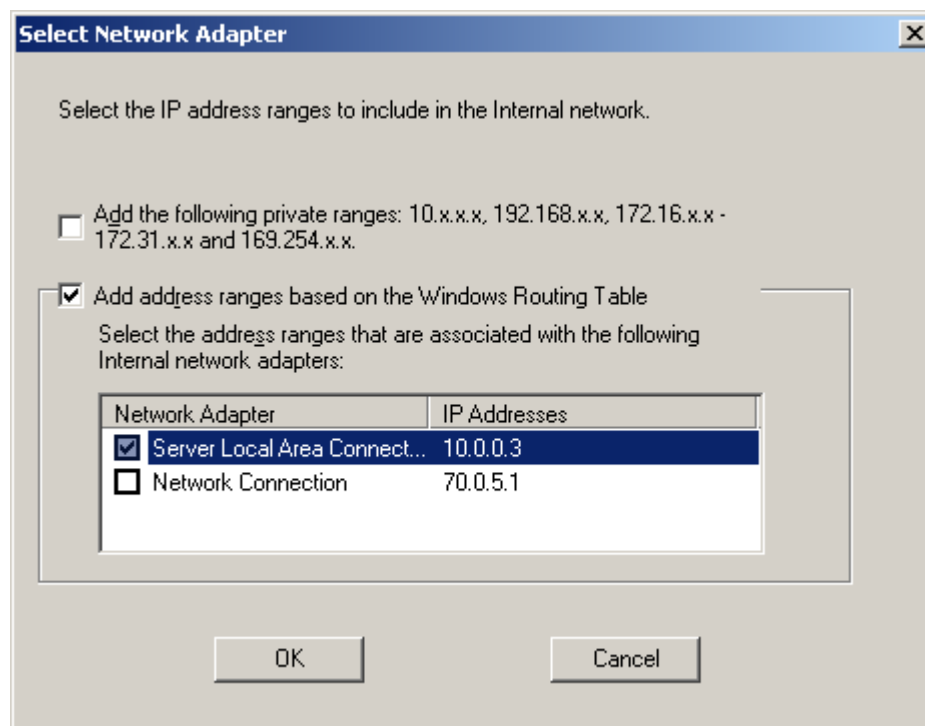
**Typical Installation** installs the ISA Server Services and ISA Server Management. **Full Installation** installs all four components. **Custom Installation** enables you to select which components you will install.

7. Click **Next**.

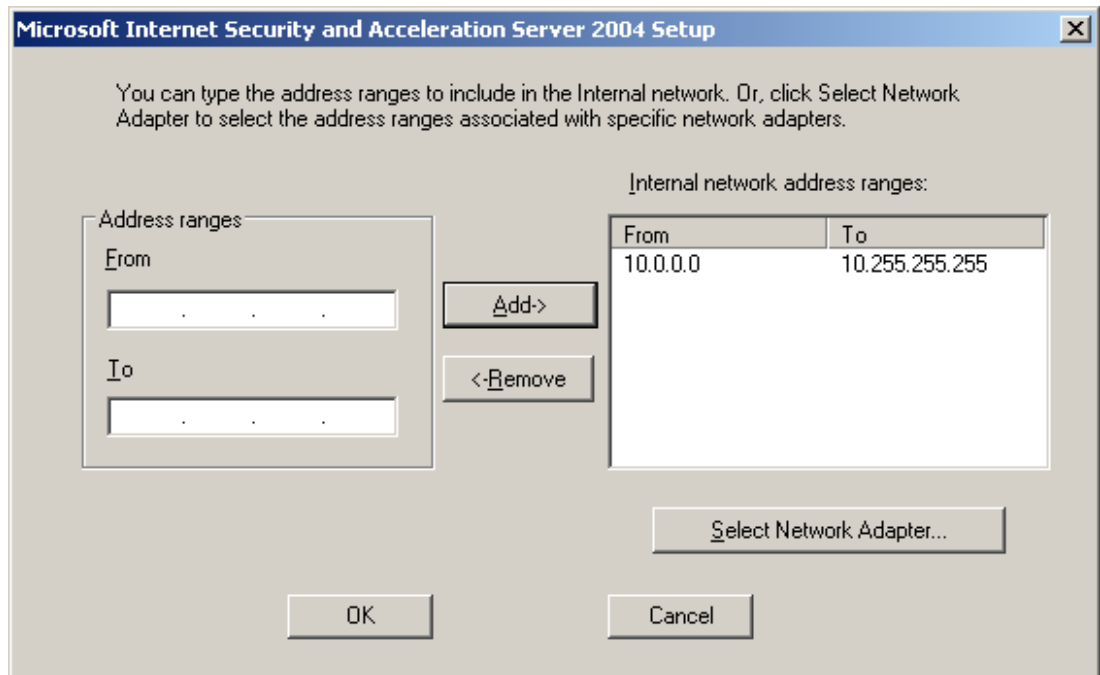


**To configure the Internal network, follow these steps.**

1. Click **Add**.
2. Click **Configure Internal Network**.
3. Select **Add address ranges based on the Windows Routing Table**.



4. Select one or more of the adapters that are connected to the Internal network. These addresses will be included in the Internal network that is defined by default for ISA Server.
5. Clear the selection of **Add the following private IP ranges**, unless you want to add those ranges to your Internal network.



6. Click **OK**. Read the Setup Message and click **OK**, click **OK** again to finish the Internal network configuration, and then click **Next**.
7. On the Firewall Client Connection Settings page, select whether you want to allow non-encrypted connections between Firewall clients and the ISA Server computer. The ISA Server 2004 Firewall Client software uses encryption, but older versions do not. Also, some versions of Windows do not support encryption. You can select the following:
  - **Allow non-encrypted Firewall client connections**, to allow Firewall clients running on versions of Windows that do not support encryption to connect to the ISA Server computer.
  - Allow Firewall clients running earlier versions of the Firewall client software to connect to ISA Server. This option is available only if the first option is selected.
8. On the **Services** page, review the list of services that will be stopped or disabled during installation of ISA Server. To continue the installation, click **Next**.
9. Click **Install**.
10. After the installation has completed, if you want to invoke ISA Server Management immediately, select the **Invoke ISA Management** check box, and then click **Finish**.

---

## Using ISA Server with Exchange Server 2003 Walk-through

### Procedure 2: Move Exchange Front-End Servers to the Internal Network

To ensure that the ISA Server computer will be the only computer exposed to the Internet, place the Exchange servers in the Internal network. The Internal network was defined in the ISA Server installation described in Procedure 1, so all that is required is that you physically connect the front-end Exchange servers to the Internal network adapter card of the ISA Server computer, or to a router that is connected to that adapter.

---

## Using ISA Server with Exchange Server 2003 Walk-through

### Procedure 3: Configure Corporate DNS Servers

There are several steps that you must take to ensure that requests for your Exchange server will be properly resolved.

Updating the MX Record to Point to ISA Server

Typically, the MX record for your organization points to a host record, which in turn points to the IP address of the SMTP gateway in your perimeter network. You must update the host record to point to the external IP address of your ISA Server computer. You can continue to use the same MX record and host name, but you must point to a different IP address.

For example, consider the following DNS entry:

```
Mail Exchanger (MX) [10] smtp.contoso.com.  
smtpHost (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 external IP address of the ISA Server computer.



#### Note

Updating the MX record must take place on the DNS server that handles name resolution requests for your Exchange server. If you have an internal DNS server that handles the requests, make the change on that DNS server. If the requests are handled by an external DNS server, submit the change to the organization that manages that server.

The remaining steps apply only when you have a corporate DNS server that handles name resolution requests for your Exchange server. If the requests are handled by an external DNS server, such as one managed by an Internet service provider, you should skip this step.

### Moving the DNS Server

Move your DNS server out of the perimeter network into the Internal network. The DNS server will now only require one network adapter, to connect it to the Internal network. Make sure the

DNS server has a static IP address, because if the IP address changes, inbound mail routing could fail.

### Publishing the DNS Server



**When you move your corporate DNS server into the Internal network, create a server publishing rule publishing the server on the DNS protocol to the external network.**

1. Expand Microsoft ISA Server Management and click **Firewall Policy**.
2. On the **Firewall Policy** task pane on the **Tasks** tab, click **Create New Server Publishing Rule** to start the New Server Publishing Rule Wizard.
3. On the **Welcome** page of the wizard, provide a name for the rule, such as **Publish Corporate DNS for Exchange Name Resolution**, and then click **Next**.
4. On the **Select Server** page, provide the IP address for the DNS server, and then click **Next**.
5. On the **Select Protocol** page, select **DNS Server**, and then click **Next**.
6. On the **IP Addresses** page, select the network on which ISA Server will listen for requests. Because you want to receive name resolution requests from the Internet, select **External**, and then click **Next**.
7. On the **Completing the New Server Publishing Rule Wizard** page, scroll through the rule configuration to verify that you have configured the rule correctly, and then click **Finish**.
8. In the ISA Server details pane, click **Apply** to apply the changes you have made. It will take a few moments for the changes to be applied.
9. You must also update your name server record for your Internet domain to point to the external IP address of the ISA Server computer.



#### Note

There is an access rule in the ISA Server system policy that allows the DNS protocol from the ISA Server computer to all networks. This rule is enabled by default when you install ISA Server, so you do not have to create this rule.

### Configuring the DNS Server to be a SecureNAT Client

You must configure your corporate DNS server to be a SecureNAT client. SecureNAT clients are computers that do not have Firewall Client software installed, and that have a default TCP/IP route to the Internet that goes through the ISA Server computer. When ISA Server forwards the incoming DNS request from the Internet to your corporate 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 network adapter.

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

**Note**

Pointing to your ISA Server computer internal network adapter assumes that your DNS server is on the same network segment as your ISA Server computer. 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.

### Testing the Corporate DNS Server from the Internet

Computers with Internet access should now be able to query your corporate 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 corporate 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 verify that the query is successful. Remember that the IP address you use for the NSLOOKUP query should be the IP address of the ISA Server external network adapter.

---

## Using ISA Server with Exchange Server 2003 Walk-through

### Procedure 4: Configure SMTP Servers

To configure SMTP servers, you will move SMTP servers out of the perimeter network and then configure the SMTP server to be a SecureNAT client.

#### Moving SMTP Servers out of the Perimeter Network

ISA Server handles all inbound traffic from the Internet. Move your SMTP gateway server out of the perimeter network into the Internal network. The SMTP server will now only require one network adapter, to connect it to the Internal network.

**Important**

Verify that the IP addresses are static for any server that ISA Server will forward requests to. 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 routing could fail.

#### Configuring the 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 computer. Configure your SMTP server to be a SecureNAT client.. To configure your SMTP server as a SecureNAT client, open the TCP/IP properties page on the server's

network adapter, and set the default gateway IP address to the IP address of the ISA Server internal network adapter.



**Note**

Pointing to your ISA Server computer internal network adapter assumes that your SMTP server is on the same network segment as your ISA Server computer. If you have a routed network and your SMTP 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.

---

## Using ISA Server with Exchange Server 2003 Walk-through

### Procedure 5: Configure ISA Server for Inbound Mail

You must configure ISA Server to allow traffic. First, configure 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.



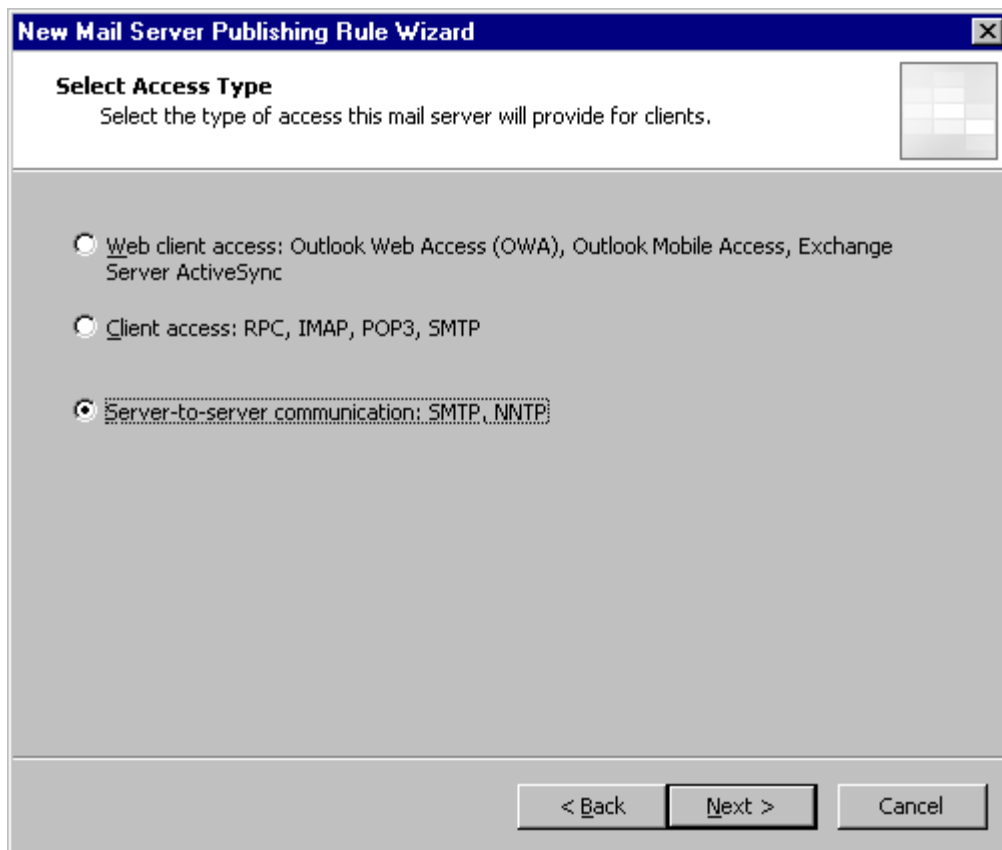
#### **Creating a Mail Server Publishing Rule for Inbound SMTP Traffic**

You must create a mail server publishing rule that instructs ISA Server to forward incoming SMTP requests to your SMTP gateway. Follow these steps to create a new mail publishing rule using the New Mail Server Publishing Rule Wizard.

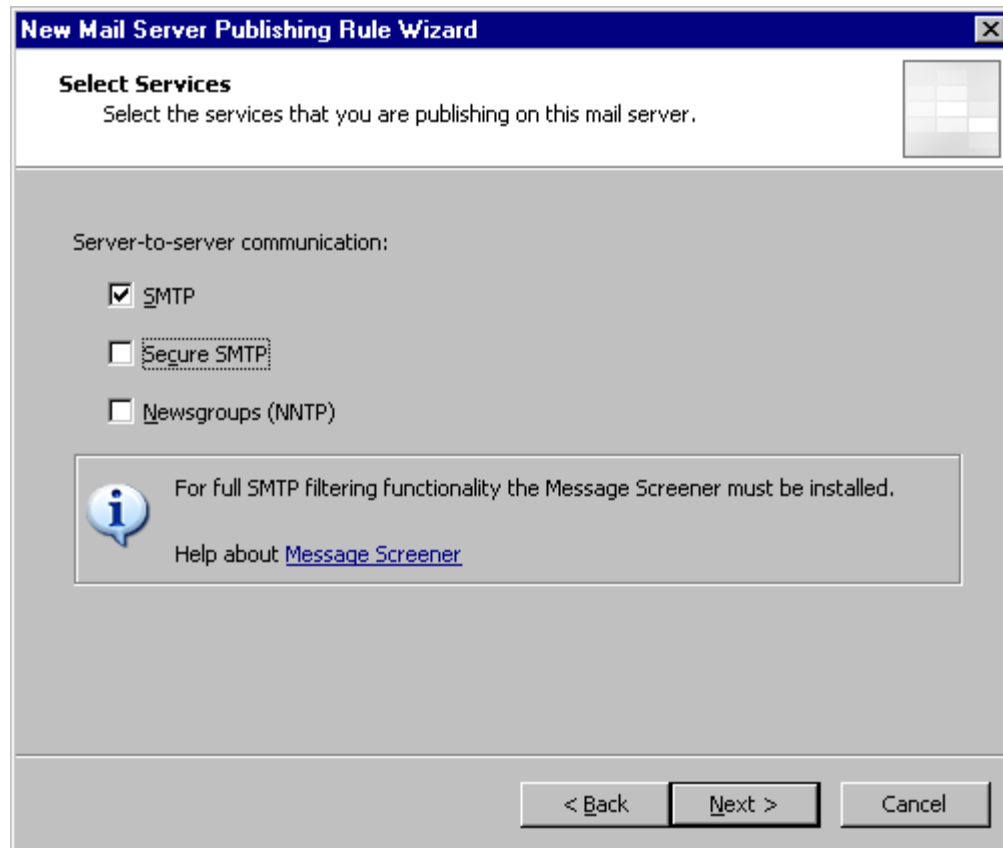
1. Expand Microsoft ISA Server Management and click **Firewall Policy**.
2. On the **Firewall Policy** task pane on the **Tasks** tab, click **Publish a Mail Server** to start the New Mail Server Publishing Rule Wizard.
3. On the **Welcome** page of the wizard, provide a name for the rule, such as **Inbound SMTP**, and then click **Next**.



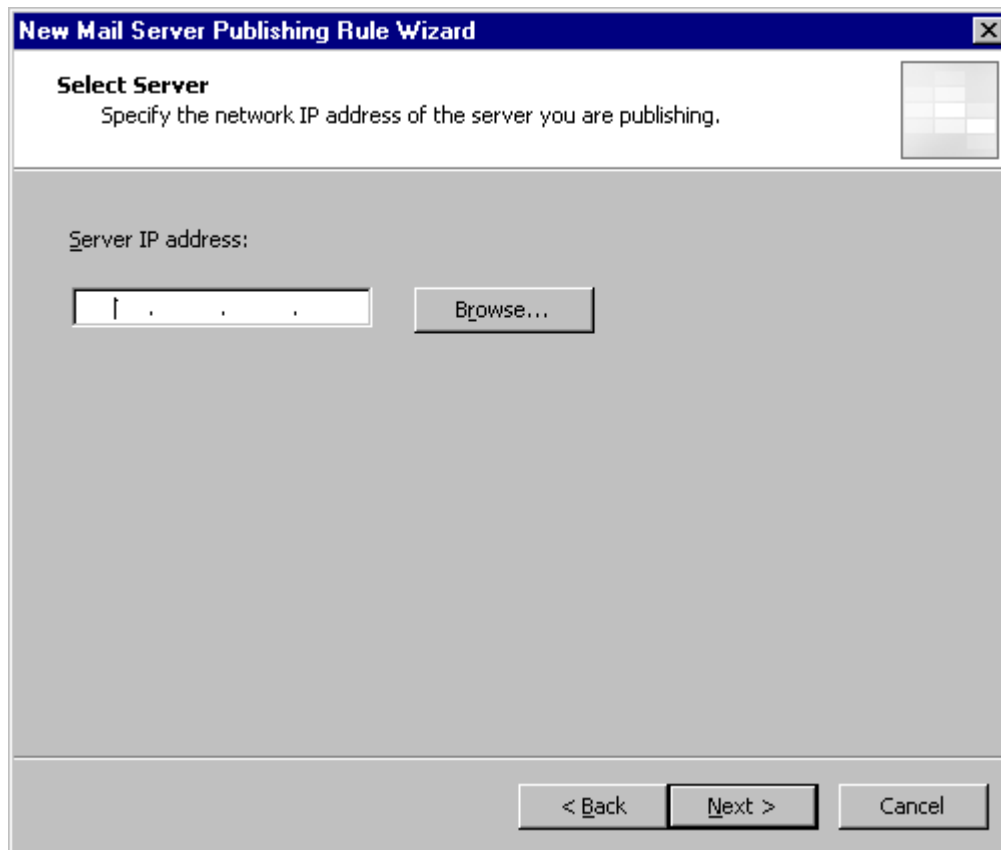
4. On the **Select Access Type** page, select **Server-to-server communication: SMTP, NNTP** and then click **Next**.



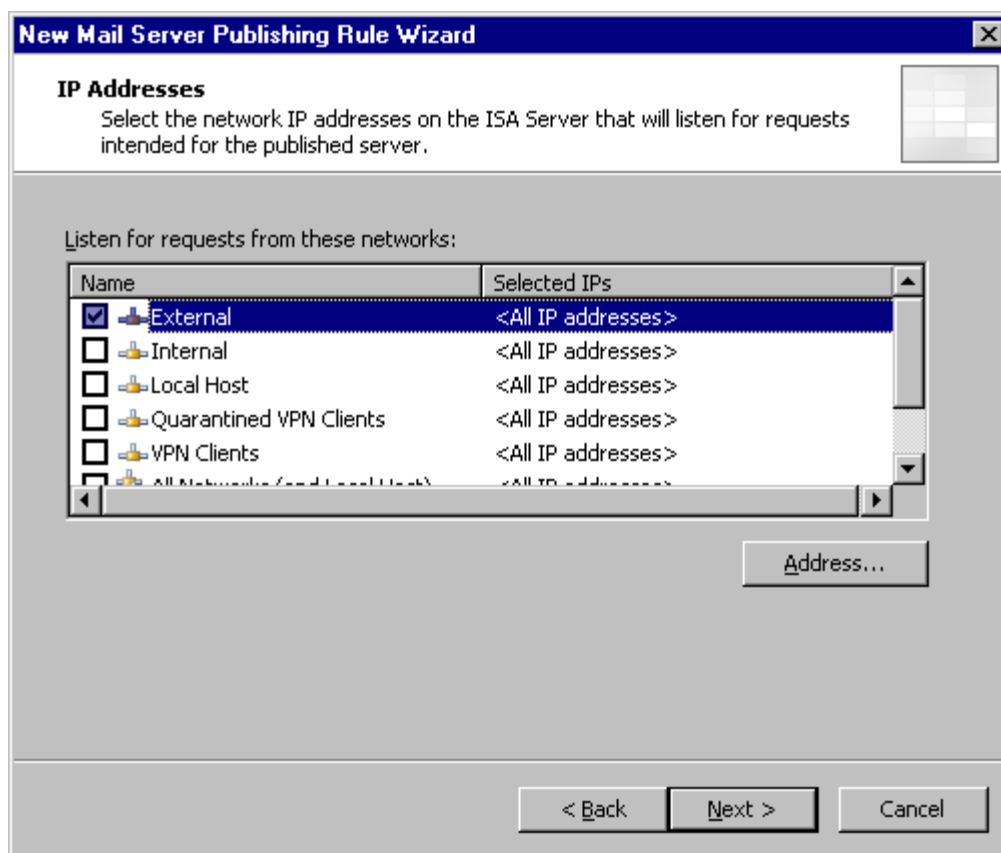
5. On the **Select Services** page, select **SMTP**. You may also select **Secure SMTP** if you want to publish your Exchange server to receive secure SMTP communication. **Newgroups NNTP** is for the publishing of a news server, to receive e-mail messages from newsgroups.



6. On the **Select Server** page, provide the IP address of the Exchange server, and then click **Next**.



7. On the **IP Addresses** page, select the network on which ISA Server will listen for requests. Because you want to receive communication from the External network, select **External**, and then click **Next**.



8. On the **Completing the New Mail Server Publishing Rule Wizard** page, scroll through the rule configuration to verify that you have configured the rule correctly, and then click **Finish**.
9. In the ISA Server details pane, click **Apply** to apply the changes you have made. It will take a few moments for the changes to be applied.

### Testing 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 corporate 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.

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 verify that it arrives.

---

## Using ISA Server with Exchange Server 2003 Walk-through

### Procedure 6: Configure ISA Server for Outbound 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.



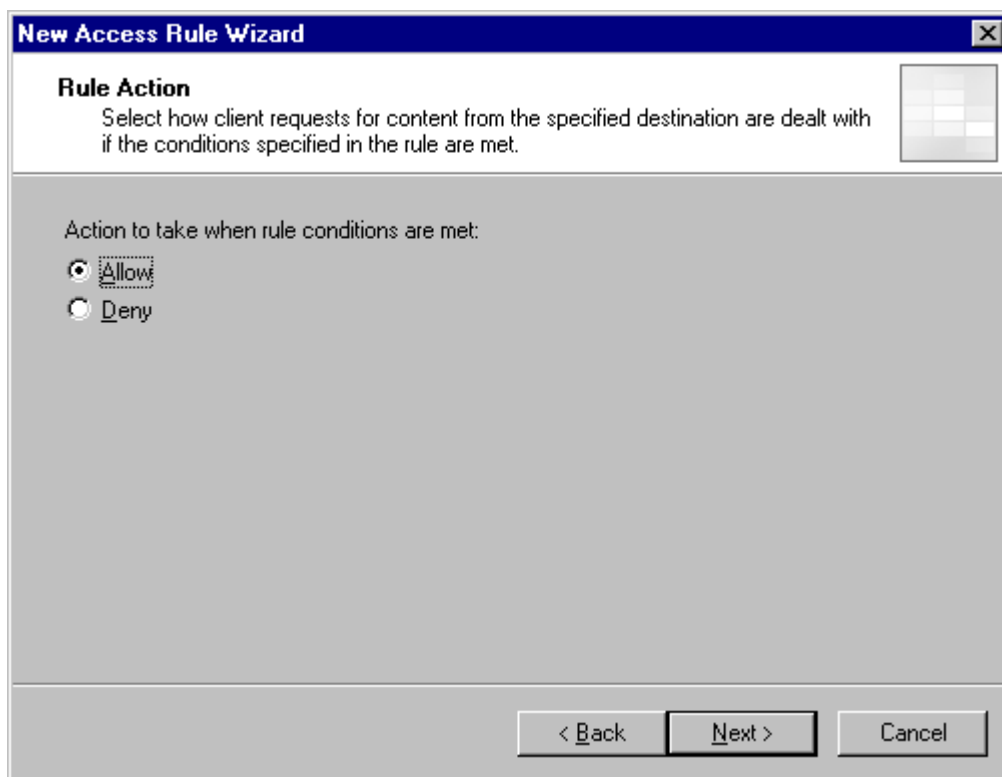
#### Creating an SMTP Access Rule

To enable outbound SMTP connections from your network, create an access rule on ISA Server that allows outbound SMTP traffic:

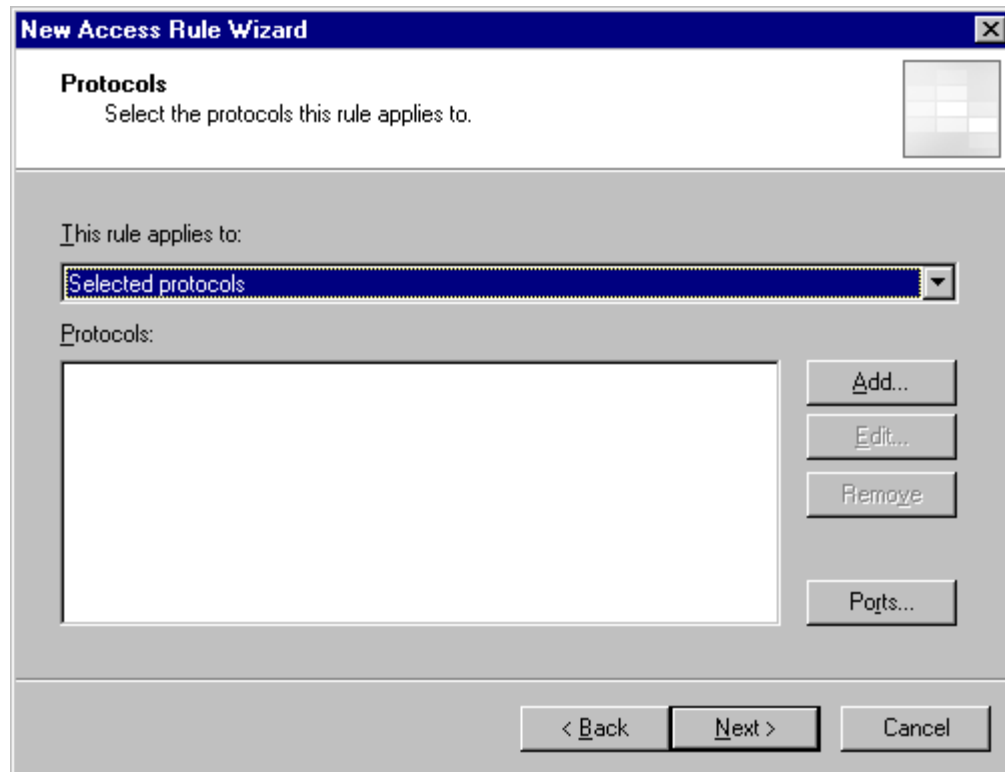
1. In the Microsoft ISA Server Management console tree, select **Firewall Policy**.
2. In the task pane, on the **Tasks** tab, select **Create New Access Rule** to start the New Access Rule Wizard.
3. On the **Welcome** page of the wizard, enter the name for the access rule, such as **Outbound SMTP**, and then click **Next**.



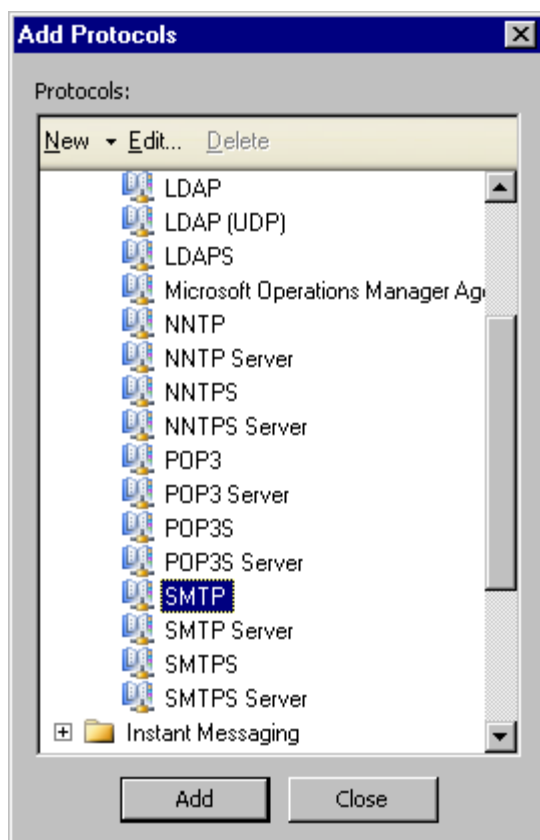
4. On the **Rule Action** page, select **Allow**, and then click **Next**.



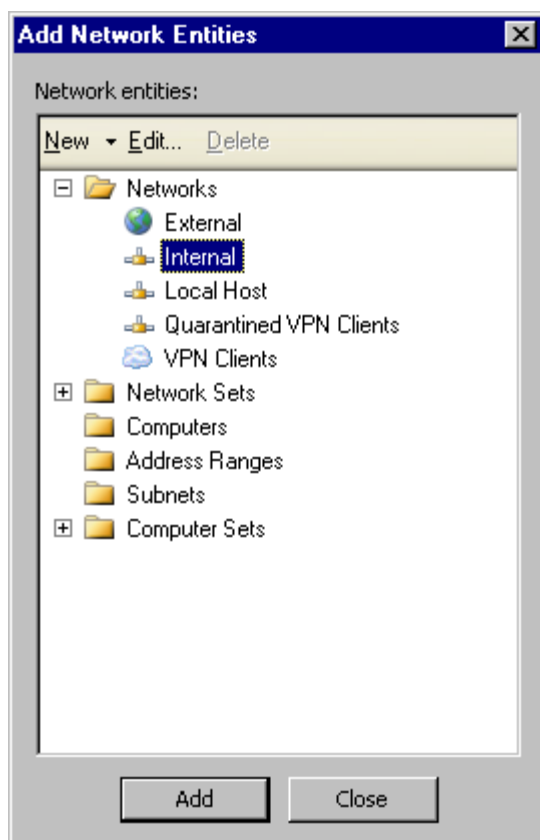
5. On the **Protocols** page, in **This rule applies to**, select **Selected protocols** and then use the **Add** button to open the **Add Protocols** dialog box.



6. In the **Add Protocols** dialog box, expand **Mail**, and select **SMTP**. Click **Add**, and then click **Close**, to close the **Add Protocols** dialog box. On the **Protocols** page, click **Next**.



7. On the **Access Rule Sources** page, click **Add** to open the **Add Network Entities** dialog box, expand **Networks**, select **Internal**, click **Add**, and then click **Close**.



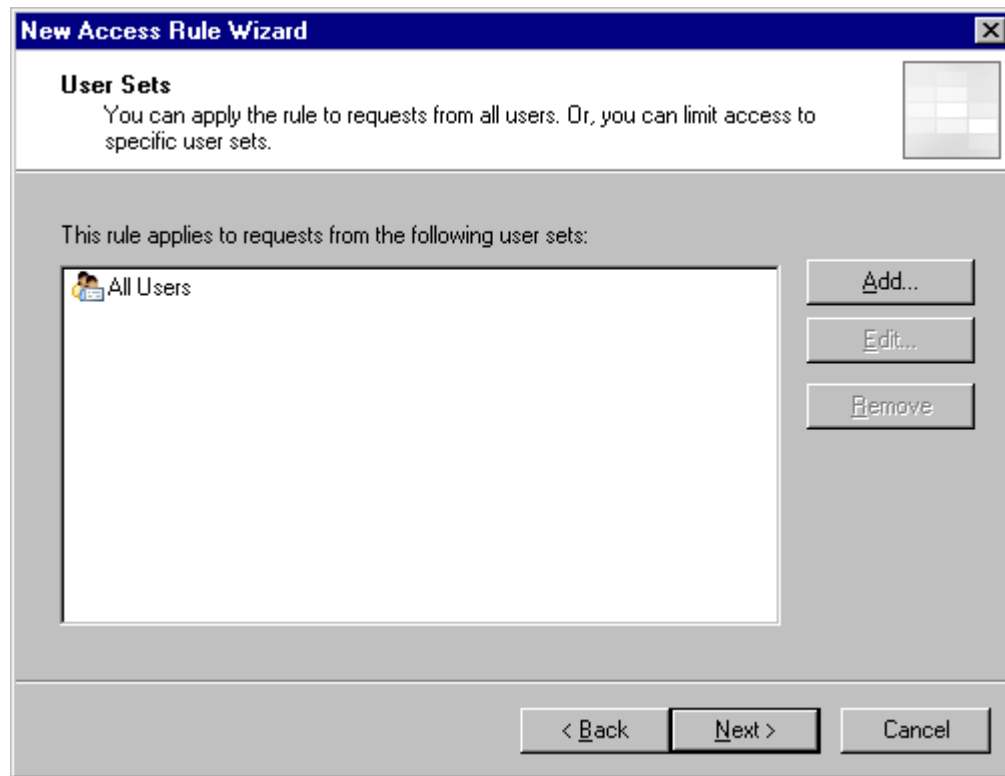
8. On the Access Rule Sources page, click **Next**.

**Note**

You can limit the access rule sources to a computer set containing the Exchange servers that handle outbound mail. If you have configured an SMTP connector on Exchange to handle all outbound mail, only that Exchange server would have to be listed (as a Computer network object) in the access rule sources. For more information about Computer and Computer Set network objects, see [Appendix A: Creating Rule Elements](#).

9. On the **Access Rule Destinations** page, click **Add** to open the **Add Network Entities** dialog box, expand **Networks**, select the External network (representing the Internet), click **Add**, and then click **Close**. On the **Access Rule Destinations** page, click **Next**.
10. On the **User Sets** page, you can specify the set of users whose credentials are used by the Exchange servers that require access, or you can leave the default user set All Users. If you want to specify a specific user set, select All Users and click Remove. Then, use the Add button to open the **Add Users** dialog box, from which you can add the user set to which the rule applies. The **Add Users** dialog box also provides access to the New User Sets Wizard

through the New menu item. For more information about user sets, see [Appendix A: Creating Rule Elements](#). When you have completed the user set selection, click **Next**.



11. Review the information on the wizard summary page, and then click **Finish**.
12. In the Firewall Policy details pane, click **Apply** to apply the new access rule. It may take a few moments for the rule to be applied. Remember that access rules are ordered, so if a deny rule matching SMTP access requests exists ahead of this allow rule in the order, access will be denied.



### Enabling Outbound DNS Traffic

To allow Exchange to send mail to Internet addresses, it has to be able to resolve DNS names on the Internet. If you have a corporate DNS server responsible for DNS resolution located on your Internal network, you must create an access rule on the ISA Server computer that allows outbound DNS queries from the DNS server. If you do not have a corporate DNS server for outgoing name resolution (name resolution is handled external to your networks), the access rule must allow outbound DNS queries from the Exchange server.

If you want to limit the access rule so that it applies only to the DNS server or Exchange server, create a Computer or Computer Set network object that contains only those servers. For information about Computer and Computer Set network objects, see [Appendix A: Creating Rule Elements](#).

1. In the Microsoft ISA Server Management console tree, select **Firewall Policy**.
2. In the task pane, on the **Tasks** tab, select **Create New Access Rule** to start the New Access Rule Wizard.
3. On the **Welcome** page of the wizard, enter the name for the access rule, such as **Outbound DNS**, and then click **Next**.
4. On the **Rule Action** page, select **Allow**, and then click **Next**.
5. On the **Protocols** page, in **This rule applies to**, select **Selected protocols** and then use the **Add** button to open the **Add Protocols** dialog box.
6. In the **Add Protocols** dialog box, expand **Common Protocols**, and select **DNS**. Click **Add**, and then click **Close**, to close the **Add Protocols** dialog box. On the **Protocols** page, click **Next**.
7. On the **Access Rule Sources** page, click **Add** to open the **Add Network Entities** dialog box, select the Computer or Computer Set network object you created previously, click **Add**, and then click **Close**. On the **Access Rule Sources** page, click **Next**.
8. On the **Access Rule Destinations** page, click **Add** to open the **Add Network Entities** dialog box, click **Networks**, select the **External** network (representing the Internet), click **Add**, and then click **Close**. On the **Access Rule Destinations** page, click **Next**.
9. On the **User Sets** page, you can specify the set of users whose credentials are used by the servers that require access, or you can leave the default user set **All Users**. If you want to specify a specific user set, select **All Users** and click **Remove**. Then, use the **Add** button to open the **Add Users** dialog box, from which you can add the user set to which the rule applies. The **Add Users** dialog box also provides access to the New User Sets Wizard through the **New** menu item. For more information about user sets, see [Appendix A: Creating Rule Elements](#). When you have completed the user set selection, click **Next**.
10. Review the information on the wizard summary page, and then click **Finish**.
11. In the Firewall Policy details pane, click **Apply** to apply the new access rule. It may take a few moments for the rule to be applied. Remember that access rules are ordered, so if a deny rule matching SMTP access requests exists ahead of this allow rule in the order, access will be denied.

### Configuring 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 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, open the TCP/IP properties page on the server's network adapter, and set the default gateway IP address to the IP address of the ISA Server internal network adapter.



#### Note

Pointing to your ISA Server computer internal network adapter assumes that the server is on the same network segment as your ISA Server computer. If you have a routed network and the 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.

### Sending 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.

---

## Using ISA Server with Exchange Server 2003 Walk-through

### Procedure 7: Enable External Client Access to the Exchange Server

You can use the New Mail Server Rule Publishing Rule Wizard to publish two categories of external client access:

- Web client access, including Outlook Web Access, Outlook Mobile Access, and Exchange Server ActiveSync.
- Client access using the RPC, IMAP, POP3 and SMTP protocols.

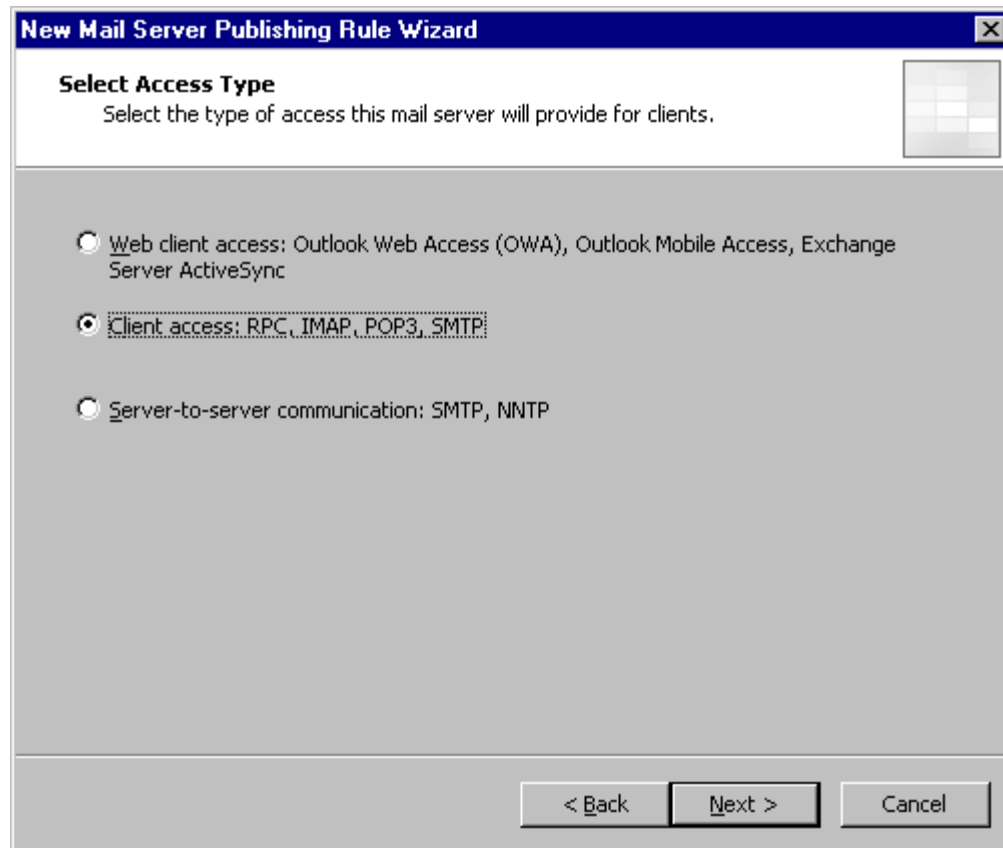
Publication of Web client access services is described in the document "[Outlook Web Access Publishing in ISA Server 2004](http://www.microsoft.com)" (<http://www.microsoft.com>). Enabling client access using the RPC, IMAP, POP3 and SMTP protocols is described in this document.



#### Creating a New Mail Publishing Rule

To enable access by external clients, create a new mail publishing rule using the New Mail Server Publishing Rule Wizard.

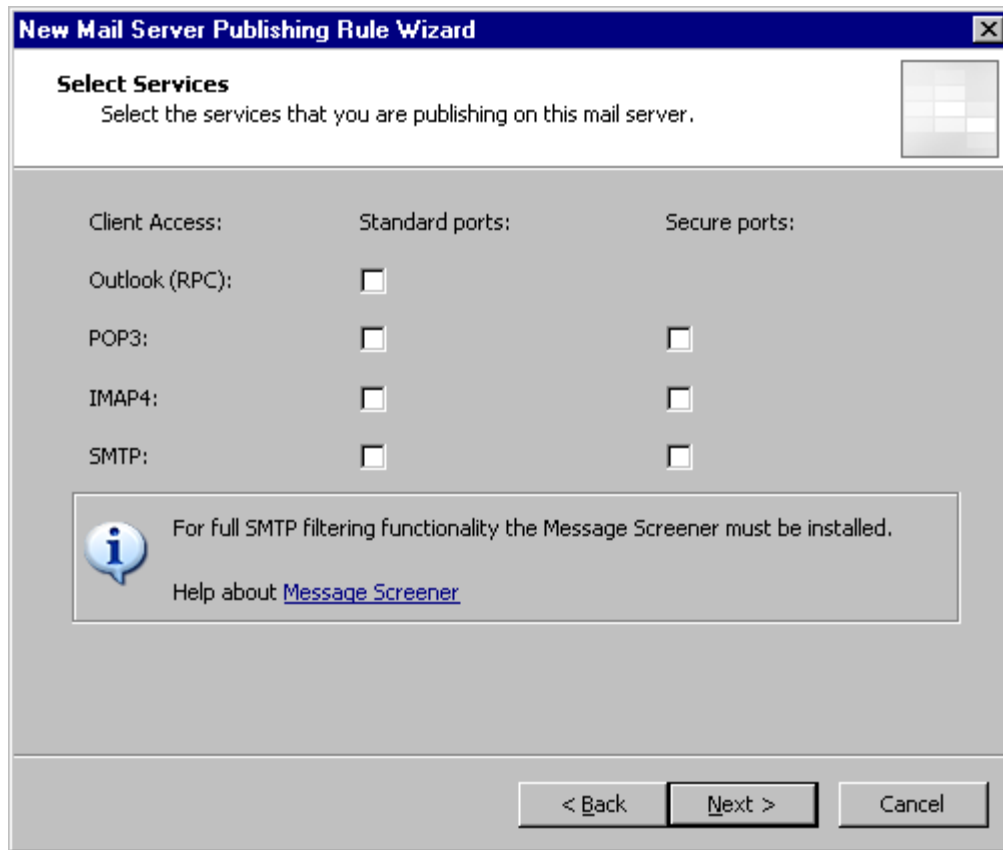
1. Expand Microsoft ISA Server Management and click **Firewall Policy**.
2. On the **Firewall Policy** task pane on the **Tasks** tab, select **Publish a Mail Server** to start the New Mail Server Rule Wizard.
3. On the **Welcome** page of the wizard, provide a name for the rule, such as **External Client Access**, and then click **Next**.
4. On the Select Access Type page, select Client access: RPC, IMAP, POP3, SMTP, and then click **Next**.



### Important

Do not confuse client access over RPC with access through RPC over HTTP, which is described in [Using ISA Server with Exchange Server 2003 Walk-through Procedure 8: Configure RPC over HTTP for Outlook 2003](http://www.microsoft.com) (<http://www.microsoft.com>). If you are going to publish RPC over HTTP, do not select RPC in the following step.

5. On the **Select Services** page, select the protocols on which you want access to be possible. The secure ports are associated with the SSL-encrypted protocols: IMAPS, POP3S, and SMTPS.



6. On the **Select Server** page, provide the IP address of the Exchange server, and then click **Next**.
7. On the **IP Addresses** page, select the network on which ISA Server will listen for requests from external clients. Because you want to receive communication from the External network, select **External**, and then click **Next**.
8. On the **Completing the New Mail Server Publishing Rule Wizard** page, scroll through the rule configuration to verify that you have configured the rule correctly, and then click **Finish**.



#### Note

The New Mail Server Publishing Rule wizard creates a separate publishing rule for each protocol you selected. You can see the individual rules in the Firewall Policy details pane.

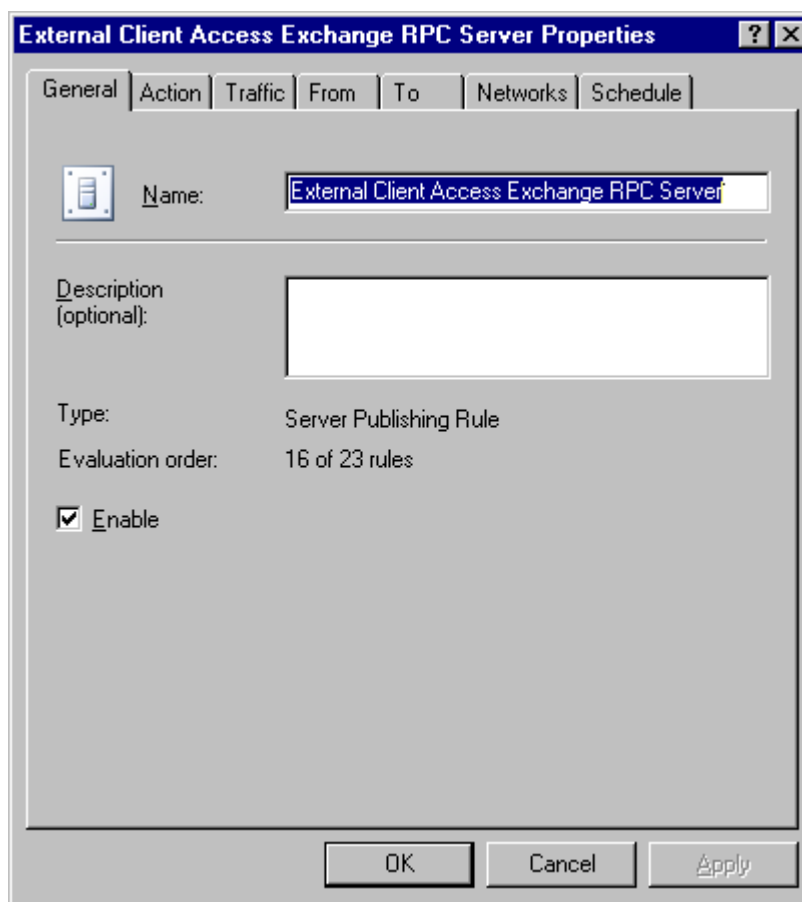
9. In the ISA Server details pane, click **Apply** to apply the changes you have made. It will take a few moments for the changes to be applied.



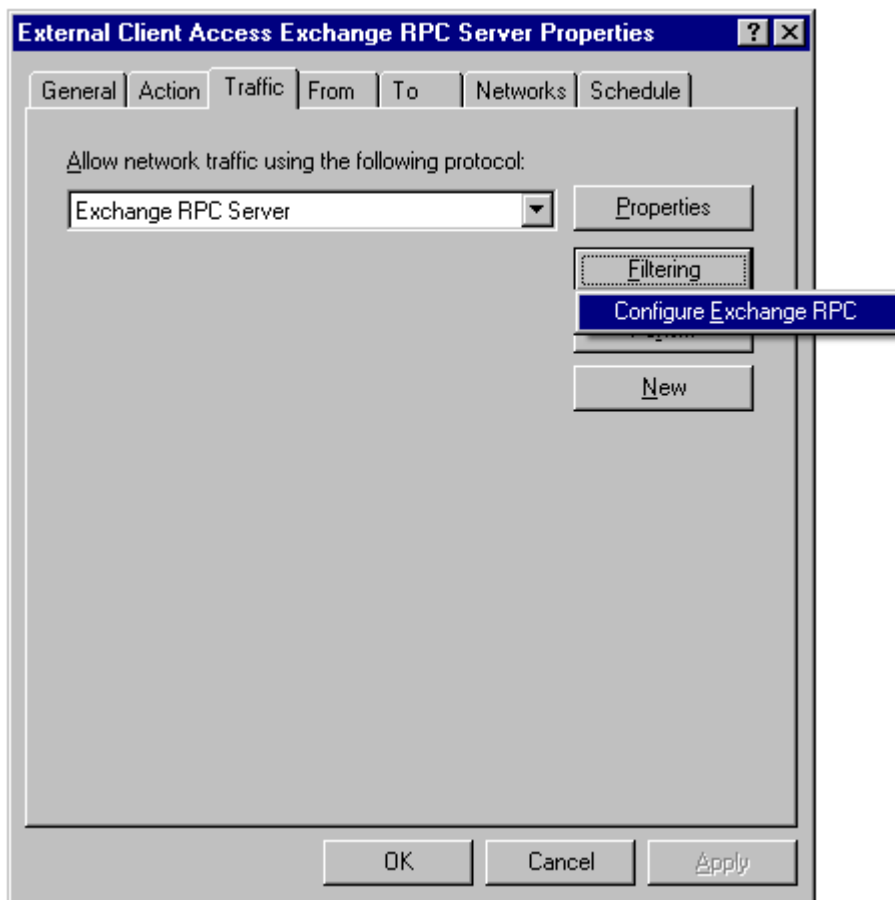
### Requiring Encryption on the RPC Rule

If you created a rule that publishes Exchange RPC Server (not RPC over HTTP, which is described in [Using ISA Server with Exchange Server 2003 Walk-through Procedure 8: Configure RPC over HTTP for Outlook 2003](http://www.microsoft.com) (<http://www.microsoft.com>), you should require encryption for those connections. To require encryption for Exchange RPC Server communication, follow these steps.

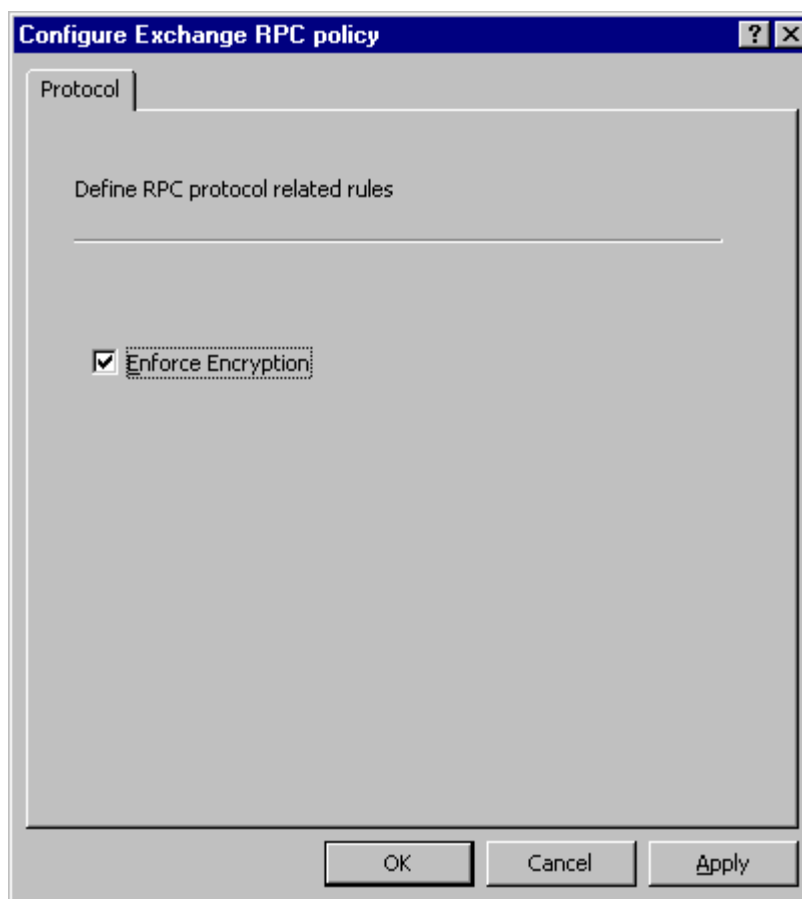
1. Expand Microsoft ISA Server Management and click **Firewall Policy**.
2. On the **Firewall Policy** details pane, double-click the Exchange RPC Server rule. The rule will have the name you provided in the New Mail Server Publishing Rule Wizard, appended with **Exchange RPC Server**, for example, **External Client Access Exchange RPC Server**.



3. In the rule properties, select the **Traffic** tab, click **Filtering**, and select **Configure Exchange RPC** to open the **Configure Exchange RPC Policy** dialog box.



4. Select **Enforce Encryption**, and then click **OK**.



5. Click **OK** to close the rule properties page.
6. In the ISA Server details pane, click **Apply** to apply the changes you have made. It will take a few moments for the changes to be applied.

---

## Using ISA Server with Exchange Server 2003 Walk-through

### Procedure 8: Configure RPC over HTTP for Outlook 2003

Microsoft Office Outlook 2003 clients can access their mailboxes using RPC over HTTP. 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, we recommend that you use your Exchange front-end server as your RPC Proxy server.



**To publish the \rpc virtual directory, create a Web publishing rule.**

1. Open Microsoft ISA Server Management, expand the ISA Server computer node, and click **Firewall Policy**.
2. On the task pane, in the **Tasks** tab, click **Publish a Web Server**, to start the New Web Publishing Rule Wizard.
3. On the **Welcome** page, in the **Name** field, type a name for the rule, such as **Publish RPC over HTTP**, and click **Next**.
4. On the **Select Rule Action** page, ensure that the default **Allow** is selected, which will allow requests to reach your Web server according to the conditions set by the rule. Click **Next**.
5. On the **Define Website to Publish** page, in **Computer name or IP address**, specify the RPC Proxy server that you want to publish. This can be the computer name or the IP address of the computer. Select **Forward the original host header**. (For more information, see the document "[Publishing Web Servers Using ISA Server 2004](http://www.microsoft.com)" (<http://www.microsoft.com>)). In **Path**, specify the **/rpc** directory. Click **Next**.

The screenshot shows the 'New Web Publishing Rule Wizard' dialog box, specifically the 'Define Website to Publish' step. The title bar reads 'New Web Publishing Rule Wizard'. The main heading is 'Define Website to Publish', with a sub-instruction: 'Specify the computer (Web server) on which the website is located. You can publish the entire website or limit access to a specified folder.' Below this, there is a text box for 'Computer name or IP address' containing 'server.fabrikam' and a 'Browse...' button. A checked checkbox is labeled 'Forward the original host header instead of the actual one (specified above)'. Below that, a text box for 'Path' contains '/rpc'. A note states: 'Based on your selection, the following Web site will be published:'. Below this, a text box for 'Site' contains 'http://server.fabrikam/rpc'. At the bottom, there is a note: 'Set the port to which requests should be redirected on the Bridging tab of the rule properties page.' The dialog box has navigation buttons at the bottom: '< Back', 'Next >', and 'Cancel'.

6. On the **Public Name Details** page, provide information regarding what requests will be received by the ISA Server computer and forwarded to the Web server. In **Accepts request**

for, if you select **Any domain name**, any request that is resolved to the IP address of the external Web listener of the ISA Server computer will be forwarded to your website. If you select **This domain name** and provide a specific domain name, such as `www.fabrikam.com`, assuming that domain is resolved to the IP address of the external Web listener of the ISA Server computer, only requests for `http://www.fabrikam.com` will be forwarded to the Web server. Because you are specifying the folder `\rpc`, that would also be required in the request: `http://www.fabrikam.com/rpc`. The required request format is shown in **Site**. Click **Next**.

The screenshot shows the 'New Web Publishing Rule Wizard' dialog box, specifically the 'Public Name Details' step. The title bar reads 'New Web Publishing Rule Wizard'. Below the title bar, the section is titled 'Public Name Details' with a subtitle: 'Specify the public domain name (FQDN) or IP address users will type to reach the published site.' There is a small icon to the right of the subtitle. The main area contains several input fields and a summary section. The 'Accept requests for:' field is a dropdown menu currently set to 'This domain name (type below:)' with a downward arrow. Below this is a note: 'Only requests for this public name or IP address will be forwarded to the published site. For example www.microsoft.com.' The 'Public name:' field contains 'www.fabrikam.com'. The 'Path (optional):' field contains '/rpc'. Below these fields is a summary line: 'Based on your selections, requests sent to this site (host header value) will be accepted:'. The 'Site:' field contains 'http://www.fabrikam.com/rpc'. At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

7. On the **Select Web Listener** page, specify the Web listener that will listen for Web page requests that should be redirected to your Web server, and then click **Next**. If you have not defined a Web listener, click **New** and follow these steps to create a new listener.
  - a. On the **Welcome** page of the New Web Listener Wizard, type the name of the new listener, such as **Listener on External network for publishing RPC over HTTP**, and then click **Next**.
  - b. On the **Listener IP Addresses** page, select the network that will listen for Web requests. Because you want ISA Server to receive requests from the External network (the Internet), the listener should be one or more IP addresses on the External network adapters of ISA Server. Therefore, select **External**, and then click **Next**.

- c. On the **Port Specification** page, the **TCP port** is set to 80 (default setting). If you want to receive HTTPS requests, select **Enable SSL**, verify that the **SSL port** is set to 443 (default setting), and provide the certificate name in the **Certificate** field. This requires that you have a digital certificate installed on the ISA Server computer. For more information about certificates, see "[Digital Certificates for ISA Server 2004](http://www.microsoft.com)" (<http://www.microsoft.com>). We recommend that you disable the TPC port, and enable SSL, so that only HTTPS (encrypted) communication can take place between the Outlook 2003 clients and your RPC Proxy server. Click **Next**.

**New Web Listener Definition Wizard**

**Port Specification**  
Specify the port that the ISA Server computer will use to listen on the selected IP addresses for incoming Web requests.

**HTTP**

Enable HTTP

HTTP port: 80

**SSL**

Enable SSL

SSL port: 443

Certificate:

Help about [Web listener port specification](#)

< Back    Next >    Cancel

- d. On the **Completing the New Web Listener Wizard** page, review the settings, and click **Finish**. On the **Select Web Listener page**, click **Next**.
8. On the **User Sets** page, the default, **All users**, is displayed. This will allow any computer in the External network to access the published Web pages. If you want to specify a specific user set, select **All users** and click **Remove**. Then, use the **Add** button to open the **Add Users** dialog box, from which you can add the user set to which the rule applies. The **Add Users** dialog box also provides access to the New User Sets Wizard through the **New** menu item. For more information about user sets, see [Appendix A: Creating Rule Elements](#). When you have completed the user set selection, click **Next**.
9. On the **Completing the New Web Publishing Rule Wizard** page, scroll through the rule configuration to verify that you have configured the rule correctly, and click **Finish**.

10. In the ISA Server details pane, click **Apply** to apply the changes you have made.

---

## Appendix A: Creating Rule Elements

An ISA Server rule element is an object that you can use to refine ISA Server rules. For example, a subnet rule element represents a subnet within a network. You can create a rule that applies only to a subnet, or a rule that applies to a whole network exclusive of the subnet.

Another example of a rule element is a user set, representing a group of users. By creating a user set and making use of it in an ISA Server rule, you can create a rule that applies only to that set of users.

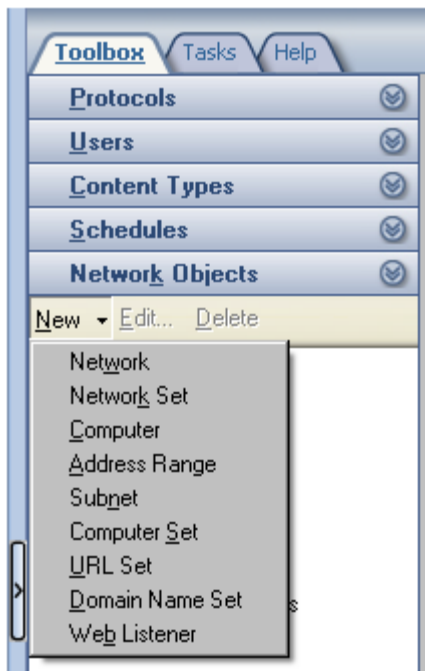
You can see the rule elements that are available to you by expanding the ISA Server computer node, clicking **Firewall Policy**, and selecting the **Toolbox** tab in the task pane. There are five types of rule elements:

- **Protocols.** This rule element type contains protocols that you can use to limit the applicability of access rules. For example, you can allow or deny access on one or more protocols, rather than on all protocols.
- **Users.** In this rule element type, you can create a user set to which a rule will be explicitly applied, or which can be excluded from a rule.
- **Content types.** This rule element type provides common content types to which you may want to apply a rule.
- **Schedules.** In this rule element type, you can designate hours of the week during which the rule applies.
- **Network objects.** In this rule element type, you can create sets of computers to which a rule will apply, or which will be excluded from a rule.



### **Follow this general procedure to create a rule element.**

1. Open Microsoft ISA Server Management, expand the ISA Server computer node, and click **Firewall Policy**.
2. In the task pane, select the **Toolbox** tab.
3. Select the rule element type by clicking the appropriate header (Protocols, Users, Content Types, Schedules, or Network Objects) for that element.
4. At the top of the list of elements, click **New**.



5. Provide the information required. When you have completed the information and clicked **OK** in the dialog box, your new rule element will be created.
6. Click **Apply** in the details pane to apply changes. If you prefer, you can click **Apply** after you have created your Web publishing rules, that is, after you have made all of your changes, rather than after each change. It will take a few moments for the changes to be applied.

---

## Appendix B: Additional Resources

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

*The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, places, or events is intended or should be inferred.*

*Information in this document, including URL and other Internet website references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, people, and events depicted herein are fictitious and no association with any real company, organization, product, person, or event is intended or should be inferred. Complying with all*

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

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

© 2004 Microsoft Corporation. All rights reserved.

*Microsoft, Active Directory, ActiveSync, Outlook, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries/regions.*

Do you have comments about this document? Send [feedback](#).