Contents

Chapter 1
How to Use the Guide

Chapter 2
Installing Certificate Services

Chapter 3
Installing and Configuring the Microsoft Internet Authentication Service

Chapter 4
Installing and Configuring Microsoft DHCP and WINS Server Services

Chapter 5
Configuring DNS and DHCP Support for Web Proxy and Firewall Client Autodiscovery

Chapter 6
Installing and Configuring a DNS Caching-only DNS Server on the Perimeter Network Segment

Chapter 7
Installing ISA Server 2004 on Windows Server 2003

Chapter 8
Backing Up and Restoring Firewall Configuration

Chapter 9
Simplifying Network Configuration with Network Templates

Chapter 10
Configuring ISA Server 2004 SecureNAT, Firewall and Web Proxy Clients

Chapter 11
Configuring ISA Server 2004 Access Policy

Chapter 12
Publishing a Web and FTP Server on the Perimeter Network
Chapter 13
Configuring the Firewall as a Filtering SMTP Relay

Chapter 14
Publishing the Exchange Outlook Web Access, SMTP Server and POP3 Server Sites

Chapter 15
Configuring the ISA Server 2004 Firewall as a VPN Server

Chapter 16
Creating a Site-to-Site VPN with ISA Server 2004 Firewalls
ISA Server 2004 Configuration Guide: How to Use the Guide
Chapter 1

For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

Welcome to the ISA Server 2004 Configuration Guide! This guide was designed to help you get started using ISA Server 2004 firewalls to protect your network and allow secure remote access to your network. While the Guide isn’t a comprehensive set of documentation of all network scenarios, it will expose you to many of the most commonly used features of ISA Server 2004.

Firewalls have traditionally been among the most difficult network devices to configure and maintain. You need to have a basic understanding of TCP/IP and networking services in order to fully understand how a firewall works. The good news is that you don’t need to be a network infrastructure professional to use ISA Server 2004 as your network firewall. ISA Server 2004 is designed from the ground up to secure your network and it does so right out of the box.

This chapter of the ISA Server 2004 Configuration Guide will:

- Help you learn about ISA Server 2004 features
- Provide advice on how to use the Guide to configure the ISA Server 2004 firewall
- Describe the details of the ISA Server 2004 Configuration Guide Lab Configuration
Learn about ISA Server 2004 features

ISA Server 2004 is designed to protect your network from intruders located on the inside of your network and those outside of your network. The ISA Server 2004 firewall does this by controlling what communications can pass through the firewall. The basic concept is simple: if the firewall has a rule that allows the communication through the firewall, then it is passed through. If there is no rule that allows the communication, or if there is a rule that explicitly denies the connection, then the communication is stopped by the firewall.

The ISA Server 2004 firewall contains dozens of features you can use to provide secure access to the Internet and secure access to resources on your network from machines located on the Internet. While this Guide can't provide comprehensive step-by-steps for all the possible features included with ISA Server 2004, we have provided for you a number of step-by-step walkthroughs that will allow you to learn how the most common, and most popular, features of the ISA Server 2004 work.

Firewalls do not work in a vacuum. There are a number of networking services required to assist the firewall protect your network. This guide provides you with detailed information on how to install and configure these services. It's critical that the network is set up properly before you install and configure the firewall. Proper network service support will help you avoid the most common problems seen in ISA Server 2004 firewall deployments.

This guide will walk you through setup and configuration of the following network services and ISA Server 2004 firewall features:

- Install and configure Microsoft Certificate Services
- Install and configure Microsoft Internet Authentication Services (RADIUS)
- Install and configure the Microsoft DHCP and WINS Services
- Configure WPAD entries in DNS to support autodiscovery and autoconfiguration of Web Proxy and Firewall clients
- Install the Microsoft DNS server on a perimeter network server
- Install the ISA Server 2004 firewall software
- Back up and restore the ISA Server 2004 firewall configuration
- Use ISA Server 2004 Network Templates to configure the firewall
- Configure ISA Server 2004 clients
- Create Access Policy on the ISA Server 2004 firewall
- Publish a Web Server on a Perimeter network
- Use the ISA Server 2004 firewall as a spam filtering SMTP relay
- Publish Microsoft Exchange Server services
- Make the ISA Server 2004 firewall into a VPN server
- Create a site to site VPN connection between two networks
Practice configuring the ISA Server 2004 firewall

The firewall is your first line of defense against Internet attackers. A misconfigured firewall can potentially allow Internet attacks access to your network. For this reason, it’s very important that you understand how to configure the firewall for secure Internet access.

By default, the ISA Server 2004 prevents all traffic from moving through the firewall. This is a secure configuration because the firewall must be explicitly configured to allow network traffic through it. However, this level of security can be frustrating when you want to get connected to the Internet as quickly as possible.

We strongly encourage you to create a test lab and perform each of the walkthroughs in this guide. You will learn how to configure the ISA Server 2004 firewall correctly and become familiar with the ISA Server 2004’s configuration interface. You can make mistakes in the practice lab and not worry about attackers taking control of machines on your network. On the lab network, you’ll be able to learn from your mistakes instead of suffering from them.
The ISA Server 2004 Configuration Guide Lab Configuration

We will use a lab network configuration to demonstrate the capabilities and features of ISA Server 2004 in this ISA Server 2004 Configuration Guide. We recommend that you set up a test lab with a similar configuration. If you do not have the resources to create a physical test lab, you can use operating system virtualization software to create the test lab. We recommend that you use Microsoft’s Virtual PC software to create your test lab. You can find more information about Virtual PC at http://www.microsoft.com/windowsxp/virtualpc/.

In this section we will review the following:

• The ISA Server 2004 Configuration Guide network
• Installing Windows Server 2003 on the domain controller machine and then promoting the machine to a domain controller
• Installing Exchange Server 2003 on the domain controller and configuring the Outlook Web Access site to use Basic authentication

ISA Server 2004 Configuration Guide Network Diagram

The figure below depicts the lab network. There are 7 computers on the lab network. However, none of the scenarios we will work with in this ISA Server 2004 Configuration Guide requires all the machines to be running at the same time. This will make it easier for you to use operating system virtualization software to run your lab network.

The network has a local network and a remote network. There is an ISA Server 2004 firewall at the edge of the local and remote networks. All the machines on the local network are members of the msfirewall.org domain, including the ISA Server 2004 firewall machine. No other machines on the lab network are members of the domain.

On our lab network, the external interfaces of the ISA Server 2004 firewalls connect to the production network, which allows them access to the Internet. You should create a similar configuration so that you can test actual Internet connectivity for the clients behind the ISA Server 2004 firewalls.

If you are using operating system virtualization software, then you should note that there are three virtual networks in this lab setup. The Internal network (which contains the domain controller) is on a virtual network, the TRIHOMELAN1 machine on a perimeter network is on another virtual network, and the REMOTECLIENT machine is on a third virtual network. Make sure you separate these virtual networks by placing the machines on different virtual switches so as to prevent Ethernet broadcast traffic from causing unusual results.
Table 1: Details of the Lab Network Configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>EXCHANGE 2003BE</th>
<th>EXTCLIENT</th>
<th>LOCALVPNISA</th>
<th>REMOTEVPN</th>
<th>REMOTECLIENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>10.0.0.2</td>
<td>10.0.0.3</td>
<td>Int: 10.0.0.1</td>
<td>Int: 10.0.1.1</td>
<td>10.0.1.2</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>10.0.0.1</td>
<td>10.0.0.1</td>
<td>192.168.1.60</td>
<td>192.168.1.60</td>
<td>10.0.1.1</td>
</tr>
<tr>
<td>DNS</td>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>WINS</td>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>Services</td>
<td>DC DNS WINS DHCP RADIUS Enterprise CA</td>
<td>IIS WWW SMTP NNTP FTP</td>
<td>ISA Server 2004</td>
<td>ISA Server 2004</td>
<td>IIS WWW SMTP NNTP FTP</td>
</tr>
</tbody>
</table>
## Lab Network Details

<table>
<thead>
<tr>
<th>Setting</th>
<th>TRIHOMELAN1</th>
<th>CLIENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>172.16.0.2</td>
<td>10.0.0.3</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>10.0.0.1</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>DNS</td>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td>WINS</td>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2003</td>
<td>Windows 2000</td>
</tr>
<tr>
<td>Services</td>
<td>DC, DNS, WINS, DHCP, RADIUS, Enterprise CA</td>
<td>IIS: WWW, SMTP, NNTP, FTP</td>
</tr>
</tbody>
</table>

## Installing and Configuring the Internal Network Domain Controller

Other than the ISA Server 2004 firewall computer itself, the second most influential machine used in the scenarios discussed in the *ISA Server 2004 Configuration Guide* is the domain controller. The domain controller computer will also be used to support a number of network services that are used in the variety of ISA Server 2004 scenarios discussed in this guide. It is for this reason that we will walk through the installation and configuration of the domain controller together.

You will perform the following steps to install and configure the Windows Server 2003 domain controller:

- Install Windows Server 2003
- Install and Configure DNS
- Promote the machine to a domain controller

The machine will be a functioning domain controller by the time you have completed these steps and will be ready for you to install Microsoft Exchange Server 2003.

### Installing Windows Server 2003

Perform the following steps on the machine that acts as your domain controller computer:

1. Insert the CD into the CD-ROM tray and restart the computer. Allow the machine to boot from the CD.
2. Windows setup begins loading files required for installation. Press ENTER when you see the *Welcome to Setup* screen.
3. Read the *Windows Licensing Agreement* by pressing the PAGE DOWN key on the keyboard. Then press F8 on the keyboard.
4. On the *Windows Server 2003, Standard Edition Setup* screen you will create a partition for the operating system. In the lab, the entire disk can be formatted as a single partition. Press ENTER.
5. On the Windows Server 2003, Standard Edition Setup screen, select the Format the partition using the NTFS file system by using the up and down arrows on the keyboard. Then press ENTER.

6. Windows Setup formats the hard disk. This can take quite some time if the disk is large. Setup will copy files to the hard disk after formatting is complete.

7. The machine will automatically restart itself after the file copy process is complete.

8. The machine will restart in graphic interface mode. Click Next on the Regional and Language Options page.

9. On the Personalize Your Software page, enter your Name and Organization and click Next.

10. On the Your Product Key page, enter your 25-digit Product Key and click Next.

11. On the Licensing Modes page, select the option that applies to the version of Windows Server 2003 you have. If you have per server licensing, enter the value for the number of connections you have licensed. Click Next.

12. On the Computer Name and Administrator Password page, enter the name of the computer in the Computer Name text box. In the walkthroughs in this Guide, the domain controller/Exchange Server machine is named EXCHANGE2003BE, so we will enter that into the text box. Enter an Administrator password and Confirm password in the text boxes. Be sure to write down this password so that you will remember it later. Click Next.

13. On the Date and Time Settings page, set the correct date, time and time zone. Click Next.

14. On the Networking Settings page, select the Custom settings option.

15. On the Network Components page, select the Internet Protocol (TCP/IP) entry in the Components checked are used by this connection list and click Properties.

16. On the Internet Protocol (TCP/IP) Properties dialog box, select the Use the following IP address option. In the IP address text box, enter 10.0.0.2. In the Subnet mask text box enter 255.255.255.0. In the Default gateway text box enter 10.0.0.1. In the Preferred DNS server text box, enter 10.0.0.2.

17. Click the Advanced button on the Internet Protocol (TCP/IP) Properties dialog box. In the Advanced TCP/IP Settings dialog box, click the WINS tab. On the WINS tab, click the Add button. In the TCP/IP WINS Server dialog box, enter 10.0.0.2 and click Add.

18. Click OK in the Advanced TCP/IP Settings dialog box.


20. Click Next on the Networking Components page.

21. Accept the default selection on the Workgroup or Computer Domain page. We will later make this machine a domain controller and the machine will be a member of the domain we create at that time. Click Next.

22. Installation continues and when it finishes, the computer will restart automatically.

23. Log on to the Windows Server 2003 using the password you created for the Administrator account.

24. On the Manage Your Server page, put a checkmark in the Don't display this page at logon checkbox and close the window.
Install and Configure DNS
The next step is to install the Domain Naming System (DNS) server on the machine that will be the domain controller. This is required because the Active Directory requires a DNS server into which it registers domain-related DNS records. We will install the DNS server and then create the domain into which we will promote the machine.

Perform the following steps to install the DNS server on the domain controller machine:

1. Click **Start** and point to **Control Panel**. Click **Add or Remove Programs**.
2. In the **Add or Remove Programs** window, click the **Add/Remove Windows Components** button on the left side of the window.
3. In the **Windows Components** dialog box, scroll through the list of **Components** and click the **Networking Services** entry. Click **Details**.
4. Place a checkmark in the **Domain Name System (DNS)** checkbox and click **OK**.
5. Click **Next** in the **Windows Components** page.
6. Click **Finish** on the **Completing the Windows Components Wizard** page.
7. Close the **Add or Remove Programs** window.

Now that the DNS server is installed, we can add forward and reverse lookup zones to support our network configuration. Perform the following steps to configure the DNS server:

1. Click **Start** and then click **Administrative Tools**. Click **DNS**.
2. In the **DNS** console, expand the server name and then click on the **Reverse Lookup Zones** node. Right click on the **Reverse Lookup Zones** and click **New Zone**.
3. Click **Next** on the **Welcome to the New Zone Wizard** page.
4. On the **Zone Type** page, select the **Primary zone** option and click **Next**.
5. On the **Reverse Lookup Zone Name** page, select the **Network ID** option and then enter **10.0.0** in the text box below it. Click **Next**.
6. Accept the default selection on the **Zone File** page, and click **Next**.
7. On the **Dynamic Update** page, select the **Allow both nonsecure and secure dynamic updates** option. Click **Next**.
8. Click **Finish** on the **Completing the New Zone Wizard** page.

Now we can create the forward lookup zone for the domain that this machine will be promoted into. Perform the following steps to create the forward lookup zone:

1. Right click the **Forward Lookup Zone** entry in the left pane of the console and click **New Zone**.
2. Click **Next** on the **Welcome to the New Zone Wizard** page.
3. On the **Zone Type** page, select the **Primary zone** option and click **Next**.
4. On the **Zone Name** page, enter the name of the forward lookup zone in the **Zone name** text box. In this example, the name of the zone is **msfirewall.org**. We will enter **msfirewall.org** into the text box. Click **Next**.
5. Accept the default settings on the **Zone File** page and click **Next**.
6. On the **Dynamic Update** page, select the **Allow both nonsecure and secure dynamic updates**. Click **Next**.
7. Click **Finish** on the **Completing the New Zone Wizard** page.
8. Expand the **Forward Lookup Zones** node and click on the **msfirewall.org** zone. Right click on the **msfirewall.org** and click **New Host (A)**.

9. In the **New Host** dialog box, enter the value **EXCHANGE2003BE** in the **Name (uses parent domain name if blank)** text box. In the **IP address** text box, enter the value **10.0.0.2**. Place a checkmark in the **Create associated pointer (PTR) record** checkbox. Click **Add Host**. Click **OK** in the DNS dialog box informing you that the record was created. Click **Done** in the **New Host** text box.

10. Right click on the **msfirewall.org** forward lookup zone and click **Properties**. Click the **Name Servers** tab. On the **Name Servers** tab, click the **exchange2003be** entry and click **Edit**.

11. In the **Server fully qualified domain name (FQDN)** text box, enter the fully qualified domain name of the domain controller computer, **exchange2003be.msfirewall.org**. Click **Resolve**. The IP address of the machine appears in the **IP address** list. Click **OK**.

12. Click **Apply** and then click **OK** on the **msfirewall.org Properties** dialog box.

13. Right click the server name in the left pane of the console and point to **All Tasks**. Click **Restart**.

14. Close the DNS console.

The machine is now ready to be promoted to a domain controller in the **msfirewall.org** domain. Perform the following steps to promote the domain to a domain controller:

1. Click **Start** and click the **Run** command.

2. In the **Run** dialog box, enter **dcpromo** in the **Open** text box and click **OK**.

3. Click **Next** on the **Welcome to the Active Directory Installation Wizard** page.

4. Click **Next** on the **Operating System Compatibility** page.

5. On the **Domain Controller Type** page, select the **Domain controller for a new domain** option and click **Next**.

6. On the **Create New Domain** page, select the **Domain in a new forest** option and click **Next**.

7. On the **New Domain Name** page, enter the name of the domain in the **Full DNS name for new domain** text box. Enter **msfirewall.org** in the text box and click **Next**.

8. On the **NetBIOS Domain Name** page, accept the default NetBIOS name for the domain, which is in this example **MSFIREWALL**. Click **Next**.

9. Accept the default settings on the **Database and Log Folders** page and click **Next**.

10. On the **Shared System Volume** page, accept the default location and click **Next**.

11. On the **DNS Registration Diagnostics** page, select the **I will correct the problem later by configuring DNS manually (Advanced)**. Click **Next**.

12. On the **Permissions** page, select the **Permissions compatible only with Windows 2000 or Windows Server 2003 operating system** option. Click **Next**.

13. On the **Directory Services Restore Mode Administrator Password** page, enter a **Restore Mode Password** and then **Confirm password**. Click **Next**.

14. On the **Summary** page, click **Next**.

15. The machine now starts to configure itself as a domain controller.

16. Click **Finish** on the **Completing the Active Directory Installation Wizard** page.
17. Click Restart Now on the Active Directory Installation Wizard page.
18. Log on as Administrator after the machine restarts.

Installing and Configuring Microsoft Exchange on the Domain Controller

The machine is ready for installing Microsoft Exchange. In this section we will perform the following steps:

- Install the IIS World Wide Web, SMTP and NNTP services
- Install Microsoft Exchange Server 2003
- Configure the Outlook Web Access Web Site

Perform the following steps to install the World Wide Web, SMTP and NNTP services:

1. Click Start and point to Control Panel. Click Add or Remove Programs.
2. In the Add or Remove Programs window, click the Add/Remove Windows Components button on the left side of the window.
3. On the Windows Components page, select the Application Server entry in the Components page. Click the Details button.
4. In the Application Server dialog box, put a checkmark in the ASP.NET checkbox. Select the Internet Information Services (IIS) entry and click Details.
5. In the Internet Information Services (IIS) dialog box, put a checkmark in the NNTP Service checkbox. Put a checkmark in the SMTP Service checkbox. Click OK.
6. Click OK in the Application Server dialog box.
7. Click Next on the Windows Components page.
8. Click OK in the Insert Disk dialog box.
9. In the Files Needed dialog box, enter the path to the i386 folder for the Windows Server 2003 CD in the Copy file from text box. Click OK.
10. Click Finish on the Completing the Windows Components Wizard page.
11. Close the Add or Remove Programs window.

Perform the following steps to install Microsoft Exchange:

1. Insert the Exchange Server 2003 CD into the machine. On the initial autorun page, click the Exchange Deployment Tools link under the Deployment heading.
5. On the Welcome to the Microsoft Exchange Installation Wizard page, click Next.
6. On the License Agreement page, select the I agree option and click Next.
7. Accept the default settings on the Component Selection page and click Next.
8. Select the **Create a New Exchange Organization** option on the **Installation Type** page and click **Next**.

9. Accept the default name in the **Organization Name** text box on the **Organization Name** page, and click **Next**.

10. On the **Licensing Agreement** page, select the **I agree that I have read and will be bound by the license agreement for this product** and click **Next**.

11. On the **Installation Summary** page, click **Next**.

12. In the **Microsoft Exchange Installation Wizard** dialog box, click **OK**.

13. Click **Finish** on the **Completing the Microsoft Exchange Wizard** page when installation is complete.

14. Close all open windows.

The Exchange Server is now installed and you can create user mailboxes at this point. The next step is to configure the Outlook Web Access site to use Basic authentication only. This is a critical configuration option when you want to enable remote access to the OWA site. Later, we will request a Web site certificate for the OWA site and publish the site using a Web Publishing Rule, which will allow remote users to access the OWA site.

Perform the following steps to configure the OWA site to use Basic authentication only:

1. Click **Start** and point to **Administrative Tools**. Click **Internet Information Services (IIS) Manager**.

2. In the **Internet Information Services (IIS) Manager** console, expand the server name and then expand the **Web Sites** node. Expand the **Default Web Site** node.

3. Click on the **Public** node and then right click on it. Click **Properties**.

4. In the **Public Properties** dialog box, click the **Directory Security** tab.

5. On the **Directory Security** tab, click the **Edit** button in the **Authentication and access control** frame.

6. In the **Authentication Methods** dialog box, remove the checkmark from the **Integrated Windows authentication** checkbox. Click **OK**.

7. Click **Apply** and then click **OK**.

8. Click on the **Exchange** node in the left pane of the console and right click on it. Click **Properties**.

9. On the **Exchange Properties** dialog box, click the **Directory Security** tab.

10. On the **Directory Security** tab, click the **Edit** button in the **Authentication and access control** frame.

11. In the **Authentication Methods** dialog box, remove the checkmark from the **Integrated Windows authentication** checkbox. Click **OK**.

12. Click **Apply** and then click **OK** in the **Exchange Properties** dialog box.

13. Click on the **ExchWeb** node in the left pane of the console, then right click on it. Click **Properties**.

14. In the **ExchWeb Properties** dialog box, click the **Directory Security** tab.

15. On the **Directory Security** tab, click the **Edit** button in the **Authentication and access control** frame.

16. In the **Authentication Methods** dialog box, remove the checkmark from the **Enable anonymous access** checkbox. Place a checkmark in the **Basic authentication**
(password is sent in clear text) checkbox. Click Yes in the IIS Manager dialog box informing you that the password is sent in the clear. In the Default domain text box, enter the name of the Internal network domain, which is MSFIREWALL. Click OK.


18. Right click the Default Web Site and click Stop. Right click the Default Web Site again and click Start.
Conclusion

In this ISA Server 2004 Configuration Guide document we discussed the goals of this guide and suggested methods you can use to get the most out of this guide. The remainder of this ISA Server 2004 Configuration Guide provided detailed step-by-step instructions on how to install and configure the domain controller computer on the internal network. In the next chapter of this guide, we will go over the procedures required to install Microsoft Certificate Services on the ISA Server 2004 firewall machine.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

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

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

© 2004 Microsoft Corporation. All rights reserved.

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, place, or event is intended or should be inferred.


The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
ISA Server 2004 Configuration Guide: Installing Certificate Services
Chapter 2

For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

Microsoft Certificate Services can be installed on the domain controller on the internal network and issue certificates to hosts within the internal network domain, as well as to hosts that are not members of the Internal network domain. We will use certificates in a variety of configuration scenarios in this *ISA Server 2004 Configuration Guide* series, including to accomplish the following:

- Allow the ISA Server 2004 firewall to use the L2TP/IPSec VPN protocol for a site-to-site VPN link
- Allow the ISA Server 2004 firewall to use the L2TP/IPSec VPN protocol for a VPN client connection from a remote access VPN client
- Enable remote users to access the Outlook Web Access site using highly secure SSL-to-SSL bridged connections
- Publish secure Exchange SMTP and POP3 services to the Internet

The certificates enable us to use SSL/TLS security. The SSL (Secure Sockets Layer) protocol is a session layer protocol that encrypts data moving between the client and server machines. SSL security is considered the current standard for providing secure remote access to Web sites. In addition, certificates can be used to confirm the identity of VPN clients and servers so that mutual machine authentication can be performed.

In this document we will discuss the following procedures:

- Installing Internet Information Services 6.0 to support the Certificate Authority’s Web enrollment site
- Installing Microsoft Certificate Services in Enterprise CA mode
Install Internet Information Services 6.0

The Certificate Authority's Web enrollment site uses the Internet Information Services World Wide Publishing Service. Because Exchange 2003 has already been installed on this machine, we will not need to manually install the IIS Web services. The Exchange 2003 setup routine requires that you install the IIS Web services so that the Outlook Web Access site functions properly. However, you should confirm that the WWW Publishing Service is enabled before starting installation of the Enterprise CA.

Perform the following steps to confirm that the WWW Publishing Service is running on the domain controller:

1. Click **Start** and point to **Administrative Tools**. Click on **Services**.

2. In the **Services** console, click on the **Standard** tab in the right pane. Scroll down to the bottom of the list and find the **World Wide Web Publishing Service** entry. Double click on that entry.

3. In the **World Wide Web Publishing Server Properties** dialog box, confirm that the **Startup type** is set to **Automatic**, and that the **Service status** is **Started**.

4. Click **Cancel** and close the **Services** console.

Now that we’ve confirmed that the WWW Publishing Service is started, the next step is to install the Enterprise CA software.
Install Microsoft Certificate Services in Enterprise CA Mode

Microsoft Certificate Services will be installed in Enterprise CA mode on the domain controller. There are several advantages to installing the CA in enterprise mode versus standalone mode. These include:

- The root CA certificate is automatically entered into the Trusted Root Certification Authorities certificate store on all domain member machines
- You can use the Certificates MMC snap-in to easily request a certificate. This greatly simplifies requesting machine and Web site certificates
- All machines can be assigned certificates using the Active Directory autoenrollment feature
- All domain users can be assigned user certificates using the Active Directory autoenrollment feature

Note that you do not need to install the CA in enterprise mode. You can install the CA in standalone mode, but we will not cover the procedures involved with installing the CA in standalone mode or how to obtain a certificate from a standalone CA in this ISA Server 2004 Configuration Guide series.

Perform the following steps to install the Enterprise CA on the EXCHANGE2003BE domain controller computer:

1. Click Start, then point to Control Panel. Click on Add or Remove Programs.
2. In the Add or Remove Programs window, click the Add/Remove Windows Components button on the left side of the window.
3. On the Windows Components page, scroll through the list and put a checkmark in the Certificate Services checkbox. Click Yes in the Microsoft Certificate Services dialog box informing you that you may not change the name of the machine or the machine's domain membership while it is acting as a CA. Click Yes to continue.
4. Click Next on the Windows Components page.
5. On the CA Type page, select the Enterprise root CA option and click Next.
6. On the **CA Identifying Information** page, enter a name for the CA in the **Common name for this CA** text box. This should be the DNS host name for the domain controller. Ideally, you will have configured a split DNS infrastructure and this name will be accessible from internal and external locations, so that external hosts will be able to check the certificate revocation list. We will not cover the issue of a split DNS infrastructure in this document. You can find more information about designing and configuring a split DNS infrastructure in the ISA Server 2000 Branch Office Kit document “DNS Considerations for ISA Server 2000 Branch Office Networks” at http://www.tacteam.net/isaserverorg/isabokit/9dnssupport/9dnssupport.htm. In this example we will enter the domain controllers NetBIOS name, **EXCHANGE2003BE**. Click **Next**.
7. If the same machine had been configured as a CA in the past, you will be presented with a dialog box asking if you wish to overwrite the existing key. If you have already deployed certificates to hosts on your network, then do not overwrite the current key. If you have not yet deployed certificates to hosts on your network, then choose to overwrite the existing key. In this example, we have not previously installed a CA on this machine and we do not see this dialog box.


9. Click Yes in the Microsoft Certificate Services dialog box informing you that Internet Information Services must be restarted. Click Yes to stop the service. The service will be restarted for you automatically.

10. Click OK in the Insert Disk dialog box. In the Files Needed dialog box, enter the path to the i386 folder in the Copy file from text box and click OK.

11. Click Finish on the Completing the Windows Components Wizard page.

12. Close the Add or Remove Programs window.

At this point, the Enterprise CA is able to issue certificates to machines via autoenrollment, the Certificates mmc snap-in, or via the Web enrollment site. Later in this ISA Server 2004 Getting Start Guide series, we will issue a Web site certificate to the OWA Web site and also issue machine certificates to the ISA Server 2004 firewall computer and to an external VPN client and VPN gateway (VPN router) machine.
Conclusion

In this ISA Server 2004 Configuration Guide document we discussed the uses of a certificate authority and how to install an Enterprise CA on the domain controller on the internal network. Later in this guide, we will use this Enterprise CA to issue machine certificates to VPN clients and servers and issue a Web site certificate to the Exchange Server's Outlook Web Access Web site.
ISA Server 2004 Configuration Guide: Installing and Configuring the Microsoft Internet Authentication Service
Chapter 3

For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

The Microsoft Internet Authentication Server (IAS) is an industry standard RADIUS server that can be used to authenticate users connecting to the ISA Server 2004 firewall machine. You can use IAS to authenticate Web Proxy clients on the internal network and VPN clients and VPN gateways calling in from an external network location. In addition, you can use RADIUS authentication to remote users who connect to Web servers published using ISA Server 2004 Web Publishing rules.

The major advantage of using RADIUS authentication for Web proxy and VPN connections is that the ISA Server 2004 firewall computer does not need to be a member of the domain to authenticate users whose accounts are contained in the Active Directory on the internal network. Many firewall administrators recommend that the firewall not be a member of the user domain. This prevents attackers who may compromise the firewall from taking advantage of the firewall’s domain member status to amplify an attack against the internal network.

One major drawback to not making the ISA Server 2004 firewall a member of the internal network domain is that you cannot use the Firewall client to provide authenticated access to all TCP and UDP protocols. For this reason, we make the ISA Server 2004 firewall computer a member of the domain in this ISA Server 2004 Configuration Guide series. However, if you choose to not join the firewall to the domain, you can still use IAS to authenticate your VPN and Web Proxy clients.

We will discuss the following procedures in this document:

- Installing the Microsoft Internet Authentication Service
- Configuring the Microsoft Internet Authentication Service
Installing the Microsoft Internet Authentication Service

The Microsoft Internet Authentication Service server is a RADIUS server. We will use the RADIUS server later in this ISA Server 2004 Configuration Guide to enable RADIUS authentication for Web Publishing Rules and investigate how RADIUS authentication can be used to authenticate VPN clients.

Perform the following steps to install the Microsoft Internet Authentication Server on the domain controller EXCHANGE2003BE on the internal network:

1. Click Start and point to Control Panel. Click on Add or Remove Programs.
2. In the Add or Remove Programs window, click the Add/Remove Windows Components button in the left pane of the console.
3. On the Windows Components page, scroll through the Components list and select the Networking Services entry. Click Details.
4. Place a checkmark in the Internet Authentication Service checkbox and click OK.

5. Click Next on the Windows Components page.
6. Click Finish on the Completing the Windows Components Wizard page.
7. Close the Add or Remove Programs window.

The next step is to configure the Internet Authentication Service.
Configuring the Microsoft Internet Authentication Service

You need to configure the IAS server to work together with the ISA Server 2004 firewall computer so that they can communicate properly. At this time, we will configure the IAS Server to work with the ISA Server 2004 firewall. Later we will configure the firewall to communicate with the IAS server.

Perform the following steps on the domain controller on the internal network to configure the IAS server:

1. Click Start and point to Administrative Tools. Click Internet Authentication Service.
2. In the Internet Authentication Service console, expand the Internet Authentication Service (Local) node. Right click on the RADIUS Clients node and click New RADIUS Client.
3. On the Name and Address page of the New RADIUS Client wizard, enter a friendly name for the ISA Server 2004 firewall computer in the Friendly name text box. This name is used to identify the RADIUS client and not used for operational purposes. Enter the fully qualified domain name of the ISA Server 2004 firewall computer in the Client address (IP or DNS) text box.
4. Click the **Verify** button. In the **Verify Client** dialog box, the fully qualified domain name of the ISA Server 2004 firewall computer will appear in the **Client** text box. Click the **Resolve** button. If the RADIUS server is able to resolve the name, the IP address will appear in the **IP address** frame. If the RADIUS server is not able to resolve the name, this indicates that the ISA Server 2004 firewall’s name has not been entered into the DNS. In that case, you can choose to enter the name of the ISA Server 2004 firewall computer into the DNS server on the domain controller, or you can use the IP address on the internal interface of the ISA Server 2004 firewall in the **Client address (IP and DNS)** text box on the **Name or Address** page (as seen above). Click **OK** in the **Verify Client** dialog box.
5. Click **Next** on the **Name and Address** page of the **New RADIUS Client** wizard.

6. On the **Additional Information** page of the wizard, use the default **Client-Vendor** entry, which is **RADIUS Standard**. Enter a password in the **Shared secret** text box and confirm the password in the **Confirm shared secret** text box. This shared secret will allow the ISA Server 2004 firewall and the RADIUS server to confirm each other’s identities. The shared secret should contain at least 8 characters and include mixed case letters, numbers and symbols. Place a checkmark in the **Request must contain the Message Authenticator attribute** check box. Click **Finish**.

7. The new RADIUS client entry appears in the right pane of the console.
8. Close the **Internet Authentication Service** console.

Later in this **ISA Server 2004 Configuration Guide** series we will configure a RADIUS server entry in the **Microsoft Internet Security and Acceleration Server 2004** management console and use that entry for Web and VPN client requests.
Conclusion

In this ISA Server 2004 Configuration Guide document we discussed the uses of a Microsoft Internet Authentication Server and how to install and configure the IAS server on the domain controller on the internal network. Later in this guide we will use this IAS server to authenticate incoming Web and VPN client connections.
ISA Server 2004 Configuration Guide: Installing and Configuring the Microsoft DHCP and WINS Server Services
Chapter 4

For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

The Windows Internet Name Service (WINS) enables machines to resolve NetBIOS names of hosts on remote networks. Machines configured as WINS clients register their names with the WINS server. WINS clients are also able to send name queries to a WINS server to resolve the names to IP addresses. Windows clients can send a broadcast to the local network to resolve NetBIOS names, but when hosts are located on remote networks (networks that are on different network segments or NetBIOS broadcast domains), the broadcasts for name resolutions fail. The only solution is a WINS server.

The WINS server is especially important for VPN clients. The VPN clients are not directly connected to the internal network, and they are not able to use broadcasts to resolve internal network NetBIOS names. (An exception is when you use Windows Server 2003 and enable the NetBIOS proxy, which provides very limited NetBIOS broadcast support.) VPN clients depend on a WINS server to resolve NetBIOS names and to obtain information required to populate the browse list that appears in the My Network Places applet.

The Dynamic Host Configuration Protocol (DHCP) is used to automatically assign IP addressing information to DHCP clients. The DHCP server should be configured on an internal network server and not on the firewall itself. When you configure the DHCP server on the internal network, the ISA Server 2004 firewall can automatically obtain IP addresses from the DHCP server and dynamically assign VPN clients to a special “VPN Clients Network.” Access controls and routing relationships can be configured between the VPN Clients network and any other network defined on the ISA Server 2004 firewall machine.

In the ISA Server 2004 Configuration Guide document, we will go over the procedures required to install the Microsoft WINS and DHCP services. We will then configure a DHCP scope with DHCP scope options.

We will discuss the following procedures in this document:

- Installing the WINS service
- Configuring a DHCP scope
Installing the WINS Service

The Windows Internet Name Service (WINS) is used to resolve NetBIOS names to IP addresses. On modern Windows networks, the WINS service is not required. However, many organizations want to use the My Network Places applet to locate servers on the network. The My Network Places applet depends on the functionality provided by the Windows Browser service. The Windows Browser service is a broadcast-based service that depends on a WINS server to compile and distribute information on servers on each network segment.

In addition, the WINS service is required when VPN clients wish to obtain browse list information for internal network clients. We will install the WINS server on the internal network to support NetBIOS name resolution and the Windows browser service for VPN clients.

Perform the following steps to install WINS:

1. Click Start and point to Control Panel. Click Add or Remove Programs.

2. In the Add or Remove Programs window, click the Add/Remove Windows Components button.

3. On the Windows Components page, scroll through the list of Components and select the Networking Services entry. Click Details.

4. In the Network Services dialog box, put a check in the Windows Internet Name Service (WINS) check box. Next, put a check in the Dynamic Host Configuration Protocol (DHCP) check box. Click OK.

5. Click Next on the Windows Components page.

6. Click OK in the Insert Disk dialog box. In the Files Needed dialog box, enter the path to the i386 folder in the Copy files from text box and click OK.

7. Click Finish on the Completing the Windows Components Wizard page.

8. Close the Add or Remove Programs window.
The WINS server is ready to accept NetBIOS name registrations immediately. The ISA Server 2004 firewall, the domain controller, and the internal network clients are all configured to register with the WINS server in their TCP/IP Properties settings.
Configuring the DHCP Service

The Dynamic Host Configuration Protocol (DHCP) is used to automatically assign IP addressing information to internal network clients and VPN clients. In the scenarios covered in the ISA Server 2004 Configuration Guide, the DHCP server will be used primarily to assign IP addressing information to the VPN clients network. Note that in a production network, you should configure all machines that do not require a static IP address to be DHCP clients.

The DHCP server service has already been installed according to the procedures you performed in Chapter 1 of this Guide. The next step is to configure a DHCP scope that includes a range of IP addresses to assign DHCP clients and DHCP options.

Perform the following steps to configure the DHCP scope:

1. Click Start and point to Administrative Tools. Click on DHCP.
2. In the DHCP console, right click on the server name in the left pane of the console and click Authorize.
3. Click the Refresh button in the mmc button bar. Notice that the icon on the server name in the left pane of the console changes from a red, down-pointing arrow to a green, up-pointing arrow.
4. Right click on the server name in the left pane of the console and click the **New Scope** command.

5. Click **Next** on the **Welcome to the New Scope Wizard** page.

6. On the **Scope Name** page, enter a name for the scope in the **Name** text box and enter an optional description in the **Description** text box. In this example, we will name the scope **Scope1** and will not enter a description. Click **Next**.

7. On the **IP Address Range** page, enter a **Start IP address** and an **End IP address** in the text boxes provided. The start and end addresses represent the beginning and end of a range of addresses you want available for DHCP clients. In this example, we will enter the start address as **10.0.0.200** and the end address as **10.0.0.219**. This provides twenty addresses for DHCP clients. The ISA Server 2004 firewall will later be configured to allow up to 10 concurrent VPN connections, so it will automatically take 10 of these addresses and use one of them for itself, with the remainder available to assign to the VPN clients. The ISA Server 2004 firewall will be able to obtain more IP addresses from the DHCP server if they are required. You can configure the subnet mask settings in either the **Length** or **Subnet mask** text boxes. In our current example, the addresses will be on the same network ID as the internal network, so we will enter the value **24** into the **Length** text box. The **Subnet mask** value is automatically added when the **Length** value is added. Click **Next**.

8. Do not enter any exclusions on the **Add Exclusions** page. Click **Next**.

9. Accept the default lease duration of **8 Days** on the **Lease Duration** page. Click **Next**.

10. On the **Configure DHCP Options** page, select the **Yes, I want to configure these options now** option and click **Next**.

11. On the **Router (Default Gateway)** page, enter the IP address of the internal interface of the ISA Server 2004 firewall machine in the **IP address** text box and click **Add**. Click **Next**.
12. On the **Domain Name and DNS Servers** page, enter the domain name used on the internal network in the **Parent domain** text box. This is the domain name that will be used by DHCP clients to fully qualify unqualified names, such as the wpad entry that is used for Web Proxy and Firewall client autodiscovery. In this example, the domain name is **msfirewall.org** and we will enter that value in the text box. In the **IP address** text box, enter the IP address of the DNS server on the internal network. In this example, the domain controller is also the internal network's DNS server, so we will enter the value **10.0.0.2** into the **IP address** text box and then click **Add**. Click **Next**.
13. On the WINS Servers page, enter the IP address of the WINS server in the IP address text box and click Add. In this example, the WINS server is located on the domain controller on the internal network, so we will enter 10.0.0.2. Click Next.

14. On the Activate Scope page, select the Yes, I want to activate this scope now option and click Next.

15. Click Finish on the Completing the New Scope Wizard page.

16. In the left pane of the DHCP console, expand the Scope node and then click on the Scope Options node. You will see a list of the options you configured.

17. Close the DHCP console.

At this point the DHCP server is ready to provide DHCP addressing information to DHCP clients on the internal network and to the VPN clients network. However, the ISA Server 2004 firewall will not actually lease the addresses until we have enabled the VPN server on the firewall.
Conclusion

In this ISA Server 2004 Configuration Guide document we discussed the uses of the Microsoft WINS and DHCP servers, installed the server services on the domain controller, and configured a scope on the DHCP server. Later in this guide we will see how the addition of the WINS and DHCP service help enhance the VPN client experience.
ISA Server 2004 Configuration Guide: Configuring DNS and DHCP Support for Web Proxy and Firewall Client Autodiscovery

Chapter 5

For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

The Web Proxy Autodiscovery Protocol (WPAD) can be used to allow Web browsers and the Firewall client application to automatically discover the address of the ISA Server 2004 firewall. The client can then download autoconfiguration information from the firewall after the Web Proxy or Firewall client discovers the address.

WPAD solves the problem of automatically provisioning Web browsers. The default setting on Internet Explorer 6.0 is to autodiscover Web proxy client settings. When this setting is enabled, the browser can issue a DHCPINFORM message or a DNS query to find the address of the ISA Server 2004 from which it can download autoconfiguration information. This greatly simplifies Web browser setup so that it automatically uses the firewall to connect to the Internet.

The ISA Server 2004 Firewall client can also use the wpad entry to find the ISA Server 2004 firewall and download Firewall client configuration information.

In this ISA Server 2004 Configuration Guide document, we discuss how to:

- Configure DHCP WPAD support, and
- Configure DNS WPAD support

After the wpad information is entered into DHCP and DNS, Web Proxy and Firewall clients will not require manual configuration to connect to the Internet through the ISA Server 2004 firewall machine.
Configure DHCP WPAD Support

The DHCP scope option number 252 can be used to automatically configure Web Proxy and Firewall clients. The Web Proxy or Firewall client must be configured as a DHCP client, and the logged on user must be a member of the local administrators group or Power users group (for Windows 2000). On Windows XP systems, the Network Configuration Operators group also has permission to issue DHCP queries (DHCPINFORM messages).

**Note:**
For more information about the limitations of using DHCP for autodiscovery with Internet Explorer 6.0, please see KB article Automatic Proxy Discovery in Internet Explorer with DHCP Requires Specific Permissions at http://support.microsoft.com/default.aspx?scid=kb;en-us;312864

Perform the following steps at the DHCP server to create the custom DHCP option:

1. Open the DHCP console from the Administrative Tools menu and right click your server name in the left pane of the console. Click the Set Predefined Options command.

2. In the Predefined Options and Values dialog box, click Add.

3. In the Option Type dialog box, enter the following information:
   - **Name:** wpad
   - **Data type:** String
   - **Code:** 252
   - **Description:** wpad entry
   - Click OK.
4. In the **Value** frame, enter the URL to the ISA Server 2000 firewall in the **String** text box. The format for this value is:

```
http://ISAServername:AutodiscoveryPort Number/wpad.dat
```

The default autodiscovery port number is TCP 80. You can customize this value in the **ISA Management** console. We will cover this subject in more detail later.

In the current example, enter the following into the **String** text box:

http://isalocal.msfirewall.org:80/wpad.dat

Make sure to enter wpad.dat in all **lower case** letters. For more information on this problem, please refer to KB article "**Automatically Detect Settings** Does Not Work if You Configure DHCP Option 252 at http://support.microsoft.com/default.aspx?scid=kb;en-us;307502

Click **OK**.
5. Right click the **Scope Options** node in the left pane of the console and click the **Configure Options** command.

6. In the **Scope Options** dialog box, scroll through the list of **Available Options** and put a checkmark in the **252 wpad** check box. Click **Apply** and then click **OK**.

7. The **252 wpad** entry now appears in the right pane of the console under the list of **Scope Options**.

8. Close the **DHCP** console.

At this point a DHCP client that has a logged on user who is a local administrator will be able to use DHCP wpad support to automatically discover the ISA Server 2004 firewall and subsequently autoconfigure itself. However, the ISA Server 2004 firewall must be configured to support publishing autodiscovery information. We will do this configuration later in this **ISA Server 2004 Configuration Guide**.
Configure DNS WPAD Support

Another method that used to deliver autodiscovery information to Web Proxy and Firewall clients is DNS. You can create a wpad alias entry in DNS and allow browser clients to use this information to automatically configure themselves. This is in contrast to the situation we saw with the DHCP method, where the logged-on user needed to be a member of a specific group in the Windows operating system.

Name resolution is a pivotal component to make this method of Web Proxy and Firewall client autodiscovery work correctly. In this case, the client operating system must be able to fully qualify the name `wpad` since the Web Proxy and Firewall client only knows that it needs to resolve the name `wpad`. It does not know what specific domain name it should append to the query to resolve the name `wpad`. We will cover this issue in detail later in the chapter.

Note:
In contrast to the DHCP method of assigning autodiscovery information to Web Proxy and Firewall clients, you do not have the option to use a custom port number to publish autodiscovery information when using the DNS method. You must publish autodiscovery information on TCP 80 when using the DNS method.

You need to perform the following steps to configure DNS support for Web Proxy and Firewall client autodiscovery of the ISA Server 2004 firewall:

- Create the wpad entry in DNS
- Configure the client to use the fully qualified wpad alias
- Configure the client browser to use autodiscovery
Create the Wpad Entry in DNS

The first step is to create a wpad alias entry in DNS. This alias (also known as a CNAME record) points to a Host (A) record for the ISA Server 2004 firewall. The Host (A) record resolves the name of the ISA Server 2004 firewall to the Internal IP address of the firewall.

Create the Host (A) record before you create the CNAME record. If you enable automatic registration in DNS, the ISA Server 2004 firewall’s name and IP address will already be entered into a DNS Host (A) record. If you have not enabled automatic registration, you will need to create the Host (A) record for the ISA Server 2004 firewall yourself.

In the following example, the ISA Server 2004 firewall has automatically registered itself with DNS because the Internal interface of the ISA Server 2004 firewall is configured to do so, and the DNS server is configured to accept unsecured dynamic registrations.

Perform the following steps on the DNS server on the domain controller on the Internal network:

1. Click Start and select Administrative Tools. Click the DNS entry. In the DNS management console, right click on the forward lookup zone for your domain and click the New Alias (CNAME) command.

2. In the New Resource Record dialog box, enter wpad in the Alias name (uses parent domain if left blank) text box. Click the Browse button.

3. In the Browse dialog box, double click on your server name in the Records list.
4. In the Browse dialog box, double click on the Forward Lookup Zone entry in the Records frame.

5. In the Browse dialog box, double click on the name of your forward lookup zone in the Records frame.
6. In the Browse dialog box, select the name of the ISA Server 2000 firewall in the Records frame. Click OK.

7. Click OK in the New Resource Record dialog box.
8. The CNAME (alias) entry appears in the right pane of the **DNS** management console.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>_nsdcs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>_sites</td>
<td></td>
<td></td>
</tr>
<tr>
<td>_top</td>
<td></td>
<td></td>
</tr>
<tr>
<td>_udp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>domaindnzones</td>
<td></td>
<td></td>
</tr>
<tr>
<td>forestdnzones</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(same as parent folder)</td>
<td>Start of Authority (SOA)</td>
<td>[31], exchange2003be.msfire...</td>
</tr>
<tr>
<td>(same as parent folder)</td>
<td>Name Server (NS)</td>
<td>exchange2003be.msfirewall....</td>
</tr>
<tr>
<td>(same as parent folder)</td>
<td>Host (A)</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td>exchange2003be</td>
<td>Host (A)</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td>isalocal</td>
<td>Host (A)</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>wpad</td>
<td>Alias (CNAME)</td>
<td>isalocal.msfirewall.org</td>
</tr>
</tbody>
</table>

9. Close the **DNS Management** console.
Configure the Client to Use the Fully Qualified wpad Alias

The Web Proxy and Firewall client need to be able to resolve the name wpad. The Web Proxy and Firewall client configurations are not aware of the domain containing the wpad alias. The Web Proxy and Firewall client operating system must be able to provide this information to the Web Proxy and Firewall client.

DNS queries must be fully qualified before sending the query to the DNS server. A fully qualified request contains a host name and a domain name. The Web Proxy and Firewall client only know the host name portion. The Web Proxy and Firewall client operating system must be able to provide the correct domain name, which it appends to the wpad host name, before it can send a DNS query to the DNS server.

There are a number of methods you can use to insure that a proper domain name is appended to wpad before the query is sent to the DNS server. Two popular methods for doing this include:

- Using DHCP to assign a primary domain name
- Configuring a primary domain name in the client operating system’s network identification dialog box.

We already configured a primary DNS name to assign DHCP clients when we configured the DHCP scope. The following steps demonstrate how to set the primary domain name to append to unqualified DNS queries:

**Note:** You do not need to perform these steps on the client machine on the Internal network in our example network. The reason for this is that the client is a member of the Active Directory domain on the Internet network. However, you should go through the following steps to see how the primary domain name is configured on non-domain member computers.

1. Right click **My Computer** on the desktop and click **Properties**.

2. In the **System Properties** dialog box, click the **Network Identification** tab. Click the **Properties** button.

3. In the **Identification Changes** dialog box, click the **More** button.
4. In the **DNS Suffix and NetBIOS Computer Name** dialog box, enter the domain name that contains your wpad entry in the **Primary DNS suffix of this computer** text box. The operating system will append this domain name to the wpad name before sending the DNS query to the DNS server. By default, the primary domain name is the same as the domain name the machine belongs to. If the machine is not a member of a domain, then this text box will be empty. Note the **Change primary DNS suffix when domain membership changes** is enabled by default. In the current example, the machine is not a member of a domain.

Cancel out of each of the dialog boxes so that you do not configure a primary domain name at this time.

Note that if you have multiple domains and clients on your Internal network that belong to multiple domains, you will need to create wpad CNAME alias entries for each of the domains.
Configure the Client Browser to Use Autodiscovery

The next step is to configure the browser to use autodiscovery. To configure the Web browser to use autodiscovery to automatically configure itself to use the ISA Server 2000 firewall’s Web Proxy service:

1. Right click on the Internet Explorer icon on the desktop and click Properties.
2. In the Internet Properties dialog box, click the Connections tab. Click the LAN Settings button.
3. In the Local Area Network (LAN) Settings dialog box, put a checkmark in the Automatically detect settings check box. Click OK.
4. Click Apply and then click OK in the Internet Properties dialog box.

The next step is to configure the ISA Server 2000 firewall publish autodiscovery information for autodiscovery Web Proxy and Firewall clients.
Conclusion

In this ISA Server 2004 Configuration Guide document we discussed the uses of a Microsoft Internet Authentication Server and how to install and configure the IAS server on the domain controller on the Internal network. Later in this guide, we will use this IAS server to authenticate incoming Web and VPN client connections.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

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

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

© 2004 Microsoft Corporation. All rights reserved.

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, place, or event is intended or should be inferred.


The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
ISA Server 2004 Configuration Guide: Installing and Configuring a DNS Caching-only DNS Server on the Perimeter Network Segment

Chapter 6

For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

DNS servers allow client systems to resolve names to IP addresses. Internet applications need to know the IP address of a destination host before they can connect. A caching-only DNS server is a special type of DNS in that it is not authoritative for any domain. This means the caching-only DNS server does not contain any domain resource records. Instead, the caching-only DNS server accepts DNS queries from DNS client systems, resolves the name in the request, caches the answer and returns the cached answer to the client that made the initial DNS query.

A caching-only DNS server is an optional component. You do not need to use a caching-only DNS server. You can move to the next document in this ISA Server 2004 Configuration Guide if you do not plan to use a perimeter network segment. If you do choose to use a perimeter network segment, you should follow the procedures outlined in this document.

DNS servers located in the perimeter network are used for two primary purposes:

- name resolution for domains under your administrative control
- caching-only DNS services for internal network clients, or as forwarders for internal network DNS servers

A perimeter network DNS server can contain DNS zone information about publicly accessible domains. For example, if you have implemented a split DNS infrastructure, the public records for your domain would be contained on the perimeter network DNS server. Internet-located hosts can query this DNS server and obtain the IP addresses required to connect to resources you have published through the ISA Server 2004 firewall.

The DNS server on the perimeter network can also act as a caching-only DNS server. In this role, the machine contains no DNS resource record information. Instead, the caching-only DNS server resolves Internet host names and caches the results of its queries. It can then return answers from cache if it has already resolved the name. If not, it can query other DNS servers on the Internet and cache the results before returning the answer to the client.

In this document we will discuss the following procedures:

- Installing the DNS server service
- Configuring the DNS server as a secure caching-only DNS server
Installing the DNS Server Service

The first step is to install the DNS server service on the perimeter network host. This machine will act as both a secure caching-only DNS server and a publicly accessible Web and SMTP relay machine.

Perform the following steps to install the DNS server service on the perimeter network host computer, TRIHOMELAN1:

1. Click Start; point to Control Panel. Click Add or Remove Programs.
2. In the Add or Remove Programs window, click the Add/Remove Windows Components button on the left side of the window.
3. On the Windows Components page, scroll through the list of Components and select Networking Services. Click the Details button.
4. In the Networking Services dialog box, put a checkmark in the Domain Name System (DNS) check box and click OK.

5. Click Next on the Windows Components page.
6. Click OK in the Insert Disk dialog box. In the Files Needed dialog box, enter the path to the i386 folder in the Copy files from text box and click OK.
7. Click Finish on the Completing the Windows Components Wizard page.

The next step is to configure the DNS server as a secure caching-only DNS server.
Configuring the DNS Server as a Secure Caching-only DNS Server

The DNS server on the perimeter network will be in direct contact with Internet hosts. These hosts can be DNS clients that query the perimeter network DNS server for addresses of publicly accessible domain resources. They can also be DNS servers on the Internet that the caching-only DNS server contacts to resolve Internet host names for internal network clients. In this example, the DNS server will act as a caching-only DNS server and will not host public DNS records for the domain.

Perform the following steps on the perimeter network DNS servers to configure it as a secure caching-only DNS server:

1. Click Start and point to Administrative Tools. Click on DNS.
2. In the DNS management console, right click on the server name in the left pane of the console and click Properties.
3. In the DNS server’s Properties dialog box, click on the Root Hints tab. The entries in the Name servers list are for Internet root name servers that the caching-only DNS server uses to resolve Internet host names. Without this list of root DNS servers, the caching-only DNS server will not be able to resolve the names of machines located on the Internet.

![TRIHOMELEN1 Properties](image)
4. Click on the **Forwarders** tab. Make sure there is not a checkmark in the **Do not use recursion for this domain** check box. If this option is selected, the caching-only DNS server cannot use the root hints list of the root Internet DNS server to resolve Internet host names. Select this option only if you decide to use a forwarder. In this case, we do not use a forwarder.

![Forwarders tab screenshot](image)

Forwarders are servers that can resolve DNS queries not answered by this server. Forward queries for names in the following DNS domains.

- **DNS domain:**
  - All other DNS domains
  - [New...](#)
  - [Remove...](#)

To add a forwarder, select a DNS domain, type the forwarder's IP address below, and then click Add.

- **Selected domain's forwarder IP address list:**
  - [Add](#)
  - [Remove](#)
  - [Up](#)
  - [Down](#)

- **Number of seconds before forward queries time out:** 5
  - [Do not use recursion for this domain](#)

5. Click the **Advanced** tab. Confirm that there is a checkmark in the **Secure cache against pollution** check box. This prevents Internet DNS servers and attackers from inserting additional records in a DNS response. These additional records could be used as part of a co-coordinated DNS attack.
6. Click the Monitoring tab. Put checkmarks in the **A simple query against this DNS server** and **A recursive query to other DNS servers** check boxes. Then click the **Test Now** button. Note in the Test results frame that the **Simple Query** shows a Pass, while the **Recursive Query** displays a Fail. The reason is that an Access Rule has not been created that allows the caching-only DNS server access to the Internet. Later, we will create an Access Rule on the ISA Server 2004 firewall that allows the DNS server outbound access to DNS servers on the Internet.
7. Click **Apply** and then click **OK** in the DNS server's **Properties** dialog box.

8. Close the **DNS** management console.

At this point, the caching-only DNS server is able to resolve Internet host names. Later, we will create Access Rules allowing hosts on the internal network to use the caching-only DNS server to resolve Internet host names.
Conclusion

In this ISA Server 2004 Configuration Guide document we discussed the uses of a caching-only DNS server and how to install and configure the Microsoft DNS server service. Later in this guide we will configure Access Policies that allow hosts on the internal network to use this DNS server and allow the caching-only DNS server to connect to the Internet.
Chapter 7

For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

In this ISA Server 2004 Configuration Guide document we will install the ISA Server 2004 software onto the Windows Server 2003 computer we installed and configured in Chapter 1. Installing ISA Server 2004 is straightforward as there are only a few decisions that need to be made during installation.

The most important configuration made during installation is the Internal network IP address range(s). Unlike ISA Server 2000, ISA Server 2004 does not use a Local Address Table (LAT) to define trusted and untrusted networks. Instead, the ISA Server 2004 firewall asks for the IP addresses defining a network entity known as the Internal network. The internal network contains important network servers and services such as Active Directory domain controllers, DNS, WINS, RADIUS, DHCP, firewall management stations, and others. These are services the ISA Server 2004 firewall needs to communicate with immediately after installation is complete.

Communications between the Internal network and the ISA Server 2004 firewall are controlled by the firewall’s System Policy. The System Policy is a collection of pre-defined Access Rules that determine the type of traffic allowed inbound and outbound to and from the firewall immediately after installation. The System Policy is configurable, which enables you can tighten or loosen the default System Policy Access Rules.

In the document we will discuss the following procedures:

• Installing ISA Server 2004 on Windows Server 2003
• Reviewing the Default System Policy
Installing ISA Server 2004

Installing ISA Server 2004 on Windows Server 2003 is relatively straightforward. The major decision you make during setup is what IP addresses should be part of the Internal network. The Internal network address configuration is important because the firewall’s System Policy uses the Internal network addresses to define a set of Access Rules.

Perform the following steps to install the ISA Server 2004 software on the dual-homed Windows Server 2003 machine:

1. Insert the ISA Server 2004 CD-ROM into the CD drive. The autorun menu will appear.

2. On the Microsoft Internet Security and Acceleration Server 2004 page, click the link for Review Release Notes and read the release notes. The release notes contain useful information about important issues and configuration options. After reading the release notes, close the release notes window and then click the Read Setup and Feature Guide link. You don’t need to read the entire guide right now, but you may want to print it out to read later. Close the Setup and Feature Guide window. Click the Install ISA Server 2004 link.

3. Click Next on the Welcome to the Installation Wizard for Microsoft ISA Server 2004 page.

4. Select the I accept the terms in the license agreement option on the License Agreement page. Click Next.

5. On the Customer Information page, enter your name and the name of your organization in the User Name and Organization text boxes. Enter Product Serial Number. Click Next.

6. On the Setup Type page, select the Custom option. If you do not want to install the ISA Server 2004 software on the C: drive, then click the Change button to change the location of the program files on the hard disk. Click Next.

Setup Type
Choose the setup type that best suits your needs.

- **Typical**
  Main program features will be installed. Requires approximately 27MB of disk space (not including cache allocation).

- **Complete**
  All program features will be installed. (Requires the most disk space.)

- **Custom**
  Choose which program features you want installed. Recommended for advanced users.

Install to:
C:\Program Files\Microsoft ISA Server\

< Back  Next >  Cancel
7. On the **Custom Setup** page you can choose which components to install. By default, the **Firewall Services** and **ISA Server Management** options are installed. The **Message Screener**, which is used to help prevent spam and file attachments from entering and leaving the network, is not installed by default; neither is the **Firewall Client Installation Share**. You need to install the IIS 6.0 SMTP service on the ISA Server 2004 firewall computer *before* you install the **Message Screener**. Use the default settings and click **Next**.

8. On the **Internal Network** page, click the **Add** button. The Internal network is different than the LAT, which was used in ISA Server 2000. In the case of ISA Server 2004, the Internal network contains trusted network services the ISA Server 2004 firewall must be able to communicate. Examples of such services include Active Directory domain controllers, DNS, DHCP, terminal services client management workstations, and others. The firewall System Policy automatically uses the Internal network. We will look at the System Policy later in this document.
9. In the Internal Network setup page, click the **Select Network Adapter** button.

10. In the **Select Network Adapter** dialog box, remove the checkmark from the **Add the following private ranges**... checkbox. Leave the checkmark in the **Add address ranges based on the Windows Routing Table** checkbox. Put a checkmark in the checkbox next to the adapter connected to the Internal network. The reason why we remove the checkmark from the add private address ranges checkbox is that you may wish to use these private address ranges for perimeter networks. Click **OK**.
11. Click **OK** in the **Setup Message** dialog box informing you that the Internal network was defined, based on the Windows routing table.

12. Click **OK** on the Internal network address ranges dialog box.

13. Click **Next** on the **Internal Network** page.
14. On the **Firewall Client Connection Settings** page, place checkmarks in the **Allow non-encrypted Firewall client connections** and **Allow Firewall clients running earlier versions of the Firewall client software to connect to ISA Server** checkboxes. These settings will allow you to connect to the ISA Server 2004 firewall using downlevel operating systems and from Windows 2000/Windows XP/Windows Server 2003 operating systems running the ISA Server 2000 version of the Firewall client. Click **Next**.

15. On the **Services** page, click **Next**.
16. Click **Install** on the **Ready to Install the Program** page.
17. On the **Installation Wizard Completed** page, click **Finish**.

18. Click **Yes** in the **Microsoft ISA Server** dialog box informing you that the machine must be restarted.
19. Log on as Administrator after the machine restarts.
Viewing the System Policy

By default, ISA Server 2004 does not allow outbound access to the Internet from any protected network and it does not allow Internet hosts access the firewall or any networks protected by the firewall. However, a default firewall System Policy is installed that allows network management tasks to be completed.

Note:
A protected network is any network defined by the ISA Server 2004 firewall that is not part of the default External network.

Perform the following steps to see the default firewall System Policy:

1. Click Start and point to All Programs. Point to Microsoft ISA Server and click ISA Server Management.

2. In the Microsoft Internet Security and Acceleration Server 2004 management console, expand the server node in the scope pane (left pane) and click on the Firewall Policy node. Right click on the Firewall Policy node, point to View and click Show System Policy Rules.

3. Click the Show/Hide Console Tree button and then click the Open/Close Task Pane arrow (the little blue arrow on the left edge of the task pane on the right side of the console). Notice that the ISA Server 2004 Access Policy represents an ordered list. Policies are processed from top to bottom, which is a significant departure from how ISA Server 2000 processed Access Policy. The System Policy represents a default list of rules controlling access to and from the ISA Server 2004 firewall by default. Note that the System Policy Rules are ordered above any custom Access Policies you will create, and therefore are processed before them. Scroll down the list of System Policy Rules. Notice that the rules are defined by:
Order number
Name
Action (Allow or Deny)
Protocols
From (source network or host)
To (destination network or host)
Condition (who or what the rule applies to)

You may want to widen the Name column to get a quick view rule the rule descriptions. Notice that not all the rules are enabled. Disabled System Policy Rules have a tiny down-pointing red arrow in their lower right corner. Many of the disabled System Policy Rules will become automatically enabled when you make configuration changes to the ISA Server 2004 firewall, such as when you enable VPN access.

Notice that one of the System Policy Rules allows the firewall to perform DNS queries to DNS servers on all networks.

4. You can change the settings on a System Policy Rule by double clicking on the rule.
5. Review the System Policy Rules and then hide the rules by clicking the Show/Hide System Policy Rules button in the console’s button bar. This is the depressed (pushed in) button seen in the figure below.

The following table includes a complete list of the default, built-in System Policy:

<table>
<thead>
<tr>
<th>Order</th>
<th>Name</th>
<th>Action</th>
<th>Protocols</th>
<th>From</th>
<th>To</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Allow access to directory services for authentication purposes</td>
<td>Allow</td>
<td>LDAP, LDAP(GC), LDAP(UDP), LDAPS, LDAPS(GC)</td>
<td>Local Host</td>
<td>Internal</td>
<td>All Users</td>
</tr>
<tr>
<td>2</td>
<td>Allow Remote Management using MMC</td>
<td>Allow</td>
<td>MS Firewall Control, RPC(all interfaces), NetBIOS Datagram, NetBIOS Name Service</td>
<td>Remote Management Computers</td>
<td>Local Host</td>
<td>All Users</td>
</tr>
<tr>
<td>Order</td>
<td>Name</td>
<td>Action</td>
<td>Protocols</td>
<td>From</td>
<td>To</td>
<td>Condition</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------</td>
<td>-------------------</td>
<td>---------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>3</td>
<td>Allow Remote Management using Terminal Server</td>
<td>Allow</td>
<td>NetBIOS Session</td>
<td>Remote Management Computers</td>
<td>Local Host</td>
<td>All Users</td>
</tr>
<tr>
<td>4</td>
<td>Allow remote logging to trusted servers using NetBIOS</td>
<td>Allow</td>
<td>NetBIOS Datagram</td>
<td>Local Host</td>
<td>Internal</td>
<td>All Users</td>
</tr>
<tr>
<td>5</td>
<td>Allow RADIUS authentication from ISA Server to trusted RADIUS servers</td>
<td>Allow</td>
<td>RADIUS RADIUS Accounting</td>
<td>Local Host</td>
<td>Internal</td>
<td>All Users</td>
</tr>
<tr>
<td>6</td>
<td>Allow Kerberos authentication from ISA Server to trusted servers</td>
<td>Allow</td>
<td>Kerberos-Sec(TCP) Kerberos-Sec(UDP)</td>
<td>Local Host</td>
<td>Internal</td>
<td>All Users</td>
</tr>
<tr>
<td>7</td>
<td>Allow DNS from ISA Server to selected servers</td>
<td>Allow</td>
<td>DNS</td>
<td>Local Host</td>
<td>All Networks</td>
<td>All Users</td>
</tr>
<tr>
<td>8</td>
<td>Allow DHCP requests from ISA Server to all networks</td>
<td>Allow</td>
<td>DHCP(request)</td>
<td>Local Host</td>
<td>Anywhere</td>
<td>All Users</td>
</tr>
<tr>
<td>9</td>
<td>Allow DHCP replies from DHCP servers to ISA Server</td>
<td>Allow</td>
<td>DHCP(reply)</td>
<td>Anywhere</td>
<td>Local Host</td>
<td>All Users</td>
</tr>
<tr>
<td>10</td>
<td>Allow ICMP (PING) requests from selected computers to ISA Server</td>
<td>Allow</td>
<td>Ping</td>
<td>Remote Management Computers</td>
<td>Local Host</td>
<td>All Users</td>
</tr>
<tr>
<td>11</td>
<td>Allow ICMP requests from ISA Server to selected servers</td>
<td>Allow</td>
<td>ICMP Information Request ICMP Timestamp Ping</td>
<td>Local Host</td>
<td>All Networks</td>
<td>All Users</td>
</tr>
<tr>
<td>12</td>
<td>Allow VPN client traffic to ISA Server</td>
<td>Allow</td>
<td>PPTP</td>
<td>External</td>
<td>Local Host</td>
<td>All Users</td>
</tr>
<tr>
<td>13</td>
<td>Allow VPN site-to-site to ISA Server</td>
<td>Allow</td>
<td>External IPSec Remote Gateways</td>
<td>Local Host</td>
<td>All Users</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Allow VPN site-to-site from ISA</td>
<td>Allow</td>
<td>Local Host</td>
<td>External IPSec</td>
<td>All Users</td>
<td></td>
</tr>
<tr>
<td>Order</td>
<td>Name</td>
<td>Action</td>
<td>Protocols</td>
<td>From</td>
<td>To</td>
<td>Condition</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------------------------------</td>
<td>--------</td>
<td>--------------------------------------------------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>15</td>
<td>Allow Microsoft CIFS protocol from ISA Server to trusted servers</td>
<td>Allow</td>
<td>Microsoft CIFS(TCP)</td>
<td>Local Host</td>
<td>Internal</td>
<td>All Users</td>
</tr>
<tr>
<td>16</td>
<td>Allow Remote logging using Microsoft SQL protocol from firewall to trusted servers</td>
<td>Allow</td>
<td>Microsoft SQL(TCP)</td>
<td>Local Host</td>
<td>Internal</td>
<td>All Users</td>
</tr>
<tr>
<td>17</td>
<td>Allow HTTP/HTTPS requests from ISA Server to specified sites</td>
<td>Allow</td>
<td>HTTP HTTPS</td>
<td>Local Host</td>
<td>System Policy Allowed Sites</td>
<td>All Users</td>
</tr>
<tr>
<td>18</td>
<td>Allow HTTP/HTTPS requests from ISA Server to selected servers for HTTP connectivity verifiers</td>
<td>Allow</td>
<td>HTTP HTTPS</td>
<td>Local Host</td>
<td>All Networks</td>
<td>All Users</td>
</tr>
<tr>
<td>19</td>
<td>Allow access from trusted computers to the Firewall Client installation share on ISA Server</td>
<td>Allow</td>
<td>Microsoft CIFS(TCP)</td>
<td>Internal</td>
<td>Local Host</td>
<td>All Users</td>
</tr>
<tr>
<td>20</td>
<td>Allow remote performance monitoring of ISA Server from trusted servers</td>
<td>Allow</td>
<td>NetBIOS Datagram NetBIOS Name Service NetBIOS Session</td>
<td>Remote Management Computers</td>
<td>Local Host</td>
<td>All Users</td>
</tr>
<tr>
<td>21</td>
<td>Allow NetBIOS from ISA Server to trusted servers</td>
<td>Allow</td>
<td>NetBIOS Datagram NetBIOS Name Service NetBIOS Session</td>
<td>Local Host</td>
<td>Internal</td>
<td>All Users</td>
</tr>
<tr>
<td>22</td>
<td>Allow RPC from ISA Server to trusted servers</td>
<td>Allow</td>
<td>RPC(all interfaces)</td>
<td>Local Host</td>
<td>Internal</td>
<td>All Users</td>
</tr>
<tr>
<td>23</td>
<td>Allow HTTP/HTTPS from ISA Server</td>
<td>Allow</td>
<td>HTTP HTTPS</td>
<td>Local Host</td>
<td>Microsoft Error Reporting</td>
<td>All Users</td>
</tr>
<tr>
<td>Order</td>
<td>Name</td>
<td>Action</td>
<td>Protocols</td>
<td>From</td>
<td>To</td>
<td>Condition</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------------</td>
<td>--------</td>
<td>-------------------</td>
<td>------------</td>
<td>-------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>1</td>
<td>This policy is disabled until the VPN Server component is activated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>These two policies are disabled until a site to site VPN connection is configured</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>This policy is disabled until a connectivity verifier that uses HTTP/HTTPS is configured</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>This policy is disabled until the SecureID filter is enabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>This policy must be manually enabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>This policy is disabled by default</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>This policy is disabled by default</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>This policy is automatically enabled when the Firewall client share is installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>This policy is disabled by default</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

At this point the ISA Server 2004 firewall is ready to be configured to allow inbound and outbound access through the firewall. However, before you start creating Access Policies, you should back up the default configuration. This allows you to restore the ISA Server 2004 firewall to its post-installation state. This is useful for future troubleshooting and testing.
Backing Up the Post-Installation Configuration

Perform the following steps to back up the post installation configuration:

1. Open the **Microsoft Internet Security and Acceleration Server 2004** management console and right click on the server name in the left pane of the console. Click the **Back Up** command.

2. In the **Backup Configuration** dialog box, enter a name for the backup file in the **File name** text box. Be sure to note where you are saving the file by checking the entry in the **Save in** drop down list. In this example we will call the backup file **backup1**. Click the **Backup** button.

3. In the **Set Password** dialog box, enter a password and confirm the password in the **Password** and **Confirm password** text boxes. The information in the backup file is encrypted because it can potentially contain passwords and other confidential information that you do not want others to access. Click **OK**.
4. Click OK in the Exporting dialog box when you see the **The configuration was successfully backed up** message.

Make sure to copy the backup file to another location on the network after the backup is complete. The backup file should be stored off-line on media that supported NTFS formatting so that you can encrypt the file.
Conclusion

In this ISA Server 2004 Configuration Guide document we discussed the procedures required to install the ISA Server 2004 software on a Windows Server 2003 computer. We also examined the firewall System Policy that is created during installation. Finally, we finished up with step by step procedures required to back up the post-installation firewall configuration. In the next document in this ISA Server 2004 Configuration Guide series, we will enable the VPN remote access server.
Introduction

ISA Server 2004 includes a new and enhanced backup and restore feature set. In ISA Server 2000, the integrated backup utility could back up the ISA Server 2000 firewall configuration. That backup file could be used to restore the configuration to the same installation on the same machine. However, if the operating system or hardware experienced a catastrophic problem requiring disaster recovery, the backup file could not be used to restore the firewall configuration.

In contrast, the ISA Server 2004 backup utility allows you to back up the entire firewall configuration or just selected elements. You can restore the configuration to the same ISA Server 2004 firewall installation on the same machine, or restore it to another ISA Server 2004 firewall on another machine. Backups should be done after performing one or more of the following procedures:

- Changing cache size or location
- Changing firewall policy
- Changing rule base
- Changing system rules
- Making changes to networks, such as, changing network definition or network rules
- Delegating administrative rights or removing delegation

The import/export feature allows you to export selected components of the firewall configuration and use them on the same machine at another time, or install those components to another machine. The import/export functionality can also be used to export the entire configuration of the machine as a method of cloning for more widespread distribution.

It is a good practice to perform a backup operation immediately after installing the ISA Server 2004 firewall software. This makes it easier to restore the firewall components to their post-installation state in the event that you want to completely remove an existing configuration and start from the beginning without reinstalling the software.

In this ISA Server 2004 Configuration Guide section, we will describe the following procedures:

- Backing up the Firewall Configuration
- Restoring the Firewall Configuration from the Backup File
- Exporting Firewall Policy
- Importing Firewall Policy
Backing up the Firewall Configuration

The ISA Server 2004 integrated backup utility makes saving the firewall configuration very easy. There are only a handful of steps required to backup and restore the configuration.

Perform the following steps to back up the entire firewall configuration:

5. Open the **Microsoft Internet Security and Acceleration Server 2004** management console and right click on the server name in the left pane of the console. Click the **Backup** command.

6. In the **Backup Configuration** dialog box, enter a name for the backup file in the **File name** text box. Be sure to note where you are saving the file by checking the entry in the **Save in** drop down list. In this example, we will call the backup file **backup1**. Click the **Backup** button.

7. In the **Set Password** dialog box, enter a password and confirm the password in the **Confirm password** text box. The information in the backup file is encrypted because it can potentially contain passwords and other confidential information that you do not want others to access. Click **OK**.
8. Click OK in the Exporting dialog box when you see the The configuration was successfully backed up message.

Make sure to copy the backup file to another location on the network after the backup is complete. The backup file should be stored off-line on media that supported NTFS formatting so that you can encrypt the file.
Restoring the Firewall Configuration from the Backup File

You can use the backup file to restore the machine configuration. The restore can be to the same machine and same ISA Server 2004 firewall installation, the same machine and a new ISA Server 2004 firewall installation, or to a completely new machine.

Perform the following steps to restore the configuration from backup:

1. Open the Microsoft Internet Security and Acceleration Server 2004 management console and right click on the computer name in the left pane of the console. Click the Restore command.

2. In the Restore Configuration dialog box, navigate to the backup file you created. In this example, we will use the backup file named backup1.xml. Click the Restore button after selecting the file.

3. Enter the password you assigned to the file in the Type Password to Open File dialog box, then click OK.
4. Click **OK** in the **Importing** dialog box when it shows the **The configuration was successfully restored** message.

5. Click **Apply** to save the changes and update firewall policy.

6. Select the **Save the changes and restart the service(s)** option in the ISA Server **Warning** dialog box (note that this is not the selected option in the figure, please select the appropriate option).

7. Click **OK** in the **Apply New Configuration** dialog box informing you that the **Changes to the configuration were successfully applied**.
The restored configuration is now fully functional and the previous firewall policies are now applied.
Exporting Firewall Policy

You may not always want or need to export all aspects of the ISA Server 2004 firewall configuration. For example, you may have problems with your Access Policies and want someone to view them for you. You can export the firewall’s current Access Policies and send the export file to an ISA Server 2004 professional who can quickly import the policies into a test machine and troubleshoot the problem.

In the following example we will export the VPN Clients configuration to a file. Perform the following steps to export the VPN Clients configuration:

1. In the Microsoft Internet Security and Acceleration Server 2004 management console, expand your server name in the left pane of the console and then right click on the Virtual Private Networks (VPN) node. Click on the Export VPN Clients Configuration command.

2. In the Export Configuration dialog box, enter a name for the export file in the File name text box. Make a note of where you are storing the file, which is displayed in the Save in drop down list. Put checkmarks in the Export user permission settings and Export confidential information (encryption will be used) check boxes if you want to save the private information included in the VPN Clients configuration (such as IPSec shared secrets). In this example we will call the file VPN Clients Backup. Click Export.
3. In the **Set Password** dialog box, enter a password and confirm the password in the **Confirm password** text box. Click **OK**.

![Set Password dialog box]

During the export process, confidential information will be encrypted. When importing the file, a password will be required to open and decrypt this information.

Set the password required when importing this file (at least 8 characters):

- **Password:** ******
- **Confirm password:** ******

Click **OK**.

4. Click **OK** in the **Exporting** dialog box when you see the message **Successfully exported the configuration**.
Importing Firewall Policy

The export file can be imported to the same machine or another machine that has ISA Server 2004 installed. In the following example, we will import the VPN Clients settings that were exported in the previous exercise.

Perform the following steps to import the VPN Clients settings from the export file:

1. In the Microsoft Internet Security and Acceleration Server 2004 management console, expand the server name and right click on the Virtual Private Networks (VPN) node. Click Import VPN Clients Configuration.

2. In the Import Configuration dialog box, select the VPN Clients Backup file. Put a checkmark in the Import user permission settings and Import cache drive settings and SSL certificates checkboxes. In this example, the cache drive settings are not important, but the SSL certificates are helpful if you want to use the same certificates that are used for IPSec or L2TP/IPSec VPN connections. Click Import.

3. Enter the password you assigned to the file in the Type Password to Open File dialog box. Click OK.
4. Click **OK** in the **Importing Virtual Private Networks (VPN)** dialog box when you see the **Successfully imported the configuration** message.

5. Click **Apply** to apply the changes and update firewall policy.

6. Click **OK** in the **Apply New Configuration** dialog box when you see the message **Changes to the configuration were successfully applied**. Note that changes in the VPN configuration may take several minutes as they are updated in the background.
Conclusion

In this ISA Server 2004 Configuration Guide section, we discussed the procedures for backing up and restoring the ISA Server 2004 firewall configuration. We also explored the export and import feature that allows you to back up selected elements of the firewall configuration. In the next section of the ISA Server 2004 Configuration Guide series, we will examine how you can use the ISA Server 2004 Network Templates to simplify the initial configuration of Networks, Network Rules and firewall Access Policies.
ISA Server 2004 Configuration Guide: Simplifying Network Configuration with Network Templates

Chapter 9

For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

The ISA Server 2004 firewall comes with a number of pre-built Network Templates you can use to automatically configure Networks, Network Rules and Access Rules. The Network Templates are designed to get you started quickly by creating a base configuration on which you can build. You can choose from one of the following Network Templates:

- **Edge Firewall**
  The Edge Firewall Network Template is used when the ISA Server 2004 firewall has a network interface directly connected to the Internet and a network interface connected to the Internal network.

- **3-Leg Perimeter**
  The 3-Leg Perimeter Network Template is used when you have an external interface, Internal interface and a perimeter network segment (DMZ) interface. This template configures the addresses and relationships between these networks.

- **Front Firewall**
  The Front Firewall Template is used when the ISA Server 2004 firewall serves as a front-end firewall in a back-to-back firewall configuration.

- **Back Firewall**
  The Back Firewall Template is used when the ISA Server 2004 firewall is located behind another ISA Server 2004 firewall, or a third-party firewall.

- **Single Network Adapter**
  The Single Network Adapter Template is a special configuration that removes the ISA Server 2004 firewall’s network firewall capabilities. Instead, the Single Network Adapter template configures the machine as a unihomed Web caching server.

In this *ISA Server 2004 Configuration Guide* document, we outline the procedures to carry out two scenarios:

- Scenario 1: The Edge Firewall Configuration
- Scenario 2: The 3-Leg Perimeter Configuration

You only need to go through the section that applies to your current setup. If you followed the complete instructions in the first chapter of this guide, then you should perform the procedures in the second scenario. Otherwise, you can use the procedures provided in the first scenario.
## Scenario 1: The Edge Firewall Configuration

The Edge Firewall template configures the ISA Server 2004 firewall to have a network interface directly connected to the Internet and a second network interface connected to the Internal network. The network template allows you to quickly configure firewall policy Access Rules that control access between the Internal network and the Internet.

Table 1 shows the firewall policies available to you when using the Edge Firewall template. Each of these firewall policies has its own set of Access Rules that it creates, ranging from an all open access policy between the Internal network and Internet to a Block All policy that prevents all access between the Internal network and the Internet.

<table>
<thead>
<tr>
<th>Firewall Policy</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Block all**                                  | Block all network access through ISA Server.  
This option does not create any access rules other than the default rule which blocks all access.  
Use this option when you want to define firewall policy on your own. |
| **Block Internet access, allow access to ISP network services** | Block all network access through ISA Server, except for access to network services such as DNS. This option is useful when your Internet Service Provider (ISP) provides these services.  
Use this option when you want to define firewall policy on your own.  
The following access rules will be created:  
1. Allow DNS from Internal Network and VPN Clients Network to External Network (Internet) |
| **Allow limited Web access**                   | Allow Web access using HTTP, HTTPS, FTP only. Block all other network access.  
The following access rules will be created:  
1. Allow HTTP, HTTPS, FTP from Internal Network to External Network  
2. Allow all protocols from VPN Clients Network to Internal Network |
| **Allow limited Web access and access to ISP network services** | Allow limited Web access using HTTP, HTTPS, and FTP, and allows access to ISP network services such as DNS. Block all other network access.  
The following access rules will be created:  
1. Allow HTTP, HTTPS, FTP from Internal Network and VPN Clients Network to External Network (Internet)  
2. Allow DNS from Internal Network and VPN Clients Network to External Network (Internet)  
3. Allow all protocols from VPN Clients Network to Internal Network |
<p>| <strong>Allow unrestricted</strong>                         | Allow unrestricted access to the Internet through ISA Server. ISAServer |</p>
<table>
<thead>
<tr>
<th>Firewall Policy</th>
<th>Description</th>
</tr>
</thead>
</table>
| access         | Server will prevent access from the Internet. The following access rules will be created:  
1. Allow all protocols from Internal Network and VPN Clients Network to External Network (Internet)  
2. Allow all protocols from VPN Clients Network to Internal Network |

Perform the following steps to configure the firewall using the Edge Firewall Network Template:

1. In the **Microsoft Internet Security and Acceleration Server 2004** management console, expand the server name and then expand the **Configuration** node. Click on the **Networks** node.

2. Click on the **Templates** tab in the Task Pane. Click on the **Edge Firewall** network template.
3. Click **Next** on the **Welcome to the Network Template Wizard** page.
4. On the **Export the ISA Server Configuration** page, you are offered the opportunity to export the current configuration. You can return the ISA Server 2004 firewall to the state it was in prior to using the Edge Firewall network template using this file. We have already backed up the system configuration, so we will not need to export the configuration at this time. Click **Next**.
5. On the **Internal Network IP Addresses** page, you define the Internal network addresses. The current Internal network address range is automatically included in the **Address ranges** list. You can use the **Add**, **Add Adapter** and **Add Private** button to expand this list of addresses. In our current example we will keep the current Internal network address range. Click **Next**.
6. On the **Select a Firewall Policy** page you can select a firewall policy and a collection of Access Rules. In this example, we want to allow Internal network clients access to all protocols to access all sites on the Internet. After you become more familiar with the ISA Server 2004 firewall, you should increase the level of security for outbound access control. But at this point, general Internet access is more important. Select the **Allow unrestricted access** policy from the list and click **Next**.
7. Review your settings and click Finish on the Completing the Network Template Wizard page.

8. Click Apply to save the changes and update firewall policy.

9. Click OK in the Apply New Configuration dialog box after you see the message Changes to the configuration were successfully applied.

10. Click on the Firewall Policies node in the left pane of the console to view the policies created by the Edge Firewall network template. These two Access Rules allow Internet network and VPN clients full access to the Internet, and the VPN clients are allowed full access to the Internal network.
<table>
<thead>
<tr>
<th>Name</th>
<th>Action</th>
<th>Protocols</th>
<th>From / Listener</th>
<th>To</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unrestricted Internet access</td>
<td>Allow</td>
<td>All Protocols</td>
<td>Internal</td>
<td>External</td>
<td>All Users</td>
</tr>
<tr>
<td>VPN Clients to Internal Network</td>
<td>Allow</td>
<td>All Protocols</td>
<td>VPN Clients</td>
<td>Internal</td>
<td>All Users</td>
</tr>
<tr>
<td>Last Default rule</td>
<td>Deny</td>
<td>All Protocols</td>
<td>All Networks</td>
<td>All Networks</td>
<td>All Users</td>
</tr>
</tbody>
</table>
Scenario 2: The 3-Leg Perimeter Configuration

The 3-leg perimeter configuration creates network relationships and Access Rules to support an Internal network segment and a perimeter (DMZ) network segment. The perimeter network segment can host your publicly-accessible resources and infrastructure servers, such as a public DNS server or a caching-only DNS server.

Table 2: 3-Legged Perimeter Firewall Template Firewall Policy Options

<table>
<thead>
<tr>
<th>Firewall Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block all</td>
<td>Block all network access through ISA Server.  This option does not create any access rules other than the default rule which blocks all access. Use this option when you want to define firewall policy on your own.</td>
</tr>
<tr>
<td>Block Internet access, allow access to network services on the perimeter network</td>
<td>Block all network access through ISA Server, except for access to network services, such as DNS on the perimeter network. Use this option when you want to define the firewall policy on your own. The following access rules will be created: 1. Allow DNS traffic from Internal Network and VPN Clients Network to Perimeter Network</td>
</tr>
<tr>
<td>Block Internet access, allow access to ISP network services</td>
<td>Prevent all network access through the firewall except for network services such as DNS. This option is useful when your Internet Service Provider (ISP) provides network services. Use this option when you want to define the firewall policy on your own. The following rules will be created: 1. Allow DNS from Internal Network, VPN Clients Network and Perimeter Network to External Network (Internet)</td>
</tr>
<tr>
<td>Allow limited Web access, allow access to network services on perimeter network</td>
<td>Allow limited Web access using HTTP, HTTPS, FTP only and allow access to network services such as DNS on the perimeter network. All other network access is blocked. This option is useful when network infrastructure services are available on the perimeter network. The following access rules will be created: 1. Allow HTTP, HTTPS, FTP from Internal Network and VPN Clients Network to Perimeter Network and External Network (Internet) 2. Allow DNS traffic from Internal Network and VPN Clients Network to Perimeter Network 3. Allow all protocols from VPN Clients Network to Internal Network</td>
</tr>
<tr>
<td>Allow limited Web access and access to ISP network services</td>
<td>Allow limited Internet access and allow access to network services such as DNS provided by your Internet Service Provider (ISP). All other network access is blocked.</td>
</tr>
<tr>
<td>Firewall Policy</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Allow unrestricted access | Allow all types of access to the Internet through the firewall. The firewall will prevent access from the Internet to the protected networks. Use this option when you want to allow all Internet access. You can modify this policy later to block some types of network access. The following rules will be created:  
1. Allow all protocols from Internal Network and VPN Clients Network to External Network (Internet) and Perimeter Network  
2. Allow all protocols from VPN Clients Network to Internal Network |

Perform the following steps to use the 3-Leg Perimeter network template:

1. Open the **Microsoft Internet Security and Acceleration Server 2004** management console and expand the server name. Expand the **Configuration** node and click on the **Networks** node.

2. Click the **Networks** tab in the Details pane and then click the **Templates** tab in the Task pane. Click on the **3-Leg Perimeter** network template.
3. Click **Next** on the **Welcome to the Network Template Wizard** page.

4. On the **Export the ISA Server Configuration** page, you can choose to export your current configuration. This is useful if you find that you need to return the firewall to its current settings in the event that the template settings do not meet your needs. We have already backed up the configuration, so we will not need to export the configuration at this time. Click **Next**.
5. On the **Internal Network IP Addresses** page, you set the addresses that represent the Internal network. The addresses included in the current Internal network are automatically included in the **Address ranges** list. We will not add any addresses to the Internal network. Click **Next**.
6. You configure the addresses that comprise the perimeter network segment on the Perimeter Network IP Addresses page. The wizard does not make any assumptions regarding what addresses should be included in the perimeter network, so the Address ranges list is empty.
7. Click the Add Adapter button. In the Network adapter details dialog box, put a checkmark in the DMZ check box. Note that the names that we previously set for network adapters appear in this list. Renaming network adapters helps you identify the network association of that adapter. Click OK.
8. The wizard automatically enters an address range to the **Address ranges** list based on the Windows routing table. Click **Next**.

![Network Template Wizard](image)

<table>
<thead>
<tr>
<th>Address ranges:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Address</td>
<td>End Address</td>
</tr>
<tr>
<td>172.16.0.0</td>
<td>172.16.255.255</td>
</tr>
</tbody>
</table>

9. On the **Select a Firewall Policy** page, you select a firewall policy that will create network relationships between the Internet, perimeter and Internal networks and also creates Access Rules. In this example, we want to allow the Internal network clients full access to the Internet and the perimeter network, and allow the perimeter network hosts access to the Internet. After you are more familiar with how to configure Access Policies on the ISA Server 2004 firewall, you will want to tighten the outbound access controls between the perimeter network segment and the Internet, and between the Internal network segment and the Internet. Select the **Allow unrestricted access** firewall policy and click **Next**.
10. Review the settings on the Completing the Network Template Wizard and click Finish.

11. Click Apply to save the changes and update firewall policy.

12. Click OK in the Apply New Configuration dialog box after you see the message Changes to the configuration were successfully applied.

13. Click on the Firewall Policy node in the left pane of the Microsoft Internet Security and Acceleration Server 2004 management console to view the rules created by the 3-Leg Perimeter network template. These two rules allow hosts on the Internal network and in the VPN clients network full access to the Internet and to the perimeter network. In addition, the VPN Clients network is allowed full access to the Internal network.
14. Expand the **Configuration** node in the left pane of the **Microsoft Internet Security and Acceleration Server 2004** management console. Click on the **Networks** node. Here you see a list of networks, including the **Perimeter** network created by the template.

15. Click on the **Network Rules** tab. Right click on the **Perimeter Configuration** Network Rule and click **Properties**.
16. In the Perimeter Configuration Properties dialog box, click on the Source Networks tab. You can see in the This rule applies to traffic from these sources list the Internal, Quarantined VPN Clients and VPN Clients networks listed as source networks.

17. Click on the Destination Networks tab. You see the Perimeter network in the This rule applies to traffic sent to these destinations list.
18. Click the **Network Relationship** tab. The default setting is **Network Address Translation (NAT)**. This is a slightly higher security configuration because it hides the addresses of the Internal network clients that connect to perimeter network hosts. However, NAT relationships can complicate access for certain protocols as not all protocols support address translation. In our current example, select the **Route** relationship to improve on the level of protocol access at the cost of a slight reduction in overall security. Keep in mind that, at this point, there are no Access Rules that allow access to the Internal network from the perimeter network.
19. Click **Apply** and then click **OK**.

20. Click **Apply** to save the changes and update the firewall policy.

21. Click **OK** in the **Apply New Configuration** dialog box after you see the message

   **Changes to the configuration were successfully applied.**
Conclusion

In this ISA Server 2004 Configuration Guide chapter, we discussed how you can use the Edge Firewall and 3-Leg Perimeter network templates to simplify initial configuration of network addresses, Network Rules and Access Rules. In the next chapter of the ISA Server 2004 Configuration Guide, we will discuss the various ISA Server 2004 client types.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

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

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

© 2004 Microsoft Corporation. All rights reserved.

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, place, or event is intended or should be inferred.


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

An ISA Server 2004 client is a machine that connects to a resource by going through the ISA Server 2004 firewall. In general, the ISA Server 2004 client is located on an Internal or perimeter network segment and connects to the Internet through the ISA Server 2004 firewall.

There are three ISA Server 2004 client types:

- The SecureNAT client
- The Web Proxy client
- The Firewall client

A SecureNAT client is a machine configured with a default gateway that can route Internet-bound requests through the ISA Server 2004 firewall. If the SecureNAT client is on a network directly connected to the ISA Server 2004 firewall, the default gateway of the SecureNAT client is the IP address of the network interface on the ISA Server 2004 firewall connected to that segment. If the SecureNAT client is located on a network segment that is remote from the ISA Server 2004 firewall, the SecureNAT client is configured with an IP address of a router that routes Internet bound requests through the ISA Server 2004 firewall machine.

A Web Proxy client is a machine whose browser is configured to use the ISA Server 2004 firewall as its Web Proxy server. The Web browser can be configured to use the IP address of the ISA Server 2004 firewall as its Web Proxy server, or it can be set to use the ISA Server 2004 firewall’s Web Proxy autoconfiguration script. The autoconfiguration script confers a higher level of flexibility in controlling how Web Proxy clients connect to the Internet. User names are recorded in the Web Proxy logs when the machine is configured as a Web Proxy client.

A Firewall client is a machine that has the Firewall client software installed. The Firewall client software intercepts all Winsock application requests (typically, all TCP and UDP requests) and forwards them directly to the Firewall service on the ISA Server 2004 firewall. User names are automatically entered into the Firewall service log when the Firewall client machine connects to the Internet through the ISA Server 2004 firewall.

The following table summarizes the features provided by each client type.

<table>
<thead>
<tr>
<th>Feature</th>
<th>SecureNAT client</th>
<th>Firewall client</th>
<th>Web Proxy client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation</td>
<td>Yes, requires some network configuration changes</td>
<td>Yes</td>
<td>No, requires Web browser configuration</td>
</tr>
<tr>
<td>Operating system support</td>
<td>Any operating system that supports TCP/IP</td>
<td>Only Windows platforms</td>
<td>All platforms, but by way of a Web application</td>
</tr>
<tr>
<td>Protocol support</td>
<td>Application filters for multi-connection protocols</td>
<td>All Winsock applications</td>
<td>HTTP, Secure HTTP (HTTPS), and FTP</td>
</tr>
<tr>
<td>User-level authentication support</td>
<td>Yes, for VPN clients only</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

We will discuss the following procedures in this ISA Server 2004 Configuration Guide document:

- Configuring the ISA Server 2004 SecureNAT client
• Configuring the ISA Server 2004 Web Proxy client
• Configuring the ISA Server 2004 Firewall client
Configuring the SecureNAT Client

The SecureNAT client configuration is simple. The only requirement is that the machine be configured with a default gateway that routes Internet-bound requests through the ISA Server 2004 firewall machine. There are two primary methods you can use to configure a machine as a SecureNAT client:

- Manually configure the TCP/IP settings on the machine
- Create a DHCP scope option that assigns the default gateway address

In the scenarios discussed in this ISA Server 2004 Configuration Guide, the domain controller is configured as a SecureNAT client. Network servers such as domain controllers, DNS servers, WINS servers and Web servers are typically configured as SecureNAT clients. The domain controller has been manually configured as a SecureNAT client.

In chapter 4 of this ISA Server 2004 Configuration Guide, you installed a DHCP server and created a DHCP scope. The DHCP scope was configured with a scope option assigning DHCP clients a default gateway address that is the Internal interface of the ISA Server 2004 firewall. The default configuration of Windows systems is to use DHCP to obtain IP addressing information.

If you are using the network configuration described in Chapter 1 of this ISA Server 2004 Configuration Guide, the Internal network client is configured with a static IP address. In the following walkthrough, we will configure the Internal network client to use DHCP to demonstrate how DHCP works, then return the client to its static IP address.

Perform the following steps to configure the Windows 2000 machine as a DHCP client and return the machine to a static IP address:

1. At the CLIENT machine, right click on the My Network Places icon on the desktop and click Properties.
2. In the Network and Dial-up Connections window, right click on the Local Area Connection entry and click Properties.
3. In the Local Area Connection Properties dialog box, click on the Internet Protocol (TCP/IP) entry and click Properties.
4. In the Internet Protocol (TCP/IP) Properties dialog box, select Obtain an IP address automatically and Obtain DNS server address automatically. Click OK.
5. Click **OK** in the *Local Area Connection Properties* dialog box.

6. Confirm the new IP address assignment by using the *ipconfig* command. Click **Start** and **Run**. In the **Open** text box, enter *cmd*.

7. In the *Command Prompt* window, enter *ipconfig /all* and press ENTER. Here you can see the IP address assigned to the client, as well as the DNS, WINS and default gateway addresses.
8. Close the **Command Prompt** window. Return to the **TCP/IP Properties** dialog box and change the CLIENT machine to use a static IP address again. The **IP address** is **10.0.0.4**; the subnet mask is **255.255.255.0**; the default gateway is **10.0.0.1**, and the DNS server address is **10.0.0.2**.
Configuring the Web Proxy Client

The Web Proxy client configuration requires that the Web browser be set to use the ISA Server 2004 firewall as its Web Proxy server. There are several ways to configure the Web browser as a Web Proxy client. It can be:

- manually configured to use the IP address of the ISA Server 2004 firewall as its Web Proxy server
- manually configured to use the autoconfiguration script
- automatically configured during Firewall client installation
- automatically configured using wpad entries in DNS and DHCP

In chapter 5 of the ISA Server 2004 Configuration Guide, you created wpad entries in DNS and DHCP to support autoconfiguration of Web Proxy and Firewall client machines. Wpad autodiscovery is the preferred method of configuring the Web Proxy client, as it allows users to automatically receive Web Proxy settings without requiring them to configure their browsers.

Another way you can automatically configure Web browsers as Web Proxy clients is to have the browsers automatically configured when the Firewall client installed. This is the preferred method of configuring browsers for machines that will also act as Web proxy clients.

The last option is to manually configure the browser. This option should be used when the automatic configuration options are not available.

If you are using the example network configuration described in this ISA Server 2004 Configuration Guide, your DNS and DHCP servers are configured to provide wpad information to the Web browsers so that they are autoconfigured. However, if you choose to not use autoconfiguration, you can manually configure the browser. We will examine browser configuration during Firewall client installation in the next section.

Perform the following steps to manually configure the Internet Explorer 6.0 Web browser:

1. On the CLIENT machine, right click on the Internet Explorer icon on the desktop and click Properties.
2. In the Internet Properties dialog box, click the Connections tab. On the Connections tab, click the LAN Settings button.
3. There are several Web proxy configuration options in the Local Area Network (LAN) Settings dialog box. Put a checkmark in the Automatically detect settings check box to enable the browser to use the wpad settings in DNS and DHCP. This is the default setting for Internet Explorer Web browsers. Place a checkmark in the Use automatic configuration script check box, and enter the location of the autoconfiguration script. The autoconfiguration script is stored on the ISA Server 2004 firewall at the following location:


   The client machine must be able to resolve the name of the ISA Server 2004 firewall included in the autoconfiguration script to the IP address on the Internal interface of the firewall. Note that if the machine is able to use wpad to Automatically detect settings, the information contained in the autoconfiguration script will be downloaded to the Web Proxy client machine. Put a checkmark in the Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections) check box, and enter the IP address on the Internal interface of the ISA Server 2004 firewall in the Address text box.
Enter the TCP port number that the Web Proxy filter lists on the Port text box, which is by default 8080. Click OK in the Local Area Network (LAN) Settings dialog box.

4. Click OK in the Internet Properties dialog box.
The Web browser is now configured as a Web Proxy client.
Configuring the Firewall Client

The Firewall client software enables you to control Internet access on a per user/group basis for all Winsock (TCP or UDP) connections to the Internet. The Firewall client software automatically sends user credentials in the background to the ISA Server 2004 firewall machine. The user accounts can belong to the local SAM on the ISA Server 2004 firewall, or, if the ISA Server 2004 and the clients belong to the same Windows domain, then the user accounts can be stored in the Windows NT 4.0 SAM or Windows 2000/Windows Server 2003 Active Directory.

The firewall client software can be installed from the ISA Server 2004 machine or from another machine on the network. If you wish to install the Firewall client software from the ISA Server 2004 firewall computer, you must enable a System Policy Rule to allow access to the share. A more secure configuration is to install the Firewall client share to a file server on the Internal network.

In the following walkthrough, we will install the Firewall client share on the domain controller computer and then install the Firewall client software on the Windows 2000 client computer.

Perform the following steps to install the Firewall client share on the domain controller computer:

1. Insert the ISA Server 2004 CD-ROM into the CD drive on the domain controller. In the autorun menu, click the Install ISA Server 2004 icon.
2. On the Welcome to the Installation Wizard for Microsoft ISA Server 2004 page, click Next.
3. On the License Agreement page, select I accept the terms in the license agreement, and click Next.
5. On the Setup Type page, select the Custom option.
6. On the Custom Setup page, click the Firewall Services entry and click the This feature will not be available option. Click the ISA Server Management entry and click the This feature will not be available option. Click the Firewall Client Installation Share entry and click the This feature, and all subfeatures, will be installed on the local hard drive. Click Next.
7. Click **Install** on the **Ready to Install the Program** page.

8. Click **Finish** on the **Installation Wizard Completed** page.

You can now install the Firewall client software from the Firewall client share on the domain controller. Perform the following steps to install the Firewall client software:

1. At the CLIENT computer on the Internal network, click **Start** and then click the **Run** command. In the **Open** text box, enter `\EXCHANGE2003BE\mspclnt\setup` and click **OK**.

2. Click **Next** on the **Welcome to the Install Wizard for Microsoft Firewall Client**.

3. Click **Next** on the **Destination Folder** page.

4. On the **ISA Server Computer Selection** page, select the **Automatically detect the appropriate ISA Server computer** option. This option will work because we have created a wpad entry in DNS. If you had not created a wpad entry, you could have selected the **Connect to this ISA Server computer** option and entered the name or IP address of the ISA Server 2004 firewall in the text box. Click **Next**.
5. Click **Install** on the **Ready to Install the Program** page.

6. Click **Finish** on the **Install Wizard Completed** page.

The next step is to configure Firewall client support for the Internal network. Perform the following steps on the ISA Server 2004 firewall computer:

1. Open the Microsoft Internet Security and Acceleration Server 2004 management console and expand the server name. Expand the **Configuration** node and click on the **Networks** node. Right click on the **Internal** Network and click **Properties**.

2. In the **Internal Properties** dialog box, click on the **Firewall Client** tab. Confirm that there is a checkmark in the **Enable Firewall client support for this network** check box. Confirm that there are checkmarks in the **Automatically detect settings** and **Use automatic configuration script** check boxes in the **Web browser configuration on the Firewall client computer** frame. Put a checkmark in the **Use a Web proxy server** check box. Use the fully-qualified domain name of the ISA Server 2004 firewall computer in the **ISA Server name or IP address** text box. In this example, the fully-qualified domain name of the ISA Server 2004 computer is **ISALOCAL.msfirewall.org**. Click **Apply**.
3. Click on the **Auto Discovery** tab. Place a checkmark in the **Publish automatic discovery information** check box. Leave the default port as **80**. Click **Apply** and **OK**.
4. Click **Apply** to save the changes and update the firewall policy.

5. Click **OK** in the **Apply New Configuration** dialog box.

We can now configure the Firewall client. Perform the following steps on the client computer on the Internal network:

1. At the CLIENT computer, double click on the Firewall client icon in the system tray.

2. In the **Microsoft Firewall Client for ISA Server 2004** dialog box, confirm that there is a checkmark in the **Enable Microsoft Firewall Client for ISA Server 2004** check box. Confirm that the **Automatically detect ISA Server** option is selected.
3. Click the **Detect Now** button. The name of the ISA Server 2004 firewall computer will appear in the **Detecting ISA Server** dialog box when the client finds the ISA Server 2004 firewall. Click **Close**.
4. Confirm that there is a checkmark in the **Enable Web browser automatic configuration** checkbox and click the **Configure Now** button. Note that based on the settings we created on the ISA Server 2004 firewall, the browser has been automatically configured. Click **OK** in the **Web Browser Settings Update** dialog box.
5. Click **Apply** and then click **OK** in the Microsoft Firewall Client for ISA Server 2004 dialog box.

The machine is now configured as a Firewall client and can access the Internet in its role as a Firewall client based on the Access Rules configured on the ISA Server 2004 firewall.
Conclusion

In this ISA Server 2004 Configuration Guide section we discussed the various ISA Server 2004 client types and the features provided by each client. After discussing the types of ISA Server 2004 clients, we went over the procedures required to install and configure each client type. In the next chapter of this ISA Server 2004 Configuration Guide, we will outline the procedures for creating and modifying the outbound access policy rules created by the Network Template.
Chapter 11

For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

The ISA Server 2004 firewall controls what communications move between networks connected to one another via the firewall. By default, the ISA Server 2004 firewall computer blocks all traffic. The methods used to allow traffic to move through the firewall are:

- Access Rules, and
- Publishing Rules

Access Rules control outbound access from a protected network to an unprotected network. ISA Server 2004 considers all networks that are not the External network to be protected. All networks comprising the External network are unprotected. Protected networks include the VPN Clients network, the Quarantined VPN Clients network, the Local Host network, the internal network, and perimeter networks. The Internet is the primary External network; although, partner networks and extranets to which protected clients connect can be considered External networks.

In contrast, Publishing Rules allow hosts on the External network access to resources on a protected network. For example, an organization may wish to host its own Web, mail and FTP servers. Web and Server Publishing Rules allow External hosts access to these resources.

In Chapter 9 of the ISA Server 2004 Configuration Guide, we used a Network Template to automatically create network relationships and Access Rules. The Access Rules were very loose in order to allow you to access all sites and protocols on the Internet. While this configuration is useful for testing basic functionality of the ISA Server 2004 firewall, a secure firewall configuration requires that you create access controls limiting what users on the Protected Networks can access on the Internet.

An Access Rule includes the following elements:

<table>
<thead>
<tr>
<th>Rule Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order (priority)</td>
<td>Firewall Access Policy is an ordered list of Access Rules. Rules are processed from top to bottom until a match for a particular connection is found. The first rule to match the connection’s characteristics is applied.</td>
</tr>
<tr>
<td>Action</td>
<td>There are two actions: Allow or Deny</td>
</tr>
<tr>
<td>Protocols</td>
<td>Protocols include all TCP/IP protocols. These include TCP, UDP, ICMP, and protocols identified by their IP protocol number. The firewall supports all TCP/IP protocols.</td>
</tr>
<tr>
<td>From/Listener</td>
<td>The source of the communication. The source can be a single IP address, a collection of IP addresses, an entire subnet, or multiple subnets.</td>
</tr>
<tr>
<td>To</td>
<td>The destination of a communication. The destination can be a domain or collection of domains, a URL or a collection of URLs, an IP address, a collection of IP addresses, a subnet, multiple subnets or multiple networks.</td>
</tr>
<tr>
<td>Condition</td>
<td>The condition is the user or group to which the rule applies.</td>
</tr>
</tbody>
</table>

Access Rules allow you to gain a fine level of control over which users have access to sites and protocols. For example, consider the following Access Rule:
<table>
<thead>
<tr>
<th>Rule Element</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order (priority)</td>
<td>1</td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
</tr>
<tr>
<td>Protocols</td>
<td>HTTP and FTP (download).</td>
</tr>
<tr>
<td>From/Listener</td>
<td>Internal Network.</td>
</tr>
<tr>
<td>Condition</td>
<td>Limited Web Access (Group).</td>
</tr>
</tbody>
</table>

This rule limits allows users that belong to the **Limited Web Access** group to use the HTTP and FTP (download) protocols. However, members of that group must be located on the internal network when they issue the request. In addition, not only must the members of the **Limited Web Access** be located on the internal network when they issue an HTTP or FTP (download) request, they can only access the www.microsoft.com and ftp.microsoft.com sites when using the protocols. This prevents users from putting the network at risk by downloading content from other Web sites which may contain untrusted or dangerous content.

The first step to strong user/group-based outbound access control is configuring the client systems behind the ISA Server 2004 firewall as Firewall and Web Proxy clients. Only Firewall and Web Proxy clients can authenticate with the firewall. By contrast, SecureNAT clients are not able to authenticate. Outbound access control is limited by the source IP address.

In Chapter 10 of the **ISA Server 2004 Configuration Guide**, you configured the CLIENT machine on the internal network as a SecureNAT, Firewall and Web Proxy client. This configuration enables the machine to send credentials to the ISA Server 2004 so that strong user/group-based Access Rules can be created.

In this chapter, you will create several Access Rules that control outbound access through the ISA Server 2004 firewall. Two rules are based on user/group membership, and one rule will control outbound access based on the source IP address of a server on the internal network.

You will perform the following procedures to create the customized firewall policy:

- Create a user account
- Disable the Access Rules created by the Network Template
- Create an Access Rule limiting protocols and sites users can access
- Create an Access Rule that provides administrators greater access to protocols and sites
- Create a DNS server Access Rule allowing the Internal network DNS server access to Internet DNS servers
- Use HTTP Policy to prevent access to suspect Web sites
- Test the Access Rules
Create a User Account

The first step is to create a user account to which we can later assign limited Internet access privileges. In practice, the user account can be created in the Active Directory or on the local user database on the firewall computer. In our current example, we will create the user account in the Active Directory.

Perform the following steps to create the user account for user2:

1. At the domain controller, click Start and point to Administrative Tools. Click on Active Directory Users and Computers.

2. In the Active Directory Users and Computers console, expand your domain name and click on the Users node. Right click on the Users node. Point to New and click.

3. On the New Object – User page, enter the name of the user in the First name text box. In this example the first name of the user is User2. Enter the value user2 in the User logon name text box. Click Next.

4. Enter a password and then confirm the password in the Confirm password text box. Remove the checkmark from the User must change password at next logon, and click Next.
5. Click **Next** on the Create an Exchange mailbox page.

6. Click **Finish** on the last page of the New User Wizard.
Disable the Access Rules created by the Network Template

The next step is to disable the Access Rules created by the Network Template. In this example, we disable the Access Rules created by the 3-Leg perimeter template. You can perform a similar procedure if you used the Front-end firewall Network Template. We want to use these rules later, so we will disable the rules instead of deleting them. Later, we will re-enable the Access Rules created by the Network Template.

Perform the following steps to disable the Access Rules created by the Network Template:

1. At the ISA Server 2004 firewall computer, open the Microsoft Internet Security and Acceleration Server 2004 management console and expand your server name in the left pane of the console. Click on the Firewall Policy node.

2. In the Details pane, click on the first rule created by the Network Template Wizard. Hold down the CTRL key on the keyboard and click the second rule created by the Wizard. Notice that both rules are now highlighted. Right click the highlighted rules and click Disable.

3. Click Apply to save the changes and update the firewall policy.

4. Click OK in the Apply New Configuration dialog box.
Apply New Configuration

Changes to the configuration were successfully applied.

OK
Create an Access Rule Limiting Protocols and Sites Users Can Access

The first Access Rule will limit users access to only the HTTP and HTTPS protocols. In addition, the users will only be able to use these protocols when accessing Microsoft operated Web properties. A custom firewall group, Limited Access Web Users, will be created and user2, located in the Active Directory, will be placed into that Active Directory group.

The Access Rule can be characterized by the entries in the following table:

<table>
<thead>
<tr>
<th>Rule Element</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order (priority)</td>
<td>3 (after all rules are created)</td>
</tr>
<tr>
<td>Name</td>
<td>Limited Access Web Users</td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
</tr>
<tr>
<td>Protocols</td>
<td>HTTP and HTTPS.</td>
</tr>
<tr>
<td>From/Listener</td>
<td>Internal</td>
</tr>
<tr>
<td>To</td>
<td>Microsoft (Domain Name Set)</td>
</tr>
<tr>
<td>Condition</td>
<td>Limited Web Users (Group).</td>
</tr>
</tbody>
</table>

The rule will look like this in the Firewall Policy Details pane:

```
    3 Limited Access Web Users Allow HTTP HTTPS Internal Microsoft Limited Web Users
```

Perform the following steps to create the limit user Access Rule:

1. At the ISA Server 2004 firewall computer, open the Microsoft Internet Security and Acceleration Server 2004 management console and expand the server name in the left pane of the console. Click on the Firewall Policy node. In the Task pane, click the Tasks tab. Click Create New Access Rule.
2. On the **Welcome to the New Access Rule Wizard** page, enter a name for the rule in the **Access Rule name** text box. In this example, we will call the rule **Limited Users Web Access**. Click **Next**.

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

4. On the **Protocols** page, select **Selected protocols** from the **This rule applies to** dropdown list. Click **Add**.
5. In the **Add Protocols** dialog box, double click on the **HTTP** and **HTTPS** protocols. Click **Close**.

6. Click **Next** on the **Protocols** page.
7. On the **Access Rule Sources** page, click **Add**. In the **Add Network Entities** dialog box, click on the **Networks** folder. Double click on the **Internal** network, and click **Close**.
8. Click **Next** on the **Access Rule Sources** page.

9. On the **Access Rule Destinations** page, click **Add**. On the **Add Network Entities** dialog box, click the **New** menu, and click **Domain Name Set**.

![Add Network Entities dialog box]

10. In the **New Domain Name Set Policy Element** dialog box, click **New**. Enter the first domain name ***.microsoft.com** and press ENTER. Enter the following three domains ***.msn.com**, ***.hotmail.com** and ***.windows.com**. In the **Name** text box, enter **Microsoft** and click **OK**.
11. In the **Add Network Entities** dialog box, click on the **Domain Name Sets** folder and then double click on the **Microsoft** entry. Click **Close**.
12. On the User Sets page, select All Users entry from the This rule applies to request from the following user sets list, and click Remove. Click Add.

13. In the Add Users dialog box, click the New menu.

14. On the Welcome to the New User Sets Wizard page, enter a name for the User Set in the User set name text box. In this example, we will name the User Set Limited Web Users. Click Next.

15. On the Users page, click Add. Select the Windows users and groups option.

16. In the Select Users or Groups dialog box, click the Locations button.

17. In the Locations dialog box, expand the Entire Directory entry and click on your domain name. In this example, the domain name is msfirewall.org. Click OK.
18. In the **Select Users or Groups** dialog box, enter **User2** in the **Enter the object names to select** text box and click **Check Names**. When the Active Directory finds the user name, it will be underlined. Click **OK**.

19. Click **Next** on the **Users** page.

20. Click **Finish** on the **Completing the New User Set Wizard** page.

21. Double click the **Limited Web Users** entry in the **Add Users** dialog box and click **Close**.

22. The **Limited Web Users** entry now appears in the **This rule applies to requests from the following user sets** list. Click **Next**.

23. Click **Finish** on the **Completing the New Access Rule Wizard** page.
Create an Access Rule Providing Administrators Greater Access to Protocols and Sites

Network administrators require a higher level of Internet access than other users on the network. However, even network administrators should be restrained from protocols that can lead to a significant risk of network compromise. One of these protocols is the Internet Relay Chat protocol, which is often used to trade viruses and pirated software. We will create a rule that allows members of the Domain Administrators group access to all protocols except for the dangerous IRC protocol.

The Access Rule can be characterized by the entries in the following table:

<table>
<thead>
<tr>
<th>Rule Element</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order (priority)</td>
<td>2 (after all rules are created)</td>
</tr>
<tr>
<td>Name</td>
<td>Administrator Internet Access</td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
</tr>
<tr>
<td>Protocols</td>
<td>All Protocols except IRC</td>
</tr>
<tr>
<td>From/Listener</td>
<td>Internal</td>
</tr>
<tr>
<td>To</td>
<td>External</td>
</tr>
<tr>
<td>Condition</td>
<td>Administrators (group)</td>
</tr>
</tbody>
</table>

The rule will look like this in the Firewall Policy Details pane:

![Firewall Policy Details pane](image)

Perform the following steps to create the administrators Access Policy:

1. In the Microsoft Internet Security and Acceleration Server 2004 management console, right click on the Firewall Policy node in the left pane of the console, point to New and click Access Rule.
2. On the Welcome to the New Access Rule Wizard page, enter the name of the rule in the Access rule name text box. In this example, we will call the rule Administrator Internet Access. Click Next.
3. On the Rule Action page, select Allow and click Next.
4. On the Protocols page, select the All outbound protocols except selected option from the This rule applies to dropdown list, then click Add.
5. In the **Add Protocols** dialog box, click on the **Instant Messaging** folder. Double click on the **IRC** protocol. Click **Close**.
6. Click **Next** on the **Protocols** page.

7. On the **Access Rule Sources** page, click **Add**. In the **Add Network Entities** dialog box, click on the **Networks** folder. Double click on the **Internal** entry and click **Close**.

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

9. On the **Access Rule Destinations** page, click **Add**. Click the **Networks** folder and then double click on the **External** entry. Click **Close**.

10. On the **User Sets** page, click **All Users** and **Remove**. Click **Add**.

11. In the **Add Users** dialog box, click the **New** menu.

12. On the **Welcome to the New User Sets Wizard** page, enter a name for the User Set in the **User set name** text box. In this example, we will name the User Set **Administrators**. Click **Next**.

13. On the **Users** page, click **Add**. Select **Windows users and groups**.

14. In the **Select Users or Groups** dialog box, click the **Locations** button.

15. In the **Locations** dialog box, expand the **Entire Directory** entry and click on your domain name. In this example, the domain name is **msfirewall.org**. Click **OK**.

16. In the **Select Users or Groups** dialog box, enter **Domain Admins** in the **Enter the object names to select** text box and click **Check Names**. When the Active Directory finds the user name, the name will be underlined. Click **OK**.
17. Click Next on the Users page.

18. Click Finish on the Completing the New User Set Wizard page.

19. In the Add Users dialog box, double click on the Administrators entry, and click Close.

20. Click Next on the User Sets page.

Create a DNS Server Access Rule Allowing Internal Network DNS Servers Access to Internet DNS Servers

We use a DNS server located on the Internet network to resolve Internet host names in our current scenario. This DNS server must be able to resolve Internet host names by contacting other DNS servers located on the Internet. Most machines that run critical network services do not typically have logged on users. For this reason, we will create an Access Rule that does not require a logged on user account. Instead, we will create a Computer Set that contains a list of all the DNS servers on the network.

A Computer Set is a collection of computer names and addresses associated with those computer names. This makes it easy to assign Access Rules that control outbound access for machines belonging to such a group. You should make Computer Groups for all your important network servers so that you do not need to depend on logged on user accounts to exercise outbound access control over these servers.

<table>
<thead>
<tr>
<th>Rule Element</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order (priority)</td>
<td>1 (after all rules are created)</td>
</tr>
<tr>
<td>Name</td>
<td>DNS Servers</td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
</tr>
<tr>
<td>Protocols</td>
<td>DNS</td>
</tr>
<tr>
<td>From/Listener</td>
<td>DNS Servers</td>
</tr>
<tr>
<td>To</td>
<td>External</td>
</tr>
<tr>
<td>Condition</td>
<td>All Users</td>
</tr>
</tbody>
</table>

The rule will look like this in the Firewall Policy Details pane:

Perform the following steps to create an Access Rule that allows the internal network DNS server access to DNS servers on the Internet:

1. In the Microsoft Internet Security and Acceleration Server 2004 management console, right click on the Firewall Policy node in the left pane of the console. Point to New and click Access Rule.
2. On the Welcome to the New Access Rule Wizard page, enter the name of the rule in the Access rule name text box. In this example, we will call the rule DNS Servers. Click Next.
3. On the Rule Action page, select Allow and click Next.
4. On the Protocols page, select Selected protocols from the This rule applies to list, and click Add.
5. In the Add Protocols dialog box, click on the Infrastructure folder. Double click on the DNS protocol. Click Close.
6. Click **Next** on the **Protocols** page.

7. On the **Access Rule Sources** page, click **Add**. In the **Add Network Entities** dialog box, click the **New** menu, then click the **Computer Set** command.

8. In the **New Computer Set Rule Element** dialog box, click **Add**. Click the **Computer** option.
9. In the **New Computer Rule Element** dialog box, enter a name for the DNS server in the **Name** text box. In this example, we'll name the first DNS server **DNS1**. Enter the IP address of the DNS server in the **Computer IP Address** text box. Click **OK**.

10. Click **OK** in the **New Computer Set Rule Element** dialog box.

11. In the **Add Network Entities** dialog box, click on the **Computer Sets** folder. Double click on the **DNS Servers** entry. Click **Close**.
12. Click Next on the Access Rule Sources page.

13. On the Access Rule Destinations page, click Add. Click the Networks folder and double click on the External entry. Click Close.


15. On the User Sets page, accept the default entry, All Users, and click Next.

Use HTTP Policy to Prevent Access to Suspect Web Sites

You can block access to Web sites based on virtually any component of the HTTP communication using ISA Server 2004 HTTP policy. For example, you might want to prevent access to all Web sites that contain a reference to the popular file-sharing application, Kaaza. This file-sharing program can present a risk to network security because the files downloaded via this application can contain viruses, worms and copyrighted material.

In the following walkthrough, you will configure the HTTP policy for the Administrator Internet Access and Limited Access Web Users rules to block all Web connections to sites that contain the string “Kaaza” in them. While this example uses a blunt approach to blocking Kaaza-related sites, it does demonstrate the power of ISA Server 2004’s deep HTTP inspection mechanisms.

Perform the following steps to prevent users from accessing Kaaza-related sites:
1. In the Microsoft Internet Security and Acceleration Server 2004 management console, click on the Firewall Policy node.
2. Right click on the Administrator Internet Access rule and click Configure HTTP.
3. In the Configure HTTP policy for rule dialog box, click on the Signatures tab.
4. On the Signatures tab, click on the Add button.
5. In the Signature dialog box, enter a name for the signature in the Name text box. In this example we will enter Kaaza URL. Select the Request URL entry in the Search in list. Enter the string kaaza in the Signature text box. Click OK.
6. Click **Apply** and **OK** in the **Configure HTTP policy for rule** dialog box.
7. Repeat the preceding steps for the **Limited Access Web Users** rule.
8. Click **Apply** to save the changes and update firewall policy.
9. Click **OK** in the **Apply New Configuration** dialog box.
Test the Access Rules

Now we have an ISA Server 2004 Access Policy in place, we can test the policy.

Perform the following steps to test Access Policy:

1. First, review the Access Policies created on the ISA Server 2004 firewall. In the Microsoft Internet Security and Acceleration Server 2004 management console, expand the server name and click on the Firewall Policy node. Review the Access Rules in the Details pane of the console.

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>Action</th>
<th>Protocols</th>
<th>From / Listener</th>
<th>To</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DNS Servers</td>
<td>Allow</td>
<td>DNS</td>
<td>DNS Servers</td>
<td>External</td>
<td>All Users</td>
</tr>
<tr>
<td>2</td>
<td>Administrator</td>
<td>Allow</td>
<td>IRC</td>
<td>Internal</td>
<td>External</td>
<td>Administrators</td>
</tr>
<tr>
<td>3</td>
<td>Limited Access</td>
<td>Allow</td>
<td>HTTP</td>
<td>Internal</td>
<td>Microsoft</td>
<td>Limited Web Users</td>
</tr>
<tr>
<td>4</td>
<td>Unrestricted</td>
<td>Allow</td>
<td>All Protocols</td>
<td>Internal</td>
<td>External</td>
<td>All Users</td>
</tr>
<tr>
<td>5</td>
<td>VPN Clients to</td>
<td>Allow</td>
<td>All Protocols</td>
<td>VPN Clients</td>
<td>VPN Clients</td>
<td>All Users</td>
</tr>
<tr>
<td></td>
<td>Last Default</td>
<td>Kerala</td>
<td>All Networks</td>
<td>All Networks</td>
<td>All Networks</td>
<td>All Users</td>
</tr>
</tbody>
</table>

2. Log on to the CLIENT computer as User2. Open the browser and enter www.microsoft.com in the Address bar. Press ENTER.

3. The home page of the Microsoft site appears in the browser. In the Internet Explorer Address bar, enter www.isaserver.org and press ENTER.

4. You will see the MSN search page indicating that the www.isaserver.org page could not be found. You can provide a more informative response to users by redirecting denied requests to an Internet Web server.

5. In Internet Explorer, enter www.msn.com and press ENTER.

6. You see the home page of the www.msn.com Web site. Note that some graphics do not appear on the page because they fall outside the range of sites allowed by the Domain Set we created for the Access Rule.

7. In the Internet Explorer Address bar, enter the URL http://www.msn.com/kaaza. An error page is returned indicating that the HTTP Security filter has blocked the connection. The Signature configured in the HTTP policy for the Access Rule detected that Kaaza was in the URL and blocked the connection attempt.
8. Log off the CLIENT machine and then log on as Administrator.


10. Enter www.isaserver.org in the Address bar of Internet Explorer and press ENTER. As an Administrator, you are able to access the site.

11. Enter www.isaserver.org/kaaza in the Address bar of Internet Explorer. You see the same HTTP Security filter error message. Again, the settings in the HTTP policy of the rule block the connection attempt.

12. Click Start and click the Run command. In the Run dialog box, enter cmd in the Open text box. Click OK.

13. At the command line, enter the line telnet ftp.microsoft.com 21 and press ENTER. You will see a banner saying 220 Microsoft FTP Service. Enter quit and press ENTER. You will then see the message 221 Thank-you for using Microsoft products!

14. At the command prompt, enter the line telnet dragons.ca.usdal.net 6667 and press ENTER. You will see an error indicating that the connection failed. If you look at the connection attempt in the ISA Server 2004 real-time log monitor, you will see that the connection attempt was actively denied by the firewall.

15. Log off the CLIENT computer.
Conclusion

In this ISA Server 2004 Configuration Guide section, we discussed the variety of methods you can use to control outbound access to the Internet using ISA Server 2004 Access Rules. In the walkthroughs, you created Access Rules that controlled access to specific Web sites and protocols based on user and group membership. In addition, you created policy elements "on the fly" while creating the Access Rules. In the next chapter of the ISA Server 2004 Configuration Guide, we examine the procedures required to publish a Web and FTP server located on the perimeter network segment.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

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

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

© 2004 Microsoft Corporation. All rights reserved.

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, place, or event is intended or should be inferred.


The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
Chapter 12

For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

ISA Server 2004 firewalls enable you to publish resources located on protected networks so external users can access those resources. There are two primary methods available to publish resources on a protected network:

- Web Publishing Rules
- Server Publishing Rules

Web Publishing Rules can be used to publish Web servers. External users connect to Web Published Web servers using the HTTP or HTTPS (SSL) protocols. Web Publishing Rules have a number of advantages over Server Publishing Rules, and you should always use a Web Publishing Rule when publishing a Web site.

Server Publishing Rules can be created for virtually any Server Protocol. You can use Server Publishing Rules to publish FTP sites, mail servers, news servers, terminal servers and many more. Use Server Publishing Rules when Web Publishing Rules cannot be used to publish a service on a protected network.

In this ISA Server 2004 Configuration Guide chapter, we will publish a Web site and an FTP site located on the perimeter network segment. You should still read this section even if you decided to use the Edge Firewall template instead of the 3-Leg Perimeter Network Template. The same publishing principles apply; the only difference is the location of the servers being published.

Follow the procedures listed below to publish the Web and FTP sites on the perimeter network:

- Configure the Web site
- Configure the FTP site
- Disable the custom rules and enable the template created rules
- Create the Web Publishing Rule
- Create the FTP Server Publishing Rule
- Test the connection
Configure the Web Site

The first step is to configure the Web site on the perimeter network segment. In a production environment, the Web site will already be configured and be ready to publish. In this current example, we need to create a default Web site document and set a few parameters so that we can test it successfully.

Perform the following steps to configure the Web site on the IIS server on the perimeter network:

1. Click **Start** and point to **Administrative Tools**. Click **Internet Information Services (IIS) Manager**.
2. In the **Internet Information Services (IIS) Manager** console, expand the server name and the **Web sites** node.
3. Right click the **Default Web Site** node and click **Properties**.
4. In the **Default Web Site Properties** dialog box, select the IP address of the server in the **IP address** list.

![Default Web Site Properties](image)

5. Click on the **Documents** tab, and click **Add**. In the **Add Content Page** dialog box, enter the name **default.txt**. Click **OK**.
6. Use the **Move Up** button to move the **default.txt** entry to the top of the list.
7. Click **Apply**; then click **OK** in the **Default Web Site Properties** dialog box.

8. Right click the server name in the left pane of the console and point to **All Tasks**. Click **Restart IIS**.

9. Select **Restart Internet Services on TRIHOMEDMZLAN1** in the **Stop/Start/Rstart** dialog box and click **OK**.

10. Close the **Internet Information Services (IIS) Manager** console.
11. Click Start and Windows Explorer.

12. Navigate to the C:\inetpub\wwwroot folder. Click the File menu, point to New and click Text Document.

13. Double click the New Text Document.txt entry in the right pane of the console. Enter into the document the following text: This is the Web site on the perimeter network segment. Click File and then click Exit. Click Yes in the Notepad dialog box asking if you want to save the changes.

Configure the FTP Site

The next step is to configure the FTP site so that it is ready to be published. You will set the IP address the FTP site listens on and configure messages for the FTP site to return to users connecting to the site. In addition, you will enable users to upload files to the FTP site. In a production environment, you may want to prevent users from being able to upload to the Web site to prevent Internet intruders from placing illegal and copyrighted material on your site.

Perform the following steps to configure the FTP site:

1. Click **Start** and point to **Administrative Tools**. Click **Internet Information Services (IIS) Manager**.

2. Expand the server name in the left pane of the **Internet Information Services (IIS) Manager** console, then expand the **FTP Sites** node.

3. Right click on the **Default FTP Site** and click **Properties**.

4. In the **Default FTP Site Properties** dialog box, select the IP address of the perimeter network server in the **IP address** list.

5. Click on the **Messages** tab. In the **Banner** text box, enter **This is the perimeter network FTP site**. In the **Welcome** text box, enter **Welcome to the ISA firewall protected FTP site**. In the **Exit** text box, enter **Goodbye!** In the **Maximum connections** text box, enter the phrase **Site is busy come back later**.
6. Click on the **Home Directory** tab. On the **Home Directory** tab, put a checkmark in the **Write** text box. Note that in a production environment you should be very careful about allowing write access to FTP sites. Internet intruders can take advantage of poorly-secured FTP sites and store illegal material on your site.
7. Click **Apply** and **OK** in the **Default FTP Site Properties** dialog box.

8. Right click the server name in the left pane of the console and point to **All Tasks**. Click **Restart IIS**.

9. Select the **Restart Internet Services on TRIHOMEDMZLAN1** entry in **What do you want IIS to do?** and click **OK**.

10. Close the **Internet Information Services (IIS) Manager** console.

11. Click **Start** and **Windows Explorer**.

12. Navigate to the folder **C:\Program Files\NetMeeting**. Select all the files in that folder and copy them to the clipboard.

13. Navigate to the folder **C:\inetpub\ftproot**. Paste the files you copied to the clipboard to this folder.
Disable the Custom Rules and Enable the Template Created Rules

In the last chapter in this ISA Server 2004 Configuration Guide, we created Access Rules that allowed for user/group-based access control for outbound connections. We now want to disable those rules and use the rules that the 3-Leg Perimeter Network Template Wizard created.

Perform the following steps to disable the custom rules created in the last chapter and enable the rules created by the Template:

1. At the ISA Server 2004 firewall machine, open the Microsoft Internet Security and Acceleration Server 2004 management console. Expand the server name and click the Firewall Policy node.

2. Click the DNS Servers policy. Hold down the CTRL key and click the Administrator Internet Access and Limited Access Web Users Access Rules. Right click one of the selected rules and click Disable.

3. Click Apply to save the changes and update the firewall policy.

4. Click OK in the Apply New Configuration dialog box.

5. Click the first rule created by the Wizard. In this example, the first rule is the VPN Clients to Internal Network rule. Hold down the CTRL key and click the second rule so that both rules are selected. Right click one of the selected rules and click Enable.
6. With the two Access Rules still selected, click the blue, up-pointing arrow in the console button bar to move the rules to the top of the list.

7. Click **Apply** to save the changes and update firewall policy.

8. Click **OK** in the **Apply New Configuration** dialog box.
Create the Web Publishing Rule

You’re now ready to create the Web Publishing Rule. The Web Publishing Rule will configure the ISA Server 2004 firewall to listen for incoming requests for your Web site. Because the ISA Server 2004 firewall is an intelligent, application layer aware firewall, it will accept requests only from external users who enter the correct Web site name to access the site. External users, hackers and Internet worms will not be able to connect to the Web site by using a simple IP address.

Perform the following steps to create the Web Publishing Rule:

1. At the ISA Server 2004 firewall computer, open the Microsoft Internet Security and Acceleration Server 2004 management console and expand your server name. Click on the Firewall Policy node.
2. Right click on the Firewall Policy node, point to New and click Web Server Publishing Rule.
3. On the Welcome to the New Web Publishing Rule Wizard page, enter a name for the rule in the Web publishing rule name text box. In this example, we will name the rule Perimeter Web Server. Click Next.
4. On the Select Rule Action page, select Allow and click Next.
5. On the Define Website to Publish page, enter a name for the Web server on the perimeter network in the Computer name or IP address text box. This is the name or IP address of the computer on the perimeter network segment, not the IP address on the external interface of the ISA Server 2004 firewall. In this example, we will use the name perimeter.msfirewall.org; this name must resolve to the IP address used by the Web server on the perimeter network. This can be done by implementing a split DNS infrastructure, or by using a HOSTS file entry on the ISA Server 2004 firewall machine. Later we will create a HOSTS file entry for the perimeter network machine. In the Folder text box, enter /*. Click Next.
6. On the Public Name Details page, select This domain name (type below) in the Accept requests for list. In the Public name text box, enter the name that external users will use to access the site. In this example we will use the name perimeter.msfirewall.org. When users enter http://perimeter.msfirewall.org into their browsers, the name will resolve to the external IP address on the ISA Server 2004 firewall that listens for incoming Web requests for the site. In the Path (optional) text box, enter /*. This allows users access to all directories they have permission to access on the Web site. Click Next.
7. On the **Select Web Listener** page, click **New**.

8. On the **Welcome to the New Web Listener Wizard** page, enter a name for the Web listener in the **Web listener name** text box. In this example we will name the listener **Listener1**. Click **Next**.

9. On the **IP Addresses** page, put a checkmark in the **External** check box and click **Address**.
10. On the External Network Listener IP Selection page, select Specified IP addresses on the ISA Server computer in the selected network. In the Available IP Addresses list, select the IP address on the external interface of the ISA Server 2004 firewall and click Add. The address now appears in the Selected IP Addresses list. Click OK.

11. Click Next on the IP Addresses page.
12. On the **Port Specification** page, confirm that there is a checkmark in the **Enable HTTP** check box and that the default **HTTP port** number is **80**. Click **Next**.
13. Click **Finish** on the **Completing the New Web Listener Wizard** page.

14. The **Listener1** entry now appears in the **Web listener** list. Click **Next**.

15. On the **User Sets** page, accept the default entry, **All Users**, and click **Next**.

16. Click **Finish** on the **Completing the New Web Publishing Rule Wizard** page.

17. Click **Apply** to save the changes and update the firewall policy.

18. Click **OK** in the **Apply New Configuration** dialog box.

The next step is to create a HOSTS file entry so that the firewall will resolve the name `perimeter.msfirewall.org` to the IP address used by the Web site on the perimeter network. In this example, the Web site is listening on IP address **172.16.0.2**.

1. Click **Start** and **Run**. In the **Run** dialog box, enter `notepad` in the **Open** text box and click **OK**.

2. Click the **File** menu and **Open**. In the **Open** dialog box, enter `c:\windows\system32\drivers\etc\hosts` in the **File name** text box and click **Open**.
3. Add the following line to the HOSTS file:

   172.16.0.2     perimeter.msfirewall.org

   Press ENTER at the end of the line so that the insertion point sits on the next line. Click File and then click Exit. In the Notepad dialog box, click Yes to indicate that you wish to save the changes.
hosts - Notepad

File Edit Format View Help

# Copyright (c) 1993-1999 Microsoft Corp.
#
# 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:
#
# # 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host

127.0.0.1 localhost
172.16.0.2 perimeter.msfirewall.org
Create the FTP Server Publishing Rule

Server Publishing Rules are simpler than Web Publishing Rules. A Server Publishing Rule forwards incoming requests to the published server and exposes them to application layer filters installed on the ISA Server 2004 firewall. The only information you need to supply to the Server Publishing Rule wizard is the IP address of the server to be published, the IP address you want the ISA Server 2004 firewall to listen for requests, and the Server Protocol that is published. Note that all Server Protocols have their primary connection set as **inbound**.

Perform the following steps to create the FTP Server Publishing Rule:

1. At the ISA Server 2004 firewall machine, open the **Microsoft Internet Security and Acceleration Server 2004** management console and expand the server name. Click on the **Firewall Policy** node.

2. Right click the **Firewall Policy** node, point to **New** and click **Server Publishing Rule**.

3. On the **Welcome to the New Server Publishing Rule Wizard** page, enter a name for the rule in the **Server publishing rule name** text box. In this example we will use the name **Perimeter FTP Server** and click **Next**.

4. On the **Select Server** page, enter the IP address of the FTP server on the perimeter network in the **Server IP address** text box. In this example, the FTP server is listening on IP address **172.16.0.2**. Click **Next**.

5. On the **Select Protocol** page, select the **FTP Server** protocol from the **Selected protocol** list. Click **Next**.
6. On the **IP Addresses** page, place a checkmark in the **External** check box. Click the **Addresses** button.

7. In the **External Network Listener IP Selection** dialog box, select the **Specified IP addresses on the ISA Server computer in the selected network** option. Select the IP address on the external interface of the ISA Server 2004 firewall in the **Available IP Addresses** list and click **Add**. The address now appears in the **Selected IP Addresses** list. Click **OK**.

8. Click **Next** on the **IP Addresses** page.

9. Click **Finish** on the **Completing the New Server Publishing Rule Wizard** page.

The next step is to correct the Network Relationship between the perimeter network and the external network:

1. In the **Microsoft Internet Security and Acceleration Server 2004** management console, expand the **Configuration** node and click the **Networks** node.

2. In the **Details** pane, click the **Network Rules** tab. Right click the **Perimeter Access** Network Rule and click **Properties**.

3. In the **Perimeter Access Properties** dialog box, click the **Network Relationship** tab.

4. On the **Network Relationship** tab, select **Network Address Translation (NAT)**. Click **Apply** and **OK**.

5. Click **Apply** to save the changes and update the firewall policy.

6. Click **OK** in the **Apply New Configuration** dialog box.
Test the Connection

We are now ready to test the connection. Internet Explorer 6.0 can access both Web and FTP sites within the browser. The only difference in the current example is that you will specify http:// for the Web site and ftp:// for the FTP site. You will also see in the following walkthrough how to configure the FTP site to accept uploads from external users.

Perform the following steps to test the Web and FTP Server Publishing Rules:

1. The first step on the external Windows 2000 client is to configure a HOSTS file entry so that the client will resolve the name perimeter.msfirewall.org to the external address on the ISA Server 2004 firewall.

2. Click Start and Run. In the Run dialog box, enter notepad in the Open text box, and click OK.

3. Click the File menu and Open. In the Open dialog box, enter c:\windows\system32\drivers\etc\hosts in the File name text box, and click Open.

4. Add the following line to the HOSTS file:
   
   192.168.1.70     perimeter.msfirewall.org

   Press ENTER at the end of the line so that the insertion point sits on the next line. Click File and then click Exit. In the Notepad dialog box, click Yes to save the changes.

5. From the external client machine, open Internet Explorer and enter http://perimeter.msfirewall.org into the Address bar. Press ENTER. The default Web page for the site will appear.

6. In Internet Explorer, enter ftp://perimeter.msfirewall.org in the Address bar and press ENTER. You will see the contents of the FTP site. By default, you can only download files from the site.
7. If you would like to upload files to the site, return to the Microsoft Internet Security and Acceleration Server 2004 management console and right click on the Perimeter FTP Server publishing rule and click Configure FTP.

8. In the Configures FTP protocol policy dialog box, remove the checkmark from the Read Only check box. Click Apply and OK.
9. Click **Apply** to save the changes and update the firewall policy.

10. Click **OK** in the **Apply New Configuration** dialog box.
Conclusion

In this ISA Server 2004 Configuration Guide document we discussed two primary methods that allow external users access to resources contained on protected networks. We first used a Web Publishing Rule to allow inbound access to resources contained in a perimeter network segment. Next, we used a Server Publishing Rule to allow inbound access to an FTP server on the perimeter network segment. You can apply the same principles can when publishing resources contained on an Internet network segment. In the next chapter in the ISA Server 2004 Configuration Guide, we will examine the procedures required to make the ISA Server 2004 firewall computer an application layer filtering SMTP relay server.
ISA Server 2004 Configuration Guide: Configuring the Firewall as a Filtering SMTP Relay
Chapter 13

For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

One of the optional components included with the ISA Server 2004 is the SMTP Message Screener. The SMTP Message Screener can inspect SMTP messages at the application layer relay or reject messages based on parameters you configure. The SMTP Message Screener can evaluate incoming SMTP mail based on the following characteristics:

- Sender mail account and sender domain name
- Attachments name, attachment extension and attachment size
- Keywords included in the subject line and body of text/plain and text/html messages

For example, a common attachment extension for Internet worms is the .pif extension. Since very few or no legitimate e-mail messages contain attachments with the .pif extension, you can configure the filter to match messages with attachments with this extension and perform one of the following actions:

- Delete the message
- Hold the message
- Forward the message to a specified e-mail account

The SMTP Message Screener is an integral part of your e-mail defense in-depth scheme. Internet worms and viruses, in addition to spam, represent some of the most significant risks to your network. Worms and viruses can attack network servers, services and workstations throughout the Internal network. Spam clogs Internal network bandwidth and consumes employee time, costing many thousands, even millions, of dollars per month in employee productivity.

E-mail defense in depth allows you to distribute the processing of incoming and outgoing e-mail messages. SMTP message evaluation is a processor-intensive activity, and the more machines the load is distributed to, the more efficient the process. You can use the ISA Server 2004 SMTP Message Screener together with the Exchange SMTP Gateway Server to provide an ideal level of e-mail defense in depth.

In the example discussed in this document, we will configure the ISA Server 2004 firewall as an inbound and outbound SMTP relay. The inbound SMTP relay component will accept incoming mail from external SMTP servers destined for e-mail domains that you manage on your Exchange Server. The outbound SMTP relay is used to screen e-mail send out from the Exchange Server to e-mail domains on the Internet (e-mail domains that you do not host or control).

To achieve these goals, you will perform the following steps:

- Restore the system to its post-installation state
- Assign a second IP address to the Internal interface of the ISA Server 2004 firewall
- Install and configure the SMTP Service
- Install the SMTP Message Screener
- Create the SMTP Server Publishing Rules
- Configure SMTP Message Screener logging
- Test SMTP Filtering
Restore the System to its Post-installation State

In order to fully test the inbound and outbound SMTP relay configuration in this scenario, we will return the machine to its post-installation state so that other Access Rules do not interfere with the scenario development. In a production environment, you would leave your current Access Rules intact and add the Server Publishing Rules required to create the inbound and outbound SMTP relays.

Perform the following steps to restore the ISA Server 2004 firewall machine to its post-installation state:

1. Open the Microsoft Internet Security and Acceleration Server 2004 management console and right click on the server name. Click the Restore command.
2. In the Restore Configuration dialog box, select the backup file you created earlier and click Restore.
3. In the Type Password to Open File dialog box, enter the password you assigned to the file in the Password text box and click OK.
4. Click OK in the Importing dialog box after you see the message The configuration was successfully restored.
5. Click Apply to save the changes and update the firewall policy.
6. Select Save the changes and restart the service(s) in the ISA Server Warning dialog box, and click OK.
7. Click OK in the Apply New Configuration dialog box.
Assign a second IP address to the Internal interface of the ISA Server 2004 firewall

We will add a second IP address to the Internal interface of the ISA Server 2004 firewall machine. This will allow us to publish the outbound SMTP relay on a different IP address than the inbound SMTP relay. While this is not required, it greatly simplifies tracking which relay is to be used by particular clients.

Perform the following steps to add a second IP address to the Internal interface of the ISA Server 2004 firewall machine:

1. At the ISA Server 2004 firewall machine, right click on My Network Places on the desktop and click Properties.
2. In the Network Connections window, right click the LAN interface and click Properties.
3. In the LAN Properties dialog box, scroll through the This connection uses the following items list and double click on Internet Protocol (TCP/IP).
4. In the Internet Protocol (TCP/IP) Properties dialog box, click the Advanced button.
5. In the Advanced TCP/IP Settings dialog box, click the IP Settings tab. In the IP addresses frame, click Add.
6. In the TCP/IP Address dialog box, enter 10.0.0.10 in the IP address text box. Enter 255.255.255.0 in the Subnet mask text box. Click Add.
7. The IP address 10.0.0.10 now appears second in the list of IP addresses. Click OK.
8. Click OK in the Internet Protocol (TCP/IP) Properties dialog box.
9. Click OK in the LAN Properties dialog box.
Install and Configure the SMTP Service

Install the IIS 6.0 SMTP service before the ISA Server 2004 SMTP Message Screener. The SMTP service works together with the SMTP Message Screener to examine and block offending e-mail messages.

Perform the following steps to install the IIS 6.0 SMTP service:

1. Click Start and point to Control Panel. Click Add or Remove Programs.
2. In the Add or Remove Programs window, click Add/Remove Window Components on the left side of the window.
3. On the Windows Components page, click Application Server in the list of Components, and click Details.
4. In the Application Server dialog box, click Internet Information Services (IIS), and click Details.
5. In the Internet Information Services (IIS) dialog box, place a checkmark in the SMTP Service check box and click OK.

6. Click OK in the Application Server dialog box.
7. Click Next on the Windows Components page.
8. Click OK in the Insert Disk dialog box.
9. Enter the path to the i386 folder in the Copy file from text box in the Files Needed dialog box.
10. Click Finish in the Completing the Windows Components Wizard page.

The next step is to configure the SMTP server service to support inbound and outbound relay:

1. Click Start and point to Administrative Tools. Click Internet Information Services (IIS) Manager.
2. In the Internet Information Services (IIS) Manager console, expand the computer name in the left pane of the console. Right click the Default SMTP Virtual Server and click Properties.

3. In the Default SMTP Virtual Server Properties dialog box, click the Access tab.

4. On the Access tab, click the Relay button in the Relay restrictions frame.

5. In the Relay Restrictions dialog box, confirm that the Only the list below option is selected. Then click Add.

6. In the Computer dialog box, select the Single computer option and enter the IP address of the Exchange Server in the IP address text box. In this example the IP address of the Exchange Server is 10.0.0.2. Click OK.

7. Click OK in the Relay Restrictions dialog box.

8. Click Apply and OK in the Default SMTP Virtual Server Properties dialog box.

9. Expand the Default SMTP Virtual Server node in the left pane of the console and right click the Domains node. Point to New and click Domain.


11. On the Domain Name page, enter the domain hosted on the Internal network in the Name text box. This is the domain that you want the SMTP relay on the ISA Server 2004 firewall to accept incoming mail from Internet SMTP servers. In this example, the Internal network domain is msfirewall.org, so enter that. Click Finish.

12. Double click on the msfirewall.org domain in the right pane of the console.

13. In the msfirewall.org Properties dialog box, place a checkmark in the Allow incoming mail to be relayed to this domain check box. Select Forward all mail to smart host. Enter the IP address of the Exchange Server on the Internal network in the text box, enclosed in straight brackets. In our current example, the IP address of the Exchange Server on the Internal network is 10.0.0.2, so we will enter [10.0.0.2]. Click Apply and OK.
14. Right click the **Default SMTP Virtual Server** node and click **Stop**. Right click the **Default SMTP Virtual Server** node and click **Start**.
Install the SMTP Message Screener

The SMTP Message Screener is an optional ISA Server 2004 component. This feature integrates with the IIS 6.0 SMTP service to examine and block SMTP mail based on parameters you configure in the Message Screener.

Perform the following steps to install the SMTP Message Screener on the ISA Server 2004 firewall computer:


2. Locate the ISA Server 2004 installation media and double click on the **isaautorun.exe** file.

3. In the autorun menu, click the **Install ISA Server 2004** icon.

4. Click **Next** on the **Welcome to the Installation Wizard for Microsoft ISA Server 2004** page.

5. On the **Program Maintenance** page, select **Modify** and click **Next**.

6. On the **Custom Setup** page, click the **Message Screener** option and **This feature, and all subfeatures, will be installed on local hard drive**. Click **Next**.
7. Click **Install** on the **Ready to Modify the Program** page.

8. Put a checkmark in the **Invoke ISA Server Management when the wizard closes** check box and click **Finish** on the **Installation Wizard Completed** page.

9. Close the **Autorun** menu.
Create the SMTP Server Publishing Rules

The SMTP Message Screener works together with SMTP Server Publishing Rules. Each SMTP Server Publishing Rule can be configured with a custom set of SMTP Message Screener parameters. This allows you to create different e-mail screening policies for the inbound and outbound SMTP relays. Different SMTP Message Screener configurations allow you to block different e-mail messages coming into the network versus what gets blocked on the way out.

Perform the following steps to create the Server Publishing Rule that listens on the external interface of the ISA Server 2004 firewall:

1. Open the Microsoft Internet Security and Acceleration Server 2004 management console and expand the server name in the left pane of the console. Click on the Firewall Policy node.

2. Right click the Firewall Policy node and point to New. Click Server Publishing Rule.

3. On the Welcome to the New Server Publishing Rule Wizard page, enter the name for the rule in the Server publishing rule name text box. In this example, we will name the rule Inbound SMTP Relay, as this rule will use the external interface of the ISA Server 2004 to accept incoming mail to be relayed. Click Next.

4. On the Select Server page, enter the IP address on the Internal interface of the ISA Server 2004 firewall that you want to publish. Enter 10.0.0.1, which is the primary IP address on the Internal interface of the ISA Server 2004 firewall machine. Click Next.

5. On the Select Protocol page, select the SMTP Server protocol from the Selected protocol list. Click Next.

<table>
<thead>
<tr>
<th>New Server Publishing Rule Wizard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select Protocol</strong></td>
</tr>
<tr>
<td>Select the protocol used by the published server</td>
</tr>
</tbody>
</table>

Selected protocol:

- SMTP Server

ISA Server has a special wizard for publishing mail servers. The mail publishing wizard lets you publish additional mail protocols and supports features such as Outlook Web Access (OWA)

For full SMTP filtering functionality the Message Screener must be installed.
6. On the IP Addresses page, put a checkmark in the External check box and click the Address button.

7. In the External Network Listener IP Selection dialog box, select Specified IP addresses on the ISA Server computer in the selected network. Click the IP address for the external interface you want to use in the rule. In this example, the IP address is 192.168.1.70. Click Add. The IP address now appears in the Selected IP Addresses list. Click OK.

8. Click Next on the IP Addresses page.


The next step is to create the Server Publishing Rule that will accept outbound relay from the Internal network Exchange Server:

1. Open the Microsoft Internet Security and Acceleration Server 2004 management console and expand the server name in the left pane of the console. Click on the Firewall Policy node.

2. Right click the Firewall Policy node and point to New. Click Server Publishing Rule.

3. On the Welcome to the New Server Publishing Rule Wizard page, enter the name for the rule in the Server publishing rule name text box. In this example, we will name the rule Outbound SMTP Relay as this rule will use the external interface of the ISA Server 2004 to accept incoming mail to relay. Click Next.

4. On the Select Server page, enter the IP address on the Internal interface of the ISA Server 2004 firewall that you want to publish. Enter 10.0.0.10, which is the secondary IP address on the Internal interface of the ISA Server 2004 firewall machine. Click Next.

5. On the Select Protocol page, select the SMTP Server protocol from the Selected protocol list. Click Next.

6. On the IP Addresses page, put a checkmark in the Internal check box and click the Address button.
7. In the **External Network Listener IP Selection** dialog box, select the **Specified IP addresses on the ISA Server computer in the selected network** option. Click the IP address on the Internal interface you want to use in the rule. In this example, the IP address is **10.0.0.10**, then click **Add**. The IP address now appears in the **Selected IP Addresses** list. Click **OK**.

8. Click **Next** on the **IP Addresses** page.

![New Server Publishing Rule Wizard](image)

9. Click **Finish** on the **Completing the New Server Publishing Rule Wizard** page.

Now we are ready to configure the SMTP Message Screener. Each Publishing Rule can be configured with a different SMTP Message Screener configuration.

Perform the following steps on the **Outbound SMTP Relay** Server Publishing Rule:

1. Right click the **Outbound SMTP Relay** rule and click **Configure SMTP**.
2. Click on the **General** tab in the **Configure SMTP Protocol Policy** dialog box. Place a checkmark in the **Enable support for Message Screener** checkbox.

3. Click on the **Keywords** tab. Place a checkmark in the **Enable this rule** checkbox. Click **Add**. In the **Mail Keyword Rule** dialog box, enter **resume** in the **Keyword** text box. Select the **Message header or body** option. Select the **Hold message** option from the **Action** list. Click **OK**.

4. Click **Apply** and then click **OK** in the **Configure SMTP Protocol Policy** dialog box.
Perform the following steps on the Inbound SMTP Relay Server Publishing Rule:

1. Right click the Inbound SMTP Relay rule and click Configure SMTP.

2. Click on the General tab in the Configure SMTP Protocol Policy dialog box. Place a checkmark in the Enable support for Message Screener check box.

3. Click on the Keywords tab. Click the Add button. In the Mail Keyword Rule dialog box, enter mail enhancement in the Keyword text box. Select the Message header or body option. Select the Hold message option from the Action list. Click OK.

4. Click Apply and then click OK in the Configure SMTP Protocol Policy dialog box.

5. Click Apply to save the changes and update the firewall policy.

6. Click OK in the Apply New Configuration dialog box.
Create the Outbound SMTP Access Rule

Perform the following steps to create an outbound SMTP Access Rule that enables the ISA Server 2004 firewall to relay SMTP from the Internal Exchange Server to SMTP servers for other domains on the Internet:

1. In the Microsoft Internet Security and Acceleration Server 2004 management console, expand the computer name in the left pane of the console and click the Firewall Policy node. Right click on the Firewall Policy node, point to New and click Access Rule.

2. In the Welcome to the New Access Rule Wizard page, enter a name for the rule in the Access Rule name text box. In this example we will call this Outbound SMTP from Local Host. Click Next.

3. On the Rule Action page, select Allow and click Next.

4. On the Protocols page, select the Selected protocols option from the This rule applies to list, and click Add.

5. In the Add Protocols dialog box, click on the Common Protocols folder and double click on the SMTP protocol. Click Close.

6. Click Next on the Protocols page.

7. On the Access Rule Sources page, click the Add button. In the Add Network Entities dialog box, click the Networks folder and double click on Local Host. Click Close.

8. Click Next on the Access Rule Sources page.

9. On the Access Rule Destinations page, click Add. In the Add Network Entities dialog box, click the Networks folder and double click on the External network. Click Close.
10. On the User Sets page, accept the default value, All Users, and click Next.
12. Click Apply to save the changes and update the firewall policy.
13. Click OK in the Apply New Configuration dialog box.
Configure SMTP Message Screener Logging

The SMTP Message Screener logs all messages moving the inbound and outbound SMTP relays. This logging feature helps you troubleshoot and access the e-mail messages moving through the server and confirm that the SMTP Message Screener is doing what you expect it to do.

Perform the following steps to configure the SMTP Message Screener logging feature:

1. In the Microsoft Internet Security and Acceleration Server 2004 management console, expand the computer name in the left pane of the console and click the Monitoring node.

2. Click the Logging tab in the Details pane. Expose the Task pane if it is not already open. In the Task pane, click the Tasks tab and Configure SMTP message Screener Logging.

3. In the SMTP Message Screener Logging Properties dialog box, note that the only logging format available is the File format. Select the ISA Server file format from the Format list. Confirm that there is a checkmark in the Enable logging for this service check box. Click the Options button.

4. In the Options dialog box, confirm that ISA Logs folder is selected. Make a note of the Log file storage limits that are configured by default, and how it Maintains log storage limit by. Change the value in the Delete files older than (days) from 7 to 30. Confirm that there is a checkmark in the Compress log files check box.
5. Click **OK** in the **Options** dialog box.

6. Click **Apply** and then click **OK** in the **SMTP Message Screener Properties** dialog box.

7. Click **Apply** to save the changes and update the firewall policy.

8. Click **OK** in the **Apply New Configuration** dialog box.
Test SMTP Filtering

Now that the SMTP Server Publishing Rule and SMTP Message Screener configurations are in place, we're ready to test the effectiveness of the Message Screener.

Perform the following on the external client machine to test the inbound SMTP relay function:

1. On the external client computer, open Outlook Express. If presented with the e-mail account Wizard, cancel out of the Wizard so that you can manually configure the e-mail account.
2. In the Outlook Express application, click the Tools menu and click Accounts.
3. In the Internet Accounts dialog box, click Add. Click the Mail command.
4. In the Your Name text box, enter your name. Click Next.
5. In the E-mail address text box, enter an e-mail address. In this example we will enter administrator@Internal.net. Click Next.
6. On the E-mail Server Names page, confirm that POP3 is selected in the My incoming mail server is a X server list. Enter a bogus entry in the Incoming mail (POP3, IMAP or HTTP) server text box. In this example, we will enter blah.com. In the Outgoing mail (SMTP) server text box, enter the IP address that the External SMTP Relay Server Publishing Rule is listening on. In this example, the External SMTP Relay Server Publishing Rule is listening on the address 192.168.1.70, so we will enter that value into this text box. Click Next.
7. On the Internet Mail Logon page, enter a bogus account name in the Account name text box. In this example, enter the name Administrator. In the password box, enter a random password. Click Next.
8. Click Finish on the Congratulations page.
9. Click Close in the Internet Accounts dialog box.
10. Click the Create Mail button in the Outlook Express button bar.
11. In the New Message dialog box, enter the address administrator@msfirewall.org. Enter mail enhancement in the Subject text box. Click Send in the button bar.
12. Return to the ISA Server 2004 firewall machine. Click Start and Windows Explorer. Navigate to C:\Inetpub\mailroot\Badmail. You will see three files with the file extensions .BAD, .BDP and .BDR. These entries represent components of the blocked e-mail message. You can view them using the Notepad application.
13. Navigate to the C:\Program Files\Microsoft ISA Server\ISALogs folder. Double click on the ISALOG_Date_EML_xxx.iis file. Open the file with the Notepad application. There you will see entries in the log regarding how the SMTP Message Screener processed the connection.
14. You can repeat the above steps on the CLIENT on the Internal network. In the e-mail message, include the word resume in the subject or body of the message. You will find that message is blocked and logged by the SMTP message screener. You can also send e-mail messages without the blocked words, and the outbound SMTP relay will forward the mail to the external e-mail user.
Conclusion

In this ISA Server 2004 Configuration Guide document, we discussed how to make the ISA Server 2004 firewall your front line protection as an e-mail defense in-depth plan. The ISA Server 2004 SMTP Message Screener can provide initial inspection and protection against dangerous and inappropriate e-mail messages. The Message Screener can perform initial evaluation of SMTP messages while also providing secure SMTP relay servers that protect the mail server on the Internal network from direct connections from untrusted servers. In the next chapter of this ISA Server 2004 Configuration Guide series, we will discuss how the firewall can be used to publish an array of Exchange Server services.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

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

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

© 2004 Microsoft Corporation. All rights reserved.

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, place, or event is intended or should be inferred.


The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

One of the main reasons to deploy a ISA Server 2004 firewall is to protect Microsoft Exchange Servers. ISA Server 2004 includes a number of technologies focused on providing enhanced support to protect Microsoft Exchange Services published to the Internet. This increased level of protection for remote access to Microsoft Exchange Server services puts the ISA Server 2004 firewall in a unique position to be the firewall for Microsoft Exchange Server.

Providing secure remote access to Microsoft Exchange Server services is a complex process. Fortunately, ISA Server 2004 includes a number of wizards that walk the firewall administrator through the process of providing secure remote to Microsoft Exchange, simplifying the procedure.

In this ISA Server 2004 Configuration Guide document, we discuss methods you can use to provide secure remote access to the Exchange Outlook Web Access (OWA) site, the Exchange SMTP service and the Exchange POP3 service. We will assume that you have issued a Web site certificate to the OWA site, exported the certificate to a file (including the private key), and imported the Web site certificate to the ISA Server 2004 firewall's machine certificate store. In addition, we will assume that the external client that connects to the OWA Web site through the ISA Server 2004 firewall has the CA certificate of the CA that issued the OWA site’s Web site certificate imported into its Trusted Root Certification Authorities certificate store.

Note: Certificate issuance and deployment is beyond the scope of this ISA Server 2004 Configuration Guide document. For detailed information on deploying Web site and root CA certificates, please refer to the ISA Server 2004 Exchange Deployment Kit.

The following walkthrough discusses basic methods used to provide remote access to the OWA, SMTP and POP3 services on the Internal network Exchange Server. In a production environment, remote access to the SMTP service would be secured using SSL and requiring use authentication. Similarly, remote access to the POP3 service would also require a secure SSL connection. We limit our discussion to non-SSL connections in the following walkthrough, for demonstration purposes only.

In addition, a number of procedures have been effected on the Exchange Server to optimize it for secure remote access OWA connections. The first chapter of this ISA Server 2004 Configuration Guide outlines these procedures. Also, the Exchange POP3 service is disabled by default and must be manually enabled.

You will need to perform the following procedures to configure the ISA Server 2004 firewall to allow remote access connections to the Exchange Server service:

- Restore the system to its post-installation state
- Create the OWA Web Publishing Rule
- Create the SMTP Server Publishing Rule
- Create the POP3 Server Publishing Rule
- Test the connection
Restore the System to its Post-installation State

In order to fully test the inbound and outbound SMTP relay configuration in this scenario, we will return the machine to its post-installation state so that other Access Rules do not interfere with the scenario development. In a production environment, you would leave your current Access Rules intact and add the Server Publishing Rules required to create the inbound and outbound SMTP relays.

Perform the following steps to restore the ISA Server 2004 firewall machine to its post-installation state:

8. Open the Microsoft Internet Security and Acceleration Server 2004 management console and right click on the server name. Click the Restore command.

9. In the Restore Configuration dialog box, select the backup file you created earlier and click Restore.

10. In the Type Password to Open File dialog box, enter the password you assigned to the file in the Password text box and click OK.

11. Click OK in the Importing dialog box after you see the message The configuration was successfully restored.

12. Click Apply to save the changes and update the firewall policy.

13. Select Save the changes and restart the service(s) in the ISA Server Warning dialog box, and click OK.

14. Click OK in the Apply New Configuration dialog box.
Create the OWA Web Publishing Rule

You can publish the Microsoft Exchange Outlook Web Access site using ISA Server 2004 Web Publishing after the site is configured to support secure SSL connections. These procedures include forcing SSL on the OWA directories and allowing the directories to accept only basic authentication.

Perform the following steps to create the Outlook Web Access Web Publishing Rule:

1. In the Microsoft Internet Security and Acceleration Server 2004 management console, expand the server name and click the Firewall Policy node.

2. Right click the Firewall Policy node, point to New and click Mail Server Publishing Rule.

3. On the Welcome to the New Mail Server Publishing Rule Wizard page, enter a name for the rule in the Mail Server Publishing Rule name text box. In this example we will call it OWA Web Site. Click Next.

4. On the Select Access Type page, select Web client access (Outlook Web Access (OWA), Outlook Mobile Access, Exchange Server ActiveSync and click Next.

5. On the Select Services page, put a checkmark in the Outlook Web Access check box. Confirm that there is a checkmark in the Enable high bit characters used by non-English character sets. Click Next.
6. On the Bridging Mode page, select Secure connection to clients and mail server and click Next.
7. On the **Specify the Web Mail Server** page, enter the name for the Internal OWA Web site in the **Web mail server** text box. In this example, we will use the name `owa.msfirewall.org`. Click **Next**.
8. On the **Public Name Details** page, select **This domain name (type below)** in the **Accept requests for** list. Enter the name external users will use to access the OWA Web site in the **Public name** text box. In this example, the external users will use the name **owa.msfirewall.org**. Click **Next**.
9. On the **Select Web Listener** page, click **New**.

10. On the **Welcome to the New Web Listener Wizard** page, enter a name for the listener in the **Web listener name** text box. In this example, we will use the name **OWA SSL Listener**. Click **Next**.

11. On the **IP Addresses** page, put a checkmark in the **External** check box. Click the **Address** button.

12. In the **External Network Listener IP Selection** dialog box, select **Specified IP addresses on the ISA Server computer in the select network**. Click on the external IP address configured on the ISA Server 2004 firewall that you want to listen for incoming requests to the OWA site in the **Available IP Addresses** list. In this example, we will select the **192.168.1.70** entry. Click **Add**. The IP address now appears in the **Selected IP Addresses** list. Click **OK**.

13. Click **Next** on the **IP Addresses** page.

14. On the **Port Specification** page, remove the checkmark from the **Enable HTTP** check box. Place a checkmark in the **Enable SSL** checkbox. Leave the **SSL port** number at **443**.

15. Click the **Select** button. In the **Select Certificate** dialog box, click on the OWA Web site certificate that you imported into the ISA Server 2004 firewall’s machine certificate store and click **OK**.

16. Click **Next** on the **Port Specification** page.

17. Click **Finish** on the **Completing the New Web Listener** page.

18. The details of the Web listener now appear on the **Select Web Listener** page. Click **Edit**.
19. In the **OWA SSL Listener Properties** dialog box, click the **Preferences** tab.

20. On the **Preferences** tab, click the **Authentication** button.

21. In the **Authentication** dialog box, remove the checkmark from the **Integrated** check box. Click **OK** in the **Microsoft Internet Security and Acceleration Server 2004** dialog box warning that the no authentication methods are currently configured.

22. Place a checkmark in the **OWA Forms-Based** authentication checkbox. Click **OK**.
23. Click **Apply** and then click **OK** in the **OWA SSL Listener Properties** dialog box.

24. Click **Next** on the **Select Web Listener** page.
25. On the **User Sets** page, accept the default entry, **All Users**, and click **Next**.

26. Click **Finish** on the **Completing the New Mail Server Publishing Rule Wizard** page.

27. Click **Apply** to save the changes and update the firewall policy.

28. Click **OK** in the **Apply New Configuration** dialog box.

The next step is to create a HOSTS file entry on the ISA Server 2004 firewall machine so that it resolves the name **owa.msfirewall.org** to the IP address of the Exchange Server on the Internal network.

4. Click **Start** and **Run**. In the **Run** dialog box, enter **notepad** in the **Open** text box and click **OK**.

5. Click the **File** menu and then click **Open**. In the **Open** dialog box, enter **c:\windows\system32\drivers\etc\hosts** in the **File name** text box and click **Open**.
6. Add the following line to the HOSTS file:

```
10.0.0.2 owa.msfirewall.org
```

Press ENTER at the end of the line so that the insertion point sits on the next line. Click **File** and **Exit**. In the **Notepad** dialog box, click **Yes** to indicate that you wish to save the changes.
# Copyright (c) 1993-1999 Microsoft Corp.
#
# 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
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:
#
#    102.54.94.97   rhino.acme.com   # source server
#    38.23.63.10   x.acme.com       # x client host
127.0.0.1       localhost
10.0.0.2         owa.msfirewall.org
Create the SMTP Server Publishing Rule

You can create an SMTP Server Publishing Rule to provide external users and servers access to the Microsoft Exchange SMTP service. In general, you will prefer to use the ISA Server 2004 firewall as a secure SMTP filtering relay to prevent external users and servers from directly connecting to the Exchange Server. The Server Publishing Rule discussed in the following walkthrough is best used to provide external SMTP servers access to the Exchange Server so they can send mail to e-mail under your administrative control.

Perform the following steps to create the SMTP Server Publishing Rule:

10. Open the Microsoft Internet Security and Acceleration Server 2004 management console, and expand the server name in the left pane of the console. Click on the Firewall Policy node.

11. Right click the Firewall Policy node and point to New. Click Server Publishing Rule.

12. On the Welcome to the New Server Publishing Rule Wizard page, enter the name for the rule in the Server publishing rule name text box. In this example, we will name the rule SMTP Server. Click Next.

13. On the Select Server page, enter the IP address of the Exchange Server on the Internal network. In our current example, the IP address is 10.0.0.2. Enter 10.0.0.2 into the text box. Click Next.


15. On the IP Addresses page, put a checkmark in the External check box and click the Address button.
16. In the **External Network Listener IP Selection** dialog box, select **Specified IP addresses on the ISA Server computer in the selected network**. Click the IP address on the external interface you want to use in the rule. In this example, the IP address is **192.168.1.70**. Click **Add**. The IP address now appears in the **Selected IP Addresses** list. Click **OK**.

![External Network Listener IP Selection dialog box](image)

17. Click **Next** on the **IP Addresses** page.

18. Click **Finish** on the **Completing the New Server Publishing Rule Wizard** page.
Create the POP3 Server Publishing Rule

Remote access to the Exchange Server POP3 service allows users located away from the office to download their mail from the Exchange Server to virtually any e-mail client application. Users must provide a user name and password when they connect to the POP3 service. They download e-mail into their e-mail client application after sending their credentials. These user credentials are sent in clear text. In a production environment, you would require an SSL-secured POP3 connection so that user name and password are not easily accessible to Internet intruders.

Perform the following steps to create the POP3 Server Publishing Rule:

1. Open the Microsoft Internet Security and Acceleration Server 2004 management console, and expand the server name in the left pane of the console. Click on the Firewall Policy node.

2. Right click the Firewall Policy node and point to New. Click Server Publishing Rule.

3. On the Welcome to the New Server Publishing Rule Wizard page, enter the name for the rule in the Server publishing rule name text box. In this example, we will name the rule POP3 Server. Click Next.

4. On the Select Server page, enter the IP address of the Exchange Server on the Internal network. In our current example, the IP address is 10.0.0.2. Enter 10.0.0.2 into the text box. Click Next.

5. On the Select Protocol page, select the POP3 Server protocol from the Selected protocol list. Click Next.

6. On the IP Addresses page, put a checkmark in the External check box and click the Address button.

7. In the External Network Listener IP Selection dialog box, select Specified IP addresses on the ISA Server computer in the selected network. Click the IP address on the external interface you want to use in the rule. In this example, the IP address is 192.168.1.70, then click Add. The IP address now appears in the Selected IP Addresses list. Click OK.
8. Click Next on the IP Addresses page.

Test the connection

We are now ready to test the OWA, SMTP and POP3 connections to the Exchange Server located behind the ISA Server 2004 firewall. The first step is to create a HOSTS file entry on the client so that it correct resolves the name of the OWA site. In a production environment, you would create a public DNS resource record that correctly resolves this name for external network clients.

Perform the following steps to test the Outlook Web Access connection:

1. The first step is to add a HOSTS file entry on the external client machine. Click Start and Run. In the Run dialog box, enter notepad in the Open text box and click OK.

2. Click the File menu and Open. In the Open dialog box, enter c:\windows\system32\drivers\etc\hosts in the File name text box and click Open.

3. Add the following line to the HOSTS file:

   192.168.1.70   owa.msfirewall.org

   Press ENTER at the end of the line so that the insertion point sits on the next line. Click File and Exit. In the Notepad dialog box, click Yes to indicate that you wish to save the changes.

4. Open Internet Explorer on the external client machine. Enter https://owa.msfirewall.org into the Address bar and press ENTER.
5. In the Outlook Web Access Log on form, enter the user name in the Domain\user name text box, and the password in the Password text box. Select the Premium client type and the Private computer Security type. In the current example, we will enter the user name MSFIREWALL\Administrator and the Administrator’s password. Click Log On.

Next, we will test the POP3 and SMTP functionality using Outlook Express:

1. On the external client machine, open Outlook Express. Click Tools and Accounts.

2. In the Internet Accounts dialog box, click the existing account and Remove. Click Yes in the Internet Accounts dialog box asking if you are sure you want to delete the account.

3. Click Add and then click Mail.

4. On the Your Name page, enter the name Administrator in the Display name text box. Click Next.

5. On the Internet E-mail Address page, enter the address administrator@msfirewall.org in the E-mail address text box. Click Next.

6. On the E-mail Server Names page, select the POP3 entry in the My incoming mail server is a x server list. Enter 192.168.1.70 in the Incoming mail (POP3, IMAP or HTTP) server text box. Enter 192.168.1.70 in the Outgoing mail (SMTP) server text box. Click Next.
7. On the Internet Mail Logon page, enter Administrator in the Account name text box and the administrator’s password in the Password text box. Click Next.

8. Click Finish on the Congratulations! page.

9. Click Close on the Internet Accounts dialog box.

10. Close Outlook Express and then open it again. Click the Create Mail button and address a message to administrator@msfirewall.org. Enter a subject and text and click the Send button. To receive the mail from the POP3 server, click Send/Recv. The message you send appears in the Inbox.

11. Close Outlook Express.
Conclusion

In this ISA Server 2004 Configuration Guide document, we discussed how to publish a Microsoft Exchange Outlook Web Access (OWA) site and how to publish the Exchange POP3 and SMTP services. In the next document in this ISA Server 2004 Configuration Guide series, we will discuss how the firewall can be used to publish an array of Exchange Server services.
ISA Server 2004 Configuration Guide: Configuring the ISA Server 2004 Firewall as a VPN Server
Chapter 15

For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

The ISA Server 2004 firewall can be configured as a VPN server. The VPN server component enables it to accept incoming VPN client calls so that the VPN client computer can become a member of a protected network. Traditional VPN servers allow VPN clients full access to the networks to which they connect. In contrast, the ISA Server 2004 VPN server allows you to control what protocols and servers VPN clients can connect to, based on the credentials used when connecting to the VPN server.

You can use the Microsoft Internet Security and Acceleration Server 2004 management console to manage virtually all aspects of the VPN server configuration. The firewall manages the list of IP addresses assigned to VPN clients and places those addresses on a dedicated VPN clients network. Access controls can then be placed on communications moving to and from the VPN clients network using Access Rules.

In the following walkthrough, perform the following tasks to enable the ISA Server 2004 VPN server to:

- Enable the VPN Server
- Create an Access Rule allowing VPN clients access to the Internal network
- Test the VPN Connection
Enable the VPN Server

By default, the VPN server component is disabled. The first step is to enable the VPN server feature and configure the VPN server components.

Perform the following steps to enable and configure the ISA Server 2004 VPN Server:

1. Open the Microsoft Internet Security and Acceleration Server 2004 management console and expand the server name. Click on the Virtual Private Networks (VPN) node.

2. Click on the Tasks tab in the Task Pane. Click Enable VPN Client Access.

3. Click Apply to save the changes and update the firewall policy.

4. Click OK in the Apply New Configuration dialog box.

5. Click Configure VPN Client Access.

6. On the General tab, change the value for the Maximum number of VPN clients allowed from 5 to 10.
7. Click on the **Groups** tab. On the **Groups** tab, click the **Add** button.

8. In the **Select Groups** dialog box, click the **Locations** button. In the **Locations** dialog box, click the `msfirewall.org` entry and click **OK**.

9. In the **Select Group** dialog box, enter **Domain Users** in the **Enter the object names to select** text box. Click the **Check Names** button. The group name will be underlined when it is found in the Active Directory. Click **OK**.
10. Click the **Protocols** tab. On the **Protocols** tab, put a checkmark in the **Enable L2TP/IPSec** check box.
11. Click the **User Mapping** tab. Put a checkmark in the **Enable User Mapping** check box. Put a checkmark in the **When username does not contain a domain, use this domain** check box. Enter *msfirewall.org* in the **Domain Name** text box.
12. Click **Apply** in the **VPN Clients Properties** dialog box. Click **OK** in the **Microsoft Internet Security and Acceleration Server 2004** dialog box that informs that you must restart the ISA Server firewall before the settings take effect. Click **OK**.

13. Click **Apply** to save the changes and update the firewall policy.

14. Click **OK** in the **Apply New Configuration** dialog box.

15. Restart the ISA Server 2004 firewall machine.
Create an Access Rule Allowing VPN Clients Access to the Internal Network

At this point, VPN clients can connect to the VPN server. However, the VPN clients cannot access any resources on the Internal network. You must first create an Access Rule that allows members of the VPN clients network access to the Internal network. In this example, you will create an Access Rule that allows all traffic to pass from the VPN clients network to the Internal network. In a production environment, you would create more restrictive access rules so that users on the VPN clients network have access only to resources they require.

Perform the following steps to create the VPN clients Access Rule:

1. In the Microsoft Internet Security and Acceleration Server 2004 management console, expand the server name and click the Firewall Policy node. Right click the Firewall Policy node, point to New and click Access Rule.

2. In the Welcome to the New Access Rule Wizard page, enter a name for the rule in the Access Rule name text box. In this example, we will name the rule VPN Client to Internal. Click Next.

3. On the Rule Action page, select Allow and click Next.

4. On the Protocols page, select All outbound protocols from the This rule applies to list. Click Next.

5. On the Access Rule Sources page, click Add. In the Add Network Entities dialog box, click the Networks folder and double click on VPN Clients. Click Close.
6. Click **Next** on the **Access Rule Sources** page.

7. On the **Access Rule Destinations** page, click **Add**. On the **Add Network Entities** dialog box, click the **Networks** folder and double click on **Internal**. Click **Close**.

8. On the **User Sets** page, accept the default setting, **All Users**, and click **Next**.

9. Click **Finish** on the **Completing the New Access Rule Wizard** page.

10. Click **Apply** to save the changes and update the firewall policy.

11. Click **OK** in the **Apply New Configuration** dialog box.
Enable Dial-in Access for the Administrator Account

In non-native mode Active Directory domains, all user accounts have dial-in access disabled by default. In this circumstance, you must enable dial-in access on a per account basis. In contrast, Active Directory domains in native mode have dial-in access set to be controlled by Remote Access Policy. Windows NT 4.0 dial-in access is always controlled on a per user account basis.

In our current example, the Active Directory is in Windows Server 2003 mixed mode, so we will need to manually change the dial-in settings on the user account.

Perform the following steps on the domain controller to enable Dial-in access for the Administrator account:

1. Click **Start** and point to **Administrative Tools**. Click **Active Directory Users and Computers**.

2. In the **Active Directory Users and Computers** console, click on the **Users** node in the left pane. Double click on the **Administrator** account in the right pane of the console.

3. Click on the **Dial-in** tab. In the **Remote Access Permission (Dial-in or VPN)** frame, select **Allow access**. Click **Apply** and click **OK**.

4. Close the **Active Directory Users and Computers** console.
**Test the VPN Connection**

The ISA Server 2004 VPN server is now ready to accept VPN client connections. Perform the following steps to test the VPN Server:

2. Double click the Make New Connection icon in the Network and Dial-up Connections window.
3. Click Next on the Welcome to the Network Connection Wizard page.
4. On the Network Connection Type page, select the Connect to a private network through the Internet option and click Next.
5. On the Destination Address page, enter the IP address 192.168.1.70 in the Host name or IP address text box. Click Next.
6. On the Connection Availability page, select the For all users option and click Next.
7. Make no changes on the Internet Connection Sharing page and click Next.
8. On the Completing the Network Connection Wizard page, enter a name for the VPN connection in the Type the name you want to use for this connection text box. In this example, we’ll name the connection ISA VPN. Click Finish.
9. In the Connect ISA VPN dialog box, enter the user name MSFIREWALL\administrator and the password for the administrator user account. Click Connect.

10. The VPN client establishes a connection with the ISA Server 2004 VPN server. Click OK in the Connection Complete dialog box informing that the connection is established.
11. Double click the Connection icon in the system tray and click the Details tab. You can see that MPPE 128 encryption is used to protect the data and IP address assigned to the VPN client.
12. Click **Start** and the **Run** command. In the **Run** dialog box, enter `\EXCHANGE2003BE` in the **Open** text box, and click **OK**. The shares on the domain controller computer appear.

13. Right click the **Connection** icon in the system tray and click **Disconnect**.
Conclusion

In this ISA Server 2004 Configuration Guide document, we discussed how to enable the ISA Server 2004 VPN server component and how to configure the VPN server. We tested the VPN server functionality by creating a VPN client connection to the server and accessing resources on the Internal network. In the next chapter in this ISA Server 2004 Configuration Guide series, we will discuss how the firewall is used to publish an array of Exchange Server services.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

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

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

© 2004 Microsoft Corporation. All rights reserved.

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, place, or event is intended or should be inferred.


The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
ISA Server 2004 Configuration Guide: Creating a Site-to-Site VPN with ISA Server 2004 Firewalls
Chapter 16

For the latest information, please see http://www.microsoft.com/isaserver/
Introduction

A site-to-site VPN connection connects two or more networks using a VPN link over the Internet. The VPN site-to-site configuration works just like a LAN router; packets destined for IP addresses at a remote site are routed through the ISA Server 2004 machine. The ISA Server 2004 firewall machine acts as a VPN gateway that joins two networks over the Internet.

Each site-to-site link can use one of the following VPN protocols:

- PPTP
- L2TP/IPSec
- IPSec tunnel mode

PPTP is the Point-to-Point Tunneling Protocol. PPTP provides a good level of security, depending on the complexity of the password used to create the PPTP connection. You can enhance the level of security applied to a PPTP link by using EAP/TLS based-authentication methods.

The L2TP/IPSec VPN protocol provides a higher level of security because it uses the IPSec encryption protocol to secure the connection. You can use computer and user certificates to provide an even higher level of security to the L2TP/IPSec connection. If you are not ready to deploy a certificate infrastructure, you can use a pre-shared key to create the site-to-site L2TP/IPSec VPN connection.

ISA Server 2004 supports IPSec tunnel mode for site-to-site VPN connections. You should only use IPSec tunnel mode when you need to create a site-to-site link with third-party VPN gateways. Third-party IPSec tunnel mode gateways do not support the high level of security provided by L2TP/IPSec, so they must use a weaker VPN protocol. IPSec tunnel mode site-to-site links are useful in branch office scenarios where the main office is still in the process of replacing their current VPN gateways with ISA Server 2004 firewall VPN gateways.

In this ISA Server 2004 Configuration Guide chapter, we will go through the procedures required to create a site-to-site link between two ISA Server 2004 firewall machines. The ISALocal machine will simulate the main office firewall, and the REMOTEISA will simulate the branch office firewall. We will use the L2TP/IPSec VPN protocol to create the site-to-site link, and a pre-shared key will be used to support the IPSec encryption protocol.

You will complete the following procedures to create the site to site VPN connection:

- Create the Remote Site at the Main Office
- Create the Network Rule at the Main Office
- Create the Access Rules at the Main Office
- Create the VPN Gateway Dial-in Account at the Main Office
- Set the Shared Password in the RRAS Console at the Main Office
- Create the Remote Network at the Branch Office
- Create the Network Rule at the Branch Office
- Create the Access Rules at the Branch Office
- Create the VPN Gateway Dial-in Account at the Main Office
- Set the Shared Password in the RRAS Console at the Branch Office
- Activate the Site-to-Site Links
Create the Remote Site at the Main Office

We will begin by configuring the ISA Server 2004 firewall at the main office. First, create the Remote Site Network in the Microsoft Internet Security and Acceleration Server 2004 management console.

Perform the following steps to create the Remote Site Network at the main office ISA Server 2004 firewall machine:

1. Open the Microsoft Internet Security and Acceleration Server 2004 management console and expand the server name. Click on the Virtual Private Networks (VPN) node.

2. Click on the Remote Sites tab in the Details Pane. Click on the Tasks tab in the Task Pane. Click Add Remote Site Network.

3. On the Welcome to the New Network Wizard page, enter a name for the remote network in the Network name text box. In this example, name the remote network Branch. Click Next.

4. On the VPN Protocol page, select Layer Two Tunneling Protocol (L2TP) over IPSec, and click Next.
5. On the **Remote Site Gateway** page, enter the IP address of the external interface of the remote ISA Server 2004 firewall machine. In this example, the IP address is **192.168.1.71**, so we will enter this value into the text box. Click **Next**.

6. On the **Remote Authentication** page, put a checkmark in the **Local site can initiate connections to remote site using these credentials** check box. Enter the name of the account that you will create on the remote ISA Server 2004 firewall computer to allow the main office VPN gateway access. In this example, in the **User name** text box, name the user account **Main** (the user account much match the name of the demand-dial interface created on the remote site). The **Domain** name is the name of the remote ISA Server 2004 firewall computer, which in this example is **REMOTEISA** (if the remote ISA Server 2004 firewall were a domain controller, you would use the domain name instead of the computer name). Enter a password for the account and confirm the password. Write down this password so that you will remember it when you create the account later on the remote ISA Server 2004 firewall. Click **Next**.
7. Read the information on the Local Authentication page, and click Next.

8. On the L2TP/IPSec Authentication page, put a checkmark in the Allow pre-shared key IPSec authentication as a secondary (backup) authentication method check box. Enter a key in the Use pre-shared key for authentication text box. In this example, use the key 123. Click Next.
9. Click Add on the Network Addresses page. In the IP Address Range Properties dialog box, enter 10.0.1.0 in the Starting address text box. Enter 10.0.1.255 in the Ending address text box. Click OK.
10. Click **Next** on the **Network Addresses** page.
11. Click **Finish** on the **Completing the New Network Wizard** page.
Create the Network Rule at the Main Office

The ISA Server 2004 firewall must know what method to use to route packets to the branch office network. There are two options: Route and NAT. A route relationship routes packets to the branch office and preserves the source IP address of the clients who make a connection over the site-to-site link. A NAT relationship replaces the source IP address of the client making the connection. In general, the route relationship provides a higher level of protocol support, but the NAT relationship provides a higher level of security.

Perform the following steps to create a Network Rule that controls the routing relationship between the main office and branch office networks:

1. Expand the Configuration node in the left Pane of the console. Click on the Networks node.
2. Click on the Network Rules tab in the Details Pane. Click on the Tasks tab in the Task Pane. Click Create a New Network Rule.
3. On the Welcome to the New Network Rule Wizard page, enter a name for the rule in the Network rule name text box. In this example, we call the rule MainBranch. Click Next.
5. In the Add Network Entities dialog box, click the Networks folder. Double click on the Internal network. Click Close.
6. Click Next on the Network Traffic Sources page.
7. On the Network Traffic Destinations page, click Add.
8. In the Add Network Entities dialog box, double click on the Branch network. Click Close.
9. Click Next on the Network Traffic Destinations page.
10. On the Network Relationship page, select Route.
11. Click **Finish** on the **Completing the New Network Rule Wizard** page.
Create the Access Rules at the Main Office

In this example, we want the clients on both the main and branch office networks to have full access to all resources on each network. We must create Access Rules to allow traffic from the main office to the branch office and from the branch office to the main office.

Perform the following steps to create Access Rules that allow traffic to move between the main and branch offices:

1. Click the Firewall Policy node in the left Pane of the console. Click the Tasks tab in the Task Pane. Click Create New Access Rule.

2. On the Welcome to the New Access Rule Wizard page, enter a name for the rule in the Access Rule name text box. In this example, enter Main to Branch. Click Next.

3. On the Rule Action page, select Allow and click Next.

4. On the Protocols page, select All outbound protocols in the This rule applies to list. Click Next.

5. On the Access Rule Sources page, click Add.

6. In the Add Network Entities dialog box, click the Networks folder and double click the Internal network. Click Close.

7. Click Next on the Access Rule Sources page.


9. In the Add Network Entities dialog box, click on the Networks folder and then double click on the Branch network. Click Close.

10. Click Next on the Access Rule Destinations page.
11. On the **User Sets** page, accept the default entry **All Users** and click **Next**.
12. Click **Finish** on the **Completing the New Access Rule Wizard** page.

The second rule will allow the hosts on the branch office network access to the main office network:

1. Click the **Tasks** tab in the Task pane. Click **Create New Access Rule**.
2. On the **Welcome to the New Access Rule Wizard** page, enter a name for the rule in the **Access Rule name** text box. In this example, enter **Branch to Main**. Click **Next**.
3. On the **Rule Action** page, select **Allow** and click **Next**.
4. On the **Protocols** page, select **All outbound protocols** in the **This rule applies to** list. Click **Next**.
5. On the **Access Rule Sources** page, click **Add**.
6. In the **Add Network Entities** dialog box, click the **Networks** folder and double click the **Branch** network. Click **Close**.
7. Click **Next** on the **Access Rule Sources** page.
8. On the **Access Rule Destinations** page, click **Add**.
9. In the **Add Network Entities** dialog box, click on the **Networks** folder and then double click on the **Internal** network. Click **Close**.
10. Click **Next** on the **Access Rule Destinations** page.
11. On the **User Sets** page, accept the default entry **All Users** and click **Next**.
12. Click **Finish** on the **Completing the New Access Rule Wizard** page.
Finally, to enable access for VPN clients:

1. Click on the **Virtual Private Network** node in the left Pane of the console.
2. Click the **VPN Clients** tab in the Details Pane. Click the **Tasks** tab in the Task Pane. Click **Enable VPN Client Access**.

3. Click **OK** in the **ISA Server 2004** dialog box informing you that the Routing and Remote Access service must be restarted.
4. Click **Apply** to save the changes and update the firewall policy.
5. Click **OK** in the **Apply New Configuration** dialog box.
Create the VPN Gateway Dial-in Account at the Main Office

A user account must be created on the main office firewall that the branch office firewall can authenticate when it creates the site-to-site connection. This user account must have the same name as the demand-dial interface on the main office computer. You will later configure the branch office ISA Server 2004 to use this account when it dials the VPN site-to-site link.

To create the account the remote ISA Server 2004 firewall will use to connect to the main office VPN gateway:

1. Right click My Computer on the desktop and click Manage.
2. In the Computer Management console, expand the Local Users and Groups node. Right click the Users node and click New User.
3. In the New User dialog box, enter the name of the main office demand-dial interface. In our current example, the demand-dial interface is Branch. Enter Branch into the text box. Enter a Password and confirm the Password. Make a record of the password because you’ll need to use it when you configure the remote ISA Server 2004 VPN gateway machine. Remove the checkmark from the User must change password at next logon check box. Place checkmarks in the User cannot change password and Password never expires check boxes. Click Create.
4. Click Close in the New User dialog box.
5. Double click the Branch user in the right Pane of the console.
6. In the Branch Properties dialog box, click the Dial-in tab. Select Allow access. Click Apply and then click OK.
Set the Shared Password in the RRAS Console at the Main Office

The pre-shared key you entered into the Microsoft Internet Security and Acceleration Server 2004 management console is not automatically copied to the Routing and Remote Access service. You must configure the Routing and Remote Access service to use the pre-shared key you configured when creating the Remote Site Network.

To configure the L2TP/IPSec pre-shared key:

1. Click **Start** and point to **Administrative Tools**. Click **Routing and Remote Access**.
2. In the **Routing and Remote Access** console, right click on the server name. Click **Properties**.
3. In the server **Properties** dialog box, click the **Security** tab. On the **Security** tab, put a checkmark in the **Allow custom IPSec policy for L2TP connection** check box. In the **Pre-shared Key** text box, enter 123. Click **Apply** and **OK**.
5. Restart the main office ISA Server 2004 firewall machine.
Create the Remote Site at the Branch Office

Now that the main office is ready, we can configure the branch office ISA Server 2004 firewall. First, create the Remote Site Network at the branch office:

Perform the following steps to create the Remote Site Network at the branch office:

1. Open the Microsoft Internet Security and Acceleration Server 2004 management console and expand the server name. Click on the Virtual Private Networks (VPN) node.

2. Click on the Remote Sites tab in the Details Pane. Click on the Tasks tab in the Task Pane. Click Add Remote Site Network.

3. On the Welcome to the New Network Wizard page, enter a name for the remote network in the Network name text box. In this example, we will name the remote network Main. Click Next.

4. On the VPN Protocol page, select Layer Two Tunneling Protocol (L2TP) over IPSec and click Next.

5. On the Remote Site Gateway page, enter the IP address on the external interface of the remote ISA Server 2004 firewall machine. In this example, the IP address is 192.168.1.70, so enter this value into the text box. Click Next.

6. On the Remote Authentication page, put a checkmark in the Local site can initiate connections to remote site using these credentials check box. Enter the name of the account you will create on the remote ISA Server 2004 firewall computer to allow the main office VPN gateway access. In this example, the user account will be Branch (the user account much match the name of the demand-dial interface created on the remote site). The Domain name is the name of the remote ISA Server 2004 firewall computer, which in this example is ISALOCAL (if the remote ISA Server 2004 firewall were a domain controller, then you would use the domain name instead of the computer name). Enter a Password for the account and confirm the Password. Note the password so you will remember it when you create the account later on the remote ISA Server 2004 firewall. Click Next.

7. Read the information on the Local Authentication page, and click Next.

8. On the L2TP/IPSec Authentication page, put a checkmark in the Allow pre-shared key IPSec authentication as a secondary (backup) authentication method check box. Enter a key in the Use pre-shared key for authentication text box. In this example, enter 123. Click Next.

9. Click Add on the Network Addresses page. In the IP Address Range Properties dialog box, enter 10.0.0.0 in the Starting address text box. Enter 10.0.0.255 in the Ending address text box. Click OK.

10. Click Next on the Network Addresses page.

11. Click Finish on the Completing the New Network Wizard page.
### Remote Sites

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Protocol</th>
<th>Remote Server</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main</td>
<td>This network represents a remote VPN site-to-site connection using L2TP. L2TP</td>
<td>L2TP</td>
<td>192.168.1.70</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

To save changes and update firewall policy, click Apply.
Create the Network Rule at the Branch Office

Just as we did at the main office, we must create a routing relationship between the branch office and the main office networks. We will configure a route relationship so that we can get the highest level of protocol support.

Perform the following steps to create the Network Rule at the branch office:

1. Expand the Configuration node in the left Pane of the console. Click on the Networks node.
2. Click on the Network Rules tab in the Details Pane. Click on the Tasks tab in the Task Pane. Click Create a New Network Rule.
3. On the Welcome to the New Network Rule Wizard page, enter a name for the rule in the Network rule name text box. In this example, enter BranchMain. Click Next.
5. In the Add Network Entities dialog box, click the Networks folder. Double click on the Internal network. Click Close.
6. Click Next on the Network Traffic Sources page.
7. On the Network Traffic Destinations page, click Add.
8. In the Add Network Entities dialog box, double click on the Main network. Click Close.
9. Click Next on the Network Traffic Destinations page.
10. On the Network Relationship page, select Route.
11. Click Finish on the Completing the New Network Rule Wizard page.
Create the Access Rules at the Branch Office

We need to create two Access Rules, one that allows traffic from the branch office to the main office, and the second to allow traffic from the main office to the branch office.

To create Access Rules that allow traffic to move between the branch and main offices:

1. Click the Firewall Policy node in the left Pane of the console. Click the Tasks tab in the Task Pane. Click Create New Access Rule.

2. On the Welcome to the New Access Rule Wizard page, enter a name for the rule in the Access Rule name text box. In this example, enter Branch to Main. Click Next.

3. On the Rule Action page, select Allow and click Next.

4. On the Protocols page, select All outbound protocols in the This rule applies to list. Click Next.

5. On the Access Rule Sources page, click Add.

6. In the Add Network Entities dialog box, click the Networks folder and double click the Internal network. Click Close.

7. Click Next on the Access Rule Sources page.


9. In the Add Network Entities dialog box, click on the Networks folder and then double click on the Main network. Click Close.

10. Click Next on the Access Rule Destinations page.

11. On the User Sets page, accept the default entry All Users and click Next.


The second rule will allow the hosts on the main office network access to the branch office network:

1. Click the Tasks tab in the Task Pane. Click Create New Access Rule.

2. On the Welcome to the New Access Rule Wizard page, enter a name for the rule in the Access Rule name text box. In this example, enter Main to Branch. Click Next.

3. On the Rule Action page, select Allow and click Next.

4. On the Protocols page, select All outbound protocols in the This rule applies to list. Click Next.

5. On the Access Rule Sources page, click Add.

6. In the Add Network Entities dialog box, click the Networks folder and double click the Main network. Click Close.

7. Click Next on the Access Rule Sources page.


9. In the Add Network Entities dialog box, click on the Networks folder and double click on the Internal network. Click Close.

10. Click Next on the Access Rule Destinations page.

11. On the User Sets page, accept the default entry All Users and click Next.

The last step we need to take in the Microsoft Internet Security and Acceleration Server 2004 management console is to enable access for VPN clients:

1. Click on the Virtual Private Network node in the left Pane of the console.
2. Click the VPN Clients tab in the Details Pane. Click the Tasks tab in the Task Pane. Click on Enable VPN Client Access.
3. Click OK in the ISA Server 2004 dialog box informing you that the Routing and Remote Access service must be restarted.
4. Click Apply to save the changes and update the firewall policy.
5. Click OK in the Apply New Configuration dialog box.
Create the VPN Gateway Dial-in Account at the Main Office

We must create a user account that the main office VPN gateway can authenticate when it initiates the VPN site-to-site connection. The user account must have the same name as the demand-dial interface created on the branch office machine.

Perform the following steps to create the account the remote ISA Server 2004 firewall will use to connect to the main office VPN gateway:

1. Right click My Computer on the desktop and click Manage.
2. In the Computer Management console, expand the Local Users and Groups node. Right click the Users node and click New User.
3. In the New User dialog box, enter the name of the main office demand-dial interface. In our current example, the demand-dial interface is Main. Enter Main into the text box. Enter a Password and confirm the Password. Make a record of the password because you'll need to use it when you configure the remote ISA Server 2004 VPN gateway machine. Remove the checkmark from the User must change password at next logon check box. Place checkmarks in the User cannot change password and Password never expires check boxes. Click Create.
4. Click Close in the New User dialog box.
5. Double click Main user in the right Pane of the console.
6. In the Main Properties dialog box, click the Dial-in tab. Select Allow access. Click Apply and OK.
Set the Shared Password in the RRAS Console at the Branch Office

The pre-shared key configured in the Microsoft Internet Security and Acceleration Server 2004 management console is not automatically copied to the Routing and Remote Access service. You must manually configure the Routing and Remote Access service to use the pre-shared key configured in the Remote Site Network configuration.

Perform the following steps to configure the L2TP/IPSec pre-shared key:

1. Click Start and point to Administrative Tools. Click Routing and Remote Access.
2. In the Routing and Remote Access console, right click on the server name. Click Properties.
3. In the server Properties dialog box, click the Security tab. On the Security tab, put a checkmark in the Allow custom IPSec policy for L2TP connection check box. In the Pre-shared Key text box, enter 123. Click Apply and click OK.
5. Restart the branch office ISA Server 2004 firewall machine.
Activate the Site to Site Links

Now that both the main and branch office ISA Server 2004 firewalls are configured as VPN routers, you can test the site-to-site connection.

Perform the following steps to test the site-to-site link:

1. At the remote client computer behind the remote ISA Server 2004 firewall machine, click Start and the Run command.
2. In the Run dialog box, enter cmd in the Open text box, and click OK.
3. In the command prompt window, enter ping –t 10.0.0.2 and press ENTER.
4. You will see a few pings time out, and then the ping responses will be returned by the domain controller on the main office network.
5. Perform the same procedures at the domain controller at the main office network, but this time ping 10.0.1.2.
Conclusion

In this ISA Server 2004 Configuration Guide document we discussed how to use the ISA Server 2004 firewall as a VPN gateway that enables site-to-site VPN links. We configured two ISA Server 2004 firewalls, one at the main office and a second at the branch office. We tested the VPN site-to-site connectivity by pinging from clients on each side to the opposite site.