Installation and Deployment Guide
Microsoft Internet Security and Acceleration Server 2000,
Standard Edition

2002. december 14.

Contents

Preface: About this Guide

The Internet provides organizations with new opportunities to connect with customers, partners, and employees. While this presents great opportunities, it also introduces new risks and concerns such as security, performance, and manageability. Microsoft Internet Security and Acceleration (ISA) Server addresses the needs of today's Internet-enabled businesses. ISA Server provides a multilayered firewall that helps protect your network resources. The Web cache of ISA Server enables organizations to save network bandwidth and provide faster Web access for users by serving objects from a local source, rather than over a periodically congested Internet.

Whether it is deployed as dedicated components or as an integrated firewall and caching server, ISA Server provides a unified management console that simplifies security and access management. Built for the Windows 2000 platform, ISA Server provides secure and fast Internet connectivity with powerful integrated management tools.

ISA Server can provide value to information technology managers, network administrators and information-security professionals in organizations of all sizes, who are concerned about the security, performance, manageability or operating costs of their networks. ISA Server can be used in a spectrum of scenarios, ranging from small offices and branch offices, to Internet service providers (ISPs) and Web hosting companies, and to e-commerce sites.

Intended Audience

This guide is intended for systems professionals, network administrators, and small business power users who want to learn how to install and deploy ISA Server in their network. The guide assumes that you are familiar with basic networking concepts, including familiarity with DNS, DHCP, Routing and Remote Access, Transmission Control Protocol/Internet Protocol (TCP/IP) networking, and other Windows networking components.

Purpose of This Guide

This guide presents an overview of ISA Server and provides the background information you need to plan your implementation of this software.

The guide also includes detailed procedures on the installation process, checklists for post-installation configuration, and detailed sample scenarios of how ISA Server might be used in your network.

This guide is organized into the following chapters:

- Chapter 1, "Introduction," introduces ISA Server and describes its features.
- Chapter 2, "Planning Considerations," describes issues to consider before installing ISA Server. This will help you determine how many ISA Server computers to install and in what configuration.
- Chapter 3, "Installing ISA Server," guides you through the installation process. It details hardware configuration and the installation process.
- Chapter 4, "Migrating from Microsoft Proxy Server 2.0," explains how existing Proxy Server 2.0 policies and configurations can be migrated to an ISA Server configuration.
- Chapter 5, "Upgrading to ISA Server, Enterprise Edition," describes how to upgrade to ISA Server, Enterprise Edition.
- Chapter 6, "Installing and Configuring Clients," describes ISA Server clients and details the steps you perform to configure ISA Server clients.
- Chapter 7, "Deployment Scenarios," illustrates some common network configurations and details the steps you need to perform to implement these scenarios, using ISA Server.

Chapter 1: Introduction

This chapter provides an overview of Microsoft Internet Security and Acceleration (ISA) Server. It also describes some common scenarios in which ISA Server might be used in your network.

This chapter includes the following sections:

- Introducing ISA Server
- Features and Usage Scenarios

Introducing ISA Server

With the exploding growth of business activities taking place on the Internet and the vast number of corporate networks which are connected to it, the need is greater than ever for a powerful and easy-to-administer Internet gateway that provides a secure connection while also enhancing and improving network performance. ISA Server meets these demands by offering a complete Internet connectivity solution that contains both an firewall and a complete Web cache solution. These services are complementary: you can use either or both of these functionalities when you install ISA Server in your network.

ISA Server secures your network, allowing you to implement your business security policy by configuring a broad set of rules that specify which sites, protocols, and content can pass through the ISA Server computer. ISA Server monitors requests and responses between the Internet and internal client computers, controlling who can access which computers on the corporate network. ISA Server also controls which computers on the Internet can be accessed by internal clients.

ISA Server offers many security options, including packet filtering and intrusion detection. You can create access policies based on user-level information or Internet Protocol (IP) addresses and control when the rule will be applied.

ISA Server features secure publishing. You can use ISA Server to define a publishing policy, protecting the internal publishing servers and making them safely accessible to Internet clients.

ISA Server implements a cache of frequently requested objects. You can configure the cache to ensure that it contains the data that is most frequently used by the organization or accessed by your Internet clients.

ISA Server is extensible. ISA Management has a corresponding COM interface which administrators can program, using high-level programming languages or scripting languages. The core firewall functionality can be extended by other developers, who implement application filters or Web filters. The cache functionality can be enhanced using the cache application programming interface (API). The ISA Management interface can be extended to provide integrated administration tools for the third-party extensions.

Features and Usage Scenarios

Microsoft has worked with customers to design a product that addresses the needs of today's Internet-enabled businesses: security, performance, and manageability. The following sections survey some common user scenarios and show how you can use ISA Server features to implement the scenarios in your network.

Internet Connectivity with Strong Security

ISA Server can be deployed as a dedicated firewall that acts as the secure gateway to the Internet for internal clients. By setting the access policies, administrators can prevent unauthorized access and malicious content from entering the network as well as restrict outbound traffic.

ISA Server presents you with a comprehensive solution for securing network access. ISA Server includes the following firewall and security features:

- Outgoing access policy. You can use ISA Server to configure site and content rules and protocol rules that control how your internal clients access the Internet. Site and content rules specify which sites and content can be accessed. Protocol rules indicate whether a particular protocol is accessible for inbound or outbound communication.
- Intrusion detection. Integrated intrusion detection mechanisms can alert you when a specific attack is launched against your network. For example, you can configure the ISA Server computer to alert you if a port scanning attempt is detected.
- System Security Wizard. The ISA Server Security Wizard enables you to lock down Windows 2000 by setting the appropriate level of security, using predefined templates.
- Application filters. ISA Server analyzes and controls application-specific traffic with application-aware filters that inspect the actual data. You can enable intelligent filtering of Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), e-mail, H.323 conferencing, streaming media, remote procedure call (RPC), and more.
- VPN support. ISA Server includes standards-based, secure remote access with the integrated virtual private networking (VPN) services of Microsoft Windows 2000.

Productive Internet Access

Internet access is an essential tool for today's knowledge worker. With the heavy Internet traffic that goes across network gateways, Web access performance can become the bottleneck for productivity. The Web caching features of ISA Server provide faster Web access performance by caching Internet content closer to the user. In addition, by using the policy-based access controls, administrators can limit which Web sites are permitted for specific users, by time of day, content type, and more. With fast caching and access control, ISA Server can help lower the cost of managing Internet connectivity and improve the productivity of Internet users. ISA Server uses RAM caching and efficient file input/output to deliver fast cache performance.

ISA Server caching features include:

- Hierarchical caching. ISA Server allows you to set up a hierarchy of caches, chaining together ISA Server computers, so that clients can access from the cache geographically nearest them.
- Reverse caching. ISA Server can cache HTTP and FTP content of publishing servers, thereby improving their accessibility.
- Scheduled caching. You can use the scheduled cache content download service to configure when the ISA Server computer should download commonly requested content from the Internet to its cache.

Fast, Scaleable Publishing and E-commerce

Whether your organization is an Internet e-commerce retailer or a large organization looking to expand your business reach, the Internet is a key part of your business strategy. Organizations cannot afford to have slow, unresponsive e-commerce Web sites, especially when the competition is one mouse-click away. The Web cache of ISA Server provides users with a fast Web experience that scales with your growing business. Caching is available also for Internet clients that request objects from computers on your local network.

ISA Server allows you to publish services to the Internet without compromising the security of your internal network. You can configure Web publishing and server publishing rules that determine which requests should be sent downstream to a server located behind the ISA Server computer, providing an increased layer of security for your internal servers.

You can use these ISA Server features to publish servers:

- Secure Web publishing. Web publishing rules allow secure access to internal Web servers. Web publishing rules grant external clients access to internal servers, while protecting from unwarranted access.

- Secure application server publishing. Server publishing rules allow you to make internal servers accessible to specific clients, without requiring tedious configuration or installation procedures on the publishing server.
  ISA Server includes a Mail Server Security wizard, which eases the configuration of Exchange Server on the local network.

Unified Management

Managing security and caching separately usually requires a separate set of network technologies, infrastructure equipment, and skilled administrators, therefore increasing complexity, cost, and inconsistency. The unified policy-based administration tool in ISA Server helps administrators manage and secure their Internet connectivity from a central location, reducing network complexity and lowering total cost of ownership.

Organizations often benefit from consistent firewall and cache policies. The management integration in ISA Server provides a single view of these policies, rather than having to separately manage firewall and cache infrastructure.

Chapter 2: Planning Considerations

This chapter concentrates on the information you need to plan and deploy Microsoft Internet Security and Acceleration (ISA) Server in your organization. Although this chapter provides much of the information you need to deploy ISA Server, it does not attempt to cover all networking issues.

The table below lists factors you should consider as you plan your ISA Server deployment.

Issue	Description	See
How many computers do I need?	Hardware configuration and Internet connectivity depend on how you use ISA Server.	“Capacity planning guidelines”
Which ISA Server features will I need?	You can choose to install specific ISA Server features to meet your specific network needs.	“Selecting ISA Server features”
What are the user requirements?	Determine what applications and services your users require, so that you can decide how to configure clients.	“Assessing client requirements”
Should I reconfigure my existing network?	Consider how ISA Server will interact with the existing network.	Existing network considerations

This chapter includes the following sections:

- Capacity Planning Guidelines
- Selecting ISA Server Features
- Assessing Client Requirements
- Interaction with Other Network Services

Capacity Planning Guidelines

For improved performance, you should plan the ISA Server hardware and Internet connectivity to meet the expected load. The following sections describe recommended system configurations for various usage scenarios.

Minimal Requirements

To use ISA Server, you need:

- A personal computer with a 300 megahertz (MHz) or higher Pentium II-compatible CPU.
- For the operating system, the computer must run Microsoft Windows 2000 Server with Service Pack 1 or later, Windows 2000 Advanced Server with Service Pack 1 or later, or Windows 2000 Datacenter Server.
- 256 megabytes (MB) of RAM
- 20 MB of available hard-disk space
- Windows 2000 compatible network adapter for communicating with the internal network
- One local hard-disk partition formatted with the NTFS file system

A maximum of four processors can be used on the computer running ISA Server. ISA Server will not install on a computer with more than four processors.

If you are using ISA Server in firewall or integrated mode, two network adapters are required.

Note

Always use the latest Service Pack.

Remote Administration Requirements

For remote ISA Server administration, you need only install ISA Management, which can run on Windows 2000 Professional or above.

Instead, you can install Terminal Services in Remote Administration mode on the computer running ISA Server. In that case, you do not have to install the ISA Management tool on another computer at all for remote administration. Instead, you can use a Terminal Services session to administer ISA Server.

Forward Caching Requirements

ISA Server can be deployed as a forward caching server, maintaining a centralized cache of frequently requested Internet objects that can be accessed by any Web browser client. In this case, consider how many Web browser clients will be accessing the Internet. The table below lists hardware configurations for expected number of internal clients accessing objects on the Internet.

Number of Users	ISA Server Computer	RAM (in MB)	Disk Space Allocated for Caching
Up to 500	Single ISA Server computer with Pentium II, 300 MHz processor	256	2- 4 Gigabytes (GB)
500 – 1,000	Single ISA Server computer with two Pentium III, 550 MHz processors	256	10 GB
More than 1,000	Two ISA Server computers, each with Pentium III, 550 MHz processors	256 for each server	10 GB for each server

As your user base exceeds 1,000 users, you can consider either using hardware with faster processors and more memory or adding more ISA Server computers. For more information, see "Adding More Computers." When you set up more than one ISA Server computer, consider upgrading to ISA Server, Enterprise Edition, so that you can group the computers in arrays. For more information, see Chapter 5, "Upgrading to ISA Server, Enterprise Edition."

Publishing Requirements (Reverse Caching)

ISA Server can provide caching for external users requesting data. For example, it can be deployed between the Internet and an organization's Web server that is hosting a commercial Web business or providing access to business partners. In this case, you need to consider how often external clients will request objects on the publishing servers.

The table below lists hardware configurations for expected number of requests from Internet (external) users, in a reverse caching scenario.

Hits per Second	ISA Server computer
Less than 100	Single ISA Server computer with Pentium II, 300 MHz processor
Up to 250	Single ISA Server computer with Pentium III, 450 MHz processor
More than 250	ISA Server computer with Pentium III, 550 MHz processor Additional ISA Server computer for each 250 hits per second. You can also use Performance Monitor to determine bottlenecks and add more servers or stronger hardware, as necessary.

For random access memory (RAM), memory requirements depend on the size of the cacheable content that you are publishing. Ideally, all cacheable content should be able to fit into memory. For example, if the Web site you are publishing is made up of 250 MB of content, then 256 MB of RAM is sufficient.

Adding More Computers

You can use the capacity planning requirements detailed above as a general guideline to determine how many ISA Server computers you require. In some cases, you face the decision whether to add an additional ISA Server computer or simply boost the performance of the existing computer by adding an additional processor. Each option has different advantages.

When you add a new computer, consider upgrading to ISA Server Enterprise Edition, so that you can create an array of ISA Server computers. Arrays help ensure a more fault-tolerant system. Should one computer crash, the other continues to function. Furthermore, because ISA Server's centralized array management means that there are few additional ISA Server management issues when you add more servers to the array.

On the other hand, adding another computer means that you will have to purchase and manage additional hardware, as well as any other software (such as the operating system) installed on the computer.

Selecting ISA Server Features

ISA Server can be installed with both firewall and caching features. You can also install just firewall features or just cache features. As part of the installation process, you choose the mode of installation: firewall, cache, or integrated.

In firewall mode, you can secure network communication by configuring rules that control communication between your corporate network and the Internet. In firewall mode, you can also publish internal servers, thereby sharing data on your internal servers with Internet users.

In cache mode, you can improve network performance and save bandwidth by storing commonly accessed objects closer to the user. You can route requests from Internet users to the appropriate Web server.

In integrated mode, all cache and firewall features are available. You can configure a policy that takes both cache performance needs and security needs into consideration.

Depending on which mode you select, different features are available. The table below lists which features are available for the firewall and cache modes. In integrated mode, all the features are available.

Selecting ISA Server Features

Feature	Firewall	Cache
Access policy	Yes	Yes (HTTP and HTTPS protocol only)
Application filters	Yes	No
Cache configuration	No	Yes
Firewall and SecureNAT client support	Yes	No
Packet filtering	Yes	No
Real-time monitoring	Yes	Yes
Reports	Yes	Yes
Server publishing	Yes	No
Virtual private networking	Yes	No
Web filters	Yes	Yes
Web publishing	Yes	Yes
Web Proxy client support	Yes	Yes

Assessing Client Requirements

ISA Server supports the following types of clients:

- Web Proxy clients. A Web Proxy client sends requests directly to the ISA Server, but Internet access is limited to the browser. You can configure Web browsers that support HTTP 1.1 as Web Proxy clients.
- SecureNAT clients. Secure network address translation (SecureNAT) clients provide security and caching, but do not allow for user-level authentication. To configure a SecureNAT client, you only have to set the default gateway on the client computer to the Internet Protocol (IP) address of the ISA Server.

Because a SecureNAT client requires no configuration other than changing the default gateway, any computer that uses Transmission Control Protocol/ Internet Protocol (TCP/IP) can be a SecureNAT client.

- Firewall clients. Firewall clients restrict access on a per-user basis for outbound access for requests that use TCP and User Datagram Protocol (UDP). To configure a Firewall client, you must install the Firewall client program on each client computer. You can install the Firewall client program only on computers running Microsoft Windows Millennium Edition, Microsoft Windows 95 OSR2, Microsoft Windows 98, Windows NT 4.0, or Windows 2000.

Before you deploy or configure client software, assess your organizational needs. Determine which applications and services your internal clients require. Assess how you will publish servers, then map these needs to the client types supported by ISA Server.

If you want to...	Then use...
Improve the performance of Web requests for internal clients	Web Proxy clients.
Avoid deploying client software or configuring client computers	SecureNAT clients. SecureNAT clients do not require any software or specific configuration
Improve Web performance in an environment with non-Microsoft operating systems	SecureNAT clients. SecureNAT client requests are transparently passed to the ISA Server's Firewall service and then to the caching service for caching.
Publish servers that are located on your internal network	SecureNAT clients. Internal servers can be published as SecureNAT clients, which eliminates the need for creating special configuration settings on the publishing server. It is not recommended to set up publishing servers as Firewall clients.
Allow Internet access only for authenticated users	Firewall clients. You can configure user-based access policy rules for Firewall clients

Interaction with Other Network Services

Previously, you may have used Routing and Remote Access in Windows 2000 Server to make network services and computers available to remote clients. ISA Server provides the remote connectivity, and extends Routing and Remote Access by offering more extensive and flexible security features. ISA Server packet filtering replaces the Routing and Remote Access packet filtering. ISA Server uses the dial-up connections that you configured for Routing and Remote Access.

Similarly, you may have previously used the Internet Connection Sharing (ICS) or network address translation (NAT) features of Windows 2000 to access the Internet. ISA Server can be used instead of NAT or ICS, replacing and enhancing its function in the organization. ISA Server provides the connectivity enabled by NAT or ICS and adds sophisticated security and caching features.

Chapter 3: Installing ISA Server

This chapter assists you as you install Microsoft Internet Security and Acceleration (ISA) Server.

This chapter includes the following sections:

- Before You Install ISA Server
- Installing ISA Server
- Next Steps

Before You Install ISA Server

Before you install ISA Server, you must set up the hardware and configure the software of the computer that will run ISA Server.

Use the information in the following sections to ensure that the ISA Server computer meets pre-installation requirements. For additional information on any task, see the documentation provided with your hardware component or Microsoft Windows 2000.

Setting Up the Network Adapter

You can choose to connect your network to the Internet through either a direct connection (such as T1, T3, xDSL, or cable modem) or a dial-up connection. If you choose a direct connection, you must set up a network adapter that connects the computer running ISA Server to the Internet.

When you set TCP/IP properties for the external network adapter, check with your ISP for the correct settings. You must have the IP address, subnet mask, default gateway, and IP addresses for the DNS servers to be used in DNS name searches. In some cases, your ISP may be using DHCP or bootstrap protocol (BOOTP) for dynamic assignment of client addresses.

Typically, ISA Server will have only one IP default gateway. You should only configure the IP address of the default gateway on the external network adapter and not on the internal network adapter. Simply leave the internal card′s Default Gateway setting blank.

Refer to the Windows on-line help for instructions on setting up network adapters.

TCP/IP Settings

When setting TCP/IP properties for any internal network adapter, you should enter a permanently-reserved IP address for the ISA Server computer and an appropriate subnet mask for your local network. Addressing assigned by DHCP should not be used for the internal network adapter, since it might reset the default gateway you selected for the ISA Server computer. The external network adapter can use DHCP or its IP address is statically defined, including the default gateway and DNS settings.

After setup, you can use the Ping.exe utility that is provided with Windows 2000 Server or a similar utility on another internal IP client computer to verify network connectivity and to check if network adapters and other hardware are configured correctly.

Setting up a Modem or ISDN Adapter

If you choose to connect to the Internet through a dial-up connection instead of a direct link by using an external network adapter, you must use a modem or an ISDN adapter with your server.

Depending on the ISDN adapter, you may not be able to view the two ISDN channels in Windows 2000. Typically, the drivers for the ISDN card manage bandwidth-based connectivity for the second channel; you cannot use Windows 2000 to manage the driver. Be sure that the network adapter is set up so that both channels can be configured and that your ISP supports connecting by using both channels.

For more information on setting up an ISDN adapter or modem, see the Windows 2000 Help.

Windows 2000 Routing Table

The local address table (LAT) is a table of all IP address ranges used by the internal network that is behind the ISA Server computer. ISA Server uses the LAT to control how machines on the internal network communicate with external networks and decides which network adapters should be protected by loading the packet filter driver.

ISA Server can construct the LAT, based on your Windows 2000 routing table. You can also select the private IP address ranges, as defined by the Internet Assigned Numbers Authority (IANA) in RFC 1918. These three blocks of addresses are reserved for private intranets only and are never used on the public Internet.

If the computer is connected to a routed internal network and you are unsure of your routing topology or how to add static routes, you can manually construct the table to contain the range or ranges of IP addresses used by your internal clients.

Since a default gateway cannot be set on the internal interface of the ISA Server computer, you will need to create static routes for your internal network to achieve full connectivity. This can be accomplished using the ROUTE command at a command prompt.

A LAT that is configured correctly ensures that ISA Server determines which network adapter to use in order to access different portions of your internal network. If you fail to set the routing table correctly, the LAT may not be built correctly. This can result in a client request for an internal IP address being incorrectly routed to the Internet or being redirected through the Firewall service.

If needed, after installation, the LAT should be edited manually to include all other network segments that are internal to your organization, including those that are located across internal routers so that the ISA Server computer and Firewall clients can correctly determine when to use ISA Server and when to access a resource directly.

When creating a LAT, you should only include addresses on the private network. This means that you should not add the external interface of the ISA Server computer, any Internet sites, or any other external addresses including the DNS server at your Internet service provider, and so forth. An incorrect configuration of the LAT could make your network vulnerable to attacks.

The LAT is maintained centrally at the ISA Server computer. Firewall clients automatically download and receive LAT updates at preset, regular intervals.

Installing ISA Server

When you install ISA Server, you will be asked for the following information.

- CD Key. This is the 10-digit number located on back of the ISA Server CD-ROM case.
- Installation options. You can select a Typical installation, Full installation, or Custom installation.
- Mode. You can install ISA Server in firewall mode, cache mode, or integrated mode.
- Cache configuration. If you install ISA Server in integrated or cache mode, then you must configure which cache drives to use and the size of the cache.
- Local address table (LAT) configuration. If you install ISA Server in integrated or firewall mode, then you must configure the address ranges to include in the LAT.

I mportant

Confirm that you have installed Windows 2000 Service Pack 1 or later before you install ISA Server.

To install server software

1. Insert the ISA Server CD-ROM into the CD-ROM drive or, run ISAautorun.exe from the shared network folder.
2. In Microsoft ISA Server Setup, click **Install ISA Server**.
3. If you accept the terms and conditions stated in the end-user license agreement, then click **Continue**.
4. Type the product identification number that is listed on the product box.
5. Read the End User License Agreement, and then, if you agree to its terms and conditions, click **I Agree**.
6. Click Typical Installation, Full Installation, or Custom Installation.
7. If you click **Custom Installation**, select the check boxes which correspond to the ISA Server components you wish to install. You can select from the following:

- ISA Services
- Add-in services
- Administration tools

1. Click the ISA Server mode you wish to install.
2. After Setup warns you that it will stop the Internet Information Service (IIS), if you chose to install ISA Server in cache mode or integrated mode, configure the cache drives.
3. If you install ISA Server in firewall mode or in integrated mode, then configure the LAT.
4. If you want to run the Getting Started Wizard when you invoke ISA Server , select the **Start ISA Administrator Getting Started Wizard** check box.

Note

1. Setup stops the IIS Web service because its default port is 80, the HTTP standard. ISA Server uses this port to allow Web publishing and will listen for Web requests on these ports from both internal and external clients when Web publishing rules are created.
2. You can select the disk drives that are available for caching during ISA Server installation. By default, the setup process searches for the largest NTFS partition and sets a default cache size of 100 megabytes (MB) if there are at least 150 MB available. When configuring the cache drives, you must, at a minimum, allocate at least one drive that is formatted by using the NTFS file system and 5 MB on that drive for caching. However, it is recommended that you allocate at least 100 MB and add 0.5 MB for each client that uses the HTTP or FTP protocols, rounded up to the nearest full megabyte.

Next Steps

After installation, ISA Server effectively blocks all communication between your corporate network and the Internet. Until you configure an access policy, with protocol rules and site and content rules specifically allowing access, no communication is allowed. Similarly, you must configure publishing rules if you want to allow Internet clients access to computers on your internal network.

Post-Installation Default Settings

After installation, ISA Server uses the default settings that are listed in the table below.

Feature	Default Setting
User permissions	Members of the Administrators group on the local computer can configure policy.
Local address table	Contains entries specified during installation process.
Packet filtering	Enabled in firewall mode and in integrated mode Disabled in cache mode.
Access control	A default site and content rule named "Allow Rule" allows all clients access to all content on all sites always. However, since no

	protocol rules are defined, no traffic is allowed to pass.
Publishing	No internal servers are accessible to external clients. A default Web publishing rule discards all requests.
Routing	All Web Proxy client requests are retrieved directly from the Internet.
Caching	The cache size is set to the size that was specified during setup. HTTP and FTP caching are enabled. Active caching is disabled.
Alerts	All alerts except the following are active: All port scan attack, Dropped packets, Protocol violation, and UDP bomb attack
Client configuration	When installed or configured, Firewall and Web Proxy clients have automatic discovery enabled. Web browser applications on Firewall clients are configured when the Firewall client is installed.

Getting Started Wizard

After you install ISA Server, you can use ISA Server to implement your corporate security and Internet access guidelines. As a first step, you should create the policy elements that describe your network. Group computers into client address sets and users into Windows 2000 security groups. Create destination sets that include computers and domains on the Internet. Define protocols that can be used to communicate with the Internet. Then use the policy elements which implement the corporate guidelines when you create policy rules.

The Getting Started Wizard will walk you through the steps of defining and configuring the ISA Server policy. After you finish, ISA Server secures your network's connection to the Internet.

The Getting Started Wizard helps you perform the following tasks:

- Creating policy elements, which you will use when you create rules.
- Creating protocol rules and site and content rules
- Setting system security level and configure packet filtering.
- Configuring routing and chaining to determine how client requests are routed to the destination server.
- Creating cache policy to determine which objects are cached.

After you configure the ISA Server policy, read Chapter 5 to learn how to set up and configure the clients in your network. Then read Chapter 6 to learn about specific deployment scenarios.

Chapter 4: Migrating from Microsoft Proxy Server 2.0

Microsoft Internet Security and Acceleration (ISA) Server supports a full migration path for Microsoft Proxy Server 2.0 users. Most Proxy Server rules, network settings, monitoring configuration, and cache configuration will be migrated to ISA Server. Furthermore, ISA Server will continue to support Winsock proxy client software, together with its own Firewall client software, in a heterogeneous client base.

ISA Server introduces many new features and changes over Proxy Server 2.0. These changes affect the server configuration and upgrade scenarios. This chapter outlines the key items that an administrator should consider as part of the upgrade process to ISA Server.

This chapter includes the following sections:

- Reasons for Migration
- Migration Process
- Migrating Proxy Server 2.0 Configuration

Reasons for Migration

ISA Server is the successor to Proxy Server 2.0, although it is much more than a "proxy." When compared with Proxy Server 2.0, new or significantly improved features in ISA Server, include the following:

- A multilayer firewall that features stateful inspection, broad application support, and integrated intrusion detection
- Integrated Virtual Private Networking
- System hardening
- RAM caching and optimized cache store, including scheduled content download
- Unified management console, including graphical taskpads and wizards for common tasks
- Transparency for all clients
- Advanced, passthrough, and Secure Sockets Layer (SSL) authentication support

- Improved monitoring features, including customizable alerts, detailed logging, and reporting
- Extensible platform with a comprehensive Software Development Kit

Migration Process

Before you can migrate an array of Proxy Server 2.0 computers, it is recommended that you remove all the members. Each member will retain an identical set of rules, which was replicated to all the servers in the array. Also, all the servers will retain identical network configuration (such as dial-on-demand settings) and monitoring configuration (such as alerts).

When you migrate Microsoft Proxy Server 2.0 to ISA Server, Standard Edition, ISA Server cannot be installed as an array member. If you want to install ISA Server as an array member, you must install ISA Server, Enterprise Edition.

There are a number of additional issues you should consider while preparing to migrate from Proxy Server 2.0 to ISA Server.

- Direct upgrade from Proxy Server 1.0, BackOffice Server 4.0 or Small Business Server 4.0 is not supported.
- There is no automatic option to return to Proxy Server 2.0 once the upgrade to ISA Server has been started.
- ISA Server does not support the IPX protocol.
- Before you upgrade from Proxy Server 2.0, perform a full backup of the current settings.

In addition, ISA Server can only be installed on computers running Windows 2000 Server or later. Therefore, if your current version of Microsoft Proxy Server 2.0 runs on Windows NT 4.0, follow these steps:

1. Stop and disable all Proxy Server services. To do this, type net stop service_name at a command prompt. Here are the Proxy Server services, with the appropriate service name.

Proxy Server service	Service name
Microsoft Winsock Proxy service	wspsrv
Microsoft Proxy Server Administration	mspadmin
Proxy Alert Notification service	mailalrt
World Wide Web Publishing service	w3svc

2. Upgrade to Windows 2000. You may receive a message indicating that Proxy Server 2.0 will not work on Windows 2000. This message can be safely ignored. For more detailed instructions, see the Proxy Server 2.0 home page at http://www.microsoft.com/proxy/default.asp.
3. You can now begin ISA Server setup. For specific instructions, see Chapter 3 for specific instructions.

Since the core services required for firewall operation are inactive during setup, it is recommended that the computer being upgraded be disconnected from the Internet for the rest of the installation procedure.

Migrating Proxy Server 2.0 configuration

Most Proxy Server rules, network settings, monitoring configuration, and cache configuration will be migrated to ISA Server.

Proxy Chains

Mixed chains of Proxy Server 2.0 and ISA Server computers are supported.

When a computer running Proxy Server 2.0 is downstream of the ISA Server computer, only Web proxy chaining is supported. Proxy Server 2.0 does not support upstream Winsock Proxy chaining.

When an ISA Server computer is the downstream server, both Web Proxy and Firewall chaining are supported. (In Proxy Server 2.0, "Firewall chaining" was called "Winsock Proxy chaining.")

Web Proxy Client Requests

Proxy Server 2.0 listened for client HTTP requests on port 80, but when ISA Server is installed, it listens on port 8080 for the Web Proxy service. Therefore, all downstream chain members (or browsers) connecting to the ISA Server computer must connect to port 8080. You can also configure ISA Server to listen on port 80.

Publishing

Proxy Server 2.0 required that you configure publishing servers as Winsock Proxy clients. ISA Server allows you to publish internal servers, without requiring any special configuration or software installation on the publishing server. Instead, the ISA Server computer treats the publishing servers as SecureNAT clients. Web publishing rules and server publishing rules that are configured on the ISA Server computer make the servers securely accessible to specific external clients. No additional configuration is required on the publishing server.

Cache

The Proxy Server 2.0 cache configuration is migrated to ISA Server, including cache drive specifications, size, and all other properties.

Proxy Server 2.0 cache content will not be migrated, because ISA Server's cache storage engine is vastly different and more sophisticated. It will be deleted as part of ISA Server setup, and the new storage engine will be instituted, based on existing cache and drive settings.

Note

Depending on the cache size and the number of objects in the cache, the deletion process may take some time.

SOCKS

ISA Server includes a SOCKS application filter, which allows client SOCKS applications to communicate with the network, using the applicable policy to determine if the client request is allowed. Migration of Proxy Server 2.0 SOCKS rules to ISA Server policy is not supported.

Authentication

ISA Server supports the following authentication methods: basic, digest, integrated Windows, and client certificate. By default, when you install ISA Server, the integrated Windows authentication method is configured for Web requests. In Proxy Server 2.0, basic and integrated authentication are enabled by default.

Internet Explorer 5 supports integrated Windows authentication, however, other Web browsers may support only the basic authentication method. In this case, no requests will be allowed, since the user cannot be authenticated. ISA Server rejects Web requests which were previously allowed by Proxy Server. You can configure basic authentication for all Web requests.

Rules and policies

The table below lists how Proxy Server 2.0 rules and other configuration information are migrated on the ISA Server computer:

Proxy Server 2.0	ISA Server computer
Domain filters	Site and content rules
Winsock permission settings	Protocol rules
Publishing properties	Web publishing rules
Static packet filters	Open or blocked IP packet filters
Web Proxy routing rules	Routing rules

Policy elements are created, as necessary, for the new rules. Additional configuration information is also migrated: local address table, automatic dial settings, alerts, log settings, and client configurations.

Web Proxy Service permissions are not migrated to the ISA Server configuration. Active caching configuration is always disabled after the migration.

Chapter 5: Upgrading to ISA Server, Enterprise Edition

As your organization grows, and the need to communicate with the Internet increases, you should consider upgrading Microsoft Internet Security and Acceleration (ISA) Server, Standard Edition to the Enterprise Edition. The Enterprise Edition includes the following features:

- It can be deployed in multiserver arrays for better scalability, performance, fault tolerance, and centralized management.
- It supports two levels of policy management. Array policy can be applied to an entire array of servers. Enterprise policy can be applied to all the arrays in the organization.
- There is no restriction on the number of processors on the ISA Server computer. (The Standard Edition is limited to four processors.)

This chapter describes how to upgrade to ISA Server, Enterprise Edition. This chapter includes the following sections:

- Upgrading to Enterprise Edition
- Understanding Arrays
- Enterprise Policy Settings

Enterprise Edition Upgrade Process

You can perform the following steps to upgrade from ISA Server, Standard Edition to ISA Server, Enterprise Edition:

1. Although the policy will be preserved when you upgrade, it is recommended that, as an extra pre Caution, you back up the ISA Server policy.
2. Run Setup from the ISA Server, Enterprise Edition CD-ROM. The setup process is very similar to the installation process for ISA Server, Standard Edition.
   The installation process sets up the ISA Server computer as a stand-alone server.
3. Run the ISA Server Enterprise Initialization program. For more information on initializing the enterprise, see the ISA Server, Enterprise Edition Help.
4. Promote the stand-alone server to an array member. For more information on promoting a server, see the ISA Server, Enterprise Edition Help.

Understanding Arrays

When you upgrade a computer running ISA Server, Standard Edition to ISA Server, Enterprise Edition, it can be set up either as an array member or as a stand-alone server.

A stand-alone server has similar functionality to ISA Server, Standard Edition. In addition to the standard functionality, ISA Server, Enterprise Edition can be promoted to an array. For more information on promoting stand-alone servers, refer to the ISA Server, Enterprise Edition Help.

An array is a group of ISA Server computers used to provide fault tolerance, load balancing, and distributed caching. Arrays allow a group of ISA Server computers to be treated and managed as a single, logical entity. All the servers in the array share a common configuration. This saves on management overhead, since the array is configured once and the configuration is applied to all the servers in the array. Furthermore, you can apply an enterprise policy to an array, allowing you to centralize management for all the arrays in your enterprise.

An array installation also means performance savings. Arrays allow client requests to be distributed among several ISA Server computers, which improves response time for clients. Because load is distributed across all the servers in the array, you can achieve good performance even with moderate hardware.

In order to install an ISA Server computer as an array member, the computer must be a member of a Windows 2000 domain. Furthermore, the ISA Server enterprise must be initialized before you can install an ISA Server computer as an array member. For more information, see the ISA Server, Enterprise Edition Help.

ISA Server, Enterprise Edition can be installed on a stand-alone server in a Windows NT 4.0 domain with no special configuration requirements.

All array members must be in the same domain and in the same site.

Enterprise Policy Settings

As part of the enterprise initialization, the enterprise administrator can select how the enterprise policy should be applied at the array level:

- **Enterprise policy only**. In this case, the administrator at the enterprise level dictates that only the selected enterprise policy applies. No new rules can be added at the array level.
- **Combined enterprise and array policy**. In this case, an array policy is added to the enterprise policy. The enterprise policy overrides the array policy. That is, the array policy can impose additional limitations but cannot be more permissive than the enterprise policy.
- **Array policy only**. In this case, no enterprise policy is applied to the array. The array administrator can create any rule to allow or deny access.

Important

If you modify the default enterprise policy settings, changing them from array policy to enterprise policy, or vice versa, then the new settings will apply only to arrays that do not use the default enterprise policy settings that was previously configured. Enterprise policy settings for arrays that use the previous default enterprise policy settings will be changed to custom settings and will be configured with the previous default settings.

Publishing rules cannot be created at the enterprise level. However, the enterprise administrator can specify whether an array is allowed to publish servers by creating Web publishing rules or server publishing rules.

Similarly, packet filtering cannot be enabled at the enterprise level. However, the enterprise administrator determines whether packet filtering is forced at the array level. Alternatively, the enterprise administrator can allow the array administrator to decide if packet filtering should be made available.

Chapter 6: Installing and Configuring Clients

After you install Microsoft Internet Security and Acceleration (ISA) Server, you can configure the clients and install the Firewall client software, as appropriate.

Before you deploy or configure clients for ISA Server, you must consider the requirements of your organization. For more information, see "Assessing Client Requirements" in Chapter 2.

This chapter describes how to configure the ISA Server clients. This chapter includes the following sections:

- Comparing ISA Server Clients
- Configuring Web Proxy Clients
- Configuring SecureNAT Clients
- Firewall Client Configuration

Comparing ISA Server Clients

ISA Server supports the following clients:

- Web Proxy clients
- Secure network address translation (SecureNAT) clients
- Firewall clients

The table below lists the client types supported by ISA Server, and compares feature support for the clients.

Feature	SecureNAT client	Firewall client	Web Proxy Client
Installation required	No, but network configuration changes are required.	Yes	No, requires Web browser configuration
Operating system support	Any operating system that supports Transmission Control Protocol/Internet Protocol (TCP/IP)	Only Windows platforms	All TCP/IP platforms
Protocol support	Protocols with primary connections and protocols defined by application filters	All Winsock applications	HTTP, HTTPS, and FTP
User-level authentication	No, only by IP address	Yes, also by IP address	Web browser passes authentication information
Server publishing	No configuration or installation required	Requires configuration file	N/A

Both Firewall client computers and SecureNAT client computers might also be Web Proxy clients. If the Web application on the computer is configured explicitly to use ISA Server, then all Web requests (HTTP, FTP, and HTTPS) are sent directly to the Web Proxy service. All other requests are handled first by the Firewall service.

Configuring Web Proxy Clients

You do not need to install any software to configure Web Proxy clients. However, you must configure the Web browser on the client computer to use the ISA Server computer as the proxy server.

Important

Unless Web browser helper applications, such as streaming media clients, can function as Web Proxy clients themselves, these applications will not use ISA Server to connect to the Web. To allow these applications to connect to the Web, use the SecureNAT client or the Firewall client in addition to the Web Proxy client.

The exact configuration steps for configuring ISA Server depend on the Web browser you use.

To Configure Internet Explorer 5:

1. Start Internet Explorer 5, and on the **Tools** menu, click **Internet Options**, click the **Connections** tab, and then click **LAN Settings**.
2. In Local Area Network (LAN) Settings, select the Use a proxy server check box.
3. In the **Address** box, type the path to the ISA Server computer.
4. In **Port**, type the port number that ISA Server uses for client connections in **Port**.
5. (Optional) If you want your browser to bypass ISA Server when connecting to local computers, select the **Bypass proxy server for local addresses** check box. Bypassing the ISA Server for local computers may improve performance.

Configuring SecureNAT clients

Although SecureNAT clients do not require specific software to be deployed on the client computers, you must configure the network appropriately. This section details network considerations for SecureNAT clients.

Setting Up the Default Gateway for SecureNAT Clients

SecureNAT clients do not require specific software to be deployed on the client computers. However, you must configure your network topology for the ISA Server computer to protect the SecureNAT clients and ensure that their requests are serviced.

Specifically, the default gateway for the SecureNAT clients must be properly configured. When setting the default gateway property, identify which type of network topology you are configuring:

- **Simple network**. A simple network topology does not have any routers configured between the SecureNAT client and the ISA Server computer.
- **Complex network**. A complex network topology has one or more routers connecting multiple subnets that are configured between a SecureNAT client and the ISA Server computer.

To configure SecureNAT clients on a simple network, you should set the SecureNAT client's Internet Protocol (IP) default gateway settings to the IP address of the ISA Server computer's internal network address card. You can set this manually, using the TCP/IP network control panel settings on the client. Alternatively, you can configure these settings automatically for the client using DHCP.

To configure SecureNAT clients on a complex network, you should set the default gateway settings to the router on the client′s local segment and make sure that the router routes traffic destined for the Internet correctly to the ISA server′s internal interface.

Optimally, the router should use the shortest path to the ISA Server computer. Also, the router should not be configured to discard packets destined for addresses outside the corporate network; ISA Server will determine how to route the packets.

SecureNAT clients will probably request objects both from computers in the local network and from the Internet. Thus, SecureNAT must be configured to use DNS servers that can resolve names both for external and internal hosts.

Internal Networks and Internet Access

For Internet access only, the SecureNAT clients should be configured with TCP/IP settings that use the DNS servers on the Internet. You should create a protocol rule that allows the SecureNAT clients to connect to a DNS server on the Internet. This protocol rule should use the predefined DNS Query (client) protocol.

If the DNS server is located on the internal network, then you will need to create a policy that allows two-way traffic. That is, you will create a protocol rule that allows DNS queries from the DNS server to reach external DNS servers, including the Internet root servers.

Firewall Client Configuration

Before you can install Firewall client software, the ISA Server software must be installed. When you set up ISA Server, you configure the ISA Server to which Firewall clients should connect when sending requests to the Internet.

After installing the client software, you can modify the server name to which the client connects by changing the name in the Firewall client software. For more information, see the Firewall Client on-line help.

Firewall Client Components

ISA Server installs the following components on the client computer during client setup:

- Mspclnt.ini is a shared client configuration file, maintained by ISA Server.
- Msplat.txt includes a shared client local address table and the local domain table, maintained by ISA Server.
- The Firewall Client application.

You can change the default settings for all of these components after installation.

To Install Firewall Client Software:

1. At a command prompt, type Path**Setup** where Path is the path to the shared ISA Server client installation files. Typically, these files are located in Systemroot\Program Files\Microsoft ISA Server\Clients on the ISA Server computer and shared as MSPclnt.
2. Follow the onscreen instructions.

Note

Do not install Firewall client software on the ISA Server computer.

Chapter 7: Deployment Scenarios

Microsoft Internet Security and Acceleration (ISA) Server can be deployed in various network topologies. This section describes some typical network configurations. While your actual network configuration may differ from those described here, the basic concepts and configuration logic provides insights that are applicable to your configuration.

This chapter includes the following sections:

- Firewall and Caching in a Small Network
- Connecting Remote Clients
- Grouping ISA Server Computers for Fault Tolerance
- Web Publishing Scenarios
- Secure Server Publishing Scenarios
- Perimeter Network Scenarios

Firewall and Caching in a Small Network

ISA Server can be deployed in a small network, providing the internal clients with secured connectivity to the network. Because of its multipurpose functionality, ISA Server can also act as the caching server for the internal clients. The scenario described in this section shows a typical setup and configuration for a small business with clients requiring access to the Internet.

Characteristics and Requirements

The corporation used in this scenario is a small office, with less than 500 users requiring Internet access. Most users require only Web access (HTTP or FTP), although one specific department also requires access to Windows Streaming Media servers. The corporation needs a reliable method to provide Internet access in an environment with the following requirements:

- The ISA Server computer is the corporation′s only connection to the Internet.
- The corporation uses demand-dial connections when connecting to the Internet.
- The corporation does not want to deploy client software to all the users.

In this scenario, the corporation includes three departments: Sales; Research and Development; and Human Resources. Business requires that Sales and Research and Development departments need unlimited HTTP access, but only to a specific list of Web sites. Employees in all departments are allowed HTTP access after hours. In addition, all employees can access Windows Media applications after hours.

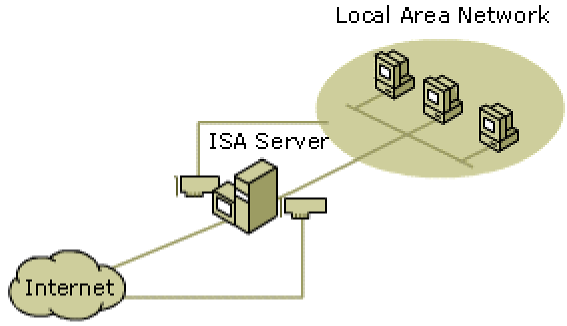
Network configuration

In this scenario, ISA Server is set up on the corporate network to serve as the connection between the local network and the Internet. The users are set up either as Web Proxy clients or SecureNAT clients. An access policy is configured on the ISA Server computer that stipulates which users are allowed to access the Internet.

Setting Up the ISA Server Computer

ISA Server is installed in integrated mode as a stand-alone server. A network dial-up connection is set up to dial to the Internet service provider (ISP). The ISA Server computer has a network card that is connected to the internal network and a modem for dialing out to the Internet.

No other services—such as Web browsers, Outlook, or Terminal Server—run on the ISA Server computer.



Setting Up Clients

For the most part, the users require only Web access. For this reason, the administrator sets up most clients as Web Proxy clients. For Web Proxy clients, the Web browsers are configured so that the proxy server is the ISA Server computer. The proxy server port on the Web browser is set to 8080, assuming that the ISA Server computer's outgoing Web request settings are also set to listen on port 8080.
Some users can use Windows Streaming Media protocols; these users′ computers are also configured as SecureNAT clients. The default gateway for the SecureNAT clients is set to the ISA Server computer's IP address. That way, all requests to the Internet will be forwarded to the ISA Server computer, which will handle the request in accordance with the access policy.

Configuring the ISA Server policy

After setting up the ISA Server computer, the administrator uses ISA Management to implement the access policy.
Before creating policy rules, the administrator creates the following policy elements:

1. Because the departments are allowed different access to the Internet, three client address sets are required, one corresponding to each department. Each client address set includes the IP addresses of the computers in the three departments: **Sales**; **Research and Development**; and **Human Resources**.
2. The business guidelines stipulate that specific sites on the Internet can be accessed during the workday. Therefore, the administrator creates a destination set – called **Work Hour Sites** – that includes those sites. This way, the rules can be applied to the single destination set.
3. The business guidelines allow Internet access to all employees after the workday, so the administrator creates a schedule called **After Hours** that can be used when creating rules that allow after-hour Internet access.
4. Because a dial-up connection is used to access the Internet, the administrator creates a dial-up entry called **Call_ISP**. The dial-up entry will be used whenever the ISA Server needs to access an object on the Internet.

Note

If Firewall Client software is installed on the client computers, then Windows 2000 user groups can be created, rather than client address sets.
The administrator follows these steps to implement an access policy:

1. Configures ISA Server′s outgoing Web request properties so that ISA Server listens on port 8080.
2. Creates a routing rule that routes Web requests to the destination server on the Internet.
   The administrator creates a routing rule, which routes all client requests to the Internet. The routing rule is configured so that ISA Server will retrieve requests for objects for all destinations directly from the specified destination on the Internet, unless a valid version of the requested object is in the ISA Server cache. The routing rule is configured to use the **Call_ISP** dial-up entry, when a request is routed to the Internet.
3. Configures firewall chaining so that all requests for non-Web objects are routed to the destination server on the Internet.
   When a client requests an object from a server on the Internet that is using a non-Web protocol, ISA Server dials out to the Internet, using the **Call_ISP** dial-up entry.
4. Verifies that a default site and content rule exists that allows everyone access to all destinations.
   ISA Server creates this rule during installation, however, users will only be allowed access after a protocol rule is created.
5. In order to allow limited Internet access for the users in the Sales department and in the Research and Development department, the administrator creates the following rules:

- A protocol rule which allows the **Sales** and **Research and Development** client address sets to always use the HTTP protocol.
- A site and content rule that allows the **Sales** and **Research and Development** client address sets access to all destinations in the **Work Hour Sites** destination set.
- A site and content rule which allows the **Sales** and **Research and Development** client address sets access to all destinations during the **After Hours** schedule.
- In order to allow users in the Human Resources department to use HTTP after the workday, the administrator creates the following rules:
- A protocol rule which allows the **HR**, **Sales**, and **Research and Development** client address sets to use the HTTP protocol during the **After Hours** schedule.
- A site and content rule which allows the **HR**, **Sales**, and **Research and Development** client address sets to access all destinations during the **After Hours** schedule.
- To allow all employees access to streaming media content, the administrator creates the following rules:

- A protocol rule which allows the **HR**, **Sales**, and **Research and Development** client address sets to use the **MMS – Windows Media Client** protocol during the **After Hours** schedule.

For more information on routing, policy elements, protocol rules, and site and content rules, see ISA Server Help.

Connecting Remote Clients

More and more employees work from home, dialing in from their home computer to the corporate network. It is becoming increasingly common for employees to establish a virtual private network (VPN) connection. In this scenario, the user dials in to the local ISP. On the other end, a server on the corporate network is connected to its ISP and a tunnel is established between the two.

Network Configuration

ISA Server is installed in integrated mode as a stand-alone server. A network dial-up connection is configured on the ISA Server computer to dial to the Internet service provider (ISP). The ISA Server computer also has a network card connected to the internal network.

The ISA Server computer is configured as a VPN server, to allow communication from specific remote clients to network resources.

Clients that connect via VPN to the ISA Server computer must be able to access corporate network resources, such as DNS and WINS.

The remote client computers must have a dial-up connection configured to dial in to the local ISP.

Configuring ISA Server

After ISA Server is set up on the computer, the administrator uses ISA Management to configure the computer as an ISA Server VPN. The administrator does the following:

1. Uses the Allow VPN Client Connections Wizard to set up ISA Server to accept client connections. The wizard:
   - Configures Routing and Remote Access as a VPN server
   - Enforces authentication and encryption methods
   - Opens static packet filters on Routing and Remote Access to allow Point-to-Point Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec) protocols.
2. Creates a network dial-up connection on the client computer which is configured as follows:
   - The network connection type is VPN. (This is accomplished by selecting **Connect to a private network through the Internet**.)
   - The destination address is the IP address of the ISA Server VPN.

Note

If ISA Server is protecting access from the corporate network to the Internet, then the remote client will have to be configured to use the ISA Server.

Grouping ISA Server Computers for Fault Tolerance

ISA Server can be used together with other Windows 2000 Server and Advanced Server services to create a fault tolerant, balanced network. The following sections describe how to configure a DNS server and how to configure Network Load Balancing in Windows 2000 Advanced Server to accomplish this goal. The following sections describe these configurations.

Using DNS

Firewall clients can achieve fault tolerance when two or more ISA Server computers are used together with a Windows 2000 DNS server.

The administrator uses DNS to assign the same name to the ISA Server computers. This way, when a client requests an object from the ISA Server computer, specifying the DNS name of the ISA Server computer, the DNS server resolves the name to either one of the ISA Server computers in a round-robin fashion. For more information on DNS and round robin, see "Configuring round robin" in Windows 2000 Help.

Follow these steps to configure the DNS server, adding a new A resource record to a zone:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **DNS**.
2. On the **Action** menu, click **New Host**.
3. In **Name**, type the DNS host name for the ISA Server computer.
4. In **IP address**, type the IP address for an ISA Server computer.
5. Click **Add Host** to add the new host record to the zone.
6. Repeat steps 3 to 5 for each ISA Server computer.

Using Network Load Balancing

For SecureNAT clients, fault tolerance can be achieved when two or more ISA Server computers are used together with Network Load Balancing in Windows 2000 Advanced Server. By combining the resources of two or more computers running Windows 2000 Advanced Server into a single cluster, Network Load Balancing can deliver the reliability and performance that Web servers and other mission-critical servers need. Each Network Load Balancing computer runs ISA Server.

Network Load Balancing clusters together several computers running server programs that use the TCP/IP networking protocol. Network Load Balancing allows all of the computers in the cluster to be addressed by an IP address while maintaining their existing addressability using unique, dedicated IP addresses. Network Load Balancing distributes incoming client requests in the form of TCP/IP traffic across the hosts.

Note

Network Load Balancing is only available with Windows 2000 Advanced Server.

Network Load Balancing requires that each ISA Server computer have a unique IP address on its internal network card. In addition, the Network Load Balancing cluster must have an IP address, which will be used by both ISA Server computers. For more information on Network Load Balancing and clusters, see "Network Load Balancing" in Windows 2000 Advanced Server Help.

Follow these steps to configure the ISA Server computers for Network Load Balancing:

1. Verify that the ISA Server computers are installed in the same mode.
2. Modify the Network Load Balancing properties on the internal network adapter on each ISA Server computer, as follows:
   - Set the primary IP address to the IP address of the Network Load Balancing cluster. This address is a cluster IP address and must be set identically for all hosts in the cluster. This IP address is used to address the cluster as a whole, and it should be the IP address for the full Internet name that you specify for the cluster.
   - Assign a unique priority to each machine in the Network Load Balancing cluster.
   - Set the dedicated IP address to the IP address of the ISA Server computer's internal network adapter. This IP address is used to individually address each host in the cluster, so it should be unique for each host. It is usually the original IP address that is assigned to the host prior to selecting an IP address for cluster operations.

For a single network adapter, the TCP/IP stack must be configured with both dedicated and cluster addresses, with the dedicated address ordered first. For a computer with two network adapters, the network adapter with the dedicated address must have a lower metric value (that is, higher priority) than that of the network adapter with the cluster address.

The default gateway for SecureNAT clients should be configured to the cluster's dedicated IP address. In other words, the cluster's virtual address should be used as the gateway address. This way, all requests will be handled by Network Load Balancing.

Web Publishing Scenarios

The Web publishing functions of ISA Server benefit organizations that want to securely publish Web content. ISA Server can protect an organization's Web server that is hosting a commercial Web business or providing access to business partners. The ISA Server computer impersonates a Web server to the outside world, while the Web server maintains access to internal network services.

The Web server you are publishing can be located either on the same computer as ISA Server or on a different computer. The following sections illustrate network configurations for Web publishing scenarios.

Configuring the ISA Server Computer

Regardless of how you set up the Web publishing scenario, ISA Server must be configured to listen for incoming Web requests. The incoming Web request properties specify which IP addresses and ports on the ISA Server computer listen for incoming Web requests. The incoming Web request properties also determine the necessary authentication required when accessing internal servers.

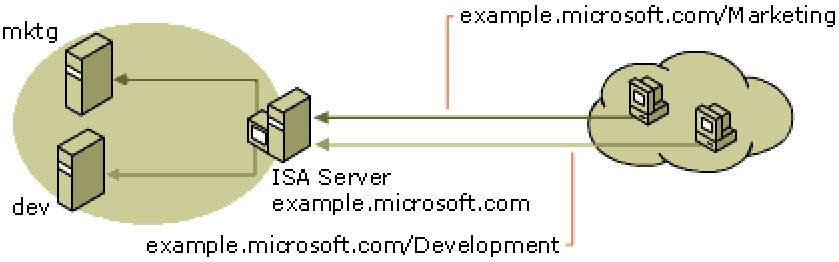
Configuring the DNS Server

When you publish Web servers, external clients may need to resolve their names with the internal DNS server. As such, the internal DNS server is itself a publishing server. If the DNS server is a SecureNAT client, then no configuration is required. After you install ISA Server, create a server publishing rule on the ISA Server computer that publishes the DNS server. For more information on server publishing rules, see the ISA Server Help.

Web Server on Local Network Scenario

In the Web publishing scenario described here, ISA Server secures content on internal Web servers that are located on computers within the local network.

The corporation described here publishes two Web sites: http://example.microsoft.com/Marketing and http://example.microsoft.com/Development. The content for the sites are on two separate internal Web servers: Mktg and Dev, respectively. When an Internet user requests an object on //example.microsoft.com/Marketing or //example.microsoft.com/Development, the request is actually sent to the ISA Server computer, which routes the request to the appropriate Web server.
The figure below illustrates the scenario.

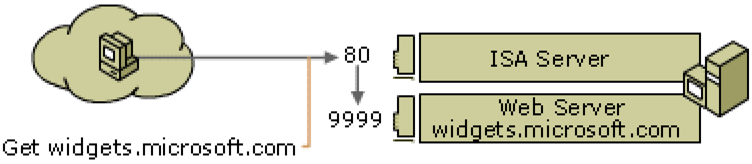

mktg
example.microsoft.com/Marketing
ISA Server
example.microsoft.com
dev
example.microsoft.com/Development

Notice that the Internet protocol addresses of the Web servers are never exposed. Instead, the Internet users gain access to the Web servers by specifying the ISA Server computer IP address.
The administrator performs the following steps to publish the internal Web servers:

1. Verifies that the DNS server maps the fully-qualified domain name to the IP address of the ISA Server computer. Internet clients use the domain name to request content.
2. Configures the ISA Server incoming Web request properties. The IP address should include the IP address of the external interface.
3. Creates the following policy elements:
   - A destination set called Marketing, which should include the computer example.microsoft.com and the path \Marketing*. This is the host header that ISA Server will try to match in order to correctly route the request to the correct internal server.
   - A destination set called Development, which should include the computer example.microsoft.com and the path \Development*.
4. Configures the following rules:
   - A Web publishing rule that publishes the Mktg computer, with the destination set configured to Marketing.
   - A Web publishing rule that publishes the Dev computer, with the destination set configured to Development.

Web Server on ISA Server Computer Scenario

Some organizations may install the Web server and the ISA Server on the same computer.
The corporation used in this scenario publishes a Web site located at http://widgets.microsoft.com.



In this scenario, the administrator can configure ISA Server to publish the Web content in one of the following ways:

- By creating Web publishing rules
- By creating IP packet filters

The following sections describe how to configure ISA Server, using these methods.

Using Web Publishing Rules to Publish a Web Server on an ISA Server Computer

In this scenario, the administrator configures the ISA Server computer to listen for incoming requests on port 80 of the external interface card. By default, the Web server also listens on port 80 for incoming requests.
To avoid this conflict, the administrator must perform one of the following:

- Configures the Web server so that it listens on a port other than 80 or on a different network adapter, then creates a Web publishing rule on the ISA Server computer that forwards requests to the appropriate port on the Web server.
- Configures the Web server to listen on a different IP address. For example, the Web server can listen on 127.0.0.1. That way, the Web server listens only for requests from the local computer. Those requests will actually come from ISA Server.

Using Packet Filtering to Publish a Web Server on an ISA Server Computer

Another way to publish a Web server located on the ISA Server computer is by configuring IP packet filters. The IP packet filter passes all packets arriving on port 80 on to the Web server, which is located on the ISA Server computer. The packet filter allows the Web server to listen on port 80 for the incoming Web requests. **Note** that, in this case, there is no conflict for outgoing Web requests, because ISA Server listens on port 8080 and the Web server listens for requests from internal clients on port 80. However, the automatic discovery feature of ISA Server should not be configured to listen on port 80 or should be disabled.

The administrator performs the following steps to publish a Web server located on the ISA Server computer:

1. Enables packet filtering.
2. Creates an IP packet filter, which allows all inbound TCP packets arriving on port 80 on the ISA Server computer′s external IP address.
3. Disables automatic discovery.

Note

Since port 80 is used by Internet Information Services (IIS), do not create Web publishing rules when using the method described here to publish the Web server on the ISA Server computer.

Automatic discovery can be used on port 8080. It can also be used from another port if you configure a DHCP server.

Secure Server Publishing Scenarios

As business-to-business e-commerce becomes more prevalent, more organizations realize the need to protect internal servers, while at the same time making them accessible to specific external users. The reverse publishing feature in ISA Server enables you to secure internal server access by external clients.

A common ISA Server scenario involves securing the Simple Mail Transfer Protocol (SMTP) communication of mail servers. For example, ISA Server can protect a Microsoft Exchange Server. The Mail Server Secure Publishing Wizard configures the policy that is needed to allow communication between an Exchange Server and the Internet. The wizard adds a set of server publishing rules which redirect communication from Internet users at a particular port to a specified internal IP address. The wizard also creates protocol rules that open ports dynamically for outgoing communication.

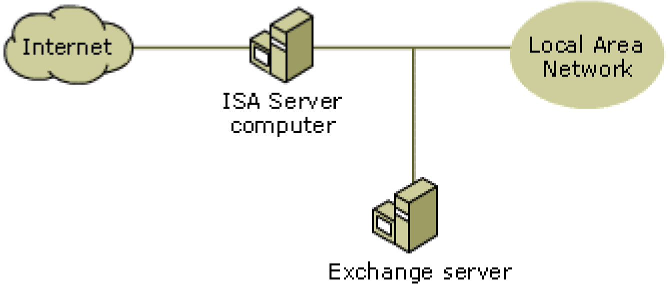
The Exchange Server that you are publishing can be located on the ISA Server computer or on the local network. The following sections describe some Exchange Server publishing scenarios.

Note

If you previously used Microsoft Proxy Server 2.0, you may have configured the Exchange Server as a Winsock Proxy client with a wspcfg.ini file to capture port 25 on the external interface of the Proxy Server computer. In this case, that configuration will work with ISA Server. However, if you use ISA Server′s server publishing rules, it is recommended that you remove the wspcfg.ini file from the Exchange Server and use the ISA Server Mail Security Wizard.

Exchange Server on Local Network

In this scenario, the Exchange Server is on the local network, protected by the ISA Server computer, as illustrated in the figure.



You can use the ISA Server Mail Server Security Wizard to configure the Exchange Server so that it is available to external clients, using one or more of the following protocols:

- Messaging Application Programming Interface (MAPI)
- Post Office Protocol 3 (POP3)
- Internet Messaging Access Protocol 4 (IMAP4)
- Network News Transfer Protocol (NNTP)
- Secure NNTP

The wizard creates one or more server publishing rules corresponding to each mail service that ISA Server protects. The server publishing rules created by the wizard have the following parameters:

- The mail server's internal IP address
- The external address exposed by the ISA Server computer
- The protocol for the selected mail service

The new rules created by the wizard are all named with the prefix **Mail wizard rule**.

The Mail Server Security Wizard also creates protocol rules, to allow outgoing mail traffic. The protocol rules have the following parameters:

- The Simple Mail Transfer Protocol (SMTP) (client).
- The client set includes the internal IP address of the Exchange Server.

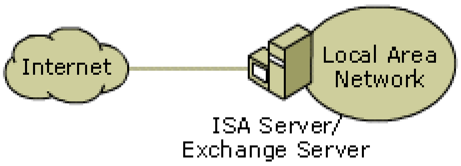
Name Resolution for Clients

Since POP3, IMAP4 and HTTP clients can access the computer that is running Exchange Server either by DNS name or IP address, it is recommended that you map the DNS name used by mail clients to the ISA Server computer external IP addresses.

For MAPI clients, a DNS server on the Internet must resolve the name of the computer running Exchange Server and match it to an IP address on the ISA Server computer's external network adapter. **Note** that, in this case, the DNS server should map the internal name of the Exchange Server computer to the ISA Server's external IP address. Therefore, the server type should be set to **Server** and not to **Mail server**. If you are publishing the SMTP service, a Mail Exchange (MX) record is also necessary and that should also point to the external IP of the ISA Server computer.

Exchange Server on the ISA Server Computer

In this scenario, ISA Server and Exchange Server are on the same computer, as illustrated below.



You can use the Mail Server Security Wizard to publish the Exchange Server located on the ISA Server computer. In this scenario, the Mail Server Security Wizard creates an IP packet filter for each mail service that you select. For example, if you run the Mail Server Security Wizard and specify Outgoing SMTP mail and POP3 client requests, the following IP packet filters will be created:

- An IP packet filter allowing inbound TCP connections on local port 25 from any remote port. This will allow incoming SMTP packets.
- An IP packet filter allowing outbound TCP connections on all local ports from remote port 25. This will allow outgoing SMTP packets.
- An IP packet filter allowing Inbound TCP connections on local port 110 from any remote port. This will allow incoming POP3 packets.
- An IP packet filter allowing outbound TCP connections on all local ports from remote port 110. This will allow outgoing POP3 packets.

Note

In this scenario, Outlook clients cannot access the Exchange Server from outside the local network.

Perimeter Network Scenarios

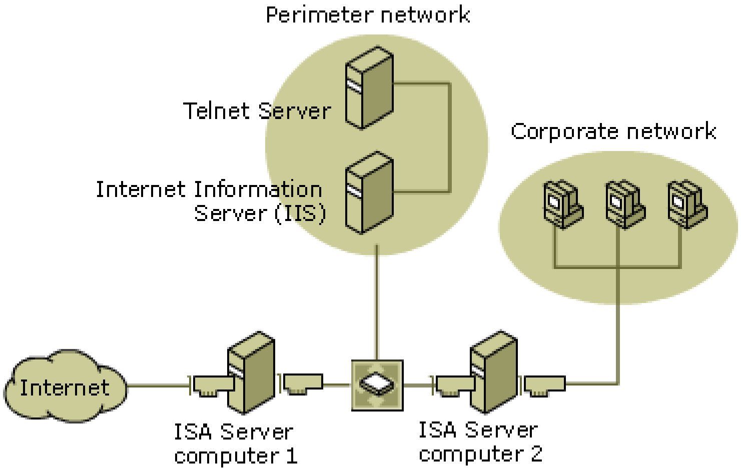
A perimeter network (also known as a DMZ, demilitarized zone, and screened subnet) is a small network that is set up separately from an organization's private network and the Internet. The perimeter network allows external users access to the specific servers located in the perimeter network, while preventing access to the internal corporate network. An organization may also allow very limited access from computers in the perimeter networks to computers in the internal network.

A perimeter network is commonly used for deploying the e-mail and Web servers for the company. The perimeter network can be set up in one of these configurations:

- Back-to-back perimeter network configuration, with two ISA Server computers on either side of the perimeter network.
- Three-homed ISA Server computer, with the perimeter network and the local network protected by the same ISA Server computer.

Back-to-Back Perimeter Network Scenario

In a back-to-back perimeter network configuration, two ISA Server computers are located on either side of the perimeter network. (A perimeter network is also known as a DMZ, demilitarized zone, and screened subnet.) The figure illustrates a back-to-back perimeter network configuration.



In this configuration, two ISA Server computers are hooked up to each other, with one connected to the Internet and the other to the local network. The perimeter network resides between the two servers. Both ISA Servers are set up in integrated or firewall mode, which reduces the risk of compromise, since an attacker would need to break into both systems in order to get to the internal network.

The administrator performs the following steps to make the servers on the perimeter network available to external clients, such as those from the Internet:

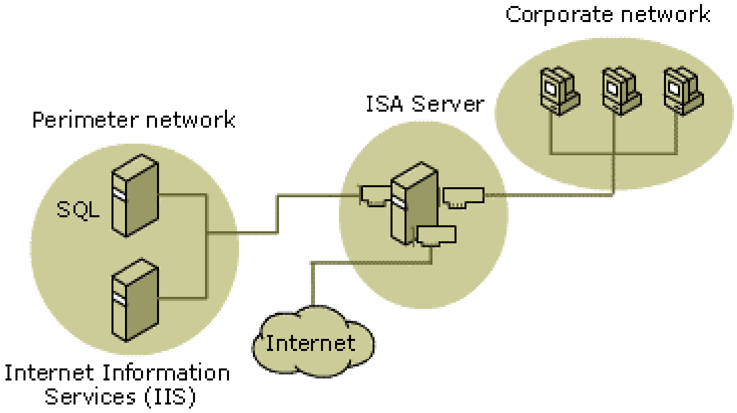
1. Configures the local address table (LAT) on the ISA Server computer that is connected to the corporate network (marked ISA Server 2) to include the IP addresses of the computers in the corporate network.
2. Configures the LAT on the ISA Server connected to the Internet to include the IP address of the ISA Server that is connected to the corporate network and the IP addresses of all the publishing servers in the perimeter network.
3. Creates a Web publishing rule to publish the IIS Server.
4. Creates a server publishing rule to publish the SQL Server, configuring the server publishing rule to apply to the SQL protocol.
5. Creates a Web publishing rule to publish the IIS Server, configuring the rule to redirect requests to the hosted site.

Three-homed Perimeter Network Scenario

In a three-homed perimeter network, a single ISA Server computer is set up with three network adapters.

- One network adapter connects to the corporate network's internal clients.
- The second network adapter connects to the corporate network servers, which are located in the perimeter network. The IP addresses of the perimeter network should not be in the local address table (LAT).
- The third network adapter connects to the Internet.

The figure illustrates this perimeter network scenario.



The administrator performs these steps to set up a perimeter network with a three-homed ISA Server:

1. Configures the LAT to include all the addresses on the corporate network. The LAT should not include the addresses on the perimeter network.
2. Enables packet filtering and IP routing.
3. Create IP packet filters for each of the servers in the perimeter network. For each IP packet filter, the local computer should be specified as the IP address of the server on the perimeter network.

end