Internet Security & Acceleration Server

Microsoft Internet Security and Acceleration Server 2000 Enterprise Edition - Installation and Deployment Guide

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 multi-layered enterprise 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 an Internet that is periodically congested.

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 to work with Windows 2000, 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, TCP/IP networking, and other Windows 2000 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.

In this guide, you will find 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 you must consider before installing ISA Server. This will help you determine how many ISA Server computers to install and what configuration is appropriate.
- Chapter 3, "Installing ISA Server," guides you through the installation process. It details hardware configuration, enterprise initialization, and the installation process itself.
- 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, "Installing and Configuring Clients," describes ISA Server clients and details the steps you must perform to configure ISA Server clients.
- Chapter 6, "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 enterprise 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. The ISA Server cache can be distributed across multiple ISA Server computers in arrays or chains of arrays. This can mean cost savings on Internet connections, because clients can obtain content from the ISA Server cache closest to them.

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 new 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 provide an overview on 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, including 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 to send you an alert if it detects a port-scanning attempt.
- *The System Security Wizard*. The ISA Server Security Wizard enables you to secure 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 calls (RPCs), and more.
- *Virtual private network support*. ISA Server includes standards-based, secure remote access with the integrated virtual private network 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, or other categories. 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 caching in random access memory (RAM) and efficient file input/output to deliver fast cache performance.

ISA Server caching features include:

- *Distributed caching*. When you set up an array of ISA Server computers, you benefit from distributed content caching. ISA Server uses the Cache Array Routing Protocol (CARP) to provide seamless scaling and extreme efficiency when using multiple ISA Server computers that are arrayed as a single logical cache.
- *Hierarchical caching*. ISA Server further extends distributed caching by allowing you to set up a hierarchy of caches, chaining together arrays of 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 refresh content that is commonly requested from the Internet to its cache.

Fast, Scalable Publishing and E-commerce

Whether your organization is an Internet e-commerce retailer or a large enterprise 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 requesting 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 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.

When you group ISA Server computers into arrays, all the array member computers can be managed centrally.

ISA Server extends centralized management for arrays to the enterprise level. The ISA Server enterprise includes all the arrays in your organization. When you set up the enterprise, you specify the enterprise policy management. You can select either a centralized enterprise policy that applies to all arrays in the enterprise or a more flexible policy whereby each array administrator can define a local policy.

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 in your enterprise, 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 section on...
How many computers do I need?	Hardware configuration and Internet connectivity depend on how you use ISA Server.	"Capacity planning guidelines"
How should I organize ISA Server computers?	Determine how to group ISA Server computers into arrays.	"Array considerations"

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
- Array considerations
- Selecting ISA Server features to install
- Assessing client requirements
- Existing network considerations

Capacity Planning Guidelines

For improved performance, you should plan the hardware and Internet connectivity of ISA Server 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, Microsoft Windows 2000 Advanced Server with Service Pack 1 or later, or Microsoft Windows 2000 Datacenter Server
- 256 MB of memory
- 20 MB of available hard disk space
- A network adapter that is compatible with Windows 2000, for communication with the internal network
- One local hard disk partition that is formatted with the NTFS file system

Note It is always recommended to use the latest Service Pack.

To implement the array and advanced policies configuration, you must also run Active Directory.

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

Remote Administration Requirements

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

Alternatively, you can install Terminal Services in Remote Administration mode on the computer running ISA Server. Then, you don't 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, which maintains a centralized cache of frequently requested Internet objects that can then be accessed by any Web browser client. In this case, consider how many Web browser clients will access the Internet. The table below lists hardware configurations according to the expected number of internal clients accessing Internet objects.

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

As your user base exceeds 1,000 users, you can either use hardware with stronger processors and more memory, or you can add more ISA Server installations. For more information, see "Adding More Computers."

When you set up more than one ISA Server computer, consider grouping the computers in arrays. For more information, see "Array considerations."

Publishing Requirements (Reverse Caching)

The ISA Server cache can be deployed to fulfill Web requests from outside of your enterprise. This is called *reverse caching*. For example, you might place an ISA Server computer between the Internet and an organization's Web server that is hosting a commercial Web business or providing access to business partners. In that case, you need to consider how often external clients will request objects from the publishing servers.

The table below lists hardware configurations for an 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
Up to 250	Single ISA Server computer with Pentium III, 450 MHz
More than 250	ISA Server computer with Pentium III, 550 MHz. For every additional 250 hits per second, add an additional ISA Server computer or use Performance Monitor to determine bottlenecks. Then, add more servers or more powerful hardware, as necessary.

Memory requirements depend on the size of the cacheable content that you are publishing, the working set of the content. Ideally, all cacheable content should fit into the available memory. For example, if the Web site you are publishing has 250 MB of content, then 256 MB of RAM is sufficient.

Adding More Computers

You can use these capacity planning requirements as a general guideline to determine how many ISA Server computers you require. In some cases, you must decide 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 and create an array of ISA Server computers, you set up a fault-tolerant system. If one computer crashes, the other continues to function. Furthermore, the centralized array management of ISA Server 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 that is installed on the computer, such as the operating system.

Array Considerations

After you decide how many servers you will install, determine how you will arrange them in your network. If you are installing more than one server, consider setting up an array of ISA Server computers. Arrays allow a group of ISA Server computers to be treated and managed as a single, logical entity. In addition, they provide scalability, fault tolerance, and load balancing.

All array members must be in the same Windows 2000 domain and in the same site. For more information, see Windows 2000 Help.

If you choose not to install ISA Server as an array member, you can install ISA Server as a stand-alone server. Stand-alone server installations do not require that the computer belong to a Windows 2000 domain.

Centralized Management

All the servers in an array share a common configuration. This saves on management overhead, since the array is configured once and then the configuration is applied to all the member servers. Furthermore, you can apply an enterprise policy to an array, allowing you to centralize management for all the arrays in your enterprise.

If you set up arrays, you may choose to set up arrays at each branch in your organization. Because each branch then has its own array, each branch can define unique usage policies that will be common to all the servers in the array. As an alternative, at the enterprise level, you can configure all the arrays in the enterprise to use one enterprise policy. At the enterprise level, you can also decide which arrays are allowed to publish servers. Furthermore, at the enterprise level, you can enforce packet filtering for the arrays in the enterprise.

Scalability and Fault Tolerance

Even if you are installing just one ISA Server computer, you should consider installing it as an array member. An array installation means that future expansion is easier—it is simple to add an additional server to the array.

ISA Server arrays help you ensure fault tolerance. If one server becomes unavailable, the other servers in the array can perform caching and security functions on its behalf. In this way, you can ensure continuous uptime for your clients.

Load Balancing

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

Comparing Arrays and Stand-alone Servers

The table below compares features and requirements for stand-alone servers and array members.

	Array	**Stand-alone server**
Scalability and fault tolerance	Can have one or more member servers.	Limited to only one member.
Active Directory requirement	Yes. Must be installed only in Windows 2000 domains with Active Directory installed. However, the local network can include Windows NT 4.0 domains.	No. Can be installed in Windows NT 4.0 domains. Configuration information is stored in the registry.
Enterprise policy	Yes. A single policy can be applied to all arrays in the enterprise.	No. Only a local array policy can be applied.

Selecting ISA Server Features

ISA Server can be installed with both firewall and caching features or you can install only the firewall features or only the cache features. As part of the installation process, you install ISA Server in firewall, cache, or integrated mode.

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 and share data on your internal servers with Internet users.

In cache mode, you can improve network performance and save bandwidth by storing frequently 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. In integrated mode, you can configure a policy that takes into consideration both cache performance needs and security needs.

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 mode**	**Cache mode**
Access policy	Yes	Yes (HTTP and HTTPS protocol only)
Application filters	Yes	No
Cache configuration	No	Yes
Enterprise policy	Yes	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 computer, but Internet access is limited to the browser. You can configure Web browsers that support Hypertext Transfer Protocol (HTTP) 1.1 as Web Proxy clients.
- *SecureNAT clients*. 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 computer. 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*. Restrict access on a per-user basis for outbound access for requests that use Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). To configure a Firewall client, you must install the Firewall Client software on each client computer. You can only install the Firewall Client software on computers running Windows Millennium Edition, Windows 95 OSR2, 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 be publishing 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 passed transparently to the ISA Server 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

Existing Network Considerations

When you install ISA Server, you are adding it to secure and connect an existing network of services. In most cases, you will not need to change your existing network configuration when you install ISA Server.

The following sections describe network issues to consider when deploying ISA Server.

Existing Windows 2000 or Windows NT 4.0 Domain

ISA Server can be installed as a stand-alone server or as an array member in a Windows 2000 domain.

When you install ISA Server as an array member in a Windows 2000 domain, the ISA Server schema is installed to Active Directory. In other words, Active Directory must be installed on the ISA Server domain to use ISA Server arrays. When you install ISA Server as a stand-alone server, it saves its configuration information to the local registry.

Arrays of ISA Server computers can also be used to connect and secure Windows NT 4.0 domain users and clients to the Internet. However, the array must be set up on a separate Windows 2000 domain. Then, a trust relationship must be established between the Windows NT 4.0 domain and the domain to which the ISA Server computer belongs.

ISA Server can be installed as a stand-alone server in a Windows NT 4.0 domain. No special configuration is required.

Interaction with Other Network Services

You may have used the Routing and Remote Access service in Windows 2000 to make network services and computers available to remote clients. ISA Server provides the remote connectivity, and extends the Routing and Remote Access features by offering more extensive and flexible security features. ISA Server packet filtering replaces the packet filtering in Routing and Remote Access. 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
- Beginning the Setup Process
- Initializing the Enterprise

- 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 (T1, T3, xDSL, or cable modem) or a dial-up connection. If you choose a direct connection, you need to set up a network adapter that connects the ISA Server computer to the Internet.

When you set Transmission Control Protocol/Internet Protocol (TCP/IP) properties for the external network adapter, check with your Internet service provider (ISP) for the correct settings. Specifically, you need 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 dynamic host configuration protocol (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.

For more information, see the Windows 2000 Help.

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 that is 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 be DHCP-enabled or its IP address can be 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 Integrated Services Digital Network (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 Windows 2000 Help.

Windows 2000 Routing Table

The local access table (LAT) is automatically constructed from the Windows 2000 Server routing table. 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 ISA Server computer's internal interface, you will later need to create static routes for your internal network to achieve full connectivity. This can be accomplished using the Windows 2000 ROUTE command from a command prompt.

An 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 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.

Beginning the Setup Process

You can start Setup from the screen that is displayed when you insert the ISA Server CD-ROM into the drive.

- If this is the first time you are installing ISA Server as an array member, then you should run the ISA Server Enterprise Initialization Tool. Start with the section on "Initializing the Enterprise."
- If you are installing a stand-alone server, or if you have previously installed an ISA Server in your enterprise as an array member, you can select Install ISA Server. Skip to "Installing ISA Server."

Initializing the Enterprise

An ISA Server computer can be set up as an array member. Before you can set up an ISA Server computer as an array member, however, the ISA Server schema must be installed to Active Directory on the domain controller. ISA Server includes an Enterprise Initialization Tool that you can use to install the ISA Server schema in Active Directory.

After the ISA Server schema is imported, all subsequent ISA Server installations to computers in the domain can use the ISA Server schema. You do not have to install the schema again.

Important In order to install the ISA Server schema to Active Directory, you must be a member of the Enterprise Admins and Schema Admins groups. For more information about Active Directory and specific instructions on user and group permissions, see Windows 2000 Help.

To Initialize the Enterprise:

1. Insert the ISA Server CD-ROM into the CD-ROM drive or, run ISAautorun.exe from the shared network drive.
2. In Microsoft ISA Server Setup, click **Run ISA Server Enterprise Initialization**.
3. If you are sure you want to initialize the enterprise and modify the Active Directory schema, click **Yes**.
4. In **ISA Enterprise Initialization**, select how you will apply the enterprise policy. You can select from the following choices:
    - Array policy only. Select **Use array policy only** if each array should have its own policy, which can be administered by the array administrator.

- Enterprise policy only. Select **Use this enterprise policy** and type the name of the enterprise policy. In this case, the same enterprise policy will be applied to all the arrays in the enterprise. Unique access policies cannot be defined for each array in the enterprise. No rules can be defined at the array level.
- Combined enterprise and array policy. Select **Use this enterprise policy** and **Allow array-level access rules to restrict enterprise policy**. In this case, array administrators can define rules that further restrict the enterprise policy. For example, if the enterprise policy allows access to all sites, array administrators could refine that policy, by creating rules denying access to specific sites.
- If array administrators are allowed to publish internal servers, making those servers accessible to external (Internet) clients, then select **Allow publishing rules to be created on the array**.
- Select **Use packet filtering on the array** if packet filtering should always be enabled for the arrays in the enterprise. If you select this option, then the array administrator will not be able to disable packet filtering.

When ISA Server Enterprise Initialization is finished, the ISA Server schema is installed to Active Directory. You can now install ISA Server as an array member, creating the array that the ISA Server should join.

Note The array creation process takes place when you install ISA Server on the first computer in the array. The information that is added to the Active Directory may take some time to replicate to all domain controllers. Therefore, if you receive an error message during installation that the ISA Server schema has not been installed, even though you have installed it, you must wait until the schema change has been replicated to the local domain controller.

Installing ISA Server

When you install ISA Server, Setup asks for the following information.

- *CD Key*. This is the 10-digit number located on the back of the ISA Server CD-ROM case.
- *Installation options*. You can select a Typical installation, Full installation, or Custom installation.
- *Array selection*. If you previously initialized the enterprise, you can select which array to join. If you did not initialize the enterprise, then ISA Server will be installed as a stand-alone server.
- *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 configuration*. If you install ISA Server in integrated or firewall mode, then you must configure the address ranges to include in the local address table.

Important You must install the Windows 2000 Service Pack 1 or later before you install ISA Server.

If the computer on which you are installing ISA Server is not part of a Windows 2000 domain, then ISA Server will be installed as a stand-alone server. You can subsequently add the server to a Windows 2000 domain, and then join it to an array.

The first server in the new array defines a new array in Active Directory. You should allow sufficient time for the array information to replicate throughout the site before you add more members to the array.

When you install an ISA Server computer as a member of an existing array, you must install it in the same mode as the other array members. For example, if all the servers in the array were installed in firewall mode, then the new ISA Server computer must also be installed in firewall mode. The new ISA Server computer adopts the array's enterprise settings, access policy, publishing policy, and monitoring configuration.

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 NTFS drive, setting aside at least 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.

The local address table (LAT) is a table of all IP address ranges used by the internal network 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 for you by basing it 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 and are never used on the public Internet.

When creating an 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 managed centrally, because it is maintained on the ISA Server computer. Firewall clients automatically download and receive LAT updates at preset, regular intervals.

To Install Server Software

1. Insert the ISA Server CD-ROM into the CD-ROM drive or, run ISAautorun.exe from the shared network drive.
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 that correspond to the ISA Server components you wish to install. You can select from the following:
   - ISA Services
   - Add-in services
   - Administration tools
8. If you did not initialize the enterprise and you want to install ISA Server as a stand-alone server, then select **Yes** and skip to Step 11.

   Otherwise, if you initialized the enterprise and you want to join the server to an array, click **Yes**.
9. If you chose to install ISA Server as an array member, then either select the array that the server should join or, to create a new array, type a new name.
10. If you create a new array, then configure the array's enterprise policy settings. Select one of the following options:

- **Use default policy settings**, if the array policy should use the enterprise's default settings.
- **Custom enterprise policy settings**. If you select this option, specify whether an array policy is used, if publishing is allowed, and if packet filtering is forced.

11. Click the ISA Server mode you wish to install.
12. 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.
13. If you install ISA Server in firewall mode or in integrated mode, then configure the LAT.
14. If you want to run the Getting Started Wizard when you invoke ISA Server, select the **Start ISA Administrator Getting Started Wizard** check box.

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 will be allowed. Similarly, you must configure publishing rules if you want to allow Internet clients access to computers on your internal network.

If you installed ISA Server as an array member, then an enterprise policy may be applied to the array. In this case, ISA Server may allow communication if the applicable enterprise policy is configured appropriately.

Default Settings After Installation

After installation, ISA Server uses the following default settings.

Feature	Default Setting
User permissions	For stand-alone servers, members of the Administrators group on the local computer can configure array policy. For arrays, members of the Domain Admins and Enterprise Admins group can configure policies.
Local address table	Contains entries that are specified during installation process.
Enterprise policy settings	When creating a new array, the array adopts the default enterprise policy settings.
Packet filtering	Enabled, in firewall mode and in integrated mode Disabled, in cache mode.
Access control	Unless the enterprise policy settings are configured to prohibit array-level "allow" rules, 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 will be 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 it 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.

After that, use the policy elements when you create policy rules, which implement the corporate guidelines.

The Getting Started Wizard walks you through the steps of defining and configuring initial enterprise and array policies. After you finish, you have configured ISA Server to secure your network's connection to the Internet.

The Getting Started Wizard helps you to perform the following tasks:

- Creating array-level policy elements, which you will use when you create array policy rules.
- Creating array-level 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.
- For array installations, configuring enterprise policy settings, which determine how the enterprise policy affects the arrays in the enterprise.
- For array installations, creating enterprise-level policy elements.
- For array installations, creating enterprise-level protocol rules and site and content rules.

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 2.0 rules, network settings, monitoring configuration, and cache configuration will be migrated in ISA Server. Furthermore, ISA Server supports 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 to Migrate
- The Migration Process
- Proxy Server 2.0 Array Considerations
- Migrating to an Array
- Migrating Proxy Server 2.0 configuration

Reasons to Migrate

ISA Server is the successor to Proxy Server 2.0, although it's much more than a "proxy." New or significantly improved features in ISA Server include:

- 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
- A 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 (SDK)

Migration Process

There are a number of 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 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/isaserver/evaluation/previousversions/default.asp.
3. You can now begin ISA Server setup. For specific instructions, see Chapter 3.

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.

Proxy Server 2.0 Array Considerations

When you migrate from Proxy Server 2.0 to ISA Server, you can install the ISA Server computer as an array member or a stand-alone server.

If you migrate Proxy Server to a stand-alone server, most of the rules and other configuration elements that were previously created for Proxy Server 2.0 are also migrated. If you migrate to a new array, the enterprise policy default settings determine how Proxy Server rules are migrated.

Before you can migrate an array of Proxy Servers, you must remove all the members of Proxy Server 2.0 array. Each member retains an identical set of rules. Similarly, all the servers will retain identical network configuration (such as dial-on-demand settings) and monitoring configuration (such as alerts).

After you remove Proxy Server 2.0 computers from the array, you can migrate Proxy Server to ISA Server. To retain a similar array configuration, perform the following steps:

1. Create a new ISA Server array. During setup, install the first computer to this array. You can also create the new ISA Server array during setup.
2. Migrate all subsequent Proxy Server computers to this array.

Migrating to an Array

You can migrate a single Proxy Server to a new array of ISA Server computers. In this case, the configuration information is migrated to the ISA Server array differently, depending on the ISA Server array's default enterprise settings.

ISA Server can be configured to use an enterprise policy only, an array policy only, or a combination of both. Depending on the enterprise policy settings, Proxy Server rules are migrated differently. The table below lists the possible enterprise settings and details how Proxy Server policy is handled for each setting.

Enterprise policy settings	Have enterprise administrator permissions?	ISA Server
Use array policy only	Yes or No	Migrates all the existing Proxy Server rules to the array policy.

Use enterprise policy only	Yes	Migrates all the existing Proxy Server rules. Enterprise policy settings for the new array are configured to **Use array policy only**.
Use enterprise policy only	No	Does not migrate any of the Proxy rules. The new array uses just the enterprise policy.
Use enterprise and array policy	Yes	Migrates all the existing Proxy Server rules. Enterprise policy settings for the new array are set to **Use array policy only**.
Use enterprise and array policy	No	Migrates only Proxy Server rules that can be migrated to deny rules—domain filters and not protocols. Enterprise policy settings for the new array use the enterprise policy, together with the array policy, which is more restrictive.

If the enterprise policy allows publishing rules, then Proxy Server publishing settings are migrated to the array policy.

If the enterprise policy does not allow publishing rules, then if you have enterprise administrator permissions, the enterprise policy settings are changed so that publishing rules are allowed on this array. Proxy Server publishing settings are then migrated to the array policy.

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 Proxy Server 2.0 server is downstream of the ISA Server, only Web Proxy chaining is supported. This is because 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 (called *Winsock Proxy chaining* in Proxy Server 2.0) are supported.

Web Proxy Client Requests

Proxy Server 2.0 listened for client HTTP requests on port 80, but when it is installed, ISA Server is configured to listen on port 8080 for the Web Proxy service. Therefore, all downstream chain members (or browsers) that connect to this 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 treats the publishing servers as secure network address translation (SecureNAT) clients. Web publishing rules and server publishing rules, 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

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

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

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 array or enterprise 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 only support the basic authentication method. In that case, no requests will be allowed, since the user cannot be authenticated. ISA Server rejects Web requests that were previously allowed by Proxy Server 2.0. 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
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 for the new rules, as necessary. In addition, the following configuration information is also migrated: local address table, automatic dial settings, alerts, log settings, and client configurations.

Chapter 5: 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	Hypertext Transfer Protocol (HTTP), Secure HTTP (HTTPS), and File Transfer Protocol (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 can 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 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 so the ISA Server computer protects the SecureNAT clients and ensures that their requests are serviced.

The default gateway for the SecureNAT clients must be properly configured. When you set 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 computer 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 protocol for the client.

If the DNS server is located on the internal network, then you will need to create a policy that allows two-way traffic. In other words, 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 the Firewall Client software, the ISA Server software must be installed. When you set up ISA Server, you configure the array to which firewall clients should connect when sending requests to the Internet, where all the array members' IP addresses are listed with the same host name.

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 "Firewall Client" in the online Help.

Firewall Client Components

ISA Server installs the following components on the firewall 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.

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

Chapter 6: 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 will provide 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
- Enterprise policy scenario
- 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 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—Hypertext Transfer Protocol (HTTP) or File Transfer Protocol (FTP)—although one 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 needs stipulate that the Sales and Research and Development departments should be allowed unlimited HTTP access, but only to a specific list of Web sites. Employees in all departments are allowed HTTP access after working hours. In addition, all employees can access Windows Media applications after hours.

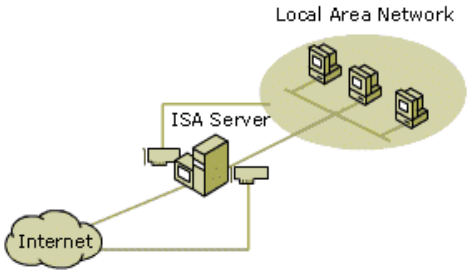
Network Configuration

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 secure network address translation (SecureNAT) clients. An access policy, which is configured on the ISA Server computer, 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 configured to dial to the Internet service provider (ISP). The ISA Server computer has a network card connected to the internal network and a modem for dialing out to the Internet.

No other services (such as Web browsers, Microsoft 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, most clients are configured as Web Proxy clients. For Web Proxy clients, the Web browsers are configured so that Proxy Server is the ISA Server computer. Proxy Server port on the Web browser should be 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 will also be configured as SecureNAT clients. The default gateway for the SecureNAT clients is configured to the ISA Server computer's Internet protocol (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**.

   If Firewall Client software is installed on the client computers, then Windows 2000 user groups can be created, rather than client address sets.
2. The business guidelines stipulate that specific sites on the Internet can be accessed during the workday, so the administrator creates a destination set that includes those sites, called **Work Hour 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**, which can be used when creating rules that allow Internet access after working hours.
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 computer needs to access an object on the Internet.

The administrator follows these steps to implement an access policy:

1. Configures ISA Server's outgoing Web request properties, so that the ISA Server computer listens on port 8080.
2. Creates a rule that routes Web requests to the destination server on the Internet.

   The administrator creates a routing rule that 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 objects other than on the Web are routed to the destination server on the Internet.

   In this way, when a client requests an object from a server on the Internet 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 which allows everyone access to all destinations.

   This rule was created when ISA Server was installed. 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 that 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 that allows the **Sales** and **Research and Development** client address sets access to all destinations during the **After Hours** schedule.
6. In order to allow users in the HR department to use HTTP after the work day, the administrator creates the following rules:
   - A protocol rule that 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 that allows the **HR**, **Sales**, and **Research and Development** client address sets to access all destinations, during the **After Hours** schedule.
7. To allow all employees access to streaming media content, the administrator creates the following rules:
   - A protocol rule that 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 are working 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 VPN 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 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 does the following:
   - 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 Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP) over Internet protocol security (IPSec) protocols.
2. Creates a network dial-up connection on the client computer, configured as follows:
   - The network connection type is VPN. (In order to use this, select the **Connect to a private network through the Internet** check box).
   - 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 must be configured to use the ISA Server computer or array.

Grouping ISA Server Computers for Fault Tolerance

In many scenarios, two or more ISA Server computers can be grouped together in an array to ensure a fault-tolerant, balanced network. This array scenario uses the Cache Array Routing Protocol (CARP) algorithm to ensure that the appropriate ISA Server computer services client requests. The array configuration ensures that, even if one array member fails, the other array members can continue to service client requests.

In the following scenarios, ISA Server alone cannot ensure fault tolerance and load balancing:

- For SecureNAT clients, which cannot identify the ISA Server by array name.
- For stand-alone servers, which cannot be grouped in arrays.

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

Using DNS

For Firewall clients, fault tolerance can be achieved when two or more ISA Server computers are used together with the Windows 2000 DNS service.

Effectively, the ISA Server computers are assigned the same DNS name using the DNS service. 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, in a round-robin fashion, to either one of the ISA Server computers. For more information on DNS and round robin, see "Configuring round robin" in Windows 2000 Server 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 or array.
4. In **IP address**, type the IP address for an ISA Server computer in the array.
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. 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 computer runs ISA Server, and Network Load Balancing balances the workload among them.

Network Load Balancing clusters together several computers running server programs that use the Transmission Control Protocol/Internet Protocol (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. On the internal network adapter on each ISA Server computer, modify the Network Load Balancing properties 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 and hence should be unique for each host. In general, it is the original IP address 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 address, 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, Network Load Balancing will handle all requests.

Enterprise Policy Scenario

ISA Server can be deployed in a large, geographically dispersed network. Arrays of ISA Server computers are deployed in the main office and at branch offices, as necessary, to accommodate user needs. This allows corporate network administrators to centralize the security and caching policy for the entire corporation. It also alleviates performance concerns in the branch office, because an ISA Server computer can service user requests for Internet objects from the local cache.

Characteristics and Requirements

The fictitious corporation used in this scenario is a large corporation, with its headquarters in the United States and two branch offices, one in Canada and one in the United Kingdom. The entire corporation requires secure Internet access in an environment with the following requirements:

- Internet access guidelines, determined at the United States headquarters, should be applied consistently throughout the corporation. For this scenario, all employees are allowed access to all sites, using the common Web protocols: HTTP, HTTPS, and FTP.
- Low costs for connecting the United Kingdom branch office to headquarters.
- The ISA Server computers in the United Kingdom branch office should cache local content. (Local content, in this case, is content from Web servers located in the United Kingdom.)
- The cache server must be in place in the Canada branch office so that the content is closer to the employees in that office and Internet traffic is reduced.

Network Configuration

Because the corporation requires a common enterprise policy for all the branch offices, the ISA Server computers must be installed as array members at all the branches, even though there will be only one computer at each branch.

ISA Server Array at United States Headquarters

Each member of the array at Headquarters is configured with two network adapters: one network adapter to connect to the internal network, and one network adapter to connect to the Internet. For this scenario, you can assume direct connectivity to the Internet service provider takes place through a router and a T1/E1 line.

ISA Server Array at Canada Branch Office

The ISA Server computers at the Canadian branch office reduce the traffic along the pipe by caching Web content. They are installed in cache mode. The ISA Server computers have two network adapters: one is connected to a local router and the other is connected to a router at Headquarters.

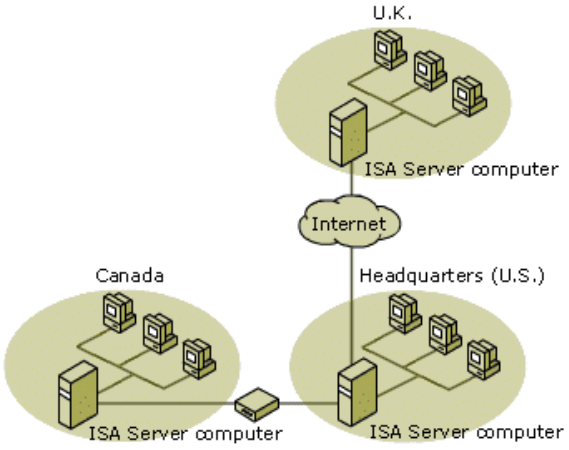
ISA Server Array at United Kingdom Branch Office

The ISA Server computers at the United Kingdom branch are set up with two network adapters: one network adapter to connect to the local network at the branch office and a modem or ISDN adapter to connect to the Internet.

The ISA Server array in the United Kingdom is set up in integrated mode, serving as the branch's firewall and cache server. The ISA Server is connected via a VPN to the array at Headquarters.

Corporate Configuration

The figure below illustrates the network configuration.



Configuring the ISA Server Policy at Headquarters

After setting up the ISA Server computers at Headquarters, the administrator uses ISA Management to implement the enterprise policy. The enterprise policy is configured at Headquarters, and is applied to all the arrays in the enterprise (Canada branch office, United Kingdom branch office, and Headquarters). In addition, employees at Headquarters can access Windows Media Streaming content.

The enterprise administrator performs the following steps:

1. Creates an enterprise policy, called **Corporate Policy**, with the following rules:
   - A site and content rule that allows everyone access to all destinations, always.
   - A protocol rule, which allows everyone to use the following protocols: FTP, HTTP, and HTTPS.
2. The United Kingdom branch office will connect to the ISA Server array at Headquarters via a virtual private network. At least one of the ISA Server computers in the United States must be configured as a VPN server. The administrator performs the following steps:
   - Configures the local address table on the ISA Server in the United States, adding the address ranges of the network in the United Kingdom.

- Uses the Local ISA VPN Server Wizard to set up ISA Server for VPN connections. This wizard starts and creates the dial-on-demand interfaces required to receive connections from remote VPN servers.

  The wizard creates IP packet filters, depending on whether you select L2TP or PPTP as the protocol. It also sets the static routes to forward traffic from the local network to hosts on the remote network via the tunnel.

  The wizard also creates a .vpc file, which is used by the remote VPN server (in the United Kingdom) when configuring the ISA Server.

Configuring the ISA Server Policy at the Canada Branch Office

Since the ISA Server in the Canada branch office is on the Headquarters' network, it requires only one network adapter, which connects it to the ISA Server at Headquarters.

The enterprise policy is applied to the ISA Server in the Canada branch, so no specific access policy rules need to be configured here.

Scheduled content download jobs are configured to pre-cache specific content at the branch offices. This will further improve perceived network performance.

The administrator performs the following steps:

1. Configures a routing rule that redirects requests from Web Proxy clients to the upstream ISA Server computer at Headquarters.
2. Creates scheduled content download jobs, to download frequently accessed objects to the local cache. If the objects are already in the cache at Headquarters, they will be downloaded from there. Otherwise, the ISA Server computers at Headquarters will forward the requests on to the Internet.

Configuring the ISA Server Policy at the United Kingdom Branch Office

The branch office in the United Kingdom is connected over the Internet, via VPN, to the Headquarters.

The administrator performs the following steps to configure the United Kingdom branch office as a VPN server

1. Set up a DNS server on the remote network that is secondary to the corporate network domains typically accessed. The DNS server should use a DNS server on the Internet as a forwarder to help resolve all other name queries.
2. Configure the local address table on the remote ISA Server computer in the United Kingdom branch office, adding the address range of the corporate network in the United States. Any external IP addresses (on the Internet) must be excluded.
3. Use the Remote ISA VPN Server Wizard to set up the remote network's ISA Server computer for VPN connections, using the .vpc file created by the enterprise administrator at Headquarters.

The Remote ISA VPN Wizard sets up a remote ISA VPN server, which can initiate connections to a local ISA VPN server. The wizard uses the .vpc file that the Local ISA VPN Wizard creates to create the dial-on-demand interfaces that are required to initiate connections to a specific local VPN server. It also configures the IP packet filters required to protect the connection and sets the static routes to forward traffic from the local network to hosts on the remote network via the tunnel.

The administrator creates routing rules to specify which requests should be routed to the array at Headquarters and which should be routed directly to an Internet service provider (ISP) in the United Kingdom.

1. He creates a routing rule that routes all requests for Internet objects in the United Kingdom directly to the Internet. Internet objects in the United Kingdom are generally indicated by a .uk suffix in the domain name.
2. He creates a routing rule that routes all other requests to the upstream ISA Server array at Headquarters.

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 detail 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

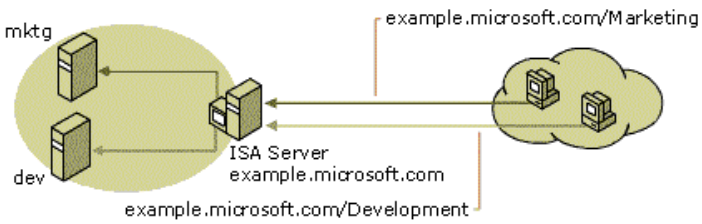
When you publish Web servers, external clients may need to resolve their names, using the internal DNS server. As such, the internal DNS server is itself a publishing server. If the DNS server is a SecureNAT client, then no configuration is required. After you install ISA Server, create a server publishing 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, 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 http://example.microsoft.com/marketing/ or http://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.



If your browser does not support inline frames, click here to view on a separate page.

Notice that the IP addresses of the Web servers are never exposed. Instead, the Internet users gain access to the Web servers by specifying the ISA Server computer's IP address.

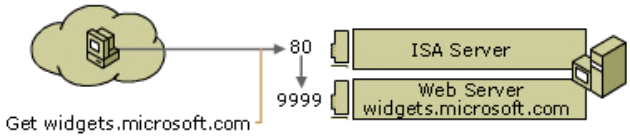
The administrator performs the following steps to publish the internal Web servers:

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 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 Web server, with the destination set configured to Marketing.
   - A Web publishing rule that publishes the Dev Web server, 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 the scenario that is illustrated below 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 the 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:

- Configure the Web server so that it listens on a port other than 80 or on a different interface card. Then, create a Web publishing rule on the ISA Server computer that forwards requests to the appropriate port on the Web server.
- Configure the Web server to listen on a different IP address. For example, the Web server can listen on 127.0.0.1. In that way, the Web server listens only for requests from the local computer — the ISA Server computer.

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. That is, 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, ISA Server's automatic discovery feature should not be configured to listen on port 80. You can also disable the feature.

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 that 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.

You can use automatic discovery on port 8080. You can also use it 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 facilitates securing internal server access by external clients.

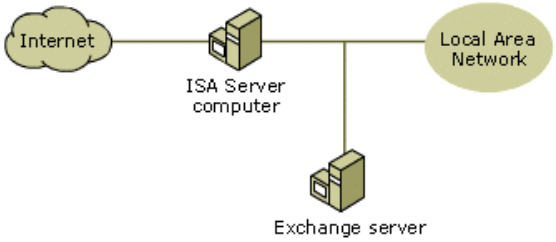
A common ISA Server scenario involves securing the Simple Mail Transfer Protocol (SMTP) communication of mail servers. For example, ISA Server can protect a Microsoft Exchange server. The Mail Server Secure Publishing Wizard configures the policy needed to allow communication between an Exchange Server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

The Exchange server that you are publishing can be 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 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, then use the Mail Security Wizard included with ISA Server.

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 that is exposed by the ISA Server
- 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 protocol is Simple Mail Transfer Protocol (SMTP) (client).
- The client set includes the internal IP address of the Exchange Server.

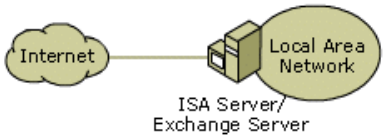
Name Resolution for Clients

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's 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 must 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, suppose you run the Mail Server Security Wizard and specify outgoing SMTP mail and POP3 client requests. In this case, the following IP packet filters will be created:

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

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

Perimeter Network Scenarios

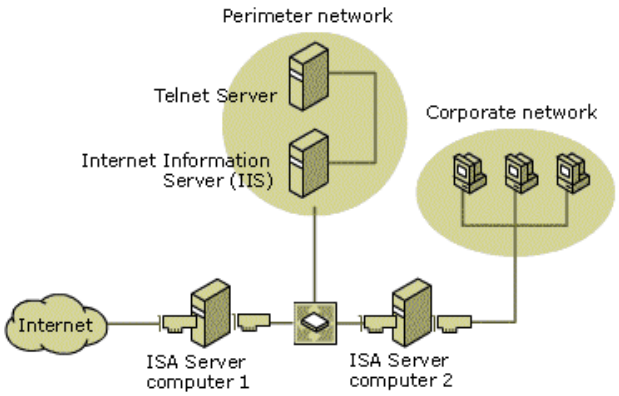
A *perimeter network* (also known as a *DMZ*, *demilitarized zone*, and *screened subnet*) is a small network that is set up separately from an organization's private network and the Internet. The perimeter network allows external users to access the specific servers located in the perimeter network, while at the same time preventing access to the internal corporate network. An organization may also allow very limited access from computers in the perimeter network 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, 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 Server computers are set up in integrated or firewall mode, essentially reducing 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 (Internet) clients:

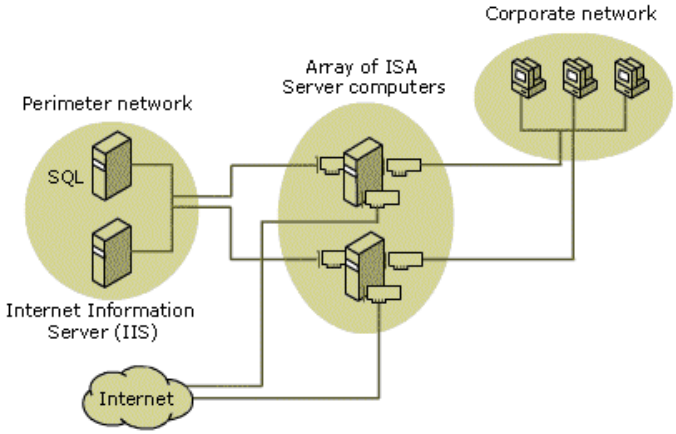
1. Configures the local address table (LAT) on the ISA Server computer that is connected to the corporate network (ISA Server 2) to include the IP addresses of the computers in the corporate network.
2. Configures the LAT on the ISA Server computer that is connected to the Internet to include the IP address of the ISA Server computer 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 (or an array of ISA Server computers) 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's servers, which are located in the perimeter network. The IP addresses of the perimeter network should not be in the local address table.
- The third network adapter connects to the Internet.

The figure illustrates this perimeter network scenario.



If your browser does not support inline frames, click here to view on a separate page.

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.

Copyright
