Chapter 1

Defending the Network with ISA Server—and Beyond

Defensive Tactics in this Chapter:

- ISA Server Overview
- Installing ISA Server
- Getting Started with ISA Server
- Installing Service Pack 1
- Supporting Network Design
- ISA Server Certification
- Beyond ISA Server

☑ Summary
☑ Defensive Tactics Fast Track
☑ Frequently Asked Questions
Chapter 1 • Defending the Network with ISA Server—and Beyond

Introduction

Our first ISA Server book, Configuring ISA Server 2000, was written while we were still struggling to master a completely new piece of software, one that was very different in features, functionality, and complexity from its predecessor, Microsoft Proxy Server 2.0. We were working with beta releases during much of the writing, and then revising the material to address changes in the final release.

In the year and a half since that book came out, we’ve gotten to know ISA Server much more intimately. Through working with it on a daily basis on our network, assisting and supporting others in the “real world” and via ISA newsgroups, mailing lists, conferences, and the www.isaserver.org Web site, we’ve come to know its quirks, peculiarities, and limitations, and learned some tweaks and tricks that will make it work better.

We have also come to understand, even more than before, that ISA or any other firewall solution is only one part (albeit an important one) of a comprehensive network security plan. The importance of multilayer security becomes more evident every day, as hackers and attackers work industriously to find ways through the barriers we set up. No single product can provide full protection for your network’s data and integrity, regardless of how good it is.

This book is the natural follow-up to the first. Although it can stand on its own for those who have some experience using ISA Server, we recommend that anyone new to the product read Configuring ISA Server 2000 first, as this book will not cover in detail the basic issues that were addressed there. This book will delve into issues that did not exist when we wrote the first (such as ISA Service Pack 1 and using ISA with Windows .NET servers) and advanced configuration and network design issues (such as using ISA Server in different types of DMZs/perimeter networks, advanced server publishing techniques involving terminal server and Exchange server, and defending your mail services with ISA Server).

The material in the next three sections of this chapter—ISA Server Overview, Installing ISA Server, and Getting Started with ISA Server—contain material that is intended for new ISA users. This is the only area of information in this book that will overlap with that of the previous book. If you already have experience with ISA, you might want to skip ahead to the section entitled Installing and Using Service Pack 1, where the all-new material begins. The remainder of the book assumes that you already have a thorough understanding of ISA Server features and functions.

This book also goes beyond ISA Server, examining other parts of your multilayered security plan. We discuss how to use Windows security features (such as the Security
Configuration Toolset, the Encrypting File System, IPSec, and IIS security) and how to implement smart card authentication and secure wireless networks.

We hope this book will provide additional guidance to network professionals who are using ISA Server in complex network situations, until it’s time to take the next step beyond ISA Server 2000: the next generation of ISA, which is code named Stingray and is in beta testing at the time of this writing.

**ISA Server Overview**

Microsoft’s Internet Security and Acceleration (ISA) Server replaced Microsoft Proxy Server 2.0, providing full-fledged firewall functionality for a much more robust security solution, along with improved caching/Web performance features. In the current security-conscious business climate (made more so by the events of September 11, 2001 and subsequent speculation that terrorists might be planning attacks on the cyberspace infrastructure), the security aspect has naturally drawn the most attention.

**The Increasing Importance of Security**

As we progress into the twenty-first century, most companies and individuals who use computers have those systems connected to the global Internet at least part of the time. Even at the consumer level, 24/7 connectivity is becoming the norm as DSL, cable modem, and satellite technologies become more widely available and increasingly easier to set up and use. This gives computer users access to a tremendous wealth of information that they didn’t have before, and makes many of their jobs easier—but it also creates vulnerabilities.

Logic dictates that if the users of your local network are able to access resources on computers all over the world, users of some of those computers might also be able to access yours. The connection is two way, and if you don’t take steps to protect your internal network from intruders, it will be easy for a moderately knowledgeable hacker to read the files stored on your network servers, copy confidential data, and even implant viruses or erase your hard disks.

However, it’s not only confidentiality of information that is at stake. Some network administrators might not realize that security can be a concern even if the data on your network is not of a “top secret” nature. The integrity of your data is also crucial. A security solution focuses on keeping outsiders from accessing data that is private and ensuring that important data is not destroyed or changed.

Security threats come in many “flavors,” but can be broadly divided into two categories: external threats and internal threats. For example, a Denial of Service (DoS) attack perpetuated by a hacker at a remote location is an external security threat. Accidental deletion of important files by a company employee onsite is an internal threat. At first glance, it might seem that ISA Server only protects you from external
threats—those that attempt to penetrate your LAN from the Internet. However, ISA also allows you to restrict outgoing network traffic, and in that way offers protection from some (although certainly not all) internal security threats as well.

The Firewall Solution

ISA Server performs the functions of a full-featured dedicated firewall. A firewall provides a much higher level of security than a proxy server (which just “stands in” for the local computers, hiding them from view on the global network). Firewalls are specifically designed to control access, preventing unauthorized data from entering the network and restricting how and what type of data can be sent out.

A network firewall acts as a barrier to prevent “bad data”—whether that be virus code or simply messages to or from unauthorized systems—from spreading from the outside network (usually the Internet) to the internal network, and also to prevent packets of a particular type or to or from a particular user or computer from spreading from the LAN to the outside network.

Firewalls can be implemented in different ways. Vendors offer a wide variety of firewall software packages that run on your gateway computer. Many vendors provide hardware firewall solutions, in which a separate device incorporates a computer system that runs special proprietary firewall software. Either way, the firewall program (or set of programs) generally works in conjunction with a router program or a Network Address Translation (NAT) program. These programs forward packets to the appropriate destination once they have been authorized to enter or leave the network. The firewall must also work with a proxy, which makes requests for Internet data and services on behalf of the internal computers.

ISA Server combines these components—proxy, NAT, and firewall—into one package. This makes it easier to deploy and administer than separate software programs and/or hardware devices.

ISA Server Features

In addition to its multilayer firewall functionality (packet filtering, circuit filtering, and application filtering), ISA Server offers such security and performance features as:

- **Integrated virtual private networking (VPN)** ISA Server can be used to set up either a remote access VPN between a client and gateway, or a multiple member VPN tunnel from server to server.

- **Integration with Active Directory** ISA access policies and server configuration information are integrated with the Windows 2000 Active Directory for easier and more secure administration.
Intrusion detection  This exciting new feature can be set up to send you an alert if/when a particular type of attack is attempted against your network (for example, if an outsider attempts to scan your ports).

Support for Secure Network Address Translation (SecureNAT)  The extensible NAT architecture that is implemented by ISA provides a secure connection for clients that don’t have the Firewall Client software installed, including Macintosh and UNIX clients and other non-Microsoft operating systems that are running TCP/IP. The SecureNAT configuration provides a true “transparent” firewall solution for your network.

Bandwidth allocation  The percentage of bandwidth allocated to a specific user, communication, client, or destination can be controlled by Bandwidth Rules that an administrator creates, to optimize network traffic usage.

Secure server publishing  Internal servers can be made accessible to specific clients, while the servers are protected from unauthorized access.

Enterprise management  ISA, like Windows 2000, was designed for greater scalability and more focus on the enterprise market than previous Microsoft products. ISA allows you to set enterprise-level policies as well as array-level policies, and management of ISA arrays is easily centralized.

Monitoring and report generation  ISA Server allows you to monitor its performance and create detailed security and access logs and graphical reports. Report generation can be scheduled, and remote administration lets administrators monitor the use and performance of the ISA server from an off-site location.

E-mail content screening  ISA Server provides for screening of e-mail content by keywords, to allow administrators to implement and enforce strict security policies.

H.323 Gatekeeper functionality  This feature allows for use of videoconferencing software, such as Microsoft NetMeeting, through the proxy, and NetMeeting directory functionality (replacing some of the functionality of ILS).

Enhanced software for use of streaming media  This includes live stream splitting, and caching of Windows Media content (when using Windows Media Server).

Extensibility  Microsoft has built into the software mechanisms to allow developers to write and implement their own security features, such as HTTP application filters that are implemented as “Web filters.” Non-Web Proxy packet inspection can be extended through the implementation of application filters.
Chapter 1 • Defending the Network with ISA Server—and Beyond

In the previous book, we looked in detail at each of ISA’s feature categories, including firewall security, Web caching, Internet connection sharing, unified management, and extensible platform features. For more specific information about all of these, please see Configuring ISA Server 2000 (Syngress Publishing, Inc. ISBN 1-928994-29-6).

ISA Server’s Layered Filtering

Firewall products support the filtering of messages to either allow data to pass through or prevent it from doing so according to specified criteria. ISA Server, when installed in firewall mode or integrated mode, can perform filtering at the packet layer, the circuit layer, or the application layer. Let’s look briefly at how each of these works.

Packet Filtering

Packet filtering does most of its work at the network layer of the OSI networking model (equivalent to the internetwork layer of the DoD model), dealing with IP packets. Packet filters examine the information contained in the IP packet header of a message, and then either permit the data to cross the firewall or reject the packet based on that information. When IP packet filtering is enabled, the ISA server will intercept and evaluate packets before passing them on to a higher level in the firewall, or to an application filter.

The information the packet filter uses to make its decision includes the IP address of the source and/or destination computer(s) and the TCP or UDP port number (the port numbers are in the transport layer header, so technically although packet filtering generally operates at the network layer, it also processes some higher-layer information). Packet filtering allows the data to proceed to the transport layer only if the packet filtering rules allow it to do so. Packet filtering lets you block packets that come from a particular Internet host, or those that are destined for a particular service on your network (for example, the Web server or SMTP server).

Because ISA Server is designed as a security solution, by default enabling packet filtering causes all packets coming into the LAN from the external network interface (the interface connected to the Internet) to be excluded—unless a packet filter, access policy, or publishing rule exists that explicitly allows them. In fact, even if packet filtering is not enabled, ISA Server will not permit packets to enter the internal network unless you explicitly configure rules to permit access.

ISA Server provides administrators with flexibility in configuring packet-filtering behavior. There are two types of static IP packet filters that can be configured:

- **Allow filters** You specify the packet types that should be allowed to pass through the firewall (either incoming or outgoing traffic); all other packets will be prevented from crossing the firewall. For a service to listen on a particular port, you will need to configure a packet filter to allow traffic on that port (unless the port is opened dynamically by a policy or publishing rule).
### Block filters
You configure filters to explicitly block specified ports. Block filters are used in conjunction with allow filters to give you more flexibility and granularity of control over exactly what traffic will be permitted through the firewall.

**NOTE**
If block and allow filters conflict, the block filters will override, thus erring on the side of more security.

Dynamic packet filtering provides higher security because it opens the necessary port(s) only when required for communication to take place, and then closes the port immediately after the communication ends.

**ISA Server Alert**
Note that dynamic packet filtering works only when the packet filter is configured to use the external interface of the ISA server as the local adapter. Dynamic packet filtering does not work when you configure packet filters to allow access to servers on a trihomed DMZ segment.

Packet filters cannot perform filtering based on anything that is contained in the data field of the packet, nor can they use the state of the communication channel to aid in making the decision to accept or reject the packet. If you need filtering decisions made based on either of these, you will need to use filtering that operates at a different layer (circuit or application filtering).

### Circuit Filtering
While packet filtering is a widely used and understood concept for many network administrators, circuit filtering might be less familiar to you. Microsoft’s ISA Server documentation makes scant mention of it, and TechNet contains only a few references to it. In fact, circuit filtering seems to be “lumped in” with packet filtering in most discussions, as if the two were the same.

In fact, there is an important difference, but there’s nothing mysterious or difficult to understand about it: circuit filters simply operate at a higher layer of the OSI model, the transport layer (host-to-host layer in the DoD model). Circuit filters restrict access based on host machines (not users) by processing the information found in the TCP and UDP packet headers. This allows you to create filters that would, for example, prohibit anyone using computer A from using FTP to access computer B.
When circuit filters are used, access control is based on TCP data streams or UDP datagrams. Circuit filters can act based on TCP and UDP status flags and sequencing information, in addition to source and destination addresses and port numbers.

The ISA Firewall service works at the circuit level with most Internet applications and protocols, making them perform as if they were directly connected to the Internet. This is true both for clients that have the Firewall Client software installed, and for those that don’t (the latter being known as SecureNAT clients). If the Firewall client is installed, Internet applications communicate using WinSock. It works a little differently for SecureNAT clients. In this case, circuit-level filtering uses a SOCKS filter to forward requests from SOCKS 4.3 applications to the Firewall service. See the discussion of SOCKS and WinSock later in this chapter.

Circuit-level filtering allows you to inspect sessions, rather than packets. A session is sometimes thought of as a connection, but actually, a session can be made up of more than one connection. Sessions are established only in response to a user request, which adds to security.

Circuit filters don’t restrict access based on user information; they also cannot interpret the meanings of the packets. That is, they cannot distinguish between a GET command and a PUT command sent by an application program. To do this, you’ll have to use application filtering.

Application Filtering
There are times when you might want to filter packets based on the information contained in the data itself. Packet filters and circuit filters don’t use the contents of the data stream in making filtering decisions, but you can do this with application filtering.

An application filter operates at the top layer of the networking model, the (appropriately named) application layer. Application filters can use the packet header information, but are also able to allow or reject packets based on the data contents and the user information.
You can use application filtering to control access based on the identity of the user, and/or based on the particular task the user is attempting to perform. With application filters, criteria can be set based on commands issued by the application. This means, for example, that you could restrict a particular user from downloading files to a specified computer, using FTP. At the same time, you could allow that user to upload files via FTP to that same computer. This is possible because different commands are issued depending on whether the user is retrieving files from the server or depositing them there.

Application gateways are considered by many firewall experts to be the most secure of the filtering technologies. This is because the criteria they use for filtering covers a broader span than the other methods. Sometimes hackers write malicious programs that use the port address of an authorized application, such as port 53, which is the DNS address. A packet or circuit filter would not be able to recognize that the packet is not a valid DNS request or response, and would allow it to pass through. An application filter, however, is able to examine the contents of the packet and determine that it should not be allowed.

Application filtering sounds like the perfect solution to all your security concerns, but there are drawbacks. The biggest problem is that there must be a separate application gateway for every Internet service that you need to support. This makes for more configuration work; however, this weakness is also a strength that adds to the security of the firewall. Since a gateway for each service must be explicitly enabled, you won’t accidentally allow services that pose a threat to your network. ISA Server solves some of these problems through the implementation of “smart” application filters.

Application filtering is the most sophisticated level of filtering performed by the Firewall service, and is especially useful in allowing you to protect your network against specific types of attacks such as malicious SMTP commands or attempts to penetrate your local DNS servers.

**ISA Server Editions**

Microsoft offers ISA Server in two different editions. Either can be installed in one of three different installation modes. We’ll take a brief look at the differences between the two editions and the three modes in this section, to assist you in making the correct choices for your network.

**ISA Standard Edition**

The ISA Server Standard Edition is appropriate for small business networks (or even sophisticated home networks), and for implementation on a departmental basis in larger organizations. This edition works well in a peer-to-peer (workgroup) environment; the Standard Edition is installed on a stand-alone Windows 2000 server or can be installed on a Windows 2000 Server that is a member of a Windows 2000 or Windows NT 4.0.
domain. ISA Server Standard Edition cannot store configuration information in the Active Directory, and it does not require Active Directory.

Nonetheless, the Standard Edition offers the same firewall functionality, Web caching capability, performance, ease of management, and extensibility as the Enterprise Edition. The Standard Edition will support a server with multiprocessor capability as long as it has no more than four processors.

Because it cannot be used as part of an array, the Standard Edition is more limited in terms of scalability. It supports hierarchical caching, as does the Enterprise Edition, but does not support distributed caching. The ISA Standard Edition cannot store policy information in the Microsoft Active Directory, as the Enterprise Edition does.

**ISA Enterprise Edition**

The ISA Enterprise Edition is designed for maximum scalability to the largest, high-traffic enterprise networks. Fault tolerance, centralized management, and multiple level policy application are at the core of the Enterprise Edition’s feature set.

Whereas the Standard Edition supports up to four processors, there is no limit on processor support in the Enterprise Edition. Perhaps more importantly, whereas the ISA Standard Edition is a stand-alone ISA Server only (although the stand-alone ISA Server can be installed on a member server in a Windows 2000 or Windows NT 4.0 domain), the Enterprise Edition allows you to group ISA servers together in arrays to provide fault tolerance and distributed caching, and spread the load of high network traffic across the group of machines. Response time for clients is improved, and if one server in the array goes down, you still maintain ISA functionality.

The Enterprise Edition integrates fully with the Windows 2000 Active Directory, where its configuration and policy information are stored. Using Active Directory, enterprise-level policies can be defined and applied to one or multiple server arrays throughout the enterprise. This is referred to as tiered policy.

Of course, increased functionality comes at a price. The Enterprise Edition is considerably more expensive than the Standard Edition (by several thousand dollars). In determining which edition of ISA Server is most appropriate for your network, you should consider your specific needs and cost/performance factors.

If you have the Enterprise Edition of the software, ISA servers can be installed as members of a server array. The Enterprise Edition can also be installed as a stand-alone server, although it would be difficult to justify the much higher price of the software if you do not intend to use what is perhaps its most important additional feature.

A big advantage of joining multiple ISA servers in an array is the ability to manage them as one entity. All the servers in an array share the same configuration; that is, you only have to configure the array itself—the configuration is then applied to all its members. Because arrays provide for distributed caching capability, performance is enhanced as well.
Fault tolerance is the basis of server clustering. To a limited extent, an ISA Server array functions as a cluster of ISA servers—in the same way Windows 2000 clustering technology causes multiple Windows 2000 servers to act as one entity, so does the formation of an ISA array enable multiple ISA servers to do the same. Also similar to clustering, arrays allow for load balancing of Web Proxy client requests to spread server requests across the group of servers.

**ISA Server Authentication**

In order to gain access to a resource on your network, users must be authenticated; that is, their credentials must be checked to determine that they have the appropriate rights and permissions to access that object. In addition to Windows 2000 authentication required for access, when the user is attempting to access the resource over the Internet, going through an ISA server in firewall or integrated mode that is protecting your network from outsiders, the user might also have to be authenticated by the ISA server.

ISA provides different authentication options, depending on the type of client. The authentication methods available for each client type are as follows:

- **Firewall clients**  Firewall client authentication is automatic; no configuration is required. The user credentials of the requesting user are used.

- **SecureNAT clients**  There is no user-based authentication for SecureNAT clients. Access can be granted or denied based on IP addresses contained in client address sets, but not based on user information.

- **Web Proxy clients**  Client authentication method can be configured. Client authentication is not required by default, but ISA can be configured to require that clients send authentication information. Authentication methods include basic, digest, integrated Windows authentication, or client certificate. It’s important to note that you can never use Kerberos to authenticate with the Web Proxy service. This is specific to Web Proxy service authentication and has no effect on the Firewall service authentication.

As you can see, there are four authentication methods to choose from when configuring settings for Web Proxy clients:

- Basic authentication
- Digest authentication
- Integrated Windows authentication
- Client certificate authentication (does not apply to browser-based Web Proxy clients, but is used in a Web Proxy chaining configuration)
These methods will be familiar to many administrators as the same authentication methods that are used by Internet Information Server (IIS) 5.0, Microsoft’s Web server software that is included with Windows 2000. The authentication method(s) can be configured in the array’s Properties sheet.

Let’s look at each of the authentication methods in a little more detail.

**Basic Authentication**

When you select the basic authentication option for the Web Proxy client access, the user will be asked to provide a username and password before being allowed access. This will be checked to confirm that there is a matching user account on the ISA Server or in a trusted domain.

Be aware that this information is sent in cleartext—no encryption is used to protect the integrity of the credentials. Although the data is a base 64 encoded text string that must be decoded to extract the password in intelligible form, anyone with knowledge of this can decode the information. Obviously, this method is more secure than requiring no authentication at all, but can present a serious security risk because the password is vulnerable to interception by a hacker using a packet sniffer, as it travels over the Internet.

**Digest Authentication**

Digest authentication goes a step further than basic authentication. Although the process is similar, the user credentials are hashed before being sent over the network. Hashing involves applying a mathematical calculation to the binary bits that make up the data being sent. This is a one-way process; that is, it is not possible to take the result of the calculation and reverse engineer it to come up with the original data (the username and password). This, of course, adds a great deal more security to the transaction.
NOTE

To use digest authentication, all members participating in the transaction must be members of a Windows 2000 or .NET domain, and passwords must be saved with reversible encryption.

Integrated Windows Authentication

ISA Server can be configured to use Windows 2000 authentication, which is especially secure because the username and password don’t have to be sent across the network. This eliminates the possibility of interception in transit. There are two protocols that can be used when integrated Windows authentication is selected:

- **Kerberos v5** The default protocol for Windows 2000 domains
- **Challenge/Response** NT LAN Manager (NTLM) authentication

**Kerberos Authentication**

Kerberos is a logon authentication protocol that is based on secret key (symmetric) cryptography. It usually uses the DES or Triple-DES (3DES) algorithm, although with the latest version, Kerberos v5, algorithms other than DES can be used.

Kerberos uses a system of “tickets” to provide verification of identity to multiple servers throughout the network. This works a little like the payment system at some amusement parks and fairs where, instead of paying to ride each individual ride, customers must buy tickets at a central location and then use those to ride the rides. Similarly, with Kerberos a client who wants to access resources on network servers is not authenticated by each server; instead, all of the servers rely on “tickets” issued by a central server, called the Key Distribution Center (KDC).

The client sends a request for a ticket (encrypted with the client’s key) to the KDC. The KDC issues a ticket called a Ticket Granting Ticket (TGT), which is encrypted and submitted to the Ticket Granting Service (TGS). The TGS can be running on the same physical machine that is running the KDC. The TGS issues a session ticket to the client for accessing the particular network resource that was requested (which is usually on a different server). The session ticket is presented to the server that hosts the resource, and access is granted. The session key is valid only for that particular session and it is set to expire after a specific amount of time. Kerberos allows mutual authentication; that is, the identities of both the client and the server can be verified.

For a more detailed explanation of how Kerberos works, see the *Kerberos v5 Administrators Guide* at www.lns.cornell.edu/public/COMP/krb5/admin/admin_2.html.
Remember: Kerberos authentication cannot be used by browser-based Web Proxy clients to communicate with the Web Proxy service. Browser-based Web Proxy clients can only use NTLM to communicate with the Web Proxy service. However, Kerberos can be used in a Hierarchical Web Caching configuration seen when you chain Web Proxy servers. In this case, the downstream ISA server can use Kerberos to authenticate with the upstream ISA server.

**NTLM Authentication**

NTLM is a Microsoft logon authentication method, used by Windows NT domains and supported by Windows 2000/.NET in case “down level” client computers (those running NT or Windows 9x) want to log on to the network. NTLM v2 is the current version, and provides more security than NTLM v1. Version 2 is supported by Windows 2000 and NT 4.0 with SP4 or higher. If the Directory Services client software (which is available on the Windows 2000 Server CD-ROM) is installed on Windows 9x computers, NTLM v2 can be used (however, it is necessary to edit the Registry to enable it).

Unlike Kerberos, when a client wants to access a server’s resources using NTLM, that server must contact the domain controller to have the client’s identity verified. The client doesn’t have credentials already issued (the session ticket in Kerberos) that the file or application server knows it can trust.

**Client Certificate Authentication**

Finally, the Web Proxy client can use Secure Sockets Layer (SSL) for authentication. This involves the use of a client certificate and a server certificate. The server first sends, in response to a client request, a server certificate that provides authentication of the server. If the server requests that the client authenticate itself, the client sends a client certificate to the server.

---

**ISA SERVER ALERT**

It is important to note that a browser-based Web Proxy client cannot establish a secure channel with its ISA Server’s Web Proxy service. Client certificate authentication is used in a Web Proxy chaining setup. The downstream Web Proxy service can present a client certificate to the upstream ISA Server’s Web Proxy service. This allows the downstream and upstream ISA servers to use a secure channel for Web Proxy chaining.

Certificates are digital “documents” that verify the identity of a client or server, and are issued by a trusted third party to which that identity has been satisfactorily proven. The trusted third party is called a certification authority (CA) and can be external (outside
the organization) or internal. Windows 2000 Server provides the ability for companies to set up their own CAs to issue certificates internally. Certificates contain identifying information about the certificate holder.

If client certificate authentication is configured, the ISA server identifies itself as an SSL Web server to the client, by sending a certificate to the client. The ISA server then requires that the client send a valid certificate before access will be granted.

The process of encrypting or decrypting client requests and then passing them on to the Web server to which they are addressed is called **SSL bridging**. This process is used by the ISA server when it initiates or ends an SSL connection. In the Web Proxy chaining configuration, you are actually bridging the HTTP request made by the browser client as an HTTPS connection between the downstream and upstream ISA Server servers. Moreover, if the original request is an HTTP request, the request is again bridged so that the HTTPS message between the ISA servers is bridged as an HTTP message that is sent to the Web server on the Internet.

When a client Web browser requests an S-HTTP (Secure HTTP) object (by default on port 8080, although if you have upgraded to ISA Server from Proxy Server 2.0, it will be 80, and can be any port you want to assign) through the ISA server, a different process is used, called **SSL tunneling**. In this scenario, the client creates a tunnel through the ISA server directly to the Web server on which the requested object resides.

### Installing ISA Server

The actual process of installing ISA Server is usually pretty straightforward. However, it’s absolutely critical that you plan your ISA deployment beforehand. The amount of thought and analysis that you put into deployment planning, especially if you are designing an ISA Server solution for the enterprise, will optimize ISA Server’s performance and minimize the chance of making a critical error that will adversely affect your security or access schemes. In this section, we will discuss:

- Planning and design issues
- Installing ISA Server as a stand-alone
- Upgrading a stand-alone ISA server to array membership
- Installing ISA Server on a domain controller

### Planning and Design Issues

The ISA server is an integral part of your security configuration scheme, and you do not want to just install the server and hope that everything works out right. Carpenters have an old saying: “measure twice, cut once.” If you thoroughly map out your design, you’ll avoid potential problems in the future.
Chapter 1 • Defending the Network with ISA Server—and Beyond

In this section, we’ll focus on planning and design issues as they are relevant to the installation of ISA Server. The primary issues of concern are:

- Network and hardware specifications
- The edition of ISA Server to be installed
- The mode in which ISA Server will be installed
- Stand-alone versus array configurations
- Client configuration requirements
- ISA Server Internet connectivity

You should make firm decisions about each of these ISA Server design issues before you begin your installation. The decisions you make at this point will determine your choices when it comes time to install ISA Server itself. Because ISA can be installed in several different ways for different functionality, there are a number of factors you must take into consideration before you start the installation process. In the following sections, we discuss each of these considerations in more detail.

Network and Hardware Requirements

Before installing ISA Server, you will need to assess what hardware is required to meet the needs of your organization’s ISA Server deployment plan. An organization that has 50 network clients and only chooses to use the Web Proxy service will have very different requirements than an organization with 30,000 network clients that wants to avail itself of all the networking services ISA Server has to offer.

System Requirements

Whether you choose to install one or one hundred ISA servers, each server must meet minimum hardware and software requirements. The minimum requirements for any ISA server—regardless of the role the machine might play on the network—are:

- Windows 2000 Server Family operating system with Service Pack 1 or above installed
- A Pentium II or K7 processor or above running at 300 MHz or faster
- At least 128MB of RAM (Microsoft recommends 256MB of RAM minimum)
NOTE

If you are “hardware challenged” and must use a minimal RAM configuration, you should dedicate the machine to only ISA and not use it for any other services. This includes file sharing and Web services. We recommend that you get as much RAM as your hardware budget allows. You will notice considerable Web cache improvement if the amount of RAM in the machine exceeds the size of your Web cache.

- A minimum of 20MB of disk space for the program files
- A minimum of 2GB of disk space for the Web cache
- At least two network interfaces—one to the internal network and a second to an external network, such as the Internet or corporate backbone (the exception would be an internal server acting as a caching-only server)
- Partitions formatted in NTFS to store the program, log, and cache files
- A Windows 2000 domain if enterprise policies will be implemented

Processor Requirements

The rate limiting factor when it comes to processor requirements can be boiled down to the number of rules per second that the ISA server needs to evaluate. An ISA server with a few rules, but high throughput, might have roughly the same requirements as a machine that has many rules but little throughput through its external interface. Therefore, you can use the speed of the external interface as a guideline for the level of processor support your ISA server requires.

See Table 1.1 to assess your processor requirements.

Table 1.1 Processor Requirements

<table>
<thead>
<tr>
<th>External Interface Data Rate</th>
<th>Processor Requirement</th>
<th>Type of Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 10 Mb/second</td>
<td>Pentium II or K6-3 300 MHz</td>
<td>ISDN, cable, or DSL</td>
</tr>
<tr>
<td>10–50 Mb/second</td>
<td>Pentium III or K7 500 MHz</td>
<td>T3 or comparable</td>
</tr>
<tr>
<td>&gt;50 Mb/second</td>
<td>Pentium III or K7 500 MHz</td>
<td>Real Fast</td>
</tr>
<tr>
<td></td>
<td>Add a processor for each increment of 50 Mb/second</td>
<td></td>
</tr>
</tbody>
</table>

Remember that these recommendations are minimums. Many factors determine hardware needs in a particular environment. For example, one consideration in your disk
space plan is for the log files and reports that will be stored on your ISA server. The log files can grow very quickly, depending on the level of logging you have configured on your server. If you enable packet filtering and detailed Web Proxy service logging, even a small network can easily generate log files in the range of 5 to 10MB per day.

If you are working on larger networks, you can expect your log files to expand at the rate of 50 to 100MB (or more) per day if you carry out detailed logging. It is a good idea to dedicate a partition of at least 1GB to your log files if you plan to carry out even a moderate amount of logging. You will need a month’s worth of log files to create many of the more interesting reports that ISA Server can generate. Moreover, you might want to create reports spanning multiple months, in which case you will need all of the log files available on disk.

**ISA Server Alert**

If you log to a database, make sure you have a large amount of disk space available. The database size will grow even faster than what you see when logging to text files on the local ISA server. You should make at least 10GB available to your ISA logging database.

---

**Network Interface Configuration**

You should have at least two network interfaces if you plan to use the ISA server as a firewall. However, if you want to use the server as a Web-caching server only, you can use a computer with a single, internal network interface.

If you configure multihomed computers, at least one of those interfaces will be directly connected to the Internet or to a network backbone. If you connect directly to the Internet, the interface can be an Ethernet connection (for example, to a DSL or cable modem), ISDN, or analog modem connection. For the internal network interface, you will likely use an Ethernet connection.

If you plan to use a perimeter or DMZ network, that network can be connected to a third interface connected to the ISA server. That interface will be considered an external interface, and should be configured with public addresses.

An ISA server that acts only as a Web-caching server can get by with a single internal network interface. Network clients will send their requests to the ISA server’s internal interface, and the ISA server will forward those requests to its gateway to the Internet. Responses from Internet servers will be returned from the Internet-connected machine to the single-homed Web-caching server, which in turn will return data to the ISA clients.
Installation Modes

Before you install the ISA Server software, you should decide in which mode to install it. There are three choices:

- Firewall mode
- Cache mode
- Integrated mode

In integrated mode, the firewall and caching modes are combined so that you get the benefits of both security and Web access acceleration in one package. When you choose to deploy ISA Server in only one mode or the other (firewall or cache), you should be aware that the feature set differs depending on the mode selected. Table 1.2 outlines which features are available in either or both modes.

<table>
<thead>
<tr>
<th>Available in Firewall Mode</th>
<th>Available in Cache Mode</th>
<th>Available in Either Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server publishing</td>
<td>Web-caching service</td>
<td>Access policy (available only for HTTP in cache mode)</td>
</tr>
<tr>
<td>VPN</td>
<td>N/A</td>
<td>Web publishing</td>
</tr>
<tr>
<td>Packet filtering</td>
<td>N/A</td>
<td>Real-time monitoring and alerts</td>
</tr>
<tr>
<td>Application filtering</td>
<td>N/A</td>
<td>Report generation</td>
</tr>
</tbody>
</table>

Installing in Firewall Mode

Firewall-mode ISA servers support virtually all ISA Server features, with the exception of the Web cache. The Web-caching feature is very memory and processor intensive; therefore, it makes sense to exclude this feature for a server whose primary purpose is to act as a firewall. A firewall should not run extra services to minimize the risk of exposure.

Installing in Cache Mode

When you install the server in cache mode, you intend that server to work as a Web Proxy server only. The Web Proxy service supports the HTTP, HTTPS, FTP, and Gopher protocols. If you want to support only these protocols and take advantage of the Web-caching features, but don’t want to implement a full-fledged policy-based firewall, the Web cache option is a good one.

A cache mode server is best placed on the internal network, in which case you can use a single interface. Be sure that you implement some type of firewall solution at the edge of your network to protect your internal computers from Internet intruders.
Installing in Integrated Mode
The integrated mode ISA server allows you to take advantage of all the features ISA Server has to offer. The ISA server acts as both a firewall and caching/acceleration solution to provide security while enhancing Web performance.

Stand-Alone versus Array Configuration
ISA Server Enterprise Edition can be installed as either an array member or as a stand-alone server. There are many advantages of installing the server as an array member, including:

- The ability to implement enterprisewide array policies via Active Directory
- The ability to implement a common configuration for multiple ISA server computers
- The option to expand the scope of a single ISA server to multiple servers with a common configuration
- Fault tolerance

For an ISA server computer to be installed as an array member, the Active Directory must first be prepared. The procedure for preparing the Active Directory is called enterprise initialization. This is accomplished via the Installation wizard included on the ISA Server CD. You can choose to manually run the ISA enterprise initialization and then install ISA Server a later time. If you choose to install ISA Server in an array configuration, the setup program will check to see if the schema has been properly modified before continuing.

Once the array member is installed, a single enterprise array policy can be implemented on any array in your organization. All arrays are able to access configuration information because the settings are stored in the Active Directory. This is a nice fault-tolerance method for your configuration because the Active Directory is replicated throughout the organization, and there will be multiple copies of your array policies distributed among all domain controllers.

**Note**
If you have the Standard Edition of ISA Server, you won’t have the choice to deploy an array. The Standard Edition is a viable solution for small companies with relatively simple requirements, but is not designed to scale to the needs of complex enterprise networks.
ISA Client Configuration

A critical aspect of your ISA Server design is the ISA Server client base you expect to support. Proxy Server 2.0 supported what were known as the Web Proxy client, WinSock Proxy client, and SOCKS Proxy client. The SOCKS service is no longer required, and the WinSock Proxy client has changed its name.

The client types supported by ISA Server include:

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

Each client type offers its own advantages and disadvantages. Let’s examine these features now and assess how they fit into an overall ISA design plan.

The Firewall Client

Network clients configured as Firewall service clients are able to access all WinSock protocols. When applications on the Firewall client send TCP or UDP requests to the Internet, the Firewall Client software installed on the Firewall client will intercept the request and forward the request to the Firewall service on the ISA server.

The primary advantage of configuring a machine as a Firewall client is that you can control access to protocols, sites, and content on a per-user or per-group basis. This allows you more granular control over your access policies than you have compared to the SecureNAT client. The SecureNAT client cannot control access via user authentication, only via IP address, in a manner similar to the SOCKS service in Proxy Server 2.0.

The disadvantage of configuring a host as a Firewall client is that you must install the Firewall client software. Not all operating systems support the Firewall Client software. The only operating systems that support the Firewall Client software are:

- Windows 95 OSR 2
- Windows 98
- Windows ME
- Windows NT 4.0
- Windows 2000
- Windows XP

This represents a departure from the support that was offered by the Firewall client’s older brother, the WinSock Proxy client. The WinSock Proxy client software provided with Proxy Server 2.0 supported Win 3.x machines using a 16-bit client software.
installation. The Firewall Client software does not include a 16-bit client. Keep this in mind if you have the ill fortune of needing to support Windows 3.x machines.

Another major advantage of using the Firewall client is that it will work with just about every application protocol, even those that will require multiple connections between the client and the server (these protocols are often referred to as “complex protocols”). NAT will not support complex protocols that require secondary connections unless there is an application filter to support the protocol.

ISA SERVER ALERT

If you must support Win 3.x machines, one workaround is to use the WinSock client provided with Proxy Server 2.0. Of course, you must have a copy of Proxy Server 2.0 to implement this solution. You can do this because the Firewall client and the WinSock client are interchangeable.

This means you do not need to install the Firewall client on your machines that already have the WinSock Proxy client installed. You can also use the Firewall Client software to connect to the WinSock Proxy service on a Proxy Server 2.0 server. While the Firewall service on the ISA Server works a bit differently than the WinSock Proxy service on Proxy Server 2.0, the client side essentially works the same. However, we recommend that you install the updated Firewall Client software on all machines that support it. This is especially important if you install ISA Server Service Pack 1. After installing ISA Server Service Pack 1, you should immediately update the Firewall Client software.

The Web Proxy Client

The Web Proxy service provides access to a limited set of protocols, including:

- HTTP
- S-HTTP (SSL secured HTTP)
- FTP
- Gopher

While we can safely dismiss Gopher from our consideration, the other protocols represent the bulk of typical Internet connectivity requirements for the majority of organizations that might want to implement an ISA Server solution.

If all you require are these protocols, a Web Proxy client/server configuration might be the best fit for your organization. Even if you need to install the Firewall Client software to take advantage of other WinSock applications, you might still want to configure your machines as Web Proxy clients because of the performance advantage you’ll gain for Web access via HTTP 1.1 CERN-compliant browsers.
ISA SERVER DEFCON 1

For security reasons, you should completely disable Gopher access from your internal network. There is a security issue related to the Gopher protocol and ISA Server (http://support.microsoft.com/default.aspx?scid=kb;en-us;q323889). You can install the patch or create a protocol rule that blocks the Gopher protocol. Gopher uses TCP port 70.

The Web Proxy client has the advantage of not requiring installation of any dedicated client software. If your browser supports Proxy client configuration, as does Internet Explorer, you can take advantage of direct communication with the Web Proxy service. The Web Proxy service supports user authentication, which gives it an advantage over the SecureNAT client.

The SecureNAT Client

SecureNAT clients require no client software or application configuration, which makes them the simplest client type in terms of setup and deployment. To become a SecureNAT client, all you need to do is:

- Configure the client to use the ISA server as its default gateway, or
- Point the SecureNAT client to a gateway that will be able to route Internet bound packets to an ISA server.

The SecureNAT client is able to take advantage of the Web cache when the HTTP Redirector Application Filter is enabled. However, even though the SecureNAT client is able to use the Web cache portion of the Web Proxy service, SecureNAT clients cannot be authenticated against the Active Directory, Windows NT 4.0’s SAM, or a server’s local security accounts database. Access controls for SecureNAT clients are implemented via IP address rather than user or group membership.

Small organizations that do not have easy access to technical support assistance or those that do not want to install or configure client software will benefit most from the SecureNAT client.

Choosing the Best Client(s) for Your Network

You are not limited to implementing a single ISA client configuration; you can take advantage of various combinations of clients. For example, you can configure an ISA client as a Web Proxy and Firewall client and take advantage of the features provided by both services, or you can configure a client to be a SecureNAT and a Web Proxy client and take advantage of authentication for Web protocols.
Chapter 1 • Defending the Network with ISA Server—and Beyond

The only mutually exclusive client configuration pair is the Firewall client and the SecureNAT client. That is because the Firewall client will always intercept all TCP and UDP communications. There is no way the SecureNAT client configuration will be able to service TCP and UDP requests when the computer is configured as both a SecureNAT and Firewall client. However, the machine configured as a SecureNAT and Firewall client will be able to access non-TCP/UDP protocols via its SecureNAT client configuration.

Internet Connectivity and DNS Considerations
ISA Server supports just about any interface you want to use to connect to the Internet. Your external interface can be:

- ISDN
- Analog
- DSL
- Cable
- T-Carrier
- X.25
- ATM

An important consideration is whether you want to implement a dedicated or a dial-up solution for Internet connectivity. The advantage of a dedicated connection is speed and reliability. The prime disadvantage of dedicated connections is cost. However, even the cost of dedicated connections is coming down. In areas that support cable and DSL connections, you can have a dedicated connection to the Internet for well under $100 US per month.

It is vital that you consider the level of service you require before deciding on what type of connection to use on the external interface. Many businesses seem almost hypnotized by the low prices and potential for high-speed access that DSL and cable connections offer. However, those businesses are often left grinding their teeth and cursing their providers.

Here’s the problem: You are not usually guaranteed bandwidth or level of service with these types of connections. Although you typically purchase a certain level of service based on the optimal down and up speeds provided by the interface, those numbers define upper limits of service more often than they guarantee a minimum level of service. Currently, both cable and DSL should not be considered reliable enough on which to base your corporate Internet solution. They are more “rich man’s hobbies,” to quote a well-heeled DSL engineer we know.
If your business requires a reliable and dedicated connection to the Internet, in our experience you will be best served by using established technologies such as T-carrier and ISDN. Although the cost of these connections is much higher, you won’t have to worry about the connection being unavailable.

**NOTE**

Some telephone companies and cable companies offer a “business level” of service that provides more guarantee of reliability than consumer service packages (and consequently costs more). However, from our experience, there is no significant improvement in reliability. The primary advantage of these types of packages is that you get a dedicated IP address. Dedicated IP addresses are mandatory if you want to implement server publishing scenarios. At the time of this writing, Microsoft is moving away from official support for server publishing on interfaces that do not have dedicated IP addresses.

**Gathering Information for the Installation**

The installation process will proceed more smoothly if you gather the answers to the following questions before beginning to install ISA Server:

- Where are the installation files that you will use to install ISA Server?
- Do you have appropriate permissions to install ISA Server?
- What is the CD key, and where is the product license?
- Will the Active Directory schema need to be updated?
- What server mode will you use?
- Where will you store the program files, log files, and Web cache?
- What are the network IDs for the hosts on your internal network?
- What ISA features do you want to include in your installation?
- Will you be creating or joining an array?

In the following sections, we will look more closely at each of these questions.

**Installation Files**

You can access the installation files either from the product CD-ROM or from a network installation share point. If you are installing from a share point, make sure that the Share and NTFS permissions at the source allow you to install the program.
Chapter 1 • Defending the Network with ISA Server—and Beyond

Permissions
You must be logged on with an account that has permission to install the program. If you are installing a stand-alone ISA server, you must at least be a member of the Administrators group for that machine. If you want to install an enterprise array, you must be a member of the Domain Administrators group. If you have a multiple forest environment, you should be a member of the Enterprise Admins group, and if you are responsible for initializing Active Directory, you also have to be a member of the Schema Admins group.

CD Key and Product License
The 10-digit CD key is located on the CD case. You might also find it on the product packaging. Have the license readily available, photocopy or scan it, and then put it in a safe place.

NOTE
Having multiple copies of your product licenses and storing them in a safe, centralized location is an important part of your fault tolerance plan. Doing this will save you a lot of grief if your company should become the subject of a software audit.

The number of processors determines how much you’ll pay for licensing ISA Server, because the licensing fees are based on the number of processors on the server. Since the costs can increment significantly for a multiprocessor machine, you might consider installing ISA Server on a system with a single processor, and then carrying out performance monitoring to aid you in making a cost/benefit analysis of a multiple processor solution.

Table 1.3 contains the pricing structure for ISA Server production licenses at the time of this writing.

Table 1.3 Production Licensing Structure for ISA Server

<table>
<thead>
<tr>
<th>ISA Server Version</th>
<th>License Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISA Standard</td>
<td>$1499.00 US per CPU</td>
</tr>
<tr>
<td>ISA Enterprise</td>
<td>$5999.00 US per CPU</td>
</tr>
</tbody>
</table>
NOTE

Production licenses are required for ISA servers that will be part of a production network. Development licenses can be obtained through MSDN, and special pricing applies to Application Service Providers (ASPs). Call your Microsoft representative for more details on special pricing structures.

Active Directory Considerations

If you plan to install an enterprise array, the machine onto which you are installing ISA must be a member of a domain. You will also need to be able to connect to a domain controller during the installation. Confirm network connectivity to a domain controller before beginning the installation.

As mentioned earlier, when you perform an enterprise initialization, you will be altering the Active Directory so that it can store array configuration information. Remember that in a Windows 2000 domain, alteration to the schema is a one-way process, and you cannot go back and restore the schema to its previous state.

NOTE

This situation is improved on Windows .NET domains. If you run a Windows .NET domain, you will be able to make changes to the schema and reverse them if you need to.

Server Mode

Decide in advance what server mode you will assign to the ISA server—cache, firewall, or integrated. The decision should be arrived at after conferring with your security group and determining exactly what function(s) this ISA server will perform on your network.

Disk Location for ISA Server Files

Determine where you want to install the ISA Server program files. These files will only require about 20MB of disk space and do not incur much read/write activity, so you will usually be safe installing them to the default location, which is in the Program Files folder on the boot partition.

You will also need to decide during installation where you want to place your Web cache files. It is best to place these on a RAID array formatted as NTFS (if available). The RAID and NTFS configuration will ensure the best performance possible.
NOTE

RAID 0 provides the highest performance. There’s no reason to use parity in your Web Caching file array since the information in the Web cache can be built up again in a short time. However, if you use a parity array, you can save some bandwidth by not requiring the cache to be built up again.

Although you will not need to decide where to put your log files during installation, you should have your server configured so that you can adjust the configuration to put the logs on their own partition if possible, and set it up so that the partition is a RAID 5 volume separate from the one on which you have the Web cache file located.

By default, the log files are placed on the boot partition, but after installation is complete, you will be able to change the location via the ISA Administration console.

Internal Network IDs and the Local Address Table

You will be asked to configure the Local Address Table (LAT) during the installation routine. To prepare the LAT correctly, you need to know what network IDs are in use inside your company. The LAT is used to determine if requests should be sent directly to an internal server, or if they should be subjected to ISA Server rules and policies. Never place the IP address of the external interface of the ISA server in the LAT.

ISA Server Features Installation

A few services are treated as “add-in” services by the ISA Server installation routine. You will want to determine beforehand whether you need to install these services as part of your ISA Server deployment. These optional services are:

- The H.323 Gatekeeper Service
- The Message Screener
- The H.323 Gatekeeper Administration Tool

The H.323 Gatekeeper allows multiple inbound and outbound calls using a program such as NetMeeting to conduct voice, video, and data sessions. The H.323 Administration tool allows you to administer the service. Thus, if you install the service, you should install the tool as well.

NOTE

As part of the installation routine, the ISA Server setup will change the TCP/IP driver’s dynamic port range. It will be increased to 65,535 (the effect takes place when the computer is rebooted after installing).
The Message Screener is a tool you use together with secure Mail Server publishing. The Message Screener tool allows you to check incoming mail for a number of elements, such as keywords. If you plan to implement secure Mail Server publishing, you should install this tool.

Addressing Special Installation Issues
For detailed guidance on planning and installing ISA Server with different network configurations, check out Microsoft’s *Installation and Deployment Guide*, which is available on the ISA Server installation CD. If you are migrating to ISA Server from Microsoft Proxy Server, you should first read the *Migrating from Microsoft Proxy Server 2.0* document that is also included on the CD.

Pre-Installation Checklist
Before starting the installation, you should perform the following tasks:

1. Ensure that Windows 2000 Server is installed on your ISA Server machine, including the most recent service pack. At a minimum, you must install W2K Service Pack 1 before you install ISA Server.

2. Configure the server that will be hosting the ISA Server installation. Check out the article on www.isaserver.org by Jim Harrison, *Configuring ISA Server Interface Settings*, which will walk you through the setup of your ISA Server machine’s network adapters. Detailed instructions for such security measures as disabling File and Print Sharing on the external interface are included in this article as well.

3. Figure out what your internal network will encompass, both presently and in the future, concerning IP addresses. If the addressing scheme is complex, write down the addresses. You will need this information again later.

4. If your internal network contains more than one range of IP addresses (for example, 192.168.x.y and 10.x.y.z), you need to create the routing table on the server that is to be the ISA server, via the command shell `route` command (if you only have one address range, Windows will do this for you). To prevent problems later, be sure to view the routing table before installing ISA Server to make sure it’s correct.
For more guidance on planning the ISA Server setup, check out two articles on www.isaserver.org by Tom Shinder and Jim Harrison, *Designing an ISA Server Solution on a Simple Network* and *Designing an ISA Server Solution on a Complex Network*. Both of these articles can be found in the Learning Zone at www.isaserver.org.

**Installing ISA Server in a Stand-Alone Configuration**

In this section, we will go through each step required to install ISA Server as a stand-alone server on a Windows 2000 Advanced Server computer. Later, we will perform the enterprise initialization and upgrade the stand-alone server to an array member.

We begin the installation by placing the installation CD into the CD-ROM drive. The autorun begins and we are presented with the installation options screen, as shown in Figure 1.1.

*Figure 1.1 Setup Allows You to Choose the Option of Installing ISA Server*

Note that you have six options:

- **Review Release Notes** Select this option to read the latest information about ISA Server that did not make it into the help files. We highly recommend that you read this first. If you don’t want to read it right away, you should at least print it. It will contain important information that you must know before beginning the configuration phase of the ISA Server.

- **Read Installation Guide** The installation guide is a pared-down version of the help file. This guide focuses on the concepts that are important to the planning, installation, and basic configuration of ISA Server. You should also print this and read it at your leisure.

- **Register ISA Server** Use this link to register your server online.
Defending the Network with ISA Server—and Beyond • Chapter 1

- **Run ISA Server Enterprise Initialization** Use this link to prepare the Active Directory for configuring an ISA Server array.

- **Install ISA Server** This option begins the installation of ISA Server.

- **Read About Migrating to ISA Server** This link opens a document that provides information about how to upgrade from Proxy Server 2.0 and Windows NT 4.0 installations that have Proxy Server 2.0 installed on them.

The following steps walk you through the process of installing ISA Server:

1. Click on the **Install ISA Server** option. The “Welcome to the Microsoft Security and Acceleration Server 2000 installation program” dialog box will appear. The information screen informs you that you can only install the product on one server, if that’s the license you have. Be aware of the different licensing guidelines for ISA Server Standard Edition and Enterprise Edition. Click **Continue**.

2. Next, you will be prompted to enter your **10-digit CD key** from the ISA Server CD case. Do so and click **OK**.

3. After entering the **CD Key** you will get your product ID number. This is the number that you must provide to Microsoft Product Support Services if you want to get any technical assistance from them. Take a screen shot of this dialog box, write down the product ID number, and put it in a safe place. Make multiple copies so that they’re always available. Click **OK** to move to the next step.

4. The next screen will show the End User License Agreement (EULA). You must click **I Agree** to continue the installation process.

5. Next, you must choose an installation option from the following:

   - **Typical Installation** Installs all the components on the boot partition and does not include the “add-on” products. The add-ons can be installed later if you choose not to install them at this time.

   - **Full Installation** Includes all the basic installation files and the add-on products, and will install them to the boot partition.

   - **Custom Installation** Allows you to choose which components you want to install in a granular fashion.

   - **Change Folder** Allows you to change the location of the core program files. If you do not want to install the program to the Program Files folder on the boot partition, click **Change Folder** and change the location of the core program files. For this walkthrough, we will click **Custom Installation**.
6. When you select the custom installation, a dialog box appears that allows you to choose the components to install. There are three options, as shown in Figure 1.2.
   - ISA Services
   - Add-in services
   - Administration tools

   You must install the ISA Services. However, you can customize your selections for Add-in services and Administration tools.

   **Figure 1.2 Selecting Which ISA Components to Install in a Custom Install**

7. If you select Add-in services and click Change Option, the dialog box in Figure 1.3 appears. Make your selection(s) and click OK.

   **Figure 1.3 Installing the H.323 Gatekeeper and/or the Message Screener as Add-In Services**
8. The Administration Tools selection allows you to install the Administration Tools and/or the H.323 Gatekeeper Administration Tool as shown in Figure 1.4. If you are installing the full product on the server, you will want to install the Administration Tools. You can also choose to install just the Administrative Tools on a Windows 2000 Professional computer and administer any server or array in your organization. If you choose to install the H.323 Gatekeeper Administration Tool, it will place a node in your ISA Administration console that will allow you to configure the H.323 Gatekeeper service. Make your selection(s) and click OK.

Figure 1.4 Selecting the Administration Tools

9. If this is the first ISA server to be installed in an array and you have not yet run the Enterprise initialization tool, you will now see a dialog box that informs you that the computer cannot join an array until it is part of a Windows 2000 network and the ISA Server schema is installed in Active Directory. You are notified that continuing the installation will install ISA Server as a stand-alone server. Click Yes to continue the installation in stand-alone mode.

10. The next dialog box asks you to choose the server mode: firewall, cache, or integrated. To use both the security and acceleration features of ISA Server, select the Integrated mode option and click Continue (you are also given an option to exit setup at this point, or to request help with selecting the appropriate mode).

11. A notification box will tell you that Setup is stopping the IIS Publishing service (W3SVC), and that after setup completes, you should uninstall IIS or reconfigure all IIS sites not to capture ports 80 and 8080. The service must be stopped to continue the installation, but will be restarted by the end of the installation. Click OK.
The next step is to configure the Web cache settings, as shown in Figure 1.5. To enable the Web cache, you must place a check mark in the **Enable caching** check box. You are also presented with a list of drives that can support the Web cache. You must place the cache on an NTFS drive. FAT partitions or volumes will not appear on the list. The default setting is to create a 100MB Web cache file on the partition that has the most free disk space. After you enter the size of the cache, you must click **Set**. After you have made these settings, click **OK**.

The Local Address Table (LAT) configuration dialog box appears next, and provides you a chance to configure the LAT during setup, as shown in Figure 1.6. If you choose not to configure the LAT at this time, or if you change your mind regarding the configuration of the LAT, you can change the settings via the ISA Server Administration Console after the installation is complete. After configuring the LAT, click **OK**.

Implications of Running IIS on an ISA Server Computer

We recommend that you avoid running IIS services on the ISA Server computer at all costs. The reason for this is that each IIS service opens a potent portal of attack for Internet criminals to take advantage of. This is especially true for the IIS WWW service. The only time you should run the WWW service on the ISA server is if you are forced to do so by your employer. You should explain to the individual who insists that you run a Web server on the ISA server itself that this is a dangerous configuration and that if at all possible, the Web server should be removed from the firewall.

If you must install a Web server on the ISA server, you should disable IIS socket pooling. IIS socket pooling is applied to all IIS services, and allows the IIS services to host multiple virtual servers and conserve system resources. However, socket pooling was not designed for multihomed machines running as firewalls. When socket pooling is enabled for a service, the service listens on **all interfaces**. This can create port contention issues when you try to publish services on the internal network.

For more information on socket pooling and how to disable it, check out Tom Shinder’s article *The Misery of IIS 5.0 Socket Pooling* at www.isaserver.org/shinder.
Figure 1.5 If You Enable Caching, You Must Set the Drive(s) and Maximum Size for Each Cache

![Configure Caching Drive and Size](image)

Figure 1.6 Configuring the LAT During Setup

![Configure LAT](image)

Configuring & Implementing...

**Configuring the LAT**

There are two ways that you can approach configuring the LAT. You can manually enter the start and end addresses in the **Edit** frame on the left side of the dialog box, or you can use the **Table** button.

When manually entering the information, you can include the entire range of your network IDs. Note that we have entered an illegal address for the start address for the LAT. This is fine and will not impair the functionality of the LAT.

If you choose to use the **Table** button, ISA Server will try to create the LAT for you based on the network ID of your internal interface. In addition to the network ID of your internal interface, it will also add the three private network ranges:

Continued
14. Next, you will be given the choice to launch the Getting Started wizard to configure array and enterprise policies. If this is your first time installing ISA Server, we recommend that you let the wizard walk you through the steps. To do so, ensure that **Start the ISA Administrator Getting Started Wizard** is checked, and click **OK**.

15. The **Getting Started** welcome screen, shown in Figure 1.7, is presented as the ISA Administration console is opened. You can use the wizard to help walk you through the steps of configuring the server. However, you should have a thorough understanding of ISA Server and all the implications of the settings you create before you work with the Getting Started wizard. Once you have a firm understanding of ISA Server, the wizard might help you configure your server in an orderly fashion.

*Figure 1.7 You Can Use the Getting Started Wizard to Configure the ISA Server*

- 192.168.0.0/24
- 172.16.0.0/12
- 10.0.0.0/8

If you choose to let ISA Server construct the table for you, be sure to check it over very carefully. If you have a network with multiple logical IP segments, you will need to include all of these segment IDs in your LAT. Otherwise, requests for those internal network clients will be subjected to the rules created for requests for external network requests.
NOTE

It is a best practice to use only the minimum required subnets in the LAT. Therefore, you should obtain the LAT configuration from the routing table of the internal interface.

The stand-alone ISA server is now installed. In the next section, we will show you how to upgrade your stand-alone server to an array member.

Upgrading a Stand-Alone ISA Server to an Array Member

You must have a Windows 2000 domain deployed and available if you want to make the server a member of an enterprise array. The computer on which you want to perform the upgrade will need to be a member of the Windows 2000 domain.

NOTE

If the machine is a member of a Windows NT 4.0 domain, the enterprise upgrade will not work because the Windows NT 4.0 domain controller does not have the Active Directory in which to store the enterprise array configuration information.

The first step, if you are creating a new array, is to initialize the enterprise.

Performing the Enterprise Initialization

Before you promote your stand-alone server to an array member, you need to complete the enterprise initialization. This is the process of updating the Active Directory schema so that it will support the ISA Server array configuration information. There are two ways you can perform the initialization:

- From the Startup Installation screen.
- From the ISA Server installation files, in the i386 directory, run the msisaent.exe application.

The same steps are involved regardless of which method you choose. In the following walkthrough, we will start the initialization from the Startup Installation screen.

1. When you put the CD-ROM in the drive, the autorun feature will bring up the same dialog box you saw in Figure 1.1. You can also get it to run by
clicking on the `isaautorun.exe` file in the root of the installation files hierarchy. To run the enterprise initialization, click on the Run ISA Server Enterprise Initialization icon.

2. The next dialog box will inform you that the ISA Server schema is about to be installed to Active Directory, and warns you that the action is not reversible. You are asked if you want to continue. Click Yes to do so.

3. Next, you will be asked how you want to apply enterprise policy, as shown in Figure 1.8. When you choose to use Array Policy Only, an enterprise policy will be created, but it will not be automatically applied to the array. You will have the opportunity to manually assign an enterprise policy to the array after the initialization is completed by configuring it in the ISA Management console. When you choose Use this enterprise policy, a default policy is created with the name Enterprise Policy 1. You can change the name if you wish. If you select this option and do not select the Also allow array policy, any array policies will be replaced by the enterprise policy. If you are thinking of choosing this option, be sure to back up your existing array policy prior to the enterprise initialization in the event that you want to restore the existing array policy (stand-alone policy as well) on the server. If you choose the Also allow array policy option, both the enterprise policy and the array policies will be applied. However, array policies can only further limit the policies set for the enterprise. What this means is that an array policy cannot have any allow rules. The only allow rules will be those determined by the enterprise policy. The Also allow publishing rules to be created on the array option does exactly that. Publishing rules must be created on each server of an array separately, because the IP address(s) listening for requests for a published server will be different for each server. If you do not choose this option now, you can do so after the enterprise is initialized and you promote the stand-alone server to an array. The Use packet filtering on the array enforces packet filtering on the array(s) to which this policy is applied. This forces packet filtering and cannot be overridden by an array policy.

**NOTE**

As indicated on the interface, the Also allow array policy option only allows you to create policies that are more restrictive than the Enterprise policy. The Use array policy only option allows you to create Web-caching arrays but avoid the use of enterprise policies. If you find enterprise policies difficult to work with, you can leverage the power of caching arrays while avoiding the somewhat cumbersome enterprise policy configuration issues.
4. After you make your selections in the previous step and click **OK**, you will see a notification box telling you to wait while Setup installs the ISA Server classes and properties in Active Directory. When the process is finished, another box will appear, advising you that ISA Server enterprise initialization successfully imported the ISA schema into Active Directory and you can now install ISA Server as a member of a domain array. Click **OK**.

**NOTE**

If there were problems with updating the Active Directory, you will receive an error dialog box and you will have to troubleshoot problems with Active Directory and perhaps connectivity. After updating the Active Directory to support your array, you can begin the process of promoting your stand-alone ISA server. Before promoting the server, confirm that you have connectivity with a domain controller in your Windows 2000 domain. You might also want to back up your configuration if you have not yet done so.

5. To promote the stand-alone ISA server to an array member, first open the **ISA Server MMC**. Right-click the **array node** in the left pane and select **Promote…**, as shown in Figure 1.9.

6. A notification box will inform you that you are about to promote the server to an array, and that the operation is not reversible, as shown in Figure 1.10. You will be asked if you want to continue. Click **Yes** to do so.

7. Now the promotion process will begin. Several things happen during the promotion, and you’ll be informed of these events in the **Promoting array** dialog box, shown in Figure 1.11. These steps include:
Chapter 1 • Defending the Network with ISA Server—and Beyond

- Converting a stand-alone server to an array
- Storing configuration in the Active Directory
- Stopping all services
- Committing changes
- Restarting all services
- Refreshing array list

**Figure 1.9** Use the ISA Server MMC to Promote the Stand-Alone Server to an Array Member

**Figure 1.10** You Will Be Informed that the Promotion to Array Is Not Reversible

**Figure 1.11** The Dialog Box Will Change as the Promotion Process Advances
After the promotion process completes, the Array Properties dialog box will show the type as “Domain,” as shown in Figure 1.12. Before promotion, the type is shown as “Standalone.”

**Figure 1.12 The Array Properties Box Showing the Type as “Domain” After the Promotion**

The Properties box will also have a new tab, Policies, that is used to configure how the array will use enterprise policies that you have configured.

**Installing ISA Server on a Domain Controller**

A common problem that we’ve encountered while supporting ISA Server users is that of installing ISA Server on a domain controller. In general, it is not recommended that you install ISA Server on a domain controller; however, this is a common issue for those who use Small Business Server (SBS) and must run all the SBS servers on a single machine.

Many of the problems that occur with this configuration are related to interface and DNS configuration. If you have only a single server, it will need to be configured as a DNS server in addition to the other Server services it is running, because an Active Directory DC needs a DNS server to add AD-related entries.

Another problem is that the ISA Server must be multihomed. Multihomed domain controllers have a number of issues, including problems with NetBIOS and the Browser service.

Despite the problems, many users have successfully installed and used ISA Server on a Windows 2000 domain controller. For detailed information on how to ensure that
ISA and your domain controller can peacefully coexist, see the article titled *Installing ISA Server on a Domain Controller* by Tom Shinder at www.isaserver.org/pages/articles.asp?art=17. We will expand on this information in Chapter 5, “Defense Plan 4: Advanced Server Publishing”. For detailed instructions on how to get Outlook Web Access to work with ISA using Small Business Server 2000, including a “how to” on disabling socket pooling, see the article entitled *OWA and ISA Server* by Martin Grasdal at http://infocenter.cramsession.com/techlibrary/gethtml.asp?ID=1107.

**Selecting the ISA Server Client**

There are three types of clients supported by ISA Server:

- **Firewall clients** Computers with the Firewall Client software installed and enabled.

- **SecureNAT clients** Computers that are ISA server clients but do not have Firewall Client software installed.

- **Web Proxy clients** Refers to client Web applications that are configured to use ISA Server.

By definition, a SecureNAT client cannot also be a Firewall client for TCP and UDP requests. On the other hand, both Firewall clients and SecureNAT clients can also be Web Proxy clients. Then, if the Web Proxy client configuration cannot handle a particular request, the Firewall and/or SecureNAT client configuration can step in. The Firewall client is the only client type that requires you to actually install client software on the client computer; however, you must configure the client machine’s Web browser to make it a Web Proxy client. See Table 1.4 for a comparison of the three client types.

<table>
<thead>
<tr>
<th>Firewall Client</th>
<th>SecureNAT Client</th>
<th>Web Proxy Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports WinSock applications</td>
<td>Requires application filters for multiconnection protocols</td>
<td>Supports the HTTP, S-HTTP, FTP, and gopher protocols</td>
</tr>
<tr>
<td>Only works on Windows operating systems</td>
<td>Works on all operating systems with TCP/IP installed</td>
<td>Works on all operating systems, via a Web browser</td>
</tr>
<tr>
<td>Supports user-level authentication</td>
<td>Does not support user-level authentication</td>
<td>Supports user-level authentication</td>
</tr>
</tbody>
</table>
Firewall Client

ISA Server’s Firewall client is equivalent to the WinSock Proxy client in Proxy Server 2.0; it is used for applications such as RealAudio, Windows Media, IRC, Telnet, and any other Internet service that is written to the WinSock application programming interface (API).

The Firewall Client software can be installed on any 32-bit Windows operating system, including the following:

- Windows 95 OSR2 (also known as Windows 95b)
- Windows 98
- Windows Millennium Edition (ME)
- Windows NT 4.0
- Windows 2000
- Windows XP

These are the only operating systems in current release at the time of this writing that will run the ISA Firewall Client software. The Firewall client is automatically enabled when installation is completed.

Installing the Firewall client writes a log file on the computer to which the software is installed. This file has setup information that includes such useful information as which services were running during installation and what client applications were installed. The log file is helpful in troubleshooting problems that you encounter during installation. Note that if you reinstall the Firewall Client software, the log file will be overwritten.

The Firewall client uses a LAT, which is installed to the hard disk of the client computer (in Program Files\Microsoft Firewall Client). The LAT file is named Msplat.txt. The LAT is used to determine whether a request made by a WinSock application should be sent to the ISA server or directly to the computer on the internal network. The LAT defines addresses that are “trusted” by the ISA server. Communications between trusted hosts are not screened by the ISA server. When the Firewall client computer calls another computer on the LAT, the communications do not go through the ISA server.

The primary advantage of the Firewall client is that it allows you to apply access policies to authenticated users, rather than just to computer IP addresses. Users who are authenticated via NTLM or Kerberos can have specific rules, such as bandwidth limitations, applied to their user accounts. This is the best reason for using the Firewall client instead of SecureNAT. Another compelling reason to use the Firewall client is that you can use a much wider range of protocols. The SecureNAT client is limited to simple
protocols, and those protocols must be listed in the Protocol Definitions node of the ISA Server Management console. The only exception to this SecureNAT client limitation is when there is an application filter in place to support the SecureNAT client’s access to complex protocols.

Once installed, the Firewall client can be configured to automatically detect the ISA server, as shown in Figure 1.13.

**Figure 1.13 The Firewall Client Can Be Configured to Automatically Detect the ISA Server**

**SecureNAT Client**

Any computer configured with a default gateway capable of routing Internet bound requests through the internal interface of the ISA server is a SecureNAT client. Although these computers will not be able to benefit from all the features of ISA without the Firewall client software, they can still use most of its access control features. SecureNAT clients do not, however, support user level authentication or complex protocols (without an application filter).

SecureNAT clients can ping external addresses (those on the other side of the ISA server), while computers configured only as Firewall clients cannot.

You do not have to install any special software on the clients to make them SecureNAT clients. However, you do need to configure their TCP/IP settings.

If your network setup is simple (that is, if there are no routers between the client computers and the ISA server), you should set the default gateway to be the IP address of your ISA Server machine. The default gateway is the “way out” of the internal network; it is the address to which packets are sent if their destination address is not on the local subnet. Thus, all Internet traffic will go to the ISA Server machine, which will then forward the requests out over the Internet (assuming the packets are not rejected because of ISA’s packet, circuit, or application filtering rules).
You can either configure the SecureNAT clients’ TCP/IP settings manually or you can use the Dynamic Host Configuration Protocol (DHCP) to assign the clients their IP addressing, subnet mask, and default gateway information. If you use DHCP, you must select the **Obtain an IP address automatically** check box on the **TCP/IP Properties** sheet.

If your network is larger and more complex and there are routers between the SecureNAT clients and the ISA server, the default gateway settings on the clients will be configured with the IP address of the router on the local subnet. In this situation, the router must be configured to route Internet bound traffic to the ISA server.

Other TCP/IP settings, such as the DNS server settings, depend on whether the clients will be requesting data from Internet servers only, or will also be requesting data from internal servers. If the former, you can use the IP addresses of DNS servers on the Internet; otherwise, a DNS server on the internal network, configured to resolve both internal and external IP addresses, should be used.

**Web Proxy Client**

We mentioned earlier that a computer can be a Web Proxy client at the same time it is a Firewall client or a SecureNAT client. The requirements for a Web Proxy client are:

- The client must have a CERN-compatible Web browser installed.
- The Web browser must be configured to use the ISA server.

A request for Web objects sent from a Web Proxy client will be directed to the Web Proxy service on the ISA server. The Web Proxy service will determine whether the access is allowed, and might retrieve the requested object from cache (if it is there) or cache the object when it is returned from the Internet.

There are two ways to configure the browser to use ISA Server’s Web Proxy service. If the Web Proxy client has the Firewall client software installed, the Web browser settings can be configured automatically during the setup of the Firewall client.

If the client isn’t automatically configured, you can manually configure the browser settings to use the Web Proxy service. If you’re using Internet Explorer, this is done via the **Tools | Internet Options | Connections setting**. You only have to check a check box (**Use a proxy server**) in the **LAN Settings** property sheet, and enter the name of the ISA server or array and a valid port number (the default for ISA Server is 8080). The SecureNAT client will use the Web Proxy service regardless of whether you have configured the CERN-compliant settings in the browser (because the default HTTP Redirector settings forward requests to the Web Proxy service), so you might wonder if making these settings is unnecessary. We highly recommend that you configure your SecureNAT client’s browsers as Web Proxy clients. This will allow user/group access controls for site and content rules. With user/group access controls for site
and content rules, you will be able to control what sites users and/or groups can access and what types of files users and/or groups can access via the Web Proxy service.

**NOTE**

CERN stands for “Conseil Europeen pour le Recherche Nucleaire” in French, or the European Laboratory for Particle Physics. Although most of the laboratory’s work is devoted to research in nuclear physics, CERN played a pivotal role in developing the World Wide Web, and setting standards that resulted in the spectacular growth that made it the global forum it is today. The most popular Web browsers, including Microsoft Internet Explorer and Netscape Navigator/Communicator, are compatible with the CERN standards.

---

**Getting Started with ISA Server**

Microsoft has thoughtfully provided a Getting Started wizard to walk you through many of the ISA configuration processes. Tasks for which you can use the wizard include:

- Creating client address sets
- Configuring packet filters
- Creating destination sets
- Configuring protocol rules
- Configuring site and content rules
- Applying server security
- Creating dial-up entries
- Configuring firewall and Web routing rules
- Configuring firewall and Web Proxy clients
- Creating cache policy

The wizard is accessed by clicking the top node in the **ISA MMC** (named Internet Security and Acceleration Server) when in Taskpad view, as shown in Figure 1.14.
NOTE

Most ISA administrators seem to find the Advanced view most useful for day-to-day ISA administration, so you might want to change from Taskpad to Advanced view after completing the wizard. To change the view, click the View menu at the top of the MMC and select the desired view.

You can make changes later to the settings that you make with the wizard.

Setting Up Open Access for Testing the ISA Installation

In the following sections, we will address the most common issue that comes up when ISA users first deploy the product: how to set up “open access” in order to determine whether ISA is working, that is, whether you still have Internet connectivity after installing ISA. The tasks involved include opening all of the packet filters, sites and content, and protocols.

ISA SERVER ALERT

The “open access” configuration is used for testing. Because all protocols, sites, and content are available to the network’s internal clients, this is not a secure configuration and should not be run on your production network, as it defeats the purpose of ISA Server. We recommend that during testing, the ISA server, along with one test client, be disconnected from the rest of the internal network. We also strongly recommend that you turn off IIS on the ISA server before opening access for testing.
Disabling Packet Filtering
Packet filtering is a powerful tool that you can use to protect your ISA Server computer from attack. However, packet filtering interferes with running applications and services on the ISA server itself. If you want to use applications on the ISA server (such as POP3 and SMTP applications), you need to create individual packet filters for them. This can be time consuming if you’re doing a simple proof-of-concept testing configuration. You can disable packet filtering and make all applications on the ISA server able to access the Internet.

Follow these steps to open all packet filters and create an open access policy for all applications on the ISA server itself:

1. In the left pane of the ISA MMC, expand the Access Policy node.
2. Right-click the IP Packet Filters node and click Properties.
3. In the IP Packet Filters Properties dialog box, remove the check mark from the Enable packet filtering check box.
4. Click Apply. Allow ISA Server to restart the services. Click OK to leave the IP Packet Filters Properties dialog box.

NOTE
Because this configuration opens the test network to attackers, make sure your ISA server and test client computer behind the ISA server are not connected to the production network. You should also ensure that IIS services are not enabled on the ISA Server computer.

Allowing All Sites and Content
The next step in configuring ISA for open access is to create a rule that will allow access to all sites and all the content on those sites (if there isn’t one already). To do so, follow these steps:

1. In the left pane of the ISA MMC, right-click the Site and Content Rules node, select New, and then select Rule. This will invoke the New Site and Content Rule wizard.
2. The first page of the wizard asks you to name the rule. Again, choose a name that describes its function (such as “Allow All”). Click Next.
3. On the next page, you are asked to select the type of action the rule will perform. Click the Allow option. Click Next.
4. On the next page, you are asked to specify whether the rule will apply to destinations, schedules, clients, or all three, or whether to create a custom configuration. Click the **Custom** option. Click **Next**.

5. On the next page, you must select destinations to which the rule will apply. Select **All destinations** in the drop-down box. Click **Next**.

6. On the next page, you must select a schedule for applying the rule. Select **Always** in the drop-down box. Click **Next**.

7. On the next page, you must specify the types of clients to which the rule will be applied. Click the **Any request** option. Click **Next**.

8. On the next page, you must select the types of content to which the rule will be applied. Select the **Any content type** option. Click **Next**.

9. The last page of the wizard summarizes your choices. Verify that they are correct and click **Finish** (or click **Back** to make changes).

The new site and content rule will appear in the right pane of the MMC.

---

**Opening All Protocols**

The third and last task you must perform to create your open access configuration is to create a protocol rule that will allow all protocols to pass through.

---

**NOTE**

Creating a protocol rule will allow Firewall clients access to all allowed protocols, but SecureNAT clients will have access only to those protocols for which there is a protocol definition.

---

Follow these steps to create the new protocol rule:

1. In the left pane of the ISA MMC, right-click the **Protocol Rules** node, select **New**, and then select **Rule**. This invokes the New Protocol Rule wizard.

2. The first page asks you to give the new protocol rule a name. Type an appropriate name (such as “Allow All”). Click **Next**.

3. On the next page, you are asked to specify the rule action. Click the **Allow** option. Click **Next**.

4. On the next page, you are asked to select the protocols to which the rule will apply. Select **All IP traffic** in the drop-down box. Click **Next**.
5. On the next page, you are asked to select a schedule for applying the rule. Select **Always** in the drop-down box. Click **Next**.

6. On the next page, you are asked to select the client types that will be allowed access to the protocols. Select **Any request**. Click **Next**.

7. The last page of the wizard will summarize your selections. Verify that they are correct and click **Finish** (or click **Back** to make changes).

The new protocol rule will appear in the right pane of the MMC. Although not necessary, it’s a good idea to restart the Web Proxy and Firewall services after changing these configurations. To do so, follow these steps:

1. In the left pane of the ISA MMC, expand the **Monitoring** node.
2. Click the **Services** node under it. For each service, right-click the service name and select **Stop**.
3. After all services have been stopped, right-click each and click **Start**.

---

**Using a Dial-Up Connection**

There are a few extra steps to take if you’re using a dial-up connection with your ISA server:

1. In the left pane of the MMC, expand the **Network Configuration** node.
2. Right-click the **Network Configuration** node and select **Properties**.
3. In the Properties dialog box, check the **Use dial-up entry** check box. Click **OK**.
4. Click the **Routing** node under **Network Configuration** in the left MMC pane.
5. Right-click the **Last** rule in the right pane, and select **Properties**.
6. In the Properties dialog box, click the check box for **Use dial-up entry**, and click **OK**.

---

www.syngress.com
NOTE

You might want to be able to test connectivity directly from the Web browser on the ISA server. You can do this by making the Web browser a Web Proxy client or by accessing the Internet directly. Since packet filtering is disabled, the client will have access to all protocols. If you want to make the browser a Web Proxy client, you can configure it with the IP address you're using for the Outgoing Web Requests listener or with 127.0.0.1.

Now you can use the open access configuration to test basic Internet functionality through the ISA server. With this configuration, you should be able to access any type of content and publish servers without problems. Once you’ve completed testing, you should disable all the open access entries (disabling them, rather than deleting them, provides you with a quick way to open all access again if you need to do so for testing purposes without having to go through this entire process again).

Installing Service Pack 1

Throughout the following chapters in this book, we take for granted that you have installed Service Pack 1 (SP1) on your ISA servers. SP1 includes several updates and fixes (in fact, SP1 itself has been updated; Microsoft recommends that customers who installed SP1 prior to January 24, 2002 should install the latest build over the previous one on all computers that run ISA Server).

NOTE

You can download the latest version of SP1 from the Microsoft Web site at www.microsoft.com/isaserver/downloads/sp1.asp.

SP1 can be applied to both the Standard and Enterprise Editions of ISA Server. It works only with licensed versions and is not compatible with the 120-day evaluation version of ISA Server. You’ll need to have Windows 2000 SP2 installed on the Windows 2000 computer on which ISA is running before you install ISA SP1. If you installed the beta version of SP1, you can upgrade it to the release version.

NOTE

SP1 is required to run ISA Server on Windows .NET Standard or Enterprise Server, beta 3 or higher.
Chapter 1 • Defending the Network with ISA Server—and Beyond

You’ll need a minimum of 36MB of free disk space to install the service pack, although it uses only 12MB after the computer is reset following installation.

What’s Included in SP1

If you’re a prudent (and typically paranoid) network administrator, you probably want to know what’s in SP1 before you install it on your machine(s). According to Microsoft, the service pack includes the following:

- Hot fixes (all that have been released)
- Fixes that address customer reports to Microsoft Product Support Services (PSS)
- Code that increases the stability of the ISA services and admin tool
- Fixes recommended by security experts outside of Microsoft
- Code that makes it possible for ISA to work with .NET Standard and Enterprise Server operating systems

SP1 also gives you the ability to uninstall specific hot fixes that are installed after SP1, on an individual basis.

ISA SERVER ALERT

The only way to uninstall hot fixes that were released/installed before you installed SP1 is to uninstall SP1 itself. This will uninstall all hot fixes included in SP1 (which includes all hot fixes released prior to its release). You cannot uninstall the fixes individually. If you installed later hot fixes after SP1, you must uninstall them individually before you can uninstall SP1. The most recently installed hot fix must be installed first.

Use the Add/Remove Programs applet in Control Panel to uninstall SP1 and/or to uninstall individual fixes installed after SP1. Just select Microsoft ISA Server Service Pack 1 and Hot Fixes. To remove an individual hot fix installed after SP1, select it from the list and click Remove. To uninstall SP1, just click Remove.

When you installed SP1, the files that are necessary to return ISA Server to its pre-service pack state are saved in a folder called $UNINSTALL_ISA_SP$ in binary form. Uninstalling SP1 will restore these files.

A detailed list of the individual fixes that are addressed by SP1 is available on the Microsoft Knowledge Base Web site. See KB Article Q313249 for this information.
Determining the Version of SP1 Installed

Here’s how to find out which version of SP1 (if any) is installed on your ISA computer:

1. Click Start | Programs | Microsoft ISA Server | ISA Management.
2. In the ISA MMC, expand the Internet Security and Acceleration Server node in the left pane, and then expand Servers and Arrays.
3. Expand the ISA server name (ISABOX in Figure 1.15).
4. Click Computer.
5. Right-click the computer name in the right details pane, as shown in Figure 1.15, and select Properties.
6. In the Properties dialog box, note the number in the ISA Server version field.

As of the writing of this book, the latest version of SP1 was 3.0.1200.166. If any number other than this appears in the Properties dialog box, you should install the current version.

NOTE

You can check the Microsoft Web site (www.microsoft.com/isaserver) to determine whether newer service pack versions have been released.

Figure 1.16 shows the Properties dialog box on a machine with no service pack installed.
Figure 1.17 shows a machine with the initial version of SP1 installed.

Download and Installing the Service Pack on the ISA Server

The first step in installing the service pack is to download it from the Microsoft Web site at www.microsoft.com/isaserver/downloads/sp1.asp. You can select from several language versions: English, French, German, Japanese, and Spanish. The file is named isas1.exe and is 2.8MB in size. Note that the filename is the same for the original and
current versions of the service pack, so you cannot tell which version of the executable
you have based on the filename.

**NOTE**

If you have a slow connection or you’re unable to download SP1 over the
Internet, you can order it on CD from Microsoft’s trial store for $9.95. The CD
includes all the language versions except Japanese. TechNet subscribers receive
the service packs on CD as part of their membership benefits.

After you’ve downloaded the service pack, run the isasp1.exe file from the local
hard disk or network share (or if you have the CD, run it from the CD). You will first
be prompted to accept the End User Licensing Agreement. Update files will be copied
to the computer. When the update is complete, the dialog box shown in Figure 1.18
appears, prompting you to restart the computer.

**Figure 1.18 You Must Restart the Computer After the Installation of SP1**

![Figure 1.18 You Must Restart the Computer After the Installation of SP1](image)

After the ISA Server computer reboots, check the Properties box again to ensure that
the latest version of SP1 (3.0.1200.166) is indeed installed, as shown in Figure 1.19.

**Figure 1.19 When You Have the Proper Version of SP1 Installed, the Version
Number Will Be 3.0.1200.166**

![Figure 1.19 When You Have the Proper Version of SP1 Installed, the Version
Number Will Be 3.0.1200.166](image)
Upgrading Client Computers to SP1

Computers running the ISA Firewall Client should be updated with the client fixes that are included with SP1, as this increases stability. The SP1 upgrade addresses problems experienced by the Firewall client when it is under a high load and using WSPAD, conflicts with third-party layered service providers that cause connectivity problems, and problems with the Firewall client that might be experienced after upgrading the operating system to Windows XP.

After SP1 has been installed on the ISA Server machine, you can upgrade the clients by connecting to the mspclnt share directory on the ISA server and running setup.exe. This starts the Firewall Client Installation wizard. Choose the Repair option, as shown in Figure 1.20.

Figure 1.20 Updating the Firewall Client in the Firewall Client Installation Wizard

When the wizard completes the update process, you will be prompted to restart the client computer.

Service Pack 1 Issues

An independent security evaluation of ISA Server Service Pack 1 was conducted by Foundstone, Inc. (www.foundstone.com) prior to the service pack’s release in February 2002. The Foundstone team uses extensive testing that includes custom hacking tools, known exploits, and other means to detect penetration and attack vulnerabilities.

According to the white paper published by Foundstone (available on the Web at www.foundstone.com/pdf/isaserver_wp.pdf), the ISA Server development team at Microsoft resolved the concerns that were presented to them after testing, and Foundstone concluded that ISA Server with SP1 is an effective firewall solution for enterprise-level networks.
Some ISA users have experienced problems with DNS queries following the installation of SP1. If you are using internal DNS servers to resolve DNS queries, you might find that DNS doesn’t work after you install the service, until you restart the ISA server a second time (following the automatic restart after the installation). This always seems to fix the DNS problem.

Supporting Network Design

Because security and network performance—the two-pronged purpose of ISA Server—are so important in today’s interconnected world, ISA Server plays a vital role in your overall network design. Of course, exactly how and where ISA will be implemented depends on the particulars of your network (including size), your security needs, and the type of business you do.

Possible scenarios include:

- ISA Server as a stand-alone firewall server to protect your small to medium-sized network from Internet intrusion.
- ISA Server as part of an e-commerce solution, to speed customer access to your Web site and provide security for financial transactions using X.509 certificates.
- ISA Server as a Web-caching server, to provide faster Web access to knowledge-based workers on your LAN.
- An ISA Server array, to distribute the load of client requests and provide fault tolerance.
- ISA Server as an Internet connection sharing solution.
- ISA Server as a secure publishing solution, to protect the Web servers on your local network.
- ISA Server as part of a perimeter network (DMZ) solution.

There are a number of circumstances in which specific network design factors or special needs of the organization will require additional solutions for fully integrating ISA Server into the network. In the following sections, we discuss how you can use Application Center 2000 to provide centralized management of your ISA servers in a network where Active Directory has not been deployed, running ISA Server on the Windows .NET Server operating systems, and third party add-on software that can be installed on your ISA servers to provide added features and functions.
Using Application Center 2000 with ISA Server

The Enterprise Edition of ISA Server allows you to manage and configure the ISA servers on your network from a central location—but it is designed to work with Active Directory. What do you do if you haven’t deployed Active Directory on your network, but still want centralized control? There is a solution: use Microsoft’s Application Center 2000 in conjunction with ISA.

Application Center 2000 is a Microsoft tool for managing Windows 2000 Web applications as part of a high availability Web services deployment plan. It allows you to automatically apply changes to a group of servers in a cluster. You can find out more about Application Center 2000 at www.microsoft.com/applicationcenter/default.asp.

Application Center can also be used to manage multiple servers running the ISA Server Standard Edition, creating a “pseudo array.” This gives you the benefits of centralized administration without requiring that you deploy Active Directory. You need to install both products—ISA Server and Application Center—on each server that will be a member of the cluster. The array policy for all the ISA servers will be stored on the machine that acts as cluster controller for the Application Center cluster, and you make changes to the array members on the cluster controller.

NOTE

Not all of the features of an enterprise array on an Active Directory network are available to the pseudo array that is created by using Application Center. Distributed Cache Array Protocol (CARP) and centralized security groups are not supported, and you cannot use tiered policies.

Using Application Center to manage your ISA servers offers many benefits, but imposes additional requirements (which might result in additional cost). For example, all the server hardware needs to be identical, and the software configurations on all the servers need to be the same.

For more information about using ISA Server with Application Center on a non-AD network, along with detailed instructions on how to set up the network and servers, see the white paper on Microsoft’s Tech Net Web site at www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/acs/deploy/MgISA-AC.asp.

ISA Server and Windows .NET

The next generation of the Microsoft server family, Windows .NET server, is available for customer preview (Release Candidate 1) at the time of this writing and is expected to be released in the last quarter of 2002 or first quarter of 2003. The .NET server family consists of four members: Standard Server, Enterprise Server, Datacenter Server,
and Web Server. The .NET framework (which can also be added to and run on Windows 2000 Server) focuses on the use of XML and the products include improved performance, security, and reliability features. Many organizations that put off upgrading to Windows 2000 and are still running NT networks are expected to upgrade directly to .NET.

ISA Server will run on Windows .NET Servers; however, there are some caveats. If you’re running ISA on a Windows 2000 Server and want to upgrade to .NET, you have to install the ISA SP1 first. If you want to install ISA on a server that’s already running .NET Server, you’ll get error messages during the installation process that say “ISA Server is not supported by this version of Windows,” because the packet filter extension driver can’t be loaded. You can go ahead and install despite the error messages, but then you must apply SP1 before ISA will work properly. The .NET Server should not be connected to the Internet until you have finished installing both ISA and SP1.

NOTE

The 120-day evaluation version of ISA Server available at the time of this writing cannot be run on Windows .NET Server. If you’re running it on Windows 2000 Server, you must remove it before upgrading the server to Windows .NET.

You might encounter some issues after you get ISA and SP1 installed on your Windows .NET Server. For example, if the Internet Connection Firewall (ICF) is enabled, the ISA Firewall service won’t start. You need to disable ICF.

Third-Party Software Add-Ons for ISA Server

Since ISA Server’s release and as it has grown in popularity, a number of third-party software vendors have developed add-on products to enhance ISA’s functionality. It’s inevitable with any piece of software such as ISA that as users learn what it will and won’t do, they develop “wish lists” of features they’d like to see added. Microsoft is generally good about listening to this type of feedback and incorporating many of these new features into future versions of their products. However, what does a company do if it really needs those features in the meantime? Moreover, what about features that aren’t needed or wanted by the majority of users, but are extremely useful to a subset of users? That’s where enterprising software developers come in.

The number of add-ons offered for ISA Server is surprising, considering the fact that, at the time of this writing, it has only been available to the public for less than two years. We counted over 40 add-on products mentioned on the www.isaserver.org Web site alone. These products fall into several different categories, including:
Chapter 1 • Defending the Network with ISA Server—and Beyond

- Access Control
- Content Security
- Intrusion Detection
- Networking Utilities
- System Hardening
- Anti Virus
- Reporting Tools
- Caching Enhancements
- High Availability and Load Balancing Solutions
- Monitoring and Administration add-ons
- Security Services

Some of the ISA add-ons that we’ve tried and/or that are most often mentioned in the ISA Server user community include GFI’s DownloadSecurity for ISA Server, Rainfinity’s RAIN Connect, N2H2’s content filtering product, and the reporting tools from Burst Technology (btLogAnalyzer) and WebTrends Corporation. We have also heard good reports about Stonesoft’s Stonebeat Full Cluster for ISA Server, which provides high availability and dynamic load balancing.

ISA Server Certification

Microsoft’s certification exam 70-227, Installing, Configuring and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, is destined to replace exam 70-088, Implementing and Supporting Microsoft Proxy Server 2.0, when the latter is retired (retirement is scheduled for June 30, 2003). The Proxy Server exam was a popular elective choice for the Microsoft Certified Systems Engineer (MCSE) track in the past, and many new MCSE candidates are choosing the ISA Server exam as one of the two required electives.

Although this book is not designed specifically as an exam prep or study guide, we hope that, used in conjunction with Configuring ISA Server 2000, it will serve as a supplement to the training materials and study kits for those who are looking for more than just a surface understanding of how ISA works “under the hood.” We believe that knowledge will help to lay a foundation for persons contemplating taking exam 70-227, especially if our books are also used in conjunction with an objective-oriented study guide.

The Microsoft exam objectives are a good starting point for anyone who aspires to master this complex product, as they cover installation (including upgrade from Proxy...
Defending the Network with ISA Server—and Beyond • Chapter 1

Server 2.0 to ISA Server), configuring and troubleshooting the ISA Server services, configuring and managing policies and rules, setting up and administering the client computers, and monitoring and analyzing ISA Server use.

All these topics are important not only to exam takers, but to working IT administrators who plan to deploy ISA Server on their networks. This book is intended for both audiences (realizing that those two audiences will overlap in many cases, as student/exam takers get jobs and must put their knowledge to work in the field, or experienced professionals who have been working with the products on production networks decide to test their knowledge and obtain official documentation of their skills).

Microsoft has targeted ISA Server for the enterprise market, and that notion is reflected in their stated audience profile for the exam: candidates are expected to have at least a year of experience operating in a medium to very large networking environment (defined as 200 to 26,000+ users and multiple physical locations) where the Windows 2000 operating system is in use. We know that some of our readers fit this description and others don’t. Our goal in writing both of these books was to provide value both to those who are rolling out ISA Server in a large-scale network for mission-critical applications, and those who are deploying it on a small home network to familiarize themselves with the product as they study for the exam.

Beyond ISA Server

Implementing the ISA Server firewall is an important step in protecting your network from intruders and attackers, as well as controlling the access of internal users to inappropriate or potentially dangerous Internet sites and services. However, there is much more that you must do as part of a comprehensive security plan.

In addition to the chapters that deal with advanced configurations of ISA Server, this book will look at some other aspects of how to secure a Windows 2000 network, including:

- **Windows 2000 built-in security features** Windows 2000 provides many built-in security features that can be used to protect your computers and network. These include the ability to change the default access control settings by refining the permissions that are granted by default to predefined security groups.

- **The security configuration toolset** This is Microsoft’s response to a need expressed by systems administrators for a centralized, easy-to-use program that would allow them to set security for domains, organizational units, and local machines, rather than having to learn and use multiple tools for these tasks. Also included is the Security Configuration and Analysis MMC snap-in that
makes it possible to quickly and easily analyze a computer’s current configuration and compare it to predefined or custom security templates and apply changes.

- **The Encrypting File System** EFS provides Windows 2000 (and XP/.NET) users with a built-in mechanism for encrypting data on the disk, on a file-by-file or folder basis. File encryption is an important part of the security plan in an environment that includes sensitive data stored on the network (such as client records, personnel information, financial data, trade secrets, or any other data that should remain confidential).

Other security considerations are not specific to Windows-based networks, but many Windows sys admins are implementing these new methods of security and need guidance in integrating them into a Windows environment. These include:

- **Smart card authentication** Windows 2000 supports the use of smart cards for logon authentication, and this gives administrators a way to increase the security of the logon process by requiring that a user provide not only something he or she knows (an account name and password) in order to log on to the network, but also something he or she has in possession: the physical card on which is embedded a chip that contains the user’s certificate and other information.

- **Wireless network security** 802.11 wireless technologies have made it possible for laptop users to roam away from their desks and still stay connected to the company network without the inconvenience of cables. However, wireless networks have opened many new security holes that must be addressed; otherwise, there is a grave risk of comprising the security of the network. Out of the box, the default settings on most wireless equipment leave the network wide open to knowledgeable intruders, but there are many measures that can be implemented to provide better security and still enjoy the benefits of wireless communications.

- **Web server security** Web servers represent a point of vulnerability for many corporate networks because they are accessible via the Internet. Microsoft’s Internet Information Services (IIS) Web server software, like other Web server software, has a number of security holes when using default settings and/or unpatched versions of the program. There are many things a savvy administrator can do to increase the security of the network’s IIS-based Web servers.

This book will address all of these issues.
Summary

In this introductory chapter, we provided an overview/review of Microsoft ISA Server’s features and functionality, installation tips, and how to update the ISA Server and clients with Service Pack 1. We included new information about incorporating ISA Server into your network design, using Application Center 2000 to manage ISA Servers in a non-Active Directory network, running ISA Server on Windows .NET Server, and information about some of the many third-party software packages that can be added to ISA Server to enhance its functionality.

We then went beyond ISA Server to discuss major network security issues that are often encountered by the administrators of Windows-based networks in the enterprise, including the use of Windows’ built-in security features such as the default access control settings, Security Configuration Toolset, and the Encrypting File System (EFS). Other security considerations we discussed include the use of smart cards to authenticate users on the network, securing 802.1 wireless networks, and providing better Web security when using IIS as your Web server.

Network security is no longer a luxury that administrators can choose to ignore; our systems are vulnerable to a plethora of potential dangers. We need only read the newspapers to know that information warfare—the use of technology to disrupt the communications infrastructure on which companies and individuals increasingly depend—is not just an interesting idea; it’s already a reality. Major corporations have lost millions of dollars due to lost productivity, data loss or damage, and other consequences of both casual and calculated attacks. Whether the work of a sophisticated and skilled hacker or a clueless script kiddie, an attack on your organization’s network can be financially devastating. It is essential that network professionals have the proper tools available to protect their networks, and the documentation that will help them to get the most out of those tools.

ISA Server, through its firewall functionality, provides one such tool. However, installing it on your network is not enough. There are many different ways in which ISA can be deployed, and many tricks to configuring it to perform exactly the functions you need in your own organization. In Chapters 2 through 6, we will delve into advanced configuration techniques that can be used to tailor your ISA Servers’ functionality to fit your individual needs. Then, in Chapters 7 through 15, we’ll go beyond ISA Server to look at other aspects of defending a Windows-based network.
Defensive Tactics Fast Track

ISA Server Overview

- Microsoft’s Internet Security and Acceleration (ISA) Server replaced Microsoft Proxy Server 2.0, providing full-fledged firewall functionality for a much more robust security solution, along with improved caching/Web performance features.
- ISA Server performs the functions of a full-featured dedicated firewall, specifically designed to control access, preventing unauthorized data from entering the network and restricting how and what type of data can be sent out.
- ISA Server, when installed in firewall mode or integrated mode, can perform filtering at the packet layer, the circuit layer, or the application layer.

Installing ISA Server

- You should make firm decisions about each ISA Server design issue before you begin your installation. The decisions you make at this point will determine your choices when it comes time to install ISA Server itself.
- Minimum hardware requirements for any ISA server—regardless of the role the machine might play on the network—including Windows 2000 Server with SP1 or above; PII or K7 processor at 300 MHz or faster; minimum of 128MB of RAM (256MB recommended); 20MB disk space for program files, 2GB disk space for Web cache, two network interfaces.
- ISA Server can be installed in one of three modes: firewall, cache, or integrated.
- ISA Server Enterprise Edition can be installed either as an array member or as a stand-alone server.
- ISA Server supports three client types: Firewall, Web Proxy, and SecureNAT.

Installing Service Pack 1

- SP1 can be applied to both the Standard and Enterprise Editions of ISA Server. It works only with licensed versions and is not compatible with the 120-day evaluation version of ISA Server.
SP1 can be downloaded from the Microsoft Web site at www.microsoft.com/isaserver/downloads/sp1.asp. You can select from several language versions: English, French, German, Japanese, and Spanish. The file is named isasp1.exe and is 2.8MB in size.

After SP1 has been installed on the ISA Server machine, you can upgrade the Firewall clients by connecting to the mspclnt share directory on the ISA server and running setup.exe.

Supporting Network Design

Application Center 2000 can be used to centrally manage ISA servers on the network if you do not have Active Directory implemented.

ISA Server will run on Windows .NET servers, but ISA SP1 must be installed (either before upgrading from Windows 2000 to .NET, or after installing ISA on a .NET server). The .NET server should not be connected to the Internet until you have finished installing both ISA and SP1.

There are dozens of third-party software add-ons available for ISA Server that add more functionality and features, many of which are reviewed on the www.isaserver.org Web site.

ISA Server Certification

Microsoft’s certification exam 70-227, Installing, Configuring and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, is destined to replace exam 70-088, Implementing and Supporting Microsoft Proxy Server 2.0, when the latter is retired (retirement is scheduled for June 30, 2003).

The Microsoft exam objectives are a good starting point for anyone who aspires to master this complex product, as they cover installation (including upgrade from Proxy Server 2.0 to ISA Server), configuring and troubleshooting the ISA Server services, configuring and managing policies and rules, setting up and administering the client computers, and monitoring and analyzing ISA Server use.

Microsoft has targeted ISA Server for the enterprise market, and that notion is reflected in their stated audience profile for the exam: candidates are expected to have at least a year of experience operating in a medium to very large networking environment (defined as 200 to 26,000+ users and multiple physical locations) where the Windows 2000 operating system is in use.
Chapter 1 • Defending the Network with ISA Server—and Beyond

Beyond ISA Server

Windows 2000 provides many built-in security features that can be used to protect your computers and network. These include the ability to change the default access control settings by refining the permissions that are granted by default to predefined security groups.

The security configuration toolset is Microsoft’s response to a need expressed by systems administrators for a centralized, easy-to-use program that would allow them to set security for domains, organizational units, and local machines, rather than having to learn and use multiple tools for these tasks.

The Encrypting File System (EFS) provides Windows 2000 (and XP/.NET) users with a built-in mechanism for encrypting data on the disk, on a file-by-file or folder basis.

Other security considerations, including smart card authentication, wireless network security, and Web server security, are not specific to Windows-based networks, but many Windows sys admins are implementing these new methods of security and need guidance in integrating them into a Windows environment.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to www.syngress.com/solutions and click on the “Ask the Author” form.

Q: Must I install the schema to Active Directory each time I install an ISA server on my enterprise network?
A: No. The ISA schema only has to be installed once for the entire enterprise, when you install the first ISA server.

Q: What are the advantages to installing a single ISA server as a lone member of an array, instead of installing it as a stand-alone server?
A: If you anticipate that you might want to extend the ISA deployment to an array in the future, it will be easier to do so if you have installed your ISA server as a sole member of an array. Then, all you have to do is add more servers to the array later. Arrays offer several advantages: all the servers in the array share a common configu-
ration and can be managed together, saving on administrative time. Enterprise policies can be applied to all the servers in an array, and having an array distributes the load across the multiple servers, increasing performance and providing fault tolerance.

Q: Can ISA Server be installed in a Windows NT 4.0 domain?
A: Yes. Although ISA Server can only be installed on a Windows 2000 Server machine, that machine can be a stand-alone server in a Windows NT 4.0 domain. ISA Server must be installed as a stand-alone server in this environment; you cannot configure an array, because the configuration information will be stored in the local Registry rather than in a centralized location (Active Directory).

Q: Can I use ISA Server to protect our network from viruses?
A: ISA Server does not come with built-in virus detection. There are a number of third-party vendors who can supply application filters for ISA Server that can protect your network from viruses. Web filters can assess data moving through the Web Proxy service and scrub the data to remove the virus content. GFI Software’s “Internet Security for ISA Server” product is a Web filter that removes viruses from the Web Proxy service communications. Other filters can examine Instant Messenger, SMTP, and NNTP traffic. The built-in SMTP Message Screener can remove attachments from e-mail, but it does not screen for viruses.

Q: What’s the best type of DNS setup for ISA Server? Is there anything I should do to optimize my network before installing ISA Server?
A: There’s a good chance that you’re going to publish internal servers so users on the Internet can access their resources. It’s very common for both internal and external network clients to want to access the same servers. The problem that most organizations run into is that internal network clients should not use the ISA server to access internal network resources. The way you get around this problem is by creating a “split” DNS infrastructure. It’s called “split” because you need to split your DNS zone configuration so that internal and external network clients access different DNS servers for the same zone. For example, if you’re hosting resources for mydomain.com on the internal network that are accessible to external network hosts, you need to create one DNS zone that external network clients will use, and another zone that internal network clients will use. Although both zones will be authoritative for mydomain.com, the IP addresses in the resource records will be different. The public DNS zone will contain the IP addresses you use on the external interface to publish the servers on the internal network, and the private
zone will contain the private IP addresses on the internal network that internal network hosts will use to connect to the servers.

Q: What client type should I use? All my systems run some version of an NT-based operating system. We have Windows NT 4.0, Windows 2000, and Windows XP systems.

A: You should configure your machines as both Firewall clients and Web Proxy clients. The combination of Firewall and Web Proxy clients will give you the best performance with the highest level of service and protection. The only machines that should be configured as SecureNAT clients are those you’re publishing to the Internet and domain controllers. It is generally a very bad idea to install the Firewall client on a domain controller.