Chapter 1

Introduction to ISA Server

If you've not worked with proxy server, firewall, or web-filtering software before, you're in for a treat as you work through this book. What interesting software! Think for a moment about what it might take to keep a person inside the private network from getting to websites that the company says should be off-limits. For example, suppose you want to establish a policy that keeps people from going to adult-oriented websites. But it seems that there must be 20 million of them—and more available each day! How are you supposed to keep track of all that?

What about the efforts you need to go through to keep people from getting *into* your private network from the Internet? Or how about keeping outside people from attacking your firewall with scurrilous Denial of Service (DoS), User Data Protocol (UDP) bomb, or other disruptive attacks?

What about if you're running a network that uses one of the private IP address ranges? When users go out onto the Internet, they need to be represented by a valid IP address. How does that happen?

You can see by the above questions where we're headed with this book. Internet Security and Acceleration (ISA) Server 2000 does all of the above and more. It's a big grown-up Microsoft Proxy Server 2.0, complete with most or all of the things that Proxy needed to make it play in the firewall world. ISA Server is a certified firewall, having achieved ICSA Labs certification on February 14, 2001. (See `www.icsalabs.com` for more information about ICSA.)

This book will introduce you to ISA Server 2000, what it does, how it works, methods of configuration, modes of operation, troubleshooting techniques, reporting options, and dozens of other things you need to know to pass the certification exam and, more important, to make the software work correctly in your network.

We start off with a basic chapter that talks about the whats and whys of this product. This chapter is an excellent place to clear up any confusion you may have about different types of server security products. Chapter 2, "ISA Server 2000 Installation," and beyond begin to segue into the nuts and bolts of ISA Server. Because we include exercises in the chapters, you may want to have a test server handy for your lab testing as you go through this book, preferably one that can connect to the Internet (even if through dial-up). You'll also need the ISA Server CD. Your lab server will need to be equipped with Windows 2000 Server, Advanced Server, or DataCenter Server—ISA won't work on NT 4.0 (though it will work in NT 4.0 networks). (Server and Advanced Server require SP1.)

The Need for Corporate Security

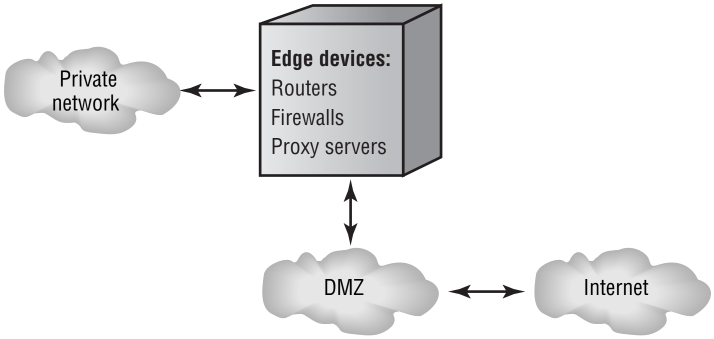
We're at a juncture in network computing where we face a highly perplexing phenomenon: We want to let our users out onto the Internet and bring the Internet in to our users because this capability facilitates so many great things. But, as we all know, the Internet has millions of people on it who have less than your company's best interest at heart. While Sally might think, for example, that she's gotten a really clever little screen background in her e-mail, what she's not aware of is that the code behind the scenes is checking her address book, deleting key files on her computer, and fixing to send itself to others in order to do the same thing.

There are those who get their kicks by trying to bring corporate websites to their knees—to stop them from functioning entirely. Big players have had it happen to them—Microsoft, Amazon, and others have experienced firsthand this kind of attack.

Some people maintain that 70–80 percent of a network's security problems come from *within,* not from without. The Sallys of the world make it difficult for administrators because unless you have extremely rigid policies in place, you just don't know what somebody's going to try to put on their computer, either by bringing it in from home or by downloading it through the web. And it goes without saying what a hassle e-mail administrators have gone through of late, what with the I Love You virus and other highly dangerous pieces of viral code that manage to slink their way through corporate e-mail servers all over the world.

Today's enterprise model dictates enterprise thinking and enterprise security modeling. Microsoft ISA Server is specifically designed to be an integral part of an enterprise security model. You use Windows 2000 Professional with policies in place to keep users from adding unwanted software to their PCs. You use an antivirus policy with a good third-party solution to keep viruses from coming through the Internet, through e-mail, or from being put onto client computers. You use ISA Servers to manage the edge of your network, that scary dropping-off point between the Internet and your private corporate network. (Web servers live between the edge of the network and the Internet in a place we lovingly call the demilitarized zone, or DMZ.) Figure 1.1 shows this scenario. A DMZ is the area where the internal network is separated by a firewall, which in turn is separated from the Internet by a firewall. There are two methods of creating a DMZ. You can set up a firewall that interfaces with the Internet, put your web and other DMZ application servers behind it, and then put another firewall behind the DMZ to protect your internal network. Or you can put three network cards in your firewall server (called a *triple-homed server*), one leg of which goes to the DMZ, one to the Internet, and one to the internal network. Either way, you're protecting both the DMZ and the internal network by use of a firewall. Web servers rarely sit on the DMZ without benefit of a forward firewall.

FIGURE 1.1 A standard private/DMZ/Internet network layout



This figure represents only one design; there are others, but you get the picture. There's at least one and probably more devices that shield the edge of your private network from Internet users and hackers. You need a router to make determinations about what packets need to go where and a firewall to prevent scurrilous individuals from trying to get into your private network and other accoutrements.

Real World Scenario

The "Lookie What I Have Here" Manager

Monica is the network manager for a mid-sized insurance company of around one thousand users. She has a fairly robust antivirus policy in place but doesn't have the staff she needs to make sure that all computers are completely updated with the latest-and-greatest virus signature files on a routine basis. Because of this, some PCs get out of date and thus become privy to new viruses that may come down the line.

Monica receives news that there is a new virus out in the world—one that ships itself through e-mail as an image document—a picture of a provocatively posed female model in a bikini. Most e-mail server antivirus-scanning software can be set to disallow any kind of file, but Monica has her e-mail server set only to disallow EXE files from coming in the door. Since this new graphic doesn't have an .exe extension, she's not filtering for it.

The file makes its way into the internal network and one of the managers opens it. While the manager admires the bikini-clad young woman in the picture, the code behind the scenes reads his e-mail address book and sends an e-mail message out to each of the users listed therein that says, "Look what I found!" The code also deletes key system DLL files and then exits.

As fate would have it, this manager doesn't have the newest antivirus-scanning software on his PC, and so when he's finished viewing the image his system halts. Further, the system won't reboot and a technician is called out to rebuild it.

Others receive the image but don't open it, while still other have up-to-date antivirus software on their computers and receive evidence that a file was at one time attached but is now no longer available (having been cleaned by the antivirus software).

Of the 450 computers that the image sent itself to, 90 of them did not have up-to-date virus scanners, 30 people opened the image, and hundreds of e-mail documents with the image in it went out onto the

Internet to e-mail users listed in people's address books, where the process started all over.

Ronnie, the hacker who wrote the virus code, thought it was cool that his virus made it all the way to the major antivirus manufacturer's website of "malicious virus" listings.

What Is a Proxy Server?

The word *proxy* means an agent or a substitute. A proxy server's primary purpose is to hide the IP addresses of internal clients from the Internet. You might need to do this because you're running a reserved IP address range on your private network (192.168.y.z, for example) or, even if you do have legitimate external addresses, because you don't want those addresses visible to Internet users.

A proxy server substitutes the internal client's IP address with a valid external address. It does this through the use of two network interface cards (NICs)—one that works on the internal net and one that's pointed to the Internet—or through a single NIC or an alternative connection to the Internet—perhaps a dial-up connection. So, for example, a user on a private network with IP address 192.168.13.42 would hit the internal proxy server NIC (perhaps 192.168.13.1), the proxy server software would turn around and handle the Internet connectivity for the user through its external NIC (perhaps 165.27.38.1), and the user would utilize the Internet without anyone on the outside knowing any inside numbers. This process is called *Network Address Translation (NAT)* and we would say that the internal user's address had been *NAT-ted*.

We should point out that the truest intent of a proxy server is to merely fetch material on behalf of a client. Therefore, NAT-ting isn't absolutely necessary. However, NAT-ting is part and parcel of MS Proxy Server and would be something you might consider a value-added component for any proxy server product you were wishing to purchase.

Benefits and Uses of a Proxy Server

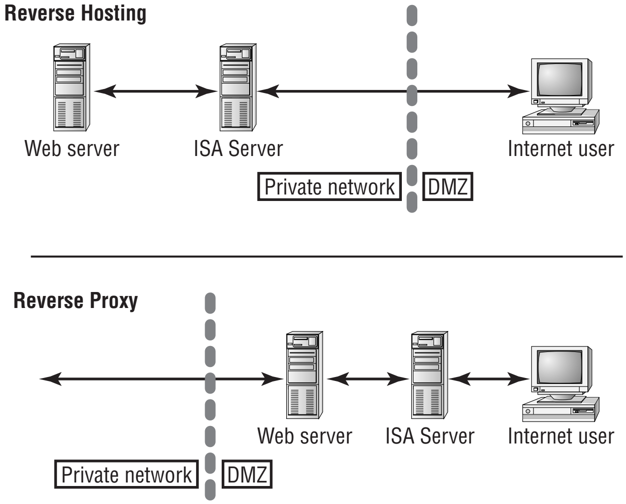
NAT-ting is a key benefit of a proxy server. But there are other benefits as well. Web caching is a feature of proxy server software. You can cache frequently hit sites locally at the proxy server, thus reducing the time that it takes for users to go directly to the site and pull up the page, increasing overall performance. You can also configure caching retention, disk space usage, and other settings.

Proxy server software allows for a concept called *packet filtering*. Don't want internal users to be able to download files off of an Internet-based FTP site? Set up a packet filter that disables FTP, and your users won't be able to perform this function any longer. You're actually filtering out the usage of the File Transfer Protocol when you set up this kind of filter. You can filter either internal usage or external usage or both. In other words, you can set up a proxy server so that it also filters out attempts to FTP in from the Internet. Many different protocols are available in the filter list—more than you may even realize are available on the Internet. With packet filtering, you control the incoming and outgoing flow of packets—which packets are allowed and which are not.

You can set proxy server software to disallow internal users from hitting certain websites. This functionality is called *web filtering*. In the case of both ISA Server and MS Proxy Server 2.0, you can key in sites that you don't want users to hit and apply the filter to certain groups of users. The problem with this scenario is that it's tedious because you have to key in each site individually and can't possibly capture the ever-changing nature of the Internet. ISA Server has a third-party *Software Developer's Kit (SDK)* that allows independent parties to develop add-in components for ISA Server. MS Proxy Server 2.0 also had this capability. In either case (ISA or Proxy Server), the developers would write an *ISAPI filter*—a filter that is customized to perform a certain function when working with either product. Web-filtering software that is more robust in its functionality is an example of a third-party software application that can be purchased to go along with ISA Server. See `www.smartfilter.com` and `www.surfcontrol.com` as examples of companies that are writing third-party add-ins for ISA Server and that wrote add-ins for Proxy Server 2.0.

Proxy servers allow for what is called *reverse hosting* (or might be referred to as *secure publishing*). The concept is simple, but its implementation can get complicated. If you have, for example, a web server on your internal network that you'd like to have available to Internet users, you can use proxy server software to allow for this. Alternatively, you can put your web server on the DMZ but behind a proxy server, thus allowing the proxy server to impersonate the web server and provide an added level of web server security. This process is called *reverse proxy*.

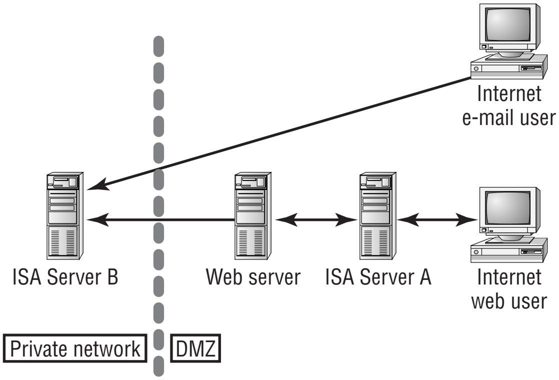
FIGURE 1.2 Differences between reverse hosting and reverse proxy



You can clearly see in Figure 1.2 the difference between the two ideas. With reverse hosting, we're actually hosting our web servers inside the private network and using ISA Server to allow secure connectivity between Internet users and the web servers. The key word here is *secure*. ISA Server makes sure that Internet users aren't able to hack into other parts of the network. You might use a scenario such as this in a situation where you don't have enough resources or your web presence isn't large enough to demand a DMZ (and all of the demands that go along with maintaining a DMZ).

On the other hand, reverse proxy merely puts an ISA Server in front of web server(s) sitting on the DMZ. This is the technique of using reverse proxy. Ideally, you'd like to see a scenario such as the one shown in Figure 1.3, where you have not only an ISA server in *front* of the web servers, but also *behind* the web servers at the entrance to the private network. You can tune the ISA servers differently so that box A performs intrusion detection and filters out certain protocols that you know you'll never allow to access the web servers, while box B acts as a complete robust firewall.

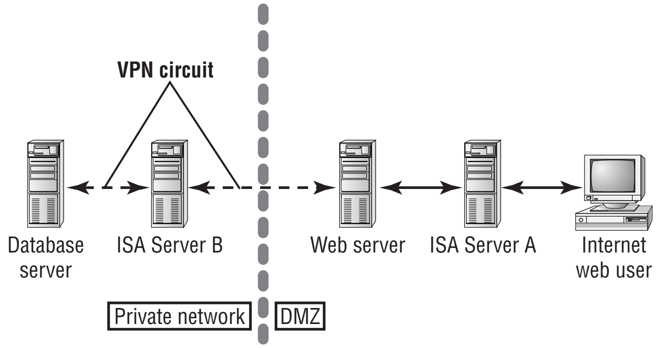
FIGURE 1.3 Ideal DMZ scenario



Note in Figure 1.3 that you may have an Internet e-mail user who desires to utilize your web servers only to send e-mail to someone. The firewall can secure the private network and still allow Internet e-mail to enter (typically on port 25).

Let's get a little more carried away. Suppose that you have a database server using Microsoft SQL Server 2000 that you want to live on the private network. Web servers that live on the DMZ need to utilize the databases on this database server for, say, e-commerce work. You could simply key in a rule that allowed only the web servers to communicate through the firewall to the inside database server. You could also go one step further and set up a *virtual private network (VPN)* between each web server and the database server. Since ISA Server can handle VPN traffic, and L2TP with IPSec creates a highly secure VPN tunnel, you'd have extremely granular security applied to your e-commerce scenario. Technically, we'd call this a secure IPSec tunnel as opposed to a VPN, but the concepts are the same for both, so we'll simply refer to the above as a VPN. Takes a lot of extra time to configure and test? Sure it does. Is it worth it? Well, recently a company that's in the e-commerce business had thousands of their credit card numbers stolen from an internal database and held for ransom until the thieves were paid. The thieves were given their money but were never caught. Figure 1.4 shows the VPN scenario.

FIGURE 1.4 E-commerce VPN scenario



In such a scenario as Figure 1.4, you really haven't added any more servers than before; you've merely upped the ante in terms of security complexity. Truly though, companies that are interested in e-commerce activity need to consider whether such extra effort is worth it or not.

Good proxy server software will also support VPN connectivity for users who desire to access the private network from the Internet.

NOTE

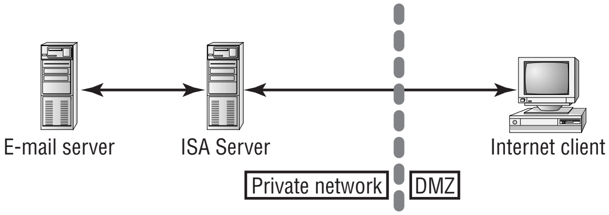
For more information regarding VPNs and the various choices you have at your disposal, see *MCSE: Windows 2000 Network Infrastructure Administration Study Guide,* Second Edition (Sybex, 2001) and *MCSE: Windows 2000 Network Infrastructure Design Study Guide* (Sybex, 2000).

Proxy server software should support Secure Sockets Layer (SSL) for encrypted sessions between an Internet user and web servers (such as an e-commerce catalog site).

Proxy server software allows for circuit layer security—listening for Telnet, RealAudio, and other sorts of circuits that users are trying to set up over the Web. You can filter out any circuits or allow them to continue; the design and implementation is your choice.

Server hosting allows for packets directed to the internal network from the Internet to be sent directly to the participating server. For example, e-mail documents can be sent directly from the proxy server to the internal e-mail server. Figure 1.5 shows this scenario.

FIGURE 1.5 Server hosting scenario



Some proxy server software comes with proprietary software that has to be installed on each computer in the network in order to accommodate all of a proxy server's functionality. For example, to make full use of MS Proxy Server 2.0's Winsock capabilities, you would have to install the Winsock client on each workstation. ISA Server supports the old MS Proxy Server 2.0 client (called the Winsock Proxy client), as well as the SOCKS client. (There is an add-on to support SOCKS v4. ISA Server does not, however, migrate MS Proxy Server 2.0 SOCKS rules at migration time.)

NOTE

If you've configured Internet Explorer with the Internet Explorer Administration Kit (IEAK) and you've pointed each user to a specific proxy server address, when you get ready to move users to an ISA Server environment that's using a different IP address, you may be forced to recompile and re-push IE with the new, good address to all clients. This can add significant time to your ISA Server rollout plans.

Windows 2000 Advanced Server supports Internet Connection Sharing (ICS) and NAT. Both features are designed for smaller offices that require the capability of dialing up to an Internet service provider (ISP) so that users can utilize the Internet. ICS allows for the sharing of a connection and for the NAT-ting of internal to external addresses. You'd likely use NAT or ICS in small office, home office (SOHO) environments where very few users are connected at one time, though it certainly might prove useful in smaller companies that can't afford or don't feel they need the horsepower of ISA Server. ICS isn't routable, so it won't work in larger organizations that span routers. NAT can work in deployments with routers. ICS and NAT cannot be installed on the same server.

Real World Scenario

Using MS Proxy Server 2.0 with an Internal Exchange 5.5 Server

When I worked as a consultant, I once had a contract with a small government agency. My task was to replace an old firewall product with MS Proxy Server 2.0. The client had an internal Exchange 5.5 Server that had to continue to communicate with the Internet (for incoming Internet e-mail purposes), so I had to pay close attention to Proxy Server's server-hosting feature. The trick is pretty simple. You add a couple of INI settings to the Exchange Server's `BIN` directory and install the Proxy Server client.

Everything should've fired off and begun working right away. But we ran into complications at the outset. I wound up calling Microsoft, opening a support ticket, and talking on the phone with them for nearly three hours while we troubleshot the problem.

Turns out that I had some permissions set wrong in the Proxy Server box, and when we straightened out its settings, the whole thing took off and ran just fine.

What Is a Firewall?

A firewall doesn't differ that much from a proxy server. Essentially, the difference is that you key *rules* into a firewall and these rules, firing in order, determine which computers may get into the private network from the Internet and which protocols they may use to get there. You can also configure rules that keep internal users from using certain protocols or certain computers from getting out onto the Internet. You can configure groups of users so that you don't have to create hundreds of individual rules. As you might imagine, asking software to run through a bunch of rules in a firewall before it makes a decision as to whether to allow a certain operation or not could really slow down activity if the rule list was too long.

There are many uses of firewalls, including the following:

- Providing circuit-level gateways. That is, after a TCP or UDP connection has been made, the security of the connection is maintained and no further checking is required.
- Providing the ability to set up application-level security for applications such as Telnet or FTP.
- Filtering packets based upon the way you configure the rules.
- Acting as proxy servers (by NAT-ting the address).

Microsoft Proxy Server 2.0 is billed as a firewall, and some may argue with that connotation, but it's perfectly true in context with what we know a firewall to do.

So how are a firewall and a proxy server different from one another? Largely, the difference lies in the ability to key in the rules that make a firewall work. You don't key rules into a Microsoft Proxy Server 2.0 setup. You enter rules into an ISA Server computer that's been equipped as a firewall.

Firewalls don't do any web filtering on their own. Generally, you use a separate product alongside a firewall to accommodate your web-filtering needs. Proxy servers can filter web content, with or without third-party add-on help.

You can buy hardware- or software-based firewalls. Cisco manufactures a wonderful firewall called Pix. Since the firewall code is built into the firmware, you get a wire-speed firewall. But you pay big bucks for it, too.

Firewalls generally start out with the premise that no protocol is allowed into the system until rules are created. Proxy servers generally start out with the premise that all protocols are allowed in until you decide to rule certain ones out. Firewalls can work with users, groups, computers, and other non-protocol types of objects, whereas proxy servers are typically concerned with IP addresses and protocols.

The Cable Modem User

Do DSL and cable modem users need a firewall? Think about it. Here you have a computer, with a NIC, connected to what amounts to an Internet network. Your cable modem/DSL-linked computer's IP address is known across the Internet. In fact, if you're at work, you can probably ping your home computer, if not by name, then certainly by IP address (provided, of course, that the broadband company's firewalls allow for pings).

This is remarkable! It means that hackers, for example, could get into your personal computer at home, which is connected to the Internet via cable modem or DSL, and change your online tax form for you so that it said you made a million dollars! That'd get a laugh out of a few hackers, thinking that you were sitting in an IRS hot seat because of a malicious little change they made. Or how about this scenario: Napster-ites, irritated by legal rulings barring them from sharing songs, decide that the 8GB of free space you have on your computer would be a good place to store some of the songs they're sharing out—making your PC a sort of surrogate Napster database server, if you will.

But there are indeed miniature firewalls available for DSL and cable modems. One that is particularly good and, best of all, free for home consumers, is called Zone Alarm. It's available by visiting `www.zonelabs.com`. This company also manufactures higher-end firewall solutions, but the fact that Zone Alarm is so good while also being free makes it a very attractive offering. Computer Associates manufactures EZ-Armor, which utilizes an incorporated firewall and antivirus product all in one, but there is a yearly charge for its use.

Common Internet Protocols and Ports

Working with a proxy and firewall server requires that you be familiar with the common Internet protocols and their associated ports. There are several key reasons for this. First of all, if you aren't familiar with at least the most common of ports, you have no way of knowing whether you're being hacked into or not. Second, if you know of a port that's commonly used and hence is a target for hackers, perhaps there are workarounds you can employ to prevent hacking. For example, HTML commonly uses port 80. Since it's a well-known port, hackers will make an initial hacking attempt at port 80. By hosting web servers at port 8080 instead, you can avert some of the security problems. (The problem is that port 8080 is now also well known—see Table 1.1 for others.) In addition, when setting up your packet-filtering rules, it's helpful to know which ports are being occupied so you don't inadvertently shut off a service that's needed by people inside your organization. While it's not important that you memorize virtually every protocol and port on this list, it is important that you memorize common protocols and ports. Table 1.1 shows some common Internet protocols and ports.

Note that you can use other ports not currently utilized by TCP/IP. Typically, these ports fall within the 1024–65,535 range. Some Internet applications or protocols might make use of a port in this upper range, and those are included in Table 1.1 as well and marked with an asterisk (*). Please note that this table does not include ports that are not registered with the Internet Assigned Numbers Authority (IANA), found on the Web at `www.iana.org`. There are certain "well-known" ports, that is, ports that are well known by hackers to be predominantly open and available for "business." These ports are noted in Table 1.1 by a plus sign (+).

TABLE 1.1 Common Internet Protocols and Ports

Port	TCP/UDP	Protocol or Service
20+	TCP	File Transfer Protocol (FTP) Data
21+	TCP	FTP File Transfer Control
*22	TCP	Secure Shell Remote Login Protocol (SSH)
23+	TCP	Telnet
23+	UDP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
42	TCP	Windows Internet Name Service (WINS) replication and other hostname servers
47	TCP	Generic Route Encapsulation (GRE) header for PPTP
53+	UDP	Domain Name System (DNS) Name Resolution and Lookup
53+	TCP	DNS Name Resolution and Lookup
67+	UDP	DHCP Client, Bootstrap Protocol (BootP)
68+	UDP	DHCP Server
69+	TCP	Remote Installations via Trivial File Transfer Protocol (TFTP—commonly used for configuring network devices such as switches and routers across a network)
80+	TCP	HTTP
88+	TCP/UDP	Kerberos v5 Authentication (default security protocol used by Windows 2000)
102	TCP	Mail Transfer Agent (MTA) using X.400 over TCP/IP
110+	TCP	Post Office Protocol v3 (POP3)
119+	TCP	Network News Transport Protocol (NNTP)

TABLE 1.1 Common Internet Protocols and Ports *(continued)*

Port	TCP/UDP	Protocol or Service
135	TCP	Used for three purposes: client/server communication, for legacy Exchange administration, and for Remote Procedure Call (RPC)
137+	UDP	NetBIOS Name Service (Handles logon sequence, Windows NT 4 trusts, Windows NT 4 secure channel, pass-through authentication, browsing, and printing)
137+	TCP	WINS registration
138+	UDP	NetBIOS Datagram Service (Handles logon sequence, Windows NT 4 trusts, Windows NT 4 directory replication, Windows NT 4 secure channel, pass-through authentication, netlogon, browsing, and printing)
139+	TCP	NetBIOS Session Service (Handles NetBIOS Translation [NBT], Server Message Blocks [SMB], file sharing, printing, logon sequences, Windows NT 4 trusts, Windows NT 4 directory replication, Windows NT 4 secure channel, pass-through authentication, Windows NT 4 administration tools [Server Manager, User Manager, Event Viewer, Registry Editor, Performance Monitor, DNS Admin], Common Internet File System [CIFS])
143	TCP	Internet Message Access Protocol (IMAP)
194+	TCP	Internet Relay Chat (IRC)
194+	UDP	Internet Relay Chat (IRC)
220+	TCP	IMAP v3
220+	UDP	IMAP v3
389+	TCP/UDP	Lightweight Directory Access Protocol (LDAP)

TABLE 1.1 Common Internet Protocols and Ports *(continued)*

Port	TCP/UDP	Protocol or Service
*407	TCP	Timbuktu (Remote control software—`www.netopia.com`)
443	TCP	HTTP Secure Sockets Layer (SSL)
445	TCP	Common Internet File System (CIFS)
464	TCP/UDP	Kerberos v5 Password
465	TCP	SMTP (SSL)
500	TCP/UDP	Internet Security Association Key Management Protocol (ISAKMP)/Oakley header and traffic (used with IPSec)
*522	TCP	User Location Protocol (ULP—`www.microsoft.com`)
531	TCP	Internet Relay Chat (IRC)
543	TCP	Kerberos Login (klogin)
544	TCP	Kerberos Shell (kshell)
*554	TCP/UDP	Real Time Streaming Protocol (RTSP—`info.internet.isi.edu/in-notes/rfc/files/rfc2326.txt`)
560	TCP	Content Replication Service
563	TCP	NNTP (SSL)
636	TCP	LDAP (SSL)
*666	TCP/UDP	Doom Internet game
750	UDP	Kerberos authentication
751	UDP	Kerberos authentication
752	TCP	Kerberos authentication
753	UDP	Kerberos User Registration Server
754	TCP	Kerberos Slave Propagation
888	TCP	Logon and environment passing

TABLE 1.1 Common Internet Protocols and Ports *(continued)*

Port	TCP/UDP	Protocol or Service
993	TCP	IMAP4 (SSL)
995	TCP	POP3 (SSL)
1024–5000	TCP	Structured Query Language (SQL) sessions
*1024	TCP	Mirabilis ICQ (dynamic assignment starting from port 1024, www.icq.com) (Also AOL ICQ)
1109	TCP	Post Office Protocol (POP) with Kerberos
1234	TCP	Used by Small Business Server's (SBS) second-tier DNS Registration Wizard
*1417–1420	UDP	Timbuktu (Remote control software—www.netopia.com)
1433	TCP	SQL session
*1490	TCP	Vocaltec Internet Phone (www.vocaltec.com)
1500	TCP	Remote Procedure Call (RPC) Client fixed-port sessions queries
*1503	TCP	T.120 (Exchange 2000 conferencing server—www.microsoft.com/exchange)
*1533	TCP	Various Internet voice conferencing services
*1558	UDP	Xingtech videoconferencing (www.xingtech.com)
1645	UDP	Remote Authentication Dial-In User Service (RADIUS) authentication (Port 1812 can be used also)
1646	UDP	Remote Authentication Dial-In User Service (RADIUS) accounting (Port 1813 can be used also)
*1720	TCP/UDP	H.323 (videoconferencing) call setup (Exchange 2000 conferencing server)

TABLE 1.1 Common Internet Protocols and Ports *(continued)*

Port	TCP/UDP	Protocol or Service
1723	TCP	Point to Point Tunneling Protocol (PPTP) Control Channel (used along with port 47—GRE header channel)
*1731	TCP	Audio call control (Exchange 2000 conferencing server)
1801	TCP	Microsoft Message Queue Server
1812	UDP	Remote Authentication Dial-In User Service (RADIUS) authentication (Port 1645 can be used also)
1813	UDP	Remote Authentication Dial-In User Service (RADIUS) accounting (Port 1646 can be used also)
*1863	TCP	Microsoft Network (MSN) Messenger Instant Messaging (`messenger.msn.com`)
*2000–2003	TCP	ICUII Video Chat program (`www.icuii.com`)
*2000–2007	TCP	iSPQ Video Chat program (`www.nanocom.com`)
*2001	TCP	Webglimpse search engine (`www.webglimpse.org`)
2053	TCP	Kerberos de-multiplexer
*2064	TCP	Distributed.net RC5/DES distributed computation (`www1.distributed.net`)
2101	TCP	Microsoft Message Queue Server
2103	TCP	Microsoft Message Queue Server
2105	TCP	Kerberos encrypted remote login (rlogin), Microsoft Message Queue Server
*2327	UDP	Netscape conferencing (`www.netscape.com`)
*2300–2400	TCP/UDP	Microsoft DirectX gaming (`www.microsoft.com/directx`)

TABLE 1.1 Common Internet Protocols and Ports *(continued)*

Port	TCP/UDP	Protocol or Service
*2592	TCP	Netrek game (www.netrek.org)
2980	TCP/UDP	Exchange 2000 Instant Messaging (IM) Service
*3128	TCP	Web proxy cache program (www.squid-cache.org)
*3130	TCP	Web proxy cache program (www.squid-cache.org)
3268		Global Catalog
3269		Global Catalog
3389	TCP	Windows 2000 Terminal Server
3527	UDP	Microsoft Message Queue Server
*4000	UDP	Mirabilis ICQ (dynamic assignment starting from port 1024, www.icq.com)
*4020	TCP/UDP	Ichat chat rooms (www.ichat.com)
*4747	UDP	Pgpfone (secure Internet phone, www.pgpi.org)
*4747	TCP	Playlink games site (www.playlink.com)
*4748	TCP	Playlink games site (www.playlink.com)
*5190	TCP/UDP	AOL Instant Messenger (www.aol.com)
*5190	TCP	AOL ICQ (www.aol.com)
*5190–5193	TCP/UDP	AOL (www.aol.com)
*5190	TCP	AOL ICQ (www.aol.com)
*5631	TCP	Symantec PCAnywhere (www.symantec.com)
*5632	UDP	Symantec PCAnywhere (www.symantec.com)
*5800 (and up)	TCP	VNC remote control (www.uk.research.att.com/vnc)

TABLE 1.1 Common Internet Protocols and Ports *(continued)*

Port	TCP/UDP	Protocol or Service
*5900 (and up)	TCP	VNC remote control (www.uk.research.att.com/vnc)
*6498	TCP	Netscape conferencing (www.netscape.com)
*6502	TCP	Netscape conferencing (www.netscape.com)
*6502	TCP/UDP	Danware Netop remote control software (www.netop.com)
6665	TCP	Microsoft Chat server to server
6667	TCP	Microsoft Chat client to server
6665–6669	TCP	Internet relay chat
*6670	TCP	Vocaltec Internet Phone (www.vocaltec.com)
*6970–6999	UDP	Apple Real-Time Transport Protocol (RTP) for QuickTime (www.apple.com)
*6970–7170	UDP	RealAudio streaming audio and video using Real-Time Streaming Protocol (RTSP) (www.real.com)
7000	TCP	VDO Live streaming video
*7070	TCP	RealAudio streaming audio and video using Real Time Streaming Protocol (RTSP) (www.real.com)
*7648–7649	TCP	CUSeeMe videoconferencing (www.cuseeme.com)
*7648–7652	UDP	CUSeeMe videoconferencing (www.cuseeme.com)
8001	TCP	HTTP
8002	TCP	HTTP
8080	TCP	HTTP
*9943	UDP	Ivisit virtual chat (www.ivisit.com)

TABLE 1.1 Common Internet Protocols and Ports *(continued)*

Port	TCP/UDP	Protocol or Service
*9945	UDP	Ivisit virtual chat (`www.ivisit.com`)
*10090	TCP	Playlink games site (`www.playlink.com`)
*14237	TCP	Palm computing hotsync (`www.palm.com`)
*14238	UDP	Palm computing hotsync (`www.palm.com`)
*18888	TCP	Liquid Audio streaming audio (`www.liquidaudio.com`)
*18888–18889	UDP	Liquid Audio streaming audio (`www.liquidaudio.com`)
*22555	UDP	Vocaltec Internet Phone (`www.vocaltec.com`)
*24032	UDP	CUSeeMe videoconferencing (`www.cuseeme.com`)
*25793	TCP	Vocaltec Internet Phone (`www.vocaltec.com`)
*26000	TCP/UDP	Quake Internet game
*28800–29000	TCP/UDP	Microsoft Network (MSN) gaming (`www.msn.com`)
*39213	UDP	Sygate manager (`www.sygate.com`)
*47624	TCP/UDP	Microsoft DirectX gaming (`www.microsoft.com/directx`)
*51200–51201	UDP	Dialpad Internet telephony (`www.dialpad.com`)
*51210	TCP	Dialpad Internet telephony (`www.dialpad.com`)
*56768	UDP	Ivisit virtual chat (`www.ivisit.com`)
*Dynamic	TCP	H.323 Call Control
*Dynamic	UDP	H.323 Call (RTP over UDP)
Dynamic	TCP	RCP Session Ports

*Indicates ports used by Internet applications or protocols.
+Indicates ports well known by hackers to be open for “business.”

ISA versus Microsoft Proxy Server 2.0

If you have experience with Proxy Server 2.0, you can expect that the very good things that Proxy Server brought to networks will be carried forth and more added besides. Existing Proxy Server 2.0 installations will integrate with new ISA Server configurations in an array-like fashion, one of Proxy Server and ISA Server's more appealing capabilities. Following are the features (some are updates from Proxy Server 2.0) of ISA Server:

Firewall Like Proxy Server 2.0, ISA Server is a firewall. ISA Server supports circuit, application, and packet filtering and is an ICSA certified firewall.

Caching server ISA Server can function as a stand-alone caching server or in an array of caching servers. Note that MS Proxy Server 2.0 had caching capabilities, but they've been greatly improved with ISA.

Dynamic packet filtering Also called *stateful inspection*. ISA Server can examine packets as they come across the wire, making decisions about their context and connection state and opening ports accordingly. With dynamic packet filtering, the appropriate port is opened when needed and closed when not needed.

Circuit-level filtering Think of an automated process running on an internal server that periodically needs to FTP into a server on the DMZ in order to place files in a folder on the external server. This process has created a circuit. ISA Server supports circuit-level filtering, allowing you to monitor the circuit and its status. Various Internet applications (such as Telnet) can be monitored through circuit-level filtering.

Application filtering With application filtering, you monitor incoming and outgoing packet flow associated with a particular application. You can use this technique to monitor, for example, bad SMTP packets going out or potential DNS hacks coming in.

Integrated virtual private networking ISA Server integrates with VPN clients. You can set up ISA Server so that it acts as a VPN host server and allows in only your known VPN users—keeping potential VPN hackers out.

System hardening The administrator has a choice of ways in which the Windows 2000 Server computer with ISA Server installed is utilized. For example, if the server also has Internet Information Service installed on it, you would set *system hardening* to Secure to allow other server services to be functional. System hardening is your way of defining the level of security that's required of your ISA Server. The more security you apply, the harder it is to get into your private network—hence the term *hardening*.

Intrusion detection New to ISA Server. You can set up the ability for ISA to detect and respond to network attacks such as the Ping of Death and DoS.

Policies ISA Server allows you to set up one of two different types of policies: enterprise or array, based upon whether you're working with servers in an array or if you desire to enforce all servers from an enterprise perspective. When installing ISA Server in an array, you can opt to configure enterprise policies and yet allow admins who'll be working with other array members to add their policies as well; you can also configure enterprise policies and *not* allow any other policies or simply allow others to configure their own policies. When you configure policies that are an addition to the enterprise policies, they are called *array policies*.

Reporting ISA Server provides for various reports showing network activity, security events, and application usage.

Secure application hosting ISA Server, like Proxy Server 2.0, allows for application and web hosting. ISA Server kicks things up a notch by allowing web, e-mail, and e-commerce servers to live behind the firewall, protected from intruders but able to be utilized by Internet traffic.

Robust logging Logging was a weak feature of Proxy Server 2.0. ISA Server changes all that by providing robust logging for cache and network activity.

Policy-based access control ISA Server allows you to set up policies by user, group, schedule, application, destination, or content type, thus providing you with very granular control over the access that your users have to the Internet and that Internet users have coming into the private network.

In addition, you can expect in ISA Server the ordinary things that you'd expect from any Microsoft server offering: Microsoft Management Console (MMC) single administration source, alerting, performance-monitoring features, and integration with Windows 2000 Active Directory (AD) and wizards.

There are some key differences between the two products and reasons to move from MS Proxy Server 2.0 to ISA Server. They are as follows:

- ISA Server is 10 times faster than MS Proxy Server 2.0.
- Greatly enhanced Internet user access control through the use of user, group, computer, schedule, bandwidth, or destination information.
- Capability of centrally managing large ISA Server deployments and support for scalability.
- Enterprise firewall certified by ICSA Labs (`www.icsalabs.com`).

Real World Scenario

Deciding to Begin Working with ISA Server

Emilio is a security administrator for a large network in the western hemisphere. The network currently has 20 Proxy Server 2.0 computers spread out over as many countries, home-runned to a headquarters office by T1 (1.544 Mbps) lines. The servers are set up in a Proxy Server array.

The enterprise server administration team has designed and deployed a brand-new Windows 2000 Advanced Server environment, completely replacing the original Windows NT 4 network.

In his studies, Emilio has learned that ISA Server will handily work with the existing Proxy Server array for smooth parallel cutover to the new system. The new ISA Servers will integrate into Active Directory, making their management and integration much easier.

Now all Emilio has to do is finish reading this book and then sit down and design his complete Proxy Server 2.0–to–ISA Server conversion project plan.

Summary

In this chapter, we talked about the differences between a proxy server, a firewall, and web-filtering software. A proxy server can NAT addresses between the internal and external networks. It can filter packets based upon their protocols and accept or deny them accordingly. Proxy servers support the idea of *circuit filtering*, providing support for Internet applications such as Telnet, e-mail, RealAudio, Microsoft Windows Media, Internet Relay Chat, and others. Proxy servers also support application filtering—monitoring incoming or outgoing packets that belong to a certain application, thus providing application-specific activities such as blocking, screening, redirecting of traffic, and so forth. Proxy servers allow for caching of web hits by internal users, thus speeding up performance. They also allow for secure publishing, the ability to publish web or e-mail services on the Internet from within the private network.

Firewalls provide the same basic services but differ a bit from proxy servers in that they have a database of rules that you create in order to facilitate the blocking that you'd like to do. Web filtering simply allows you to control which websites users can go to.

ISA Server incorporates all of the great features of MS Proxy Server and includes many more updates and additions as well, such as increased support for secure publishing, various client levels, integration with Active Directory (in an ISA Server array), web filtering, intrusion detection, and enhancements to previous Proxy Server functionality. ISA Server, like Proxy Server, is extensible by virtue of a Software Developer's Kit.

Key Terms

Before you take the exam, be certain you are familiar with the following terms:

circuit filtering

demilitarized zone (DMZ)

Network Address Translation (NAT)

reverse hosting

reverse proxy

secure publishing

server hosting

Software Developer's Kit (SDK)

stateful inspection

system hardening

virtual private network (VPN)

Review Questions

1. Aliakbar needs to configure his ISA Server installation so that website administrators can use Telnet to connect to a server on the DMZ. Aliakbar wants to make sure that the connection is managed and monitored and that he can examine the session at any time. What kind of filtering is required?

   A. Packet

   B. Dynamic packet

   C. Circuit

   D. Application

2. Juliet is the security administrator for a large Windows 2000–based enterprise containing several disparate networks. Currently, various administrators are using different firewall products. Juliet would like to bring in one product to take the place of the current hodgepodge of firewalls. What two features of ISA Server will lend credence to her argument?

   A. Integration with Windows 2000 Active Directory

   B. Web page caching

   C. Web filtering

   D. Arrays

3. What feature of ISA Server will prevent Denial of Service (DoS) and Ping of Death (PoD) attacks?

   A. Packet filtering

   B. Intrusion detection

   C. Dynamic caching

   D. Policies

4. Your internetwork department handles all of the routers, firewalls, switches, and infrastructure for your company. Your supervisor has given you a mandate to come up with a method whereby you can control the sites that internal users are allowed to visit. What are your alternatives for solving this problem? (Choose all that apply.)

   A. Windows 2000 Group Policy Object (GPO)

   B. Proxy Server

   C. ISA Server

   D. Talk to internetworking team

5. Leah is the network administrator for a small engineering company. The company currently has no connection to the Internet, but Leah has been given permission to set up a dial-up connection. Which products can Leah use to accomplish this task? (Choose all that apply.)

   A. Windows 2000 Advanced Server

   B. MS Proxy Server 2.0

   C. ISA Server

   D. Exchange 2000 Enterprise Server

6. Kim is the network administrator for a small engineering firm located in a single building that has an unprotected 56KB connection to their ISP. Besides the obvious security benefit, what other benefits can Kim present to her boss to get approval for purchasing a computer and ISA Server software to act as the firewall? (Choose all that apply.)

   A. Web caching

   B. ISA Server array

   C. Bandwidth management

   D. Server publishing

7. Faldad administers a 1000-node network that has a T1 connection to an ISP. The ISP currently blocks incoming packets that Faldad has determined should not be allowed in, but the added monthly costs for the service are prohibitive and Faldad would like to install his own ISA Server. Another of his objectives is to prohibit access by all users to websites that may have objectionable content. He has had requests from many managers for this service. Which products can Faldad use to accomplish this goal? (Choose all that apply.)

   A. Windows 2000 Advanced Server ICS or NAT

   B. Microsoft Proxy Server 2.0

   C. ISA Server

   D. Microsoft Proxy Server 2.0 with third-party access-control software

   E. ISA Server with third-party access-control software

8. You want to provide access to web servers on your private network without having to create a DMZ. What ISA Server functionality will accomplish this for you?

   A. Server publishing

   B. Reverse hosting

   C. Packet filtering

   D. Circuit filtering

9. Pick a feature that ISA Server *does not* have.

   A. Web caching

   B. Routing

   C. Packet filtering

   D. Policies

10. What are some of the key differences between a firewall and a proxy server? (Choose all that apply.)

    A. A firewall uses rules.

    B. A proxy server can't perform packet filtering.

    C. A proxy server can't perform Network Address Translation.

    D. A firewall can be either hardware- or software-based.

11. You are a contractor who's been hired by a five-person dental office to set up a network. In particular, the persons hiring you want two people to be able to regularly access the Internet through their dial-up ISP in addition to performing the normal file/print functions. Which solutions might be appropriate in this situation?

    A. Microsoft Proxy Server 2.0

    B. ISA Server

    C. NAT

    D. ICS

    E. Equipping both PCs with a modem and phone line

12. Suppose that you wanted to have an internal web server available for Internet clients. What features of ISA Server would you use? (Choose all that apply.)

    A. Reverse hosting

    B. Negative proxy

    C. Secure publishing

    D. Application publishing

13. What does caching do?

    A. Keeps Internet pages in memory

    B. Keeps web activity in a log

    C. Keeps protocols used in a log

    D. Keeps protocols prohibited in a log

14. What is system hardening?

A. Providing a very sturdy case for the ISA Server

B. Putting the ISA Server on a cluster

C. Drilling down on the ISA Server security restrictions

D. One of the ISA Server installation modes

15. Using the following table, working from the private network out, put the servers in proper order.

	ISA Reverse Hosting server
	ISA Server
	Web server
	Private network server

16. Oliver is an administrator of an environment that currently has an array of Microsoft Proxy Server 2.0 computers. He wants to upgrade the array to ISA Server. What are some of the chief functionalities that Oliver can hope to gain from the new ISA Server array? (Choose all that apply.)

A. Sharing of packet filters

B. Web cache hierarchy

C. Web cache sharing

D. Sharing of firewall rules

E. Allowing individual administrators to create their own packet filters and firewall rules

17. What is the reason for using a Microsoft Proxy Server 2.0 installation?

A. It keeps Internet users from hacking into the internal network.

B. It hides internal network addresses.

C. It provides intrusion-detection mechanisms.

D. It filters web content.

18. What is to be gained by upgrading to or installing ISA Server? (Choose all that apply.)

A. Intrusion detection

B. Reports

C. Robust logging

D. Web-content filtering

E. Alerting

F. Capability of operating in an array

19. Miguel is the enterprise administrator for a large network of disparate "mini-LANs" that are operated by independent administrators. Some of these administrators have voiced a desire to house their own firewall and, in fact, have taken steps toward procuring and installing one. Miguel is recommending an ISA Server array to solve the problem. What are some benefits to be obtained from using an ISA Server array? (Choose all that apply.)

A. Both enterprise and local (array) policies can be maintained.

B. Local sites can cache web content, and content can be cached at the DMZ.

C. Local administrators can create their own rules.

D. Local administrators must adhere to enterprise rules.

E. All members of the array can sit on different DMZs.

20. Should an ISA Server computer be connected to an internal network domain? (Choose all that apply.)

A. Yes it should; there are ample security restrictions out-of-box to prevent hacking.

B. Yes it should; however, security restrictions need to be immediately applied.

C. Yes it should; however, only certain administrators should be allowed access to it.

D. No it should not.

Answers to Review Questions

1. C. Circuit-level filtering allows for the monitoring of a connected session using common Internet protocols such as IRC, Telnet, and others. Typically, this kind of monitoring can be used for internal application–to–external application monitoring or by a person trying to set up a session with an Internet-based computer. Packet filtering can be set up to examine incoming and/or outgoing packets of certain protocols or port numbers. Dynamic packet filtering does the same kind of packet filtering, but on the fly as the packets are streaming inward or outward. The key difference between packet filtering and dynamic filtering is that with dynamic filtering the port needed is open during the session and closed at session closure time. Application filtering allows you to monitor common Internet applications for such things as bad SMTP packets or attacks on internal DNS servers.

2. A, D. While answers B and C are certainly appealing, they're not relevant in terms of desirable reasons to move to ISA Server. However, ISA Server's ability to run in a hierarchical array and to integrate with AD are wonderful reasons to consider the switch.

3. B. ISA can monitor for incoming network attacks and prevent them accordingly, in addition to notifying the administrator of the attack.

4. B, C, D. You can prevent users from hitting certain websites with either Proxy Server or ISA Server. It's important to talk to the internetworking team so that they know your plans for introducing ISA Server—you'll potentially need their help.

5. A, B, C. You can use Windows 2000 Advanced Server with either its Network Address Translation (NAT) or Internet Connection Sharing (ICS) program. You can also use Proxy Server 2.0 or ISA Server to dial your favorite ISP and make an Internet connection anytime users need one.

6. A, C, D. Kim's site is small so she wouldn't need an ISA array. However web caching, the ability to curtail Internet activity by bandwidth, and server publishing are all great reasons to set up an ISA Server.

7. D, E. NAT and ICS are too small for a 1000-node shop and they won't handle Faldad's need for access control. Proxy Server 2.0 and ISA Server can provide a modicum of access control, but configuration is a manual process and really not satisfactory for the objectives that Faldad has. In order to really leverage Web-filtering, he needs to supply either an MS Proxy Server 2.0 or an ISA Server computer and purchase third-party web-filtering software to go along with it. Microsoft provides SDKs for products such as this to encourage third-party snap-in/add-on software to enhance the initial capabilities. You can create destination sets and apply these to users and groups in ISA (with much more granular control than you had with Microsoft Proxy Server 2.0), but if you're trying to filter out objectionable content such as porn sites, you really have to resort to third-party snap-ins to ISA.

8. A. Web servers aren't the only type of server that can take advantage of this feature but probably the most apt one to use it at first. Note that in large enterprises with many servers, it may make more sense to set up a DMZ and use ISA Server to reverse host, thus protecting the web servers and acting as the first line of defense on the big bad Internet.

9. B. ISA Server is not a router and does not function as a router. Routing is a function of Windows 2000 Server, not ISA. Windows 2000 Server has the ability to take on many forms of routing: Routing Information Protocol (RIP), RIP v2, Open Shortest Path First (OSPF), and others.

10. A, D. A proxy server is almost like a firewall but with a couple of key exceptions: A proxy server doesn't use rules like a firewall does to keep traffic out (or in, as the case may be), and a firewall can be either hardware- or software-based.

11. C, D. In a situation such as this, ICS and NAT are probably the best considerations. You can set up one Windows 2000 Server that can be utilized for file and print services as well as for hosting NAT and ICS.

12. A, C. Reverse hosting, or as it's been referred to, secure publishing, through ISA Server allows you to maintain internal web servers that can be hit by Internet users.

13. A. Caching keeps track of the Internet sites that have been hit and caches them in memory for a short time. The cache time and length are adjustable. A feature of both ISA Server and Microsoft Proxy Server 2.0 is that you can ask for either server product to periodically go out to sites you're interested in maintaining crisp congruity with and refresh the cache with updated pages. You can nest caching servers (more on that in the array chapters). Caching speeds up Internet response times for users.

14. C. You can choose how secure you want the ISA Server to be. There are three levels of system hardening.

15.

Private network server
ISA Server
Web server
ISA Reverse Hosting server

Remember that reverse hosting means that the ISA Server is in *front* of the web servers on the DMZ, protecting them from intruder attacks, filtering packets, and doing all the things good firewalls do. The ISA server *behind* the web servers protects the private network from the same things, perhaps even more. In larger web server environments, the web servers sit on the DMZ in between the two firewalls. The private network server sits behind the firewall server that protects the private network from the DMZ and Internet.

16. E. In an ISA Server array, your first installation sets up the array. At that time, you have the option to create enterprise policies. You can opt to allow other array members to add to your enterprise policies, you can force the enterprise policies to be the only policies that are in place, or you can opt to allow the array member admins to create their own policies. This is not a feature that you'd realize with Microsoft Proxy Server 2.0 and one reason you'd want to upgrade to ISA Server. We talk a lot more about arrays in Chapter 5, "Configuring ISA Server for the Enterprise."

17. A, B, D. Proxy Servers are chiefly able to perform packet filtering, which, to some extent, keeps intruders from hacking into the network. It also NATs the internal network addresses, hiding them from the outside world. Microsoft Proxy Server provides no intrusion-detection mechanism without some third-party intervention. While it is possible to filter out Web content using rules, you wouldn't use this kind of functionality to rule out objectionable sites in a corporate environment. You need more horsepower than the rules can give you, and so you'd probably resort to a third-party ISAPI snap-in.

18. A, B, C, E. Without a third-party add-on component, ISA Server still cannot do web-content filtering. However, in both Microsoft Proxy Server 2.0 and ISA Server, you can set up sites that are off-limits to users. A site and content rule in ISA Server means that you can set up a rule to explicitly allow or deny some forms of content. It does not utilize advanced searching methodologies that rule out sites with specific content. Both Proxy Server and ISA can operate in an array.

19. A, B, C, D. You would probably not set up an array where each array member was at the edge of a different DMZ, even in an environment such as the one above. You would use arrays to control the enterprise rules and, if so desired, allow local admins to *add to* (not take away from) the rules. You could cache web content both locally and at the DMZ. Best of all, you'd have an even playing field of subject matter experts who were knowledgeable about a single product, and the whole thing would run over Active Directory.

20. B, C. The entire concept behind ISA Server is that it NATs internal addresses for users to access the Internet through disguised addresses. On top of that, ISA can take advantage of users, groups, and computers but can only see those users, groups, and computers if it's a member of a domain. However, you cannot simply plug in and run an ISA Server computer. You'll need to establish rules that specifically allow or deny certain Internet access.