CHAPTER 1

Introducing ISA Server 2006

IN THIS CHAPTER:

- Understanding the Need for ISA Server 2006
- Detailing the Additional Advantages of ISA Server
- Understanding the History of ISA Server 2006
- Exploring ISA Server 2006's New Features
- Detailing Deployment Strategies with ISA Server 2006
- Augmenting an Existing Security Environment with ISA Server 2006
- Administering and Maintaining an ISA Server 2006 Environment
- Using ISA Server 2006 to Secure Applications
- Summary
- Best Practices

The rise in the prevalence of computer viruses, threats, and exploits on the Internet has made it necessary for organizations of all shapes and sizes to reevaluate their protection strategies. No longer is it possible to ignore or minimize these threats because the damage they can cause can cripple a company's business functions. A solution to the increased sophistication and pervasiveness of these viruses and exploits is becoming increasingly necessary.

Corresponding with the growth of these threats has been the development and maturation of the Internet Security and Acceleration (ISA) Server product from Microsoft. The latest release of the product, ISA Server 2006, is fast becoming a business-critical component for many organizations who are finding that many of the traditional packet-filtering firewalls and technologies don't necessarily stand up to modern threats. The ISA Server 2006 product provides for that higher level of application security required, particularly for common tools such as Outlook Web Access (OWA), SharePoint Products and Technologies, and web applications.

In addition to a new array of firewall functionality, ISA Server 2006 provides robust Virtual Private Networking (VPN) support and enhanced web-caching capabilities, all within a simplified management interface. It also provides for a high degree of integration into an environment with existing security infrastructure in place, providing for an additional layer of security that could not have been achieved otherwise.

This book gives an in-depth analysis of the ISA Server product, with an emphasis on exploring "best practice" approaches that can be used when implementing an ISA

Server environment. These examples are gathered from real-world implementations and lessons learned from the field with the product. Because a majority of ISA Server implementations are established to complement—rather than replace—existing security infrastructure, particular emphasis is placed on the information and tools necessary to supplement these environments with ISA Server 2006. Third-party security tools, intrusion detection techniques, and firewall and VPN products working in coexistence with ISA Server 2006 are detailed throughout the chapters.

NOTE

The specific focus of this book is on the 2006 version of the product; all the examples and step-by-step guides assume the use of this latest version. For in-depth knowledge into the ISA Server 2004 product, we recommend reviewing the *ISA Server 2004 Unleashed* book by the same author and publisher.

Understanding the Need for ISA Server 2006

A great deal of confusion exists about the role that ISA Server can play in a network environment. Much of that confusion stems from the misconception that ISA Server is only a proxy server. ISA Server 2006 is, on the contrary, a fully functional firewall, VPN, web-caching proxy, and application reverse-proxy solution. In addition, ISA Server 2006 addresses specific business needs to provide a secured infrastructure and improve productivity through the proper application of its built-in functionality. Determining how these features can help to improve the security and productivity of an organization is subsequently of key importance.

In addition to the built-in functionality available within ISA Server 2006, a whole host of third-party integration solutions provides additional levels of security and functionality. Enhanced intrusion detection support, content filtering, web surfing restriction tools, and customized application filters all extend the capabilities of ISA Server and position it as a solution to a wide variety of security needs within organizations of many sizes.

Outlining the High Cost of Security Breaches

It is rare that a week goes by without a high-profile security breach, denial-of-service (DoS) attack, exploit, virus, or worm appearing in the news. The risks inherent in modern computing have been increasing exponentially, and effective counter-measures are required in any organization that expects to do business across the Internet.

It has become impossible to turn a blind eye toward these security threats. On the contrary, even organizations that would normally not be obvious candidates for attack from the Internet must secure their services because the vast majority of modern attacks do not focus on any one particular target, but sweep the Internet for any destination host, looking for vulnerabilities to exploit. Infection or exploitation of critical business infrastructure can be extremely costly for an organization. Many of the recent productivity gains in business have been attributed to advances in Information Technology functionality, and the loss of this functionality can severely impact the bottom line.

In addition to productivity losses, the legal environment for businesses has changed significantly in recent years. Regulations such as Sarbanes-Oxley (SOX), HIPAA, and Gramm-Leach-Blilely have changed the playing field by requiring a certain level of security and validation of private customer data. Organizations can now be sued or fined for substantial sums if proper security precautions are not taken to protect client data. The atmosphere surrounding these concerns provides the backdrop for the evolution and acceptance of the ISA Server 2006 product.

Outlining the Critical Role of Firewall Technology in a Modern Connected Infrastructure

It is widely understood today that valuable corporate assets cannot be exposed to direct access to the world's users on the Internet. In the beginning, however, the Internet was built on the concept that all connected networks could be trusted. It was not originally designed to provide robust security between networks, so security concepts needed to be developed to secure access between entities on the Internet. Special devices known as *firewalls* were created to block access to internal network resources for specific companies.

Originally, many organizations were not directly connected to the Internet. Often, even when a connection was created, there was no type of firewall put into place because the perception was that only government or high-security organizations required protection.

With the explosion of viruses, hacking attempts, and worms that began to proliferate, organizations soon began to understand that some type of firewall solution was required to block access to specific "dangerous" TCP or UDP ports that were used by the Internet's TCP/IP protocol. This type of firewall technology would inspect each arriving packet and accept or reject it based on the TCP or UDP port specified in the packet of information received.

Some of these firewalls were ASIC-based firewalls, which employed the use of solid-state microchips, with built-in packet-filtering technology. These firewalls, many of which are still used and deployed today, provided organizations with a quick and dirty way to filter Internet traffic, but did not allow for a high degree of customization because of their static nature.

The development of software-based firewalls coincided with the need for simpler management interfaces and the capability to make software changes to firewalls quickly and easily. Firewall products such as CheckPoint, Cisco, PIX, Sonicwall, and other popular firewalls are all software-based. ISA Server itself was built and developed as a software-based firewall, and has the ability to perform the traditional packet filtering that has become a virtual necessity on the Internet today.

More recently, however, holes in the capabilities of simple packet-based filtering technology have made a more sophisticated approach to filtering traffic for malicious or spurious content a necessity. ISA Server responds to these needs with the capabilities to perform Application-layer filtering on Internet traffic.

Understanding the Growing Need for Application-Layer Filtering

Nearly all organizations with a presence on the Internet have put some type of packet-filtering firewall technology into place to protect the internal network resources from attack. These types of packet-filter firewall technologies were useful in blocking specific types of network traffic, such as vulnerabilities that utilize the RPC protocol, by simply blocking negotiation ports or other high ports that the RPC protocol uses. Other ports, on the other hand, were often left wide open to support certain functionality, such as the TCP 80 port, utilized for HTTP web browsing. As previously mentioned, a packet-filter firewall is able to inspect only the header of a packet, understanding which port the data is meant to utilize, but unable to actually read the content. A good analogy to this would be if a border guard was instructed to allow only citizens with specific passports to enter the country, but had no way of inspecting their luggage for contraband or illegal substances.

The problem that is becoming more evident, however, is that the viruses, exploits, and attacks have adjusted to conform to this new landscape, and have started to realize that they can conceal the true malicious nature of their payload within the identity of an allowed port. For example, they can piggy-back their destructive payload over a "known good" port that is open on a packet-filter firewall. Many modern exploits, viruses, and "scumware," such as illegal file-sharing applications, piggy-back off the TCP 80 HTTP port, for example. Using the border guard analogy to illustrate, the smugglers realized that if they put their contraband in the luggage of a citizen from a country on the border guard's allowed list, they could smuggle it into the country without worrying that the guard would inspect the package. These types of exploits and attacks are not uncommon, and the list of known Application-level attacks continues to grow.

In the past, when an organization realized that it had been compromised through its traditional packet-filter firewall, the common knee-jerk reaction was to lock down access from the Internet in response to threats. For example, an exploit that would arrive over HTTP port 80 might prompt an organization to completely close access to that port for a temporary or semipermanent basis. This approach can greatly impact productivity, especially in a modern connected infrastructure that relies heavily on communications and collaboration with outside vendors and customers. Traditional security techniques involved a trade-off between security and productivity. The tighter a firewall was locked down, for example, the less functional and productive an end user could be.

In direct response to the need to maintain and increase levels of productivity without compromising security, Application-layer "stateful inspection" capabilities were built into ISA Server that could intelligently determine whether particular web traffic was legitimate. To illustrate, ISA Server inspects a TCP packet traveling across port 80 to determine whether it is a properly formatted HTTP request. Looking back to the smuggling analogy, ISA Server is like a border guard who not only checks the passports, but is also given an X-ray machine to check the luggage of each person crossing the border.

The more sophisticated Application-layer attacks become, the greater the need becomes for a security solution that can allow for a greater degree of productivity while reducing the types of risks that can exist in an environment that relies on simple packet-based filtering techniques.

For more information on the specifics of working with and setting up application-based filtering technology to secure inbound traffic and control access to internal resources, refer to Part III of this book, "Securing Servers and Services with ISA Server 2006."

Detailing the Additional Advantages of ISA Server

In addition to being a fully functional firewall solution, ISA Server contains a host of other security and productivity features. ISA Server is often deployed for other nonfirewall tasks such as Virtual Private Network (VPN) access, web caching, and intrusion detection. Taking it one step further, a slew of dedicated ISA hardware devices have become available from various manufacturers. An understanding of what these types of capabilities are and how they can best be utilized is key.

Allowing for More Intelligent Remote Access with Virtual Private Networks (VPNs)

In addition to having robust firewall capabilities, ISA Server is also a fully capable Virtual Private Network (VPN) solution. Built into the functionality of the product, VPN capabilities allow trusted users that exist outside a network to authenticate with ISA Server and gain elevated access to internal network resources. In addition to authenticating against Active Directory domains, ISA Server 2006 can utilize RADIUS (Remote Authentication Dial-In User Service) to authenticate users. This capability opens up a range of new architectural capabilities with ISA because the ISA server no longer is required to be a domain member to provide authentication between users. In addition, Internet Authentication Service (IAS) can be used to enable authentication between multiple domains that do not have trust relationships in place, as illustrated in Figure 1.1.

An added advantage to the Virtual Private Network support in ISA Server 2006 is the capability to treat VPN users as a separate network. This allows for a more granular policy control. For example, ISA can be configured to allow only authenticated VPN users to access an Exchange Server. Another function of ISA VPNs is to quarantine VPN clients that do not conform to an organization's security requirements into a restricted network in ISA that has access to only a small range of predetermined services.

NOTE

ISA Server 2006 supports both Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) for VPN Connections.

For more information on how to set up, configure, and manage Virtual Private Networks with ISA Server 2006, refer to Chapters 9, "Enabling Client Remote Access with ISA Server 2006 Virtual Private Networks (VPNs)," and 10, "Extending ISA 2006 to Branch Offices with Site-to-Site VPNs."

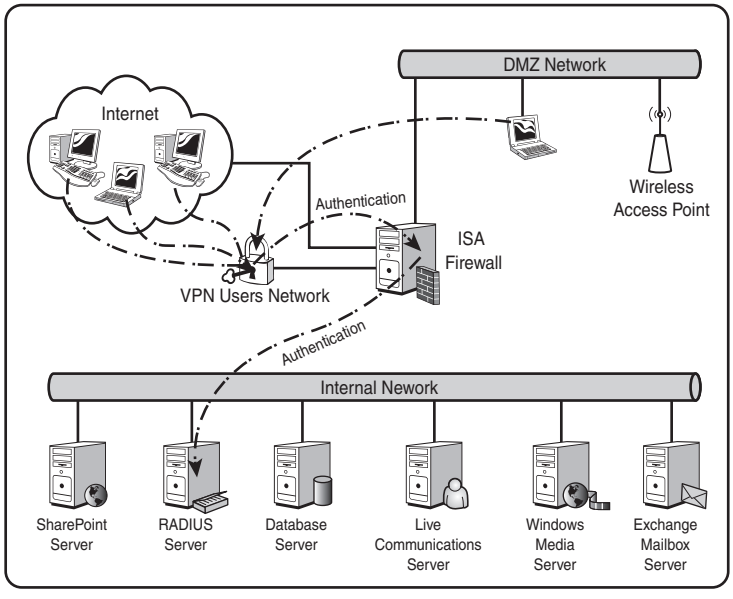

FIGURE 1.1 Utilizing Virtual Private Networks with ISA Server 2006.

Using Web Caching to Improve and Control Web Browsing

The "acceleration" portion of the Internet Security and Acceleration product refers to ISA Server's capability to act as a proxy for network clients, caching commonly used web sites and their associated graphics, text, and media, and serving them up to end users more quickly than if they had to access the content across the Internet. An additional benefit to this approach is the fact that all outbound web and FTP traffic is then scanned by ISA for threats, exploits, and restricted content. ISA has long been a product of choice for those seeking web-caching capabilities. In fact, the previous iteration of the product, Microsoft Proxy Server, was primarily used for that capability by itself in many organizations. ISA Server 2006 caching builds upon this success by further improving the system's caching capabilities.

Utilizing the caching capabilities of ISA Server 2006 is a straightforward and easy-to-deploy method of getting more bandwidth out of an Internet connection. In addition to the capability to cache requests made to web and FTP sites, ISA Server also provides for the capacity to provide commonly used content from web sites for caching by downloading it on a regular basis. Content download rules can be set up easily to update the cache on a regular basis for sites that administrators designate. This concept can further improve the speed and reliability of web and FTP browsing.

For more information on setting up and configuring ISA Server 2006 to act as a web-caching solution, refer to Chapter 8, "Deploying ISA Server 2006 as a Content Caching Server."

Reducing Setup and Configuration Time with an ISA Server 2006 Hardware Solution

One of the complaints with previous versions of the ISA Server product was the fact that it acted in many ways like a traditional server application. It was installed on a base Windows operating system that would subsequently need to be manually secured by a local administrator. This manual securing of the infrastructure on a device touted as a security solution caused many organizations to shy away from deploying it into their environment. In some cases, specific functionality that was offered by ISA Server but not offered by other firewall solutions was passed over in favor of more "traditional" firewalls, which did not require an operating system setup and security process.

To address this concern, Microsoft worked closely with several hardware vendors to offer prebuilt and prehardened ISA Server 2006 Hardware Appliances. These servers look and feel like traditional firewalls and come pre-built with multiple NICs, quick-restore CDs, and a presecured Windows Server 2003 Operating System installed. Many of the ISA servers deployed utilize these hardware devices, and their popularity is subsequently increasing.

There are many advantages to deploying an ISA Server solution using a dedicated hardware device. Installation time is greatly reduced, recovery is simplified, and many of these devices offer specialized functionality, such as specialized VPN appliances, caching servers, and enhanced intrusion detection capabilities.

Reducing Administrative Overhead and Potential for Errors with Simplified Management Tools

A major source of security breaches on all firewalls and security solutions comes down to simple misconfiguration of those devices by administrators. A robust, secure firewall solution becomes nothing more than a router if an administrator accidentally opens it up to all traffic. This concept is often glossed over during a security design process, but it is stunning how often simple typos or misconfigurations result in security breaches.

ISA Server 2006 sports a greatly simplified and easy-to-understand set of management tools that reduce the chance of security breaches through misconfiguration. Functionality is not sacrificed for the sake of simplicity, however, and ISA's simplified Management Console, shown in Figure 1.2, allows for a high degree of customization and functionality while simplifying the method in which this functionality is displayed.

NOTE

One of the most common methods hackers use to breach security is to take advantage of a misconfigured firewall. This was one of the main reasons that the ISA tools were simplified and the wizards streamlined, to reduce the chance that an overly complex interface would result in a security breach.

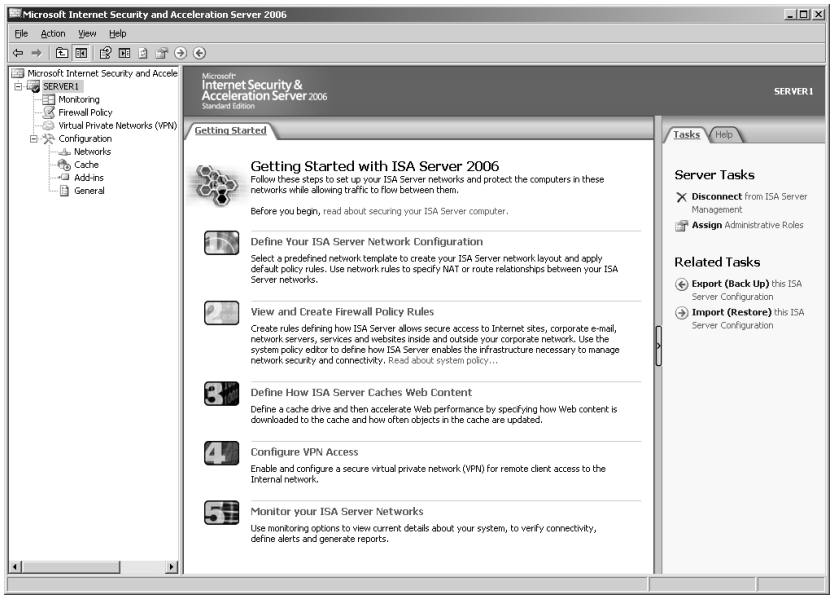

FIGURE 1.2 Using the ISA Server 2006 Management Console.

For more information about the ISA tools and how to effectively use them, refer to Chapter 3, "Exploring ISA Server 2006 Tools and Concepts."

Preserving Investment in Existing Security Solutions

One of the common misperceptions about ISA Server 2006 is that it is an "all or nothing" security solution. For example, it was thought that the goal of ISA was to replace other firewall or security devices with Microsoft-only devices. Subsequently, many Security Administrators were hesitant to consider deploying ISA, seeing it as a potential threat to existing firewalls and technologies. The reality of modern ISA deployments, however, is that they are most commonly deployed as an additional layer of security for an organization, not as a replacement for other security layers. For example, many ISA servers are being deployed as reverse-proxy devices that sit in the DMZ network of an existing firewall solution. As organizations have begun to realize that they do not need to put all their proverbial eggs in Microsoft's basket to be able to utilize some of ISA's enhanced functionality, many of the arguments against deploying ISA have become moot.

The real key to ISA's success lies within its flexibility and its capability to adapt to different security roles within an organization. For smaller organizations that require a complete firewall solution, it delivers. For other larger organizations that are simply looking to secure their Outlook Web Access (OWA) traffic from the Internet, it delivers as well. The different hats that ISA wears are numerous: VPN server, web proxy, Application-layer filter, RPC filter for WAN segment traffic, intrusion detection server, and many more. The capability of ISA to integrate and work with existing security solutions enables organizations to preserve their existing investment in security solutions.

NOTE

For more information on deploying ISA as an additional security layer to an existing third-party security environment, see Chapter 7, "Deploying ISA Server as a Reverse Proxy in an Existing Firewall DMZ."

Understanding the History of ISA Server 2006

Although ISA Server has only recently begun to gain wide industry acceptance, it actually has a long history relative to other computer products. The original version of this product, Proxy Server 1.x/2.x, was geared more toward web caching and proxy capabilities, but newer versions, namely ISA Server 2000, ISA Server 2004, and the newest version, ISA Server 2006, have stressed and focused on the security aspects of the product, improving them and adding functionality. To better understand where ISA Server is today, it is important to get a better understanding of how it got where it is.

Outlining Initial Microsoft Security Solutions

In the early days of networking, before the wide acceptance of the Internet, the focus of security was more directed toward making sure that files and folders on a network were kept safe from prying eyes. Communications between computers were deliberately built to be open and extensible, to facilitate the transfer of information between the devices on the network. As networking evolved, these networks became more and more interconnected, often to other networks that could not be trusted, such as the Internet in general. To protect computers from access via these outside networks, devices known as firewalls were placed between the untrusted and trusted networks to block access from the former to the latter.

While this was occurring, Microsoft products were changing and evolving to match the computing needs of the time, and focus was placed on making Microsoft products embrace the Internet. Focus was put on the need to provide enhanced access for clients to the Internet. As a direct result of this, the development of a product to provide web proxy capabilities to Microsoft clients took shape.

Exploring a New Product—Proxy Server

In 1996, the Internet browser wars between the Netscape Navigator product and Microsoft's Internet Explorer were in full swing, and Microsoft was constantly looking for ways to improve the capabilities of Internet Explorer. Netscape had begun to sell a web proxy product, which optimized Internet web browsing by caching the images and text from web pages to local servers, enabling clients to access them quickly. At this time, connections to the Internet were much more expensive, relatively speaking, and the need to take full advantage of the bandwidth provided to an organization created the need for products to optimize these connections.

In direct response to these needs, Microsoft released the first version (1.0) of Proxy Server, a new product to provide web proxy capabilities for clients. The capabilities of version 1.0

of the product were significantly less than those of Netscape or other proxy products available at this time, however, and industry support for the product was lacking.

Following closely on the release of version 1.0 was version 2.0 , which equalized many of the disparities between Microsoft's Proxy Server product and the competitors. Proxy Server 2.0 introduced the capability to create arrays of servers for redundancy and provided support for HTTP 1.1 and FTP. In addition, the capability to "reverse proxy" was added, protecting internal web servers by acting as a bastion host, or first layer of defense for untrusted traffic. The release of this version of the product was much more successful, and the Proxy Server product celebrated much wider industry acceptance as a web-caching and reverse-proxy product.

Unleashing a New Model: The Internet Security and Acceleration Server 2000

Although Proxy Server 2.0 provided for a wide array of security features, it did not enjoy broad industry acceptance as a security device for one reason or another. Microsoft wanted to focus more attention on the product's security capabilities, so it added more to the 3.0 version, and rebranded it as the Internet Security and Acceleration (ISA) Server 2000. This rebranding directed attention to its security capabilities, while still giving a nod to the web acceleration component, the caching capabilities.

ISA Server 2000 introduced an impressive new array of features, nearly all of which focused on turning it into a full-functioned security device. This version of the product was the first that marketed it as a firewall by and of itself. It was this claim that was greeted with skepticism by the security community, given the somewhat shaky track record that Microsoft products had at that time.

The politics of the security community being what they were, ISA Server 2000 faced an uphill battle for acceptance. In addition, deficiencies such as the lack of multi-network support, confusing firewall rules, and a haphazard interface limited the large-scale deployment of ISA 2000.

Unveiling the Next Generation: ISA Server 2004

While ISA Server 2000 was slowly gaining ground, the ISA Server team started work on the next version, code-named Stingray. The result of this project was the product released as the Internet Security and Acceleration Server 2004. This version of ISA was vastly improved over the previous versions of the product, and it quickly became noticed in the wider security community. In addition to fine-tuning and honing the capabilities it inherited from ISA Server 2000, ISA Server 2004 introduced a wide variety of new and improved security features that further extended its capabilities.

ISA Server 2004 was originally released with only a standard edition of the product. The Enterprise edition debuted the following year, expanding upon ISA's capabilities even further. Finally, predating the release of ISA Server 2006, Service Pack 2 for ISA Server 2004 added many of the same pieces of functionality recently included in ISA Server 2006, such as HTTP compression support, DiffServ, and other enhancements.

Expanding on ISA Server 2004's Success with ISA Server 2006

Microsoft released the next interim build of ISA Server 2004 as a new generation and relabeled it as ISA Server 2006. This version is similar in many ways to ISA Server 2004, with specific enhancements made to several key areas. In a way, it really can be thought of as ISA Server 2004 Service Pack 3, but instead it has been relabeled. The learning curve between ISA 2004 and ISA 2006 is not steep, however, and administrators familiar with ISA 2004 will immediately be familiar with the 2006 model. That said, the evolution of the ISA Server 2006 product to the spot that it inhabits today is impressive.

What's extremely important to note about ISA Server 2006 is that it is one of the first security products released by Microsoft that has really been taken seriously by the broader Internet Security community. ISA Server 2006 is a full-fledged Internet firewall, with Virtual Private Network (VPN) and web-caching capabilities to boot. The debate between pro-Microsoft and anti-Microsoft forces is far from over, but politics aside, the product that has been released is an impressive one.

Exploring ISA Server 2006's New Features

In addition to the enhanced features in ISA Server 2000, ISA Server 2004 and 2006 introduced the following new features:

- **Multiple network support and per-network policies—**ISA Server 2006 introduced the capability to set up and secure ISA between multiple networks. For example, you can set up ISA to act as a firewall between the Internet, an internal network, a perimeter (DMZ) network, a wireless access network, a VPN clients network, and many more. In addition, you can configure unique policies between each network, such as restricting traffic to a DMZ network or securing RPC traffic across WAN segments. For more information on this feature set, see Chapter 5, "Deploying ISA Server 2006 as a Firewall."
- **Support for complex and customizable protocols—**In addition to including a wide array of known protocol support for rules, ISA Server 2006 includes support for custom protocols. These protocols can be defined and specific filters can be created to scan for defined attack patterns in the custom traffic.
- **New server and OWA publishing rules—**ISA Server 2006 includes a vast assortment of server publishing rules, including sophisticated OWA publishing rules that utilize advanced functionality such as forms-based authentication and reverse-proxy capabilities. For additional reading on these features, see Chapter 12, "Securing Outlook Web Access (OWA) Traffic."
- **Remote Procedure Call (RPC) filtering support—**Of particular note in ISA Server 2006 was the addition of RPC filtering support, which enables an administrator to specify what type of RPC traffic will be allowed from one network to another. For example, a rule could be set up to allow only MAPI Exchange access or Active Directory replication traffic across segments, while blocking other RPC access, such

as the kind that spawns attacks and exploits. For more information on RPC filtering, see Chapter 14, "Securing Web (HTTP) Traffic."

- **End-to-end secure web publishing capabilities—**The web publishing rules improved in ISA Server 2006 allow for end-to-end securing of Secure Sockets Layer (SSL) encrypted web traffic from client to ISA Server, and then back to web server. When the traffic is decrypted at the ISA Server, it can be inspected for viruses and HTTP exploits. The traffic is then re-encrypted before being sent to the web server.
- **RADIUS and SecurID authentication support—**In addition to supporting Active Directory authentication, ISA Server 2006 now supports authentication natively against a RADIUS or RSA SecurID authentication infrastructure. This enables an ISA Server to be a member of a workgroup, as opposed to a domain member.
- **Stateful inspection for VPN connections—**In this version of ISA Server, all traffic that passes through ISA is inspected for Application-layer attacks (stateful inspection). This includes VPN connections as well.
- **VPN quarantine control features—**ISA Server 2006 introduces the capability to provide granular control to VPN clients by enabling administrators to restrict new VPN connections to a separate quarantine network. This network can have strict access restrictions placed on it. In this model, VPN users are not moved into the regular VPN users network until it can be established that they satisfy certain criteria, such as the installation of virus-scanning software.
- **Enhanced monitoring, logging, and reporting—**ISA Server 2006 includes superb reporting, monitoring, and logging capabilities, including capabilities to write logs to a SQL-desktop version (MSDE) database. ISA can be configured to automatically generate rich reports for client web access, security events, protocol utilization, and much more. Monitoring of ISA is further enhanced with the use of the ISA Management Pack for Microsoft Operations Manager (MOM) 2000/2005. For more information on monitoring ISA Server, refer to Chapter 19, "Monitoring and Troubleshooting an ISA Server 2006 Environment."
- **Forms-based authentication for all web sites—**This includes cookie-based auth forms for SharePoint Products and Technologies, OWA, and other web sites. This is a new feature in the 2006 release of the product.
- **Enhanced branch office support tools—**Another feature new in ISA 2006, the support for branch office VPN using ISA Server has been greatly enhanced and streamlined with a new Branch Office VPN wizard.

The wide variety of features included in ISA Server 2006 makes it very versatile, and it can be deployed to take advantage of one, two, or multiple functions. For example, ISA could be deployed as a full-function firewall, allowing VPN access and web caching. Or it could be deployed simply to filter RPC connections between network segments. An added advantage to this flexibility is the fact that only those functions that are required are turned on. This reduces the surface area that is exposed to attack, reducing the overall threat.

Choosing the Operating System for ISA Server 2006

It is necessary to install and deploy ISA Server 2006 servers on the Windows Server 2003 platform. Improvements in reliability, functionality, and, most importantly, security dictate this. With ISA Server 2004, it was previously possible, though not recommended, to install ISA Server 2004 on the Windows 2000 Operating System. This is no longer an option with the 2006 version. In fact, 2006 requires both 2003 and Service Pack 1 at a minimum to be installed.

It is important to note that because the ISA server holds a very important security role, it is essential that you patch the operating system with the critical updates Microsoft releases. This includes the necessary Service Pack 1 or Windows Server 2003 R2 Edition and any new Service Packs for ISA Server 2006, when they become available, which both introduce advanced security and functionality. For more information on updating ISA Server and Windows with the latest in security and updates, see Chapter 2, "Installing ISA Server 2006."

Choosing Between ISA Server 2006 Enterprise or Standard Editions

ISA Server 2006 comes in two versions: an Enterprise version and a Standard version. Each version offers different functionality, with the Standard version of the product geared toward small and mid-sized organizations, and the Enterprise version designed for medium to large organizations. The Enterprise version of the software includes all the functionality of the Standard edition, but with the addition of the following:

- **Array Capabilities—**ISA Server 2006 Enterprise edition includes the capability to create *arrays*, which allow multiple servers connected to the same networks to act in tandem to process firewall, VPN, and cache requests. These arrays use the Cache Array Routing Protocol (CARP) to communicate changes and topology information.
- **Integrated Network Load Balancing (NLB)—**In addition to the general NLB support provided by the Standard version, the Enterprise version of ISA Server includes advanced integrated support for NLB, allowing an administrator to make changes and manage NLB directly from the ISA Management Console.
- **ADAM Centralized Storage—**A huge improvement over ISA Server 2000 Enterprise edition is the added capability for Enterprise Configuration information to be stored in a separate instance of Active Directory in Application Mode (ADAM), rather than in the internal Active Directory forest schema. This enables the external-facing ISA Enterprise servers to maintain their configuration in an isolated environment, without unnecessarily exposing internal Active Directory services to attack.
- **Centralized Management and Monitoring—**ISA Server Enterprise edition allows for management of a highly scalable ISA solution, with multiple ISA arrays in multiple locations. This allows for centralized management of a complex network infrastructure.

For more information on the advanced capabilities of the Enterprise edition of ISA Server 2006, refer to Chapter 6, "Deploying ISA Server Arrays with ISA Server 2006 Enterprise Edition."

Detailing Deployment Strategies with ISA Server 2006

What makes ISA Server stand out as a product is its versatility and capability to play the part of multiple roles in an environment. In addition to the capability to be deployed as a fully functional Application-layer firewall, ISA can also provide web caching, Virtual Private Network support, reverse proxy, and combinations of any of them. It is subsequently important to understand all the potential deployment scenarios for ISA when considering the product for deployment.

Deploying ISA Server 2006 as an Advanced Application-Layer Inspection Firewall

ISA Server 2006 was designed as a full-function firewall that provides for the type of functionality expected out of any other firewall device. At a base level, ISA enables you to block Internet traffic from using a specific port, such as the RPC or FTP ports, to access internal resources. This type of filtering, done by traditional firewalls as well, provides for filtering of Internet Protocol (IP) traffic at the Network layer (Layer 3). The difference between ISA and most other firewalls, however, comes with its capabilities to filter IP traffic at the more complex Application layer (Layer 7). This functionality enables an ISA firewall to intelligently determine whether or not IP traffic contains dangerous payloads, for example.

Because of the advanced IP filtering capabilities of ISA, it is becoming more common to see small to mid-sized organizations deploying ISA Server 2006 as a full-fledged edge firewall, similar to what is shown in Figure 1.3. ISA Server 2006 has passed many of the security tests that have been thrown at it, and it has proven to have firewall functionality beyond many of the more common firewall products on the market today.

For more information on the capabilities of ISA Server 2006 as a firewall device, refer to Chapter 5.

Securing Applications with ISA Server 2006's Reverse-Proxy Capabilities

Although ISA Server 2006 is marketed as an edge firewall, it is more common in organizations, particularly in mid-sized and larger ones, to see it deployed strictly for reverse-proxy capabilities. This functionality enables ISA to protect internal web and other application resources from external threats by acting as a bastion host.

To hosts on the Internet, the ISA Server looks and acts like a regular web or application server. Requests made by the client are then relayed back to the actual machine that performs the services, but not before being inspected for exploits or threats. In addition, it

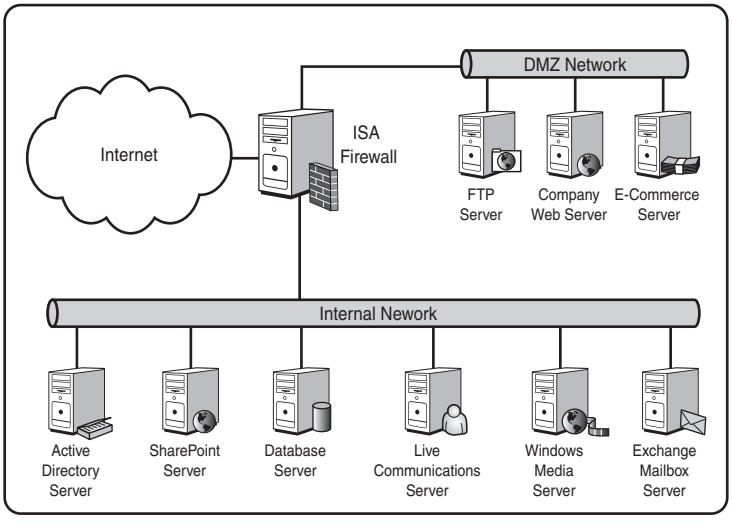

FIGURE 1.3 Deploying ISA Server 2006 as a firewall.

can also be configured to authenticate the user in advance before allowing requests to be relayed back, further securing the infrastructure.

For more information on utilizing the reverse-proxy capabilities of ISA Server, see the chapters in Part III.

Accelerating Internet Access with ISA Server 2006's Web-Caching Component

The original function of ISA Server when it was still known as Proxy Server was to act as a simple web proxy for client web traffic. This functionality is still available in ISA Server, even as the focus has been directed more to the system's firewall and VPN capabilities. By enabling the caching service on an ISA server, many organizations have realized improved access times for web and FTP services, while effectively increasing the available bandwidth of the Internet connection at the same time.

The concept of web and FTP caching in ISA Server 2006 is fairly straightforward. All clients configured to use ISA for caching send their requests for web pages through the ISA Server, similar to what is shown in Figure 1.4. If it is the first time that particular page has been opened, the ISA Server then goes out to the Internet, downloads the content requested, and then serves it back to the client, while at the same time keeping a local copy of the text, images, and other HTTP or FTP content. If another client on the network requests the same page, the caching mechanism delivers the local copy of the page to the user instead of going back to the Internet. This greatly speeds up access to web pages and improves the responsiveness of an Internet connection.

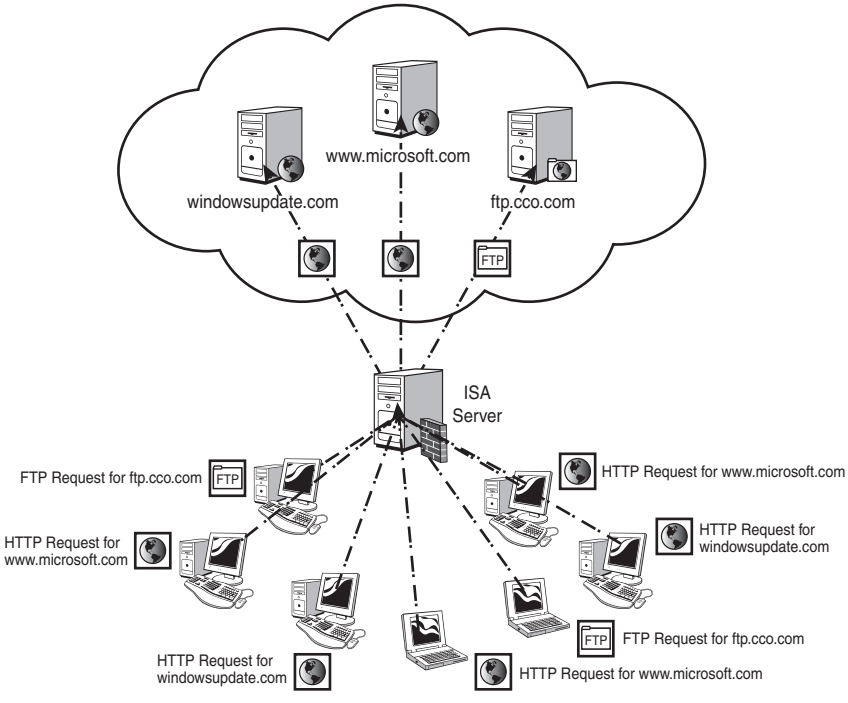

FIGURE 1.4 Deploying ISA Server 2006 as a web-caching server.

NOTE

An added advantage to using ISA Server 2006 as a content-caching server is that all of the HTTP traffic that clients request is scanned for exploits and viruses as well, decreasing the threat of clients being infected with spyware, viruses, and other scumware.

For more information on configuring ISA for web and FTP caching, refer to Chapter 8.

Controlling and Managing Client Access to Company Resources with Virtual Private Networks

Some of the more major improvements to ISA Server 2006 have been in the area of Virtual Private Networks (VPNs). VPN functionality has been greatly improved, and the flexibility of the VPNs for access rules is robust. Deployment of an ISA Server 2006 VPN solution is an increasingly common scenario for many organizations. The capabilities for clients to securely access internal resources from anywhere in the world is ideal for many organizations.

VPN deployment with ISA Server 2006 typically involves a secure, encrypted tunnel being set up between clients on the Internet and an Internet-facing ISA firewall. After the clients have authenticated, they are granted access to specific internal resources that are defined

by the ISA administrator. The resources that can be accessed can be designated via access rules, so the control can be very granular.

In addition to this control, ISA Server also makes it possible to quarantine VPN users that do not comply with specific rules that can be set up. For example, ISA can be configured to quarantine clients that do not have antivirus programs installed. Different access rules can be configured for the Quarantine VPN Users network as well, restricting their access even further, for example.

Finally, ISA Server also includes the ability to set up site-to-site VPN connections to remote sites across the Internet. This enables networks to be joined across VPN links. An added advantage is that the Internet Key Exchange (IKE) protocol used to set up this connection can also be used to set up a site-to-site VPN between an ISA Server and another third-party VPN product. This functionality has been greatly enhanced over the 2004 version of the product as well.

For more information on working with VPNs in ISA Server 2006, refer to Chapters 9 and 10.

Using the Firewall Client to Control Individual User Access

In addition to the default capability to support traffic from any Internet client (SecureNAT clients), ISA includes the capability to restrict, control, and log individual user firewall access through the installation and configuration of ISA firewall clients. Although it is a less common deployment scenario by virtue of the need to install and support a client component, using the ISA Firewall Client can create scenarios that are more secure, and also enable an administrator to control firewall policy based on individual users or groups of users.

For more information on deployment scenarios involving the ISA Firewall Client, see Chapter 11, "Understanding Client Deployment Scenarios with ISA Server 2006."

Augmenting an Existing Security Environment with ISA Server 2006

One of the major steps forward for ISA Server was the change in focus from an assumption of ISA in a Microsoft-only environment to a focus where ISA is an additional layer of security to existing security technologies. ISA Server is being deployed more often recently to supplement security in many organizations, and this capability to "play well" with other firewalls and security applications is a welcome improvement.

Utilizing ISA Server 2006 in Conjunction with Other Firewalls

A common deployment scenario for ISA Server 2006 systems has been as a reverse proxy or dedicated VPN server that sits as a unihomed (single network card) server in the Perimeter (DMZ) network of an existing firewall. This is where the integration of ISA with other security devices really shines. The advantage to deploying ISA in this method is that it serves as an additional layer of security in an existing environment, improving the environment's overall security. Security works best in layers because it is more difficult to

compromise a system that has multiple mechanisms that must be defeated before an unauthorized user is able to gain access.

To this end, ISA is proving to be a commonly used security tool that satisfies specific needs, rather than a whole host of needs at once. For example, a large number of ISA deployments serve a single purpose: to secure traffic to Outlook Web Access servers or other web-related servers while sitting in the DMZ of an existing packet-layer firewall, similar to what is shown in Figure 1.5. Of course, ISA can do more, but it is this capacity to do specific jobs very well that bodes well for ISA's acceptance among the overall security industry.

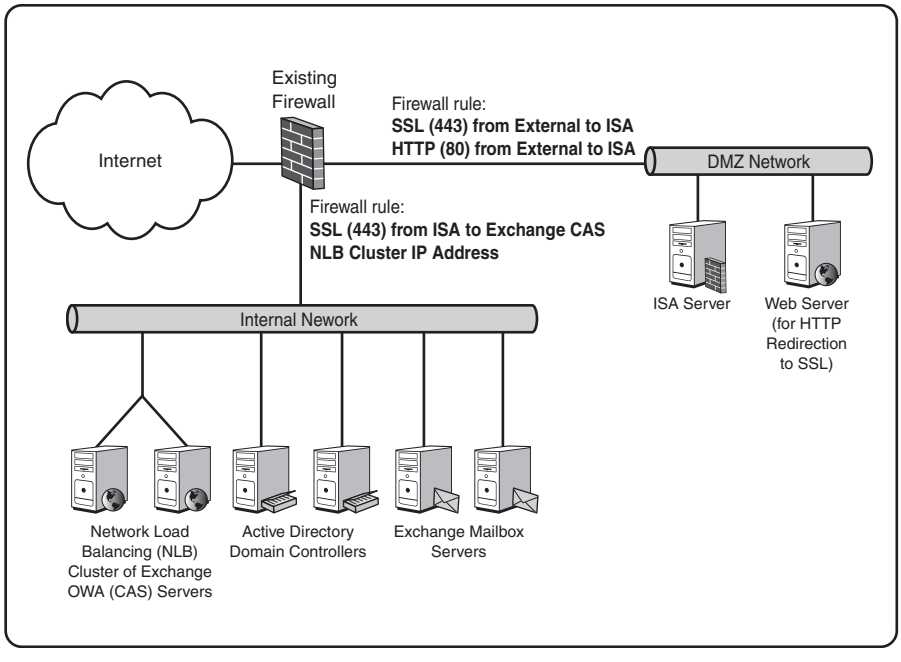

FIGURE 1.5 Deploying ISA in the DMZ of an existing firewall to secure OWA traffic.

For additional reading on this concept, see Chapter 7.

Deploying ISA Server 2006 in a RADIUS Authentication Environment

ISA Server 2006 supports authentication and logging against a Remote Authentication Dial-In User Service (RADIUS) environment, allowing for security integration in environments with an existing investment in RADIUS technologies. By providing this support, ISA also allows for scenarios where the ISA server is not a Windows NT/AD Domain Member. This decreases the overall threat associated with deploying an ISA server in certain circumstances, such as when it is deployed in the DMZ network of an existing firewall.

NOTE

The addition of RADIUS authentication support enables ISA to integrate with a vast array of third-party authentication mechanisms that can use RADIUS protocols to validate users. This substantially increases the breadth of ISA Server 2006 deployment options.

Administering and Maintaining an ISA Server 2006 Environment

After ISA is deployed, the important job of administering and maintaining the environment begins. Fortunately, ISA Server 2006 provides powerful yet easy-to-use tools to assist administrators in these tasks. The ease of use of these tools overshadows the impressive functionality that they provide. Thankfully, the straightforward approach that Microsoft took when designing the tools helps administrators to more easily administer and maintain an ISA Server environment.

Taking Advantage of Improvements in ISA Management Tools

The ISA Server Management Console, shown in Figure 1.6, provides straightforward wizards to assist with complex tasks, and puts all ISA's functionality at the fingertips of an administrator. Configuration, reporting, logging, monitoring, and securing can all be done from the centralized console, simplifying the management experience and making it less likely that configuration mistakes will result in security breaches.

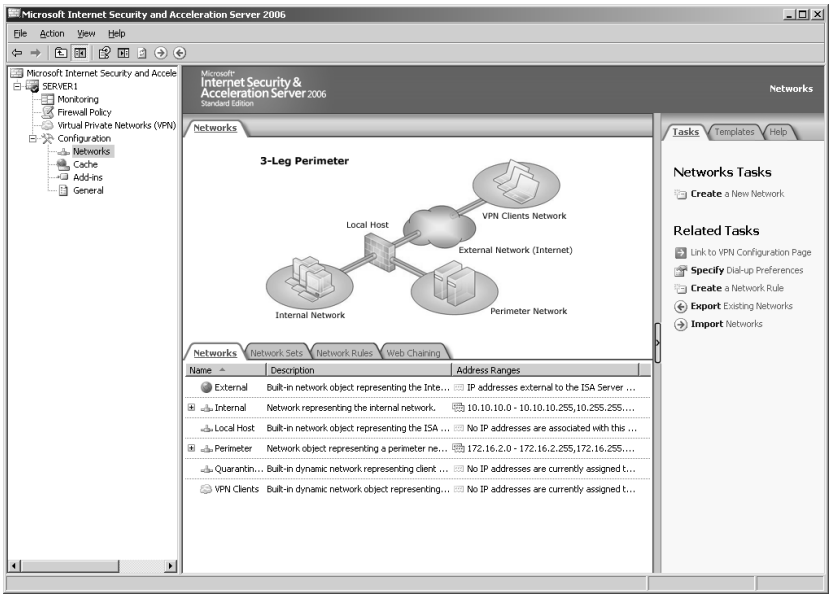

FIGURE 1.6 Using the ISA Server Management Console.

The ISA console also includes several built-in wizards and templates that enable an administrator to perform common functions and procedures, such as publishing a mail server, creating access rules, defining networks, and the like. For example, the New Network Wizard allows the creation of additional networks and their associated network rules quickly, easily, and securely. After the networks are created, the network rules and policies can then be modified to suit the needs of the organization. This offers administrators the best of both worlds, with the simplicity of a wizard combined with the power of a customizable toolbox.

For more information on administering ISA Server 2006, see Chapter 16, "Administering an ISA Server 2006 Environment."

Backing Up and Restoring ISA Server Environments

Backing up and restoring Windows environments has often been a complex and cumbersome process. Fortunately, ISA Server 2006 has learned a lesson from many of its firewall peers, and included an incredibly simple method of backing up the firewall configuration to an XML (essentially text) file that can be then re-imported on other ISA servers or saved for restoration purposes. In addition to the capability to back up the entire configuration to this file, individual ISA elements such as firewall rules can be backed up to individual files, allowing one-by-one restores of ISA elements. This flexibility allows for reduced restoration times and ease of recoverability of whole servers or individual elements.

For more information on backing up and restoring ISA Server 2006 environments, see Chapter 18, "Backing Up, Restoring, and Recovering an ISA Server 2006 Environment."

Maintaining an ISA Server Environment

The "care and feeding" of an ISA Server environment that has been put into place is a key component to an ISA Server deployment plan. Although ISA is typically low maintenance, there are still several important procedures and proactive steps that should be followed to keep ISA running smoothly. Chapter 17, "Maintaining ISA Server 2006," covers many of these procedures, and includes the types of daily, weekly, monthly, and quarterly tasks that should be performed to keep ISA in top shape. In addition, the concept of updating ISA with OS and other patches is covered in this chapter.

Monitoring and Logging Access

Deployed out of the box, ISA includes a robust logging mechanism that can be configured to use a SQL-style MSDE database for logging purposes. These logs can be easily queried, and powerful reports, such as the one shown in Figure 1.7, can be generated to provide administrators with a detailed analysis of the type of traffic sent across ISA servers.

NOTE

The MSDE Database, installed as an option with ISA Server 2006, is configured to allow only local access from a user logged in to the console. This prevents attacks such as SQL Slammer, which take advantage of a SQL or MSDE server with open ports to the network.

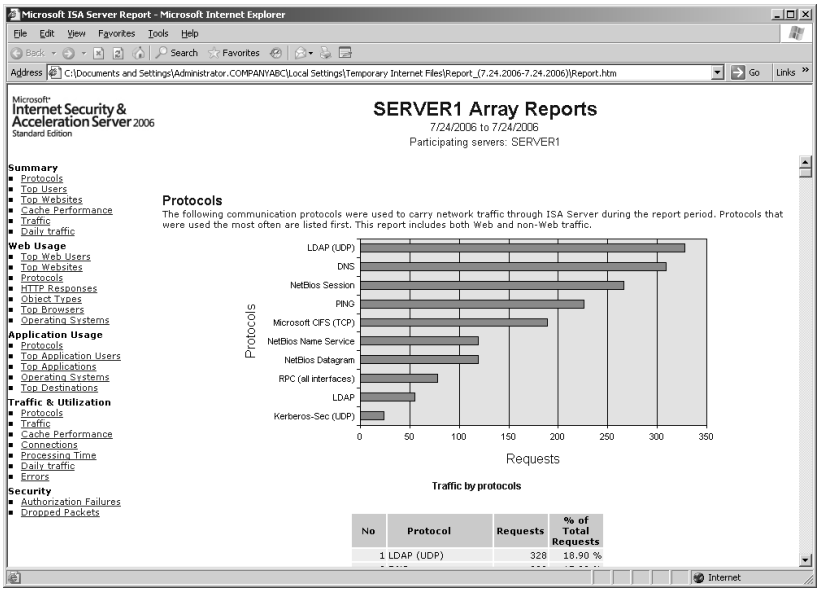

FIGURE 1.7 Viewing an ISA Server 2006 report.

It is critical to proactively respond to ISA alerts, intrusion attempts, and performance data generated by ISA servers; therefore, it may be prudent in certain cases to deploy a means of gathering ISA logging and performance data in a centralized location and automatically alerting on this information. Chapter 19 covers the use of the ISA Server 2006 Management Pack for Microsoft Operations Manager (MOM), which allows for proactive management, monitoring, and troubleshooting of an ISA environment.

Using ISA Server 2006 to Secure Applications

One of the distinct advantages to an ISA Server 2006 solution is the software's capability to scan all traffic that hits it for exploits and threats, before that traffic hits its intended target. As previously mentioned, ISA performs these functions through a process of scanning that traffic at the Application layer through a series of customizable filters, such as an HTTP filter for web traffic that knows to look for common exploit strategies like those employed by the Code Red, Nimbda, and Ject viruses. These capabilities are the central selling point for one of ISA's most popular features: the capability to secure and protect Internet-facing applications from attack.

Securing Exchange Outlook Web Access with ISA Server 2006

The current single most common deployment scenario for ISA Server 2006 involves an ISA Server being set up to provide reverse proxy to Exchange Outlook Web Access (OWA) servers. The ISA development team worked very closely with the Exchange development team when developing specific OWA filters for this, and the integration between the two

technologies is very tight. In addition to the standard benefits that reverse-proxy capabilities provide, deploying ISA to secure OWA also has the following key selling points:

- **SSL to SSL end-to-end encryption—**ISA Server 2006 is one of the few reverse-proxy products to currently support end-to-end Secure Sockets Layer (SSL) support from the client to the ISA server and back to the Exchange OWA server. This functionality is provided via certificates installed on both Exchange and the ISA server, allowing the OWA traffic to be unencrypted at the ISA box, scanned for exploits, then reencrypted to the Exchange servers. This allows for a highly advanced ISA design, particularly in configurations where ISA is deployed in the DMZ zone of an existing firewall.
- **Forms-based authentication on ISA—**Introduced with Exchange Server 2003, forms-based authentication (FBA) enables users to authenticate against an OWA server by filling out information on a form, such as the one shown in Figure 1.8. This also has the added advantage of preventing any unauthenticated traffic from accessing the Exchange server.

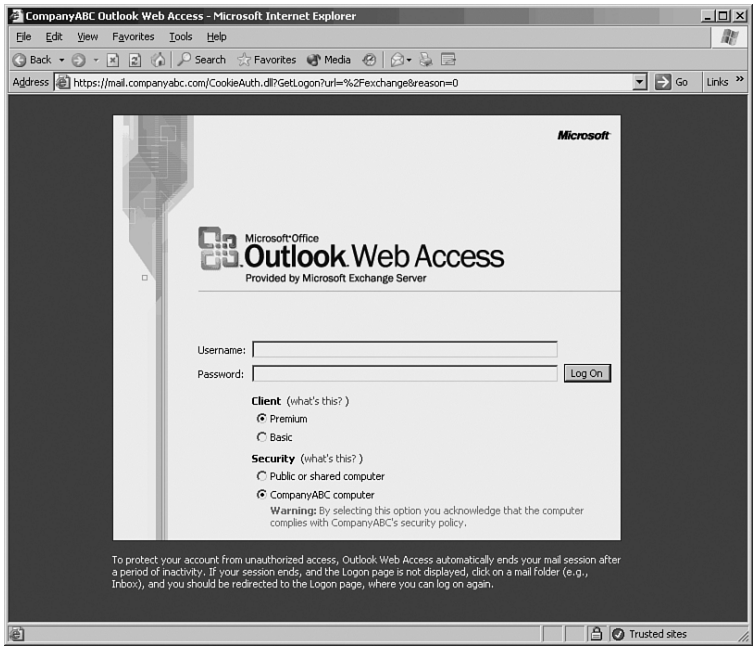

FIGURE 1.8 Using forms-based authentication to authenticate against OWA servers.

- **Unihomed ISA Server support—**ISA OWA Publishing also can be deployed on a unihomed (single network) card in the existing DMZ of a firewall such as a Cisco PIX or other packet-filter firewall. In fact, this is one of the more common deployment

scenarios for ISA Server. This flexibility enables ISA to function as an appliance server that serves as a bastion host to Exchange services.

NOTE

Many Exchange deployment designs are replacing Exchange front-end servers in the DMZ with ISA servers in the DMZ that communicate with front-end servers in the internal network. This has the added advantage of securing the services in a DMZ configuration, but without opening the multitude of ports required by a front-end server to be able to communicate with Exchange database servers and Global Catalog servers.

In addition to filtering and protecting OWA traffic, ISA also includes custom filters to scan and protect other mail-related traffic such as Simple Mail Transport Protocol (SMTP) and Exchange MAPI (Outlook-style) access. For more information on securing mail-related services, including step-by-step deployment scenarios, see Chapter 12.

Locking Down Web Application Access

As previously mentioned, the HTTP filter included with ISA Server 2006 includes pre-installed knowledge to identify and eradicate HTTP threats before they access any web services, including traditional web servers and web applications. It is under this pretext that ISA can be deployed to secure external-facing web servers and web traffic. In addition, the HTTP filter is customizable, and can be modified or extended manually or can use third-party software products to do things such as limit specific HTTP calls, block executable downloads, or limit access to specific web sites. For more information on setting up ISA to secure web services, refer to Chapter 14, "Securing Web (HTTP) Traffic."

Securing Remote Procedure Call (RPC) Traffic

One of the more potent threats to Windows infrastructure in recent years has been the rise of viruses and exploits that take advantage of Remote Procedure Call (RPC) functions to take over computers and wreak havoc on client operating systems. Many of these threats have been extremely damaging to the infrastructure of organizations, and the method of containing the spread of them in the past has involved a complete shutdown of the RPC communications infrastructure between network segments.

ISA Server 2006 provides an invaluable tool against these types of RPC exploits through its capability to screen RPC traffic and intelligently open only those ports that are necessary for specific RPC services to function. For example, an ISA server could be positioned as a router between multiple network segments, a server segment, and client segments, and filter all RPC traffic between those segments, as the diagram in Figure 1.9 illustrates. It could then be configured to allow only Exchange MAPI Access (a form of RPC traffic) to that segment, blocking potentially infected clients from infecting servers or other clients on other segments.

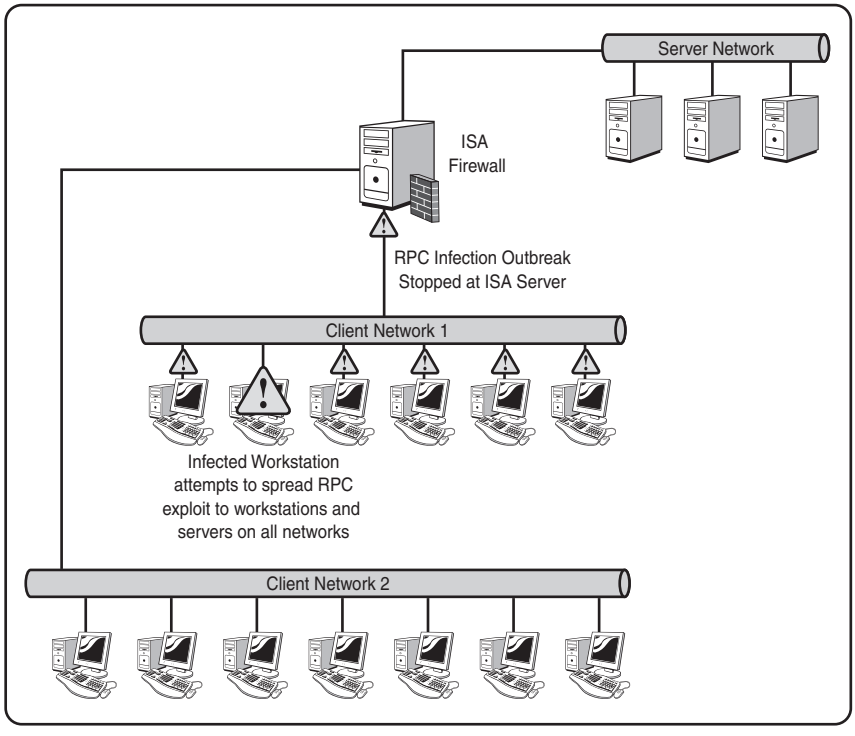

FIGURE 1.9 Securing RPC traffic between network segments.

For more information on the RPC filtering capabilities of ISA Server 2006, see Chapter 14.

Summary

The growth of Microsoft's Internet Security and Acceleration Server has corresponded with the increase in the types and quantities of threats faced by organizations on the Internet today. Fortunately for these organizations, the capabilities of ISA Server 2006 are many, and it has found a place in their security topology as a firewall, caching server, VPN device, reverse-proxy machine, RPC filter, and more.

ISA Server 2006's simple and eloquent design sits on top of a complex and capable security platform, capable of advanced Application-layer packet inspection, complex firewall rules, and multiple network support. Before deploying ISA, it is important to understand the specifics of what it can do and how to configure it. Consequently, the subsequent chapters of this book present detailed descriptions of ISA's capabilities, as well as step-by-step deployment scenarios, best practices, and tips to help organizations make the most out of an ISA Server investment.

Best Practices

- Become familiar with the wizards, toolbox, and tasks in the ISA Server Management Console.
- Consider deploying ISA Server 2006 as an additional security layer to an existing firewall environment, particularly where a strong investment currently exists.
- Consider the use of an ISA Server Hardware solution that provides prebuilt and presecured ISA solutions.
- Where possible, take advantage of the enhanced caching capabilities of ISA Server 2006, which are turned off by default.
- Secure Outlook Web Access (OWA) by using ISA reverse-proxy and forms-based authentication whenever possible.
- Consider deploying the Enterprise version of ISA Server 2006 if more than two ISA servers will be deployed or if there are advanced design considerations.
- Deploy ISA Server 2006 on the latest Windows and ISA security patches.
- Consider the use of third-party add-ins for ISA Server that can enable advanced intrusion detection, web-content filtering, improved VPN support, and much more.
- Document and back up the ISA Server 2006 configuration often to ensure quick recovery in disaster recovery scenarios.