Guide to the Secure Configuration and Administration of Microsoft ISA Server 2000

The Network Applications Team

of the

Systems and Network Attack Center (SNAC)

Author:
Trent Pitsenbarger

Updated: 8 Aug. 2002
Version 1.5

This Page Intentionally Left Blank

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**

- Many of the security related issues associated with ISA Server are interrelated. The reader is encouraged to gain familiarity with the entire document before proceeding.

- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.

- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- This document is current as of the date listed on the cover page. Please keep track of the latest security patches and advisories on the ISA Server home page at http://www.microsoft.com/ISAServer/ and the Microsoft security bulletin page at http://www.microsoft.com/technet/security/current.asp

Warnings

This Page Intentionally Left Blank

Acknowledgements

Acknowledgements

Trademark Information

Microsoft, MS-DOS, Windows, Windows 2000, Windows NT, Windows 98, Windows 95, Windows for Workgroups, and Windows 3.1 are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries.

All other names are registered trademarks or trademarks of their respective companies.

Table of Contents

Table of Figures

Table of Figures

Table of Tables

Table of Tables

This Page Intentionally Left Blank

Introduction

The purpose of this document is to describe the security mechanisms offered by the Microsoft Internet Security and Acceleration (ISA) Server 2000 (hereafter simply called *ISA Server*). This document addresses the security related configuration settings of the ISA Server that are available to the administrator and the way in which they can be used to enforce an organization's network security policy.

Although a short overview of the general concepts underlying ISA Server is provided in chapter 1, this document is primarily intended for those individuals who are already familiar with these basic concepts and who are very familiar with the TCP/IP protocol. This document is intended to enhance that knowledge by highlighting the specific security settings that are available in ISA Server. As such, there are several ISA Server features that are not addressed simply because they are not security related. For those needing additional background in overall ISA Server administration, numerous books and training programs are available from commercial sources.

It is also assumed that the reader is a knowledgeable Windows 2000 administrator.   A knowledgeable Windows 2000 administrator is defined as someone who can create and manage accounts and groups, understands how Windows 2000 performs access control, understands how to set policies, is familiar with how to setup auditing and read audit logs, etc. This document does not provide step-by-step instructions on how to perform these basic Windows 2000 administrative functions – it is assumed that the reader is capable of implementing basic instructions regarding Windows 2000 administration without the need for highly detailed instructions.

This document is structured as follows. The various chapters are presented in an order that follows the same sequence of events that an administrator might use in setting up ISA Server. It starts with an important notice about operating system security and then proceeds to ISA Server installation, configuring access controls within ISA Server, setting up the packet filter and intrusion detection features, working with ISA Server extensions, enabling the publishing features to allow information from inside the ISA server to be published on the external network (if desired), and finally monitoring the ISA server. The document also details client setup issues. Each section is formatted to provide a narrative introduction followed by a checklist that summarizes the narrative. This is intended to provide both a level of detail for those who may not be familiar with a certain aspect of ISA Server, while also offering a more concise checklist for those who do not need the background material. The checklists are complete – those who are intimately familiar with ISA Server and just want to verify that the proper security related settings have been considered can quickly thumb through the document and only review the checklists.

The document covers the enterprise version of ISA Server.

Getting the Most from this Guide

The following list contains suggestions to successfully secure the Microsoft Server 2000 according to this guide:

WARNING: This list does not address site-specific issues and every setting in this book should be tested on a non-operational network.

- ❑ Read the guide in its entirety. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.

- ❑ Perform pre-configuration recommendations:

  - o Perform a complete backup of your system before implementing any of the recommendations in this guide

- ❑ Follow the security settings that are appropriate for your environment.

Commonly Used Names

Throughout this guide a variety of network names and IP addresses are used in the examples, screenshots, and listings.

WARNING: It is extremely important to replace the network names and IP addresses used in the examples with the appropriate network name and subnets for the networks being secured. These names are not real networks and have been used for demonstration purposes only.

About the Guide to Securing the Microsoft ISA Server 2000

This document consists of the following chapters:

Chapter 1, "Introduction to ISA Server," provides a very basic overview of how ISA Server can be used to improve the security posture of a network.

Chapter 2, "ISA Server Installation," discusses numerous issues related to security that must be considered during an install of ISA Server.

Chapter 3, "Access Control," contains detailed information on the two fundamental elements in implementing this feature in the ISA Server -- *protocol rules* and *site and content rules*.

Chapter 4, "Packet Filtering and Intrusion Detection," recommends enabling specific security measures when configuration these features within the ISA Server.

Chapter 5, "Extensions," gives a brief overview of the extensions that ship with ISA Server with additional detail provided for those settings that are particularly relevant from a security standpoint.

Chapter 6, "Publishing," contains recommendations in regards to publishing servers behind an ISA server.

Chapter 7, "Array and Enterprise Policy," discusses the use of enterprise and array policies as a means of simplifying and consolidating ISA server administrative actions.

Chapter 8, "ISA Clients," discusses the four options for connecting clients on the internal network to the ISA Server – installing ISA firewall client software, use of network address translation clients, using web browsers with a proxy server connection option, and using SOCKS.

Chapter 9, "Monitoring – Alerts and Logging," contains configuration recommendations for types of alerts, alert options, and logging reports.

Chapter 10, "Other Security Relevant Issues," recommends ensuring that the organization's backup policy protects ISA Server settings.

Appendix A, "Further Information," contains a list of the hyperlinks used throughout this guide.

Appendix B, "References," contains a list of resources cited.

Introduction

An Important Note About Operating System Security

This document does not deal with operating system security per se, but instead focuses directly on ISA Server issues. While permissions, registry settings, password usage, user rights, and other issues associated with Windows 2000 security have a direct impact on the overall security of a network, operating system security settings are beyond the scope of this document.

The recommended source of information for how to securely configure the Windows 2000 server and workstation is NSA's Windows 2000 security guide. This guide is comprised of a series of documents covering various aspects of Windows 2000 security which can be obtained at http://www.nsa.gov.

Introduction

This Page Intentionally Left Blank

Chapter

1

Introduction to ISA Server

This chapter provides a very basic overview of how ISA Server can be used to improve the security posture of a network. Many of the concepts presented in this chapter are greatly oversimplified but will be expanded in subsequent chapters.

Overview of ISA Server

ISA Server comprises features that are commonly associated with proxy servers and with firewalls.

The proxy server features of ISA Server are used to enhance the security of communications between client and server applications by allowing the ISA server to service access requests to an external network (typically the Internet) on behalf of the user. ISA Server can authenticate client requests and verify, based upon rules defined by the ISA Server administrator, if the organization's security policy allows the requested connection. Provided the client is requesting an allowed service, it acts on behalf of a client in relaying connection requests from the internal network to the external network and relaying the response back to the client.

When a client packet passes all of the access rules that the ISA Server is configured to enforce, ISA Server will modify the packet, changing the "from" IP address to its own Internet Protocol (IP) address, and pass the packet to the intended external server. The server's response to the packet will then be sent back to the ISA Server and not the original requestor. The ISA server will stop this packet and perform another series of examinations on this incoming packet. If the packet is permitted to enter the internal network, ISA server will send the packet to the target client; thus, the ISA Server will be masquerading as the application server.

Security is enhanced by virtue of the fact that the clients never directly connect to the external network -- the external world can only see one IP address for the entire organization. Security is also enhanced through the enforcement of traffic controls based on service requests. If a service (e.g., FTP) is not approved for use in an organization (or that specific user or computer is not allowed access to that service) the ISA Server can be configured to prevent that service's data from flowing to and from the external network.

In other words, ISA Server supports secure communication between clients and servers by masquerading as servers to the clients and as clients to the servers. It is able to accomplish this task because it resides between the clients and servers on the only path between the two different networks. In essence, it acts as a gateway between the server and client networks. During the masquerading process, the ISA server is able to enforce a series of actions on the packets that are passed.

The firewall features of ISA Server entail the per-user or per-computer access control mechanisms mentioned above along with packet filters and intrusion detection capabilities.

The packet filtering mechanism is another means of controlling the flow of packets between the ISA server and the external network (typically the Internet) by allowing or denying connections from the outside network based upon such variables as source IP address and service type. This can be thought of as a first line of defense – packets that are explicitly blocked by packet filters are not allowed regardless of any other access control setting. For example, even if the proxy server features of ISA Server allow a specific user access to a specific service, for example the Simple Mail Transport Protocol (SMTP), no user will be able to connect to SMTP if a packet filter is enabled to block those packets. The packet filter mechanism is also used to enforce access to published servers that reside on the ISA computer itself and in certain demilitarized zone configurations.

The intrusion detection mechanism monitors traffic through the ISA Server for activity indicative of a small number of common attacks.

Figure 1 illustrates a typical ISA Server setup. There are an infinite number of variations on this basic structure, but in general ISA server is used as illustrated – to provide a security barrier between a trusted network (e.g., an organization's intranet) and an untrusted network (e.g., the Internet). All of the ISA features, which have only been briefly introduced in this section, will be described in much greater detail in the remainder of this document. This document will from time to time build upon this basic setup as necessary to illustrate key concepts, some of which are applicable only in the context of a more involved network.
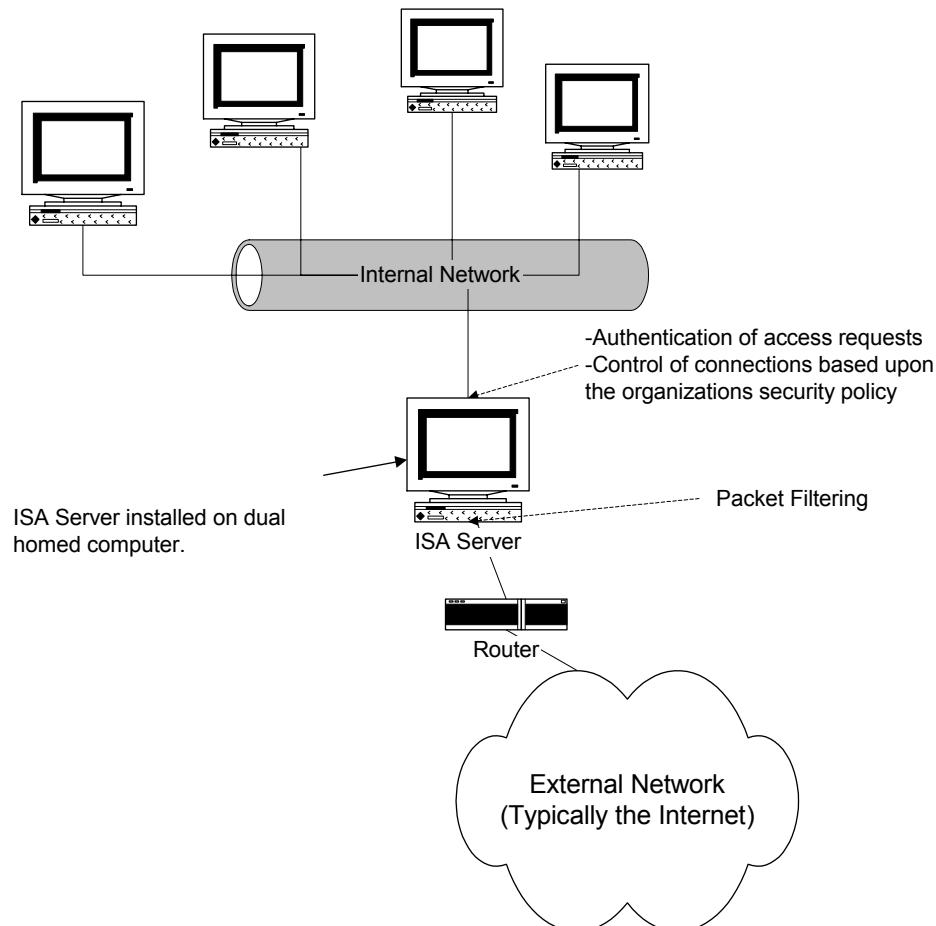
Figure 1 -- A Network Using ISA Server

ISA Server is available in enterprise and standard editions. The enterprise edition is the full-featured version while the standard edition is a simpler product offering a subset of the features. This document focuses on the complete feature set offered by the enterprise edition; however, the guidance offered here is also applicable to the standard edition for those features it shares with the enterprise version. A comparison of the two editions is available at
http://www.microsoft.com/isaserver/productinfo/editioncompare.htm

This Page Intentionally Left Blank

Chapter

2

ISA Server Installation

Pre-Installation

Operating System Security

Operating system security is critical to the secure operation of ISA Server. The recommended source for Windows 2000 operating system security guidelines is the series of guides mentioned on page 3.

It is not uncommon for operating system security guidelines to cause incompatibilities with certain applications. This can happen if permissions on a file or a registry key are made too restrictive, to give a simple example. ISA Server, configured as suggested in this document, has been tested against this operating system guide and no such incompatibilities have been found.

Eliminate Unnecessary Services

In addition to the operating system guidelines detailed above, a series of additional steps toward securing the operating system is recommended:

❑ Do not run unnecessary services or server applications on the computer on which ISA Server will be installed. Note that there is a common misconception that Internet Information Server (IIS) is required to be installed on the machine on which ISA Server is installed. This is not the case – IIS is not required. It is also recommended to unbind **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks** from the external network interface card (NIC) and to disable **NetBIOS over TCP/IP.** To access these settings, open the properties page for **My Network Places** and then open the properties page for the external NIC.

❑ If Terminal Services is installed on the ISA Sever computer it is recommended to unbind it from the NIC on the external interface card. This can be accomplished by opening the **Terminal Services Configuration** utility, opening the property page for **RDP-Tcp**, and navigating to the **Network Adapter** tab. More information concerning the secure configuration of Terminal Server is available in the *Guide to Securing Microsoft Windows 2000 Terminal Services* available at http://www.nsa.gov.

Policy Overview

Before beginning a discussion on installation issues, an understanding of the model ISA server uses for propagating security policies among the various ISA Servers that a larger organization may have is necessary.

ISA Server offers a hierarchical model for controlling how security policies are propagated. ISA Server does this with what is referred to as *enterprise* and *array* policies. Enterprise and Array policies allow an organization to implement a top-down security policy where corporate wide policies are pushed down, via settings in the Active Directory, to all ISA Servers in the organization. Consider as an example a regional corporation which has offices in Baltimore and Washington. Assume that each of these offices uses ISA Server as their gateway to the Internet and that each is sufficiently large so that several ISA Servers are required at the corporate office building in each city to handle the load. Finally assume that all employees are to be allowed to surf the web via HTTP but, perhaps due to a history of employee misuse, a corporate policy has been set that no one in the company is to use the Network News Transport Protocol (NNTP).

The hierarchical policy enforcement mechanisms of ISA Server support this scenario quite nicely. The enterprise policies are at the top of the hierarchy. As the name implies, enterprise policies apply to the entire organization. In this example, the enterprise policy would allow HTTP access but not NNTP.

The next level of hierarchy is *array policies*. The numerous ISA Servers installed at each location would belong to an array. An array policy, as it naturally follows, is the set of rules that applies to all of the ISA Servers within that array – it allows one to manage the array as if it were a single device. If allowed by enterprise policy, rules can be applied at the array level that further restrict enterprise policy – an array policy in our example could not enable NNTP given that its use is prohibited by enterprise policy.
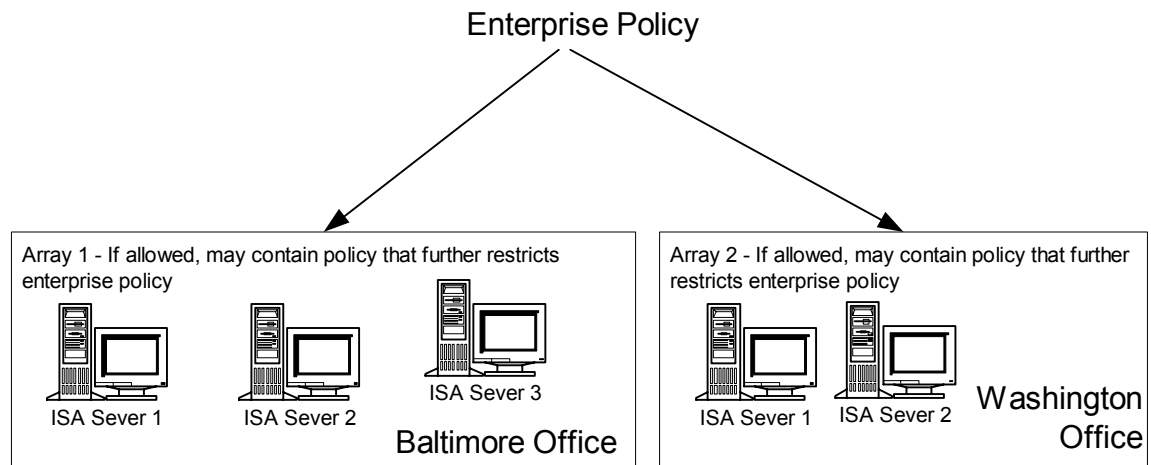
Figure 2 -- ISA Servers Installed In An Array

In order to take advantage of enterprise and array policies ISA Server must be installed into a Windows 2000 domain so that it can have access to the policy information stored within the active directory.

Finally, it is possible to install ISA Server as an independent server. Independent servers do not need to be part of a Windows 2000 domain and can not take advantage of array or enterprise policies.

The appropriate decision regarding whether or not to use enterprise and array policy or independent servers is site dependent and is frequently driven by the size of the network. Standalone servers may suffice for smaller networks while larger networks would tend to

require the use of an array or arrays. This document assumes that arrays are being used.

Installation

There are numerous issues related to security that must be considered during an install of ISA Server:

- Domain Structure

- Policy model and the use of the Enterprise Initialization Utility

- Installation directory and component selection

- Array or independent installation

- Server mode

- Local Access Table

Domain Structure

There are a wide variety of network architectures that can be supported by ISA Server. This document cannot cover the entire variety of possible implementations, but can present a nominal network architecture along with a number of considerations to keep in mind when deciding upon a specific network architecture and deciding where to place ISA Server in the Windows 2000 domain structure.

A very common network architecture that ISA Server readily supports is the notion of a demilitarized zone (DMZ) between the internal network and the external, untrusted network. This builds upon the network example provided in Figure 1 by the addition of a buffer between the internal and external networks and offers a place where services – for example, a web server -- can be published for access by those on the external network. Anytime access is allowed from an untrusted environment there is an obvious security risk. The DMZ, which is sometimes referred to as a *perimeter network*, mitigates this risk by helping to ensure that connections to the published server do not have the ability to access the internal network. A common method of implementing a DMZ is shown in Figure 3:

Intranet — Firewall-b (Allows no incoming connections from Internet) — DMZ — Web Server — Firewall-a (Allows incoming connection from Internet only to the Web Server in the DMZ.) — Internet
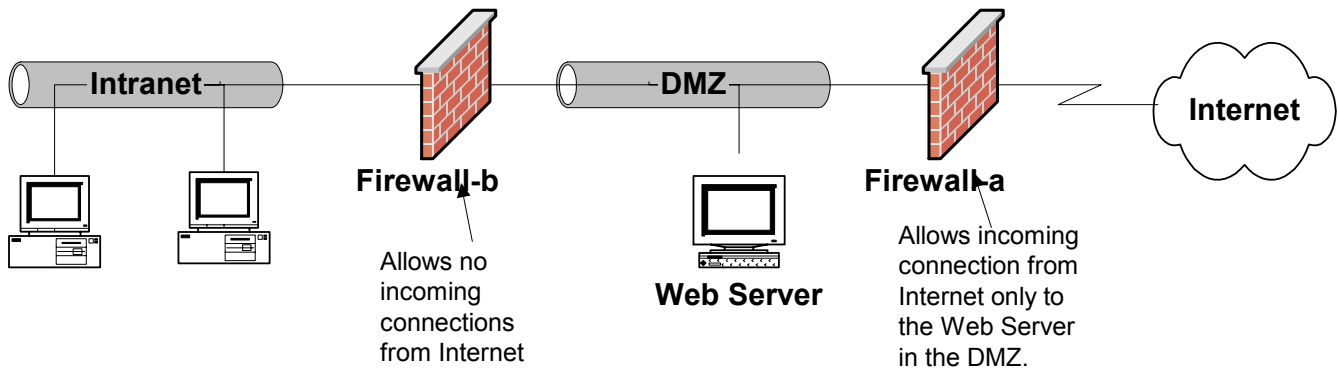
Figure 3 -- A DMZ Utilizing Two Firewalls

While Firewall-a allows incoming connection requests to the web server in the DMZ, security is enhanced in that no incoming connection requests are allowed by Firewall-b. This, of course, helps preclude Internet based attacks from reaching the internal network. Security is optimized if different firewall products are utilized. While Firewall-a in this illustration allows HTTP connection requests to the web server, all other connection requests originating from the Internet should be rejected. If an attacker is able to exploit a vulnerability in Firewall-a to compromise this access policy, having a different firewall at the perimeter of the intranet may decrease the chance that the same vulnerability could be utilized to gain further access.

While ISA Server can be used as either Firewall-a or Firewall-b, its feature set makes it a prime candidate for Firewall-b. ISA Server allows – for those clients running Windows and having appropriately configured clients – the definition of access rules based upon user authentication. Using ISA Server as Firewall-b and making it part of the internal domain structure will allow these per-user rules to be developed. In no case should an ISA Server that fronts an untrusted network (Firewall-a) be part of the internal domain structure. This is also a convenient architecture because in many instances a router is used to connect to the external network. Using a router with a filtering capability can serve the dual role of functioning as Firewall-a. If a filtering router is being utilized, a recommended source for assistance in configuring it is the *Router Security Configuration Guide* which is available from the source listed on page 3.

Policy Model – The Enterprise Initialization Utility

The concept of enterprise and array policies has already been introduced and is discussed in detail in the chapter *Array and Enterprise Policy*. Before you can set up ISA Server as an array member, the ISA Server schema must be installed to Active Directory. ISA Server includes an Enterprise Initialization utility that is used to perform this function. The utility is accessed by running *ISAAutorun.exe* from the ISA Server installation CD and selecting it from the menu that is presented. After the ISA Server schema is imported, all subsequent ISA Server installations to computers in the domain can use the ISA Server schema – it does not have to be installed again.

ISA Server Installation – Installation Directory/Components, Array Policies, Server Mode, Local Access Table

The first decision that one is faced with when installing ISA server is typical for the installation of most applications – deciding which components to install (Figure 4). Most of the components are fundamental to the operation and must be installed. Two components – the *message screener* and the *H.323 gatekeeper service* – warrant discussion. The message screener is used to filter SMTP/POP e-mail traffic associated with a published mail server; however, it is typically not necessary to install the message screener on the ISA Server itself. This is discussed in more detail in the ***SMTP filter*** section. The H.323 gatekeeper service is only required for organizations that require H.323 applications, such as NetMeeting, to work through the ISA Server. If this is not the case, do not install the service.

Both of these services are accessed under the add-in services option highlighted in Figure 4.

The same dialog box also allows one to specify the installation directory. It is recommended that ISA Server be installed on a partition other than where the operating system is installed.   This is sound practice for the installation of all applications in that it can simplify recovery in the event of a hard drive failure or other calamity.
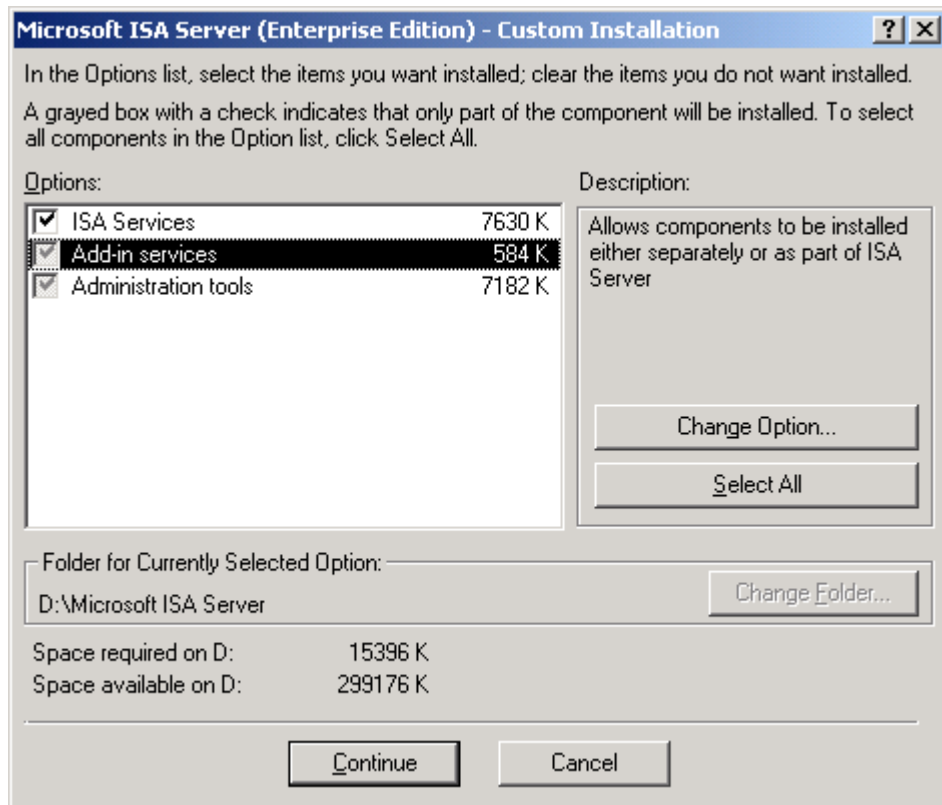
Figure 4 -- Installation Of Add-in Services

The next security related decision one is faced with during an install relates to the discussion detailed above regarding enterprise and array policy. Specifically, one may select to install the ISA server as a standalone server or as part of an array (Figure 5). Again, the specific choice is installation dependant.
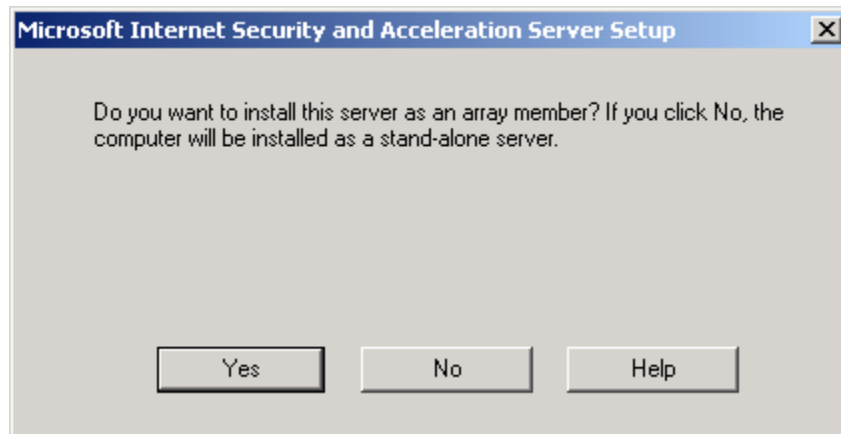
Figure 5 -- Option To Install As An Array Member

If one chooses to install the ISA server as a member of a new array, one will be faced with a decision regarding whether or not enterprise policy should be applied to this new array (Figure 6).
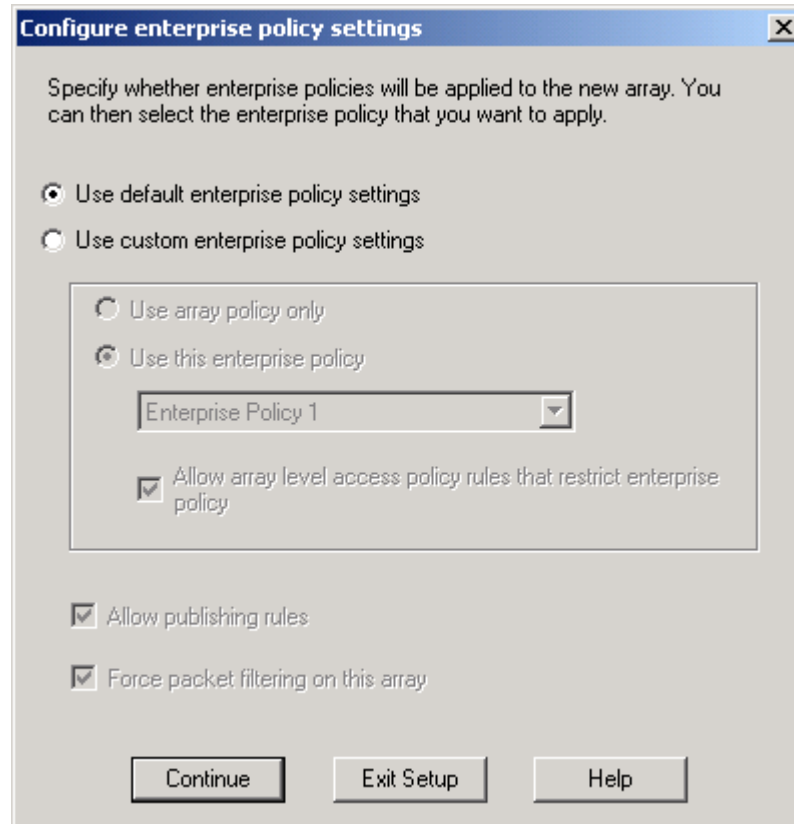
Figure 6 -- Enterprise Or Array Policy

These options allow the enterprise administrator to determine the degree of central authority to be enforced over ISA Servers in the organization. A restrictive policy can be implemented by selecting **use default enterprise policy settings**. A very liberal policy can be allowed by selecting **use custom enterprise policy settings** and **use array policy only** which means that all ISA Server settings are controlled at the array level. A balanced approach can be achieved by selecting **use custom enterprise policy settings, use this enterprise policy** (and selecting the appropriate policy from the drop down list) and **allow array level access policy rules that restrict enterprise policy**.   In this case, the array administrator can define array policy rules but only those which further restrict the enterprise policy rules. It is important to note that some of these settings cannot be undone after installation. A more in-depth discussion of enterprise and array policy is provided in the chapter *Array and Enterprise Policy*.   It is recommended that the organization's ISA Server structure be well thought out before proceeding.

Other options on this dialog box include the option to allow publishing rules to be created. If enabled, this will allow the placement of a server – for example a web server – behind the ISA Server allowing connections by users on the external network (Internet). This is generally a very bad idea unless precautions are taken to partition that web server from the internal network. A popular concept called a demilitarized zone was introduced earlier to help mitigate the associated risks and will be discussed in detail in the chapter *Publishing.*

One can force the enabling of packet filtering. Packet filtering is a fundamental security feature that is highly recommended.

The third security relevant dialog box that is presented during the install relates to the mode of operation for the server. The ISA Server installation offers the choice of installing the server in *firewall mode, cache mode*, or *integrated mode* (Figure 7).
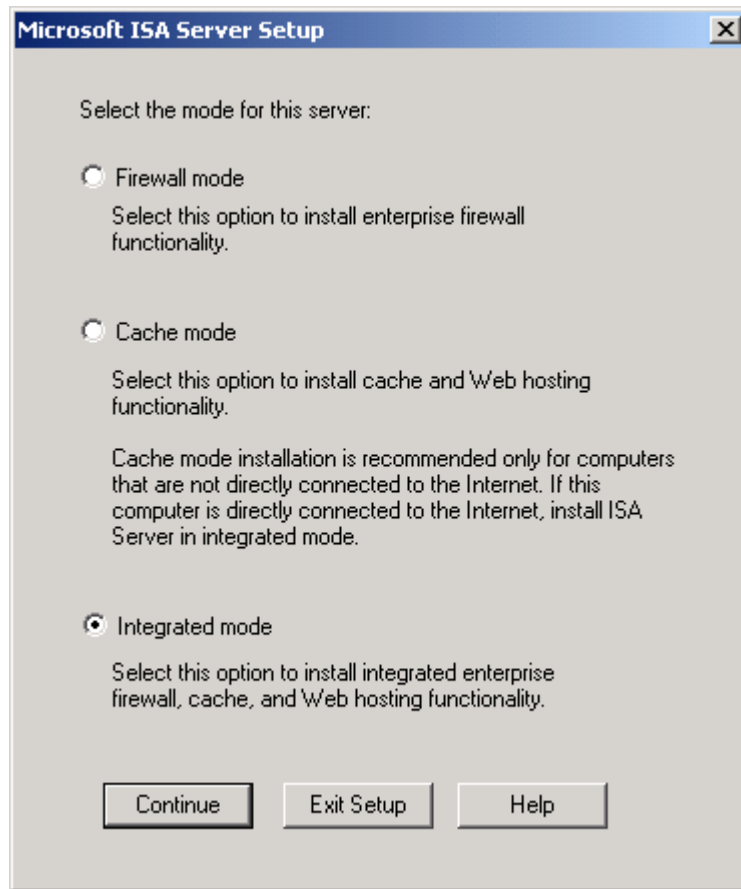
Figure 7 -- Firewall, Cache, Or Integrated Mode

Cache mode is used to support web access. It offers a local cache of frequently accessed web pages which can greatly speed Internet access and reduce traffic between the internal and external (Internet) networks. From a security perspective it only offers the proxy features described above for web access not for any other protocols. It also does not offer any firewall security features. The firewall mode, as the name implies, offers the full suite of firewall features but does not offer web caching. Integrated mode installs both the firewall and cache mode. The decision on how to proceed is dependent on what portion of the organization's security policy is to be implemented by ISA Server. Most organizations will probably desire to have the firewall features available which dictates the use of firewall or integrated mode.

The fourth concern relates to setting up the Local Address Table (LAT) (See Figure 8). The LAT is used by ISA Server to determine which set of IP addresses represents the internal network. If this is defined incorrectly, one can effectively deny local users access to the external network while allowing the outside world free access to the internal network. There are two methods that can be used to construct the LAT – either IP addresses can be added manually or ISA Server can construct the LAT automatically.

Whichever method is used, make certain that the resultant LAT (which will be displayed after generation) contains only IP addresses for the internal network.
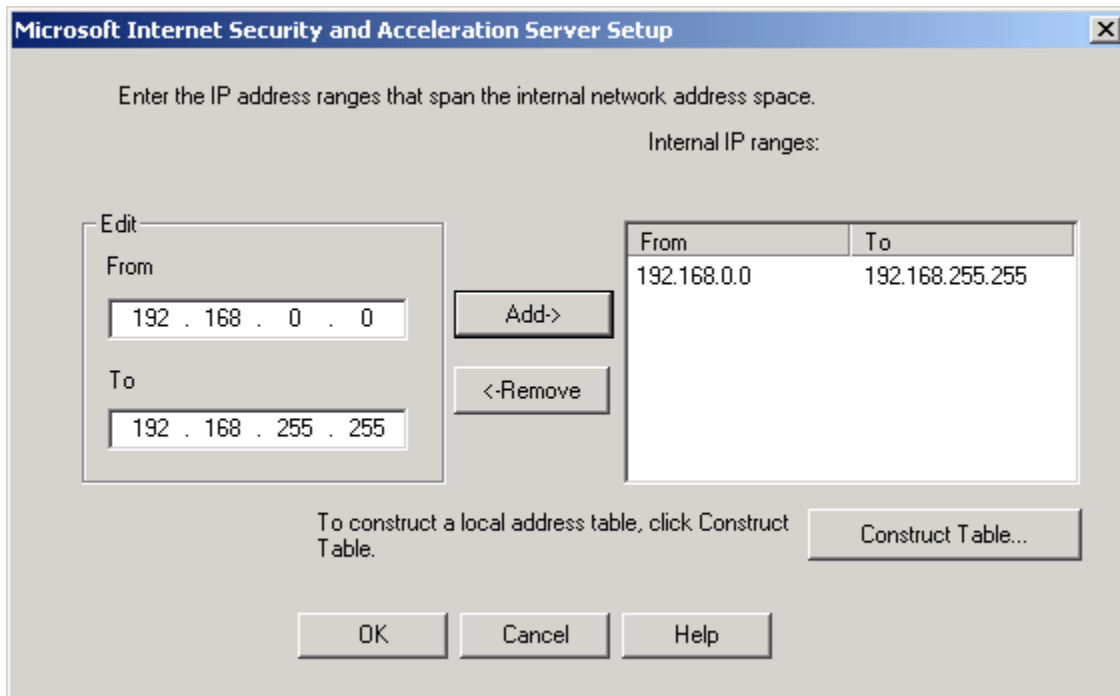
Figure 8 -- Construction of the LAT

Post Installation

Service Packs

It is always prudent to keep the ISA computer up-to-date with operating system service packs and hot fixes. It may be tempting to believe this isn't necessary give the protection offered by the firewall; however, it is important to remember that ISA Server relies heavily on the operation system for its foundation.

Patches/Hot Fixes

Microsoft has released security relevant service packs and hot fixes for ISA Server. It is recommended to review the security bulletins at http://www.microsoft.com/technet/security/current.asp for the latest information. It is critical to install security related fixes as soon as possible.

It is also prudent to review the information at Microsoft's ISA web page at http://www.microsoft.com/isaserver/. Occasionally Microsoft will announce hotfixes at this site that are not exposed as security bulletins such as the April 2002 release of a hotfix related to the rules engine.

Directory and File Permissions

The following file and directory permissions are recommended for the ISA Server installation.

Directory	Permissions
[Installation Directory] Do not allow inheritance from parent folder. Apply these settings to this folder, subfolders, and files.	Administrators: Full Control Creator/Owner: Full Control System: Full Control
[Installation Directory]/Clients Do not allow inheritance from parent folder. Apply these settings to this folder, subfolders, and files.	Administrators: Full Control Creator/Owner: Full Control System: Full Control Authenticated Users: Read & Execute
Urlcache Do not allow inheritance from parent folder. Apply these settings to this folder, subfolders, and files.	Administrators: Full Control Creator/Owner: Full Control System: Full Control

Table 1 -- Recommended File Permissions

In order to simplify the application of these file permissions, an .inf file is provided that can be used in conjunction with the Windows 2000 Security Configuration Editor (SCE). The file name is *ISA.inf* and is available at http://www.nsa.gov. Please note that this .inf file assumes that ISA Server was installed to *D:\Microsoft ISA Server*. If a different destination was used, then modify the .inf file prior to its use.

In addition to these directory permission settings, modify the permissions on the *mspclnt* share such that authenticated users have read access. This is the only permission required on the share.

Summary

In summary, when installing ISA Server:

❑ Invoke the operating system security guidelines contained within the security guide referenced on page 3.

❑ Remove or at least disable any unnecessary applications and services. Note that IIS is not required to be installed on the ISA Server computer.

❑ Unbind *Client for Microsoft Networks* and *File and Printer Sharing for Microsoft Networks* and disable NetBIOS over TCP/IP on the external NIC.

❑ If Terminal Services is installed on the ISA Server computer it is recommended to unbind it from the external NIC.

- ❑ If the ISA Server is exposed to an untrusted network, do not make it part of the internal domain structure.

- ❑ Unless H.323 access is required, do not install the gatekeeper service.

- ❑ Select array policies, enterprise policies, or both depending on the organization's administrative model.

- ❑ Do not allow publishing rules to be created unless the server being published is well partitioned from the internal network (e.g., in a DMZ).

- ❑ Enable packet filtering.

- ❑ Install onto a partition other than where the operating system is installed.

- ❑ Use firewall or integrated mode.

- ❑ Ensure that the LAT contains only addresses from the internal network.

After installing ISA Server:

- ❑ Install all applicable service packs and security patches/hot fixes.

- ❑ Set file and directory permissions per the guidelines offered in Table 1.

- ❑ Modify the permission on the *mspclnt* share such that authenticated users have read access. This is the only permission required on the share.

Chapter

3

Access Control

A primary feature of ISA Server is the ability to control user access to services on the external network. ISA Server uses *protocol rules* and *site and content rules* as the two fundamental elements in implementing this feature.

While it is impossible for a guide written for a wide audience to offer specific guidance on access control, it is generally recommended that access controls follow the concept of *least privilege*. Least privilege is a basic tenet of computer security that basically means "giving a user only those rights that s/he needs to do their job". The access control features of ISA Server can be used to support this concept.

Protocol Rules

Protocol rules specify, on a protocol-by-protocol basis, access that users or client machines are allowed. If the Microsoft firewall client or web proxy client is being utilized on client machines, access can be controlled on the basis of the specific user making the connection request. If using the Network Address translation features of ISA Server to connect the client machine, or if connecting via SOCKS, then access control decisions are made simply on the basis of the IP address of the client computer. These two different approaches are discussed in more detail in the chapter *ISA Clients;* however, please note at this point that a finer degree of access control is available when using the Microsoft firewall client or web proxy client allowing more detailed security policies to be implemented. For example, use of the firewall client will allow the option of specifying access to NNTP for some users while continuing to block it for all others.

It is recommended to use the firewall and web proxy clients in order to enable finer degree of control over access rights and to use Windows 2000 groups as the basis of assigning permissions. For example, one could create groups called *web users*, *e-mail users*, and *newsgroup* users and then implement a series of protocol rules as illustrated in Figure 9:

Protocol Rules						
Name	Scope	Action	Description	Protocol	Applies To	Schedule
Allow Mail	Enterprise	Allow		POP3,SMTP	Accounts: TRENTCO\email users	Always
Allow News	Enterprise	Allow		NNTP	Accounts: TRENTCO\news users	Always
Allow Web	Enterprise	Allow		HTTP,HTTPS	Accounts: TRENTCO\web users	Always

Figure 9 -- Sample Protocol Rules

Now, only users who are members of the corresponding group can access mail (POP3/ SMTP), newsgroups (NNTP), or browse the web (HTTP, HTTPS). Managing access is

simple – to grant or deny an individual access to one of the protocols simply add/delete that person from the corresponding group.

There are other salient points to consider when creating a protocol rule that offer a great deal of flexibility in rule definition. The following are the complete set of dialog boxes used to configure a rule using as an example an organization that wishes to grant some employees the right to download files via a FTP client. The first dialog box is accessed under either enterprise or array policy. Select **protocol rules** and click on **create a protocol rule**.
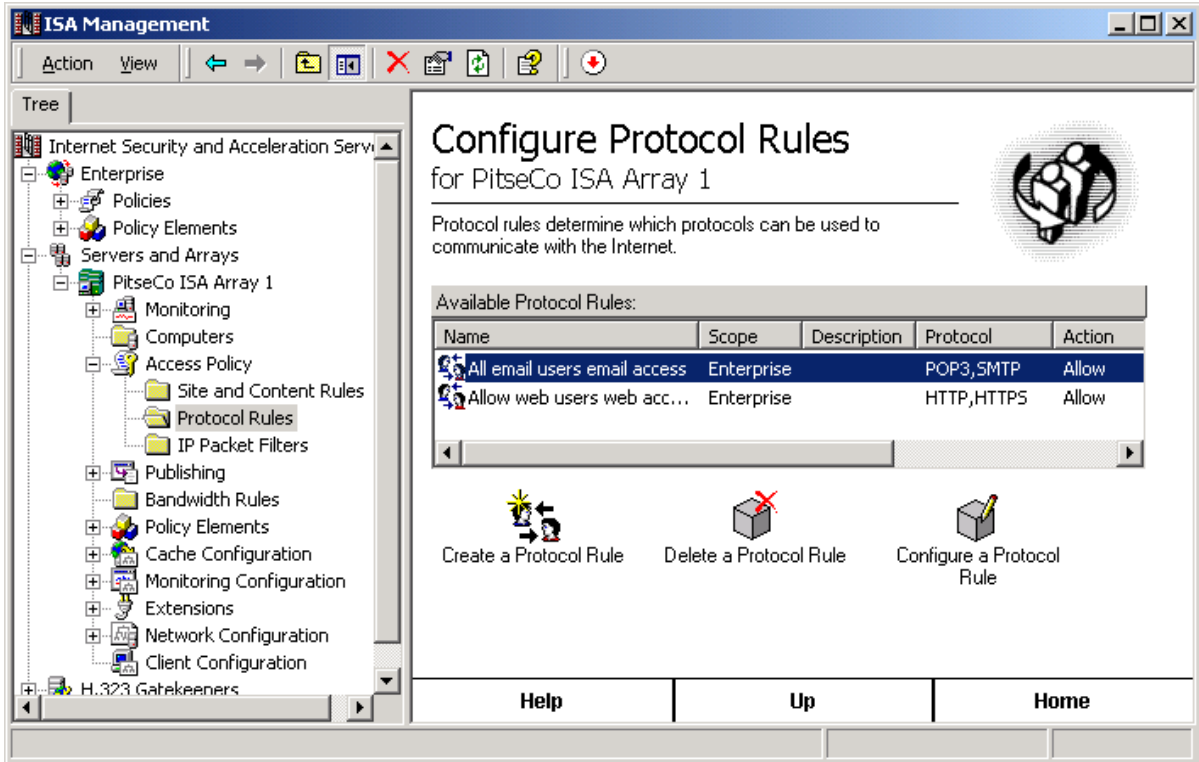
Figure 10 -- Location of Array Level Protocol Rules

The first dialog box of the create protocol rule wizard (Figure 11) simply asks for a name to be assigned to the rule. This example uses *FTP*.

Figure 11 -- Creating A Protocol Rule

The second dialog box (Figure 12) offers the choice of creating an *allow* or *deny* rule. The names are self-explanatory. Of note is the fact that deny rules always take precedence over allow rules. For example, assume that a user is a member of two Windows 2000 groups – *web users* and *engineering* – and that web users are allowed access to HTTP but the engineering group is specifically denied access to that protocol by a deny rule. That user will not be able to access the web via HTTP inasmuch as the deny rule takes precedence. This is true regardless of the order in which the rules are listed. While some firewall products interpret rules sequentially and make a final accept/reject decision based upon the first rule that applies, ISA Server will always reject a connection regardless of where on the list of protocol rules the deny rule exists. In this example, however, an allow rule for FTP will be created.
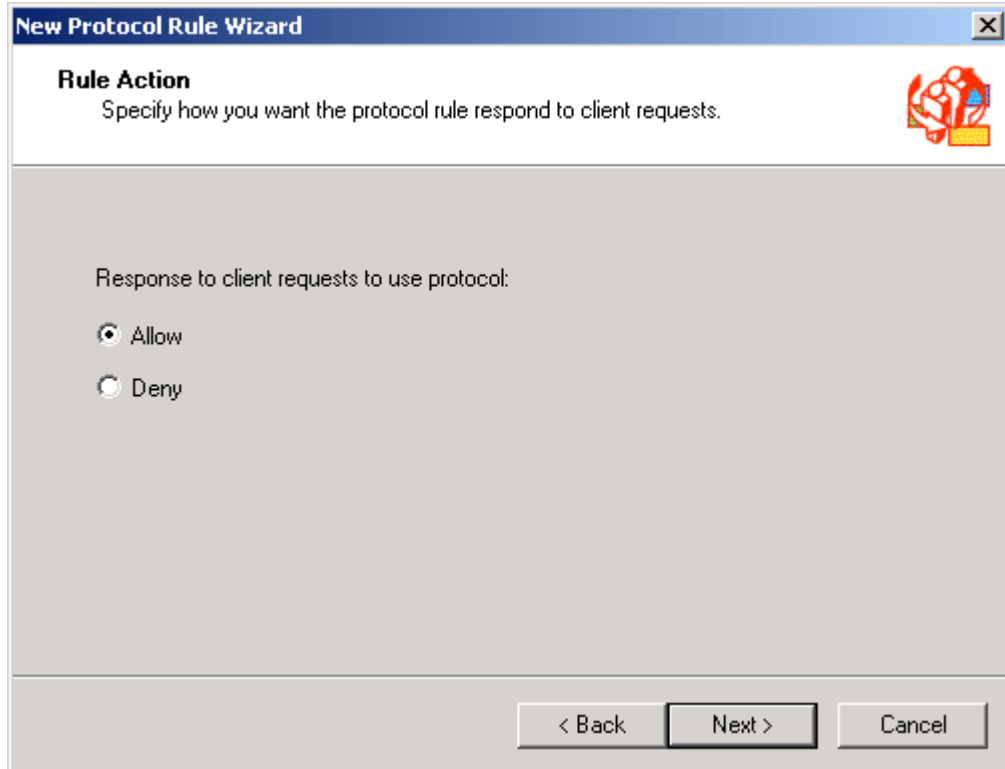
Figure 12 -- Allow And Deny Rules

Next, (Figure 13) one selects the protocol for which this rule applies which in this case is **FTP Download only**.
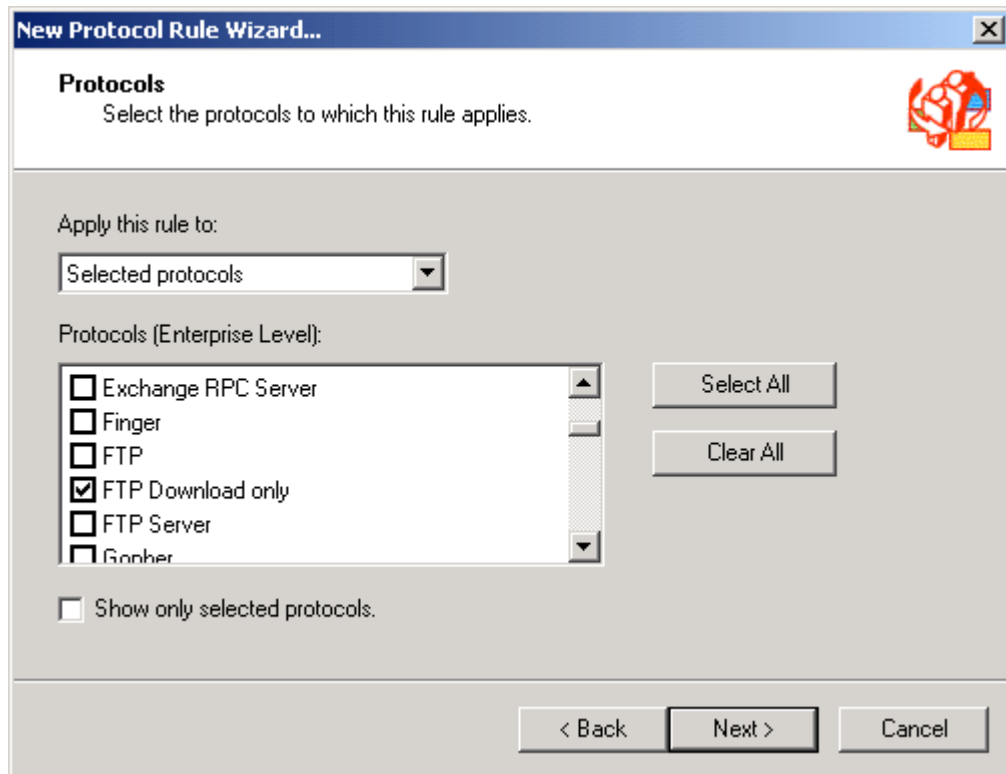
Figure 13 -- Selecting The Appropriate Protocols

The list of protocols that can be selected is extensible. A complete list of the defined protocols is provided under the **protocol definitions** object which is found under the **policy elements** object. One can add new protocols to the list or review existing ones to ascertain their makeup.

One can also choose the time of day the rule applies (Figure 14). This has little utility from a security perspective and therefore will not be discussed any further.
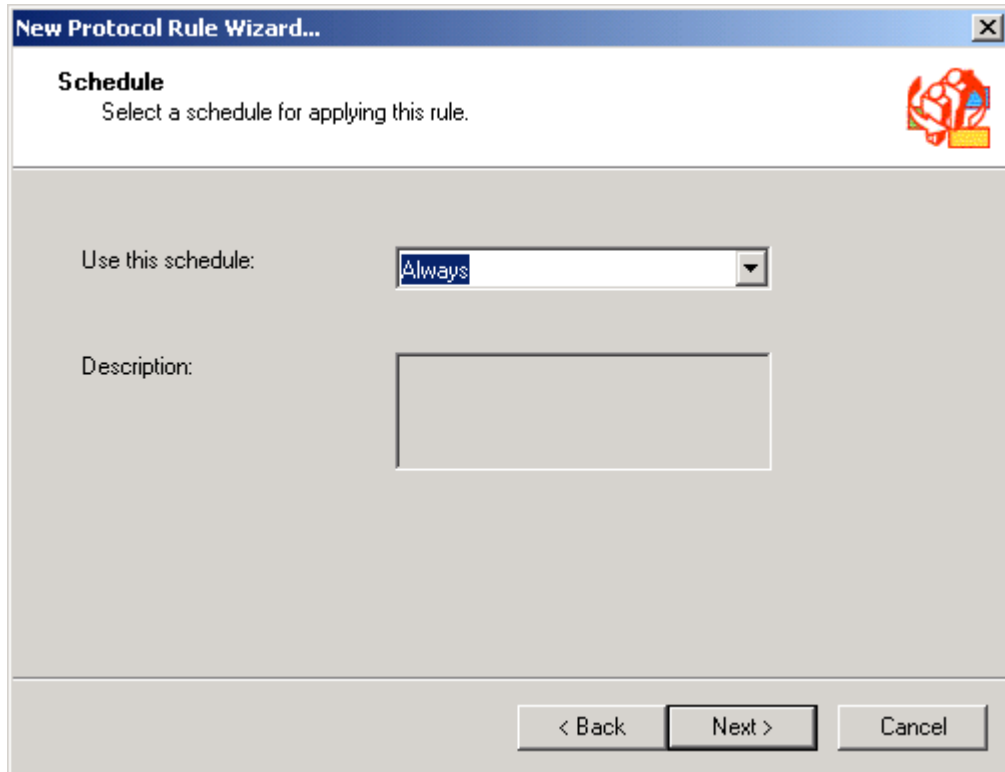
Figure 14 -- Choosing When The Rule Applies

Three options are presented for identifying to whom the rule applies (Figure 15):

- *Any request.* Select this to apply the rule to all connections regardless of from where or from whom on the internal network they originated. This offers the least amount of access control and would be used to allow, or deny, access to a protocol for everyone on the internal network.

- *Specific computers (client address sets).* This is used when it is desired to base access control decisions upon the IP address of the client machine making the request. This offers a higher degree of control in that one can specify allow/deny rules for specific computers.

- *Specific users and groups.* This allows one to explicitly identify which users are allowed or denied access to the protocol. The firewall client must be installed in order for this feature to be effective.

In this example **specific users and groups** is selected and then the Windows 2000 user group called **FTP users** is selected.
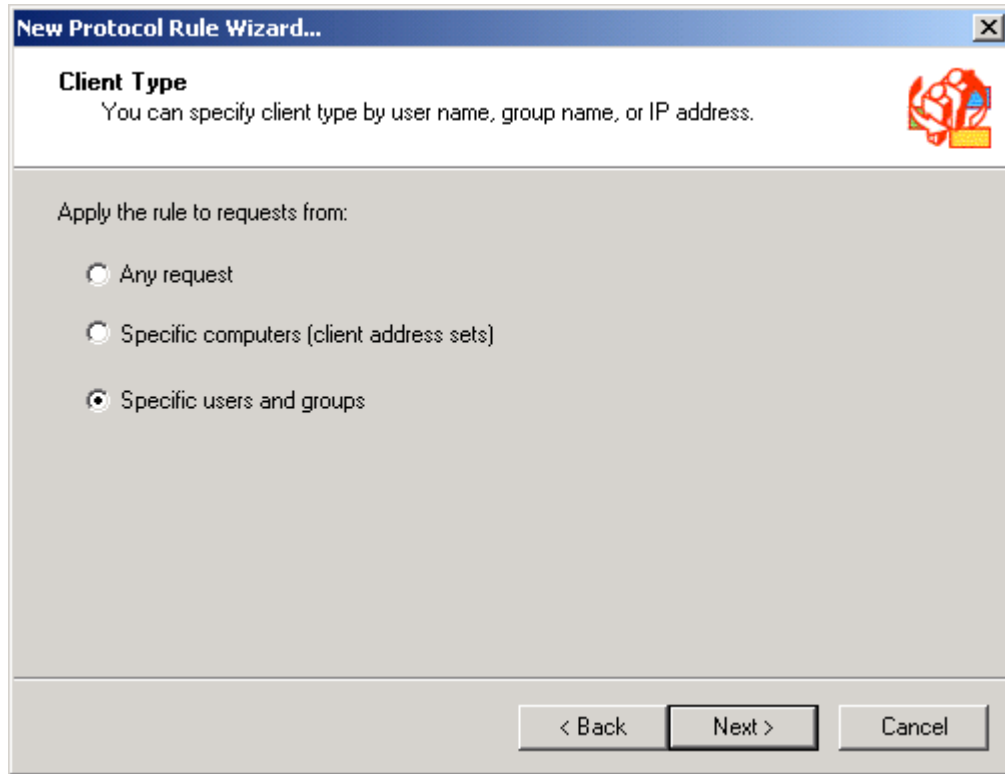
Figure 15 -- Selecting For Whom The Rule Applies

If client address sets are being utilized, they are created via the **client address sets** object underneath the **policy elements** object for both enterprise and array policy.

After clearing a dialog box summarizing the rule the final product appears as follows:

Figure 16 -- New Protocol Rule In Effect

Site and Content Rules

The utility of site and content rules is as implied by the name. First, site and content rules allow the administrator to specify which *sites* users are allowed to connect to. For example, even though a user may be allowed access to FTP via a protocol rule, s/he will only be able to access a specific FTP site if it is allowed by a site and content rule.
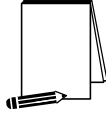
NOTE: Packet Filters also come into play as discussed in *Packet Filtering and Intrusion Detection*.

The *content* portion of site and content rules are only applicable to HTTP and tunneled FTP[1] requests.   This feature is used to specify the content types allowed at specific sites. For example, one may choose to block the download of documents that may contain macros as a countermeasure against the mobile code threat. It is important to note that while this feature has potential value from the standpoint of controlling bandwidth requirements (one could block receipt of video, for example), its utility from a security perspective is less significant. To continue with the same example, while one could block potentially dangerous documents which contain macros, the content settings will have no effect on the same documents being delivered via e-mail or downloaded via a FTP client. Furthermore, this feature cannot block active content such as Java or ActiveX (although a custom firewall extension could potentially provide this feature).

It is also important to note that the site and content rules are tricky to configure if using the firewall client to forward web browser traffic to the ISA Server.   For this reason, it is recommended to use the web proxy client for web browsers. It may be necessary to use the firewall client for support of other protocols (e.g., non-web protocols); the web proxy client can be used in addition to the firewall client if necessary. More information on the various clients is provided in the section ***ISA Clients***.

There are a few other salient points to consider when creating site and content rules. The following are the complete set of dialog boxes used to configure a rule. They serve as a useful mechanism for describing the security considerations associated with the range of possible site and content rules that can be developed. The first dialog box is accessed under either enterprise or array policy. Select **site and content rules** and click on **create a site and content rule**.

---

[1] A term used in Microsoft's documentation to refer to FTP access via a web browser.
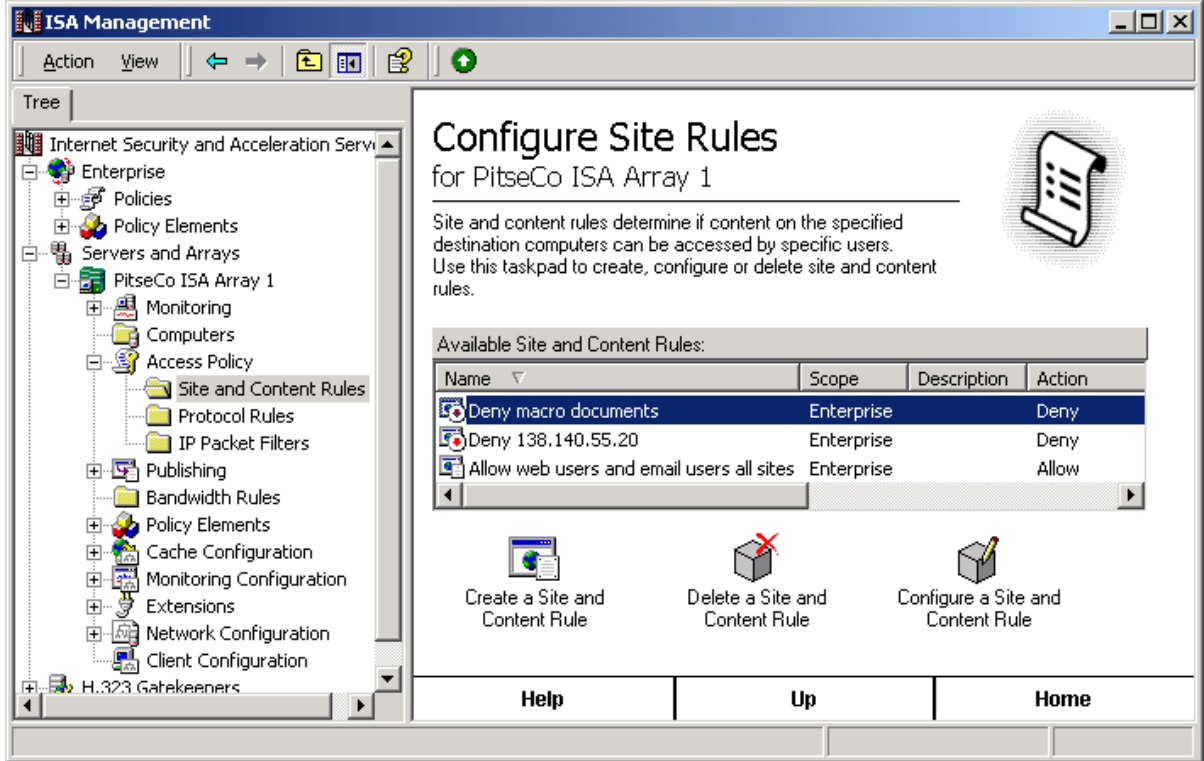
Figure 17 -- Location Of Array Level Site And Content Rules

The first dialog box of the create protocol rule wizard simply asks for a name to be assigned to the rule (Figure 18). This example uses **Macro Documents**. As implied by the name, this rule will be used to block browser delivery of documents which could contain macros.

Figure 18 -- Creating A Site And Content Rule

The second dialog box allows one to define if this is an *allow* or *deny* rule (Figure 19). Deny is selected in order to preclude access.
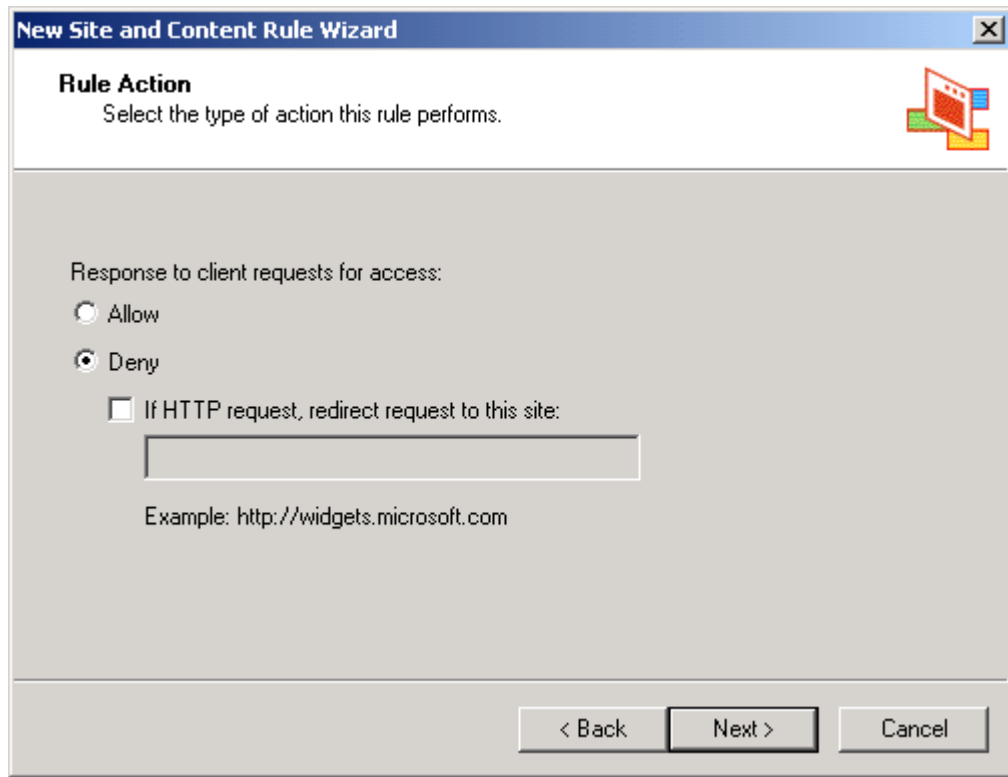
Figure 19 -- Allow And Deny Rules

Next, one can select to whom the rule applies (Figure 20)[2]. The rule can apply to:

- Certain destinations
- Certain times
- Certain clients
- All of the above (by selecting "custom" on this dialog box)
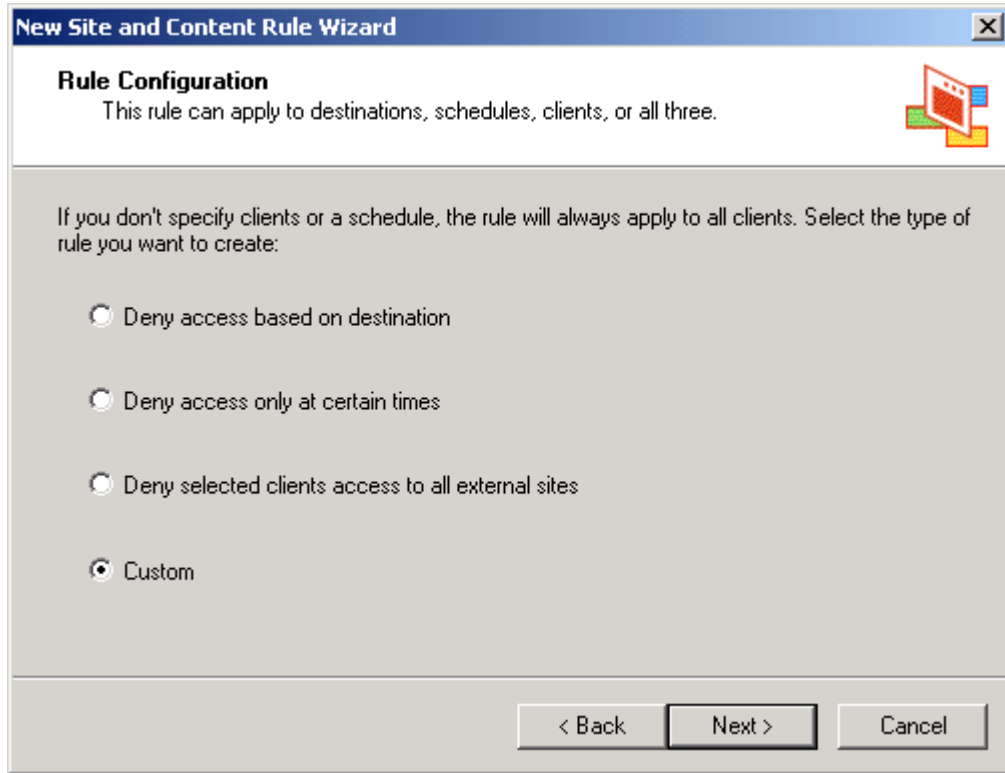
Figure 20 -- Choosing Access Control Mechanism

In this example **custom** is selected so that the wizard can be fully explored. This selection will allow the three other options to be manipulated through the wizard.

---

[2] This dialog box will not appear if a protocol rule has not been previously configured. In this case the wizard defaults to a selection of "custom" but proceeds immediately to the dialog box of Figure 21.

The next dialog box (Figure 21) allows one to define the specific destinations for which the rule applies. One can deny access to documents which may contain macros regardless of the source, can specify certain sites in a destination set, or can deny access to such documents from all sites on either the internal or external network. Destination sets are established via the **destination sets** container under **policy elements.** For this example, **all destinations** is selected.
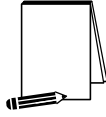
> **NOTE: Web browsers typically allow the option of bypassing the proxy server for a defined set of addresses, typically those on the internal network. This is a useful feature in that it can reduce the workload on the ISA Server if it does not have to process requests for access to the trusted, internal site. While the risk should be minimal provided one truly has a level of trust in local sites please be aware, however, that one of the consequence of enabling this feature is that ISA Server can not enforce site and content rules when it is bypassed. More on browser setup is provided in _ISA Clients_.**
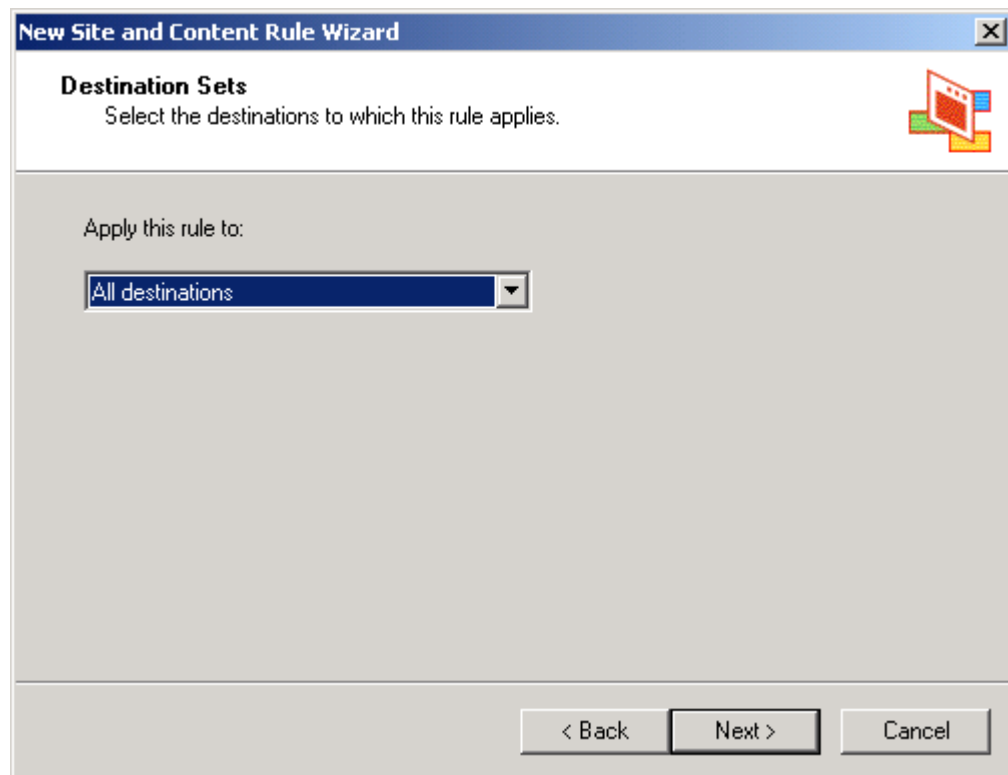
Figure 21 -- Choosing The Destination Set

As with protocol rules, one can select when to apply the rule (Figure 22):
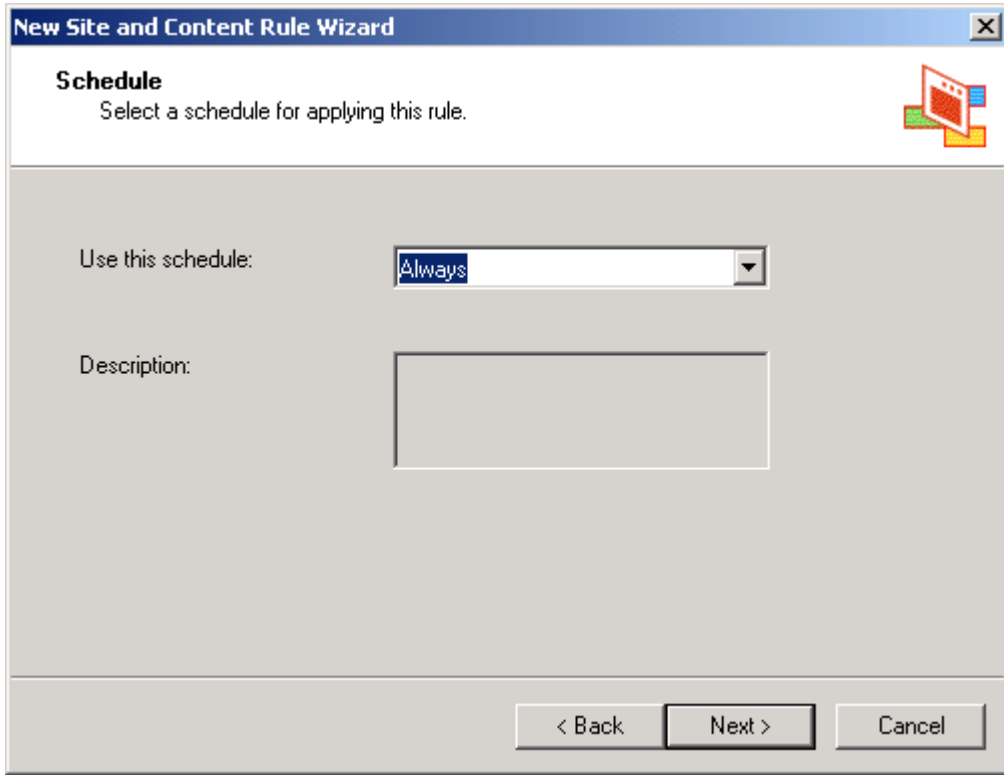
Figure 22 – Choosing When The Rule Applies

Next, one selects which users or computers the rule applies (Figure 23). In this case we want to block access for all web users.
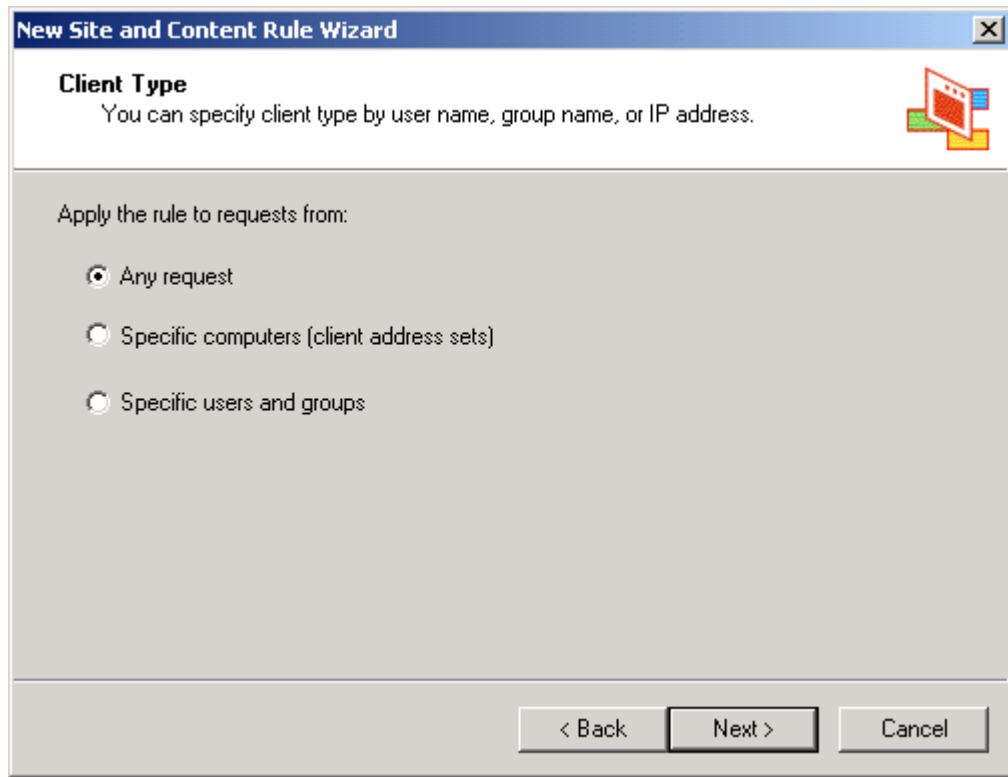
Figure 23 -- Selecting For Whom The Rule Applies

Finally, you select which types of content are applicable to this rule. In this case, macro documents are selected (Figure 24).
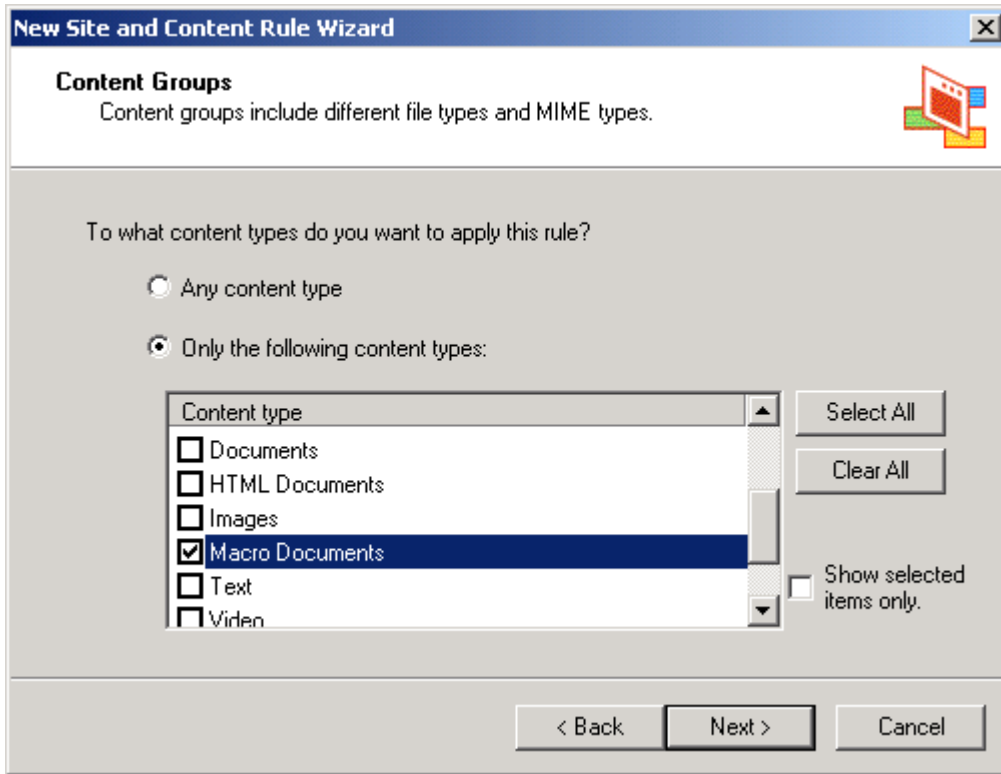
Figure 24 -- Selecting The Content Group

The content groups are based upon mime types and file extensions. Content group definitions can be reviewed or modified, and new content groups added, by selecting the **content groups** object under **policy elements**.

The site and content rule wizard completes by showing a summary of the rule and creating it. Once completed, the result appears as illustrated in Figure 25:

Figure 25 -- New Site And Content Rule In Effect

Note that two rules are required. The first allows access to all content from all sources. The second is the one just created to preclude access to macro documents. While the ordering of the rules is immaterial, it is necessary to have two rules. As discussed at the start of this section, ISA server only allows a connection if a site and content rule specifically allows it and a protocol rule exists which allows access to the protocol being used. In this case the first site and content rule allows web browsing in general while the second denies access to the content deemed risky.

Summary

In summary, the following are recommended when implementing access controls using ISA Server:

- ❑ Use protocol rules and site and content rules to implement organizational security policy.   It is recommended to give users only those minimal rights they need to do their job, consistent with that policy.

- ❑ Use the protocol rules feature to specify user access to services. It is recommended that this be done on the basis of Windows 2000 groups (e.g., Web Users group, e-mail group, etc.).

- ❑ Use site and content rules to enforce any restrictions regarding the sites that users are allowed to connect.

- ❑ Use site and content rules to enforce restrictions regarding the content that users are allowed access to via HTTP and tunneled FTP. Note that content restrictions do not apply to other protocols (e.g., SMTP).

- ❑ Understand that the type of client utilized has an impact on the utility of protocol rules and site and content rules. It is recommended to always use the web proxy client for web browsing. Reference *ISA Clients*.

This Page Intentionally Left Blank

Chapter

4

Packet Filtering and Intrusion Detection

Packet Filtering

The packet filtering mechanism has applicability to both incoming and outgoing connection requests. For outgoing connection requests, packet filters can be thought of as the last line of defense. In other words, even if a connection request were allowed by a protocol rule and a site and content rule, it would be blocked if an applicable deny packet filter exists. Take the following example:

- Protocol rule: Allow HTTP access for the group "web users"

- Site and Content rule: Allow access to all sites for the group "web users"

- IP Packet Filter: Block access to IP address 110.110.110.100

With this rule set users who are part of the web users group would have HTTP to any site except for 110.110.110.100 – the deny packet filter takes precedence over the protocol and site and content rules.   This can be a very useful mechanism for quickly responding to a security concern. For example, SANS recently issued an alert that recommended, among other things, blocking all access to a certain IP address.   This can be accomplished easily by creating an appropriate packet filter rule[3].

Additionally, the packet filtering mechanism is used to control inbound and outbound connection requests to/from the ISA Server computer itself. For example, ensuring that the packet filter rules do not allow the ISA Server to issue ICMP echo responses will prevent a potential hacker from detecting the ISA Server via a ping.

Packet filters are also used to control access to the DMZ when it is constructed using a tri-homed server.   This is not the preferred method of constructing a DMZ (reference the ***Publishing*** section); however, if a tri-homed server is being used, the ISA Server help topic *three-homed perimeter network configuration* explains the use of packet filters in this environment.

In all cases, the packet filter mechanism accomplishes this control by allowing or denying connections from the outside network based upon such variables as source IP address and service type. This will be illustrated with a simple scenario as presented in Figure 26.

---

[3] Site and content rules can also be used to block access to a site as mentioned in the preceding chapter.
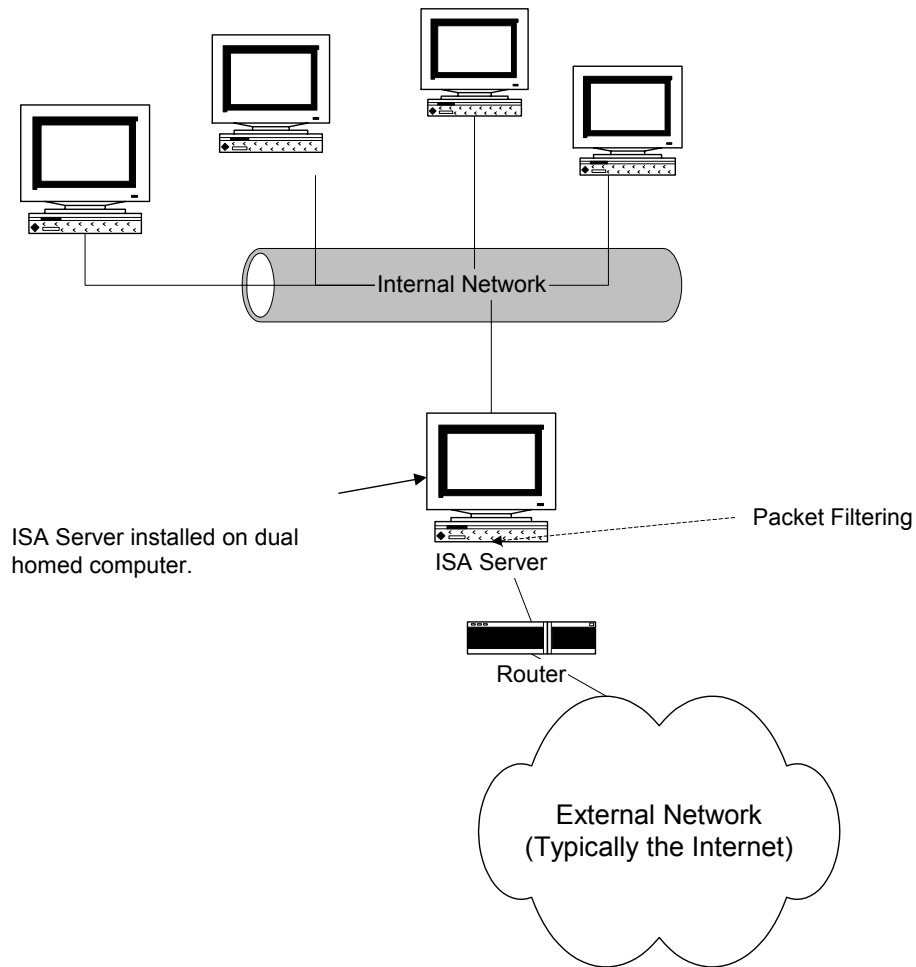
Figure 26 -- Typical ISA Server Installation

Packet filters are used in this scenario in three ways. First, they control access requests from the external network to the ISA Server. Unless specifically allowed by a packet filter or publishing rule, connection requests are denied. Second, they allow access to the external network for services running on the ISA computer itself. For example, if a web server intended for external use was being hosted on the ISA Server it would be necessary to open port 80 via a packet filter rule to allow external users to connect to the web server. (Please note that doing this without the use of a DMZ is strongly discouraged.) And finally, as with the example above, packet filters serve as a means of

blocking access to the external network such that, for example, a site that was known to contain malicious code could be blocked with a packet filter.

Packet filters are defined based on protocol type (e.g., TCP, UDP), port number (e.g., 119 which is the TCP NNTP port), local computer IP address, and remote computer IP address. The remote computer refers to the computer(s) on the external network for which the rule applies. The local computer refers to the ISA Server or, in the case of a tri-homed ISA Server computer servicing a DMZ, the DMZ computer for which the rule applies. IP packets filters are static -- communication through a specific port is always either allowed or blocked. Allow filters allow the traffic through, unconditionally, at the specified port. Blocked filters always prevent the packets from passing through the ISA Server computer.

The following illustrates the complete set of dialog boxes applicable to defining a packet filter rule. These settings are accessed by selecting **access policy/IP packet filters** under the specific array name and clicking on **create a new packet filter** (Figure 27). This example illustrates the blocking of all connections to IP address 110.110.110.100 for the array TrentCo ISA Array1.
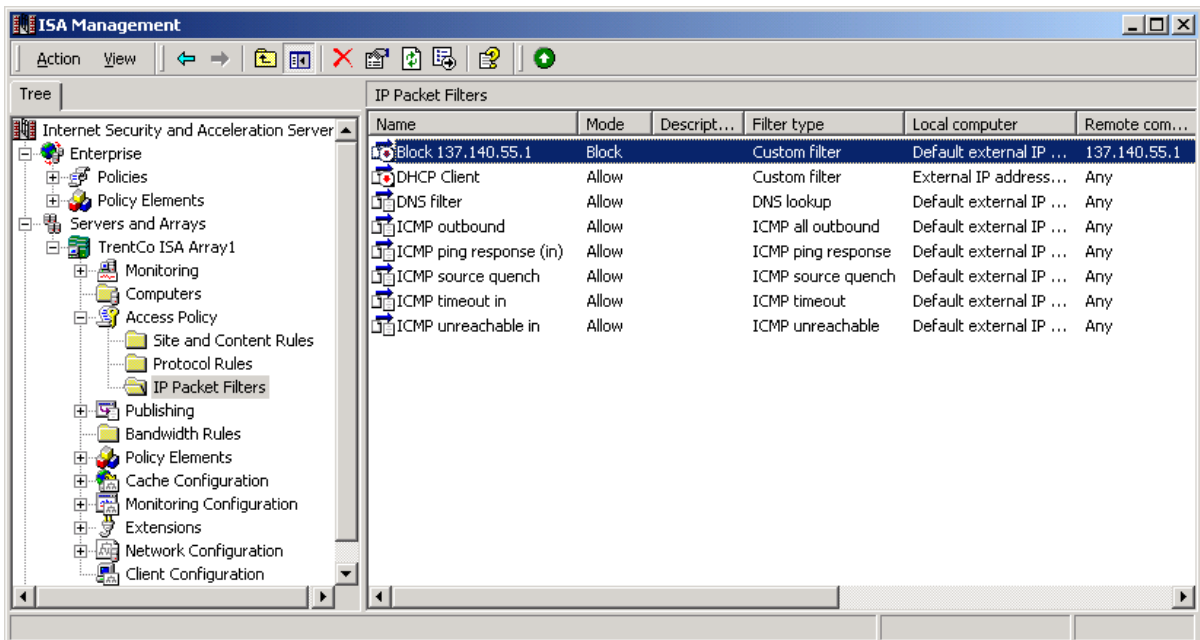
Figure 27 -- Location Of Packet Filter Settings

Chapter 4 - Packet Filtering and Intrusion Detection

The first dialog box simply allows the entry of a descriptive name for the filter (Figure 28).

Figure 28 -- Creating A Packet Filter

Next, the wizard allows us to apply the setting to either all ISA Servers in the array or to select a specific server. **All ISA Server computers in the array** is selected (Figure 29).
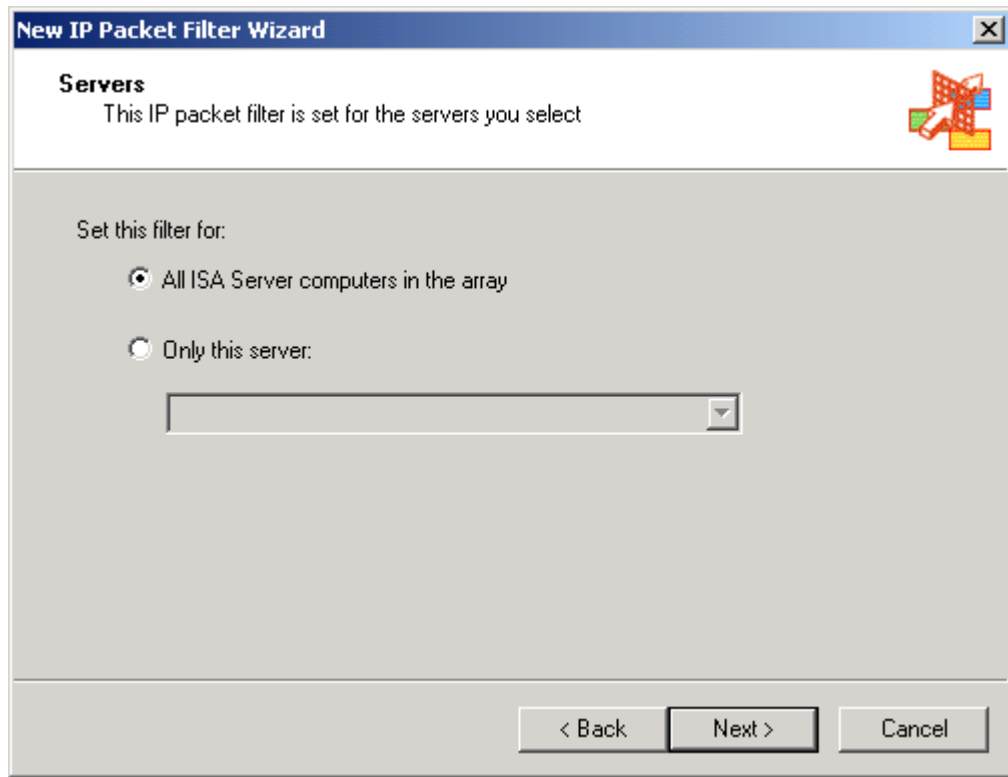
Figure 29 -- Select The Applicable ISA Server

The wizard now prompts for the type of packet filter desired – **allow** or **block** (Figure 30). In this example, access is blocked.
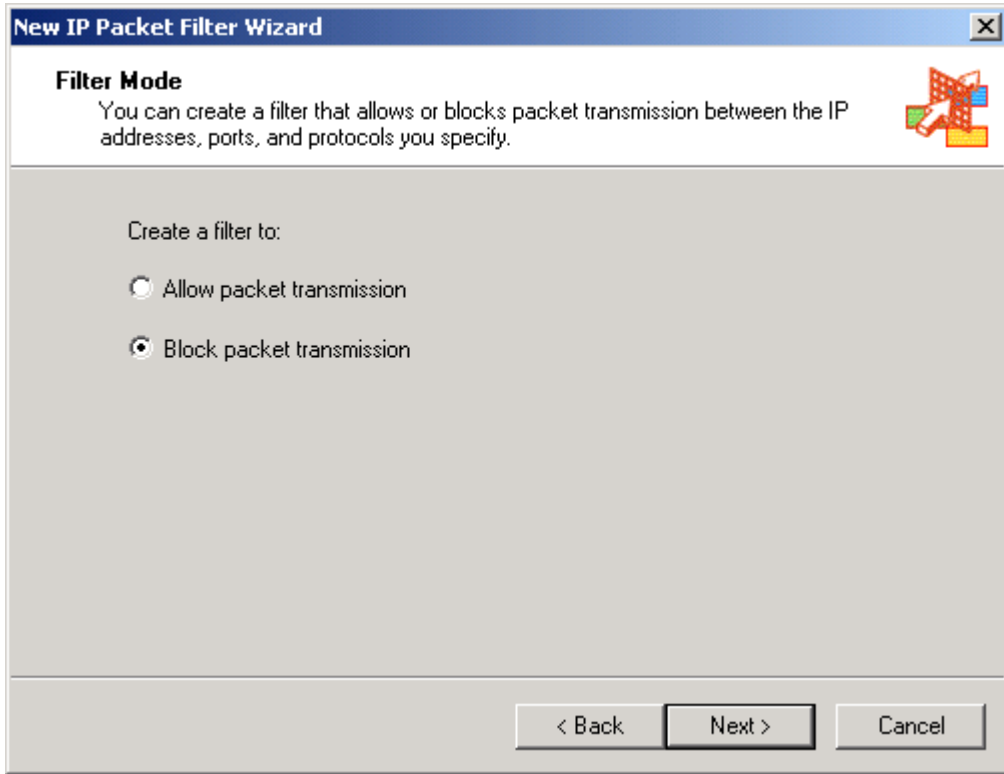
Figure 30 -- Allow or Block Filters Can Be Created

Next the appropriate protocol is selected (Figure 31). Since this assumes that all access to address 110.110.110.100 is to be blocked, choose **custom**. The choice **predefined** presents a rather extensive list of protocol choices that would be applicable only if it was desired to limit the action of this filter to selective protocols.
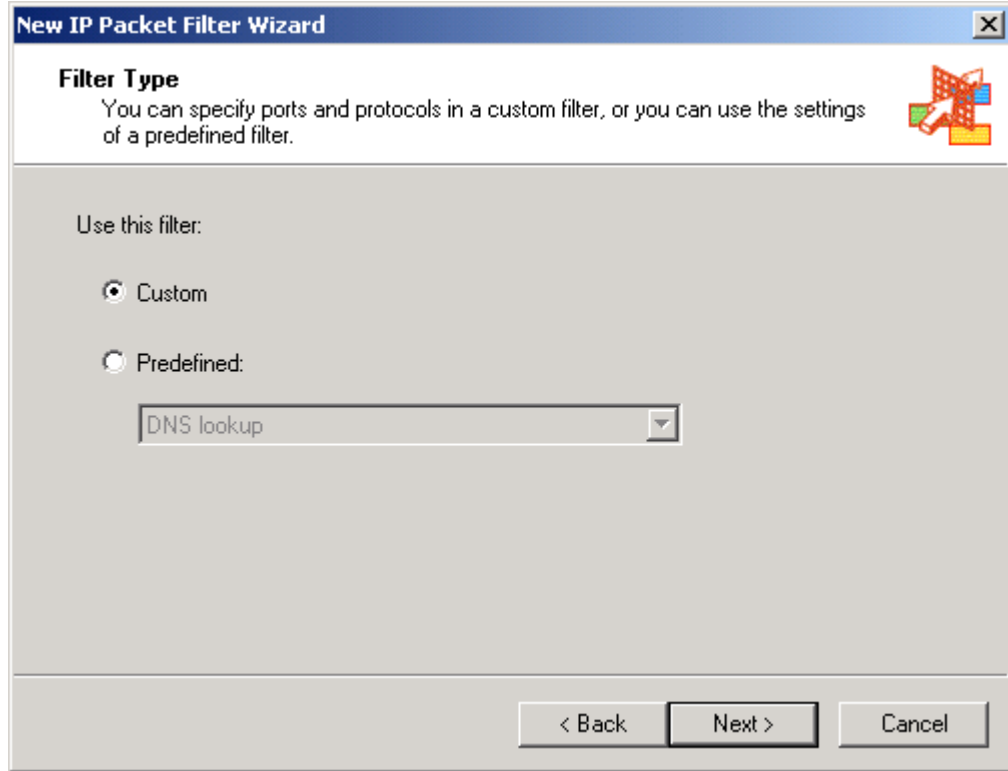
Figure 31 -- Selecting The Appropriate Protocol

Next, the wizard allows the definition of the custom filter type (Figure 32). Choices include the kind of protocol applicable to this rule (e.g., TCP, UDP, etc.), the connection direction for which the rule applies (e.g., incoming, outgoing, etc), and the specific port numbers applicable to the rule. For this example, **any** is selected as the IP protocol and **both** is selected as the direction. This will enforce the goal of blocking all access to the site.

Figure 32 -- Defining The Applicable Protocol

The filter is applied to the external interface of the ISA Server computer (Figure 33). Note that it is from this page that one could elect to create a filter applicable to a computer in the DMZ, provided the DMZ was built using a tri-homed ISA Server as discussed earlier in this chapter.
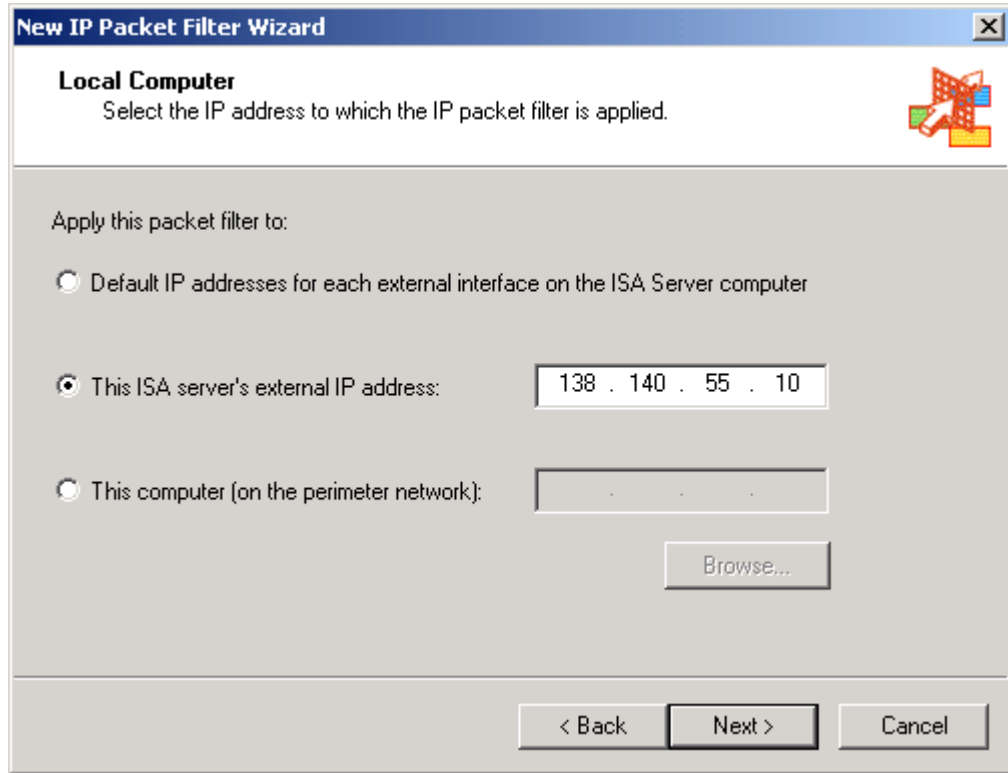
Figure 33 -- Applying The Filter To The ISA Server's External NIC

The rule is then applied to the remote computer in question – 110.110.110.100 (Figure 34).
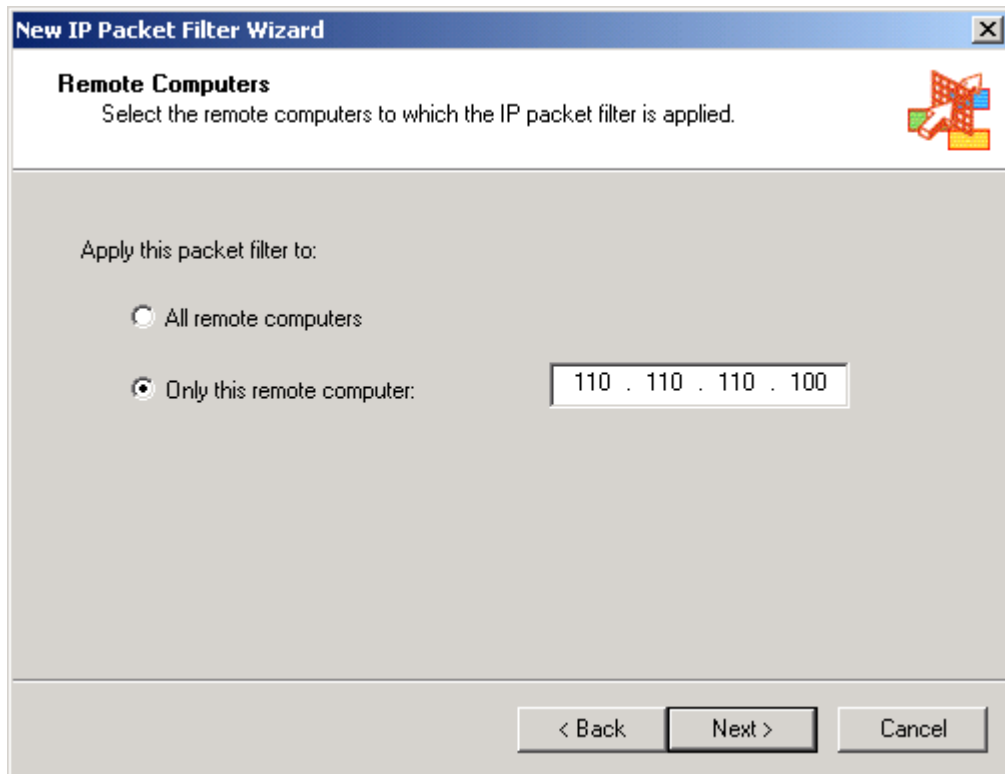
Figure 34 -- Entering The Remote Computer

The wizard then presents a summary page illustrating all the settings entered and finally creates the packet filter.

There are a few additional things to keep in mind when using packet filters. First, ISA Server extensions (discussed in detail in the *Extensions* chapter) can have an effect on packet filter settings. For example, if the H.323 filter that ships with ISA Server is enabled, then port 1720 will be open regardless of the packet filter settings. Disable the H.323 filter if H.323 conferencing support is not required. Publishing rules have a similar effect. As a precaution to ensure that the packet filter rules are as restrictive as possible, it is advisable to run a port scanner from the external network to ensure that only those ports that are minimally required are left open. Second, the packet filter feature has the ability to support filtering of IP fragments. IP fragments are not inherently bad – they are intended as a way of transferring data that is too large to fit into a single packet. Hackers have used IP fragmentation as an attack mechanism by constructing packets in such a way that they look innocuous on the surface but can do the network harm when reassembled. It is recommended to enable this function, but be aware that when this feature is enabled ISA Server will drop all fragmented packets – it makes not attempt to determine if the packet is malicious or not.   Finally, ISA Server can block packets with the IP options flag set. IP options are sometimes used by hackers to do such things as source routing, where they exercise control over how the packet is routed over the Internet. It is recommended to enable this function.

To access the IP fragments and IP options settings, expand **Servers and Arrays**. Expand the **[array name]** container, then navigate to the "**Access Policy**" container and select **IP Packet Filter**. Right click and select **Properties**, and then go to the **Packet Filter** tab. Figure 35 illustrates these settings.
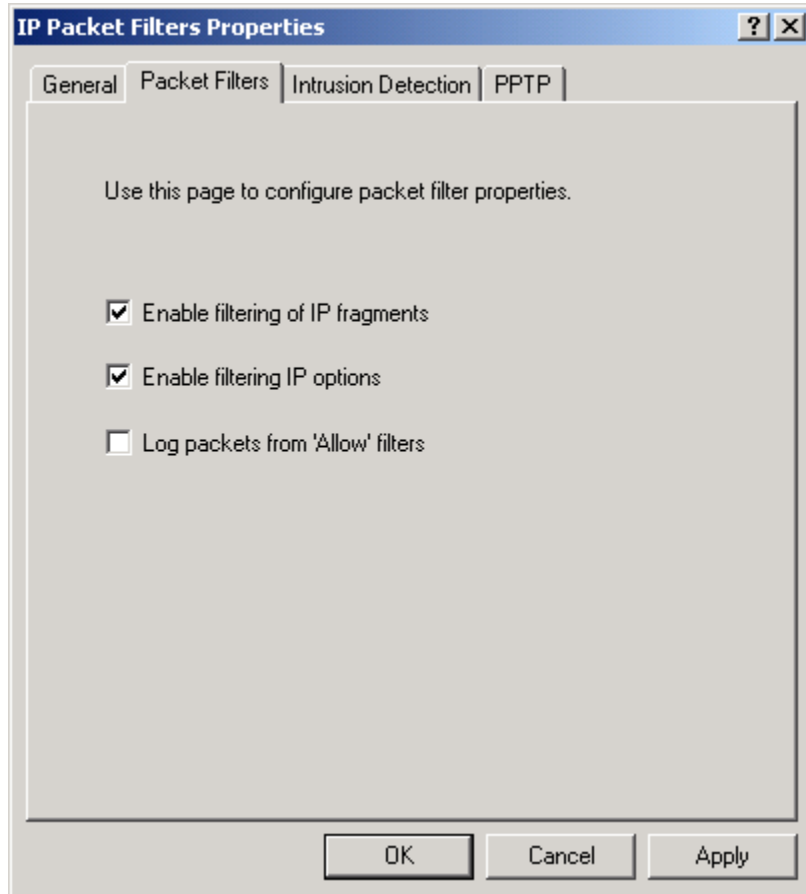
Figure 35 -- IP Fragments And IP Options

A variety of allow packet filters are pre-defined with the ISA installation. Provided the recommendations contained in the section *Installation* were followed, these canned packet filters will be enabled upon completion of the install. The rules include:

- *DNS Lookup.* This allows ISA Server to access Domain Name Servers (DNS) on behalf of internal web clients. It is necessary to have this rule if resolving names in this manner. Alternately, names can be resolved from an appropriately configured DNS server on the internal network or DMZ. The *Guide to Securing Microsoft Windows 2000 DNS* offers guidance on a variety of DNS architectures. This guide is available from the source on page 3.

- *A variety of ICMP rules*. These include rules that allow Internet Control Message Protocol (ICMP) packets to flow to and from the ISA Server and the external network. These packets are in support of such things as flow control. The default rules are fairly innocuous – for example, the default set of rules will not allow the ISA Server to

respond to ping requests which could be used by a hacker scanning for possible targets. It is recommended to leave the rules in place.

Intrusion Detection

ISA server includes a basic capability to perform intrusion detection. The intrusion detection features are split between two locations in the ISA Server MMC and are accessible under the **IP packet filter** container and the **extensions** container. Those features assessable under the packet filter container are addressed here while extensions are covered in a later chapter.

The intrusion detection features located under the packet filter container are disabled by default. Two settings must be enabled in order to turn on intrusion detection. First, go to **[array name]/access policy/IP packet filters**, open the properties page, and select the **general** tab and select **enable intrusion detection**. Also ensure that packet filtering is enabled – the intrusion detection features will not function otherwise.
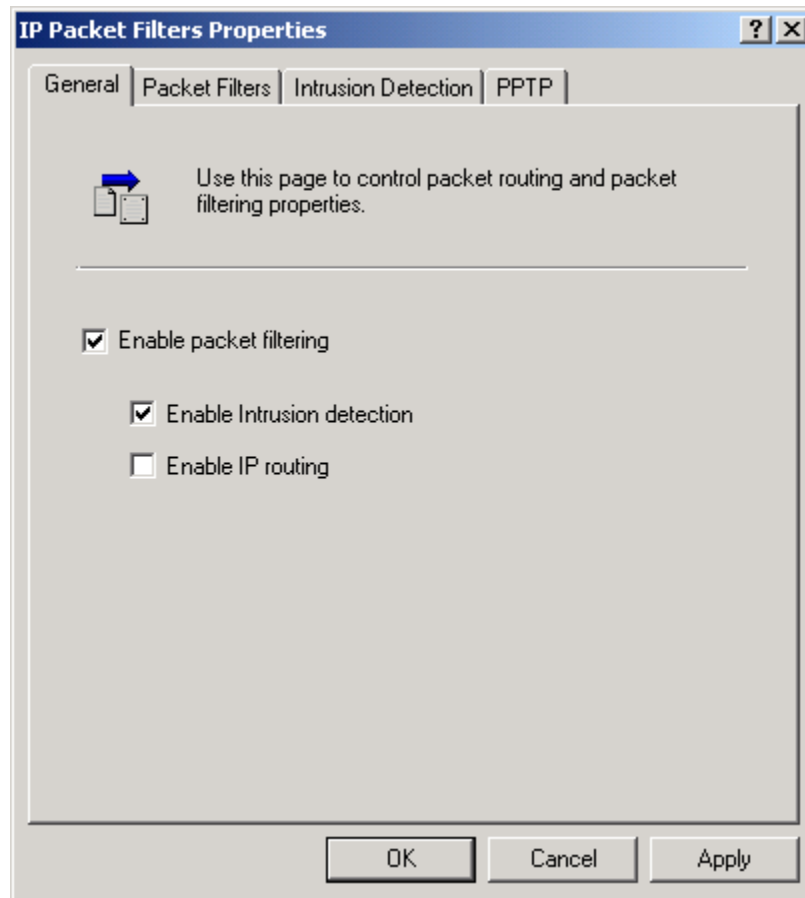
Figure 36 -- Enabling Intrusion Detection

Before continuing with the intrusion detection discussion, a quick mention of the other option on this dialog box – **enable IP routing** – is warranted. This option is generally not

required, and should not be enabled, except as noted under **_Publishing a Mail Server -- DMZ With Filtering Router &Tri-Homed Firewall._**

And now that that sidebar is completed, to continue setting up the intrusion detection features go to the **intrusion detection** tab and enable the listed attacks (Figure 37).
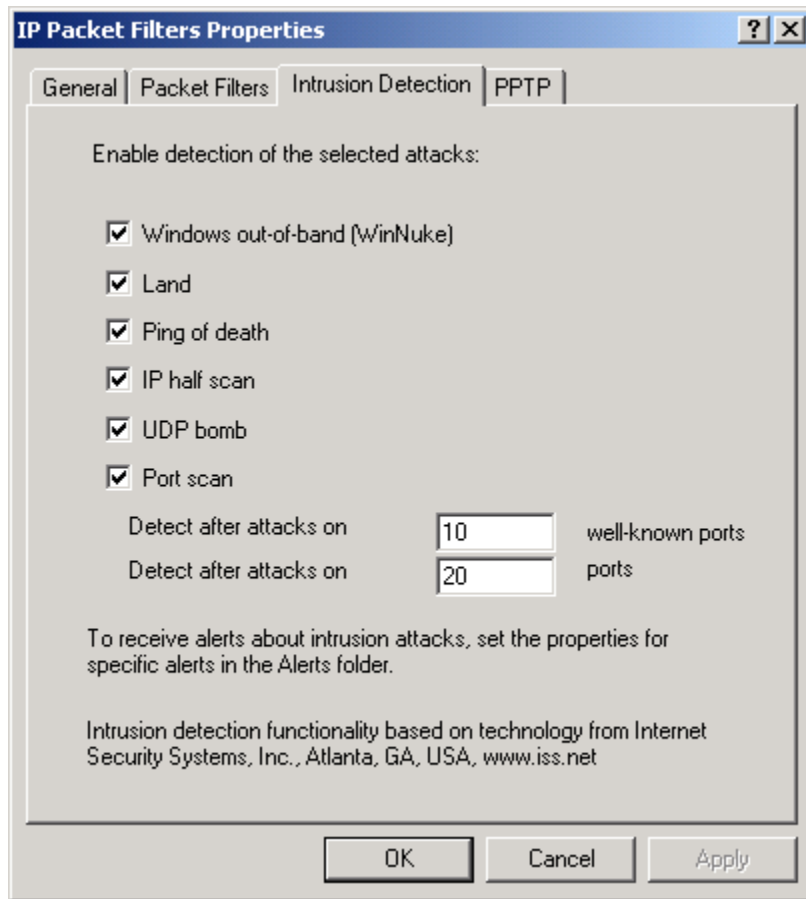
Figure 37 -- Selecting Specific Attacks For Monitoring

The attacks covered by the intrusion detection mechanism include the following (source: ISA Server help file):

Port scan attack

This alert notifies that an attempt was made to catalog the services running on a computer by probing each port for a response.

If this alert occurs, one should identify the source of the port scan. Compare this with the services that are running on the target computer. Also, identify the source and intent of the scan. Check the access logs for indications of unauthorized access. If indications of unauthorized access are detected, the system may have been compromised. Note that if packet filtering is enabled and configured as recommended, only ports that are purposely opened – as in the case of published servers – will respond to the port scan probe.

IP half scan attack

This alert notifies that repeated attempts to complete a TCP handshake with a computer were made, and no corresponding ACK packets were communicated.

A standard transmission control protocol (TCP) connection is established by sending a SYN packet to the destination computer. If the destination is waiting for a connection on the specified port, it responds with a SYN/ACK packet. The initial sender replies with an ACK packet, and the connection is established. If the destination computer is not waiting for a connection on the specified port, it responds with an RST packet.

Most system logs do not log completed connections until the final ACK packet is received from the source. Sending an RST packet instead of the final ACK results in the connection never actually being established and, therefore, the connection is not logged. Because the source can identify whether the destination sent a SYN/ACK or RST packet, an attacker can determine exactly which ports are open for connections without sending the final ACK packet and therefore the destination is unaware of the probing.

If this alert occurs, note the address from which the scan occurs. Configure the ISA Server IP packet filters to block traffic from the source of the scans.

Land attack

This alert notifies that a TCP SYN packet was sent with a spoofed source IP address and port number that matches that of the destination IP address and port. If the attack is successfully mounted, it can cause some TCP implementations to go into a loop that crashes the computer.

If this alert occurs, configure the IP packet filters to inhibit traffic from the source of the scans.

Ping of death attack

This alert notifies that a large amount of information was appended to an Internet Control Message Protocol (ICMP) echo request (ping) packet. If the attack is successfully mounted, a kernel buffer overflows when the computer attempts to respond, which crashes the computer.

If this alert occurs, create a rule that specifically denies incoming ICMP echo request packets from the Internet. Note that by default, ICMP echo requests are rejected by the packet filter mechanism from all sources.

UDP bomb attack

This alert notifies that there is an attempt to send an illegal User Datagram Protocol (UDP) packet. A UDP packet that is constructed with illegal values in certain fields will cause some older operating systems to crash when the packet is received. If the target machine does crash, it is often difficult to determine the cause.

If this attack occurs, block the source with an IP packet filter rule.

Windows out-of-band attack

This alert notifies that there was an out-of-band denial-of-service attack attempted against a computer protected by ISA Server. If mounted successfully, this attack causes the computer to crash or causes a loss of network connectivity on vulnerable computers.

If this attack occurs, block the source with an IP packet filter rule.

When a possible intrusion attempt is detected the *intrusion detected* alert can be triggered which can take action ranging from simply logging the event to shutting down the ISA Server. The section entitled *Monitoring* covers this in detail, but in short it is recommended to configure this alert to send a notification in whatever method is most likely to catch the attention of the appropriate administrator.

The events written to the application log by the intrusion detection alert are very useful in diagnosing and responding to intrusion attempts. Figure 38 illustrates the event log entry in response to a Windows out-of-band attack. Note that it clearly indicates the source IP address.
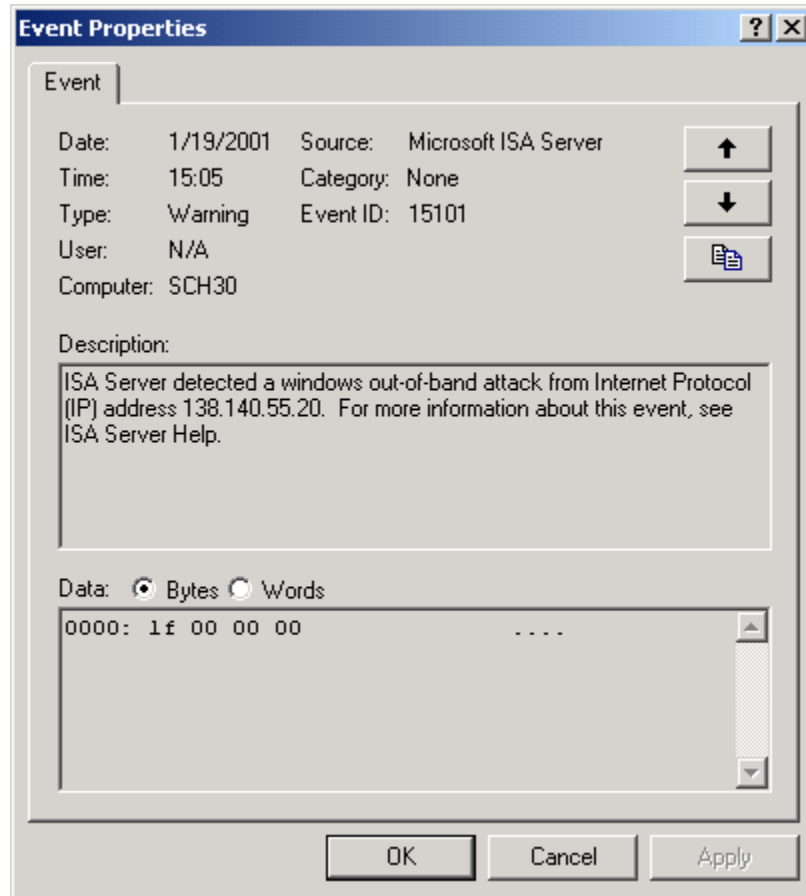
Figure 38 -- Intrusion Detection Event Log

Note that intrusion detection technology is far from foolproof and ISA Server's intrusion detection facilities are no exception. Also note that ISA Server only makes a very modest attempt at intrusion detection – there are many attack scenarios which it does not cover. As long as the limitations are recognized, the intrusion detection features can be utilized for a modest level of protection.

Summary

In summary, the following recommendations are made with regard to packet filtering and the related intrusion detection features:

- ❑ Enable packet filtering.

- ❑ Enable filtering of IP fragments.

- ❑ Enable filtering of IP options.

- ❑ Disable the H.323 extension if practical.

- ❑ Do not enable IP routing except as noted under ***Publishing a Mail Server -- DMZ With Filtering Router &Tri-Homed Firewall***.

- ❑ Consider enabling the intrusion detection (ID) mechanisms, particularly if not running a separate ID system.

- ❑ If the ID features are enabled, configure the corresponding alert to take appropriate action upon detection of a suspected intrusion attempt.

- ❑ As a precaution, run a port scanner from the external network to ensure that only those ports minimally required are left open.

Chapter

5

Extensions

Extensions offer additional functionality to the firewall features of ISA Server. They access the data streams associated with sessions being serviced by ISA Server to allow additional activities to be performed on those sessions. For example, a POP3 filter is provided that monitors for possible buffer overflow attacks against a published POP3 server.

A brief overview of the extensions that ship with ISA Server is offered below with additional detail provided for those settings that are particularly relevant from a security standpoint. These extensions can be accessed by selecting **[array name]/extensions/application filters** in the ISA Server MMC. Most of these descriptions are from the ISA help facility which does an excellent job of describing the functionality of the extensions.

DNS Intrusion Detection Filter

The DNS intrusion detection filter intercepts and analyzes DNS traffic destined for the internal network. It can be configured to monitor four kinds of activity:

- *DNS hostname overflow*. A DNS hostname overflow occurs when a DNS response for a host name exceeds a certain fixed length. Applications that do not check the length of the host names may overflow internal buffers, allowing a remote attacker to execute arbitrary commands on a targeted computer.

- *DNS length overflow.* DNS responses for Internet protocol (IP) addresses contain a length field which should be four bytes. By formatting a DNS response with a larger value, some applications executing DNS lookups will overflow internal buffers, allowing a remote attacker to execute arbitrary commands on a targeted computer.

- *DNS zone transfer from privileged ports (1–1024)*. A DNS zone transfer from privileged ports (1–1024) occurs when a system uses a DNS client application to transfer zones from an internal DNS server using a source port of 1-1024.

- *DNS zone transfer from high ports (above 1024)*. Similar to the above, but focused on high port connections.

It is recommended to enable the DNS intrusion detection filter and to configure it to monitor all four kinds of activity. To access these settings select the **DNS intrusion detection filter** object and right click to access the properties page.

It is also important to note that this filter works in conjunction with the DNS intrusion alert settings. As described in the *Monitoring* chapter, this alert should be enabled with alerts issued in whichever manner is most likely to catch the attention of the appropriate administrator. It is recommended that the event tab for this alert be set as illustrated in Figure 39. Note that this configures the alert to trigger on any DNS intrusion. To access these settings, navigate within the ISA Server MMC to **[array name]/monitoring configuration/alerts** and open the **property** page for the DNS intrusion alert.
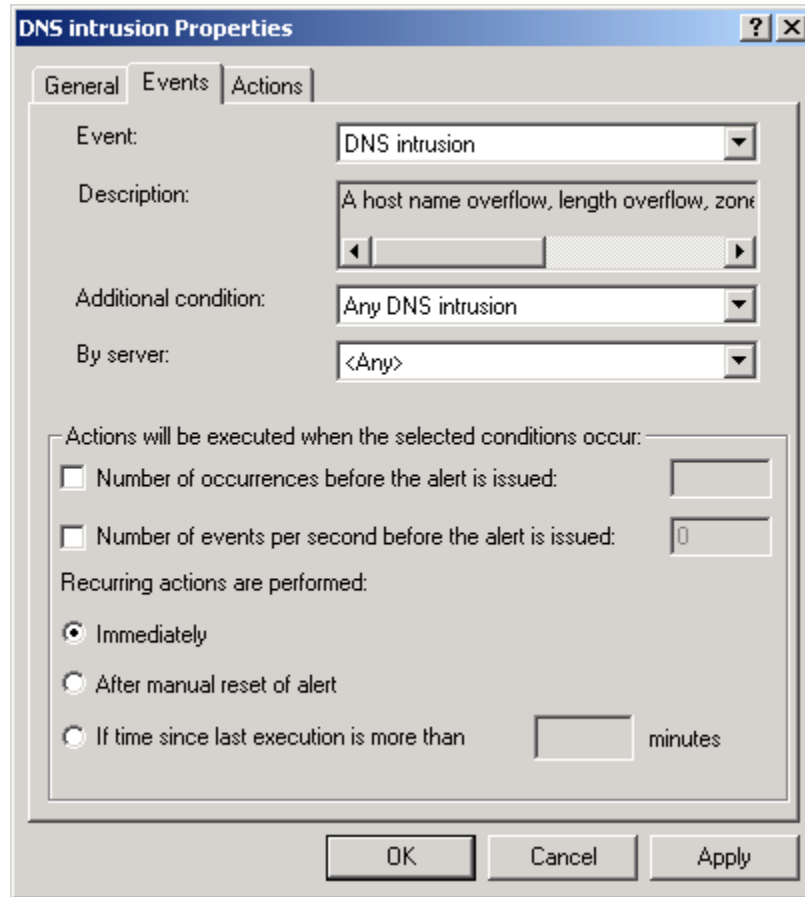
Figure 39 -- DNS Intrusion Detection Alert Settings

There are a number of things to keep in mind regarding the DNS intrusion detection filter. First, this extension monitors traffic destined for the internal network – suspicious activity directed toward the ISA computer itself will not result in an alert. Second, while this filter is useful, do not rely on it as total protection against zone transfers. Windows 2000 relies heavily on DNS and the ability to obtain the complete DNS record for a site offers a potential adversary a great advantage. Make certain that no internal DNS servers are exposed to the external network. If it is necessary to expose DNS information, do so from the DMZ and only expose that data which is truly required by external users. The document *Microsoft Windows 2000 Network Architecture Guide*, part of the operating system security guide mentioned in ***An Important Note About Operating System Security*** discusses this is some detail.

FTP access filter

This extension is one that is not configurable by the administrator except that it offers the option of being enabled or disabled. This filter forwards FTP requests from secure network address translation (NAT) clients to the firewall service. The filter dynamically opens secondary ports, which are required by the FTP protocol, and performs necessary address translation for NAT clients. It is generally recommended to enable this filter (which is the default).

H.323 protocol filter

The H.323 protocol filter allows H.323 applications, such as NetMeeting, to work through ISA Server. If this filter is enabled, ISA Server will open port 1720 on the ISA Server's external connection. It is therefore recommended to disable this filter if H.323 support is not required.

HTTP redirector filter

This filter is analogous to the FTP access filter in that it forwards HTTP requests from the firewall and secure network address translation clients to the Web Proxy service.   This feature is necessary to support basic ISA Server functionality so it is generally recommended to enable this filter (which is the default).   If the recommendation contained on page 83 to always use the Web Proxy Client for HTTP access is followed, then the HTTP redirector option to reject HTTP requests from Firewall and secure NAT clients should be enabled.

POP intrusion detection filter

The Post Office Protocol (POP) intrusion detection filter intercepts and analyzes POP traffic destined for the internal network. Specifically, the application filter checks for POP buffer overflow attacks. A POP buffer overflow attack occurs when a remote attacker attempts to gain root access of a POP server by overflowing an internal buffer on the server. There are limits to the utility of this filter, as is typically the case for intrusion detection technology. Nonetheless, if publishing a POP3 server it is recommended to enable this filter (which is the default) and to configure the corresponding alert in a manner similar to that described for the DNS intrusion detection filter.

ISA Server will disconnect the POP connection upon triggering of the alert. This is not persistent – an adversary can reconnect to the published POP server immediately upon disconnection. It is possible to take the added precaution of configuring the alert to shut down the POP3 service in the event a possible intrusion is detected. This is configured from the **actions** tab of the POP intrusion alert. To access this tab, navigate within the ISA Server MMC to **[array name]/monitoring configuration/alerts** and open the **property** page for the POP intrusion alert (Figure 40). The author's intent is simply to highlight the availability of the feature – a decision regarding whether or not to do this must weigh the possible consequences of an attack against the inconvenience of shutting down the POP3 service.
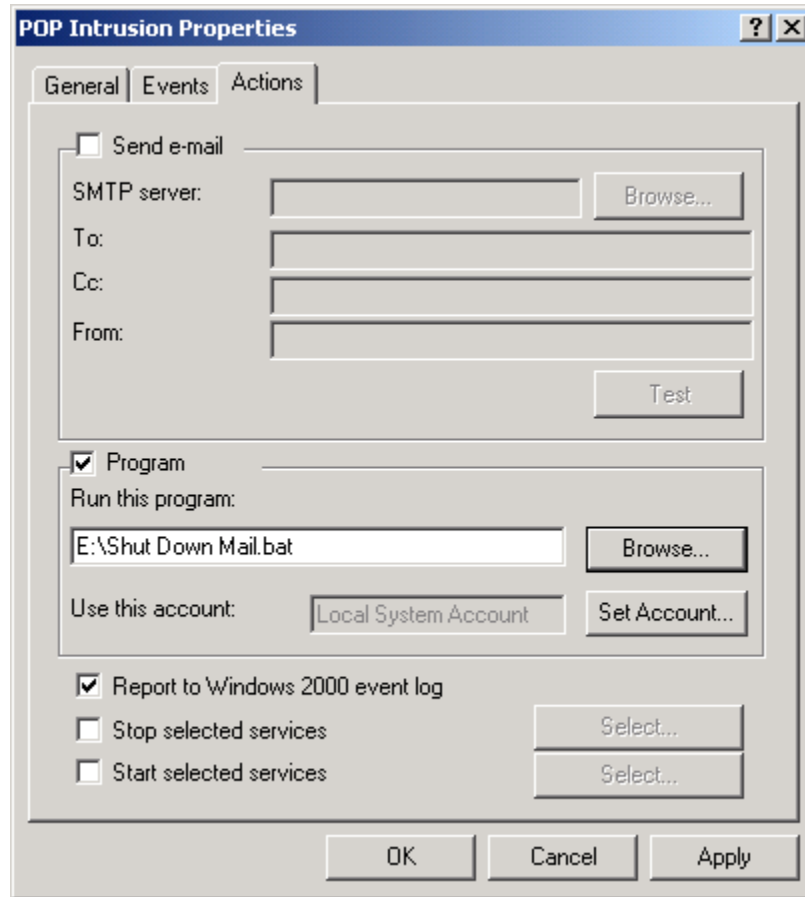
Figure 40 -- Shutting Down POP3 Server In Response To An Attack

RPC Filter

The RPC filter enables publishing of RPC servers, making them accessible to external clients. The most common application for this is the publishing of Exchange Servers; however, if the Exchange server is published via SMTP, POP3, and/or IMAP4, it is recommended to disable this filter.

SMTP filter

The Simple Mail Transfer Protocol (SMTP) filter intercepts all SMTP traffic that arrives on the SMTP port (port 25) of the ISA Server computer. It is intended to allow the definition of filter mechanisms that can reject messages destined for published SMTP servers based upon a variety of parameters such as sender, attachment type, attachment name, etc. The filter accepts the traffic, inspects it, and passes it on only if it the rules allow it. Getting the messaging filtering features to function properly has proved to a challenge for many administrators. In the author's attempts at screening messages destined for a published Exchange 2000 Server, the additional step of installing the message screener on the Exchange Server was the only "trick" required; however, other architectures may require different procedures. The ISA help file and the Shinder book listed in the references may be helpful.

Note that unlike the other extensions, the SMTP filter is disabled by default. If publishing SMTP severs behind an ISA Server, it is recommended to enable the filter and configure it as detailed below; however, note that without preventive action this could create a possible denial of service condition. Please reference the Microsoft knowledge base article at http://support.microsoft.com/support/kb/articles/Q292/0/10.ASP.

Attachment Tab

The options on this tab are designed to allow the filtering of messages based upon attachment names or extensions. Blocking attachments that represent executables can be useful as a countermeasure against malicious attachments, but it is important to recognize that it is generally impractical to block all file attachments that could contain malicious code. Many operationally critical document files can contain an executable component (e.g., Word macros) and therefore it is important to also utilize other malicious code countermeasures such as virus scanning and the intrinsic malicious code countermeasures available with some applications.

Deciding which attachment types to block is a trade-off between operational functionality and security. The following set of file attachments is recommended as a starting point. In addition to executable file types it includes a variety of common system files and configuration files.

.acm – Windows Systems File	.msi – Windows Installer Patch
.bas – Visual Basic Class Module	.msp – Windows Installer Patch
.bat – Batch file	.mst – Visual Test Source File
.bin – Binary file	.ocx – OLE Control Extension
.chm – Compiled HTML help file	.otm – VBA Project File
.cmd – Windows Command Script	.ov* - Program Overlay File
.com – MS Dos Application	.pif – Program Information File
.cla – Java applet	.pl – Perl Script
.class – Java applet	.reg – Registry File
.cpl – Control Panel Extension	.scr – Screen saver
.crt -- Certificate	.scf – Explorer Command File
.drv – Device driver	.sct – Windows Script Component
.exe – Application	.shb – Document Scrap Object
.fon -- Font	.shs – Shell Scrap Object
.fot -- Font	.sys – System File
.dll – Dynamic Link Library	.tlb – Type Library
.hta – HTML Applications	.url – Internet Shortcut
.ini – Initialization file	.vb – VBScript File
.inf – Setup Information File	.vbe –VBScript Encoded Script File
.ins – Internet Communication Settings	.vbs – VBScript Script File
.isp – Internet Communication Settings	.v*d – Virtual Device Driver
.js – JScript file	.ws – Windows Scripting File
.jse – JScript Encoded Script File	.wsc – Windows Script Component
.lnk – Shortcut	.wsf – Windows Script File
.mpd – Mini-port Driver	.wsh – Windows Scripting Host Settings

It may be prudent to add, or delete files from this list depending upon operational realities. For example, if they are not operationally required it may be prudent to block applications within the Microsoft Office family, all of which can contain an executable component. Most notable are Microsoft Access files, which compared to other members

of the Office family, has more limited intrinsic protection against malicious macros[4]. Other examples include Corel script files (*.csc).
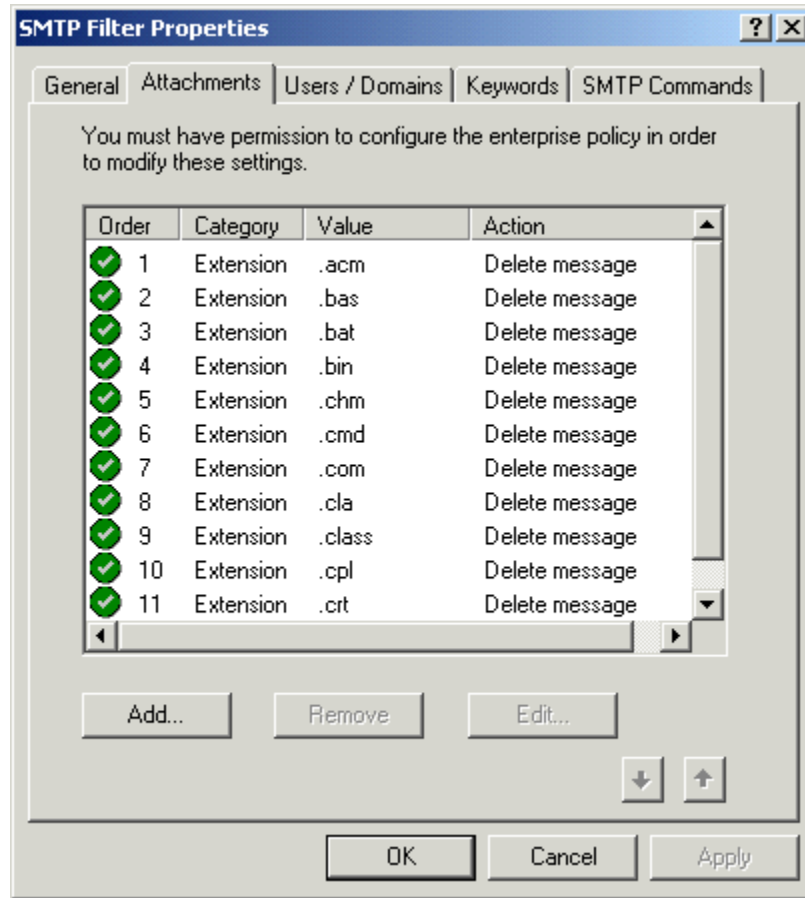
Figure 41 -- Filtering Based Upon Attachment Name/Type

---

[4] For organizations desiring to allow Microsoft Office files, the guide *Microsoft Office 2000 Executable Content Security Risks and Countermeasures*, available at http://www.nsa.gov, is recommended. This guide details the extensive countermeasures against the malicious code threat that is available within most Office applications.

Users/Domains Tab

These settings allow one to filter mail such that specific users (e.g., elvis@foobar.com) or specific domains (all users at foobar.com) cannot connect to the SMTP server. This can be used to filter out known SMTP abusers such as spammers or known purveyors of malicious e-mail.
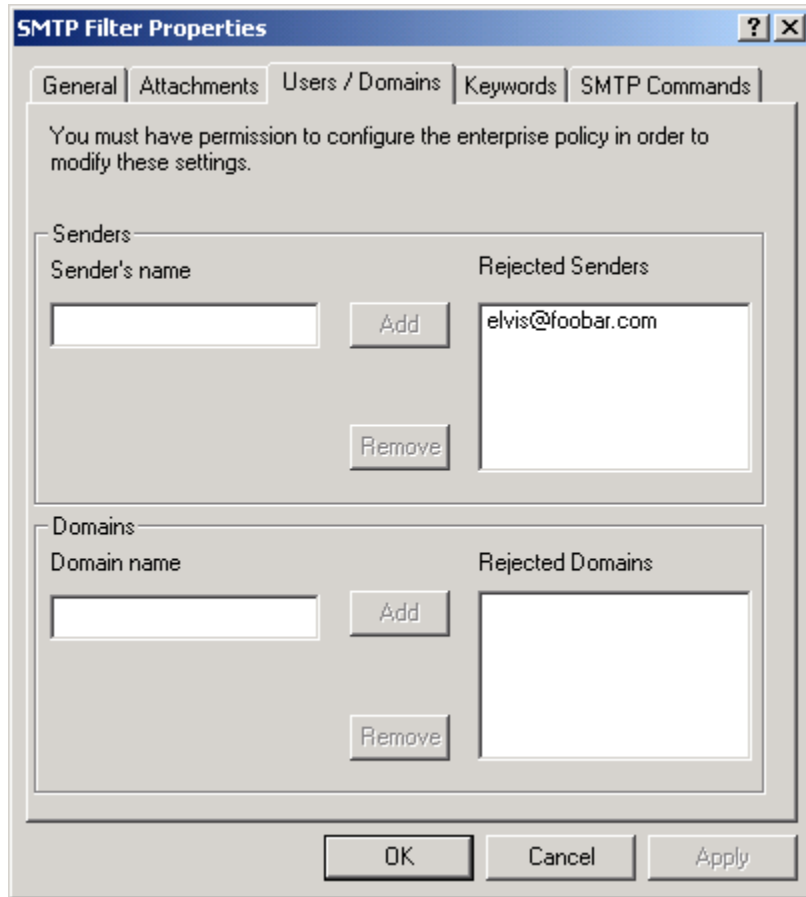
Figure 42 -- Filtering Based Upon Users/Domains

Keywords Tab

These options can be used to filter messages based upon key words contained with the header or body of the message. For example, one could filter all messages with ILOVEYOU in the header as one countermeasure against the infamous ILOVEYOU worm.
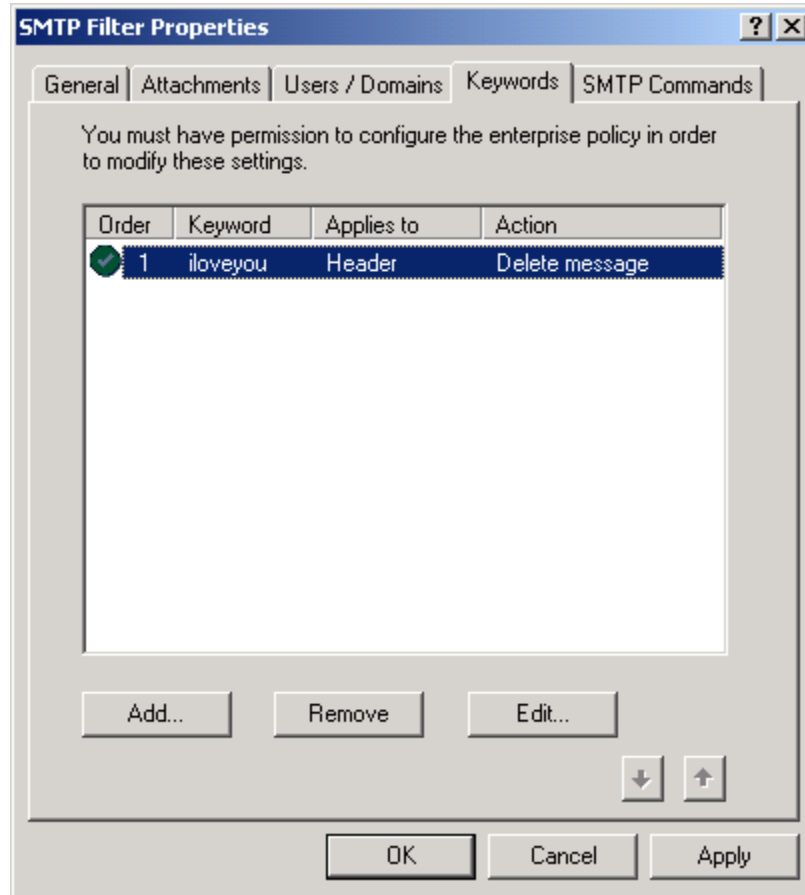
Figure 43 -- Filtering Based Upon Keywords

SMTP Commands Tab

The **SMTP commands** tab (Figure 44) allows one to set thresholds for the maximum size of various commands that will be accepted by the ISA Server on behalf of published SMTP servers. It is recommended to accept the default settings for this tab with the exception of disabling the following commands.

- EXPN. The EXPN command expands a distribution list, providing the requester with all account names in a distribution list. Generally it is not desired to publish this information.

- VRFY. The VRFY command can be used by a client to verify a user's name with the SMTP server. This has the unintended effect of offering a potential attacker a convenient way of obtaining account names.

- TURN. The TURN command is used to reverse the role of the client and server. This is typically used in environments where an organization has a part time

connection to an upstream smart host. The organization's mail server contacts the smart host, forwards outgoing mail, and then issues the TURN command to instruct the smart host to transmit any incoming mail that it is holding for the organization. Most organizations do not rely on this command and it is therefore generally recommended to disable it.

- NOOP. The NOOP is somewhat analogous to an ICMP ping command – it simply requests that the server respond with a positive reply code. This command is also somewhat superfluous and can therefore be disabled.
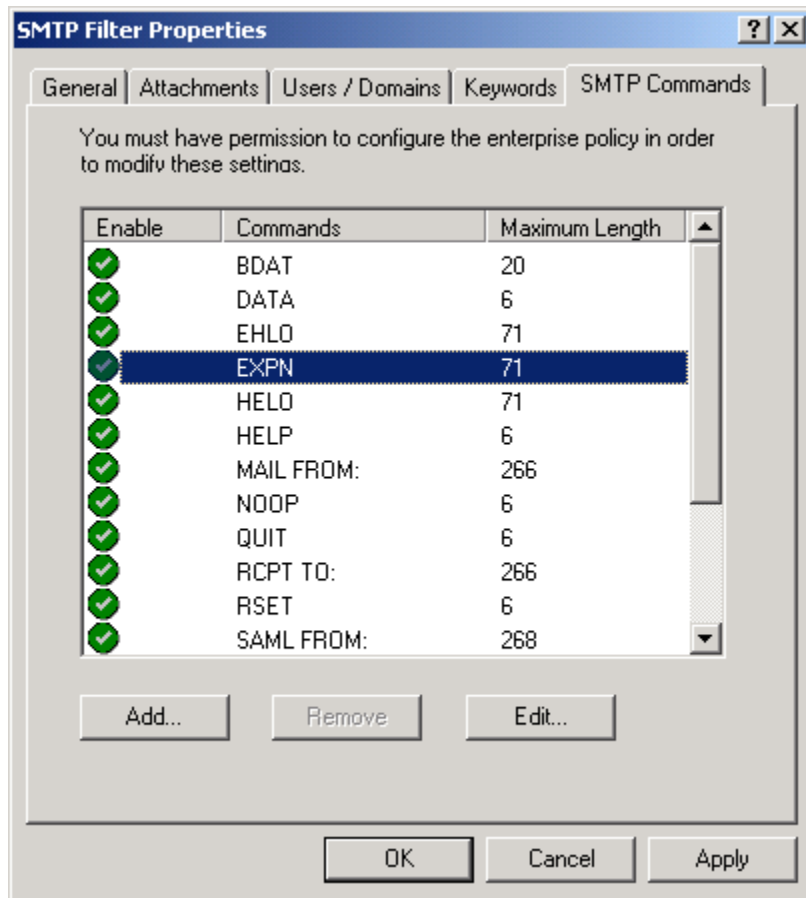
Figure 44 -- SMTP Commands

NOTE: The ISA Server rejects commands not listed and an SMTP filter alert is issued.

SOCKS V4 filter

The SOCKS filter forwards requests from SOCKS applications to the Firewall service. ISA Server then checks the access policy rules to determine if the client is allowed to

communicate with the external network. The primary use of this filter is to support compatibility with Unix applications. There are no specific security concerns associated with its use; however, it is important to realize that SOCKS version 4 does not support the notion of user authentication. Access control under SOCKS can only be accomplished per IP address using client sets.

Streaming Media Filter

The streaming media filter can enhance network performance by splitting live streams. *Live stream splitting* refers to the ability of the filter to obtain information from the external network once and then make it available locally for multiple clients. There are no specific security settings associated with its use.

Summary

In short, the following recommendations are offered in relation to ISA Server extensions:

❑ Enable the DNS intrusion detection filter and configure it to monitor all four types of activity under its purview. Also, appropriately configure the associated alert.

❑ Remember that the DNS intrusion detection filter is not a substitute for a sound network design. Make certain that no internal DNS servers are exposed to the external network.

❑ Disable the H.323 filter unless H.323 support is required.

❑ If the recommendation contained on page 83 to always use the Web Proxy Client for HTTP access is followed, then the HTTP redirector option to reject HTTP requests from Firewall and secure NAT clients should be enabled.

❑ If publishing a POP server, enable the POP intrusion detection filter.

❑ If practical, disable the RPC filter.

❑ If publishing a SMTP server:

○ Enable the SMTP filter and disable the following under the SMTP commands tab: EXPN, VRFY, TURN, NOOP.

○ If using the message screener, reference http://support.microsoft.com/support/kb/articles/Q292/0/10.ASP

○ Use the message screener to block potentially dangerous file attachments (a recommend list of attachment types along with a known issue is provided here as a starting point) destined for any published SMTP servers.

○ Use the message screener to block e-mail based upon keywords – this can is particularly useful in response to an ongoing malicious code incident.

○ Keep in mind that the message screener has the ability to block access to specific users or domains as a countermeasure against known malicious users.

❑ If utilizing SOCKS clients, make certain the SOCKS filter is enabled and recall that user based access controls are not possible – only IP based authentication (client sets) are applicable.

Chapter

6

Publishing

Overview

Publishing refers to allowing access from the external network to a select server, or group of servers, behind the ISA Server. This is typically done to allow external access to a web, database, or mail server.

Anytime access is allowed from an untrusted environment there is an obvious security risk. This risk can be mitigated through the use of a demilitarized zone (DMZ) which is also sometimes referred to as a *perimeter network*. A DMZ is an additional network utilizing private IP addresses and residing between the external and internal networks and used to provide an added layer of security. For example, if an organization had the need to publish a web site to the Internet, it is critical to avoid putting this web server on the internal network since an attacker compromising the web server would have a very convenient launching point for attacks against the internal network. Placing the web server in a DMZ is an alternative that provides an additional layer of security by avoiding access in the internal network from the untrusted Internet. One method of implementing a DMZ is shown below:

Intranet   **Firewall-b**   DMZ   **Firewall-a**   **Internet**

Web Server

Allows no
incoming
connections
from Internet

Allows incoming
connection from
Internet only to
the Web Server
in the DMZ.
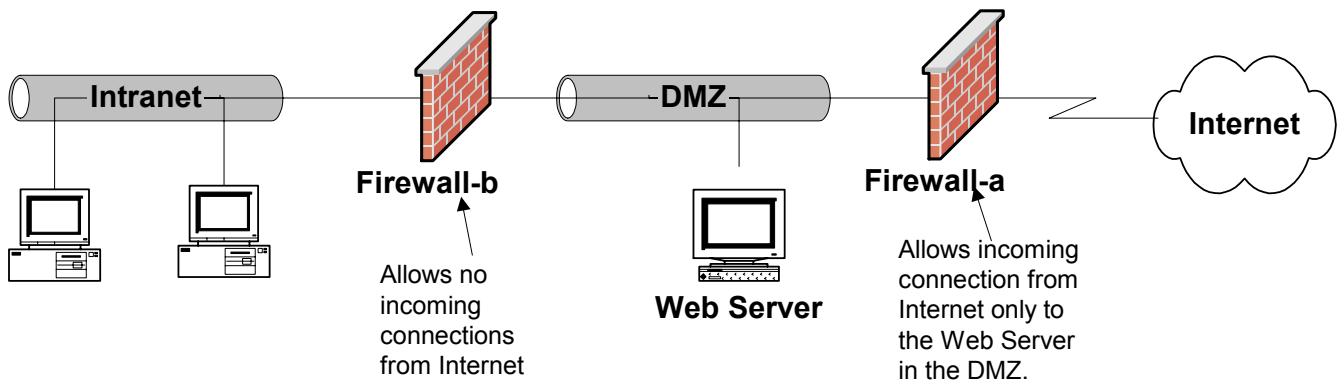
Figure 45 -- A DMZ Utilizing Two Firewalls

While Firewall-a allows incoming connection requests to the web server in the DMZ, security is enhanced in that no incoming connection requests are allowed by Firewall-b. This, of course, helps preclude Internet based attacks from reaching the internal network. Security is optimized if different firewall products are utilized. While Firewall-a in this illustration allows HTTP connection requests to the web server, all other connection requests should be rejected. If an attacker is able to exploit a vulnerability in Firewall-a to compromise this access policy, having a different firewall at the perimeter of the intranet may decrease the chance that the same vulnerability could be utilized to gain access.

This is also a convenient architecture in that in many instances a router is used to connect to the external network. Using a router with a filtering capability can serve the dual role of functioning as Firewall-a. If a filtering router is being utilized, a recommended source for assistance in configuring it is the *Router Security Configuration Guide* which is available at http://www.nsa.gov.

ISA server is best suited for use as Firewall-b since, in Windows environments, its protocol rules and site and content rules could allow for fine grain access control.

An alternative DMZ architecture is illustrated in Figure 46. It operates on the same principal as the prior example, except only one firewall is utilized. This firewall includes three network interface cards allowing connection to the Internet, DMZ, and intranet.
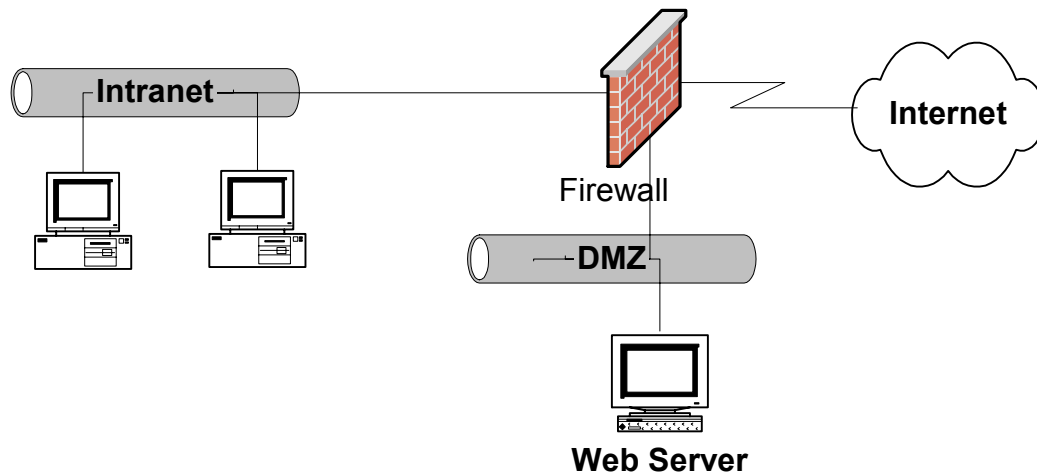
Figure 46 -- A DMZ Utilizing A Tri-Homed Server

In this approach the same rule set applies – connections requests from the Internet are only accepted for the web server in the DMZ. This approach has the obvious advantage of requiring less hardware, but at the loss of the additional layer of protection afforded by the second firewall. This architecture also has the disadvantage in that in order to support this configuration ISA server must be configured to route the packets directly to the DMZ. As a consequence there is no translation of IP addresses for data flowing to-from the DMZ and the only rules that are enforced are packet filter rules.

Finally, a third generic DMZ architecture is presented in Figure 47. This is lifted from the network diagram included in the *Microsoft Windows 2000 Network Architecture Guide*. It combines attributes from both of the prior examples. In this example it is assumed that the external router actively mediates access for clients and servers and for network services by performing packet filtering and stateful inspection. The router helps to enforce the organization's security policy by allowing only approved connection requests to access the DMZ or internal network. Adjacent to the external router is a tri-homed firewall with access to both the internal network and the DMZ. This architecture allows the use of a tri-homed firewall while preserving the positive benefits of the two-firewall solution.
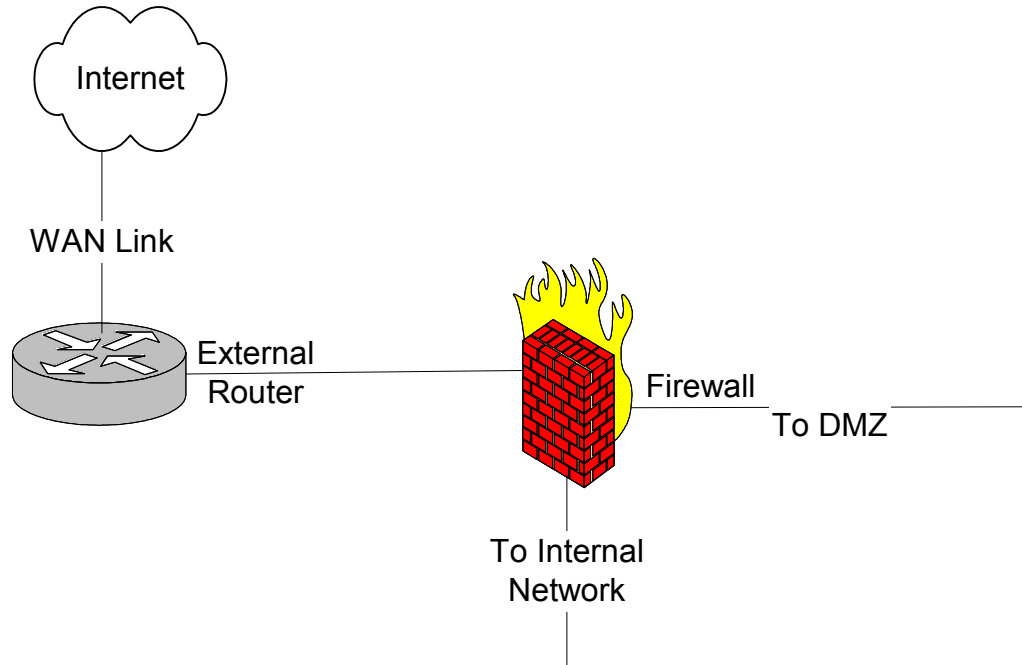
Figure 47 -- DMZ With Filtering Router And Tri-Homed Firewall

ISA Server is able to support all three scenarios. The ISA Server help file provides additional details on how to set up ISA Server to support these scenarios (although, understandably, it assumes ISA server is the only type of firewall being used).

The procedures for enabling publishing vary depending upon which DMZ architecture is being used. In the first example, assume for a moment that Firewall-a is an ISA Server. Publishing rules are used in this architecture to allow access from the external network (Internet) to servers in the DMZ. Publishing rules are created under the **publishing** container. Select either the **web publishing rules** or **server publishing rules** container, right click, and select **new, rule**. For publishing e-mail servers, a **secure mail server** option is also provided. Note that this name is something of a misnomer – running this wizard does not ensure a secure e-mail server as it has no ability to configure the e-mail server or the e-mail clients that are critical to a secure e-mail system. Instead, use of the word *secure* simply infers that the wizard will only open up those ports which are necessary to publish the mail server. Publishing rules do not work in the case where a tri-homed ISA Server is being utilized. Instead, packet filtering rules are used which allow connections from the external network to the server being published in the DMZ.

Publishing rules provide a straightforward function – they instruct the ISA Server to listen to its external connection for certain connection requests and forward those requests to the appropriate computer within the DMZ. For example, if a SMTP/POP3 server is being published within the DMZ, the ISA Server will forward connection requests on port 25 and 110 (the SMTP and POP3 ports) to the DMZ computer specified in the publishing rule.

The security issues related to publishing servers via ISA Server is best illustrated with a series of examples.

Publishing a Mail Server – A DMZ Using Two Firewalls

The following illustrates how to setup server publishing rules using as an example a SMTP/POP3 server. This example assumes that the preferred method of building a DMZ – placing it between two firewall products – is being utilized. As mentioned earlier, the optimal solution when using this kind of DMZ is to utilize two different firewall products around the DMZ and that ISA Server is perhaps best suited for the interior firewall (Firewall-b in Figure 45). However, since this guide is intended to illustrate ISA Server security concepts it will assume for the moment that ISA Server is being used as the exterior firewall (Firewall-a in Figure 45) which is where publishing rules are created. The secure mail server wizard is used to create the appropriate rules on this exterior ISA Server.

To access the secure mail server wizard expand **Servers and Arrays** from within the ISA Management console. Expand the **[array name]** container, then **select** publishing. In the right pane, click "Secure E-mail Server." After proceeding past an introductory dialog box, the first dialog box of consequence in the wizard simply requests the range of mail features that are to be published (Figure 48). The options are those expected for mail related services – SMTP, POP3, IMAP4, and the NNTP protocols are supported by the wizard. Also, one can specify if the mail server requires the protocol to be tunneled through SSL. Based upon the selections the wizard will configure ISA Server to listen on the appropriate ports for connection requests – port 25 for SMTP, port 110 for POP3, port 995 for POP3/SSL, etc. In this example **Incoming SMTP** and **Incoming POP3** is selected.

> **NOTE: The user is given the option to apply content filtering. This is recommended - please reference the chapter entitled** *Extensions* **for more information and some notable limitations.**

Figure 48 -- Specifying The Applicable E-mail Protocols

In the next dialog box the IP address of the ISA Server's external network interface card is entered (Figure 49). This simply instructs ISA server to listen for incoming SMTP and POP3 connection requests on that interface card. This has a very positive security implication in that clients on the external network will connect to this IP address to access the mail server – ISA Server helps to protect the details of the composition of the DMZ network.

Mail Server Security Wizard

ISA Server's External IP Address
Clients send requests for mail services to the external IP address of the ISA Server computer

Enter the external IP address of the ISA Server computer.

External IP address: 138 . 140 . 55 . 10   Browse...

Find IP...

< Back   Next >   Cancel
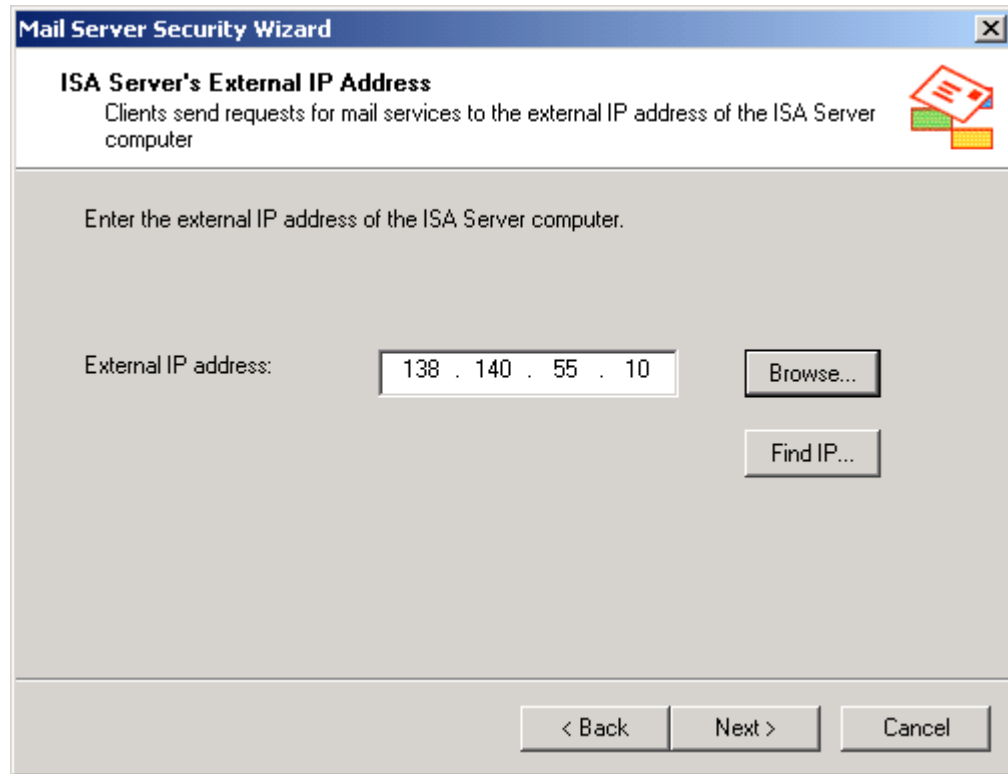
Figure 49 -- Entering The IP Address Of The ISA Server

Next, the address of the internal server (the SMTP server in the DMZ) is specified (Figure 50). This completes the mapping that instructs ISA Server to forward connection requests on port 25 and 110 to the appropriate computer in the DMZ.
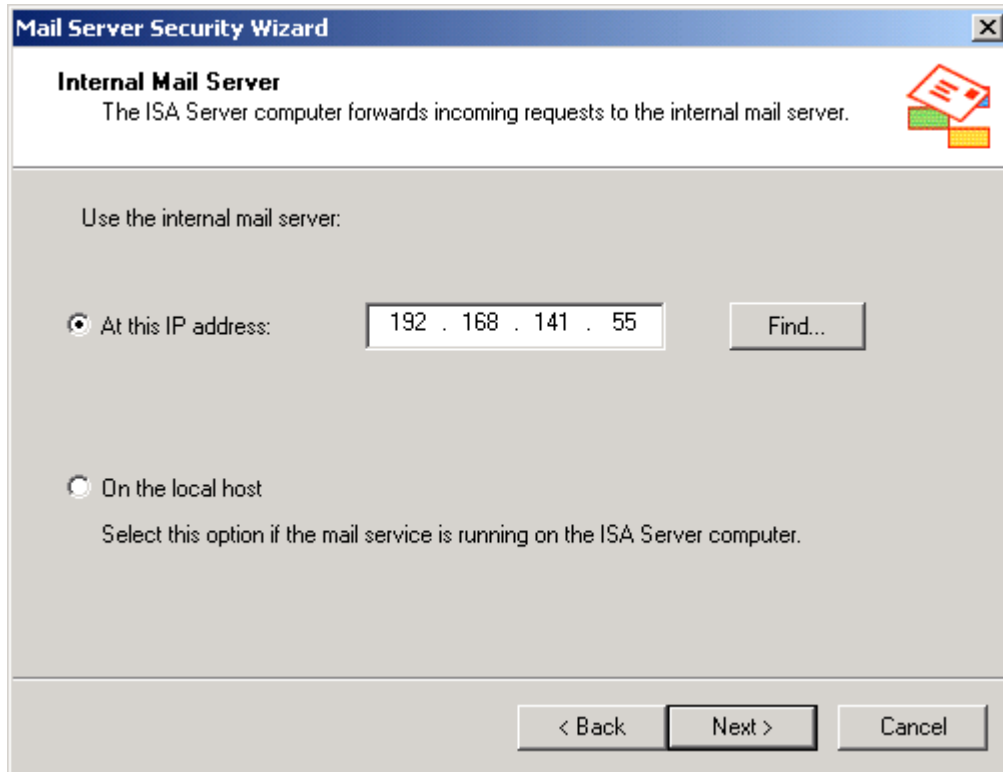
Figure 50 -- Specifying The E-mail Server Being Published

At this point the wizard presents a summary of the requested actions and is then complete. Unfortunately, the wizard ends somewhat prematurely in that there is another option to consider. ISA Server allows the administrator to restrict, by IP address, the set of computers that are allowed to access the published server. For a general purpose SMTP/POP3 server intended for wide ranging use these settings may be non-applicable, but in more closed environments it may be possible to restrict access to a certain set of computers. These restrictions should be put into place if possible. To do so, simply open the property page for the rules created by the wizard and select the **applies to** tab.

Publishing a Web Server – A DMZ Using Two Firewalls

A second example is offered to illustrate how to construct publishing rules without the benefit of the secure e-mail wizard. This example also assumes that the preferred method of building a DMZ – placing it between two firewalls – is being utilized. A web server will be used for this example.

Publishing a web server is a little more involved as there are additional options to consider. Assume that it is desired to create a web publishing rule to publish HTTP and HTTPS services from the DMZ to the Internet. The following summarizes the steps required and amplifies the more salient security considerations.

The first step is to create and configure a web listener. This is accomplished under the **[array name]** container. Open the properties page and select the **incoming web requests** tab. A web listener could be applied to any IP address on the ISA Server computer that is not in the local address table (reference *ISA Server Installation – Installation Directory/Components, Array Policies, Server Mode, Local Access Table*). To ensure that the listener is configured for the proper IP address, it is generally best to select the **configure listeners individually per IP address** option. Click **add** and select the IP address connected to the external network (Figure 51). Also, if HTTPS (HTTP over a SSL tunnel) is to be supported, select the appropriate SSL server certificate. If a server certificate has not been installed on the ISA Server computer it will be necessary to do so before the ISA Server computer can accept HTTPS connection requests. A server certificate can be obtained from a variety of certificate authorities and the ultimate source will vary depending on local policies. Some organizations may run their own certificate authorities; others may outsource this function to any number of companies that provide such services. Finally, select the authentication method. The options for authentication are those that are available for Microsoft Internet Information Server. The *Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0*, available at http://www.nsa.gov, describes these options in detail. Since this example illustrates publishing a web server for access from Internet users in general, no authentication is required.
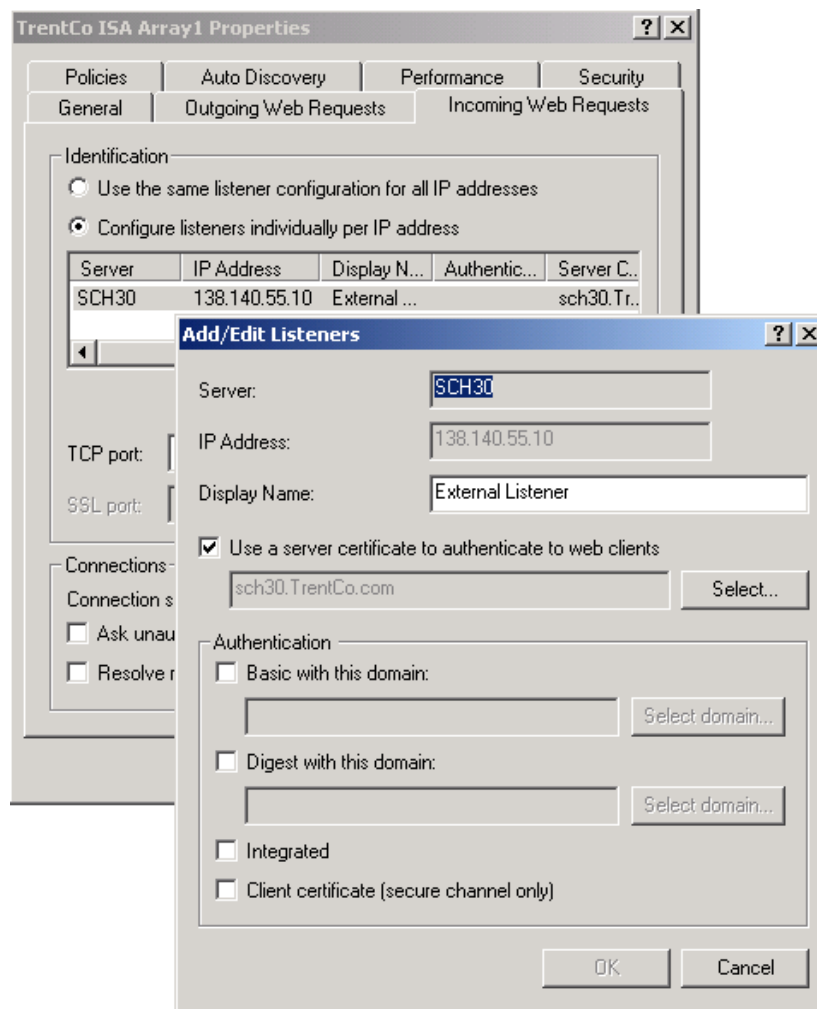
Figure 51 -- Setting Up Listeners

If accepting HTTPS requests it is also necessary to enable SSL listeners on the incoming web requests tab (Figure 52). Finally, specify the ports used for both HTTP (labeled *TCP port*) and HTTPS (the *SSL port*).
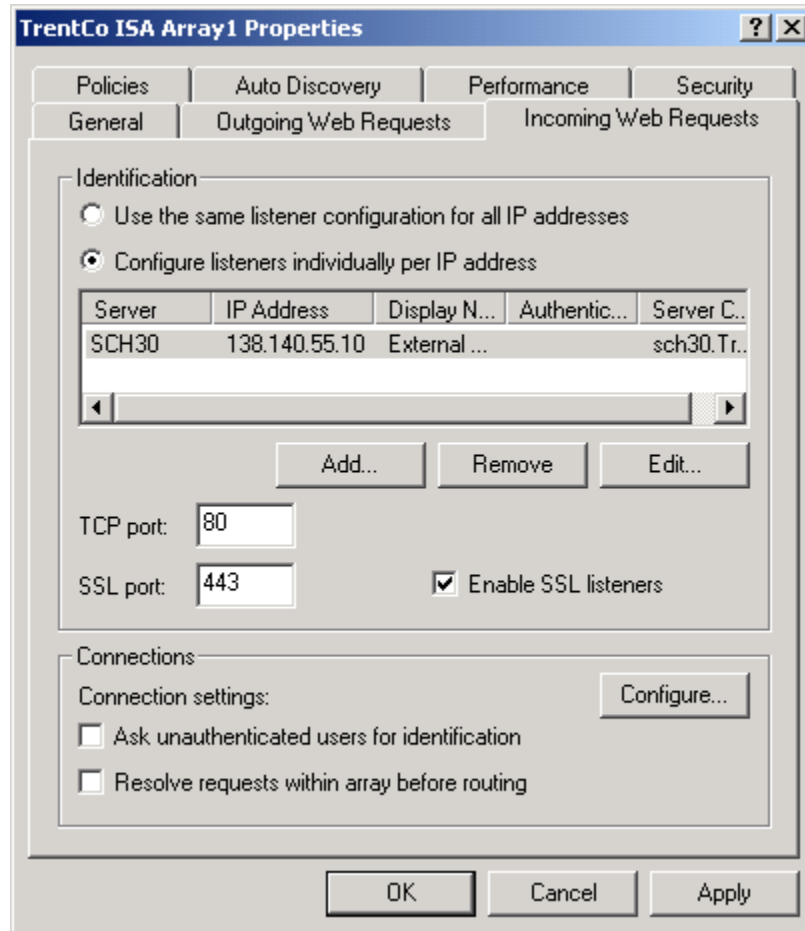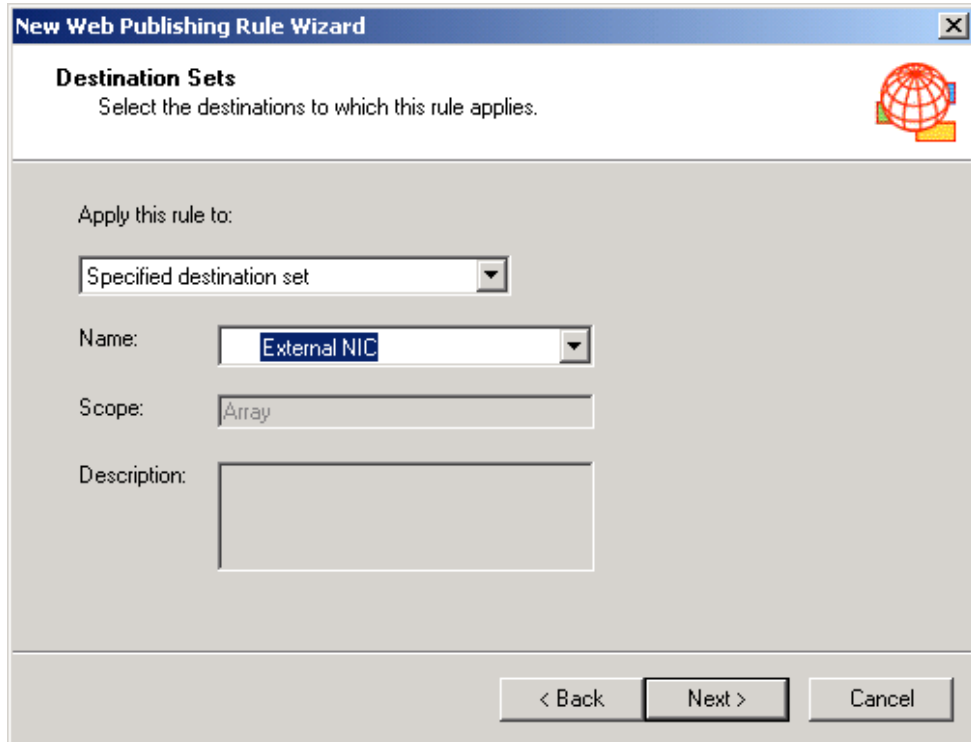
Figure 52 -- SSL Listeners

After the listener has been set up, it is necessary to define the web publishing rule. Web publishing rules are created under the **publishing** container. Select the **web publishing rules** container, right click, and select **new**, **rule**.

After entering a descriptive name for the rule, the web publishing wizard asks for the applicable destination sets (Figure 53). For web publishing the destination set must include the IP address of the network interface card attached to the external network. Create a destination set with just that IP address and select it via the drop-down list.

Figure 53 -- Specify The External NIC As The Destination Set

Next, specify which clients are allowed to connect to the published server (Figure 54). Since this example assumes the server is to be accessible by the general Internet community, **any request** is selected. It is always desirable to restrict access as much as possible - in a more closed environment it may be possible to utilize the other options on this dialog box which restrict access by account or by IP address.
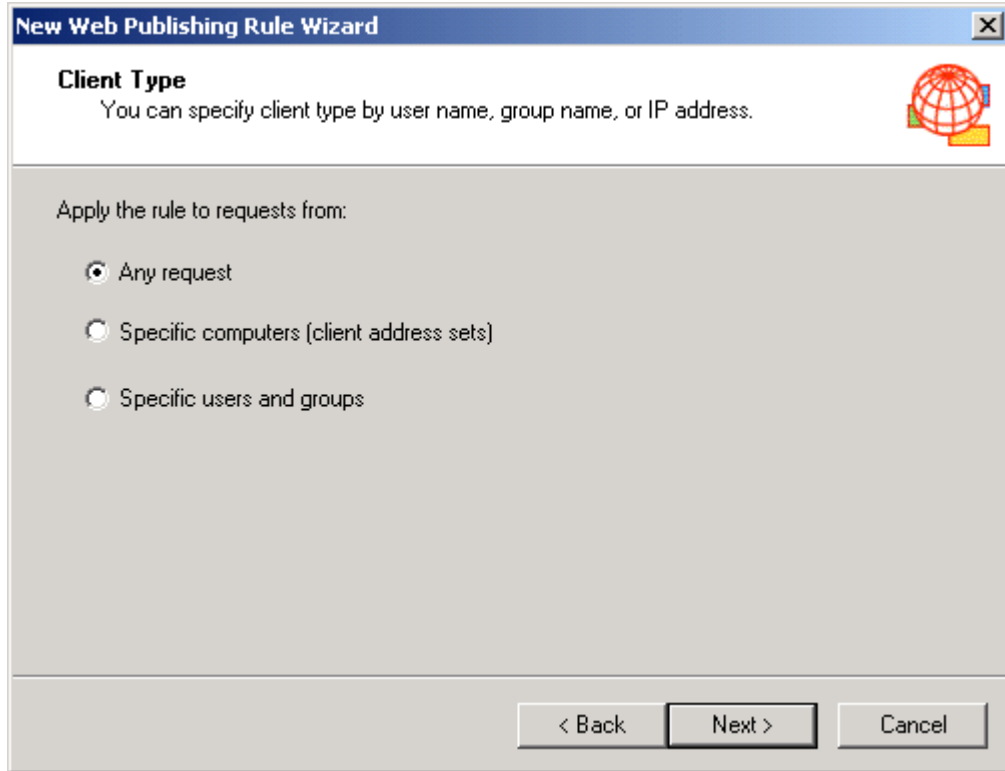
Figure 54 -- Specifying The Client Set

Specify the computer to be published as well as the applicable ports. This instructs ISA Server to forward incoming requests to the appropriate web server and port within the DMZ (Figure 55).

Figure 55 -- Specifying The Web Server Being Published

After the wizard is completed, open the newly created rule and go to the **bridging** tab (Figure 56). This dialog page is used to configure how HTTP and HTTPS packets are forwarded to the internal server. HTTP packets, which are unencrypted when received by the ISA server, may remain unencrypted as they are forwarded to the server being published or they may be encrypted prior to forwarding. Similarly, HTTPS packets from the external network, which are encrypted in transit and then unencrypted by the ISA Server computer, may remain unencrypted or may be re-encrypted prior to being sent to the server being published. This setting has no effect on the link from the client on the external network to the ISA Server, but instead deals solely with the issue of the connection between the ISA Server and the published server. The specific settings utilized are dependent on the local environment. In the case where physical and logical access to the published server and network is restricted, it may be acceptable not to encrypt this link. In cases where such protection is not available, it might be prudent to encrypt this link in the case of HTTPS connections from the client.

In this example HTTP packets are forwarded as HTTP. This means that unencrypted packets from the client on the Internet will remain unencrypted as they pass from ISA Server to the published server. This is sensible since the unencrypted packets transverse the high-risk environment of the Internet, there is no value in encrypting them for the short haul between ISA Server and the published server.

Similarly, in this example HTTPS packets are not encrypted between ISA Server and published server under the assumption that the path is physically protected. Connections to clients on the Internet that use the HTTPS protocol will be encrypted; however, when

incoming data is received by the ISA Server it will decrypt them and NOT re-encrypt them before forwarding to the published server. Similarly, packets originating from the published server will not be encrypted until they reach the ISA Sever where they will be encrypted prior to their transmittal over the Internet. Once again, please remember that these settings are simply intended as an example and may not be appropriate for other environments.
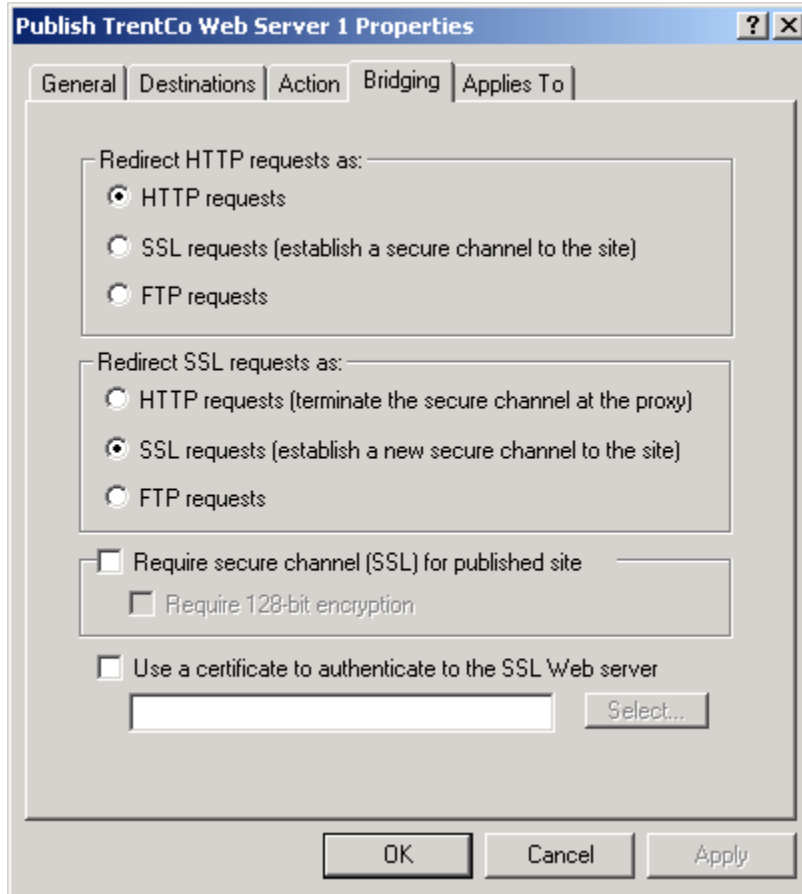
Figure 56 -- Bridging

Note also that HTTP and HTTPS requests can be redirected as FTP requests. This would be used to allow access to a FTP server via a HTTP connection. Security guides relating to a variety of different web servers as well as the FTP server that ships as part of Microsoft's Internet Information Server are available from http://www.nsa.gov.

Microsoft recommends that you do not enable directory browsing on the Web server that is published by ISA Server. Also, the published web server cannot require digest or basic authentication. If it does, the internal name or IP address of the Web server may be exposed on the Internet. Reference the ISA Server help file under the topic *web publishing rules*.

Finally, keep in mind that ISA Server includes a set of error messages that are returned to web browser clients when appropriate. These error messages are stored in the \ErrorHTMLs directory under the ISA Server installation directory. When returning these error messages it is able to distinguish between internal and external client requests with the error messages

with a *R* suffix (for *reverse*) used to service external clients. If publishing a web server it may be prudent to modify these error messages such that references to the ISA server are removed. This will deny a potential adversary an easy method for determining which firewall is being utilized.

Publishing a Mail Server -- DMZ With Filtering Router &Tri-Homed Firewall

Publishing rules do not work when publishing a server contained in a DMZ on a tri-homed ISA Server. Instead, packet filter rules are used. In order to illustrate the security relevant considerations when publishing in this manner, a final example will be presented which once again publishes a mail server.

This is a fairly simple process. First, make certain that the LAT contains only the addresses for the internal network and NOT the DMZ. Second, create a packet filter which allows incoming TCP connections to port 25 (SMTP) and port 110 (POP3). Details on how to create packet filter rules are provided in the section entitled *Packet Filtering* and will not be repeated here. Figure 57 and Figure 58 illustrate the most relevant settings relating to publishing the mail server which, in this example, is located at 137.140.55.20
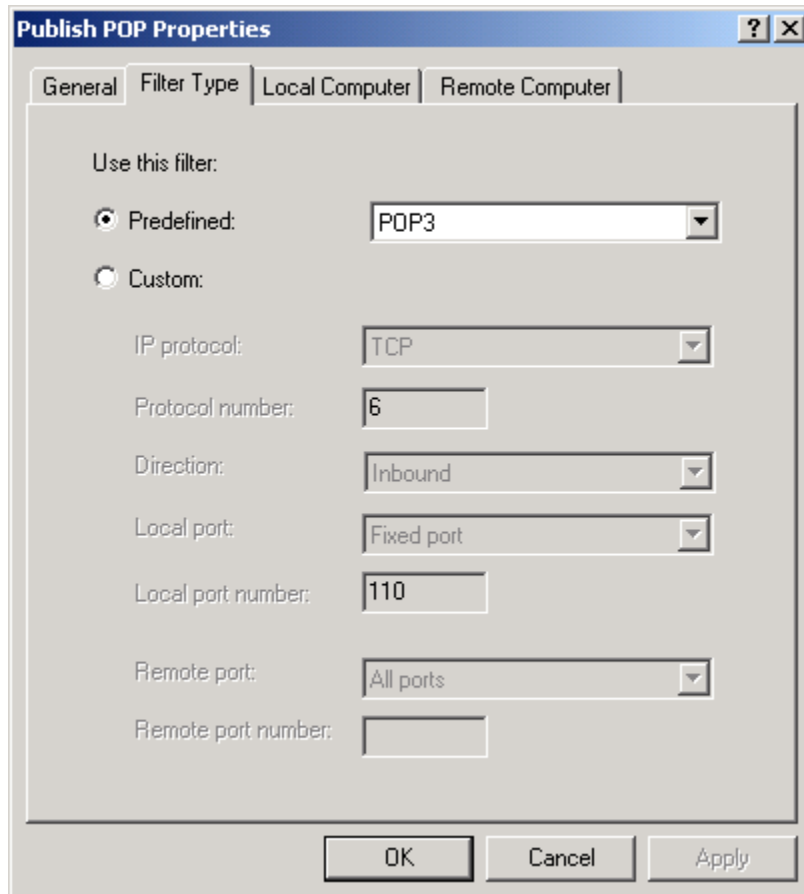
Figure 57 -- Packet Filtering Rule to Publish POP3
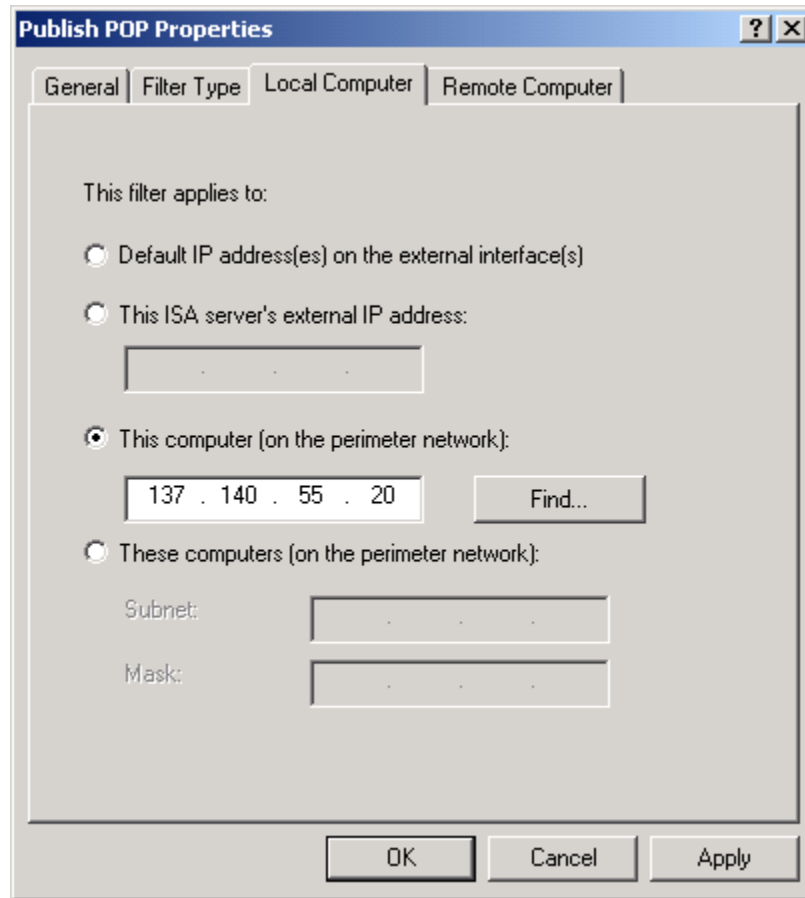
Figure 58 -- Specifying Published E-mail Server

Note: When using this method of publishing an e-mail server, as opposed to the prior examples where publishing rules were used, it is necessary to apply the rule to the published server instead of the ISA Server computer (Figure 58). This is because, when using a tri-homed configuration, clients on the external network will connect to the IP address of the published server. Turning on IP routing will allow the ISA Server to pass incoming connection requests to the e-mail server. The IP routing functions are accessed from the packet filter properties page which is located under [array name]/access policy/P packet filters. Connection requests will now flow through and are mediated by the ISA Server, but the IP address of the DMZ computer must be revealed to the external network – in other words, ISA Server does not perform its masquerading function in this scenario as was described in the section *Overview of ISA Server*. To help preclude an intruder from probing this machine for vulnerabilities that are perhaps even unrelated to the mail service, be certain to only allow connection requests that are minimally necessary to this computer – in this case, SMTP and POP.

Summary

In summary, the following recommendations are made in regards to publishing servers behind an ISA server:

- ❑ Do not publish servers without the use of a DMZ.

- ❑ A DMZ architecture utilizing dual firewall products is preferred over a single tri-homed firewall. ISA Server is best suited to front the intranet, but can be used anywhere within the DMZ. Private IP addresses should be used in the DMZ.

- ❑ Firewalls utilized in the DMZ should use the most restrictive set of access rules possible.

- ❑ The firewall adjacent to the internal network should not accept connection requests from the DMZ or external network.

- ❑ When publishing servers that utilize SSL, remember that the user's SSL session is terminated at the ISA Server. It may be prudent to re-encrypt the data before forwarding it to the published server.

- ❑ Unless general access is required, as may be the case if publishing a server for Internet access, access to the published server should be as restrictive as possible.

- ❑ Microsoft recommends that you do not enable directory browsing on the Web server that is published by ISA Server. Also, the published web server cannot require digest or basic authentication. If it does, the internal name or IP address of the Web server may be exposed on the Internet. Reference the ISA Server help file under the topic *web publishing rules*.

- ❑ If publishing a web server it is recommended to modify the error messages with a *R* suffix such that references to the ISA server are removed.

This Page Intentionally Left Blank

Chapter

7

Array and Enterprise Policy

Overview

ISA Server supports the concept of an array of servers. An array is simply a group of ISA servers that are managed as one. When the configuration of one member of the array is modified, all the ISA Server computers in the array are also modified. The feature is provided to support load balancing and to simplify administration.

Protocol rules, packet filters, web publishing rules, and server publishing rules can all be defined at the array level and collectively are known as the *array policy*. As the name implies, the array policy applies to all the ISA Servers in the array but only to the ISA Server computers in that array. During installation one is given the option of adding the ISA server to an array or installing it as a stand-alone server. The appropriate decision is based largely on the size of the network – smaller networks may be able to get by with a standalone server while larger networks would tend to require the use of an array or arrays.

Enterprise policy extends the concept of array policy by allowing the implementation of policies that can be applied to multiple arrays across the network. The enterprise policy includes site and content rules and protocol rules and can be applied to any array. Enterprise policy can also specify if arrays are allowed to publish servers and can force the use of packet filters.

The enterprise administrator has the option of allowing array level policy to further restrict access if necessary. For example, if enterprise policy allows access to a suite of protocols array policy can modify this list by denying access to some (or all) of the protocols. Array policy could not, to continue with this example, allow access that is denied by enterprise policy.

Multiple enterprise policies can be created and applied as appropriate to the arrays within the organization. The decision as to whether or not to use enterprise policies is once again dependent upon the situation – generally speaking, the larger the network the greater the propensity to use enterprise policy.
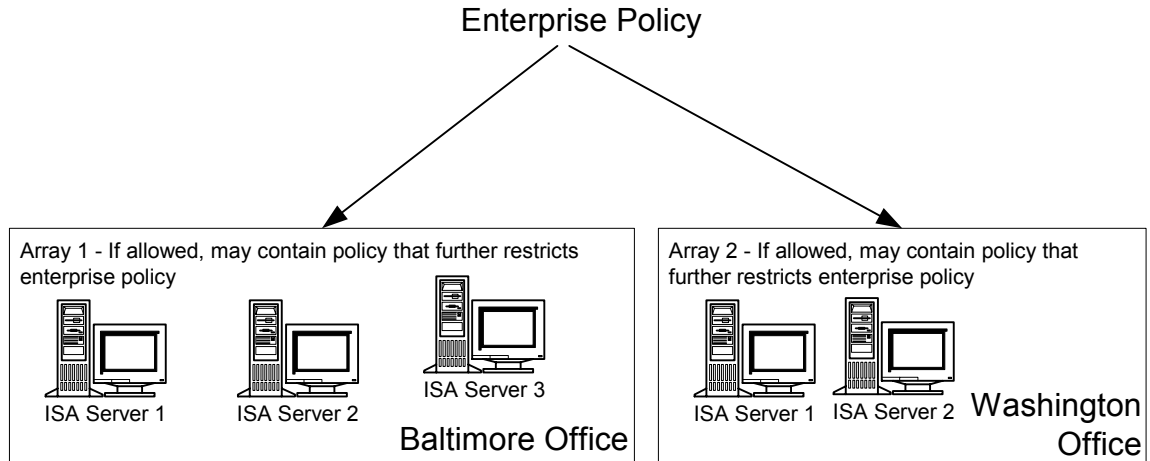
Enterprise Policy

Figure 59 -- Enterprise And Array Policy

Enterprise Policy is set from a variety of locations under the **Enterprise** container within the ISA Management MMC as illustrated below. Note that **Enterprise Policy 1** is displayed and that it has a check mark beside it indicating that it is the default policy.

Site and content rules and protocol rules are set via the containers underneath each enterprise policy as shown in Figure 60. Site and content rules and protocol rules are defined here in the same manner as described in the *Access Control* chapter. Policy elements – schedules, destination sets, client address sets, protocol definitions, and content groups – can also be defined for enterprise policy.

Figure 60 -- Enterprise Policy

Additional enterprise policy elements are accessible via the **set defaults** option under the **Enterprise** container (Figure 61). It is accessible by right clicking the container. Here one can define a number of settings that apply to the arrays within the enterprise. These options including the ability to force arrays to use a specific enterprise policy and whether or not that policy can be further restricted at the array level, whether or not those arrays can create publishing rules, and whether or not packet filtering will be forced.
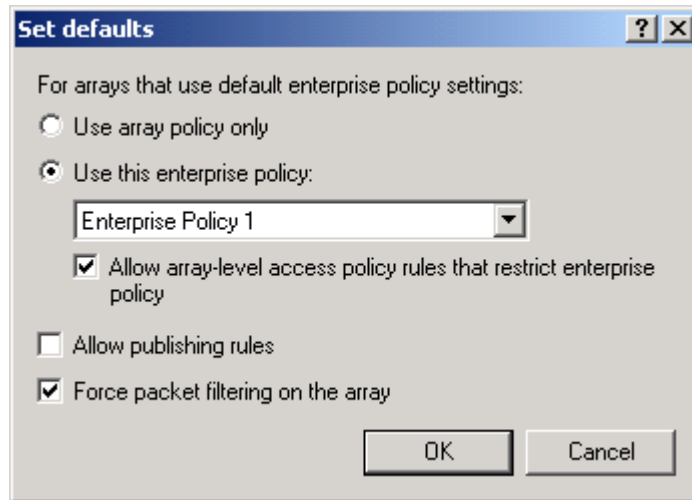
Figure 61 -- Specifying The Use Of Enterprise Or Array Policy

This dialog box is somewhat misleading in that it implies one can change the enterprise policy settings such that only array policy is used. In fact, if one had chosen to use enterprise policy during ISA Server installation one cannot later revert to array policy only. The reverse is also true.

It was also noticed during testing that arrays configured to use the default enterprise policy do not *appear* to pick up the new settings when a different enterprise policy is selected as the default policy. This behavior is noticed when viewing the array policy under the **[array name]/array policy** container. In fact, the policy does change but the new default enterprise policy settings will not display under the access policy container until the MMC is closed and reopened.

Given these inconsistencies, it is prudent to test the array level policy whenever changes are made to enterprise policy to ensure that the intended results were achieved.

Finally, ISA Server supports the use of access control lists (ACLs) to define who can manipulate enterprise and array policy settings. These ACLs are accessible from the **Enterprise** container and the [*array name*] container. The default set of permissions is reasonable. By default, only the *enterprise administrators* group and the *system* account have write access to the Enterprise container. At the array level, domain administrators also have write access. These defaults should be reviewed in light of local policy. As a general rule, write access should be granted to the minimum extent practical.

Specific settings for the use of enterprise and array policy are once again dependent on the security policy of the organization; however, it is generally recommended to force packet filtering and to be very judicious in allowing publishing. When using enterprise

policy it is also generally a good idea to allow those policies to be further restricted at the array level. This will allow local administrators the ability to create additional restrictions based upon local needs – for example, denying access to NNTP for an employee who has abused the privilege.

Summary

In summary, the following recommendations are made in regards to enterprise and array policy:

❑ Consider the use of enterprise and array policy as a means of simplifying and consolidating ISA server administrative actions. This will be particularly useful for larger organizations. The specific content of enterprise and array policy will be based upon the local security policy.

❑ If using enterprise policy, it is recommended to allow the use of more restrictive array policy.

❑ If using enterprise and/or array policy, always test connectivity after creating or modifying policy to ensure the intended effect was implemented.

❑ Set ACLs on the **Enterprise** and **[array name]** containers such that write access is restricted to the maximum extent practical.

Chapter

8

ISA Clients

There are four options for connecting clients on the internal network to the ISA Server – installing ISA firewall client software, use of network address translation clients, using web browsers with a proxy server connection option, and using SOCKS.

Firewall Client

Of these four options, the use of the firewall client software offers users and ISA administrators the most flexibility and capability in homogenous Windows networks. It offers connectivity to the most protocols and, for many of these protocols, it is the only method by which users can be identified and fully authenticated by ISA Server.

The firewall client has the distinct disadvantage of only working in Windows ME, Windows 95, Windows 98, Windows NT 4.0, or Windows 2000 environments. Also, site and content rules for web protocols are tricky to use with the firewall client and are governed by a complex set of rules and exceptions which are detailed in the ISA Server help file under the topic *rules and authentication*. If site and content rules are being utilized to implement a portion of the organization's security policy, it is recommended that the web proxy client be used in addition to the firewall client.

After installing the client, remove any permissions afforded the *everyone* group and replace with the following permissions applied to the installation directory and all subfolders and files:

- Authenticated Users. *Read and Execute* but without the advanced rights to change permissions and take ownership.

- Administrator. *Full Control*.

Finally, under no circumstances should the firewall client be installed on the ISA Server computer – this is an unsupported option that, per Microsoft, will "cause unpredictable results".

Secure NAT Client

Network address translation (NAT or secure NAT as it is frequently referred to in Microsoft's ISA literature) clients do not require any special software installed on the computer. The default gateway is set to the ISA Server computer's IP address or to a router that routes requests to the ISA Server computer. That way all requests to the external network will be forwarded to the ISA Server computer. NAT is simple to configure since no software must be installed on the client computer and, unlike the firewall client, works over a wide range of operating systems.

The disadvantage is that NAT clients are not authenticated; therefore it is not possible to enforce rules on a per-user basis. To continue with an example used repeatedly

throughout this document, assume it was desired to allow access to NNTP to only a particular user. With the secure NAT client this is not possible, however, a protocol rule can be specified such that access is only allowed for a certain IP address. The method for accomplishing this is described under the *Access Control* chapter. As with the firewall client, it is recommended that it be used in conjunction with the web proxy client.

Web Proxy Client

For Web Proxy clients, the Web browser is configured so that its proxy server setting points the ISA Server computer with the proxy server port on the web browser set to 8080 (Figure 62). This is simple to configure and has the advantages of being applicable to a wide range of operating systems. The web proxy client only supports the HTTP, HTTP-S, tunneled FTP, and Gopher protocols, so it should be used in conjunction with the firewall client or secure NAT client if additional protocol support is required.

Like the firewall client, the web proxy client is able to provide authentication information regarding the user which allows the definition of per-user access roles for the supported protocols listed in the preceding paragraph.
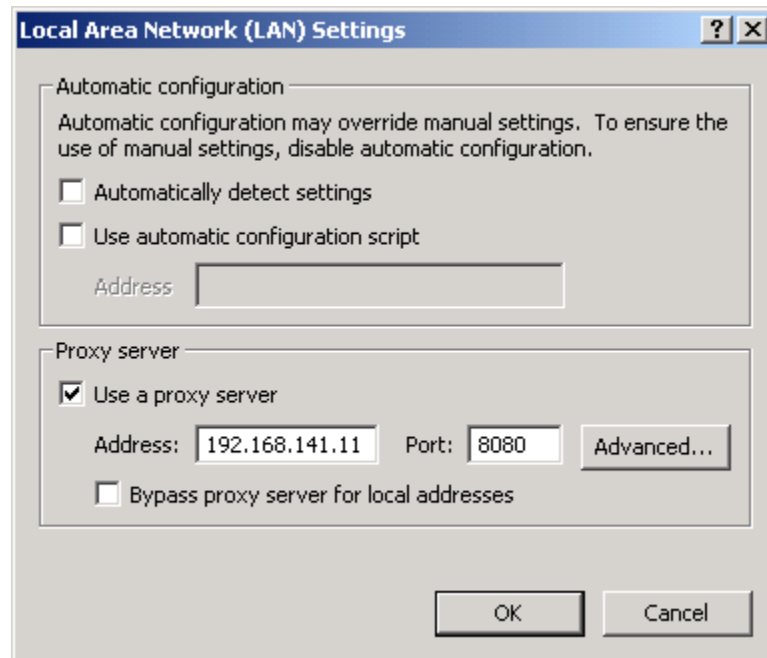
Figure 62 -- Web Proxy Client Settings Within Internet Explorer

The manner in which ISA Server authenticates web proxy client connections is controlled by the **Outgoing Web Requests** tab of the properties page of the **[server name]** container. Integrated windows authentication is generally recommended, but this requires the use of Internet Explorer browsers. In more homogenous networks utilizing a variety of web browsers, digest authentication or basic authentication over a VPN is recommended. In conjunction with this setting, it is also important to enable the **Ask unauthenticated users for identification** option to ensure that connection requests are authenticated.

Socks Client

The primary use of the SOCKS client is for compatibility with Unix applications. There are no specific security concerns associated with its use; however, it is important to realize that SOCKS version 4, the only version supported out-of-the box with ISA Server, does not support the notion of user authentication. Access control under SOCKS can only be accomplished per IP address using client sets.

Summary

The following table summarizes the features available with the four clients.

Feature	Secure NAT Client	Firewall Client	Web Proxy Client	SOCKS Client
Installation required	No	Yes	No, requires Web browser configuration	No, requires application configuration
Operating system support	Any O/S that supports TCP/IP	Only Windows platforms	All platforms, but by way of Web application	All platforms but by way of SOCKS compliant apps
Requires changing network configuration	Yes — default gateway, routers, …	No	No	No
Protocol support	Requires application filters for multi-connection protocols	All Winsock applications	HTTP, HTTP-S, FTP, and Gopher	Any protocol supported by SOCKS compliant applications
User-level authentication	No	Yes – but not recommended for use with HTTP/HTTPS	Yes	No

Table 2 -- Client Summary

In summary, the following recommendations are made in regards to ISA clients:

❑ If client access is required to protocols outside of those supported by web browsers, use the firewall, secure NAT, or SOCKS client. Use of the firewall client is preferred as it allows user level authentication; however, the firewall client only works in Windows environments.

❑ If installing the firewall client, replace the permissions granted to the *everyone* group with the permissions detailed above.

❑ While the firewall client and secure NAT clients are capable of handling web protocols, it is recommended not to rely on them for these applications – use the web proxy client in addition to the firewall or secure NAT client.

This Page Intentionally Left Blank

Chapter

9

Monitoring – Alerts and Logging

Alerts

A wide variety of alerts are available which can provide notification of <u>intrusion detection events</u> and allow the administrator to monitor a host of critical ISA Server functions. These alerts are accessible under the **[array name]/monitoring configuration/alerts** container.

The default condition has all the alarm events enabled except for:

- Cached object discarded

- Event log failure

- IP packet dropped

- IP Protocol violation

- Network configuration changed

- Server publishing is not applicable

These default settings are generally acceptable except that it is recommended to enable **network configuration changed**, and **IP protocol violation**.

There are a number of pre-configured alerts in the alerts container. For each alert, one can specify the number of events required to trigger an alert. This allows one to reduce the number of "nuisance" alerts by setting reasonable thresholds. By right clicking on one of the pre-defined alerts in the alerts container, an events tab can be accessed to specify the number of events required to trigger an alert (Figure 63). The defaults events settings are generally acceptable but should be reviewed – it may be desirable to modify these over time in response to conditions on the network. For example, if one has noticed specific suspicious activity that has triggered an alarm it may be desirable to lower the alarm threshold to provide more immediate notification.
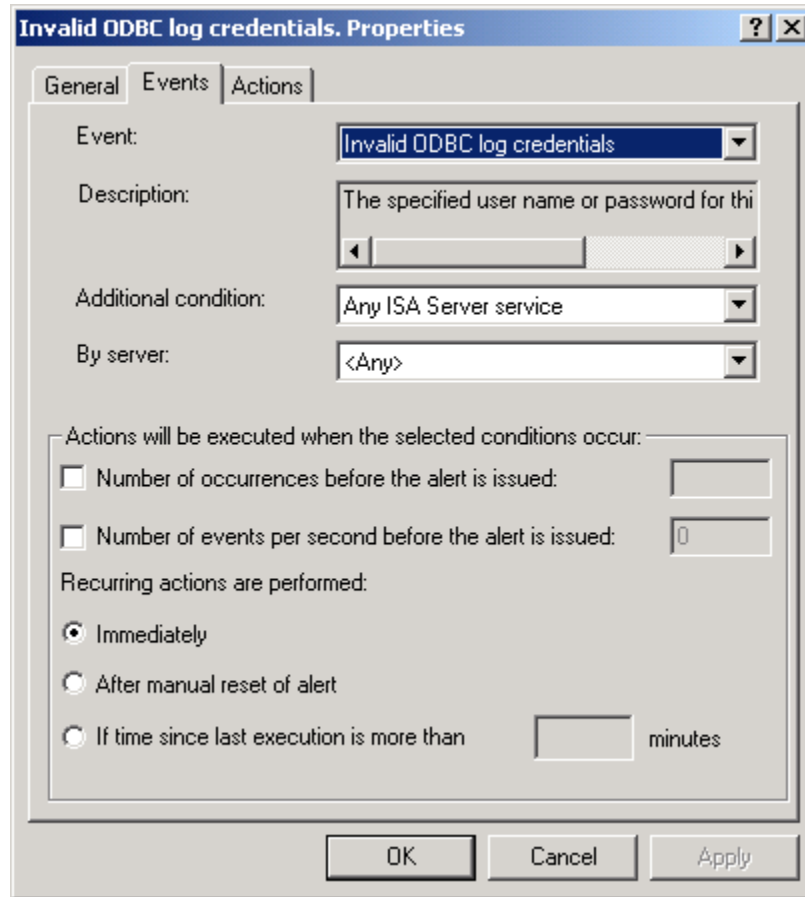
Figure 63 -- Alert *Events* Tab

For each alert the administrator can choose one of five options (Figure 64) which dictate how notification is provided in the event of an alarm trigger:

- E-mail notification

- Execution of a program

- Report to Windows 2000 log

- Stop a selected service

- Start a selected service

No attempt will be made to recommend for each of these alerts the proper alert mechanisms. Generally speaking, the notification mechanism which is most likely to draw the attention of the appropriate administrator should be used (Figure 64). The section ***POP intrusion detection filter*** also provides an illustration of how these settings can be used to provide a more proactive response to an alert.
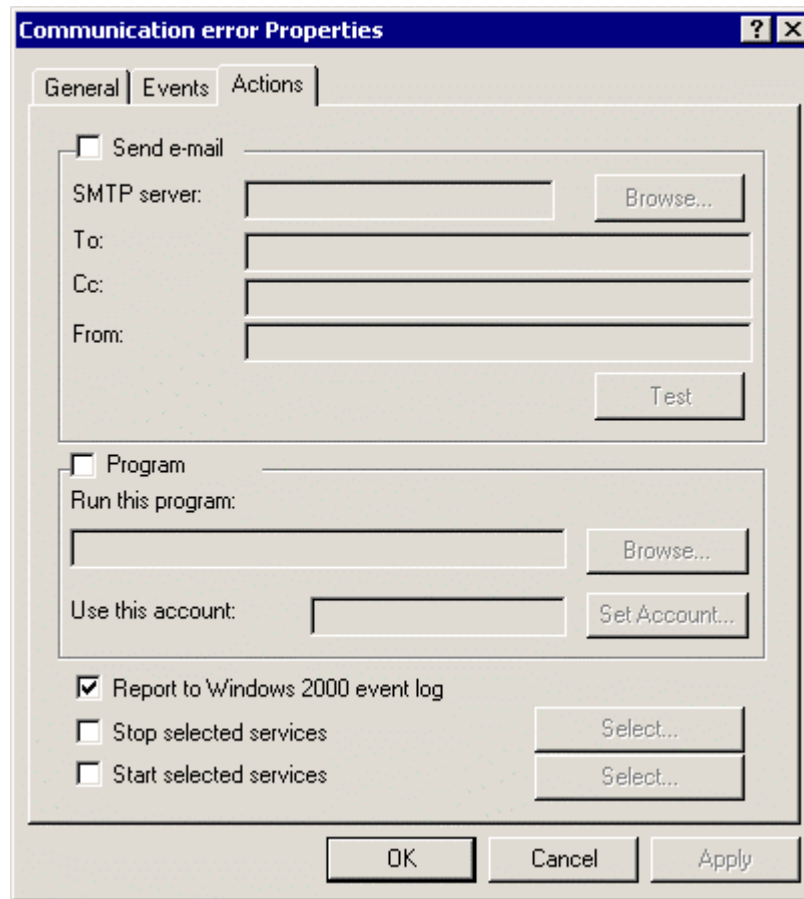
Figure 64 -- Specifying Alert Actions

Logging and Reports

In addition to alerts, ISA Server can log a variety of data regarding connections requests made to the ISA Server. These are configurable under the *monitoring configuration/logs* container. It is recommended to log all available options. Log files can be made to a text file or to a database file. It is recommended to use the database option to help facilitate data analysis. Microsoft provides on the ISA Server CD a series of files containing SQL commands that can used to create tables in SQL Server for the purposes of logging to a database.

ISA Server supports the generation of reports concerning usage, traffic volume, and a host of other data presented in a well formatted and easy to read graphical format. These reports are probably more useful from a maintenance standpoint than a security standpoint, but do offer the ability to quickly determine who has connected to the ISA Server and the sites that have been visited. Reports are configured under the *monitoring configuration* container but viewed under the *monitoring/reports* container.

Current Sessions

ISA Server provides the ability to monitor, and disconnect if necessary, the sessions currently being serviced. These are accessible under the **monitoring/sessions** container. The obvious benefit of this feature is that it provides real-time snapshots and control of who is using the system.

Summary

In summary, the following recommendations are made with regards to monitoring ISA server.

- ❑ Enable most of the alerts as detailed above with notification provided in whichever way is most likely to draw the attention of the appropriate administrator.

- ❑ Log all available options under the **logs** container. Logging to a database is preferable.

- ❑ Enable report generation.

Chapter

10

Other Security Relevant Issues

Backup

No security plan is complete without a robust backup strategy and backing up all ISA Server settings should be covered by that strategy to ensure that a means exists for rapid recovery. An overall backup strategy for the organization is well beyond the scope of this document, however there are a few details that are worth noting when developing such a strategy.

First, it is important to note where ISA Server settings are stored. If ISA Server is set up as an array member, its configuration information is stored in Active Directory. If ISA Server is installed as a stand-alone server, the configuration settings are stored in the server's local registry.

Second, ISA Server provides a method of backing up, and restoring, most array configuration information. In order to understand how the ISA Server backup feature can be used as part of the overall backup strategy, it is important to understand its limitations. Per the ISA Server help file, the ISA Server backup feature backs up all of the array's general configuration information. This includes access policy rules, publishing rules, policy elements, alert configuration, cache configuration, and array properties. Some server-specific configuration information is not backed up. This includes cache content, activity logs, reports, and effective enterprise policy. Other elements of the backup strategy should preserve a copy of these elements. The ISA Server help topic *backing up and restoring an array configuration* is a useful reference.

The ISA Server's backup feature is assessable under both the **enterprise** and **[array name]** containers. Right click and select **back up.** The enterprise and array level backups are independent of one another – in other words, backing up at the enterprise level does not back up additional settings entered at the array level and vice versa.

Summary

❑ Ensure that the organization's backup policy protects ISA Server settings.

Appendix

A

References

Galloni, Raymond, (1998), *Microsoft Proxy Server 2.0 Security Assessment*

Goldberg, David S.; Labonte, Susan J.; Schmidt, Charles M., *Security Assessment of the Microsoft Proxy Server Version 2.0*

Microsoft Product Documentation/Help file – *Microsoft ISA Server 2000 Enterprise Edition*

Shinder, Dr. Thomas W and Shinder, Debra LittleJohn. Configuring ISA Server 2000. ISBN 1-928994-29-6.

Weirer, Jeff; Mosmeyer, Daniel; (1999) *Tips from the Proxy Server Gurus – Configuring & Troubleshooting Services and Applications to Work with MS Proxy Server 2.0 FAQ.* Available via HTTP from HTTP://proxyfaq.networkgods.com

Change Summary

Version 1.1. Added information related to a security patch. Added details concerning when an organization might use the SMTP TURN command.

Version 1.2. Modified the recommended permissions for the firewall client installation directory.

Version 1.21. Modified the e-mail address on the cover page.

Version 1.3. Changed the recommendation to enter IP addresses (as opposed to URLs) where possible when creating site and content rules. This change was made after testing confirmed that ISA Server will do reverse lookups in enforcing site rules.

Version 1.4. Made the following changes or additions:

- Added an additional point on why a tri-homed ISA Server is not the preferred DMZ solution.

- Added a recommendation that the HTTP redirector option to reject HTTP requests from Firewall and secure NAT clients should be enabled if the web proxy client is utilized as recommended.

- For the sake of greater clarity, modified several graphics to reflect the use of private IP addresses within the DMZ as was recommended in the text.

- Updated the document to reflect successful implementation of the message screener – added recommendations for its use along with notice of a known bug.

- Repaginated portions of the document so that in more cases graphics appear on the same page as the associated text.

- Incorporated a few readability changes based upon comments received from the Mitre Corporation.

- Updated the list of applicable service packs/patches/hot fixes.

- Updated Figure 6.

Version 1.41.

- Deleted references to specific patches – the reader is pointed instead to the Microsoft security home page for the very latest patch information.

- Expanded the list of file attachments that one might want to consider filtering.

- Add a caution related to enabling IP fragment filtering.

- Added a recommendation to edit the default error messages when publishing a web server.

Version 1.42

- Clarified that only SOCKS version 4 is supported out-of-the-box by ISA Server

Version 1.5

- Added additional recommendations for eliminating unnecessary services.

- Added a reference to the NSA guide entitled *Microsoft Office 2000 Executable Content Security Risks and Countermeasures*

- Updated the SMTP filter [attachment tab](#) section to remove an illustration of a problem that was noted with early releases of ISA Server. The problem was not reproducible in the current release.