GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Microsoft ISA Server 2004 Beta 2

A Guide to Installation and Web Publishing

Jeff Jirka
GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b, Option 1
March 28, 2004

Introduction

ISA Server 2004 is Microsoft's latest version of their Internet Security and Acceleration Server product. The current release is Beta 2. ISA Server combines a firewall (security) with a caching server (acceleration).

This product is a significant upgrade of its predecessor, ISA Server 2000, and contains many new features such as:

- Extensive protocol support
- Multiple network configuration
- Unique per-network policies
- Routed and NAT network relationships
- Stateful inspection for VPN
- Export and import [of configurations]
- Delegated permissions wizard for firewall administrator roles (What's New in ISA Server 2004)

This paper will provide the reader with step-by-step installation instructions, a tour of the management interface and an example of configuring ISA Server for web publishing. Discussion of the other features of ISA Server is beyond the scope of this document.

Network Configuration

For the purposes of this paper, the subject ISA server (ISA1) will be implemented using a three-legged configuration. The server will be comprised of one external, one perimeter and one internal network interface, as shown below. The web server (WEB1) will be used when discussing web publishing later in this paper.

Installation Requirements

The minimum hardware and software requirements for installing ISA Server 2004 are:

- Computer with 300MHz or faster CPU
- 256MB of RAM
- Two network adapters
- 150MB of available disk space formatted as NTFS; additional space is necessary if enabling web caching functionality
- Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows Server 2003 Standard or Enterprise Edition

Note: If installing ISA Server on a Windows 2000 operating system service pack 4 or higher, Internet Explorer 6 or later must be installed. In addition the hotfix described in Microsoft article Q821887 must be applied.

Pre-Installation Tasks

Obtain the ISA Server 2004 Beta 2 code. The software can be downloaded from Microsoft at http://www.microsoft.com/isaserver/beta/privacy.asp. In addition, a CD is available for the cost of shipping plus applicable sales taxes and can be ordered at http://microsoft.order-9.com/isabeta.

Install and configure either Windows 2000 or 2003 Server, then configure the internal, perimeter and internal network IP settings. To keep the three network interfaces straight during installation and testing, consider renaming them in the Network and Dial-up Connections applet of Control Panel as shown below.

Verify each of the network interfaces are working properly by pinging another host on each of the three connected networks.

Double click the External Network and then click properties. Disable *Client for Microsoft Networks* and *File and Print Sharing for Microsoft Networks* on the external interface.
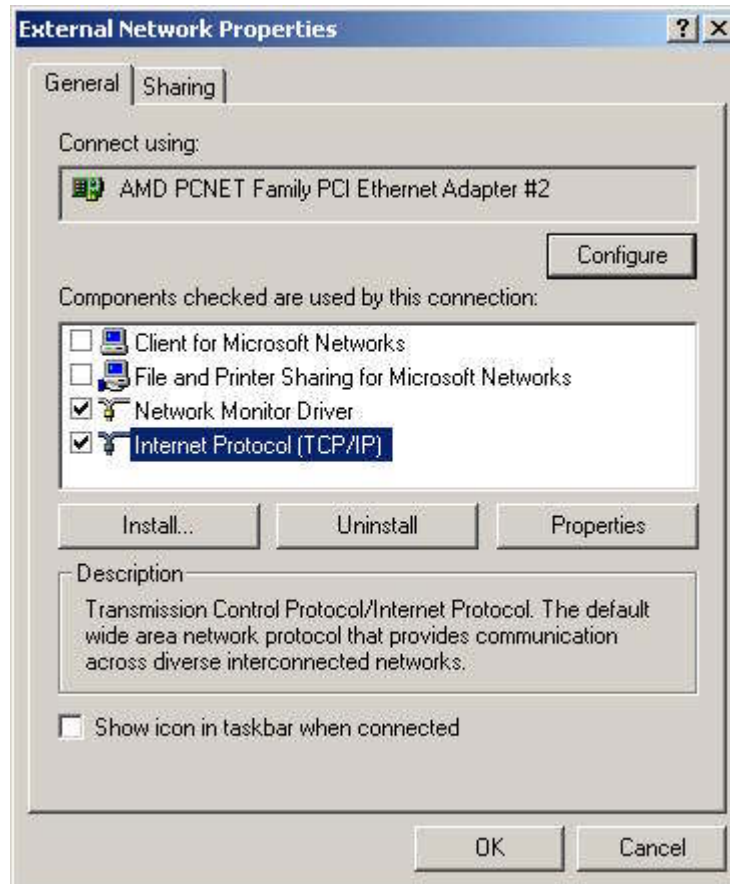
If you are skilled at protocol analysis, load the Microsoft Network Monitor component (if available as part of the operating system) on your test system for validating client to ISA communications. Installation can be done through the Add or Remove Programs applet of Control Panel and then selecting Add/Remove Windows Components. Network Monitor is one of the options listed under Network and Monitoring Tools.
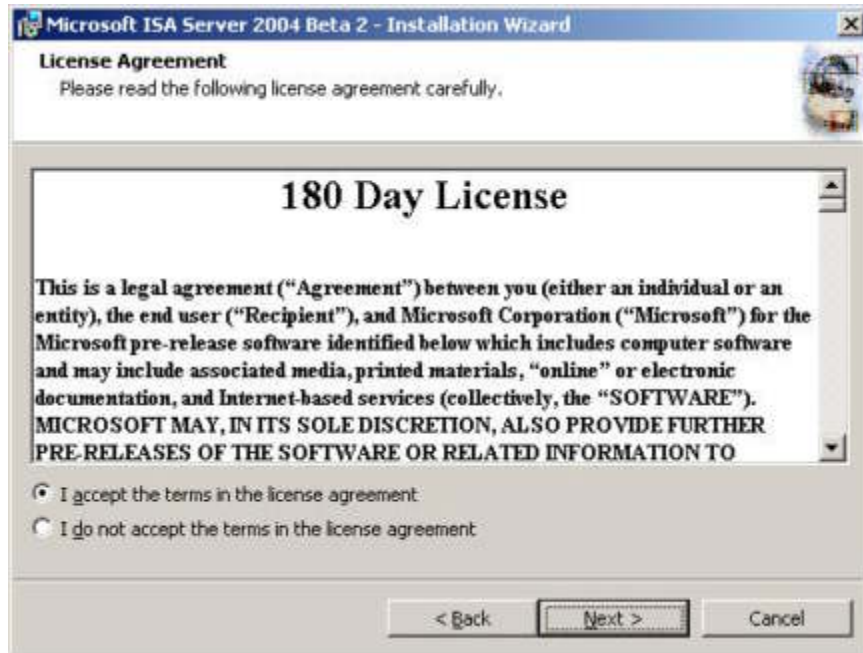
Installation

Insert the ISA Server 2004 Beta 2 CD into the CD drive and wait for the installation program to begin. If your system is not configured for auto run or you opted to download and unzip the contents of the CD, open Windows Explorer, locate isaautorun.exe and double-click the file to begin the installation.

Click on Install ISA Server 2004.

Click Next.

After reading the licensing agreement, select "I accept the terms in the license agreement" and click Next. If you choose not to accept the licensing agreement, you will be unable to continue with these instructions.
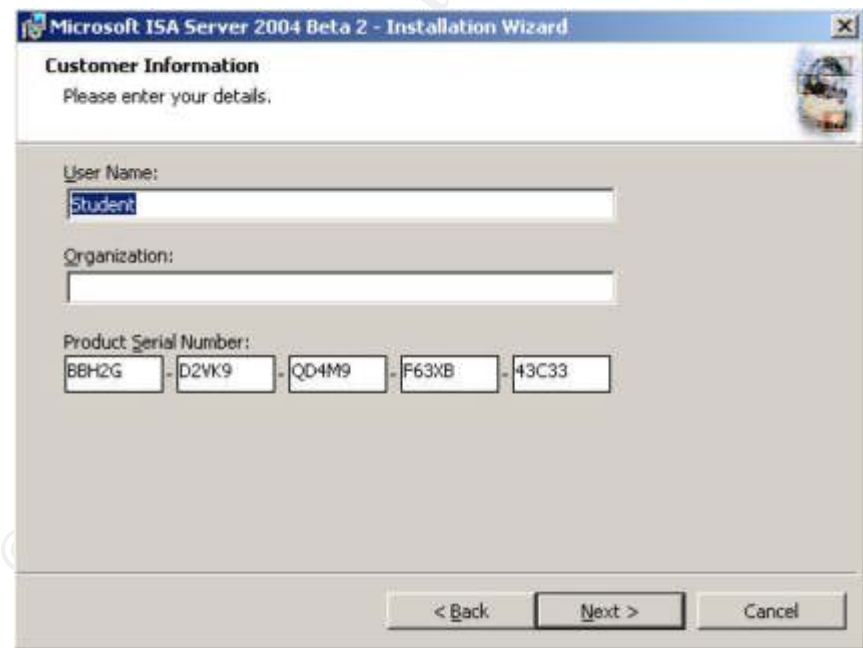
Complete the User Name and Organization fields as necessary and click Next. Note that the product serial number field is pre-populated with a valid serial number.

The table below shows the default features installed depending on the selected installation option.

Program Feature	Typical	Complete	Custom
Firewall Services	X	X	X
ISA Server Management	X	X	X
Firewall Client Installation Share	X	X	X
Message Screener NOTE: To install Message Screener, an SMTP virtual server must be pre-installed on this server.		X	

Note the directory where the application will be installed. For purposes of this paper select Custom and click Next.
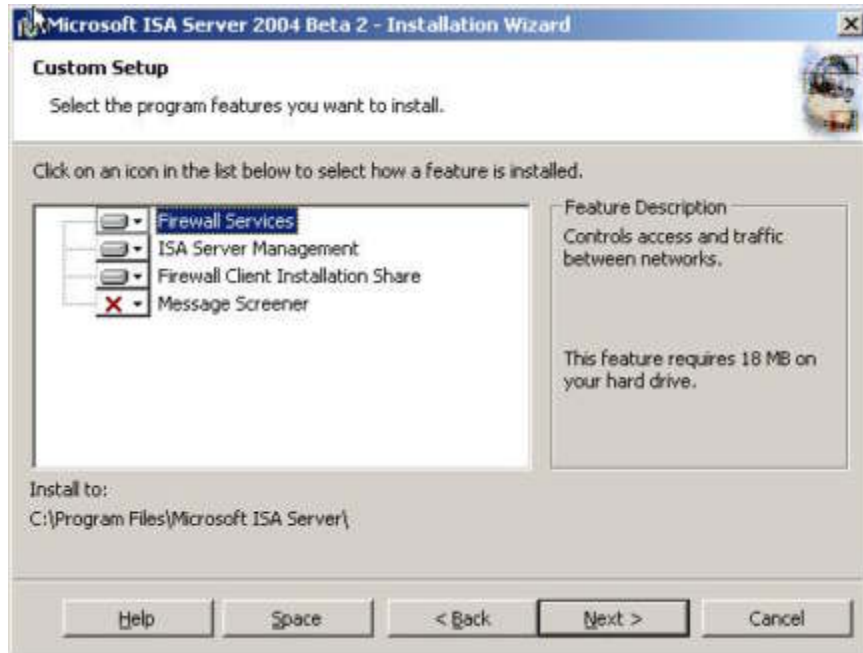
The table below lists the program features and descriptions for each of the items available for installation. These descriptions can also be found on the Setup screen as shown above.

Program Feature	Description
Firewall Services	Controls access and traffic between networks
ISA Server Management	Provides the management interface for configuring ISA Server 2004
Firewall Client Installation Share	Creates a \\servername\mspclnt network share as a firewall client installation point
Message Screener	Allows content filtering of incoming SMTP messages as they arrive at the ISA Server

After reviewing the selections click Next.
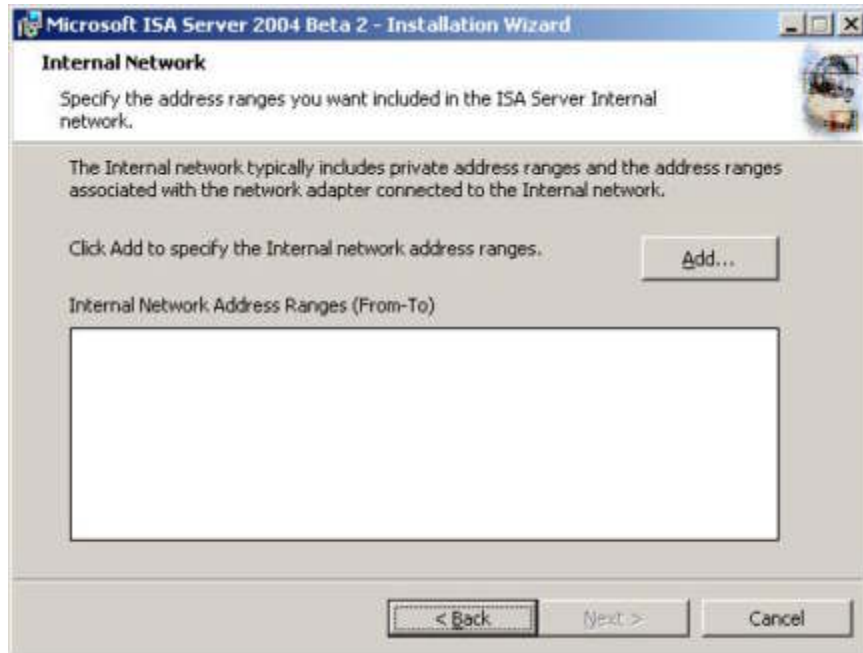
To configure the internal network IP ranges click Add.
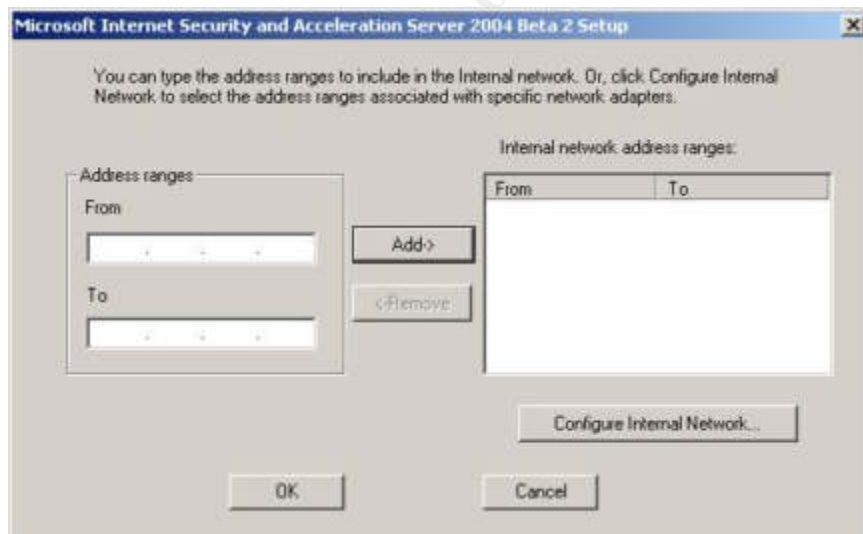
There are three ways to specify the internal network address ranges:

1. Manually type in the address ranges
2. Click Configure Internal Network and select the network
3. Use a combination of the above methods

To familiarize the reader with option 2, click Configure Internal Network.
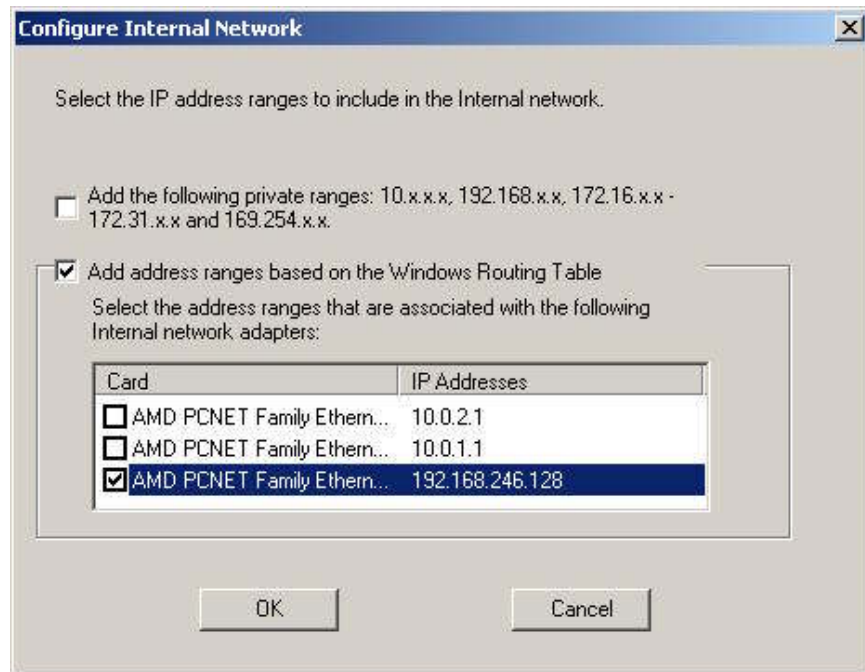
The first check box is used to easily assign the special-use IPv4 addresses to the internal network address ranges.

The address ranges 10.x.x.x, 172.16.x.x – 172.31.x.x, 192.168.x.x and 169.254.x.x are detailed in RFC 3330. The first three ranges have been set aside by the Internet Assigned Numbers Authority (IANA) for private use. The last range is used by hosts on a single network. "Hosts obtain these addresses [169.254.x.x] by auto-configuration, such as when a DHCP server may not be found." (IANA) If one or more of your network cards was configured to use DHCP and it was unable to locate a DHCP server, it will assign itself a 169.254.x.x address.

The second check box is used in conjunction with the remaining Card check boxes – one for each defined network interface card – to quickly select address ranges based on the Windows routing table.
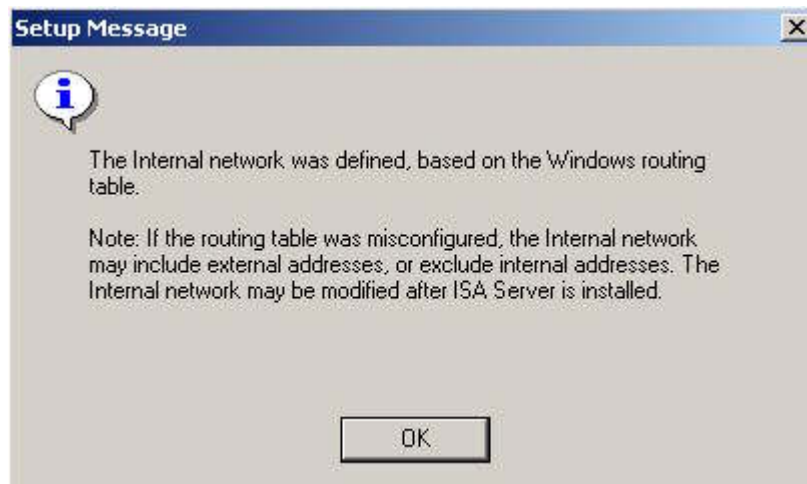
It is very important to properly identify the internal network address ranges. If they are not properly configured, firewall policies may allow unwanted traffic to pass through the ISA server to the internal network.
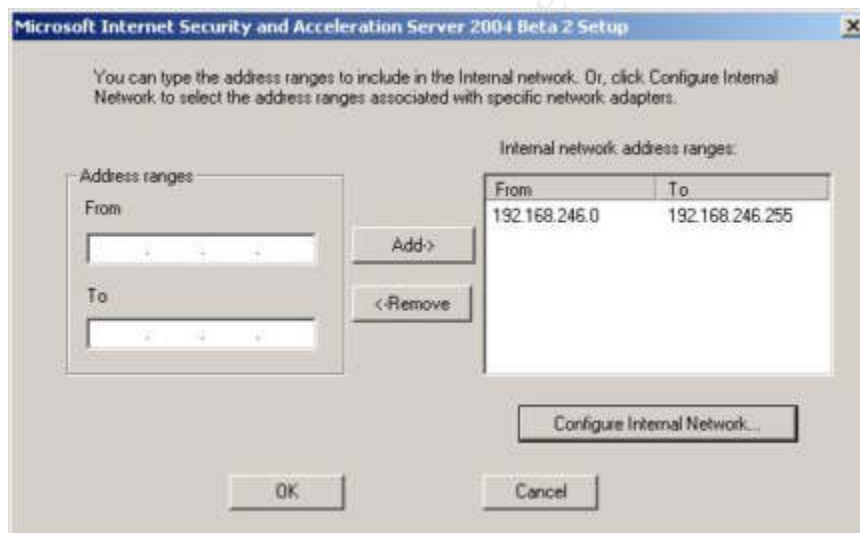
Once all the internal networks have been defined, click OK.
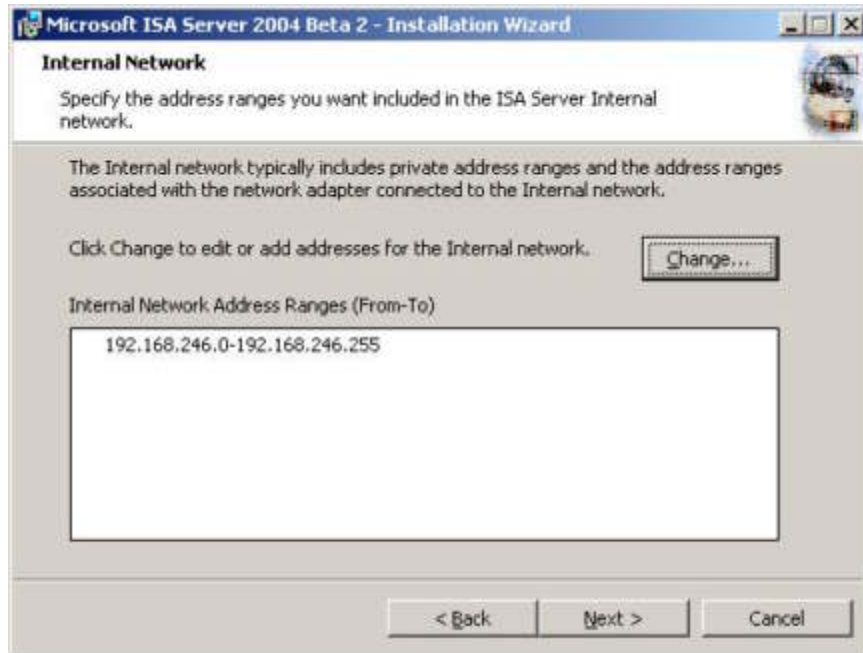
The installation process allows you one more chance to review and update the internal network ranges. This is one indication that properly configuring the internal networks is important. When satisfied the ranges are complete and correct, click Next.
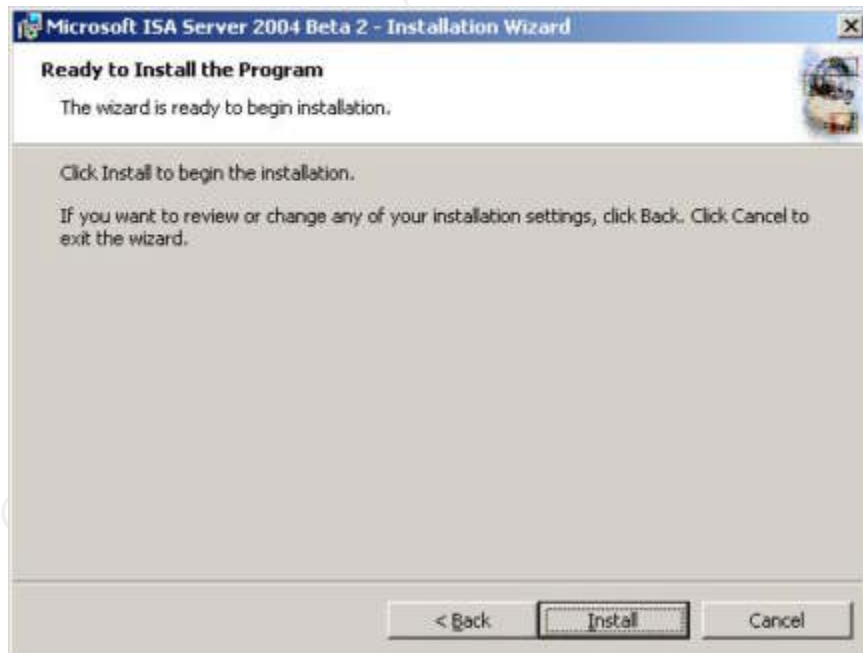
Note the option to go back to any screen up to and including the opening installation screen to review or change your selections. When satisfied with your selections, click Install.

The installation program copies files, installs components and initializes the system.
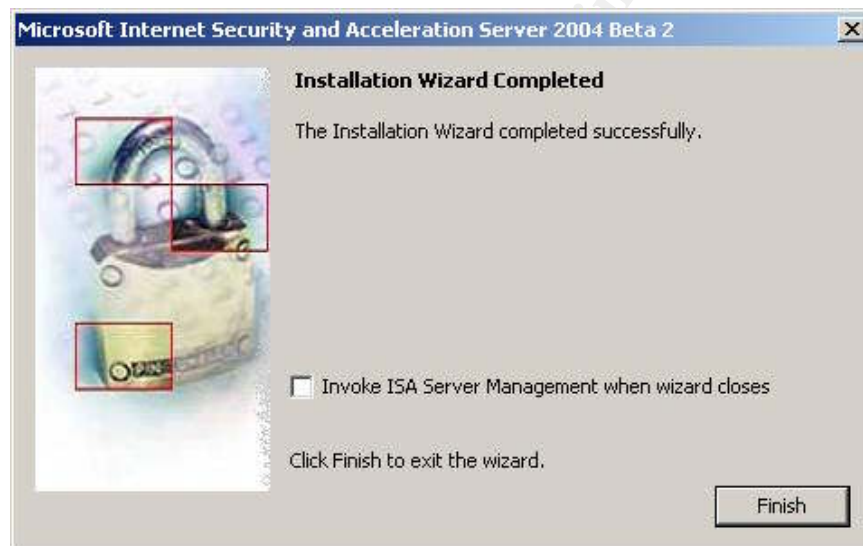
Once the installation has completed, click Finish.

A check of services reveals the six new services installed for ISA Server 2004. The Microsoft Desktop Engine (MSDE) is installed for use in logging events.

In addition to the services, one new program group and two new applications are installed. Selecting ISA Server Performance Monitor brings up Performance Monitor with 21 pre-loaded and running ISA specific counters. The performance monitor file is msisaprf.msc.

ISA Server 2004 Tour
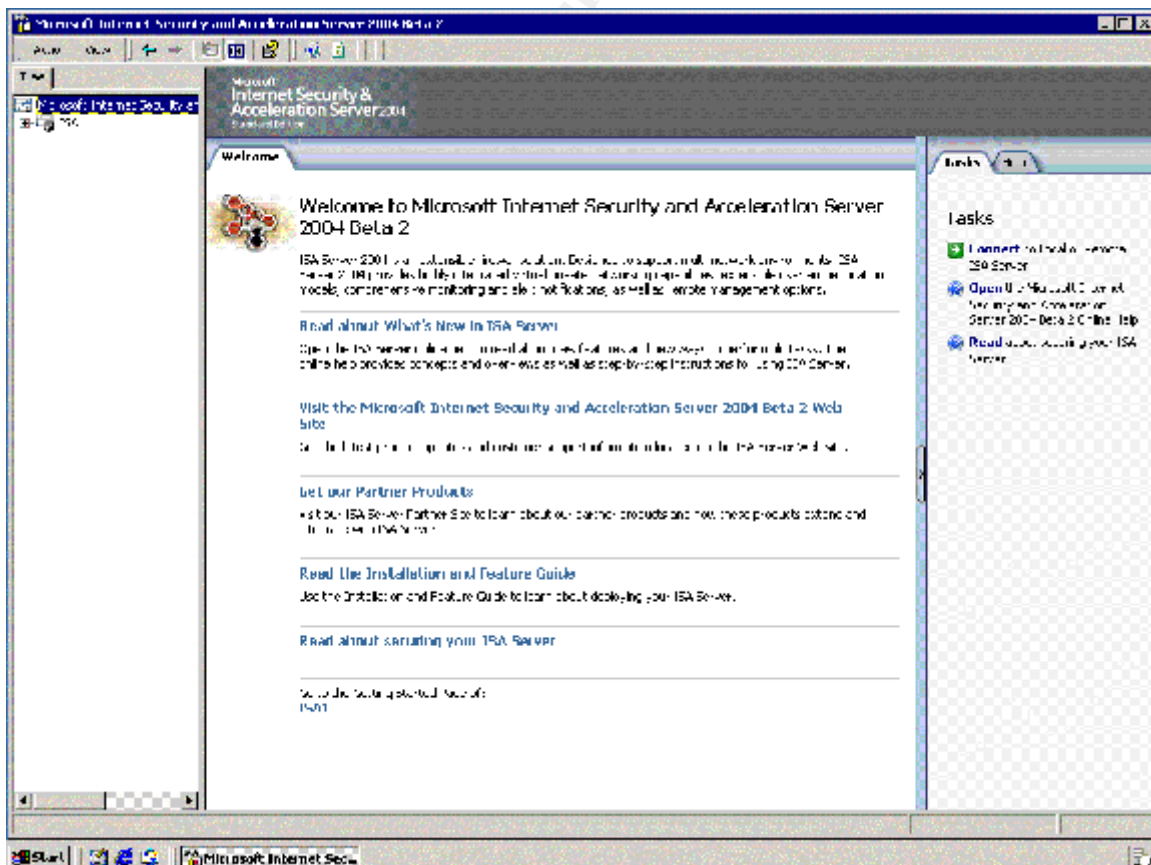
Selecting ISA Server Management from the program menu starts the management user interface (UI) and defaults to the Welcome page. Before configuring the ISA Server for web publishing we'll take a quick look at the different screens of the UI.

Expand ISA1 in the left hand pane and then Configuration to show the entire list. Select Monitoring from the left hand list.
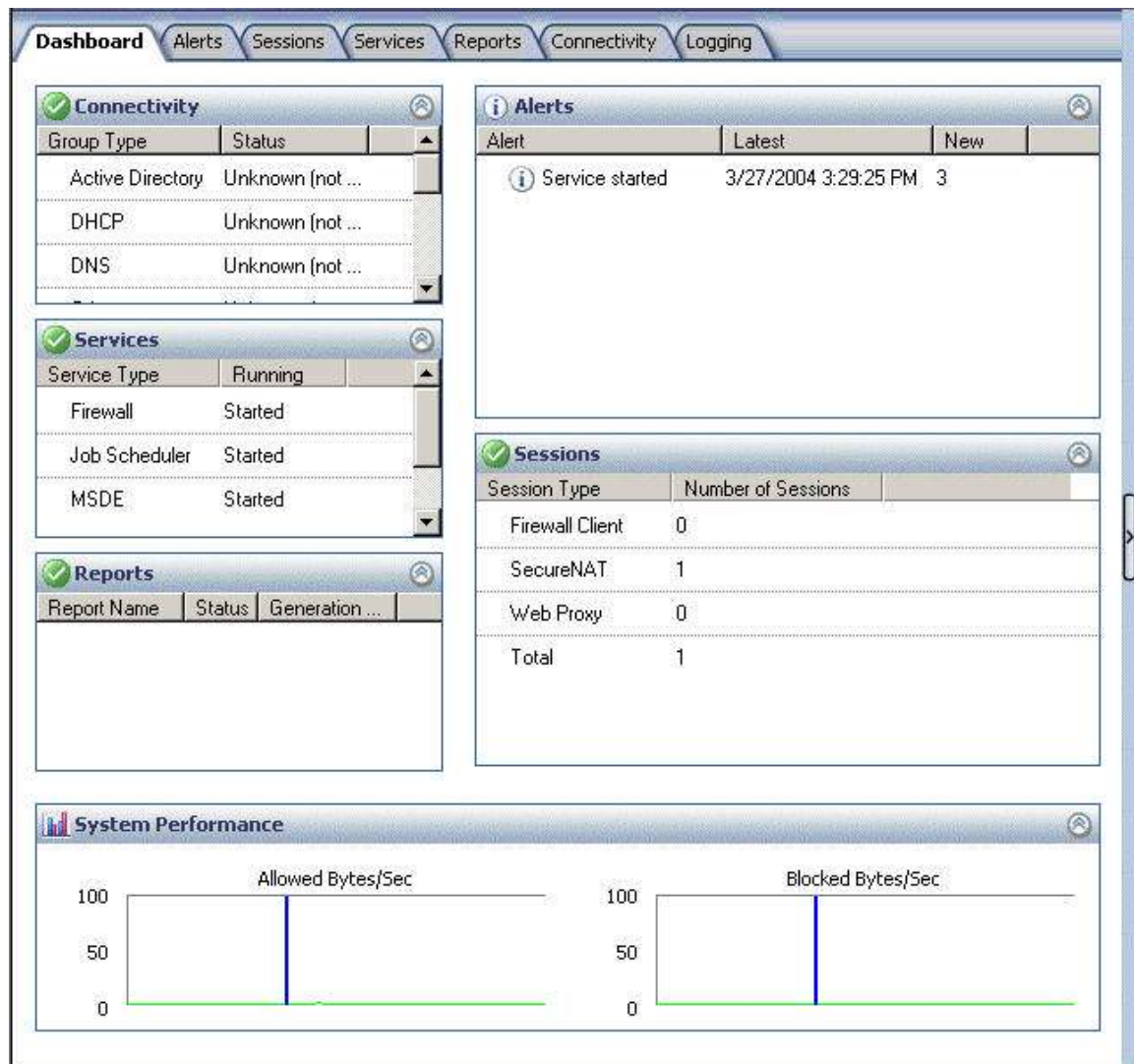
This brings up the "quick view" dashboard. For the purpose of this tour only captured the portion of the screen that will be discussed. The left hand list and right hand task pad and help sections have been removed from these graphics.

The dashboard provides a health-at-a-glance look at the current state of the ISA server.

There are a myriad of pre-defined alerts in ISA Server. In addition, the administrator has the ability to build new alert definitions. Each alert can then be configured to trigger actions such as sending email notifications, running a program, writing an event to the Windows event log and stopping and starting services.

The sessions tab lists all of the current active sessions on the ISA server. In the default configuration, sessions list the activation time, session type, client IP, source network, username and hostname. This view, as are most of the views within ISA Server, is fully customizable.

Services provides an interface to control the state (running or stopped) of the firewall, data engine and job scheduler services. Stopping the Microsoft Data Engine also stops the Firewall service, no doubt for security reasons. Controlling the Microsoft ISA Server Control, Microsoft ISA Server Storage and MSSQLServerADHelper services must be done through the Services program of the operating system.

The Reports tab (using the right hand task pane) is used to schedule and manage reports.

Connectivity allows the administrator to configure connectivity "tests" and thresholds for monitoring the availability and performance (response time) of specific systems. If the response does not meet the configured criteria an alert can be triggered.

Logging provides a real-time view to the traffic attempting to pass through the ISA server. As traffic is allowed or blocked it is logged along with the most pertinent information such as source and destination networks, ports and IP addresses, the ISA rule that was triggered and in the case of web servers, the method (GET, HEAD, POST…) and URL.
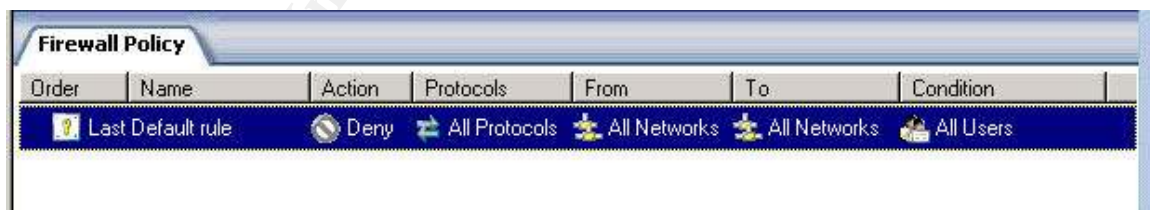
The next item in the left hand pane is Firewall Policy. A fresh installation of ISA appears to Deny all protocols from all networks to all other networks for all users however there are 26 System Policy Rules that are in effect. To view these rules right click Firewall Policy in the left hand pane, select View, then Show System Rules. Keep this in mind when configuring ISA server and reviewing logging. These rules, if there is a concern they may compromise security, can be disabled using the System Policy Editor. Keep in mind a loss of functionality or

connectivity may occur if you inadvertently disable the wrong rule. A partial view of the System Policy Rules is shown below.

Order	Name	Action	Protocols	From	To	Condition
? 7	Allow DNS from local hos...	Allow	DNS	Local Host	All Networks	All Users
? 8	Allow DHCP request from...	Allow	DHCP(requ...	Local Host	Anywhere	All Users
? 9	Allow DHCP reply to fire...	Allow	DHCP(reply)	Anywhere	Local Host	All Users
? 10	Allow ICMP(PING) from tr...	Allow	Ping	Internal	Local Host	All Users
? 11	Allow ICMP from firewall t...	Allow	ICMP Infor... ICMP Time... Ping	Local Host	All Networks	All Users
12	Allow VPN clients to fire...	Allow	PPTP	External	Local Host	All Users
13	Allow VPN site-to-site to f...	Allow		External IPSec Rem...	Local Host	All Users
14	Allow VPN site-to-site fro...	Allow		Local Host	External IPSec Remote Gate...	All Users
? 15	Allow Microsoft CIFS prot...	Allow	Microsoft Cl... Microsoft Cl...	Local Host	Internal	All Users
? 16	Allow Remote logging usi...	Allow	Microsoft S... Microsoft S...	Local Host	Internal	All Users

According to Shinder (2004), "System Policy Rules that are disabled by default have a tiny down-pointing red arrow in their lower right corner. The disabled System Policy Rules will become automatically enabled when you make configuration changes to the ISA Server 2004 firewall, such as when you enable VPN access."

Next on the list is Virtual Private Networks (VPN). As the configuration of VPNs is a bit more complex than configuring firewall rules, ISA Server 2004 attempts to provide a step-by-step guide. However, step one, two (Specify Windows Users) and three all end up in the VPN Client Properties dialog box either on the General tab (step one and three) or the Protocols tab (step two). The RADIUS Server link on step two takes you to the RADIUS tab of the Virtual Private Networks (VPN) Properties dialog box. Step four and five take you to the Firewall Policy and Networks screens respectively.
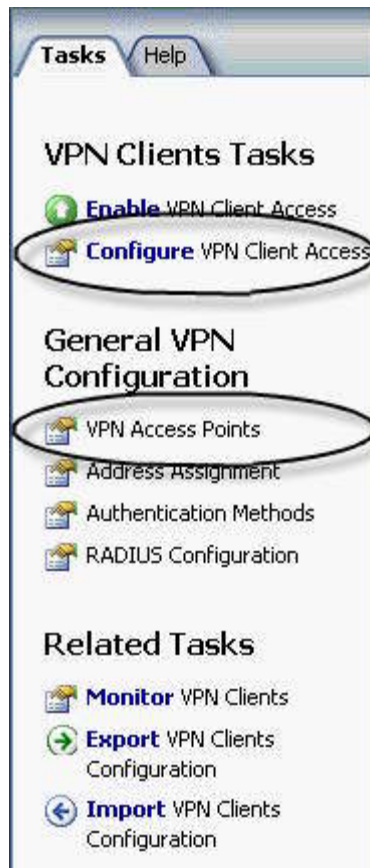
When configuring a VPN it may be easier using the right hand pane task pad. Selecting Configure VPN Client Access and VPN Access Points, and then clicking through all of the tabs that appear in these two tasks will accomplish steps one through three.

VPN setup is completed by configuring remote sites, firewall policies and network rules.

This may sound a bit confusing but after clicking through the options for VPN configuration and reviewing each of the associated tabs it should become clear.
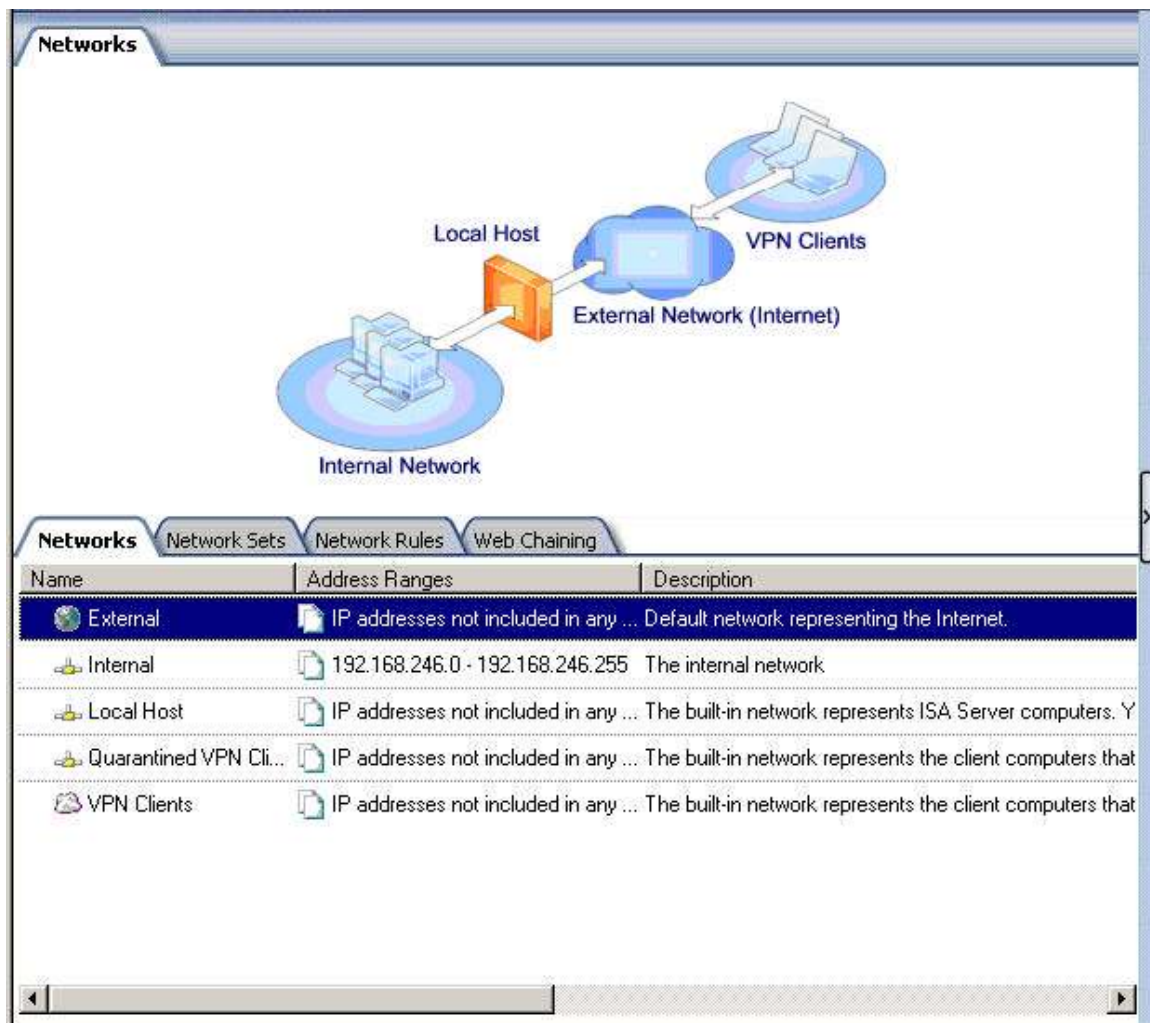
Moving down the list, select Networks. The first screen shows a graphical representation of the "network template" that is configured. On the right hand pane are templates for five different configurations:

- Edge Firewall (default)
- 3-Leg Perimeter
- Front
- Back
- Single Network Adapter
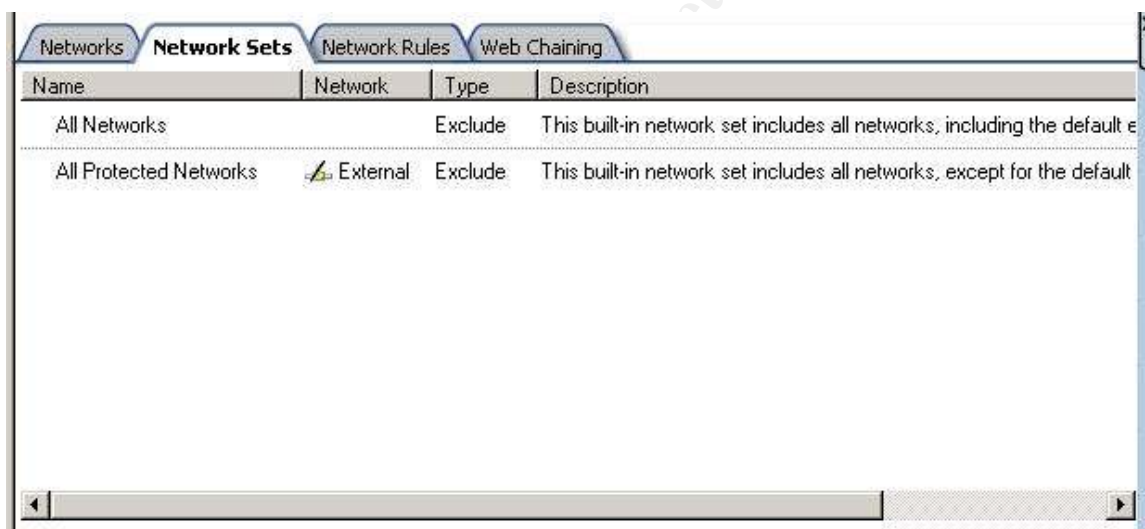
The edge firewall is also known as a bastion host. According to searchSecurity.com, a bastion host is defined as "the only host computer that a company allows to be addressed directly from the public network and that is designed to screen the rest of its network from security exposure."

A 3-leg perimeter configuration provides an extra layer of security between the external and internal networks. Published servers such as web or mail servers reside on a perimeter network. Traffic destined for those servers is allowed

between the external and perimeter networks with typically very minimal or no traffic allowed to pass from the external or perimeter networks and the internal network. In this configuration, ISA Server 2004 is simulating a dual firewall DMZ.

A true dual firewall DMZ can be setup using two ISA servers, one acting as a front firewall and the other, a back firewall. This is the most secure of the configurations as an attacker would need to compromise two firewalls to gain access to the internal network. Some companies use different vendor's firewall products for the front and back firewalls since an attacker that can compromise the first ISA server may be able to easily compromise the second.

The single network adapter firewall, according to the description given with the network template, is used inside a perimeter or corporate network. In this configuration it cannot be used as an edge firewall, 3-leg, front or back firewall as these all require multiple network adapters. In addition this configuration "will not support: IP-level and transport level packet filtering, VPN, server publishing and Firewall clients." (ISA Server 2004 Beta 2 Network Template Description)

Network Sets allow you to define a group of networks for use in firewall policy rules. For example, the "All Protected Networks" set combines the Internal, Local Host, Quarantined VPN Clients and VPN Clients networks into one set. The only network it excludes is the External network. When you define a set, you select whether the networks are included or excluded from the set. Once built however, you need to pay attention when editing the list of networks contained in the set. If it is an include set, the checked networks are contained in the set. If it is an exclude set, the checked networks are excluded from the set. Examples of include and exclude network sets are shown on the next page.
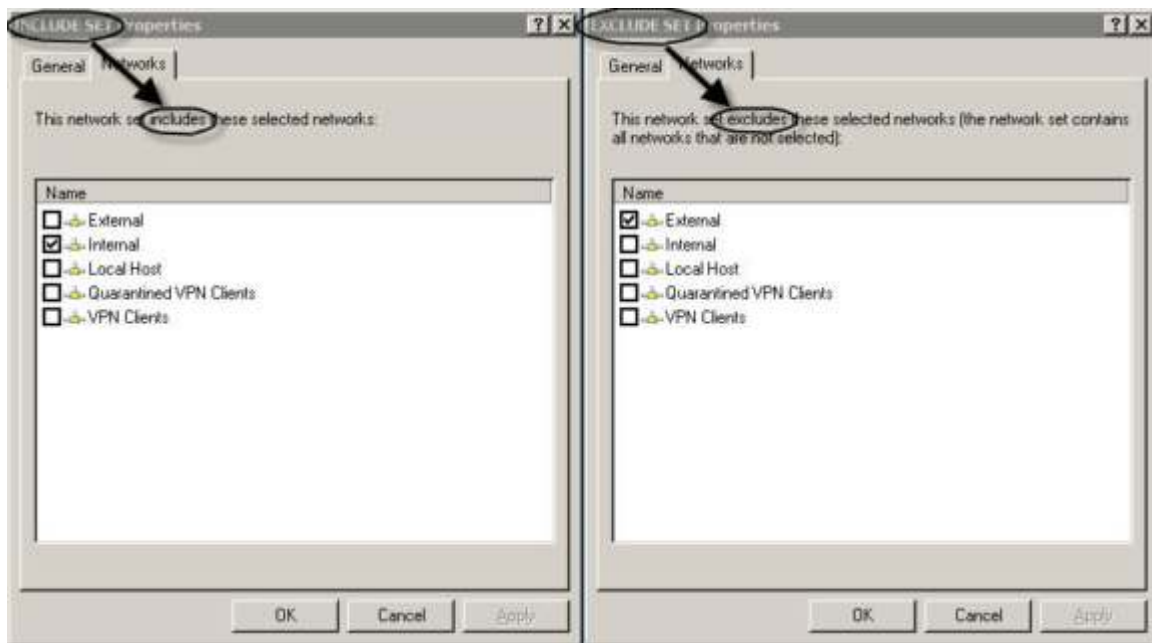
The next tab is Network Rules.

Network rules are used to define which networks are allowed to communicate with each other and how they will communicate. The communication methods (listed as Relation on the configuration screen) that can be used are routing and NAT. "Routed networks are bidirectional. That is, if a routed relationship is defined from network A to network B, a routed relationship also exists from network B to network A. Conversely, NAT relationships are unique and unidirectional. If a NAT relationship is defined from network A to network B, no network relationship can be defined from B to A." (Installation and Feature Guide)

Networks	Network Sets	Network Rules	**Web Chaining**			
Order	Name		To		Condition	
	Last Default rule		All Networks		Retrieve the request directly	
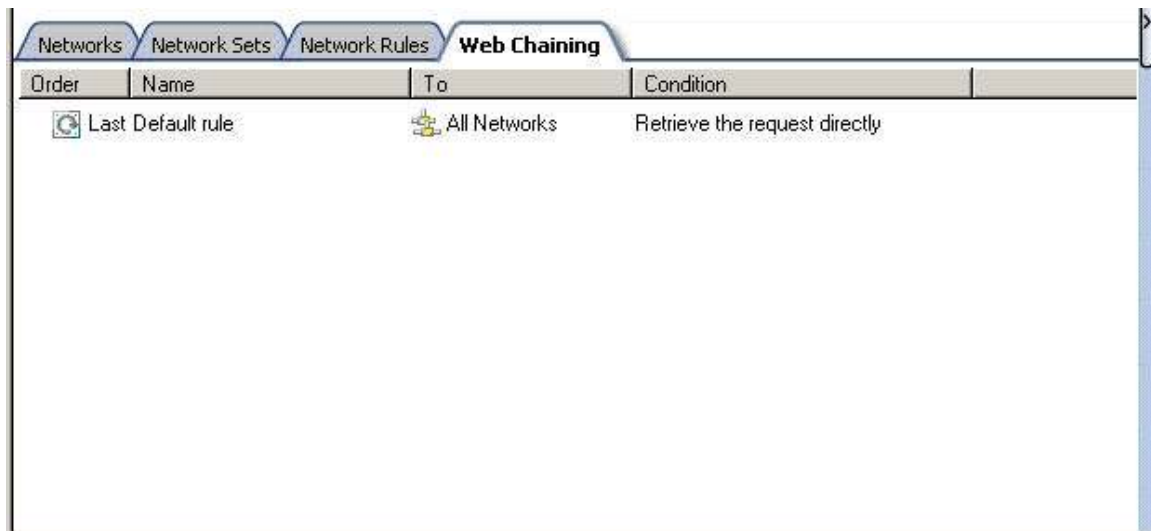
The last tab in this section is web chaining. Chaining of ISA servers is used primarily to bring cached content closer to users. Consider a branch office in Chicago, connected to their headquarters in New York. The company has one connection to the Internet and that connection is in New York. A user in Chicago requests a page from http://isaserver.org. An ISA server in Chicago receives the request from the client and passes it up the chain to an ISA server in New York. This server processes the request based on firewall policy rules. If the request is allowed, it sends the request to isaserver.org and caches the results before sending them to the ISA server in Chicago. The ISA server in Chicago receives the results, caches the page and sends the results to the client. Using this hierarchical method of caching, subsequent requests from clients in Chicago are processed by their local ISA server.

Cache Drives	Cache Rules	Content Download Jobs		
Server		Cache Size ...	Disk Size ...	Free space on NTFS drives (MB)
ISA1		100	4086	2458
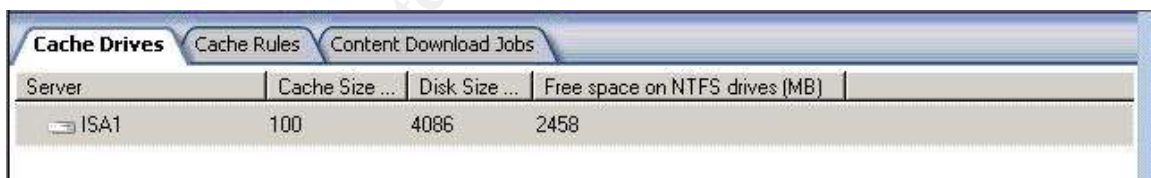
The nest item listed in the left hand pane is Cache. Caching is used to improve performance and reduce bandwidth utilization. ISA server is capable of providing both forward and reverse caching. Forward caching is used for internal clients requesting pages from the Internet. Reverse caching is used when publishing a web server that provides content to Internet users.

The first tab, Cache Drives, is used to configure the size and location of the ISA cache.

The next tab is used to configure Cache Rules. These rules provide the administrator with a very robust set of caching criteria. Some of the criteria are:

- How content in cache is retrieved
- How content should be stored in cache
- What types of content are cached
- Size limit of objects stored in cache
- Should SSL responses be cached
- Time-to-Live (TTL) parameters for HTTP and FTP objects

Content Download Jobs allow an administrator to configure and pre-fetch Internet content based on a defined schedule. For example, every morning at 8:00 am your Chicago office personnel need to pull data from selected news agency sites all over the world. With scheduled content download jobs, all of the data that they require can be automatically pulled at 2:00 am and stored on the local ISA server.

Add-ins are application and web filters that extend the functionality of ISA Server. According to the definitions found in ISA Server Help, application filters "intercept, analyze, or modify any data stream" while web filters are used for "viewing, analyzing, blocking, redirecting, or modifying Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP) traffic." Although written for ISA Server 2000, Shinder details some of ISA's built-in filters in his article, *Introducing the ISA Server 2000 Application Layer Filtering Kit.* This article can be found at http://isaserver.org/articles/spamalfkit.html.

The last item in the list in the left hand pane is General, shown on the previous page. Of special note is the Delegate User Roles and Permissions link. This is one of the new features incorporated into ISA Server 2004. Using this wizard you can configure three distinct levels of access:

- Basic Monitoring
- Extended Monitoring
- Full Administrator

Basic monitoring provides access only to the basic ISA Server monitoring features. Extended monitoring adds read-only access to configuration settings. Full administrator as its name implies, allows full access to the ISA server.

Configuration

As previously stated when discussing network templates the default configuration is Edge Firewall. For purposes of this paper we will first need to convert this to a 3-Leg perimeter.
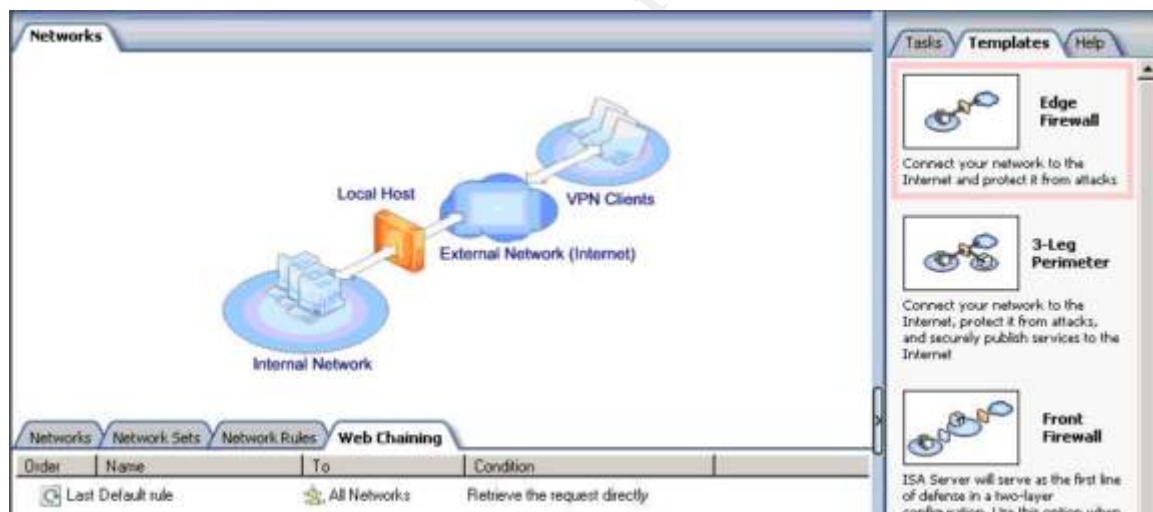
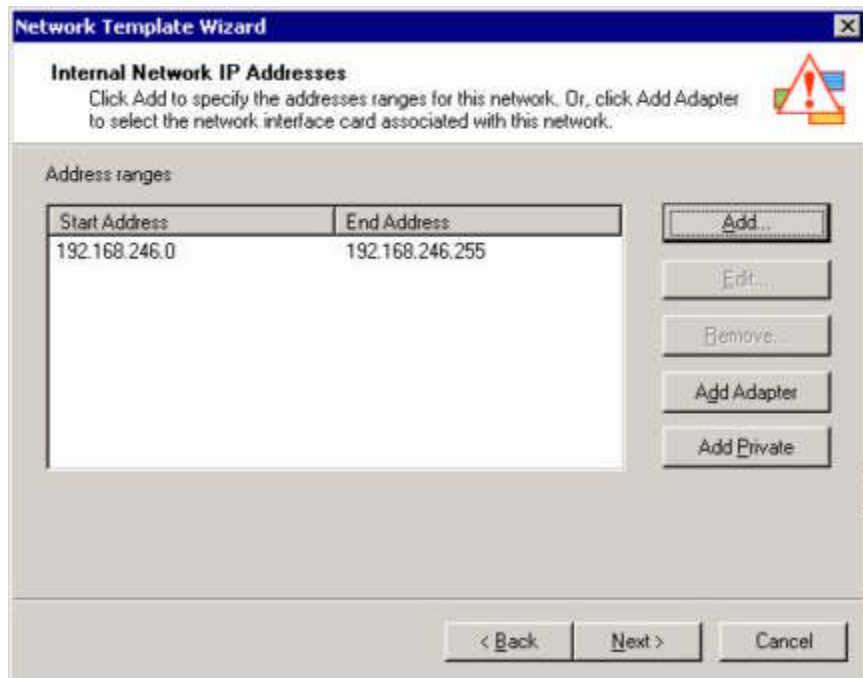Begin by clicking on the Templates tab of the right hand pane for any of the Networks items.

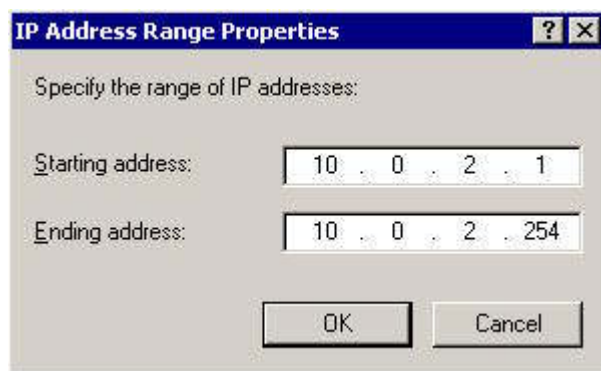Click on the 3-Leg Perimeter to start the wizard.
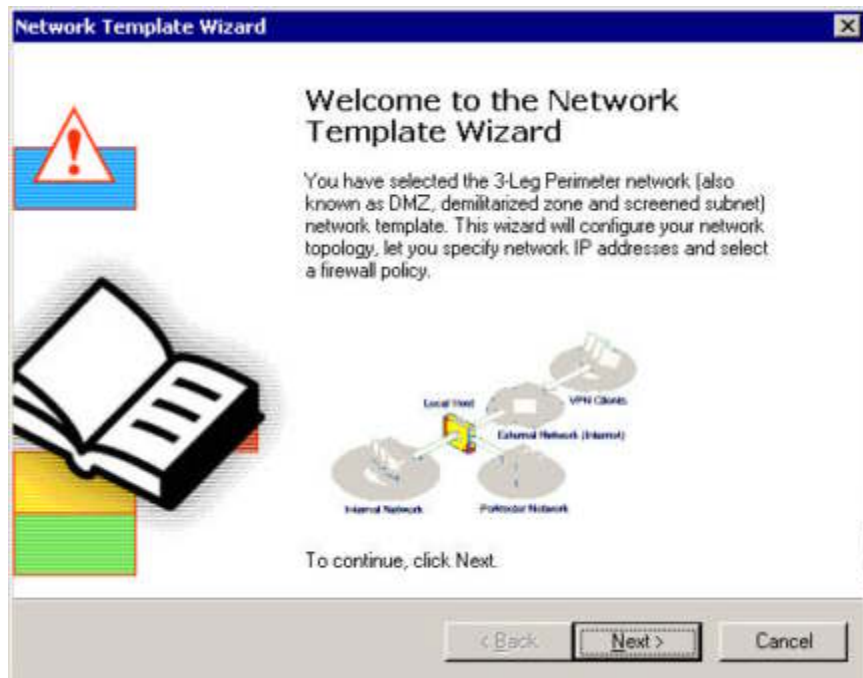
Click Next.

As this was a fresh installation and we did not make any configuration changes, click Next.

Since we already configured the internal network as part of the initial installation, click Next.
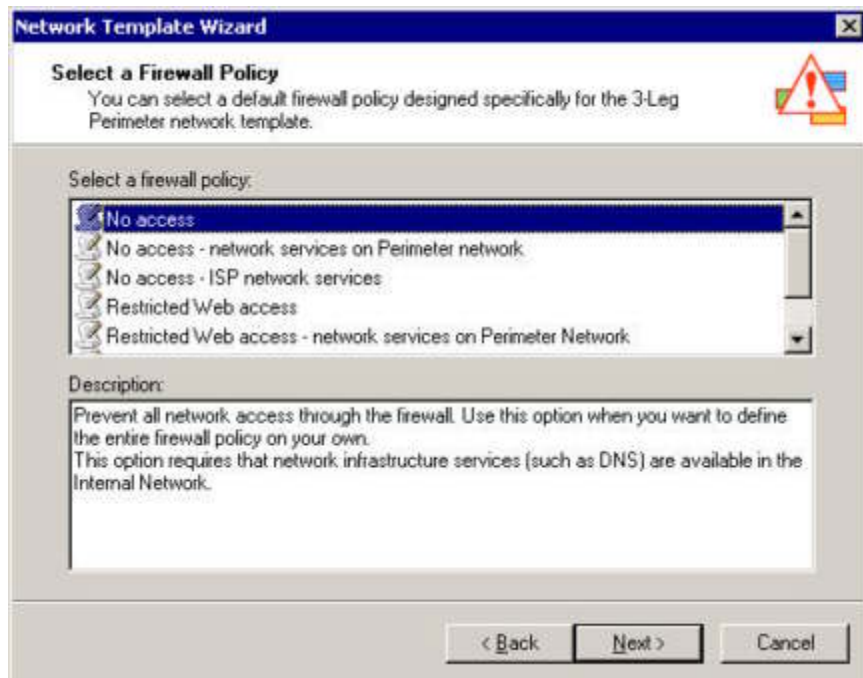

We now need to define the IP address range of the perimeter network. Click Add.

Enter the starting and ending address for the IP range and click OK.

Click Next.

This is where it gets a bit tricky. You are given the opportunity to select from a number of pre-defined firewall policies. Selecting the incorrect option here may require hours of work to properly configure the ISA server for a production environment. For purposes of this paper, select "No access" and click Next.
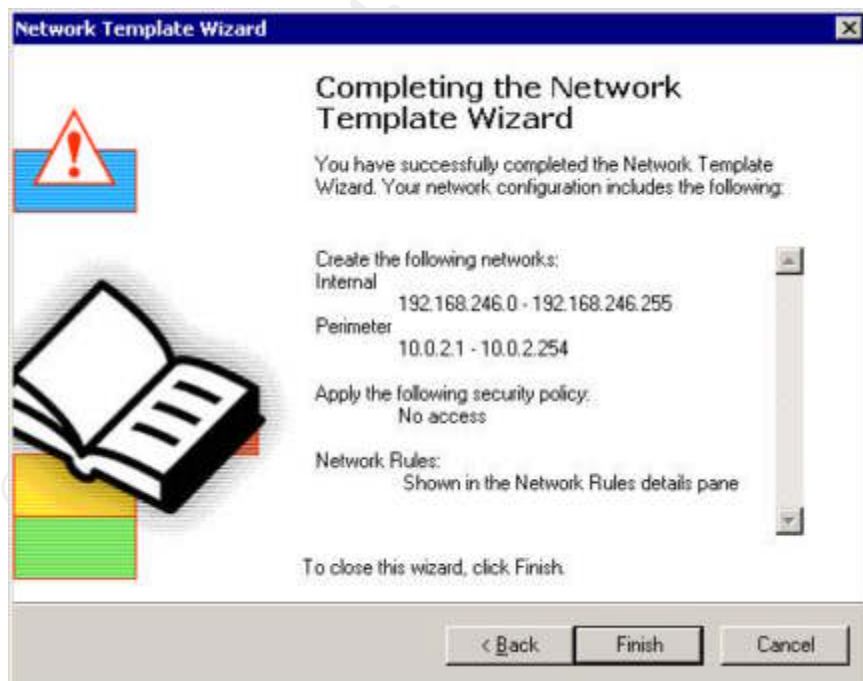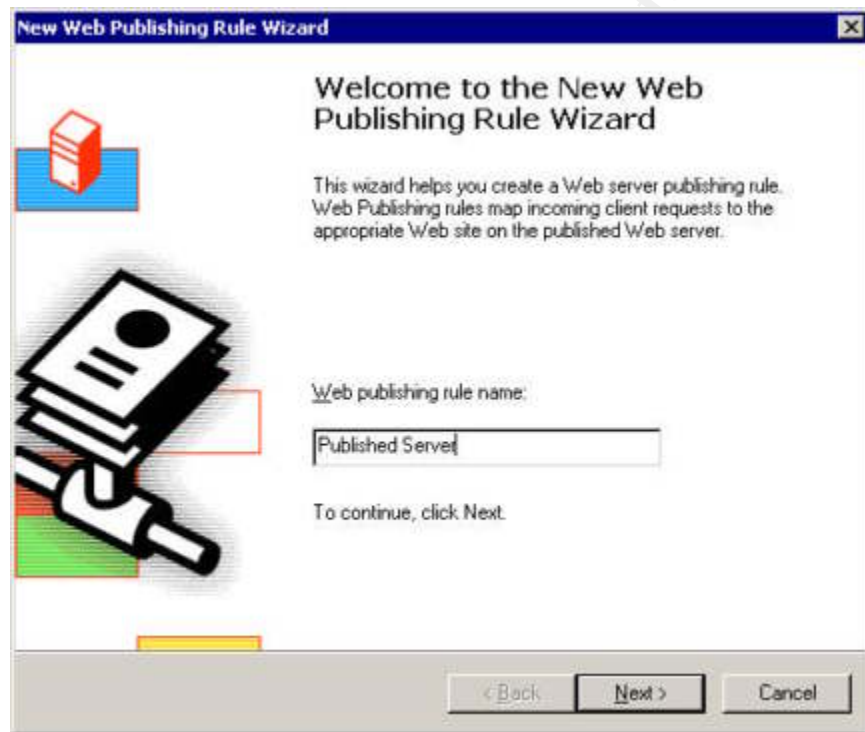

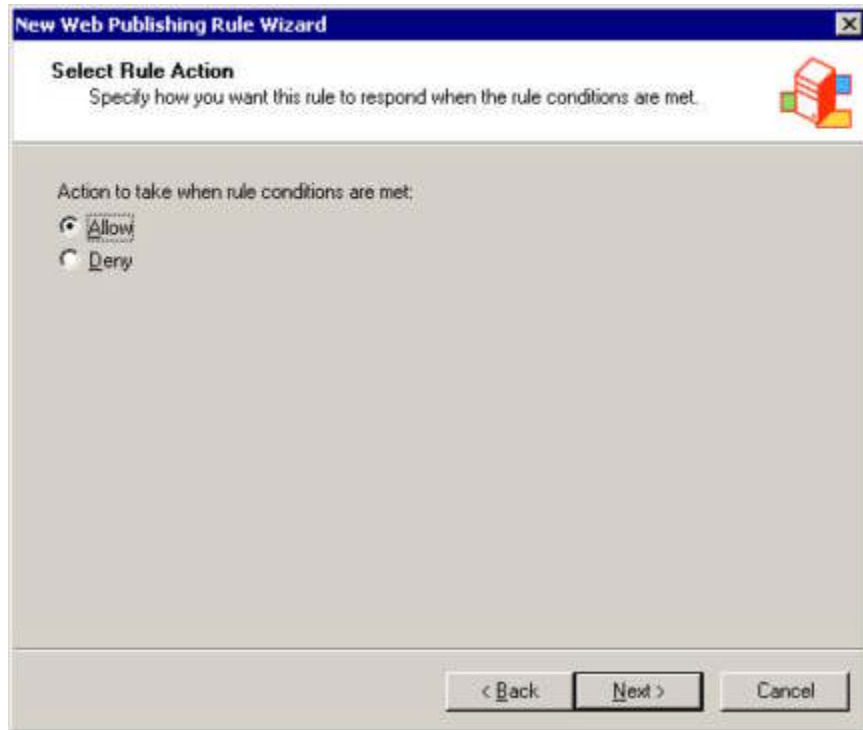Click Finish.
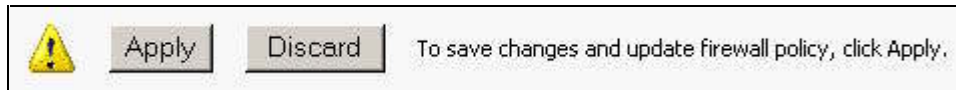
To apply the change, click Apply.

Now that we have our ISA server configured as a 3-Leg Perimeter firewall we can now publish the web server.
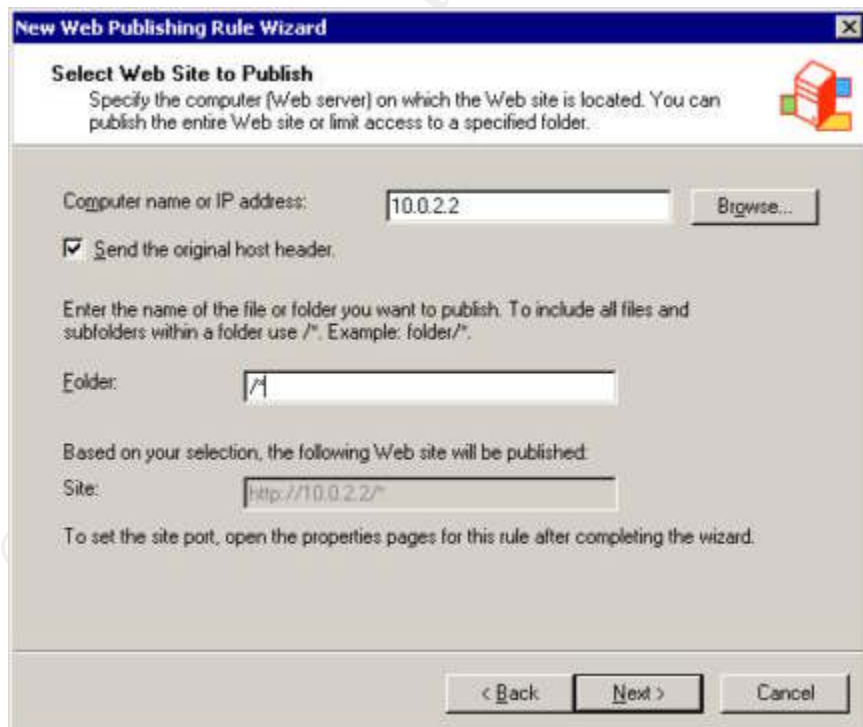
Publishing a Web Server

Begin by clicking on Publish a Web Server in the right hand task pane to start the wizard.
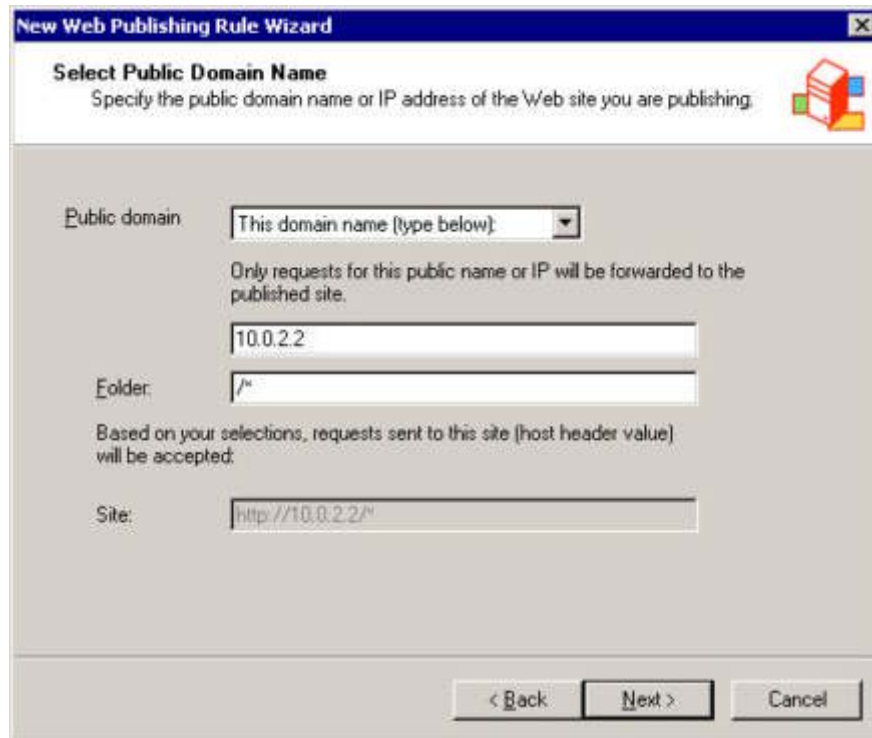

Name the rule Published Server and click Next.

Select Allow and click Next.

Enter the IP address of the web server. Checking the Send the original host
header checkbox causes ISA server to pass the host header it receives on to the
web server. This is useful when hosting multiple sites on one web server using
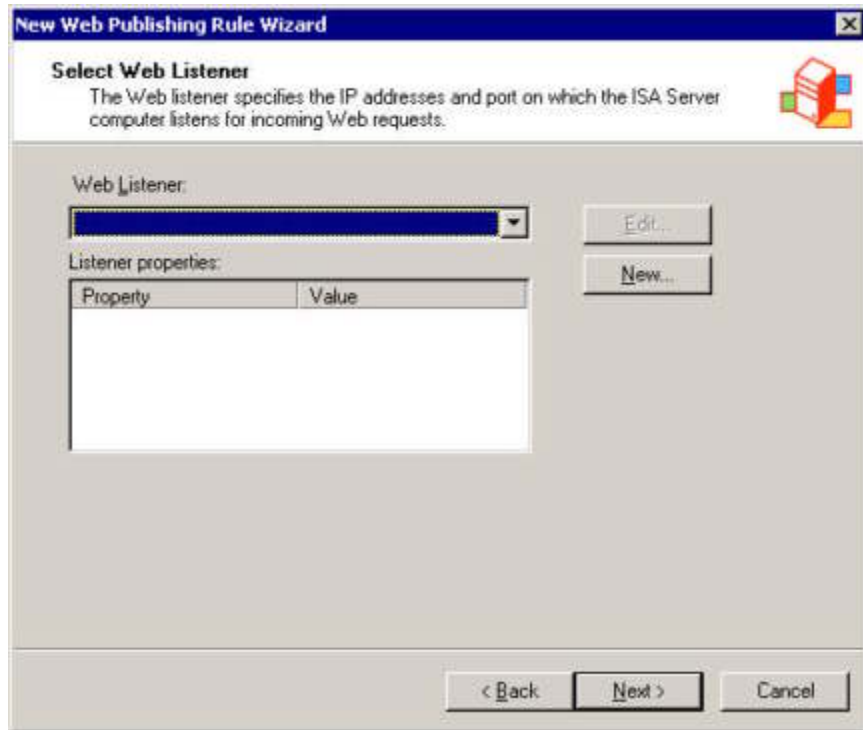
host headers to distinguish them from each other. The folder entry of "/*" causes all page requests that match to be sent to the single web server. Rules can be configured to route traffic for certain subfolders to alternate servers for processing. Click Next to proceed.

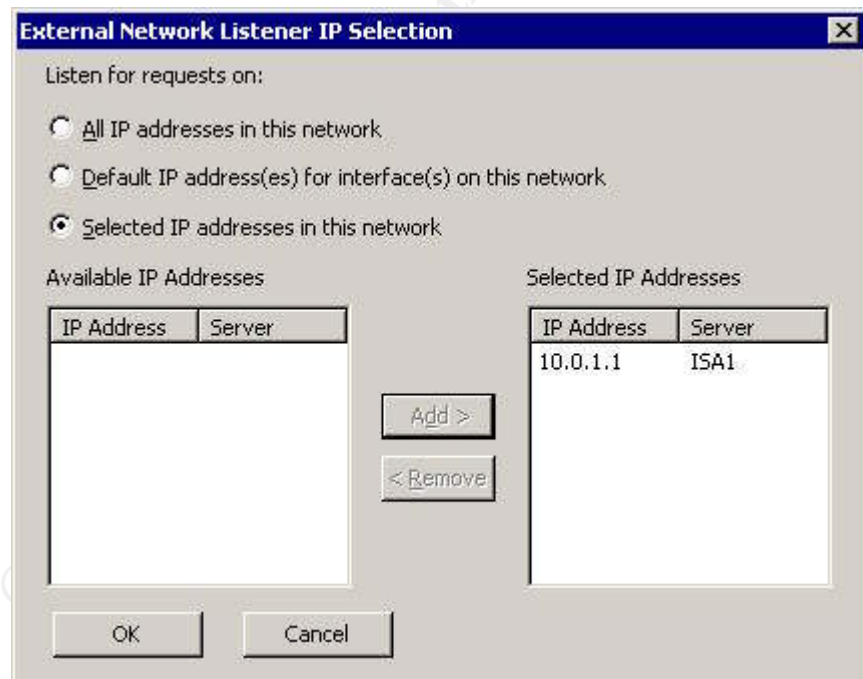Enter the IP address of the web server and click Next.

A web listener specifies the address and port that ISA should "listen" on for incoming requests. To begin the wizard, click New.
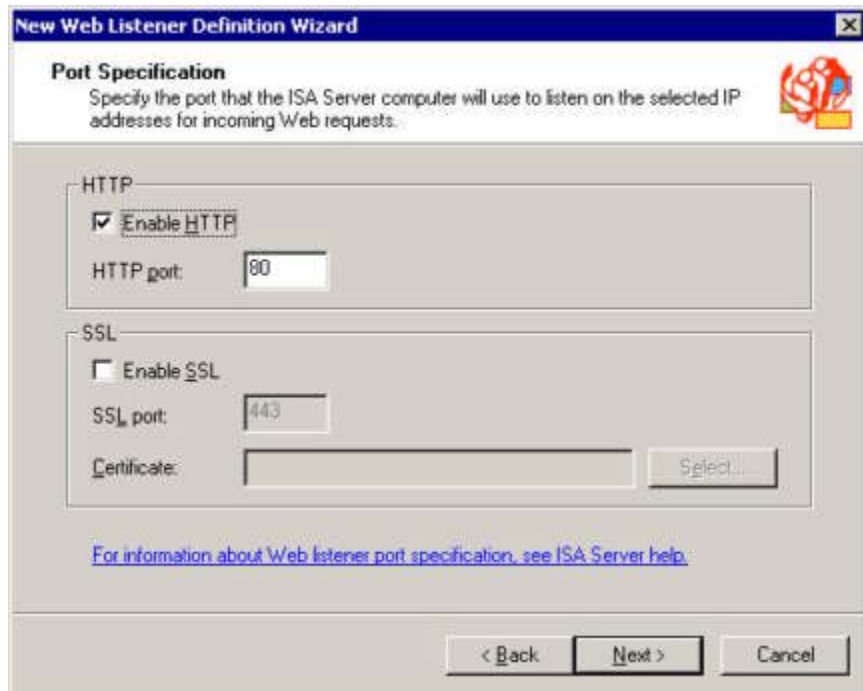

Name the listener HTTP and click Next.

Click External and then Address.

Click the Selected IP addresses in this network radio button, highlight the server's IP address and click Add. Click OK then Next.
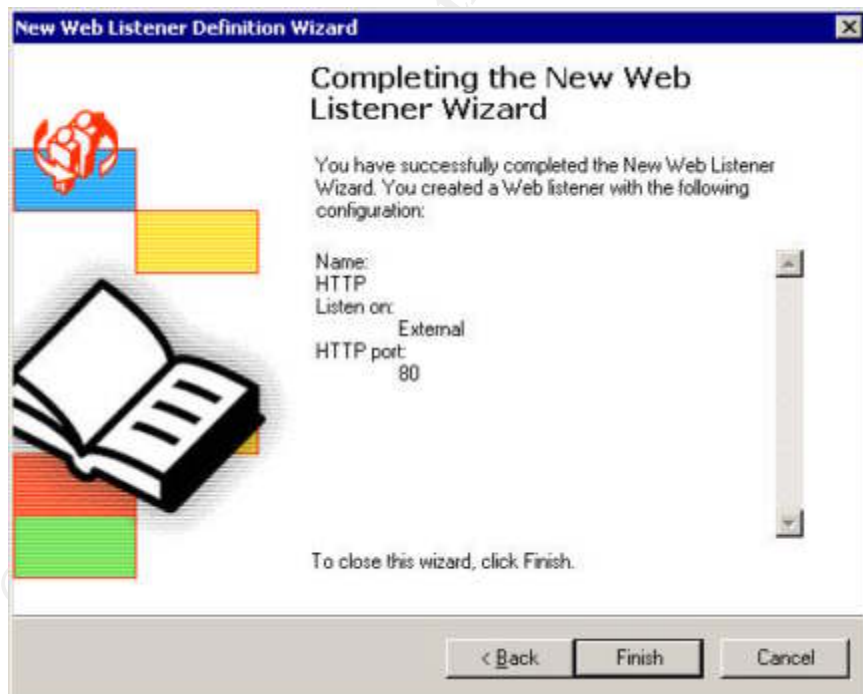
Click Next.

Click Finish to complete the web listener wizard.
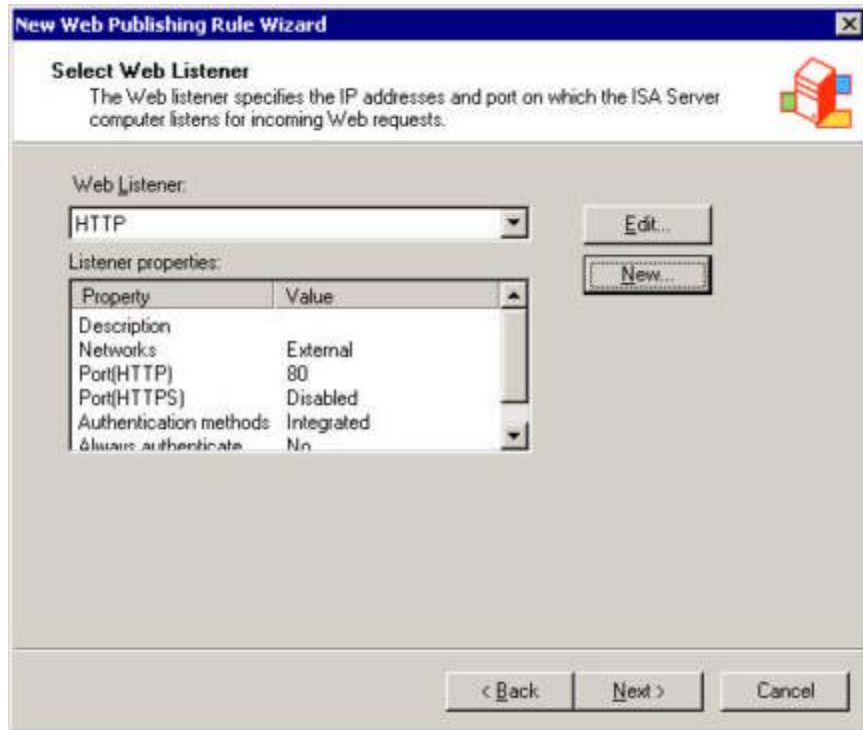
Click Next.

Click Next.

Click Finish and then apply the changes.

The web server is now published and available to internet users. To test, you may need to configure hosts files or DNS, then open a browser, type in the URL for the server and press Enter.

Summary

The paper began with a description of a sample network configuration for our ISA server that included three networks. Installation requirements and pre-installation tasks were discussed.

Next we walked through an entire installation of ISA Server 2004 Beta 2, discussing the most important screens and selections. Once the software was loaded we took a tour of the management UI. Wh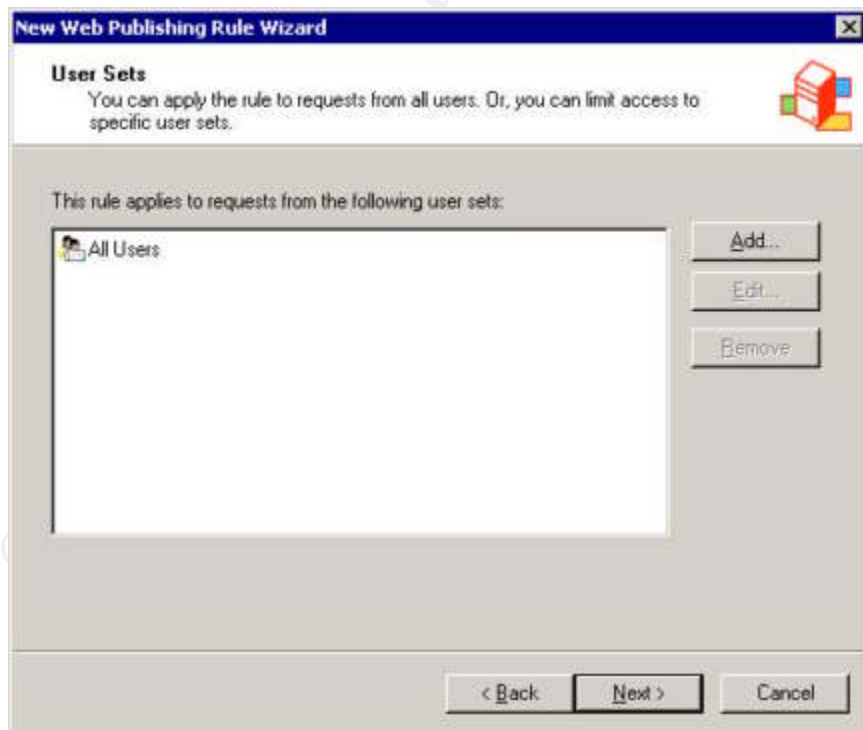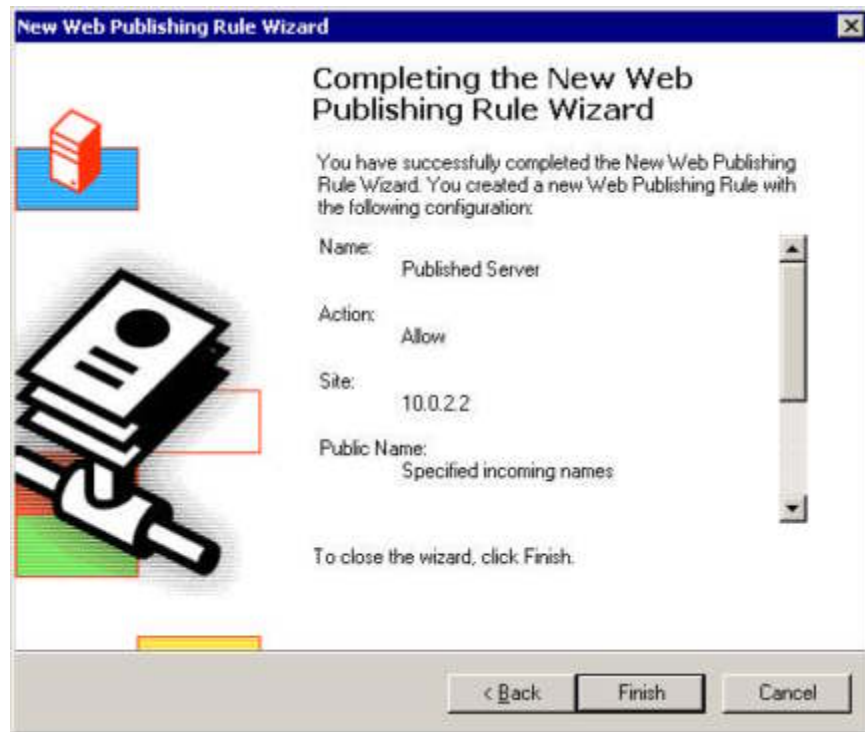ile we looked at each of the main screens within ISA Server 2004, there are many more configuration and properties screens that we did not discuss.

Finally, we completed the configuration of the ISA server and published a web server.

Although this paper touched on many of the features of ISA, becoming familiar with all of the features and configuration parameters will take time and further research. As this is a Beta 2 product look for more information to become available in the near future.

References

"What's New in ISA Server 2004." Jan 2004. Microsoft Corporation. 27 Mar 2004. <http://download.microsoft.com/download/d/d/e/dde6159d-e84f-4afe-9290-bb45a51d0357/ISA2004WhatsNew.doc>.

IANA "Special-Use IPv4 Addresses." Sep 2002. Network Working Group. 27 Mar 2004. <http://www.ietf.org/rfc/rfc3330.txt?number=3330>.

"ISA Server 2004 Installation and Feature Guide." 2003. Microsoft Corporation. 27 Mar 2004. <http://www.microsoft.com/isaserver/beta/default.asp>.

"ISA Server 2004 Solution Documentation." 2003. Microsoft Corporation. 28 Mar 2004. <http://www.microsoft.com/isaserver/beta/default.asp>.

Shinder M.D., Thomas W. "Introducing the ISA Server 2000 Application Layer Filtering Kit." 15 Dec 2003. 28 Mar 2004. <http://isaserver.org/articles/spamalfkit.html>.

Shinder M.D., Thomas W. "Get Up and Running with ISA Server 2004 Beta 2." 27 Jan 2004. 27 Mar 2004. <http://www.isaserver.org/articles/isa2004beta2.html>.

Shinder M.D., Thomas W. " Using ISA Server 2004 Network Templates to Automatically Create Access Policy: The Edge Firewall Template." 16 Feb 2004. 28 Mar 2004. < http://www.isaserver.org/tutorials/2004edgefirewall.html>.

"Events for authorization roles are not logged in the security log when you configure auditing for Windows 2000 Authorization Manager Runtime." Microsoft Corporation. 18 Feb 2004. 27 Mar 2004. <http://support.microsoft.com/default.aspx?scid=kb;en-us;821887>.

Green, Jack. "Installing Microsoft's Internet Security and Acceleration Server (ISAS): Getting Started and Testing." 1 Nov 2001. 27 Mar 2004 <http://www.sans.org/rr/papers/66/210.pdf>

"ISA Server 2004 Beta." Microsoft Corporation. 27 Mar 2004. <http://www.microsoft.com/isaserver/beta/default.asp>.

Edery, Yigal. "ISA Server 2004 Developing an Application Filter for Microsoft Internet Security and Acceleration Server 2004." MSDN Magazine March 2004: 89-101.

"bastion host." searchSecurity.com. 28 Mar 2004.
<http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214476,00.html>.

ISA Server 2004 Beta 2 Help. 2004. 28 Mar 2004.