brainbuzz.com™
Cramsession

# Cramsession™ for Installing,Configuring, and Administering Microsoft ISA Server 2000, Enterprise Edition

This study guide will help you to prepare for Microsoft exam 70-227, Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition. Exam topics include Implementing, administering, and troubleshooting information systems, Managing and troubleshooting Policies and Rules and ISA Server Services, and Monitoring and Analyzing ISA Server Use.


Check for the newest version of this Cramsession
http://cramsession.brainbuzz.com/checkversion.asp?V=2452054&FN=Microsoft/ISAServer2000.pdf


Rate this Cramsession
http://cramsession.brainbuzz.com/cramreviews/reviewCram.asp?cert=ISA+Server+2000


Feedback Forum for this Cramsession/Exam
http://boards.brainbuzz.com/boards/vbt.asp?b=678

## More Cramsession Resources:

Search for Related Jobs
http://jobs.brainbuzz.com/JobSearch.asp?R=&CSRE

CramChallenge - practice questions
http://www.cramsession.com/signup/default.asp#day

IT Resources & Tech Library
http://itresources.brainbuzz.com

Certification & IT Newsletters
http://www.cramsession.com/signup/

SkillDrill - skills assessment
http://skilldrill.brainbuzz.com

Discounts, Freebies & Product Info
http://www.cramsession.com/signup/prodinfo.asp


# FTP & HTTP virus scanning & content filtering for ISA server

## LANguard Content Filtering & Anti-Virus for ISA Server

**LANguard** provides content checking and anti-virus of HTTP downloads, web browsing and FTP downloads, protecting your network against web-borne viruses, Trojans, objectionable material and more. Also helps prevent unproductive use of the Internet.

**Scans FTP & HTTP traffic!**

**Click here to download your copy today!**

LANguard

Microsoft Certified Solution Provider

GFI

USA: Tel: +1-888-2GFIFAX; UK & ROW: Tel: +44-(0)20-8546 0640; Email: sales@gfi.com; Web: www.gfi.com



ISA server .org

**Includes FAQ's, add-on software listings, tutorials, tips, books, message boards, discussion lists & more - all related to Microsoft ISA Server 2000!**

**www.ISAserver.org**


# Contents:

# Overview of ISA Server Features

## Application Filters

Application filters extend the abilities of ISA Server. For example, the SMTP application filter can be used to block harmful attachments or messages with offensive content. In another example, the H.323 filter can help control how ISA Server handles H.323 audioconferencing and videoconferencing traffic (NetMeeting uses H.323).

## Caching

ISA Server can store copies of all Web and FTP objects it retrieves locally on its hard drive. Whenever a user requests an object, ISA Server checks to see if a copy of it has already been retrieved and is stored locally. If the object already exists in the cache, it is returned to the user's Web browser directly from the ISA Server. ISA Server only has to forward requests on to the Internet when there is no copy of an object stored in its cache or the object is not fresh enough. This reduces an organization's bandwidth costs and enables client requests to be processed much more quickly.

## Firewall

Like the firewall that protects the occupants of a vehicle from its engine compartment, ISA Server includes a powerful firewall that stands between the Internet and your internal network to provide security. Through *packet filtering*, ISA Server has the ability to examine each packet of traffic that passes through the firewall and decide whether to open a port to allow it through or to reject the packet depending on the rules ISA Server has been configured with. This ability to examine each packet is called *stateful packet inspection.*

Microsoft ISA Server also includes sophisticated *Intrusion Detection* features which constantly scan for common attacks and immediately notify the server administrator when one is detected.

## Firewall Client

Microsoft Provides a special Firewall Client for Windows platforms that can be used to provide different levels of security for different groups of users throughout the enterprise (this is not possible using SecureNAT). One of the primary advantages of

the Firewall Client is that is can authenticate internal client systems before allowing access to resources located beyond the firewall. It also allows Winsock applications full access to all protocols without requiring protocol definitions and the ability to manage complex protocols without the aid of application filters.

### SecureNAT

SecureNAT combines the ease of configuration of Network Address Translation with ISA Server's powerful stateful packet inspection capabilities to provide complete support for heterogeneous computing environments or environments where all users enjoy the same level of access. Simply configure the ISA Server as the default gateway in the SecureNAT client machine's TCP/IP settings, and ISA Server will handle all translation of traffic from your privately addressed network to the public network.

### Server/Web Publishing

You can provide an extra layer of security by placing your servers (e.g., Web, e-mail, etc.) behind your ISA Server and having it publish information to Internet users on their behalf. By acting as the intermediary, the ISA Server is presented to malicious Internet users rather than the actual servers whose information is being published.

## Installing ISA Server

### 1. System requirements

| Component | Standard Edition | Enterprise Edition |
|---|---|---|
| CPU | 300 MHz or faster Pentium II, maximum of 4 processors | 300 MHz or faster Pentium II, no limit to number of processors |
| RAM | 256 MB | 256 MB |
| Hard Disk | 20 MB (NTFS file system required for cache) | 20 MB (NTFS file system required for cache) |
| Operating System | W2K Server or Adv. Server (SP1 or higher), or W2K Datacenter Server | W2K Server or Adv. Server (SP1 or higher), or W2K Datacenter Server |
| Active Directory Integration | No | Yes (needed to join an ISA Server to an array) |

## 2. Preconfigure network interfaces

The server must have two or more network interfaces installed if it is configured as a firewall (caching only servers require a single internal network interface). A network adapter is required to communicate with the internal network, while a modem, ISDN adapter, or network adapter can be used for the external Internet connection.

Both network interfaces must have the TCP/IP protocol bound to them. The external interface may receive its IP address dynamically from a DHCP server but the address of the internal network adapter must be static.

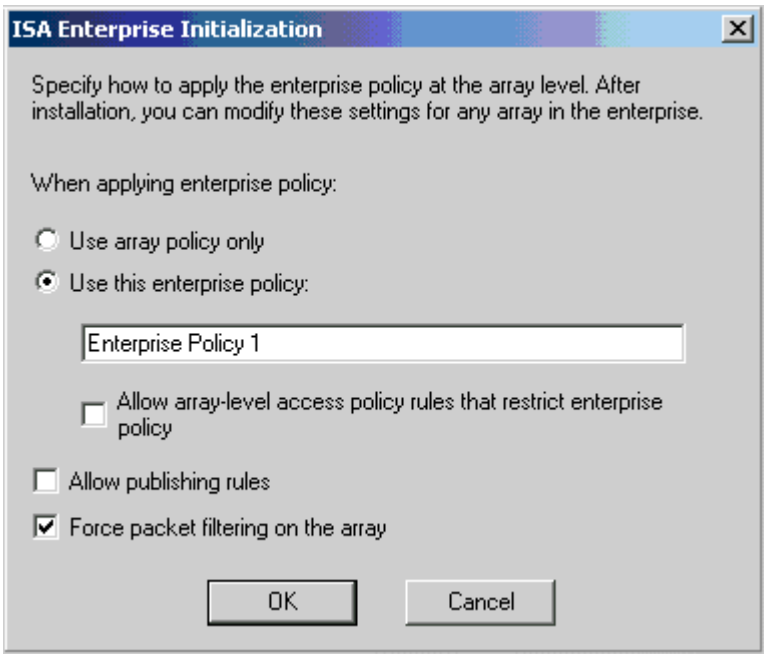
Configure your DNS settings prior to installing ISA Server – many of ISA Server's features will not function properly if they cannot resolve a fully qualified domain name (FQDN) to its IP address.

## 3. Install ISA Server

### Enterprise Initialization

To install ISA Server in Enterprise mode you will first need to add ISA Server specific extensions to the Active Directory Schema. You will need to be logged on with an account that belongs to the Schema Admins group to do this. Using this account, run **msisaent.exe** from the \isa\i386 directory on the ISA Server CD-ROM or installation share.

You will be prompted to choose how you want to apply your *Enterprise Policy*. You can choose to allow administrators of each array to set their own policies or force all arrays to adhere to an enterprise policy. This can be changed at any time later on.




## Beginning Installation

To install ISA Server you must belong to either the Administrators or Server Operators group. Start installation of ISA Server by running **setup.exe** from the \isa directory on the ISA Server CD. Setup will immediately inspect your system for membership in Active Directory and the presence of ISA Server Schema extensions in Active Directory. If the extensions are found, you are prompted to choose between installing in *Enterprise* mode or as a *stand-alone* server. If the Schema extensions are not found you will only be able to install ISA Server in standalone mode.

There are three installation modes:

- *Firewall mode:* ISA Server runs as a security firewall only.
- *Cache mode:* ISA Server runs as a cache only, accelerating Internet access for client machines by caching frequently accessed content locally.
- *Integrated mode:* Both the firewall and caching capabilities are installed providing increased security and performance for Internet access.


## Cache Configuration

During installation in Cache or Integrated Mode, you must choose where to place the cache initially. ISA Server tries to place a 100 MB cache on drive C: by default (if C: is formatted with NTFS). The cache *must* be placed on an NTFS formatted drive. ISA server cannot cache to a drive that has not been assigned a drive letter (W2K allows you to mount drives inside folders).

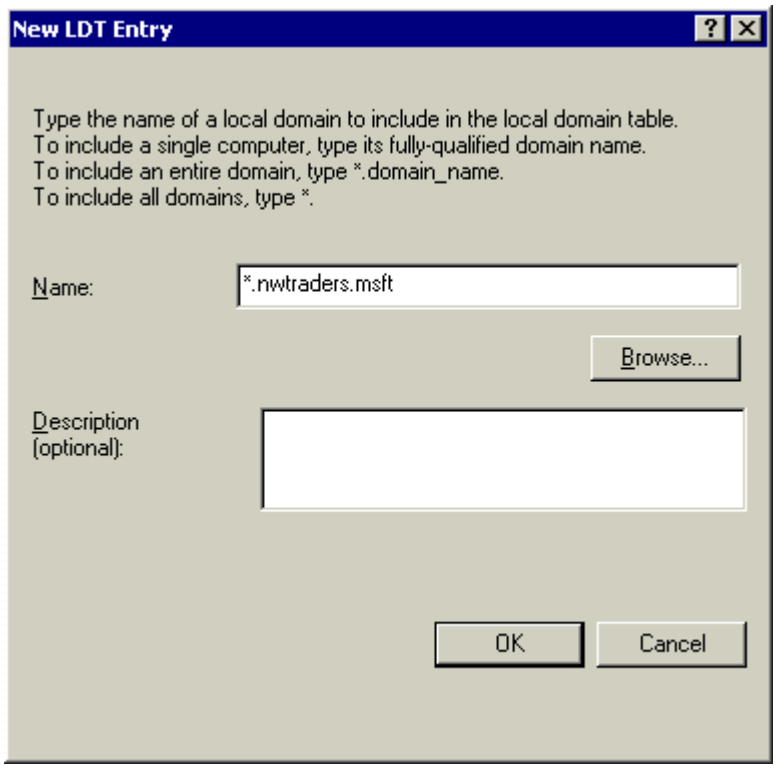
## Local Address Table (LAT)

ISA Server can automatically construct a Local Address Table (LAT) that includes addresses the Internet Assigned Numbers Authority (IANA) has set aside for private use. These ranges are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255. All addresses that appear within the LAT are translated so beware of placing public IP addresses here (there's really no need to).

Firewall Clients use a file named **msplat.txt** to store Local Address Table information in. This is refreshed periodically from the server. You can also create custom LATs on the client if you want to deviate from the LAT used by ISA Server using the **locallat.txt** file.

## Local Domain Table (LDT)

Local (internal) domains are entered into the Local Domain Table (LDT). Firewall clients use the LDT in order to decide whether to request a resource directly or to pass it on to ISA Server. If an address has a period in it, it's considered a remote domain, unless there is an entry for it in the LDT. For ALL domains, type "*." (without quotes). For an entire domain, type "*.*domain.com*" (*domain.com* can be substituted with the name of your domain). For a specific machine, enter its Fully Qualified Domain Name (FQDN) such as, "*hostname.domain.com*" (replace *hostname* with the host name of the machine you wish entered into the LDT).




## 4. Upgrade MS Proxy Server 2.0 to ISA Server

### Migration Process

Stop all Proxy Server 2.0 services on the Windows NT 4.0 Server. If the server is part of a proxy array, you must remove it from the array. You can now upgrade the Windows NT 4.0 Server to Windows 2000. You can now install ISA Server.

ISA Server will detect and migrate all Proxy Server 2.0 settings. If your proxy server was a standalone its policies will be migrated to the new standalone ISA Server. If your proxy server was part of an array, the Enterprise Policy Settings you have configured for your ISA Server array will determine how your Proxy Server 2.0 configuration settings are carried over. For example, if the ISA Array Rules allow Web publishing, old Proxy 2.0 publishing settings are migrated to the new ISA Server settings.


Proxy Server 2.0 cache settings are automatically carried over into ISA Server. Cache content itself is not migrated because ISA Server uses a newer and faster caching engine that is incompatible with its predecessor. Old cached content is deleted as part of the setup.

SOCKS rules from Proxy Server 2.0 are not supported under ISA Server. ISA Server includes a SOCKS application filter that refers to both Array and Enterprise policies before processing SOCKS traffic requests.

Proxy Server 2.0 and ISA Server can be mixed together in *chains* (hierarchical caching), but they cannot co-exist together in the same *array* (distributed caching).

## Key Differences

Under Proxy Server 2.0 all internally published servers, except for Web servers, had to be configured as Winsock Proxy Clients. You also had to mess around with the WSPCFG.INI file which was annoying, to say the least. ISA Server treats all internally published servers as SecureNAT clients so you don't need to configure anything other than the default gateway on the server being published now (w00t!).

ISA Server does not require that IIS be running on the server, unlike Proxy Server 2.0. In fact, it is recommended that if you do have a web server on the ISA Server, you change the port the Web Server is using before you install ISA Server. You will not be able to use ISA Server Web Publishing rules unless Web Server uses a different port other than TCP port 80.

Support has been dropped for IPX/SPX in ISA Server. All proxy clients will need to have TCP/IP bound to their network adapters.

ISA Server listens for HTTP proxy requests on port 8080 by default. Downstream proxies and clients should be configured to use this port. Proxy Server 2.0 used to use port 80. If upgrading from Proxy Server 2.0, this will create some issues for client connectivity immediately after the upgrade has completed. See below.

Authentication was required when members of a Proxy Server 2.0 array communicated with each other. Members of an ISA Server array do not need to

authenticate with each other as this functionality is provided through Kerberos 5 and Active Directory.

## 5. Troubleshoot setup issues

ISA Server says that it can't find the Schema information it needs to install in Enterprise mode and that I can only install it as a standalone server. *The Schema hasn't been initialized properly. If you are a Schema Admin you need to run* ***msisaent.exe*** *or you need someone who has sufficient authority to do this for you.*

ISA Server barfs and spits out all kinds of error messages during the installation. *For troubleshooting purposes ISA Server creates an installation log file called* ***isas.log*** *which can be found under \Program Files\Microsoft ISA Server. Reading it will probably give you a headache. In most cases MS recommends uninstalling and re-installing ISA Server through the* ***Add/Remove Programs*** *applet in the Windows 2000* ***Control Panel****.*

Now that I've installed ISA Server my clients can't connect to the Internet even though I've set it as the default gateway! *Doh! This is the default behavior of ISA Server. You need to configure* Access *and* Protocol Rules *before traffic will be allowed past the firewall.*

Internal clients are accessing the Internet and they're not supposed to be! *Check your LAT – did you mistakenly include external IP addresses?*

My LAT is screwy – I'm getting LAT errors*. Did you put the address of your external network interface in your LAT? Is your routing table configured properly? Do you have overlapping IP address ranges in your LAT?*

I've just upgraded from Proxy 2.0 – how come my Web proxy clients can't access the Internet now? *Your Proxy 2.0 clients used to use port 80 for HTTP connections – you either need to configure this in ISA Server (it defaults to port 8080) or configure all of your Web clients to point to port 8080 on the ISA Server computer/array. If you aren't using a proxy auto-configuration file your workload just went up.*

The ISA Control Service won't start. If you configure the external network interface as part of the LAT on a machine that belongs to an array, it won't be able to

communicate with Active Directory and pull down its configuration info (and you wind up with nasty *Control Service* errors in your Event Viewer).

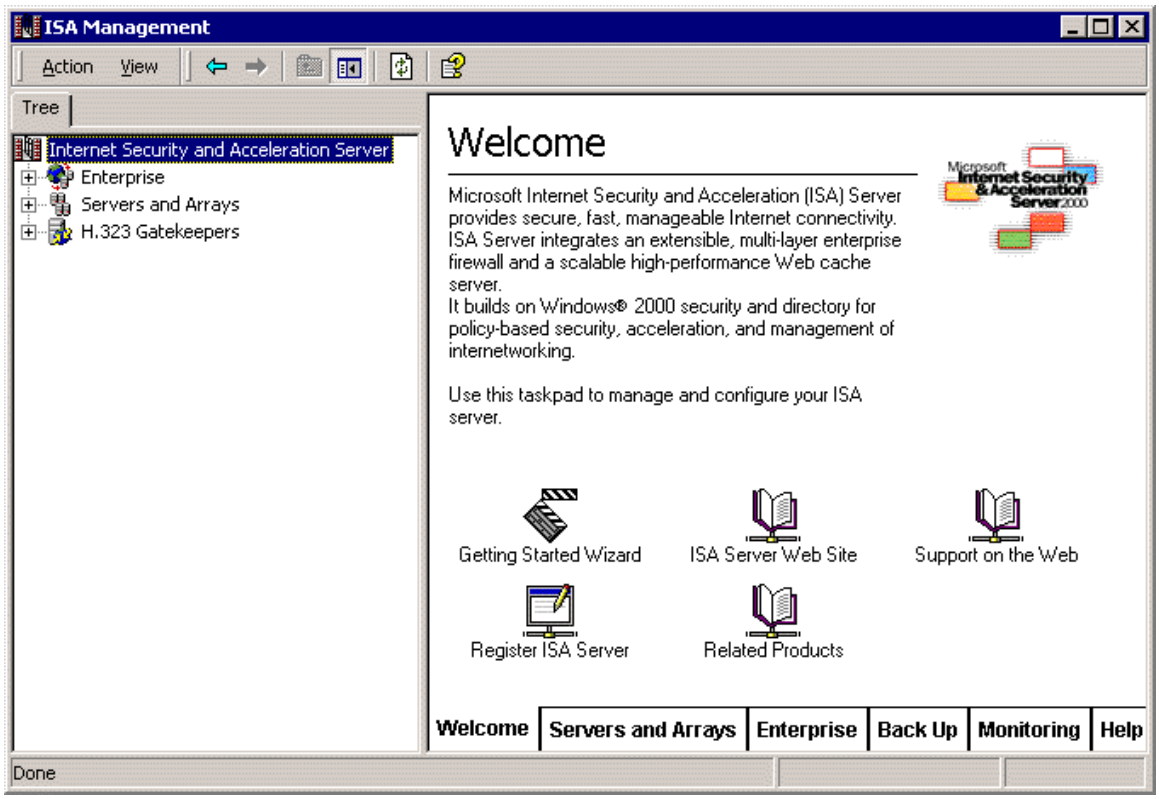
I can't join my ISA Server to an existing array! Start pinging other array members and domain controllers for your current domain to ensure network connectivity.

Important: Did you notice how many of these errors are related to your Local Address Table? Make a point of misconfiguring your LAT to find out what happens first hand – you may be grateful for this experience come exam day.

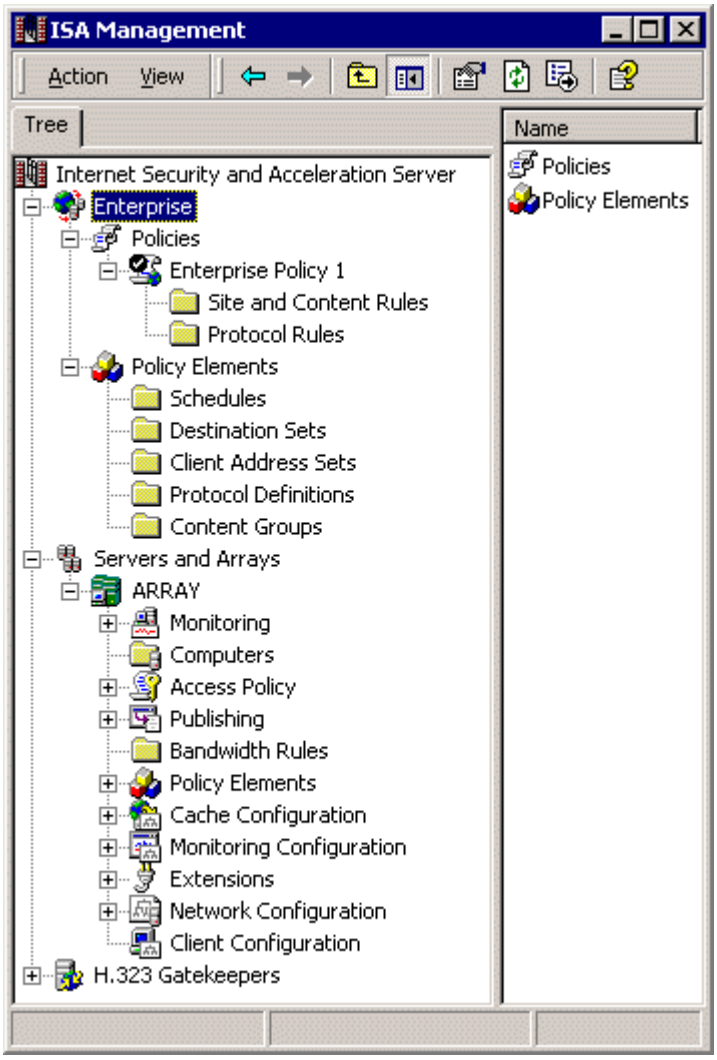
# Configure and Troubleshoot ISA Server Services

## 1. Introduction to the ISA Management Tool

The shortcut for the **ISA Management** interface is placed in your Programs Menu during ISA Server installation. It is essentially a Microsoft Management Console (MMC) that uses the ISA Management snap-in. You can add this snap-in to your own custom MMCs and create taskpads to help in administering ISA Server. By default, ISA Server defaults to a Taskpad view immediately after installation:




Under the **View** menu select **Advanced** and you will be switched to the advanced administration view shown below:

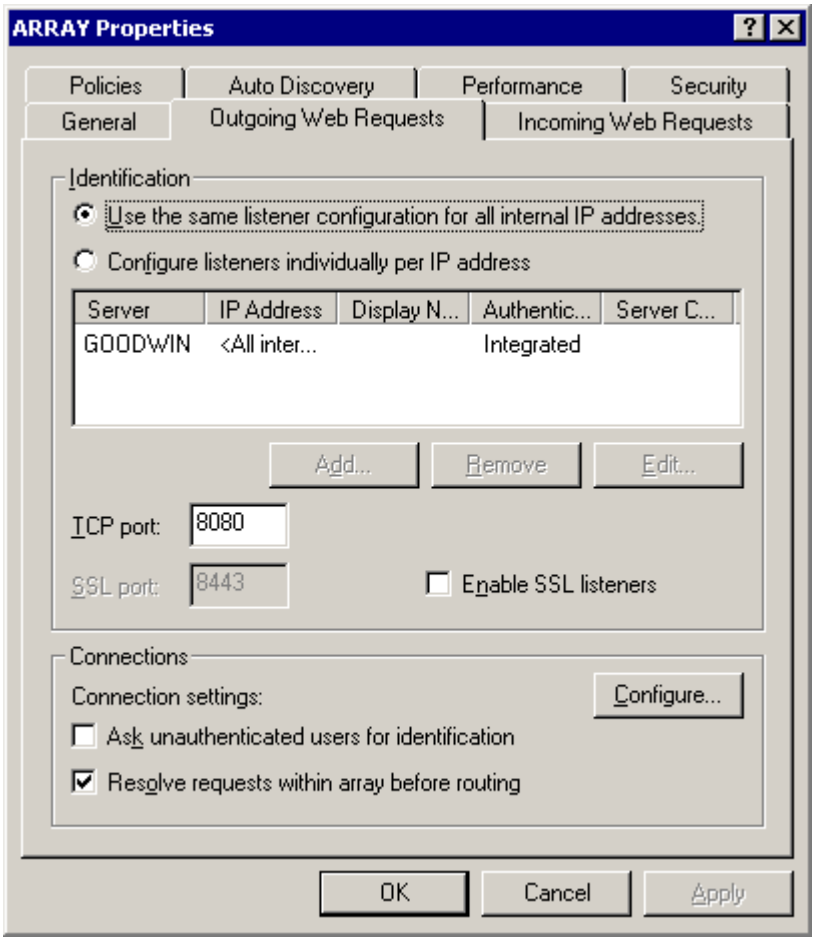



## 2. Configure and troubleshoot outbound Internet access

### Outgoing Web requests

ISA Server configures a listener for outgoing Web requests on port 8080 by default. Because Web Proxy clients don't automatically send authentication info to the ISA Server, you have the option of asking unauthenticated users for, well, authentication. :)

Caveat: If you configure the outgoing listener to ask for authentication then you must have the Web Proxy Client configuration set in all your browsers or you'll have unhappy users who are unable to Web surf. If users are configured as Firewall or SecureNAT clients only, they will be denied access when you require authentication.




## SecureNAT clients

There is no user-level authentication with SecureNAT clients. The only restrictions you can use are:

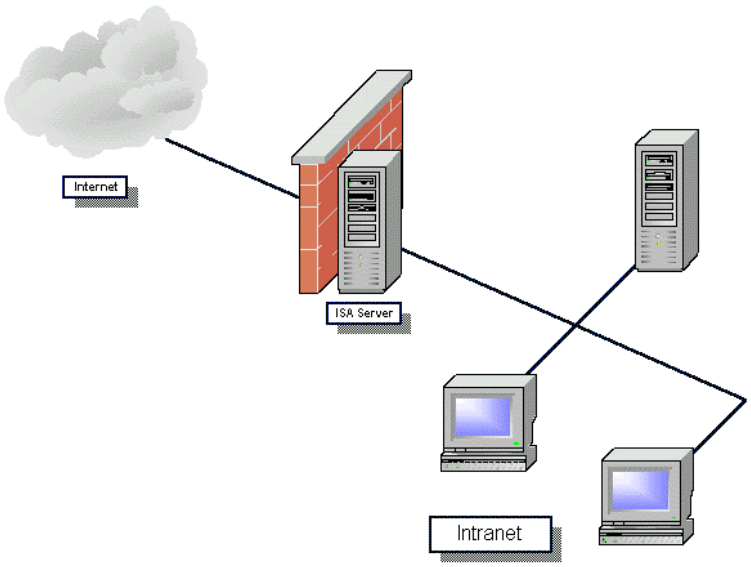
- Site
- IP address

- Protocol
- Schedule

## Firewall clients

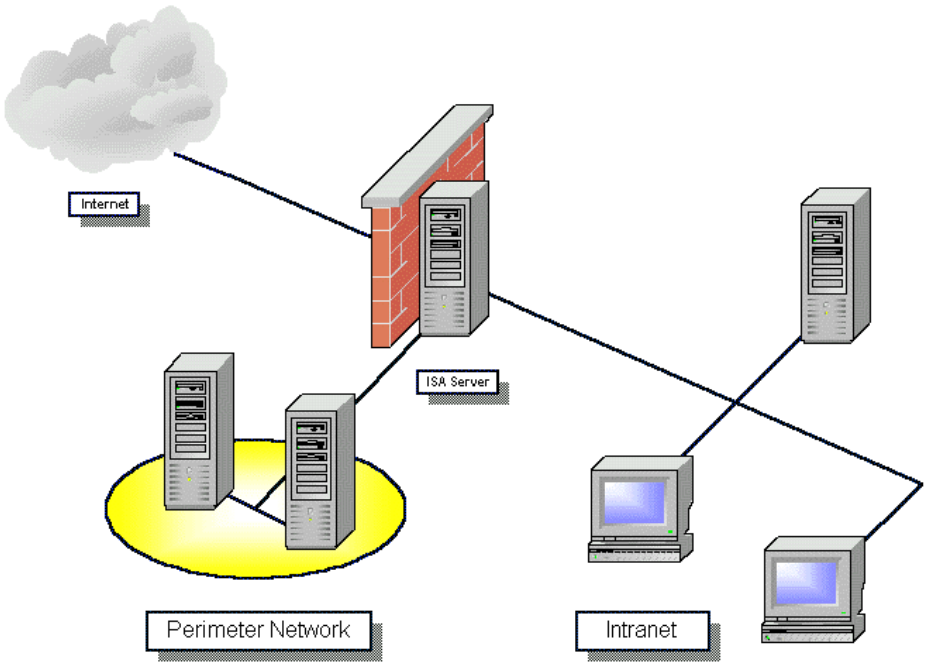
Firewall clients automatically pass user credentials along and authenticate with the ISA Server. This is great if you're running Windows 95, Windows 98, Windows ME, Windows NT 4.0, Windows 2000, and Windows XP because these are the operating systems the firewall client works with. If you're running any other operating system –– no client for you (you're stuck with SecureNAT).

## 3. Configure ISA Server hosting roles




### Bastion Host

*Bastion Hosts* have two network adapters; one is connected to the Internet and the other is connected to the internal network. It provides a single point of defense against attacks on the internal network from the Internet. This deployment scenario is inexpensive and easy to administer, but is not advisable when you have to provide access to resources on your internal network as it allows Internet users to directly access resources on your intranet.



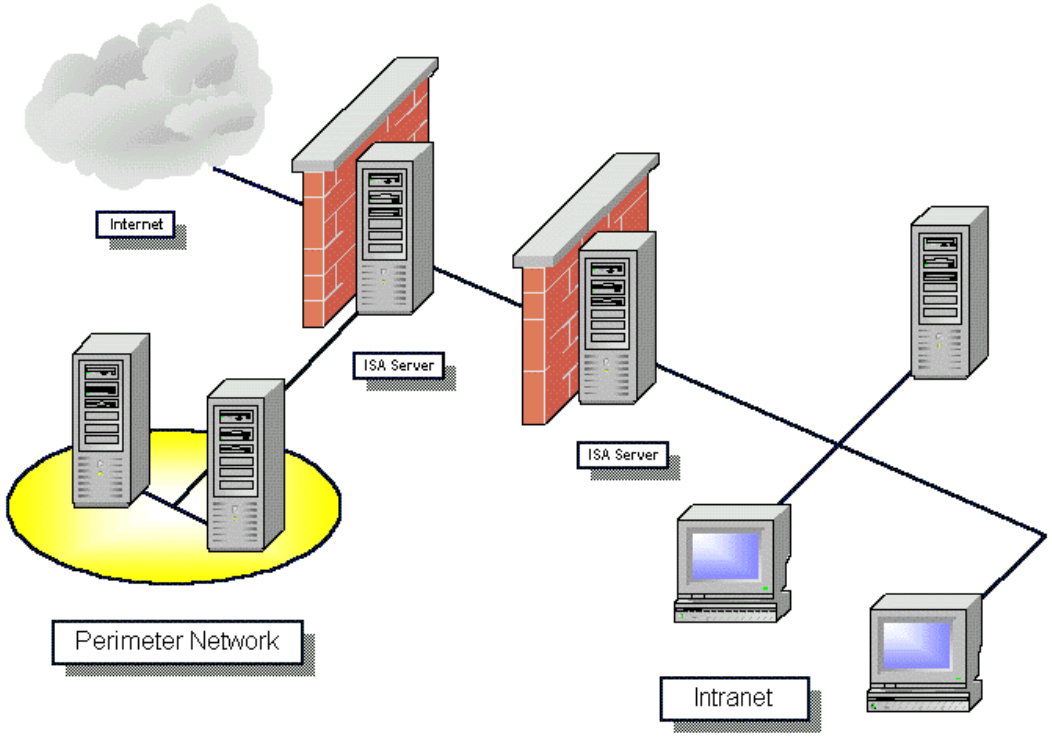

## Three-homed Firewall with DMZ

A *Three-homed Firewall with DMZ* (demilitarized zone) is a server with three network adapters. One is connected to the Internet, one is connected to a secured subnet (the DMZ or perimeter network) and the last is connected to the internal network. Traffic from the Internet is routed to the servers in the DMZ. This traffic does not actually go through the firewall; it uses routes setup in Windows 2000's Routing and Remote Access Services (RRAS). This is more secure than a Bastion Host where Internet traffic is passed directly to the internal network. Internal clients can access resources in either the DMZ or on the public Internet.

To configure the DMZ for a 3-homed perimeter network, you must use real, routable IP addresses (not the private addresses) in the perimeter network. You must ***not*** include the address range for the perimeter network in the LAT. Access to the perimeter network occurs through routing, which you must enable in the ISA Server

console in the Packet Filter properties, and Packet Filters. Server Publishing would be used to publish servers on your *internal* to your perimeter network For example, your web server in the perimeter network may need access to the SQL server on your internal network. You publish the SQL Server to your perimeter network to provide that access.

## DMZ with Back-to-back Firewalls




A *DMZ with Back-to-back Firewalls* provides the most security and is one of the most popular firewall designs. It is also one of the most expensive and involves increased administrative overhead. Specify this design for organizations that require the highest level of security.

The DMZ is located between two firewalls. The DMZ itself uses private addressing and all IP addresses should appear in the LAT of the external ISA Server. The servers in the DMZ are published through the external ISA Server computer/array. As most


conventional DMZs use public IP addresses and packet filtering, Microsoft's recommended method of using Network Address Translation, and publishing the servers in the DMZ, provides additional security.

## Web Publishing

Web publishing allows you to place one or more Web servers behind an ISA Server computer or array and have the ISA Server computer(s) process requests on behalf of the Web servers. This provides an extra degree of security, as Internet users are not actually accessing the servers themselves, so far as they know the ISA Server itself is the Web server. In reality ISA Server is acting as an intermediary between the Internet client and the real Web server(s).

Steps to publishing a Web site:

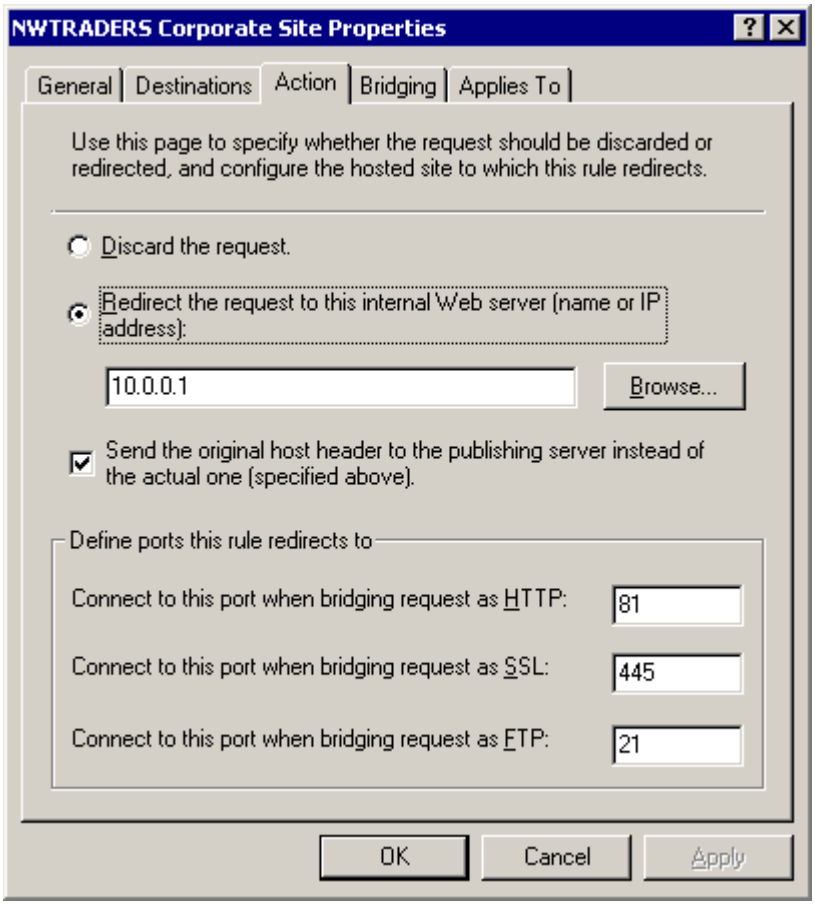
- Make sure you configure a listener for inbound Web requests on port 80.
- Configure the appropriate level of authentication for your listener
- Setup your Web site and configure it to use host header information
- Name your Web publishing rule
- Create a destination set for your internal Web server – use the Fully Qualified Domain Name for the Web server in your destination set
- Choose the client type – specific computers, specific users and groups, or all computers/users.
- Create a publishing rule that redirects traffic using the specified host header to the internal IP address of the published Web server.

The order of your Web publishing rules matters – they are processed from the top of the list to the bottom where you'll find the default rule. The default rule discards all incoming requests (so don't put it at the top of the list).

When you configure the listener for Web requests you can force users to authenticate with the ISA Server itself – this is in addition to any authentication required by the published Web server.

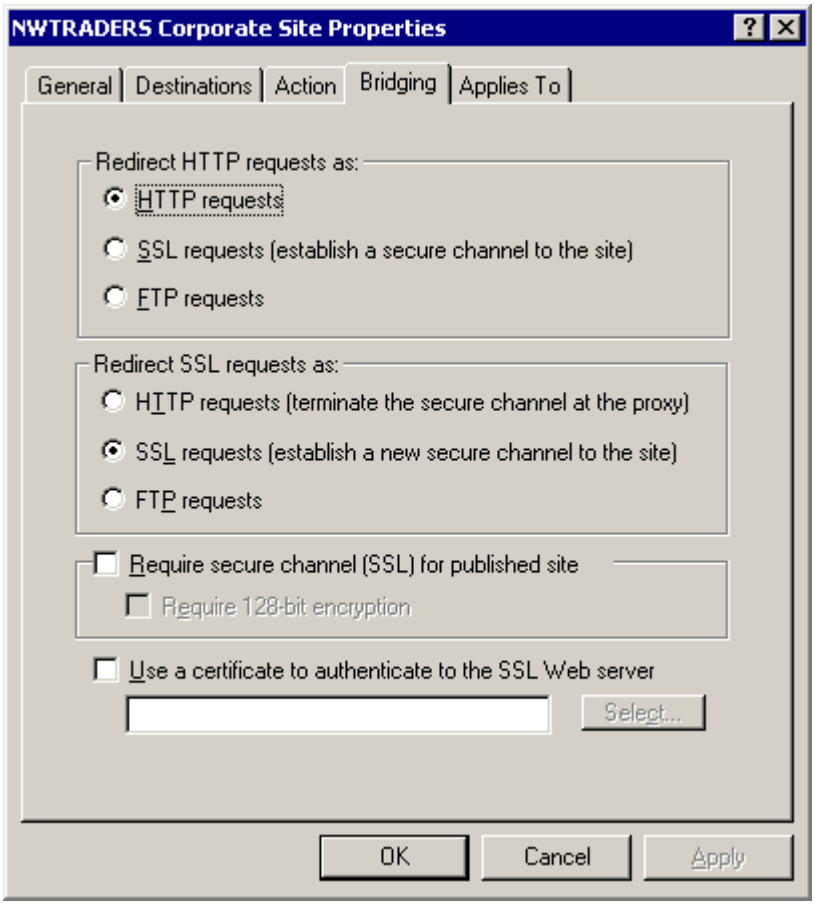
With Web publishing you have the ability to change the ports during redirection of the request. For example, if you are also using the ISA Server as a Web server, your

Web server cannot listen for requests on port 80 as that's where the Web Proxy Service lives. Instead, change the port your Web server uses to port 81 and configure your Web publishing rule to redirect inbound HTTP traffic for that site to port 81. You can do the same with SSL and FTP requests (example shown below – FTP port not changed):




As your server is published, it makes sense to have ISA Server accept SSL connections, bridge them, and pass them on to the secure Web server as an HTTP request (this process is called bridging). To do this you need to install a certificate in ISA Server and enable SSL listeners in the Incoming Web Requests properties (defaults to port 443). See this article for more information.

The following screen shot shows the options on the bridging tab:




## Server Publishing

Through Server Publishing, you can securely publish other servers such as FTP, E-mail (Exchange, SMTP, POP3, and IMAP4), IRC, Usenet News, and more. The servers are published as SecureNAT clients with ISA Server handling all Network Address Translation and acting as the intermediary between the Internet Client and the published server. Clients never actually communicate with the published server itself.

Server publishing works similarly to Web publishing with the following exceptions:

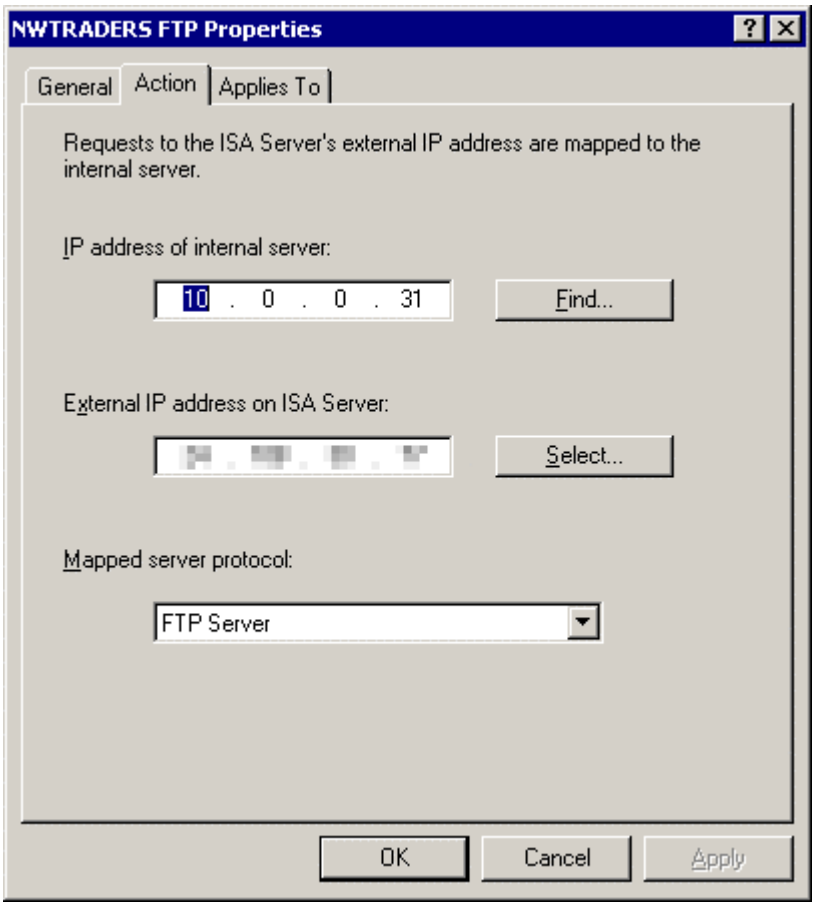
- You don't have to create Destination Sets

- You cannot redirect ports. If your server uses a non-standard port you must create a custom inbound protocol definition for it (policy element)
- If additional information is embedded in the packet header for secondary ports, you will require an application filter (e.g., both the FTP and H.323 protocols require application filters for this reason).
- If you are publishing a server that embeds additional information in the packet header and you don't have an application filter for it, you will need to use the **wspcfg.ini** file to bind the published server to the external network adapter of your ISA Server.
- The order of Server publishing rules doesn't matter
- If you have IP Packet filtering enabled you must create packet filters for published servers (e.g., port 110 inbound for POP3)

Steps for publishing a server:

- Name your Server Publishing Rule
- Configure address mapping by providing the internal IP address of the published server and the external IP address of the ISA Server
- Choose protocol for published server (whatever you've entered into your protocol definitions will appear on this list)
- Choose the client type – any request or specific client address sets (only works if IP Packet filtering is enabled)

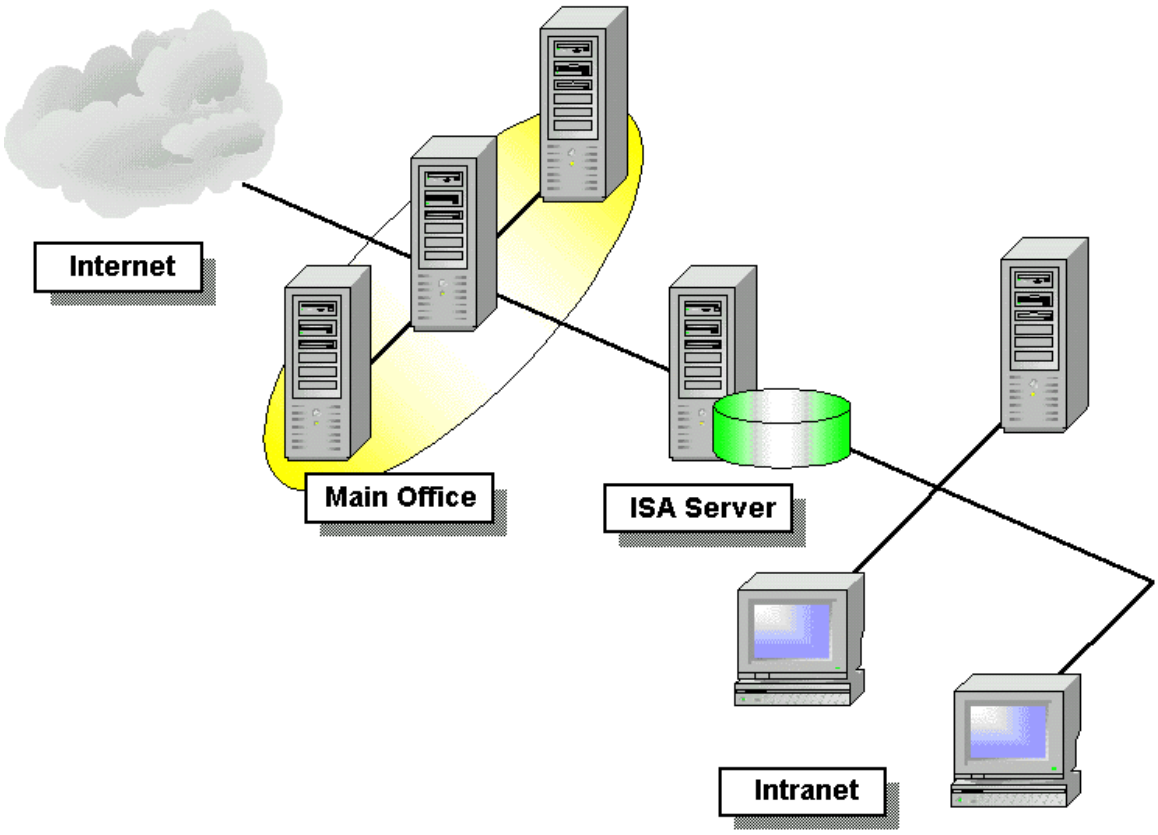
Here's a screen shot of the action taken by the Server Publishing rule I've created for my published FTP Server (yeah, I'm paranoid – the external IP address is blurred for a reason):




## 4. Deployment Scenarios

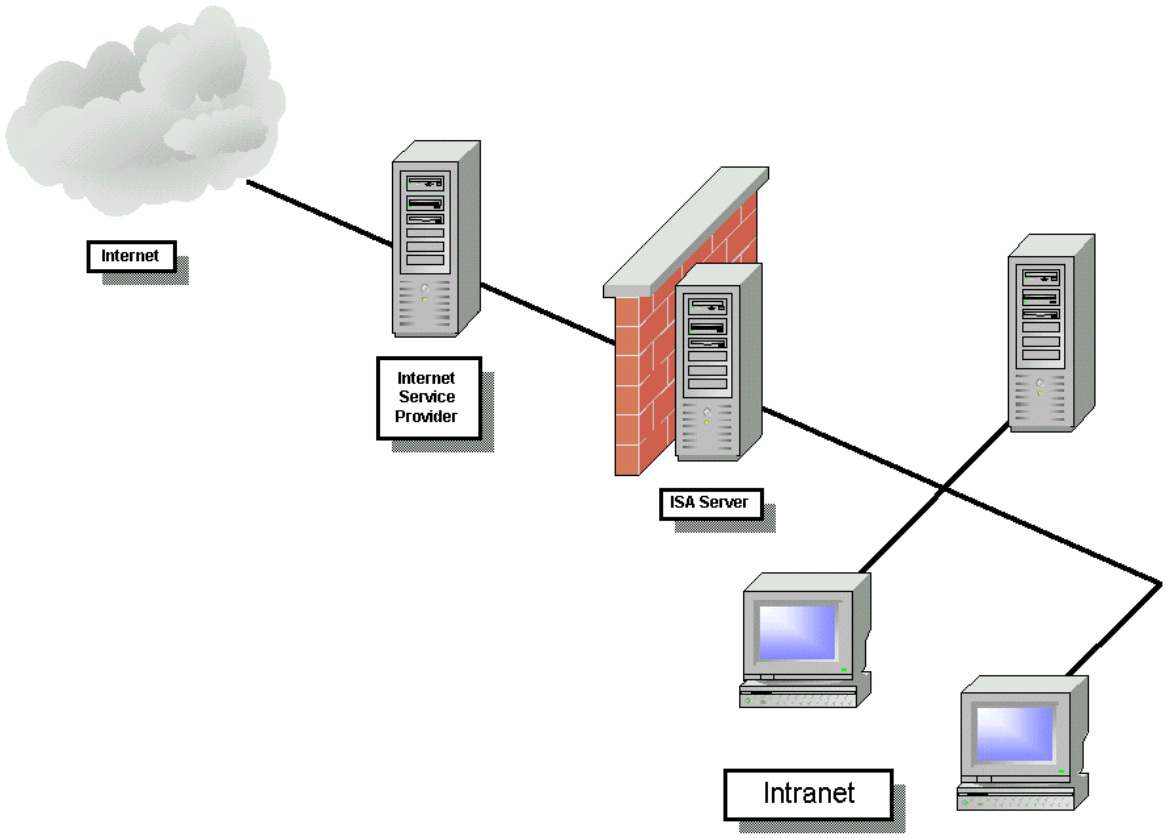
### Standalone Cache

Employed as a standalone caching server in a branch office or department, ISA Server minimizes the amount of network traffic between the branch office and the main office by returning frequently requested objects from its cache. This takes the load off of the outbound Internet connection and reduces bandwidth charges. See below for a diagram.




## Standalone Firewall

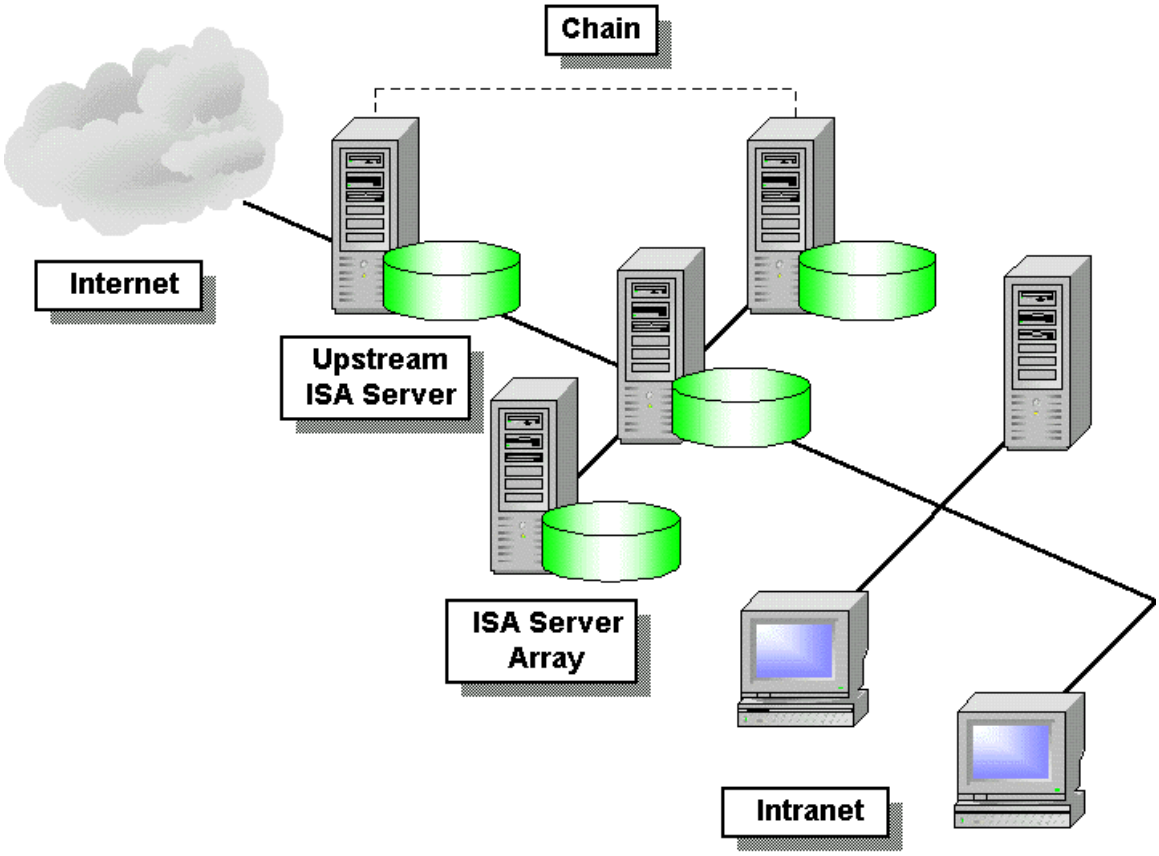
Employing ISA Server as a standalone firewall is only recommended in small networks with no more than 250 clients. The standalone server is basically a Bastion Host that provides security only. The firewall should be transparent to clients unless they try to access a resource they've been denied access to.




## Enterprise Cache

ISA Servers can be chained to one another or configured in an *Array* to enhance performance and reliability. When ISA Servers are *chained* (hierarchical caching), the local caching server can forward a request to an upstream ISA Server when it cannot return an object out of its own cache. This provides increased reliability and performance.

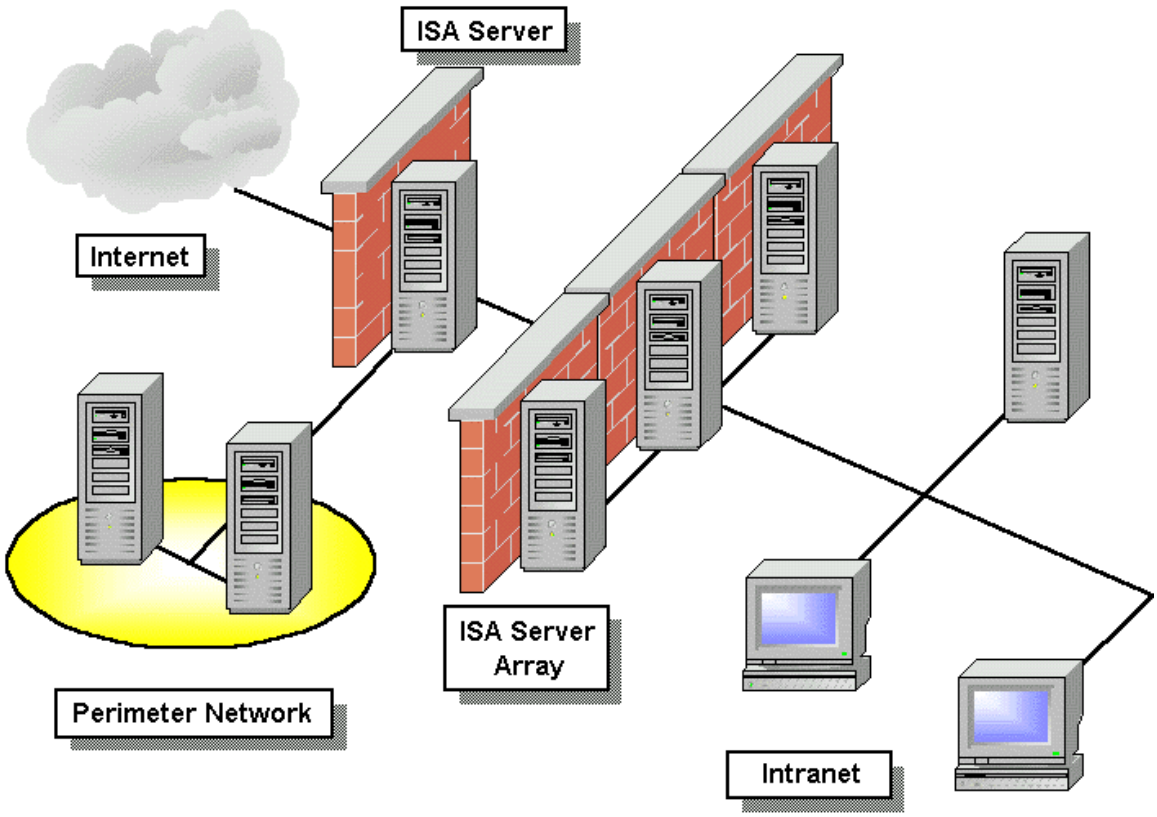
Arrays provide load-balancing and fault-tolerance in an enterprise environment. When ISA Servers are configured as an array, the load can be distributed equally across all servers or set according to server capacity. To increase performance simply add more servers to the array.




In the illustration shown above an array of caching ISA Servers is chained to an upstream ISA Server.

## Enterprise Firewall

Enterprise firewalls generally include back-to-back firewall configurations with a perimeter network, or DMZ, for servers that are accessed from the public Internet. ISA Servers can be placed in a load-balanced array for increased performance.




## 5. Configure H.323 Gatekeeper

### About H.323

The H.323 protocol is a standard defined by the ITU that specifies how multimedia services and equipment communicate over a network without Quality of Service (QoS) controls that guarantee bandwidth. Microsoft NetMeeting and White Pine's CUSeeMe are two popular applications that use the H.323 protocol.

ISA Server includes an H.323 gatekeeper to facilitate calls between users both on the internal network and users on the Internet. The gatekeeper not only controls access to the network, it facilitates placement of calls by providing address resolution services for callers.

Here's what happens when I place a NetMeeting call from my office to my wife who is using a machine behind an ISA Server firewall on my home network:

- I place the call to my wife using her e-mail address
- The gatekeeper intercepts the call
- The gatekeeper hits up DNS to find a user registered with my wife's e-mail address – it finds it through the SRV record I've entered (I'll get to that shortly)
- The gatekeeper now completes the call to my wife.

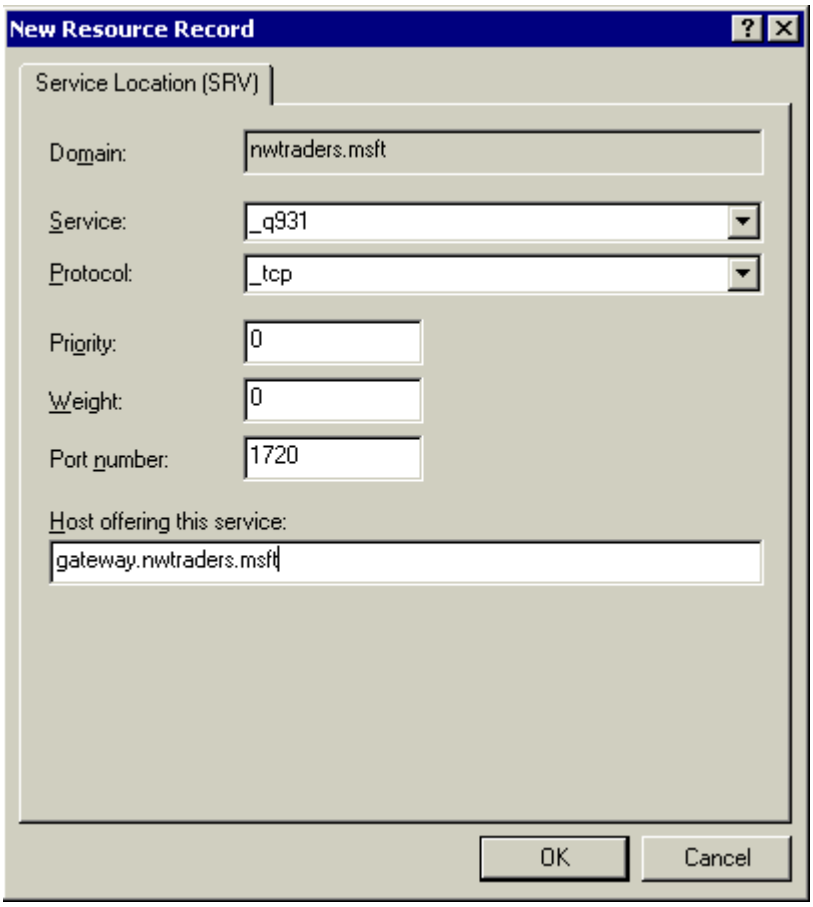
It doesn't matter that my wife is on a privately addressed network – the gatekeeper handles the network address translation.

More information on H.323 can be found here:

*http://support.intel.com/support/videophone/trial21/h323_wpr.htm*
*http://www.elemedia.com/Main/h323center/centerhome.htm (provides some basic information on the H.323 standards)*
*http://www.packetizer.com/iptel/h323/*
*(good list of other links can be found here)*

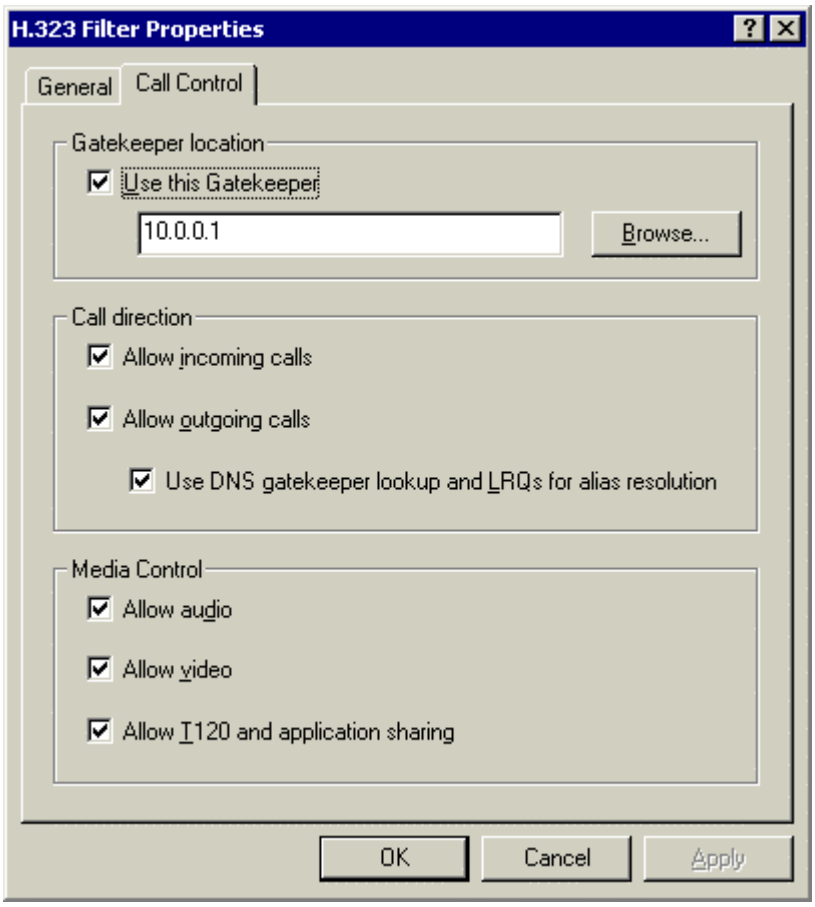
## Configuring an H.323 gatekeeper

Make sure you enter your Service Location (SRV) record first. Don't forget the underscore in front of _q931 or you'll end up banging your head on your desk for a week and a half like I did until a friend pointed out my configuration error.




In the ISA Management console tree, right-click **H323 Gatekeepers** and then choose **Add Gatekeeper**. Choose where you want the gatekeeper to run and then click OK.

Finally, make sure that your H.323 Protocol Filter is enabled. If you want, you can place restrictions on what call directions are allowed in addition to permitted media types (as shown below).




## 6. Configure and troubleshoot VPN access

### We're off to see the Wizard…

The nicest thing about setting up VPN connections in ISA Server is that everything is Wizard based. Launch the appropriate Wizard for what you want to do and the Wizard will create the appropriate packet filters and even configure the necessary RRAS settings for you. Kudos to the MS team for doing a great job here.

### Configuring the firewall to pass PPTP traffic

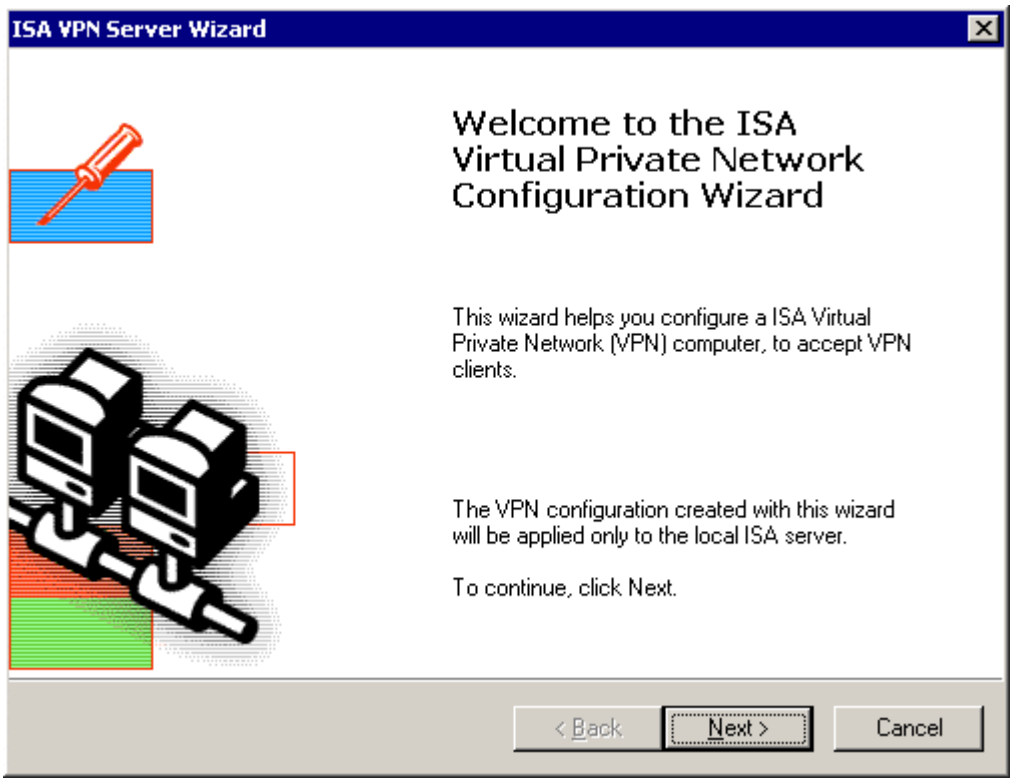
For each array, open **Access Policy,** right-click on **IP Packet Filters** and then choose **Properties** from the context menu. When the **IP Packet Filters**

**Properties** dialog appears click on the **PPTP** tab. Put a check mark in the **PPTP through ISA Server firewall** box. Your firewall will now allow outbound PPTP connections to other servers.

Caveat one: If you want to prevent users from accessing restricted content, remember that they can bypass your ISA Server and access content from the remote server they are connected to instead. Don't enable the IP Packet Filter for PPTP until you've thought things through otherwise SecureNAT clients can establish VPN connections and side-step your site and content rules. You may have to enable the PPTP filter only on specific arrays and only allow privileged users to access those arrays.

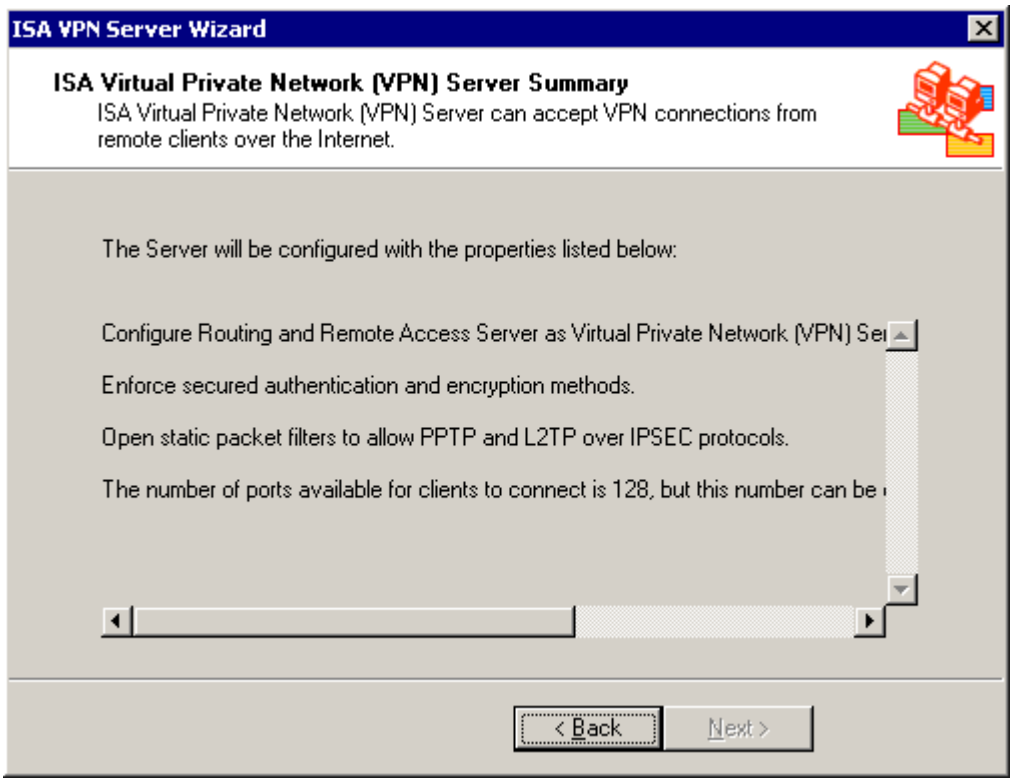
Caveat two: Your firewall can pass PPTP traffic, but not IPSec traffic. IPSec encrypts the packet headers and this breaks the Network Address Translation feature of ISA Server which needs to swap out addresses in the packet header. If you *have* to use IPSec, your only option is to configure a secure tunnel between two ISA Servers using L2TP.

## Configuring a VPN server to accept client connections




I was able to launch this wizard by right-clicking **Network Configuration** in my ISA Management console tree and selecting **Allow VPN Connections**. Running this wizard allows you to configure your ISA Server to accept incoming VPN connections from clients using PPTP and L2TP. Please note that while your ISA Server can accept *incoming calls* using IPSec, this is because there is no Network Address Translation involved. IPSec encrypts packet headers, which breaks NAT. IPSec works on incoming calls because NAT isn't used here.

Here is a summary of the changes the VPN Wizard made to my ISA Server:




- The wizard configured RRAS for me
- It automatically configures the VPN to try for the highest possible level of security when establishing a VPN session
- Necessary static packet filters are created
- Let's you know how many clients your VPN server accommodates (can be changed but is 128 by default)

In my case my RRAS service had not been started – the VPN Server wizard prompted me to start the service so it could finish configuring my settings:


## Configuring VPN tunneling between ISA Servers

Here are the steps for configuring the local VPN Server:

- In the ISA Management Console tree expand **Servers and Arrays** followed by the **Array** you are configuring the VPN for and then highlight and right-click **Network Configuration**. Choose **Setup Local ISA VPN Server** from the context menu.
- Name the local connection – ISA Server creates a VPN Connection with the format *localservername_remoteservername*
- Select the level of security: PPTP or L2TP over IPSec. You can also configure the server to try for L2TP first but drop down to PPTP if necessary.
- Indicate which servers can initiate communication. If you want the local server to be able to initiate communication then you need to provide some additional information about the remote server.
- Provide the remote addresses that your local VPN Server will be able to access
- Provide the address of the local VPN server
- Save the configuration file (.VPC file extension). This file is password protected – make sure you record your password in a safe place.

Here are the steps for configuring the remote VPN Server:

- In the ISA Management Console tree expand **Servers and Arrays** followed by the **Array** you are configuring the VPN for and then highlight and right-click **Network Configuration**. Choose **Setup Remote ISA VPN Server** from the context menu.
- When the wizard launches provide the location of the .VPC configuration file and enter the password.

- Your VPN server will be configured based-on the settings in the file. Review the settings before closing the wizard and accepting the changes.

## 7. Configure ISA Server for Network Load Balancing

Network Load Balancing (NLB) provides fault tolerance for firewall clients. You can make multiple ISA Servers appear to clients as a single ISA Server by using NLB to assign a virtual IP address to the internal NICs of the ISA server array. Clients send their traffic to the NLB virtual IP address and Windows 2000 Network Load Balancing decides which server to forward the traffic to.

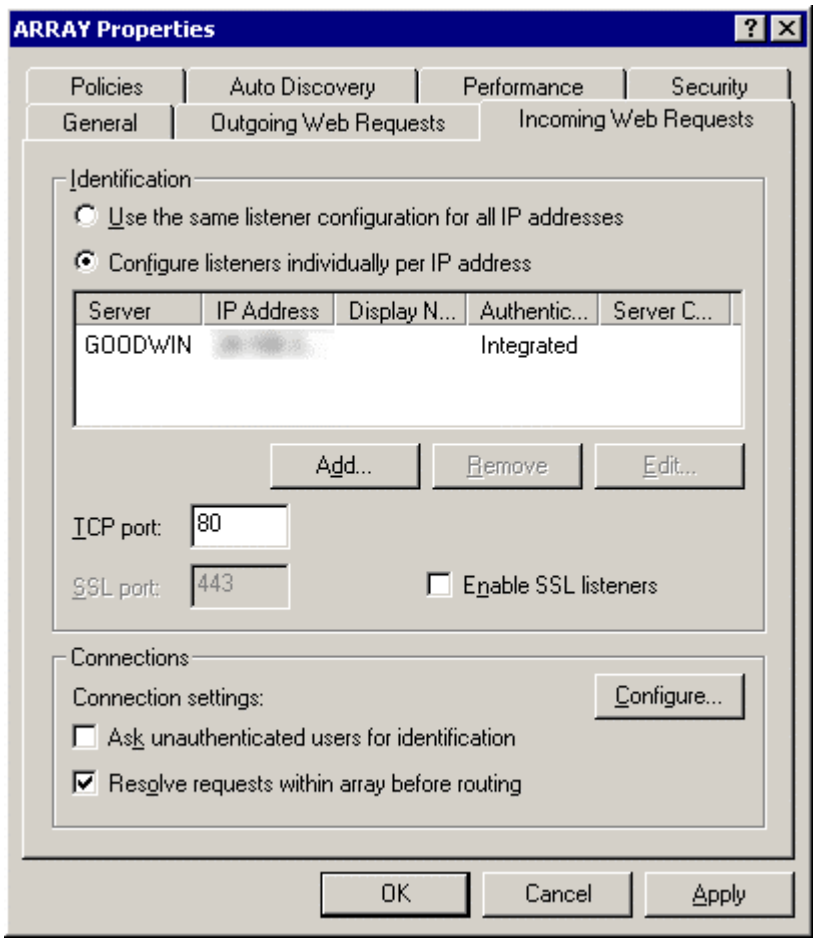
When you are configuring inter-array communication it is a *really bad idea* to use the load-balanced virtual IP address. Use the actual IP address of the ISA Server instead.

## 8. Configure ISA Server for CARP

### CARP basics

ISA Server uses Caching Array Routing Protocol (CARP) to provide load balancing and fault-tolerance for object caching across multiple ISA Servers. Microsoft's implementation also has the advantage of making sure that the same object is not duplicated across different servers. This is good in that it saves disk space. It's bad in that it can affect performance for clients if you don't configure CARP properly. Here are the gotchas to know about:

- Make sure you configure your array to resolve all requests internally before routing the request to the Internet. What this means is that if your ISA Server cannot find an object in its own cache, it checks to see if it exists in the cache of the other array members before retrieving it from the Internet. This helps prevent duplication of cached objects on different array members and helps out with network traffic.
- You must configure one listener on each array member otherwise attempts to resolve requests in the array will be ignored.




- Make sure you've provided the correct address for inter-array communication!! If you used the NLB virtual IP address you'll see some strange behavior here.
- Make sure you use proxy auto configuration scripts with Web proxy clients whenever possible. This allows clients to go directly to the correct ISA Server to retrieve a cached item (determined by using a hashing algorithm on the URL being retrieved) and prevent duplication of cached objects across different ISA Servers.

### Using the proxy auto configuration script

The proxy autoconfiguration file (.PAC file extension) makes Web browsers aware of the structure of your caching array. Your Web browser uses a hashing algorithm to break apart the URL. Because the browser knows where to go to retrieve cached objects, this speeds up things greatly on the client end. The address of your proxy auto config file which ISA Server generates is:

*http://array:8080/array.dll?Get.Routing.Script*

(Where array is the name of your array and port 8080 is the default but can be changed).

## Configure, Manage, and Troubleshoot Policies and Rules

### 1. Configure and secure firewall according to corporate standards

### Two types of policy in the Enterprise

- Enterprise level policy – can be used to allow or deny access to Internet resources and protocols.
- Array level policy – **deny only**. Policies can be set at the array level to further restrict Enterprise policy through denying access to resources/protocols.

You don't have to use array policies – this can be changed at any time. You can also choose to allow to use array policies on one array, but deny use of them on another.

### Access policies consist of these components

- Policy elements – settings that are used as part of rules (e.g. Destination Sets or schedules).
- Protocol rules – all protocols used by ISA Server must be defined here.
- Site and content rules – allows admins to specify which types of content and which sites are allowed or denied.


### Policy elements

- Bandwidth priorities – let an admin choose which connection receives priority over another. ISA Server bandwidth rules are based on the Quality of Service (QoS) protocol.
- Client address sets – when used in access policy rules, these are computers on the internal network. You can specify a computer name, IP address, or range of IP addresses
- Content groups – groupings of common file types and file extensions
- Destination sets – computers that are NOT on the internal network (one or more computers)
- Protocol definitions – can be pre-defined or user defined. (e.g. I use Yahoo! Messenger so I added a protocol definition for Yahoo! on TCP port 5555 inbound with no secondary connections)
- Schedules – use schedules to specify the dates and times when a rule is active (great for keeping janitorial staff from surfing naughty sites overnight)

### Default settings

By default ISA Server includes a site and content rule called "Allow All" – this rule allows access to all sites and content types. However, you will need to configure protocol rules to Internet access before users will be able to access the Internet. By default there are NO protocol rules installed.

## 2. Create and configure access control and bandwidth policies

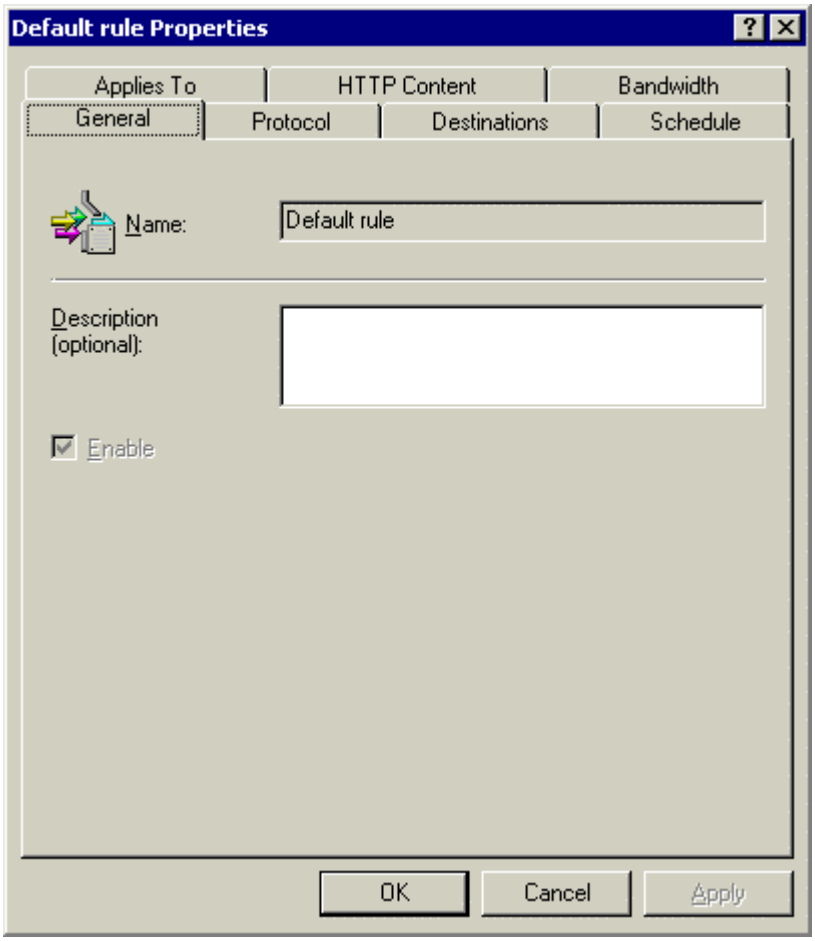
### How you configure your policies depends on your client type

Remember – you can only set policies by user-level for clients using the Firewall Client. If it's imperative that management be able to surf naughty Web sites but Joe Schmoe user cannot, then the client machines in the management OU should have the firewall client installed.

If you are trying to set access for SecureNAT and Web proxy clients, you can restrict them by content type, client address set, destination set, schedule, and protocol rules – but NOT user or group.

## Bandwidth, you say?

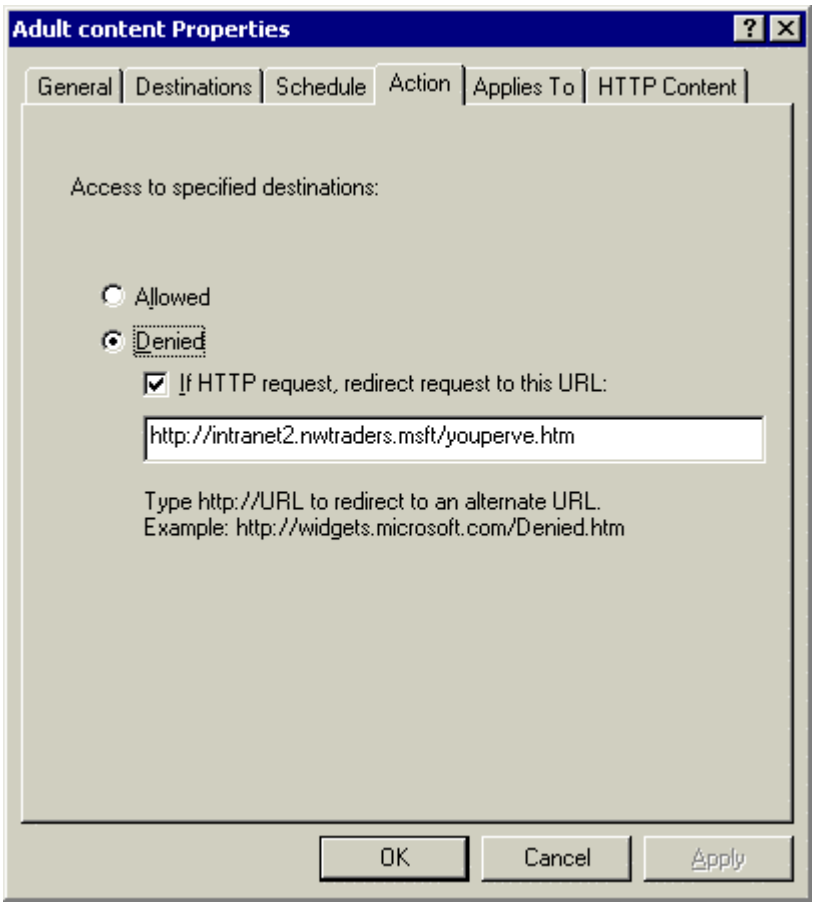
Bandwidth priorities are configured with a number between 1 and 200. The higher the number, the higher the priority. If an ISA Server is getting maxed out for bandwidth, it will continue passing packets for protocols that have a higher priority (e.g., IMAP4 at priority of 100) while dropping packets for protocols set with a low priority (e.g., Winamp Shoutcast at priority of 10). You can set different priorities for inbound and outbound traffic.



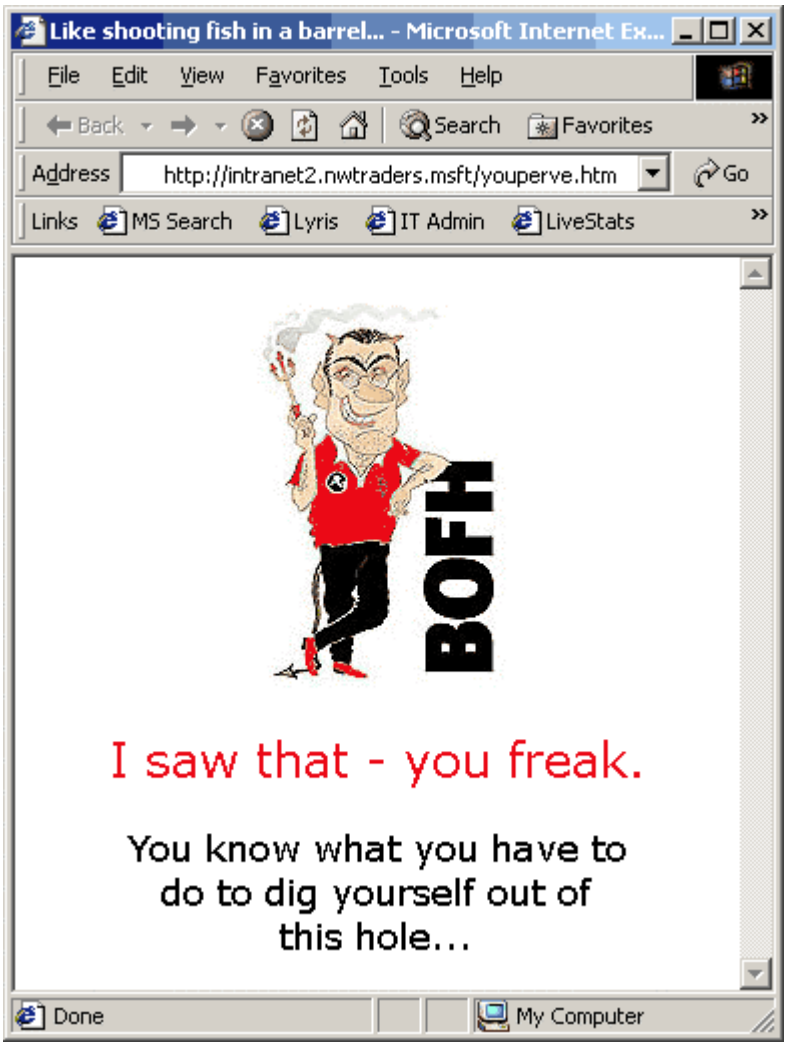

Bandwidth rules (properties show above) can be applied to client address sets, users and groups (firewall client only), protocols, destination sets, and HTTP content types. You can use scheduling in your bandwidth rules to set different bandwidth priorities for different times of the day.

## The fine art of slapping down a user

When you deny access to a particular Web site you have the option of rubbing a user's nose in it as shown in the following site and content rule I've created named "Adult content":



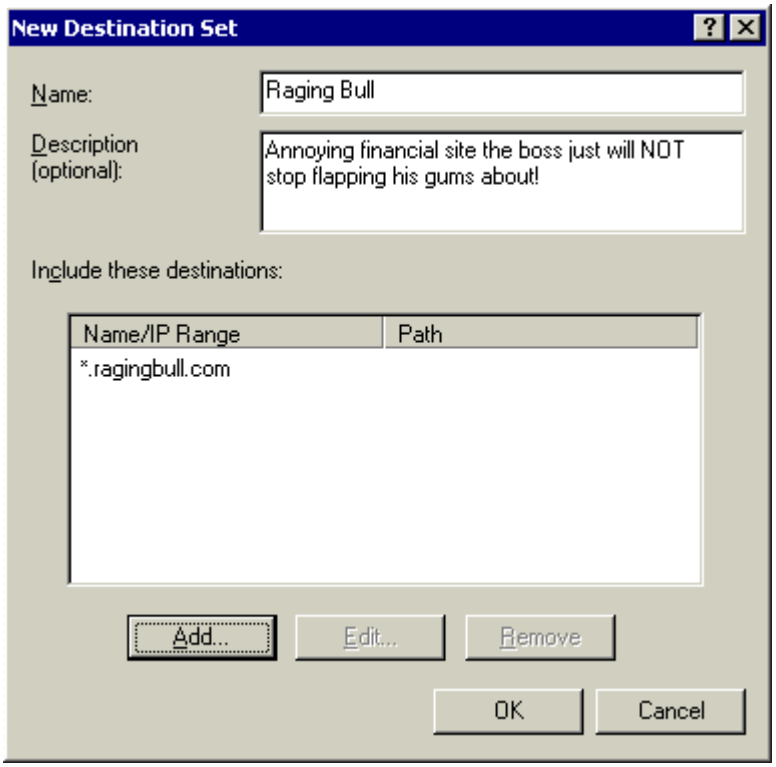

This rules includes destinations like sex.com, youngstuff.com, etc. Whenever a user tries to access any of these forbidden destination sets, their browser is redirected to the following page: http://intranet2.nwtraders.msft/youperve.htm. Said page berates them for attempting to surf a naughty site and lets them know where to pay the bribe if they want to keep this transgression out of their personnel file (as shown below).




* The BOFH and the above graphic are the copyrighted property of Simon Travaglia. If you haven't read the exploits of the BOFH then you just aren't living! Better go catch up on this right away and make sure you buy PLENTY of merchandise: http://www.theregister.co.uk/content/30/index.html

## Remember to create necessary policy elements FIRST

Policy elements are used in rules. Before you can create the rule, you have to create the policy elements it needs. For example, before you can create a site and content preventing users from surfing Raging Bull and discovering just how worthless their stock options are, you will need to create the appropriate policy element first – in this case a destination set. Once the destination set is created you can use it in a site and content rule.




## Available policy elements at the Enterprise level

- Schedules
- Destination Sets
- Client Address Sets
- Protocol Definitions

- Content Groups

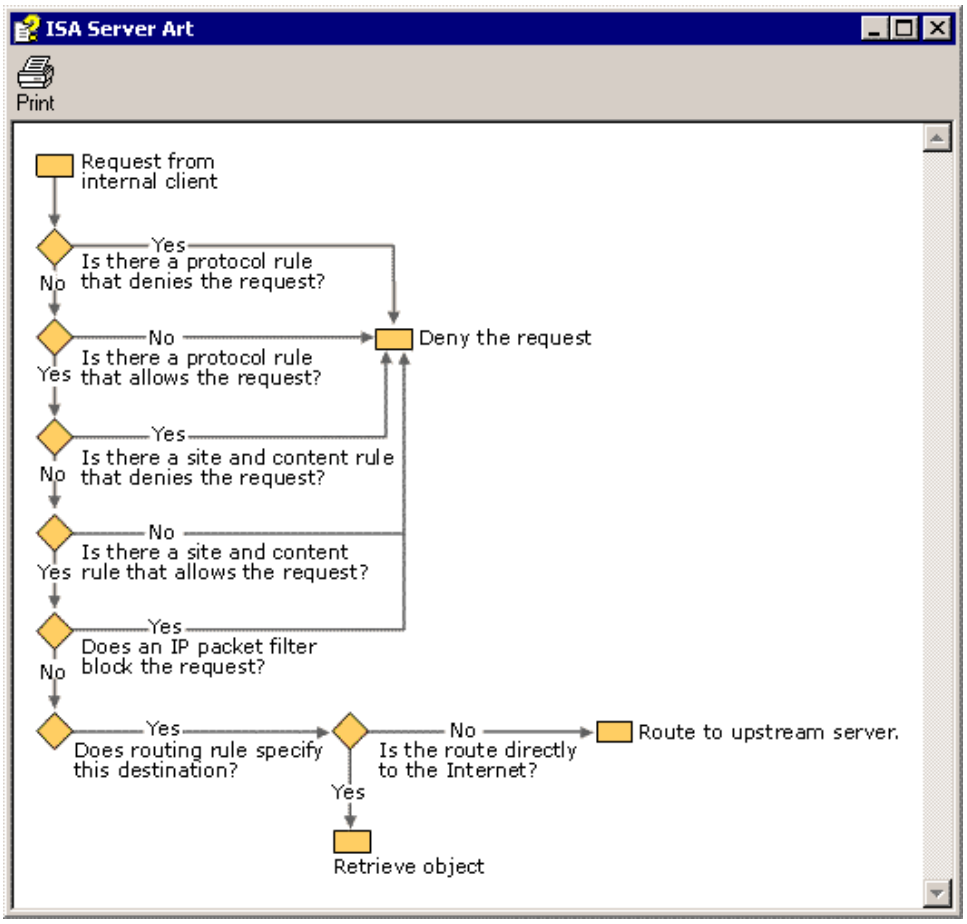
### Available policy elements at the Array level

- Schedules
- Bandwidth Priorities
- Destination Sets
- Client Address Sets
- Protocol Definitions
- Content Groups
- Dial-up Entries

## 3. Troubleshoot access problems

### The order rules are processed in

I've taken a screen shot from the help files in ISA Server that explain the order Rules are processed in:




Memorize how this chart works – if you understand this process you can troubleshoot any question that involves problems with rules on the exam.

## Don't worry about the order of protocol rules

With protocol rules, rules that deny a protocol are processed **before** rules that allow the same protocol. If you have two rules, one that allows ICQ and one that denies ICQ, ICQ will be denied regardless of what order you put the rules in. Don't get fooled by the order of the rules in an exam exhibit – it doesn't matter.

For example, you have to allow management (the bums) unrestricted Web access but ordinary users are not allowed HTTP access. Period. You discover that while ordinary users are prevented from surfing the Web, management is as well. Upon

investigating you find that you've blocked "Domain Users" from the HTTP protocol and that the affected managers also belong to the "Domain Users" group. You'll have to reshuffle users amongst your groups a bit to fix this.

### The order of Routing and Web Publishing Rules DOES matter

Both Web Publishing and Routing rules work kind of like the protocol binding order on your network adapter. The items nearest the top are processed first. Use the **move up** and **move down** buttons to sort your routing rules into the order that works for you.

## Deploying, Configuring, and Troubleshooting the Client System

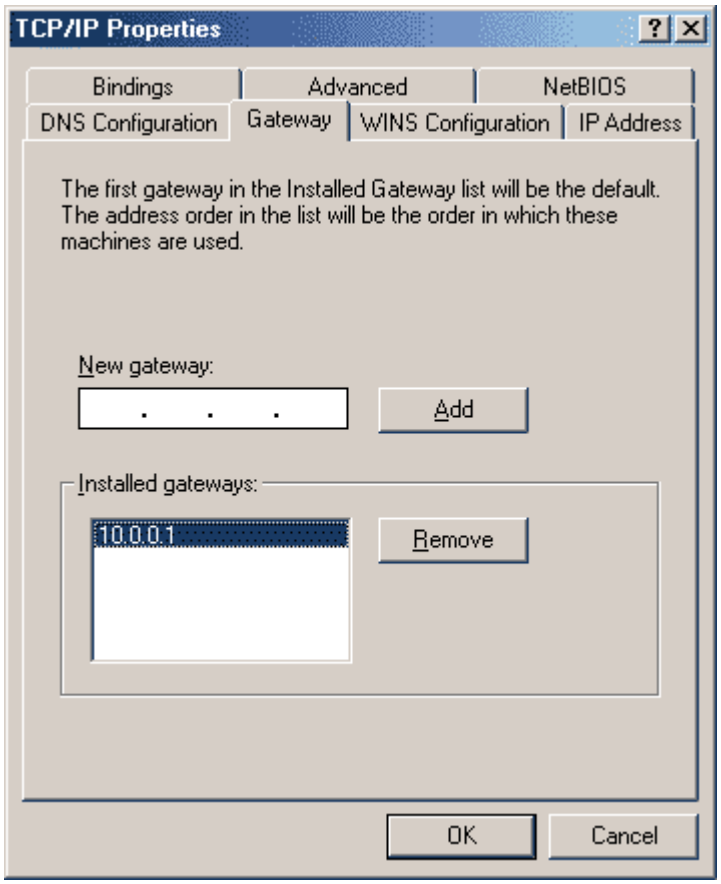
### 1. Plan client deployment

| Organizational Requirement | Supported by Firewall Client | Supported by Web Proxy Client | Supported by SNAT Client |
|---|---|---|---|
| User-level authentication | Yes | No | No |
| All systems run Windows 95OSR2/98/Me, Windows NT 4.0, and Windows 2000 | Yes | Yes (if browser supports HTTP version 1.1) | Yes |
| Non-Windows systems using TCP/IP protocol | No | Yes (if browser supports HTTP version 1.1) | Yes |
| No additional software needed to deploy | No | Yes (if browser supports HTTP version 1.1) | Yes |
| Improved Web request performance | No | Yes (if browser supports | No |

| | | | |
|---|---|---|---|
| | | HTTP version 1.1) | |
| Non HTTP TCP requests and requests using UDP protocol | Yes | No | Yes |
| Publishing servers from behind the corporate firewall | No | No | Yes |

## 2. Configure and troubleshoot SecureNAT clients

No special software is needed to turn a client system into an SNAT Client. In a non-routed environment, simply set the default gateway of the client system to point to internal IP address of the ISA Server (as seen below). In a routed environment, point the client systems to the appropriate router and set your routers to forward Internet traffic to the internal IP address of the ISA Server or load-balanced server array.




Use SNAT when all users have the same level of access to the Internet, when you are publishing a server to the Internet, when limited resources do not allow installation of the firewall client on client systems, and for clients running something other than a 32-bit Windows operating system (e.g., Mac, Linux, Unix, and Be).

SNAT will transparently pass along all client requests to the firewall and also to the caching service if objects are being requested that can be cached.

DNS is needed to resolve names for SNAT clients. If you won't be accessing any resources on the internal network then pointing the clients to an external DNS server is fine (you will need to configure a protocol rule for this). You should deploy DNS servers internally if internal resources are being accessed (a DNS protocol rule is not

needed for internal DNS servers). Many admins prefer to configure their internal DNS Servers as forwarders (if you can't configure your DNS as a forwarder, chances are that the DNS is configured with the root "." domain). This means you won't have to touch your client configuration on your S-NAT clients and that your internal servers will develop a respectable cache.

## 3. Configure and troubleshoot clients using Firewall Client

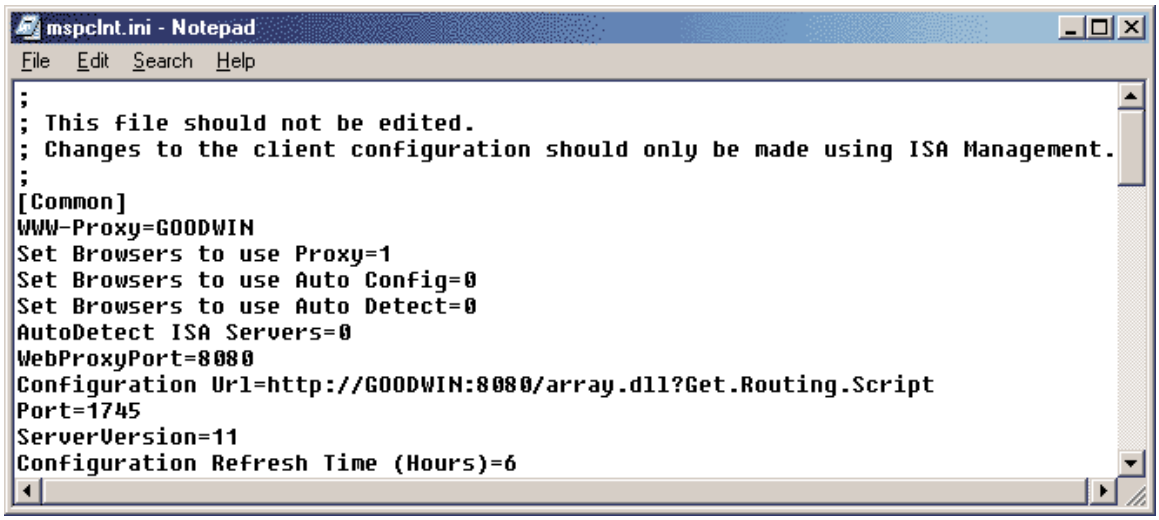
ISA Server includes firewall client software that can be installed on client computers running 32-bit Microsoft Windows operating systems. The client software is used only when there is a need to restrict access to TCP or UDP resources by user or by group.

The firewall client can be installed from a network share (created by default when ISA Server is installed) or from a Web location. The address for the network share is *isaserver*\\mspclnt**setup.exe**. (Replace *isaserver* with your server name.)

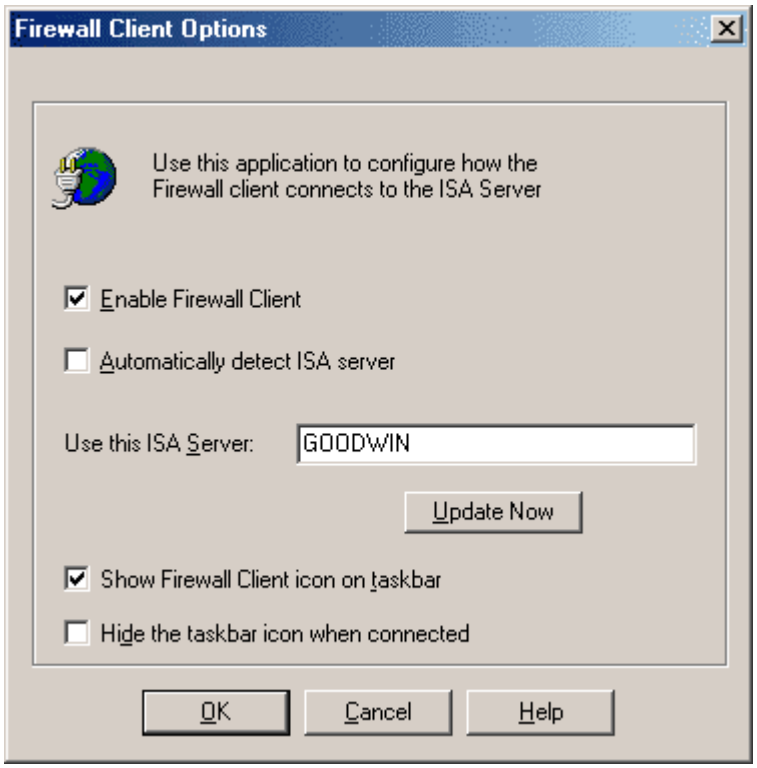
To install from a Web location you need to copy the **default.htm** and **setup.bat** files from the \Program Files\Microsoft ISA Server\Clients\WEBINST folder to a Web server and then connect to the web server from a browser on a client system and load **default.htm**. Next click on the **ISA client software** link. All this does is download a file called **setup.bat** which contains one line pointing to the share in the previous paragraph: *isaserver*\mspclnt\setup.exe. (Replace *isaserver* with your server name.)

Finally, you have the choice of using Active Directory to publish or assign the firewall client software to Windows 2000 clients. Simply assign the **MS_FWC.msi** installer package which is found in the \isa\clients directory of the ISA Server CD to the appropriate OUs.

Once the client is installed no additional configuration is needed. Whenever the client system is started it will connect to the ISA Server and download a new copy of a file called **mspclnt.ini** – the contents of this file are controlled by the ISA Server. By default this file will refresh itself every six hours as well.




You can configure which ISA Server your client software connects to using the GUI tool provided by Microsoft:

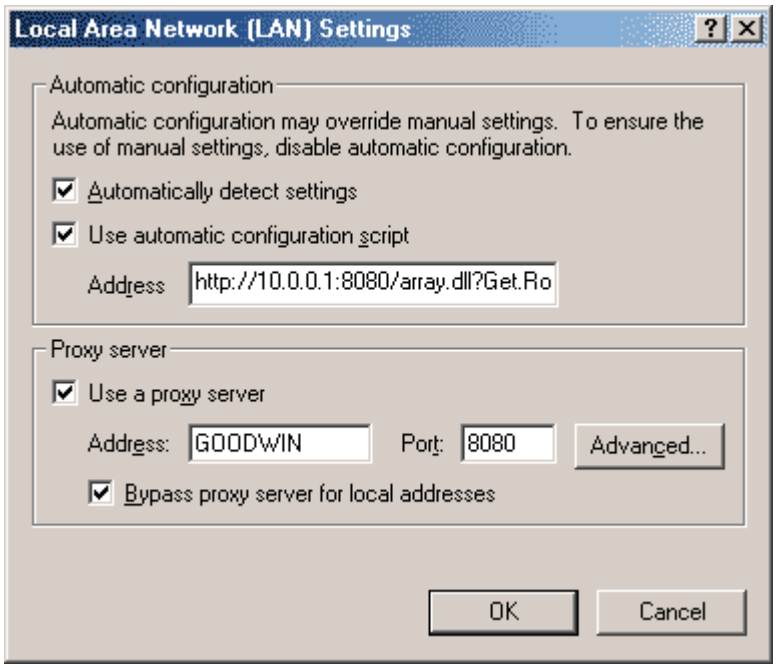



If you need to configure winsock specific settings for applications you are running, you can do so using a file called **wspcfg.ini**. This file was used to publish servers from behind a firewall with Proxy Server 2.0. You do NOT need to do this with ISA Server as any resources published from behind the firewall should be published as SecureNAT (SNAT) clients.

**Never** install the firewall client on the ISA Server itself or you'll wind up with a large mess on your hands.

## 4. Configure client's Web browser for HTTP proxy

Web Proxy Client settings are configured through the Web browser on client systems. The dialog used to configure settings for Internet Explorer 5.5 is shown below:




You can access the settings for Internet Explorer by choosing **Start** > **Settings** > **Control Panel** > **Internet Options** > **Connections** > **LAN Settings**.

When **Automatically detect settings** is selected, IE will automatically sniff out information published by the ISA server and configure itself accordingly (this works on DHCP and DNS clients using the WPAD.DAT file).

The Web proxy client provides the best performance for internal clients making Web requests. If you are deploying a Firewall Client, you can have it configure your Web Proxy Client settings on the client system for you.

## 5. Configure SOCKS Version 4 Clients

Although you will probably not be tested on this, it is important to note that ISA Server includes a SOCKS4 Application Filter that can be used to pass SOCKS traffic through the firewall on port 1080. You can either enable or disable this filter and change the port it operates on, but you cannot set permissions by user or by group – it's all or nothing.

## 6. Troubleshooting ISA Client Issues

Many problems with ISA Clients are often related to improper LAT configuration, so consider whether your LAT is correctly configured before you engage in extended troubleshooting.

*Can you access internal resources on the network?* If yes, then your TCP/IP connectivity is probably not an issue. If no, check your connectivity and TCP/IP configuration.

*Can you access Web-based resources?* If yes, your Web Proxy settings are OK. If not, check your Web Proxy settings and make sure ISA Server is configured to pass HTTP Proxy traffic.

*Can you access the Internet using Winsock-based applications using the Firewall client?* If no, check to make sure Firewall Client is enabled and pointed to the correct ISA Server or Array. Also check ISA Server to make sure access is allowed to the proper protocols and user has permission to access them.

*Can you access the Internet using socket-based applications through SNAT?* If not, did you configure your default gateway properly? If you can connect to internal resources, your TCP/IP connectivity is probably alright. Are the proper protocol rules setup in ISA Server?

*I've configured my Web Proxy Clients and now I can't connect to Internet resources.* Did you enter the address of the ISA Server properly? Did you enter the correct port (8080 by default)? Do your access rules permit HTTP traffic?

# Monitoring, Managing, and Analyzing ISA Server Usage

## 1. Monitor security and network usage using logging and alerting

### Logging overview

There are three types of logs:

- Firewall service logs – records communication through the Firewall service
- Packet filter logs – records packet traffic through the ISA Server computer
- Web proxy service – records communications using the Web Proxy service

Three different log formats:

- ISA format – only use with applications that can interpret ISA Server log data. Unselected fields are logged using a dash character.
- ODBC database – save logs to either an Access or SQL database
- W3C format – use when compatibility is needed with applications that support the W3C logging format. Does not log unselected fields (saves space when smaller log files are needed).

## Logging to a SQL database

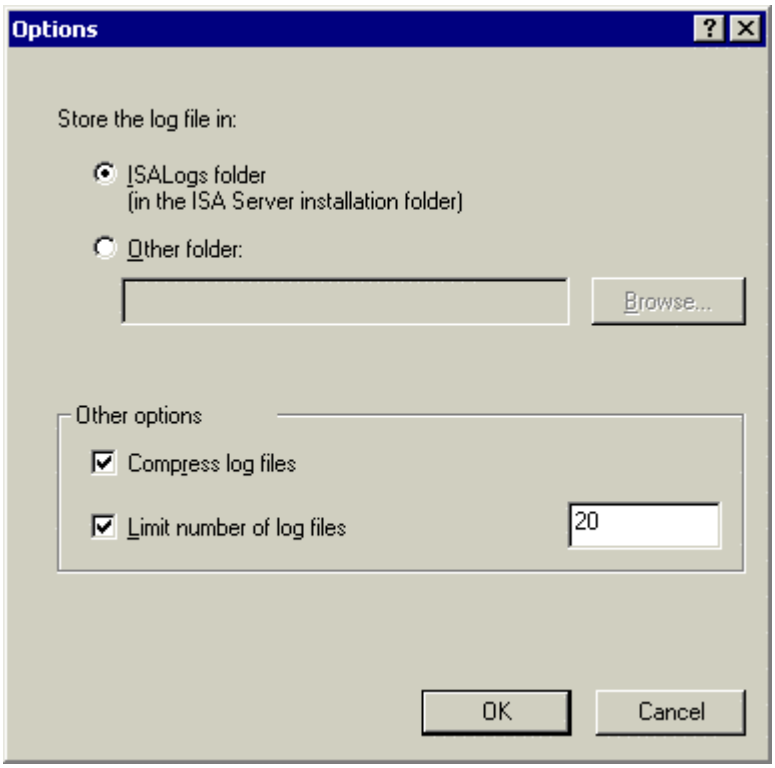
You can log ISA Server data to a SQL database if you really want to. MS has included the following scripts with ISA Server for defining service log tables:

- FWSRV.SQL – defines the FirewallLog table for the Firewall Service
- PF.SQL – defines the PacketFilterLog table
- W3PROXY.SQL – defines the WebProxyLog table for the Web Proxy Service

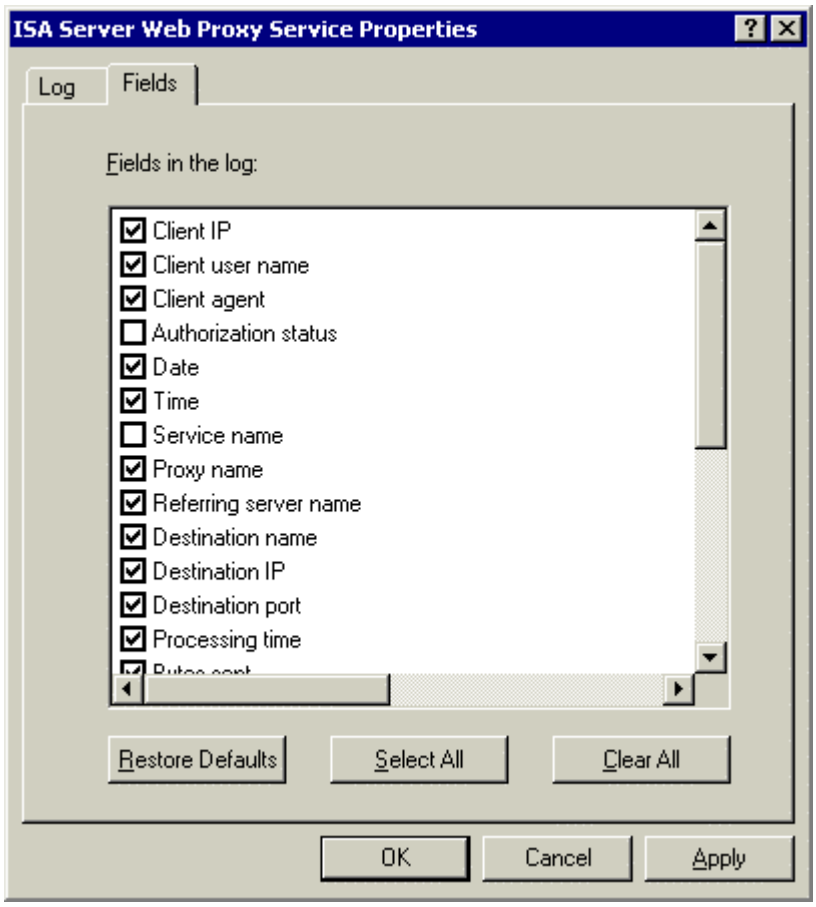
## Troubleshooting log headaches

You can wind up with a LOT of very large log files in a hurry, especially in an enterprise environment with thousands of users. Watch for the following problems:

- Too many log files – you can limit the number of log files in a directory (shown below). When the limit is reached, older files are deleted.




- Log files too large – you can compress your log files (shown above) or limit the number of fields you log (shown below)




- Too much disk activity – if your users are reporting that Internet access is slower than sin, go into **perfmon** and check out your logical and physical disk counters. If your disk activity is going through the roof, you need to move your log files to a different PHYSICAL disk drive.

## 2. Troubleshoot problems with security and network usage

### Configuring Intrusion Detection

ISA Server looks for the following types of packet-level intrusions:

- All ports scan attack
- IP half scan attack


- Land attack
- Ping of death attack
- UDP bomb attack
- Windows out-of-band attack

ISA Server looks for the following types of application level attacks (POP and DNS):

- DNS hostname overflow
- DNS length overflow
- DNS zone transfer from privileged ports
- DNS zone transfer from high ports
- POP buffer overflow

### Configuring Alerts

When an alert is generated, you have the following options:

- Send an e-mail message
- Run a program
- Generate event log entry
- Start selected ISA Server services
- Stop selected ISA Server services

## 3. Analyze ISA Server performance by using reports

### About Reports

ISA Server allows administrators to analyze server logs and build reports that can be viewed in a Web browser. There are five different types of reports:

- Application usage – based on Firewall service logs. Lets admins view usage by traffic, users, applications, and destinations. Used to determine network capacity and bandwidth policies.
- Security – based on Firewall, Packet Filter, and Web Proxy Service logs. Lists attempts to crack your network.

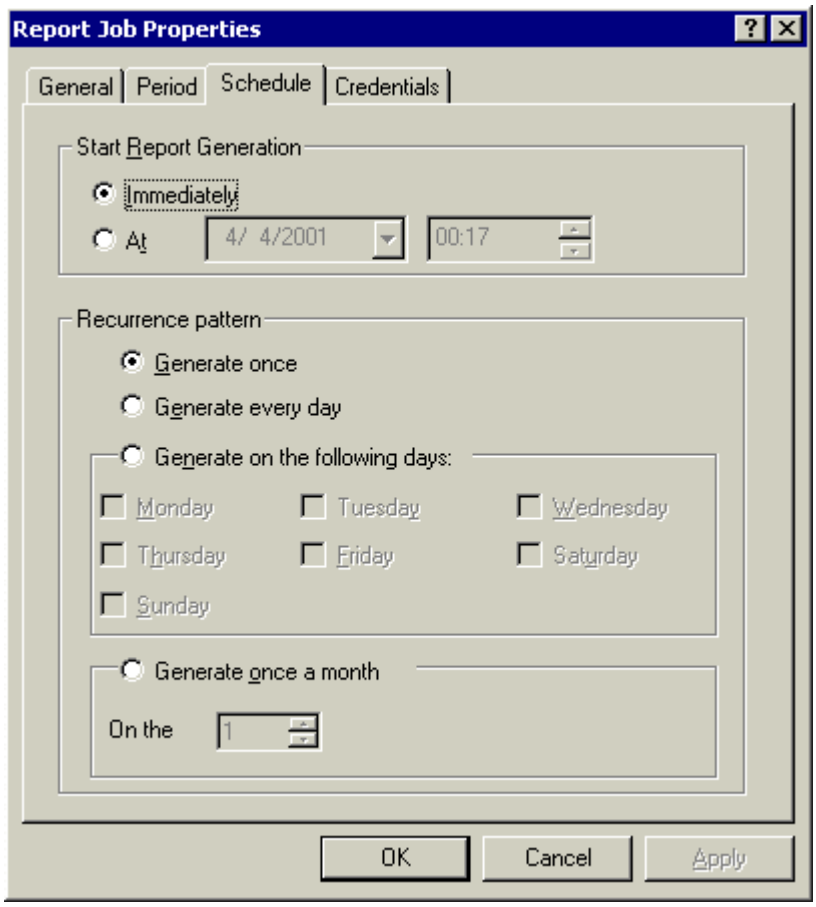
- Summary – based on Firewall, Packet Filter, and Web Proxy Service logs. Includes a set of reports displaying network traffic sorted by application.
- Traffic/utilization – based on Firewall and Web Proxy Service logs. Used for troubleshooting network traffic issues and for capacity planning. Can break down traffic by protocol, cache hit ratio, errors, etc.
- Web usage – based on Web Proxy Service logs. Lists top sites, users, and browsers.

## Configuring Reports

The first step to creating reports is to configure *log summaries.* In ISA Management under the console tree select **Monitoring Configuration**, then right-click **Report Jobs** and select **Properties** from the context menu. Make sure that **Enable daily and monthly summaries** is checked.

Next, we have to create a *report job* (right-click on **Report Jobs** in the consoled tree and select **New** | **Report Job**). There are five steps to creating the report job:

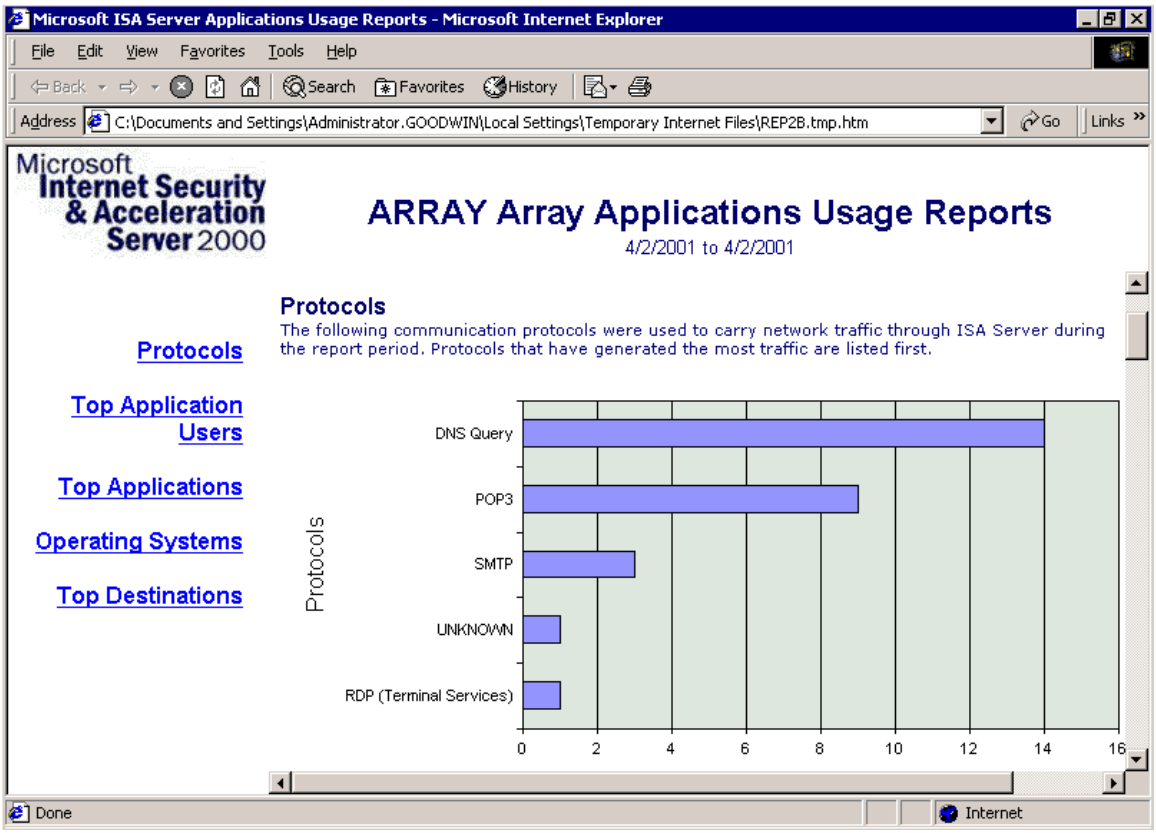
- Give the report a name
- Give it a duration
- Specify when it is generated (shown below)
- Specify the recurrence (shown below)
- Present user credentials (must be a local admin on the ISA Server computer and have permission to launch DCOM objects)




Remember that even if you choose to generate a job immediately, it could take a while for ISA Server to summarize the log files and create the report – be patient. Also worth mentioning – since reports are created for log summaries, and log summaries are created daily at 12:30 AM, you will have to wait until after that time on the first day to be able to be able to view any report.

## Viewing Reports

In the console tree open up **Monitoring** | **Reports**, and then double-click on the report you want to view – it will open in a Web browser (sample shown below).




## Saving Reports

Reports can be saved in either HTML (.htm) format or as an Excel (.xls) workbook.

## Using Performance Monitor

A bunch of performance objects appear in Performance Monitor after you install ISA Server – they fall into the following categories:

- Bandwidth control – used to check out assigned and actual bandwidth in order to detect connection related bottlenecks
- Firewall service – used to determine active sessions and server usage
- Packet filter – can monitor all packet filtering activity in real-time

- Server cache – mainly used to monitor the effectiveness of your caching. If you're seeing too many cache hit miss errors, you need to tweak your caching or set the content pre-fetching more aggressively.
- Web proxy service – used to monitor total number of users, and transfers between local and remote ISA Servers.

## 4. Optimize ISA Server performance

### Quick and dirty ways to make your ISA Servers run faster

- When running an array, adding more array members adds more capacity and reduces the strain on existing array members
- Two words: more RAM. ISA Server is RAM intensive – make sure you feed your ISA Servers lots and lots of physical memory
- Separate your cache from your system disk for better performance (the same goes for your logs)
- Adding more disks to a RAID array improves disk performance
- Reduce the amount of data being logged if large log files/disk performance is an issue
- Set your active caching to aggressively cache content during off-peak hours when HTTP traffic during business hours becomes an issue.
- Use chained and distributed caching (CARP) to balance the load among servers
- Installing caching servers in branch offices and chain them to the array in your head office when HTTP traffic over WAN links is a concern.

### Configuring caching to improve performance

Using caching allows ISA Server to store a local copy of objects retrieved from the Internet. When another user requests the same object, ISA Server first checks to see if the item exists in its cache and if it is fresh enough. If a current version of a requested object is found in ISA Server's cache, the object is returned from there instead of being retrieved from the Internet. This has the following benefits:

- It reduces the amount of traffic on an organization's Internet connection
- It accelerates Internet requests for users. Having an object returned from cache is many times faster than having it returned from the Internet.

There are three types of caching to configure in ISA Server:

- *HTTP* – you can define the default properties of cached HTTP objects here including their Time To Live (TTL). A shorter TTL means fresher content. A longer TTL places less burden on the outbound Internet connection (important if high traffic is an issue)
- *FTP* – your only options here are to enable caching of FTP objects and specify the TTL. The default TTL is 24 hours (1440 minutes).
- *Active caching* – this is whack. When Active Caching is enabled ISA Server automatically keeps track of which objects are most popular and pre-fetches them from the Internet guaranteeing that there is always a fresh copy in the cache. Setting Active caching to retrieve objects frequently provides the best client performance. Setting Active caching to retrieve objects less frequently provides the best network performance.

Special thanks to Sean McCormick for contributing this Cramsession, and Dr. Tom Shinder, co-author of

Configuring ISA Server 2000: Building Firewalls for Windows 2000
(Syngress Publishing), for providing a technical edit of this material.

To send feedback to Sean, please post a message labelled "Attention Cramsession Author" here:

ISA Server 2000 Forum