



Microsoft 70-227

**Microsoft Internet Security  
and Acceleration Server 2000**

Study Guide  
DEMO Version

Copyright (c) 2003 Chinatag LLC. All rights reserved.

## **Important Note Please Read Carefully**

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

## **Study Tips**

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

## **Latest Version**

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to [feedback@chinatag.com](mailto:feedback@chinatag.com).

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team  
Chinatag LLC.

## TABLE OF CONTENTS

### List of Tables

### Introduction

## 1. Overview and Installation Preparation

1.1 ISA Server Modes and Architecture

1.2 Windows 2000 Integration

1.3 ISA Server Features

1.4 ISA Server Firewall Overview

1.4.1 Filtering Techniques

1.4.1.1 IP Packet Filtering

1.4.1.2 Circuit Level or Protocol Filtering

1.4.1.3 Application Filtering

1.4.2 ISA Server Intrusion Detection Capabilities

1.4.3 Bandwidth, Virtual Private Networking and Secure Publishing

1.5 ISA Server Caching Overview

1.5.1 Forward and Reverse Web Caching with ISA Server

1.5.2 Scheduled Caching and Active Caching

1.5.3 Hierarchical Caching

1.5.4 Cache Array Routing Protocol (CARP)

1.6 Preparing to Install ISA Server

1.6.1 ISA Server Mode Considerations

1.6.2 Array Requirements

1.6.3 Internet Connectivity Considerations

1.6.4 Network and Topology Considerations

## 2. Installing ISA Server

2.1 Structuring the Local Address Table (LAT)

2.2 ISA Server Default Configuration

2.3 Upgrading Proxy Server 2.0 to Microsoft ISA Server

2.3.1 Upgrading the Proxy Server computer to an Array of ISA Server Computers

## 3. Internet Access Configurations



- 3.1 Configuring Secure Internet Access for Client Computers
  - 3.1.1 Firewall Client Configurations
  - 3.1.2 SecureNAT Client Configurations
  - 3.1.3 Web Proxy Client Configurations
- 3.2 Configuring Dial up Entries in ISA Server
- 3.3 Configuring Dial on Demand in ISA Server
- 3.4 Configuring Automatic Discovery for ISA Server Clients
- 3.5 Starting and Stopping ISA Server services
- 3.6 Troubleshooting Errors in client and Dial up Configurations

## **4. Internet Security and Internet Acceleration Configurations**

- 4.1 Creating and Configuring Access Policies for Internet Security
  - 4.1.1 Defining an Access Policy
    - 4.1.1.1 Client Authentication
    - 4.1.1.2 Utilizing the Getting Started Wizard to Create an Access Policy
    - 4.1.1.3 Setting ISA Server System Security
  - 4.1.2 Defining Policy Elements
    - 4.1.2.1 Schedules
    - 4.1.2.2 Destination Sets
    - 4.1.2.3 Client Address Sets
    - 4.1.2.4 Client Users and Groups
    - 4.1.2.5 Protocol Definitions
    - 4.1.2.6 Content Groups
  - 4.1.3 Creating and Configuring Protocol Rules in ISA Server
  - 4.1.4 Creating and Configuring Site and Content Rules in ISA Server
  - 4.1.5 Creating and Configuring IP Packet Filters
    - 4.1.5.1 IP Packet Filter Methods
  - 4.1.6 Configuring ISA Server for Intrusion Detection
- 4.2 Accelerating Internet Connectivity via the ISA Server Cache
  - 4.2.1 Defining a Cache Policy and Creating Routing Rules
    - 4.2.1.1 Routing Rules
    - 4.2.1.2 ISA Server Processing Procedure for Caching Objects
  - 4.2.2 Configuring Cache Properties
    - 4.2.2.1 Cache Drives
    - 4.2.2.2 Configuring which Content ISA Server should Cache
    - 4.2.2.3 Expiration Policy
    - 4.2.2.4 Configuring Caching in ISA Server
  - 4.2.3 Creating and Configuring Scheduled Cache Content Downloads

## **5. Configuring Enterprise Policies, ISA Server Arrays and VPN Connectivity**



- 5.1 Configuring Enterprise Policy Settings
  - 5.1.2 Backing up and Restoring Enterprise Configuration Parameters
- 5.2 Creating and Configuring Arrays
  - 5.2.1 Promoting Standalone Servers to Array Members
  - 5.2.2 Array Membership, and Backing up and Restoring Array Configuration
  - 5.2.3 ISA Server Fault Tolerance Feature
  - 5.2.4 Configuring CARP
- 5.3 ISA Server and VPNs
  - 5.3.1 The ISA Server VPN Configuration Wizards

## **6. Server Publishing with ISA Server**

- 6.1 ISA Server Publishing Policy Rules
- 6.2 Publishing Web Servers
- 6.3 Publishing Mail Servers

## **7. ISA Server and H.323 Gatekeeper**

- 7.1 An Introduction to the H.323 Gatekeeper
- 7.2 Endpoints and Well-Known Aliases
- 7.3 Installing H.323 Gatekeeper
- 7.4 H.323 Call Routing Rules

## **8. Monitoring, Optimizing, Tuning and Troubleshooting ISA Server and its Performance**

- 8.1 ISA Server Alerts
- 8.2 ISA Server Logs and Reports
  - 8.2.1 The Firewall and Web Proxy Service Logging Fields
  - 8.2.2 The Packet Filter Service Logging Fields
  - 8.2.3 ISA Server Reports
- 8.3 Tuning ISA Server Performance and ISA Server Cache Performance
- 8.4 Configuring Effective Bandwidth, Bandwidth Priorities and Bandwidth Rules
  - 8.4.1 Effective Bandwidth
  - 8.4.2 Bandwidth Priorities

8.4.3 Bandwidth Rules

8.5 ISA Server Performance Objects and Counters

8.6 Troubleshooting Tools

8.7 Troubleshooting Techniques

## **LIST OF TABLES**

TABLE 2.1:	Installation Methods of ISA Server
TABLE 8.1:	Firewall Service and Web Proxy Service Logging Fields
TABLE 8.2:	Packet Filter Service Logging Fields

# 70-227 MCSE Microsoft Internet Security and Acceleration Server 2000

**Exam Code: 70-227**

## **Certifications:**

**Microsoft Certified Systems Engineer (MCSE)**

**Elective**

## **Prerequisites:**

Knowledge on Windows 2000 Operating System and features, and implementing TCP/IP features would be advantageous.

## **About This Study Guide**

This Study Guide is based on the exam questions for the 70-227 MCSE: Microsoft Internet Security and Acceleration Server 2000 exam. It presents all the information necessary to pass the 70-227 Microsoft Internet Security and Acceleration Server 2000 exam, and is detailed on the particular proficiencies examined in the exam. The Microsoft Internet Security and Acceleration Server 2000 exam is designed to test your knowledge on installing and configuring ISA Server 2000, and configuring the different ISA Server features. The information provided in this Study Guide is specific to the 70-227 examination, and does not symbolize a complete reference work on the any other areas covered by the MCSE series of exams.

The following topics are covered in this Study Guide: ISA Server Features, ISA Server Modes and Architecture, Windows 2000 Integration, ISA Server Firewall Overview, ISA Server Caching Overview, Preparing to Install ISA Server, Installing ISA Server, ISA Server Default Configuration, Configuring Secure Internet Access for Client Computers, Configuring Dial up Entries in ISA Server, Configuring Dial on Demand in ISA Server, Creating and Configuring Access Policies for Internet Security, Accelerating Internet Connectivity via the ISA Server Cache, Configuring Enterprise Policy Settings, Creating and Configuring Arrays, ISA Server and VPNs, ISA Server Publishing Policy Rules, Publishing Web Servers, Publishing Mail Servers, ISA Server and H.323 Gatekeeper, ISA Server Alerts, ISA Server Logs and Reports, Tuning ISA Server Performance and ISA Server Cache Performance, ISA Server Performance Objects and Counters, and Troubleshooting Tools and Strategies

## **Intended Audience**

This Study Guide is targeted specifically for those persons wanting to acquire knowledge on designing, implementing and supporting Internet Security and Acceleration Server 2000 who desire to complete the 70-227 Microsoft Internet Security and Acceleration Server 2000 exam. The information in this Study Guide is specific to that exam. It is not a complete reference work on the other exam topics relating to the MCSE qualification. Although our Study Guides are aimed at new comers to the world of IT, the concepts dealt

with in this Study Guide are complex. Knowledge on Windows 2000 Operating System and features, and implementing TCP/IP features would be advantageous.

### **How To Use This Study Guide**

To benefit from this Study Guide we recommend that you:

- Study each chapter carefully until you fully understand the information. This will require regular and disciplined work. Where possible, attempt to implement the information in a lab setup.
- Be sure that you have studied and understand the entire Study Guide before you take the exam.

Good luck!

# 1. Overview and Installation Preparation

ISA Server is an **Internet firewall** and **Web caching server** that is built on the Windows operating system (OS). ISA Server can be implemented and set up as a Web cache server or firewall. It can also be set up as both a Web cache server and firewall (integrated mode). The Web cache server allows an organization to supply enhanced Web access to clients by supplying objects locally. ISA Server's multilayer firewall secures an enterprise's network resources and at the same time provides **enhanced performance, scalability and manageability**.

ISA Server is available in two editions, the ISA Server Standard Edition and the ISA Server Enterprise Edition. ISA Server's security, caching and management attributes are identical for each edition though. This study guide concentrates on the ISA Server Enterprise Edition.

- **ISA Server Standard Edition:** This edition operates as a standalone ISA Server computer. It offers local policy level support, with support for 4 CPUs. ISA Server Standard Edition does however supply superb performance for an enterprise's network resources.
- **ISA Server Enterprise Edition:** This edition supports multiserver arrays with centralized management. ISA Server Enterprise Edition was designed with the purpose of supporting Internet environments that handle huge quantities of traffic flow. This edition too provides enterprise and array policy level support, server clustering via arrays and includes fault tolerant features. ISA Server Enterprise Edition has no hardware scalability limit.

## 1.1 ISA Server Modes and Architecture

As mentioned previously, ISA Server can be installed in firewall, cache, or integrated (firewall and cache) mode.

- **Internet Firewall:** In this implementation strategy, ISA Server is installed as a dedicated firewall. It performs like a gateway to the Internet for internal clients, and enforces the enterprise's security policy for all traffic flowing through it. It determines which computers internal clients can access on the Internet, and also controls access to the enterprise's network. ISA Server is transparent to users and applications moving through it.
- **Secure Publishing Server:** An ISA Server computer can be configured to manage external client requests for the internal publishing server. In this manner, ISA Server makes it possible for services to be securely published to the Internet.
- **Forward Web Cache Server:** When ISA Server acts as a forward Web cache server, it manages a centralized cache consisting of frequently requested Internet content. The cache can be accessed by Web browsers of the secure or private network which in turn enhances browser performance, while decreasing Internet connection bandwidth utilization and response time.
- **Reverse Web Cache Server:** Here, ISA Server manages client requests for Web content held in its cache. Any requests that the cache is unable to fulfill, ISA Server transmits to the Web server.
- **Integrated Firewall and Web Cache Server:** ISA Server can be installed as an integrated firewall and Web cache server. In this mode, ISA Server supply both fast and secure Internet connections.

ISA Server operates at different communication layers to secure the network. ISA Server performs packet filtering at the packet layer, by inspecting inflowing and out flowing traffic. Once traffic is permitted to move over the packet layer, it is forwarded to the Firewall and Web proxy services. The rules of ISA Server are then applied to the requests. ISA Server protects the following clients:

- **Firewall clients:** A firewall client is a computer running Firewall Client software. Any firewall client requests for objects are transmitted to the Firewall service residing on the ISA Server computer. The Firewall service decides whether to permit or deny the request. Firewall client requests for HTTP objects are forwarded to the Web Proxy service who could serve the object, or cache the object requested.
- **SecureNAT clients:** A SecureNAT client is a computer that does not have Firewall Client software running. Any SecureNAT client requests for objects are initially transmitted to the NAT driver. The NAT driver then translates the SecureNAT client's internal address to a global IP address that can be routed on the Internet. When the address translation is completed, the client request is transmitted to the Firewall service which then decides whether to permit or deny the request. As with firewall clients, all client requests for HTTP objects are forwarded to the Web Proxy service.
- **Web Proxy clients:** A Web Proxy client is a CERN compatible Web application. Web Proxy client requests are forwarded to the Web Proxy service who could serve the object from the cache, or cache the object requested.

## **1.2 Windows 2000 Integration**

ISA Server is an Internet firewall and Web caching server that is built on the Windows operating system (OS). The following Windows 2000 technologies can operate with ISA Server:

- **Active Directory:** ISA Server Enterprise Edition holds its policy and configuration data in Active Directory's directory store.
- **Administration Component Object Model (COM) Object:** ISA Server supply access to the rules engine.
- **Alerts:** ISA Server records alerts in the Windows 2000 Event Log
- **Authentication:** ISA supports the following Windows authentication methods:
  - Kerberos
  - NT LAN Manager (NTLM)
  - Digital Certificates
  - Basic
  - Anonymous
- **Client Auto Discovery:** ISA Server supports Web Proxy Autodiscovery Protocol (WPAD). This makes it possible for ISA Server clients who run Firewall Client software to automatically connect to ISA Server.
- **Integrated Virtual Private Networking (VPN):** ISA Server can be set up as a VPN server. Here, ISA Server provides secure remote access connections over the Internet. Windows 2000 based VPN offers support to Layer 2 Tunneling Protocol (L2TP)/Secure Internet Protocol (IPSec) and Point to Point Tunneling Protocol (PPTP).

- **Microsoft Management Console (MMC):** ISA Management, a MMC snap-in, is the management interface of ISA Server. Because MMC is extensible, third party vendor products can be integrated with the management console if ISA Server.
- **Multiprocessor support:** ISA Server uses Windows 2000 symmetric multiprocessing (SMP).
- **Network Address Translation (NAT):** NAT translates private addresses to global public addresses that can then be routed on the Internet. The private IP address is hidden as traffic flows on the public network. ISA Server can implement ISA Server policy for SecureNAT clients.
- **Quality of Service (QoS):** ISA Server also supplies bandwidth control management.
- **System Hardening:** The Windows 2000 security templates are utilized by ISA Server to harden the OS at various security levels.
- **Tiered Policy Management:** With ISA Server Enterprise Edition multiple enterprise policies can be specified and applied to arrays
- **Web filters:** ISA Server has Web filters which examine File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP) traffic. The Web filters are derived from Internet Server Application Programming Interface (ISAPI)

### 1.3. ISA Server Features

ISA Server supports numerous Internet protocols such as **HTTP**, **FTP**, **H.323**, **Windows Media streaming**, Internet Relay Chat (**IRC**); and **RealAudio** and **RealVideo**. A few third party vendors provide products that can be integrated with ISA Server. These extensions to ISA Server comprise of content filtering and reporting mechanisms, virus detection; and administration tools. ISA Server also offer a complete software development kit (SDK) that enable customers to create their own extensions. ISA Server offers API documentation and samples that can be utilized to create any further application filters, MMC snap-ins, and other capabilities.

ISA Server Enterprise Edition enables ISA Server computers to be grouped into **arrays**. This provides **distributed caching**, **load balancing**, and **fault tolerance** capabilities, which in turn lead to enhanced performance and improved response time for client requests. The group of ISA Server computers is managed as one logical unit.

**Network Load Balancing (NLB) Services** included in Microsoft Windows 2000 Advanced Server and Windows 2000 Datacenter Server provides **fault tolerance**, high availability, and improved performance by means of clustering ISA Server computers.

ISA Server uses Windows 2000 SMP to **scale performance**. The ISA Server Standard Edition can support four processors on one computer, while the ISA Server Enterprise Edition supports limitless CPUs by using arrays.

A few firewall security features associated with ISA Server are:

- ISA Server dynamically inspects all traffic passing through the firewall



- ISA Server is capable of filtering application specific traffic using data aware filters. It can filter FTP, HTTP, SMTP, Remote Call Procedure (RPC), email, H.323 conferencing, and streaming media.
- Secure server publishing secures Web and email servers, and ecommerce applications.
- With Web server publishing, rules can be specified for internal Web servers which protect these internal servers from unauthorized external access.
- ISA Server provides robust authentication by supporting the following Windows authentication methods: Kerberos, NTLM, Digital Certificates, Basic and Anonymous authentication
- SecureNAT makes it possible for internal IP addresses to be translated to global IP addresses.
- ISA Server includes intrusion detection, derived from Internet Security Systems (ISS) technology, which can identify certain intrusive traffic behaviour that could be indicative of network attacks.
- ISA Server supports VPN access.
- ISA Server makes it possible to lock down the OS at various security levels.
- ISA Server's streaming media filters makes it is possible to split media streams.
- ISA Server also provides end to end filtering, and security with dual hop SSL authentication. ISA Server permits encrypted data to be examined prior to it arriving at the Web server.

A few Web caching features associated with ISA Server are outlined below:

- ISA Server provides high performance Web caching for internal clients accessing the Internet, and for external clients accessing the organization's Web server.
- Distributed content caching can be configured between an array of ISA Server computers. A hierarchy of caches can also be set up to enable faster client access.
- ISA Server is capable of identifying those Web sites that are most popular. It then determines how often site content should be refreshed, and automatically preloads that content into cache. ISA Server bases these decisions on when the object was last retrieved, and the duration that the object has been cached.
- ISA Server also enables scheduled caching by allowing the cache to be preloaded with Web sites based on a specified schedule.

A few management features associated with ISA Server are outlined below, with a more in depth outline following the précis:

- The MMC snap-in or Microsoft Windows 2000 Terminal Services can be utilized to remotely manage ISA Server.
- Graphical task pads and configuration wizards ease the configuration of common operations
- ISA Server enables policy based access control. Access can be administered by user and group, destination, application, type of content and schedule.
- ISA Server Enterprise Edition supports multiserver arrays with centralized management. It provides enterprise and array policy level support
- Bandwidth can be managed and prioritized for certain Internet requests.

- ISA Server rules and configuration data can be centrally stored and managed with Active Directory.
- ISA Server provides security and access logs, reports, and alerts based on particular events.

ISA Management is a MMC snap-in which supply the interface utilized for common management tasks of ISA Server. With ISA Server, firewall and cache capabilities can be integrated in one or in an array of servers. In this manner, integrated administration is enabled because administration is performed through a **single** management interface. Access control policies which control Internet access, can be defined for the firewall, and are applicable to the Web cache server as well. Both the firewall and Web cache server utilize common and identical logging, reporting and alerting ISA Server services. When the ISA Server computers have the identical access policies, administrative tasks performed on a single computer are then enabled on all the ISA Server computers.

Step by step wizards can be utilized for the following tasks:

- Deploying local and remote VPNs, and client to server VPNs.
- Specifying a protocol rule, site and content rule, and bandwidth rule
- Configuring a site, as well as secure publishing
- Configuring a mail server
- Specifying policy for the mail services

With ISA Server, **Internet access policy** can be specified and applied to requests of both directions. ISA Management can be utilized for configuring policy elements. The policy elements are then utilized when defining an access policy. ISA Server rules utilize predefined policy elements:

- **Bandwidth priorities**
- **Client address sets**
- **Content groups**
- **Destination sets**
- **Protocols**
- **Schedules**

A **publishing policy** that comprises of server publishing and Web publishing rules can be specified for ingress requests. The server publishing rules maps a request to a suitable internal server located behind the ISA Server computer, while the Web publishing rules maps the request to the suitable internal Web server.

While the ISA Server Standard Edition operates only as a standalone ISA Server computer with local policy, ISA Server Enterprise Edition supports the following two levels of policy:

- **Array policy:** Whether ISA Server Enterprise Edition is deployed as a standalone server or as an array member, the configuration is common to the members of the array. The array policy includes the IP packet filters and the following rules:
  - Site and content
  - Protocol



- Server publishing
  - Web publishing
- 
- **Enterprise policy:** The enterprise policy contains site and content, and protocol rules; and is applied to arrays. The enterprise policy can further be amplified by the individual policy of the array. When both policies are defined, it basically ensures that the corporate policy is applied within the organization.

## 1.4. ISA Server Firewall Overview

### 1.4.1 Filtering Techniques

#### 1.4.1.1 IP Packet Filtering

With IP packet filtering, all IP packets to and from ISA Server are examined prior to it being forwarded to an application filter. IP packet filtering can be set up to permit certain IP packets to move through ISA Server, and to block other specific packets. IP packet filtering filters packets on:

- Source computer name
- Destination computer name
- Service type
- Port number

Because IP packet filters are applicable to particular ports, **allow filters** permit traffic to move through the particular port, while **block filters** stop packets from moving through.

ISA Server packet filtering can be configured to block packets:

- that could be connected with certain network attacks;
- that come from particular Internet hosts;
- that is intended for services on the internal network.

#### 1.4.1.2 Circuit Level or Protocol Filtering

When circuit level filtering is enabled, sessions are examined, and not packets. A session could possibly comprise of multiple connections. Access policy rules and publishing rules have to be defined when utilizing circuit level filtering. Circuit level filtering also includes support for protocols with **secondary connections**. The primary and secondary connection of the protocol is configured by setting the port number, protocol type, inbound/outbound direction; and Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). With **dynamic filtering**, access policy rules and publishing rules have to be specified. Ports are automatically opened when needed for communication. Ports are closed when they no longer required.

#### 1.4.1.3 Application Filtering

Application filtering is the superior method of filtering. Application filtering examines, modifies, redirects, or blocks the data for a specific application as it moves through ISA Server. ISA Server offers the application filters listed below:



- The **FTP access filter** inspects FTP data.
- The **HTTP redirector filter** redirects any HTTP requests originating from SecureNAT clients and the firewall clients to the Web Proxy service.
- The **H.323 filter** regulates H.323 packets, and provides call control for H.323 packets utilized for multimedia. The H.323 filter and the H.323 gatekeeper function together to enable communication for H.323 registered clients. When these clients utilize applications compliant with the H.323 gatekeeper, the H.323 gatekeeper supply call routing and directory services to these registered clients.
- **POP and DNS intrusion** detection filters block attacks targeted at the internal servers by inspecting for particular intrusive activity.
- The **RPC filter** inspects RPC requests.
- The **SMTP filter** examines SMTP email traffic prior to it accessing the mail server.
- The **SOCKS filter** transmits the requests from SOCKS 4.3 applications to the ISA Firewall service. It is capable of supporting any client platform.
- The **streaming media filter** manages industry standard media protocols such as Microsoft Windows Media Technologies, Progressive Networks Audio (PNA) and Real Time Streaming Protocol (RTSP).

ISA Server includes approximately 100 defined application protocols. Any additional protocols can be defined according to port number, protocol type, inbound/outbound direction; and TCP or UDP. Support for protocols with secondary connections is included.

#### **1.4.2 ISA Server Intrusion Detection Capabilities**

ISA Server includes intrusion detection capabilities that detect network attacks. ISA Server intrusion detection mechanism runs at the packet filter and application filter levels. Alerts can be configured to signal when an attack is detected. It is also possible to configure a specific action to occur in response to a certain network attack. Response actions could include logging an event in Windows Event Log, executing a program, or stopping the Firewall service.

ISA Server can detect the network attacks listed below:

- **Enumerated port scan attack:** The intruder probes every port for a response with the purpose of determining the number of services running on a computer.
- **All port scan attacks:** Additional ports, other than the defined amount of ports are trying to be accessed.
- **IP half scan attack:** The intruder continuously tries to connect to a destination computer with the purpose of probing for, and identifying any open ports.
- **Ping of death attack:** In this attack, a huge quantity of information is added to an Internet Control Message Protocol (ICMP) echo request or ping packet.
- **Land attack:** Here, a spoofed IP address/port number which match the destination IP address and port number requested the TCP connection. Successful land attacks could result in computer crashes.
- **UDP bomb attack:** This attack mostly impacts the older OSs. With this attack, certain illegal values are included in the UDP packet.

- **Windows Out of Band attack:** In this instance, a Denial of Service (Dos) attack is launched against a computer.

POP and DNS application intrusion detection filters block attacks targeted at the internal servers by inspecting for particular intrusive activity. The POP intrusion detection filter inspects inbound POP traffic, while the DNS intrusion detection filter inspects DNS traffic.

POP and DNS application intrusion detection filters can be defined to monitor for the intrusions listed below:

- **DNS Host Name Overflow:** In this case, the DNS response for a host name is greater than a specified fixed length. When the host name length is not verified by applications, it could result in the application returning overflowing internal buffers which could enable an intruder to execute arbitrary commands on the computer.
- **DNS Length Overflow:** Here, the DNS response for an IP address is greater than a specified fixed length. This could also result in the application returning overflowing internal buffers which could enable an intruder to execute arbitrary commands on the computer.
- **DNS Zone Transfer from Privileged Ports:** With this intrusion, a client system utilizes a DNS client application to transfer zones from an internal DNS server. The source port in this instance is a port number between 1 and 1024.
- **DNS Zone Transfer from High Ports:** With this intrusion, a client system utilizes a DNS client application to transfer zones from an internal DNS server. The source port in this instance is a port number over 1024.
- **POP Buffer Overflow:** In this intrusion, an intruder attempts to overflow the internal buffer with the purpose of accessing the POP server.

### **1.4.3 Bandwidth, Virtual Private Networking and Secure Publishing**

ISA Server **bandwidth rules** inform the Windows 2000 QoS packet scheduling which network connections should have priority over other network connections. A network connection that has a bandwidth rule linked to it is scheduled ahead of connections that have no bandwidth rules linked to it. The default scheduling priority is applied to all network connections that do not have any bandwidth rules linked to it.

Virtual Private Networks (VPN's) provide secure and advanced connections (communication) to private organizations through a non secure network by securing private data in a public environment. ISA Server can be set up as a VPN server. ISA Server therefore supports client to gateway, and gateway to gateway remote access over the Internet. In this configuration, the local ISA Server VPN computer and the remote ISA Server VPN computer are each connected to their own ISP. The local VPN wizard resides on the local network's ISA Server, while the remote VPN wizard resides on the remote network's ISA Server. Data is encrypted and transmitted through the VPN tunnel when a local network computer connects with a remote network computer.

ISA Server utilizes server publishing to forward requests to the **internal** servers residing behind the ISA Server computer. When computers on the internal network publish to the Internet, the requests and responses move through the ISA Server computer. ISA Server uses the ISA Server computer's IP addresses when publishing a server.

## 1.5 ISA Server Caching Overview

### 1.5.1 Forward and Reverse Web Caching with ISA Server

ISA Server's Web Proxy service provides a cache of Web objects that is utilized to deal with requests from the cache. The ISA Server computer caches the response to the request when the Web server replies to it. A new request is set off only when the cache is unable to deal with the client request. ISA Server provides fast RAM caching which holds all the frequently requested objects in RAM. This leads to faster response time.

When implemented as a **forward Web caching server**, ISA Server manages a central ISA Server cache that contains the frequently requested Web objects. These objects can be accessed by Web browsers of internal clients. The ISA Server computer uses the Web object from its cache instead of requesting it from a server on the Internet. When an object is dealt from the ISA Server cache, enhanced Web browser performance and decreased response time benefits are realized.

When implemented as a **reverse Web caching server**, the ISA Server computer operates like a Web server by managing client Web requests. The ISA Server computer forwards the requested object to the client when the object is stored in the ISA Server computer's cache. Requests are forwarded to the Web server when the requested object does not exist in the ISA Server cache.

### 1.5.2 Scheduled Caching and Active Caching

The **ISA Server Scheduled Content Download** feature enables HTTP content to be downloaded to the ISA Server cache, making it possible for requests to be dealt with directly through the ISA Server cache. Multiple URLs or a complete Web site can be downloaded to the ISA Server cache. This can be done on a request or scheduled basis. The content that should be downloaded can be limited. Content can be limited to text only as well. With the ISA Server Scheduled Content Download feature, scheduled content downloads can be specified for both inward bound and outward bound Web requests. For inward bound Web requests, content is downloaded from the internal Web servers to the ISA Server cache. For outward bound Web requests, objects is downloaded from the Internet to the ISA Server cache

ISA Server can **automatically** refresh the content in the ISA Server cache when active caching is enabled. In this technique, ISA Server studies the cache's objects to identify those objects most frequently accessed, and then automatically refreshes the content when the objects are about to expire. With active caching, ISA Server only refreshes those objects that would almost certainly be accessed again.

### 1.5.3 Hierarchical Caching

Hierarchical or chained caching can be enabled when utilizing ISA Server Enterprise Edition. Chaining provides server **load distribution** and **fault tolerance** for the ISA Server computers. It provides a backup route when the primary route is not available. Chaining describes a hierarchical connection among ISA Server computers, or a hierarchical connection among arrays of ISA Server computers. The request of the client is submitted through the chained hierarchical connection of cache servers. Once the requested object is located, the object is cached at the cache of each chained server, to the point that the client receives it.

### 1.5.4 Cache Array Routing Protocol (CARP)



CARP is utilized in an ISA Server Enterprise Edition implementation. The protocol provides a **request resolution path** through an array when multiple ISA Server computers are arrayed as one logical cache. The request resolution path identifies the location of the information in the array, and also determines whether the information should be requested from the Internet. The **hash based** routing utilized by CARP prevents the duplication of the most frequently requested content. Because CARP utilizes hash based routing, it is able to automatically adapt when a server is added or taken offline. CARP turns out to be quicker as more servers are added, that is, it has positive **scalability**. CARP makes certain that the cache objects are shared among the servers in the array. CARP also allows the load factor for a server in the array to be configured, and it can be configured for Web requests in both directions. Web Proxy routing rules enables requests to be routed based on destination.

### **1.6 Preparing to Install ISA Server**

The minimal hardware requirements for an ISA Server Installation are:

- A computer running Windows 2000 Server, or Windows 2000 Advanced Server (Service Pack 1), or Windows 2000 Datacenter Server
- A network adapter for internal network communication
- A network adapter, ISDN adapter or modem for Internet communication
- A local hard disk that is NTFS formatted, and 20 MB available hard disk space
- 256 MB RAM
- Windows 2000 Active Directory is needed on the network if array and enterprise policies are going to be configured.
- ISA Management needs to be implemented to remotely administer ISA Server. In addition to this, the computer utilized for ISA Management has to be a member of the Windows 2000 domain for it to communicate with an ISA Server computer.

When installing ISA Server as a **dedicated firewall**, the following throughput CPU and Internet requirements should be considered for Firewall and SecureNAT clients:

- **1 – 25 MBits/seconds:** ISA Server should be running on Pentium II, 300 MHz. T1, xDSL, or cable modem for the Internet connection.
- **25 – 50 MBits/seconds:** ISA Server should be running on Pentium III, 500 MHz. T3 or finer for the Internet connection.
- **Greater than 50 MBits/seconds:** ISA Server should be running on one Pentium III, 550 MHz for every 50 MBits/seconds needed. T3 or finer for the Internet connection.

When installing ISA Server as a **forward Web and FTP caching server**, the following throughput, memory and disk requirements should be considered:

- ISA Server must be installed on a computer that contains a **NTFS** formatted partition when utilizing the ISA Server caching feature



- **250 users:** ISA Server should be running on Pentium II, 300 MHz. 2 – 4 GB disk space should be available for caching with 256 MB RAM.
- **2 000 users:** ISA Server should be running on Pentium III, 550 MHz. 10 GB disk space should be available for caching with 256 MB RAM.
- **Greater than 2 000 users:** ISA Server should be running on one Pentium III, 550 MHz for every 2 000 users supported. 10 GB disk space should be available for caching per 2 000 users with 256 MB RAM per 2 000 users.

When installing ISA Server before a **Web server** hosting a commercial Web business, the following hardware requirements should be considered for the different hit rates:

- **Fewer than 500 hits/second:** ISA Server should be running on Pentium II, 300 MHz with 256 MB RAM
- **500 – 900 hits/second:** ISA Server should be running on Pentium III, 550 MHz with 256 MB RAM
- **Greater than 900 hits/second:** ISA Server should be running on one Pentium III, 550 MHz for every 800 hits/second with 256 MB RAM for each server

### **1.6.1 ISA Server Mode Considerations**

The following ISA Server mode choices exist:

- **Firewall:** In this mode, rules are configured that control the connections among the organization's network and the Internet. Internal servers can also be published in this mode. In firewall mode, access and enterprise policies, server and web publishing, application and packet filtering, alerts, and monitoring features can be set up.
- **Cache:** In this mode, frequently accessed Internet objects are stored in the ISA Server cache. Internet users' requests can be directed to the fitting internal Web server. In Cache mode, access policy for HTTP and enterprise policies, server publishing, cache configurations, alerts, and monitoring features are set up.
- **Integrated:** Rules are also configured that control the connections among the organization's network and the Internet. Internal servers can also be published in this mode. In integrated mode, frequently accessed Internet objects are also stored in the ISA Server cache. Internet users' requests can be directed to the fitting internal Web server. Therefore, the features applicable to the Firewall and Cache modes are available in Integrated mode.

### **1.6.2 Array Requirements**

When many computers are going to be required to manage the network load, installing an array of ISA Server computers that can be administered as one logical unit is ideal. Recall from an earlier discussion that the array servers all have a common configuration. An enterprise policy can be specified for an array when utilizing ISA Server Enterprise Edition, and individual array policies can be implemented for every array. Installing an array of ISA Server computers leads to:

- Improved performance with less hardware
- Improved response times for clients



- Centralized management

The following requirements should be considered for an array installation:

- The computer on which ISA Server is to be installed on has to be a member of a Windows 2000 domain. A domain is a grouping of computers that have a common Active Directory directory store.
- The members of the array have to exist in the same domain and site. A site is a grouping of computers in a connected TCP/IP network.
- ISA Server Enterprise Edition has to be enabled prior to installing ISA Server as an array member.
- When installing ISA Server as a standalone server, it is not necessary that the computer be a member of a Windows 2000 domain. It is however recommended to install the computer as an array member. This implementation strategy provides simpler future expansion capabilities.

### **1.6.3 Internet Connectivity Considerations**

The following issues should be addressed in the ISA Server installation planning phase:

- Selecting the fitting ISP and access method such as DSL, cable modem, T1 and satellite. When selecting these two components, data throughput, cost and reliability should be take into account.
- When utilizing DSL, cable modem or a direct line for connectivity, an external network adapter has to be installed.
- When opting for a dial up link, an ISDN adapter or modem has to be utilized.
- When planning for ISA Server to publish Web servers, static IP addresses have to be reserved with the ISP. A domain name has to be registered with an Internet Corporation for Assigned Names and Numbers (ICANN) approved registrar.
- An internal DNS server can be utilized to resolve external client requests.

### **1.6.4 Network and Topology Considerations**

The following **network factors** should be addressed in the ISA Server installation planning phase:

- When ISA Server is deployed as a standalone server in a Windows NT 4.0 domain, and an array of ISA Server computers are going to be utilized, the array has to be installed on a Windows 2000 domain. A trust relationship has to be configured between the two domains.
- Active Directory has to be installed on the Windows 2000 domain to which ISA Server belongs to.
- If ICS was formerly utilized for Internet connectivity, disable ICS prior to installing ISA Server
- When installing ISA Server it is no longer necessary to utilize Windows 2000 Server's remote access server to provide remote access connectivity.

The following points could assist when defining the **network topology**:

- When installing ISA Server is a small office network environment, one ISA Server computer can be located between the organization's LAN and WAN; and the Internet to supply Internet connectivity. It is recommended to configure the ISA Server computer as an array member.



- When installing ISA Server in a large corporate network environment that includes a central location and different branch locations, at least one array is typically installed at every different location. An enterprise policy is normally specified at the central location. Each branch location has to adhere to the enterprise policy. A more stringent policy can be implemented at each branch location.
- When publishing Web content, the Web server being published can be placed on the identical computer as ISA Server or it can be located on another computer:
  - When the identical computer is utilized for the Web server and ISA server, the two servers should be specified to utilize different ports to detect incoming requests, or an IIS server can be specified to utilize another IP address.
  - When another computer is utilized, the Web server can be placed behind the ISA Server computer. ISA Server can ensure security for the Web server in this implementation strategy.
- A typical ISA Server implementation often includes ISA Server securing a Microsoft Exchange Server. The Exchange Server being published can be placed on the identical computer as ISA Server or it can be located on the local or perimeter / DMZ network. The perimeter network can also contain the Web server, and can be a back to back perimeter network configuration or a three homed perimeter network configuration.
  - With a **back to back** perimeter network configuration, two ISA Server computers are implemented on each end of the network
  - With a **three homed** perimeter network configuration, one ISA Server computer is implemented with three network cards.