Global Information Assurance Certification Paper

An Introduction to Internet Security Accelerator (ISA) 2000

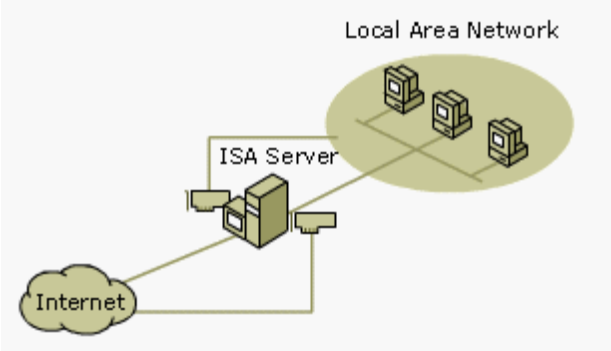
James Carlson

GSEC Practical Assignment Ver. 1.2c

May 5th, 2001

Introduction

Internet Security Accelerator 2000 (also known as ISA Server) replaces Microsoft Proxy Server. Microsoft markets ISA 2000 as an enterprise firewall solution. Large organizations can deploy "arrays" of ISA Servers that support load balancing and fault tolerance. In addition, ISA supports virtual private networks (VPNs) for management of servers across remote sites. This introduction to ISA Server will focus on the Standard Edition and not the Enterprise Edition. The Standard Edition installs on a single system. Typically, an organization protects itself by installing the ISA Server on the perimeter of its network. The typical deployment scenario is a multi-homed system with one connection going to the Internet and the other connection to the internal network. ISA Server provides firewall services, network address translation, and a web proxy for internal network clients. All network traffic should pass through the ISA Server. The following diagram depicts typical deployment of ISA Server Standard Edition.



ISA Standard Version Deployment

Installation:

Configuration of the network interface cards is essential for proper operation of the ISA Server. The internal interface should be configured with a DNS Server address on the internal network. This allows the ISA Server to resolve incoming requests for internal services. Configure the default gateway for the external interface only. Disable bindings on the external interface to improve security. For additional security disable LMHOSTS lookup and NetBIOS over TCP/IP under Advanced TCP/IP Settings.

The ISA Server can be installed in one of three modes. The modes are cache only, firewall only or integrated mode. Cache mode installs the web proxy service and allows

storing of web pages locally. This improves network performance and decreases Internet access costs. Firewall mode allows internal clients to access the Internet more securely. After one decides which mode is best for his or her organization, the next decision is the size and location of the web cache. These answers are based on hard drive space and number of web users. After that, one defines the internal network address space. Ideally, private network addresses should be used. Private IP's assigned by the Internet Assigned Numbers Authority (IANA) can be found in RFC1918 at **http://www.faqs.org/rfcs/rfc1918.html**.

Access Policy Configuration

The next step is to configure the access policy for the firewall. The access policy should be based on an organization's security policy. ISA Server's access policy consists of the following three rules or filters:

1) Protocol Rules
2) Site and Content Rules
3) IP Packet Filters

Protocol rules state which protocols clients can use to access the Internet. Protocol Definitions are used to create protocol rules. ISA Server comes with all the common Internet protocols predefined. In addition, protocols can be configured as needed. Protocol definitions consists of the following:

1) The Port Number for the Initial Connection.
2) The Low Level Protocol used (TCP or UDP).
3) The Direction of the Connection (inbound or outbound)
4) Secondary Connections if needed

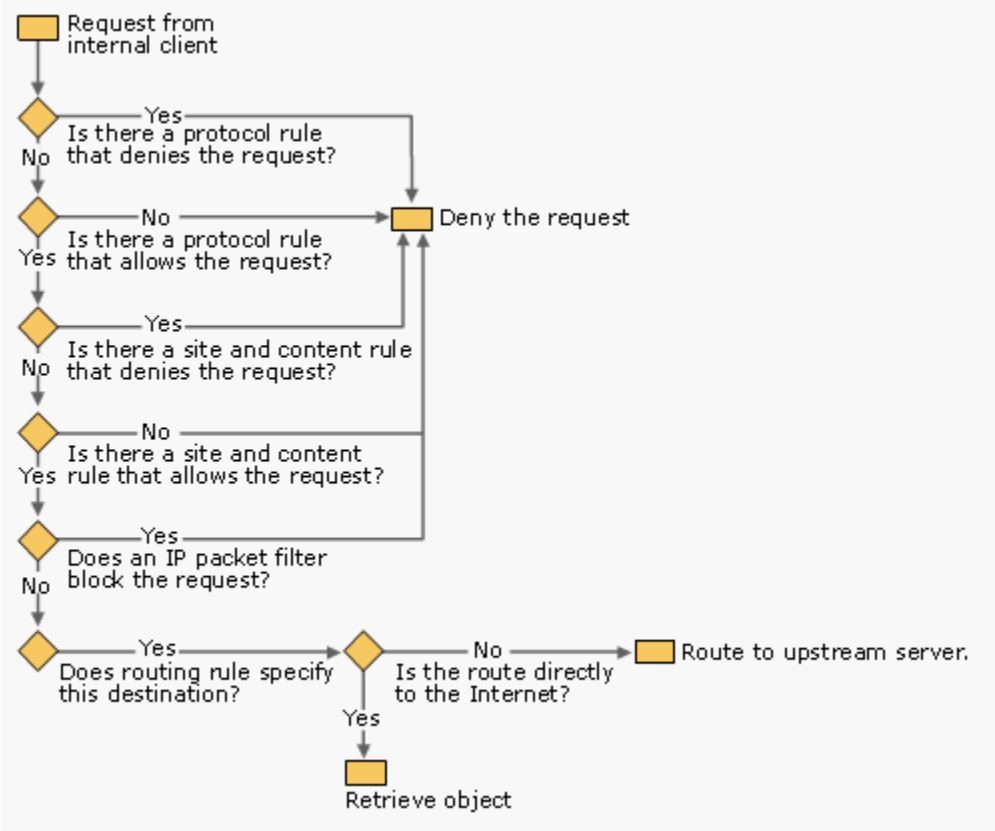
Protocol rules must be configured and enabled to allow client access to external network addresses. ISA Server can allow or deny access to all Internet Protocols or selected protocols. Furthermore, protocol access can be restricted by user ID, group name, network address or time of day.

In addition to protocol rules, access policy configuration includes Site and Content rules. Site and Content rules can be configured to allow specific computers access to selected content on specified sites. Destination Sets and Client Sets are policy elements that aid in configuring Site and Content rules. Destination Sets include external sites and/or specific directories that clients can access. Client Address Sets allow specifying ranges of network addresses that are allowed access to Site and Content rules.

The final step in configuring access policy is applying IP packet filters. Packet Filters block or allow packets from passing through specific ports. By default no packets can pass through the ISA Server. Once packet filtering is enabled, all packets on the external interface are dropped unless explicitly allowed. Packets can be filtered by type of service, port number, source and destination address. In addition to static packet filtering

ISA Server provides a more secure method of filtering called stateful inspection. Stateful inspection verifies traffic is behaving, as it should. In other words the state of the connection is known. Another type of filter used by ISA Server is an application filter. Application filters intercept traffic at the application level. These filters inspect the data portion of the packet and can drop packets with malicious data.

In summary, protocol rules state which protocols clients can use to access the Internet. Site and Content rules determine if and when users or client address sets can access content on specific destinations sets. Packet Filtering allows or blocks ports on the external interface. In addition to static packet filtering, ISA Server uses stateful inspection of packets and application filters. The following flowchart summarizes the access policy for ISA Server when a client request is made to the Internet.



ISA Server Clients

A single internal-networked system can be configured as all three types of clients. Each type of client provides different functionality. ISA Server supports the following three types of clients:

1) Web Proxy Clients
2) Firewall Clients

3) SecureNAT Clients

A Web Proxy client is one whose web browser is configured to use the ISA Server. The browser can be configured manually or by downloading the firewall client software from the ISA Server. Web proxy clients use the web proxy service. This is a separate service that manages connections for the common http protocols only. Firewall and SecureNAT clients use the firewall service.

A firewall client is a computer with the Firewall software installed on it. It must have a windows based operating system. The software can automatically configure web proxy clients, update the local address table and set the DNS settings for the client. Once the client software is installed and enabled the client can run Winsock applications that interact with the firewall service. The client can be easily disabled from the control panel. The Firewall client can pass user credentials to the ISA Server for protocols that require authentication for access. This is a big advantage over SecureNAT clients.

SecureNAT clients require no special software. All operating systems can use SecureNAT clients. ISA SecureNAT provides network address translation (NAT) for the internal network. NAT improves security by hiding the client's network address from the Internet. To configure SecureNAT set the default gateway of the client computer to point to the internal interface of the ISA Server. To ease configuration it is recommended that a DHCP Server be installed on the internal network. In addition, DNS needs configuring since ISA Server doesn't provide DNS to SecureNAT clients. In addition, a protocol rule must be setup to allow DNS queries.

SecureNAT clients have some limitations. First, a protocol definition must exist for each protocol used by a client. The connection can not pass through a protocol rule that applies to "all IP traffic". SecureNAT clients unlike firewall clients need a protocol rule defined explicitly. A second limitation for SecureNAT Clients is the requirement that application filters are needed for complex protocols. The final limitation is that user-based authentication is not supported for SecureNAT clients.

Intrusion Detection

ISA Server has built-in intrusion detection. It can detect the signature for port scans, "Ping of Death", IP Half Scan and "Land Attack". Port scans and half scans can lead to system compromise. The "Ping of Death" and "Land Attack" are denial of service attacks. Half scans violate the three-way handshake for TCP connections. The attacker can gain valuable information about what ports are open. In addition, the scan is not logged because the TCP connection was not established. The "Ping of Death" so named because it uses the ICMP protocol. It denies service to a system by sending fragmented packets greater than 65535 bytes. Another availability attack, the "Land Attack" uses "IP Spoofing" to craft packets with the same source, destination and same port numbers. Proper configuration of ISA's access policy can prevent some of these attacks. ISA can block access to the ICMP protocol preventing the "Ping of Death" attack. However, other protocols that use IP can exploit this attack. To prevent the

"Land" attack access policy can deny inbound access to packets whose source address is an internal network address. The ISA Server utilizes an alerting service for events such as intrusion detections. Alerts can be sent as e-mails or logged to the windows event viewer. The e-mail notification service must be configured correctly. If not, the ISA Server can start a small-scaled denial of service attack on your e-mail client. In addition, alert notification can trigger the stopping of the firewall service thus cutting off routing to the internal network. These types attacks exploit security vulnerabilities in the TCP/IP protocol stack. Therefore, security patches must be installed to further protect the internal network.

Logging, Monitoring, and Reporting

Additionally, ISA can log access, monitor in real-time, provide statistical reports and send out alerts. Logs are kept for the Firewall Service, Web Proxy Service, and IP Packet Filtering. Log files can be transferred to a database or stored as standard text files. The firewall logs and Web Proxy logs access information from internal clients, while the IP Packet Filtering log defaults to showing block packets. In addition to logging, ISA Server provides real-time monitoring of alerts, running services and client sessions. ISA Server generates reports at pre-configured intervals. Reports can be easily viewed in html. In addition, reports include statistics on web usage, application usage, and traffic and utilization. Security Reports show numbers on blocked packets and unauthorized access.

Conclusion

Internet Information Security Accelerator 2000 is a firewall solution for securing internal networks from the Internet. The installation process is trouble-free. The ISA Management Console provides administrators with the tools needed to configure access policy and monitor the ISA Server. However, the ISA Server's access policy must be configured correctly and continuously monitored. This still doesn't prevent attacks originating from the internal network or new e-mail macro viruses from penetrating the network. A "Defense in Depth" strategy is the best way to secure a network. The foundation is a well-written security policy that protects both systems and people. Enforcing good password policy, eliminating unneeded services, frequent penetration testing and applying the latest security patches improves network security. So, ISA Server can't stop all attacks

References:

Microsoft Corporation. Internet Security Accelerator's Home Page.
URL: http://microsoft.com/isaserver

Shinder,Tom "Designing An ISA Server Solution on a Simple Network" 23 Apr. 2001.
URL:http://isaserver.org/shinder/tutorials/designing_an_isa_server_solution_on_a%20_simple_network.htm
(27 Apr. 2001) .

Shinder,Tom "The SecureNAT Client" 7 May 2001.

URL:http://isaserver.org/shinder/tutorials/secure_nat_client.htm (7 May 2001)

Microsoft Corporation. Internet Security Accelerator Product Documentation
URL:http://www.microsoft.com/technet/isa/isadocs/default.asp

Microsoft Corporation. The Minimum System Requirements for Internet Security Accelerator.
URL:http://www.microsoft.com/technet/isa/isadocs/M_S_H_SettingUpHW.htm

Internet Security Systems. X-Force Home Page.
URL: http://xforce.iss.net/

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event