Global Information Assurance Certification Paper

Halt! Who Goes There? And Where? And Why? And How?

Matt Melton
GSEC, Version 1.4, Option 1

Abstract:

For every company, the issue of how to protect your network from malicious outside attacks must be addressed. In fact, the idea of having Internet connectivity without a firewall is not only absurd, it would be an offense which could require the responsible network administrator to get his resume up to date. The challenge of selecting a comprehensive solution is compounded when you factor in the need to allow Internet access to employees. While firewalls can offer this functionality, they aren't necessarily optimized for high-speed web access. Comparatively, proxy servers offer speedy response for web browsing, but sacrifice flexibility and security in other areas.

This paper provides an overview of how Microsoft's Internet Security and Acceleration Server (ISA) can be used as a solution to this dilemma. In the following pages I will outline the different modes of installation, explore the various components of the web proxy and firewall services, and highlight what I feel are the most valuable features therein. The discussion will include the different types of filters available through the firewall service and how these filters are deployed in order to protect your network. The conclusion to draw from this is that ISA provides secure access between an internal network and the Internet, making it sufficient to serve as a complete proxy and firewall solution.

Modes:

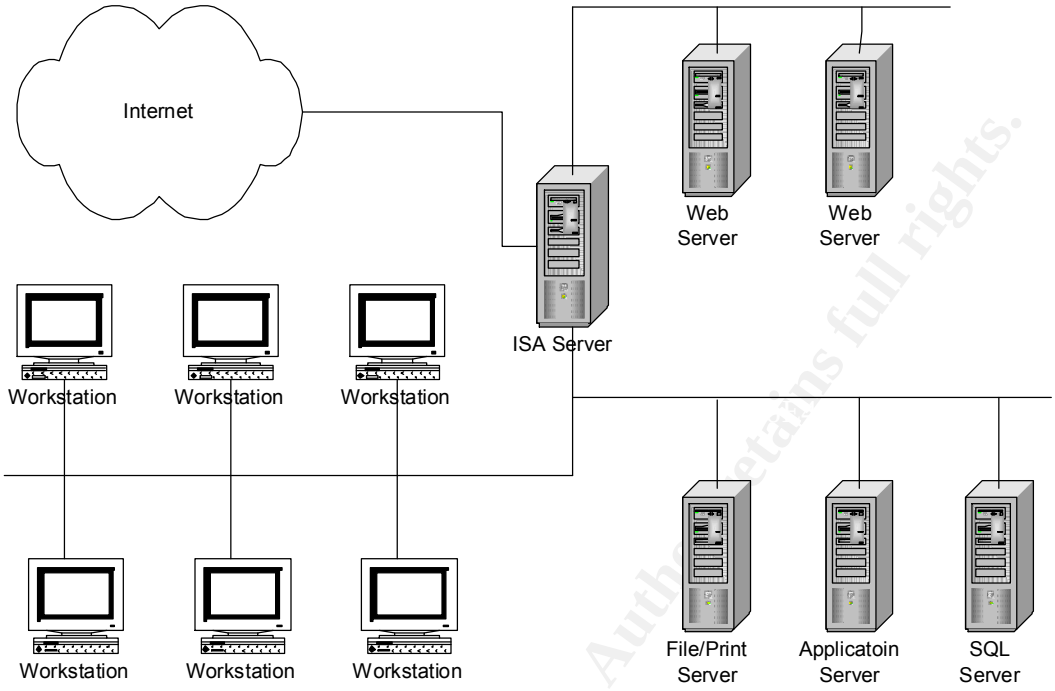
When evaluating ISA, the first decision to make is what mode would you like to install it in. The three different options are Firewall mode, Cache mode, and Integrated mode.[7] Firewall mode installs only those features associated with securing network communication between the internal network and the Internet.

While speed is taken into consideration, the firewall's primary concern is security. It is responsible for opening and closing ports, allowing or disallowing packets, and countless other tasks. Essentially, Firewall mode can handle any traffic to and from your network. While it isn't optimized as a web proxy, it can handle HTTP traffic. However, its strength lies in its ability to allow or disallow any type of traffic based on many different variables. These numerous settings are all configurable by the administrator.

Cache mode provides the functionality of a proxy server and increases performance by storing commonly accessed Internet files locally. Cache mode is tuned to only handle high-speed web traffic. Managing only HTTP and SSL traffic, it provides high throughput to the Internet for the user community. Its speed performance enhancement primarily comes from ISA caching frequently requested web sites on the server, eliminating the need to track down every request on the Internet. Interestingly, this feature only gets better with time. The more sites it has the chance to cache, the quicker it will respond to a wide range of requests.

Installing in Integrated mode allows you to take advantage of all the features associated with both the firewall and cache modes. It seems like an easy decision to take advantage of both modes by selecting Integrated. However, just because you can use the firewall service, that doesn't necessarily mean you should. While the proxy service is fairly easy to get up and running, the firewall service adds several layers of complexity. In spite of the fact that the management console is friendly, it does take some time to get all the filters set up and tuned in. Additionally, there will be ongoing maintenance in creating new access rules and cleaning up old ones. Therefore, it would be wise to consider the business case for each of the services prior to installing.

The diagram below illustrates a common corporate network topology and where ISA would fit within that scheme. Notice that ISA not only provides protection for internal clients and servers from the Internet, it also isolates the web servers on a different segment. This prevents outsiders from gaining access to the web servers, a favorite target among hackers, and launching attacks aimed at the internal servers from there. Regardless of which mode ISA is installed in, it will serve as the primary gateway between the internal network and the Internet. Placement of the server is critical in ensuring its effectiveness.



Web Proxy Service:

As Microsoft's next generation proxy product, ISA instantly had a strike against it. This was due to the reputation of its older brother: Proxy 2.0. This previous release came to be considered by most who worked with it as a marginally useful tool. While this product did have the capability to serve as both a web proxy and firewall of sorts, it came up short on performance. The interface was very clunky and it was easy to get misguided. Once rules were created, there was no easy way to see what ports were open under which rule. The worst of it all was, despite the fact that you may have created a rule properly, it sometimes just wouldn't work. It could still do the job as a proxy, but speed and reliability were not its cornerstones. Because of these facts, there were many skeptics when ISA hit the market.

With the web proxy service of ISA, the number one priority was to speed up response time when browsing the web. The average user doesn't care about all the technical details; they just want to get to their site, and the want to get there fast! In order to please the masses, Microsoft added many features to speed web browsing response time. One way to accomplish this task is for ISA to take advantage of its cache in a variety of new ways. The most noticeable of

these features is the added Cache Array Routing Protocol (CARP). This routing algorithm increases efficiency and prevents duplication of cached contents between two or more ISA servers. Essentially, this will allow multiple ISA servers, configured in an array, to use one logical cache.[1] Let's say, for instance, a company has three ISA servers at one site. All three are in cache mode and are configured in an array. Needless to say, with an average user base, these servers are going to field identical Internet requests. It is safe to assume that many users will make a request for CNN.com, Yahoo.com, and ESPN.com. Instead of each server individually going out and getting these pages, the first server to make the request will download the data and store it in cache. Then, when the next request for the same site comes from a different server, it will check the cache to see if it can retrieve the files from there. Specifically, it uses hash-based routing to provide a request resolution path and determine where, precisely, it can pull a request from cache, or if it needs to make an Internet request. This prevents duplication of cached content that you would typically find on multiple stand-alone proxy servers.

In an effort to shave a little more off the response time, ISA has also incorporated active caching. When it comes to finding out who won last night's game or getting the weather, there are a few sites that are far more popular among users than others. Because of this, a large percentage of people will continuously access the same sites throughout the day. ISA capitalizes on this predictability with active caching. When objects are close to expiring, this feature automatically initiates a request to update cached file objects, without the user asking for it.[2] Simply stated, ISA will get the information and put it in cache before anyone asks for it. The longer it is deployed and active caching is enabled, the more efficient it will be. This is because it studies objects in cache to determine which are most frequently accessed. The more you use it, the better it gets.

Cache mode will not only speed internal requests, it will also help with Internet requests to your network. For those sites that are most frequently accessed by the public, ISA will utilize reverse caching. This feature enables the server to cache the most commonly requested objects from internal web servers.[2] ISA will notice that people are continually making a request for your company's home page. Seeing the same request come through, it will take it upon itself to store that page in cache. Instead of having to travel all the way to the web server for a page, the user will retrieve the page from the ISA server. This will speed the request by deleting a hop and it will eliminate additional network traffic. This

makes life easier on the web server and, by preventing a trip from the outside to the web server, potentially reduces the risk of attack.

And the results you ask? Well it turns out that the press Microsoft released with regard to the speed of this product is true. The increased performance in the web proxy is not just a perceived change. It is a measurable difference that has taken this product from the bottom of the heap with its previous release (Proxy 2.0), to rivaling the best performers in the field. How do we know? A company by the name of The Measurement Factory (TMF) has conducted an annual web cache-off for the last several years. The goal of this contest is to provide a means to directly compare different products that typically have a wide range of results in multiple areas. For this reason, TMF developed a price/performance ratio that compares throughput, hit ratio, and price on all competitors.[8] This yields a tangible bottom line for each product. The results of the third such competition showed ISA emerging as the top performer in price/performance and a top five finisher for throughput.

First of all, to say that ISA outperformed its previous incarnation is an understatement at best. Previous tests of Proxy 2.0 showed that it was capable of filling 180 requests per second.[8] While that sounds like a lot to manage in one second, consider that ISA was benchmarked at handling 2,083 requests per second.[8] That is more than ten times faster. Compared to other products the difference is not as dramatic, but the results still show ISA as the top performer. When comparing speed to dollars, ISA turned out 78 hits/second per $1000 and 145 requests/second per $1000.[8] That outperformed other entrants at a rate of 1.5X to 4.5X faster. The second place finisher came in with just over 50 hits/second per $1000.[8]

As stated previously, ISA accomplishes these results largely by taking advantage of its cache. Retrieving the page locally significantly cuts response time. However, not only does this provide snappier web browsing, it also results in bandwidth savings. With more hits coming from cache, fewer Internet requests are made and therefore less traffic is on the network. This provides greater bandwidth availability for other business essential functions.

Firewall Service:

While the cache portion of ISA does a great deal of work and goes a long way in increasing the speed of standard web traffic, the real meat and potatoes of the

secure side of ISA lies in the firewall service. The firewall provides security through employing various filtering methods. It combines these methods in order to provide protection at multiple network layers. A standard rule of thumb is the more layers of security you have, the more secure you are. The firewall service nicely incorporates many highly configurable filters and rules to provide security in depth.

The most notable feature of ISA is what you could consider its multi-layer firewall.[5] Security is primarily maintained through the use of packet filters, circuit-level (protocol) filters, and application filters. There are many other security measures in place, but these do the bulk of the work.

Out of the box with a default install, ISA blocks everything. Nothing gets in and nothing gets out. So, just installing the software and plugging in the cable doesn't do the trick. You have to allow the specific packets you want leaving and entering your network before any communication can take place.[1] That is where packet filtering comes into play. The packet filter allows you to control the flow of IP packets going into and out of the ISA server.[6] Once packet filtering is enabled, the system will evaluate each packet prior to passing it on in order to determine what should be done with it. It has the capability to allow or deny traffic based on source address, destination address, port or payload. This grants you the ability to block based on specific troublesome Internet hosts, block unwanted traffic to internal web servers, or block packets associated with common attacks. Very valuable protection provided by just one of the filters.

Commonly, a user's session through ISA to the Internet will include multiple connections. Circuit-level filtering allows you to inspect these sessions as opposed to packets. This way, ISA will only open ports as they are requested during that session. Once the session has ended, all ports are closed. This considerably reduces your exposure by leaving ports closed until they are needed. These can either be opened dynamically, as the ports are requested, or through a session based protocol rule where primary and secondary connections are defined. To help get you up and running a little quicker, ISA sets up a few predefined circuit level filters. These are in place for the more common protocols, such as HTTP, HTTPS, DNS zone transfer, Kerberos, NNTP, SMTP, SNMP and MSN Messenger to name a few.[7] If you don't find the filter you are after, you can easily get one set up. To create a new protocol definition, it is as simple as following the bouncing ball. ISA manager allows you to create a definition for the needed port and name it appropriately. So, for that one-site-

only protocol definition, you can give it the name of the site or application, making it a little easier to keep track of what definition is needed for what. Intuitive naming goes a long way when it comes to ease of management. Within this portion of the console, you have the ability to sort by protocol name, description, who made the definition, protocol type, direction, and, most importantly, port number. This helps to avoid creating multiple protocol definitions for the same port. Not only does this provide a cleaner environment, but also a more secure one.

Application filtering is the most complex form of traffic inspection. This filter will inspect the traffic then perform protocol-specific or system-specific tasks. It has the capability to block, redirect, or modify the data. For instance, ISA includes the following built-in application filters:

- HTTP Redirector Filter: Forwards HTTP requests from firewall and SecureNAT clients to the web proxy service. Provides transparent caching for those clients with incorrectly configured browsers.[7]

- FTP Access Filter: Intercepts and checks FTP data, and, provided the traffic is approved, supplies high-performance data transfer.[7]

- SMTP Filter: Intercepts and checks SMTP e-mail. Has the ability to screen messages for content or size and accept or reject accordingly.[7]

- SOCKS Filter: Forwards requests from SOCKS 4.3 applications to the firewall service. Determines whether the SOCKS client application is allowed out to the Internet. Popular for its support across multiple platforms.[7]

- RPC Filter: Provides sophisticated filtering of RPC requests on predefined interfaces. Allows capability to select which RPC interface to expose.[7]

- H.323 Filter: Routes packets used for multimedia communications and teleconferencing. Provides call control, handles incoming calls and connects to specific H.323 gatekeeper.[7]

- Streaming Media Filter: Supports industry-standard media protocols. Conserves bandwidth by splitting live Windows Media streams.[7]

- POP and DNS Intrusion Detection Filters: Provides protection for internal servers from DNS Host Name Overflow, DNS Zone Transfer, and POP Buffer Overflow.[7]

In conjunction with the previously detailed filters, ISA employs the use of stateful packet inspection. This is sometimes also referred to as dynamic packet filtering. Stateful inspection works at the network layer tracking each connection across all ports verifying whether they are valid or not. Dynamic packet filtering has the ability to examine data "in the context of its protocol and the state of the connection."[5] Therefore, when an inbound connection is requested at the firewall, ISA will inspect that packet to see if it matches a request that originated internally. If it matches, the connection is allowed. If it doesn't match, the connection is refused. The connections and associated protocols are managed through a state table. ISA compiles information about the port, protocol, destination and source of every outbound request. It stores that information in a table for later reference. As connections come in, ISA inspects the traffic and compares it to the information captured in the state table. If it can find a matching original request, it will allow the traffic.

An example of this put into practice would be John User needing to get some data onto his machine via some non-standard port. John would initiate a session by making a request to Somelargecompany.com. ISA would grab the packets and note in the state table who made the request, the port it is on, what protocol it is and what the destination is. It would then forward the request onto the destination. Then, when Somelargecompany responds, ISA would inspect those packets for the same information previously gathered. When it finds the corresponding record in its table, it will open the appropriate port and allow the connection to proceed. Conversely, if someone attempts to initiate a session from outside, the firewall will inspect the request and, finding no previous record in the state table, it will drop the packets and keep the ports closed. With this feature you can rest assured that any traffic coming in through the firewall originated from and internal request.

Although packet filtering, circuit-level filtering and application filtering provide a solid foundation of security, the ISA firewall also has other tricky methods for keeping unwanted activity out of your network. Web site publishing is one of these important methods. It gives those who ascribe to the theory of 'security through obscurity' the warm-fuzzies. ISA can be deployed in front of a web server to allow access to corporate sites with an extra layer of protection. The

web server is actually "published" in the ISA server. This allows the true address of the web server to remain hidden. "Traffic to and from the web site is not merely filtered through the firewall, but received at its external interface and then forwarded to the internal host."[3] This way, the only machine touching the web server is your trusted ISA server. You can couple this feature with packet filtering to allow through only that traffic which you deem necessary.

As an added bonus, Microsoft, in conjunction with Internet Security Systems (ISS), has included an intrusion detection mechanism within ISA. This feature will keep watch for common attacks and respond accordingly. By setting alerts to trigger when an attack is detected, ISA can page you when it thinks your system is under attack, or take specific actions under certain conditions. Some common attacks ISA detects are enumerated port scans, IP half scan, land attack, ping of death, UDP bombs, various DNS attacks, all port scan attack, and windows out of band attack.

While everything sounds rosy from the outside, this solution is far from perfect. Unfortunately, like most other Microsoft products, ISA is not without its problems. Shortly after it was offered publicly, Microsoft released Service Pack 1 for ISA. This was released in order to address several problems experienced by many users. It was determined that ISA was vulnerable to DoS and other attacks as well as saddled with some stability issues. Additionally, Microsoft discovered that some settings weren't working or didn't take effect, even though all rules were correctly applied.[9] SP1 was released in order to address these and other issues. After applying SP1, users experienced greater stability and were protected from the known exploits.

Since the release of SP1 however, there have been some additional hotfixes as well. Most recently, Microsoft Bulletin MS02-027: Unchecked Buffer in Gopher Protocol Handler Can Run Code of Attacker's Choice. Microsoft first introduced a work-around for this problem, but as of June 14th have a patch available. These various vulnerabilities clearly illustrate that ISA is lacking in some areas. While the firewall solution appears complete and the theory behind it is sound, there are still shortcomings in the product that would warrant further investigation prior to implementation. Having said that, keep in mind that no firewall solution is impervious out of the box. While other products may not have as many known vulnerabilities, all are suspect.

Conclusion:

While the concepts I have touched on are the core features of ISA, the list of configurable security measures goes on and on. ISA's largest advantage over the competition comes from its extensibility, allowing customization of almost every component. As a result, many companies are developing modules to extend the functionality of ISA to their product. Not only has ICSA Labs certified ISA as a secure enterprise firewall[3], functionally it has proven to be intuitive and endlessly flexible. This is a product that can be deployed at the enterprise level with confidence. For all of their effort, Microsoft has a product that has proven to be a comprehensive firewall and proxy solution.

References:

1) Dockter, M.A. "Microsoft ISA Server." Proxy Servers. 19 March 2002. http://serverwatch.internet.com/reviews/proxy-msisa.html#whatsnew. (15 May 2002).

2) Nance, Barry. "Review: Microsoft's ISA Server is a good choice for keeping users in and hackers out." 13 March 2002. http://www.windowsadvantage.com/interactive_office/01-14-02_isa_server.asp. (15 May 2002).

3) Bragg, Roberta. "Ten Reasons To Install MS ISA Server On Your Network." http://www.8wire.com/articles/?aid=1734. (14 May 2002).

4) Hunt, Steve. "Microsoft's New Firewall: Just Where Do You Think You're Going Today?" 4 October 2000. http://www.microsoft.com/isaserver/evaluation/ISAGiga.pdf. (15 May 2002).

5) "ISA 2000 Server Features Overview." Fact Sheets. http://www.microsoft.com/partner/businessresources/salesresources/factsheets/ISA_2000_Server_Features.asp. (15 May 2002).

6) Fratto, Mike. "Microsoft ISA Server Adds To A Firewall But Can't Replace It." 5 February 2001. http://www.networkcomputing.com/1203/1203sp2.html. (15 May 2002).

7) Mackin, J.C. Microsoft Internet Security and Acceleration Server 2000. Redmond: Microsoft Press, 2001.

8) "Results Are in: ISA Server Takes Top Honors in Third Industry Cache-Off." 3 May 2001. http://www.microsoft.com/isaserver/evaluation/competitive/tmfcacheoff.asp (6 June 2002).

9) "Release Notes. Microsoft Internet Security and Acceleration Server 2000 Service Pack 1." http://download.microsoft.com/download/ISAServer2000/readme/SP1/NT5/EN-US/ISA_SP1_Release_Notes.htm#contents. (24 June 2002).

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event