Global Information Assurance Certification Paper

What's Defending Your Network? – ISA Server 2000
Robert A Andrews II
Version 1.2f
December 17, 2001

When thinking about Microsoft's flagship products, several different software packages probably come to mind immediately. Products like the Windows 2000 and Windows XP operating systems, Exchange Server 2000, SQL Server 2000, and Office 2000 and Office XP all have been highly touted and promoted by Microsoft. These products have been very popular not only within the business world, but also in the home user market.

Although these are all excellent products that have earned their reputation in the industry, Microsoft publishes a much longer list of equally impressive software titles every year. One of those products is hidden deep within the vast Microsoft software catalog, and is probably the best kept secret in the industry. This product is the Internet Security and Acceleration (ISA) Server 2000.

Microsoft's ISA Server 2000 is the Windows 2000 version and successor of the very popular Microsoft Proxy Server 2.0. Both ISA Server 2000 and Proxy Server 2.0 are designed to stand between a company's internal network infrastructure and the public internet. They act as a barrier to help stop unwanted access to the private network from the public network. And like any good successor, ISA Server 2000 takes all the successful technology that was included in Proxy Server 2.0 and built on it to create a very formidable first line of defense for any private network.

A Quick Overview

ISA Server 2000 is available in two different versions to provide a high level of security to small, medium, and large networks.

> ISA Server 2000 Enterprise Edition – is a highly scalable version designed to provide Web caching, firewall services, and SecureNAT services for medium to large sized enterprise networks. This edition integrates with Windows 2000 Server or Advanced Server (with at least Service Pack 1) or Windows 2000 Datacenter Server, and the Windows 2000 Active Directory. This complete integration gives administrators the ability to create, centrally manage, provide failover protection, and load balancing using ISA Server Arrays. Multiple levels of security access policies can also be configured with the Enterprise Edition.
>
> ISA Server 2000 Standard Edition – is an ideal solution for small business, workgroups, and departmental environments. This edition provides the same Web caching, firewall services, and SecureNAT services of the Enterprise Edition. However, the Standard Edition can not be configured in an ISA Server Array, and only one level of security access policies (local policies) can be configured.

ISA Server Configuration Modes

Both editions of ISA Server 2000 can be configured in one of several different ways.

Caching Mode – ISA Server 2000 can be a fully functioning caching server.

Forward caching occurs when clients in the internal network make requests for web objects on the public internet. Both the request for the web object from the internal client and the response from the external web server passes through the ISA Server. As this happens, the ISA server saves a copy of the web object in its cache (for a certain amount of time) for later use. When another internal client later requests the same web object, it can be returned from the ISA server's cache rather than searching for it on the public internet.

Reverse caching works in the same way that forward caching works. The only difference is in reverse caching, the request for a web object is initiated on the public internet to the internal network. All requests and responses again pass through the ISA Server and those web objects can be cached.

Firewall Mode – ISA Server 2000 can act as a fully function and integrated firewall server. When in firewall mode, the ISA Server has the ability to control what requests and responses are allowed to pass through the server.

The ISA Server firewall controls access internally and externally using filters. There are several methods of filtering through the ISA Server including IP Packet Filtering, Circuit Level (Protocol) Filtering, Dynamic Filtering, and Application Filtering. Access is also controlled through the firewall server via Secure Publishing which will be described later.

Integrated Mode – Not only can ISA Server 2000 act as caching server or a firewall server, but it can act as both. In Integrated Mode, ISA Server will give a network all the benefits of the caching server and the benefits of the firewall server.

ISA Server 2000 also has the ability to help hide a private network using a private IP addressing scheme. SecureNAT can be configured on the ISA Server to provide network address translation between internal private addressing scheme and the public internet.

ISA Server Security

ISA Server 2000 integrates into a network strategy to provide many types and levels of security. The integration of Windows 2000 and ISA Server 2000 can create a very effective first line of defense for a network of any size. ISA Server also allows the integration of third party tools into the server to provide for an even greater line of defense for a network.

Caching Mode Security

When ISA Server is configured as a caching server, it will provide a network with a certain level of security. As described earlier, ISA Server can be a forward caching or reverse caching server. When on a network, all web related requests are forwarded to the internet and internally through the ISA Server acting as a web caching server. This is the old Proxy Server 2.0 technology at work.

Proxy Server 2.0 is mentioned here because that is exactly the way ISA Server 2000 acting as a web caching server works. Proxy Server 2.0 got its name because it was providing security to an internal network by acting as a 'proxy' (an intermediary) between networks. When an ISA Server sits between two networks (ex: a private internal and the public internet), all web related requests can be made through the ISA Server.

In an example of explanation, consider a web request originating from a client on an internal private network to a public web server like www.yahoo.com. In this situation (forward caching), the following steps will occur:

1. The internal client makes a request for a web object from www.yahoo.com.
2. The internal client request is sent to the ISA Server acting as a caching server.
3. The ISA Server takes the request and evaluates the parameters of the request, and checks to see if the object already exists in the ISA Server's cache. (If the object already exists in the ISA Server's cache and the object is still valid, the ISA Server will return the object to the internal client without connecting the public web server at www.yahoo.com.)
4. If the content does not already exist in the cache, the ISA Server then contacts the web server at www.yahoo.com and makes the request for the web object on behalf of the internal client.
5. The web server at www.yahoo.com returns the requested web object to the ISA Server.
6. The ISA Server takes the web object and saves it to cache for a predetermined and configured amount of time.
7. The ISA Server then returns the web object to the original internal client on behalf of the web server at www.yahoo.com.

When ISA Server is configured as a forward caching server, the level of security it provides is that the internal clients never have a direct connection to potentially dangerous web servers or other clients on the public internet. Because of the caching, the ISA Server does not have to access public internet as often. This reduces their exposure to danger in certain situations.

Reverse caching by an ISA Server also provides and internal network a level of security. Web Publishing (Secure Server Publishing) is a feature of ISA Server that works with reverse caching to offer security for web servers located on the internal network that are configured to provide web objects to the public internet.

With a web server published by an ISA Server and the appropriate DNS records updated, clients from the public internet are directed to the ISA Server instead of the web server. The ISA Server will evaluate the request, retrieve the appropriate web objects, and return the web objects to the requesting client. As with forward caching, the public internet client never has a direct

connection to the internal web server. The ISA Server acts as the proxy between the public internet clients and the internal web server.

To further the security offered by reverse caching, ISA Server can be configured to perform Active Caching and/or Scheduled Content Downloads. When Active Caching is configured on the ISA Server, the cache is evaluated and ranked. The most popular and active web objects are automatically refreshed by the ISA Server when their cache TTL (Time To Live) expires. When Scheduled Content Downloads are configured, the ISA Server will refresh the desired web objects at the appropriate intervals automatically.

Both features help to provide the most up-to-date content to the clients requesting web objects at a faster speed, and both features help make it unnecessary for the ISA Server to make a direct connection to the internal web server when a public internet client is connected to the ISA Server.

Finally, when ISA Server is configured as a caching server, one last level of security can be configured. Client and Destination Sets can be configured to control access to web objects on internal web servers, and what clients get access to them. Destination Sets control where requests from public internet clients are directed to inside the internal network. Client Sets control what clients on the public internet are granted or denied access to web objects on internal web servers protected by an ISA Server.

Firewall Mode Security

When ISA Server is configured as a firewall server, it provides a different level of defense. As discussed earlier, ISA Server is a fully functional and integrated firewall server. It can act as a secure gateway between clients on an internal network and the public internet. This is a new technology for the ISA Server and is a significant upgrade from Proxy Server 2.0.

ISA Server configured as a firewall server employs several levels of filtering to protect an internal network from outside intruders.

IP Packet Filtering

When packet filtering is enabled on an ISA Server 2000, traffic entering the server through the external interface is examined before it is allowed to pass through the server. As the packets are evaluated, they are dropped unless they are explicitly allowed. This filter is applied is applied before the packets are sent to any other filters in the ISA Server.

IP Packet Filtering in ISA Server is applied to ports, and is configured to either completely Allow access or Deny access to the specific port. IP Packet filters can be applied to evaluate incoming traffic for specific network services (ie. SMTP, DNS, etc.), port numbers, or source or destination computer name. This allows ISA Server to block packets from specific sources on the public internet.

IP Packet filters also help ISA Server detect packets that are involved in some of the most common network attacks. This is through the Integrated Intrusion Detection mechanisms of the ISA Server.

> ***FYI*** *- Microsoft has licensed technology from Internet Security Systems (ISS), Inc (www.iss.net) to be the base of the intrusion detection system for ISA Server. ISS, Inc is the developer of the RealSecure™* Protection *System and now owns the widely popular BlackICE Defender.*

Some of the attacks that ISA Server can detect are All Ports Scan Attacks, Enumerated Port Scan Attacks, IP Half Scan Attacks, Land Attacks, Ping of Death Attacks, UDP Bomb Attacks, and Windows Out of Band Attack.

When ISA Server detects such an attack, it can be configured to any one or more of serveral different actions. Some of these actions include writing information to the Windows 2000 Event Log, triggering alerts that email system administrators, executing a predefined scripts, or even shutting down the services running on the ISA Server.

Ciruit Level (Protocol)Filtering

Circuit Level Filtering allows the ISA Server to perform 'stateful inspection' of data sessions to the server. Sessions are inspected (monitored) to determine whether or not they are valid. If the session is determined to be valid by the filtering, then the session is allowed to pass through the firewall service.

ISA Server determines whether or not a session is valid by comparing the session to a set of rules that are configured on the server. All packets are denied and dropped by default unless they are explicitly allow by the configuration settings of the ISA Server.

Circuit Level Filtering is also the mechanism that allows the ISA Server to evaluation and control sessions that require multiple connections. An example of this is internal client connections to an external FTP server.

Application Filtering

When Application Filtering is configured on an ISA Server, data streams can be evaluated for specific applications. Application filters give ISA Server the ability to inspect, screen, block, redirect, or modify data that goes through the server. Application-level firewall filters also have the ability to provide detailed session logs and user authentication when configured.

As an example of an application filter, ISA Server comes with a predefined filter to evaluation SMTP traffic. This filter can be configured to block all executable (.exe) attachments from making their way through to a client desktop through an email application. Other predefined application filters that are included with ISA Server are:

- HTTP Redirector Filter

- FTP Access Filter
- SOCKS Filter
- RPC Filter
- H.323 Filter
- Streaming Media Filter
- POP and DNS Intrusion Detection Filters

ISA Server also has the ability to integrate other 3rd party tools into the Application Filtering functionality to provide filtering for a wider range of applications. An example would include LANguard Content Filtering and Anti-virus for ISA Server (www.gfisoftware.com/lanisa/index.html).

LANguard was developed to integrate seamlessly with ISA Server and provide internal networks with protection from viruses, Trojans, and questionable material. Among its other features, it can also be configured to quarantine file downloads until they are deemed safe for the network environment.

LANguard is not the only 3rd party tool available to integrate into the ISA Server. Other 3rd party tools are also available and include:

- SmartFilter (www.securecomputing.com)
- Websense Enterprise (www.websense.com)
- SurCONTROL (www.surfcontrol.com)
- InterScan WebManager (www.trend.com)
- N2H2 Filtering (www.n2h2.com)
- Chaperon 2000 (www.cornerpostsw.com)
- bt-ifilter (www.burstek.com)
- X-Stop XLM 4.5 (www.8e6technologies.com)

Dynamic Packet Filtering

The final filtering method offered by ISA Server is Dynamic Packet Filtering. This method of filtering allows the ISA Server to respond automatically to requests for access through the server. With Dynamic Packet Filtering, all ports remain closed. The only time a port is opened, is when a request for services meets all the configured requirements. The port only remains open for the duration of the connection. As soon as the connection is terminated, the port is closed and remains closed until another connection meets the requirements to open it.

Integrated Mode Security

When an ISA Server is configured in Integrated Mode, it simply means that both the Web Caching service and the Firewall service are running at the same time. In Integrated Mode, the ISA Server is able to combine all the security features of both services to offer multiple levels of defense for an internal private network.

SecureNAT Security

ISA Server 2000 provides another level of protection for internal private networks. Secure Network Address Translation allows the IP addressing scheme of an internal private network to be a private IP addressing scheme.

Because private IP address ranges are not routable on the public internet, SecureNAT offers an internal private network the extra security of not being visible to possible intruders from the public internet. The SecureNAT drivers of the ISA Server translate IP traffic from the internal private network to the public internet and vice a versa. This translation is transparent to all clients involved in the network communication. The public internet clients never see the private IP address of the internal client. The public internet clients only see the external interface of the ISA Server.

Other Security

Because ISA Server 2000 integrates seamlessly into the Windows 2000 Server operating system, it can take advantage of many of the security features included with the operating system. These features can add yet another level of security to an ISA Server that is protecting an internal private network.

Some of the extra features include:

- Virtual Private Networks (VPNs) for secure connections through the public internet.
- System Hardening to lock down the operating system and protect it from potential security breaches.
- Windows 2000 Active Directory or Windows NT SAM for support of almost all the authentication types that Windows 2000 supports.
- Policy-Based Management for ease of administration and security configuration.
- Windows 2000 Logging and Alerts to help identify problems, threats, and security breaches immediately.

Conclusions

With all the different levels of defense that ISA Server 2000 offers, it becomes a natural choice for a line of defense for any private network. Even though it is never the best choice to have a single product from a single vendor protecting a private network, ISA Server is a very good starting point of any network.

Integration with several 3rd party tools makes ISA Server an even more attractive choice for defending a network. Even if ISA Server is chosen to be a line of defense in addition to an existing firewall or other defense system, the ISA Server will provide the flexibility needed to react to the changing threats a network can face.

Upgrading from a current system running Proxy Server 2.0 is also a very good idea. Proxy Server 2.0 systems have served networks very well in the past, but ISA Server 2000 offers an upgrade in technology and security too significant to ignore. Considering also that Proxy Server

2.0 must be installed in conjunction with Internet Information Server (IIS), the potential security risks of not upgrading are too high. ISA Server can integrate into a Windows NT 4.0 network and provide more protection than Proxy Server 2.0 can even if the whole network is not ready to upgrade.

References:

1. Microsoft, ISA Server 2000, Firewall Security Services with Microsoft Internet Security and Acceleration Server 2000, May 11, 2001 http://www.microsoft.com/isaserver/techinfo/planning/FirewallSecurity.doc, (Dec 1, 2001)

2. ISAserver.org, Access Control, http://www.isaserver.org/software/access_control.htm, (Nov 29, 2001)

3. Daily, Sean, Features and Benefits of ISA Server 2000, InstantDoc #9745, August 14, 2000, http://www.win2000mag.com/Articles/Index.cfm?ArticleID=9745&Key=Proxy%20Serv (Nov 30, 2001)

4. ISAserver.org, Content Filtering, Keeping corporate web use productive and secure, http://www.isaserver.org/pages/wp/content%20filtering.htm (Dec 1, 2001)

5. Mackin, J.C., MCSE Training Kit: Microsoft Internet Security and Acceleration Server 2000, Redmond, Microsoft Press, 2001

6. Bragg, Roberta, MCSE Training Guide (70-227): Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Chicago, New Riders, 2001

7. Simmons, Curt, Microsoft ISA Configuration & Administration, New York, Hungry Minds, Inc, 2001