Global Information Assurance Certification Paper

Andrew W. Wills
Version 1.4b
GIAC Security Essentials Certification Practical Assignment 1 Option 2
Using Microsoft ISA Server as a Cost-Effective Firewall Solution

Abstract

Many small organizations and home users have no security measures in place to protect their electronic data and computing resources from Internet attacks and security breaches. Often, these groups are forced to work with minimal budgets to provide some type of security defense, or, as the only other alternative, have none at all.

In this practical, I explore the rationale of why small business and home users have important security needs just as large corporations do. To help illustrate my point, I walk through a case study presenting myself and a small organization for which I do consulting work. I present the initial analysis of the situation, the implementation plan, lessons learned, and items of consideration for others who may be in a similar situation.

Table of Contents

Introduction

In a time where corporate scandals are numerous and Internet hackers are born overnight, companies have an increasing responsibility to determine the value of their electronic resources and to estimate monetary importance should security be compromised. Large corporations have plush budgets for information security and can afford to implement and integrate all of the latest technological advances into their overall corporate network structure; however, small companies and home users simply do not have either the human resources or monetary assets to devote to network security. Does this make their data less important? Does this leave them less vulnerable to intruders?

The above questions pose an interesting dilemma for this group of users. Perhaps their minimal size does leave them at a lesser risk for attack, but their information is often just as valuable as any large corporation. Maybe their visibility is not as vast as a Fortune 500 company, but many hackers realize that it may be an easier target for them to exploit.

Corporate IT staff members and senior level management must ask themselves several difficult questions to determine their level of risk. Inquiries such as "How important is securing corporate computing resources?" and "What would happen if an intruder gained access to the company network?" must be examined and answered to help them assess their level of risk.

The aforementioned items are almost always of great important to any company regardless of their size and to individuals who possess and maintain important data on home resources. One recurring motif, though, is that many of these smaller users simply do not have the monetary resources needed to provide the level of security to protect their important resources leaving the nagging question of what this class of users must do in order to protect information.

Another item of great interest is that many security breaches often occur within the corporate network's boundaries providing another level of concern to the management of an organization (Cioara 5). Not only does management have to be concerned with Internet-based attacks on their networks, but they must also be aware of inside attempts to breach security.

What Does an Information Security Breach Cost?

Even though the above questions are important to consider when planning for network security, it is even more important to determine what might happen should network security be compromised from either inside or outside the corporate infrastructure. Many of these items are covered adequately within a disaster recovery plan if a corporation has exerted the effort to compile one. Most of these plans contain obvious replacement costs for equipment and resources lost to forces of nature. In addition, they typically outline a data

backup plan and media storage strategy. But, companies tend to ignore the human resource costs of either recovering from a natural disaster or a network intrusion. These elements should be an integral part of any disaster recovery plan.

Though it is very difficult to think of many positive items that have come from our Post-September 11 era, one important factor that has been given more attention is security and recovery from disasters since terrorists may also choose to attack company resources rather than traditional terrorist activities. But, are companies actually realizing the total amount of monetary resources that it would take to recover from any type of security compromise, whether it is from a terrorist or a sixteen year old Internet hacker?

George V. Hulme states that "losses attributed to security breaches in the United States are trending down" (1). A security expert interviewed in the article states that costs are not necessarily spiraling downward because of a decrease in security breaches, but rather that companies are valuing their intellectual and computing resources lower than before (Hulme 1). This illustrates that many of the larger companies are paying more attention to the actual cost associated with recovering from security breaches.

Though larger companies are certainly more aware of these costs, many smaller companies and home users simply either do not think about these issues or do not have the time or money to invest in such an analysis. Theoretically, intruders could still gain access to important company information if an employee works on company-related business from home or if they hire an outside consultant to work with classified information.

Experiences with Security in Small Organizations and Home Users

One of the primary reasons I am discussing the above points is that I do consulting work for a very small organization where I am the IT department. I am paid on a consulting basis and almost all of the work I do for them is completed at my home. An interesting caveat also brought about by this situation is that the majority of work that this small company does is for a very large, well-known, national client. The large client has invested the time and monetary resources to ensure customer information privacy within their network boundaries, but they have never asked if we have security measures in effect to help protect their trade secrets and customer data that we manage for them.

To further complicate the matter, not only should they be concerned about the small organization's security, but they should also be somewhat worried about who handles the information outside of both organizations. Through the four years that I have done work for this small organization, none of these questions have ever been posed by management from either side to determine whether security for electronic data is in place.

After becoming more experienced with security issues, I posed some of these questions to the small organization to help assess our levels of risk. With new federal privacy laws in place, these issues simply cannot be ignored any longer. Part of the dilemma is that both I and the small organization simply do not have thousands of dollars to throw at the problem to ensure it is adequately solved. We both needed a cost-effective solution to ensure that we are able to state with confidence that we are handling their data in a secure fashion.

Current Structure

Before I discuss the chosen solution for our problems, let me first outline the structures of the networks at both my home and at the small organization.

As a home user, I had already implemented some security measures. I have a broadband cable modem connection and one standalone machine. Immediately after obtaining cable service, I purchased a LinkSys Cable Router so that I could share my broadband connection with my laptop computer. Next, I installed Norton Internet Security 2002 as a software firewall to run on my Windows XP machine since it houses all of the confidential consulting data. The cable modem directly connects into the router to provide connectivity to my desktop and laptop computers.

The small organization has a business DSL connection. A DSL Modem/Router brings the connection into a switch that provides networking to all of the workstations. A centralized server is also installed and connected to the same switch. The Windows 2000 Server acts only as a file server within this environment. With the exception of NAT provided by the DSL Modem/Router, no other security exists on this network.

Disaster Recovery Plan

As a home user, I must admit that I have no formal disaster recovery plan in place simply because I had never given it any thought. Just because I do not have a written plan, though, does not mean that I do not practice good habits with the information I store and maintain on my home computer. With mission critical data, I ensure it is backed up to avoid substantial losses in the event of a hardware failure or a security breach. I keep backup media secured in a small fire-proof home safe to help recover essential information to my consulting work should the unexpected occur.

Much like me at home, no formal disaster recovery plan existed within the organization. I had setup a daily backup plan for them where media was stored in a fireproof safe. In addition, we did have a limited form of offsite storage and data replication because I had most of the electronic data stored in various places on my home computer. Those were the only components of a plan that were in place.

After working through the Disaster Recovery Plan in the GSEC curriculum, I decided that this passive attitude would no longer work and I must have something in place in both locations. I felt I could implement better network security at home and at the office, along with a formal disaster recovery plan at the office at the same time.

The Analysis

After realizing that both networks were very insecure, I decided to conduct some research to determine what software firewall would be the best fit for the organization and at home. It was important to me to have similar configurations at both my home and at the office to provide ease of implementation and maintenance since part of my consulting duties at the company consists of the role of Network Administrator.

Through my analysis, I evaluated and researched several different products manufactured by Symantec, Network Associates, and Microsoft. Part of my research included reading technical reviews and case studies in similar-size organizations. I found it very difficult to find many reviews or opinions on using a dedicated server/firewall in a home environment, so I decided to strictly focus on how it performs in a small business environment and deduced it that strategy would be adequate for my home network.

One of the most challenging aspects through this entire process was convincing the president of the small organization that a firewall was a necessity. She agreed that in theory we required protection, but was extremely hesitant about implementation without having viable facts that security breaches were indeed a threat to the organization and the protection of customer information.

As a compromise, we agreed to upgrade one of the spare computers at the office with more memory and a better processor and use trial versions of the software package I selected to determine if this would meet our needs. The primary reason why I agreed to this is that it provided us with an immediate, though temporary, solution to address the security concerns. Furthermore, it would also provide me with the justification I needed with factual information in the software application logs illustrating attacks to convince her to invest the financial resources needed to implement a software firewall solution on a permanent basis.

At home, I already had a spare computer whose hardware would be more than adequate as a server running a firewall software package. In turn, I also was going to implement trail versions of the software packages to give me a good basis for comparison after these items had been in use for a reasonable period of time.

Selecting the Right Solution

A cost-effective solution that answers many of the aforementioned questions rests with Microsoft ISA Server 2000. This software package provides a good level of security combined with a price tag that does not drain financial resources. Its ease of implementation and relatively low cost of ownership provides a respectable combination of security for the financial resources needed for implementation.

Though Microsoft ISA Server is traditionally seen in larger enterprise environments coupled with the use of other security devices, it also works very well in a small environment often when it is the only device providing security to the network.

Another important consideration that influenced my decision to select Microsoft ISA Server was that Microsoft offers both trial versions of Windows Server software and Microsoft ISA Server. Utilizing those in conjunction with existing hardware at both locations provided an ideal environment to implement this solution.

Lastly, I chose Microsoft ISA Server because it has been certified by ICSA Labs, one of the industry's most respected-independent laboratories. This certification gave me a great amount of confidence that this product would provide a good level of security for our needs and modest budget (Smith).

Features of Microsoft ISA Server

Though the above reasons provided enough justification to try Microsoft ISA Server, the primary features it offers as a software firewall really convinced me to use this product at both locations.

The most important feature Microsoft ISA Server provides is its ability to provide firewall functionality. Its ability to secure internet connectivity from both outside and inside the network through a multi-layer approach works as an efficient approach to provide first level security (Course 9). Even though Microsoft ISA Server lacks adequate internal security, it was really not a factor when I selected Microsoft ISA Server simply because I am the only IT person within that organization (Fratto). External security was our primary focus of concern.

Microsoft's multi-tiered approach to software firewall security was ideal for our scenarios. Firstly, ISA Server employs packet filtering that accepts or rejects incoming and outgoing packets based on services, devices, and/or port numbers. Secondly, it also provides circuit-level or protocol filtering opening ports only when needed, thereby increasing network security. Lastly, ISA Server provides application-level filtering giving it the ability to customize network traffic based on the application requesting access (Course 9-13).

After conducting this research, I was convinced that these items provided us with a great software firewall framework for both locations because our networks were small and non-complex (Fratto).

As an added bonus Microsoft ISA Server provides the ability to setup Virtual Private Networks to facilitate multiple office locations. Furthermore, additional features such as secure publishing and e-mail content screening provide pertinent services to small organizations and home users without the need for additional software or hardware. Though these items were not immediately needed in the present or the immediate future, it was appealing to know we could utilize these should the need ever arise.

A second major task of Microsoft ISA Server is the ability to provide caching. Many organizations simply do not have the monetary resources to lease T1 or similar high-speed Internet connections, as in our case. Because slow response times can be inconvenient or even unacceptable, the caching feature of Microsoft ISA Server can provide a small boost in the overall speed of the connection the users realize when performing tasks without incurring the additional costs of faster connections. This was another attractive benefit for us since one of the constant complaints I receive from my users is that the DSL connection becomes consistently slow during peak usage times within the office.

Flavors of Microsoft ISA Server

Microsoft ISA Server 2000 comes in two flavors—standard and enterprise editions. The enterprise edition comes with a wide range of additional features that are targeted toward large organizations planning to utilize several ISA servers within their network, along with a $4,000 increase in price. Because of these reasons, the standard edition was a better fit for both locations and a trial version was available for it.

The Implementation

The purpose of this practical is to discuss how I implemented this solution at both locations to solve our problems, not a step-by-step guide on how to implement Microsoft ISA Server in this type of a situation. Because of this reason, the information presented below will be mostly summary data and should not be interpreted as a step-by-step guide.

To better acquaint myself with Microsoft ISA Server, I decided to implement it at home first and then use the experience garnered to implement it at the office location. During the process, I installed a fresh copy of Windows Server 2003 on my spare computer to prepare it to be used as a server. I installed and configured two network cards; one to be used for the internal network and one to be used for the external network. Furthermore, I revamped my network topology

to utilize a small hub to share the connection to both my desktop machine and my laptop computer.

One of the features that I really appreciated with Microsoft ISA Server is that it denied ALL access until I configured it with the proper policies and rules. To me, this was a very positive feature of the software since it illustrated a fundamental concept in information security—block all access and grant only what is required. Though I had to configure several rules, this paradigm provided a more secure network environment.

At home, I knew that I did not want to restrict access to particular websites and I wanted tremendous flexibility mixed with an appropriate level of security. Therefore, I decided not to implement any content filtering. After speaking with the small organization's president, we both determined that blocking particular websites served no useful purpose since no major problems with employees abusing their Internet access have been discovered. Furthermore, I wanted all of my connection's bandwidth at home associated with any computer attached to the network, so I chose not to implement any bandwidth restrictions on my home network and we agreed not to impose any at the office.

Another concern for implementation was I wanted to ensure the underlying Windows operating system was as secure as possible. Microsoft ISA Server included a wizard to help choose a security level to automatically implement. Because both servers will be only used as firewalls, I configured both as dedicated firewalls.

Since both locations were strictly Microsoft shops, all of our applications were very standard and all core services (such as e-mail and website hosting) were outsourced. Because of that, there was no need to define any additional protocols other than TCP and UDP. Likewise, I chose to utilize only Packet Filtering and disable IP Routing and to leave all default packet filters enabled.

Since tweaking the web caching feature was not necessarily that much of an advantage for one user at home or for eight users at the office, I decided to leave it at its default level.

Next, I configured my home machine to point to the ISA Server for both DNS and as the default gateway. I configured my web browser to automatically look for a proxy server and I had Internet connectivity on my home machine once again.

Lastly, as a final security checklist, I went through and enabled Intrusion Detection, disabled the Client for Microsoft Networks on the external interface, and disabled NetBIOS over TCP/IP on the external interface to provide a greater level of security.

Now that my Microsoft ISA Server was running smoothly, I went to the small organization and mirrored the same installation there. With the experience I gained from the installation at home, the amount of time I spent configuring the new server there was quite minimal and everything appeared to be running quite smoothly. As an advantage, both locations were already using private IP addressing, even though I had to configure each client at the office (and at home, as mentioned above) to look to the ISA Server for DNS and for the default gateway.

The implementation experience was certainly an educational one and illustrated the important concept that textbooks and the Internet are great research tools, but cannot replace the real education involved with actually conducting the implementation yourself.

Post Implementation Challenges, Concerns, and Successes

Both locations have been using the new software firewall for almost one month. No major complaints from my users have surfaced and functionality is essentially transparent to them.

Even though things appeared to run smoothly after implementation, I had some immediate concerns. I feel the server operating system deserves more attention to ensure its security. Furthermore, I'm going to work diligently on creating very specific, custom rules to further restrict incoming and outgoing access to the Internet now that I have more experience with Microsoft ISA Server 2000.

One additional issue that must be addressed is allowing streaming media to each individual workstation within the small organization. Due to the nature of our business, this type of median will become more prevalent in the upcoming year. I will need to ensure that the Microsoft ISA Server is properly configured to handle those types of requests, yet still maintain its overall security.

Through my research, one item of interest is that Microsoft ISA Server lacks the ability to provide real protection from internal attacks on the network. This is a serious drawback for the software package if it is used in a larger organization. It is an important consideration for anyone who is thinking about utilizing Microsoft ISA Server as a firewall, but really was not much of a factor for the small organization and my home environments where this was implemented (Fratto).

On a positive note, two very advantageous items have stemmed from the implementation of a more secure network—the value of our data and a formal disaster recovery plan. Though not an IT person, the president of the company has become more aware of potential security risks toward the organization.

The web caching feature of Microsoft ISA Server has also yielded good results in that a couple of employees have stated that the connection seems faster when

everyone is accessing information via the Internet. After analyzing the server performance monitor, the server confirmed what the employees had stated. It seems as if Microsoft ISA server has provided a very positive acceleration for the DSL connection in that environment.

Furthermore, we have devised a formal disaster recovery plan to ensure the as-smooth-as-expected operation of the corporation should a security, natural, or terrorist disaster occur. Lastly, we have estimated the quantity of financial and monetary resources that it might take to recover from different levels of disasters, ranging from a Denial of Service attack to a fire that destroys everything. Certainly everyone hopes that the unthinkable never happens, but should it, we are certainly more prepared than before to deal with the consequences.

Are Our Networks More Secured?

From a managerial perspective, the question "Are Our Networks More Secured?" must be answered after implementation of security devices. After examining security logs at the organization and at home, I found that nothing dramatic had really happened other than several port scans.

Even though these were not some of the more publicized security breaches, it is still very important to realize that these were now stopped by the Microsoft ISA Server and that our network is more secured because of this implementation. Though we have no basis of comparison since we had virtually no security before, it is important to remember that these actions have minimized the likelihood that our security will be compromised.

Conclusion

This entire process has been nothing less than an amazing educational opportunity for me through the entire security assessment of a network—from conception to completion. Most importantly, I had precise boundaries in which I had to work and very limited budgets to achieve my goals.

Since implementation of the test systems, I have convinced the president of the company to purchase the necessary full versions of Microsoft ISA Server and additional Windows 2000 Server licenses so that we can put this into full use both at my home and at the office. Currently, this low-cost solution to a firewall in a simple-network situation has proven to be an excellent decision.

Works Cited

Allen, Doug. "Strategies & Issues: Cost-Cutting Strategies at Mission Control." Network Magazine 5 Mar. 2003. 4 Jul. 2003 <http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleID=8703511>.

Cioara, Jeremy. MCSE Guide to Microsoft Internet Security and Acceleration (ISA) Server 2000. Boston: Course Technology Division of Thompson Learning, 2002.

"Cyber Attacks Continue, but Financial Losses Are Down." Computer Security Institute. 4 Jul. 2003 < http://www.gocsi.com/awareness/fbi.jhtml>.

Fratto, Mike. "Microsoft ISA Server adds to a firewall, but can't replace it." Network Computing 5 Feb. 2001. 4 Jul. 2003 <http://www.networkcomputing.com/1203/1203sp2.html>.

Garg, Ashlish. "What Does an Information Security Breach Really Cost? Evidence and Implications." Information Strategy: The Executive's Journal Summer 2003. Ebsco Research Databases 4 Jul. 2003. <http://www.ebsco.com>.

Hulme, George V. "When Security Helps Stem Business Losses." Information Week 23 Jun. 2003. 4 Jul 2003 <http://www.informationweek.com/story/showArticle.jhtml?articleID=10700729>.

Miastkowski, Stan. "Step-By-Step: Bulletproof Your PC with a Software Firewall." PCWorld Aug. 2003. 9 Jul 2003 <http://www.pcworld.com/howto/article/0,aid,111124,00.asp>.

Microsoft Corporation. "Caching with Internet Security and Acceleration Server 2000 White Paper." 22 May 2001. 4 Jul. 2003 <http://www.microsoft.com/isaserver/techinfo/planning/cachingwp.asp>.

Microsoft Corporation. "Security with Internet Security and Acceleration Server 2000 White Paper." 8 Jun. 2001. 4 Jul. 2003 <http://www.microsoft.com/isaserver/techinfo/planning/firewallsecuritywp.asp>.

Shinder, Thomas. "ISA Server Security Checklist – Part 2 Securing the ISA Server Configuration." ISAServer.org 5 Feb. 2002. 8 Jul. 2003 < http://www.isaserver.org/tutorials/ISA_Server_Security_Checklist__Part_2_Securing_the_ISA_Server_Configuration.html>.

Smith, Del. "Why ISA Server is a good solution for SMOs." 11 Apr. 2001 < http://www.techrepublic.com/article.jhtml?src=search&id=r00220010411del01.htm>.

Last Updated: July 24th, 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
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
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 Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	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 Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
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
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