GCFW Practical

John
Swartzendruber

GCFW Practical
Version 4.0

Date: November
20, 2004

Abstract

The document consists of three sections, followed by an appendix and a listing of references.

Section one is a short research document on the topic of Biometric Security. Focusing primarily on Fingerprint Recognition, it starts with a brief introduction to Biometrics, gives a description of how fingerprint recognition works, and explains the types of errors that can occur. After a discussion of benefits and problems associated with biometrics, the paper presents trends in the field and implications on perimeter security. The section concludes with things to consider before implementing biometric recognition in a business setting.

Section two describes a small business in the fortune cookie saying industry. It presents the requirements for implementing a network capable of running an e-commerce operation, including the access needs of a variety of people. It then documents the systems involved in enabling the business operation, and includes a discussion of the security philosophy for the business.

Section three documents the firewall configuration for implementing the business solution from section two. A description of the different sections explains what need the configuration is trying to address, and how the implementation meets that need.

The appendix is simply a complete configuration listing for the firewall.

Table of Contents

List of Figures

Assignment 1 – Biometrics and IT Security

Background / Introduction

Accurate identification of people accessing just about anything has been an issue for those in charge of security since way before the days of computers. Whether it is having possession of a key, knowing the secret knock or password, or as simple as being recognized by a guard, people have developed many methods for allowing access to some while denying access to others.

With the introduction of computer systems and even more so with the rapid growth and acceptance of the internet as a medium for doing business, the requirement for accurate identification has compounded greatly. For years, knowing a user ID and password have been an acceptable means of gaining access. In some situations the added security of a token or smart card was deemed appropriate. More recently, there has been an increased interest in biometrics as a preferred means of identification.

Just what is biometrics? Is it a ‘silver bullet’ for the security world, providing the perfect mix of security, usability and affordability? Is now the time to look at implementing biometrics recognition for your computer systems? In this assignment I will explore these questions, and hopefully start you down the road to finding your own answers.

Problem Domain

The first step in keeping the bad guys out while allowing the good guys in is to be able to quickly and accurately differentiate between them. And even the good guys need to be kept in their own application areas, and not allowed to roam freely throughout the realm. Accurate personal identification is a must for implementing security.

In the computer world, UserIDs and passwords are the most common means of identifying users, and it is convenient for the user since the user carries the knowledge of the password with them at all times. As long as the password is known only to the user it is reasonably secure. But passwords which are easily remembered are also frequently easily guessed. Passwords which are hard to remember are frequently written down somewhere easily accessible. And a password may be observed by a curious bystander. These points raise concerns about the real security of password based authentication.

Another popular means of identification involves the use of tokens. With a token, you must have something as well as know something, so there is an additional layer of security. However, there is additional cost and complexity involved with this solution. For the user, there is now the need to have this token with you anytime and anywhere you need to access the system. And for the administrators there is the additional overhead of another system to maintain.

The challenge is to find a method of identifying users that is accurate, easy to use, easy to administer, and easy to get into the budget! Many advancements have been made and continue to be made in the field of biometrics.

Introduction to Biometrics

> A *biometric system* is essentially a pattern recognition system that recognizes a person by determining the authenticity of a specific physiological and/or behavioral characteristic possessed by that person.[1]

Biometric identifiers such as fingerprints, signatures, facial features, voice, iris and retinal scans provide a means of identification simply by using a unique physical aspect of a person. Biometrics is a term commonly used to refer to the automated process of recognizing a person by one of these identifiers.

The idea of biometrics is not new. Fingerprints have been used for identification for over a century, particularly in law enforcement. But many years before that, Egyptians used physical characteristics such as size, face shape, complexion and scars to help identify the workers building the great pyramids.[2] But it is just in more recent years, particularly since 9/11, that interest in biometrics has really taken off.

As mentioned above, there is an assortment of identifiers that can be used. When they are compared in terms of how easily they are collected, how stable the identifier remains over the years, how distinctive they are from person to person, and how well they are accepted by the users; it can be seen that they all have their own strengths and weaknesses. Because of their good balance of a variety of factors (nearly everybody has them, they are distinctive, they are generally permanent, images are easily collected), fingerprints are the most commonly used biometric identifier, claiming a 52% market share.[3] The rest of this assignment will focus on fingerprint recognition.

[1] Maltoni, Maio, Jain, Prabhakar. Handbook of Fingerprint Recognition, p 3
[2] http://www.out-law.com/php/page.php?page_id=debunkingsixmyths1089377584&area=news
[3] Biometric Market Report 2003-2007, http://www.kiosks.org/pdfs/BMR_2003-2007.pdf

The Basics of Fingerprint Recognition

The first and most basic step of fingerprint recognition is to acquire an image of the fingerprint. An off-line image can be made by using ink on the fingertip and pressing the finger on paper to make an impression. The paper image can then be scanned to get a digital representation. A live-scan image is acquired by using a sensor that is able to scan the fingertip directly, and create a digital representation of it. The rest of this paper will assume the use of live-scan images.

There are four primary types of live-scan fingerprint acquisition.[4]

1. FTIR/optical: This is the most mature live-scan technology. FTIR stands for Frustrated Total Internal Reflection, and involves a fingertip pressed against one side of a prism, and a CCD or CMOS camera converting the reflected image to a digital representation. Because the dampness of skin can vary its reflective nature, it also impacts the quality of the image.
2. CMOS Capacitance: The ridges and valleys of a fingertip, when pressed against a CMOS chip grid, create an accumulation of different electrostatic charges, which can be converted to a digital value. The quality of the image is affected by the dampness of skin, the small size of the scan area is problematic, and the sensor can be affected by electrostatic discharge.
3. Thermal: The sensor is made of pyro-electric material. A finger is swiped over the sensor, which measures changes in temperature. These sensors are supposedly less affected by skin dampness, but they are limited in the dynamic range or gray scales that they are able to produce.
4. Ultrasound: An ultrasonic beam is used to scan the fingertip, and the ridge depth is determined from the reflected signal. Skin dampness and other contaminants affect this method less, and the image is a better representation of the actual topography of the ridges and valleys. However, the sensors tend to be large, and take a longer time to acquire an image.

Once an image of the fingerprint has been acquired, the second step is to determine the print's unique characteristics. A fingerprint contains ridges and valleys, which form the loops, whorls and arches. The main features of a fingerprint which are used in recognition systems are ridge termination, where the ridge actually ends, and ridge bifurcation, where a single ridge splits into two ridges. These terminations and bifurcations are called minutiae.

Step three takes the locations, size, quality and type of minutiae found in step 2, and from these creates a template. The template is stored in a central database, on a local workstation, or even on a smartcard. These three steps involved in acquiring and storing the template are referred to as the enrollment phase.

[4] Ratha, Senior and Bolle. "Automated Biometrics". http://researchweb.watson.ibm.com/ecvg/pubs/ratha-auto.pdf

The final step is where the actual biometric recognition takes place. A new image is acquired through a repeat of steps one and two, and this new image is compared to one or more stored templates to determine if a match exists. When the images are compared, they are given a score indicating the degree of similarity between them. A user configurable threshold setting is used to determine what score will be acceptable to indicate a match.

Biometric recognition can be used to identify a person or to verify the identity of a person. Identification mode involves a one-to-many comparison, where an image of a fingerprint is acquired, and a database is searched to find a match to determine the identity of the person. Verification mode is one-to-one, where the acquired image is compared to the stored image for one particular person, to verify that the person is who they claim to be.

Errors with Biometric Recognition

Unfortunately, biometric recognition is not 100% accurate. As mentioned above, when a comparison is being made, it is given a score to indicate the degree of similarity. And the administrator of the system has control to determine how much similarity is required to indicate a match. Two types of errors are possible, a false match and a false non-match.

A false match (also referred to as false acceptance) happens when two different fingers are mistaken for the same one. The fingerprints are compared, the generated score is greater than the threshold setting, and they are accepted as a match, allowing possible access to an imposter. The immediate response might be to raise the bar by setting the threshold level higher, and while this may be appropriate, it may also result in an unacceptable false non-match rate (see below). Current biometric systems claim false match rates (FMR) ranging from 0.0001% to 0.1%.[5]

At the other end of the scale, a false non-match (also referred to as false rejection) is just the reverse of a false match. Two readings of the same fingerprint are compared, the generated score is below the threshold, and they are declared different, possibly preventing access to a legitimate user. Current systems claim false non-match rates (FNMR) ranging from 0.00066% to 1.0%.[6]

The graph in Figure 1 shows the relationships between error rates and the threshold setting. The Y-axis represents the number of errors, and the X-axis represents the threshold setting. This graph would be unique for different types and models of fingerprint readers, and gives an indication of the personality of

[5] Convenience vs Security. Recognition Systems Inc. http://www.findbiometrics.com/Pages/guide2.html

[6] http://www.findbiometrics.com/Pages/guide2.html

the device. The equal error rate (EER) is the threshold setting at which the false match rate equals the false non-match rate. While it is not suggested that the EER value is the appropriate threshold setting, it provides a comparison value between sensors. The lower the EER the better.

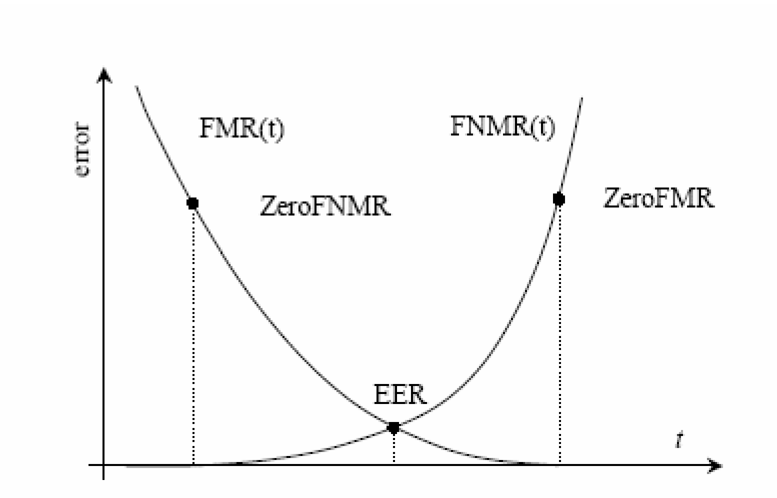

Figure 1: Error Rates[7]

Another error to consider is the failure to capture rate. This is the percentage of times that the device will not be able to capture an image of the fingerprint. If this happens during the enrollment process, the system may not be able to create a template for a given user. If it happens during authentication, a comparison cannot be made, and access would not be allowed. Failure to capture can happen when a fingerprint, for whatever reason, does not have sufficient identifying characteristics. While rare, it does happen.

Benefits of using Biometric Recognition

For security professionals, the primary question is whether the use of biometric recognition has the potential to improve security. With its ability to identify or verify a person's identity based on a unique attribute of the person; rather than on something that can be easily lost, stolen, forgotten, observed, or shared; it provides the ground floor for implementing secure access. For high-risk applications, the benefit of increased security alone might provide justification for implementing a biometric recognition system.

Another argument for using biometric recognition is that in the long run it will save money. While this is still debatable, a strong case can be made to support its cost saving potential. There are multiple areas where cost savings may be realized.

[7] Maltoni, Maio, Jain, Prabhakar. Handbook of Fingerprint Recognition, p 17

One area is in system administration. Since a biometric recognition system has the potential to eliminate the use of passwords, there is room for elimination of a significant workload from help desk personnel. With sensors costing less than $100 and their high accuracy, fingerprint recognition can be cost effective. Dealing with supports calls for expired and forgotten passwords can take a considerable percentage of help desk time. IDC puts the costs of handling password-related calls at $200-$300 per user per year[8], and that doesn't include the lost user productivity.

Another area of potential cost savings requires doing a risk assessment to determine the estimated cost of a security breach. While this savings is harder to quantify, it should be considered. In a high-risk environment where unauthorized access could result in death or the financial ruin of a company, the potential savings are significant.

Users can see the benefit of increased convenience. They will no longer be bothered by the need to change passwords every few months. They will not spend time keying and re-keying passwords to login. They will not spend time waiting on the help desk to reset their passwords when they get locked out.

In situations where biometric recognition has been implemented, banks have reported significant decreases in check fraud. Eliminating time and attendance abuse has saved businesses millions of dollars, and governments have reported a 25% reduction in fraudulent welfare claims after installing biometric recognition systems.[9]

The Downside of Biometric Recognition

The initial implementation of a biometric recognition system will be a significant investment. There is the cost of the sensors (which can be bought for less than $100) and the administration system, as well as the time cost for training and enrolling users. And there will be the ongoing costs for IT staff to administer the system and integrate it with other existing systems.

Biometric recognition systems are not 100% accurate. This does open the possibility that an imposter will gain access, or the more likely scenario that a valid user will be denied access. But one must remember that those possibilities also exist with systems based on password or tokens, probably to a much higher degree.

[8] http://www.biometritech.com/features/shen1102.htm
[9] http://www.ibia.org/understa.htm

There will be situations where a user is not able to complete the enrollment process. This could be due to a physical handicap or disability, or their fingerprint may simply not have sufficient distinguishing characteristic. Sensors are getting better at picking up weak fingerprints, but there will always be that possibility, and you will need to have a plan for how to deal with those situations. Options include using the finger with the best print, lowering the threshold setting (if it can be lowered for just individual users), and using an alternate biometric or non-biometric method.

As with most new technologies, there is the issue of user acceptance. Objections to using biometric recognition may include the feeling that it is undignifying to humans, that it is non-hygienic, that there is a criminal stigma attached, or that it is an invasion of one's privacy. There may also be those who object based on religious grounds.

Fingerprint recognition requires the presence of a suitable fingerprint sensor. While sensors are gradually being incorporated into keyboards, mice, notebook computers, PDAs and cell phones, they have certainly not reached a saturation point. Sensors have gotten smaller in size, and have even been included with some USB attached flash drives, providing a very portable solution.

As with other network-based systems, there is a potential for denial of service. This could be a result of a network-based attack, or from some other problem resulting in the administration service being unavailable. There is also the possibility that the reader could become damaged (either deliberately or accidentally), making it unusable.

Fingerprint recognition is not fraud proof. Tsutomu Matsumoto, a Japanese cryptographer, has been able to fool a variety of sensors using a fake finger made of gelatin. He has had a great deal of success when a mold is made from the actual finger. But he has also been able to fool the sensor starting only with a latent fingerprint, using a process involving cyanoacrylate adhesive, a digital camera, PhotoShop, and a photo-sensitive printed-circuit board (PCB) to develop a three-dimensional image, from which he makes a gelatin finger.[10] It is possible that sensors will need to include some means of determining whether the finger is live. Methods for doing this include sensing pulse, temperature, skin tone, electrical properties and blood flow.

A lack of standards between the various vendors makes it difficult to implement a system that integrates different makes of sensors. CBEFF (Common Biometric Exchange File Format) is being developed by the NIST (National Institute of Standards and Technology) to describe a set of data elements which will facilitate the exchange of data between components and systems. Hopefully this will promote the integration of various biometric hardware and software solutions.

[10] http://www.schneier.com/crypto-gram-0205.html - 5

Trends

Since 9/11 there has been a push to use biometrics to help secure our borders and keep out terrorists. The proposed US-VISIT (United States Visitor and Immigrant Status Indicator Technology) system would implement both fingerprint and facial recognition capabilities into passport and visa documents. The Department of Homeland Security has asked for a two year extension from the initial implementation deadline of October 2004, saying that they believe they can have the issues resolved in that time.[11]

The National Commission on Terrorist Attacks upon the United States (better known as the 9/11 commission) included numerous references to using biometric recognition as a deterrent to terrorist activities. It promotes the use of biometrics to identify terrorists, speeding up the adoption of biometric standards, and accelerated sharing of biometric data at all levels of government in the U.S. and with allied nations.[12]

Other federal legislation from the past few years is having a major impact on security in the commercial world. HIPAA (Health Insurance Portability and Accountability Act) has some stringent security requirements for the health business. And the Gramm-Leach-Bliley Act places similar requirements on the financial world. While biometric recognition is not explicitly required, it may play a role in meeting the rules these acts put in place.

American Express and the New York Police Department are a couple of examples of business and organizations that are using biometrics to identify employees. Continental Airlines is using biometrics to grant employee access to restricted areas.

The International Biometrics Group (IBG) projects that from 2003 to 2008 the fingerprint recognition market will increase from $198 million to $1.493 billion[13], and that total biometric revenues will increase from $719 million to $4.639 billion.[14]

Fingerprint recognition sensors are being integrated into a number of types of computing hardware. Notebook computer manufacturers including Gateway, MicronPC, IBM and Fujitsu all offer models with built-in sensors. Sensors have also been incorporated into keyboards, mice and flashcards.

These are all indications that biometric recognition is on a definite upward trend.

[11] http://www.global-electronics.net/id/24516/CMEntries_ID/55623
[12] Biometrics Advocacy Report Volume VI • Number 13 • Friday, July 23, 2004. http://www.ibia.org/newslett.htm
[13] http://www.planetanalog.com/printableArticle.jhtml?articleID=22104864
[14] http://www.biometricgroup.com/reports/public/market_report.html

Impact on Perimeter Security

Biometric recognition will impact some areas of perimeter security, while having little impact on others. It will introduce new systems and tools which need to be integrated into existing security structures. It will change and introduce new techniques used by hackers who attempt to break into secured systems, and require corresponding new methods to be used by security personnel to avert those attacks.

But biometrics do not hold much promise for mitigating attacks that already bypass any kind of login. Security holes that allow an authorized person to run programs at the administrator or root level will not be magically patched by a more secure authorization system.

Remote computing in particular is an area where biometrics could play a role in increased security. In an office setting there is some natural biometric recognition happening in that you can see the person sitting at the computer or hear the person talking in the cubicle next to you. In a remote computing environment, without biometrics you must trust that the password has not been shared, written down, or otherwise compromised; or that a token has not been misplaced or stolen. So biometrics can add a layer of security in those situations.

Another layer to consider when looking at multiple layers of security is physical access, and this is also a good application for biometrics. The concepts are the same as those for accessing computer systems, only this time it opens a door. And there is the hope of someday tying all the systems together to realize the benefits of centralized management.

Conclusions

As previously stated, fingerprint recognition does have its weaknesses and drawbacks. In many ways it is still in its infancy, with many of the implementation and acceptance issues that affect any developing technology.

There are numerous businesses in the biometric recognition industry today, and there is bound to be a lot of shake out as the industry matures. Sensors will need to improve in accuracy and fraud prevention. Standards need to be developed and adopted to improve interoperability, and CBEFF is a step in that direction.

There are benefits to be realized now, but there is also cost involved. Over time, the benefits should continue to increase while the costs go down. Whether your business or organization is ready to jump into biometrics today may be a question of your corporate culture as much as anything. If you are in a culture that promotes adopting new technologies and being near the cutting edge, it’s probably time to at least start familiarizing yourself with biometrics. If your culture prefers to let things settle down until the technology is more stable, you may want to wait a few years.

Either way, it is not something to jump into lightly. You need to plan for integrating it into your existing security structure, dealing with exceptions and dealing with user acceptance. And with changing federal legislation and requirements, you may be forced into dealing with it sooner than you think.

Fingerprint recognition, and biometric recognition in general, is not a silver bullet that is going to solve all computer security problems, prevent terrorist attacks, and rid the world of other evils. It is not able to perform miracles, but it is currently capable of being a part of a comprehensive security program. I think the best way to view it is as another tool that is available to use in implementing a security program based on the concept of security in depth.

Assignment 2: Security Architecture

Company Background

GIAC Enterprises (or simply GIAC) is a giant in the world of fortune cookie sayings, despite its relatively small size as a business. It was formed by four college friends who enjoyed Chinese food, but were usually disappointed in the quality of sayings in their fortune cookies. They talked to the cookie manufacturers about this, and found that they also were frustrated with the situation. Being bright young visionaries, the four friends saw an opportunity and ran with it.

GIAC was run as a strictly paper operation while the friends finished college. Their areas of study provided the necessary skills for starting and running a business. One was a business major, one was communications, one majored in computer science, and the fourth received an interdisciplinary liberal arts degree, so he could do anything. After they graduated from college and were able to devote all their attention to the business, things really took off.

One of the first changes was to computerize their operations, and that led quickly to doing business over the internet. When friends and families back home saw how well things were going for GIAC, they wondered how they could get involved. The four friends decided to open satellite offices, one in each of their hometowns, so they now have four regional offices as well as the main office in the college community.

Long-term viability of GIAC has always been a primary concern, and that has led to security being a top priority. They realize the importance of having multiple layers of security, so that if any one layer is compromised there is still at least one more layer protecting their assets. This Defense-in-Depth strategy has served them well, and they continue to work at ways to enhance the total security of their business.

Access Requirements

There is a wide variety of types of relationships that people have with GIAC. The following section will present them and define their requirements for accessing GIAC systems.

General Public

This group includes anybody who has not yet established some type of business relationship with GIAC. They are considered potential customers, so their access should be easy and pleasing. At the same time, they are also a potential threat, so their access needs to be limited. They will be granted access to browse the GIAC web site using regular HTTP and send email using SMTP. At the point they decide to place an order, they become customers.

Customers

GIAC customers range from one time private purchasers from the web site using a credit card, to large commercial customers with standing orders and regular billing. In addition to the access granted to the general public, customers will also be able to place orders, check on the status of an order, and look up account information if they are regular customers. All web traffic involving any type of private information will be secured using SSL (HTTPS).

Suppliers

Most of the fortune cookie sayings sold by GIAC are written by employees of the company. However, occasionally GIAC receives requests for special order sayings that they can not produce themselves. To cover these situations, GIAC has developed relationships will several other businesses to provide these custom written sayings. Suppliers will use secure FTP (SSL encryption) to deliver their product in addition to previously mentioned access to the web site and account information.

Partners

GIAC has expanded into the international market by partnering with other similar businesses in strategic locations. This allows them to have their sayings translated and sold in a variety of languages, as well as offering GIAC the option of selling non-English sayings to their customers. Transfer of sayings between partners is accomplished using secure FTP, account information is available using HTTPS, and web and email are available as above.

Employees

The majority of GIAC employees work on-site in the home office. The company makes a conscious effort to maintain a balance between trust and security. Each employee is provided with a unique user ID to access GIAC systems, and is only allowed into the systems that are necessary for performing their jobs.

Home office employees are on the same internal trusted network as the primary servers and they are all granted the same access to the internet. Web services that they utilize include HTTP and HTTPS for web browsing, and FTP for file transfer. Other services used for accessing GIAC servers located in the trusted, DMZ and Remote Access networks (discussed below) include secure telnet (using SSL), Lotus Domino/Notes traffic (using port 1352) and a range of ports used to administer the IBM iSeries servers.

Employees at each remote office never number more than five. They share a DSL connection to the internet and are protected behind a firewall. They are able to access the home office trusted network via a VPN connection, where they are granted the same access as the home office employees.

There is also a small sales force that connects as mobile employees. They have dial-up internet access via a national ISP. This allows them to access the GIAC company web site directly. The also can utilize a SSL VPN to allow access to limited resources on the home office trusted network.

Architecture Components

There are many systems and components that work together to enable and protect GIAC business processes. System and network design needs to find a balance between three factors: Security, Usability, and Cost. The only 100% secure system is one that is completely disconnected from any means of access and locked in a safe. The only 100% usable system is one to which everyone has complete and unrestricted access. Achieving a high level of security AND usability is possible, but can get very expensive.[15]

GIAC has tried to make choices that maximize security and usability while maintaining a reasonable budget. Sometimes that has meant choosing options that on their own might not be able to provide the highest level of security, but when all of the separate features are combined together they form a total system which is highly usable and secure, yet affordable.

For the most part, GIAC has chosen to implement systems which each provide one primary function, rather than combining multiple functions into one system. (The exception to this would be their choice of server systems, which will be covered in a section on servers.) Systems that provide multiple functions are seldom industry leaders in any one of those functions. It can also create problems when looking to replace just one of the functions.

[15] Jesper M. Johansson, Microsoft Security Management; January 5, 2004. http://www.microsoft.com/technet/community/columns/secmgmt/sm0104.mspx

Network Diagram

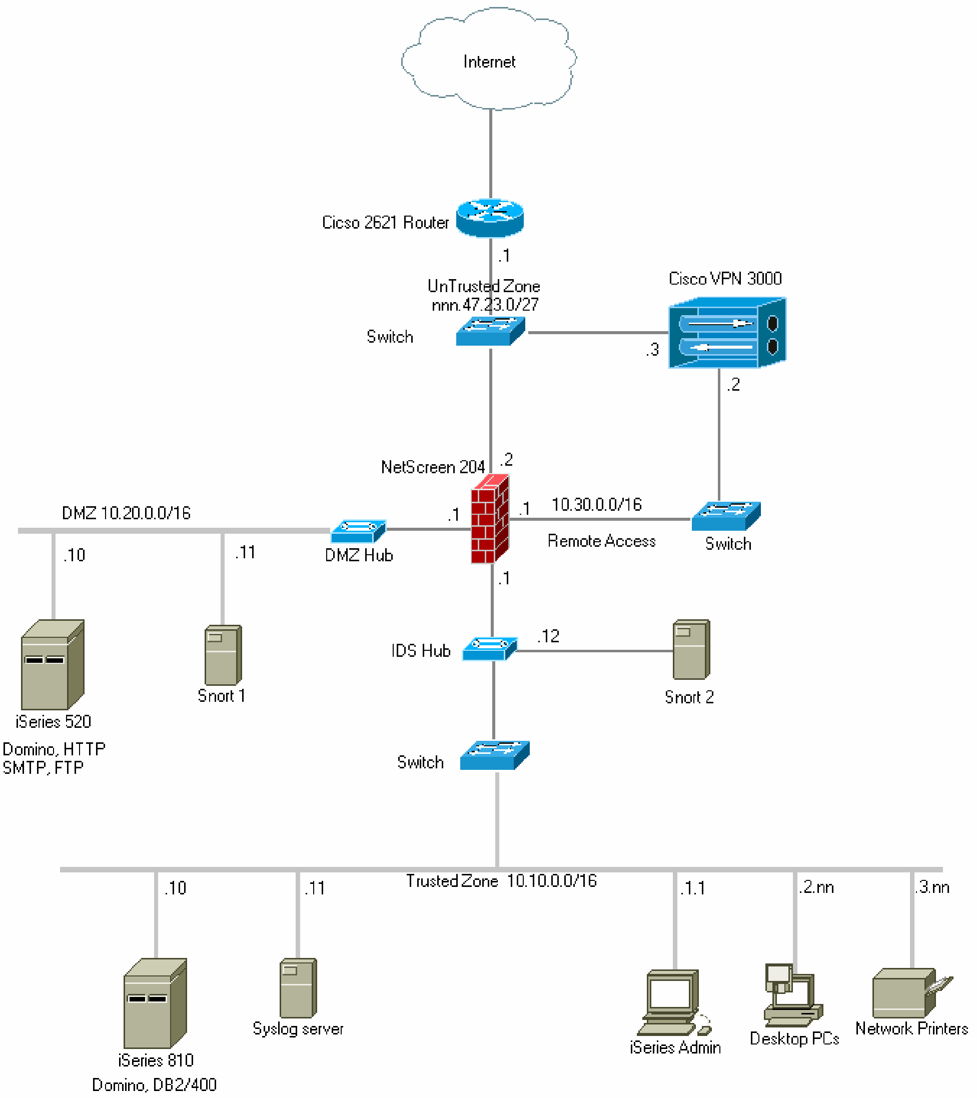

Figure 2: GIAC Network

Filtering Router

The border router used by GIAC is a CISCO 2621, with IOS version 12.0. As the device that connects the GIAC network to the internet, it is the outpost and provides the first line of defense against attacks. The book Securing Cisco Routers[16] was used as a resource for configuring the router. The router provides basic ingress and egress static packet filtering, blocking many services and ports before the packets even have a chance to enter the GIAC network. Management access to the router is only allowed from the GIAC network.

Firewall

GIAC has chosen a NetScreen model 204 firewall with firmware version 5.0 as their only firewall, providing the primary layer of defense to the GIAC network. The model 204 easily provides sufficient performance for a company the size of GIAC, and its four ports allow for a nice segmentation of the GIAC network by function.

The decision to go with just one firewall is an example of a choice where the extra level of security which could be provided by implementing multiple firewalls was weighed against the additional costs of implementation, administration and maintenance, and GIAC decided the return wasn't worth the expense. With some firewall type functionality being provided by the border router, and the level of segmentation possible with the firewall's four ports, GIAC felt that an additional layer was not the best business decision.

The firewall divides the GIAC network into the following four zones:

- The untrusted zone, which is connected to the border router, where incoming traffic has not yet passed through the firewall. This zone is allowed limited access to the DMZ zone, but no direct access to either the trusted or remote access zones.
- The DMZ zone, which provides web accessible services. This zone has fairly open access to the untrusted zone, very limited access to the trusted network for transfer of data and email, and no access to the remote access zone.
- The trusted zone, which includes home office employees and internal servers. This zone has access to all the other zones as appropriate for systems management and web services. However, no access is allowed directly from the untrusted zone to the internal zone.
- The remote access zone, which is where VPN connections are terminated and where the remote users enter the network. At this point the VPN is the only remote access supported, although this would also be the zone where dial-up or wireless access would attach if it were added in the future.

The firewall pushes its log files to a syslog server located on the internal network. GIAC also implements NetScreen firewalls (model 5GT) at the remote offices to protect the systems there. Having NetScreen firewalls throughout the company simplifies configuration and management.

[16] Wright and Stewart, Securing Cisco Routers, The SANS Institute; 2002

VPN

GIAC has implemented a CISCO VPN 3000 concentrator (version 4.1) to provide VPN access to remote users. This allows the remote office users to use an IPSec client to connect to the GIAC home office network.

The NetScreen firewall has the capability to support VPN connections directly, but GIAC preferred to move this processing workload elsewhere, and not require the firewall to do it. In addition to moving processor workload, the CISCO VPN appliance provides SSL VPN capability, which is used by the mobile workforce. And having a dedicated VPN appliance allows more flexibility when it's time to upgrade or replace the current solution.

Servers

GIAC has chosen to use IBM iSeries Servers[17] for both the internal server and the DMZ based server for web services. The internal server is a model 810 running version 5 release 2 of OS/400 (the operating system). The web server is a model 520 running version 5 release 3. In addition to the built-in TCP/IP and database functionality that come included with every iSeries server, GIAC is running Lotus Domino[18] (version 6.5) on both servers. Domino provides email and the HTTP server, as well as the application framework for many of the GIAC applications.

It is worth noting the reasons why GIAC chose to go with the IBM iSeries servers, particularly in relation to security. One reason is simply a matter of numbers. Windows and Linux based systems have a larger install base, and so they also present a larger target for potential attacks. The smaller install base for iSeries systems allows them to remain under the radar from the point of view of most hackers. In addition to not being susceptible to most of the general attacks, this also means that when a hacker targets a specific business, and the business is running on an iSeries server, there are fewer resources available to help him in his attack.

Another aspect of iSeries systems is their built-in virus resistance[19]. This is not to say that the systems are 100% safe from a targeted attack, but most general attacks are not a threat to an iSeries server. One reason for that is the object-based operating system, in which all objects are strongly typed. This means that an executable file cannot masquerade as something else to slip in and then run expectedly. Another feature is the separation of program and data stacks, which prevents a buffer overflow situation from running code that could allow a hacker to gain unauthorized access to the system.

[17] http://www-1.ibm.com/servers/eserver/iseries/
[18] http://www.lotus.com/products/product4.nsf/wdocs/dominohomepage
[19] http://eservercomputing.com/iseries/articles/index.asp?id=754&dir=/iseries/articles/

The OS/400 operating system was designed from the ground up with an integrated security management system. IBM recently added digital signatures to all operating system objects, which provides the ability to determine whether any system objects have been altered or tampered with in some way. Non-IBM objects can also be digitally signed to ensure integrity.

The iSeries servers are capable of efficiently managing multiple applications and workloads on one system. Because of this, GIAC feels comfortable running multiple functions on each iSeries server, even though that goes against their base philosophy of one system, one function. The DMZ system provides HTTP serving and SMTP email via Domino, and FTP serving via the native OS/400 FTP server. The internal system also runs Domino to provide email and calendar functions to employees running the Lotus Notes client, as well as other Domino/Notes applications. The built in DB2/400 database serves as the database system. This system also functions as the file and print server for GIAC employees.

Network based IDS sensors

Two strategically placed IDS sensors monitor for incoming malicious packets that have made it through the first layers of security. Since GIAC's primary concern is running a business and not doing in depth security analysis, they are interested in monitoring traffic that has made it past the filters and rules implemented in the border router and the firewall. One sensor is monitoring the DMZ zone, since that is where most inbound traffic will be going. A second sensor monitors the trusted zone to make sure only approved traffic is allowed there.

The IDS sensors are running Snort v2.2[20] on hardened WindowsXP systems. The systems are connected to hubs that are placed between the firewall and the switches which provide connectivity for the rest of the devices on the segment. This allows them to monitor any traffic flowing between the firewall and other hosts on that segment.

An IP addressing scheme

GIAC uses static Public IP addresses externally for devices that are in the untrusted zone. The contract GIAC has with their Internet Service Provider (ISP) grants them a block of 30 addresses in the range nnn.47.23.0/27. This is more addresses than they currently need, but it gives them some flexibility for future needs.

[20] http://www.snort.org/

Internally, all addresses are private, non-routable addresses as defined by RFC1918.[21] Primarily for reasons of convenience and flexibility, GIAC has implemented each private segment as a Class B network. The trusted zone has the address range 10.10.0.0/16, the DMZ zone uses 10.20.0.0/16, and the remote access zone uses 10.30.0.0/16. This approach makes it simple to relate an address to a zone and to specify subnet masks.

Additional Considerations

GIAC contracts with Postini[22] to remove SPAM and viruses from incoming email before it enters the GIAC network. DNS mx records for GIAC direct mail to Postini, with Postini then forwarding the mail that passes screening on to the GIAC SMTP server. This reduces the virus threat while at the same time eliminating a lot of undesired email traffic.

All GIAC desktops are protected by Symantec AntiVirus[23] virus protection as well as ZoneAlarm[24] personal firewall. Symantec AntiVirus is centrally managed by a central server which pushes out virus signature updates as they become available.

GIAC does not provide its own external DNS server. The internal iSeries server provides DNS service for internal use, but GIAC utilizes the DNS services of its ISP to provide the service for external use. Since their DNS requirements are limited, this provides a convenient and efficient solution.

Implementing Defense in Depth

There are many bits and pieces that play a role in the total security structure for GIAC. On there own, any one of them might be easily broken. But tied together, like the proverbial bundle of sticks, they complement each other to result in a much more secure total system than any of the individual components can provide on their own.

[21] http://www.rfc-editor.org/rfc/rfc1918.txt
[22] http://www.postini.com/
[23] http://www.symantec.com/
[24] http://www.zonelabs.com/

Assignment 3 – Firewall Policy

This section documents the configuration of the GIAC NetScreen 204 firewall. Rather than listing the entire configuration here, the significant portions are included, along with a brief description. The entire listing can be found in the appendix.

One of the basic philosophies used in configuring the firewall is to only allow what is needed, and deny everything else. This sometimes results in making configuration changes when new needs arise, but security it always a work in process, so this is not viewed as unacceptable.

Primary Firewall Security Policy[25]

Set a new admin name and password, and a host name.

```
set admin name "GIAC3Admin"
set admin password "nNjvOYrWHX4Dc9LEasWOU8Ptt5Pjyn"
set hostname giacfw1
```

GIAC attempts to keep all system clocks synchronized to the same time setting. This is very helpful, particularly when comparing logs that come from different places. These entries set the time zone and ntp servers for setting the clock.

```
set clock ntp
set clock timezone -6
set ntp server "time.nist.gov"
set ntp server backup1 "nt2.usno.navy.mil"
```

The firewall does not have the ability to store much log information itself, so it will send logs to a syslog server in the trusted zone.

```
set syslog config "10.10.0.11"
set syslog config "10.10.0.11" facilities local0 local0
set syslog config "10.10.0.11" log traffic
set syslog src-interface ethernet1
set syslog enable
```

ScreenOS comes with a number of predefined services, but it is by no means complete. The entries below are for custom services defined to allow traffic for Lotus Domino/Notes and for iSeries specific services.

```
set service "Domino/Notes" protocol tcp src-port 1024-65535 dst-
port 1352-1352
```

[25] Equipment was not available to do a complete testing of the configuration.

```
set service "iSeries" protocol tcp src-port 1024-65535 dst-port
8470-8476
set service "iSeries" + tcp src-port 1024-65535 dst-port 446-446
set service "iSeries" + tcp src-port 1024-65535 dst-port 449-449
set service "iSeriesSSL" protocol tcp src-port 1024-65535 dst-
port 9470-9476
set service "iSeriesSSL" + tcp src-port 1024-65535 dst-port 449-
449
set service "iSeriesSSL" + tcp src-port 1024-65535 dst-port 448-
448
set service "iSeriesAdm" protocol tcp src-port 1024-65535 dst-
port 2001-2001
set service "iSeriesAdm" + tcp src-port 1024-65535 dst-port 5544-
5544
set service "iSeriesAdm" + tcp src-port 1024-65535 dst-port 5555-
5555
set service "iSeriesAdm" + tcp src-port 1024-65535 dst-port 5577-
5577
set service "iSeriesAdS" protocol tcp src-port 1024-65535 dst-
port 2010-2010
set service "iSeriesAdS" + tcp src-port 1024-65535 dst-port 5544-
5544
set service "iSeriesAdS" + tcp src-port 1024-65535 dst-port 5566-
5566
set service "iSeriesAdS" + tcp src-port 1024-65535 dst-port 5577-
5577
```

GIAC also uses the SSL support found in some FTP and Telnet servers and clients to encrypt traffic.

```
set service "FTP_SSL" protocol tcp src-port 1024-65535 dst-port
990-990
set service "Telnet_SSL" protocol tcp src-port 1024-65535 dst-
port 992-992
```

GIAC uses the default NetScreen zones Trust, Untrust and DMZ, but needed a new zone to use in the Remote Access zone.

```
set zone id 100 "RA"
set zone "RA" tcp-rst
```

GIAC uses all four ethernet ports on the firewall, with each one assigned to a different zone.

```
set interface "ethernet1" zone "Trust"
set interface "ethernet2" zone "DMZ"
set interface "ethernet3" zone "Untrust"
set interface "ethernet4" zone "RA"
```

The untrusted segment uses an address supplied from the ISP, and traffic is routed.

```
set interface ethernet3 ip nnn.47.23.2/27
set interface ethernet3 route
```

The other three interfaces use private IP address and Network Address Translation (NAT)

```
set interface ethernet1 ip 10.10.0.1/16
set interface ethernet1 nat
set interface ethernet2 ip 10.20.0.1/16
set interface ethernet2 nat
set interface ethernet4 ip 10.30.0.1/16
set interface ethernet4 nat
```

Define virtual IP interfaces on the untrusted physical interface. These will be used by traffic coming from the internet to get to the web services available on the iSeries server in the DMZ zone. There are multiple virtual interfaces setup to make it less obvious that all services are running on the same server, and also to make it easier to actually change them to separate servers if that decision is made in the future.

```
set interface ethernet3 vip nnn.47.23.10 80 "HTTP" 10.20.0.10
manual
set interface ethernet3 vip nnn.47.23.10 + 443 "HTTPS" 10.20.0.10
manual
set interface ethernet3 vip nnn.47.23.11 25 "MAIL" 10.20.0.10
manual
set interface ethernet3 vip nnn.47.23.12 1352 "Domino/Notes"
10.20.0.10 manual
set interface ethernet3 vip nnn.47.23.13 21 "FTP" 10.20.0.10
manual
set interface ethernet3 vip nnn.47.23.13 + 990 "FTP_SSL"
10.20.0.10 manual
```

The NetScreen device can only be managed by a host attached to the Trust zone on interface ethernet1. The other interfaces are disabled for management purposes.

```
set interface ethernet1 ip manageable
unset interface ethernet2 ip manageable
unset interface ethernet3 ip manageable
unset interface ethernet4 ip manageable
```

ScreenOS allows assigning a name to a host or network. These definitions can then be used when defining policies, and can make the policies more readable. Having the addresses defined in one place also simplifies future changes. If the address of a host changes, it only needs to be changed in the address definition and not every place where the address is used in policies.

```
set address "Trust" "iSeries_Internal" 10.10.0.10 255.255.255.255
"iSeries server in Trusted Sgmnt"
set address "Trust" "iSeriesAdmin" 10.10.1.1 255.255.255.255
"iSeries Administrator"
set address "Trust" "Syslog1" 10.10.0.11 255.255.255.255 "Syslog
Server Internal"
set address "Trust" "Trusted Segment" 10.10.0.0 255.255.0.0
set address "Untrust" "RFC1918a" 10.0.0.0 255.0.0.0 "Private
address block 1"
set address "Untrust" "RFC1918b" 172.16.0.0 255.240.0.0 "Private
Address block 2"
set address "Untrust" "RFC1918c" 192.168.0.0 255.255.0.0 "Private
Address Block 3"
set address "DMZ" "DMZ Segment" 10.20.0.0 255.255.0.0
set address "DMZ" "iSeries_DMZ" 10.20.0.10 255.255.255.255
"iSeries server in DMZ"
set address "RA" "VPN1" 10.30.0.2 255.255.255.255
set address "RA" "RA Segment" 10.30.0.0 255.255.0.0
set group address "Untrust" "Private Addresses"
set group address "Untrust" "Private Addresses" add "RFC1918a"
set group address "Untrust" "Private Addresses" add "RFC1918b"
set group address "Untrust" "Private Addresses" add "RFC1918c"
```

ScreenOS uses policies to define what traffic is permitted and what is denied. In a policy, the main options to specify are the from and to zones, IP source and destination addresses, the service(s), whether to permit or deny the traffic, and logging preference.

The policies below are grouped by zones. In each group, the final (and sometimes only) policy is to deny and log all packets. This will ensure that traffic that has not been specifically allowed by a previous packet will not be allowed through.

Trust zone to Untrust zone: All internal employees are allowed the same access to basic internet functions.

```
set policy id 4 name "Allow Basic Internet" from "Trust" to
"Untrust" "Trusted Segment" "Any" "DNS" permit
set policy id 4
set service "FTP"
set service "FTP_SSL"
set service "HTTP"
set service "HTTPS"
set service "NTP"
set service "PING"
set service "Real Media"
set service "TRACEROUTE"
exit
```

```
set policy id 5 name "Deny and LOG" from "Trust" to "Untrust"
"Any" "Any" "ANY" deny log
```

Trust zone to DMZ zone: Basic internet services are allowed to any address in the DMZ. Lotus Notes and iSeries traffic is only allowed to the iSeries server, and only the iSeries administrator is allowed to use some services.

```
set policy id 3 name "Basic access" from "Trust" to "DMZ"
"Trusted Segment" "Any" "FTP" permit
set policy id 3
set service "FTP_SSL"
set service "HTTP"
set service "HTTPS"
set service "PING"
set service "TELNET"
exit
set policy id 10 name "Lotus Notes" from "Trust" to "DMZ"
"Trusted Segment" "iSeries_DMZ" "Domino/Notes" permit
set policy id 8 name "iSeriesBasicAccess" from "Trust" to "DMZ"
"Trusted Segment" "iSeries_DMZ" "iSeries" permit
set policy id 9 name "iSeries Admin" from "Trust" to "DMZ"
"iSeriesAdmin" "iSeries_DMZ" "iSeriesAdS" permit log
set policy id 9
set service "Telnet_SSL"
exit
set policy id 11 name "Deny and Log" from "Trust" to "DMZ"  "Any"
"Any" "ANY" deny log
```

Trust zone to RA zone: Only limited traffic is allowed to the Remote Access zone, mostly for administrative use.

```
set policy id 6 name "Administration" from "Trust" to "RA"
"Trusted Segment" "Any" "HTTP" permit
set policy id 6
set service "HTTPS"
set service "PING"
set service "TELNET"
exit
set policy id 7 name "Deny and Log" from "Trust" to "RA"  "Any"
"Any" "ANY" deny log
```

Untrust zone to Trust zone: No traffic is allowed from the Untrusted to Trust zones.

```
set policy id 2 name "Deny all UT to T" from "Untrust" to "Trust"
"Any" "Any" "ANY" deny log
```

Untrust zone to RA zone: No traffic is allowed from the Untrusted to RA zones.

```
set policy id 36 name "Deny and log" from "Untrust" to "RA"
"Any" "Any" "ANY" deny log
```

Untrust zone to DMZ zone: Since there is some traffic permitted from the untrust zone to DMZ zone, the very first policy is to deny any traffic that has a source address from the blocks of private addresses defined in RFC1918. These addresses would not normally be found in internet traffic, so this is just another layer of defense against potentially harmful packets. Traffic is allowed for HTTP(s), FTP serving, SMTP for mail, and Lotus Notes traffic to the Domino server running on the iSeries.

```
set policy id 35 name "Block private" from "Untrust" to "DMZ"
"Private Addresses" "Any" "ANY" deny log
set policy id 12 name "Allow HTTP" from "Untrust" to "DMZ"  "Any"
"VIP(nnn.47.23.10)" "HTTP" permit log
set policy id 12
set service "HTTPS"
exit
set policy id 13 name "Allow FTP serving" from "Untrust" to "DMZ"
"Any" "VIP(nnn.47.23.13)" "FTP" permit log
set policy id 13
set service "FTP_SSL"
exit
set policy id 15 name "Notes from WEB" from "Untrust" to "DMZ"
"Any" "VIP(nnn.47.23.12)" "Domino/Notes" permit log
set policy id 38 name "Mail from WEB" from "Untrust" to "DMZ"
"Any" "VIP(nnn.47.23.11)" "MAIL" permit log
set policy id 14 name "Deny and Log" from "Untrust" to "DMZ"
"Any" "Any" "ANY" deny log
```

DMZ zone to Trust zone: The only traffic allowed is Lotus Notes traffic between the Domino servers. This allows the Domino server to send mail and database updates using port 1352.

```
set policy id 16 name "Notes" from "DMZ" to "Trust"
"iSeries_DMZ" "iSeries_Internal" "Domino/Notes" permit
set policy id 18 name "Deny and log" from "DMZ" to "Trust"  "Any"
"Any" "ANY" deny log
```

DMZ zone to Untrust zone: The iSeries server needs to be able to send SMTP mail, and to connect to other FTP servers. We also need to allow DNS, and we allow web browsing.

```
set policy id 19 name "Mail" from "DMZ" to "Untrust"
"iSeries_DMZ" "Any" "MAIL" permit
set policy id 37 name "FTP" from "DMZ" to "Untrust"
"iSeries_DMZ" "Any" "FTP" permit
set policy id 37
set service "FTP_SSL"
exit
set policy id 21 name "DNS" from "DMZ" to "Untrust"  "DMZ
Segment" "Any" "DNS" permit
set policy id 22 name "Browse" from "DMZ" to "Untrust"  "DMZ
Segment" "Any" "HTTP" permit
set policy id 22
set service "HTTPS"
exit
```

```
set policy id 20 name "Deny and Log" from "DMZ" to "Untrust"
"Any" "Any" "ANY" deny log
```

DMZ zone to RA zone: No traffic is allowed.

```
set policy id 17 name "Deny and Log" from "DMZ" to "RA"  "Any"
"Any" "ANY" deny log
```

RA zone to Trust zone: Access is allowed to the internal iSeries server for Notes and other applications. We also allow access for remote administration of the server.

```
set policy id 24 name "Notes" from "RA" to "Trust"  "RA Segment"
"iSeries_Internal" "Domino/Notes" permit
set policy id 25 name "iSeries_User" from "RA" to "Trust"  "RA
Segment" "iSeries_Internal" "iSeries" permit
set policy id 25
set service "iSeriesSSL"
set service "TELNET"
set service "Telnet_SSL"
exit
set policy id 26 name "iSeries_Admin" from "RA" to "Trust"  "RA
Segment" "iSeries_Internal" "iSeriesAdm" permit
set policy id 26
set service "iSeriesAdS"
exit
set policy id 28 name "Deny and Log" from "RA" to "Trust"  "Any"
"Any" "ANY" deny log
```

RA zone to DMZ zone: HTTP, FPT and Notes traffic is allowed to the server in the DMZ.

```
set policy id 29 name "Browsing" from "RA" to "DMZ"  "RA Segment"
"iSeries_DMZ" "HTTP" permit
set policy id 29
set service "HTTPS"
exit
set policy id 30 name "FTP" from "RA" to "DMZ"  "RA Segment"
"iSeries_DMZ" "FTP" permit
set policy id 30
set service "FTP_SSL"
exit
set policy id 31 name "Notes" from "RA" to "DMZ"  "RA Segment"
"iSeries_DMZ" "Domino/Notes" permit
set policy id 32 name "Deny and Log" from "RA" to "DMZ"  "Any"
"Any" "ANY" deny log
```

RA zone to Untrust zone: The only access allowed is for browsing.

```
set policy id 33 name "Basic Web Access" from "RA" to "Untrust"
"RA Segment" "Any" "DNS" permit
set policy id 33
set service "HTTP"
set service "HTTPS"
```

```
exit
set policy id 34 name "Deny and Log" from "RA" to "Untrust"
"Any" "Any" "ANY" deny log
```

Appendix A – NetScreen Firewall Configuration Listing

```
set clock ntp
set clock timezone -6
set vrouter trust-vr sharable
unset vrouter "trust-vr" auto-route-export
set service "Domino/Notes" protocol tcp src-port 1024-65535 dst-port 1352-1352
set service "FTP_SSL" protocol tcp src-port 1024-65535 dst-port 990-990
set service "Telnet_SSL" protocol tcp src-port 1024-65535 dst-port 992-992
set service "iSeries" protocol tcp src-port 1024-65535 dst-port 8470-8476
set service "iSeries" + tcp src-port 1024-65535 dst-port 446-446
set service "iSeries" + tcp src-port 1024-65535 dst-port 449-449
set service "iSeriesSSL" protocol tcp src-port 1024-65535 dst-port 9470-9476
set service "iSeriesSSL" + tcp src-port 1024-65535 dst-port 449-449
set service "iSeriesSSL" + tcp src-port 1024-65535 dst-port 448-448
set service "iSeriesAdm" protocol tcp src-port 1024-65535 dst-port 2001-2001
set service "iSeriesAdm" + tcp src-port 1024-65535 dst-port 5544-5544
set service "iSeriesAdm" + tcp src-port 1024-65535 dst-port 5555-5555
set service "iSeriesAdm" + tcp src-port 1024-65535 dst-port 5577-5577
set service "iSeriesAdS" protocol tcp src-port 1024-65535 dst-port 2010-2010
set service "iSeriesAdS" + tcp src-port 1024-65535 dst-port 5544-5544
set service "iSeriesAdS" + tcp src-port 1024-65535 dst-port 5566-5566
set service "iSeriesAdS" + tcp src-port 1024-65535 dst-port 5577-5577
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set admin name "GIAC3Admin"
set admin password "nNjvOYrWHX4Dc9LEasWOU8Ptt5Pjyn"
set admin auth timeout 0
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone id 100 "RA"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
set zone "VLAN" tcp-rst
set zone "RA" tcp-rst
set zone "Untrust" screen icmp-flood
set zone "Untrust" screen udp-flood
set zone "Untrust" screen winnuke
set zone "Untrust" screen ip-sweep
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen icmp-flood
set zone "V1-Untrust" screen udp-flood
set zone "V1-Untrust" screen winnuke
set zone "V1-Untrust" screen ip-sweep
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet1" zone "Trust"
set interface "ethernet2" zone "DMZ"
set interface "ethernet3" zone "Untrust"
set interface "ethernet4" zone "RA"
unset interface vlan1 ip
set interface ethernet1 ip 10.10.0.1/16
set interface ethernet1 nat
set interface ethernet2 ip 10.20.0.1/16
set interface ethernet2 nat
set interface ethernet3 ip nnn.47.23.2/27
set interface ethernet3 route
set interface ethernet4 ip 10.30.0.1/16
set interface ethernet4 nat
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet1 ip manageable
unset interface ethernet2 ip manageable
unset interface ethernet3 ip manageable
unset interface ethernet4 ip manageable
set interface ethernet3 vip nnn.47.23.10 80 "HTTP" 10.20.0.10 manual
set interface ethernet3 vip nnn.47.23.10 + 443 "HTTPS" 10.20.0.10 manual
set interface ethernet3 vip nnn.47.23.11 25 "MAIL" 10.20.0.10 manual
set interface ethernet3 vip nnn.47.23.12 1352 "Domino/Notes" 10.20.0.10 manual
set interface ethernet3 vip nnn.47.23.13 21 "FTP" 10.20.0.10 manual
set interface ethernet3 vip nnn.47.23.13 + 990 "FTP_SSL" 10.20.0.10 manual
set domain giac.net
set hostname giacfw1
set dns host dns1 nnn.47.2.4
set dns host dns2 nnn.47.2.5
set address "Trust" "iSeries_Internal" 10.10.0.10 255.255.255.255 "iSeries server in
Trusted Sgmnt"
set address "Trust" "iSeriesAdmin" 10.10.1.1 255.255.255.255 "iSeries Administrator"
set address "Trust" "Syslog1" 10.10.0.11 255.255.255.255 "Syslog Server Internal"
set address "Trust" "Trusted Segment" 10.10.0.0 255.255.0.0
set address "Untrust" "RFC1918a" 10.0.0.0 255.0.0.0 "Private address block 1"
set address "Untrust" "RFC1918b" 172.16.0.0 255.240.0.0 "Private Address block 2"
set address "Untrust" "RFC1918c" 192.168.0.0 255.255.0.0 "Private Address Block 3"
set address "DMZ" "DMZ Segment" 10.20.0.0 255.255.0.0
set address "DMZ" "iSeries_DMZ" 10.20.0.10 255.255.255.255 "iSeries server in DMZ"
set address "RA" "VPN1" 10.30.0.2 255.255.255.255
set address "RA" "RA Segment" 10.30.0.0 255.255.0.0
set group address "Untrust" "Private Addresses"
set group address "Untrust" "Private Addresses" add "RFC1918a"
set group address "Untrust" "Private Addresses" add "RFC1918b"
set group address "Untrust" "Private Addresses" add "RFC1918c"
set ike respond-bad-spi 1
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set policy id 4 name "Allow Basic Internet" from "Trust" to "Untrust"  "Trusted Segment"
"Any" "DNS" permit
set policy id 4
set service "FTP"
set service "FTP_SSL"
set service "HTTP"
set service "HTTPS"
set service "NTP"
set service "PING"
set service "Real Media"
set service "TRACEROUTE"
exit
set policy id 5 name "Deny and LOG" from "Trust" to "Untrust"  "Any" "Any" "ANY" deny
log
set policy id 3 name "Basic access" from "Trust" to "DMZ"  "Trusted Segment" "Any"
"FTP" permit
set policy id 3
set service "FTP_SSL"
set service "HTTP"
set service "HTTPS"
set service "PING"
set service "TELNET"
exit
set policy id 10 name "Lotus Notes" from "Trust" to "DMZ"  "Trusted Segment"
"iSeries_DMZ" "Domino/Notes" permit
set policy id 2 name "Deny all UT to T" from "Untrust" to "Trust"  "Any" "Any" "ANY" deny
log
set policy id 6 name "Administration" from "Trust" to "RA"  "Trusted Segment" "Any"
"HTTP" permit
set policy id 6
set service "HTTPS"
set service "PING"
set service "TELNET"
exit
set policy id 7 name "Deny and Log" from "Trust" to "RA"  "Any" "Any" "ANY" deny log
set policy id 8 name "iSeriesBasicAccess" from "Trust" to "DMZ"  "Trusted Segment"
"iSeries_DMZ" "iSeries" permit
set policy id 9 name "iSeries Admin" from "Trust" to "DMZ"  "iSeriesAdmin"
"iSeries_DMZ" "iSeriesAdS" permit log
set policy id 9
set service "Telnet_SSL"
```

```
exit
set policy id 11 name "Deny and Log" from "Trust" to "DMZ"  "Any" "Any" "ANY" deny log
set policy id 35 name "Block private" from "Untrust" to "DMZ"  "Private Addresses" "Any"
"ANY" deny log
set policy id 12 name "Allow HTTP" from "Untrust" to "DMZ"  "Any" "VIP(nnn.47.23.10)"
"HTTP" permit log
set policy id 12
set service "HTTPS"
exit
set policy id 13 name "Allow FTP serving" from "Untrust" to "DMZ"  "Any"
"VIP(nnn.47.23.13)" "FTP" permit log
set policy id 13
set service "FTP_SSL"
exit
set policy id 15 name "Notes from WEB" from "Untrust" to "DMZ"  "Any"
"VIP(nnn.47.23.12)" "Domino/Notes" permit log
set policy id 38 name "Mail from WEB" from "Untrust" to "DMZ"  "Any"
"VIP(nnn.47.23.11)" "MAIL" permit log

set policy id 14 name "Deny and Log" from "Untrust" to "DMZ"  "Any" "Any" "ANY" deny
log
set policy id 16 name "Notes" from "DMZ" to "Trust"  "iSeries_DMZ" "iSeries_Internal"
"Domino/Notes" permit
set policy id 17 name "Deny and Log" from "DMZ" to "RA"  "Any" "Any" "ANY" deny log
set policy id 18 name "Deny and log" from "DMZ" to "Trust"  "Any" "Any" "ANY" deny log
set policy id 19 name "Mail" from "DMZ" to "Untrust"  "iSeries_DMZ" "Any" "MAIL" permit
set policy id 37 name "FTP" from "DMZ" to "Untrust"  "iSeries_DMZ" "Any" "FTP" permit
set policy id 37
set service "FTP_SSL"
exit
set policy id 21 name "DNS" from "DMZ" to "Untrust"  "DMZ Segment" "Any" "DNS"
permit
set policy id 22 name "Browse" from "DMZ" to "Untrust"  "DMZ Segment" "Any" "HTTP"
permit
set policy id 22
set service "HTTPS"
exit
set policy id 20 name "Deny and Log" from "DMZ" to "Untrust"  "Any" "Any" "ANY" deny
log
set policy id 24 name "Notes" from "RA" to "Trust"  "RA Segment" "iSeries_Internal"
"Domino/Notes" permit
set policy id 25 name "iSeries_User" from "RA" to "Trust"  "RA Segment"
"iSeries_Internal" "iSeries" permit
set policy id 25
set service "iSeriesSSL"
set service "TELNET"
set service "Telnet_SSL"
exit
set policy id 26 name "iSeries_Admin" from "RA" to "Trust"  "RA Segment"
"iSeries_Internal" "iSeriesAdm" permit
set policy id 26
set service "iSeriesAdS"
exit
set policy id 28 name "Deny and Log" from "RA" to "Trust"  "Any" "Any" "ANY" deny log
set policy id 29 name "Browsing" from "RA" to "DMZ"  "RA Segment" "iSeries_DMZ"
"HTTP" permit
set policy id 29
set service "HTTPS"
exit
set policy id 30 name "FTP" from "RA" to "DMZ"  "RA Segment" "iSeries_DMZ" "FTP"
permit
set policy id 30
set service "FTP_SSL"
exit
set policy id 31 name "Notes" from "RA" to "DMZ"  "RA Segment" "iSeries_DMZ"
"Domino/Notes" permit
set policy id 32 name "Deny and Log" from "RA" to "DMZ"  "Any" "Any" "ANY" deny log
set policy id 33 name "Basic Web Access" from "RA" to "Untrust"  "RA Segment" "Any"
"DNS" permit
set policy id 33
set service "HTTP"
set service "HTTPS"
exit
set policy id 34 name "Deny and Log" from "RA" to "Untrust"  "Any" "Any" "ANY" deny
log
set policy id 36 name "Deny and log" from "Untrust" to "RA"  "Any" "Any" "ANY" deny log
set syslog config "10.10.0.11"
set syslog config "10.10.0.11" facilities local0 local0
set syslog config "10.10.0.11" log traffic
set syslog src-interface ethernet1
set syslog enable
set ssh version v2
set config lock timeout 5
set ntp server "time.nist.gov"
set ntp server backup1 "nt2.usno.navy.mil"
set ntp interval 60
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
exit
```

References

Assignment 1: Biometrics and IT Security

Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar. Handbook of Fingerprint Recognition. Springer, 2003

T.J Klevinsky, Scott Laliberte, Ajay Gupta. Hack I.T.. Addison-Wesley, 2002

Nalini K. Ratha, Andrew Senior and Ruud M. Bolle. “Automated Biometrics”. http://researchweb.watson.ibm.com/ecvg/pubs/ratha-auto.pdf

Ravi Das. “Business and Technical Factors To Be Taken Into Consideration Before Implementing a Biometric System At Your Place of Business”. http://www.findbiometrics.com/Pages/feature articles/business-technical-factors.html

Recognition Systems Inc.. “Convenience vs Security: How Well Do Biometrics Work”. http://www.findbiometrics.com/Pages/guide2.html

The Biometrics Consortium. “Biometrics 101 - The Basics”. http://www.findbiometrics.com/Pages/guide3.html

Russ Davis. “Debunking six myths of biometrics”. http://www.out-law.com/php/page.php?page_id=debunkingsixmyths1089377584&area=news

Dennis Carlton. "Integrity and Security at the Borders: The US VISIT Program". http://www.biometricgroup.com//US-VISIT.html

National Institute of Standards & Technology (NIST). “Fingerprint Vendor Technology Evaluation (FpVTE) 2003”. http://fpvte.nist.gov/index.html

The Biometric Consortium. http://www.biometrics.org/

International Biometric Group. “Biometric Market Report 2003-2007”. http://www.kiosks.org/pdfs/BMR_2003-2007.pdf

HTG Advance Systems. http://www.htgadvancesystems.com/Advance/biometrics/index.html

Craig Liddell. “Biometrics benefits individuals: expert”. electricnews.net June 15 2004. http://www.electricnews.net/news.html?code=9539478

Virginia Franke Kleist. “Organizational Risk and the Costs and Benefits of Biometrics” (Presentation to the European Biometrics Group, May 14 2004). http://www.be.wvu.edu/divmim/mgmt/kleist/BiometricsEU.ppt

International Biometric Industry Association. Biometrics Advocacy Report Vol VI Number 14. Aug 13 2004. http://www.ibia.org/newslett.htm

Economist.com. “Prepare to be Scanned”. http://www.economist.com/science/tq/displayStory.cfm?story_id=2246191

CBC News Online. “Biometrics: The future of security”. http://www.cbc.ca/news/background/airportsecurity/biometrics.html

NIST. ”CBEFF: Common Biometric Exchange File Format”. http://www.itl.nist.gov/div895/isis/bc/cbeff/

CDW Solutions. “The Biology of Security”. http://www.cdw.ca/webcontent/editorial/technologies/073102_TheBiologyOfSecurity.asp?printable=1

Processor.com. “Enterprises Slowly Warm To Biometrics”. Vol.26 Issue 32 Aug 6, 2004. http://www.processor.com/editorial/article.asp?article=articles/p2632/32p32/32p32.asp&guid=

Mike Scott. “Fingers Point Toward Biometrics”. For the Record Vol. 16 No. 16. Aug 9 2004. http://www.fortherecordmag.com/archives/ftr_080904p29.shtml

Bruce Schneier. “Crypto-Gram Newsletter”. May 15, 2002. http://www.schneier.com/crypto-gram-0205.html - 5

global-electronics.net. “Biometric passport delay continues”. http://www.global-electronics.net/id/24516/CMEntries_ID/55623

Junko Yoshida. “TI readies fingerprint biometrics tool”. http://www.planetanalog.com/printableArticle.jhtml?articleID=22104864

Assignment 2: Security Architecture

Joshua L. Wright and John N. Stewart. Securing Cisco Routers: Step-by-Step. The SANS Institute. 2002

Jesper M. Johansson. “Security Management: The Fundamental Tradeoffs”. Microsoft TechNet. http://www.microsoft.com/technet/community/columns/secmgmt/sm0104.mspx

Midrange servers: iSeries. http://www-1.ibm.com/servers/eserver/iseries/

Pat Botz, Carol Woodbury. “What Makes OS/400 Virus-Resistent?”. eServer Magazine, Oct 2003. http://eservercomputing.com/iseries/articles/index.asp?id=754&dir=/iseries/articles/

Postini. http://www.postini.com/

Snort. http://www.snort.org/

Jon Bull. “Snort's Place in a Windows 2000 Environment”. http://www.snort.org/docs/snort-win2k.htm

Symantec. http://www.symantec.com/index.htm

ZoneAlarm. http://www.zonelabs.com/store/content/home.jsp

RFC1918. http://www.rfc-editor.org/rfc/rfc1918.txt

Assignment 3: Firewall Policy

Robert Bayley. “Configuring a NetScreen Firewall” http://www.sans.org/rr/papers/21/812.pdf

NetScreen Technologies, Inc. “Netscreen Concepts and Examples: ScreenOS Reference Guide”. http://www.juniper.net/techpubs/software/screenos/screenos5x/ce_all_5_0.pdf

NetScreen Technologies, Inc. “Netscreen-200 Series User’s Guide”. http://www.juniper.net/techpubs/hardware/netscreen-appliances/netscreen-appliances50/ug_200.pdf

Juniper Networks, Inc. “Juniper Networks Netscreen CLI Reference Guide Version 5.0.0 Command Descriptions”. http://www.juniper.net/techpubs/software/screenos/screenos5x/cli_5_0.pdf