

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Table of Contents 1
William_Lorfing_GCFW.doc 2

© SANS Institute 2005, Author retains full rights.

William Lorfing
GCFW Practical Assignment
Version 4.0
December 18, 2004

Biometrics and their Use as Authentication Mechanisms for Remote Access

© SANS Institute 2005, Author retains full rights.

Summary 2
Assignment 1 2
- Basic Biometrics Guide 2
- Classifications of Biometrics 3
- Remote Access using Biometrics 4
- Advantages and Disadvantages of Biometrics 5
- Summary 7
- References 7

Assignment 2 – Security Architecture 10
- Network Security Architecture 10
- Required Ports, Protocols and other Restrictions for each group 12
- Network Diagram 13
- Analysis of Security Components for Defense-in-Depth 15

Assignment 3 – Firewall Policy 19

© SANS Institute 2005 Author retains full rights.

Summary
This practical contains three parts. The first part looks at the different types of biometrics and their advantages and disadvantages for use in remote access. This is followed by a network design for a small business with remote offices. The design includes network security requirements for the business, a network drawing and a description of the components used in the design. The final section analyzes the firewall rules that would have been used for the small business.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Assignment 1

Biometrics and their Use as Authentication Mechanisms for Remote Access

Focus: Discuss the advantages and limitations of using biometrics for remote access.

Generally, system authentication takes many different forms, and is usually broken down into three types of authentication:

- something you know – a password, PIN or piece of personal information
- something you have – a card key, smart card, or token
- something you are – a biometric [1]

It is this third authentication type, biometric, that I will be looking at to see how well it will work as an authentication method for remote access. So, to get a better understanding of biometrics, let us look at a basic guide on how a biometric system works. First, let's look at the different types or classifications of biometrics that can be used for authentication. Then specifically look at the authentication methods that are best suited for remote access.

Finally, I will look at some of the advantages and disadvantages of biometrics for remote access and the affect that it will have on the people that are in charge of them and the people that use them.

Basic Biometrics Guide

Biometrics is a technology that looks at the physiological or behavioral characteristics of a person and takes this information and processes it to generate a unique signature of a person. These characteristics or classifications come from fingerprints, hand geometry, a retina, an iris, a face, a signature or voice patterns. The process used to generate this unique signature or template is similar no matter which classification is used. This process can best be described using the diagram below, as taken from Liu and Silverman's – "A Practical Guide to Biometric Security Technology"[2]:

---

[1] Liu, Simon and Mark Silverman. "A Practical Guide to Biometric Security Technology." Computer.org. No date. IEEE Computer Society. 14 Oct. 2004. <http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm>.

[2] Liu and Silverman.

© SANS Institute 2005 Author retains full rights.

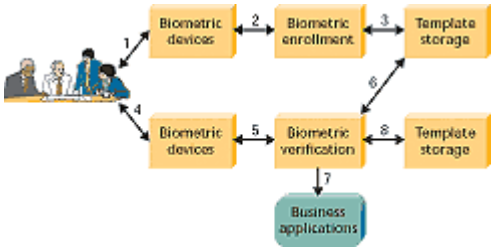


Figure 1. How a biometric system works.
(1) Capture the chosen biometric; (2) process the biometric and extract and enroll the biometric template; (3) store the template in a local repository, a central repository, or a portable token such as a smart card; (4) live-scan the chosen biometric; (5) process the biometric and extract the biometric template; (6) match the scanned biometric against stored templates; (7) provide a matching score to business applications; (8) record a secure audit trail with respect to system use.

Classifications of Biometrics

Fingerprints

Fingerprints have been used for hundreds of years, but by the early 20th century fingerprints were being used by the FBI for criminal investigations and identification of unknown persons. During the 1960's, a technology called "live-scan" was created that allowed images to be taken without the use of ink and greatly changed the use of fingerprints as an authentication method. Today, fingerprints are taken using optical sensors (light) or non-optical sensors (capacitance, ultrasonic wave, heat or pressure). [3] These images are then verified either by matching minutiae (traditional police method), straight pattern matching, moiré fringe patterns or ultrasonic.[4] Although fingerprinting can be accurate, the readers have to be maintained and kept clean for valid authorization.

Hand Geometry

Hand geometry measures and analyzes the characteristics of the hand and fingers. This biometric can have a high rate of accuracy and can be used in a wide array of applications. New York City Law Department uses hand geometry for accessing their offices and recording time and attendance.[5]

Retinal Scanning

Retinal scanning uses a low-intensity light to scan the layer of blood vessels of the retina and determine the unique patterns that exist. This technique can be very accurate, however, it is met with some resistance due to the user having to look through a receptacle and focus on a given point.[6]

---

[3] About Fingerprint Technology. No Date. BioEnable. 14 Oct 2004. <http://www.bioenabletech.com/biometrics_fingerprint_technology.htm>.
[4] Ashbourn, Julian. "A Biometric White Paper." Biometricsinfo.org. 1999. Biometrics information resource. 14 Oct 2004. <http://www.biometricsinfo.org/whitepaper4.htm>.
[5] Caruso, Jeff. "Biometrics early adopters reveal secrets, challenges." Network World Fusion. 28 Oct 2004. Network World. 28 Oct 2004. <http://www.nwfusion.com/news/2004/1028biometrics.html>.
[6] Liu and Silverman.

© SANS Institute 2005 Author retains full rights.

Iris recognition
Iris recognition uses a normal digital camera to analyze the feature of the colored ring tissue surrounding the pupil. This type of data acquisition is considered less obtrusive, since the user does not have direct contact with the reader.

Facial recognition
As the name suggests, facial recognition analyzes the characteristics of the face. As with iris recognition, this biometric does not require direct contact with the reader. Today, facial recognition is in use in some prominent applications: casino industry for catching scam artists[7], Illinois Department of Motor Vehicles for catching fraud and people trying to get multiple licenses[8] and in large crowds like the Super Bowls.

Signature verification
Signature verification is the analysis of the way a person signs their name. Surprisingly, the analysis just does not include the final signature, but the speed, velocity and pressure that a person uses to create this signature.[9]

Voice
The voice can be used for authentication or verification and for voice recognition. Voice authentication is based on a technology that converts voice to text and then this text is used for authentication.[10] Voice recognition is currently in use in the cellular phone industry for hands free operations.

Remote Access using Biometrics

Given these seven different biometrics, it is not surprising that some of these would be better suited for use as remote authentication devices than others. The biggest problem is how to integrate the capturing device in a remote system including the size of the device to make it usable as a remote access device. Let's look at the different biometrics and the feasibility of using them as a remote authentication device.

Fingerprint readers are now small enough that they can be integrated into many different types of input devices, thus making it an available option for remote access. Motion Computing, out of Austin, TX, is a good example of a computer system that has an integrated fingerprint reader built in.[11] With the reader being built in, a user does not need to attach or drag along another device to read

---

[7] Liu and Silverman.
[8] Caruso.
[9] Liu and Silverman.
[10] Liu and Silverman.
[11] M1400 Tablet PC's. No Date. Motion Computing. 22 Nov 2004. <http://www.motioncomputing.com/products/tablet_pc.asp>.

© SANS Institute 2005 Author retains full rights.

fingerprints. Even if the fingerprint reader is not built in there are a number of mice, keyboards and PCMCIA devices available that can be added on to any system.[12]

Since hand geometry readers are at least the size of a user's hand if not larger, it does not seem feasible or practical to use this as a remote input device. Retina scanners, much like the hand geometry readers, are too large to use as a remote input device, unless a user wound like to drag around a two pound input device.[13]

Iris and face recognition systems could be considered as another option for remote access authentication. These systems rely on software for doing the number crunching, but rely on normal digital cameras for getting the input. Because digital cameras are so common and the fact that webcams are so small now, these devices can easily be used.

At first, I thought signature recognition would not be an option for remote access because of the hardware, pen and digital pad, normally thought to be required. However, I found a pen[14] that doesn't use a digital pad, so this could be another option for use as a remote access device.

Advantages and Disadvantages of Biometrics

Now that we have looked at the basic process for gathering biometrics, the different type of biometrics that can be used and looked briefly at biometrics that would be best suited for remote access, let us look at the advantages and disadvantages and the implications that remote access biometrics will have on the people that administer them.

The main advantage, no matter which biometric is used for authentication, is that the user is the key and thus the key can not easily be taken away or lost.[15]

To gain access to a system remotely, a user presents their biometric to the system for either identification ("Who is this?") or verification ("Is this the person who he/she claims to be?"). After a positive reading, the user is granted access to the system. [16]

---

[12] Search Page. No Date. CDW. 22 Nov. 2004. <http://www.cdw.com/shop/search/Results.aspx?key=biometric&platform=all>.
[13] Kandasamy, Nadarajah and Bansode Rishipal. Biometric Authentication. No Date. Louisiana State University. 22 Nov 2004. <http://isds.bus.lsu.edu/cvoc/projects/techlibrary/Bio/retinascan>.
[14] Products. No Date. DynaSig Biometric System. 22 Nov. 2004. <http://www.dynasig.com/page/Products.htm>.
[15] Biometrics 101 – The Basics. No Date. TopicZ. 14 Oct. 2004. <http://www.findbiometrics.com/Pages/guide3.html>.
[16] Kawamura, Cynthia. "Security White Paper - Remote Access for Healthcare – HIPAA and Beyond." Rainbow Technology. 2003. Rainbow Technology. 9 Oct. 2004. <http://www.safenet-inc.com/Library/8/Remote%20Access%20for%20Healthcare%20-%20HIPAA%20and%20Beyond.pdf>.

© SANS Institute 2005 Author retains full rights.

The first step in a biometric system is capturing the biometric and translating the code into a template. While this sounds easy, problems arise with a large remote user base that is not near this input device. Either all of the remote users would go to the device or someone would be sent out to the remote user to collect the sample. Either way, this could cost a lot of time and money.[17]

The main disadvantage of having remote access is the need to have some type of biometric reader at each of the locations a user might need to authenticate. So, depending on how many users or remote locations need access, the hardware cost alone will start adding up. Beside the hardware costs, a firm must also consider how much time and resources it will take to setup each of the devices and keep them running.

Once the template and the sample are ready to go, administrators must be aware of how the biometric system works and how to tweak the input devices to give the most accurate authentication results for the system it secures. As part of this tweaking, many vendors have two different methods for determining the accuracy of a biometric system, however they both mean the same thing. One method is called the false-acceptance rate and the other is the false reject rate. False acceptance is when a positive authentication is given for an invalid entry.

As the system is tweaked, if the template and the sample are to be as closely matched as possible the false-accept rate is lower, but the rejection rate is higher which could cause a valid user to be rejected. So, by going the other way, if the requirement that the samples match as closely and the false-reject rate is lowered, the acceptance rate now becomes higher. This means that someone not authorized to access the system might gain access.[18] Although this really doesn't have any advantages or disadvantages for the remote user, it could have a disadvantage on the day-to-day operations, in that the IT department might need additional personnel on staff to handle the additional load of users being unable to access the network.

Although the user has authenticated remotely, this does not necessarily mean that the user is in control, because a number of biometric solutions are still using only one-factor authentication methods.[19] One-factor authentication is where only one method (password or signature) is required to be given access. A way to improve the security is to use an additional token to verify the identity. This could be a one time key, a password or some other token. Biometrics are still vulnerable to replay attacks. There are a number of different ways replay attacks occur. One possible way an attack can occur is the hacker has

[17] Challenges in Large-scale Biometrics Deployment. No Date. SentryCom Ltd. 14 Oct. 2004. <http://forsure.sela.co.il/Large_scale.doc>.
[18] Liu and Silverman.
[19] Kawamura, Cynthia. "Security White Paper - Remote Access for Healthcare – HIPAA and Beyond." Rainbow Technology. 2003. Rainbow Technology. 9 Oct. 2004. <http://www.safenet-inc.com/Library/8/Remote%20Access%20for%20Healthcare%20-%20HIPAA%20and%20Beyond.pdf>.

© SANS Institute 2005 Author retains full rights.

somehow intercepted the transmission of the template taken from the reader. The hacker then re-injects this template back into the system when he or she wants to gain access using this stolen information.[20]

There have been studies done to show that biometric systems can be attacked or fooled by fake fingers and digital pictures. One of these studies looked at the use of artificial "gummy" fingers to fool fingerprint systems. The fingers were molded out of gelatin from either a live sample or from a digital picture that was made into a mold and then used to fool the biometric reader.[21] Another study showed that pictures of a subject could be taken and placed on a laptop. Then, by holding the laptop up to the facial recognition system, the researchers were able to get access to the system.[22] (17)

Summary

The use of biometrics has come a long way since fingerprints were first used. This can be seen well in the use of biometrics for remote authentication. As the input devices become smaller, more manageable and cheaper, we will start to see biometrics being used more and more as authentication devices. But as biometrics are deployed, network security personnel have to be aware of the overhead costs for managing these systems and combat the different types of attacks that could be used against systems. Biometrics is not perfect, but if it is one less thing we have to remember, then it will always help in the long run.

References

About Biometrics Technology. No Date. BioEnable. 14 Oct. 2004. <http://www.bioenabletech.com/biometrics_infomation.htm>.

About Fingerprint Technology. No Date. BioEnable. 14 Oct. 2004. <http://www.bioenabletech.com/biometrics_fingerprint_technology.htm>.

Ashbourn, Julian. "A Biometric White Paper." Biometricsinfo.org. 1999. Biometrics information resource. 14 Oct. 2004. <http://www.biometricsinfo.org/whitepaper4.htm>.

Ashbourn, Julian. "Remote Network Access." 1to1.org. 2001. Avanti. 30 Sept 2004. <http://www.avanti.1to1.org/remoteaccess.html>.

Biometrics. No Date. BambooWeb Dictionary. 14 Oct. 2004. <http://www.bambooweb.com/articles/b/i/Biometrics.html>

Biometrics 101 – The Basics. No Date. TopicZ. 14 Oct. 2004. <http://www.findbiometrics.com/Pages/guide3.html>.

[20] Kawamura.

[21] Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada and Satoshi Hoshino. "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems". Proceedings of SPIE. 24 – 25 Jan. 2002. The International Society of Optical Engineers. 14 Oct. 2004. <http://cryptome.org/gummy.htm>.

[22] Thalheim, Lisa, Jan Krissler and Peter-Michael Ziegler. "Body Check." Heise c't – WWW. Nov. 2002, Page 114 – Biometrie. 14 Oct. 2004. <http://www.heise.de/ct/english/02/11/114/default.shtml>.

© SANS Institute 2005 Author retains full rights.

Caruso, Jeff. “Biometrics early adopters reveal secrets, challenges.” Network World Fusion. 28 Oct. 2004. Network World. 28 Oct. 2004. <http://www.nwfusion.com/news/2004/1028biometrics.html>.
Challenges in Large-scale Biometrics Deployment. No Date. SentryCom Ltd. 14 Oct. 2004. <http://forsure.sela.co.il/Large_scale.doc>.
Cherry, Kyle. “Biometrics: An In Depth Examination.” SANS Reading Room. Nov. 2003. SANS.org. 14 Oct. 2004. <http://www.sans.org/rr/whitepapers/authentication/1329.php>.
Choosing a Biometric Solution. No Date. TopicZ. 14 Oct. 2004. <http://www.findbiometrics.com/Pages/guide5.html>.
Convienience vs Security: How Well Do Biometrics Work. No Date. TopicZ. 14 Oct. 2004. <http://www.findbiometrics.com/Pages/guide2.html>.
Dunker, Mary. “Don’t Blink: Iris Recognition for Biometric Identification.” SANS Reading Room. 20 Nov. 2003. SANS.org. 14 Oct. 2004. <http://www.sans.org/rr/whitepapers/authentication/1341.php>.
Glossary. No Date. TopicZ. 14 Oct. 2004. <http://www.findbiometrics.com/Pages/glossary.html>.
Identification versuses Verification. No Date. TopicZ. 14 Oct. 2004. <http://www.findbiometrics.com/Pages/guide4.html>.
Kawamura, Cynthia. “Security White Paper - Remote Access for Healthcare – HIPAA and Beyond.” Rainbow Technology. 2003. Rainbow Technology. 9 Oct. 2004. <http://www.safenet-inc.com/Library/8/Remote%20Access%20for%20Healthcare%20-%20HIPAA%20and%20Beyond.pdf>.
Liu, Simon and Mark Silverman. “A Practical Guide to Biometric Security Technology.” Computer.org. No date. IEEE Computer Society. 14 Oct. 2004. <http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm>.
Kandasamy, Nadarajah and Bansode Rishipal. Biometric Authentication. No Date. Louisiana State University. 22 Nov. 2004. <http://isds.bus.lsu.edu/cvoc/projects/techlibrary/Bio/retinascan>.
M1400 Tablet PC’s. No Date. Motion Computing. 22 Nov. 2004. <http://www.motioncomputing.com/products/tablet_pc.asp>.
Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada and Satoshi Hoshino. “Impact of Artificial ‘Gummy’ Fingers on Fingerprint Systems”. Proceedings of SPIE. 24 – 25 Jan. 2002. The International Society of Optical Engineers. 14 Oct. 2004. <http://cryptome.org/gummy.htm>.
Myers, Lisa. “An Exploration of Voice Biometrics.” 19 Apr. 2004. SANS GSEC Practical. 14 Oct. 2004. <http://www.sans.org/rr/whitepapers/authentication/1436.php>.
Olsson, Tricia. “Strengthening Authentication with Biometric Technology.” 26 Aug. 2003. SANS GSEC Practical. 14 Oct. 2004. <http://www.sans.org/rr/whitepapers/authentication/1226.php>.
Products. No Date. DynaSig Biometric System. 22 Nov. 2004. <http://www.dynasig.com/page/Products.htm>.
Publications and Periodicals. No Date. The Biometric Consortium. 14 Oct. 2004.

© SANS Institute 2005 Author retains full rights.

<http://www.biometrics.org/html/publications.html>.
Search Page. No Date. CDW. 22 Nov. 2004.
<http://www.cdw.com/shop/search/Results.aspx?key=biometric&platform=all>.
Slade, Rob. "REVIEW: 'Biometrics for Network Security', Paul Reid." Online Posting – News Thread. 01 Oct. 2004. No Listserv. 14 Oct. 2004.
<http://groups.google.com/groups?hl=en&lr=&threadm=cjscvg%24qqm%240%24208.20.133.66%40netheaven.com&rnum=1&prev=/groups%3Fhl%3Den%26lr%3D%26q%3Dbruce%2Bbarnett%2Bbiometrics>.
Spinella, Edmund. "Biometric Scanning Technologies: Finger, Facial and Retinal Scanning." 28 May 2003. SANS GSEC Practical. 14 Oct. 2004.
<http://www.sans.org/rr/whitepapers/authentication/1177.php>.
Thalheim, Lisa, Jan Krissler and Peter-Michael Ziegler. "Body Check." Heise c't – WWW. Nov. 2002, Page 114 – Biometrie. 14 Oct. 2004.
<http://www.heise.de/ct/english/02/11/114/default.shtml>.
What are Biometrics. No Date. TopicZ. 14 Oct. 2004.
<http://www.findbiometrics.com/Pages/guide1.html>.

© SANS Institute 2005, Author retains full rights.

Assignment 2 – Security Architecture

The purpose of this assignment is to look at the security architecture for GIAC Enterprises. GIAC Enterprises is a small business that sales fortune cookie sayings to customers worldwide, with approximately fifty employees. A majority of these employees work in or close to the corporate office and the rest are distributed geographically around the world. All sales are done via the Internet.

Network Security Architecture
Here are the access requirements and restrictions for different groups that interact with GIAC Enterprises.

Customers
Companies or individuals that purchase fortune cookies will be required to login to the web server on the service network using a Secure Socket Layer (SSL) connection on the web server. They will enter their orders on the web server and the transaction will be sent encrypted to the Enterprise Resource Planning (ERP) system located on the service network. Customers will have the ability to create an online account.

Suppliers
Companies that supply fortune sayings will be required to login to a special section of the web server for transferring sayings to GIAC. All traffic will be through a SSL connection on the web server. All data will reside on the ERP system and all traffic from the web server to the ERP system will be encrypted. GIAC will issue username and passwords to companies that are authorized suppliers.

Partners
International companies that translate or resell fortunes will be required to login to the web server for transferring translated sayings or ordering fortune cookies. All traffic to and from the partner companies will be through a SSL connection on the web server. The data will reside on the ERP system and all traffic to and from the ERP system to the web server will be encrypted. GIAC will issue the username and passwords to companies that are authorized partners.

Customers, Suppliers and Partners will be allowed to change their passwords as long as the new passwords are at least 6 characters long and contain at least 1 number or symbol.

GIAC Enterprise employees on internal network
Accounting, Sales & Manufacturing
These departments will access the external web server through the SSL connection using individual username and password combination. Depending on the user permissions, they can access the accounting section, the sales section and/or the fortunes database through the web server.

© SANS Institute 2005 Author retains full rights.

Administrators
These users will have access to all servers, routers and firewalls on the service network and internal network through SSH.

All Employees
All employees will have web access to the Internet using a proxy server sitting on the service network.

There will be a file server available for data storage, where the data can be stored in either a personal directory or if files need to be shared they can be placed in a directory that is accessible by a group.

Everyone will be able to retrieve email off of the internal mail server through POP or IMAP and send email through the SMTP port on this server.

DNS will be resolved by the internal DNS server. NTP or network time will be available from the DNS/NTP server.

All workstations will have virus protection on them

GIAC Enterprise remote users
Access for remote users will be the same as the internal users, except the remote user must establish a VPN connection to the corporate VPN concentrator before access to any system is allowed. For users in the regional offices, a VPN tunnel will be established between the Cisco router at the regional office and the VPN concentrator at the corporate office.

For users not located in a regional office, the user will need a personal firewall running and then they will need a VPN client on their workstation to gain access to the corporate network.

With a valid username and password, a remote user can access the web server directly using SSL, for placing orders or accessing the fortune database.

All network traffic in the regional office will pass through a packet filtering router. All workstations will have virus protection on them.

General Public access and General Notes for GIAC Enterprise
Everyone will have access to the public web server for accessing web pages. Basic product information and basic company information will be available on the public web server.

All Inbound mail will go through a mail relay server, located in the service network, where it will be scanned for viruses and spam, and then the mail will be forwarded on to the internal mail server.

© SANS Institute 2005 Author retains full rights.

DNS queries from the internet will be handled by the DNS server located on the service network.

All outbound mail will be checked for viruses.

Required Ports, Protocols and other Restrictions for each group

Customers

- In from Internet to DMZ TCP Port 443 – SSL connection to web server

Suppliers

- In from Internet to DMZ TCP Port 443 – SSL connection to web server

Partners

- In from Internet to DMZ TCP Port 443 – SSL connection to web server

GIAC Enterprises Employees on the Internal Network

- In from Inside to DMZ TCP Port 443 – SSL connection to web server
- In from Inside to DMZ TCP Port 80 – connection to web server
- In from Inside to TCP Port 22 – SSH connection to all servers
- In from Inside to DMZ TCP Port 80 – Internet WWW traffic will be redirected to Proxy Server on Service Network
- In from Inside to Inside TCP Port 110 – POP3 connection to mail server
- In from Inside to Inside TCP Port 995 – POP3S connection to mail server (Encrypted Session)
- In from Inside to Inside TCP Port 143 – IMAP connection to mail server
- In from Inside to Inside TCP Port 993 – IMAPS connection to mail server (Encrypted Session)
- In from Inside to Inside TCP Port 53 – Internal DNS
- In from Cisco to Inside UDP Port 514 – Syslog from Cisco Router 2851 to logging server
- In from Cisco to Inside UDP Port 123 – Network time from Cisco Router 2851 to NTP server

GIAC Enterprises remote Users

- In from VPN to DMZ TCP Port 443 – SSL connection to web server
- In from Internet to VPN concentrator for IPSEC
  Protocol 50 – Encapsulating Security Payload (ERP)
  UDP Port 500 – Internet Key Exchange (IKE)
- In from Internet to VPN concentrator
  Protocol 47 – Generic Routing Encapsulation (GRE) for VPN
  TCP Port 1723 – VPN
  TCP Port 443 – SSL Connection to VPN for web access

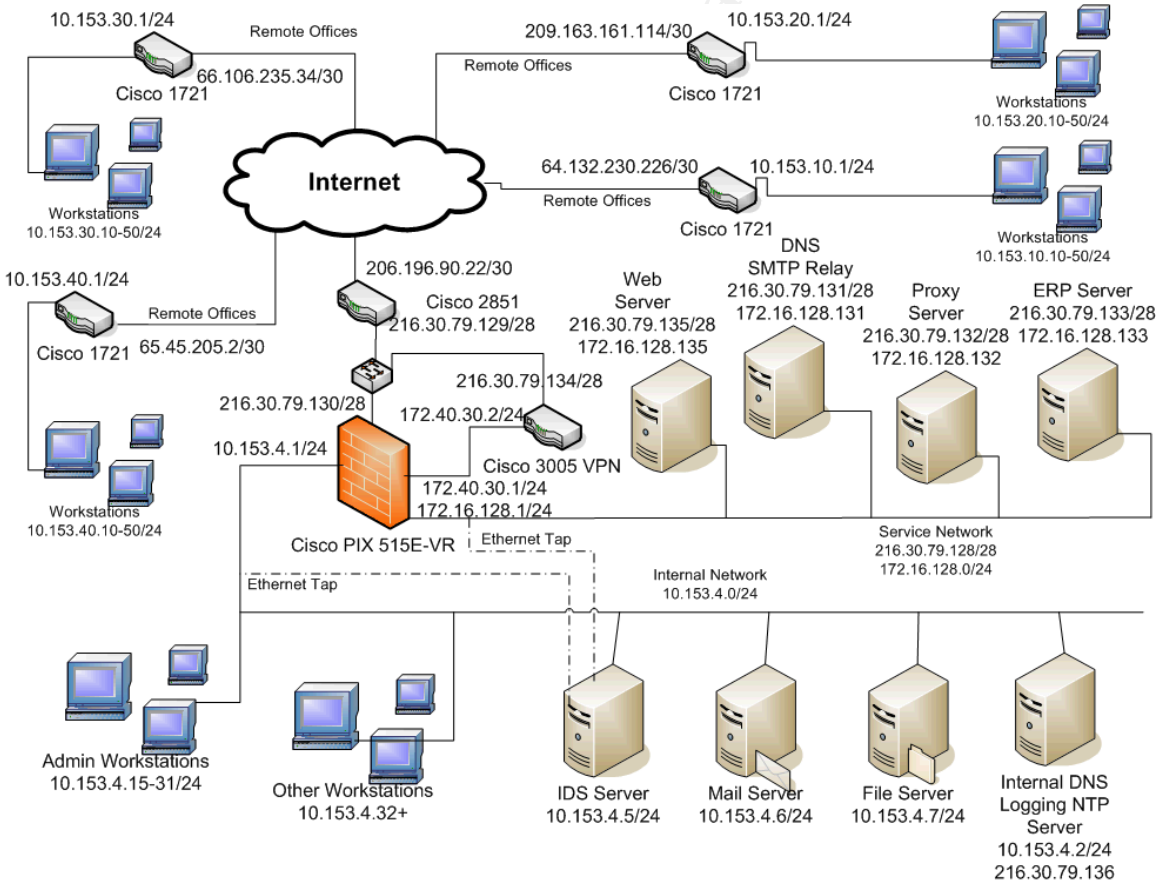
© SANS Institute 2005 Author retains full rights.

- In from VPN to Inside TCP Port 110 – POP3 connection to mail server
- In from VPN to Inside TCP Port 995 – POP3S connection to mail server (Encrypted Session)
- In from VPN to Inside TCP Port 143 – IMAP connection to mail server
- In from VPN to Inside TCP Port 993 – IMAPS connection to mail server (Encrypted Session)
- In from VPN to Inside TCP Port 53 – Internal DNS
- In from VPN to TCP Port 22 – SSH connection to all servers

General Public

- In from Internet to DMZ TCP Port 80 – Web server interface
- In from Internet to DMZ TCP Port 53 – External DNS
- In from Internet to DMZ TCP Port 25 – SMTP Relay Server

Network Diagram



Filtering Routers:

Cisco 2851 - CISCO2851-SEC/K9

IOS - 12.3(8)T

© SANS Institute 2005 Author retains full rights.

Cisco 1721 – CISCO1721-VPN/K9

- IP/ADSL/FW/IDS IPSEC 56 or IP/ADSL/FW/IDS IPSEC 3DES depending on where unit is installed at in the world
- This can also be referenced as IOS version Advanced Security feature.
- IOS - 12.3(8)T

Firewall:

Cisco PIX 515E-UR Version 6.3(4)

Firewall with 6 ports (4 used)

1 – Cisco 2851
1 – Service Network
1 – Inbound Port of the Cisco 3005 VPN Concentrator
1 – Internal Network

VPN:

Cisco 3005 – IOS 4.1.7.C

Web server

FreeBSD 5.3 with Apache 1.3+SSL
Tripwire to make sure nothing is changed

DNS/SMTP relay server

FreeBSD 5.3
Bind 9 with external addresses in DNS
Sendmail – Inflex, SpamAssassin, McAfee virus protection

Squid Proxy Server

Web traffic will need to be diverted to the proxy server so that it can perform access control and filtering.

IDS Snort with sensors on Service network and internal network

Mail server

Sendmail with McAfee virus protection

File server

Internal DNS, Logging, and NTP Server

Bind 9 with internal addresses in DNS
All Cisco logs will be sent here
NTP server for handing out Network Time

Workstations running virus protection (Norton)

© SANS Institute 2005 Author retains full rights.

Analysis of Security Components for Defense-in-Depth

Cisco 1721 Router

The Cisco 1721 is used in the remote offices as the router to the internet and as the end point for creating either an IPSEC tunnel or VPN connection back to the corporate office. I will use the firmware image that has the stateful firewall built in and use that for filtering inbound and outbound traffic. Because of the small number of employees in the remote office this should not hurt the performance of the router.

The weakness of using only the router as the firewall is that if anyone breaks in, they are completely into the remote office with the potential to come back across the secure tunnel to the corporate office. Another possible weakness is that we will possibly have to use the weakest encryption algorithm for the VPN connections depending on where in the world the remote office is located. The use of the weakest algorithm is due to Crypto Laws that regulate what encryption can be sent outside the US. Another weakness of the router is that it does not have any place to store logs, so the logs will need to be sent to an external server.

A benefit of using this router is that I will be able to use Network Address Translation (NAT) to convert the private IP address on the internal network to a public address that can talk to the internet. By using NAT, the workstations are not sitting directly on the internet.

Cisco 2851 Router

The Cisco 2851 is a router designed for a small to medium sized company that is reasonably priced, but has the flexibility to accept over 50 different WAN interface cards, as the company grows. The purpose of this router is to route traffic from the Internet Service Provider (ISP) to GIAC's public internet address space and to filter some unwanted traffic coming in.

The router can be used as a VPN termination point and firewall software could be loaded, but I chose to use a separate VPN concentrator and firewall box to offload these processes from the router. I am still going to use filters on the router to protect the router from attacks and to make sure we are not sending out non-routable IP addresses and other ports. This router has the same logging issue, in that the logs will need to be sent to an external server.

Cisco PIX 515E-VR

The PIX Firewall will be an integral part of the depth-in-defense design. It will allow for filtering and packet checking on a number of different interfaces through the stateful firewall. The placement of the PIX gives us a number of different ways that we can protect the network. First, the internal network will be using Network Address Translation (NAT) for all traffic coming in and out of the network. Second, we can isolate the Service Network and filter traffic coming in

© SANS Institute 2005 Author retains full rights.

and out. Finally, the inbound interface of the VPN concentrator is connected to another interface on the PIX, so inbound and outbound traffic for the VPN concentrator can be scrutinized also.

As with any device there are some strengths and weaknesses that we should look at. Some of the strengths include, no underlying operating system where security flaws or speed limitations can hurt us, no moving parts since everything is stored in flash memory and finally software upgrades are easy since. To upgrade a system, an image needs to be put on the flash memory and then install this on the machine in question. However, the PIX has problems with keeping logs locally because of the limit flash memory, so the logs will need to be sent to an external log server for processing and review.

Cisco 3005 VPN Concentrator

The VPN Concentrator will be used to terminate IPSEC and VPN tunnels from the remote offices and remote users using VPN clients. The VPN concentrator is connected to the Service Network for its external IP address and then the internal IP connection is connected to the PIX firewall. This configuration was used so that all traffic is going through the firewall, so it can be properly filtered. If needed, a VPN connection can be established through a SSL connection directly to the VPN concentrator for establishing a secure connection.

Although this isn't a weakness to this design, a drawback to having the VPN concentrator connect on the service network and connect back to the firewall is that we use up another interface on the firewall. However, by connecting back to the firewall instead of connecting to the internal network, all traffic is checked and we are not leaving a back door into the network.

The VPN connections could have easily been terminated in either the PIX or the 2851, but I chose to use a separate device so that the other devices didn't have to worry about the overhead of connecting the tunnels to these other devices. This does add additional cost to the design, but it gives us a better defense-in-depth for the remote users.

Squid Proxy Server

All web traffic will be redirected to the proxy server, where the proxy server will then retrieve the requested web page from the web server, if it is not already stored in the proxy server's cache. From a security stand point, the proxy server is used as an access control point, in that it can filter the web pages that are presented on a number of different levels. Although this filtering seems like it might not help much, the proxy server could possibly prevent malicious active-x scripts from being run on a workstation, which could cause major damage to the workstation and the network. The proxy server is located in the service network so that in the event the proxy server is compromised the hacker will still have to break through the firewall to get to the internal network.

© SANS Institute 2005 Author retains full rights.

Proxy servers are not without their problems. Some systems show slower performance due to intense CPU cycles and limited memory space. This problem can be mitigated by getting a system that has more memory and CPU cycles or by adding additional proxy servers and running them in parallel. Even though we specified that all web traffic was to be diverted to the proxy server, some traffic will just get passed through the proxy server out to its original destination. SSL traffic is a good example, because the traffic is already encrypted when it reaches the proxy server. So the proxy server can not decrypt the traffic since it is not one of the terminating end points.

Squid was chosen because it is an open source product, so the cost is kept low for the software portion of the server. There are also a number of modules that can be added on that can help increase the functionality and filtering capabilities of the proxy server.

Network Intrusion Detection System (NIDS)
The NIDS system watches the network for any abnormal traffic or traffic that it has signatures for and alerts the operator on anything that is found. The main security function is monitoring the network for any attempted penetrations, hacks or suspicious activity. Ethernet taps will be used to acquire the data off of the internal network and service network instead of using a mirror or monitor port on the network switches. The reason we are using a tap rather than the switch is because, if the switch becomes too busy or is overloaded usually the first thing it stops doing is forwarding traffic to the monitor port. If that happens, we lose the ability to monitor what might be going on, on the network. The taps are placed at the point where the network goes into the firewall. This is done so that we capture all the traffic going in and out. The only drawback to where the taps are placed is that we might not capture bad traffic going between hosts.

The NIDS system I have chosen to use is SNORT. Although there is a large deployment of SNORT systems, the biggest weakness to the system comes from new exploits that have just been introduced, but the SNORT system does not have any signatures for this exploit. However, one of the benefits of using SNORT comes from the ease that a new signature can be written and installed on the server to protect from the network from this new exploit.

Web Server
This server will serve out web pages for both the public portion of the web site, as well as, for the secure sections of the website. This device also serves as the front end to the ERP system, so that the ERP system is not touched directly by the public. Although this is a basic web server, it will have Tripwire and a local firewall running. The firewall will be used to make sure only the traffic we expect to be coming in, is coming in. I will also be running Tripwire to check for file consistency. The drawback to running Tripwire is that it is not running in real time, so the adminstrator will not immediately know that a critical file has been changed. One weakness of the whole system is that if the web server is

© SANS Institute 2005 Author retains full rights.

compromised, the hacker might be able to then attack the ERP system. This weakness is mitigated some by having a firewall running locally and having tripwire scheduled to run a couple of times a day to make sure nothing has changed. All the software on the system is open source, so this helps cut down on the cost of deploying the system.

External DNS and Mail Server

This server is a dual function system. The first part of the system hands out external DNS information. The internal and external DNS functions have been separated to help mitigate any problems that could arise if the DNS system is hacked or the DNS tables become corrupted. The other function that this server performs is handling incoming email. All mail from the internet comes to this server first. Email is scanned for viruses and any undesirable attachments are held until they can be validated that they are valid files. Email is also run through SpamAssassin to mark any mail that is considered spam. Once all of this security checking has been done, the mail is forwarded on to the inside mail server where the mail could be possibly checked again for viruses. This server is located on the service network, because if anything is compromised on the server, we do not want a hacker getting to an inside server. This server is also using open source programs for everything but the virus scan, in which case, McAfee Antivirus is being used.

Internal DNS, Logging and NTP server

The purpose of this server is to reply to internal DNS queries, act as a syslog server for the Cisco Routers and act as a network time server. Although none of these processes are directly involved in the security of the network, they compliment the other systems that are involved in securing the network. By keeping a local time server, all devices can have a fairly accurate date and time stamp when needed. This accuracy comes into play when we start looking at all the logs that are going to be kept on this server for storage and processing. One weakness of this server is that there are a number of processes running that have to have a port open to the network. With the more ports open, the more difficult it becomes to secure a server. This is still a concern, but not as bad since this server is not directly connected to the internet.

© SANS Institute 2005 Author retains full rights.

Assignment 3 – Firewall Policy

```
: Saved
: Written by enable_15 at 00:20:32.656 UTC Sat Dec 18 2004
PIX Version 6.3(4)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
!---
!--- These commands name and set the security level for
!--- their respective interfaces. Only 4 of the 6 interfaces
!--- are being used.
!---
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
nameif ethernet3 dmzvpn security60
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
!---
enable password x2OosqqMAlEh1s5a encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixie
domain-name giac.org
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!---
!--- The order of the access list rules are not dependent on the order
!--- since they are all permit rules and there is an explicit rule that
!--- if something is not allowed then it is denied. So the only time that rule order
!--- might have a problem would be if some deny rules were present, in which
```

© SANS Institute 2005 Author retains full rights.

```
!--- case rule order would matter and some rules might not get run.
!---


!---
!--- This following seven statement make up an access list, named outside_int.
!--- Each line represents a different port and/or protocol.
!--- This line allows SMTP traffic originating from anywhere to reach the
!--- DNS/SMTP server. This is one of the general rules that smtp traffic
!--- from the outside will be directed to the relay server. Mail is only allowed
!--- to come into one server, so scanning and processing is easier.
!---
access-list outside_int permit tcp any host 216.30.79.131 eq smtp
!---
!--- The next two lines allow our external DNS server to be queried as needed.
!--- Traffic for tcp and upd are allowed into the DNS server. If the DNS server is
!--- hacked information is limited to the external address since the DNS
functions
!--- are on two machines. Sometimes the names of servers, give away too much
!--- about what  a system does.
!---
access-list outside_int permit tcp any host 216.30.79.131 eq domain
access-list outside_int permit udp any host 216.30.79.131 eq domain
!---
!--- The next two lines allow web unencrypted (www) and encrypted (https) traffic
!--- to reach the external web server. Although the traffic was broken out for
!--- specific groups, it ends up that everyone will have access to the http and
!--- https server. Web traffic is limited to one server and if the server is broken
!--- into, it is still in the DMZ.
!---
access-list outside_int permit tcp any host 216.30.79.135 eq www
access-list outside_int permit tcp any host 216.30.79.135 eq https
!---
!--- The next two rules allows only the router to query the the ntp server for the
!--- and it also allows the router to send system logs to the loggin server. These
!--- two lines are important as far as security goes so we have the correct time
on
!--- any traffic that is logged.
!---
access-list outside_int permit udp host 216.30.79.129 host 216.30.79.136 eq ntp
access-list outside_int permit udp host 216.30.79.129 host 216.30.79.136 eq
syslog
!---
!--- The next statement creates an access list named dmz_int. The only traffic
!--- allowed out of the Service Network (DMZ) is mail going from the relay server
!--- to the internal server. By having the mail scanned on another machine, if
!--- something happened to the external mail server, a user would still be able to
```

© SANS Institute 2005 Author retains full rights.

```
!--- get mail off the internal mail server.
!---
access-list dmz_int permit tcp host 172.16.128.131 host 10.153.4.6 eq smtp
!---
!--- The next six lines create an access list named inside_int. This is traffic that
!--- will be going out of the internal network. This first line is for administrator
!--- access to outbound ssh. By using ssh, data is encrypted between the
!--- administrator and the server. This is one of the network requirements.
!---
access-list inside_int permit tcp 10.153.4.0 255.255.255.224 any eq ssh
!---
!--- This next line allows web traffic to go out. In my network drawing, web traffic
!--- from the internal network was suppose to go the Squid Proxy Server.
!--- However, I could not figure out how to get the PIX to redirect any outbound
!--- web traffic to the proxy server. The proxy server was suppose to limit the
!--- exposure of workstations to invalid or inappropriate web sites.
!---
access-list inside_int permit tcp any any eq www
!---
!--- This next line permits the internal NTP server to go out to external ntp servers
!--- to update it's time. Allows the internal time server to keep it's clock set
!--- correctly.
!---
access-list inside_int permit tcp host 10.153.4.2 any eq 123
!---
!--- The next two lines allow web unencrypted (www) and encrypted (https) traffic
!--- to reach the external web server. Although the traffic was broken out for
!--- specific groups, it ends up that everyone will have access to the http and
!--- https server. This is one of the network requirements that internal users
!--- can access these servers. DNS will handle the different ip address between
!--- being inside and outside.
!---
access-list inside_int permit tcp any host 172.16.128.135 eq www
access-list inside_int permit tcp any host 172.16.128.135 eq https
!---
!--- This last access list is for the dmzvpn interface. This is the interface where
!--- the VPN concentrator connects.
!--- The next two lines allow our internal DNS server to be queried as needed.
!--- Traffic for tcp and upd are allowed into the DNS server. This just allows
!--- remote users to use the internal dns.
!---
access-list dmzvpn_int permit tcp any host 10.153.4.2 eq domain
access-list dmzvpn_int permit udp any host 10.153.4.2 eq domain
!---
!--- This next line allows any vpn connection to establish an ssh tunnel to the first
!--- group of machines on the internal network. If this was not allowed no one
```

© SANS Institute 2005, Author retains full rights.

```
!--- be able to ssh to any device when coming through the VPN. By using SSH,
!--- sessions traffic between remote users and specific servers is encrypted.
!---
access-list dmzvpn_int permit tcp any 10.153.4.0 255.255.255.224 eq ssh
!---
!--- The next four lines are for connecting either pop3 or imap clients to the
!--- internal mail server. There is also the possiblity of doing this through an
!--- ssh tunnel so POP3S (995) or IMAPS (993) could be used to connect to
!--- the server.
!---
access-list dmzvpn_int permit tcp any host 10.153.4.6 eq pop3
access-list dmzvpn_int permit tcp any host 10.153.4.6 eq 995
access-list dmzvpn_int permit tcp any host 10.153.4.6 eq imap4
access-list dmzvpn_int permit tcp any host 10.153.4.6 eq 993
!---
!--- The next two lines allow web unencrypted (www) and encrypted (https) traffic
!--- to reach the external web server. Although the traffic was broken out for
!--- specific groups, it ends up that everyone will have access to the http and
!--- https server. This is one of the network requirements that VPN users
!--- can access these servers. DNS will handle the different ip address between
!--- being inside and outside.
!---
access-list dmzvpn_int permit tcp any host 172.16.128.135 eq www
access-list dmzvpn_int permit tcp any host 172.16.128.135 eq https
!---
pager lines 24
logging on
logging timestamp
logging buffered debugging
logging trap alerts
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu dmzvpn 1500
mtu intf4 1500
mtu intf5 1500
!---
!--- These are the IP addresses for each of the PIX interfaces
!---
ip address outside 216.30.79.130 255.255.255.240
ip address inside 10.153.4.1 255.255.255.0
ip address dmz 172.16.128.1 255.255.255.0
ip address dmzvpn 172.40.30.1 255.255.255.0
no ip address intf4
no ip address intf5
!---
```

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

```
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address dmz
no failover ip address dmzvpn
no failover ip address intf4
no failover ip address intf5
pdm history enable
arp timeout 14400
!---
!--- These two commands establish port address translation (PAT) for traffic
!--- on the internal network and traveling outside.
!---
global (outside) 10 interface
nat (inside) 10 10.153.4.0 255.255.255.0 0 0
!---
!--- The next two static line entries essentially prevent the inside and
!--- dmzvpn networks from getting translated when packets are trying to reach
!--- the dmz network.
!---
static (inside,dmz) 10.153.4.0 10.153.4.0 netmask 255.255.255.0 0 0
static (dmzvpn,dmz) 172.40.30.0 172.40.30.0 netmask 255.255.255.0 0 0
!---
!--- The next line translates the external address 216.30.79.131 to
!--- 172.16.128.131 for DNS/SMTP relay server in the dmz.
!---
static (dmz,outside) 216.30.79.131 172.16.128.131 netmask 255.255.255.255 0
0
!---
!--- The next line translates the external address 216.30.79.132 to
!--- 172.16.128.132 for Squid Proxy server in the dmz.
!---
static (dmz,outside) 216.30.79.132 172.16.128.132 netmask 255.255.255.255 0
0
!---
!--- The next line translates the external address 216.30.79.135 to
!--- 172.16.128.135 for Web server in the dmz.
!---
static (dmz,outside) 216.30.79.135 172.16.128.135 netmask 255.255.255.255 0
0
!---
!--- The next line translates the external address 216.30.79.136 to
```

© SANS Institute 2005 Author retains full rights.

```
!--- 10.153.4.2 for the ntp and logging server in the internal network.
!---
static (inside,outside) 216.30.79.136 10.153.4.2 netmask 255.255.255.255 0 0
!---
!--- The next four lines assign what access lists are paired to what interface
!--- and whether the traffic is in or out.
!---
access-group outside_int in interface outside
access-group inside_int in interface inside
access-group dmz_int in interface dmz
access-group dmzvpn_int in interface dmzvpn
!---
route outside 0.0.0.0 0.0.0.0 216.30.79.129 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
http server enable
http 10.153.4.15 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh 10.153.4.0 255.255.255.0 inside
ssh timeout 60
console timeout 0
terminal width 80
Cryptochecksum:b6ef3df23fa7c4c26974dd2f6d1428d0
: end
```

© SANS Institute 2005, Author retains full rights.