Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst Practical Assignment
Version 4.0
By: Jeff Stoklosa
September 19, 2004

Table of Contents

Abstract

This paper includes three major sections that correspond to the assignments of the GIAC Certified Firewall Analyst Practical Assignment. The first section, Assignment 1, is a paper that addresses the use and future of Biometrics in the security field. The second section, Assignment 2, defines and explains the security architecture of a small company, GIAC Enterprises. The architecture includes access requirements and restrictions for all parties involved with the GIAC Enterprises business model. This section also includes an explanation of each security device and how it contributes to defense in depth. The last section, Assignment 3, provides and explains the rule base for the primary firewall in the GIAC Enterprises network. This section discusses the specific details such as rule base ordering and how the rule base reflects the security requirements laid forth in the security architecture.

The Future of Biometrics in Perimeter Security

This paper will discuss biometrics and the future role that this technology may play in the security industry. This paper will lay a foundation of what biometrics is, how the technology works, the advantages and disadvantages, and the future impact to the industry. Biometrics as a whole deals with authentication in multiple facets of life including banking, law enforcement, airports, military etc. This paper will specifically deal with biometrics as it deals with remote access, network perimeter security and the philosophy of defense in depth.

Biometrics is defined as automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are; face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. (1) Basic user authentication usually consists of three variables, something you have, something you know and something you are. By definition biometrics incorporates the last piece something you are.

Authentication is usually referred to as one factor, two factor or three factor dependent upon what types of authentication are implemented. The more variables that are combined in user authentication the tougher a system is to break. What you have refers to things such as a SecurID or some brand of token or access card. A user carries the token or access card and when prompted uses the code on it to authenticate. Secondly something you know refers to a password or pin that you create. This is the most common type of authentication but also has a great deal of flaws and no guarantee that the person using the username and password is actually who they say they are. Lastly something you are refers to biometrics and a feature of you. Strong user authentication should incorporate at least two factor authentication. For instance, a user may need a password and a fingerprint to be successfully authenticated into a domain.

To understand the process of how biometrics is incorporated in perimeter security the components should first be defined. The first part of the system is the human user who needs to be authenticated as being physically present at the site and time of authentication, a general-purpose computer running a general-purpose operating system, a biometric device sensor and a central database. (2) These four defined pieces of a biometric authentication solution are all reliant on each other to have high security standards. If one piece of the overall system is vulnerable to attack than the whole system could be compromised or brought down. For instance, a biometric solution would not be extremely beneficial to a company if the computers users are logging in on are vulnerable to known attacks. The network between the sensor and the central database should also be protected. If data sent across the network is not encrypted it could lead to various types of attacks. Strong encryption algorithms should also be implemented on the various parts of the biometric system to keep data confidential.

In a day and age where identity theft is such a concern database security will be of utmost importance. When a user adds his or her biometric information they need to be at ease as to who can access this data and that data is not being transferred to any other parties. If security flaws are found in the encryption techniques or in a particular element of the communication path it could very well cause a slow user acceptance. Many people are already very concerned when giving out certain personal information. Devices involved in biometrics now hold or pass information that is only unique to you. If this information was to slip into the wrong hands it could be detrimental to the user as well as the technology as a whole. The biometrics industry will need to gain large scale user and company acceptance that its devices and communication algorithms are not susceptible to attacks. One key to any remote access solution is that users feel comfortable with the solution a company has decided to roll out.

The technology of biometrics works in a similar fashion to regular user authentication to a remote access VPN device. The first step of the process is called enrollment. Each user must have a personal template created in the biometrics central database repository. This would be similar to a user profile in a standard remote access setup. The password would be replaced with the biometric information that is specific to each user.

Once each user has gone through the enrollment process the database must be configured on how to handle information that it processes. The database can be configured to either match and accept or reject. The database configuration will vary on an implementation-by-implementation basis because of the factors that must be considered. A strong security policy should incorporate the use and acceptance terms by the company and of any user accessing company property via biometric techniques.

The security policy should take into consideration false acceptance and false rejection. False acceptance occurs when a defined user template is matched by the central database when in fact it is not correct. Also referred to as the false matching rate or false acceptance rate, security administrators must define what an acceptable level of false positives is for the network in which they protect. On the other hand the false rejection rate or false non-matching rate measures the denials of valid users attempting to gain access. Security administrators need to evaluate which is more important to the environment they manage a higher degree of false acceptance rates and lower degree of false rejection rates or the opposite a higher degree of false rejection rates and low degree of false acceptance rates. This stance is a tough decision for security administrators because it may not be acceptable to let unauthorized users into your network because their biometric template matched to 80% of a valid user. On the other hand is it acceptable to have a valid user's profile not matched because the matching must be perfect between profiles? The first instance leads to unauthorized access while the second instance could lead to users not being

able to authenticate due to variables outside of their control. Administrators must way each option carefully for their unique environment. Security for remote access is the most important but if users are not accepting of the technology due to the fact that authentication fails on a regular basis the solution may not be in place very long.

After the enrollment process is complete and a policy regarding the different matching rates is defined the next step is user authentication or as it is called in the biometrics world “matching”. For authentication to occur each end user must have a biometric adapter. Two of the products on the market today that can be used include keyboards with a fingerprint sensor or fingerprint readers that plug into a standard USB adapter. Other equipment might include a microphone installed on a computer, a standard keyboard, or digital imaging products that can scan a hand or face. The security policy will also need to define what type of devices and methods a user can use to authenticate into the network. Various types of authentication techniques will be discussed in the next section.

User authentication or matching occurs when the template provided by the remote device matches to an acceptable level the template that was defined in the enrollment process for a particular user. As stated earlier an acceptable thresh-hold level needs to be defined so that valid users will be able to access the network at an acceptable rate while unauthorized users are denied privileges. (2)

This section will define and explain different types of biometrics. Since this paper’s main focus is on how biometrics effects network perimeter security and defense in depth only certain types and techniques will be covered. Biometrics can be categorized into two different types, physiological and behavioral. Physiological biometrics are based on measurements and data derived from direct measurement of a part of the human body. Fingerprint, iris-scan, retina-scan, hand geometry, and facial recognition are leading physiological biometrics. Behavioral characteristics are based on an action taken by a person. Behavioral biometrics, in turn, are based on measurements and data derived from an action, and indirectly measure characteristics of the human body. Voice recognition, keystroke-scan, and signature-scan are leading behavioral biometric technologies. One of the defining characteristics of a behavioral biometric is the incorporation of time as a metric – the measured behavior has a beginning, middle and end. (3)

The physiological biometric that may be used most often for remote access users and network perimeter security is fingerprint matching. Fingerprint matching is one of the least expensive types of physiological biometrics. Fingerprint matching also only requires a relatively simple piece of equipment versus a retina scanner or facial recognition equipment. Law enforcement

agencies have been using fingerprints for a long period of time and continue to do so today. Fingerprinting has been tested and used for many years giving validity to the statement that no two people have the identical fingerprint. A person's fingerprint is totally unique to them. It will never change, you cannot loose it or forget it and it can never be borrowed, lost or stolen. The business benefit is faster, easier, more secure access with auditable network logon. (4)

Some problems that arise with fingerprint matching are that fingerprints can be acquired or replicated to create a fake finger. Fingerprint molds have been made in the past that can match a system's acceptable threshold level enough for user privileges to be granted. A recent article in Information Weekly suggested that fingerprint biometrics would be more of a convenience logging in quickly to many sites on the Internet than a device that should be protecting financial and other private records. In the article Microsoft warns that the XP Fingerprint Reader shouldn't be trusted to secure access to corporate networks or to protect sensitive data, such as financial information. (5)

Other physiological biometric techniques that may be used are retinal scanners, face recognition devices and hand dimension scanners. It would not seem very likely in the near future that these techniques would be deployed in a wide scale for use with remote access and perimeter security. Device scanners for these techniques would be extremely expensive to deploy for each remote access user. Although there are some products on the line that are reasonably priced the quality of scanning is not the best. A biometrics system as stated earlier is really only as secure as its weakest link. Also with these types of techniques it is not as convenient as a finger print scanner. These technologies would need to be coupled with another growing area, single sign on identity. This would allow a user to only have to perform the scan one time versus every time a user would be challenged for authentication.

Behavioral characteristics that may be used in network perimeter security and defense in depth may include keystroke matching, voice recognition, or signature-scanning. Each of these matching techniques is based off of an action that a user would need to perform.

Keystroke dynamics is the process of analyzing the way a user types at a terminal by monitoring the keyboard inputs thousands of times per second in an attempt to identify user based habitual typing rhythm patterns. (6) This method evaluates certain patterns in your typing of passwords and other common key combinations. Do you type the identical way each type you enter your password? This could be one disadvantage of the technology. If a user does not keep the same keystroke pattern and rhythm each day to match a defined profile then they may encounter quite a few problems with login prompts. One advantage of this type of method is that it would be very inexpensive because the only piece of hardware is a keyboard that each user already owns. This technique may play a

future in perimeter security techniques if the keystroke algorithms are able to calculate keystroke rhythm at a very high success rate.

Voice recognition is a technique used to match a user template based on multiple characteristics of a human voice. This technology is also inexpensive compared to some of the other types of biometrics in regards to remote access security. Using a simple microphone connected to the computer users could easily incorporate voice recognition into the authentication process. One main disadvantage of voice recognition is that a person's voice may vary through time or even throughout the day. A common cold or sore throat could potentially cause problems with the recognition piece. Another security risk that would need to be taken into consideration would be a play back attack. If a recording was taken of a user's voice it may be able to be replayed into a system causing a false positive match and unauthorized access.

Lastly signature-scanning is another type of behavioral biometric. This method has two different options. The first option creates a user template based on a word/signature that is written by the user. Subsequent logins would require the user to sign the word/signature identically to the way it was done earlier. The other method of signature-scanning involves pattern matching not only on a single word but on all aspects of the signature. The aspects that may be taken into account are speed and pressure points with the word/signature. Signature-scanning has the same problem as voice recognition in that a user's signature needs to stay constant over a period of time. The other problem is forgery could occur. This would occur with more probability if the scanning system relied on a one-word match for authentication. One more drawback of this type of authentication is that a user's signature may evolve over time. Factors such as age or disabilities could cause a signature to become invalid. This type of method is probably geared more toward other industries than it is for remote access technologies.

The field of biometrics has the potential of a strong future in the security industry. It will be critical that the various techniques discussed earlier in this paper continue to be developed. As has been the case in the past if there is a flaw in any part of the authentication or communication path it is a matter of time before it is exploited. The technologies presented earlier will also only be able to flourish after a strong user acceptance for products is displayed. The sale and manufacturing of biometric devices has the potential to impact the security industry in a very positive way. As companies see money being spent on these types of products more research and development will occur.

Biometrics also has the potential to tighten perimeter security. Today where a single password can carry out user authentication in the future it might rely specifically on a biometric technique. It is extremely tough for administrators to enforce strong passwords or preventing users from insecurely storing them. The use of biometric techniques would require and enable a standard across all

users. Companies may also look forward to a cost reduction in the amount spent on password management and a standardized login. For instance, each user will need to have a fingerprint. Fingerprints cannot be lost, stolen or even forgotten as opposed to static passwords and PIN numbers.

It is extremely important in the present and future that biometric methods are not solely depended upon. Biometrics may become the industry standard but two or more factor authentication should still be used whenever possible. Using a mix of something you know, something you have and something you are is an extremely powerful way to strengthen perimeter security.

Bibliography

1. The Biometric Consortium, An Introduction to Biometrics, http://www.biometrics.org/html/introduction.html

2. Edgard Danielyan, The Lures of Biometrics, http://www.cisco.com/en/US/about/ac123/ac147/archived_issues/ipj_7-1/lures_of_biometrics.html

3. Simple Technology Inc., How is Biometrics Defined?, http://www.simpletechnology.com/News/biodefine.htm

4. Products, ISL-Biometrics, http://www.isl-biometrics.com/products.htm

5. Alex Veiga, Fingerprinting XP, 2004 http://www.informationweek.com/story/showArticle.jhtml?articleID=47101918

6. Fabian Morose and Aviel Rubin, Keystroke Dynamics as a Biometric for Authentication, http://avirubin.com/fgcs.pdf

GIAC Enterprises

GIAC Enterprises, referenced as GIAC throughout the rest of the paper, is a small company of 50 employees that is focused on selling its world-class fortune cookie sayings worldwide. The network design is based on security and scalability for the anticipated growth of the company over the next 5 years. The company currently has both 2 remote offices

Currently GIAC does not have a standard or a preference of freeware product versus purchased fully supported products. When making decisions on which product to purchase GIAC will evaluate the total cost of ownership but more importantly GIAC is concerned with the functionality of the product and whether or not it meets or exceeds all of the defined requirements.

Business Interaction

GIAC has multiple units that are involved in its overall business structure. The following section defines each unit and the access that will be granted based on requirements. The appropriate access to each unit is a key to the overall success of the company and a secure GIAC network. The security architecture defines what each unit will be able to access within GIAC as well as to and from the Internet.

Customers

Customers have the ability to access their account online, make payments, and order more supplies. Customers access the public webpage as the general public does over HTTP, port 80. Customers can then click on the "Customers" link that will take them via HTTPS port 443 to the secured Customer Database located on server in the Customer Services VLAN. Customers are also able to contact GIAC via email.

Source	Destination	Port
Any	97.0.0.20 (Public Web Server)	80
Any	97.0.0.19 (SMTP Relay Server)	25

Suppliers

Suppliers are based around the world. GIAC maintains business with 4 main suppliers. 2 suppliers are within the US and 2 are located in the Far East. GIAC Enterprises supports both English and Chinese fortune sayings. Each supplier must have a perimeter device that can terminate a site to site VPN connection. A VPN connection will be established from these organizations networks to the appropriate Suppliers Databases in the Supplier/Partner VLAN within the GIAC Enterprise datacenter. Suppliers will have HTTP, HTTPS and FTP access to the Partners/Suppliers Database server.

Source	Destination	Port
VPN Site to Site GW	192.168.1.6	80, 443, 21

Partners

GIAC Enterprises has a number of partners inside and outside of the United States in various countries. Partners translate the Chinese or English on GIAC Enterprises to the appropriate language.

Partners also access GIAC Enterprises via VPN. Due to the high cost of a frame relay circuit a VPN solution has been put into place. Partners will be allowed HTTP, HTTPS as well as FTP access to pull large amounts of Fortune Cookie sayings for translation from the Partners/Suppliers Database server.

Source	Destination	Port
VPN Site to Site GW	192.168.1.6	80, 443, 21

Employees

Employees will have access to the Internet via a proxy server. Employee's access to the data center servers will be restricted. Employees will have HTTP, HTTPS, FTP, SMTP, DNS port access to the respective server in the datacenter. An SMTP mail relay for outgoing and incoming mail will be used. A proxy will be put into place for web traffic.

Source	Destination	Port
172.16.0.0/23	97.0.0.22	80
172.16.0.0/23	97.0.0.18	53
172.16.0.0/23	192.168.0.2	25
172.16.0.0/23	192.168.0.5	53
172.16.0.0/23	192.168.0.6	http, https, ftp

Remote Offices

GIAC employees locate in the remote offices will be granted the same access as employees on the local LAN. Access will come through a site-to-site VPN that will terminate on the firewall.

Mobile Sales Team

The mobile sales team will use the Cisco remote access solution and have the same access as an Employee who is on the local LAN. A Cisco VPN profile will be distributed to each of the sales team that may need VPN access.

General Public

The general public will be able to access the public web server via HTTP port 80. The web server will give company information. To generate business people there is a daily fortune saying as well as the ability to sign up for a free email fortune each day. The general public will also be able to contact GIAC through email correspondence.

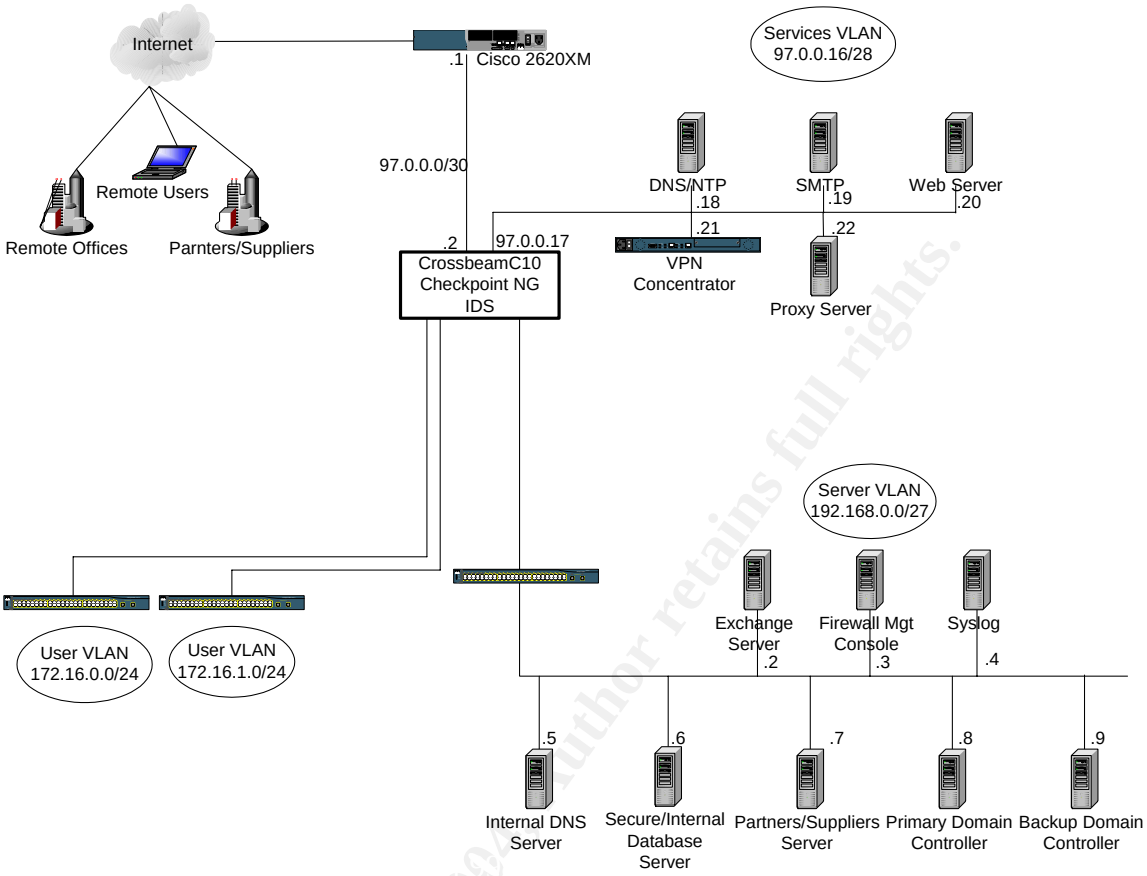
Source	Destination	Port
Any	97.0.0.20 (Public Web Server)	80
Any	97.0.0.19 (SMTP Relay Server)	25

IP Addressing Scheme

GIAC's ISP has assigned them the 97.0.0.0/24 of public address space. GIAC will implement a /30 between the ISP router and GIAC's border router. Aggregates of the 192.168.0.0/16 RFC 1918 Private space will be used for Infrastructure IP addresses and aggregates of the172.16.0.0/12 space will be used for Employees desktop assignments. The 10.0.0.0/8 private space is currently not being used by GIAC and will be filtered on the egress router accordingly. One concern for GIAC is for addresses to be easily summarized for routing purposes, especially as the company grows.

There are a couple of important reasons for using public and private address space appropriately. Public address space is at a premium in terms of availability as well as monetarily. It is extremely important to address only publicly accessible devices on the GIAC network with publicly routed IP space. This will ensure another layer of security is added into the GIAC network. If all devices had a public IP address then access lists and ACLs are the primary control point to keep unauthorized access from the internet to these hosts. Since GIAC is using private non routable RFC 1918 space for internal devices it is more difficult to gain access to these networks from the outside world. Additionally the use of private address space and no ip source routing on the border router can add a layer of defense to the network.

GIAC Network Diagram



Defense in Depth

Defense in Depth is a key theme the GIAC security architecture. The following section will list each device, its placement and its role in the defense in depth design. The GIAC network is comprised of a border router, a primary firewall, an IDS, a VPN device, and a proxy server. Other servers that exist on the public services network or the private network are also listed with the function they perform and the techniques that GIAC has used to increase the security of each box.

Border Router

The first piece of the defense in depth architecture is the border router that connects the GIAC Enterprises to the internet. GIAC Enterprises has decided to go with a Cisco 2620XM series router running the latest version of IOS, 12.3. Cisco was chosen in part due to its dominance on the internet and the staff level of knowledge about the Cisco platforms.

As part of the first and last line of defense the border router will be used in an effective way to mitigate unnecessary traffic. First the border router will

function as a static filtering router. Static filtering is not the ideal in all situations but since this is the first line of defense it will be sufficient. Static filtering will allow GIAC Enterprises to filter spoofed addresses such as the RFC 1918 space from ever entering or leaving the network. Standard and Extended Access control lists on the border router are not extremely CPU intensive and help to mitigate what is hitting the firewall behind it.

One of the first things that will be addressed on the border router is anti-spoofing. We will be filtering the 192.168.0.0, 172.16.0.0 and the 10.0.0.0 RFC 1918 address space from passing into or out of our network. GIAC Enterprises will also be filtering its own 97.0.0.0/24 public space on the ingress to avoid spoofing of its own network.
GIAC Enterprises will also use access control lists on the border router to block common vulnerable ports inbound and outbound. For example, some services that will be blocked are tcp 135-139 and 445. GIAC Enterprises will also be block tftp (udp 69), snmp (udp 161), snmp-trap (udp 162) and syslog (udp 514). By filtering these additional ports it will add an additional layer of security no longer relying only on the firewall to block this traffic. In the future if any of these ports need to be opened GIAC Enterprises will suggest that it is tunneled through SSH or an IPSec VPN be used. (1)

GIAC Enterprises will not filter the IANA unassigned address space. GIAC Enterprises will accept the risk associated with spoofing these addresses due to the administrative overhead of keeping the unassigned list up to date. Since GIAC Enterprises relies on the web for all of its business black holing newly address blocks may have a negative impact to the business.

Management access to the firewall will also be restricted via access lists. Access to the router via telnet will also be limited to the employee network addresses by ACLs. SNMP access to the router will also be limited through the use of access-lists. The community string should be changed to a password that is not “public”.

GIAC Enterprises will also use other best security practices such as disabling ip-source routing, TCP and UDP small server (disabled by default in IOS 12.3), http server, bootp server and finger services. GIAC will also disable at the interface level ip directed-broadcasts, ip unreachables and cdp. GIAC will enable service password-encryption which allows the password to be encrypted in the configuration.

A warning banner will be placed on the border router. The banner motd command will be used to clearly state that unauthorized access is prohibited and is subject to the terms and agreements in the GIAC Enterprises acceptable use policy.
(2)

GIAC Enterprises will be monitoring the border router via the Syslog server in the datacenter. The logging 192.168.0.4 command will be used to send any log information to the Syslog server. A loopback interface will be used on the border router that will be used for Syslog and other management traffic. Lastly, GIAC Enterprises will also ensure that each unused port on the router is administratively turned down.

Firewall Device

GIAC has chosen the Crossbeam C10 appliance running Checkpoint AI R55. The C10 was chosen due to the high performance, administrator familiarity with Checkpoint and total cost of management. The C10 appliance will also incorporate the IDS solution on a single platform. This may not be an ideal solution for security in depth but GIAC is accepting the risk due to lower operational and administrative costs.

The C10 appliance will be placed between the border router and the GIAC network and is viewed as the main access control point. It will have one interface connecting to the public services network, the internal services network, the user VLAN and the border router pointing out to the internet. The firewall will be placed in the network in this fashion to prevent malicious activity from compromising multiple segments of the network.

In the GIAC network the firewall is considered the second line of defense from the internet. All traffic entering that passes the ACLs on the border router or leaving the network will hit the firewall. GIAC will implement the same basic filtering from the internet giving the company a multiple vendor solution that follows best security practices so an exploit in Cisco should not adversely affect the firewall. The firewall will perform stateful packet filtering. Stateful packet filtering is much more robust and flexible in terms of management than the static filtering on the border router.

All traffic originating from the internet must pass through this firewall and terminate on the public services network. The firewall will block any traffic from the internet that is trying to directly access services or devices on the user VLAN or internal services network. Access from the public services network to an internal network will be specifically defined by source, destination and port in the firewall rule base.

Internal users must also pass through the firewall to access the private services network, the public services network or the internet through the proxy. This network will have access to servers and services on each network as defined in the firewall rule base.

A routing protocol will not be run on the firewall. A routing protocol has the potential to cause high CPU utilization on the firewall. The firewall will have a

default route pointing to the connected interface of the border router and more specific routes for the internal networks and public services network.

The firewall will also be responsible for the site-to-site VPNs that connect the headquarters office to the 4 remote locations and partners. Checkpoint software will be configured to terminate a VPN tunnel from the firewall to a device located in the remote location. Traffic that traverses this tunnel is encrypted to ensure integrity between GIAC and its partner. GIAC employees in the 4 remote offices will have the same access as those employees on the local LAN. Access for the partners and suppliers will be restricted by rules on the primary firewall. Allowing the VPN tunnel to terminate on the firewall adds some processing to the firewall but more importantly it adds another layer of security compared to the terminating the VPN tunnel on the border router.

IDS Device

As stated earlier in the Firewall Device section GIAC will be implementing the IDS solution on the Crossbeam C10 appliance. The C10 appliance has the ability to implement an IDS that monitors data on both sides of the firewall, meaning traffic before it hits the firewall as well as traffic that has passed through the firewall. Since GIAC is a small company with limited man power it has made the decision to implement the IDS sensor only on traffic that is passed by the firewall. Monitoring all traffic that hits the firewall is an extremely extensive task and one that GIAC being a small company will not be able to handle. GIAC is willing to accept the risk based on the defense in depth theory. With the Crossbeam device a shadow port is configured for traffic that crosses the interfaces for the public services network and private services network. The Crossbeam appliance allows for the high throughput with a shadow port of a max 700Mbps. With the Crossbeam device these multiple physical segments can be combined into one IDS sensor easing manageability as well as lowering costs. GIAC has decided that monitoring the public services network and the private services network is the most critical. The placement of this shadow port also allows GIAC to check if certain malicious traffic is getting passed by the firewall. With the IDS monitoring the traffic in this location it is adding yet another layer of defense in the critical segments of the GIAC network.

GIAC has chosen RealSecure ISS version 7.0 as its solution for IDS. RealSecure is a static IDS system that is easy to use and can be incorporated with the Black Ice personal firewall in the future. Currently GIAC has decided not to implement personal firewalls on user's machines due again to cost restraints and manpower. RealSecure is deployed within GIAC using its network based IDS. This system will be able to monitor packets on the wire searching and alerting on signature files that it may find. Since GIAC is limited on resources another advantage of RealSecure is its central manageability. One drawback of any IDS is the amount of false positives that occur. False positives are extremely troublesome because it uses valuable resource time to troubleshoot what

appears to be a network event. To eliminate the time and cost associated with false positives GIAC should try verifying each detect before assuming it is a valid attack. (3)

With the presence of an IDS GIAC will present a clear network usage policy to be sure that each user is aware of their expectation level of privacy. A network usage policy is a key document that may help to protect GIAC in the future.

Public Services Network Devices

This section will define each of the components that are located on what GIAC defines as the public services network. The simplest characteristic of these devices is that each one is accessible from the internet. By hardening each of these devices it adds another layer of security to the overall GIAC security posture.

VPN Device

GIAC has decided to implement a Cisco 3005 VPN Concentrator for remote access users. The Cisco VPN 3005 Concentrator was chosen due to its ease of manageability as well as cost effectiveness. The 3005 VPN concentrator provides the ability for 200 simultaneous IPSec connections and 100 LAN-to-LAN connections. The 3005 model is designed for bandwidth requirements up to a T1/E1 (4Mbps maximum performance). Though the 3005 model is not be field upgradeable to the 3030 or 3060 models as the 3015 model, it is half the cost and will provide GIAC with a solution for the next few years based on projected growth.

Security features (4):

- Full support of current and emerging security standards allows for integration of external authentication systems and interoperability with third-party products.
- Firewall capabilities through stateless packet filtering and address translation to ensure the required security of a corporate LAN.
- User and group level management offers maximum flexibility. WebVPN offers granular access control per group and detailed logging information.

This device will be placed in the public services network. Users that access the network through the Cisco VPN concentrator have the same privileges that they have on the local LAN through the use of user groups.

Users will be able to access the VPN Concentrator from any address on the internet. A 32 character pre-shared key will be used for IKE phase 1. When the 32 character pre-shared key is accepted the user will be challenged to authenticate using their Windows 2000 username and password. This authentication has some risk involved but administration of SecureID tokens is not possible with the limited resources. A strong password policy will be

incorporated for Windows 2000 user passwords. The passwords for each user must be “strong”. A password will need to be a minimum of 8 characters long and contain at least one of each of the following: an uppercase letter, a lowercase letter, a number and a special character. Passwords should also not be words that can be found in a dictionary nor words that have a few letters changed to numbers making them susceptible to brute force attacks. Users will also need to change their password every 60 days. A password policy document for GIAC further defines this policy and will be distributed to each employee.

Public/Private DNS Servers

GIAC will be using a split DNS model using a Solaris V120 server running Bind 9 for external DNS resolution. A separate Solaris V120 server, located on the internal services network, will be responsible for internal DNS resolution. Split DNS on the GIAC network is another valuable attribute to the defense in depth architecture. GIAC will take precautions necessary to lock down these DNS servers. Two main security points to consider with a DNS box are zone transfers and recursion. In the GIAC network since there is no secondary DNS server no zone transfers will be allowed from the master DNS server. Zone transfers are a quick and easy way to map a network. Secondly, recursion will be turned off for users from the internet but will be allowed for GIAC networks, a feature in Bind 8 and higher (5). Recursion allows the DNS server to do the work for a client if it does not know the answer to a query. Recursion can be very processor intensive if internet users find that the DNS server is recursive and use it for lookups.

Web Server

The web server will also be run on its own independent server. Apache web server has been chosen by GIAC running on a Compaq DL 360 with 1 Gig of RAM. The OS, Linux 9.0 of this system should continue to be patched so that no other security flaws will be able to mitigate the Apache web server. GIAC implements various tactics to lock down the Apache server. First the httpd process should be running as the nobody user rather than root. (6) GIAC also only permits the root account to have write permissions on this box. Lastly GIAC has determined it important to change the Apache banner so that this information cannot be used in against them. Removing this information is just one more simple way to help mitigate the risk of a security event as well as adding to the layers of security.

Sendmail Server

GIAC has also chosen to implement a mail relay server on its public services network. This server will be running sendmail on Compaq DL 360 with 1 Gig of RAM. All email to GIAC from the internet and from GIAC to the internet must pass through this mail relay server. Sendmail will be using the latest version

which is 8.13.1 running on a Linux 9.0 platform. It will be critical for GIAC administrators to continue to keep this box updated with fixes and patches to the Sendmail software as it becomes available. One main concern about the mail relay server is outbound mail headers that may give valuable company information away. GIAC has configured its sendmail relay server to strip outbound headers. (7) This is again a simple way to minimize information that the public is able to attain about the GIAC network.

Squid Proxy

GIAC will run a Squid proxy server, version 2.5 on a Linux 9.0 server, which will handle traffic from the user VLAN out to the internet. The hardware for this box will be the GIAC standard Compaq DL 360 with 1 Gig of RAM. A Squid proxy has excellent caching capabilities for quick user access reducing load on the web server and DNS lookups. At this stage GIAC will implement this as an outgoing proxy. In the future it may be used to proxy incoming connections to the public web server. Squid has a lot of functionality which includes user authentication and access control lists for specific networks. GIAC will only allow its user VLAN connectivity to the Squid proxy server when trying to reach the Internet. The Squid proxy server will strengthen GIAC's security posture by adding another layer between the user desktop and the outside world. From the outside world web connections from the GIAC network will be seen as coming from one source address, therefore mitigating risk of vulnerabilities for GIAC users.

NTP Server

GIAC has decided to implement NTP on its DNS box to mitigate cost since the server is nowhere near its performance limits. GIAC is willingly accepting the risk of having multiple services running on the same box. Multiple services mean more vulnerabilities and more ports to work with on a single server. GIAC uses NTP to synchronize time throughout its network. Two publicly accessible stratum 2 servers will be pointed to for use by the GIAC NTP server. The use of NTP will aid GIAC administrators when they are investigating logs or incidents by giving synchronized time on each device. Synchronized time and logs is essential to troubleshooting problems and evaluating events.

Internal Network

Syslog Server

GIAC has also decided to implement a syslog server on its internal network. This server will be a Compaq DL 360 with 1 Gig of RAM. Devices in the GIAC network will be configured to send logging traffic to the syslog server via port 514. A syslog server allows GIAC the ability to store its log details in a single

repository. This will aid troubleshooting as it allows administrators easy access to view logs from multiple devices quickly and efficiently.

FW Management Console

The Checkpoint firewall management console will run on a Sun V120 server with 1 Gig of RAM. The OS will be a hardened Solaris 9.0 build. To secure this box further only those employees with FW administration rights will be able to access it. The use of management IP function will be used within the Checkpoint software which will only allow defined GUI management clients access. Each admin will have a defined static address for this purpose.

User desktops

At this point in time a personal firewall is not supported by the GIAC team. Black Ice will be evaluated in the future due to its compatibility with the RealSecure IDS product. User desktops must have a defined SOE, standard operating environment, image running on their workstations. Each machine will be monitored and patched for all updates when it logs into the domain each day. This will ensure that GIAC hosts are patched and not susceptible to know security risks.

Bibliography

1. Chris Brenton, Packet filters, 2004, (Module 5)
2. http://www.quepublishing.com/articles/article.asp?p=102180&seqNum=5
3. Chris Brenton, Defense in Depth, 2004, (Module 2 ISS RealSecure)
4. http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_data_sheet09186a00801d3b56.html
5. Chris Brenton, Defense in Depth, 2004, (Module 2 DNS)
6. Chris Brenton, Defense in Depth, 2004, (Module 2 Locking Down Apache)
7. Chris Brenton, Defense in Depth, 2004, (Module 2 Sendmail)

GIAC Primary Firewall Rule Base Design

This section will explain GIAC's philosophy for creating and maintaining the primary firewall rule base. This section will also explain each rules purpose and placement within the rule base.

GIAC took into consideration multiple factors when it designed the primary firewall rule base. The rule base is based on the network map and the requirements set forth in the security policy and connectivity matrix. The main considerations that GIAC took into consideration were:

1. The GIAC rule base is based on a "deny all" that is not specifically defined.
2. Rule base order is extremely important and must be taken into consideration.
3. Each rule is evaluated for its need and verification that it does not circumvent other rules. Rules will be continued to be audited for there need.

As part of the rule base if services are not specifically defined then the service will be denied. This allows GIAC strict access to know what services should be accessing the network. This mentality allows a strengthened security presence on primary firewall. The downside to this type of design is it can leads to more administration of the firewall. For instance, if requirements are not specifically defined by application owners or if they are incorrect traffic will be dropped. GIAC is willing to accept the disadvantage of more administration since it leads to a much stronger primary rule base.

Proper rule base order is critical to the success of the primary firewall for both security and performance. Checkpoint firewalls are stateful firewalls that process rules sequentially. Once a match is made for the specified traffic it is either accepted or denied. For this reason specific rules need to be placed before general rules for the same type of traffic. For example, GIAC wants to filter traffic out from the banned malicious IP addresses. The rule for denying the traffic should be placed in front of the rule that allows all Internet traffic to the GIAC web server. Rule base ordering is also very critical to the performance of the firewall. Rules that are commonly matched should be placed at the top of the rule base above those which have very few hits. A proper rule base order will allow the GIAC firewall to process packets faster if frequently matched rules are first. It would not be beneficial for the firewall to search through a long list of rules when common traffic is either passed or denied by the firewall.

The GIAC team will continue to audit the firewall rule base for its validity and effectiveness. As the rule base continues to grow GIAC will continue to evaluate each new rule. Newly defined rules should not compromise any previous rule. It is also important that the firewall administrators work with application owners to specify communication paths between devices. A properly defined

communication path does not leave unneeded ports and protocols open to be exploited. It will be a standard also that each time a rule base change is made that the administrator marks in the comments his/her comments and what change request the change is associated with. The GIAC team should continually evaluate rules so that unneeded rules can be removed from the rule base, improving security and performance.

Rule base explanation

Before the defined firewall rules are processed there are implied rules that are processed. The Implied rules are managed under the Global Properties section. Most of the communication in the implied rules has to do with the management traffic. Also defined in the implied rules is to deny ICMP packets both to the firewall and through the firewall. An encryption rule is also automatically created when configuring site to site VPN communities.

FW Administration Rules (Rules 1-3)									
1	FW_Admins	Primary-FW	Any Traffic	TCP SSH icmp-proto	accept	Log	Primary-FW	Any	Admin access to Firewall- js- CR 17
2	FW_Admins	FW_Management_192.168.0.3	Any Traffic	Any	accept	Log	Primary-FW	Any	Admin access to Firewall Management Console- js- CR 17
3	Any	Primary-FW	Any Traffic	Any	drop	Log	Primary-FW	Any	Stealth Rule to drop traffic destined for firewall- js- CR 17

Rules one and two allow access directly to the firewall and Checkpoint management console for management purposes. Access to these devices is restricted to the statically defined source IP addresses of the firewall administrators. These services are critical to manage the box. The third rule is a stealth rule that will drop any traffic destined to the firewall or the firewall management console not defined in the first two rules. This rule is placed after the first two rules because it is a more general deny rule. Rules one and two are placed at the top of the rule base so that they are never compromised by another rule.

Internet to Public Services Network (Rules 4-8)									
4	Top_10_banned_IPs	Public_Services_Net	Any Traffic	Any	drop	None	Primary-FW	Any	Drop all traffic from the SANS top 10 IPs- js- CR 17
5	Any	Public_Web_Server_97.0.0.20	Any Traffic	TCP http TCP https	accept	Log	Primary-FW	Any	Internet to Web server- js- CR 17
6	Any	Public_DNS_NTP_97.0.0.18	Any Traffic	dns	accept	None	Primary-FW	Any	Internet to DNS Server- js- CR 17
7	Any	Mail_Relay_97.0.0.19	Any Traffic	TCP smtp	accept	None	Primary-FW	Any	Internet to Mail Relay Server- js- CR 17
8	Any	VPN_Concentrator_97.0.0.21	Any Traffic	IPSEC	accept	Log	Primary-FW	Any	Internet to Remote Access VPN- js- CR 17

The next group of rules define access from the internet to the public services network. Rule four is a specific rule that drops any traffic from a banned list of the 10 top ten most malicious IPs. This rule is implemented before allowing all other specified access into the public services network. Rules five, six and seven permit any public IP, except those dropped by rule four, to access various servers on the defined port. These rules are placed at the top of the rule base because customer satisfaction is a main concern for GIAC. Since all of GIAC's

business transactions are performed over the internet it is extremely important to increase performance.

Rule eight defines remote user VPN access from the internet. This rule allows any IP address access to the VPN concentrator for authentication purposes. It is not the most secure rule since it allows any access to the VPN concentrator but the defense in depth including patch management and strong password authentication lessen the degree of risk.

Giac destined Internet traffic (Rules 9-11)									
9	Public_DNS_NTP_97.0.0.18	* Any	Any Traffic	ntp dns	accept	None	Primary-FW	* Any	Allow DNS/NTP server out internet- js- CR 17
10	User_Net_172.16.0.0	Web_Proxy_97.0.0.22	Any Traffic	TCP http TCP https	accept	Log	Primary-FW	* Any	Allow users to web proxy- js- CR17
11	Web_Proxy_97.0.0.22	* Any	Any Traffic	TCP https TCP http dns	accept	Log	Primary-FW	* Any	Allow web proxy out to the internet- js- CR 17

Rule nine allows the DNS/NTP server access to the internet to perform its proper functions. This rule is placed relatively high in the rule base because of its frequent traffic. Rule ten defines access from the user VLAN to the internet. All user traffic to the internet must go through the defined proxy server. Rule eleven defines access to the internet for the web proxy. This rule allows the proxy server to access any http or https site as well as perform DNS lookups.

User VLAN to Private Services Network (Rules 12-15)									
12	User_Net_172.16.0.0 Remote_Office_GWs Remote_Access_Users_Net	PDC_192.168.0.8 BDC_192.168.0.9	Any Traffic	NBT	accept	None	Primary-FW	* Any	Allow Windows domain traffic from users to the PDC and BDC- js- CR 17
13	User_Net_172.16.0.0 Remote_Office_GWs Remote_Access_Users_Net	Internal_DNS_192.168.0.5	Any Traffic	dns	accept	None	Primary-FW	* Any	Allow users to query the Internal DNS server- js- CR 17
14	User_Net_172.16.0.0 Remote_Office_GWs Remote_Access_Users_Net	Internal_Mail_Server_192.168.0.2	Any Traffic	TCP smtp	accept	None	Primary-FW	* Any	Allow users to internal mail server- js- CR 17
15	User_Net_172.16.0.0 Remote_Office_GWs Remote_Access_Users_Net	Giac_DB_192.168.0.6 Giac_Partners_DB_192.168.0.7	Any Traffic	TCP http TCP https TCP ftp TCP SSH	accept	Log	Primary-FW	* Any	Allow user access to the database servers- js- CR 17

Rules twelve, thirteen, fourteen and fifteen allow specific traffic sourcing from the user VLAN, the site to site VPN remote office and the remote access VPN user IPs specified access to the private service network. The source addresses are defined this way because in the security policy it is defined that GIAC employees in remote offices and remote access VPN users should have the same privileges as those employees on the local network.

Partner/Supplier Site to Site VPN Rules (Rule 16)									
16	Partner_1 Partner_2 Partner_3 Partner_4 Supplier_1 Supplier_2	Giac_Partners_DB_192.168.0.7	Any Traffic	TCP ftp TCP http TCP https	accept	Log	Primary-FW	* Any	Allows partners/suppliers to their database throgh VPN tunnel- js- CR17

Rule sixteen defines the partners and suppliers access to the Partners/Suppliers database which is located on the private services network. Checkpoint automatically creates a VPN rule which is by default hidden from the view in the rule base. The automatically created VPN rule is based on the

properties that are defined in the VPN community. The rule above states any traffic from the defined VPN gateway members and the network it protects to the GIAC gateway is encrypted and then sent to the rule base for proper processing. The rule base will then decide if the traffic should be accepted or rejected.

Public Services Network to Private Services Network (Rules 17-18)									
17	Mail_Relay_97.0.0.19 Internal_Mail_Server_192.168.0.2	Internal_Mail_Server_192.168.0.2 Mail_Relay_97.0.0.19	Any Traffic	TCP smtp	accept	None	Primary-FW	Any	Allow communication between internal mail server and mail relay server- js- CR 17
18	Router_97.0.0.1 Public_Web_Server_97.0.0.20 Public_DNS_NTP_97.0.0.18 VPN_Concentrator_97.0.0.21 Mail_Relay_97.0.0.19	Syslog_Server_192.168.0.4	Any Traffic	UDP syslog	accept	Log	Primary-FW	Any	Allow device to send syslog traffic- js- CR 17

Rule seventeen allows the internal Exchange mail server to communicate with the mail relay server and vice versus. The next rule defines access between the public services network and the private services network. Rule eighteen is specific for syslog traffic destined for the syslog server.

Private Service Network to Public Services Network (Rule 19)									
19	Private_Services_Net_192.168.0.0	Public_DNS_NTP_97.0.0.18	Any Traffic	ntp	accept	None	Primary-FW	Any	Allow servers on Private services network NTP access- js- CR 17

Rule nineteen permits NTP traffic from the private services network to the DNS/NTP server on the public services network. This rule is located toward the bottom of the rule base because of priority and because the configuration of the polling intervals for devices will be set to a high value.

Drop Any Cleanup Rule (Rule 20)									
20	Any	Any	Any Traffic	Any	drop	Log	Primary-FW	Any	Deny All Rule- js- CR 17

Rule twenty represents a catch all drop any rule. Any traffic that does not match a rule will get dropped and logged by this rule. This rule is important because it supports GIAC's stance of denying all but specified traffic. It is also important to log this rule so that GIAC firewall administrators have an idea of what traffic is getting to but being dropped by the firewall. The log information can allow corrective action to be taken if needed to strengthen the defense in depth model.