Global Information Assurance Certification Paper

GSLC Security Leadership Certification
Practical Assignment - Version 2.0

Submitted: Jo-Ann Abbott
Title: Manager, Security
Date Submitted: March 7, 2005

Table of Contents

GSLC Abstract

This paper has been written to fulfill the practical assignment which is one requirement to obtain GIAC Security Leadership Certification. This practical consists of a review and critique of a GCFW Network Design. The design chosen is a design submitted by Jared McLaren on April 25, 2004. This submission consists of four separate components and is detailed with the following key sections Security Architecture, Security Policy, Design under Fire and Verifying the Firewall Policy. For this exercise, this review will focus on the Security Architecture and Security Policy components. This review will not include the Design under Fire component as it is not directly related to the network submission being critiqued. It has been reviewed and given it significant consideration, in order to provide a better understanding of Jared's knowledge level, in relation to security concerns and requirements that are relative in the industry today.

Executive Summary

The first requirement for GIAC's network design is to accommodate the employee base, the majority of which work out of the head office in Iowa. Approximately 25 percent work remotely and have a significant travel commitment to the company. This requirement is handled very well by this design, with the router being the only point of entry/exit to the Internet. Positioning the firewall behind the router offers a central point in which to focus the security effort, mainly accomplished by utilizing the firewall's filtering capabilities. The strategic placement of the firewall ensures all ingoing and outgoing traffic must pass through the firewall. Moreover, the access list design controls all access by IP address, ensuring the design can provide secured server access for all employees, which includes those entering through the local network and those connecting remotely through the Internet.

Another requirement is to provide a secure method of transferring files from the partner company and other users who provision fortune cookie sayings, to GIACS database server. While the users and the third-party companies only have a requirement to transmit and store files securely, the partner company also has a requirement to retrieve files from the server, those that require written translation. This design fulfills this requirement with the use of SSH and further enhances security by using the access lists to prevent access unless a rule has been specifically coded to allow it. This approach will also prevent administrators from inadvertently providing more access than is required.

The design limits the potential for scalability, by recommending lower-end server solutions without excess capacity and open source code which may not be compatible with future requirements. The recommendations listed in the Improvement section will enhance the design by addressing this issue and adding the ability to expand and accommodate the future growth that is

anticipated with the investment of the partner. The partnership was formed to enable written translations in Spanish, French, German and Italian thus providing an immediate opportunity for expansion into the international market for GIAC. Therefore, the initial design must be one that can easily scale to accommodate this growth.

The last requirement results from the initiative to move the company in the "direction of the future" by utilizing online order processing. Along with the requirement of expanding the market base, this requires that particular attention be given to some additional mitigating factors, which can have a direct impact on the company's bottom line and the ability to serve its customers. One of the most critical factors is the ability to place orders and complete financial transactions in a reliable, secure manner over the Internet. The second most critical factor is availability – as the market area expands across time zones, consideration must given to the increased demand for availability. The biggest concern with this design is the limitations incorporated by lack of redundancy which can severely jeopardize network availability and, in this case, the company's future. Although the designer recognized this as a key factor and at different points stated this requirement, it was not included in the design. The improvements suggested here to provide adequate redundancy will improve the availability of this network. Although not providing a fully redundant environment, the main requirements would be satisfied and further redundancy can be built in as the market area grows.

It is also worth noting that competing in the international market may bring many different considerations and/or business requirements from a technical aspect. As such, a separate in-depth review should be completed to ensure gaps and differences are identified. Considerations in the review should encompass the technical aspects of dealing in an international market such as the specific requirements relating to the financial aspect, as well as legal and business requirements. Also items such as availability, grade of service, delivery of product must be maintained in this market area, as it is locally, without compromising security in the process.

These challenges are not unique in our market today. However, careful consideration must be given to all requirements, starting at the design phase and carrying through to the production and/or run state. Each piece of this design will require extensive testing to ensure the infrastructure can perform the role, protect the information and assets of GIAC, as well as lead itself well for scalability without a costly redesign.

Technical Solution:

1.0 Proposed Infrastructure Components

The proposed infrastructure consists of a Border Router, a multi-interfaced firewall, two remote access solutions, a distributed network based Intrusion Detection System and an IP addressing scheme. The architectural design was submitted by Jared McLaren on April 25, 2004 and can be viewed at the following URL: http://www.giac.org/practical/GCFW/Jared_McLaren_GCFW.pdf .

1.1 Border Router

The developer's solution consists of installing a CISCO 3725 running IOS 12.2 with IP Plus IPSEC 3DES feature set as the border router. The feature set is required to create a 3DES VPN connection for the partner network. The router is connected to a T3 connection with 6mb of bandwidth through the routers high-speed serial interface and will be the only entry/exit point to GIAC's network.

This particular router was chosen by the developer in consideration of the availability requirement. Network availability is an important factor to this company's success, as a directive was underway to promote sales through the online ordering process. Therefore, the developer opted to invest the capital required to provide a router solution that would offer adequate reliability for the connection to the partner company, and one that had enough capacity to provide some basic filtering.

As mentioned above, this router is intended to serve two purposes. First, it will enable a secured VPN connection to the MetaLingual network, the partner company who provides written translations for the Fortune Cookie Sayings. Second, it will provide some initial packet filtering to provide an initial clean up of known "bad" traffic both entering and leaving GIAC's network, and to establish a layer of the defense-in-depth strategy. The developer feels this solution mitigates a known weakness in this router, its filtering ability and also gave consideration to the CPU intensive nature of both the VPN connection and in-depth packet filtering. He is confident this router has sufficient capacity to handle both the VPN connection and the basic Ingress (incoming) and Egress (outgoing) packet filtering, moving the more in-depth filtering to the firewall.

1.1.0 Configuration:

The Border router's configuration file establishes the following settings: SSH, VPN, IPSEC, etc. The router name is set, password encryption is

defined as MD5 hash, services not required are locked down, logging is set and individual access lists establishing access into and out of the network are defined. There are four access lists set up in this configuration: the first one limits access to SSH, the second list defines inbound access (the main ingress filter) on the high speed serial interface as well as blocking some ports to ensure certain traffic not enter the network. The third list begins the egress filtering on the high speed Ethernet port and also blocks the same ports that were blocked inbound, while the fourth access list defines the two hosts that will be communicating in the VPN tunnel between GIAC's high-speed serial interface and the partner company's designated IP address. The configuration file is completed with some console login settings and the NTP timeserver is enabled and defined on the network.

1.2 Multi-Interfaced Firewall

Traffic traversing the network from the router will be passed to a firewall, which consists of four interfaces; the External network segment, the DMZ segment, the secure segment and the internal network segment. The proposed firewall is presented as an OpenBSD 3.4 system running 'pf', which enables stateful packet inspection. A description of OPENBSD packet filtering can be viewed at the following URL: http://www.openbsd.org/faq/pf/filter.html#intro.

The developer's choice for the firewall was based on several factors; the OpenBSD pf firewall is known to be secure, efficient with processing and memory usage, versatile, highly configurable and can be downloaded without a fee. The developer states that based on these attributes this design is ideal to support the GIAC environment which is comprised of 4 Ethernet interfaces, a 20-user network, 10 servers and the Internet connection.

The network design positions this firewall directly behind the router ensuring all traffic, both Ingress and egress is required to pass through its external interface. This is accomplished in part by, assigning all publicly routable IP addresses to the external interface. The 1-to-1 network address translation table will then pass the traffic to the appropriate node. The developer states that the placement for this firewall is optimal, as it ensures all traffic must pass through in-depth filtering rules upon entering and leaving the network and gives the ability to create a very granular level of network security.

1.2.0 Configuration:

To run OpenBSD with pf as a firewall, a couple of configuration changes need to be made prior to modifying the pf firewall configuration. These changes are required to enable IP forwarding and to enable pf to run at system boot time. The firewall's external interface file requires updates to assign IP addresses directly to the firewall's external interface which are being assigned to avoid any ARP problems associated with NAT. This

process is actually assigning multiple IP addresses to a single interface.

The developer has decided the quickest and most secure rule processing for this network would be to place a deny all at the top of the access list, followed by process “quick” block rules (quick - evaluates packets on a first match basis), normal block rules, “quick” pass rules and finally normal pass rules. The firewall rules must also be placed in order of options, normalization, queuing, translation and filtering.

The *options section* for this firewall defines all macros, such as those assigning descriptive names for all interfaces and server names to IP addresses. A block policy is set to return RST & ICMP error messages.

The *normalization section* is set with two scrub commands, one to reassemble fragmented traffic and the other to scrub traffic to contain a randomized IP ID field.

The *translation section* translates all internal outbound connections to the public IP address of the firewall, avoiding the need to use Internet-routable addresses for the entire internal workforce. This also makes the internal network unreachable by outsiders with standard routing. The redirect rules make the public services available to the Internet (the DNS, SMTP, WWW and SSH). There are two redirect rules following this to assign publicly routable addresses to the syslog server and the NTP server to allow the router to communicate with these. The last rule in this section gives the database an Internet-routable IP address for the partner’s access via VPN. The rule gives access to SSH and port forwarding within SSH will give access to the MySQL database.

The last section of the pf configuration file is the *filtering section* which is quite in-depth as this is where the majority of the filtering occurs. The filtering begins with a block section that blocks all rules for all inbound and outbound traffic. This actually requires packets to match a pass rule, to get into or out of, the network. Block rules are also listed to block traffic for networks that cannot be routed, packets bound for broadcast address and traffic bound directly for the firewall. There are specific block rules blocking access to specific services – most of which are set up in a table which enables incorporating multiple IP addresses into one variable. The last block rule is written to block the internal interface to everyone and to protect the DMZ and Secure segments from sending out unspecified network traffic. The rules are written such that only traffic that is explicitly stated may leave the networks.

The pass section contains rules written to identify:
- traffic allowed into the internal networks including TCP, UDP and ICMP
- SSH access to IMAP
- hat SMTP relays mail to the internal mail server using a port filter

ensuring an ephemeral port is used to send
- Firewall administrators connectivity to the firewall thru SSH.

These rules are specific to the Secure segment to allow the following:
- the web server to connect to the database server
- database administrator connectivity to database server
- security administrator access to IDS systems and syslog servers thru SSH
- any server on DMZ access to output logs to syslog servers
- the partner's ability to access database server with SSH only, to ensure end to end encryption.

These rules are specific to the DMZ segment to allow the following:
- inbound and redirected traffic to the public servers
- the public DNS server to perform queries
- outbound SMTP connections
- SSH server access out of the DMZ which allows remote users mail access
- all internal network and secure network systems to communicate with the NTP server.

1.3 Two Remote Access Solutions

The first remote access solution (VPN) will be implemented on the border router as outlined in that section.

The second VPN solution presented is an OpenSSH implementation using a 3.2 GHz system with 1024 MB of memory running on OpenBSD 3.4 with one Ethernet interface. This server will be located on the DMZ segment and will fulfill two functions; the first being the SSH server providing the mobile workforce with remote access, and the second being the actual file server. This design allows utilization of the built-in SSH secure copy function that offers easy and secure file transfer, making it a convenient location for the file server.

This solution was chosen on the basis that this is a simple implementation and can adequately provide remote access for the mobile work force, as well as fulfill the requirement for a file server. The minimal cost for this solution was also one of the decision factors with the costs simply consisting of hardware, setup and administration (OpenBSD is available to download without a fee). Additional savings are realized by combining functions on this server avoiding the purchase of a separate file server. The developer believes this system can handle the requirements for the mobile workforce even with a full 6mb of dedicated SSH traffic.

The developer also identifies this server as a probable point of risk relating to

hackers and Internet noise, as it is required to be Internet accessible to support the mobile workers. He also feels the key to mitigating this risk is through proper configuration and patch management practices.

SSH authentication will be accomplished through the use of digital certificates. This will require each of the mobile workers to have a client certificate set up on his or her laptop. The developer indicates there are pros and cons with this; the advantage is the users will not have to remember passwords. The weakness, in the event that a user's laptop is compromised, the certificate will allow access to the file server and email server. Realizing the implications and impacts of this, he suggests the mobile workforce's laptops be configured securely to protect the certificates. He recommends that GIAC utilize host-based firewalls for every laptop, along with installing anti-virus software and establish procedures to patch critical software vulnerabilities when the workers are in the home office.

1.3.0 Configuration:

The SSH server will serve a VPN function for the remote workforce and will be the file server for the remote workers. The file transfer will be through the secure copy capabilities of SSH. The SSH server will also forward IMAP connections to the Internal mail server to allow remote worker access to their email. To accomplish this each user machine will require PuTTY (SSH client) and WinSCP (SCP client) with certificate-based authentication. The user accounts of SSH will have difficult and lengthy passwords as the user will not be required to know them.

The PuTTY implementation requires an OpenSSH download, which is freeware. This download will require changes to enable the daemon configuration file to run successfully in the organization. The changes consist of enforcing the use of version 2, preventing the use of the root account, generating private and public keys, running SSH authentication in the background to add the user keys to the system, adding the public and private keys of the user to the authentication agent, and storing the keys (must run this command from the directory where public and private keys are stored).

The WinSCP configuration requires the use of a drag and drop interface. The user is required to fill in the WinSCP login screen, enter the SSH server IP address, user name, and reference the private key file, and then save the information.

1.4 Network Based Intrusion Detection System

The Intrusion Detection system that is proposed for this network is Snort version 2.1.2, running on a 3.2 GHz system with 1024 mb memory and 2 network interfaces. One interface will be dedicated to sniffing the traffic while

the other will be a management interface. The IDS system will consist of three IDS components, all residing on the secured segment. They will be used to monitor three of the network interfaces the DMZ, the internal and the secure network segments. The external interface will not be monitored as the developer finds more value in seeing what actually gets through the firewall. The firewall and router logs will contain the activity of the failed attempts to access the network on the external segment – these can be reviewed at a future time.

The developer chose Snort as the Intrusion Detection System based on the following reasons Snort has a large user base, is noted to supply more detailed alert data than most commercial solutions and the developer has significant experience with the use of this product. Once again, cost was also a consideration as this tool is available through download free of charge.

Although Snort is capable of being configured to trigger responses and to react to an attack these IDS components will be set to passively monitor and log the traffic. The developer states a preference to monitoring the Snort logs and making manual network changes based on analysis and evaluation of the logs, rather than reactive triggered responses. This preference is based on his own experience relating to the number of false positives (instances that raise an alert but the instance is valid and should not be acted upon) and malicious traffic (traffic crafted to further manipulate once the reactive measure has been initiated). All logs, including the firewall and router logs, will be sent to the syslog server to be stored for future analysis. The developer states that a major weakness of Intrusion Detection Systems is that they are reactive systems and mitigation of this risk requires a strict patching policy and tight firewall rules.

1.5 IP addressing scheme

The Border Router's high speed serial interface has a 30-bit subnet masked IP assigned from the Internet Service Provider. GIAC will have a publicly addressable network (12.2.3.0/24) and the internal router IP address will be assigned one of these addresses (12.2.3.1). The internal structure will use RFC 1918 reserved address space, a set of predefined address blocks assigned by the Internet Assigned Numbers Authority (IANA) as reserved for use within private networks http://www.faqs.org/rfcs/rfc1918.html. The DMZ Segment will use a block of Class C network numbers (192.168.0.0/24), the Secure Segment will also use a block of Class C numbers (192.168.10.0/24) and the Internal address structure will use Class B addresses (172.16.0.0/24). The choice to use RFC 1918 addresses was made based on the internal requirement of only a few servers requiring Internet-routable addresses. Therefore, the developer decided to use address translation and firewall rules to accommodate that requirement. The use of address

translation will also add a little more protection for the internal systems.

All network segmentation will be achieved by using the firewall design, which segments the network into four network segments. The ***External*** segment is where Internet-routable IP addresses reside. All Internet-routable addresses will be assigned to the External network interface of the firewall. The ***DMZ*** segment is where all internal Internet accessible servers will be placed; the NTP server will also be located on this segment. Most servers on this segment will be assigned a 1-to-1 Network Address translation to a routable Internet address on the firewall's External network interface. The ***Internal*** segment is where all internal servers and employee workstations will be placed. This segment is designed to be completely unreachable by direct connection attempts from the Internet; it also has the most external access. The servers that are located on this segment are the mail server and the internal DNS server, which is completely independent from the one that would be accessible from the Internet (which resides on the DMZ segment). The last segment created by the firewall is the ***Secure*** segment. All servers containing critical and sensitive material will be placed on this segment. Firewall rules will grant access to the secure network via IP addresses and specific ports.

2.0 Agreement:

2.1 The Border Router

As the border router is the entry/exit point into GIAC's network and has sufficient capacity. It is excellent strategy to do some initial packet filtering since this would prevent a lot of the basic attempts at accessing GIAC's network as well as preventing any invalid entries from leaving the network. It would also establish a layer for the defense-in-depth strategy. Jared's design accommodates this easily without adding complication to the design. Ingress rules are defined on the serial interface and the egress rules are defined on the Ethernet interface, this allows for easy modification and clarity as new common threats become identified.

The IPSEC 3DEC feature set is a fairly good choice for this router as it will provide the VPN connection for the partner while providing 3DES encryption, a sound encryption algorithm. Although AES (Advanced Encryption Standard) was defined as the NIST Standard in May 2002, the 3DES algorithm is still largely considered the "defacto" standard and a secure algorithm. The drawback is that it is fairly slow on the newer 32 and 64-bit architectures, hence the request for the AES technology development. The 3DES encryption algorithm uses 3 stages of DES which has been in circulation since the mid 1970's and remained "unbreakable" until the mid-to-late 1990's. A good review of DES and 3DES by Kenneth Castelino is available for review on the following URL: http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html. This review also contains some other very informative links related to this subject overall.

Research indicates MD5 is a good solid choice for the password encryption. With reliance on the NIST documentation referenced in the previous DES discussion – although MD5 is not a defined as a Federal Information Processing Standards – it is widely used within the industry today as it provides 128-bit message digest. A good basic explanation of this hash can be viewed at the following URL: http://bfl.rctek.com/guides/?guide=md5

2.2 Multi-Interfaced Firewall

The network design places the firewall behind the router making it the single entry/exit point to the network. This is an excellent strategy because it ensures all traffic passes through filtering rules, which provides a very granular level of security. This placement ensures that this level of granularity can be achieved on both the incoming traffic as well as the outgoing traffic. The firewall configuration file creates descriptive "alias" names for all interfaces, servers, and administrators. This practice assists with our security efforts and with the defense-in-depth strategy as using descriptive names reduces the chances of errors (such as typos and transposing numbers

which occurs frequently when entering numbers). It also enhances the simplicity for ongoing support of this firewall, making rule updates and modifications a more straightforward exercise. The filtering rules are defined providing maximum security for the network and are written in a manner that allows for optimal support (the rule sets are separated and defined by network segments).

2.3 Remote Access Solutions

The recommendation is to implement OpenSSH running on an OpenBSD system. The file transfer requirement would be handled using the built-in function SCP of OpenSSH. The most advantageous component of this implementation is the SCP (secure copy feature). This feature enables encryption of all data, end to end, in comparison to just between servers, as with most encryption products. A paper written by John Fitzgibbon dated September 2004 provides some good explanations and details relating to this topic and can be viewed through the following URL: http://www.jfitz.com/tips/ssh_for_windows.html#What_is_SSH

2.4 Intrusion Detection:

The proposal recommends implementing Snort version 2.1.2 as the Intrusion Detection System, Gartner's quadrant information on Intrusion Detection Systems recommends that enterprises who have not yet selected a network IDS product, should install Snort to gain experience with IDS before committing additional resources. Based on the results of research in this area, the only conclusion to be reached on using Snort for Intrusion Detection is full agreement with the developer. With both the architecture implementation and it's set up as a passive monitoring agent opposed to triggered responses based on events. There is one requirement that must be stipulated in relation to this, that being, all changes resulting from the monitoring activity must adhere to Change Management requirements (as is with all changes to production environment). The only other recommendation to present here would be, review the latest version of Snort prior to implementation. Based on the timelines, it's questionable if the latest release of Snort was in general circulation when this proposal was submitted. The Gartner quadrant information can be reviewed by reviewing the following URL: http://www.gartner.com and searching for:

Magic Quadrant for Intrusion Detection Systems, 2H03
Author: Richard Stiennon
Date: April 2004

2.5 IP addressing scheme

The IP addressing scheme submitted here looks very thorough and a good

solution for the network design that is being proposed. Part of the addressing scheme is to use RFC 1918 IP addresses and address translation for Internet-routable addresses. The developer assessment is correct; this will accommodate GIAC's needs, as only a limited number of addresses will actually require this translation. This adds another layer of protection for those internal addresses, again supporting the defense-in-depth strategy. The developer has done a good job in creating separation of the network segments and in accommodating the requirements through the IP addressing for each of these segments. Ensuring the servers were on the correct segments, depending on the requirements and use of each server, allows access tables and rules to be written and maintained with the least amount of effort. This actually results in maintaining efficiencies related to support requirements as well as reducing the opportunities for errors, which are often generated from poorly constructed rule and access tables.

3.0 Disagreement:

3.1 The Border Router

The greatest concern related to this technology is availability. This router is the single point of entry/exit to GIAC's network and has no redundancy within this design. The directive is to promote and grow the online processing and although the majority of employees reside within the local environment a very significant success factor for GIAC will be the ability for the partner company, third-party suppliers and the external sales employees to have unimpeded access to the internal network. Without redundancy there is a risk the internal network may be inaccessible for an indeterminable period of time. The outage duration could be dependant on many factors, for example: when did the router go down (Is there monitoring in place? Was it during work hours? Is there after hour support? How soon can it be restored?). Without a backup plan in place to mitigate this risk, it has the potential to be very costly.

The other concern to note would be the developer's own comment related to this very issue, in the Architecture Improvements section of his submission. It is not clear if there were cost constraints imposed with his design, which may explain why a redundant solution wasn't presented. Availability is critical for this organization; therefore, a redundant solution should have been submitted as at least a recommended piece of the architecture (an optional component, if nothing else). The developer also mentions the ISP provider as another single point of failure. There would be a Service Agreement negotiated between GIAC and the ISP relating to the Internet service being provisioned to GIAC. This agreement should include a very detailed section related to outages, downtime and overall service. To this point, redundancy concerns should be noted to ensure it is adequately addressed within the Internet Service Providers agreement, but it is not something that should incorporated into this design nor would not be cost effective to do so.

3.2 Multi-Interfaced Firewall

There was much to consider with reference to OpenBSD and the solution being put forward. Being unfamiliar with this operating system, research was required to make an informed decision about this product. Although the Internet is a great place to start it often doesn't provide in-depth details, so once again referencing Gartner, a trusted resource for our company and one that has been relied on for many years. A perspective titled: *BSD Operating Systems* by Mary I Hubley was listed in Gartner's research documents. Although it was written in December 2001, the major points are still very valid today. Based on this and other research, although the OpenBSD operating system is considered one of the most secure operating systems in the

industry and provides a low cost, reliable solution, there are definite concerns using this technology within our company.

There is a need to be cognizant of the long term impacts and considerations relating to the implementation of this solution. In saying this, a large concern is with on-going support and growth, in today's industry OpenBSD, is still considered a "niche" product, meaning there is no vendor support. Most of the support that is available is mainly through user support forums where questions are posed to other product users. This may not be a great concern for a company with an abundance of staff that have past experience with the product but a real concern for a company that does not have this skill set in abundance. Consideration must be given for the long term support for this product as very serious implications could arise if problems surfaced within this technology and the company was unable to readily provide or obtain the required skill set to resolve the issue. This could prove to be very costly to the business.

Also, since considering OpenBSD as a "niche product" many applications do not configure their products to support this operating system. The future application requirements and application compatibility must be considered as GIAC's stated their intent is to expand Internet usage which in turn will expand the business. Therefore, while considering the future growth there must be a realization that with growth also comes opportunities to create efficiencies, many of which are recognized with software products designed to reduce overhead. As such, software compatibility also must to be a consideration.

Some may argue that the solution only needs to be viable for the lifespan of the equipment, which would be between 3 – 5 years. To that end, it may not be a wise business decision to create these types of limitations, considering the rate of advancement in today's technology. It is better to build an architecture that can expand easily when the need arises and ensure support capabilities are readily available, especially when that architecture is vital to your business's success.

Once again, referencing the developer's comments in the Architecture Improvements section in his submission, he states that the firewall solution may be considered inadequate due to software or hardware implementations and references the benefits of Cisco Pix firewalls.

3.3 Remote Access Solutions

The recommendation is to implement OpenSSH running on an OpenBSD system. Again, the points made previously in relation to the OpenBSD operating system are relevant also with this server. In recognition of the fact that this server is also being presented as the file server, the lack of readily

available support for this product would be a greater consideration. The developer indicates that proper configuration and patch management practices are key factors in mitigating the risk associated with this server as it is publicly accessible from the Internet. This server and its availability, as the main interface for the remote workers and the partner company, are critical to the success of the company. The ability to ensure sound reliable support can not be compromised.

The use of digital certificates as the tool for authentication is an excellent choice; however, there are several concerns to mention here. The first relates to not requiring a password. The configuration section elaborates on this, stating that an "extraordinarily long and complicated password will be assigned to discourage brute forcing and that will work fine because GIAC employees will not need to know their password". This creates a very large vulnerability, if the logon procedure is automated to enable access without the user having to supply a password, anyone who gains access to the user's laptop will have full access with absolutely no effort. This cannot be supported; the risks are too great to even consider a configuration design that does not require some form of active authentication.

The developer also recognizes the fact that there is a risk involved with the suggested authentication setup. A suggestion to mitigate the risk is GIAC incorporate a requirement for host-based firewalls for every laptop in the mobile work force, plus anti-virus and mobile patch management (stated as: when mobile workers are in the home office). Considering the number of virus attacks and the increased rate of propagation, this is totally unacceptable. At minimum the network design must include a list of suggested recommendations for these components which would help ensure the network integrity. This would also assist in determining if vulnerabilities are actually inherent or have resulted from a weakness within the design.

A number of questions come to mind from the suggested patch management practice (when mobiles workers are actually in the home office). Specifically, What if the mobile worker never connects from the home office? What about when attempts to patch fail on specific laptops, due to unsupported software or versions or the like?

During the review of this document there were a number of unanswered questions related to the laptops, design and other security items. This design submission lacked a critical piece of information, which would be supplied as either a list of assumptions in which the developer used for consideration when creating his design or a list of related requirements to assist in ensuring the on-going integrity of this design. Either of these would assist in understanding what requirements are expected or required to ensure there is adequate security incorporated into the design. Without this, the network

could be compromised almost immediately and the security the developer had attempted to build in would not only be an exercise in vain but also could have very negative impacts on the company, both present and future.

One of the last points to mention with this section is, with the configuration requirements on the desktops of OpenSSH and Putty. In some parts of the configuration section it appears that the mobile users, the majority of which will consist of sales people, will be responsible to complete the required setup on the laptop. This configuration should be done by resources that are familiar with completing setups and have sufficient knowledge to successfully handle any incidents that may arise during the setup process, whether it is an error resulting from a typo or any error that may occur during the setup.

In the Architecture Improvements section of the submission, the developer talks about the fact that the Cisco 3724 can handle the VPN load, but goes on to state it is not the optimal server for this use. As well, he suggests running VPN on dedicated hardware to allow for future growth and provide the remote work force with a more robust solution to remote access. Based on these comments, an assumption could be drawn that the developer may have presented this design adhering to some cost restrictions. Therefore it may be beneficial to request the developer rework this section presenting what he feels would be the optimal solution for this requirement.

4.0 Improvements:

As concerns have been noted during this review, particularly with the patching practices and on-going maintenance for laptops, clarification is needed to specify, that issues related to this matter will not be given further consideration at this time. So, for the purpose of this review and in the interest of staying within the defined scope of this exercise, the assumption is that GIAC provides adequate management and support for the laptop/desktop environment, using a product such as Active Directory to perform patch management and ongoing maintenance, managing security threats in an effective and efficient manner.

4.1 Design Improvements

The main recommendation in this review is to replace the OpenBSD operating systems with systems that are more widely recognized and offer vendor support and a broader support presence overall. Although OpenBSD is a secure and reliable product, the future long term support and application compatibility with the infrastructure must be ensured.

Note: With the exception of the Border router, the specific brand of hardware was not stated for any other hardware. Therefore, these recommendations include both the hardware and vendor supplied operating systems.

The items recommended for improvements consist of the following:

- A second Cisco Router (for redundancy)
- A Cisco PIX 515 firewall (well recognized and supported)
- A Cisco PIX 501-ul (stand-alone VPN - allowing for future growth)
- An xSeries 226 with a tape drive (for backup requirements and Windows 2003 (implemented as a stand alone fileserver).

4.2 Total Cost of Ownership

As initial costs for the hardware were not supplied in this submission, for the purpose of this exercise they will be included in the overall hardware costs. These recommendations are based on the server requirements based over a 3 year commitment (hardware life).

Overall Hardware Requirements (with software)	$55,000
Implementation	
Technical Resource – build and test	
(75hours @ 125.00 per hour)	$ 9,375
Ongoing Server Support – contracted out	
(204 hours per year x 5 servers@ 100.00 per hour x 3yr)	$61,200
Network Annual Fee (ISP) (26,400 x 3yr)	$79,200

Total	$204,775

4.3 Return on Investment

This design creates an infrastructure that will increase sales and acquire new business (both due to Internet availability and expansion into the International market place). Therefore the Return on Investment will be calculated based on perceived number of new contracts acquired, combined with savings achieved by contracting out the on-going support skills required to maintain the new equipment (upgrades, patching, etc).

Revenue Opportunity:

New Contracts (based on one year)	
(20 contracts @ average of 15,000)	$300,000
Full-Time Salary w/benefits – Contract costs 1yr	
(80,000 salary – 20,400 1yr contract cost)	$ 59,600
Total	$359,600

Yearly Costs:	
Hardware/Software Maintenance	$ 6,000
Ongoing Server Support – contracted out	
(204 hours per year x 5 servers@ 100.00 per hour x 3yr)	$20,400
Network Annual Fee (ISP) (26,400 x 3yr)	$26,400
Total	$52,800

First Year ROI = (359,600 – 204,775) 204,775 = 76%
Total Payback period (counting in ongoing operational costs) = 18.9 months

4.4 Security Awareness Program

The Security awareness program will need a complete review and will require modification to incorporate the additional network capabilities and the do's and don'ts associated with having access to the Internet.

A full blown awareness campaign will be required before the Internet is introduced to the company. The employees will need to be briefed on the common pitfalls and vulnerabilities associated with being connected to the Internet. They will also require an understanding of:

- The terminology
- What their individual responsibilities are relating to security and the network - The benefits of security to the organization and working environment
- Where they get information on GIAC's security policies and standards
- Where and how they report security incidents

To do this effectively a communication plan needs to be developed ensuring key messages are included. Besides the ones listed above, some other key messages for reinforcement include:

- The Security teams mission statement
- Vulnerabilities associated with the internet (spam, phishing, etc)
- Reiteration of other security related items, things they should already know.

  Such as locking devices for laptops, strong password practices, keyboard locking, and contact points for security questions and answers.

4.5 Policy Updates

GIAC's security policy will need a complete review and a gap analysis completed to incorporate the added components that require consideration upon implementation of this network design. They will include the following components:

- Requirements and considerations as they relate to a virtual employee base
- International security policies, as they relate to Information Technology
- Security considerations as they relate to Internet usage from a business perspective.
- Other considerations resulting from the in-depth review into the intricacies of competing in the IT field in the International market.

Conclusion:

In conclusion, if this design was created based on assumptions by the developer relating to a secure environment for laptops, managed by GIAC's internal support team, this design was very well thought out. The developer appears proficient in the design of access rules and basic filtering requirements and has a very good overall understanding on securing the network both from an equipment and software perspective.

Although the design will work as presented, a greater level of availability would be achieved with the implementation of some redundant equipment and with software that is more widely recognized and supported. This will also add the flexibility required to easily accommodate growth and network expansion with less complexity, as well as enabling more options for expansion.

As noted in the section on disagreements there were many questions relating to the lack of attention and detail to ongoing laptop maintenance which has the ability to seriously jeopardize the network security. If either a list of assumptions or a list of on-going laptop and server maintenance requirements had been provided with this submission, it would have provided the additional details required to ensure the appropriate measures were taken to secure the network environment.

The design layout, in itself, minimizes both the unauthorized access attempts and invalid attempts to leave the network. However the assumption is that this design was completed with a large effort on minimizing cost which has presented some limitations with availability and growth. However, should the improvement recommendations be incorporated – this design would easily accommodate all of the requirements for GIAC's network and realize a return on investment in approximately a year and a half.

References:

1. “Securing the Fortune”, practical assignment submitted by Jared McLaren, http://www.giac.org/practical/GCFW/Jared_McLaren_GCFW.pdf .

2. OpenBSD – Packet Filtering, http://www.openbsd.org/faq/pf/filter.html#intro.

3. RFC 1918 (RFC1918), Internet RFC/STD/FYI/BCP Archives, http://www.faqs.org/rfcs/rfc1918.html.

4. 3DES encryption by Kenneth Castelino, http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html

5. Handy Dandy Guide, MD5 and Passwords, http://bfl.rctek.com/guides/?guide=md5

6. Gartner: A perspective titled: *BSD Operating Systems* by Mary I Hubley, written December 2001

7, Gartner: Magic Quadrant for Intrusion Detection Systems, 2H03
Author: Richard Stiennon Date: April 2004

8. ITIL – The Key to Managing IT Services Version 1.0
Electronic ITIL Security Management Publication
Published by TSO for OGC 2004

Last Updated: May 26th, 2017

Upcoming Training

SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
Community SANS Seattle MGT512	Seattle, WA	Aug 14, 2017 - Aug 18, 2017	Community SANS
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS New Orleans MGT512	New Orleans, LA	Aug 21, 2017 - Aug 25, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS New York MGT512	New York, NY	Aug 28, 2017 - Sep 01, 2017	Community SANS
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Toronto MGT512	Toronto, ON	Sep 18, 2017 - Sep 22, 2017	Community SANS
Community SANS Columbus MGT512	Columbus, OH	Sep 25, 2017 - Sep 29, 2017	Community SANS
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced