GCFW Practical Assignment Critique

The purpose of this practical is to critique a GIAC Certified Firewall Analyst (GCFW) practical to enable implementation in a public healthcare company. The GCFW practical was chosen from papers numbered above 400. The key areas of analysis will be related to business requirements, risk management, regulatory compliance, cost, technical merit, and management. The design chosen was developed by Jonathon Berry and is titled "DEFENCE IN DEPTH: PREVENTING THE COOKIE FROM CRUMBLING." The intended outcome of the critique is ...

SANS GSLC Practical Assignment
Version 2.0
Administrivia version 2.9

GCFW Practical Assignment Critique

"DEFENCE IN DEPTH:
PREVENTING THE COOKIE
FROM CRUMBLING"
Prepared by: Jonathon Berry

(*http://www.giac.org/practical/GCFW/Jonathon_Berry_GCFW.pdf*)

Assessment By: Bart L. Hubbs

Table of Contents

Abstract

The purpose of this practical is to critique a GIAC Certified Firewall Analyst (GCFW) practical to enable implementation in a public healthcare company. The GCFW practical was chosen from papers numbered above 400. The key areas of analysis will be related to business requirements, risk management, regulatory compliance, cost, technical merit, and management.

The design chosen was developed by Jonathon Berry and is titled "DEFENCE IN DEPTH: PREVENTING THE COOKIE FROM CRUMBLING." The intended outcome of the critique is to have a design that can be presented to upper management as a suitable implementation in a regulatory rich healthcare environment.

1.0: Executive Summary

Healthcare companies that operate as for-profit entities are facing a multitude of challenges. The regulatory environment is becoming more restrictive, viruses and worms are growing more pervasive and damaging, and our stakeholders are demanding more flexible access to our systems.

The regulatory focus is on the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX). Both pieces of legislation highlight the need for good systems administration and controls, but focus on different aspects of the business. The main focus of HIPAA is to protect personally identifiable health information while SOX is concerned with data that impacts financial reporting. Violations may be met with both civil and criminal penalties. Therefore, the company must be ever watchful of new threats to our systems, data, and business operations.

The most prevalent security related threat to on-going business operations is the continued development and propagation of viruses and worms. Virus and worm prevention or containment is a vital component to the overall risk mitigation strategy. Virus and worm outbreaks have multiple cost aspects for the company including lost patient charges due to system unavailability, lost productivity because of recovery efforts due to infection, and potential regulatory impacts depending on the virus or worm payload. However, the company must balance risk with opportunities to serve our stakeholders and grow the business.

Our stakeholders include multiple groups that depend on or need access to our clinical and/or financial systems to help support and grow the company. The access requirements and associated risk model varies by user group. The main access groups are internal only users (i.e. nurses, hourly employee, etc.), internal/remote users (i.e. salaried employees, doctors, etc.), and business partners (i.e. collection agencies, banks, etc.). Risk mitigation solutions must be developed for each user group to help ensure that the company recognizes the benefit that each brings and minimizes the risk to business operations. Furthermore, the solutions developed must be cost effective to implement and support so that the benefit is not unreasonably diluted.

The proposed solution with improvements provides the system access needed by each user group while helping to reduce the associated risk. Furthermore, the solution proves that the company is prudent from a regulatory standpoint while still containing cost. Some new technologies are introduced with the proposed solution; however, using each technology fully was a major focus.

2.0: Technical Solution

The solution presented for critique was created by Jonathon Berry (http://www.giac.org/practical/GCFW/Jonathon_Berry_GCFW.pdf) and was originally created for GIAC Enterprises to support the sale of fortune cookie sayings on the Internet.

2.1: Overall Design

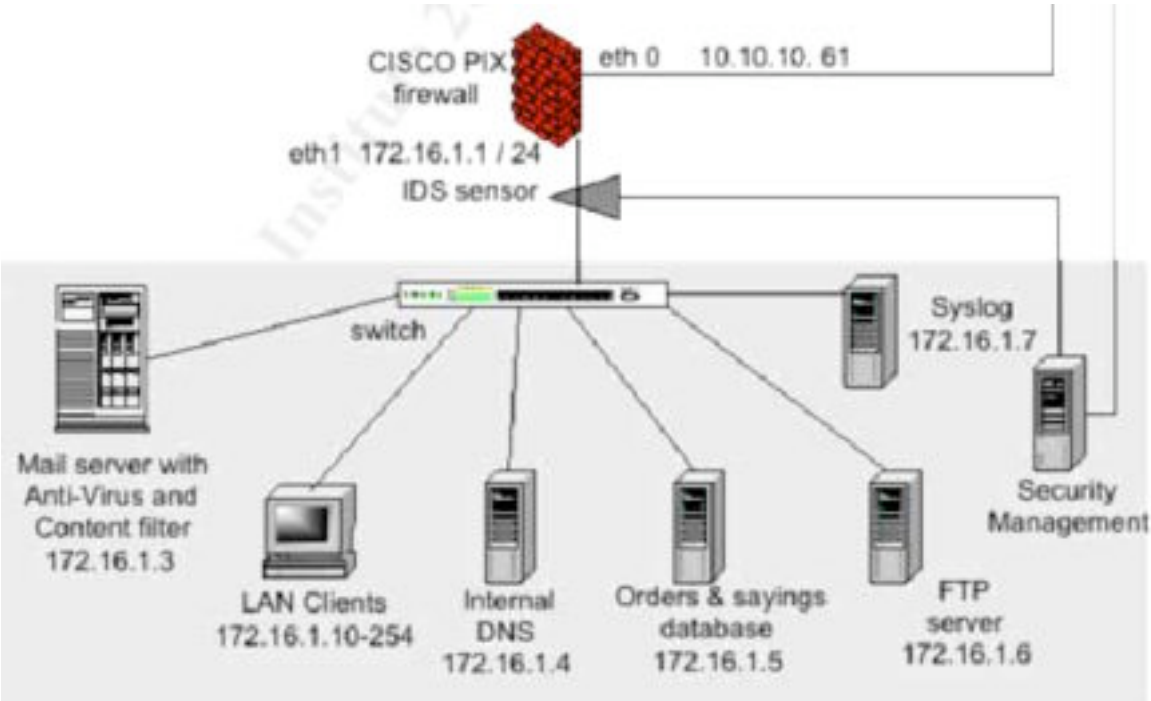
The design utilizes multiple technologies referenced as "layers" to help establish networks of different trust levels where the "Defense-in-Depth" concept is implemented. The "Internal LAN" is established as a network with private Internet Protocol (IP) addresses segregated from the "trusted" and "untrusted" network by a firewall at each entry point. The "trusted" and "untrusted" networks are both numbered with private IP address space and are connected to the Internet by a different ISP for redundancy with separate firewalls for each connection. A total of four firewalls are used to connect and compartmentalize the three GIAC networks and connect to the Internet. The Internet is used to connect remote entities (i.e. customers, partners, and employees) to the GIAC networks.

2.2: The Internal LAN

The "internal" LAN is the heart of the GIAC network. This network will contain the most prized and protected assets of the company, therefore, minimum connections are permitted inbound from either the "trusted" or "untrusted" networks. However, outbound connections from the "internal" LAN are permitted to the http proxy for Internet browsing and directly to the "trusted" and "untrusted" networks for systems administration and general maintenance.

The "internal" LAN is a switched private network controlled at the two perimeters by Cisco PIX 535 firewalls. The paper does not explain the detail of how the "Inner Firewalls" are configured except to say the firewalls do not permit any inbound connections sourced from external networks. Additionally, the firewalls are used to perform network address translation (NAT) for connections bound for either the "trusted" or "untrusted" networks.

An Intrusion Detection System (IDS) sensor is located on the "internal" LAN just off the firewall interface to monitor all passing traffic. The IDS sensor software product is ISS Real Secure and will be network-based. The sensor will be connected to a hub that sets between the circuits on the internal side of the firewall. The hub is used so that all traffic is broadcast to all nodes connected. The IDS sensor will be connected to the hub and a "Management Server" on the "internal" LAN. See the proposed design below.



2.3: The Untrusted Network

The "untrusted" network is best described as a traditional Demilitarized Zone (DMZ). However, this DMZ is configured with private IP addresses instead of public. The DMZ has the following devices:

- Web server – Hosts the company web site (GIAC.com);
- Simple Mail Transfer (SMTP) relay server with anti-virus and content filtering – Services outbound and inbound mail;
- World Wide Web (WWW) outbound proxy – Manages outbound Hypertext Transfer Protocol (HTTP) and Secure Hypertext Transfer Protocol (HTTPS) for "internal" LAN users; and
- An external Domain Name Service (DNS) Server – Provides domain name to IP address resolution for GIAC.com and resolves Internet DNS addresses.

Individual servers host each service to help ensure that compromise of one service will not compromise the entire zone. Furthermore the switch connecting the servers to the firewall blocks "server-to-server" communication so that if a server is compromised it cannot be used to try and attack the other servers.

Additionally, an Intrusion Detection System (IDS) sensor is located on the "untrusted" network just off the firewall interface to monitor all passing traffic. The sensor will be connected to a hub that sets between the circuits on the internal side of the firewall. The hub is used so that all traffic is broadcast to all nodes connected. The IDS sensor will be connected to the hub and a "Management Server" on the "internal" LAN.

Network access to the “untrusted” segment is controlled by two firewalls and a router. The Cisco PIX 535 controls access to the network from the “internal” LAN and the Checkpoint NG firewall controls access to and from the Internet. The Cisco 1760 router with the firewall feature set is configured to drop private IP networks (as defined in RFC 1918) like the ones used within the company. The Checkpoint NG firewall is the main configuration point for inbound and outbound connections for this network. The following is an explanation of the Internet facing firewall rule-base with comments on some elements that may have been left out by mistake.

- *Rule One* – This rule is important to enable other Internet hosts to determine the IP addresses for the company hosted servers. This rule allows any address to query the External DNS server (UDP – 53) on the “untrusted” network. This rule does not permit DNS zone transfers (TCP - 53) from Internet hosts.
- *Proposed Rule One B* – Allow the External DNS server to also query any host on the Internet. This rule would allow the hosts on the “untrusted” network to obtain DNS information so they can work. The SMTP server and WWW proxy would have a tough time completing outbound service requests without DNS.
- *Rule Two* – Allow the internal DNS server to query and DNS server and/or initiate a zone transfer. This rule could be removed as long as the internal DNS server was configured to forward any requests it didn’t have the answer for on to the External DNS server. It must be assumed that the PIX 535 is configured to also permit DNS access to the DNS server on the “untrusted” network.
- *Rule Three* – Allow any host to connect to the web server on the “untrusted” network over HTTP and/or HTTPS. This rule is important because it allows Internet hosts to connect to the company web site.
- *Rule Four* – Allow any host to connect to the SMTP server on the “untrusted network” using the SMTP protocol. This rule enables the company to receive inbound Internet email.
- *Rule Five* – Allow the SMTP server to send email out to any host using SMTP. This rule enables the company to send outbound Internet email. The rule also permits the server to download virus updates from any host. This rule could also be split to only permit the SMTP server to download virus updates from the anti-virus vendor’s site instead of any host.
- *Rule Six* – Allows the proxy server to connect to any host using the HTTP and HTTPS protocols. The rule does not log, but the proxy server should be configured to log requests.
- *Rule Seven* – Allows ICMP-requests to be accepted by the firewall (trans) from the “untrusted” network and the PIX 535. It should also be noted that a review of the hosts included in the “UntrustedPublicServicesActual” group might be advisable. Some of the hosts “In Group” seem to be

"Internal" LAN hosts, based upon the object label, instead of the "Untrusted" network hosts as intended.

- *Rule Eight* – Drop and alert on any external connections to the "internal" LAN or "UntrustedDepthFirewall" not previously accepted.
- *Rule Nine* – Reject any other access by hosts defined in the "UntrustedPublicServicesActual" group, the "Internal" LAN, or the "UntrustedDepthFirewall." The reject action is used because the sources are internal hosts and should receive back an error message. If the drop action was used, the internal users would get no error.
- *Rule Ten* – Drop any requests not previously permitted. This rule is often called the "clean-up" rule because it ensures that all other network traffic is managed.

The last component of control is the PIX firewall. The detail configuration for the PIX was not defined in the paper. However, the configuration should block most connections originating from the "untrusted" network bound for the "internal" LAN and permits certain connections from the "internal" LAN to the "untrusted" network. The configuration would have the following attributes base upon the requirements noted:

- Allow DNS queries and zone transfers from the "DNS_ServerInternal" to only the "DNS_ServerExternal" or in a different configuration the "DNS_ServerInternal may be permitted to initiate a DNS query or transfer to any host.
- Allow the "Internal" LAN to access the "WebServerExternal" and the "HTTP_Proxy using the HTTP and HTTPS protocols.
- Allow the "internal" LAN mail server to access the "SMTP_RelayExternal" via the SMTP protocol. This rule is needed to allow internal users to relay email via the SMTP server to external email addresses.
- Allow the "SMTP_RelayExternal" to access the "internal" LAN mail server via the SMTP protocol. This will be the one exception to the rule barring connectivity originating from the "untrusted" network to the Internal LAN. If this rule is not in place, users will not be able to receive email from the outside world via the SMTP relay.

2.4: The Trusted Network

The "trusted" network has the main purpose of supporting the business functions of known entities (i.e. partners, suppliers, etc.) which have a business relationship with the company. The configuration of the "trusted" network was not defined within this paper like the "untrusted" network. However, it must be assumed that the configuration of the Internet facing firewall should allow users with a valid VPN client and user ID/password to connect. All connections are set to "encrypt" the session. It must also be assumed that ftp, http, and https are permitted based upon the servers available in the "trusted" network.

An Intrusion Detection System (IDS) sensor is located on the “trusted” network just off the firewall interface to monitor all passing traffic. The sensor will be connected to a hub that sets between the circuits on the internal side of the firewall. The hub is used so that all traffic is broadcast to all nodes connected. The IDS sensor will be connected to the hub and a “Management Server” on the “internal” LAN.

The final component of control is the PIX firewall. The detailed configuration for the PIX was again not defined in the paper. However, the configuration should block all connections originating from the “trusted” network bound for the “internal” LAN and permits certain connections from the “internal” LAN to the “trusted” network to administer the servers, retrieve files from the ftp, and update and retrieve information from the http server.

3.0: Agreement

3.1: Using the configuration in a healthcare environment

The network design proposed for GIAC Enterprises has many elements that would make it suitable for a healthcare environment. The minimal need for non-VPN connections to company networks makes it a viable candidate for the highly regulated and privacy focused healthcare industry. Furthermore, the two external networks only requiring minor access to the “internal” network make this design a good starting point.

3.2: User connectivity to the Internet

The healthcare industry is changing rapidly to help drive cost out of the system. The Internet is being used as one of the tools of cost savings. The industry is seeing health insurance companies, ambulance services, prescription drug stores, reference sources, etc, establishing Internet based services to automate various functions and therefore reduce cost and increase efficiency. Therefore, it is vital that most users within healthcare companies have access to the Internet. However, with user access comes many potential risks via web browsing and email. The proxy solution presented for both email and browsing in the design is attractive because it helps provide a central point of control and can enable a quicker response if a threat is realized. Furthermore, the implementation of both content filtering and virus scanning on the mail relay is a great solution.

3.3: Multi-Layered Approach

The multi-layered approach to data and systems protection is vital in a healthcare environment. The most critical data to protect on the network for a healthcare company is patient information. However, it is the patient data that must be used widely on the "Internal" network to help automate and streamline operations by minimizing the number of times the data is reentered. Therefore, segmenting the network and restricting connectivity is the best broad based line of defense. The policy that would be implemented with this design is that healthcare information is only available for access on the "Internal" network.

The layers with the design presented go further that just the network. The virus scanning capabilities for the email system are implemented in three distinct layers: mail gateway, internal mail server, and network client. The multi-layer email scanning architecture also provides the opportunity to deploy multiple anti-virus packages to hopefully obtain the most effective protection from new viruses.

3.4: Systems Monitoring

The design presented has two logging elements that are very useful in a healthcare environment. The implementation of IDS and syslog are important services that will help with the centralized monitoring of systems and will contribute to the overall HIPAA program

The implementation of a syslog server on the "Internal" network will provide a place to centrally monitor logs generated by systems and devices on the network. Furthermore, according to Ian Eaton "A defence in depth approach to system security goes hand in hand with a defence in depth approach to logging." (6). The IDS will be used to monitor the traffic and the network layer and provide additional depth to the syslog facility which will show the actual activity that happens on the host.

The two keys to help leverage the syslog component of the design is to ensure that all systems are configured to log to the syslog server and that all devices utilize a consistent time source. The next step is to implement an automated system, like swatch, to alert on logs sent to the syslog server. The automated monitoring of logs is critical to success because hiring and army of employees to monitor logs is not an option.

3.5: Centralized User Authentication

Management of user accounts is a major cost for any healthcare company. The tenant in user account management is the fewer points of administration the better. Additionally, the user experience and subsequent productivity is closely tied with the number of user ID's and passwords the user must remember. The Meta Group asserts that managing users, user stores, and authentication and access control consume an average of 54,180 hours/year. Furthermore, META

gives the indication that even a 25% improvement in efficiency would result in a time savings of 13,545 hours (6.7 FTE). Therefore, any opportunity to configure a network device to utilize a centralized account management system is an opportunity for cost savings, reduced Total Cost of Ownership (TCO) and potential productivity gains.

The design presented has two central user account management systems proposed. The Microsoft © Active Directory (AD) system is used to manage accounts on the "internal" network and Lightweight Directory Access Protocol (LDAP) server is used on the "trusted" DMZ network. The solution presented is a great fit for a healthcare company due to the large number of users necessary to properly administer healthcare, process claims, and administer the financials.

4.0: Disagreement

4.1: Overview of Disagreement

The network design has many great attributes that are useful in a healthcare environment. The high-level management goals of the implementation are as follows:

- Support the business and balance security with cost;
- Maintain and enhance security without significantly increasing management overhead or complexity;
- Implement systems that are supportable, scalable, and fault-tolerant;
- Ensure that the design is implemented to help ensure compliance with regulations.

The areas of disagreement are not exclusively focused on the security aspects of the solution, but more on the balance of security with overall cost, manageability, supportability, and regulatory compliance.

4.2: Cost-Based Disagreements

The initial area of disagreement comes with the implementation of both Checkpoint and PIX firewalls. Leveraging multiple firewall technologies is great for security, but can be very costly. The proposed solution depicts Cisco 1750 routers that have the firewall feature set installed, but many of the firewall features are not used. Additionally, the Cisco Catalyst 2950 switches can be used for simple and extended ACL's based upon the general policy of the organization. Better utilizing the existing security features of the Cisco routers and switches will provide the diversity in security technologies without using the PIX firewalls. The PIX firewalls provided network segmentation and it is a preference to keep the segmentation. Therefore, the segmentation will be kept

using additional interfaces on the Checkpoint firewalls. The cost impact of this recommendation will be presented in the “Improvements” section of this paper.

4.3: Management Overhead and Complexity Based Disagreements

Reduction in management overhead and complexity will help reduce support cost and hopefully enhance the user experience. It is a safe assumption that money can be saved and efficiency gained by looking for ways to improve solutions through scheduling routine jobs to run automatically, central management, and automated monitoring/alerting. Employee salaries and benefits are often one of the largest ongoing expenses a company recognizes on its income statement.

The first management overhead and complexity disagreement arises with the http proxy server which allows user access to the Internet. The proxy server is shown to exist on the “untrusted” network. The http proxy placement and configuration is a critical component on the security side, but can also increase cost and management if deployed without planning for the future.

The PIX firewall on the “internal” network is configured to perform NAT and it must be assumed that the NAT is source. Therefore, the activity logs on the proxy server will always show the NAT address and not the actual client IP address. The management overhead associated with tracing logs to a specific client could be very significant. After addressing the log tracing issues, it is time to focus on problems with user account management.

User account management is a big opportunity in the proposed design. The “trusted” network utilizes an LDAP server for SecuRemote user authentication. The “trusted” network also contains an http and an ftp server. Each server and associated application has user account requirements. The current configuration should use the LDAP server to centralize the user accounts for both the http and ftp server. Furthermore, the “internal” network has an AD system that can be used to centralize account management for many of the servers. The integration would save account management overhead, significantly improve the user experience, and the cost would be minimal. The next area is file transfer.

The “trusted” and “internal” networks both contain file transfer protocol (ftp) servers as a part of the design. Ftp is a clear-text protocol and the usage should be closely analyzed in a healthcare environment for any potential of transmitting or storing Electronic Patient Health Information (EPHI). The HIPAA rules have provisions for both privacy and security included. Tom Grove states the following regarding HIPAA and encryption “Covered entities are encouraged in the Rule's preamble to consider use of encryption technology for transmitting EPHI.”

Therefore, in a healthcare environment it is suggested that the ftp servers be changed to use openssh for both administration and file transfer. The reason for

change is that EPHI in the form of transcription files, medical reports, and medical claims will be transmitted using the file transfer servers.

Unfortunately, the use of sftp will negate the effectiveness of the Checkpoint content checking at the perimeter. Therefore, the sftp servers should be installed with virus scanning software. More detail on this solution will be listed in the "improvements" section of this paper. The last disagreement is related to central logging and the use of syslog.

The last overhead and complexity disagreement exists with central logging using syslog. The design on the "internal" network calls for the implementation of a syslog server. However, the configuration calls for the UDP based syslog system vs. the newer syslog-ng that enables both UDP and TCP syslog. Michael Bauer explains the following about the benefits of syslog-ng, "Syslog-ng ("syslog new generation") is an attempt to increase syslog's flexibility by adding better message filtering, better forwarding, and eventually (though not quite yet), message integrity and encryption." Furthermore, Bauer explains "Syslog-ng supports remote logging over both the TCP and UDP protocols." The implementation of TCP based syslog helps ensure that all the logs get to the central server versus the old UDP-based syslog which was not concerned with delivery.

4.4: Disagreements related to supportable, scalable, and fault-tolerant systems

The network and associated systems are critical in a healthcare environment for patient care, charge capturing, financials, and vendor transactions. Therefore, system outages normally mean loss of revenues and/or an increase in expenses, not to mention the potential that the company misses opportunities to convert accounts receivable (patient charges) to cash. As a result, system uptime is important and planning is a must.

The first area of disagreement is the configuration of Internet Service Provider (ISP) connections and associated routers. The design uses two different ISP's for connectivity and a router for each. If either of the ISP connections or the routers are down an externally accessible network is impacted. Furthermore, if either ISP or router is down a part of the business suffers. The next area of concern is the firewall structure.

The design uses a separate firewall for each Internet accessible network. This implementation can be good from a security perspective, but to make the solution fault-tolerant two additional firewalls must be added. The additional firewalls add cost for hardware, software, and management. The current configuration makes each firewall a single point of failure. The final area of disagreement in this area is name resolution.

A case can be made that if DNS is down the whole network is down. Most users and many servers/services do not know or maintain the actual IP address associated with the network resource. Therefore, if DNS is down most systems will not function correctly. The network design depicts one DNS server on the "internal" and one on the "external" network. If the internal DNS server is down, users will not be able to access internal resources and will probably not be able to reach the http proxy server. If the external DNS server is down for an extended period then Internet users would not be able to access "untrusted" network resources. Therefore, additional improvements related to redundancy should be made in this area.

4.5: Compliance with regulations.

Regulations that impact or govern Information Technology implementations are often subsets of a larger scope like HIPAA and SOX. Systems which comply with regulations can be implemented one way and cost a significant amount of money in people and technology. However, if critical planning is done early on then compliance can still be achieved without significantly impacting the overall cost. The disagreements noted in the previous sections impact the cost of compliance with regulations. Leveraging central logging and alerting, user account management, and fault-tolerant systems can help support compliance without hurting the budget.

5.0: Improvements

The solution presented by Jonathon Berry utilizes various layers of protection that include hardware, software, network design, and systems configuration. Each layer contributes to the defense-in-depth strategy. However, some of the solutions provided are more focused on security and less focused on other areas that significantly contribute to management acceptance and organizational support. This section will begin with the detail of the improvements and benefits. The last part of this section will provide the upper management briefing overview with financial roll-up, TCO, and Return on Investment (ROI) information.

5.1: Consistent Time Source

The first improvement is the addition of a central time source. The network time protocol (NTP) service can be implemented in the proposed design and reside on the syslog servers. NTP is considered a "core-service" because it is a critical component for overall supportability and provides a key element that can enable log correlation. All network devices should be pointed to the central time source. The additional improvements below will help reduce cost, improve uptime, and maintain an acceptable security framework.

Summary of Cost Impact (Consistent Time Source)

Item	Cost	Quantity	Total (Not Including Tax)
NTPD Software	$ -	2	$ -
configuration time ($42 per hour)	$ 42.00	1.5	$ (63.00)
Total Net Cost			$ (63.00)

5.2: Firewall Improvements

The first area of improvement comes through reducing, consolidating, and enhancing the configuration of the firewalls. The first recommendation is to remove the PIX 535 firewalls and increase the number of network interfaces on the Checkpoint firewalls. The Checkpoint firewall currently has two interfaces, but can be increased to support more networks. Increasing the interfaces on the firewalls to five will allow the support of the "internal." "trusted," "untrusted," and Internet networks while using the fifth interface as a "heartbeat" and synchronization interface to support firewall redundancy and clustering. The recommendation is to use a product like the Checkpoint "ClusterXL" to enable the firewall infrastructure to maintain enhanced uptime and therefore better support the business operation. The cost impact of the change can be seen in the summary below.

Summary of Cost Impact (Firewall)

Item	Cost	Quantity	Total (Not Including Tax)
Cisco PIX 535	$8,877.95	2	$ 17,755.90
ClusterXL for Loadsharing	$4,660.70	1	$ (4,660.70)
Total Net Savings			$ 13,095.20

The next improvement to help maintain diversity in the firewall solution involves better leveraging the current technology. The proposed solution uses Cisco 1750 routers that have the firewall feature set installed, but many of the firewall features are not used. Additionally, the Cisco Catalyst 2950 switches can be used for simple and extended ACL's based upon the general policy of the organization. Better utilizing the existing security features of the Cisco routers and switches will provide the diversity in security technologies without needing the PIX firewalls. Therefore, the segmentation will be maintained using additional interfaces on the Checkpoint firewalls and diversity will be maintained using security features of the proposed routers and switches. Additionally, the overall security posture is not impacted; however, cost and complexity issues are reduced. The time savings associated with management of the PIX firewalls is somewhat offset by the enhanced configuration of the routers and switches. Therefore, the time savings was not included in the summary above.

5.3: HTTP Proxy Improvements

The proposed solution shows the http proxy placed on the "untrusted" network with the source address controlled by NAT. Additionally, a good audit trail is critical for maintaining compliance in the healthcare industry. Furthermore, the log information generated should be stored centrally to enable more effective review and management. Furthermore, it is critical to ensure that the access can be tied to an individual user and not just an IP address. Therefore, the following are recommended improvements:

1. Move the http proxy server to the internal network.
2. Utilize the syslog server with syslog-ng to remotely journal the proxy logs.
3. Leverage the 'ntlm_auth' for squid, so the proxy can do pass-through authentication with Active Directory.
4. Install and configure the 'squid-vscan' open-source package to virus scan all traffic going through the proxy for known viruses.

The recommendations will enable better log information, centralized log access and analysis, central user authentication, and virus protection. The hard benefits of the recommendations are control of Internet access via authentication, reduced virus exposure, and the ability to centrally analyze logs and correlate with other sources. The central log consolidation with syslog-ng, the consistent time source, and the user ID will save a minimum of two hours per week due to employee access log requests by managers and directors. The savings is due to the ability to find the user ID attached to the log instead of correlating IP addresses to workstation to users and the need to process the logs off proxy. The syslog server can be used to collect the logs and process requests for log detail from management.

The cost impact summary below includes "hard costs" that can be calculated. One "soft cost" that should be mentioned is the addition of anti-virus scanning to the http proxy server. The threat of infection by web-based viruses is significant. However, the estimation of savings from the implementation of anti-virus is dependent on many factors. Therefore, the cost impact summary is limited to the hard-costs that are noticed through savings on software, hardware, or employee time.

Summary of Cost Impact (HTTP Proxy)

Item	Cost	Quantity	Total (Not Including Tax)
Move the HTTP Proxy	$ -	1	$ -
Remotely journal logs			
Additional syslog server storage	$ 527.85	1	$ (527.85)
syslog-ng software	$ -	1	$ -
configuration time ($42 per hour)	$ 42.00	1	$ (42.00)
Leverage ntlm_auth			
ntlm_auth software	$ -	1	$ -
configuration time ($42 per hour)	$ 42.00	1	$ (42.00)
Install and configure 'squid-vscan'			
squid-vscan software	$ -	1	$ -
configuration time ($42 per hour)	$ 42.00	1	$ (42.00)
Cost Savings (Two hours per week employee time)	$ 42.00	104	$ 4,368.00
Total Net Savings			$ 3,714.15

5.4: User Account Management and Security Improvements

The proposed solution utilizes AD on the internal network and LDAP on the "trusted" network. User account management consumes a significant amount of time and effort related to account setup, password management, account management, etc. Each server will have a minimum of three-thousand accounts that need administration. A very conservative estimate is that each account will require five minutes of administration per year. Therefore, consolidating and reducing the number of user account repositories adds up to significant saving in administration time.

The improvements include the following:

1. Convert the ftp servers to openssh and use sftp and scp. Configure the sftp servers with a scponly shell. The scponly shell can be given to non-administrators.
2. Configure the ssh server on the trusted network to utilize the LDAP server for authentication using pluggable authentication modules (PAM) on the ssh server. The internal ssh server used for sftp can also be configured to utilize AD for authentication using PAM. The reduction in time associated with administering multiple user accounts is significant. Additionally, the ability to disable access by removing an account from one or two locations instead of each server is a big win for security.
3. Install virus scanning software like 'vscan' on each sftp and http server to help minimize the possibility of infection.

4. Ensure that the sftp servers are configured with syslog-ng and journal logs to the syslog server. This improvement does not have any hard savings tied, but it will help in central monitoring and alerting.
5. Configure the http server to use mod_ldap for authentication using the LDAP server.

Summary of Cost Impact (User Account Management and Security)

Item	Cost	Quantity	Total (Not Including Tax)
Use sftp instead of ftp			
Openssh software	$ -	1	$ -
SFTP-only shell	$ -	1	$ -
configuration time ($42 per hour)	$ 42.00	1.5	$ (63.00)
Leverage AD and LDAP			$ -
PAM Software	$ -	1	$ -
configuration time ($42 per hour)	$ 42.00	2.5	$ (105.00)
Install and configure 'vscan' (3 servers)			
vscan software	$ -	1	$ -
configuration time ($42 per hour)	$ 42.00	2	$ (84.00)
Remotely journal logs			
Additional syslog server storage	$ 527.85	1	$ (527.85)
syslog-ng software	$ -	1	$ -
configuration time ($42 per hour)	$ 42.00	2	$ (84.00)
HTTP Server using mod_ldap			$ -
mod_ldap software	$ -	1	$ -
configuration time ($42 per hour)	$ 42.00	1	$ (42.00)
Cost Savings Summary			
Leverage AD and LDAP			
3000 user accounts per server (3 Servers)		9000	
Administration Time $28 (per 12 Accounts)	$ 28.00	750	$ 21,000.00
Total Net Savings			$ 20,094.15

5.5: Centralized Logging and Alerting Improvements

The proposed solution depicts a syslog server on the "Internal" network. The syslog server should be configured with syslog-ng to provide better reliability for remote log delivery. Additionally, it is recommended that resources in the "trusted" and "untrusted" zones be configured to remotely log as well. The best case would be that the internal syslog server is used as the single point of collection. The single point of collection will also enable a central point of monitoring and alerting.

The monitoring and alerting features can be implemented using a tool like swatch to simply watch the logs and send alerts when specific criteria are met. The benefit of this central logging and alerting method is that all servers can be monitored effectively without increasing staff the complete the monitoring activities. This improvement does not bring a hard cost savings, but does enhance "detective controls" by automatically monitoring logs and generating alerts when necessary. Furthermore, the additional cost associated with central logging and monitoring is minimal, but the enhanced security without increasing on-going staff effort is significant.

The central logging and alerting solution will also provide a facility to cross reference IDS alerts with actual host logs. The IDS analyst can use the IDS to see the network traffic and then when alerts are seen, the analyst can cross-reference the syslog-ng server alerts to see any host-based logs generated. Furthermore, as the IDS analyst documents the correlations between IDS and host logs, a swatch configuration can be built to make the filtering process more efficient. The process of maturing the centralized logging and alerting of server logs with IDS alerts may also help streamline the implementation of a Security Event Management (SEM) system at a later point.

The proposed improvements are beneficial as long as the services are working correctly. Therefore, it is very important in this central logging configuration that the syslog-ng service is up and listening on the syslog server and that all the "client" servers are running the syslog-ng process and logging correctly. Therefore, it is also recommended that the 'mon' application be utilized on each server to monitor the syslog-ng services and alert if they are not operating as expected. Below is a summary of the expected cost.

Summary of Cost Impact (Central Logging and Alerting)

Item	Cost	Quantity	Total (Not Including Tax)
Central Logging with syslog-ng			
syslog-ng software	$ -	1	$ -
configuration time and hardening ($42 per hour)	$ 42.00	1.5	$ (63.00)
Central Alerting			
swatch software	$ -	1	$ -
configuration time ($42 per hour)	$ 42.00	3.5	$ (147.00)
Syslog rotation and backup			
logrotate software	$ -	1	$ -
configuration time ($42 per hour)	$ 42.00	2	$ (84.00)
Configuration of syslog-ng monitoring services (Server and clients)	$ 42.00	8	$ (336.00)
Total Net Cost			$ (630.00)

5.6: Reduction of Single Points of Failure

The proposed solution depicts a few "core services" that appear to be redundant, but may need some additional focus to ensure that the redundancy is effective. The first area of needed redundancy was addressed in section 5.1 describing the firewalls. The original design depicted two checkpoint firewalls and two PIX firewalls, but the needed redundancy for network access was not fully recognized. The new solution proposed addresses the redundancy issue in this area. The next area focuses on Internet connection redundancy.

The solution presented contains Internet connections from two different ISP's. However, the circuits provided services to different Internet connected networks. In the new design with the firewall consolidation it is easier to achieve Internet connection redundancy. The suggested improvement involves using both Cisco routers in a high availability configuration. Additionally, it is recommended that the routers be configured to utilize both circuits simultaneously so that Internet connectivity is not impacted if either circuit is down. The solution improvements can be configured during installation and do not take significantly more time to complete, therefore, no cost impact is shown. The benefit to this configuration is that uptime for the Internet connection should be greater and bandwidth is consolidated. The hard cost associated with the increased uptime cannot be calculated effectively without detail on downtime losses. Therefore, no cost summary will be illustrated for this recommendation. The next area of improvement is regarding DNS.

The DNS servers shown are both single points of failure. The DNS service utilized is BIND ver 9.2.1.2 which can be configured to utilize a slave server. The service requires very little server resources to run and the slave service can be strategically placed on existing servers. The recommended improvements are as follows:

1. Install the BIND ver 9.2.1.2 software on the sftp server on the "internal" network and configure it as a slave. The primary DNS server should also be configured to recognize the slave, permit zone transfers, and notify the slave about zone changes. All network devices that need DNS should have both server IP addresses configured for DNS services.
2. Install the BIND ver 9.2.1.2 software on the SMTP server and configure similarly to the "internal" network. The entries for the public DNS servers should be updated to reflect the new server. Additionally, the firewall rules will need to be modified to permit DNS traffic to the SMTP server. The firewall rule edits will not be reflected in the cost due to the minor time need to add and additional service to the rule.

Summary of Cost Impact (Central Logging and Alerting)

Item	Cost	Quantity	Total (Not Including Tax)
BIND install and configuration			
BIND Software	0	2	$ -
Primary DNS (No time increase)	$ -	2	$ -
Secondary DNS	$ 42.00	2	$ (84.00)
Total Net Cost			$ (84.00)

5.7: IDS Improvements

The IDS solution provided in this design appears to be effective. However, the weak link in the proposed solution is the implementation of a hub to gain network traffic visibility in a switched network. The big drawbacks with using the hub in this situation are as follows:

1. Bandwidth limitations – The hub supports 100mb total bandwidth. The hub will have three connections and will therefore max out at quite a bit less that 100Mb because of the three port connections that need visibility. The best solution would provide full 100Mb bandwidth to all connections.
2. Fails closed – A hub will typically not fail often, however, if the hub does fail all the connectivity is lost. The best solution is a device that fails open in this situation.

The issues noted above can be mitigated by using a network tap instead of a hub. The network tap provides unrestricted data flow and will fail open. Therefore, the tap is recommended to replace the hub. The taps will cost more than the hubs, but the benefit of maximum bandwidth and uptime are important.

Unfortunately, providing hard numbers to the bandwidth and uptime benefits is a guess at best. A summary of the cost impact is provided below.

Summary of Cost Impact (IDS Improvements)

Item	Cost	Quantity	Total (Not Including Tax)
Replace Hubs with Network Taps			
Hub reduction by one due to the firewall consolidation	$ 75.00	1	$ 75.00
Increased cost for taps	$ 175.00	3	$ (525.00)
Total Net Cost			$ (450.00)

5.8: Upper Management Briefing

The healthcare industry is experiencing significant regulatory pressures that mandate prudent Information security and systems management practices. Furthermore, the continued pressure to reduce cost requires that management focus on streamlining operations, reducing management overhead and minimizing human intervention.

The proposed design focuses on all the elements needed to help minimize cost while maintaining prudent security. The following chart shows the benefits the company will gain in the current period implementing the proposed improvements.

Summary of Current Year Benefits

Recommended Improvements	Financial Impact
Improvement in Core Services	**$ 19,317.15**
Central Time Source	$ (63.00)
Account Management Consolidation	$ 20,094.15
Central Logging/Alerting	$ (630.00)
DNS Redundancy	$ (84.00)
Device Optimization	**$ 16,359.35**
Firewalls	$ 13,095.20
HTTP Proxy	$ 3,714.15
IDS Improvements	$ (450.00)
Total Benefit (Year 1)	**$ 35,676.50**

The benefits in the current year are important and provide the largest yearly impact. However, the improvements also provide future benefits from ongoing cost savings. The ongoing cost savings are due to account management

consolidation and http proxy log centralization. The chart below shows the future benefits to the company from ongoing savings.

Future Savings/Benefits

Ongoing Savings Area		Amount
Account Management Savings	$	21,000.00
HTTP Proxy Log Centralization	$	4,368.00
Total Ongoing Savings	$	25,368.00

The following table represents the return on investment (ROI) associated with the improvements. The return on investment has been adjusted to reflect the results in current period dollars by discounting the savings by 5.85% which represents the company cost of capital.

Return on Investment Summary (On Improvements)

Period	Cost Present Value	Savings Present Value	Discount Rate	Savings
0	$ 7,522.40	$43,198.90	N/A	$43,198.90
1		$23,965.99	5.85%	$25,368.00
2		$22,641.46	5.85%	$25,368.00
3		$21,390.14	5.85%	$25,368.00
Totals	$7,522.40	$111,196.49		
	Net Return (Savings - Cost)	$103,674.09		
	Percent Return (Net Return/Cost)	1378%		

The return on investment is an important part of the overall analysis. However, the impact on Total Cost of Ownership (TCO) is just as important. The total cost of ownership reduction includes the ongoing support cost associated with maintaining the system. Therefore, a clear reduction in TCO can be realized with the elimination of the two Cisco PIX firewalls.

The ongoing support cost will be calculated using a very conservative estimate of thirty percent of the initial cost per year. The savings on the initial cost of the PIX firewalls are represented in the ROI analysis above. Therefore, an additional calculation called “TCO Support Reduction” is included to show the benefit not included in ROI. The reduction of TCO related to firewall elimination can be seen in the table below.

Total Cost of Ownership Savings (PIX Firewall Reduction)

Period	Initial Investment	Support Costs (30%)	Growth
0	$13,095.00	$3,928.50	N/A
1		$3,928.50	N/A
2		$3,928.50	N/A
3		$3,928.50	
	$13,095.00	$15,714.00	
	Total TCO Reduction	$28,809.00	
	TCO Support Reduction	$15,714.00	

The improvements to the security design will provide significant benefits in the overall security state, ongoing cost, future maintenance, and regulatory compliance. Furthermore, no changes to corporate policy will be required and the security awareness program will not need to be updated with the proposed improvements.

Conclusion

The proposed network design brought many features which are needed in a healthcare environment. The main areas of agreement were in encrypted external connectivity, minimal need for internal network access, controlled user access to the Internet, multiple security layers, central logging concepts, and some implementation of central user management.

While the overall network design elements were good, the lack of attention to configuration detail, cost savings, overall complexity, and lack of redundancy were not good for a healthcare company. Furthermore, the network design did not address the key configuration decisions which drive cost, uptime, and overall manageability.

Therefore, while I agree with the overall concept of the proposed network design the actual implementation leaves much to be desired. The healthcare industry is heavy on regulations, cost conscious, user access dependent, and uptime is critical. The solution has the right feel, but lacked the depth without significant improvements necessary to be accepted by upper management.

Bibliography

Bauer, Michael D. Building Secure Servers with Linux. Boca Raton, FL. Cambridge, MA: O'Reilly, 2002

Eaton, Ian. The Ins and Outs of System Logging Using Syslog. 14 August 2003 < http://www.sans.org/rr/whitepapers/logging/1168.php>

Grove, Tom. Summary Analysis: The Final HIPAA Security Rule. Feb. 2003, <http://www.hipaadvisory.com/regs/finalsecurity/summaryanalysis.htm>.

The META Group, and PricewaterhouseCoopers. META Group White Paper: The Value of Identity Management. June 2002, <http://www.pwcglobal.com/Extweb/service.nsf/docid/88A387CDB58B4C0085256C6A006E0036>.

Last Updated: May 27th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced