Global Information Assurance Certification Paper

GIAC Enterprises
Internet DMZ Analysis
And Security Recommendations

Information Security Officer Training
GISO Practical Assignment
(Version 1.1 (December 12, 2001))

Submitted By: William M. Curtis
January 17, 2002

GIAC Enterprises Organizational Information

Description of GIAC Enterprises:

GIAC Enterprises is a manufacturing company that produces a relatively small and exclusive line of products. GIAC Enterprises manufactures personal hovercraft vehicles. These hovercrafts retail between three and twelve thousand dollars each and are the primary contributor to GIAC Enterprises four billion dollars a year revenue generation. GIAC Enterprises employs five thousand employees and operates two primary development and manufacturing locations, Phoenix, Arizona and Farmington Hills, Michigan. GIAC Enterprises also has two hundred thirty-six international sales offices and business partner relationships with eighteen companies.

GIAC Enterprises has the responsibility to secure many types of information such as their internally generated intellectual property, employee records, customer records, information that is gathered through on-line e-store transactions, information that is obtained through its business partner relationships and internal classified and confidential documents. To be successful in this venture GIAC Enterprises security policies and procedures must balance the requirement to secure the businesses vital information while being an enabler of the businesses operational activities.

GIAC Enterprises IT Infrastructure:

The GIAC DMZ network infrastructure supports communications for remote and on the road GIAC employees, between GIAC and their business partners, and between GIAC and their customers. [Appendix A should be referred to and accompanies the following DMZ network infrastructure component descriptions] The ability for the business to communicate at all the levels identified above weighs very heavily on the design and implementation of the organizations network DMZ. The process of designing and implementing the network DMZ should not be entered into lightly and improper design or implementation could result in the compromise of the data that is at the heart of GIAC Enterprises success. The following are core elements of the GIAC network DMZ:

- *Internet Border Router* provides for an initial level of security through the use of Access Control List's and source NAT'ing.
- *Remote User Virtual Private Network (VPN)* establishes a secure method for remote communications with GIAC employees and business partners through the use of Checkpoint's SecurClient VPN. GIAC's implementation forces the remote user to install a 'outgoing & encrypted' security policy on their remote system, allows for only 3-DES encryption, requires the use of IKE and uses two factor authentication via SecurID from

RSA Security. All communications to and from GIAC Enterprises are via an encrypted tunnel.

- *Site-to-Site VPN* allows for the extension of the GIAC Enterprises network to remote GIAC offices and exclusive business partners. The Site-to-Site tunnel is established with Cisco hardware on both ends and then passed through a stateful inspection firewall prior to entering the GIAC network.
- *Internet Facing Firewalls (Stateful Inspection)* provide for security separation between the Internet, DMZ ONE and the Intranet Facing Firewalls (Packet Filter). Traffic initiated from the Internet will pass into this firewall and will only pass onto DMZ ONE. Servers in DMZ ONE can either respond to an Internet initiated communication or communicate directly to a server in DMZ TWO. No Internet traffic will ever be allowed to pass directly to DMZ TWO or the GIAC Intranet.
- *Intranet Facing Firewalls (Packet Filter)* provide for security separation between the Internet Facing Firewalls, DMZ TWO and the GIAC Intranet. DMZ ONE servers can request information from a server in DMZ TWO as well as the GIAC Intranet. The GIAC Intranet can in turn communicate with DMZ ONE, DMZ TWO or the Internet.
- *DMZ ONE Network Space* – Systems that will be placed into this security zone will be communicated to directly from the Internet. Included in DMZ ONE will be such services as SMTP, External DNS, anonymous and secured FTP, HTTP, and HTTPS. As these servers will be vulnerable to attacks from the Internet they will be required to be meet a stringent set of requirements prior to being placed into this network space. Examples of these requirements are server hardening, vulnerability scanning and OS and Application maintenance. The details of these requirements will be drawn out further in the section of this document that addresses security policies and procedures. DMZ ONE servers will not be permitted to store customer sensitive or personally identifiable information such as name, address, social security number, credit card, etc.
- *DMZ TWO Network Space* – Systems that will be placed into this security zone will only be communicated to either by systems in DMZ ONE or from the GIAC Intranet. The purpose for DMZ TWO is to provide a separation network between the web servers in DMZ ONE and the third-tier database and mainframe servers in the GIAC Intranet. Servers in DMZ TWO will be authorized to process and temporarily store customer sensitive or personally identifiable information such as name, address, social security number, credit card, etc. Long-term storage of this information will take place on database servers located within the GIAC Intranet.

The GIAC DMZ Network Infrastructure was designed to:

- Be fully redundant between the Phoenix and Farmington Hills locations in the support of e-business communications. Confidentiality, Integrity & Availability are essential.
- Employ security zones to further secure information within the network DMZ space. Security zones are also implemented within the GIAC Intranet network to control access to critical business systems found within the engineering, human resources, and finance departments.
- Provide defense in depth security as a strategy that enables protection, detection and reaction. The specific elements used to secure the GIAC Enterprises DMZ network

included router access control lists, stateful inspection and packet filter firewall policies, placement of web and application servers into separate security zones, intrusion detection, host based security and anti-virus software activation. DMZ traffic analysis is a critical component of the overall defense in depth model. GIAC Enterprises made the decision to outsource the review and correlation of the estimated six gigabits of log traffic generated daily. Within the policy and procedures sections of this document we will discuss the requirements that have been established concerning the review process and how what is reviewed will be handled and if necessary communicated to GIAC Enterprises.

In addition to the detailed design efforts that went into the GIAC Network DMZ an understanding of the necessary policies and procedures for additions to and the maintenance of the space were outlined. Management of the GIAC Network DMZ does not stop at the completion of the design and its implementation. The DMZ was designed to house computer systems and to enable those computer systems to conduct the companies business across the Intranet and Internet networks. The challenge to the GIAC Enterprises IT Security Department is to provide data confidentiality, integrity and availability. As the GIAC Enterprises DMZ policies and procedures were drafted the following questions were considered:

- What standards will a new system being added to the DMZ be measured against prior to its addition? How are we to be assured each new system meets the established system hardening standards? How do we ensure security compliance throughout the DMZ?
- How are we to ensure the newly added piece of equipment is secure and does not possess security vulnerabilities that could be exploited by an Internet or Intranet hacker?
- How is the DMZ network space managed? Who will manage the infrastructure equipment? Who will manage the business web and application servers? How will GIAC Enterprises know systems in the DMZ are fully compliant with the latest levels of OS and application patches? How will the reporting of these statistics be managed?
- How will the DMZ space be monitored? How will reporting of incidents be handled?
- How will GIAC Enterprises respond to suspicious activity alerts?
- How will critical system log files be maintained and processed?
- How will the activities of the GIAC DMZ be reported to management?
- What management is required on a daily, weekly and monthly basis and who will perform that management? Will these tasks be outsourced? Will the GIAC Enterprises IT personnel complete them? Will GIAC Enterprises use a combination of both?
- GIAC Enterprises DMZ management personnel were not operating in conjunction with their systems and application development teams and as a result the introduction of new DMZ systems would be delayed. It would take several days and at times weeks to properly audit, harden and prepare these systems. Who was responsible to eliminate this un-necessary delay? How was the DMZ management team going to get in front of the systems and application development process?

GIAC Enterprises answer to some of these questions will be outlined in the policies and procedures section of this document.

GIAC Enterprises Business Operations:

GIAC Enterprises instituted a product development, sales and customer support business model that presented many challenges to the GIAC Enterprises IT organization. Product development was a coordinated effort between the Phoenix and Farmington Hills development centers and several outsourced engineering organizations around the country. Sales activities took place at the two hundred and thirty-six offices but these offices do not operate independently. Sales support activities are equally as important to the organization as product development and manufacturing. GIAC Enterprises values their customers and works hard to implement a customer support environment second to none. GIAC Enterprises raised the bar very high and as a result the following IT security operational business requirements surfaced:

- Secured data transmissions. All data that GIAC Enterprises generates and transmits while collaborating with development business partners, while GIAC Enterprises staff is on the road and while doing business with their customers must be secured. No development related or confidential data transmitted between GIAC Enterprises and its employees or business partners will be transmitted in the clear.
- Remote user access via a VPN. All individuals (GIAC Enterprises employees or business partners) needing access to the GIAC Enterprises business network will be required to utilize the GIAC Enterprises remote user VPN solution. The solution that has been implemented is a Checkpoint SecurClient VPN operating on a Nokia network appliance. The established connection will require a policy to be pushed down to the remote users desktop computer, will require the use of IKE, will require 3DES and will require two-factor authentication using RSA SecurID technology. Further, GIAC Enterprises has taken a position, and has documented this position in a corporate policy, that no modems will be installed in the GIAC Enterprises network for the purpose of remote access dial-in. Violation of this policy is grounds for immediate dismissal. Exceptions must be reviewed by the Director of Information Security and must then be signed off by a business officer at a Vice President or above level.
- Remote site access via a Site-to-Site VPN. For locations that are considered to be a small office (remote sales offices or remote business partner locations) connection to the GIAC Enterprises business network will be through a Cisco Site-to-Site VPN. The secure tunnel will originate at the remote location, will incorporate 3DES encryption standards, and will terminate at a router within the GIAC Enterprises DMZ network. Prior to then entering the GIAC Enterprises LAN the connection will then pass through a stateful inspection Checkpoint firewall.
- Real-time video & audio conference, instant messaging and meeting collaboration. All collaboration activities with locations outside of the main GIAC Enterprises development and manufacturing location will be conducted via either one of the two VPN methods identified above.
- Limited access to development tools and code. Business partners collaborating with

product development teams within the GIAC Enterprises development environment will have their access controlled through system level, file level and where appropriate object level security. Account ids will be assigned and passwords will be maintained per the policy, which addresses password management.

- Access to GIAC Enterprises for email, file services, Intranet web services, and other internal GIAC network offerings. All authorized employees who require access to internal GIAC Enterprises computing services and are not physically located at either one of the two development and manufacturing locations or a remote sales office which has Site-to-Site VPN capabilities will be required to connect to the GIAC Enterprises network via the authorized remote user VPN solution.
- On-line product ordering. The GIAC Enterprises product catalog is available to all Internet users for review and product purchase. Customer confidential information such as personal information, credit information, purchasing preferences will all be accepted on the web server, processed on the application server located in DMZ2 and stored on the database server secured within a fire walled network zone within the GIAC Enterprises internal network. All communication will be secured and the data stored on the backend database will be encrypted.
- Web access to on-line customer support. The GIAC Enterprises DMZ will provide on-line web services to allow customers access to product support information.
- Secured and anonymous sites for transferring data to and from GIAC Enterprises. The GIAC Enterprises DMZ will provide both secured (ID & Password) and anonymous FTP services. These services will enable customers, business partners and GIAC Enterprises employees the sharing of data files. The secured FTP server will retain data for no longer than 14 days. The anonymous FTP server will hide all directory contents and will remove all data files after 48 hours.

GIAC Enterprises Organizational Risk Assessment And Security Policies

GIAC Enterprises Areas of Security Risk:

The GIAC Enterprises organization information provided above presents security concerns in several areas. Some of these security concerns if not addressed would present a high level of risk for the business. Is the risk that GIAC Enterprises faces quantitative or qualitative? To assist in answering this question the following information is provided.

Quantitative Risk Analysis:

This approach employs two fundamental elements; the probability of an event occurring and the likely loss should it occur.

Quantitative risk analysis makes use of a single figure produced from these elements.

This is called the 'Annual Loss Expectancy (ALE)' or the 'Estimated Annual Cost (EAC)'. This is calculated for an event by simply multiplying the potential loss by the probability.

Qualitative Risk Analysis:

Most qualitative risk analysis methodologies make use of a number of interrelated elements:

THREATS

These are things that can go wrong or that can 'attack' the system. Examples might include fire or fraud. Threats are ever present for every system.

VULNERABILITIES

These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire vulnerability would be the presence of inflammable materials (e.g. paper).

CONTROLS

These are the countermeasures for vulnerabilities. There are four types:

1. *Deterrent controls reduce the likelihood of a deliberate attack.*
2. *Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact.*
3. *Corrective controls reduce the effect of an attack.*
4. *Detective controls discover attacks and trigger preventative or corrective controls.*[1]

Risk that if not managed could result in the loss of reputation, revenue, and customer or business relationships. Of the security concerns that exist five that present a high degree of risk will be identified and each will be discussed in detail. These five areas of security risk are:

1. Management of the GIAC Enterprises DMZ network infrastructure.
2. The addition and management of business systems into the GIAC Enterprises DMZ.
3. Intrusion detection, reaction and management.
4. Security personnel knowledge and certifications.
5. Secure transmission and storage of key GIAC Enterprises data.

Management of the GIAC Enterprises DMZ network infrastructure:

[1] C & A Security Risk Analysis Group

The process by which business DMZ networks come to be is often times where significant interest in the design and implementation exists. The time spent in researching and evaluating the necessary components, purchasing, configuring and installing will be considerable. After the DMZ is functioning the project will be completed, interest will lessen and in many cases this is where the significant risk can begin.

Why is this risk of particular concern to GIAC Enterprises? Special attention needs to be given to the network space that separates the public Internet from the private Intranet and houses many critical business systems. The absence of proper management can result in critical defenses being weakened or made ineffective. If a component of the businesses DMZ space was successfully exploited the business would suffer from loss of revenue, loss of intellectual business data, defacement, compromise of customer information and in a worst case scenario the business would find itself in a court of law as a defendant. Proper management of this space will reduce the risk and involves elements such as security personnel with the proper training and experience, technology that will securely enforce the required business policies, regular operating system, application and hardware support practices and monitoring and reaction procedures for suspicious activities. The DMZ network space is a serious business asset and if management activities are not taken seriously the business will experience loss.

To mitigate the risks identified above the following steps should be considered and implemented as appropriate within the business:

- Inventory all infrastructure equipment within the DMZ. Include as many details such as OS and APP versions, serial numbers, maintenance contracts, locations, support contacts, etc.
- Assign qualified individuals the direct responsibility for maintaining the inventory. UNIX systems within the control of UNIX administrators, NT systems with NT administrators, etc.
- Assign qualified individuals with the responsibility to ensure all necessary OS and APP upgrades and patches are applied and firewall policies are regularly reviewed and managed. Consider the use of a product such as Symantec's Enterprise Security Manager (ESM). ESM provides scalable security assessment and policy management.
- Establish a DMZ systems maintenance window when all systems will be considered unavailable and the outage will be for the express purpose of applying the necessary system upgrades, patches, replacements and additions. If a business system is critical enough that it cannot accept a window of unavailability then the business unit who is responsible for this system must introduce an alternate system that can go active while this maintenance window is open. These sorts of issues must be drawn out during the interview process that must precede the addition of any system or application to the production DMZ. This interview activity is discussed in further detail later into this document.
- Perform regular system scans to determine if vulnerabilities exist and to ensure regular systems and application maintenance is taking place.

The addition and management of business systems into the GIAC Enterprises DMZ:

The management of business systems such as web and application servers is essential and should employ the same steps as identified above in the previous outlined risk of managing the DMZ network infrastructure. As for the addition of new business systems within the already established DMZ network infrastructure care must be exercised to ensure the system fits within the established security guidelines and does not pose a threat to other business systems or the DMZ infrastructure.

Earlier in this document a question was asked -- *How was the DMZ management team going to get in front of the systems and application development process?* This question was asked in response to a problem with system delays going into the DMZ. This question directly relates to the risk at hand. If a DMZ bound business system has been under development for several months or even a year or more and the project has approached implementation only to find that the system fails at the security review how has the business worked together to provide for success. It is in this scenario that the risk exists. How will the organization mitigate this risk?

The DMZ management team must get in front of the applications and systems development processes within GIAC Enterprises. A system/application interview must take place between the business unit representative requesting entry into the DMZ and a member of the Information Security Team. During this interview the business unit representative must understand the business security requirements and the security team member must understand the requirements for the new system/application. Once this information has been shared progress can be made to certify the system or application. More details on this process are presented further into this document.

An example of successful communications during this interview process - If the application team knows that the only way HTTP is going to pass through the DMZ firewalls is on port 80 and not on a custom port that the application team felt appropriate this information will assist in avoiding a delay. If the application team has a new proprietary protocol that must exist for the web server in DMZ1 to talk to the application server in DMZ2 then time must be given for that protocol to be researched. Is the protocol already accepted as an industry standard and therefore is registered within the firewalls rule sets? If not is there an alternative protocol that could be used that is industry accepted? If not can the protocol be externally secured by another application or process? If the answer is still no then GIAC Enterprises management will need to make the decision to either accept the risk of allowing the protocol or not. The application team must be given the time necessary to properly prepare for their application architecture's introduction to the secured DMZ network space.

Intrusion detection, reaction and management:

Knowing that an intruder is banging on your front door or worse yet has made their way into the house is information that we are all better off having. If we do nothing with that information we are in fact no better off than is we had not had it at all. With our DMZ network space the story is quite the same with one minor difference. We need to implement the detection mechanisms that will give us the information necessary to signal an attempted attack or illegal

entry into our systems or networks. Successfully exploiting a business by repeatedly attacking its perimeter or by passing beyond the perimeter and accessing the vital DMZ systems could result in significant loss to a business. This loss could be represented in many ways. A few of these could be harmful to the businesses reputation, could cause the business to involuntarily cause network disruptions or data loss to another business, could cause a loss in business revenue or could cause loss of business or customer confidential information.

Businesses today rely on the Internet for the instant partner and customer collaboration needed to maintain a competitive advantage. The same open and flexible nature of the Internet that drives e-Business growth, however, also renders corporations vulnerable to debilitating computer security breaches. Companies can be attacked from any Internet connection, via seemingly secure extranet connections, or from internal elements. Security breaches can take many forms, including targeted hacking, data theft, sabotage, and random acts of computer vandalism. A successful attack can spark a chain reaction that begins with a breach of proprietary data, and may lead to a degradation of customer confidence and significant revenue loss. Recent FBI/Computer Security Institute findings reveal that more than 70% of U.S. corporation and government agencies reported security breaches in 2000, underscoring the urgent need for business information security protection.[2]

Risk here is presented in two areas. This first is risk associated with never listening for the suspicious activity. Instead by not being aware and assuming the installed security devices are without fault we accept this risk as managed when in fact it may be far from. The second risk is equally significant. This risk is found in the implementation of detection mechanisms with no procedure to review, no procedure to react, or no ability to tune a system to reduce the occurrences of false-positives. Implementing the processes to monitor suspicious activities and equipping the security staff to respond to those activities is as important to a businesses security posture as implementing the detection mechanisms in the first place.

To address the first of the two security risks identified in this area we will discuss how detection of suspicious network and systems activities are observed. Suspicious activity detection or intrusion detection is accomplished in several ways. A few of these ways are described here. To provide for a complete detection environment a complement of these detection methods are recommended.

- Log file activities – The data that passes through border routers, firewalls, proxy servers, web and application servers and Intrusion Detection Systems (IDS) is all logged to system logging files. On average ninety-five percent of this logged data is a result of normal day-to-day business activities. It is critical that these log files are reviewed regularly and activities that are categorized suspicious investigated. Equally important is the rotation and storage of these very large system files. It is estimated that the GIAC Enterprises system logs are generating 2.5 gigabits of data per day. The log files must be made available with either on-line or near-line storage for up to one year beyond the date the data was recorded. It is also critical that this data be made available for up to ten years

[2] http://www.riptech.com/services/index.html

beyond the date the data was recorded for the purpose of criminal investigations.

- Host based IDS – Allows for the detection of suspicious system and application activities on individual hosts. Host based IDS can be tuned to look at very specific information that pertains to an individual system. The logging will generate large amounts of data and this must be managed for content and must be stored similar to the specifications mentioned above for system log files.
- Network IDS – Provides for an overall analysis of the traffic that will pass across the network segment the IDS device is listening on. The Network IDS device will monitor the flow of data at wire speeds and is placed, as shown in Appendix A, just prior to and just after critical network entry points and critical network security devices.
- Integrity checking of information systems – Tripwire for Servers enables you to establish network policies that detect intentional tampering, user error, software failure, and introductions of malicious software, as well as "open doors" for robust protection of critical systems. Tripwire for Routers and Switches provides an integral layer in your networking security infrastructure. Changes in a router or switch configuration file can seriously disable network operations, leading to widespread network outages and high costs associated with lost productivity, lost revenue, and lost customer confidence. To tie these Tripwire components together Tripwire Manager is a fully functional, cross-platform management console that allows you to easily manage all installations of Tripwire for Servers across an enterprise network. Tripwire Manager eliminates the need to manually monitor multiple discrete network platforms and point solutions. Instead, you have a comprehensive view of data and network integrity status from a single, centralized console. Tripwire Manager saves time by pinpointing integrity violations and reduces management costs by providing rapid access to detailed reports and actionable data.[3]

The second of the two security risks within the area of intrusion detection, reaction and management is the reaction and management component. All best intentions aside if properly trained personal are not assigned full time responsibility for this task the attention needed to properly manage this space will not be given. The work required for the review and aggregation of system, host and network IDS logs is significant. GIAC Enterprises has decided to outsource this activity to a company that manages this space not only for GIAC Enterprises but also many other companies with similar sized network DMZ's. There are several advantages to this outsourced relationship. The company with the contract assigns analysts to continually monitor the network activity of several companies. This often times will allow the analyst the edge of early detection of a suspected network attack (attacks will move from the east to the west coast) With this early information the analyst can advise the necessary contacts at the companies for which the logs are being reviewed to apply countermeasures to lessen or eliminate the impact of the activity. With this important task being professionally managed GIAC Enterprises will have the personnel and time necessary to address the many other security concerns that require equal attention.

Security personnel knowledge and certifications:

[3] http://www.tripwire.com

The personnel who manage the GIAC Enterprises DMZ network space are given great responsibility and operate with many different technologies to make the whole process come together. For GIAC Enterprises to receive the most out of their investment they must place great emphasis on the knowledge and ultimately the capabilities of their support staff. The engineers, specialists, analysts and programmers all should pursue technical education that results in certification testing of their acquired knowledge. It is the responsibility of the GIAC Enterprises management to ensure the training budget for the technical security staff is sufficient to meet this requirement. For a year worth of training 8-10 thousand dollars should be allocated for each member of a technical security team. As your security team is educated and certified their level of knowledge will allow for through management of the DMZ space.

When interviewing for additional staff to compliment the DMZ security team the position requirements should not only look for experiences but also industry certifications. The decisions the DMZ security staff will need to make have considerable circumstances.

If the technical security staff at GIAC Enterprises is not properly trained the decisions made by these employees could compromise business practices thus making vulnerable the computing environment of the businesses DMZ network. Uneducated decisions could have a snowball effect if not monitored and not corrected. Periodic internal audit of the technical security function should be a checkpoint for GIAC management to better understand the security happenings within this network space.

The capabilities of the technical security personnel as well as the rest of the organization to respond to information security threats are an issue that must be addressed. GIAC Enterprises found that during the year 2001 outbreaks of Code Red, Code Blue & Nimda that the organization was not prepared to manage this environment. The outbreak caused several hundred machines to become infected and the process by which the GIAC Enterprises recovered was a "learn as you go" approach. GIAC Enterprises management has taken the steps to ensure future malicious code outbreaks are contained and resolved as quickly as possible. The business management decided to establish a malicious code emergency response team. This team would be given the primary responsibility to stay current with malicious code incidents, detection tools, reaction techniques and when the next outbreak takes place within GIAC Enterprises this group would lead the internal assault. In preparing to take on this role the team would also focus on:

- Team drills.
- Identification of team roles and responsibilities.
- Identification of additional IT resources roles and responsibilities.
- Development of incident response procedures.
- Preparedness drills.
- Team training standards.
- Audit trail guidelines.

Secure transmission and storage of key GIAC Enterprises data:

With GIAC Enterprises relying on day-to-day communications and project collaboration with businesses partners and employees at remote sites the business must find a secure means to transmit, process and store its information. If GIAC Enterprises does not secure the communication processes and the data that is being shared they run the risk of significant business losses. Unauthorized use or release of customer information and business intellectual property would both cause the business revenue loss and possible legal implications.

There are two security concerns to be discussed here. How will GIAC Enterprises secure their Internet based business communications and how will they secure the information that is generated as a result.

The Internet based business communications, as described earlier within this document, will employ site-to-site VPN technologies. The communications will utilize IPSec tunnels. IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.[4]

Data processing of web information within the DMZ network will take place within the DMZ2 security zone. By restricting the communication into this network space to only the web servers in DMZ1 or the GIAC Intranet servers that require access we have provided a level of access security to protect the data. For application processing within the GIAC Enterprises intranet separate network security zones have been established and access is controlled on an as needed basis.

GIAC Enterprises Security Policies:

A security policy is the set of decisions that, collectively, determines an organization's posture toward security. More precisely, a security policy determines the limits of acceptable behavior, and what the response to violations should be.[5] In this section of the document security policies that will aid the GIAC Enterprises organization in managing the risks identified above will be presented.

GIAC Enterprises Security Policy GIAC-POLICY001

Management of the GIAC Enterprises DMZ Network Infrastructure

Purpose: This policy is being established to provide guidelines by which the support

[4] Cisco Systems On-line Documentation, Configuring IPSec Network Security
[5] Cheswick, R. William & Bellovin, M. Steven

maintenance for the systems located in the DMZ network space will be managed.

Scope: This policy will apply to the owners of both the DMZ infrastructure equipment (firewalls, routers, switches, caching servers, etc.) and DMZ servers (customer web and application servers). In addition this policy will establish the procedures by which the equipment in the DMZ will be managed. Details to be included will be:

- Policy for providing maintenance of the systems in the DMZ
- ❖ Policy for inventorying the systems within the DMZ
- o Policy for performing regular system vulnerability scans

Policy Statement:

- To properly allow for the continued operation of the systems within the GIAC Enterprises DMZ time must be allocated for scheduled systems maintenance. All business owners of the web and application servers as well as the Technical Security Team must implement their systems with this scheduled outage in mind. There will be no exceptions to this systems outage and maintenance window. During this scheduled time upgrades and patches to operating systems and applications can be applied, vulnerability scans completed or any other system or application level maintenance performed.

- ❖ All equipment placed into the GIAC Enterprises DMZ will be inventoried prior to entry. This information must also be maintained and will be checked for accuracy twice a year.

- o All systems destined for the GIAC Enterprises DMZ network are first hardened and scanned for known vulnerabilities. These vulnerability scans will also be performed at a minimum twice a year. The purpose for this vulnerability scan is to ensure the continued security of the services in the DMZ through regular maintenance.

Responsibility:

Review and Modification: The individual elements of this GIAC Enterprises policy will be reviewed and modified as necessary by the Director of Information Security for GIAC Enterprises.

Compliance: The responsibility for review and insurance of compliance of this and all policies within the GIAC Enterprises organization is the Office of the Director, Internal Audit. In addition compliance with this policy is the responsibility of each employee operating within the DMZ network.

- The responsibility for ensuring compliance of and establishing the definition of the scheduled maintenance windows falls to the Manager of Security Operations. The

analysts reporting to the Manager of Security Operations will have the responsibility to schedule and perform the required maintenance activities.

- ❖ Inventorying the systems within the DMZ is the responsibility of the analysts who report to the Manager of Security Operations. These same analysts are also responsible for the bi-yearly audit to ensure the inventory is being maintained.

- o Performing the vulnerability scans of the business web and application servers in the DMZ if the responsibility of the server owner which the web or application resides. Ensuring compliance with this policy will be the responsibility of the Manager of Security Operations and the analysts that report to that position.

Action:

- ▪ To prepare for the scheduled outage maintenance window the business or IT analyst will identify the applicable OS and application upgrades or patches and stage them for installation. The IT analyst will also at this time review the health and well being of the server to ensure optimum operation.

- ❖ Electronic inventory forms will be created and will be made available for use by the owners of the systems located within the DMZ. The analyst reporting to the Manager of Security Operations will consolidate this information into a single database and provide inventory report as required. The inventory will include hardware as well as software information to include versions, patch/firmware levels, maintenance information, etc.

- o The maintenance outage window will allow for time to scan the operating system and applications on the servers within the DMZ. A rotation of the servers to be scanned will need to be established, as all servers cannot be scanned all the time. These scans will be used to ensure the systems do not exhibit a known vulnerability, are patched to the current level and are also in-line with the inventory information being maintained.

GIAC Enterprises Security Policy GIAC-POLICY002

Addition and Management of Business Systems Into the GIAC Enterprises DMZ

Purpose: This policy governs the procedures by which a new system is added to the existing GIAC Enterprises DMZ network.

Background: Systems destined for the GIAC Enterprises DMZ in the past have been delayed in their implementation. The primary reason was the lack of communications between the application/system development team and the information security team.

This type of delay is avoidable. It is the intention of this policy to ensure that happens.

Scope: This policy will cover security team involvement in project meetings, the preparation of technical security project documentation, the availability of a test lab to verify security compliance and a formalized documentation approval process.

Policy Statement: This policy will ensure:

1. the system is inventoried and that information recorded.
2. the security guidelines are documented and made available to any systems development team for incorporation into their initial project documentation.
3. a detailed system communications diagram is provided for review to ensure compliance with the established security guidelines.
4. a security test environment will exist that is identical to the production DMZ that allows the systems development team the ability to test their systems for compliance. In this test lab environment system functionality as well as vulnerability should be reviewed.
5. upon completion of all system reviews and subsequent approvals documentation will be completed to show the acceptance. As the systems prepare to enter the DMZ ensure the process that was followed to ensure preparedness has been captured for later review (if necessary).

Responsibility:

The analysts reporting to the Manager of Technical Security Operations will ensure:

- Inventory of DMZ systems completed and current
- Technical security guidelines provided to application teams at project launch
- Security test lab built and maintained to include scheduling and configuration changes

The project lead or other business representative for the incoming DMZ application will ensure:

- Project complies with security guidelines established by Technical Security
- System destined for the DMZ lab has been thoroughly tested within the test lab
- All necessary documentation has been completed, signed and recorded with the official project documentation.

Action:

- The inventorying of all equipment destined to the DMZ network space must be completed and reviewed prior to the enabling of the necessary firewall rules enabling the application to communicate.
- Review of all inventoried systems will be completed twice a year, at a minimum, and will be completed during the scheduled maintenance outage windows.

- Detailed process communication documentation must be provided to the technical security organization prior to testing of the systems within the security test lab.
- Owners of systems destined for the DMZ must have complied with all requirements set forth by the technical security organization and must have successfully completed system testing within the authorized security test lab prior to being allowed into the production DMZ network. The filing of project documentation with the program management office must also be completed prior to addition to the DMZ.

GIAC Enterprises Security Policy GIAC-POLICY003

Intrusion Detection, Reaction and Management

Purpose: This policy establishes the procedures to be used within the GIAC Enterprises DMZ network to monitor the flow of traffic and react as necessary to suspicious activities.

Background: Twelve months ago GIAC Enterprises invested in IDS technologies and implemented ISS RealSecure on Nokia network appliances. The project plan completed on schedule but when all was done the organization realized they had never fully considered the tasks associated with reaction and management. This policy will address first these two areas then the review and management of the firewall logs, host based IDS logs and finally integrity checking of the information systems in the DMZ.

Scope: This is an activity analysis policy and will address the management of network traffic into, through and out of the DMZ network. All applications placed in the business DMZ are subject to the inspection of traffic destined to and originating from their systems.

Policy Statement, Responsibility & Action:

The first item to be addressed will be the monitoring and management of network & host based IDS and firewall logs and the reaction to suspicious activities.

- Policy Statement:
  - GIAC Enterprises has entered into a maintenance agreement with Riptech to provide the monitoring of all DMZ IDS and firewall logs. Riptech will analyze the data and will alert GIAC Enterprises of any activities that are considered critical. This alert process and the overall review of the logs will follow an agreed upon Service Level Agreement (SLA) entered into between the two companies.
  - GIAC Enterprises will provide the response team to react to the alerts from Riptech. GIAC Enterprises will also manage on-site copies of all log files sent to Riptech for review.

- Responsibility:
  - This policy can be reviewed and recommendation for changes submitted to the

Manager of Security Operations. Responsibility for log aggregation, log storage and incident reaction are outlined above.

- Action:
  - Riptech log monitoring and alerting is a 24x7x365 operation. Riptech will submit a daily report each weekday by 8:00 a.m. CST and a monthly report by 12:00 p.m. CST the 1st of each month. If the 1st is a weekend or holiday the report will be due the following business day.
  - GIAC Enterprises will have a incident reaction team available 24x7x365 to address any suspicious activities reported by Riptech.
  - GIAC Enterprises will ensure the hourly rotation of all IDS and firewall logs to near line storage.

The second item to be addressed will be the monitoring and management of the Tripwire integrity checking tools.

- Policy Statement:
  - This policy will provide for the monitoring and analysis of critical system files on servers as well as network devices.
- Responsibility:
  - The primary administrator assigned to the system will perform the daily review of all systems equipped with Tripwire technologies. Reporting of the alerted activities will be forwarded to the on-call technical security analyst.
- Action:
  - Reviews of the Tripwire system reports will take place each morning and the report consolidated and sent to the on-call security analyst by 12:00 p.m. CST. For alerts that require immediate attention the primary administrator will respond to the issue and request the assistance of the on-call security analyst as needed.

GIAC Enterprises Organizational Security Procedures

GIAC Enterprises Security Procedure GIAC-PROCEDURE001

The following procedural document will outline how the GIAC Enterprises policy *GIAC-POLICY002* is to be implemented.

Scenario for which this procedural document will be executed:

A representative from one of GIAC Enterprises businesses approaches the GIAC IT Security group requesting assistance with introducing a new computer system/application to the GIAC DMZ network.

Steps to follow in response to the above scenario:

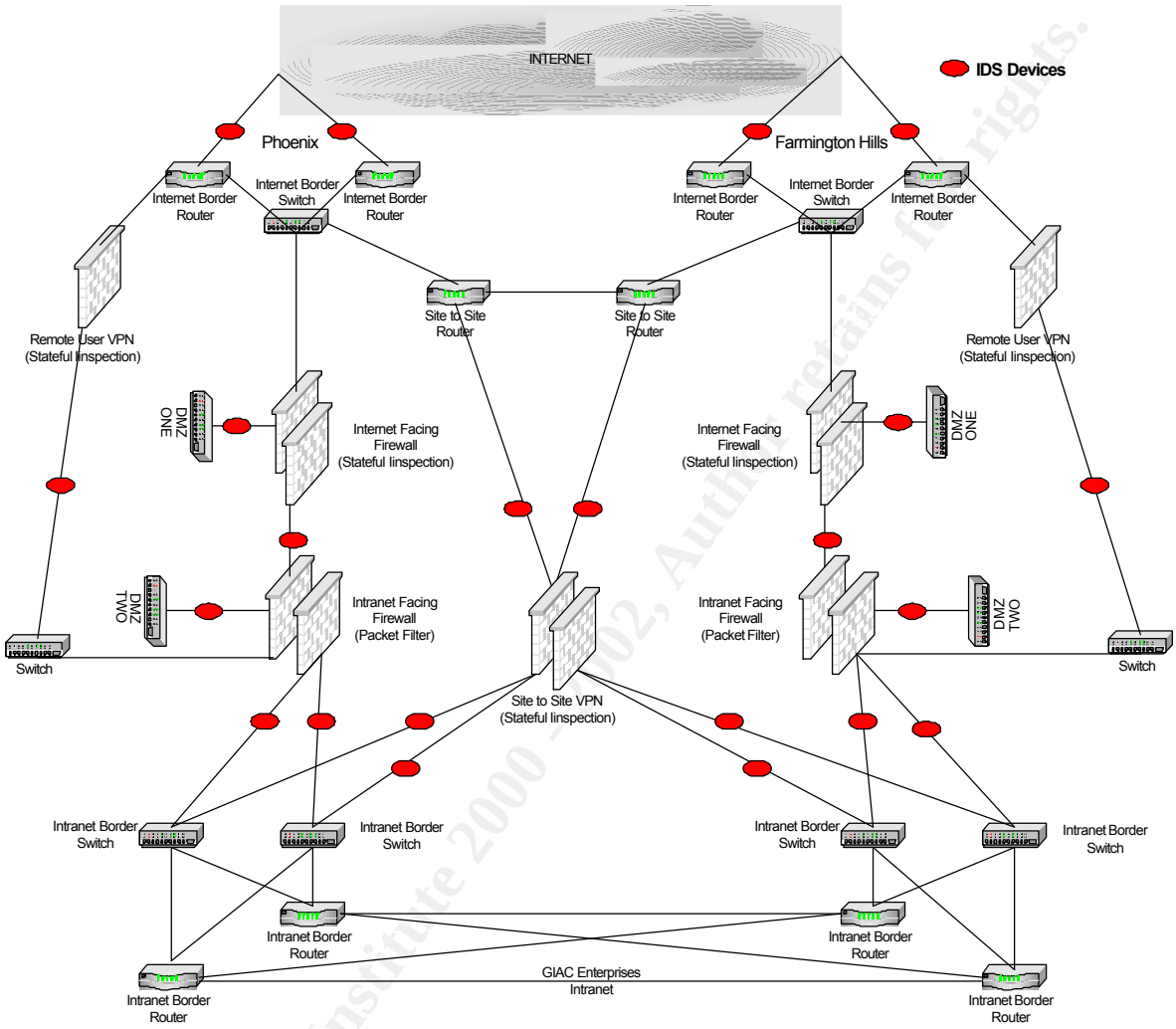
1. Provide the business representative a copy of the inventory document. The document will be completed and entered into the GIAC Enterprises Security Asset Database. The collection of this information is essential to allow the managers of the GIAC DMZ space to understand at all times what systems and applications exist. This inventory provides critical information such as the application or system owner, services running, equipment and software types (OS & application releases, patch levels and manufacturers), other systems and applications communicated with, etc.
2. A member of the GIAC Enterprises Technical Security team will meet with the business representative and conduct an initial security interview. At this interview the business representative will introduce the basic principles of the system to be added to the DMZ. The security team member will take notes and open a security compliance folder on the business system/application. The security team member may ask for additional information or documentation to be added to the created folder. The security team member will also be listed on the project documentation as the security contact throughout this entire process. This interview is important because it provides for the sharing of critical information between both the provider of the IT service and the business representative that is the IT customer. This interview will contribute to the overall success of the customers project.
3. The security team member will then provide the business representative with a copy of the established security guidelines governing the introduction of servers and systems into the GIAC Enterprises production DMZ. This information will ensure the business representative understands what security requirements must be met prior to the addition of the system or application to the production DMZ.
4. When the business unit introducing the new system is ready to evaluate the system for security compliance a request will be made to the technical security contact assigned during the initial interview for time in the security test lab.
5. The business unit will enter into the test lab and with the assistance of the test lab operator will as thoroughly as possible exercise the system/application checking for compliance with the established security guidelines. The test lab models exactly the production DMZ. If the system/application passes the security checks the system will also pass security checks in the production DMZ. This step is critical to ensure time is not wasted in introducing a new system/application to the production DMZ.
6. After the system/application has passed the test lab evaluation the following documents will be gathered by the technical security contact and will be signed off by both the business representative and the security contact then added to the official project security folder:
    a. Application security compliance checklist
    b. Test lab summary report
    c. Security acceptance document
    d. Firewall modification request form

    This step is essential to ensure all the necessary steps have been completed and results accepted by both the business representatives and the security organization.

As this procedure is executed it will be the responsibility of the Manager of Security Operations to periodically review the security compliance folder. Any missing documents or missed procedure steps identified will cause the project to immediately go under a security audit review. The security team member and business representative will meet with the Manager of Security Operations and the missing information will be provided.

If the security organization is going to be an enabler of the business process of adding systems and applications to the DMZ then this procedure must be followed to the letter. Compliance is a requirement.

Appendix A – GIAC Enterprises Network Design



Appendix B – GIAC DMZ Equipment Inventory

GIAC Enterprises
Internet DMZ Inventory

	Platform	Model	OS	OS Version	Software	Software Version	Services and Applications
INTERNET BORDER							
Internet Border Router (PHX)	Cisco	7206	IOS	12.0.20			Router ACL
Internet Border Router (PHX)	Cisco	7206	IOS	12.0.20			Router ACL
Internet Border Router (FH)	Cisco	7206	IOS	12.0.20			Router ACL
Internet Border Router (FH)	Cisco	7206	IOS	12.0.20			Router ACL
Site-to-Site Router (PHX)	Cisco						Router ACL
Site-to-Site Router (FH)	Cisco						Router ACL
Internet Border Switch (PHX)	Cisco	3548	IOS				
Internet Border Switch (FH)	Cisco	3548	IOS				
Remote User VPN (PHX)	Nokia	IP650	IPSO	3.4	Checkpoint FW-1	4.1 SP5	Checkpoint Firewall-1
Remote User VPN (FH)	Nokia	IP650	IPSO	3.4	Checkpoint FW-1	4.1 SP5	Checkpoint Firewall-1

	Platform	Model	OS	OS Version	Software	Software Version	Services and Applications
DMZ ONE							
Internet Facing Firewall - VRRP Pair (PHX)	Nokia	IP650	IPSO	3.4	Checkpoint FW-1	4.1 SP5	Checkpoint Firewall-1
Internet Facing Firewall - VRRP Pair (FH)	Nokia	IP650	IPSO	3.4	Checkpoint FW-1	4.1 SP5	Checkpoint Firewall-1
SMTP Server (PHX)	SUN	Netra	Solaris	2.7	Sendmail	8.12.1	SMTP Mail Relay
SMTP Server (FH)	SUN	Netra	Solaris	2.7	Sendmail	8.12.1	SMTP Mail Relay
DNS Server (PHX)	SUN	Netra	Solaris	2.7	BIND	9.2.0	External DNS
DNS Server (FH)	SUN	Netra	Solaris	2.7	BIND	9.2.0	External DNS
WWW1 Server (PHX)	HP	Netra	Windows	2000	IIS	5	Web Services
WWW2 Server (PHX)	HP	Netra	Windows	2000	IIS	5	Web Services
WWW3 Server (PHX)	HP	Netra	Windows	2000	IIS	5	Web Services
Cisco Local Director (PHX)	Cisco	Local Director				LDIR-416	Balancer
WWW1 Server (FH)	HP	Netra	Windows	2000	IIS	5	Web Services
WWW2 Server (FH)	HP	Netra	Windows	2000	IIS	5	Web Services
WWW3 Server (FH)	HP	Netra	Windows	2000	IIS	5	Web Services
Cisco Local Director (FH)	Cisco	Local Director				LDIR-416	Balancer
Anonymous FTP (PHX)	HP	Netserver	Windows	NT 4.0	WS_FTP	2.04	File Transfer Services
Anonymous FTP (FH)	HP	Netserver	Windows	NT 4.0	WS_FTP	2.04	File Transfer Services
Secure FTP (PHX)	HP	Netserver	Windows	2000	WS_FTP	2.04	File Transfer Services
Secure FTP (FH)	HP	Netserver	Windows	2000	WS_FTP	3	File Transfer Services

	Platform	Model	OS	OS Version	Software	Software Version	Services and Applications
DMZ TWO							
Intranet Facing Firewall - VRRP Pair (PHX)	SUN	E450	Solaris	2.7	Symantec Enterprise Firewall	6.5	Packet Filter Firewall
Intranet Facing Firewall - VRRP Pair (FH)	SUN	E450	Solaris	2.7	Symantec Enterprise Firewall	6.5	Packet Filter Firewall
APPS1 Server (PHX)	SUN	Ultra 2	Solaris	2.6	Custom Apps	2.5	
APPS2 Server (PHX)	SUN	Ultra 2	Solaris	2.6	Custom Apps	2.5	
APPS1 Server (FH)	SUN	Ultra 2	Solaris	2.7	Custom Apps	2.5	
APPS2 Server (FH)	SUN	Ultra 2	Solaris	2.7	Custom Apps	2.5	

	Platform	Model	OS	OS Version	Software	Software Version	Services and Applications
INTRANET BORDER							
Intranet Border Router (PHX)	Cisco	7206	IOS	12.0.20			Router ACL
Intranet Border Router (PHX)	Cisco	7206	IOS	12.0.20			Router ACL
Intranet Border Router (FH)	Cisco	7206	IOS	12.0.20			Router ACL
Intranet Border Router (FH)	Cisco	7206	IOS	12.0.20			Router ACL
Intranet Border Switch (PHX)	Cisco	3548	IOS				
Intranet Border Switch (PHX)	Cisco	3548	IOS				
Intranet Border Switch (FH)	Cisco	3548	IOS				
Intranet Border Switch (FH)	Cisco	3548	IOS				

Appendix C – List of References

1
C & A Security Risk Analysis Group
URL: http://www.security-risk-analysis.com/introduction.htm

2
Riptech, Inc. Company Website
URL: http://www.riptech.com/services/index.html

3
Tripwire, Inc. Company Website
URL: http://www.tripwire.com

4
Cisco Systems On-line Documentation, Configuring IPSec Network Security
URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scipsec.htm#xtocid214171

5
Cheswick, R. William & Bellovin, M. Steven. Firewalls and Internet Security – Repelling the Wily Hacker. Reading: Addison-Wesley Publishing Company, 1994. 4.