Global Information Assurance Certification Paper

GIAC Enterprises: Secure Windows 2000 Infrastructure Design

By

Brian C. Rudzonis

GCWIN Practical v3.1, Option 1

Table of Contents

Abstract

The following pages describe the network and Active Directory design for GIAC Enterprises, Inc. The paper covers the network topology and layout with a focus on the Active Directory design and the structure supporting it. Of particular importance are the functions pertaining to the security of the Active Directory. Therefore, this paper will cover only the aspects of the design that contribute to the overall security of the design and the rationale behind the design decisions.

1.0 Introduction

GIAC Enterprises, Inc. (GIAC) is a Delaware corporation, founded in 1999. The founders are five engineering graduates from Stevens Institute of Technology, in New Jersey. For several years following their graduation, they worked in various technical fields, from network administration and engineering to programming. All had achieved industry standard certifications, such as the Cisco Certified Network Associate (CCNA), and the Microsoft Certified Systems Engineer (MCSE). By 1999, each had achieved several certifications. On their annual vacation, they compared their experiences to achieve their certifications. Commonalities existed between them all. The commonalities all related to the lack of a complete study tool. Some tools contained adequate test simulators, others contained good questions. However, no tool was complete.

Out of this, GIAC was born. The company produces a product that is a test simulator with an excellent set of questions and a learning tool that teaches appropriate topics. The product is downloaded via the company's web site, www.giac.com. Once downloaded, the student purchases modules inside the product. A third party provides the payment services. Once the purchase has been verified, it unlocks the particular module within the product. A proprietary technology binds the key to the student's computer. If loaded on another computer, another key has to be purchased. The practice test material and related learning tool information cannot easily be printed.

GIAC is headquartered in a single leased office building in Melbourne, Florida. Company executives poured over much data to determine where the company should be located. Attractive climate, an educated workforce, and easy access to relatively inexpensive air travel were deciding factors. The founders were not interested in running the company. The entire executive team was hired after extensive interviews. The founders instead decided to concentrate on the research and development (R&D) of their flagship product. Due to the proprietary nature of their product and the competitive nature of their industry, they opted for a completely separate facility for the research and development. Since they were able to choose anywhere they wished, they chose the secluded paradise of Lihue, Hawaii, on the island of Kauai.

The Florida office contains all operations of the company with the exception of research and development. The notable departments in this office are Sales and Marketing, Finance and Human Resources, the Information Security Team, and the system administrators responsible for the site. The GIAC web presence is also located in the Florida office.

The Kauai location is used exclusively for research and development. The founders use this location to perfect their product and to plan new products and

entries into related industries. A Virtual Private Network (VPN) over the Internet connects this office to the Florida office. To provide an additional layer of security, the Kauai office can only access the Internet by first tunneling into the Florida office (more details are provided in section 4.5 Additional Security). In addition, many members of the R&D team work at home or on the road by using a VPN client loaded onto their laptop computer.

GIAC has approximately 50 employees at the Melbourne site and 15 employees at the R&D site.

2.0 Network Design and Diagram

Assumption: The goal of this paper is only to present the information relevant to the Active Directory design of GIAC. It is the opinion of this author that too many GCWIN v3.1 practicals contain padding in the form of definitions, "how to" (meaning how to configure group policy settings, for example), and third party product information that does not contribute to the overall Active Directory design. Therefore, the information presented in the following pages should be devoid of this type of information. It is assumed the reader understands Active Directory, its components, and basic network design.

The network design for GIAC is shown below:

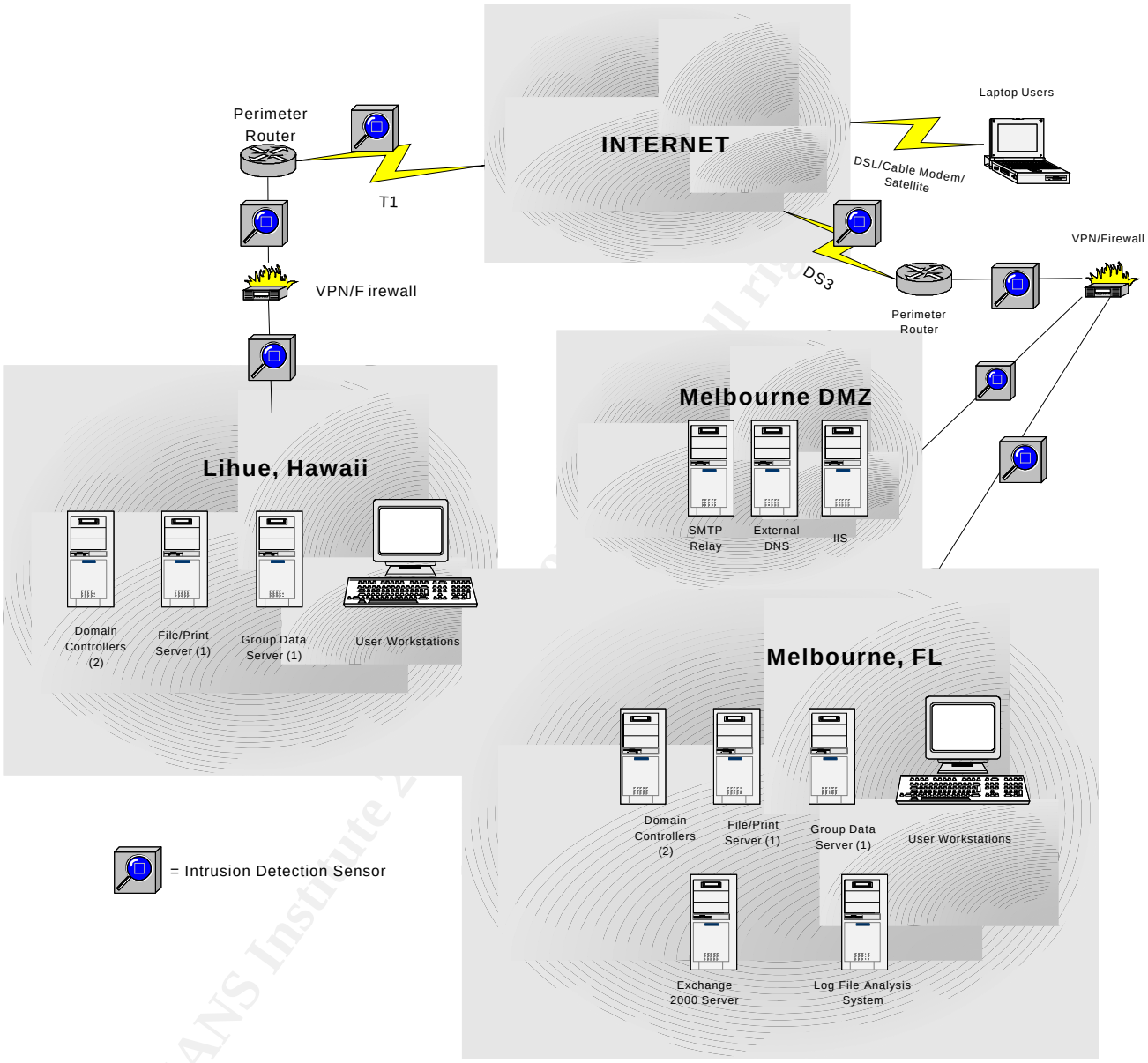


Figure 1 - GIAC Network Diagram

GIAC is composed of a single Windows 2000 domain running Active Directory (AD) in native mode. There are two sites – one in Melbourne, Florida; one in Lihue, Hawaii. The two sites each possess a single external connection. Melbourne has a DS3 (44.736Mbps) to the Internet and Lihue has a T1 to the Internet. The offices are connected to each other via a VPN over the Internet. The only traffic physically allowed external to the Kauai office is routed to the Melbourne office over the VPN. All other traffic is blocked by the firewall.

Internet browsing, e-mail, and similar services are all first routed to Melbourne. No traffic travels directly to the Internet from Kauai. Melbourne has a VPN firewall/router that separates traffic bound for the internal network or for the demilitarized zone (DMZ). The DMZ contains the public presence for GIAC – the public web server, DNS, and the SMTP relay. The DMZ is firewalled from the rest of the network and the VPN tunnel begins and ends on the DMZ's external interface in order to decrypt the traffic for processing by the intrusion detection system (IDS). For additional security, there are three IDS sensors listening on the Melbourne network – one on the segment external to the DMZ, one on the segment internal to the DMZ, and the third is on the internal network segment. All IDS sensors are integrated into a single log server and management station, monitored by the Information Security Team (Infosec).

Assumption: One of the key design elements is the security of the R&D site.

It is for this reason all traffic destined for the Internet is first routed through the Melbourne site and the firewall only allows the VPN traffic. Therefore, the site is hidden behind the Melbourne network. Additionally, some R&D team members enjoy working at home or on the road and are authenticated into the network via a VPN client.

Assumption: For the purposes of this design document, most of the hardware specifications for servers and workstations are considered to be more than adequate. Each is running Windows 2000 with Service Pack 3 with the latest hot fixes. The only file system in use is NTFS.

Assumption: A key element impacting the network design is simplicity, with well-known and relatively low-maintenance methods of adding performance and fault tolerance. This element facilitates a lower total cost of ownership. By stressing simplicity and adding high-return security and fault tolerance features, GIAC is able to keep fewer administrators and engineers on staff. This is crucial in achieving the lowest cost product in the industry.

The following is a description of each type of server, the number of each server if appropriate, its role and placement, and any other relevant details:

2.1 Domain Controllers (DC's)

There are four DC's. Two are located at each physical site. There are two at each site for redundancy. The operating system is installed on a mirrored 4GB volume. The swap file, transaction logs and event logs are stored on another partition (unmirrored because of the swap file), this one 60GB in size. External RAID10 arrays store the AD and many software packages that are used for distribution to workstations. A hardware RAID10 solution was chosen for performance and fault tolerance, with low cost of labor. RAID10 is effectively a

mirrored stripe set. (http://www.unt.edu/benchmarks/archives/2001/december01/raid.htm) Striping provides the performance, while mirroring provides the fault tolerance. The size of the RAID10 array is 100GB. All DC's will be Global Catalog servers as well.

Assumption: The company remains fairly stable and there are very few changes to the AD, therefore we are not worried about replication over the VPN. Additionally, the T1 connection to the R&D site should not pose any problems during times of peak replication activity.

The first DC will serve as the Flexible Single Master Operation (FSMO) Master for all five FSMO roles (PDC Emulator Master, RID Master, Infrastructure Master, Schema Master, and Domain Naming Master). The first DC resides in the internal Melbourne network. Since simplicity is a key design element, all roles residing on the first installed DC should not pose a problem. The network is relatively small and almost static and the DC's and network infrastructure can all handle a much larger workload than the anticipated peak workload. As AD and DNS are integrated, the DC's will also handle the internal network's DNS. External requests are forwarded to the external DNS server in the DMZ. Since Kerberos is the authentication protocol of choice for GIAC, the DC's all serve as Kerberos Key Distribution Centers (KDC's).

For performance and to avoid a single point of failure, the DC's are installed on two separate switches on the network. Therefore, if one switch fails in the path of one of the DC's, the other DC will still be accessible to some or all workstations.

2.2 IIS Server

The GIAC web server is installed in the DMZ and is the primary means for customers to download the software study tool product. IIS 5.0 is installed on a server with plenty of hardware to handle a large amount of traffic. The Windows 2000 operating system is installed onto a mirrored 4GB volume. Transaction logs, event logs and the swap file are installed onto a 60GB volume (unmirrored because of the swap file). A hardware RAID10 solution is installed for the web site and miscellaneous storage space used for maintenance and work with the web server. The RAID10 array is 100GB.

The web server is also dual homed (meaning that it has two Network Interface Cards (NIC's)). The NIC's are both Fast Ethernet. One NIC is attached to the DMZ for external access by the public customer. The second NIC is attached to the DMZ for internal access by administrators and the web site authors. Routing is disabled between the two interfaces. The server is a member of the domain in order to make administration easier. The security of the perimeter and the hardening of the box should mitigate the risk of being a domain member.

In addition, the web server has been set up with the following file structure for the web site: (GCWIN Course Material, Securing IIS Module, p.40)

\GIACweb
\Mainsite
\root (.htm and .html)
\images (.gif, .jpg, etc.)
\scr (.asp and .pl)
\exe (.dll, .exe)
\inc (.inc)

As with other servers, all services that are not needed have either been removed or disabled. The following is a list of some of the hardening steps taken:

- ✓ The Resource Kit is not installed.
- ✓ Internet printing is disabled.
- ✓ 8.3 name generation has also been disabled.
- ✓ NetBIOS has been disabled.
- ✓ Default permissions are Full Control for Administrators and System.
- ✓ Indexing is disabled.
- ✓ WebDAV is disabled.
- ✓ IIS samples and help files have been removed.

2.3 SMTP Relay

A smaller server is installed into the DMZ and used as a mail relay. It is running Windows 2000 with an SMTP relay agent and has been hardened in such a way as to the only software and services present are used exclusively for relaying mail. The only traffic permitted to this server is mail traffic. Administration is performed at the console, which is locked up in the data center. The operating system is mirrored onto two 4GB volumes. The mail relay software, transaction logs and event logs are stored on a 40GB mirrored volume. The swap file exists on a 20GB unmirrored volume.

2.4 External DNS Server

Also inside the DMZ is an external DNS server. All internal DNS requests are forwarded to this server and it performs the name resolution by querying Internet DNS servers. There should be no DNS requests from the Internet except for e-mail and web services. Therefore, this DNS server will not forward requests to the internal server. Windows 2000 is installed and is hardened to only include the necessary services. In addition, the following DNS settings apply:

- ✓ Only records for e-mail and the web server are stored. No other services should be accessible by the public.
- ✓ Dynamic updates are disabled.
- ✓ Zone transfers are disabled.
- ✓ Active Directory-integrated zones are not used.

2.5 Enterprise Certificate Authority (CA)

A single Enterprise CA exists for the purposes of creating and exporting digital certificates for use on laptops using the Encrypting File System (EFS). This server is stored powered off in a vault and is only powered on when a certificate needs to be created and exported for a laptop user. The occasion of creating certificates is a rare event since the original rollout of EFS. The physical security and distribution methods of the certificates is considered more than adequate (see 4.5 Additional Security)

2.6 File/Print/DHCP Servers

Four File servers exist within the network, two of which perform the role of print server, and two of which perform the role of DHCP server. There are two file servers, one at each location, that store the "My Documents" folder for users. These servers have also taken on the role of DHCP servers for each site. The combination of roles is considered adequate with the anticipated light workload for DHCP in a small network. The important security point to consider was to separate the DC's from the DHCP servers. Adding the DHCP role to protected internal file servers does not increase the risk profile and eliminates the cost of two additional servers. In addition, there are two file servers, one at each location, that store shared files. Each of these servers also performs the role of print server for each location. The shared file structure loosely follows the organizational chart for GIAC. The need for sharing files dictates the structure. Group membership controls access to the directory structure. All four servers are identical in their setup. Windows 2000 is the operating system. The operating system is installed onto mirrored 4GB volumes. An unmirrored volume of 20GB stores the swap file and event logs. A RAID10 array of 120GB stores the user and group files.

2.7 Exchange 2000 Server

There exists a single Exchange 2000 server on the internal Melbourne network. For simplicity of administration, GIAC chose not to install a second server at the R&D site. During the design study, it was determined most of the R&D staff spend their time in development and do not check their e-mail more than once or twice a day. From this study it was concluded a second server would have

complicated and increased the cost of administration. The R&D staff accesses their e-mail through the VPN. The server itself is running Windows 2000. The operating system is installed onto mirrored 4GB volumes. An unmirrored volume of 40GB stores the swap file, event logs and the Exchange transaction logs. The message stores are housed on a RAID10 array of 120GB. The server has been hardened and all unnecessary services and components have been disabled or uninstalled.

2.8 User Workstations

All user workstations are late model, name brand workstations with sufficient processing power, memory, and hard drive space. The operating system is currently Windows 2000 Professional, however, there are plans to Windows XP Professional. For ease of administration, master images are kept of each combination of hardware and software. Each workstation has a standard set of office automation tools (Office XP, Outlook, Internet Explorer, etc.). Various groups require different software, most of which is controlled through Group Policy Objects (GPO's). GPO's also control many aspects of locking down the workstations as well. See section 4.3 – Additional Group Policy – User Workstations for more information. Anti-virus software is also installed with automatic updates of virus definitions.

2.9 User Laptops

Several users also have GIAC-owned laptops in their possession. Most of these employees belong to the R&D team. They believe in being able to perform their development from anywhere they wish. The laptops are locked down and use EFS to protect their data. The laptop users gain access to the network via the VPN client located on their desktop. Windows 2000 Professional running on late model laptops with sufficient hardware resources is the GIAC standard laptop.

2.10 Miscellaneous Servers and Network Equipment

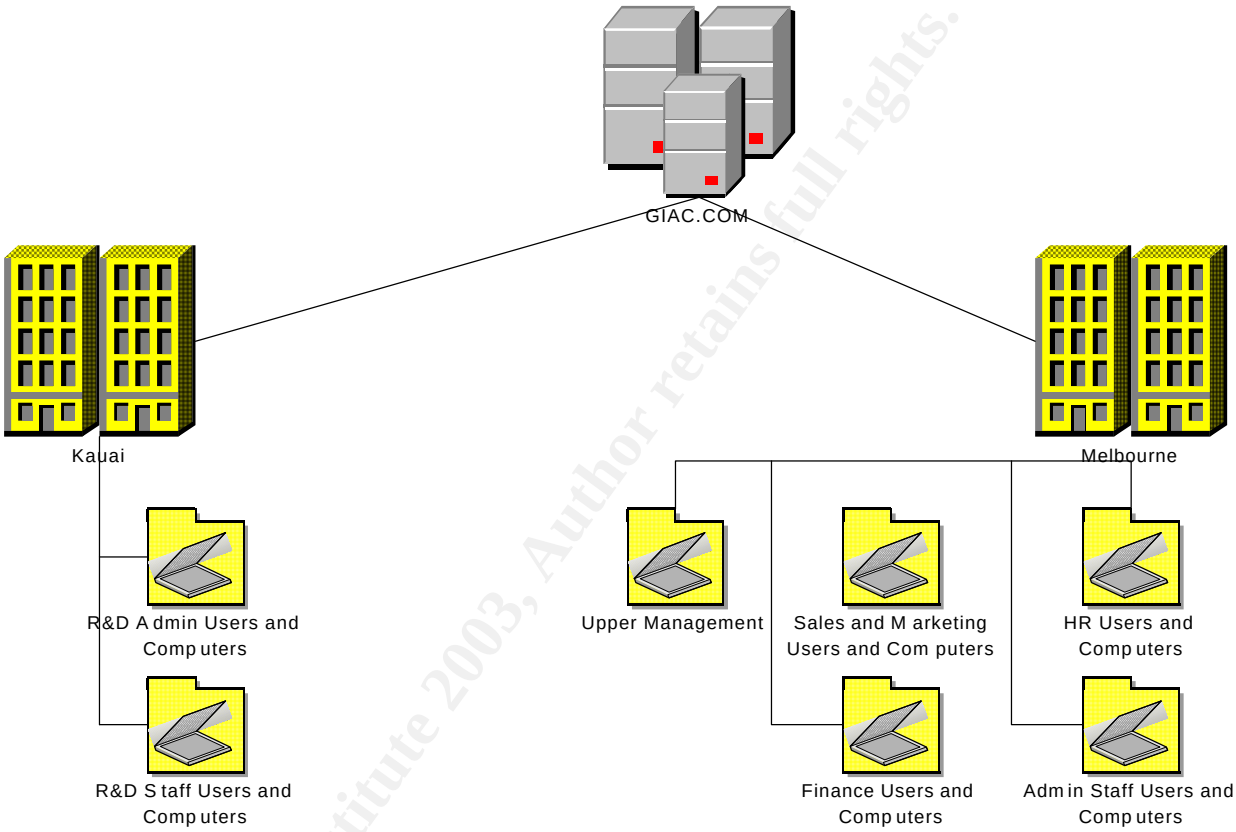
There are several other components that are key to the security and operation of the network, but are outside the scope of this document. Therefore, they will only warrant a brief statement to acknowledge their existence.

Both the Kauai and Melbourne networks are attached to their relative ISPs through a hardened router. These routers are attached to the VPN/Firewall. In the case of the Melbourne firewall, it contains a connection into the DMZ and the internal network. All routers and firewalls are hardened in such a way as only the minimum necessary traffic is allowed to each host and on each segment. On each segment, there are IDS sensors. Each sensor connects directly to a

management console. Host-based intrusion detection systems are also in use and analyzed at a central console.

3.0 Active Directory Design

The Active Directory structure for GIAC is depicted below:



As depicted in the drawing, the GIAC AD structure can simply be defined as a single domain within a single forest containing two sites separated by geography, each containing their own set of containers for the purposes of administrative delegation and GPO applicability.

Assumption: All readers should have a basic understanding of AD components. Therefore, the discussion will be limited to design choices and rationale.

3.1 Active Directory Domain Structure

A single domain within a single forest was chosen for simplicity, cost, and reduced overhead. GIAC is a small company with a single Internet domain name

and a common set of security policies. Reasons for choosing separate forests are having parts of a company that differ enough to cause differences in schema control or configuration and forbid specific users from ever gaining access to resources in the other forest. None of these conditions apply, therefore a single forest has been chosen. (Active Directory Architecture White Paper, p. 17)

Naturally, having a single domain automatically means having a single tree in a forest. However, just to be absolutely clear, there can be reasons to choose two separate domains in the same forest or two domains in which one is a child of the other. One valid reason to have two domains is when two namespaces exist. GIAC is a single organization, therefore it only has a single namespace. (Active Directory Architecture White Paper, p. 18)

Another valid reason to have two separate domains deals with a lack of a reliable connection between resources. GIAC has plenty of bandwidth and it is considered reliable, therefore this is not a valid reason to create another domain. Sometimes organizations merge and it is easier to connect their resources by creating separate domains. GIAC was started from the ground up and has no current plans to merge with another organization, therefore this is not a valid reason to maintain more than one domain.

Maintaining a separate organization is often a valid reason to create a second domain. The argument may be made that GIAC fits this profile with the separation of its R&D from its main office. However, GIAC has chosen to implement this separation in a more cost effective means. The study resulting in the current design concluded it would have added too much overhead and cost when separation could instead be achieved by using sites and other security measures (VPN over the Internet with locked down perimeter). Therefore, this reason was not valid due to cost considerations. (GCWIN Course Material, Active Directory Module, p. 171)

Differences in domain-wide policy settings between organizations or sites can be another reason to opt for two or more domains. GIAC uses common practices for its overarching security policies. Other differences in policies can be implemented by linking GPO's to certain groups through grouping resources into Organizational Units (OU's).

3.2 Active Directory Sites

Within the GIAC.COM domain, there are two sites. They are based on the geography of the company. The first site is the Melbourne site and contains all the resources within this office. The second site is the Kauai site and contains the resources within this office.

Many of the benefits of maintaining two sites could also have been achieved by maintaining two domains. However, to keep the cost and complexity down, GIAC chose a single domain with two sites. The use of two sites helps to make efficient use of network resources and efficient use of the VPN connection. Users and computers will seek out DC's within their own site in order to log in. This keeps the traffic local instead of traveling over the VPN. Replication of AD information between sites over the VPN is also optimized and has the ability of allowing scheduling. (Active Directory Architecture White Paper pp. 21-22)

3.3 Active Directory Organizational Units

Within the Melbourne site, several Organizational Units (OU's) have been added to assist with the administration of the system. The goal of the design is to represent a balance of security with simplicity. In order to achieve this goal, it was decided to create OU's that align with the different functional groups within the site and to separate out the administrative staff (the helpdesk, system administrators, and engineers). This permits the use of GPO's to control users and their workstations by function within the company and to easily roll out software unique to each group. Separating the administrative staff removes many of the restrictions imposed by GPO's linked to each OU.

The default groups Users and Computers will not be used in this AD design. Instead, the users and their workstations will be kept in OU's pertaining to each department to which they belong. The following OU's have been created:

- ✓ Upper Management Users and Computers
- ✓ Sales and Marketing Users and Computers
- ✓ HR Users and Computers
- ✓ Finance Users and Computers
- ✓ Admin Users and Computers

The Kauai site has been built in the same way. Since it is a very small site, it contains fewer OU's. For the most part, the R&D staff do not need much in the way of support. There is only a single administrator to keep up with the day-to-day tasks. The following OU's have been created within Kauai:

- ✓ R&D Users and Computers
- ✓ R&D Admins and Computers

3.4 Global Security Groups

The global security groups GIAC uses to grant permissions to files and folders and for the delegation of tasks for the administrative staff follows the principle of using tight security with a lack of complexity. The groups also mimic the OU

design. This mirrored setup contributes to the simplicity of design. If there were some users or computers in one OU and the user appeared in a different security group, then it would add to the complexity of administration. In this design, HR users will all appear in the HR security group, and the Finance users will appear in the Finance global security group. This should remove the risk of inadvertently assigning users to a global security group to which they should not belong, thus granting access to resources for which they do not have a need.

The global security group structure is also used for delegation of administrative tasks. Members of the Admin Users and Computers are a compilation of the three-tier support structure and the Information Security Group (Infosec). The first tier is the helpdesk. Their function is to take calls from users at the Melbourne site and attempt to solve simple problems (such as password resets) or open trouble tickets for administrators. The second tier is the administrators. They work off trouble tickets opened by the helpdesk and are the workhorses of the system. Their power extends over all the resources within the Melbourne site. The third tier is the engineers. They assist administrators with the more complex problems present on the system and they also maintain the workstation baselines for the various groups. They create new software packages for distribution and research and prototype new technology. They also function as the Domain Admins when troubleshooting extends between Melbourne and Kauai. A fourth group within the administrative staff is Infosec. They are responsible for the IDS's and the analysis of logs from all system resources. They are also the only group that creates and exports certificates for laptops that use EFS.

The following are the list of GIAC's global security groups:

- ✓ Management
- ✓ HR
- ✓ Finance
- ✓ Sales and Marketing
- ✓ Finance
- ✓ Helpdesk
- ✓ HQ Administrators
- ✓ Engineers
- ✓ Infosec
- ✓ Kauai Administrators
- ✓ R&D

The Helpdesk group requires further attention because it has been delegated specific tasks in order to optimize the efficiency of the support structure. Besides being the front line of support for users and their troubles, it has been decided that password resets and modifications of group membership are very simple tasks that high-paid administrators do not need to perform. Therefore, this duty falls on the helpdesk. The Delegation of Control Wizard was used to grant these

abilities. The “Reset password” and “Modify the membership of a group” tasks were chosen for the Helpdesk group and applied to the OU’s of Upper Management Users and Computers, Sales and Marketing Users and Computers, HR Users and Computers and Finance Users and Computers. It is important to note that these tasks do not extend to the administrative staff OU.

The system administrators are also set up in a similar fashion. Since the administrators are broken into two groups (by site), their power is delegated by site. The HQ Administrators have been delegated full control over the Melbourne site using the Delegation of Control Wizard. This is performed by creating a custom task (in the Tasks to Delegate page) and selecting the Melbourne site and applying Full Control permissions. Kauai Administrators is set up in the same way, but delegating Full Control over the Kauai site. Through group policy, both groups will be granted additional rights over each site. This is to keep these rights assignments at the domain level, rather than having to push them down to the OU level. In addition, it gives the larger staff of the Melbourne office more ability to help out the R&D site in Kauai.

3.5 Miscellaneous Active Directory Design Notes

There are some other miscellaneous design notes relevant to the AD structure for GIAC. All computer resources (servers and workstations) have their time synchronized in order to avoid time related problems with Kerberos and for audit trail analysis by Infosec. A second design note is that all permissions to resources are granted to groups rather than individual users. The SYSKEY.EXE utility has been used to change the default storage option for the System Key. GIAC has decided to store the System Key on a floppy disk and keeps the disks in the drives of all servers. A copy of each System key floppy disk has been made and stored in a safe inside a secure room within the data center. As discussed later, physical security is considered to be good enough to store the System Key on a floppy disk. Further, it would be considered a burden administratively to have to enter a password upon boot or to manually put the System Key floppy disk in the drive. (Course material, AD p. 74-75)

4.0 Basic Group Policy and Security

Because one of the main goals of the GIAC network design is simplicity with a lot of security, GPO’s are a key element. A GPO is a powerful tool for administrators and engineers to enforce uniform configurations and effect system-wide changes with minimal labor. Due to its flexible design, a GPO is also a great tool for enforcing security and preventing users from overstepping their need to access resources and configure their workstations. The Default Domain Policy is used by the GIAC administrative staff to enforce policies and settings that all users and computers adhere to. Naturally, the DC’s require

greater security and are subject to the Default Domain Controller Policy. To achieve the granularity of control necessary to lock down most users, give freedom to the administrative staff, and roll out department-specific software, additional GPO's are used and linked to specific OU's for enforcement. This also has the effect of leaving the Default Domain Policy fairly static, which is an advantage since it affects all users and computers in the entire network. Most of the changes will happen with the additional GPO's, which will isolate any problems that were not discovered during testing. In addition, the GPO's that are used permanently (Default Domain, Default Domain Controller, and the User Desktop) are refreshed daily. The refresh time of each GPO occurs at night and is separated so they are not all being refreshed at once.

4.1 Default Domain Policy

During the initial study that resulted in the current design for GIAC, it was decided to follow the National Security Agency (NSA) recommended group policy settings (Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set). There are also a few settings that have been changed from NSA recommendations in order to reduce administrative tasks. In each instance, proper explanation will be given. The settings given in the following pages are by no means comprehensive, although they will be the most noteworthy or deviant from either the default settings or NSA recommendations.

Table 4.1-1 - Account Policies→Password Policy	
Enforce password history	24 Passwords
Maximum password age	90 Days
Minimum password age	1 Day
Minimum password length	8 Characters
Passwords must meet complexity requirements	Disabled
Store password using reversible encryption for all users in the domain	Disabled

Most of the password settings listed above conform to NSA standards and set a strong password policy. Two settings that do not follow NSA guidelines are the "Minimum Password Length" and the "Passwords must meet complexity requirements". Research by GIAC engineers concluded that too complex a password policy can unravel the intended security benefits because users will start writing down passwords or use easy to remember passwords and append numbers or change an "i" to a "1" or an "e" to a "3". Therefore, it was determined that with little effort a custom password filter would be created. This password filter forced users to create passwords at least 8 characters in length, forced the use of characters from all four sets (uppercase, lowercase, numbers, symbols), and performed a check against a third party dictionary that looks for common types of strong passwords using the types of substitutions above.

Table 4.1-2 - Account Policies→Account Lockout Policy	
Account lockout duration	15 Minutes
Account lockout threshold	5 Invalid logon attempts
Reset account lockout counter after	15 Minutes

The intent of the Account Lockout Policy settings is to inhibit the use of brute-force or dictionary attacks or password guessing. NSA recommends the use of 3 Invalid Logon Attempts as the setting for "Account Lockout Threshold". However, experience has shown that too many helpdesk calls result from this setting. In today's online world, users have many passwords to remember. Asking users how their accounts became locked out resulted in a few common themes. One was they typed in the wrong password and thought they typed it in wrong and then found themselves locked out. Another group of users often had Caps Lock enabled, which resulted in their lockout. The third group had trouble remembering their password and would have been spared a call to the helpdesk if they had just a couple more attempts. In all cases, if they had waited 15 minutes, their invalid logon counter would have reset. However, users always want everything immediately. Therefore, using 5 attempts has struck a good balance between security and reduced helpdesk calls. The point of having a lockout count is to counter password guessing. Just having that lockout is a powerful countermeasure compared to the default setting of no lockout counter.

Table 4.1-3 - Account Policies→Kerberos Policy	
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 Minutes
Maximum lifetime for user ticket	10 Hours
Maximum lifetime for user ticket renewal	7 Days
Maximum tolerance for computer clock synchronization	5 Minutes

The Kerberos settings are all standard to NSA recommendations and the default settings as well. Kerberos is built as a strong authentication method "out of the box", therefore it should not require additional locking down. Even though these are the default settings, they deserve mention since Kerberos is the authentication method of choice for GIAC.

Table 4.1-4 - Local Policies→Audit Policy	
Audit account logon events	Success/Failure
Audit account management	Success/Failure
Audit directory service access	No auditing
Audit logon events	Success/Failure
Audit object access	Failure
Audit policy change	Success/Failure

Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	Success/Failure

Auditing is a very important aspect of maintaining the health of the system and the security of the system. With this in mind, GIAC has sized its servers appropriately in both disk space and processing power. The settings above mirror NSA's recommendations. At times it may be necessary to increase auditing, either on users or computers. This can be accomplished with separate GPO's linked to appropriate containers and then more granularly targeted by removing the "Apply Group Policy" and "Read" Access Control Entries. (Windows 2000 Group Policy White Paper, p. 6)

One of the settings that may cause a second look as to why auditing is not turned on is the "Audit directory service access" setting. The directory service resides on DC's, therefore it would not apply to workstations and servers. This setting will be present in the Default Domain Controller Policy.

One setting that may result in a large amount of audit data is "Audit logon events". It is important to track whether or not accounts were logged into the system. GIAC has plenty of disk space on all its resources and plenty of processing power, so this will not pose a problem.

Other settings such as "Audit process tracking" and success of "Audit privilege use" can be turned on as needed for certain events, like possible attacks, or investigations of certain individuals.

Table 4.1-5 - Local Policies→User Rights Assignments

Access this computer from the network	Authenticated Users
Add workstations to the domain	(No one)
Back up files and directories	Domain Admins, HQ Administrators, Kuaui Administrators
Bypass traverse checking	Domain Admins, HQ Administrators, Kuaui Administrators
Change the system time	Domain Admins, HQ Administrators, Kuaui Administrators
Debug programs	Domain Admins, R&D
Force shutdown from a remote system	Domain Admins, HQ Administrators, Kuaui Administrators
Load and unload device drivers	Domain Admins, HQ Administrators, Kuaui

	Administrators
Manage auditing and security log	Domain Admins, HQ Administrators, Kuaui Administrators, Infosec
Restore files and directories	Domain Admins, HQ Administrators, Kuaui Administrators
Shut down the system	Authenticated Users
Take ownership of files or other objects	Domain Admins, HQ Administrators, Kuaui Administrators

Most rights within the system are left in the capable hands of the system administration and engineering teams. This policy will be applied to workstations, so many rights have been taken out of the hands of the users in order to save administration costs. Adding workstations to the domain is a task that occurs on DC's, therefore it is specified here only to demonstrate this right will be used within the Default Domain Controller policy. Some of the tasks GIAC does not want a user to perform are to change the system time (to interfere with Kerberos and collection of accurate audit events), backing up and restoring files (files should be stored on file servers and master images are used to quickly restore faulty desktops), bypass traverse checking (NTFS permissions become more restrictive deeper into the file system, so there should be no need for this right), debugging programs (except for the R&D team, which creates GIAC's product), forcing shutdown of remote systems, loading and unloading device drivers (users who think they can install custom hardware can think again – they must initiate the proper work request and have the administration staff install the device), managing the auditing and security logs (also used by Infosec for audit log analysis) and taking ownership of files and directories.

One right granted to users is the ability to shut down the system. This resulted from experiences with users who have had this right revoked in the past. These restricted users will become frustrated when they attempt to shut down their machine and instead resort to using the power button or pulling out the power cord. This has resulted in the corruption of systems and contributed to a greater overall cost of support. Therefore, it has been decided to grant users this right in order to provide them an opportunity to perform one of the few tasks they can handle almost flawlessly – the PDPU (Power Down Power Up).

Table 4.1-6 - Local Policies→Security Options	
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Audit use of backup and restore privilege	Enabled
Clear virtual memory pagefile when system shuts down	Enabled

Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (when possible)	Enabled
Disable media autoplay	All drives (0x000000FF)
Do not display last user name in logon screen	Enabled
Generate audit event when the audit log reaches a percent full threshold	90
LAN Manager authentication level	Send NTLMv2 response only/refuse LM & NTLM
Message text for users attempting to log on	SEE BELOW
Message title for users attempting to log on	***WARNING***
Network Security: Disable IP source routing	Disable source routing completely
Network Security: Enable ICMP redirect	Disabled
Network Security: Keep alive time for TCP connection	5 Minutes
Network Security: Maximum number of half-open retired TCP sockets to maintain	160
Network Security: Maximum number of half-open TCP sockets to maintain	200
Network Security: Protect against Computer Browser spoofing attacks	Enabled
Network Security: Protect against SYN attacks	Better protection
Number of previous logons to cache (in case domain controller is not available)	0 logons
Prompt user to change password before expiration	14 Days
Rename administrator account	SEE BELOW
Rename guest account	SEE BELOW
Restrict CD-ROM access to locally logged on user only	Enabled
Restrict floppy access to locally logged on user only	Enabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled

Many of the settings in the Security Options section are used to counter specific vulnerabilities. For example, many of the Network Security settings counter Denial of Service attacks. Other Network Security settings counter known problems with IP source routing and ICMP redirects. Most of these settings are also used at the perimeter in routers and firewalls. Therefore, from the Internet, this provides an additional layer of defense. Because there is always the threat

of the insider, these types of settings help to fend off attacks from these types of adversaries. Some of the settings used may very slightly from NSA recommendations. In security testing, these numbers have been tweaked because all GIAC resources can handle quite a few connections before the processor becomes overloaded.

There are also settings to digitally encrypt and sign secure channel data and other communication. Although digital certificates are not in widespread use within GIAC, since these types of settings are not required, they will not break the system. However, they are already in place for a future rollout and the settings can be elevated to "Always" should testing prove successful.

Anonymous users are heavily restricted within the system. There should be no reason for anonymous users to gain access to any resources except for what is explicitly granted to the IIS User account.

Backup and restore privileges are audited to coincide with the Privileged Use auditing. Disabling this right will mean all other privileged use will be audited except for backup and restore. GIAC has plenty of disk space and a host-based IDS to handle the potential excessive size of log files.

The pagefile from all systems is cleared upon shutdown. This ensures there will be no information resident on the system that is not specifically authorized by administrators or controlled by users.

The removable drives (floppy and CD-ROM) are also restricted. Autoplay is turned off to prevent malicious code from being auto-launched without even having to authenticate to the system. With autoplay, an individual can just walk by a computer and insert a CD-ROM without ever logging on and it will automatically launch the autoplay file on the CD-ROM. The drives are also restricted to the locally logged on user.

The last user to log in is displayed in the logon dialog box by default. This allows an individual to automatically have a username with which to attempt to gain access to the system. However, this can often be a small reward since usernames follow standard conventions involving names and can often be figured out with a little bit of effort.

Auditing is a large part of GIAC's system. Log file analysis takes place with automated tools and is fine-tuned and further analyzed by Infosec. It is for this reason GIAC has chosen to have the system generate an audit event when the audit log reaches 90% capacity. This audit event is one that is flagged by the analysis software and can indicate either a problem with the system (either the system itself or the audit log backup and clearing processes) or a possible attack that includes flooding audit logs.

The LAN Manager authentication level is set to the highest setting (Send NTLMv2 response only/refuse LM & NTLM) since the whole system should be able to use Kerberos and there are no backwards-compatible systems that need to be accounted for.

The logon banner uses a variant from the Department of Justice. It was taken to a lawyer to ensure proper action can be taken for any attempted misuse of the system. The banner text is as follows:

WARNINGWARNING**WARNING**WARNING**WARNING**WARNING

The GIAC Enterprises, Inc. computer system is provided for Official Use Only. Any information placed in the system belongs to GIAC Enterprises, Inc. and may be monitored, used and/or disclosed by authorized personnel. The data on the system may be searched at the request of law enforcement or other persons, as appropriate, and may be disclosed and used for disciplinary or civil action or criminal prosecution. Use of this computer system constitutes consent to these policies.

WARNINGWARNING**WARNING**WARNING**WARNING**WARNING
(http://www.itsc.state.md.us/info/InternetSecurity/BestPractices/WarnBanner.htm)

This policy has also been set up not to cache logons. GIAC intends for users to only be able to log on when a DC is reachable. It is for this reason there are redundant DC's on the network and they are on separate subnets.

Earlier in the policy, the password age time was shown to be 90 days. With a relatively quick expiration time (in the point of view of users), users need time in order to be warned to change their passwords. The setting of 14 days should be ample warning and should handle most absences and also serve as a constant reminder to the lazy user who always waits until the last minute to perform the password change.

Also of great importance is the renaming of the guest and administrator accounts. This is performed when master images are created and the names are the equivalent of strong passwords. And, of course, the guest account is disabled. The usernames and passwords are stored in a sealed envelope in a safe within the secure room within the data center. It is rare these should be needed, but these extra precautions are taken just in case the need arises.

Table 4.1-7 - Event Log→Settings for Event Logs	
Maximum application/security/system log size	4194240 Kbytes
Restrict guest access to application/security/system log	Enabled
Retention method for application/security/system log	Manually

Shut down the computer when the security audit log is full	Disabled

Audit log settings are very important to the log file analysis program put in place by Infosec. Part of the implementation was to ensure all workstations and servers had more than enough hard drive space to store audit logs and handle the growth in size of operating system and application upgrades. Therefore, the log files have been set to their maximum size. The log files have also been restricted from guests and null logons. Since the log file analysis system aggregates logs and clears out the log files automatically, log retention should not be an issue. We also do not want to shut down the system in case the audit files fill up. We have already set a warning event to be logged in case they reach 90% full. Also, in the event of a system attack, the log analysis should be able to detect it. In the event of a system problem that logs extensively, the administrators would like the chance to view the system as it is instead of having to shut it down and restart it. This may clear an intermittent error and complicate troubleshooting instead of possibly offering a chance at gathering data to help solve the problem.

4.2 Default Domain Controller Policy

The settings specified in this section pertain only to the differences between the Default Domain Policy and the Default Domain Controller Policy. This is mostly due to the fact that certain settings apply only to interactions with the AD, which resides on a DC.

The setting for Local Policies→Audit Policy→Audit directory service access was not set for the Default Domain Policy because it did not apply to workstations and member servers. However, since the directory service is resident on the DC's, the setting chosen is to audit access failures.

Table 4.2-1 - Local Policies→User Rights Assignments

Add workstations to the domain	Domain Admins, HQ Administrators, Kauai Administrators
Shut down the system	Domain Admins, HQ Administrators, Kuaui Administrators

Adding workstations to the domain is only relevant where the AD resides, which is on the DC's. The system administrators and engineers will be the only individuals allowed to add workstations to the domain in order to keep control of

the system and the directory. The administrators and engineers will be the only individuals permitted to shut down DC's.

4.3 Additional Group Policy – User Desktop

The settings that are enforced through the Default Domain Policy and the Default Domain Controller Policy help to enforce security only so far. There are still settings that must be enforced, but must be done so without preventing the administrative staff from being able to perform their function. GIAC desires to lock down user desktops and has chosen to do so by creating a separate policy to link to the users and their workstations. The goal of the policy is to remove some of the common sources of customization by the user: the control panel, drive mappings, registry editing tools, the command prompt and storing their files locally. The settings chosen to implement were part of the study performed prior to designing the network and represent topics for a disproportionate amount of helpdesk calls. Attempting to eliminate these trouble calls and further securing of the desktop are direct results of these settings.

One of the goals of GIAC's design is to ensure all files users work with are stored on servers. This ensures they are backed up daily, they are accessible from any workstation and any problems resulting in a new workstation image do not cause loss of files. In order to accomplish this, users have been encouraged to store their files in the "My Documents" folder. This folder has been redirected to the appropriate user file servers at each site. To accomplish this, under Folder Redirection→My Documents, advanced redirection specifies the appropriate path for each group. All groups are redirected to the Melbourne server except for R&D and Kauai Administrators, which are redirected to the Kauai site's user file server.

Settings in Administrative Templates under Windows Components→Windows Explorer are also used to lock down user desktops. The settings "Hide these specified drives in My Computer" and "Prevent access to drives in My Computer" are used together to hide and prevent access to all drives. Together with Start Menu & Taskbar:" Remove Run menu from the Start Menu" and System: "Disable the command prompt" it will be very hard for the ordinary user to poke around and attempt to run other applications or access drives.

One of the biggest reasons for trouble calls relates to users who play around with the Control Panel. There is really no logical reason for a user to ever be in the Control Panel. Most of this results from using the Control Panel on home systems and feel they have an inalienable right to do the same on their corporate owned workstations. This is not permissible at GIAC. All users are trained to realize they will not be able to alter their desktop settings in an attempt to personalize their desktop. Granting this privilege has shown it also has the effect of increasing the amount of trouble calls due to the inability for users to give in to

the temptation of changing something else in the Control Panel and asking themselves, “I wonder what this will do?” Therefore, it has been decided to disable the Control Panel for users. Control Panel: “Disable Control Panel” is used to do this.

Since the GIAC policy has disabled the use of the Control Panel, it will use Group Policy to set specific screen savers and characteristics. The Control Panel→Display section is used to do this. “Screen saver executable name” is fixed for all users, however, with sufficient requests from users it has been changed from time to time to allow for variety and as a training point for new system administrators. The important point to note is that it is fixed and unalterable for users. “Password protect the screen saver” and “Screen saver timeout” are used to force authentication to remove the screen saver and to activate the screen saver after 10 minutes of inactivity. Finally, the “Activate screen saver” is used to force the use of the screen saver and the use of the previously defined settings.

There are also some miscellaneous settings that contribute to the overall security and protection of the desktop from the curious, well-meaning, or even dangerous user. System: “Disable registry editing tools” takes this capability out of the hands of the user so they cannot even comprehend the possible damage they may be able to achieve or to even browse settings. System→Logon/Logoff: “Disable Task Manager” prevents users from launching the Task Manager, which may help users to stop misbehaving applications, but could cause more harm than good.

4.4 Additional Group Policy – Software Deployment and Scripts

GIAC makes extensive use of GPO’s for the purpose of rolling out software. Each department has specialized applications that are all updated through the use of GPO’s that are linked to that department’s OU. GIAC engineers typically use the Windows Installer Service (MSI) in conjunction with GPO’s to accomplish the software updates. All packages are assigned to force automatic installation and in the case of site-wide (or domain-wide) distribution (for patches, service packs, etc.) the GPO is linked one OU at a time.

One of the problems with workstations is their software becomes out of date soon after their deployment. This is another reason GIAC uses GPO’s with MSI packages to roll out their software. The engineers test these packages extensively before they are rolled out. Like patch deployment, this is executed a single OU at a time to retain control and the ability to solve problems throughout the deployment. GIAC uses a third party MSI package editor.

There are occasions that arise where GIAC engineers create scripts and assign them to specific OU’s. Sometimes this is done to replace a certain file on all

workstations that may patch an older version. At other times the administrators and engineers may want to collect a certain file on all workstations and would use a script assigned through a GPO as well. Any other ad-hoc scripts that need to be applied to all workstations or all users either within a single OU or combination of OU's are easily accomplished through GPO's.

The final note concerning group policy is the decision not to include setting NTFS permissions on user workstations. This would be a great way to further lock down the desktop and keep it that way, however, each workstation image has been set up this way in advance and it was felt that using a GPO or including these settings within the user workstation GPO was unnecessary. The study performed resulting in the GIAC network design indicated that once users are fairly well locked down, more extreme measures to further lock their desktops do not provide an equal return on investment as the initial measures. Therefore, the baseline of permissions is determined right on the master images.

4.5 Additional Security

One of the most important aspects of security outside of technical security is physical security. Physical security is often overlooked when systems are designed, or more often when systems are upgraded, it is difficult to retrofit physical security into the new design. GIAC is fortunate to be able to have its network designed from the ground up and physical security is built in. As a matter of fact, the office buildings were chosen with physical security in mind.

The Melbourne office is a freestanding three-story office building, with a data center on the interior of the second floor. The data center is slab-to-slab floor to ceiling concrete construction. The administrative staff all have offices within the data center space. Therefore, access is strictly controlled to the data center. Entry into the office building is controlled via badges with 4-digit PIN entry. To gain access into the data center space, individuals must badge in as well.

Within the data center, there is also a secure room where the log analysis system resides and Infosec spends much of its time. Backup tapes and any company sensitive information are stored in safes in this room. The offline CA server is also stored in this vault and is only turned on when a certificate has to be created and exported for EFS on sensitive company notebook computers. Backup copies of the system key floppies are also stored within the safes.

The Kauai office has been made to be fairly secure as well. While there is not much available office space, a suite in a building in Lihue was found suitable enough. It was retrofitted with some security measures. Badge access with 4-digit PIN is also required to enter the suite. Within the suite is a secure room that is also accessible only via badge reader. In this secure room is the small data center containing the site's servers, the router and the VPN/firewall. Most of the

R&D staff work at home or on the road, so the office usually contains a skeleton crew and does not need much office space.

As mentioned previously, the R&D staff enjoys working wherever they wish on their notebook computers. Since the R&D staff holds the key to the company's survival, the information stored on these notebook computers is paramount. Therefore, it was decided to use EFS to protect the information stored on the notebooks. When the notebooks were originally purchased and configured, the R&D team was in Melbourne on travel. The certificates were created and exported and given to the R&D team. Once this initial EFS rollout was complete, the plan going forward was to turn on the CA server, create and export a certificate, and hand it in person to the R&D team member. This would only need to take place with a new member of the team or the configuration of a new notebook computer. Typically, new R&D team members spend their first month at the Melbourne office becoming acquainted with the company. So this plan would not pose a problem. At this point in time there have been no problems related either to the operation of creating and exporting keys for handing off to the R&D staff or for the security of the information contained within the notebook computers.

Mentioned earlier, an important part of the measures used to keep the R&D site cloaked is hiding them within the logical network behind the VPN. From outside the network, there are two ways to reach R&D. One is to attempt to break directly in through the external router and the firewall. This also assumes the attacker knows where to direct the attack. The external router and the firewall are extremely well locked down and from an Internet perspective, only VPN traffic passes through. The second method to reach R&D is going through Melbourne first. The only information going back and forth from Melbourne to Kauai is VPN traffic. Therefore, any attacks first must make it into the Melbourne site and then be authorized to be carried across the VPN. This structure is considered to be very secure and hides the R&D site rather well.

For a small company, GIAC maintains a vigilant security awareness program. Employees are required to attend an annual briefing that restates the company security policies and any new security related information occurring within the past year. New employees must also attend a briefing. Since many companies have very lax security and allow their users to treat their computer systems as playgrounds, new GIAC employees often need this briefing in order to change their perspectives.

The backup and recovery system is a very key component to security. GIAC maintains a comprehensive plan. Daily incremental backups are performed on servers along with weekly full backups. When tapes are rotated out of the tape library, they are stored in a fireproof safe in the secure room within the data center. GIAC also maintains a disaster recovery plan that is updated quarterly.

Already mentioned previously in the Network Design section was the use of VPN technology to connect the Melbourne and Kauai offices over the Internet. The exact design and configuration of the VPN is not important to the Active Directory design other than to say that it adequately protects the information while it is communicated between sites.

Other security devices mentioned are the use of firewalls and IDS's. Their configuration and use is outside the scope of this paper, but it is important to note they exist and contribute to the overall security of the system.

A vigorous anti-virus program is maintained. Virus scanning software is installed on all workstations and it is updated automatically as new virus definitions are made available. Anti-virus software is also used to scan incoming email. GIAC also has a security policy in effect that requires all media to be scanned for viruses before it is loaded into any company system. A different vendor product is used to scan the media than is present on the system, just to provide slightly greater depth to the anti-virus program (since not all virus software may detect all viruses). This is also aided by preventing users from accessing their drives, through the application of GPO's. It is mostly the administrative staff that would find itself handling media.

A final aspect of the security program is to promote a culture to the administrative staff to use their normal user account when they are not administering the system. It is usually too easy to log in with an account with administrative privilege just to check email or to type up a document. Part of the annual security training stresses this point. Not all administrators adhere to this policy at all times, however, the response is usually worth the effort of attempting to educate the administrators. GIAC is trying to ensure administrators do not damage the system with their administrative accounts while performing normal tasks or to have their accounts compromised. The more an administrator is out there on the system with their fully capable account, the higher the probability there will be even an inadvertent miscue.

5.0 Conclusion

The GIAC network design is by no means infallible. GIAC must live in a competitive business environment and cannot afford to live in a world of risk avoidance. Therefore, the balance had to be made between security and simplicity. The network design presented in the previous pages definitely keeps the design toward the side of simplicity. But it does not sacrifice much in the way of security. Once the choices were made, the best and most affordable security options were implemented. The results speak for themselves. The GIAC network has not had any external or internal security problems and the network is considered fairly easily managed by its administrative staff. In addition, GIAC

has become an industry standard and is currently looking to leverage its success into vertical markets.

6.0 References

Active Directory Architecture White Paper. (2000) Microsoft Corporation: Redmond, WA.

Fossen, Jason. (2002) GIAC Certified Windows Security Administrator Course Material. SANS Institute.

Gustavus, Duane. IDE Raid Technology. Retrieved May 23, 2003 from http://www.unt.edu/benchmarks/archives/2001/december01/raid.htm.

Haney, J. (December 3, 2002) Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set. National Security Agency: Ft. Meade, MD.

Logon Warning Banners. Retrieved May 23, 2003 from http://www.itsc.state.md.us/info/InternetSecurity/BestPractices/WarnBanner.htm.

Windows 2000 Group Policy White Paper. (2000) Microsoft Corporation: Redmond, WA.