Global Information Assurance Certification Paper

GIAC Certification

GCWN Practical Assignment
Version 3.1

Option 1

Secure Windows 2000 network for GIAC Enterprises

Prepared by: Jason Lam

Description of GIAC Enterprises

GIAC Enterprises (GIAC hereafter) is an e-business which deals with the sale of online fortune cookies. Being in the industry for 3 years, GIAC grows at an astounding rate. The business started off with five persons and now the staff count had grown to over 150.
GIAC Enterprises generate most of its revenue through its web site (giac.org). Customers from different parts of the world would buy direct through the web site with credit card payment. Aside from the direct sale, GIAC also act as a fortune sayings wholesaler, reselling to different retailer all over the world. Most of the retailers would then translate these sayings into different languages for the local market. All the wholesale transactions also happens through the website (same domain), payments related to wholesaling would be based on a credit term basis.
GIAC's internal structure has recently been revised, there are currently four departments, each of them carries different role and functions to ensure efficient and effective business operation for the company. The departments and their functions are as follows,

Research and Development
The main duty of this department is to research and write new fortune sayings. Some of the staff research the trend of fortune sayings while other technical writers translate the new thoughts into delighted words. Due to the innovative nature of this business, sometimes students are hired as temporary for short period to extract new thoughts from the fresh minds. The department currently has 50 full-time staff and on average 10 part time employee throughout the course of the year. All the staffs are currently based in the main office building.

Sales and Marketing
A company would not prosper if its product does not sell. With 50 full time staff, the sales and marketing department is responsible for the online advertising and marketing campaign. Half of the staff (25 persons) focus on advertising the online direct sale business and corporate image, while the other half keep in close contact with wholesale partner across the world to promote the wholesale business. All of the staff in this department has recently been moved to a new office. There are recent plans to open up a few more satellite offices in different countries as an effort to expand the wholesale business in foreign countries and continents.

Finance and Human Resources
With the growth rate of GIAC Enterprises, human resources have to be efficiently managed. The Finance and Human Resources department handles the internal accounting as well as any human resources activities, such as hiring and employee record keeping. All of 25 employee in this department are based in the head office.

IT and operation

The IT and operation department is responsible for all IT requirements of the company. As GIAC is an e-business and most of the sales happen online, the stress on IT department is very high. The staffs in this department ensures that all the servers are running all the time as well as constantly updating the fortune cookies for sale after the R&D department create them. Internal computing needs is also a responsibility of the IT department. The department also has to keep the sensitive information in GIAC from leaking to un-authorized parties.

GIAC had undergone a few major changes in recent months. Two months ago, a major corporate restructure was executed to segregate responsibility accordingly. Also, in order to solve the problem of crowed office space in the head office, the Sales department has moved to a newly developed commercial area of the city a month ago. This new location is about 20 minutes drive away from the head office.

Together with all these changes, the management of GIAC noticed that the internal computer network and organization is not cooping with the organization's growth. While the management set their sight on staff count growing to 250 within a year and double that in the next 4 years, the computer network infrastructure which is formed by mixed Windows and Unix servers and clients seemed to be in a state of chaos, workstations' OSs are not consistence across the company, some files are stored locally and some centrally.

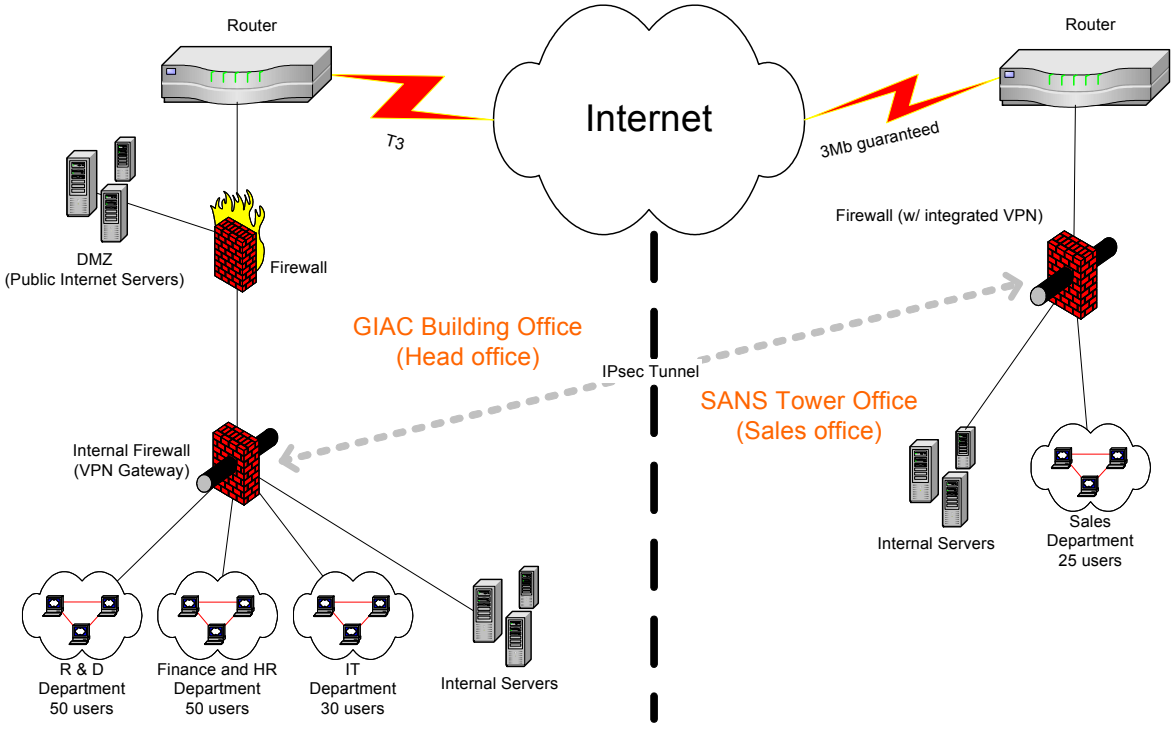
To quickly correct this problem, the management of GIAC decided to standardize on Windows internal file servers and clients and keep the mixed platform scenario for the Internet servers. For workstations and internal servers, Windows 2000 was the chosen platform for GIAC, all workstations were upgraded to Windows 2000 and future desktops all will have XP loaded.

Aside from these platform standardizations, the management also decided to implement a well design Active Directory having the following features,

- Allowing each department to participate in their own internal administration. Offloading most trivial support issues from IT department.
- Scalable, must allow each department to grow independently and freely.
- Security of information must be maintained. Since fortune cookies are the biggest asset of GIAC and such asset will be stored on the servers, information in the server must be secure.
- Controllable workstations. Having the bad experience of uncontrolled and chaotic computer workstation scenario, the importance of tightly centralized controllability has to be stressed.
- Ability to accommodate new sites, such as the planned satellite offices for sales department.
- Centralized control, eliminate redundant administration tasks and human resources for this directory service. GIAC plans to have one single IT department responsible for the IT operation throughout the company, this reduces the redundant IT cost with each department.

Network Design and Diagram

Physical network connection diagram



GIAC choose to have a VPN network to connect both offices, all inter-office communication including file sharing and E-mail will be encrypted by the IPSec tunnel between the two firewalls, so any potentially sensitive inter-office communication travelling on the Internet are secured.

A direct frame relay connection could serve the same effect but the VPN connection is chosen based on the cost factor. The cost of having a direct frame relay connection between the offices is very similar to the cost of an Internet connection of the same speed (especially that SANS Tower is a “smart building” which bundles Internet connection in the office lease).

Besides the cost advantage, there are also a few advantages of using the VPN approach. Firstly, the Internet bound traffic from the SANS tower office will go straight to the Internet which may lower latency and reduce the load of such traffic on the head office’s network (In the Frame relay scenario, all Internet traffic from SANS tower office will go through the head office first then re-routed). Also, any future office that has a VPN connection can establish a direct connection (encrypted channel) to both offices and not a routed connection through the head office, this can greatly reduce administration and equipment cost for future offices.

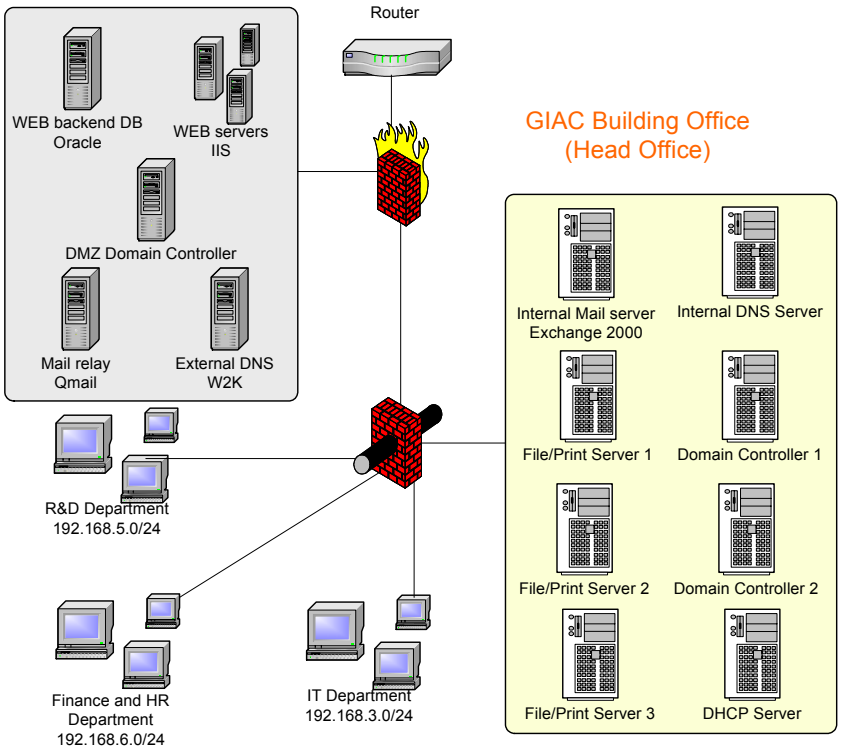
Here is a list of major security components in the diagram and their significance,

External (Main) Firewall for GIAC Building Office (head office)
The main firewall device carries an important role for GIAC's network infrastructure. It uses its stateful filtering feature to filters traffic for the DMZ public servers, avoiding unauthorized traffic from reaching to those public servers. Another of the firewall function is to allow appropriate Internet traffic to the internal firewall. These traffic would likely be the internal workstations Web traffic as well as the inter-office IPsec tunneled traffic

Internal Firewall for GIAC Building Office (head office)
This firewall segments all different internal networks which belongs to different departments. It also protect the internal servers from internal attack. Another duty of the internal firewall is to do NAT (Network address translation) for the internal host to communicate with Internet hosts. The firewall is also IPSec VPN capable, it tunnels and encrypt all traffic from internal segment of the head office to the SANS Tower Office. The VPN will feature a split tunnel which it only encrypt traffic between the two offices and according to the ruleset, allow other traffic to the Internet (via the external firewall) without tunneled.

Firewall for SANS Tower Office (Sales office)
The firewall's main purpose is to provide an IPSec tunnel for all traffic heading to the IP addresses of the GIAC Building office, as well as allowing appropriate traffic to travel between the internal workstations and the Internet, these traffic would only be the Internal host accessing the WEB. Also, the firewall segments the internal workstations from the Internal servers located in the office to avoid internal attack on the servers. Similar to the internal firewall at the head office, this firewall does NAT for the internal host with RFC 1918 addresses to conserve public accessible IP addresses.

Logical Diagram of GIAC head office



WEB Servers

The web servers are the revenue-generating infrastructure of GIAC. GIAC has settled on Windows 2000 Advanced Server with Internet Information Server (IIS) as the platform for the web site. There are currently 5 servers running in a load balanced configuration to provide fault-tolerance and high performance web serving platform. The load balancing function is provided by the built in Network Load Balancing Service (NLBS), so a separate hardware load balancer is not needed. GIAC's invested a lot of effort in its early days developing the e-business site with PHP scripting language which is still currently being used.

Since web servers are considered to be external serving servers, all web servers are located in the de-militarized segment of the network. Only computers in that segments allows incoming connections (such as web) which is obviously required by Web servers. Each of the web servers have its own IP addresses and all of the servers answers to one virtual IP addresses which is the web server's IP address accessed from the Internet. Currently, the web servers each have its own storage devices locally which hosts the dynamic web pages. The dynamic web pages interact with the backend Oracle database to access online fortune cookies and store each clients credentials and state information.

Specs of web servers
All 5 web servers are of same config P3-1G, 512M RAM, 18G SCSI HDD Windows 2000 Advanced Server with all latest patch. IIS 5.0 PHP 4.2.1

File and Print Servers

There are three file/print server in the head office, each of the server serve their own respective department. As the name implies, the file server provide centralized storage for all the users on the network. It also spool all print jobs for the user in order to provide efficient printing as well as centralized manageable printing for GIAC. The servers are properly protected by the internal firewall so only necessary traffic can get through to the appropriate server.

Specs of File/Print servers
All 3 File/Print servers are of same config P3-1G, 512M RAM, 100G RAID 1 Windows 2000 Server with all latest patch

Domain Controller 1 & 2 (Internal)

Internal domain controllers (DC) are responsible for the internal domain. They keep track of all Active Directory Information and replicate those information to other DCs in the domain.

The two internal domain controllers in the head office provide fault tolerance for each other. Both of the DC are running as a global catalog server. The roles of FSMO (Flexible Single Master Operation) is split between the two DC. While one DC has schema master and domain naming master role; the other DC has PDC emulator master, RID Master and Infrastructure master roles. This is done so that one DC is responsible for all “one per domain” functions and the other is carrying all the “one per forest” function. If in the future, the need of having other domains in the forest arises, it could simply be retiring the local domain master DC as the global catalog server (since GC and infrastructure master cannot be on the same host) and that DC can serve as the dedicated domain DC (root level).

The two DC are protected by both layer of firewalls, avoiding any communication between the DC and any Internet hosts. Access from internal hosts to the DC are also restricted to the necessary port to perform the DC functions.

Specs of internal domain controller
Two DC are of same configuration P3-1Ghz, 1G RAM, 40G RAID 1 Windows 2000 Server with all latest patches

Domain Controller (DMZ)

DMZ domain controller (DC) is responsible for the DMZ domain. This domain does not span site, since it only contains DMZ servers which are located in one location. This domain currently have less than 10 computers, the requirement on

this platform is minimal. There is only one single DC for this domain which carries all the master roles, but there are future plans to implement another DC for this domain for redundancy.

Specs of DMZ domain controller
P3-500Mhz, 512M RAM, 9G HDD Windows 2000 Server with all latest patches

Internal DNS Server

The internal DNS server responds to request for IP address resolution and resource location. The internal DNS server not only resolves internal hosts but it also forward all requests about all non-local domains to the external DNS server which will do the actual look up services. The internal DNS server does not respond to any requests generated outside of the network (due to the firewall), to avoid leaking internet network structure information. It also does not allow any zone transfer of its zones, but it downloads information from the external DNS by zone transfer to act as a secondary server of the DMZ segment, this is done so internal machines can resolve to DMZ machines. This DNS server is integrated with Active Directory and is acting as a dynamic DNS server.

Specs of internal DNS Server
P3-733Mhz, 512M RAM, 9G HDD Windows 2000 Server with all latest patches

External DNS Server

The external DNS server is responsible for name resolution of GIAC external servers as well as recursive lookup for internal workstations accessing the Internet. External DNS only contains external servers information but not internal host record, this would avoid outsider from accessing unnecessary information regarding GIAC internal network. The DNS server only process recursive lookup from the internal DNS server, for looking up name and IP addresses on the Internet on behalf of the internal workstations. This is done for the internal workstations to access C resources. The external DNS server also allows zone transfer to the internal DNS server so the internal server can have the information regarding the giac.org hosts.

Instead of having an on-site secondary DNS server resolving IP for giac.org. GIAC's management decided to outsource the secondary DNS service to a third party company. The external DNS server serves as the master and only allow zone transfer to the secondary DNS server owned by the DNS company.

Internal Mail Server

The internal mail server is running Microsoft Exchange server. It is responsible for internal messaging as well as handling all incoming E-mail from the Internet. The internal mail server does not directly send and receive E-mail from and to the Internet. All outgoing and incoming internet mails are routed through the external mail relay to strip off unnecessary header information and as an extra layer of security.

The internal mail server is located in the internal server segments, this segments does not allow any direct external connections, so servers are protected from direct vulnerability attacks. There is only one mail server in GIAC organization structure, employee from sales office would also have to connect to this e-mail server to send and retrieve mail.

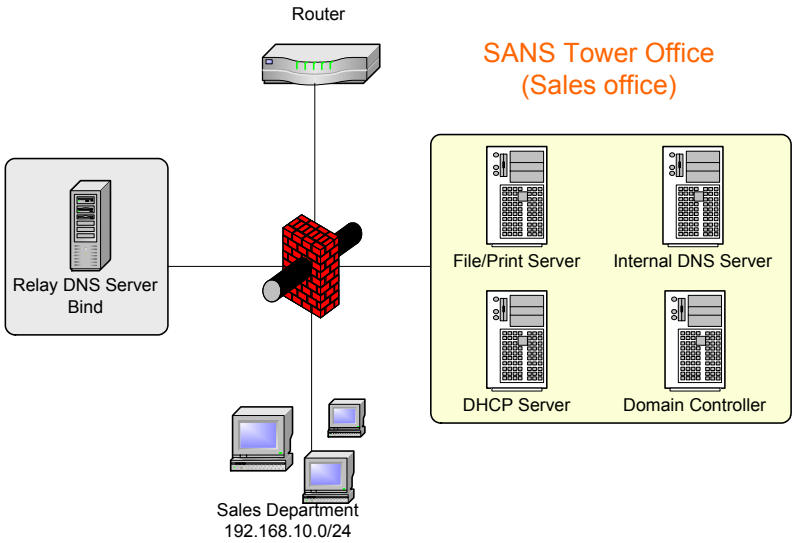
Specs of internal mail servers
P4-1.6G, 1G RAM, 36G RAID 0+1 Windows 2000 Server with all latest patch Exchange Server 2000 SP2

Mail Relay

Mail relay basically protects the internal mail server from direct attacks as well as keeping the internal network structure information from leaking out. All inbound mail from the Internet reaches mail relay and are then forwarded to the internal mail server. When the mail relay receives mail from the internal mail server, it strips off all un-necessary header information and forward it to the destination host.

Specs of mail relay
P3-500Mhz, 256M RAM, 20G IDE HDD FreeBSD 4.6 Qmail 1.03

Logical Diagram of GIAC sales office @ SANS Tower



Domain Controller

Similar to the DCs in head office, this DC is responsible for the internal domain. There are automatic replication between the head office's DCs and this DC so all Active Directory information are kept consistence across the whole domain (company). This DC is placed in this office so even if the Internet connection does down, local resources and authentication can still happen. This redundancy

avoids the Internet connection a single point of failure for all network resources in the sales office. The hardware and software specification is same as the head office.

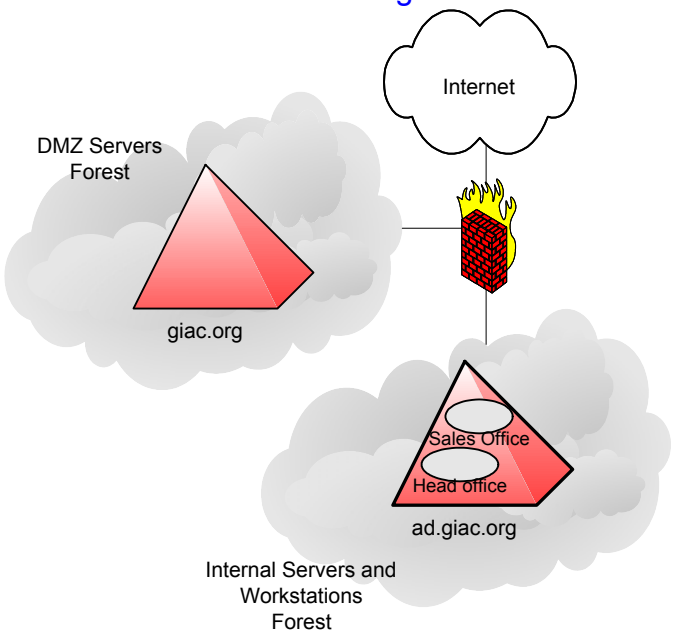
File/Print Server
Similar to the servers in the head office, this server is dedicated to provide file storage and print spool for the internal workstations at this location.

Internal DNS Server
Similar to DNS server in the head office, it serves all DNS requests by the internal clients. For all internet host resolution requests from internal clients, it would forward those requests to the relay DNS server located in the DMZ segment of this office. The server would also zone transfer the “giac.org” domain information so the internal hosts can resolve to those hosts.

Relay (Caching only) DNS Server
The caching only DNS server only respond to the internal DNS server at this location. It is basically there so that the internal server at this location does not have to consult the primary external DNS server at the head office. So, if head office’s Internet connection is down, this sales office location can still have full Internet connectivity. The caching only DNS server does not host any zone and does not know anything about the internet network structure since those information are irrelevant to the purpose of simply doing looking up for internal name server.

Active Directory (AD) Design and Diagram

GIAC forest and domain diagram



Forests

GIAC Enterprises has two forests within the organization. One forest is dedicated to the DMZ infrastructures while the other one is for the internal networks. While two forests design seems to make things complicated, GIAC's unique requirement justify for this design. Microsoft's advise on multiple forests is, "You must realize that by defining multiple forests you will be requiring users in your organization to take a series of complex steps just to use the directory."[1] It may sound very discouraging for the use of multiple forests, however, in the same literature, "a multiple forest model can be an effective tool for creating privacy and security".[2] The keyword "security" is the key to justifying this two forests design.

GIAC Enterprises operates its business based on the selling electronic version of fortune cookies which are essentially data stored in computers. GIAC's biggest asset is the data stored in the internal networks, such as the research material in the R&D department and the client information in the sales department. The leak of those information would not only cause embarrassment to the company but will cause direct lost in asset and revenue.

Since the DMZ network has to allow incoming connection to the servers, the security level is not as high as the internal hosts (which does not allow any incoming connection), therefore, internal network should be separated from the

[1] Spealman, Pg.93
[2] Spealman, Pg.93

DMZ hosts as much as possible. With this requirement, one single domain incorporating both internal and DMZ hosts is impossible because there is no separation between those objects within one single domain. Another obviously choice would be to separate the internal and DMZ network into different domains, but this would not work either because domains within a forest have transitive trust relationship between them. If one single DC in this scenario is compromised (such as the DMZ DC), all the other Active Directory information in other DC within the same forest is at risk. According to a Microsoft article on administration of Active Directory, "the breach [in security] of a single domain controller can have effects throughout a forest."[3] The only way to truly isolate the DC and prevent single compromised DC from affecting or even compromising the whole network is to have two totally separate forest in the organization in the organization.

In a two forests scenario, a compromised DC in the DMZ network will only affect the Active Directory objects within the DMZ and cannot directly compromise internal network. The only drawback to this design is administration, having two forests greatly increased the administration complexity in the organization. A set of explicit trusts relationship could seem to be a solution since this will make internal user accessible to DMZ forest's resource with one set of user credentials. However, to establish a trust relationship between the domains in the forest will require the firewall to open up a lot of ports between the DC in the two domains, which almost defeat the purpose of having separate forest, since the attacker might be able to perform a two stages attack against the internal DC.

It is a lucky fact that GIAC only allows certain individuals in the IT and production department to access the resources in the DMZ. Aside from this, most of the heavy duty web site content update are done via Oracle's SQL*NET from the IT department to the Oracle DB which has a separate access control system and not integrate with the Active Directory's authentication scheme. The other administration tasks are little enough that RRAS Terminal services is able to handle. All specific person in IT and production department having access to both forests have two separate sets of credentials for these domains/forests and these persons are explicitly told not to use the same passwords for both domains/forests. This is done to further isolate the forests and reduce the chances of an attacker using trying the same credentials on the internal network after compromising the DMZ DC.

The splitting of forests should cause very minimal disturbance to the work routine of GIAC's user. In most networks, the biggest resistance of going two forests is in the Exchange server configuration. Exchange server is complicated to configure for two forests scenario. In GIAC's scenario, Exchange does not even present in the DMZ domain, because there is really no user on that domain, just administrators (who also have account in Internal domains).

[3] Microsoft, "Design Considerations for Delegation of Administration in Active Directory"

Domains

There are a total of two domains throughout GIAC Enterprises, one domain inside each of the two forests. Corresponding to their respective forest, the domains are separated into the DMZ domain and the internal domain. With the DMZ domain bearing the "giac.org" namespace and the internal domain bearing "ad.giac.org" namespace. While "giac.org" and "ad.giac.org" may seem to have a parent and child relationship, this does not apply to GIAC's Active Directory implementation. The internal forest has only one tree and the root domain is "ad.giac.org", it is the ultimate and only parent inside that Active Directory forest. Hosts and DC in that domain would not recognize the DMZ domain as the parent domain as in the case of normal Internet DNS. The main goal of such setup is to preserve the DMZ namespace so it is identical to the Internet DNS name which can greatly enhance administration, as well as keeping the internal namespace to a logical name. Notice that the "ad.giac.org" is never recognized on the Internet simply because Internet hosts refer to the DMZ domain's DNS server for lookup and this DNS server only has hosts that belong to that segment. It has absolutely no idea about the internal name space with the prefix "ad". This can protect the architecture of internal network from leaking by DNS. In the reverse direction, the internal clients needs to know all the servers under "giac.org" from their "ad" directory, this is done by zone transfer from the external DNS server to the internal DNS servers, so the internal DNS has information of all the hosts in the DMZ.

For the DMZ domain – "giac.org", there is only single domain without any child. This domain consists of the different administrators accounts as well as the Internet servers for GIAC Enterprises. The reason to have one single domain is apparent; There is only one team of people to manage this domain, this same group is also the only user of this domain, so this does not constitute the need for multi-domains. All domain security policy can be common throughout all the servers which also allows the use of only single domain. There is also no location or replication consideration which requires multi-domain, since every object existing in this domain is located in GIAC's head office connected together by LAN connection. On the other hand, having one single domain is often recommended by Microsoft[4], since this makes the Directory design much simpler.

The internal domain "ad.giac.org" contains all the non-Internet serving hosts and users of GIAC Enterprises. This domain can be viewed as the soul of the Active Directory infrastructure of GIAC. Every workstations, internal servers and all users across the two locations belongs to this domain. With this one domain setup, all administration delegation and logical groupings happens in organization unit (OU) level.

The reason for GIAC Enterprises' internal network to have single domain may not be as apparent as the DMZ domain, but the reasons behind it is valid and sound.

[4] Spealman, P.121

The current number of employees in GIAC Enterprises is just over 150 and is considered to be a small organization, multi-domain seems to be an overkill for the company, especially since the NT SAM (Security Accounts Manager) size limitations to 40,000 objects in a domain does not apply to Windows 2000 anymore. This essentially mean the size is not a constraint to single domain design even for large organization anymore so the focus should not be on size but security, administrative and replication requirements.

As mentioned in earlier section, GIAC wanted a highly centralized and highly consistent network and computer architecture throughout the organization. Domain specific policy such as password policy and account lockout policy can be set to a default highly secure value and be consistent throughout the organization, so the need for separate domain to accommodate different domain policy does not exist. For a highly centralized administration model, GIAC has only one IT department and it is responsible for all the IT needs inside the organization. All domain administrator (as well as enterprise administrator in this single domain scenario) are trusted by the company to handle potentially sensitive information. The employees in IT department holding domain administrations all went through background security check and has been with the company for years before given such rights. This decision to have centralized administration is basically a balance between network complexity, costs and security. Management is well aware of the potential danger of administrators having access to sensitive information but the cost and complexity reduction in single domain is more important than the security of the internal risk related to administrators.

Replication may seems to be a drawback in this single domain setup, but GIAC's unique business goal and future plan seems to mitigate this problem. Since all objects in the domain is replicated throughout the domain to every DC, this means as the domain grow larger, the replication traffic will also grow. For single location, this may seem irrelevant but in GIAC's situation where future foreign sales office are planned, this may not seems to be a good choice because size replication to foreign country may be costly and the connection speed may be slow. A lot of organization split off different countries or continents into separate domains, taking advantage of the fact that in-between domain replication traffic is much less than within a huge domain. (Only global catalog is replicated between different domains). This may greatly help to reduce traffic requirement in between different locations. GIAC's future plan to setup wholesale sales office would be in highly developed countries where people are mostly literate (to make most business sense) and would most likely have high bandwidth Internet connection widely available so VPN connections in between the offices in different countries would be possible. With a high speed Internet connection, the replication can happen at night and should finishes within matter of hours at the very most. So, replication is a concern for single domain but it is not a preventing factor.

The single domain design also allows the accessing of resources in the internal network very efficient. Since resources are all inside the same domain and all the DC has information of every resources within the domain, there is no need to query another GC or another DC of another domain.

One other factor that GIAC's IT department considered during the design of the Active Directory implementation is the possibility of acquisition of another company. With the size of small of GIAC and it's uniqueness in a niche market, the possibility of finding a acquisition target is minimal, as the management would highly prefer to have internal growth rather than growth by acquisitions. The management is certain that no acquisition will happen in the next two years. And even if any acquisition does happen after two years, the target would likely be a start-up company under 100 employees. Based on this prediction, GIAC's decided that it is not even worth to plan for the accommodation of acquired company into the Active Directory, because it might be easier to manually join every computer to the existing GIAC Active Directory than to make the new company join into the forest or setup trust relationships.

Sites

GIAC currently have two office locations within the same city with a relatively high speed VPN connection between them. Each of the location would be designated a site. Even though the bandwidth between the two locations can be considered high, GIAC would like to fully utilize the bandwidth for inter-office communication (such as file exchange and VoIP) during office hours. So sites boundaries have to be created to control the replication time to after office hour and lunch time, making as much bandwidth available to other applications as possible.

Since the internal domain span two physical location, two DC is located in the head office and one DC is located in the sales office to provide fault tolerance. When the Internet connection or VPN tunnel is down, access to local (site) resources would not be affected.

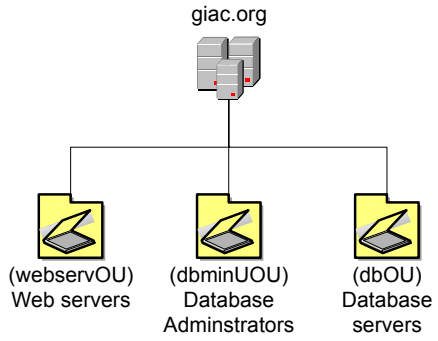
The protocol used for replication is TCP/IP, this is done because of the relatively high speed connection between the two sites. With GIAC's organization's size, the replication traffic should be easily handled by the connection between the two sites.

OU

"The primary reason for defining an OU is to delegate administration"[5] In order to delegate the popular level of administrative rights for GIAC network components and servers, OU structures are created. GIAC took scalability of OU structure into consideration while designing the OU structure so the OU layout can accommodate future growth of the organization.

[5] Spealman, P184

DMZ domain OU Design



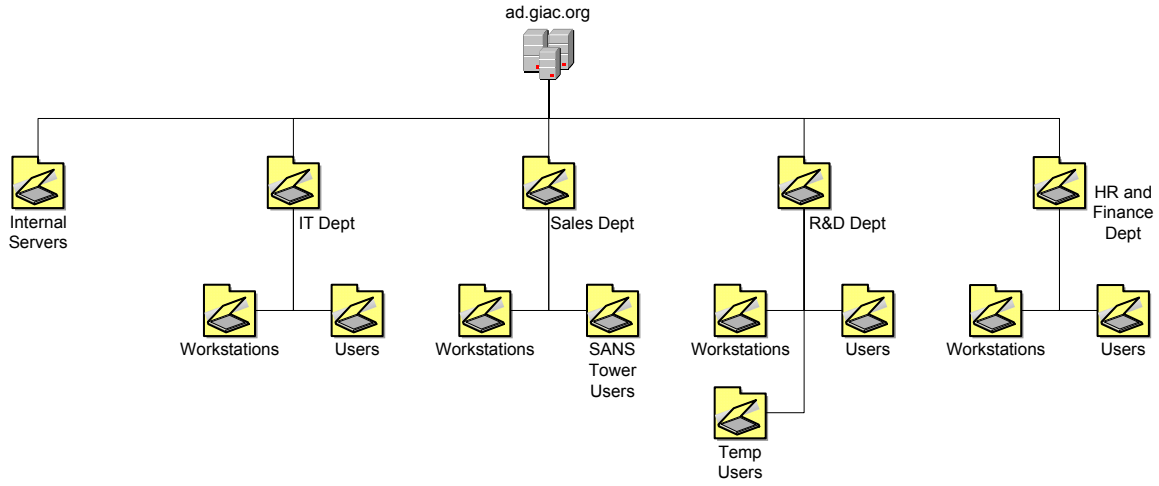
The DMZ domain has 3 OUs, one dedicated to Web servers, another to database servers and the last one to database administrators. The OU design in this domain is very simple, mainly because of the low number of objects in this domain and also the tightly controlled access to this domain.

Web servers
This OU contains the 5 web servers in the DMZ. Group policy is applied to this OU not only to apply consistent policy between the web server but also install patches on the web servers.

Database administrator
The database administrators are only responsible for database administrations tasks and are not involved in system or domain administration work. They belong to this OU which have policies to control the behaviors of their desktops.

Database Servers
This OU contains the only database server in the DMZ. While this OU is currently very small, it is expected to grow in the future. Database Servers are separated from web servers not only because of policy differences but also on patches, sometimes patches are for web servers only and are not needed on database servers. Another main differences is audit, while web server may be need to audit certain events, database servers does not need to audit those, so a separate OU is necessary.

Internal domain OU Design



Internal domain employs a nested OU structure to address the need for delegation of administration. The OU structure is similar to the actual organization structure. This is mainly due to the office and location strategy of GIAC Enterprises as well as the political requirements in GIAC. Since most offices (except head office) are expected to host one single department, the separation by department at top level should be more appropriate. If OU were separated at top level by location, each of the departments would be broken apart and department oriented policy cannot be easily implemented.

Each of the four departments each has its own OU. Each of the OU is controlled by the department head so if they decide to have department wide policy, it can be implemented here. While it seem to serve a great purpose, these top level department OU are merely logical containers for other nesting subordinate OU belonging to the respective department. The control of this OU is merely a symbol of power in the department and is assigned just for political reasons. Currently, there are no group policies assigned at any of these OUs. Policies that are implemented at this level might not be suitable for every object in the lower level such as computers and users. Also, inheritance of policy may slow down the processing of policy at execution and should be avoided at all cost.

Internal Servers
This OU contains all internal departmental file/print servers, it contains only computer objects. The policy applied to this OU have tight audit and security control on the servers.

IT Department, HR and Finance Department
Both of these OU contains both the workstations and users OU, and they are very similar in OU structure. The workstations are obviously for all of the workstations computers in these departments. Similarly, users in these departments are assigned to the OU respecting to the department.

Sales Department
This OU is similar to IT department. GIAC is ready for adding another nested OU under sales department after the sales office in another country starts up. When that happens, workstations would remain the same, since all workstations in this department, regardless of their location should remain the same but there will be a new OU for the employee at the new office to delegate administration authority. So there will be three or more OU nested under Sales Department in the future.

R&D Department
The R&D department's OU is again similar to the other departments' with the exception of a temp workstation OU. Since the R&D department employs a lot of temporary employees for research and the trust level for these employee are lower than any other staff, they would have very strict security policy to avoid security breaches by the temporary employees.

Group Policy and Security

GIAC's infrastructure relies heavily on group policy to ensure the corporate security policies are properly executed. Most of the group policies of GIAC are based on the NSA's recommended configurations for Group Policy (http://nsa2.www.conxion.com/win2k/guides/w2k-3.pdf). However, since every organizations have different requirement, GIAC modified the recommendations to suits its own requirements and policies.

Default domain policy for DMZ domain

Default Domain Policy > Windows Settings > Security Settings > Account Policies > Password Policy

Policy	*Setting*
Enforce password history	15 Passwords
Maximum Password Age	90 days
Minimum Password Age	1 day
Minimum Password Length	10 characters
Passwords must meet complexity requirements	Enable
Store password using reversible encryption for all users in the domain	Disable

Enforce password history
Computer stores 15 previous passwords, so the user cannot re-use previous password. This greatly enhances password strength since user cannot be flip-flopping between a few beloved passwords.

Maximum Password Age
GIAC's security policy requires all passwords to be changed every 90 days and this setting enforces just that.

Minimum Password Age
Minimum password age policy specify the length of time which the user is disallowed to change his/her password again followed by a password change. This setting prevents user from changing the password back to a previous one immediately after a forced password change (by the administrator or the system). In GIAC's case, the user would have to wait 1 day before he/she can change the password again. Teaming up with the password history, the user would have to at least wait 15 days (assume password is changed everyday) to revert password to an old time favorite one. Basically a deterrent for user that wants to use couple of "favorite password" that are easy to remember.

Minimum Password Length
This policy specify the minimum password length is at least 10 characters. Since most dictionary words are less than 10 characters, forcing the users to have a password with at least 10 characters forces the user to be creative about their password and hence, making dictionary brute force cracking harder. The length of the password also make the brute force password cracking more time consuming. GIAC also mandates password choosing education program and encourage user to choose pass-sentence (instead of one phase) with proper mutation (such as ROT13) and the use of non-printable ASCII password characters which can be a problem for some standard brute force cracking program.

Passwords must meet complexity requirements
If this policy is enabled, all passwords entered would have to pass the built-in complexity filter. The filter ensures that the user's password is complex enough and is not easily guessable. The requirements to pass the filter is as follows,

- Does not contain all or part of the user's account name
- Is at least six characters in length
- Contains characters from three of the following four categories:
    - English upper case characters (A..Z)
    - English lower case characters (a..z)
    - Base 10 digits (0..9)
    - Nonalphanumeric (For example, !,$#,%) [6]

GIAC would like all passwords to be complex enough so normal dictionary attack would not be successful. The attacker would have to make more brute force attempt to crack or guess the passwords.

Store password using reversible encryption for all users in the domain
If enabled, all passwords stored on the machine would be encrypted with a two way encryption instead of the default one way encryption which means passwords on the server might be retrievable if the encryption method has been known and is extremely insecure. Microsoft suggests that, "this policy should never be enabled unless application requirements outweigh the need to protect password information." [7] GIAC's does not have any application that requires such requirements so this setting is set to disable.

Default Domain Policy > Windows Settings > Security Settings > Account Policies > Account Lockout Policy

[6] Microsoft, *Passwords must meet complexity requirements of the installed password filter*, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/615.asp
[7] Microsoft, *Store password using reversible encryption for all users in the domain*, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/615.asp

Policy	*Setting*
Account lockout duration	120 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	120 minutes

Account lockout threshold
After 5 invalid logon attempts, the account will be automatically lockout for the specified amount of time. This is done to avoid or slow down brute force password cracking. In GIAC Enterprises, an attacker could possibly "try" 5 passwords and then the attacker will have to wait 120 minutes (specified by another policy) before trying another 5, this slows down the attack a lot. It might also cause interruption to normal users when they become forgetful about their password or about the caps lock key, 5 password tries is a good balance between security and user friendliness in GIAC Enterprises' case.

Account Logout duration
As mentioned in the above policy, if the user is locked out of the account, the amount of time specified in this policy will have to be elapsed before the user can attempt to logon again. 120 minutes or 2 hours is found by GIAC's staff to be a good brute force hacking deterrent as well as causing reasonable level of interruption in the case of a "forgetful" event. In such event that a legitimate user get logout due to the accidental password logout (bad password day), there is an administrator hotline to immediately re-activate the account. With the password education program that GIAC has, the number of logout incident in the organization is minimal.

Reset account lockout counter after
The invalid logon attempts count will be cleared every 120 minutes. So user will have to make sure they do not mis-type or forget their password more than five times every 2 hours. This is fairly reasonable for most situation and should not accidentally lockout user.

Default Domain Policy > Windows Settings > Security Settings > Local Policies > Audit Policy

Policy	*Setting*
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit system events	Success, Failure

Audit account logon events

Whether to audit every instances of user logon using the current computer to validate the account. This policy does not govern the local logon events but only events where user logon to a computer and that computer consult the current computer to validate the account. In GIAC's scenario, all of the account validation events are to be logged.

Audit account management
Whether to audit any of the account management events on the computer. Account management events includes adding and deleting accounts as well as changing passwords. These events are potentially dangerous and should be monitored closely, so all successful and un-successful attempts are logged. If a user somehow get access to adding a fake account with administrator privileges, the log would record such event.

Audit logon events
Wether to audit logon and logoff events to the local computer only if the account is located on the local computer. If a user logon to a workstation which authenticate with a DC, then such event will be govern by above option "**Audit account logon events**". Only when the user logon to an account which is located locally (such as a user logging into a DC locally) then this policy will be consulted. As stated above, GIAC wanted to log all logon and logoff attempts, so this policy will log both successful and un-successful attempts.

Audit object access
Whether to audit accessing of objects which have its own security ACL. [8] Notice that this policy does not mean audit of every objects but only those that have a specific ACL. Such ACL can be created at object level (usually at the properties of each object). GIAC has a few more sensitive network resources (mostly files and folders) that require close monitoring. This policy, together with auditing security ACL at object level allows the GIAC administrators to monitor objects at a highly controllable fashion.

Audit policy change
As the name implies, this policy dictates whether to audit any policy change. Such events are obviously high risk, since an improper or unauthorized policy change could lead to security compromised at a wide scale, these events are to be monitored carefully. Even un-successful attempts can mean early detection of hacking attempts. So both successful and un-successful attempts are audited.

Audit privilege use
Whether to audit the use of user rights. All events such as exercising of user rights (below) are governed by this policy. Such rights can be risky so GIAC administrators decided to log all such events.

---

[8] Microsoft, *Passwords must meet complexity requirements of the installed password filter*, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/615.asp

Audit system events
Obviously, this policy decides whether all system events are to be audited. GIAC administrators wanted to be able to know any system components failure, mis-configuration and any other system events that might help with incidents handling so such events are audited.

Default Domain Policy > Windows Settings > Security Settings > Local Policies > User Rights Assignment

Policy	*Setting*
Access to this computer from the network	Administrators, Authenticated Users
Change the system time	Administrators
Log on locally	Administrators, DB Operator
Shut down the system	Administrators

Access to this computer from the network
This policy dictates which groups are allowed to access the current computer from the network. The default everyone seems to be very in-secure since even the guests would be able to access the computers from the network. So this policy is tightened to only allow administrators and authenticated user groups.

Change the system time
This policy decides which groups have the rights to change the system time. Since Kerberos is extremely sensitive about time and any offset in time with different computer could cause authentication to fail, the system time of every computer can only be changed by the administrator groups. While this means a bit more administration tasks for the administrators, it may actually save time and resources in a long run just because of the time saved to deal with authentication problems related to offset clock tempered by user.

Log on locally
Dictates which groups of users can logon locally. Administrators and DB Operators are the only two groups of users that should be able to access the computers in this domain for maintenance purposes.

Shut down the system
Limit the shutdown rights to the specified groups of user. Since all computers are servers in this domains, it is just too risky to let anyone else other than administrators to shutdown these servers (it could effectively be an internal DoS attack). This right is left only to administrators group.

Default Domain Policy > Windows Settings > Security Settings > Local Policies > Security Options

Policy	*Setting*
Additional restrictions for anonymous access	No access without explicit anonymous permissions
Allow system to be shut down without having to log on	Disabled
Digitally sign client communications (always)	Enabled
Digitally sign server communications (always)	Enabled
Do not display last user name in logon screen	Enabled
LAN Manager authentication level	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on	Warning
Message title for users attempting to log on	By logging to this network, you are agreeing to the rules set by GIAC Management. All un-authorized access will be prosecuted.
Prevent users from installing printer drivers	Enabled
Prompt user to change password before expiration	14 days
Rename administrator account	the bad guy
Rename guest account	criminals terrorists
Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Enabled

Additional restrictions for anonymous access
Anonymous user, by default has access to resources that are accessible by the Everyone group. In GIAC's network, this is not suitable, resources are meant to be accessible by the specific user, no un-authorized access to any resources are allowed. So, unless the resources are explicitly assigned to anonymous access, all resources assigned to everyone is not accessible by anonymous user.

Allow system to be shut down without having to log on
Since all the computers in this domains are meant to run 24/7, there is no point of letting any un-authenticated user to shutdown the computer. This would improve the physical security of the computers in this domain since attacker with physical access would still need to authenticate (to become administrator, the only group that can shutdown, see above) before they can shutdown the computer and succeed a DoS attack.

Digitally sign client/server communications (always)
Enabling these two policy makes communication between server and client digitally signed, effectively avoid "men-in-the-middle" attack. These signed SMB

messages are only supported by Windows 2000 (and XP). Since there are no downlevel OS in GIAC's network, these policy are enforced in GIAC to improve internal security (These attack would only originate inside GIAC's network).

Do not display last user name in logon screen
GIAC chose not to display last user name in logon screen, the decision is very obvious, there is no point of letting any possible attacker to have an extra piece of information. It would make an attaker's job a lot harder if they don't even know a login name.

LAN Manager authentication level
GIAC operates a Windows 2000+ network without any downlevel clients or servers. It would be logical to take advantage of the strongest authentication method supported by Windows 2000 (which is not supported by downlevel OS) – NTLMv2. This policy specify the use of NTLMv2 and refusing the other inferior authentication methods.

Message text/title for users attempting to log on
GIAC's management requested everyone logging on to the network to agree to a legal notice before proceeding to access any network resources. This is strictly for legal purposes.

Prevent users from installing printer drivers
There is no point of having any printer in this domain (DMZ), hence, there's no printer driver necessary in the domain. Notice that this policy does not affect power user, so the administrators can still add printer if there's such a need. Even for a domain that has printer, it should be the administrators responsibility to install printer drivers and not the users'.

Prompt user to change password before expiration
In reference to the password expiration of 60 days (above), enabling this policy will let the user have a 14 days notice before their password expires so they can have time to think of a new password.

Rename administrator account
By default, the administrator account is called "administrator" which could be the weakness point for brute force attacker to take advantage of. This policy allows the "administrator" account to be renamed so administrator account name is not easily guessable.

Rename guest account
Similar to the above policy, but this policy is for the default "guest" account.

Secure channel: Digitally encrypt or sign secure channel data (always)
By enabling this policy, the communication between the computer account and the domain controller will be either signed or encrypted instead of letting the

client and server automatically negotiate. This option should only be applied if all clients and servers are at least Windows 2000 which is the case at GIAC. So to take advantage of enforcing signed and encrypted messages over the network, this policy is enabled.

Secure channel: Require strong (Windows 2000 or later) session key
GIAC is located in a country without US encryption export control and all servers are using strong encryption pack. To enable the use of strong encryption key across the domain, this policy is enabled.

Default Domain Policy > Windows Settings > Security Settings > Event Log

Policy	*Setting*
Maximum application log size	100000KB
Maximum security log size	20000KB
Maximum system log size	15000KB
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retention method for application log	By Days
Retention method for security log	By Days
Retention method for system log	By Days

Maximum application/security/system log size
These policies defines the maximum size the log files can grow to. Since most computers are Internet servers and having very similar logging space requirements, these settings are set at domain level. The application log are set to 100M which should accommodate enough log for incident handling and correlation.

Restrict guest access to application/security/system log
These policies specifies guest access to log files. GIAC treat log file as sensitive data because it not only contain privacy information (eg. who logged on at what time) but also configuration information which could lead to leak of configuration information to un-intended parties, which in turn could lead to configuration weakness exposed unnecessarily.

Retention method for application/security/system log
These policies specifies the retention method for logs. GIAC choose to implement the log retention system by the age of the log. Log entries older than 8 days are automatically deleted, thus providing GIAC administrator 8 days worth of live log to review and refer to. Aside from that, Administrators would backup the logs every 5 days, before the old log entries gets deleted. This creates a medium to long term log file repository for forensics and audit purposes. While any short term (in the past week) audit are being done with the log files on the server or computer.

Default Domain Policy > Windows Settings > System Services

Policy	*Setting*
Internet Connection Sharing	Disabled at startup Read for Interactive Group Full Control for Administrators
Netmeeting Remote Desktop Sharing	Same as above
DHCP Client	Same as above
NT LM Security Support Provider	Same as above
TCP/IP NetBIOS helper	Same as above
Telnet	Same as above

Internet Connection Sharing
None of the computer in GIAC utilizes “Internet Connection Sharing”, so this service is disabled. This is especially dangerous for the computers in the DMZ because any mis-configuration of the connection sharing can make the computer become a hacker’s proxy server effectively let a hacker attack third party without exposing the attacker’s true identity.

Netmeeting Remote Desktop Sharing
Similarly, Netmeeting is not used in GIAC, especially not running on the server.

DHCP Clients
All computers in the domain are running under static IP addresses and therefore there is no need for DHCP clients.

NT LM Security Support Provider
GIAC is a Windows 2000 based network, NT LM authentication is not used so there is no need to have these services running.

TCP/IP NetBIOS helper
This policy controls whether NetBIOS over TCP is available on the computer. GIAC does not use such protocol, so this policy is disabled at start up.

Telnet
Telnet is a well known insecure protocol that allows clear text messages to be sent across the network. GIAC have no need for such service, so it is disabled.

Default Domain Policy > Administrative Template > printers

Policy	*Setting*
Web-based printing	Disabled

Web-based printing
Web based printing let a user print over the network on a web interface. There has been previous IIS vulnerabilities related to web printing. GIAC does not allow web printing on any server (this policy only affect servers, will not stop clients printing to a server), so this policy is set to disabled.

User Configuration

Default Domain Policy > Administrative Templates > Control Panel > Display

Policy	*Setting*
Activate screen saver	Enabled
Hide Screen Saver tab	Enabled
Screen saver executable name	scrnsave.scr
Password protect the screen saver	Enabled
Screen Saver timeout	600 seconds

Most of the user/group specific policy are defined at the OU level. This gives high level of flexibility for the administrators to create wide range of different security settings and levels based on different OUs. The only user policy standard across all computers in GIAC is the screen saver policy. Password protected screen saver is activated for all user, this setting cannot be altered by user. This settings are to improve security for everyone in the organization when a user logon and walk away from the computer, this password protected screen saver should hopefully lock the desktop and avoid tampering when the user is away.

Group Policy for the Domain Controllers in DMZ

The policy for the domain controllers are very similar to the default domain policy. The GPO for domain controllers would be the same as the default domain policy except the differences that are discussed here.

Default Domain Controller Policy > Windows Settings > Security Settings > Local Policies > Audit Policy

Policy	*Setting*
Audit directory service access	Success, Failure

Audit directory service access
With this option, all Active directory access are being logged. On a DC, this is very important for incident handling as well as troubleshooting.

Default Domain Controller Policy > Windows Settings > Security Settings > Local Policies > User Rights Assignment

Policy	Setting
Log on locally	Administrators
Add workstations to domain	Administrators

Log on locally
Only administrators are allowed to logon locally at the DC. Other user should not have direct access to the DC as it should only be administrators' responsibility to manage the domain at the DC.

Add workstations to domain
Administrators are allowed to add workstations (computer accounts) to the domain only at the DC. So, all administrators must gain access to the DC before any workstations can be added to the domain. This prevents any malicious adding of computer account by any user in the domain.

Default Domain Controller Policy > Windows Settings > Security Settings > Event Log

Policy	Setting
Maximum security log size	250M
Maximum system log size	250M

Maximum application/security/system log size
The maximum log size for the DC should be changed to a larger size because DC has to log every directory service attempts and login attempts within the domain.

This should concludes the policies for the DMZ domain.

Internal Domain policies

The policies in the internal domain (ad.giac.org) is very similar to the DMZ domain, the policies are manually duplicated and modified to suite the need for internal domain. The differences between the policies of internal domain and DMZ domains are discussed below. Notice that the difference only occur in default domain policy, the default domain controller policy is exactly the same between the two domains.

Default Domain Policy > Windows Settings > Security Settings > Local Policies > User Rights Assignment

Policy	Setting
Log on locally	Administrators, Fulltime staff

Shut down the system	Administrators, Users

Log on locally
Obviously, the internal domain would have to let the employee logon, otherwise all network infrastructure would be useless. This policy allows all administrators and staffs to logon locally to access resources. The fulltime staff groups contains all employees in the company. This policy is not as restrictive as in the DMZ domain simply because internal domain have to serve more diverse groups of user.

Shut down the system
Systems (computers) in this domain have much different purpose than those in DMZ. Users must be able to shutdown their workstations (this means most of the computers in this domains). Although servers will have different settings in OU policy to avoid them from being shutdown or logon by any user.

Default Domain Policy > Windows Settings > Security Settings > Local Policies > Security Options

Policy	*Setting*
Automatically log off users when logon time expires	Enabled
Rename administrator account	George Bush
Rename guest account	United States

Automatically log off users when logon time expires
Some users in the internal domain would have logon time limit, this policy ensures these users are not able to access any resources outside of the valid logon hours.

Rename administrator/guest account
As discussed above, the administrator and guest account are being renamed. These account name are different between the two domains so the administrators won't be confused about which sets of credentials to use (since the two domain admin have different passwords). The byproduct of this would be more separation between the two domain in terms of security, if an attacker compromised the administrator account in one domain, the attacker would still have to start from ground up when attacking the other domain.

This concludes the minimal difference between the policies of these domains.

Additional Group Policy

Default domain policies is a very general set of policies that covers the whole domain. Certain settings or policies may not be suitable for specific group of users or computers. OU policies solves this problem, it can be applied to specific

OU to alter the default domain policies (since it is processed after domain policy) for a specific group of users or computers.

Two OU policies are to be discussed, since OU would automatically inherit all domain policies (unless inheritance is blocked, which is not the case in GIAC), only the policies having a different setting than the default domain policy would be present in the OU level policy.

1. SANS Tower users OU

The SANS Tower users OU contain users in the sales department who are currently located in SANS Tower. This OU is linked by a policy which contain only user policies, since computer (workstation) policy is already applied (linked) to the workstation OU located inside the Sales department OU much like the SANS Tower users OU.

There is only user policies in this GPO, the computer configuration settings is disabled (Under General Tab of the policy's properties). This could save some CPU cycles trying to process the computer settings.

User Configuration > Windows Settings > Folder Redirection

Policy	*Setting*
Application Data	Basic, \\Salesserver\ home\%username%
Desktop	Basic, \\Salesserver\ home\%username%
My Document	Basic, \\Salesserver\ home\%username%
Start Menu	Basic, \\Salesserver\ home\%username%

These policies setup folder redirection. For the user roaming to truly work, all user data should be located on the server. These redirections ensures that the applications settings, desktops and my documents folder are all on the server, so the user can travel to other workstations to work on the data without any problem. One of the biggest advantage of having all user data on the server is backup, all data on the server are backup regularly to protect the integrity of the data.

User Configuration > Administrative Templates > Windows Components > Internet Explorer

Policy	*Setting*
Disable Internet Connection Wizard	Enabled
Disable AutoComplete for forms	Enabled

Do not allow AutoComplete to save passwords	Enabled

Disable Internet Connection Wizard
This policy controls whether the Internet connection wizard is available to the user. Configuration of the Internet connection setting should be a task of the administrators. User should not have the rights to alter such configuration.

Disable AutoComplete for forms/ Do not allow AutoComplete to save password
These two policy dictate whether the user can use AutoComplete feature for Internet Explorer. This feature saves the responses to web form the first time and later fill in the same form for the user on the next exit. A lot of user uses this feature to store passwords which potentially compromise the security of the password. There are also a lot of privacy issues related to GIAC storing such form for the employees. So, the AutoComplete feature is disabled for most users (even in other OUs) in GIAC.

User Configuration > Administrative Templates > Start Menu & Taskbar

Policy	*Setting*
Remove Network and Dial-up Connections from Start Menu	Enabled
Disable personalized menus	Enabled
Disable and remove links to Windows Update	Enabled

Remove Network and Dial-up Connections from Start Menu
User in this UO should not be configuring any connections. Therefore, the menu item is not shown in the start menu.

Disable personalized menus
Personalized menu tends to hide seldom used programs away from the menu and only shows often used ones until user choose to extend the menu which then shows all menu items. This often causes confusion to the user and therefore is set to enabled which disable this feature.

Disable and remove links to Windows Update
When set to enabled, the Windows Update option is not shown in the start menu and it also blocks user's access to the update website. Updating Windows should be a responsibility of the administrators, so this policy is set to enabled.

User Configuration > Administrative Templates > Desktop

Policy	*Setting*
Prohibit user from changing My Documents path	Enabled

Prohibit user from changing My Documents path
This policy basically works with the redirection of folders. After the redirection, the user may still change the My Documents' location away from the server. To avoid this, this policy is set to enable, preventing the user from storing files elsewhere.

2. Temp User OU

Temp User OU contains user that are working as temporary for R&D departments. These are usually students working as part-time for GIAC. The trust level for these workers are lower than the full-time employee which went through background and financial check at hiring. These temporary employees works at specific desks (area) dedicated for them, they are not assigned any specific desks. The computers for these employees would have heightened security settings, but such settings would not confuse or affect the work of these temporary staffs. Notice that sometimes other employee from other office (and other departments) would be involved in the creative development projects of the R&D department and these roaming user would also use these temporary computers with more restrictive settings.

This OU has a GPO linked to it which achieve the higher security level limited to these computers and users. This GPO would include both user and computer settings, it would also inherit the domain settings like all other OUs. Due to the inheritance of policy from domain, the GPO would only contain the difference between the intended settings and the domain settings. This GPO would be in loopback processing mode, which means no matter who logs on to the computers in this OU, their original policy shall be ignored and the current computer's OU GPO would be applied. The Temp User OU would also include all policy defined above in the SANS Tower User OU (unless re-defined below).

Computer Configuration > Administrative Templates > System > Group Policy

Policy	*Setting*
User Group Policy loopback processing mode	Replace Mode

User Group Policy loopback processing mode
As mentioned above, the loopback mode would be enabled for this GPO so all computers with this GPO applied would not respect the original user settings (related to the user) but instead apply the setting in the current GPO. The replace mode means ignore all existing user settings and replace all user setting with settings from the current GPO.

Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment

Policy	Setting
Log on locally	Administrators, Fulltime staff, Parttime Staff

Log on locally
Parttime Staff group of user should also be allowed to login at these workstations.

Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options

Policy	Setting
Allow system to be shut down without having to log on	Enabled
Prevent users from installing printer drivers	Enabled

Allow system to be shut down without having to log on
With this policy enabled, there is a shutdown option at the login prompt. Since these workstations may not be utilized all the time, this option is convenient for shutting down the computers without logging on. There is not much of security risks with these computers since they are used as console workstations and this policy can only allow un-occupied workstations to be shutdown.

User Configuration > Windows Settings > Folder Redirection

Policy	Setting
Application Data	Basic, \\RD\home\%username%
Desktop	Basic, \\RD\home\%username%
My Document	Basic, \\RD\home\%username%
Start Menu	Basic, \\RD\home\%username%

Similar to the redirection in the Sales OU (above), all users' files are stored in R&D's server. All work done by the user can be saved to the R&D server.

User Configuration > Administrative Templates > Start Menu & Taskbar

Policy	Setting
Disable programs on Settings menu	Enabled
Add Logoff to the Start Menu	Enabled

Disable programs on Settings menu

With this policy enabled, the settings menu are not shown. This can further avoid user from tampering with the workstations.

Add Logoff to the Start Menu
This policy dictates whether a logoff item is shown in the start menu. Putting the logoff item on the start menu can simplify logoff process, so the user does not have to search around for logoff item. This can help to prevent user walking away without logging off.

User Configuration > Administrative Templates > System

Policy	*Setting*
Disable the command prompt	Enabled
Disable registry editing tools	Enabled

Disable the command prompt
When enabled, this policy will stop the user from running the command prompt (shell). This effectively reduces tampering with the workstations. However, this is still not a foolproof preventive measure, the user is still allowed to run batch file scripts. It would only stop low level malicious user from tampering.

Disable registry editing tools
When enabled, this policy will prevent the user from using the registry editing tools. Similar to the policy above, the less the user can tamper with, the more secure the network can be.

Additional Security

The powerful Group Policy helps GIAC to enforce a lot of security policy, however, it is no “silver bullet” for securing the infrastructure. GPO still cannot enforces some security requirements that are needed by GIAC Enterprises. Below is a list of requirements and issues that cannot be addressed with the use of GPO in GIAC Enterprises.

Malware (virus and trojan horse)
Group policy does not offer any protection or defense against virus. Detection and eradication has to be done with third party tools, since Microsoft does not have any anti-virus products. The two main entry points of virus are file download and E-mail, and to a lesser extend physical media (CD, DVD). The true protection is to scan all incoming files before they are run and to educate the user not to run anything unnecessary or suspicious. Anti-Virus software should be installed at workstations and configured to at least scan periodically (if not set to scan all opening file). Also, anti-virus software should be installed at the E-mail server and scan all incoming e-mails for virus.

Although GPO does not handle or mitigate threats from malware, it could be used to distribute new virus signature for the anti-virus software. All virus signature should be kept up-to-date and not up-to-week because modern virus tends to spread very quickly inside an organization.

Social Engineering aspects

Social Engineering is one part of security policy that cannot be addressed just by GPO. In fact, its causes have nothing to do with the computers or networks. A simple, common and yet still quite effective social engineering method to compromise password would be to call up a person in a company and then pose as the administrators from IT department asking them their username and password and tell the victim it is needed for maintenance. This approach works (most of the time) because of the general trust relationship between human beings and the worries of losing the computer account.

It should be obvious that these attacks would never be easily solved by computer security policy (such as GPO) and security settings. The only true solution is to educate the user of not exposing any unnecessary information to anyone and basically preach to every employee to make them as paranoid as the administrators. This is not an easy task by any means but is necessary to properly secure the network.

In GIAC's scenario, this education process would be much simpler due to the size of the organization. Especially with delegated administration tasks, all users would basically know the persons responsible for administrating their accounts, so the above mentioned scenario would not easily happen. However, social engineering leading to information leak is not limited to user account information and would still take a lot of education for the users to learn to be "careful".

Network (physical) Security

GPO does not interact with any of the networking equipment and does not manage any of them in GIAC. All networking equipment are managed separate of the Active Directory structure. If there is a mis-configuration in the networking equipment or mis-managed network, it could lead to some internal malicious attacker having the possibility of plugging in a computer (such as a notebook) to the network via an unused network jack. The possibility of this happening is very high, even if there is no empty jack, users could unplug some existing connection and plug in the malicious computer. With this malicious computer connected, the user could theoretically scan the network for vulnerabilities and attack any un-patched server. All of these cannot be controlled from the GPO.

There is current development of CNS (Cisco Networking Services) and DEN (Directory-enabled Networking) that addresses some of these issues. Short term mitigation can be enforcing MAC address at switch level. But this could only slow attacker, since MAC address can still easily be forged. There is no easy solution to this problem except to pro-actively enhanced internal security and maybe to utilize IPSec (with authientication) to ensure only authorized computer are allowed to connect and communicate.

Notification or detection of events
GPO does not specify or manage any intrusion detection effort in the organization. GPO basically provides a means of configuring logging or audit so it can be consistence within the management unit. There is however, no mechanism to detect any malicious attempts of using the network resources or even hacking attempts. Intrusion detection can be done at the host level or the network level, both of these detection methods are not provided by GPO itself but other tools and human effort. In todays network environment, intrusion detection in an organization is a necessity.
Whether GPO is implemented or not, most of the log analysis would still have to be done manually. Tools are available to ease this task but human effort is still required.

Backup
Backup is obviously one of the important tasks in a network as all equipments are bound to fail at some point of time and data could be lost. Data integrity is clearly one of the goal in information security. In regards to backup, group policy does not offer any functions or features for backing up data. All of the backup would have to be done with third party software. In GIAC's scenario, backup would mostly happen from the server since all client data are stored on the server. Notice that it is also essential to backup the Active Directory itself, Windows 2000 has its own backup utility (developed by Veritas) for backing up the Active Directory on the DC.
Aside from the actual backup, GIAC also requires a logical backup and restore procedure/policy which mandates the frequency of backup and how to securely store the backup media.

WEB server program
Since GIAC runs a web server with customized PHP scripts as the basis of the e-business serving platform. The security of these programs has to be constantly audited by the staff and internal quality control team. Any of the vulnerabilities in the PHP scripts on the website could be a serious threat to the security of GIAC Enterprises. The security requirement of such program development cannot be configured or managed by group policy. The only way to improve program security is to focus on security at planning stage and possibly employ third party to audit the source code of the programs (if budget allows).

Hotfix (MSI)
Group policy provides a means of remote installation of software, this greatly saves the time of the administrators. This would have been a great way to distribute hotfixes and other patches to workstations or servers. Microsoft does not currently provide any hotfix in the MSI package format which is required by the software installation in GPO, so officially hotfixes can still not be distributed by group policy.
There are instructions on the Internet (https://lspservices.iupui.edu/docs/win2k/hotfix.asp) on how to manually create

the MSI package required for the remote distribution. This is un-supported by Microsoft, so the user is taking his/her own risk, but it is currently the working solution to remotely distribute patches.

References:

Meredith B. Derby, “Single forest vs. multi-forest Active Directory design”, 13 Mar 2002, http://searchwindowsmanageability.techtarget.com/originalContent/0,289142,sid33_gci803579,00.html

Microsoft, “Design Considerations for Delegation of Administration in Active Directory”, http://www.microsoft.com/windows2000/docs/addeladmin.doc

Rick Kingslan, “Sanity check please!“, http://www.mail-archive.com/activedir@mail.activedir.org/msg01950.html

Brian Arkills, “Windows 2000 Server Security Checklist”, 24 May 2002, http://windows.stanford.edu/docs/w2kservseccheckl ist.htm

Microsoft, “MSDN Library”, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/615.asp

Melissa C. Craft, Thomas Llewellyn, “Windows 2000 Active Directory Second Edition”, Syngress Publishing Inc.

Jill Spealman, “Designing a Microsoft Windows 2000 Directory Services Infrastructure”, Microsoft Press.

Brian Komar, “Designing Microsoft Windows 2000 Network Security”, Microsoft Press.

Sakari Kouti, Mika Seitsonen, “Inside Active Directory: a system administrator’s guide”, Addison Wesley.

Philip Cox, Tom Sheldon, “Windows 2000 Security Handbook” Osborne.

Micky Balladelli, Jan De Clercq, “Mission-Critical Active Directory”, Digital Press