Global Information Assurance Certification Paper

Kathleen A. Durkin

Giac Certified Windows Security Administrator (GCWN) Practical Assignment
Version 3.1 (Revised April 8, 2002).

Assignment Option 1 – Design a Secure Windows 2000 Infrastructure

Title: The Design and Implementation of a Secure Windows 2000 Infrastructure for GIAC Enterprises

Abstract:

This paper deals with the design of a windows 2000 infrastructure for a sample corporation, GIAC Enterprises. The focus on this paper is in the security aspects of the infrastructure. The Active Directory elements are designed along with Group Policy Objects. These Group Policy Objects form the core of the security of GIAC Enterprises and a variety are described including those for the Domain, Domain Controllers, DMZ servers, and user desktops. In addition, further security measures are described.

Description of GIAC Enterprises:

GIAC Enterprises is a chemo informatics company with a global customer base. They specialize in selling web based internet access to scientific databases. Access to this data is sought by various industries involved in cutting edge molecular research. Their customer base includes the pharmaceutical, semiconductor, materials and coatings, and health care industries. Access to the data products is based on annual or monthly subscription fees.

The web based data access depends on GIAC's proprietary database engine called ALLMOL. ALLMOL is the core database technology upon which all of the data interface products depend and provides high speed data retrieval of complex molecular data.

The data interface products which access ALLMOL are client side web browser plug-ins. These plug-ins provide appropriate graphics interfaces which allow users to define their data search criteria. There are a variety of data products which customers may access. Customers use specific plug-in features based upon which data product they wish to access.

The data products for sale via internet access include:

LD50: a database of information about how much of a given substance is required to kill 50% of a population of standard lab mice. Users can search by molecule name, chemical formula, or optionally they can draw in a whole or partial chemical structure.

FP: a database of information about the reactivity and volatility of molecular substances. The data includes the known flash point, explosive characteristics, and other safe handling information. In addition to searching on name, formula, or structure, users can search based on keywords related to known industrial accidents (dates, locations, company name).

JA: a database of information about the status of molecular substances as they are controlled Federal Narcotics and Export Statutes. Manufacturers need to verify the molecular substances they make, transport, sell, or export are handled according to federal guidelines as specified by the Justice Department. In addition to searching on name, formula, or structure, users can search based on keywords related to statutes, countries, tariff types, etc.

In addition to the internet data access, GIAC Enterprises also markets custom database design and installation for companies wishing to use the ALLMOL engine to search and store their own data. Chemical and pharmaceutical manufacturers need good data storage systems to keep track of all of their products in development. In addition to selling on-site database design, GIAC Enterprises also markets consulting and training.

GIAC Enterprises maintains close ties to university researchers who partner in algorithm research and development.

The main units of GIAC Enterprises include:

Research and Development: This is a team of scientists and engineers who operate under the guidance of product managers. There is a Core Product Manager whose team does the basic database design and development. In addition to this Core Team, there is a group of Data Product Managers whose teams are responsible for the development of individual data and data interface product lines. These Data Product Teams also keep the data products current by updating the content. Content updating is a big effort which requires constant monitoring of publicly available information, data entry, data verification, and so on. Because of the cutting edge nature of the databases, it is important for the R&D teams to have close ties with the Customer Service unit of the company. To this end, each product manager of a Research and Development team has an individual partner manager in Customer Service. This Customer Service Partner Manager handles the support aspects of any data product brought to market, from their specific Research and Development Product Manager's team.

The Core Product Manager for R&D has ties to various university research programs which specialize in basic and applied database research. In addition, this Manager is the leader in starting potential new data products.

Customer Service: This unit handles all support aspects for data and data interface software marketed and sold by GIAC Enterprises. This includes the custom design, training and consulting aspects of the business. The personnel in this unit include help desk technicians, software and service training specialists, and engineers who provide consulting and specialized database installation. This unit is the core of the commitment to quality for the customer base. It has close ties to the Research and Development unit as well as to the Sales and Marketing unit.

It should be noted that Customer Service not only provides the basic support bundled with all data access sold by GIAC Enterprises, but also sells service agreements and training as additional products. For example, a typical data access subscription contract comes with help desk support, Monday through Friday, 9 to 5 EST. If a customer requires a higher level of support, additional service agreement packages are available for purchase.

Each Customer Service Product Manager handles only one of the major data product line made by the company. There is a Senior CS Product Manager who oversees all of the individual CS Data Product Managers. This Senior CS Product Manager also oversees the interaction of Customer Support with the Legal and Sales and Marketing units.

Legal: This unit handles patent applications and proprietary software license agreements. They also manage joint research agreements with their university research partners. Each legal team is assigned one or more Research and Development Product Managers. The legal team handles those issues related to those data products developed by their assigned R & D partner.

Sales and Marketing: This unit develops sales materials and documents. They also do market research, customer surveys, and onsite demonstrations. They work with Legal for review of sales materials but their closest partner internal to GIAC Enterprises is the Customer Service unit. In many companies, Customer Service is a direct subsidiary of Sales and Marketing. However, for GIAC Enterprises, the Customer Service unit generates revenue through its training and service products, and is therefore a product creation entity analogous to Research and Development. Thus Customer Service is more of a partner to Sales rather than a subsidiary.

The personnel in Sales are essentially independent agents, working on commission. Marketing is a separate subunit, designing materials, and doing market research. Each subunit (Sales, Marketing) has a manager. These individual managers report to the Senior Manager for Sales and Marketing. The Senior Manager in this unit works with the Customer Service Senior Manager to perform two functions: specification and review of contents of marketing materials and, handoff of new sales clients to individual Customer Service Product Managers.

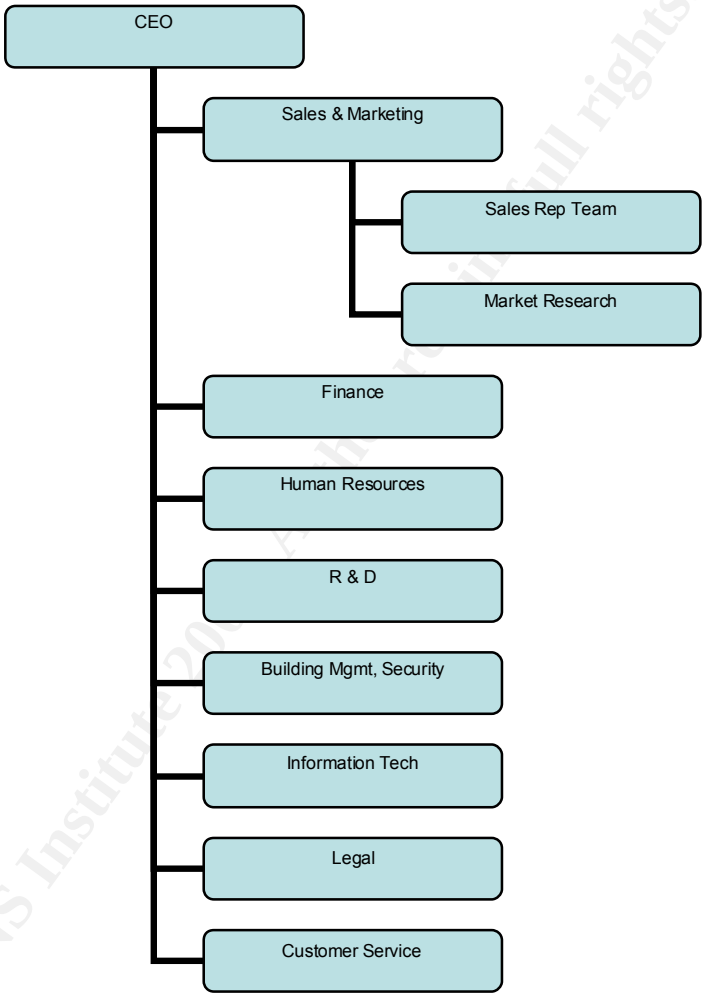
Human Resources: Human Resources is a division which handles all of the standard personnel services.

Finance: Finance is a division which handles customer billing, budget allocation to each of the corporate divisions, expenditure accounting and long term financial planning.

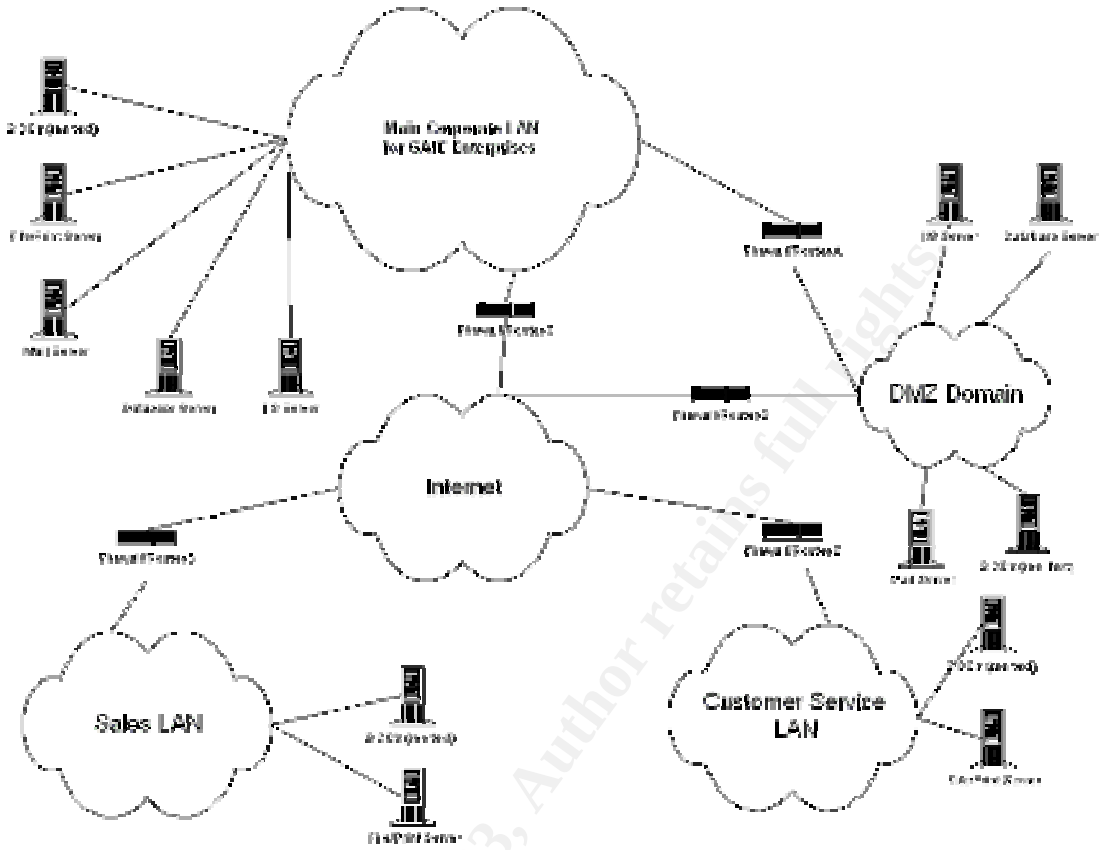
Information Technology; Building Management and Security: These two divisions support infrastructure and security. It should be noted that the proprietary nature of the database design along with the intense competition at the cutting edge of modern scientific research means that corporate security is paramount, particularly for the Research and Development unit. This includes physical security at the various locations along with information technology security.

Each of these unit divisions is lead by a Senior Manager who answers directly to the CEO of GIAC Enterprises.

The basic corporate layout is described below.



Network Design & Diagram:



There are 3 separate main LANS that make up the units of GIAC Enterprises. Sales & Marketing is located in the Boston Area. This location was chosen as part of a strategic effort to expand sales in the Biotechnology sector which is growing rapidly in Boston. Customer Service has offices in the New Jersey Area, reflecting the current large client base in the chemical industry. Corporate Headquarters is located in Berkeley, CA and includes all of the remaining units of the company. This location reflects the original site of GIAC Enterprises as started by a graduate of the University of California.

In addition to the 3 main LANS, there is a single DMZ LAN segment. This DMZ is physically housed in the Corporate Headquarters location but is logically isolated from the main corporate communications traffic. This will be discussed in more detail below.

Each separate main LAN is a firewall protected entity with two Domain Controllers, along with File and Print Servers. The separate LANs are connected to the commodity internet but are logically connected to each other as a single corporate intranet.

The DMZ segment supports the publicly available IIS server. This IIS server contains freely accessible public information including marketing and sales materials, contact information for sales, job postings for human resources, and related materials. This IIS server also contains the web interface for the paying customers of the data products. Customers who are authenticated on the server are allowed access to the data products. Customers who are not authenticated are redirected to a web page listing contact information for Sales representatives.

This DMZ segment also supports a database server running the GAIC Enterprises database engine, ALLMOL. The web based data product interface, which runs on the DMZ IIS server, makes calls to the DMZ database server. Customer queries are input into the IIS server interface and then passed on to the database server. The database query responses are returned to the IIS server and thereby to the customer. These servers are behind a firewall to provide a line of defense against hackers. The DMZ database server is a redundant copy of the main corporate LAN database server. The DMZ database server only accepts traffic from the IIS server on the DMZ segment or traffic from the main database server behind its firewall. In the event of corruption however, the DMZ database server can be replicated from the main database server.

There is also a mail server on the DMZ. This is a Windows 2000 server running IIS but only the SMTP processing is enabled. DNS MX records list this as the root level domain name for the purpose of mail delivery. Mail received by the DMZ mail server is sent over the firewall/router A every 15 minutes. It is sent to the internal mail server on the corporate LAN. In a like fashion, the internal mail server sends outgoing mail across the firewall/router A every 15 minutes. In addition, there is a single Domain Controller on the DMZ LAN.

The Firewall/Routers labeled C, D and E are actually each two physical units. C, D & E are each made of and outer firewall and an inner RRAS server. The outer units, connected to the commodity internet, are basic static packet filtering firewall appliances from SonicWall, model SOHO3. These firewalls are all configured to forward traffic only to and from the IP addresses of the 3 inner RRAS servers. Further, only L2TP packets are allowed. Packets with a destination of UDP port 500 or protocol ID 50 (ESP header) are allowed. Outgoing packets are allowed with a source of UDP port 500 or protocol ID 50.

The inner units are Windows 2000 RRAS servers. These RRAS servers are used to effectively create a single logical intranet by acting as VPN channels between the three main LAN units. These run Windows 2000 with the High Encryption Pack installed. This requires Service Pack 2 which is also installed. The communication between these routers uses 168-bit 3DES with L2TP over IPSec. This includes ESP encryption on the payload of the packet. The RRAS routers are configured to drop all packets coming from systems other than those from their partner VPN routers. Note that RRAS servers are provide backup to the firewalls by doing their own packet filtering. These RRAS servers accept only

packets destined for UDP port 500 (IKE) or packets destined for UDP port 1701 (L2TP). In this step, we consider port 1702 because RRAS doesn't see the protocol ID for the ESP header. IPSec strips it off before passing the packet to the RRAS service. Further, outgoing packets are similarly filtered, allowing only UDP source port 500 or 1701 packets to pass. Fragmented packets on UDP 500 are allowed since packets containing certificates can be fragmented.

Each of these RRAS servers has a computer certificate and the Root CA certificate installed. Since there are only a few RRAS servers of configure, these certificates are obtained and managed with the Certificates MMC snap-in on the individual RRAS servers.

These RRAS servers have static IP addresses and act as DHCP servers on their individual LAN segments. The RRAS servers are high speed processor systems with special network cards designed to handle IPSec traffic at the hardware level.

The Firewall/Router labeled A is also a firewall and RRAS server pair. It has a similar configuration to C, D and E with a few exceptions. The firewall unit is on the DMZ side and the RRAS unit is on the corporate LAN side. Neither unit provides DHCP service. Each server on the DMZ LAN has its own static IP address. C, D and E are RRAS servers that handle router to router VPN traffic over the internet. RRAS server A only handles traffic between the corporate LAN and the DMZ servers. The firewall and RRAS server only allow traffic for updates of the database and IIS servers in the DMZ, along with the SMTP traffic. This update traffic is sent over SSH/TCP. Only this port is allowed. SMTP traffic is sent across the SSH/TCP channel. Only traffic from specific IP addresses on the corporate LAN is allowed to the go to the DMZ servers at carefully controlled time intervals. These DMZ servers are also specified by IP address in the filtering rules.

The Firewall/Router labeled B is a single hardware firewall appliance as described above. No RRAS server is required here. The firewall itself provides packet routing to the DMZ LAN. This firewall only allows traffic that is HTTP (port 80) or SSL (port 443) based that is directed to or from the IP address of the IIS server. In addition, it allows SMTP traffic (TCP/port 15). It does not allow traffic directed to the IP address of the DMZ database server. The DMZ database server has packet filtering rules which only accepts traffic from the DMZ IIS server or from the database server inside the main corporate LAN (traffic passing through router A).

The email traffic within the corporate VPN is handled entirely by the mail server on the corporate LAN. Only mail that is incoming or outgoing to the internet is transferred through the DMZ mail server.

The basic configuration for all of the main servers in GIAC Enterprises is Windows 2000 with the High Encryption Pack (along with Service Pack 2). This

suite includes the Domain Controllers, File & Printer servers, Mail servers, database servers and IIS servers. One of the domain controllers in the main corporate LAN is an Enterprise Root Certificate Authority. Keymigrate.exe has been run to upgrade the private key protection on this and all certificate servers. This domain controller is also the DNS server for the corporate network. Domain controllers on each other LAN (on the Sales LAN and on the Customer Service LAN) are also Certificate Issuing Authorities. This two-tier model is sufficient for a medium sized company like GIAC Enterprises.

The IIS server (version 5.0) in the DMZ has its own IP filtering rule set that acts as a fall back for the packet filtering on the firewall/router. The public information traffic is over ordinary HTTP (port 80) but customer authentication and database access requires SSL (port 443). 128-bit SSL encryption is required for customers in order to protect the privacy of access to the proprietary database product. Access from source port >1023 to destination ports 80 or 443 is allowed. The IIS server is a 2.8GHz dual Xeon system with 1GB RAM and uses hardware based RAID (total disk mirroring). Separate volumes are used for content, operating system, and logs.

IIS server content and database content are updated by corporate personnel *inside* the main LAN. Content managers *do not* access the DMZ systems directly. Only system administrators control content transfer into the DMZ.

All primary servers have redundant power supplies and RAID hardware for disk redundancy. In each case the Active Directory database and the associated log files are on separate volumes formatted for NTFSv5. Circular logging is used but data is saved with incremental tape backups. Further, the Domain Controllers have identical twin backup systems which can be used in a “failover” scenario in case of main system failure. Currently the DMZ IIS server is a single system but there are plans for a load balancing solution as customer demand increases.

All of these servers are physically secured, in locked rooms available only to authorized administers. Similar arrangements exist for tape backup systems.

The database server in the corporate LAN diagram (for the ALLMOL product) actually represents two systems – a “stable” database release used to update the DMZ database server, and a second “testing” database system used by actively working engineers for patch and upgrade testing.

All Corporate intranet client systems are exclusively Windows XP with High Encryption Pack installed.

Active Directory (AD) Design and Diagram:

The Windows 2000 AD Domain structure for GIAC Enterprises follows the DNS domain naming structure. The DNS name for GIAC Enterprises is giac.com. The Windows 200 AD root domain for GIAC Enterprises is corp.giac.com. Most of the corporation exists in this one single root domain. Second tier domains exist for Sales (sales.giac.com) and Customer Service (cserv.giac.com). While it has the name of a DNS style sub domain, the DMZ domain (dmz.giac.com) is not actually part of the main GIAC Enterprises AD forest. This was a done to better control trust relationships. More discussion on this point will follow.

The decision to create second tier domains for Sales and Customer Service was based on security and replication issues. It is not necessary for the logical domain structure to follow physical site structure but GIAC Enterprises is structured in this fashion for several reasons. Due to the distance between sites, it was determined to be more flexible to allow for local administration and control at the sub domain level. Since there is a lot of turnover in the workforce in Sales and Customer Service it was determined to allow local administration of user accounts these domains. Further, marketing and sales representatives are either on commission or on contract. They are basically independent agents. They have no need to be logically considered with the rest of the corporate structure.

The Customer Service unit does a great deal of hands on work with clients. This interaction was perceived to be a possible security issue with the possibility of corrupt file transfer or inappropriate access. By structuring Customer Service as its own domain, it was hoped to mitigate this threat.

The sites are configured to replicate the Global Catalog. It is easier replicate Global Catalog traffic rather than the entire AD database.

Since the entire Windows 2000 domain for GIAC Enterprises is made up of Windows 2000 servers and Windows XP clients, all Domain Controllers are set up without permissions compatible with pre Windows 2000 clients. Null user sessions are not allowed. This is to enforce security over the contents of the AD database. Domain Controllers operate in Native Mode. The company operated in mixed mode for over a year while the transition was made to fully Window 2000 compatible applications on all legacy systems.

There are three physical sites for the company and these are matched in the Windows 2000 AD Sites for the purpose of AD replication. Active Directory Global Catalog Replication between Domain Controllers in different sites uses RPC-over-IP. Replication occurs over the IPSec secured VPN. The Sales site and the Customer Service site each consist of a single subnet. The Corporate Headquarters site has several subnets.

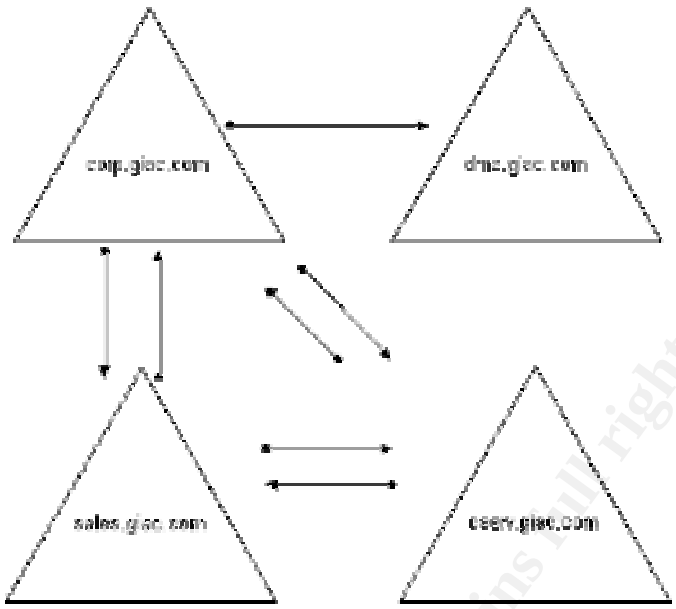
All of the GIAC Enterprises DC servers use the High Encryption Pack. All Domain Controllers are physically secured in locked rooms available only to authorized administers. The log files on the DC's are regularly monitored, particularly for failed access attempts to \NTDS and \SYSVOL. The files permissions on \NTDS are set to Administrators:Full Control, System:Full Control.

There are two Domain Controllers in the main corporate LAN. Each has separate FSMO roles. One is the RID Master, Schema Master and Domain Naming Master. This also serves as a Global Catalog Server. There is no need for PDC Emulation but the second Domain Controller is the Infrastructure Master.

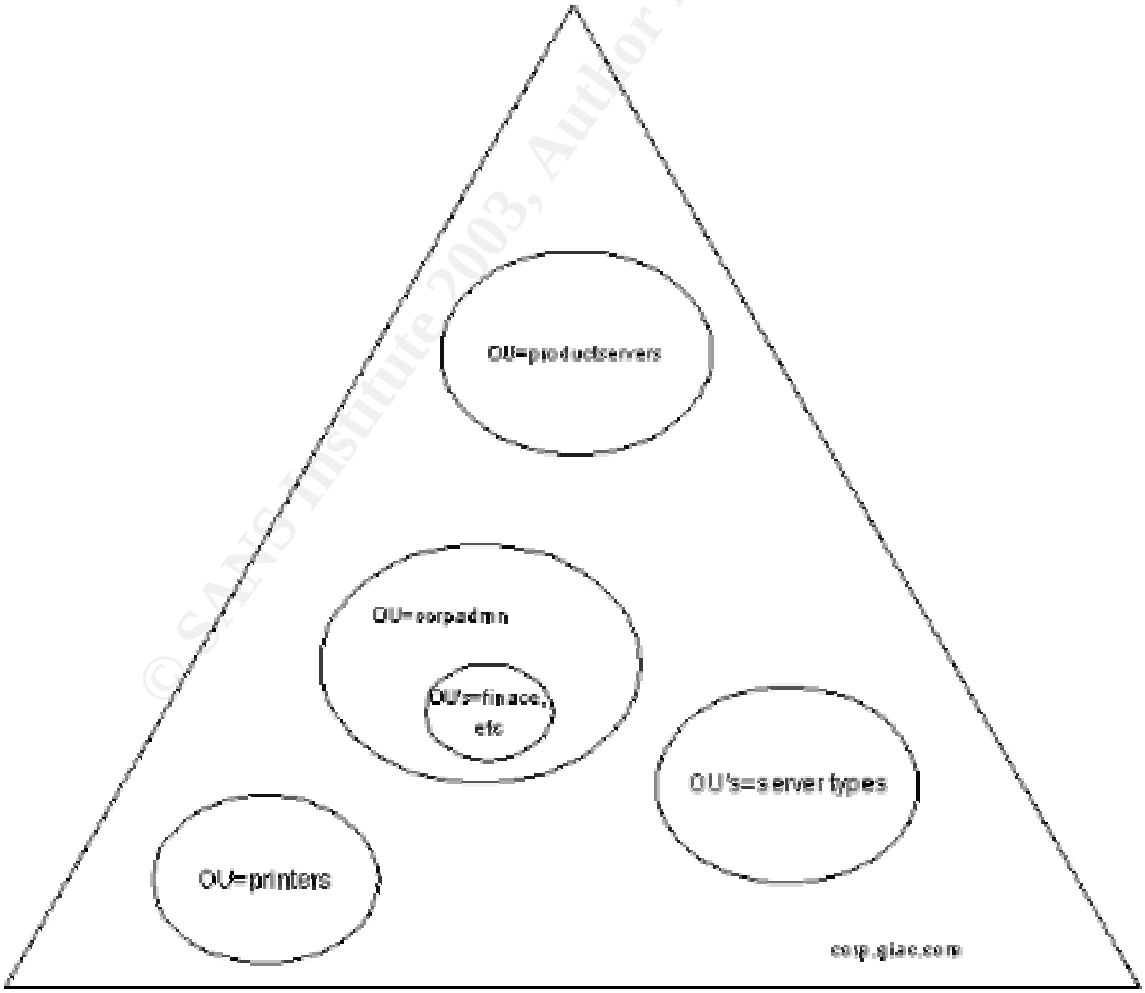
The following settings exist for the Domain Controllers with FSMO roles. The Schema Master is not configured to allow changes to the schema. There are no members of the Schema Administrators Group. Administrators are added only for the purpose of schema changes. Administrator accounts are removed from this Group after the changes have been implemented. Changes to the schema are carefully logged and audited along with failed access to the schema naming context.

A similar setup exists for the Domain Controllers on the sales.giac.com and cserv.giac.com domains. In each case there is a DC which is a FSMO RID Master and also acts as the Global Catalog server. There is a second DC which is the Infrastructure Master.

Trusts: The domains, corp.giac.com, sales.giac.com, and cserv.giac.com, all are part of the same forest. Because of the nature of traffic to dmz.giac.com, an explicit one way trust is manually configured so that dmz.giac.com trusts corp.giac.com. Thus, dmz.giac.com is not truly joined to the forest. In contrast, the domains, corp.giac.com, sales.giac.com and cserv.giac.com, have the Windows 2000 two-way transitive trust structure. There are no shortcut trusts configured in this domain structure.



Trust diagram for GIAC Enterprises.



Sample OU diagram for corp.giac.com domain.

Organizational Units: These are subunits of the domains outlined above. All of the OU's outlined below are populated with groups rather than individual users or computers. This was done for ease of management. The groups contain users and/or computers and are further described later in this section.

The root domain (corp.giac.com) has the following main organizational units.

1. OU = productservers – This OU contains the group that includes the products servers. These product servers are those which contain product data and related resources. These include the ALLMOL database server and IIS server used to update the corresponding systems on the DMZ domain.
2. OU = printers – This OU contains the printer group. This group includes all of the printers in the main corporate LAN. This was chosen as an OU to allow for individual personnel to be given power over the management of these systems.
3. OU = corpserver – This OU contains the print and fileserver group and mail server group. These groups are populated by particular server computers.
4. OU = adserver – This OU contains the group which in turn contains Domain Controllers.
5. OU = research – This OU contains the Research and Development Division group. This includes the users and computers in the R&D section.
6. OU = corpadmin – This OU contains a series of nested OU's. The nested OU's include Building Maintenance (bmaint), Finance (finance), Human Resources (hr), Legal (law), and Executive (ceobranch). These nested OU's are populated by groups which themselves include the users and computers in those units. Note that the OU's are not deeply nested as this can cause latency issues in Group Policy processing response times.
7. OU = it – This OU contains groups of users and groups of computers in the Information Technology support section of GIAC Enterprises.

The Sales domain (sales.giac.com) contains the following OU's.

1. OU = market – This OU contains groups of users and computers used by the market research team.
2. OU = sales – This OU contains the groups of users who are sales representatives and groups of their computers.
3. OU = adserver – This OU contains the group which in turn contains Domain Controllers.
4. OU = otherserver – This OU contains the group which in turn contains other domain servers.

The Customer Service domain (cserv.giac.com) contains the following OU's.

1. OU = helpdesk – This OU contains the groups of users and groups of computers that make up the helpdesk team and equipment.
2. OU = custom – This OU contains the groups of users and groups of computers who provide customized database solutions for customers.
3. OU = train – This OU contains the groups of users and groups of computers who do on-site training for customers.
4. OU = adserver – This OU contains the group which in turn contains Domain Controllers.
5. OU = otherserver – This OU contains the group which in turn contains other domain servers.

The DMZ domain (dmz.giac.com) contains the following OU's.

1. OU = server – This OU contains the group for database and IIS servers in the DMZ domain.
2. OU = updates – This OU contains user groups that manage update schedules.
3. OU = adserver – This OU contains the group which in turn contains Domain Controllers.
4. OU = mailserver – This OU contains the group which in turn contains other domain servers.
5. OU = allserver – This OU contains all of the server OU's in the DMZ (1, 3, 4).

All organizational units were chose to facilitate delegation of authority over resources and to manage the deployment of Group Policy objects. Since rights and permissions cannot be assigned to organizational units, the organizational units chosen for GIAC Enterprises do not directly reflect the corporate organizational structure. Rather, the intention is assign authority over these organizational units to individual users and groups.

Groups: IN GIAC Enterprises, group assignment plays a critical role in the security of the system. Access to appropriate group membership is used to control user access to resources.

There are a series of predefined local groups which come with any Windows 2000 system configured with a computer account in a domain. These include Account Operators, Administrators, Backup Operators, Guests, Print Operators, Replicators, Server Operators, and Users. These are local groups (local to the domain). These local groups are not to be confused with the built-in machine local groups which are installed by default on all Window 2000 and XP client (desktop) and server systems. These groups, which are in the \Groups folder and are part of the Computer Management Console, allow for certain tasks local to the individual computer. These groups exist regardless of domain membership. Built-in machine local groups include Administrators, Backup Operators, Guests, Power Users, Replicators and Users.

The domain local groups are critical to secure resource management so it bears clarification of the roles of some of these critical groups, along with their default membership. The default settings for the Account Operators group allows members to create, delete, or modify user and group objects but they cannot modify the Administrators or Operators group. This group has a lot of power. They can add new computers in the domain and they can shut down servers. This group should have strictly limited membership for security purposes.

The domain local Administrators group members are even more powerful and can perform administrative throughout the domain, including on domain controllers. This local group contains the default global groups (see below) for Domain Admins and Enterprise Admins. It also contains the Administrative user.

The User group contains users who have accounts in the domain. This is the default group when a new user account is created. This contains the Domain Users global group by default. Users only have the rights and privileges which are explicitly assigned.

The default global groups on Windows 2000 include: Domain Admins, Domain Guests, Domain Users, and Enterprise Admins. The Domain Admins group is included by default in the domain local group for Admins. The Administrator user is included. The members of this global group can act as administrators on any machine in the domain! It is important to control usage of this group. To prevent administration of a particular machine by a Domain Admin member, this group should be removed from the Administrator group on that particular machine.

Another global group of interest is the Domain Users group. Members of this group are added by default to the local domain Users group. Default membership also includes the Administrator, Guest, IUSR_*computername,* and IWAM_ *computername* accounts.

Universal groups are a powerful feature of Windows 2000, particularly in Native mode. These can be enterprise wide groups including all domains in a given AD forest.

There is only one universal group in GIAC Enterprises.

1. Universal Group = Mailing List – This universal group contains several global groups. These global groups are for each of the personnel categories in each of three domains in the giac.com AD forest. The purpose of this group is to indirectly collect all users in the entire GIAC Enterprises corporate structure into one unit, for the purpose of sending email. Rather than directly collecting all of the individual users into this universal group, only the global groups are included. The global groups themselves contain the users for their individual domains. This allows for more efficient control of replication traffic of the

global catalog. The universal group contents do not change with the addition or departure of an employee. Rather, it is the contents of the individual global group that changes. This data is not in the global catalog and therefore does not affect replication traffic. Because the entire corporation is structured in Native Mode, we can use the universal security group feature. This however is strictly a distribution type group and cannot be assigned rights or permissions.

There are a variety of global and local groups in the different domains. Starting with corp.giac.com, the following groups exist.

1. Domain Local group = Corporate People – this is a security local group which contains other global groups for all of the subunits (R&D, IT, HR, Finance, Building Mgmt, Legal, Executives) in the main corp.giac.com domain. This group thereby includes all of the employees in the corp.giac.com domain. It is also used for email distribution.
2. Global group = R&D – this is a security global group which contains all of the employees in the Research & Development section of GIAC Enterprises. It is also used for email distribution.
3. Global group = IT – this is a security global group which contains all of the employees in the Information Technology section of GIAC Enterprises. It is also used for email distribution.
4. Global group = HR – this is a security global group which contains all of the employees in the Human Resources section of GIAC Enterprises. It is also used for email distribution.
5. Global group = Finance – this is a security global group which contains all of the employees in the Finance section of GIAC Enterprises. It is also used for email distribution.
6. Global group = Building Mgmt – this is a security global group which contains all of the employees in the Building Maintenance & Security section of GIAC Enterprises. It is also used for email distribution.
7. Global group = Legal – this is a security global group which contains all of the employees in the Legal Services section of GIAC Enterprises. It is also used for email distribution.
8. Global group = Executives – this is a security global group which contains all of the employees in the Executive branch of GIAC Enterprises. This group includes the CEO and the Senior Managers of the individual Divisions at Corporate Headquarters. Most of these users also belong to the global groups of their individual divisions as well. This group is also used for email distribution.
9. Domain Local group = Corp desktops – this is a security local group and contains other global groups (Executive Desktops, Legal Desktops, Finance Desktops, Building Mgmt Desktops, HR Desktops). These groups together contain all of the desktop and laptop computers in the corp.giac.com domain except for the R&D and IT divisions. Note this group does not contain the R&D Desktops and IT Desktops group.

10. Global groups = Executive Desktops – this is a security global group which contains all of the desktop and laptops of managers and executives in corp.giac.com. There are similar global groups for Legal Desktops, Finance Desktops, Building Mgmt Desktops, and HR Desktops.
11. Global group = IT Desktops – this is a security global group which contains all of the desktop and laptops of IT Personnel.
12. Global group = R&D Desktops – this is a security global group which contains all of the desktops and laptops of R& D Personnel.
13. Global group = Domain Admins – the members of this group are the administrators for the desktops, laptops, and servers (domain controllers, file and print servers).
14. Global group = Database Admins – the members of this group are mostly from R&D and control the updates to the database server.
15. Global group = IIS Admins – the members of this group are mostly from R&D and control the updates to the IIS server.
16. Other Domain Local groups = Print & File servers, Product Servers (database, IIS server), Domain Controller group.

In sales.giac.com there are the following groups.

1. Domain Local group = Sales and Marketing Personnel – this is a security local group and contains two other global groups (Sales Reps and Market Consultants). These groups together contain all of the employees in the sales.giac.com domain. It is also used for email distribution.
2. Global group = Sales Reps – this is a security global group which contains all of the sales representatives and their managers. It is also used for email distribution.
3. Global group = Market Consultants – this is a security global group which contains all of the market researchers and their managers. It is also used for email distribution.
4. Domain Local group = Sales and Marketing desktops – this is a security local group and contains two other global groups (Sales Reps Desktops and Market Consultants Desktops). These groups together contain all of the desktop and laptop computers in the sales.giac.com domain.
5. Global group = Sales Reps Desktops – this is a security global group which contains all of the desktops and laptops of sales representatives and their managers.
6. Global group = Market Consultants Desktops – this is a security global group which contains all of the desktops and laptops of market researchers and their managers.
7. Global Group = Domain Admins – the members of this group are the administrators for the desktops, laptops, and servers (domain controllers, file and print servers).

In cserv.giac.com there are the following groups.

1. Domain Local group = Customer Service Personnel – this is a security local group which contains three other global groups (Techies, Trainers, and Customizers). Together, these are all of the employees in the cserv.giac.com domain. It is also used for email distribution.
2. Global group = Techies – this is a security global group which contains all of the help desk support personnel and their managers. It is also used for email distribution.
3. Global group = Trainers – this is a security global group which contains all of the training specialist personnel and their managers. It is also used for email distribution.
4. Global group = Customizers – this is a security global group which contains all of the custom database design personnel and their managers. It is also used for email distribution.
5. Domain Local group = Customer Service desktops – this is a security local group and contains three other global groups (Techie Desktops, Trainer Desktops and Market Consultants Desktops). These groups together contain all of the desktop and laptop computers in the cserv.giac.com domain.
6. Global group = Techie Desktops – this is a security global group which contains all of the desktops and laptops of help desk personnel and their managers.
7. Global group = Trainer Desktops – this is a security global group which contains all of the training specialist personnel and their managers.
8. Global group = Customizer Desktops – this is a security global group which contains all of the custom database design personnel and their managers.
9. Global Group = Domain Admins – the members of this group are the administrators for the desktops, laptops, and servers (domain controllers, file and print servers).

Local groups exist in each of the domains in GIAC Enterprises. The local groups are mostly used for resource management and are largely populated either by groups of user or by groups of computer systems.

It is necessary for the administrators from the corp.giac.com domain to access and control the servers in the dmz.giac.com domain. Fortunately, local groups can contain global groups from trusted domains. The DMZ domain has an explicit one-way trust to the corp.giac.com domain. On the DMZ domain, dmz.giac.com, the local admin group contains the global admin group from the corp.giac.com domain.

Local groups can contain global groups. Local groups are limited to a single domain. Local groups in this configuration are used to control access by users to network resources in a single domain. Permissions are set to grant user access to these resources. This is discussed in detail in the Group Policy Section.

Group Policy for the Domain and Domain Controllers:

Group Policy is the key to GIAC Enterprises information technology security. Primarily, the GP is configured in two basic categories. One category of GP settings controls computer configuration and the other controls user configuration. The computer configuration settings are applied at the time of system boot and are further applied to every user who logs in at any time. There is an order to the processing of the group policy objects and an understanding of this order is required to create a secure configuration. Policies that are applied later override policies that are applied earlier. As a system boots, the first GPO is the local GPO. This is then followed by non-local GPO's (for site, domain, OU). Since the local GPO is overridden by the subsequently applied non-local GPO's, the local GPO only has a major impact in non-domain systems.

After the system boots and all local and non-local GPOS for computer configuration are applied, users can log in. There are GPO settings at the user level as well. Like in the computer configuration GPO's user configuration GPO's have an order of processing. Once again, local GPO's are applied before non-local GPO's (site, domain, OU). If a user logs in to a local computer account rather than a domain account, then only the local GPO's for user accounts are applied. Non-local GPO's are applied only if the user logs into a domain account. After the user GPO's are applied, and then logon scripts based in GP are run.

The main security policy sections for group policy are:

Account Policy/Password Policy: This refers to password age, length and complexity. Account Policy/Account Lockout Policy: This refers to account lockout, duration, threshold trigger and reset time. Account Policy/Kerberos Policy: This refers to lifetime of tickets. Local Policies/Audit Policy: This refers to auditing of specific events. Local Policies/User Rights: This defines rights to log on locally or from the network along with other settings. Local Policies/Security Options: This defines registry values related to security. Event Log: This enables monitoring of actions according to their success or failure. Restricted Groups: This defines who belongs to a specific group. System Services: This determines the mode of services. Registry: This sets permissions on registry keys. File System: This sets permissions on folders, subfolders and files.

There is a default group policy object specially configured for each domain in GIAC Enterprises. Since the site configuration for GIAC Enterprises basically maps to the domain structure, with the exception of the separate dmz.giac.com domain, there are no site specific GPO's. The main non-local GPO configuration occurs at the domain level.

The tool used to configure the domain GPO's is the "AD Users and Computers" Screen. The Group Policy Tab allows one to select and then edit the default domain policy.

Domain GPO: The most important setting at the domain GPO level is the "No Override" value! This prevents administrators down the line from the domain level from overriding these settings with their own custom GPO's.

GIAC Enterprises has focused on account and password related policies at the domain level so that all domain accounts are included. The settings focus on the Computer Configuration options.

A critical point to emphasize here is the "No Override" value. It is very tempting to lock down everything at the Domain level. An examination of publicly published GPO's for several sites and from Microsoft's templates indicates that this is not a common practice. Most entities seem only to focus on these very general account and password issues (UW, Stanford).

Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history=10 Passwords remembered
Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length=8 Characters
Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age=2 days (changes are immediate)
Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age=100 days
Windows Settings\Security Settings\Account Policies\Password Policy\
Passwords must meet complexity requirements=Enabled
Settings\Account Policies\Kerberos Policy\Enforce user logon restrictions=Enabled
Windows Settings\Security Settings\Account Policies\Kerberos Policy\Maximum lifetime for service ticket=600 minutes
Windows Settings\Security Settings\Account Policies\Kerberos Policy\Maximum lifetime for user ticket=10 hours
Windows Settings\Security Settings\Account Policies\Kerberos Policy\Maximum lifetime for user ticket renewal=7 days
Windows Settings\Security Settings\Account Policies\Kerberos Policy\Maximum tolerance for computer clock synchronization=5 minutes
Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold=3 invalid attempts
Windows Settings\Security Settings\Account Policies\Account Lockout Policy \Reset account lockout counter after=30 minutes
Windows Settings\Security Settings\Restricted Groups=Domain Admins

Windows Settings\Security Settings\Local Policies\Security Options\LAN Manager Authentication Level=Send NTLMv2 response only\refuse LM & NTLM
Windows Settings\Security Settings\Local Policies\Security Options\Additional restrictions for anonymous connections=Do not allow enumeration of SAM accounts or shares
Windows Settings\Security Settings\Local Policies\Security Options\Send unencrypted password to connect to third-party SMB servers=Disabled
Windows Settings\Security Settings\Local Policies\Security Options\Message test for users attempting to log on=Only authorized GIAC Enterprises users are permitted to use and access this computer.
Windows Settings\Security Settings\Local Policies\Security Options\Audit use of Backup and Restore privilege=Enabled
Windows Settings\Security Settings\Local Policies\User Rights Assignment\Enable user and computer accounts to be trusted for delegation= Administrators

The account and password policy options were chosen to balance complexity with user compliance. Longer passwords might lead to post-it note password storage. Account Lockout Policy is critical to foil hackers and password guessing. The basic concept for these settings was recommendations from Microsoft as well as a survey of institutions who have posted their domain level policies on the internet. Modifications were made to better address the GIAC Enterprises environment.

The password history was chosen to encourage folks not to reuse passwords and complexity is enforced to avoid simple words which are easily guessed. The account lockout policies assume that folks will occasionally mistype their passwords but repeated mistakes might imply a hacker using a brute force attack. The lockout time is short enough not to disrupt productivity but long enough to encourage hackers to move on to easier targets.

It should be noted that these policies also apply to the routers at the domain boundaries. These systems are otherwise quite prone to attack.

GIAC Enterprises experimented with auditing at the domain GPO level. These settings were tried but proved to cause a conflict with desired settings at the level of the domain controller GPO.

Audit Policy: Audit account logon events=Success,Failure
Audit account management=Success,Failure
Audit directory service access=Failure
Audit logon events= Failure; Audit object access=Failure
Audit policy change=Success,Failure
Audit privilege use=Success,Failure
Audit system events=Success,Failure

Domain Controller GPO: The most important setting at the domain controller GPO level is the "No Override" value! Because of the "No Override" setting at the domain GPO, it is not possible to apply conflicting settings at the domain controller level. It might be possible to configure conflicting settings if we configure the permissions so that the Domain Controller group is assigned Deny Read and Deny Apply Group Policy permission for the domain GPO. That way the domain level GPO would not actually apply to the domain controllers. It would then be possible to replicate all of the domain settings at the domain controller level, modifying them as seemed appropriate. This is tempting as it seems like a good idea to include some auditing at the domain GPO level (see above). This would help trouble shooting in the event of system problem on desktops, laptops and other machines. However, auditing at the domain GPO level poses a set of problems. It is hard to manage all of that data input. Further, stricter auditing is desired at the domain controller level. The domain controllers are so critical to security that it is important to get a lot of logging information. The level of logging required at the domain controller level is too much to apply at the entire domain level. However, if a good management and processing solution appeared for this data, it would be nice to apply auditing across the domain. Many security breaches begin on user desktops and it would be good to look for this proactively.

A good place to begin for configuration of group policy for the domain controller settings is the default hisecdc.inf from Microsoft stored in %Systemroot%\Security\Templates. This can be applied after basicdc.inf and securedc.inf as they are cumulative. With that in mind, the following settings are selected for discussion emphasis. The focus here is again on Computer Configurations options.

Windows Settings\Security Settings\Local Policies\Audit Policy\Audit account logon events=Success,Failure
Windows Settings\Security Settings\Local Policies\Audit Policy\Audit account management=Success,Failure
Windows Settings\Security Settings\Local Policies\Audit Policy\Audit directory service access=Failure
Windows Settings\Security Settings\Local Policies\Audit Policy\Audit logon events=Success,Failure
Windows Settings\Security Settings\Local Policies\Audit Policy\Audit object access=Failure
Windows Settings\Security Settings\Local Policies\Audit Policy\Audit policy change=Success,Failure
Windows Settings\Security Settings\Local Policies\Audit Policy\Audit privilege use=Success,Failure
Windows Settings\Security Settings\Local Policies\Audit Policy\Audit system events=Success,Failure

Windows Settings\Security Settings\Event Log\Settings for Event Logs\Maximum application log size=51200 KB
Windows Settings\Security Settings\Event Log\Settings for Event Logs\Maximum security log size=51200 KB
Windows Settings\Security Settings\Event Log\Settings for Event Logs\Maximum system log size=51200 KB
Windows Settings\Security Settings\Event Log\Settings for Event Logs\Restrict guest access to application log=Enabled
Windows Settings\Security Settings\Event Log\Settings for Event Logs\Restrict guest access to security log=Enabled
Windows Settings\Security Settings\Event Log\Settings for Event Logs\Restrict guest access to system log=Enabled
Windows Settings\Security Settings\Event Log\Settings for Event Logs\Retention method for application log=By days
Windows Settings\Security Settings\Event Log\Settings for Event Logs\Retention method for security log=By days
Windows Settings\Security Settings\Event Log\Settings for Event Logs\Retention method for system log=By days
Windows Settings\Security Settings\Event Log\Settings for Event Logs\Retain security log=30 days
Windows Settings\Security Settings\Event Log\Settings for Event Logs\Retain system log=30 days
Windows Settings\Security Settings\Event Log\Settings for Event Logs\Retain application log=30 days
Windows Settings\Security Settings\Local Policies\Security Options\Allow server operators to schedule tasks=Enabled
Windows Settings\Security Settings\Local Policies\Security Options\Allow system to be shut down without having logon=Disabled
Windows Settings\Security Settings\Local Policies\Security Options\Audit the access of global system objects=Enabled
Windows Settings\Security Settings\Local Policies\Security Options\Audit use of Backup and Restore privilege=Enabled
Windows Settings\Security Settings\Local Policies\Security Options\Disable CTRL+ALT+DEL requirement for logon=Disabled
Windows Settings\Security Settings\Local Policies\Security Options\Restrict CD-ROM access to locally logged-on user only=Enabled
Windows Settings\Security Settings\Local Policies\Security Options\Restrict floppy access to locally logged-on user only=Enabled
Windows Settings\Security Settings\Local Policies\Security Options\Digitally sign client communication (when possible)=Enabled
Windows Settings\Security Settings\Local Policies\Security Options\Digitally sign server communication (always)=Enabled
Windows Settings\Security Settings\Local Policies\Security Options\Digitally sign server communication (when possible)=Enabled
Windows Settings\Security Settings\Local Policies\Security Options\Do not display last user name in logon screen=Enabled

Windows Settings\Security Settings\Local Policies\Security Options\Clear virtual memory page file when system shuts down=Enabled
Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time=Administrators
Windows Settings\Security Settings\Local Policies\User Rights Assignment\Debug programs=Administrators
Windows Settings\Security Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system=Administrators
Windows Settings\Security Settings\Local Policies\User Rights Assignment\Log on as a batch job=Administrators
Windows Settings\Security Settings\Local Policies\User Rights Assignment\Log on locally=Administrators
Windows Settings\Security Settings\Local Policies\User Rights Assignment\Manage Auditing and Security Log=Administrators
Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify firmware environment values=Administrators
Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile single process=Administrators
Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile system performance=Administrators
Windows Settings\Security Settings\Local Policies\User Rights Assignment\Remove computer from docking station=Administrators
Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories=Administrators
Windows Settings\Security Settings\Local Policies\User Rights Assignment\Shut down the system=Administrators

On the domain controllers, we are interested in auditing a variety of system related events, success or failure.

The “Clear virtual memory page file when system shuts down” option was chosen to prevent inadvertent storage of sensitive information in memory. Other options were chosen to prevent inappropriate access to hardware devices and to disallow insecure communications.

Event Log settings were chose to balance inclusion of sufficient information with the available disk space and the desire not to overwrite information of interest.

It should be noted that neither IIS nor SMTP are enabled on the domain controllers. There are specific mail and web servers to handle these services.

Based on examination of published GPO’s for other sites (Stanford, UW) it seems that the settings for systems at the domain level are quite minimal. They focus on user related properties as well as on auditing.

The GPO's defined above are linked to the domain and the domain controller OU, respectively.

Additional GP configurations in GIAC Enterprises:

DMZ TCP/IP GPO: The Domain Controller GPO is used for the servers OU on the DMZ as well. Because of the critical nature of the domain controllers and other servers, along with a concern about attacks on the TCP/IP stack on Windows 2000, some additional registry settings were selected for the systems on the DMZ. These settings can help prevent denial of service attacks. These settings are further described in the Microsoft Knowledge Base (article Q315669). These are part of the recommendations of the Member Sever Baseline Policy.

The settings are registry entries in HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\

EnableICMPRedirect=0
EnableSecurityFilters=1
SynAttackProtect=2
EnableDeadGWDetect=0
EnablePMTUDiscovery=0
KeepAliveTime=300,000
DisableIPSourceRouting=2
TcpMaxConnectResponseRetransmissions=2
TcpMaxDataRetransmissions=3
NoNameReleaseOnDemand=1
PerformRouterDiscovery=0
TCPMaxPortsExhausted=5

Microsoft also recommends settings which harden servers against dynamic backlogs. These settings are:

HKLM\System\CurrentControlSet\Services\AFD\Parameters\

DynamicBacklogGrowthDelta=10
EnableDynamicBacklog=1
MinimumDynamicBacklog=20
MaximumDynamicBacklog=20000

Other Computer Configurations that seem reasonable on the DMZ include the following. All of these settings are applied using group policy on the DMZ OU containing servers.

Windows Settings\Security Settings\Local Policies\System Services\Alerter=Disable

Windows Settings\Security Settings\Local Policies\System Services\ClipBook=Disable
Windows Settings\Security Settings\Local Policies\System Services\Computer Browser=Disable
Windows Settings\Security Settings\Local Policies\System Services\DHCP Client=Disable
Windows Settings\Security Settings\Local Policies\System Services\Distributed File System=Disable
Windows Settings\Security Settings\Local Policies\System Services\Distributed Link Tracking Client=Disable
Windows Settings\Security Settings\Local Policies\System Services\Distributed Link Tracking Server=Disable
Windows Settings\Security Settings\Local Policies\System Services\Distributed Transaction Coordination=Disable
Windows Settings\Security Settings\Local Policies\System Services\Fax Service=Disable
Windows Settings\Security Settings\Local Policies\System Services\File Replication Services=Disable
Windows Settings\Security Settings\Local Policies\System Services\Indexing Services=Disable
Windows Settings\Security Settings\Local Policies\System Services\Internet Connection Sharing=Disable
Windows Settings\Security Settings\Local Policies\System Services\License Logging Service=Disable
Windows Settings\Security Settings\Local Policies\System Services\NetMeeting Remote Desktop Sharing=Disable
Windows Settings\Security Settings\Local Policies\System Services\Network DDE=Disable
Windows Settings\Security Settings\Local Policies\System Services\Network DDE DSDM=Disable
Windows Settings\Security Settings\Local Policies\System Services\Print Spooler=Disable
Windows Settings\Security Settings\Local Policies\System Services\QoS RSVP=Disable
Windows Settings\Security Settings\Local Policies\System Services\Remote Access Auto Connection Manager=Disable
Windows Settings\Security Settings\Local Policies\System Services\Remote Access Connection Manager=Disable
Windows Settings\Security Settings\Local Policies\System Services\Remote Registry Service=Disable
Windows Settings\Security Settings\Local Policies\System Services\Removable Storage=Disable
Windows Settings\Security Settings\Local Policies\System Services\Telephony=Disable

Desktop GPO: There GPO which is linked to several OU's which are made up of groups of computers which are user desktops and laptops. The primary concern for these settings is the desire to prevent the installation of software, drivers, and device files without authorization. In particular, there are limits set on which administrative tools a user can access. Further, there is a desire to redirect user files to a network folder for backup and reliability. The settings listed here were based on suggested settings from other institutions.

Windows Settings\Local Policies\Security Options\Prevent users from installing printer drivers=Enabled
Administrative Templates\Windows Components\NetMeeting\Disables the remote desktop sharing=Enabled
Administrative Templates\System\Logon\Delete Cached copies of roaming profiles=Enabled
Administrative Templates\System \Logon \Log users off when roaming profile fails=Enabled
Administrative Templates\Network\Offline Files\At Logoff, delete local copies of user's offline files=Enabled
Windows Settings\Folder Redirection\Desktop=P:\ (DFS network folder shared from fileserver.)
Windows Settings\Folder Redirection\My Documents=P:\My Documents
Administrative Templates\Windows Components\NetMeeting\Application Sharing\Disable the application sharing=Enabled
Administrative Templates\Windows Components\NetMeeting\Application Sharing\Prevent sharing=Enabled
Administrative Templates\Windows Components\NetMeeting\Application Sharing\Prevent sharing desktop=Enabled
Administrative Templates\Windows Components\NetMeeting\Application Sharing\Prevent sharing command prompts=Enabled
Administrative Templates\Windows Components\NetMeeting\Application Sharing\Prevent sharing Explorer windows=Enabled
Administrative Templates\Windows Components\NetMeeting\Application Sharing\Prevent control=Enabled
Administrative Templates\Windows Components\NetMeeting\Application Sharing\Prevent sharing applications in true color=Enabled
Administrative Templates\Windows Components\Windows Explorer\Hide Hardware tab=Enabled
Administrative Templates\Windows Components\Microsoft Management Console\Restrict the user from entering author mode=Enabled
Administrative Templates\Windows Components\Microsoft Management Console\Restrict users to the explicitly permitted list of snap-ins=Enabled
Administrative Templates\Start Menu and Taskbar\Remove user's folder from the start menu=Enabled
Administrative Templates\Start Menu and Taskbar\Disable and remove links to Windows Update=Enabled

Administrative Templates\Start Menu and Taskbar\ Do not keep history of recently opened documents=Enabled
Administrative Templates\Start Menu and Taskbar\Add Logoff to the start menu=Disabled
Administrative Templates\Desktop\Prohibit user from changing My Documents path=Enabled
Administrative Templates\Desktop\Don't save settings at exit=Enabled
Administrative Templates\Control Panel\Add\Remove Programs\Disable Add\Remove Programs=Enabled
Administrative Templates\Control Panel\Add\Remove Programs\Hide Change or Remove Programs page=Enabled
Administrative Templates\Control Panel\Add\Remove Programs\Hide Add New Programs page=Enabled
Administrative Templates\Control Panel\Add\Remove Programs\Hide Add\Remove Windows Components page=Enabled
Administrative Templates\Control Panel\Add\Remove Programs\Hide the "Add a program from CD-ROM or floppy disk" option=Enabled
Administrative Templates\Control Panel\Add\Remove Programs\Hide the "Add programs from Microsoft" option=Enabled
Administrative Templates\Control Panel\Add\Remove Programs \Hide the "Add programs from your network" option=Enabled
Administrative Templates\Control Panel\Printers\Disable deletion of printers=Enabled
Administrative Templates\Control Panel\Printers\Disable addition of printers=Enabled

Application Server GPO: The Microsoft recommended security template for application servers is Baseline.inf. This is a suggested set of values for a secure server configuration.

File and print server GPO: The key settings for print services are in Computer Configuration\Administrative Templates\Printers. The basic settings for the print and file server GPO are the same as those for the domain controllers merged with the recommendations for the Microsoft Member Server Baseline Policy. The following represent changes or key settings.

Computer Configuration\Administrative Templates\Printers\Allow printers to be published=Enabled
Computer Configuration\Administrative Templates\Printers\Web-based printing=Disabled
Computer Configuration\Administrative Templates\Printers\Printer browsing=Enabled
Computer Configuration\Administrative Templates\System\Disk Quotas=1GB
Computer Configuration\Windows Settings\Security Settings\Local Policies\ System Services\Print Spooler=Enabled

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Digitally sign client communication (always)=Disabled
This must be disabled to allow all clients to view the print queue. This was Enabled for the domain controllers.

Note that the Member Server Baseline Policy securely configures numerous files especially those in %SystemDrive%.

Additional Security:

In order to improve security at GIAC Enterprises, there is an all encompassing security policy that includes computer security as well as physical security. While this paper deals mostly with the computer security, it is important to note the physical security environment as it impacts the computer security.

Server computers are stored in locked rooms which require card key access. Only building security personnel and server administrators have access to these rooms. Because the corporate headquarters is only a few meters from the seismically active Hayward fault line, there is a procedure in place for regular transfer of backup materials to an off-site location. The off-site location is also secure with access restriction like those at headquarters.

The focus of the computer security is multi facetted. First there is a commitment to software maintenance whereby there is regular analysis of the latest security alerts from application and operating system vendors. There is a rapid response team that can be called to action in the event of a serious threat or breach. Such threats crop up periodically and often the window of opportunity is small. This is particularly true for server systems on the DMZ. As an example, there was a recent vulnerability discovered in a popular SMTP agent. The rapid response team patched the DMZ SMTP server in the short window between the announcement of the vulnerability and before any damage occurred from hackers. Similarly, routers and firewalls need constant vigilance for potential new security holes.

In addition to the DMZ, there is a commitment to software maintenance inside the firewalled domains. It is important to keep the systems up to date with the latest operating system service packs. These are installed using MSI installation scripts which are controlled with group policy. Temporary OU's are created for the purpose of MSI installation. Computers temporarily assigned to these OU's, a few at a time. The MSI installation only applies to these temporary OU's. This procedure allows for load balancing of the MSI installation procedure.

Virus checking software is installed on all user desktop and laptop systems and runs are scheduled regularly. Again, group policy is used to push out updates of the virus definition files and force the scheduled checking. This is particularly critical on the sales.giac.com and cserv.giac.com domain as there is a lot of email and file exchange with outside entities. In addition to the virus software on the user side, the SMTP server also does some virus checking and can cut out some fraction of the incoming corrupted data.

Servers are regularly challenged with hacker scripts by the IT staff in an effort to assess the nature of security threats. This is most often done on the DMZ. However other server systems are also challenged. Regular scanning is done to

look for open ports and unusual network traffic. The third party tools used to perform the intrusion detection include Tripwire and Snort. The third party tools used to perform the vulnerability testing include CyberCop from Network Assosciates and Internet Scanner from Internet Security Systems.

In a related effort the IT staff has configured a honeypot server on the DMZ to look for popular server attack motifs. This server is often the trial system for potential new applications or services. Vulnerability is therefore assessed on this test system before any production systems are installed.

Another key area of security is the use of IPSec policies and certificates. All systems use the High Encryption Pack and the strongest encryption is required 168-bit 3 DES. The RRAS servers all are configured so that the Connection Profiles \ Encryption Tab has only the strongest option checked. The other options are unchecked so that a lower level of encryption cannot be used. Communication from the RRAS servers going outside the firewalls is limited only to the other RRAS servers. The router between the DMZ and the corp.giac.com domain uses both IPSec and RRAS based packet filtering.

Certificates are distributed by computer auto enrollment and group policy is used to distribute root certificates. All systems have service pack 2 installed. Syskey.exe was used to move the System Key off of the CA. This is stored on a secure, locked location.

NTFS permissions are enforced so that users have access to only their own profiles including the local \RSA and \Protect file folders.

The IIS servers were configured using the IISLockdown tool which is part of the Security Toolkit from Microsoft. The IIS servers are static IP systems so can be configured as such. The first set of configurations is script map disabling for the Index Server Web Interface (.idq, .htw, .ida), Internet Data Connector (.idc), Server side includes (.shtml, .shtm, .stm), HTR scripting (.htr), Active Server Pages (.asp), Internet printing (.printer). In addition, several directories were removed including the printer virtual directory, Scripts virtual directory, MSADC virtual directory, IIS Samples virtual directory, IISAdmin virtual directory, and IISHelp virtual directory. Anonymous IIS users are prevented from running system utilities and from writing to content directories. WebDAV is disabled. Finally, URLScan filtering is used. This filters and rejects requests that are considered to be suspicious traffic.

Another key security measure is incremental backups of all user data at regular intervals. Each backup is followed by validation measures to ensure the integrity of the backup. In this fashion, recovery after security incidents or system failures is possible. User data is stored on the domain file servers so individual desktop failures or corruptions are manageable events.

In an effort to control damage in the event of a stolen laptop, all mobile systems that leave any corporate office require smart cards for network logon.

References:

Zandri, Jason. “Learn AD in 15 Minutes a Week”. 19 December 2002. URL: http:\\www.serverwatch.com\tutorials\article.php\1559891
(10 March 2003).

Shapiro, Jeffrey, R. and Boyce, Jim. “Windows 2000 Server Bible”. New York: Hungry Minds. 2000.

Microsoft Knowledge Base article Q315669, "HOW TO: Harden the TCP/IP Stack in Windows 2000 Against Denial of Service."

“Introduction to Windows 2000 Group Policy: White Paper”. 17 May 1999. URL: http:\\www.microsoft.com\windows2000\techinfo\howitworks\management\grouppolicyintro.asp
(9 March 2003).

“Step-by-Step Guide to Understanding the Group Policy Feature Set”. 31 January 2000. URL: http:\\www.microsoft.com\windows2000\techinfo\planning\management\groupsteps.asp
(9 March 2003).

Rice, David, C. NSA: Group Policy Reference”, 2 March 2001. URL: http:\\nsa2.www.conxion.com\win2k\guides\w2k-4.pdf
(9 March 2003).

“The Stanford Tree Mandatory Group Policies”. 10 December 2002. URL: http:\\windows.stanford.edu\Public\Infrastructure\treegpos.html
(9 March 2003).

“UW Forest Group Policies”. 13 November 2002. URL: http:\\www.washington.edu\computing\support\windows\2000\gpolicy.html
(9 March 2003).

“Microsoft Tech Net, Windows 2000 Security”

http:\\www.microsoft.com\technet\treeview\default.asp?url=\technet\security\prodtech\windows\windows2000\staysecure\secops04.asp
(11 March 2003).