Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Implementation of a Secure Windows 2000 Infrastructure at GIAC Enterprises

Trent R. Fox

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Figures

Tables

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Introduction

GIAC Enterprises begun as a fortune cookie manufacturer in 1990. The company was started by a vision a family had to provide creative fortune cookies and sayings to specialty stores, restaurants and commercial vendors worldwide. The family consisted of a father, his sister, his daughter and his two sons. They worked very hard. Sixteen-hour days and seven-day workweeks were the norm. GIAC Enterprises grew quickly. They seemed to always be at all the conventions and trade shows and were continually interviewed in articles for trade magazines and newspapers. The company spirit was energetic, aggressive, entrepreneurial, and very focused on sales, much to the chagrin of its competitors.

The company prides itself on its customer service as well as its secure and confidential business practices. In addition, the company has been envied for how it secured its Windows 2000 network. As a result, GIAC Enterprises has been able to create and maintain a steady, rapidly growing client base throughout the world.

During the early days, the organization was fairly conservative in terms of its adoption of information technology. They believed in staying with the formula that was working for them and that meant a lot of paper and filing. For example, they did not begin using computers until 1997 and even at that time they were using mainly desktop computers using Windows 95. None of the desktop computers were networked together. The family had thought about investing money into an internal infrastructure but decided to wait and spend the money on it when they were ready for offering its catalog on the Internet. As a result, in 1998, GIAC Enterprises contracted a national web development and hosting company to provide an Internet web site for them. Their patience was definitely a virtue and as a result, by late 1999, they saw phenomenal growth.

The next step was to continue its investment and bring their web site "in-house." This also meant they had to invest heavily in a new internal network infrastructure for the company. They decided to invest in Microsoft Windows 2000 for their new network. Upon doing a lot of due diligence, they felt this was the proper choice especially because of its size and its overall organizational structure. Due to the company's success from its web business, their attitude toward technology completely changed and now was quite enthusiastic. Thus, they chose Windows 2000.

Some reasons why GIAC Enterprises had seen exponential growth are due to its vision and constant planning for the future. By being one of the first fortune cookie companies to offer web-based ordering to its retail and commercial customers, the company carved out a niche market.

GIAC Enterprises has a standardized enterprise infrastructure and is mostly based on Microsoft Windows 2000, which facilitates implementing a centrally managed desktop and server environment. By having a uniform IT infrastructure (common directory), GIAC Enterprises can continue to centrally administer, but also has the ability to support changing business demands such as those generated by its e-commerce initiatives. In addition, the company's vision for the

© SANS Institute 2000 - 2005 Author retains full rights.

future sees the scalability of the Windows 2000 environment specifically Active Directory as the right decision for its organization.

Business Background:

GIAC Enterprises is a company headquartered in downtown Milwaukee, Wisconsin, USA. It has grown to a total 365 employees with 265 employees working from the headquarters facility. The company is privately held. They do not anticipate making any public stock offerings. It prides itself on state-of-the-art facilities with excellent, redundant, high bandwidth availability at all its office locations. GIAC Enterprises is located in its own physical building where all its departments are situated including manufacturing and distribution. The building, also known as "HQ" is comprised of two floors. Currently, this is the only facility used for its headquarters; however, if growth continues they will need to find additional space nearby.

The following table represents the business by department and its functions:

Department	Business Functions
GIAC Enterprises	
Finance	All accounting functions for the company.
Customer Service	Handles all post-sale service related issues for new, existing or previous customers.
Distribution	Staff in charge of coordination and shipping of orders.
Executive	Includes all senior, executive management for GIAC.
Human Resources	In charge of all employee-related information.
Information Technology	Supports and builds the business by building, testing, implementing, and supporting all of GIAC Enterprises network infrastructure and web-based business. This group includes individuals who assist in driving the company's security baselines, procedures and policies. Provides recommendations and solutions for IT department. Continually involved in ensuring the confidentiality, integrity and availability of critical business assets.
Manufacturing	Responsible for the manufacturing, printing, and packaging of fortune cookie sayings.
Marketing	In charge of entire marketing plans including demographics, advertising, public relations and new product marketing rollouts. Work closely with sales staff.
Research & Development	Handles all product research, research, development, and testing of new classified fortune cookie sayings.
Sales	Performs all GIAC pre-sales either in person, via telephone, or online sales and work with outside 3rd parties to offer turnkey fortune cookie solutions.

Table 1 - Company Department and Functions

The approximate size of the operations located at the headquarters facility in Milwaukee, Wisconsin is as follows:

- Finance – 20 employees
- Human Resources – 20 employees

© SANS Institute 2000 - 2005 Author retains full rights.

- Executive – 10 employees
- Marketing – 25 employees
- Sales – 50 employees
- Manufacturing – 70 employees
- Distribution – 14 employees
- Customer Service – 21 employees
- Research & Development – 5 employees
- Information Technology – 30 employees

At its three remote sites, GIAC Enterprises also has its own physical buildings, which as mentioned have the latest network technology.

GIAC Enterprises has a centralized business model. Even though there are remote offices, they still follow company procedures that are dictated by the management and all remote office employees and their supervisors report to the Executive management located at Headquarters. There are an additional three remote offices. The offices (including HQ) and their functions are as follows:

Office Location	Responsibility	Employees
Milwaukee, WI (HQ)	All departments based at this location.	265
Cleveland, Ohio	Sales Office	35
Rotterdam, Netherlands	Sales Office	30
Hong Kong, China	R & D and Sales Office	35

Table 2 - Office Location and Responsibility

Scope Description

A secure Windows 2000 network infrastructure that uses Active Directory. Although GIAC Enterprises deals with outside parties such as customers, suppliers, partners, the scope of this document deals mainly with the requirements for the internal network used by GIAC Enterprises' employees.

This document addresses three major areas of GIAC Enterprises' secure Windows 2000 infrastructure:

1. **Network Design and Diagram** – a detailed description of network specifics, including server locations and their roles, rationale of network design, and various network diagrams.

2. **Active Directory Design and Diagram** – a description and explanation of the

© SANS Institute 2000 - 2005 Author retains full rights.

logical Active Directory structure of the GIAC network, which includes its domains, organizational units, trees/forest, and the affect of Active Directory on network administration, performance and security.

3. **Group Policy and Security** – appropriate security settings for GIAC Enterprises' Group Policy for domains, Domain Controllers, and other security settings including rationale behind decisions, any issues relevant to security settings, and additional security requirements that cannot be maintained by Group Policy.

Within the framework of the three major areas, recommendations, alternative options and various considerations are discussed to give the reader insight and to provide additional information pertaining to the Windows 2000 infrastructure.

Network Design and Diagram

The GIAC Enterprises network is fairly simple and straightforward. Each geographic location is located in its own physical building, which house the aforementioned departmental offices. Thus, there are four physical locations. The locations make up GIAC Enterprises Wide Area Network. Dedicated circuits connect each location and use a dedicated, T-1 (1.544 mbps) frame relay. The Headquarters facility uses redundant multi-line, T-1, ISP service. GIAC Enterprises overall network includes an internal switched corporate HQ network, two different demilitarized zones (screened services), and three branch offices. All office networks utilize fast Ethernet.

The GIAC Enterprises IT security baseline mandates all new and existing installations of Windows 2000 utilize NTFS on all disk drives on all machines. In addition, there are several web based checklists on the intranet which guide the IT staff in system hardening and assist them in following the current company security baselines. Some additional areas of importance include disabling all unnecessary services on machines, renaming administrator accounts, requiring a minimum of seven character passwords, applying the latest service pack, relevant hot fixes, high encryption packs and all the latest security updates from Microsoft.

Throughout GIAC Enterprises networks, all the departmental servers as well as Windows 2000 Exchange Server, Domain Controllers (with Active Directory & DDNS) are securely located in a climate controlled secure locked physical server room. Only authorized personnel with the appropriate smart card swipe key can enter and exit this room. All new, network devices are setup with new strong passwords. There is only one central server room at GIAC Enterprises headquarters. It is important to note that all hardware (routers, switches, hubs servers, etc.) and software within the DMZ and internal corporate server room follow the GIAC Enterprises mandatory change control procedure. Upon testing and backup, the company tries to perform required updates for firmware or software on a monthly basis.

As mentioned previously, GIAC Enterprises is mostly standardized on Windows 2000 with the exception of some desktop machines not on the network as well as some Sun Solaris machines used for file serving and database applications. Thus, most workstations and mobile computers

© SANS Institute 2000 - 2005 Author retains full rights.

are running Windows 2000 Professional. Most enterprise servers are running Windows 2000 Server; however, in order to take advantage of the multi-processing, load-balancing, Windows 2000 Advanced Server is installed for machines running Microsoft SQL Server 2000 and IIS Web Server. All servers utilize the popular configuration of RAID 5; hot swap 10,000-rpm drive and dual power supplies. In case of power outages, GIAC Enterprises facility utilizes backup battery power to ensure the availability of systems (in accordance with GIAC Enterprises Disaster & Recovery Baseline).

GIAC Internal Corporate HQ Network Specifics

The company places importance in providing confidentiality, high availability, accountability and proper authentication to all GIAC Enterprises employees is part of its overall mission statement. As a result, this company provides all the enterprise applications and necessary systems to its employees.

The external router (choke) connects the company's internal network to the Internet (ISP). In addition, a Checkpoint firewall is positioned directly behind the choke router and in front of any incoming branch connections and the DMZ. The firewall will control the type of allowable traffic based on its protocol and/or port. Internet traffic is allowed between the corporate internal network and Internet. The Checkpoint firewall and its secure-remote VPN solution offer IPSEC to provide encryption to any remote client computer logging into the internal corporate network. At this time, GIAC Enterprises only allows VPN via an Internet connection. There are no dial-up services offered. In addition, all branch office Internet traffic also is routed directly to same router and Internet. A strategic security measure includes several ISS IDS network sensors positioned in front of the Checkpoint firewall, behind the Checkpoint firewall and in front of the internal corporate network. By strategically placing ISS IDS network sensors in these locations, GIAC Enterprises is able to audit the external firewall and its current policies and is able to confirm any inbound/outbound traffic that passes through the firewall. All Checkpoint firewalls and ISS network sensors run on the Nokia 440 appliances and the Checkpoint firewalls have multiple network interfaces. The Nokia appliances have the latest IPSO image and all latest patches and software versions from Checkpoint and ISS have been applied.

The ability for GIAC Enterprises to expand its offices is relatively easy since the network infrastructure has incorporated the necessary network devices to accomplish future growth. Three dedicated, T-1 frame relay connections connect the branch offices to the GIAC Enterprises corporate facility. These T-1 connections are connected to routers. Behind the routers are a switch and a DMZ 1 and DMZ 2. There are two additional Checkpoint Firewalls in between DMZ 1 and DMZ 2 and DMZ2 and the internal corporate HQ network. This additional firewall will provide additional security for database traffic (and future proposed applications to be added to DMZ 2) and will provide another layer of firewall security for the internal corporate network. Lastly, there is another ISS IDS network sensor directly behind the Checkpoint firewall and directly in front of the internal corporate network router.

The reason for having two DMZs is DMZ 1 is mainly utilized for semi-public Web applications, FTP traffic, proxy traffic, and proxy server (Microsoft ISA Server). These are zoned on purpose

© SANS Institute 2000 - 2005 Author retains full rights.

so the external servers in DMZ1 are separated from the SQL Server database servers in DMZ 2. In addition, DMZ 2 is set up for future growth and can contain external servers, which might need additional security than DMZ 1 such as third party web applications, etc. Moreover, having a DMZ 2 will be the more secure place for sensitive data such as personal data than storing it in DMZ 1.

Cleveland, Ohio Office Specifics

The Cleveland office is primarily involved in sales for GIAC Enterprises. The office has approximately 35 employees although there were over 50 at one time. This physical building which GIAC Enterprises leases, houses only GIAC employees. Since most of the company's applications are located in Milwaukee, WI (HQ), a dedicated T-1 connects to GIAC Headquarters to provide plenty of available bandwidth to the employees. In addition, all Internet traffic must go through the GIAC Enterprises corporate HQ network, thus, a T-1 connection is important. There is an on site Network administrator who is part of the IT department. Finally, there is a Windows 2000 Domain Controller (DC) and Print & File Server for the local employees. The local DC is used for authentication purposes at this time.

Rotterdam, Netherlands Office Specifics

This building is also primarily a sales office and has approximately 30 employees. It is situated in downtown Rotterdam, Netherlands and thus has great communication and transportation links. This office has a T-1 connection to the corporate HQ network. There are two key servers that include a local DC and a Print & File Server. Since the office is projecting major growth, it was decided that it is better to have a local DC for authentication, which is able to handle an increase in employees. Lastly, there is a full time network administrator on site who is part of the IT department

Hong Kong, China Office Specifics

The Hong Kong Facility is another state-of- the-art facility. It has approximately 35 employees. It has a T-1 connection to the corporate HQ network, which provides ample bandwidth for the use of several enterprise applications. The building houses the R & D department as well as a Sales department. This office is where a lot of the research and designs are developed. Two network administrators are staffed as part of the IT staff.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

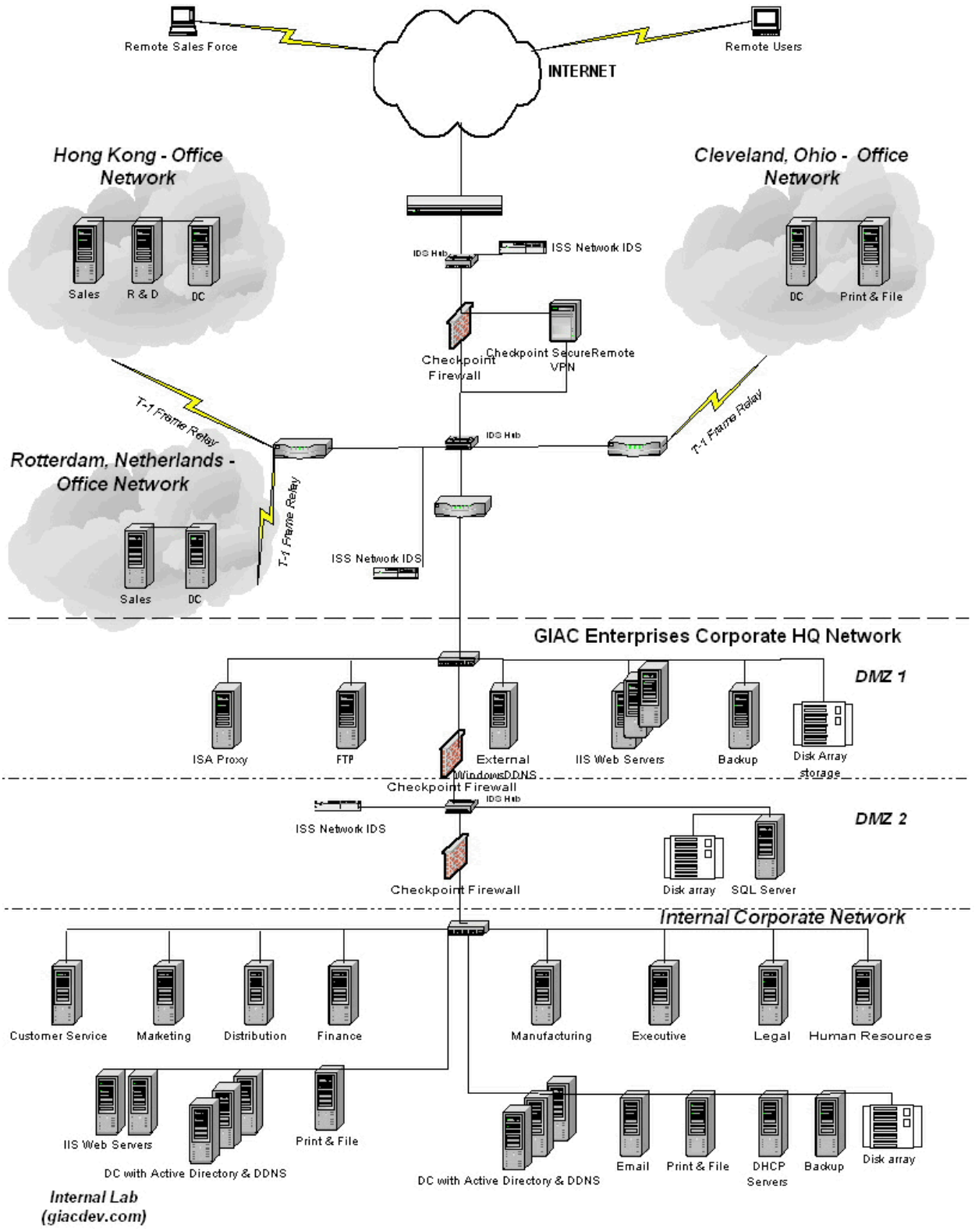


Figure 1 - Overall Network Design for GIAC Enterprises

© SANS Institute 2000 - 2005 Author retains full rights.

Locations and Roles of Key Servers

The critical and key servers for the company are all located behind a pair of firewalls depending on the criticality of the servers. The key servers and their locations as depicted in Figure 1 and are as follows:

- IIS Web Servers – GIAC Enterprises has two configuration sets of Microsoft IIS 5.0; one located internally to be used in the intranet and the other within the DMZ 1. Both of these Microsoft IIS Web Server installations are on Microsoft Advanced Server 2000. The availability criticality of both the external and internal web servers are crucial for the intranet and extranet web based applications. Thus, load balancing is utilized.
- Microsoft Mail Exchange Server 2000 – Email server is used for GIAC Enterprises employees and is located in the GIAC Corporate HQ internal network. The only ability of remote users to retrieve mail is to tunnel via a Checkpoint VPN.
- Windows 2000 Domain Controllers (DC) and Microsoft DNS - a Windows 2000 domain controller is a server that hosts the Active Directory and that runs the Kerberos KDC authentication service. There are three Active Directory DCs with integrated Dynamic Domain Name System located within the internal corporate network and within the internal lab.
- DHCP Servers – primary and secondary dedicated DHCP servers are used. Within the DHCP scope, all Net Bios has been disabled.
- Microsoft SQL Server 2000 Database Servers – the database platform standard at GIAC Enterprises There is a dedicated SQL Server 2000 located in DMZ 2 to provide an additional layer of security. In addition, some departments utilize SQL Server 2000 on a their department server for basic database services.
- Microsoft ISA Server – GIAC Enterprises Proxy services standard. It also provides caching for web pages for employees, which increases overall Internet web browsing performance. The proxy server is located in the DMZ 1 for overall security purposes. It acts as an overall forwarding proxy and web-caching server.
- Backup –utilized in both the DMZ and Internal corporate HQ network The standard backup system includes Veritas tape backup as well as legato. The actual policies such as day, time, regularity of backups and the procedures such as offsite storage, restorations of data etc. are detailed in the GIAC Enterprises baselines.
- VPN – located on the external perimeter of the company's network It performs IPSEC encryption (at Internet Protocol level) for all remote computer connections to the Checkpoint Secure-remote VPN appliance. There are no dial-up services offered at this time.
- Print & File Server – located within the internal corporate network. In addition, there is a Print & File Server located at each branch office location. The primary purpose of these dedicated machines provide pooling of print jobs locally as well as home directories for users and departments within GIAC Enterprises.
- Verisign Certificate Authority – third party certificate server issues x.509 certificates in order to secure e-business transactions with Secure Socket Layer (SSL). The authenticity of GIAC Enterprises' web sites is verified with a Verisign private key.

© SANS Institute 2000 - 2005 Author retains full rights.

Server Configuration

As previously stated, using the latest techniques of hardening at the time the servers were configured assists in securing the environment. This includes, but is not limited to, applying hot fixes, service packs, limiting services, and changing default account names, etc. Any relevant patches or hot fixes are applied monthly unless a security bug is reported.

DNS Design

Windows 2000 Domain Controllers and clients require DNS. DNS is no longer an optional service on Microsoft Windows 2000 networks.[1] Windows 2000 requires DNS entry during initial setup. The general DNS setup standards include the following:

- The DNS zone records are separated based on their associated GIAC enterprises namespace, which provides better security.
- Internal TCP/IP settings are retrieved from internal DHCP servers.
- GIAC clients register names within internal DNS network.
- Dynamic DNS (Windows 2000 DDNS) is deployed for the internal network. This is a key administrative burden, which is eliminated by the old, manual DNS change method.
- DMZ DNS is independent of Windows 2000 Active Directory and thus the Active Directory is not deployed in DMZ. In addition, servers within DMZ are only known and resolve names within DMZ and Internet
- The DNS design (refer to Figure 2) within GIAC Enterprises based on their respective namespace:
    - giac.com – Internet specific applications and DMZ services. This domain is legally registered and provides name services for the DMZ and external
    - corp.giac.com – GIAC Enterprises internal network
    - devgiac.com – GIAC Enterprises internal development network, is strictly for internal and is not connected to Internet. Also, it is on its own subnet.
- Each DNS namespace correlate to their respective Active Directory namespace.

Active Directory is designed to use DNS as a locater service to allow it to exist with the global Internet name space.[2] GIAC planned and made as many considerations available to them when designing the actual DNS structure. The company wanted an all encompassing as possible domain that could cover the entire organization

Active Directory Design

The key step in any Active Directory implementation includes the design and build of the overall

[1] Jason Fossen, 5.1 Windows 2000 Active Directory and Group Policy, SANS Institute, 93.

[2] David Iseminger, Active Directory Services for Microsoft Windows 2000: Technical Reference, (Redmond, WA: Microsoft Press, December 1999) 94.

© SANS Institute 2000 - 2005 Author retains full rights.

Active Directory structure. The owners of GIAC Enterprises spent considerable time studying the way they would structure the Active Directory around the way their enterprise is administered. They were told they could go with a design as simple as a single domain model or they could create additional domains based on their geographic locations. They knew large corporations had successfully implemented a single domain model so this was not a huge concern. However, the company wanted their design to be able to allow for growth without completely rebuilding their Active Directory.

GIAC owners thought about creating domains per geographic locations but decided against geographic domains for the time being because of the increased administrative and physical hardware costs. They knew they could always use an existing OU or could create an OU to migrate into a domain in the future. However, they did decide to design the Active Directory with an "empty root" for easier administration of the schema and so they would have the option for future growth.. Although the family did not think reorganization was plausible given the tight ownership relations, they still planned for the "just in case" scenario.

This section provides a description and explanation of the logical Active Directory structure of the GIAC network, which includes the affect of Active Directory on network administration, performance and security.

Domain Design

The Windows 2000 Domain structure is an inverted tree structure with the root at the top. The root domain is giac.com, and the child domain is corp.giac.com as depicted in Figure 2. A single child domain (sub-domain) of the root domain has all users, computers, and group accounts in a single child domain except those that are directory administrators in the forest root. Thus, by using a dedicated root domain, the overall administration membership is limited and the dedicated domain will not become obsolete. A top-level domain hosts the root of the namespace and contains only specific administrator accounts. This structure allows the flexibility of adding multiple domain trees in a single forest without rebuilding the forest.[3]

[3] Gary L. Olson, (September 2001). Windows 2000 Active Directory Design and Deployment, 446.

© SANS Institute 2000 - 2005 Author retains full rights.

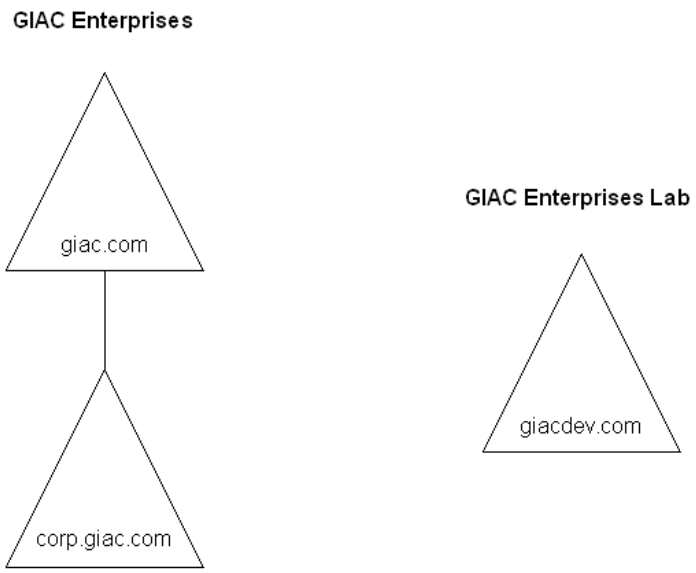


Figure 2 – GIAC Enterprises – Windows 2000 DNS/Domain namespace

There is a separate development environment, giacdev.com; however, this is strictly used as both a sandbox to test various applications before installing them in the production environment and as a training tool. The development environment is quite volatile and so it utilizes its own single subnet. It is usually updated quarterly by using back up tapes with a replica of production which are then restored into the development environment. However, there are times when the Active Directory database becomes corrupted from testing and training and needs a restoration of production more frequently. The standard corporate policies and procedures do not apply for the development environment. Lastly, developers who use the giacdev.com environment have separate logins and typically use a dedicated workstation to access the development environment.

Note: The development environment (giacdev.com) is not in scope for this project and is used as needed.

Organizational Unit (OU) Design

The organizational unit provides the flexibility needed to allow change within GIAC Enterprises' organization without the penalty of adding hardware and the time-consuming operation of installation and configuration. OUs can be created to reflect any organizational entity desired.[4] This means that an administrator can manage users and resources in an OU even though he or she cannot access the same resources in other parts of the domain. Having said this, there are two primary uses for the organization unit: delegation of administration and also a way to implement security via Group Policy for GIAC Enterprises. GIAC Enterprises has focused more of their efforts on the Group Policy security than they have with delegation of administration since the delegation still needs to be defined by senior management at this time. However, there

[4] Gary L. Olson, (September 2001). Windows 2000 Active Directory Design and Deployment, 131.

© SANS Institute 2000 - 2005 Author retains full rights.

are some departments that are beginning to perform some administrative duties.

During the initial design of GIAC Enterprises' OU hierarchy, security was the primary goal when creating an environment that would allow for the future ease and simplicity of centralized administration. The management is centralized in Milwaukee and drives all department agendas. Following this premise, the company has created an OU structure, which it believes to match its overall administrative model and organizational methodology. The company is continually trying to define itself in terms of its actual organization. GIAC Enterprises has been trying to redefine how its departments operate and also provide more departmental guidelines. In the past, because the business was young, small and less defined, departments were more or less names. The responsibilities could cross over into several other areas, but now these areas are beginning to be more functionally oriented. As a result, there are some basic administrative tasks that have begun to be delegated at the department level such as password or account resets and user management. Typically these tasks have been handled by the IT staff, but some of these tasks are starting to be managed by the respective Finance, HR, R&D, Sales, Marketing, Customer Service.

There is a multitude of ways in which to organize objects within OUs. GIAC Enterprises took the basic and simple approach in its creation of OUs. The way in which GIAC Enterprises chose to structure their OUs was to classify the users and computers within an associated functional OU, which is driven by business requirements and specific corporate policies. The department first-level OU containers are used more for a placeholder at this time. Under the OUs, GIAC Enterprises created sub OUs (second level OU container), which separates its users and workstations. For simplicity and for commonality, the departments that function synonymously were included in the same sub OU container. For instance, the Sales/Marketing departments are in the same OU and the Manufacturing and Distribution departments are in their own OU. Thus, some Organizational Units include more than one department but with Group Policy can segregate what policy is applied to a particular group of users (discussed later in the Group Policy section). The rationale behind this was that these departments share similar corporate policies and functions that would be easier to administer and presently, it just makes the most sense.

GIAC Enterprises views its flat OU structure (often defined as one or two levels of OUs), as an opportunity to assist in driving business requirements at the department level instead of at the senior management level. Over time, the company sees its different departments' functions increasing and thus, will require their own OU. However, at this time, the company is quite satisfied with just being able to have a standardized environment with built-in security to manage all their users and their workstations throughout the organization.

If GIAC Enterprises wants to expand its remote locations, they can expand their Active Directory infrastructure. Some options include: creating additional domains and adding them to the forest or they may use additional OUs to take care of expansion. The practice of using OUs to separate users and computers has become very popular and thus, GIAC Enterprises pursued this design.[5]

Group policies were developed to be deployed across the domain for security such as general

[5] Gary L. Olson, (September 2001). Windows 2000 Active Directory Design and Deployment, 173.

© SANS Institute 2000 - 2005 Author retains full rights.

user permissions and rights. These will be supplemented by the functional group policies applied at the organizational unit level (2nd level) for each grouping of users and workstations

To summarize the diagram in Figure 3, the users and workstations policies are stored in their associated OU container for the purpose of easier and future delegated administration and also for the purpose of the Group Policy being applied to the appropriate departments.

The Executive OU contains the senior management users and workstations. The Executive OU was created more for segregation purposes. In addition, the executive group's overall policy has more restrictions than IT or R&D but fewer restrictions than the rest of the departments. The senior management uses some tools, which the rest of the company does not. Also, they typically will call the IT department if they have a question especially regarding security. Segregating the Executive printers is also important.

The Finance OU has two sub OUs. One OU is for the Finance users and one is used for the Finance workstations. The OU structure is also the same for the Customer Service, HR, and R&D OU Containers. The HR users and the Finance users have slightly different policies regarding delegation of administrative duties since some employees in the HR group can modify some types of user information while Finance cannot.

The Manufacturing and Distribution Group was created once again for general ease of administration. These two departments work hand in hand and the types of uses and functions typically amount to printing, email and on-line entry. The sub OUs for the Manufacturing Users and Distribution users separates the users by department for the purposes of distinguishing the users from their departments, but their workstations security is applied the same.

The R&D OU is its own group because they use a lot of developing tools and thus this group requires fewer controls in order to be able to develop their creative solutions. There is the least restriction in this OU and only domain level security is applied to this group. There are a few basic administrative tasks that are delegated to the Hong Kong office to prevent in the middle of the night wake up calls even though these are unpreventable. These will be discussed in the Group Policy section.

The Sales & Marketing OU contains two sub OUs: one for the Sales users and one for the Marketing users. Both Sales & Marketing share the same Sales and Marketing Workstations OU policy because they require the same kind of machine security. In addition, this group is performing some administrative tasks that the IT staff is beginning to delegate. There are a few trusted, employees who have some additional administrative privileges, which assist the departments. It also helps resolve basic inquiries and issues to the remote office Sales departments.

The IT & IT Security OU segregates its IT department and its IT Security department by its sub OUs for users. The IT/IT Security sub OU for workstations applies to both. This is a logical grouping for an OU, since all the basic, intermediate and advanced administration is handled in this area. There is the least restriction in this OU. It should be noted no additional security

© SANS Institute 2000 - 2005 Author retains full rights.

polices are applied to the IT staff other than the GIAC Enterprises domain policy. This is obviously done to provide fewer restrictions so they can perform their jobs.

In order to separately control the different kinds of servers it was necessary to segregate the servers into different organizational units. The Domain Controllers have their own OU to allow for special security and audit features. Servers that are not Domain Controllers are placed in their own servers OU called Member Servers. These servers include various application and file servers typically shared among multiple departments. Thus, they are separated from the workstations so the special trusted individuals within the IT department could easily administer them.

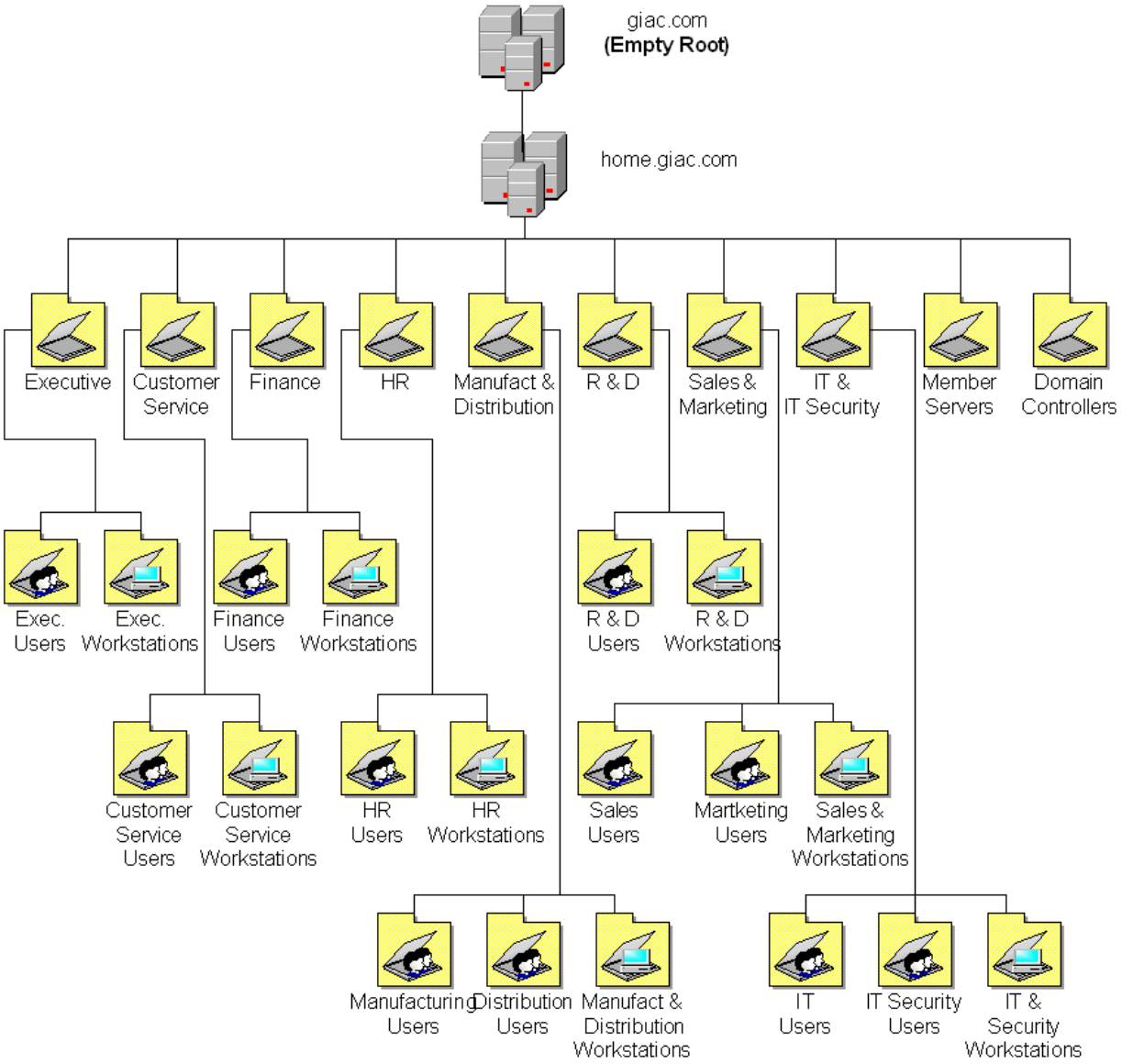


Figure 3 - Organizational Unit (OU) Design (two-tier)

© SANS Institute 2000 - 2005 Author retains full rights.

Note: Deeply nested OUs are usually a sign of faulty OU design. As a general rule of thumb, you should only use first-and second-level OUs. When you begin creating OUs at the third level and beyond, a warning light should come on in your head. Third level OUs are usually a sign that your OUS structure is growing too much or that your hierarchal design is not broad enough.[6]

Trust Relationship

Kerberos is the security protocol in Windows 2000. Kerberos trusts are two-way transitive trust relationships that are automatically created and configured by the Active Directory.[7] Thus, when a new child domain is created, the child domain automatically trusts the parent domain and vice versa. This means that authentication requests can be passed between the two domains in both directions. The child domain, corp.giac.com and root domain, giac.com, automatically trust each other due to two way transitive trusts.

Active Directory Infrastructure

There are three, remote physical branch sites that are all connected to the hub site (Milwaukee) via dedicated T-1 links. These physical sites are not required to have their own Domain Controllers, however, to ensure availability and faster logons, global catalogs exist on remote DCs.

Windows 2000 Active Directory - Site Design

The components of a Windows 2000 Active Directory Replication design are IP Subnets, collections of IP subnets called Sites, the connections between those sites called Site Links and the collection of all Site Links. The basic design reflects the overall topology of the WAN. The next section discusses the classification of sites, and identifies replication design components.

Active Directory - Site Classification

The definition of a site is a set of well-connected (LAN speeds or greater) IP subnets.[8]

During the site design, there was more than one perspective on the meaning of a site. Since slightly different terminology can be used, the definition of a site became confused with other areas of Active Directory. Microsoft also defines a site link as a connection object between two or more sites. By creating a site link, the administrator can then assign a cost, a replication schedule, and a transport for replication. Cost is an arbitrary value selected by the administrator to reflect the relative speed and reliability of the physical connection between the sites; the lower the cost, the more desirable is the connection.[9] As more sites are created and as the physical network connections vary for different sites, it is an important setting which must be accurately included.

---

[6] Curt Simmons, (November 2000). Active Directory Bible, Hungry Minds, Inc. 57.
[7] Curt Simmons, (November 2000). Active Directory Bible, Hungry Minds, Inc, 42.
[8] Microsoft Corporation: Best Practice Active Directory Design for Managing Windows Networks, 83. http://www.microsoft.com/windows2000/docs/bpaddsgn.doc
[9] Microsoft Corporation: Active Directory Branch Office Planning Guide, Chapter 3, Planning Replication for Branch Office Environments, 3.7. http://www.microsoft.com/windows2000/docs/ADBOC03P.doc

© SANS Institute 2000 - 2005 Author retains full rights.

The number of users in a location and the services required are two factors in making this decision. Replication traffic, availability, and security issues are considerations, which will usually result in placement of a domain controller in each branch. The assumption can be made when two sites are part of a site link, any two of the sites can communicate at the cost specified by the administrator.[10] The administrator for the sites must be knowledgeable about the company's overall network speed and factors that can affect the overall capacity of the site.

Certain characteristics of network operations at GIAC Enterprises geographic locations can be used to categorize those locations into mainly Core Sites. By being able to categorize the branch offices, it facilitates grouping of sites. When the sites are grouped, a similar design and implementation factors can be applied to multiple locations rather than considering every location as a special case. This enables standardization of the environment into several discrete levels.

The following table specifies the site classes based on available bandwidth, traffic considerations and business impact:

Office Location (All are Core)	External Network Bandwidth (30%-40% utilization)	# of users	Local Data	Business Continuity Impact	Typical Network Services
Milwaukee, WI (HQ)	High >1.544 mbps	265	Much	Critical	Multiple redundant server pairs
Cleveland, Ohio	High >1.544 mbps	35	Some	Low	Single Server
Rotterdam, Netherlands	High >1.544 mbps	30	Some	Low	Single Server
Hong Kong, China	High >1.544 mbps	35	Medium	Medium-High	Single Server

Table 3 - Site Classification

Site definition is important because there are several considerations that determine where in the topology that certain types of servers should and should not be placed. Windows 2000 has recommended that specific servers perform certain operations in the Active Directory environment. These servers are designated for the Flexible Single Master Operation (FSMO) Roles as shown in Table 4. They are all centrally managed locally at the corporate headquarters site.

[10] Microsoft Corporation: Best Practice Active Directory Design for Managing Windows Networks, 86. http://www.microsoft.com/windows2000/docs/bpaddsgn.doc

© SANS Institute 2000 - 2005 Author retains full rights.

FSMO (Flexible Single Master Operation)	**ROLE**	**GIAC. COM**	**CORP. GIAC.COM**	**Remote Sites Domain Controllers**
Schema Master • *Installed with Domain Naming Master on same AD machine at root in the internal corporate HQ network*	*It makes changes to the Active Directory schema. The entire forest shares the same schema. There is one Schema Master per forest.*	X		
Domain Naming Master • *Installed with Schema Master on same AD machine at root in the internal corporate HQ network* • *It is also the Global Catalog Server for GIAC Enterprises.*	*It can only add or delete domains within the forest.*	X		
RID Master • *Installed on same dedicated server as the PDC Emulator*	*It is responsible for supplying blocks of object IDs for the creation of objects within a domain. There is one RID master per domain.*	X	X	
PDC Emulator • *Installed on same dedicated server as the RID Master*	*It acts as a Primary Domain Controller for all down-level clients. There is one PDC Emulator for each domain.*	X	X	
Infrastructure Master • *Installed as a non-Global Catalog server but has direct connection to the global catalog*	*It is responsible for updating cross-domain group-to-user references within a domain. It does this by updating the references locally then using replication to update the rest of the domain.*	X	X	
Domain Controller/Global Catalog Server • *Cleveland* • *Rotterdam* • *Hong Kong*				X X X

© SANS Institute 2000 - 2005 Author retains full rights.

Table 4 – Flexible Single Master Operation Server Roles

As depicted in Table 4, GIAC Enterprises' Active Directory design deployed a separate DC/GC server at each of its remote office sites. This improves performance and provides an alternate authentication method in case the link for the WAN is interrupted. This is a recommended practice by Microsoft: "A global catalog server is required for logon to native-mode Active Directory domains. To eliminate the need to contact a global catalog server in a distant site for logons and for forest-wide searches, designate at least one domain controller per site as a global catalog. Setting site link parameters on site link objects configures inter-site replication. Thus, each site link object represents the WAN connection between two or more sites.[11]
The following steps are used to control how replication occurs between sites:

1. Connect sites with site links to model the way that your locations are connected
2. Name the site links
3. Set site link parameters
    - Cost
    - Schedule
    - Interval

Active Directory Administrative Roles

The success of this administrative model depends upon standardization of functions to help guarantee consistency in the application of policies and procedures. As mentioned, the company is currently trying to redefine more defined functional roles. Active Directory will allow GIAC Enterprises to delegate control for any Active Directory object and containers to administrators for localized administration should the requirement be needed.[12] In addition, requiring auditing functions to help guarantee compliance with those items will help determine success.

This model is meant to be simplistic, but at the same time has the ability of growing and becoming more complex as the enterprise utilizes more features including delegated administration. The current environment uses various levels of administration including: enterprise administrators, schema administrators, domain administrators and administrators. These roles are more or less implied by Active Directory and specific, trusted individuals are chosen to be members of specific administrator groups.

Active Directory Security Design

Active Directory represents physical entities such as persons or computers as user accounts or computer accounts. Active Directory uses user and computer accounts to perform authentication, security administration, allow/deny access to resources, and auditing functions.[13]

[11] Microsoft Corporation: Best Practice Active Directory Design for Managing Windows Networks, 91. http://www.microsoft.com/windows2000/docs/bpaddsgn.doc
[12] David Iseminger, Active Directory Services for Microsoft Windows 2000: Technical Reference, (Redmond, WA: Microsoft Press, December 1999) 149.
[13] David Iseminger, Active Directory Services for Microsoft Windows 2000: Technical Reference, (Redmond, WA:

© SANS Institute 2000 - 2005 Author retains full rights.

The authorization for specific personnel is required upon entry to any locked computer server room storing various Domain Controllers and Active Directory servers. The approved personnel are Schema, Enterprise, Domain and sometimes Site Administrators, which for now are one in the same with the former administrators. Their entry card is the only way in which entry into these rooms is permitted. In addition, all server access is logged. These mandatory secure measures have been taken as an overall push for physical security access.

Another aspect of security involves domain level and global catalog security. Since a global catalog replica is stored on all the Domain Controllers, it is important that access be secure. As mentioned in the Network Design section, all servers have been properly hardened and non-required services have been disabled. All servers incorporate IT security baselines and are routinely backed up with media being stored offsite. The security policies applied to these machines add another layer of security. Some of these, to name a few, include password protected screen savers, non-display of previous accounts on login screen and login warnings, which are discussed in the next section.

Finally, there are only four trained and trusted employees with the privileges to make any enterprise-wide changes. These are the designated members of the Enterprise Administrators and Schema Administrators group. They are responsible for maintaining domain security and requisite enterprise-level functions.

Group Policy and Security

Group Policy is a way of enforcing many configuration settings on groups of users/computers. In Windows 2000, the primary means in which security is configured is with Group Policy. Group Policies are effective in ensuring the corporate policies are met from a user's desktop to the servers themselves. By utilizing Group Policy, GIAC Enterprises is able to centrally manage and enforce security across the domain through enforcement of rights and rules dictated by the company.

By creating a simplified, functional OU structure, GIAC Enterprises is able to apply the appropriate policy to the proper department. As previously mentioned, the company is primarily concerned with security settings being applied throughout the organization. Thus, the predominant policy throughout the enterprise is the GIAC Enterprises Domain Policy.

Other policies that apply additional security include the Default Domain Controllers Policy, Server Members Policy, and the Executive, Customer Service, Finance, HR, Manufacturing/Distribution, and Sales/Marketing. The Group Policy is divided into two main areas: user configuration and computer configuration. The computer policies are set on the associated computer whereas the user configuration is associated with the user and thus will follow the user no matter where that user tries to login.

Microsoft Press, December 1999) 62.

© SANS Institute 2000 - 2005 Author retains full rights.

It is important to note, the policies load in local, site, domain, and OU (LSDOU) order, and settings of policies applied last prevail. By default, Group Policy implements inheritance in the opposite order, so OUs inherit domain-level settings, which in turn inherit site-level policies. You can block Group Policy inheritance, but doing so usually is not a recommended practice.[14] GIAC Enterprises is not using Site policies at this time, because the OU specific objects.

Security Groups

GIAC Enterprises currently utilizes Global Groups to manage and control user accounts. These groups are used to apply permissions based on the roles of the users. The user accounts are setup in a logical manner with others of same functional responsibilities. These Global Groups are created for the appropriate groups specifically, Executive, Customer Service, Finance, HR, Manufacturing and Distribution, R&D, Sales, and IT. They are applied and populate the Local Groups and their respective OU. Thus, provide the final access type. Once the Local Groups have been populated, the policy is tattooed on the local machine. Local Groups typically provide the "actual" access to resources.

Many Group Policy experts recommend that an organization assign permissions through group membership and provide access to the user by ensuring that the user is put in an appropriate group.[15] By performing this type of assignment, there is a decreased need for setting permissions for each user and can be applied to the groups instead.

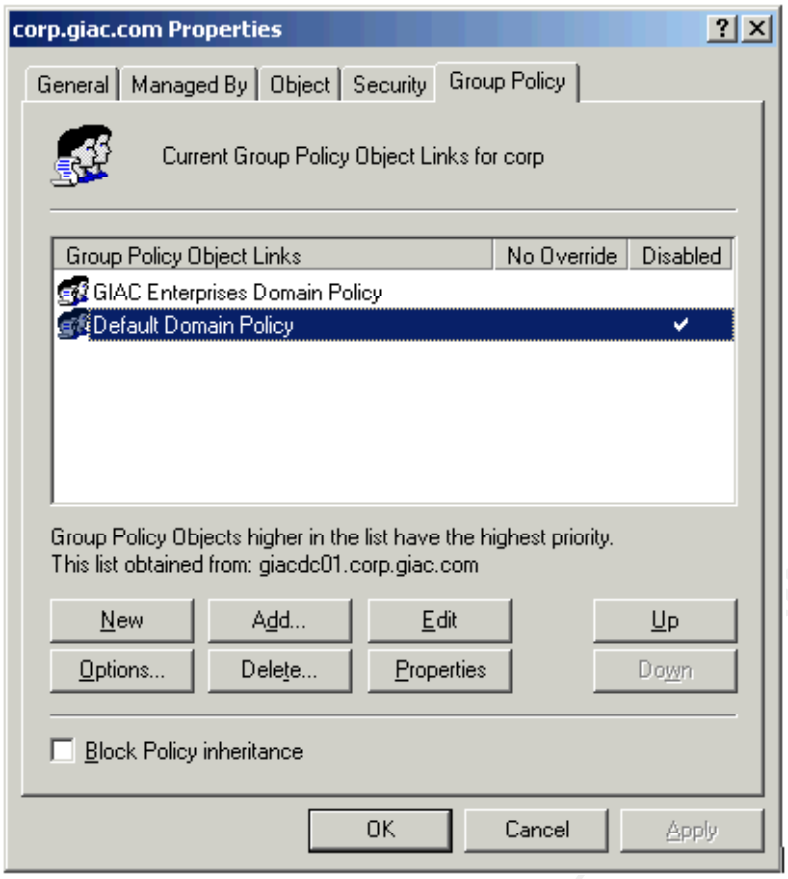
DOMAIN GROUP POLICY

The GIAC Enterprises' Domain Policy is a newly created policy based on the Default Domain Policy. This was created in order to simplify and make it recognizable that this is in fact the company's domain policy. The GIAC Enterprises Domain Policy uses some additional settings that provide additional types of security and is also applied to the root domain. The Default Domain Policy is left alone and it is disabled as illustrated in the example. Most of the settings in the Default Domain Policy have been incorporated into the GIAC Enterprises Domain Policy.

Note: There is an enterprise virus system in use. All machines have virus protection on them and perform a "pull" from the central virus signature update server located internally.

[14] Roger Jennings, (November 2000). Admin 911: Windows 2000 Group, McGraw-Hill, 5.
[15] Joe Casad, & Jane Brownlow, (April 2000). Windows 2000 Active Directory, McGraw-Hill, 137.

© SANS Institute 2000 - 2005 Author retains full rights.



The Group Policy, as mentioned previously, is separated into two areas: computer and user configuration. In the GIAC Enterprises Domain Policy, the focus is on computer policy section being used throughout the enterprise. Therefore, by using a base computer configuration for the enterprise, the company is able to incorporate the minimum company requirements based on its policies and provide standardization. There are only a few settings (password protected screen savers) for the user configuration section within the GIAC Enterprises Domain Policy. This is done so more specific settings can be at the OU level applied based on the function of the department and/or user and it enhances overall performance. Also, by doing this, specific OU groups such as IT and R&D can continue to have fewer restrictions than the rest of the OUs.

The important settings as they pertain to GIAC Enterprises and security are discussed. If a setting is not shown, it is either using a default setting or it is not required at GIAC Enterprises.

The software setting is not used at this time since GIAC Enterprises is not using automatic installation of software feature within Active Directory at this time. GIAC Enterprises is using a third party solution, Altiris.

Password Policy	Computer Setting
Enforce password history	10 passwords
Maximum password age	90 days

© SANS Institute 2000 - 2005 Author retains full rights.

Minimum password age	1 day
Minimum password length	7 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

The password settings are chosen to keep users from using the same passwords. If a user continually uses same password, it is quite possible someone in his or her work area will know it and be tempted to use their login if their account is not working. By enforcing a password history, the same passwords cannot be reused. Passwords expire after 90 days. A password cannot be changed for at least a day. This is done so a user cannot immediately change a password back to a frequently used one. In addition, these settings make it more difficult to guess someone's password because of the character length. The complexity requirements for the password is enabled, which means the password must incorporate three out of four character types: uppercase, lowercase, numeric, and special characters such as comma etc. This also combats brute force attacks or general password guessing. Lastly, storing passwords should never be enabled because it is basically the same as storing clear-text versions of the passwords.

Account Lockout Policy	**Computer Setting**
Account lockout duration	30minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Computer Configuration\Windows Settings\Security Settings\ Account Policies\Account Lockout Policy

The company IT security policy requires the uses of the above settings. In addition, these settings assist in providing protection for password cracking. If the user fails to logon after 5 attempts, he/she must wait thirty minutes or get their account reset.

Kerberos Policy	**Computer Setting**
Enforce user logon restrictions	Default
Maximum lifetime for service ticket	Default
Maximum lifetime for user ticket	Default
Maximum lifetime for user ticket renewal	Default
Maximum tolerance for computer clock synchronization	Default

Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy

© SANS Institute 2000 - 2005 Author retains full rights.

Kerberos is an authentication mechanism used to verify user or host identity. The Kerberos v5 authentication protocol is the default authentication service for Windows 2000.[16] At this time, the Kerberos Policy is set at the 'out-of-the-box' default options. However, these settings may be changed depending upon future company discussions.

Audit Policy	Computer Setting
Audit account logon events	Failure
Audit account management	Success
Audit object access	Failure
Audit system events	Success, Failure

Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Poilicy

Audit Policy can track activity that occurs on an object such as a printer object or resources. GIAC Enterprises uses auditing to track resource abuse, possible security breaches, and troubleshooting. There are not any limitations on log space based on the log settings. The audit policy assists in troubleshooting events and assists IT staff with auditing account issues. Typically, the IT staff will review the audit logs when issues arise, but employees are beginning to view the logs when they have additional time.

The account logon is set to failure, which tracks all unsuccessful logons to a computer. This can be helpful because it can log information of suspected unauthorized persons attempting to logon to a machine. The account management is set to success. This setting will track when a user account is created, changed, deleted, renamed, disabled, enabled or when a password is set/changed. This is good information especially in performing security analysis.

The audit object access determines whether to audit the event of a user accessing an object such as a printer or file. Some of the Executive files and printers objects are being audited. Lastly, the audit system events assist in determining a system error.

Security Options	Computer Setting
Additional restrictions for anonymous connections	No access without explicit permissions
Digitally sign client communications (when possible)	Enabled
Digitally sign server communications (when possible)	Enabled
Disable ctrl-alt-delete for login	Disabled
Do not display user name	Enabled
Rename Administrator account	GiacAd001,

[16] Windows 2000 Server Resource Kit, "Authentication Methods in Windows 2000 Server."

© SANS Institute 2000 - 2005 Author retains full rights.

Rename Guest account	Guestisoff and disabled
LanManager Authentication Level	Sent NTLM v2 responses only/refuse LM
Message text for users logging on	Enabled (see below)
Secure Channel: digitally encrypt secure channel data (when possible)	Enabled
Secure Channel: Digitally sign secure channel data (when possible)	Enabled
Secure Channel: require strong session keys (windows 2000 or later)	Enabled

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

This section is very important in configuring security in Windows 2000. Therefore, the important options will be applied at the domain level. The above settings are configured within the Security Options.

By setting the additional restrictions for anonymous connections to no access without explicit permissions keeps anonymous or null users from accessing the network and enforces valid accounts only.

By enabling the digitally sign client and server communications (when possible) allows secure transmission of data between client/server; however, unsecured transmission can still occur because of the setting when possible.

In order to not allow users from automatically logging in, the disable ctrl-alt-delete must be disabled because the default value allows this.

When a user logs off and walks away from his or her desk, Do not display user name makes it more difficult for someone to guess who has logged in last.

Renaming the administrator account is a basic security measure to keep hackers from using the default account. All the employees who need access know this setting. The same is true for the Guest account, which is disabled.

An important setting is the LanManager using NTLM v2. Since the GIAC Enterprises network is native mode Windows 2000, this setting affects the ability of Windows 2000 computers from communicating with NT 4.0 and earlier computers. This level of authentication provides a more secure authentication protocol and keeps hackers from using the older LM and NTLM protocols which has been a popular hacker practice.

The message text for users who log in is as follows:
"This system is the property of GIAC Enterprises. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to GIAC Enterprises, and law enforcement personnel, as well

© SANS Institute 2000 - 2005 Author retains full rights.

as authorized officials of other agencies, both domestic and foreign. ***By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or GIAC Enterprises personnel."***

Secure channel digital encryption and signatures can be utilized because all the Domain Controllers in the domain support are signing and sealing.

Event Log Policy	Computer Setting
Maximum application log size	5 MB
Maximum security log size	10 MB
Maximum system log size	2 MB
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retain Application Log	Overwrite events older than 14 days
Retain Security Log	Overwrite events older than 14 days
Retain System Log	Overwrite events older than 14 days
Retention Method for Application Log	Overwrite Events as needed
Retention Method for Security Log	Overwrite Logs – as needed
Retention Method for System Log	Overwrite Events every 5 days

Computer Configuration\Windows Settings\Security Settings\Event Log

The Event Log Policy is somewhat interrelated with the Audit Policy. These settings define the behavior of the logs. They are applied to all the computers with the domain. However, these settings will be increased for additional security on the Domain Controllers policy.

These settings are set to allow enough time for the support staff to perform any troubleshooting and also provide minimal system degradation performance. The primary purpose for these settings is for troubleshooting and security. GIAC Enterprises would like to be able to have their users review their logs at least once a week, however, they do not want to enforce this activity since it would cut into its business time.

System: Group Policy	Computer Setting
Group Policy refresh intervals	90 minutes
Group Policy refresh interval for Domain Controllers	30 minutes

Computer Configuration\Administrative Templates\System\Group Policy

These settings allow for any changes or modifications that will be updated on the machine. For

© SANS Institute 2000 - 2005 Author retains full rights.

the DCs, they need to refresh more often and thus the setting every 30 minutes. If a user needs to have the policy take effect sooner, re-logon will force the changes to take place sooner.

The only user configuration setting for the GIAC Enterprises Domain Policy is with the screen saver section. The settings are listed below.

Control Panel - Display	User Setting	GIAC Explanation
Password protect the screen saver	Enabled	This setting secures the machine so a walk-by or neighbor will not be able to view confidential data.
Screen saver timeout	Enabled	This is set to 300 seconds (5 minutes). It is one area that the president of the company mandated.

User Configuration\Administrative Templates\Control Panel\Display

DOMAIN CONTROLLER GROUP POLICY

The Default Domain Controller Group Policy settings are used. Most settings are applied to the Domain Controllers OU. The Default Domain Controller Policy is applied to the empty root (giac.com). Password and account lockout policies are taken from the default domain policy. Therefore, some policies are not required. Only the settings, which are different than the GIAC Enterprises Domain Policy, are discussed for the Domain Controllers. Access is given to select members of the Windows 2000 Administrators team.

Audit Policy	Computer 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	Failure
Audit system events	Success, Failure

Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy

The audit policy settings for Domain Controllers are more granular and thus have more settings than the Default Domain Policy settings. GIAC Enterprises wants to be able to audit all the various options in case the Audit team or any investigative analysis is required. The Domain administrators along with the server administrators try to review the logs on a weekly basis. Currently, the logs are stored locally and there are no reported issues with performance or space. The account logon is set to Success/Failure, which tracks all successful and unsuccessful logons to a computer. This can be helpful because it can log information of suspected unauthorized persons attempting to logon to a machine. An entry is logged for each user that is validated against that domain controller even though the user is logging on to a workstation that is part of

© SANS Institute 2000 - 2005 Author retains full rights.

the domain.

The audit account management setting logs when groups or users are created, changed or deleted or when a user account is renamed, disabled or enabled or a password change.
The account management is set to success or failure. This is good information especially in performing security analysis.

The audit object access determines whether to audit the event of a user accessing an object such as a printer or file. Some of the Executive files and printers objects are being audited.

The audit privilege use determines whether to audit each instance of a user exercising a user right. Since GIAC Enterprises likes to use the logs for troubleshooting, this was set to failure. The setting will also show if a user is attempting to use an access right that is not authorized

Lastly, the audit system events assist in determining a system error.

Event Log Policy	Computer Setting
Maximum application log size	10 MB
Maximum security log size	20 MB
Maximum system log size	5 MB
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retain Application Log	Overwrite events older than 14 days
Retain Security Log	Overwrite events older than 28 days
Retain System Log	Overwrite events older than 14 days
Retention Method for Application Log	Overwrite Events as needed
Retention Method for Security Log	Overwrite Logs – as needed
Retention Method for System Log	Overwrite Events as needed
Shut down the computer when the security audit is full	Disabled

Computer Configuration\Windows Settings\Security Settings\Event Log

The Domain Controllers require more security and thus additional auditing measures are added to the Default Domain Controllers Policy. It is important to be able to keep a history of the security logs for four weeks. However, if they fill up, will be overwritten as needed to avoid any major issues. There are no disk space issues for the storage of these logs and the settings should not pose any substantial performance hits. Typically, the administrators who manage the DCs review these logs every week. If the logs are flooding too rapidly, then the administrator can make the necessary adjustments.

© SANS Institute 2000 - 2005 Author retains full rights.

Next, additional settings are applied to the DC Policy for the user rights assignment within the computer configuration of the Group Policy.

User Rights Assignment Policy	Computer Setting	GIAC Explanation
Access this computer from the network	Administrators, Authenticated Users	These settings enable authenticated users and administrators to connect to the computer over the network. There is also no "Everyone" group.
Add workstations to domain	Domain Administrators	It is important to note the significance of the OU setup to add workstations to Domain. The Domain/System Administrators have the rights to add workstations to the domain. This setting is only valid to the Domain Controllers.
Bypass traverse checking	Server Operators Backup Operators Administrators	The default setting included the Everyone group, which has been removed.

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

As noted in the third column, these are the required changed settings GIAC Enterprises enforces using the User Rights Assignment Policy. There are approximately thirty additional default settings (Default Domain Controller Policy), which the company believes to be acceptable and are used.

MEMBER SERVERS GROUP POLICY

This OU consists of servers that include Application and Web Servers. These settings are not as granular as the Domain Controller settings because the needs for the increased audit/logging are not required for these servers and therefore, the settings are changed slightly. The GIAC Enterprises Domain Policy still applies to this group. The only different settings applied are the audit and event log areas as listed below. Access is given to the Windows 2000 Administration team as well as the Web Server and Application Server administrators.

Audit Policy	Computer Setting
Audit logon events	Success, Failure
Audit account logon events	Success, Failure
Audit object access	Success, Failure
Audit system events	Success, Failure

Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy

The same reasoning applies to this group, as with the previously mentioned audit policy, however less auditing is necessary with this group.

© SANS Institute 2000 - 2005 Author retains full rights.

Event Log Policy	Computer Setting
Maximum application log size	5 MB
Maximum security log size	10 MB
Maximum system log size	5 MB
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retain Application Log	Overwrite events older than 7 days
Retain Security Log	Overwrite events older than 14 days
Retain System Log	Overwrite events older than 14 days
Retention Method for Application Log	Overwrite Events as needed
Retention Method for Security Log	Overwrite Logs – as needed
Retention Method for System Log	Overwrite Events as needed
Shut down the computer when the security audit is full	Disabled

Computer Configuration\Windows Settings\Security Settings\Event Log

FUNCTIONAL OU GROUP POLICIES

There are hundreds of combinations of settings that can be applied to desktops, application software and specific security. GIAC Enterprises has configured settings in Group Policy that they believe will provide better security for the company. These settings will change as the enterprises changes, but changes will only take place after following the company change control process.

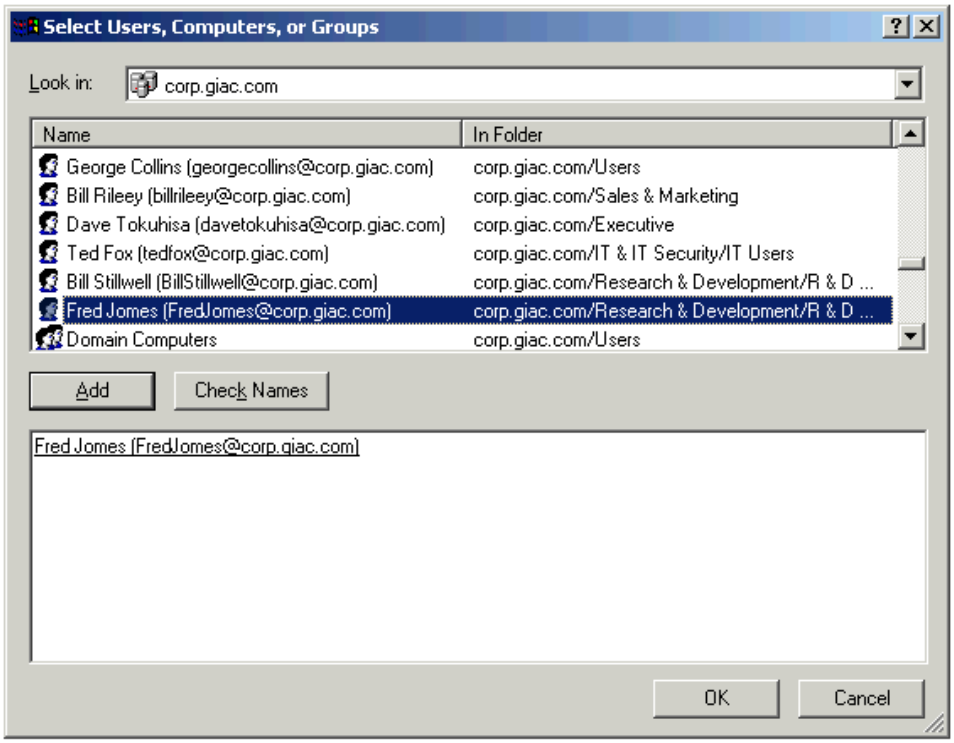
As mentioned in the Active Directory section, GIAC Enterprises used the popular method of creating a placeholder OU and placing secondary or sub-OUs under their respective OU. The Group Policy is applied to the second level OUs that consist of users and workstation. By applying Group Policy at the second level, it provides better administration and performance. In other words, group policies for workstations only need workstation policy, and thus do not need user configuration and vice versa. This minimizes the amount of settings and makes it easier for overall use.

The delegation is minimal and the only departments that are performing any delegation are Customer Service, R&D, HR and Sales. The delegation includes administrative duties such as: password reset, creating, deleting, and managing user accounts. The other departments depend on the IT department for assistance. The settings from GIAC Enterprises Domain Policy continue to apply to the entire department OUs. Also, it has been mentioned that GIAC Enterprises uses Altiris to provide software updates and various other solutions. Thus, software installation portion of Group Policy is not configured.

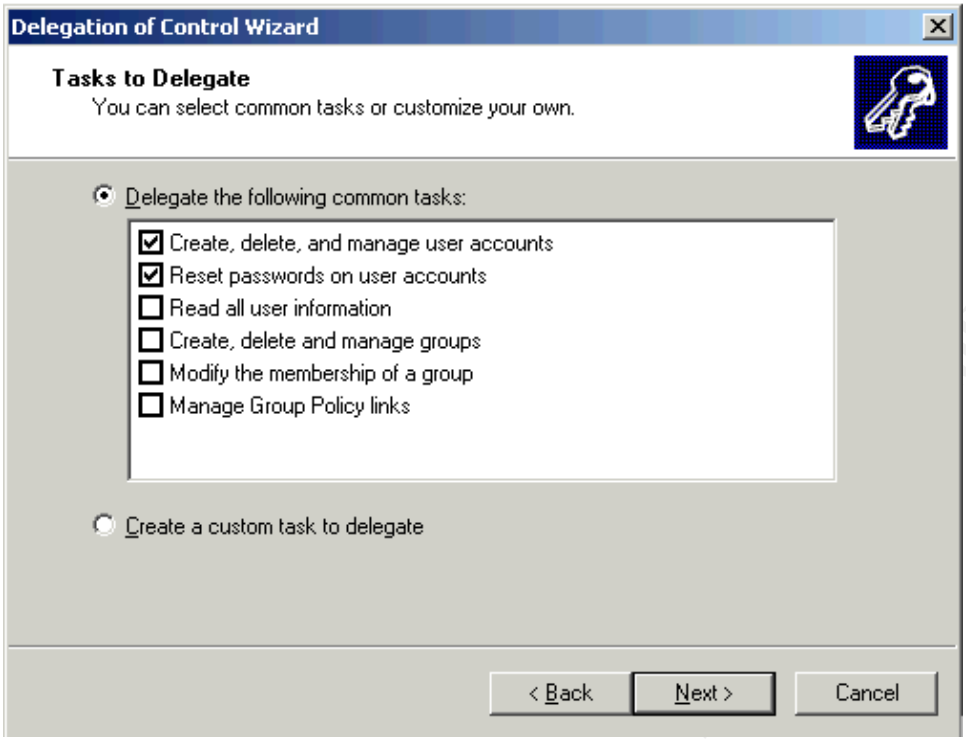
© SANS Institute 2000 - 2005 Author retains full rights.

R&D Group Policy

There is basic delegation of password resets, add, delete and manage user accounts. This privilege is given to the local IT administrator and the manager. The reason the delegation was initiated was the time zone difference could cause a long wait time for things like passwords to be resolved if the local administrator was busy with other tasks. Also, the IT folks were tired of being paged in the middle of the night for a password reset when the administrator was not available.



© SANS Institute 2000 - 2005 Author retains full rights.



Note: IT & IT Security and R&D department OUs use the GIAC Enterprises Domain Policy as their primary GPO and do not have any additional GPOs applied at this time. The ability to have more flexible access and fewer restrictions than other groups is imperative for these two groups to perform their jobs properly.

Executive Group Policy
Currently, there is no delegation of administration within this group. The settings are applied and performed by the IT department.

The additional settings apply to the Exec workstations for this group is listed below.

Internet Explorer	Computer Setting	GIAC Explanation
Disable automatic install of Internet Explorer components	Enabled	Prevents additional explorer components from being installed
Disable periodic check for Internet Explorer updates	Enabled	The goal is to keep the browsers standardized and to only allow the IT department to determine when updating is necessary.

Computer Configuration\Administrative Templates\Windows Components\Internet Explorer

Windows Installer	Computer Setting	GIAC Explanation
Enable User to patch elevated products	Disabled	Keeps standardized environment.

Computer Configuration\Administrative Templates\Windows Components\Windows Installer

© SANS Institute 2000 - 2005 Author retains full rights.

Again, the settings are more for caution and standardization. However, this setting will prevent new patch being applied that may not be compatible with other programs. The IT department does not want to restrict the Executives (per their direct request) from too much since they will allow this type of activity for their area.

Network and Dial Up Connections	Computer Setting	GIAC Explanation
Allow configuration of connection sharing	Disabled	This removes the tab and wizard page from being seen.

Computer Configuration\Administrative Templates\Windows Components\Network\Network and Dial-up Connections

By removing the tab for connection sharing, the vulnerability of spoofing or viruses such as worms is reduced.

Printers	Computer Setting	GIAC Explanation
Allow printers to be published	Disabled	This is disabled to provide more autonomy and secrecy to the executives' printers.

Computer Configuration\Administrative Templates\Windows Components\Printers

At this time, there is no need for other employees to be able to view or print to the senior management printers.

The user configuration settings applied to the Exec Users group are listed below.

Internet Control Panel	User Setting	GIAC Explanation
Disable the Security Page	Enabled	Removes the security tab from the interface in the Internet Explorer\Options window

User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel

The Internet Control Panel setting will maintain the Internet Explorer security zone and maintain the medium zone security.

MMC Console snap-ins	User Setting	GIAC Explanation

© SANS Institute 2000 - 2005 Author retains full rights.

Restrict users to the explicitly permitted list of snap ins.	Enabled	Prevents users using any additional snap in. The allowable snap ins are the following: Disk Manager, Disk Defragmenter, Services, Shared Folders, System Properties, Event Viewer, Performance Logs and Alerts, Local Users and Groups, Services.

User Configuration\Administrative Templates\Windows Components\Microsoft Management Console

The MMC console can be used for the aforementioned tools. If the any of the executive staff should require more, they will be turned on per their request.

Start Menu and Taskbar	User Setting	GIAC Explanation
Disable and remove links to Windows Update links	Enabled	Again, this is created for standardization reasons. This will hide the update links shortcut in the start menu.

User Configuration\Administrative Templates\Start Menu & Taskbar

Control Panel - System	User Setting	GIAC Explanation
Disable registry editing tools	Enabled	This will harden the OS and not allow employees to modify or customize their registry.

User Configuration\Administrative Templates\System

It is important to not restrict the Executive users too much. Occasionally, they want to use certain features within Internet Explorer as well as NetMeeting and thus the major settings are not activated for this group. The senior management has expressed this, and said they would use the caution.

Customer Service Group Policy

This group allows delegation of administration to the department manager for password resets, create, delete and manage user accounts within the Customer Service group. She is trained and trusted to make these changes.

The workstation settings applied to the computers for the Customer Service group is listed below.

Net meeting	Computer Setting	GIAC Explanation
Disable remote Desktop Sharing	Enable	It is not allowed at this time for this department.

Computer Configuration\Administrative Templates\Windows Components\NetMeeting

© SANS Institute 2000 - 2005 Author retains full rights.

Net Meeting would pose a security threat especially for less technical users, and might open up ports for applications, thus it is not allowed. If a remote presentation is required, employees create a presentation in word or power point and email it before having a teleconference call.

At present, GIAC Enterprises does not allow this department to use Net Meeting applications.

Internet Explorer	Computer Setting	GIAC Explanation
Disable automatic install of Internet Explorer components	Enabled	Prevents additional explorer components from being installed
Disable periodic check for Internet Explorer updates	Enabled	The goal is to keep the browsers standardized and to only allow the IT department to determine when updating is necessary.

Computer Configuration\Administrative Templates\Windows Components\Internet Explorer

The above settings are used to follow the company standards. Also, it provides an acceptable level of Internet Explorer security at this time.

Windows Installer	Computer Setting	GIAC Explanation
Disable Windows installer	Enabled	Prevents software installs and forces any software installations to be performed by IT administrator.

Computer Configuration\Administrative Templates\Windows Components\Windows Installer

The Windows Installer is disabled because it is the feeling of senior management that these users do not need additional applications unless approved.

Network and Dial Up Connections	Computer Setting	GIAC Explanation
Allow configuration of connection sharing	Disabled	This removes the tab and wizard page from being seen.

Computer Configuration\Administrative Templates\Windows Components\Network\Network and Dial-up Connections

The user configuration settings applied to the Customer Service Users group is listed below.

Internet Control Panel	User Setting	GIAC Explanation
Disable Advanced Page	Enabled	The advanced tab in the Internet Explorer options dialog box is not available.
Disable the Content Page	Enabled	This disables the ratings settings, the certificate settings, Profile Assistant settings, AutoComplete for forms and AutoComplete for passwords.

© SANS Institute 2000 - 2005 Author retains full rights.

Disable the Connections Page	Enabled	This setting disables the internet connection wizard, disables changing connection settings, proxy settings or automatic configuration settings.
Disable the Security Page	Enabled	Removes the security tab from the interface in the Internet Explorer\Options window

User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel

By configuring the settings within the Internet Control Panel many settings override the settings in the Internet Explorer. The settings explained above were configured so an employee could still browse the Internet, but could not open up possible holes in security such as auto-complete for saving passwords, or changing certificates. This setting will maintain the Internet Explorer security zone and maintain the medium zone security. The general tab in the Internet Explorer\Tools\Options are set since many users may want to view their history or create a personalized home page. The rest of the settings and their reasons are explained above.

MMC Console snap-ins	User Setting	GIAC Explanation
Restrict users to the explicitly permitted list of snap ins.	Enabled	Prevents users using any additional snap ins from the following: Device Manager, Disk Manager, Disk Defragmenter, System Properties, Event Viewer, Performance Logs and alerts, Local Users and Groups, Services.

User Configuration\Administrative Templates\Windows Components\MMC

The MMC console can be used for the aforementioned tools. These tools were allowed because they can assist the user as well as the IT department. The more powerful snap-ins was not allowed because they could provide opportunity for mischief.

Start Menu and Taskbar	User Setting	GIAC Explanation
Add Logoff to Start Menu	Enabled	This makes it easier for the employee to logoff and back especially if they need a group policy to take affect quicker.
Disable and remove links to Windows Update links	Enabled	Again, this is created for standardization reasons. This will hide the update links shortcut in the start menu.
Hide Add/Remove Windows Components page	Enabled	Makes the pre-configured machine more difficult to customize and follows the corporate standard.

© SANS Institute 2000 - 2005 Author retains full rights.

Hide the “Add a program from CD-ROM or floppy disk” option	Enabled	Makes the pre-configured machine more difficult to customize and follows the corporate standard.
Hide the “Add programs from Microsoft” option	Enabled	Makes the pre-configured machine more difficult to customize and follows the corporate standard.
Remove Run Menu from the Start Menu		This only affects the start menu and does not affect the help menu

User Configuration\Administrative Templates\Start Menu & Task Bar

By configuring the above settings, the policy helps harden the workstation from possible unlicensed software and continues to keep things standardized.

Add/Remove Programs	User Setting	GIAC Explanation
Disable Add\Remove Programs	Enabled	This policy removes Add/Remove Programs from Control Panel and removes from menus and prevents from adding or removing programs.

User Configuration\Administrative Templates\Control Panel\Add/Remove Programs

The setting standardizes the users workstation and makes more difficult to uninstall/install programs. The settings assist in standardizing the users workstation.

System	User Setting	GIAC Explanation
Disable registry editing tools	Enabled	This will harden the OS and not allow employees to modify or customize their registry.
Run only allowed Windows Applications	Enabled	A list of programs such as Word, Excel, Power Point, Access, Outlook, etc are listed.

User Configuration\Administrative Templates\System

Manufacturing & Distribution Group

These groups’ settings are identical to the previously mentioned group, Customer Service. Thus, The workstation settings from the Customer Service OU are the same for these groups’ workstations and likewise for the Manufacturing and Distribution user OUs. The only difference with this group is that there is no delegation of duties. The IT staff performs all administration and there are no plans to provide delegation within Manufacturing and Distribution departments.

Finance Group

Currently, there is no delegation within the Finance Group. They refer all issues and questions to the IT department.

The user configuration settings applied to the Finance workstations group is listed below.

© SANS Institute 2000 - 2005 Author retains full rights.

Net meeting	Computer Setting	GIAC Explanation
Disable remote Desktop Sharing	Enable	It is not allowed at this time for this department.

Computer Configuration\Administrative Templates\Windows Components\NetMeeting

Internet Explorer	Computer Setting	GIAC Explanation
Disable automatic install of Internet Explorer components	Enabled	Prevents additional explorer components from being installed
Disable periodic check for Internet Explorer updates	Enabled	The goal is to keep the browsers standardized and to only allow the IT department to determine when updating is necessary.

Computer Configuration\Administrative Templates\Windows Components\Internet Explorer

The above settings are used to follow the company standards. Also, it provides an acceptable level of Internet Explorer security at this time.

Windows Installer	Computer Setting	GIAC Explanation
Enable User to patch elevated products	Disabled	Keeps standardized environment.

Computer Configuration\Administrative Templates\Windows Components\Windows Installer

This department has the ability to use the Windows installer but not for upgrading programs.

Network and Dial Up Connections	Computer Setting	GIAC Explanation
Allow configuration of connection sharing	Disabled	This removes the tab and wizard page from being seen.

Computer Configuration\Administrative Templates\Windows Components\Network\Network and Dial-up Connections

The user configuration settings applied to the Finance Users group is listed below.

Internet Control Panel	User Setting	GIAC Explanation
Disable the Content Page	Enabled	This disables the ratings settings, the certificate settings, Profile Assistant settings, AutoComplete for forms and AutoComplete for passwords.
Disable the Connections Page	Enabled	This setting disables the internet connection wizard, disables changing connection settings, proxy settings or automatic configuration settings.
Disable the Security Page	Enabled	Removes the security tab from the interface in the Internet Explorer\Options window

© SANS Institute 2000 - 2005 Author retains full rights.

User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel

By configuring the settings within the Internet Control Panel many settings override the settings in the Internet Explorer. The settings explained above were configured so an employee could still browse the Internet, but could not open up possible holes in security such as auto-complete for saving passwords, or changing certificates.
This setting will maintain the Internet Explorer security zone and maintain the medium zone security.
The general tab in the Internet Explorer\Tools\Options are set since many users may want to view their history or create a personalized home page. The rest of the settings and their reasons are explained above.

MMC Console snap-ins	User Setting	GIAC Explanation
Restrict users to the explicitly permitted list of snap ins.	Enabled	Prevents users using any additional snap ins from the following: Device Manager, Disk Manager, Disk Defragmenter, System Properties, Event Viewer, Performance Logs and alerts, Local Users and Groups, Services.

User Configuration\Administrative Templates\Windows Components\MMC

The MMC console can be used for the aforementioned tools. These tools were allowed because they can assist the user as well as the IT department. The more powerful snap-ins was not allowed because they could provide opportunity for mischief.

Start Menu and Taskbar	User Setting	GIAC Explanation
Add Logoff to Start Menu	Enabled	This makes it easier for the employee to logoff and back especially if they need a group policy to take affect quicker.
Disable and remove links to Windows Update links	Enabled	Again, this is created for standardization reasons. This will hide the update links shortcut in the start menu.
Hide Add/Remove Windows Components page	Enabled	Makes the pre-configured machine more difficult to customize and follows the corporate standard.

User Configuration\Administrative Templates\Start Menu & Task Bar

Add/Remove Programs	User Setting	GIAC Explanation

© SANS Institute 2000 - 2005 Author retains full rights.

Disable Add\Remove Programs	Enabled	This policy removes Add/Remove Programs from Control Panel and removes from menus and prevents from adding or removing programs.

User Configuration\Administrative Templates\Control Panel\Add/Remove Programs

The Add/Remove setting standardizes the users workstation and makes it difficult to uninstall/install programs. The settings assist in standardizing the users workstation.

System	User Setting	GIAC Explanation
Disable registry editing tools	Enabled	This will harden the OS and not allow employees to modify or customize their registry.

Human Resources Group

The Human Resources Group does perform basic delegation. This is authorized for the HR manager. The manager performs basic delegation tasks (password resets, add, delete and manage user accounts).

Note: The configured settings are listed, however many of the settings are similar to the Finance Group. It was important for separation of duties to include the HR group and the Finance Group in their own OUs. Lastly, if the rationale or reasoning is unclear, refer to a previous section such as Customer Service. Many of the reasons are the same and thus, reasons are not needed to avoid being too repetitive.

The user configuration settings applied to the Human Resources workstations group is listed below.

Net meeting	Computer Setting	GIAC Explanation
Disable remote Desktop Sharing	Enable	It is not allowed at this time for this department.

Computer Configuration\Administrative Templates\Windows Components\NetMeeting

Internet Explorer	Computer Setting	GIAC Explanation
Disable automatic install of Internet Explorer components	Enabled	Prevents additional explorer components from being installed
Disable periodic check for Internet Explorer updates	Enabled	The goal is to keep the browsers standardized and to only allow the IT department to determine when updating is necessary.

Computer Configuration\Administrative Templates\Windows Components\Internet Explorer

The above settings are used to follow the company standards. Also, it provides an acceptable level of Internet Explorer security at this time.

© SANS Institute 2000 - 2005 Author retains full rights.

Windows Installer	Computer Setting	GIAC Explanation
Enable User to patch elevated products	Disabled	Keeps standardized environment.

Computer Configuration\Administrative Templates\Windows Components\Windows Installer

This department has the ability to use the Windows installer but not for upgrading programs.

Network and Dial Up Connections	Computer Setting	GIAC Explanation
Allow configuration of connection sharing	Disabled	This removes the tab and wizard page from being seen.

Computer Configuration\Administrative Templates\Windows Components\Network\Network and Dial-up Connections

The user configuration settings applied to the Human Resources Users group is listed below.

Internet Control Panel	User Setting	GIAC Explanation
Disable the Content Page	Enabled	This disables the ratings settings, the certificate settings, Profile Assistant settings, AutoComplete for forms and AutoComplete for passwords.
Disable the Connections Page	Enabled	This setting disables the internet connection wizard, disables changing connection settings, proxy settings or automatic configuration settings.

User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel

By configuring the settings within the Internet Control Panel many settings override the settings in the Internet Explorer. The settings explained above were configured so an employee could still browse the Internet, but could not open up possible holes in security such as auto-complete for saving passwords, or changing certificates. On the other hand, HR users can change the security zone because there are web applications that sometimes require a weaker zone within the browser. The general tab in the Internet Explorer\Tools\Options are set since many users may want to view their history or create a personalized home page. The rest of the settings and their reasons are explained above.

MMC Console snap-ins	User Setting	GIAC Explanation

© SANS Institute 2000 - 2005 Author retains full rights.

Restrict users to the explicitly permitted list of snap ins.	Enabled	Prevents users using any additional snap ins from the following: Device Manager, Disk Manager, Disk Defragmenter, System Properties, Event Viewer, Performance Logs and alerts, Local Users and Groups, Services.

User Configuration\Administrative Templates\Windows Components\MMC

The MMC console can be used for the aforementioned tools. These tools were allowed because they can assist the user as well as the IT department. The more powerful snap-ins was not allowed because they could provide opportunity for mishap or funny business.

Start Menu and Taskbar	User Setting	GIAC Explanation
Add Logoff to Start Menu	Enabled	This makes it easier for the employee to logoff and back especially if they need a group policy to take affect quicker.
Disable and remove links to Windows Update links	Enabled	Again, this is created for standardization reasons. This will hide the update links shortcut in the start menu.
Hide Add/Remove Windows Components page	Enabled	Makes the pre-configured machine more difficult to customize and follows the corporate standard.

User Configuration\Administrative Templates\Start Menu & Task Bar

By configuring the above settings, the policy helps harden the workstation from possible unlicensed software and continues to keep things standardized.

Add/Remove Programs	User Setting	GIAC Explanation
Disable Add\Remove Programs	Enabled	This policy removes Add/Remove Programs from Control Panel and removes from menus and prevents from adding or removing programs.

User Configuration\Administrative Templates\Control Panel\Add/Remove Programs

The Add/Remove setting usually requires the employee to call IT department for support. The setting standardizes the users workstation and makes it difficult to uninstall/install programs.

System	User Setting	GIAC Explanation
Disable registry editing tools	Enabled	This will harden the OS and not allow employees to modify or customize their registry.

User Configuration\Administrative Templates\System

© SANS Institute 2000 - 2005 Author retains full rights.

Sales & Marketing Group
To avoid repetition, the rationale for many of the settings remains consistent. The main focus is on the configuration of settings.

The sales users group requires some additional settings from the other departments due to mobility of the portable workstations. GIAC Enterprises does not want viruses or worms to be spread into the network. Firewall applications (Black Ice) installed on all the laptops because there are some users who use broadband ISPs from their homes. Lastly, the Internet Explorer settings are set stronger.

The Sales team works out of their office or use a Checkpoint Secure Remote VPN connection. When away from the office, usually at a client site, the sales users can tunnel into the GIAC network from their laptop. These types of mobile, remote connections increase the security for the connection and the transferred data. In addition, it is expected that all sales and marketing employees follow the GIAC Enterprises corporate baselines and IT Security policies. Lastly, the sales managers at each location are given basic delegation rights: password resets, add, delete and manage user accounts.

Security Options	Computer Setting	GIAC Explanation
Clear virtual memory page file when windows shuts down	Enabled	This ensures that sensitive information from process memory that might have made it into the page file is not available to an unauthorized Enabling this security option also causes the hibernation file (hiberfil.sys) to be zeroed out when hibernation is disabled on a laptop system.

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

The above setting is more for the laptop users, however it should not pose any issues for the non-laptop users.

Net meeting	Computer Setting	GIAC Explanation
Disable remote Desktop Sharing	Enable	It is not allowed at this time for this department.

Computer Configuration\Administrative Templates\Windows Components\NetMeeting

At present, GIAC Enterprises does not allow these departments host or view shared applications. This is a strong policy and may be changed some day, but at this time, it is felt that non-permission is the best policy because it prevents security vulnerabilities.

Internet Explorer	Computer Setting	GIAC Explanation

© SANS Institute 2000 - 2005 Author retains full rights.

Disable automatic install of Internet Explorer components	Enabled	Prevents additional explorer components from being installed
Disable periodic check for Internet Explorer updates	Enabled	The goal is to keep the browsers standardized and to only allow the IT department to determine when updating is necessary.

Computer Configuration\Administrative Templates\Windows Components\Internet Explorer

The above settings are used to follow the company standards. Also, it provides an acceptable level of Internet Explorer security at this time.

Network and Dial Up Connections	Computer Setting	GIAC Explanation
Allow configuration of connection sharing	Disabled	This removes the tab and wizard page from being seen.

Computer Configuration\Administrative Templates\Windows Components\Network\Network and Dial-up Connections

This feature is not allowed and therefore is not able to be configured.

The user configuration settings applied to the Marketing Users group is listed below.

Internet Control Panel	User Setting	GIAC Explanation
Disable the Content Page	Enabled	This disables the ratings settings, the certificate settings, Profile Assistant settings, AutoComplete for forms and AutoComplete for passwords.
Disable the Connections Page	Enabled	This setting disables the internet connection wizard, disables changing connection settings, proxy settings or automatic configuration settings.
Disable the Security Page	Enabled	Removes the security tab from the interface in the Internet Explorer\Options window

User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel

The Marketing Users have less restriction in their Internet Explorer control panel.

MMC Console snap-ins	User Setting	GIAC Explanation

© SANS Institute 2000 - 2005 Author retains full rights.

Restrict users to the explicitly permitted list of snap ins.	Enabled	Prevents users using any additional snap ins from the following: Device Manager, Disk Manager, Disk Defragmenter, System Properties, Event Viewer, Performance Logs and alerts, Local Users and Groups, Services.

User Configuration\Administrative Templates\Windows Components\MMC

Start Menu and Taskbar	User Setting	GIAC Explanation
Add Logoff to Start Menu	Enabled	This makes it easier for the employee to logoff and back especially if they need a group policy to take affect quicker.
Disable and remove links to Windows Update links	Enabled	Again, this is created for standardization reasons. This will hide the update links shortcut in the start menu.
Hide Add/Remove Windows Components page	Enabled	Makes the pre-configured machine more difficult to customize and follows the corporate standard.
Hide the "Add a program from CD-ROM or floppy disk" option	Enabled	Makes the pre-configured machine more difficult to customize and follows the corporate standard.

User Configuration\Administrative Templates\Start Menu & Task Bar

By configuring the above settings, the policy helps harden the workstation from possible unlicensed software and continues to keep things standardized. The Add/Remove program from CD-ROM or floppy disk option is currently being reviewed. This is a strong setting and might be allowed in the future.

Add/Remove Programs	User Setting	GIAC Explanation
Disable Add\Remove Programs	Enabled	This policy removes Add/Remove Programs from Control Panel and removes from menus and prevents from adding or removing programs.

User Configuration\Administrative Templates\Control Panel\Add/Remove Programs

This policy makes it more difficult to install and uninstall programs but it does not prevent users from using other tools to uninstall/install programs.

System	User Setting	GIAC Explanation
Disable registry editing tools	Enabled	This will harden the OS and not allow employees to modify or customize their registry.

User Configuration\Administrative Templates\System

© SANS Institute 2000 - 2005 Author retains full rights.

It is unnecessary for this group of users to modify the registry files.

The user configuration settings applied to the Sales Users group is listed below.

Net Meeting	User Setting	GIAC Explanation
Enable automatic configuration	Disabled	Does not allow NetMeeting to download settings for users each time it starts.

User Configuration\Administrative Templates\Windows Components\NetMeeting

Application Sharing	User Setting	GIAC Explanation
Disable Application Sharing	Enabled	Disables the host or viewed of sharing applications

User Configuration\Administrative Templates\Windows Components\NetMeeting\Application Sharing

Internet Control Panel	User Setting	GIAC Explanation
Disable the Advanced Page	Enabled	Not allowed to change advanced internet settings.
Disable the Content Page	Enabled	This disables the ratings settings, the certificate settings, Profile Assistant settings, AutoComplete for forms and AutoComplete for passwords.
Disable the Connections Page	Enabled	This setting disables the internet connection wizard, disables changing connection settings, proxy settings or automatic configuration settings.
Disable the Programs Page	Enabled	Sales Users cannot change or see the settings for the internet programs. This is beneficial because it might be tempting to point your mail program to a different email client.
Disable the Security Page	Enabled	Removes the security tab from the interface in the Internet Explorer\Options window

User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel

The sales users have all the pages disabled except the general page. As mentioned, this is a secure measure applied specifically to the sales users.

Browser Menu	User Setting	GIAC Explanation
Disable save this program to disk option	Enabled	Setting will not allow random downloads thereby keeping mobile computers clean from potential viruses, Trojan horses, etc.

© SANS Institute 2000 - 2005 Author retains full rights.

User Configuration\Administrative Templates\Windows Components\Internet Explorer\Browser Menu

This is setup for the Sales users to increase the security.

MMC Console snap-ins	User Setting	GIAC Explanation
Restrict users to the explicitly permitted list of snap ins.	Enabled	Prevents users using any additional snap ins from the following: Device Manager, Disk Manager, Disk Defragmenter, System Properties, Event Viewer, Performance Logs and alerts, Local Users and Groups, Services.

User Configuration\Administrative Templates\Windows Components\MMC

The MMC console is the company standard. Device Manager is chosen to be available to assist in a hardware issue driver issue.

Start Menu and Taskbar	User Setting	GIAC Explanation
Add Logoff to Start Menu	Enabled	This makes it easier for the employee to logoff and back especially if they need a group policy to take affect quicker.
Disable and remove links to Windows Update links	Enabled	Again, this is created for standardization reasons. This will hide the update links shortcut in the start menu.
Hide Add/Remove Windows Components page	Enabled	Makes the pre-configured machine more difficult to customize and follows the corporate standard.
Hide the “Add a program from CD-ROM or floppy disk” option	Enabled	Makes the pre-configured machine more difficult to customize and follows the corporate standard.
Hide the “Add programs from Microsoft” option	Enabled	Makes the pre-configured machine more difficult to customize and follows the corporate standard.
Remove Run Menu from the Start Menu	Enabled	This only affects the start menu and does not affect the help menu and keeps users from running special commands.

User Configuration\Administrative Templates\Start Menu & Task Bar

The Add/Remove program from CD-ROM or floppy disk option is currently being reviewed. This is a strong setting and might be allowed in the future.

GIAC Enterprises did not want the Run command available to the Sales users because their machines are quite often left attended for moments at a time, which would allow opportunities

© SANS Institute 2000 - 2005 Author retains full rights.

for customization and possible bypassing of the settings.

Add/Remove Programs	User Setting	GIAC Explanation
Disable Add\Remove Programs	Enabled	This policy removes Add/Remove Programs from Control Panel and removes from menus and prevents from adding or removing programs.

User Configuration\Administrative Templates\Control Panel\Add/Remove Programs

This policy makes it more difficult to install and uninstall programs but it does not prevent users from using other tools to uninstall/install programs.

System	User Setting	GIAC Explanation
Disable registry editing tools	Enabled	This will harden the OS and not allow employees to modify or customize their registry.

User Configuration\Administrative Templates\System

Users are unable to modify or tweak the registry files which could corrupt the entire OS.

Outlook 2002 - Security	User Setting	GIAC Explanation
Prevent users from customizing attachment security settings	Enabled	This is an overall security measure.
Allow access to e-mail attachments	Enabled – Specific attachments allowed, but .exe and others disallowed.	Prevents from additional viruses from being propagated such as Code Red.
Prevent users from adding HTTP e-mail accounts	Enabled	Prevents alternative means of email that is against IT security policy.

User Configuration\Administrative Templates\Microsoft Outlook 2002\Tools\Options\Security

These settings help filter potential viruses and worms by the Sales Users. Encryption for mobile computers is not utilized at this time. It is unable to use Encrypting File System via Group Policy and thus; a main reason it is not used. However, GIAC Enterprises is in the evaluation stage for comparing encryption products such as EFS and other third party solutions.

Conclusion

Even though GIAC Enterprises is a smaller size company, they have been able to demonstrate the success in securing their Windows 2000 network infrastructure. The key to the company's implementation was proper planning. They performed analysis and documented a project plan and then followed their blueprint in a phased type System Development Lifecycle approach. They built their infrastructure for "today" but set it up with plans and options for the future. This

© SANS Institute 2000 - 2005 Author retains full rights.

is key in a Windows 2000 implementation. Moreover, without the proper planning and documentation, it will be quite difficult to perform a solid, standardized rollout especially for the Group Policy.

GIAC Enterprises can now centrally manage their entire enterprise with less administrative issues and more robust features. Currently, the overall Active Directory Group Policy is configured so it may be modified and more security policies applied as the company grows and the confidence/knowledge level of the different administrators increases.

It can be said that initially the Windows 2000 Active Directory had a learning curve for GIAC Enterprises IT department. Over time, the comfort level and the skill level increased to where they are trying to get senior management to allow additional features and functionality. The next step is for the GIAC Enterprises senior management to provide more organizational details in terms of department responsibilities/roles as well as more distinct user roles. Once this is accomplished, more Active Directory features can be applied or added to Active Directory.

© SANS Institute 2000 - 2005, Author retains full rights.

References

© SANS Institute 2000 - 2005 Author retains full rights.

Anthes, Mary A. "A Secure Windows 2000 Infrastructure Design" September 26, 2001. URL: http://www.giac.org/practical/Mary_Anthes_GCNT.zip

Brandt, Brian "Remotely Administering Windows 2000" July 28, 2001. URL: http://www.giac.org/practical/Bryan_Brandt_GCNT.zip

Canady, Shawn "GIAC: Windows 2000 Design & Security" November 15, 2001. URL: http://www.giac.org/practical/Shawn_Canady_GCNT.zip

Casad, Joe, Brownlow, Jane. (April 2000). Windows 2000 Active Directory, McGraw-Hill

Currie, Robert "Windows 2000 Encrypting File System" July 24, 2001. URL: http://www.giac.org/practical/Robert_CURRIE_GCNT.zip

Fossen, Jason, "Windows 2000: Active Directory and Group Policy 5.1" The SANS Institute, August 2001.

Fossen, Jason, "Windows 2000: PKI, Smart Cards and EFS 5.2 " The SANS Institute, August 2001.

Fossen, Jason, "Windows 2000: IPSEC & VPN 5.3" The SANS Institute, August 2001.

Fossen, Jason, "Securing Internet Information Server 5.0, 5.4" The SANS Institute, August 2001.

Fossen, Jason, "Windows 2000 Scripting for Security and Auditing 5.5" The SANS Institute, August 2001.

Govanus, Gary & King, Robert. (August 2000). Windows 2000 Directory Services Design, Sybex Incorporated.

Iseminger, David. (December 1999). Active Directory Services for Microsoft Windows 2000: Technical Reference, Redmond, WA: Microsoft Press.

Jennings, Roger. (November 2000). ADMIN 911: Windows 2000 Group Policy, Berkeley, CA: Osborne/McGraw-Hill.

Lewis, Brett "Security Considerations for Windows 2000 Infrastructure Design. http://www.giac.org/practical/Brett_Lewis_GCNT.doc

Olson, Gary L. (September 2001). Windows 2000 Active Directory Design and Deployment, Indianapolis, IN: New Riders.

Securing Windows 2000 Step by Step. Version 1.5. SANS Institute, July 1, 2001.

Simmons, Curt L. (November 2000). Active Directory Bible, Foster City, CA: IDG Books.

Windows 2000 Server Resource Kit, Supplement 1, Redmond, WA: Microsoft Press, 2001.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.