Global Information Assurance Certification Paper

Security Considerations for Windows 2000 Infrastructure Design

Securing Windows
GCNT Practical Assignment
Version 3.0 – Option 1

Brett Lewis

15-Nov-2001

Table of Contents

Figures

Part 1
Introduction

This paper is the blueprint for a secure Windows 2000 network for a fictitious company named GIAC Enterprises. As a business engaged in the online sale of fortune cookie sayings, GIAC Enterprises deals with various outside parties, including customers, suppliers, and partners. However, this blueprint is focused on the internal network used by GIAC employees.

> Note: This paper was prepared as the practical assignment for the author's GCNT certification, the SANS Institute's accreditation in Securing Windows. All IP addresses included in this paper are for illustration purposes only.

The following main elements are included in the blueprint herein.

- **Network design** – An overview of the LAN/WAN environment provides a general idea of the logical and physical network architecture, as well as a description of the roles for the more important servers in the infrastructure. This section also explains why certain servers are placed in specific segments of the network. Furthermore, an overview of security considerations in regard to the server hardware is presented.

- **Active Directory design** – The Active Directory logical and physical architectures are presented in this section, with an explanation for each object that comprises the directory. Considerations for network administration, performance and security are addressed.

- **Group Policy and security design** – As the primary means by which security is configured and applied in the Windows 2000 environment, an overview of the Group Policy design for GIAC Enterprises is presented in this section. Included are details for some of the major security issues related to authentication, passwords, auditing, and security options for specific systems. Furthermore, the employment of Security Templates, which provide both a means of documenting and applying policy, is also reviewed. Some of the shortcomings of Group Policy are also discussed, and some workarounds for these shortcomings are suggested. Additionally, a look at some of the Group Policy features in Windows XP and Windows .NET Server show some of the improvements that are becoming available. Finally, an overview of GIAC's administrative model illustrates the various levels of administrative responsibilities and how these responsibilities are implemented.

Besides providing a sample blueprint, the paper is also intended to convey various considerations related to Windows 2000 infrastructure design and implementation. Even where certain design choices were not employed in the blueprint, an attempt is made to point out these other options. Furthermore, checklists are provided to help guide readers through the development of their own Windows 2000 infrastructure designs.

About GIAC Enterprises

GIAC Enterprises is a medium-sized company, with a total of one thousand employees in three locations in New York State. The corporate office, located in Troy, has nine hundred, fifteen permanent employees. The two branch offices, in Cambridge and Ithaca, have seventy-five and ten employees respectively. The branch offices exist because they are in close proximity to suppliers and partners.

The company is comprised of the following departments.

- **Customer Services** – Interfaces with the customer via web-based and e-mail communications.
- **Executive** – Includes the company's Chairman and CEO, President, as well as other top officials and their administrative support staffs.
- **Finance** – Responsible for the company's finances and insurance needs.
- **Human Resources (HR)** – Handles all matters related to personnel.
- **Information Security Office (ISO)** – Ensures the confidentiality, integrity and availability of critical information assets, while maintaining the ability of the business units to meet their missions.
- **Information Technology (IT)** – Designs, implements and manages the company's network and computing infrastructures. Develops web-based programs required to support the company's e-business.
- **Marketing** – Analyzes market trends and conditions as related to the demand for fortune cookie sayings.
- **Research and Development (R&D)** – Continuously engaged in developing new and improved fortune cookie sayings. Also assists in the development of new ad campaigns.
- **Sales** – Develops online ad campaigns for GIAC's web site, as well as for hosting on partner web sites. Manages all online sales. Works with suppliers and partners on all issues related to the company's e-business.

All departments are physically located at the company's headquarters in Troy. Additionally, the Ithaca branch office has employees in the Sales department, and the Cambridge office has employees in the Finance, HR, IT and Sales departments.

Part 2
Network Design

This section discusses the overall network design for GIAC Enterprises, including a LAN/WAN overview, DNS and DHCP strategies, and an overview of enterprise services provided on the network. Also included in this section are some standards and guidelines for the server environment.

Network Overview

The GIAC Enterprises network is essentially comprised of an internal corporate network, a compartmentalized perimeter network, including a screened services network (also known as a demilitarized zone, or DMZ), and two branch office networks. The company is connected to the Internet via a full T1 connection.

The external firewall controls all inbound and outbound traffic between the Internet and the GIAC network. No Internet traffic is allowed directly between the internal corporate network and the Internet. Only certain types of traffic are allowed between the Internet and the screened services network. Similarly, only certain types of traffic are allowed between the internal corporate network and the screened services network.

The In general, redundant network and system components are employed wherever feasible to ensure high availability and performance. Network devices (e.g. firewalls, switches, hubs, routers) are maintained at current versions of firmware. And all network devices are configured with strong passwords. (It's important to note that many network devices come factory-configured with passwords that are well documented and, therefore, easy for attackers to determine.)

Windows 2000 is ubiquitous at GIAC Enterprises. All servers are built on Windows 2000 Server; Windows 2000 Advanced Server is employed where services must provide clustering or network load balancing, for example on the internal and external web farms. Additionally, all client computers – both desktop PCs and laptops – run Windows 2000 Professional. Disk drives on every machine are configured to use NTFS. All systems are kept up to date with the latest Windows 2000 Service Packs and hot fixes, and all are configured for high encryption (128 bit). And all systems are configured with the latest anti-virus software and signature files from GIAC's antivirus vendor.

Critical Windows 2000 systems and systems that are more exposed to attack are hardened by removing unnecessary services, strengthening NTFS permissions on the appropriate objects, and employing host-based packet filtering. In general, all critical

systems utilize RAID 5 disk configurations with hot-swappable drives. And all servers are backed up regularly.

Figure 2.1 illustrates the overall LAN/WAN environment.

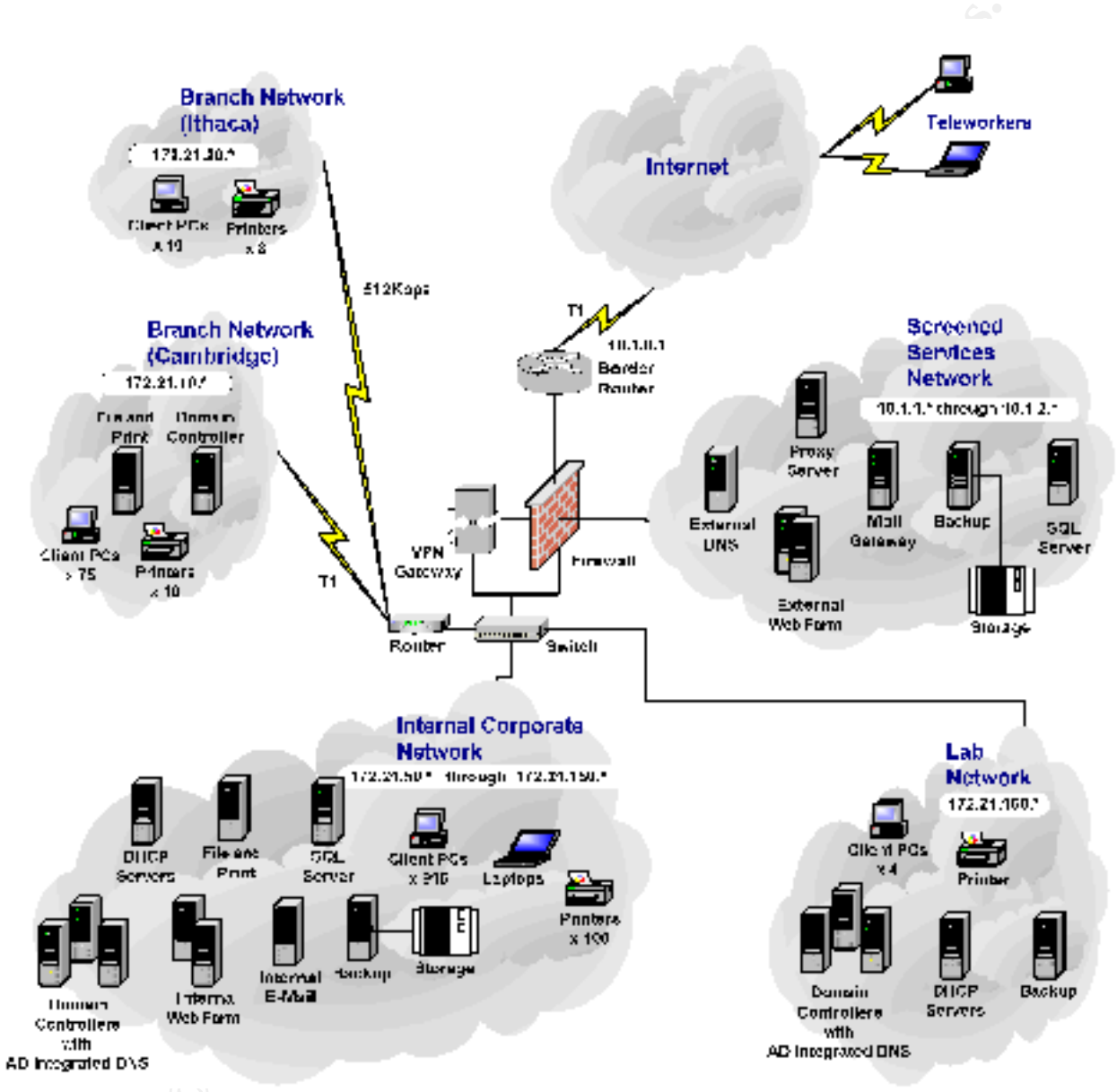

Figure 2.1 – Overview of network design for GIAC Enterprises

Internal Corporate Network

The internal corporate network, physically located in a single building in Troy, supports enterprise services for all of the company's employees. The entire internal network is

built on Fast Ethernet (100 Mbps), with redundant components to ensure high availability and performance.

The server farm employs an internal firewall to create a separate internal protected services network, which contains most of the company's critical systems, including the Windows 2000 domain controllers, DHCP servers, and internal web, mail, and database servers. The following services are available via the company's server farm.

- **Windows 2000 domain controllers** – Three domain controllers reside at the Troy site, and each also runs Microsoft Active Directory-integrated DNS. The details about the domain controllers are described in the section of this paper on Active Directory physical architecture.

- **DHCP** – Two dedicated Dynamic Host Configuration Protocol (DHCP) servers are employed, one primary and one backup.

- **File and Print Services** – Several file servers provide home directories for all users and departmental data for the entire company. Home directories have disk quotas set by default to 150 MB. Departmental data from the various file servers are made available to users a single logical view through distributed file system (DFS). Four dedicated print servers are used to spool the 100 printers at the Troy location.

- **Mail Services** – Microsoft Exchange Server 2000 is employed for the enterprise mail service.

- **Web Services** – GIAC's intranet site is built on Microsoft IIS 5.0. Because the company's model for business applications is a distributed, web-based architecture, availability and performance of the intranet is critical. Therefore, two IIS servers are built on Windows 2000 Advanced Server, with network load balancing. A staging platform mirrors the production platform and provides an area for administrators and users to test new and revised system and application software before it is moved to production. A development platform is also configured similarly, but is comprised of a single node.

- **Database Services** – Microsoft SQL Server 2000 is employed for the enterprise database solution. Currently the production platform is not clustered; however, GIAC system engineers are considering configuring this platform for fail-over clustering in the near future. To match the company's web development and staging platforms, a single SQL Server 2000 machine also exists within each of these platforms.

- **Backup Services** – An enterprise tape backup system backs up all servers on a regular basis. In accordance with the company's information security and disaster recovery policies, copies of the tapes are kept at a protected, off-site location.

The internal corporate network also includes 915 Windows 2000 Professional desktop PCs. Windows 2000 laptop computers are also permitted to connect to the internal network as necessary. All clients are configured to use DHCP.

Cambridge Branch Network

Cambridge, the larger of the two branch offices, also has a local area network built on Fast Ethernet, and is connected to the corporate network via a T1 circuit. Because the Cambridge office has 75 employees, a Windows 2000 domain controller is deployed there (more details in the Active Directory design section), as well as a file and print server. Although employees at the Cambridge office are authenticated locally, they rely upon connectivity with the corporate office in Troy for most of the enterprise services they utilize.

Ithaca Branch Network

The Ithaca branch office also has a local area network built on Fast Ethernet, and is connected to the corporate network via a 256 Kbps circuit. However, with only 10 employees, Ithaca does not have a local domain controller and therefore relies on connectivity with the corporate office in Troy for authentication, as well as all enterprise application services.

Screened Services Network

The screened services network, also physically located at the Troy site, provides services that are available via the public Internet. As previously mentioned, the company's external firewall allows only the appropriate traffic in and out of this network, thereby significantly limiting its exposure. To compartmentalize the screened services network, a firewall within this network separates the external database server from the rest of the servers in the DMZ.

Note that the DMZ does not employ Windows 2000 Active Directory, nor is it a part of any Windows NT domain. Although employing Active Directory in the DMZ would allow GIAC system administrators to more easily manage the servers on this network, it would make those servers more vulnerable.

The following services are provided in the DMZ.

- **DNS** – Two standard Microsoft Windows 2000 DNS servers are placed in the screened services network, one primary and one secondary. The primary server is authoritative for the giac.com domain. More information about the DNS implementation is in the section on DNS design herein.

- **Mail Gateway** – Microsoft Windows 2000 Server with SMTP services is configured as a mail relay server to pass e-mail to and from the internal MS Exchange Server.

- **Web Services** – GIAC's public web site is also built on Microsoft IIS 5.0. Because the company's online business relies upon high availability and performance, the external web farm is built on Windows 2000 Advanced Server, with network load balancing employed.

- **Database Services** – Microsoft SQL Server 2000 is employed for the external database solution. Databases include the fortune cookie sayings database, as well as customer databases and sales records. The database provides much of the dynamic content on the company's external web site.

- **Proxy Services** – Microsoft ISA Server, configured as a forward proxy server, provides Internet access for GIAC's employees. Proxy services significantly limit exposure to the internal corporate network by not requiring a hole to be opened in the firewall for each client computer to access the Internet. Additionally, as GIAC employees browse the web, the proxy server locally caches that web content, thereby improving performance for other employees who subsequently request the same web pages.

- **Backup Services** – An enterprise tape backup system backs up all DMZ servers in the on a regular basis. And just like with the internal backups, in accordance with the company's information security and disaster recovery policies, copies of these tapes are kept at a protected, off-site location.

DNS Design

Microsoft Windows 2000 DNS is used exclusively for name services at GIAC Enterprises. Because Windows 2000 is ubiquitous at the company, there is no need to maintain backward compatibility using WINS servers. For security purposes, each GIAC-controlled namespace is placed in a separate DNS zone.

DNS Namespace Design

GIAC utilizes three distinct DNS namespaces for its network. The first, "giac.com", is the company's registered domain name. This part of the company's DNS only serves to provide name services for the servers in the DMZ. The other two namespaces, "corp.giac.com" and "lab.giac.com", are used internally and build off of the company's registered domain name. Figure 2.2 illustrates the DNS namespace design.

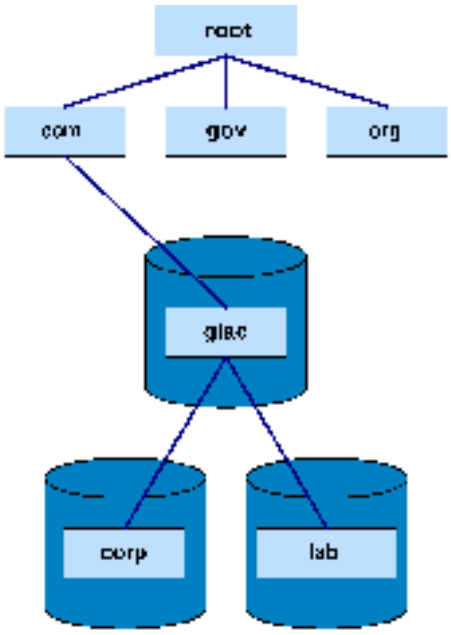

Figure 2.2 – DNS namespace design for GIAC Enterprises

The following list describes the purpose of each DNS namespace.

- **giac.com** – Screened services environment for hosting services and applications on the public Internet. This domain name is the company's registered domain name.
- **corp.giac.com** – Internal (private) network, supporting GIAC Enterprises computer users.
- **lab.giac.com** – Lab environment, providing an isolated environment to test changes before making those changes in the production environment.

DNS Implementation

DNS is implemented within the screened services network via standard primary and secondary Microsoft DNS servers. These servers provide name resolution for only servers on the screened services network; they are not aware of any servers on the internal GIAC Enterprises network. The primary server is authoritative for the giac.com domain.

The internal DNS servers handle all internal name resolution. Each of the internal DNS namespaces matches its corresponding Active Directory namespace, and GIAC has chosen to leverage Active Directory-integrated DNS for internal use. For security purposes, each GIAC-controlled namespace is placed in a separate DNS zone.

On all GIAC DNS servers, both internal and external, server addresses are configured manually into the DNS database. Clients are configured to get their TCP/IP settings via DHCP and to register their addresses in DNS.

Remote Access

GIAC allows remote access into the private network through two mechanisms: dial-in access through modems and Virtual Private Network (VPN) access via the Internet. In both of these mechanisms, ensuring the security of the network is of utmost importance. It is critical for the integrity of data stored on the network that all persons connecting through these means are those who are known users and who are allowed to remotely connect the network. A RADIUS (Remote Authentication Dial-In User Service) is employed on the GIAC network to authenticate all remote access users – both modem and VPN users – via GIAC Enterprises internal corporate Active Directory. VPN access is provided via a device that allows authorized users to establish an IPSec or PPTP tunnel from a remote client computer to the VPN device over the Internet, encrypting all traffic between the two points at the IP level.

Part 3
Active Directory Design

This section provides the blueprint for GIAC's two Active Directories, each running in native mode. First, an overview explains why two discrete Active Directories are implemented. Next the logical and physical architectures for each directory are presented.

Overview

The GIAC Enterprises production environment is architected as a single-domain Active Directory, spanning two sites. However, the design also includes a second Active Directory in a separate forest for the lab environment. The lab domain is used to test new software and configuration changes. Because some software and configuration changes can have an impact on the entire forest (e.g. Exchange Server 2000), it is critical to test these changes in a separate Active Directory forest before installing new software or making configuration changes in the production forest.

Figure 3.1 illustrates the overall forest and domain architecture for GIAC Enterprises. Note that an explicit two-way trust is established between the two domains; this trust exists simply to allow for easier management by IT staff.

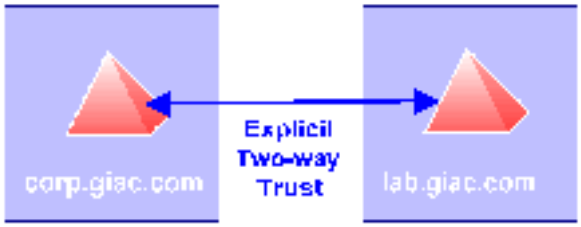

Figure 3.1 – Domain architecture

Corporate Active Directory Architecture

Logical Architecture

This Active Directory supports the internal GIAC enterprise computing infrastructure, and is implemented as a single forest and a single domain. The AD namespace, "corp.giac.com", is an extension of the company's registered Internet domain name.

OU Hierarchy

Figure 3.2 illustrates the OU hierarchy for the "corp.giac.com" domain. The structure is a hybrid model, with both physical locations and resource types representing the top-level of the hierarchy. All second-level OUs represent GIAC business units where there was a need to provide a separate container for administrative purposes.

Most of the business units fall into the "GIAC" OU within each location OU. However, the Finance, R&D, and Sales teams assist in the management of their resources; therefore, each of these teams has its own Organizational Units. More information about what administrative responsibilities are delegated to the Finance, R&D and Sales teams is specified later in this paper, under Administrative Model.

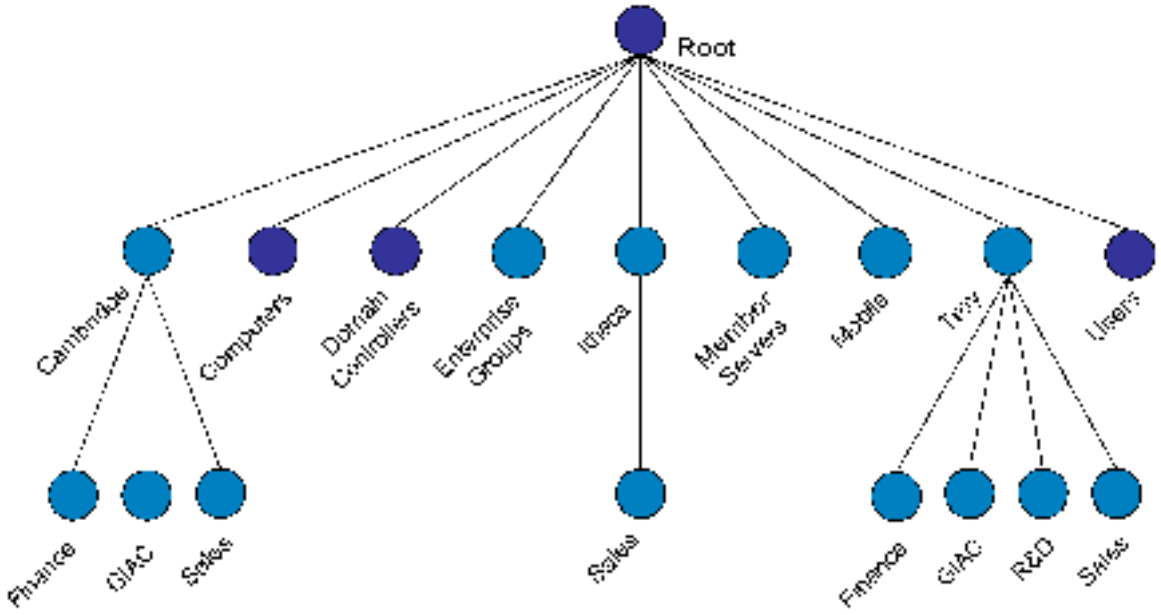

Figure 3.2 – OU hierarchy for corp.giac.com domain

The following list describes the purpose of each organizational unit.

- Cambridge – Contains the following second-tier OUs representing GIAC resources at the Cambridge location.
  - Finance – Contains user accounts, security groups, client computers, and printers that are particular to the Finance team at the Cambridge location.
  - GIAC – Contains user accounts, security groups, client computers, and printers that are particular to the Human Resources and Information Technology teams at the Cambridge location.

    - Sales – Contains user accounts, security groups, client computers, and printers that are particular to the Sales team at the Cambridge location.
- Computers – Built-in container; not used.
- Domain Controllers – Built-in container; contains all domain controller objects for the domain.
- Enterprise Groups – Contains all top-level enterprise security groups.
- Ithaca – Contains the following second-tier OUs representing GIAC resources at the Ithaca location.
    - Sales – Contains user accounts, security groups, client computers, and printers that are particular to the Sales team, the only GIAC team at the Ithaca location.
- Member Servers – Contains all member server objects for the domain, including DHCP servers, file and print servers, database server, web servers, mail servers, and backup servers.
- Mobile – Contains all laptop and other mobile computer objects.
- Troy – Contains the following second-tier OUs representing GIAC resources at the Troy location.
    - Finance – Contains user accounts, security groups, client computers, and printers that are particular to the Finance team at the Troy location.
    - GIAC – Contains user accounts, security groups, client computers, and printers that are particular to the Customer Services, Executive, Human Resources, Information Security, Information Technology, and Marketing teams at the Troy location.
    - R&D – Contains user accounts, security groups, client computers, and printers that are particular to the Research and Development team at the Troy location.
    - Sales – Contains user accounts, security groups, client computers, and printers that are particular to the Sales team at the Troy location.
- Users – Built-in container; not used.

Physical Architecture

The GIAC Enterprises Active Directory contains one hub site in Troy, one branch site with a domain controller in Cambridge, and one other smaller site in Ithaca without domain controllers.

Active Directory Site Topology

The GIAC Enterprises Active Directory contains one primary site in Troy, one branch site with a domain controller in Cambridge, and one other remote site in Ithaca without domain controllers. The latter remote site, without domain controllers, has fewer than 25 users and, therefore, authenticates from the domain controllers in the Troy site. Figure 3.3 illustrates the high-level Active Directory site architecture. Table 3.1 lists the Active Directory sites for the Corp domain.

Active Directory Sites for corp.giac.com				
Site Name	**Site Location**	**Link Speed**	**Users**	**DCs**
Troy	GIAG corporate building	100 Mbps	915	3
Cambridge	GIAC Cambridge branch office	T1	75	1
Ithaca	GIAC Ithaca branch office	512 Kbps	10	0

Table 3.1 – Active Directory sites in corp.giac.com domain

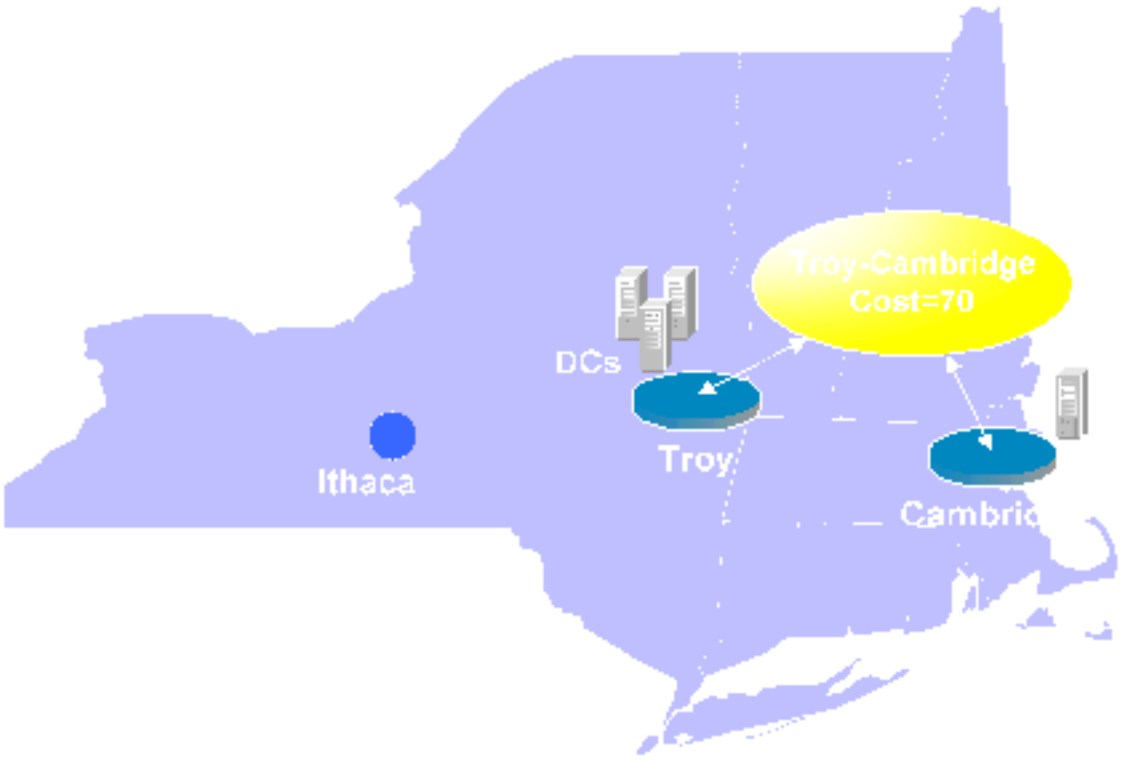

Figure 3.3 – Active Directory site topology for corp.giac.com domain

Domain Controllers

Figure 3.4 illustrates the placement of domain controllers within the “corp.giac.com” domain, as well as the roles placed on each domain controller. Following the diagram is a listing of the domain controllers with more details about the functions each performs.

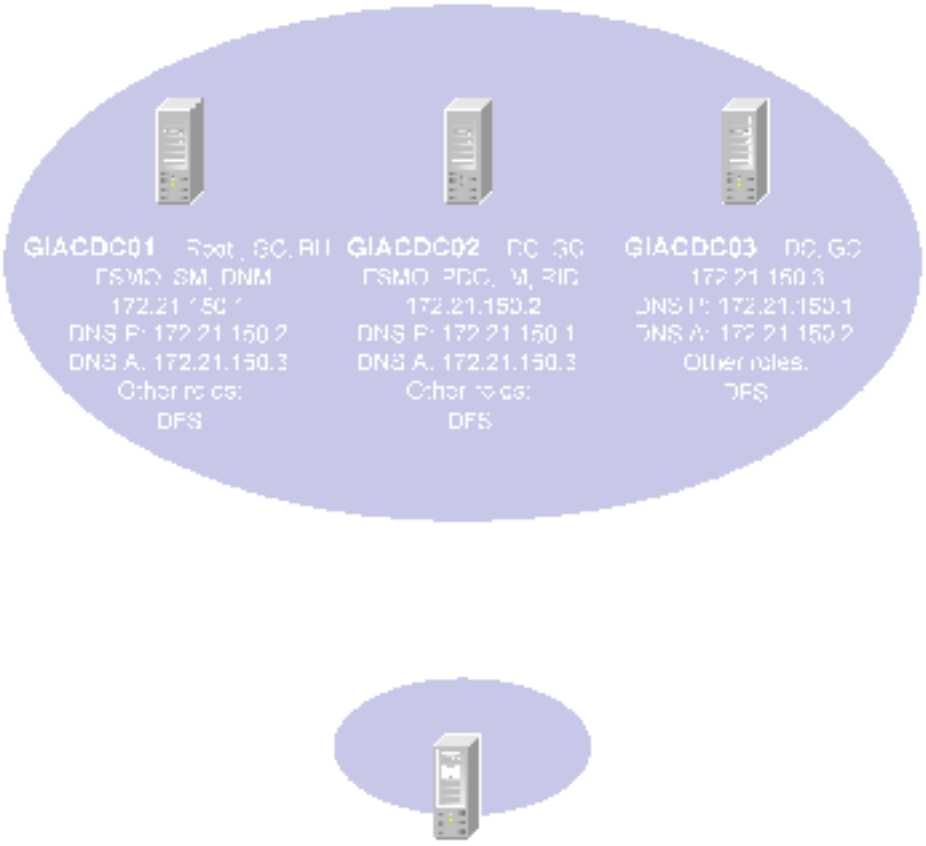

Figure 3.4 – Domain controllers for corp.giac.com domain

The following list describes each domain controller in more detail.

- **GIACDC01** – This server is the root server (the first server to be installed), and as such will initially hold all five Operations Master roles. Additionally, as the root server, it is also the global catalog server. Microsoft recommends leaving the global catalog role on this server.

Microsoft also recommends that one server also hold most of the Operations Master roles, except for the Infrastructure Master role, which should not be on a global catalog server. Therefore, this server holds the two enterprise wide Operation Master roles, Schema Master and Domain Naming Master. In the event this server must be taken offline for maintenance, the Operations Master roles will be temporarily transferred to server GIACDC02.

Additionally, this server is the bridgehead server for the Cambridge branch site. As such, it is the server in the hub site that receives all inter-site replication traffic from the branch site.

This server also provides DFS services and backup DNS services for the domain.

- **GIACDC02** – This server is a root domain controller and a Global Catalog server. Additionally, it holds the three domain-wide Operations Master roles, PCD Emulator, Infrastructure Master, and RID Master. In the event this server must be taken offline for maintenance, the Operations Master roles will be temporarily transferred to GIACDC03.

  This server also provides DFS services and backup DNS services for the domain.

- **GIACDC03** – This server is also a root domain controller and a Global Catalog Server. Additionally, it is the preferred DNS server for the domain, and it provides DFS services.

- **CAMDC01** – This server is the domain controller for the Cambridge branch site. Because Exchange 2000 services are provided to this site, CAMDC01 is also a Global Catalog server.

  The server also provides DNS services to the branch site. The domain controller points to itself as the primary DNS server, and to the bridgehead server in the hub site for the alternate DNS server.

Security Considerations for Domain Controllers

Because Active Directory employs multimaster replication architecture, every domain controller in a particular domain contains a replica of the directory; therefore, it is crucial to ensure both physical and logical security of all domain controllers. Several measures have been implemented to help ensure logical access to these computers. First, the servers are hardened by applying customized security templates and strengthening access permissions on objects. Additionally, unnecessary services have been removed. Also, the domain controller event logs are audited on a regular basis for signs that might be indicative of unauthorized access or tampering.

Physical security is also crucial. While physical security of the server farm is easier to address than that of the remote site, it is still an issue. The server farm security policy and procedures addresses the various issues related to physical security needed to protect the domain controllers (and other equipment in this facility). For example, redundant power sources and cooling systems are required, regular backups are performed and periodically tested to ensure restores can be done, and only select individuals have physical access to the domain controllers and other critical systems.

The domain controller at the Cambridge site physically resides in a locked telecommunications closet at the site. Only the site building manager and the local IT management has access to the closet. Additionally, the remote domain controller is plugged into uninterruptible power supply (UPS) with surge-protection.

Besides controlling physical and logical access to the domain controllers, a disaster recovery plan has been developed to ensure critical systems and data can be restored in the event of a catastrophic system failure. As part of this plan, a copy of all backups for critical systems, including domain controllers, is kept at a secure, off-site location.

Lab Active Directory Architecture

The purpose of this domain is to provide a separate domain and forest for testing purposes. Only IT staff will have access to this domain. While it is subject to many changes through experimentation, there are rules for how the lab environment may be used, including required documentation of all changes. Occasionally, the lab environment will also be rebuilt from scratch to provide a clean platform for new projects. Like the corporate Active Directory, the AD namespace, “lab.giac.com”, is an extension of the company’s registered Internet domain name.

Logical Architecture

The logical architecture of the lab domain, “lab.giac.com”, essentially mirrors that of the corporate environment. The baseline OU structure is exactly the same as “corp.giac.com”, although it is subject to change in order to test software installations and configuration changes.

Physical Architecture

The lab domain, “lab.giac.com”, is implemented in two sites, a hub site and a branch site. Although the physical location of the sites is actually the same (the corporate office in Troy), two AD sites are implemented to provide a scaled-down version of the corporate Active Directory environment for testing purposes. The hub site is named ‘LabHub’, the branch site ‘LabBranch’. Both are physically placed in the GIAC server farm.

Domain Controllers

The lab Active Directory also has three domain controllers, just as the production environment has, but the lab machines have much less horsepower. Additionally, the roles of each domain controller mirror those of the corporate Active Directory. The lab environment is on its own subnet (171.21.160.*).

Although the lab environment is strictly for testing, security policies and procedures still apply, especially since an explicit two-way trust is established between the corporate and the lab domains.

Part 4
Security Design

While some of the security issues pertaining to the infrastructure design were examined in the previous parts of the paper, this part gets into some of the details of how security is managed within GIAC's Windows 2000 infrastructure.

Before getting into the details, it is important to note that all procedures and standards that GIAC has implemented conform to the company's information security policies.

Administrative Model

It is GIAC Enterprises' policy that its IT department maintains central control of the entire network and computing infrastructure. The ability to centrally administer all servers and client computers on the network ensures that the computing environment remains consistent, efficient, and secure. Some specific administrative rights are delegated to other groups, but only select IT personnel have full administrative rights at the domain level, and only a few senior system administrators have administrative rights at the forest level. Figure 4.1 illustrates the overall administrative hierarchy for the GIAC Enterprises Active Directory.

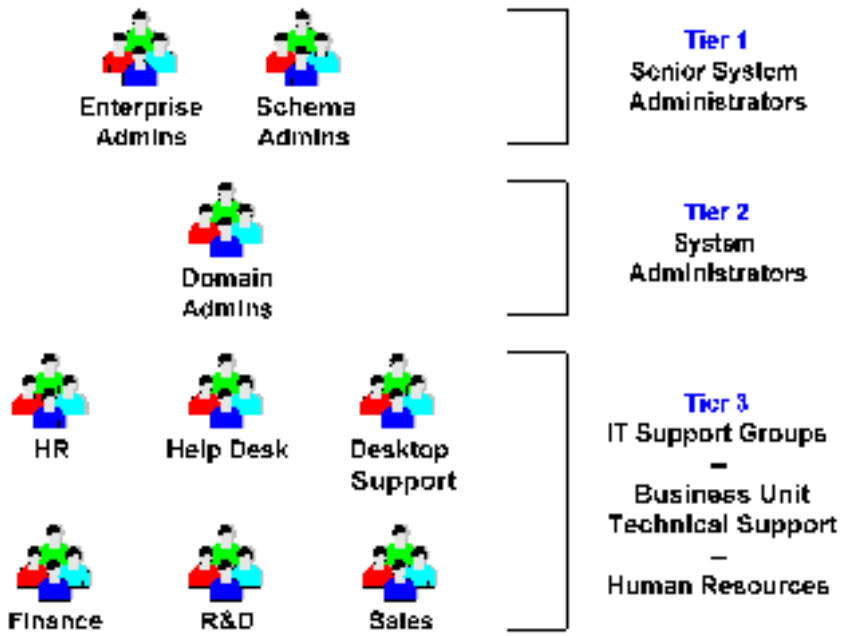

Figure 4.1 – Administrative hierarchy for "corp.giac.com" domain

All users in the administrative hierarchy have two separate user accounts, one for normal use and one for 'special access'. Normal user accounts are used for normal day-to-day activities, such as e-mail and working with MS Office documents. Only special access accounts have rights to perform administrative tasks, and the procedure for using special access accounts is to do so via 'Run As' whenever possible. Administrators should almost always log on locally to client computers using their normal user accounts; however, only special access accounts have the right to log on locally to servers.

In the hierarchy illustrated in figure 4.1, the Tier 1 administrators – the Enterprise Admins and Schema Admins – are the company's senior system administrators from the IT department. And while these few employees have administrative rights at the forest level, before exercising these rights they are still obligated to follow procedures in accordance with the company's forest change policy.

At the second tier of the administrative hierarchy are the system administrators from the IT department – a significantly larger group than the senior system administrators. The system administrators, as well as the senior system administrators, are members of the Domain Admins group. This group handles all day-to-day administrative and troubleshooting tasks at the domain and OU levels, such as Group Policy management, creating and modifying membership of security groups, setting file permissions, and adding new servers to the Active Directory.

The third tier of the administrative hierarchy is comprised of the following groups that have specific administrative rights.

- Human Resources (HR) – Responsible for managing all normal user accounts (not special access accounts). The rationale for HR performing this function that is typically performed by IT ad many organizations is simply that the user account database should precisely match the active personnel database. Therefore, HR creates user accounts, maintains the properties for these accounts as necessary, and disables and deletes accounts when employees leave the company.

- User Help Desk – This team has the right to reset passwords for user accounts, thereby eliminating the need to escalate such requests to higher-level technicians. To reduce the risk of unauthorized parties obtaining temporary passwords, new passwords will not be given out verbally via a telephone conversation. Instead, the Help Desk will forward the new password directly to the user's voice mail, where the user will have to use his or her private PIN (Personal Identification Number) to access the voice mailbox and obtain the new password.

- Desktop Support – The Desktop Support team has rights to join client computers to the Active Directory and to manage those computers. A Desktop Support global security group contains the special access accounts for each member of the Desktop Support team, and the global group is a member of the local Administrators group on each client computer.

- Business Units – A few technical support people in the Finance, R&D and Sales departments have special access accounts with the rights to modify membership of groups and to manage printers in their Organizational Units (OUs).

Security Group Strategy

Although security groups are enhanced in Windows 2000, GIAC's simple Active Directory architecture doesn't require many of these new enhancements. A rundown of the types of groups available and how GIAC Enterprises uses each type is as follows.

- **Universal Groups** – Except to utilize the built-in universal groups, "Enterprise Admins" and "Domain Admins", this type of group is not a part of GIAC Enterprises' group strategy. Universal groups become beneficial in multiple-domain environments, because universal groups defined within a particular domain can be used in any other domain in the forest. However, because GIAC's environment is a single domain, there is no need to utilize universal groups.

- **Global Groups** – Global groups are used to organize user accounts into logical teams of the same classification. The global groups are then used to populate local groups, which are in turn used to grant access to resources. Membership of global groups consists of user accounts from the same domain. Global groups can also be nested; for example, an "Admin Services" global group can be comprised of two other global groups called "Finance" and "HR".

- **Domain Local Groups** – This type of group can be used to grant access to resources in a domain, although GIAC typically uses local groups for this purpose (see below).

- **Local Groups** – Local groups are also used to grant access to resources, but the scope of local groups is on a particular machine. As much as possible, global groups are used to assign membership, but user accounts from the domain or the local machine can also be used to assign membership.

Figure 4.2 illustrates the strategy for how security groups are utilized for granting access to resources in the GIAC Enterprises Windows 2000 infrastructure. Essentially, user accounts are placed as members in global groups. Global groups are then used to populate local groups, which are then used to grant access to resources. Individual user accounts are not directly granted access to resources.

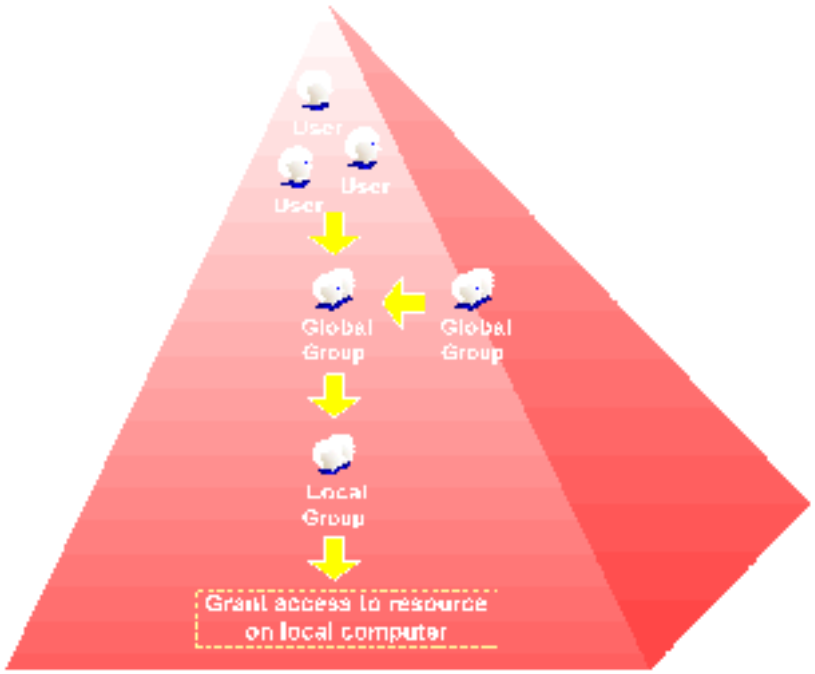

Figure 4.2 – Security group strategy for "corp.giac.com"

Security Templates

Currently, security templates are utilized for all GIAC workstations and IIS servers. The out-of-the-box templates for workstations (secure workstation) and web servers (high security web server) were used as the baseline templates and then customized and tested by GIAC system administrators before implementing them in the production environment.

The high security web server template is manually applied to new web servers using the Security Templates snap-in for Microsoft Management Console (MMC). The web server template is also manually reapplied to servers as necessary. Before applying the template, the Security Configuration and Analysis snap-in for MMC is used to first graphically compare the template settings to the current web server settings, and then to actually apply the template settings. Alternatively, system administrators can use the "secedit" command line tool to obtain the same results.

The workstation security template is applied to every workstation in the company using Group Policy. More information about how the template is pushed out to all machines is provided in the section below on Group Policy Design.

Security templates combined with the MMC and command line tools not only provide a convenient method to analyze and configure the security settings on a system, but the

template itself is actually a working copy of the security policy for a particular machine or group of machines.

Group Policy Overview

Group Policy is an extremely powerful and effective way to manage a Windows 2000 infrastructure, allowing system administrators to centrally configure sets of rules that are automatically applied to targeted objects in Active Directory – that is, specific groups of computers and user accounts. The section on Group Policy Design for GIAC enterprises delves into some of the specific Group Policy settings that are available. For now, the following list represents the basic types of functions that can be handled using Group Policy.

- Registry-based policy settings
- Security policies
- Software installation and maintenance settings
- Script execution (startup, shutdown, logon, and logoff)
- Folder redirections (store users' folders on network shares)

Every Windows 2000 computer has a local Group Policy Object (GPO). Additionally, Group policies can be applied to Active Directory sites, domains and organizational units (OUs). As Windows 2000 computers start up and as users log into the Active Directory domain, multiple policies can be applied to those computer and user objects.

Group Policy Inheritance Model

Active Directory containers inherit Group Policy from their parent containers. Note that the processing of GPO's for AD sites has the greatest scope – that is, it affects the most objects – and the scope decreases as the domain-based and OU-based GPO's are processed. As the processing progresses, the default behavior is that the settings in each subsequent GPO override any settings of the same type that were previously applied. However, the default inheritance behavior can be modified in individual GPO's by setting the "no override" option to prevent GPOs in child containers from overriding the GPO's settings. Similarly, the "block inheritance" option can be set to prevent inheritance of all policies from parent containers. The highest 'no override' takes precedence over lower 'no overrides' (e.g. domain-level takes precedence over OU-level). And 'no override' takes precedence over 'block inheritance'. Figure 4.3 illustrates the Group Policy inheritance model.

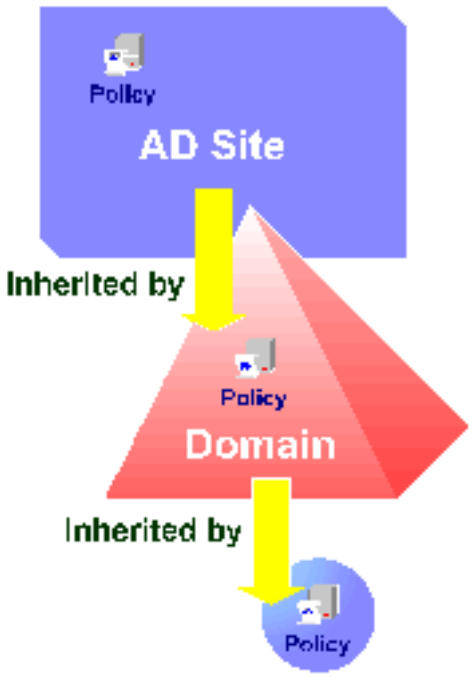

Figure 4.3 – Group Policy inheritance model

The processing order for Group Policies is 1) local GPO, 2) AD site GPO's, 3) AD domain GPO's, and then 4) AD organizational unit GPO's. As the processing progresses, the settings in each subsequent GPO override any settings of the same type that were previously applied. The final outcome from all GPOs being applied to an object is referred to as the Resultant Set of Policy (RSoP). When developing the Group Policy strategy, it is important to document the settings being used and to thoroughly test all GPOs together in a lab environment before implementing new or changed GPOs in production.

Group Policy Design

GIAC's implementation of Group Policy consists of the default domain policy, the only domain-level policy, and the default domain controller policy. Additionally, three more machine class security policies are set for member servers, workstations, and laptop computers and applied to the appropriate OUs. The workstation policy could be applied at the domain level, however, setting it at the OU level gives system administrators to make minor modifications to each OU as necessary. Figure 4.4 illustrates the high level Group Policy design for GIAC Enterprises.

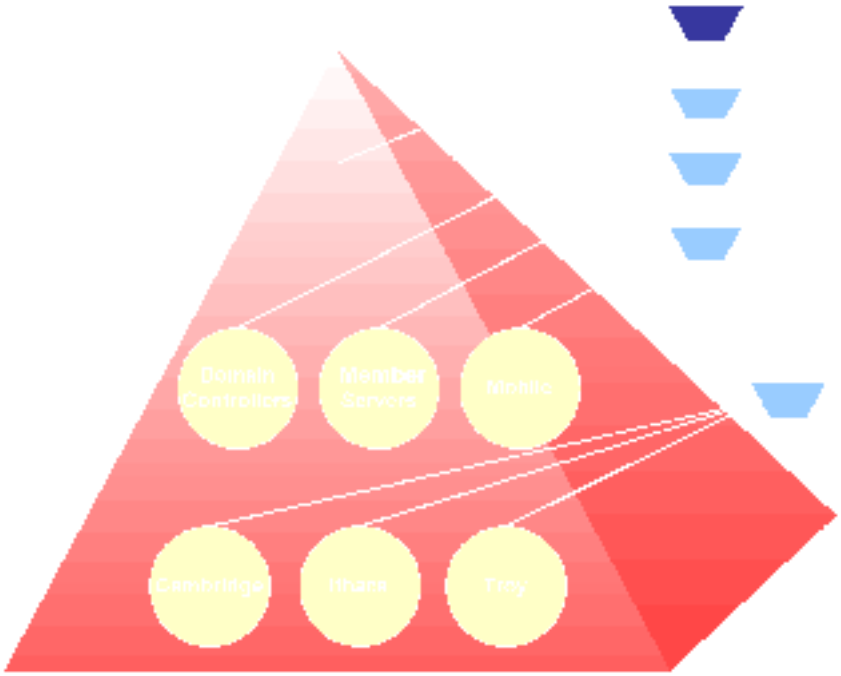

Figure 4.4 – Group Policy design for GIAC Enterprises

Default Domain Policy Settings

The default domain policy includes settings that affect every computer in the domain. It is important that account policies – password, account lockout, and Kerberos policies – be applied via the Default Domain Policy GPO. These settings must be applied at the domain level in order to apply them to domain controllers. In other words, if password, account lockout, and Kerberos policies are not set at the domain level, domain controllers will ignore them.

Password Policy

Policy	Default Setting	GIAC Setting
Enforce password history	0 passwords remembered	15 passwords remembered
Maximum password age	42 days	60 days
Minimum password age	0 days	1 day
Minimum password length	0 characters	8 characters
Password must meet complexity requirements	Disabled	Enabled

Store password using reversible encryption…	Disabled	Disabled

The password policy is intended to be fairly strong, with a length of eight characters and complexity requirements enforced. Enabling the complexity requirements means that the following rules apply.

- Three of the following four requirements must be met:
  - Contains uppercase letters
  - Contains lowercase letters
  - Contains numbers
  - Contains special characters

- Valid characters for passwords are shown in the following table. (Note: spaces in passwords should be avoided).

Description	Examples
Letters (uppercase and lowercase)	A, B, C,...; a, b, c,...
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols (all characters not defined as letters or numerals)	` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /

Setting the minimum password age to one day closes the loophole whereby a user could potentially change his password in rapid succession (15 times) in order to reuse a favorite password

Account Lockout Policy

Policy	Default Setting	GIAC Setting
Account lockout duration	Not defined	30 minutes
Account lockout threshold	0 invalid logon attempts	4 attempts
Reset account lockout counter after	Not defined	30 minutes

The account lockout policy helps prevent 'password guess attacks' by locking user accounts if more than four incorrect passwords are attempted. Legitimate users who accidentally get locked out must either wait 30 minutes or call the Help Desk to get their account unlocked.

Kerberos Policy

All Kerberos policy settings will be left at the defaults.

Security Options

Policy	Default Setting	GIAC Setting
Message text for users attempting to log on		See below
Message title for users attempting to log on		GIAC Enterprises

The only security options setting that is applied at the domain level is one that displays a message to all users attempting to logon to any computer in the domain. The message should state that only authorized persons are allowed to use the system and that by accessing and using the system, persons consent to monitoring activity for law enforcement purposes. The reason for implementing this message is twofold. First, for legal reasons, the message serves as an electronic 'no trespassing' sign and can be useful in the event that GIAC Enterprises must take legal action against people who enter or use a system unlawfully. Second, it ensures that if GIAC decides to monitor activity on a system, the Communications Privacy Act of 1986 is not violated.

Default Domain Controller Settings

These group policy settings will be applied to Default Domain Controllers GPO, which is linked to the Domain Controllers OU. Note that the password, account lockout, and Kerberos policies are not included here; this is because these account settings set at the OU level are ignored by domain controllers. Account settings are applied at the domain level in order to apply them to the domain controllers.

Audit Policy

Policy	Default Setting	GIAC Setting
Audit account logon events	No auditing	Success, Failure
Audit account management	No auditing	Success, Failure
Audit logon events	No auditing	Success, Failure
Audit policy change	No auditing	Success, Failure

Audit system events	No auditing	Success, Failure

The audit policy settings shown represent the minimum audit log settings for all computers in the company and are intended to help investigate attacks and breaches. Auditing account logon events can help show signs of persons attempting to break into a system – for example, if there are repeated failures for a particular account. Auditing account management and policy changes can help leave a trail of unauthorized changes.

User Rights Assignment

Policy	Default Setting	GIAC Setting
Access this computer from the network	Everyone, Administrators, Authenticated Users	Administrators, Authenticated Users
Add workstations to domain	Authenticated Users	[empty]

This listing represents some of the more important changes GIAC has made to the User Rights Assignments for domain controllers. First, remove the Everyone group from the "Access this computer from the network" right.

Another important change is to remove all groups from the "Add workstations to domain" right. In order to accomplish what this right intends, the best practice is to set permissions on the appropriate Active Directory containers (that contain workstation objects) to allow the desired groups to create computer objects (see Microsoft KB article Q251335 for details). So, in GIAC Enterprises' Active Directory, Domain Admins and Desktop Support employees are granted permissions to create computer objects in all the business unit containers (all of the tier 2 OUs). Additionally, R&D technical support staff are granted permissions to create computer objects only in the R&D container.

Most of the other default settings are alright for the User Right Settings.

Security Options

Policy	Default Setting	GIAC Setting
Additional restrictions for anonymous connections	Not defined	No access without explicit anonymous permissions
Clear virtual memory pagefile when system shuts down	Not defined	Enabled
Digitally sign client	Not defined	Enabled

communication (always)		
Do not display last user name in logon screen	Not defined	Enabled
LAN Manager Authentication Level	Not defined	Send NTLMv2 response only\refuse LM & NTLM
Prompt user to change password before expiration	Not defined	14 days
Restrict CD-ROM access to locally logged-on user only	Not defined	Enabled
Restrict floppy access to locally logged-on user only	Not defined	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	No defined	Enabled
Secure channel: Digitally encrypt secure channel data (when possible)	No defined	Enabled
Secure channel: Digitally sign secure channel data (when possible)	No defined	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Not defined	Enabled
Unsigned driver installation behavior	Not defined	Do not allow installation
Unsigned non-driver installation behavior	Not defined	Do not allow installation

These security options are important steps in generally hardening the domain controllers. The settings related to authentication and signing and encrypting the Secure Channel are set to provide medium and high security. The “additional restrictions for anonymous connections” setting prevents anonymous users from enumerating certain system objects, such as user accounts. And it is GIAC’s policy to not allow the installation of unsigned drivers or software on any server.

Event Log

Policy	Default Setting	GIAC Setting
Maximum application log size	Not defined	25600 KB
Maximum security log size	Not defined	25600 KB

Maximum system log size	Not defined	25600 KB
Restrict guest access to application log	Not defined	Enabled
Restrict guest access to security log	Not defined	Enabled
Restrict guest access to system log	Not defined	Enabled
Retain application log	Not defined	60 days
Retain security log	Not defined	60 days
Retain system log	Not defined	60 days
Retention method for application log	Not defined	Overwrite as needed
Retention method for security log	Not defined	Overwrite as needed
Retention method for system log	Not defined	Overwrite as needed
Shut down the computer when the security audit log is full	Not defined	Disabled

The intent of the event log settings is essentially to help keep from losing important – even potentially critical – log data. Although the "overwrite as needed" retention method is set for each log, the size of each is set to 25 MB; these settings provide a large enough log to ensure data is maintained for a suitable amount of time. Guest access to all event logs is not allowed.

Policy Settings for Member Servers, Workstations and Laptops

Because the security requirements varies somewhat between member servers, workstations and laptops, separate GPOs exist for member these types of computers. Some of the settings vary somewhat from the default domain controller security policy settings; however, the default domain controller policy provides an idea of what's available.

For each of these three machine classes, GIAC has created a security template. When it is necessary to make changes to group policy on servers, workstations and laptops, GIAC system engineers make the change in the security template. The template is then imported into the appropriate OU container(s) in the lab.giac.com Active Directory to test the changes. Once the test results are correct, the template is imported into the production Active Directory, and a copy of the template is safely stored.

References

1. Cone, Eric K., Jon Boggs and Sergio Perez. Planning for Windows 2000. Indianapolis: New Riders Publishing, 1999.

2. Norberg, Stefan. Securing Windows NT/2000 Servers for the Internet. Sebastopol: O'Reilly & Associates, Inc, 2001.

3. "Active Directory Branch Office Planning Guide." URL: http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/branchoffice/default.asp (November 14, 2001) *A downloadable version is available

4. "Windows 2000 Group Policy." URL: http://www.microsoft.com/windows2000/docs/grouppolwp.doc (November 14, 2001)

5. Fossen, Jason. "Securing Windows 2000." GIAC training course from New England SANS, 2001.

6. Cox, Philip. "Hardening Windows 2000." Version 1.2, May 25, 2001. URL: http://www.systemexperts.com/win2k/hardenW2K12.pdf (November 14, 2001)

7. Haney, Julie M. "Guide to Securing Microsoft Windows 2000 Group Policy." Version 1.1, September 13, 2001. URL: http://nsa1.www.conxion.com/win2k/guides/w2k-2.pdf (November 14, 2001)

8. Rice, David C. "Group Policy Reference." Version 1.0.8, March 2, 2001. URL: http://nsa1.www.conxion.com/win2k/guides/w2k-4.pdf (November 14, 2001)

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

10. Anthes, Mary A. "A Secure Windows 2000 Infrastructure Design." September 26, 2001. URL: http://www.sans.org/y2k/practical/Mary_Anthes_GCNT.zip (November 14, 2001)

11. Microsoft Product Support Services. "Q251335: Domain Users Cannot Join Workstation or Server to a Domain." URL: http://search.support.microsoft.com/kb (November 15, 2001)
    * URL shown is the MS knowledge base search page; enter the article number – the 'Q' number – to quickly find this particular article.

Last Updated: July 22nd, 2017

Upcoming Training

SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**