GIAC Enterprises: Windows 2000 and Active Directory Design

Securing Windows Practical Assignment
Version 3.0 – Option 1

Gregory Rick
May 24, 2002

Table of Contents

Chapter 1 – Introduction

1.1 – Project Overview

GIAC Enterprises, an e-business that deals in the online sale of fortune cookie sayings, has been attempt implementing Windows 2000 (Win2K) and Active Directory (AD) corporate-wide. GIAC Enterprises is implementing Windows 2000 to foremost heighten security, but increasing administration efficiency and network performance is also especially important. This document is a formal design to implement a secure, efficient Windows 2000 network for GIAC Enterprises, containing technical details of the target Windows 2000 and Active Directory environment.

1.2 – Assumptions

GIAC Enterprises is currently a small enterprise with only two locations, the Home and Remote office. Fortunately, the current physical network infrastructure is stable, secure, and has plenty of room for expansion. The switches, routers, and firewalls are on Cisco hardware updated with the latest IOS and security precautions. Both Local Area Networks (LANs) are on 100 megabit Ethernet backbones with secure access to all cabling, switches, routers, and servers. Both locations also have a dedicated T1 circuit to the Internet, provided by two different ISPs.

A dedicated T1 circuit and a secure site-to-site Virtual Private Network (VPN) connection connect the Home and Remote offices. The secure VPN connection provides both fault tolerance and load balancing. GIAC implemented the secure tunnel with a Cisco VPN Concentrator at the Home office and a Cisco VPN router at the Remote office, utilizing hardware level 168-bit triple DES encryption (IPsec). Although the VPN Concentrator can be configured to connect individual users, GIAC is not allowing other VPN sessions at this time.

By utilizing internal and external Cisco Pix firewalls with only the needed ports opened, both locations have a secure DMZ and internal network.

There are currently no wireless access points, and current policy does not allow installation. GIAC's auditing policy includes weekly scanning for unknown wireless access points at both locations, to identify any unauthorized installations.

GIAC has fully implemented a robust intrusion protection system. The Internet Security System "RealSecure Network Protection" solution was deployed with four RealSecure 6.5 for Nokia Network Sensors, one located on each segment. Each server has a RealSecure 6.5 Server Sensor installed and Web Server Protection implemented on all the external web servers. The Network Sensors report to a Workgroup Manager running on a Compaq Prolient DL 380 running Windows 2000 Service Pack 2. (see diagram in Figure 1)

The existing NT 4.0 Domain controllers were not determined economically feasible to upgrade and are going to be left in place until all clients are migrated. Three new servers will be purchased for the new Win2K domain controllers. Exchange 2000 is running on a Win2K server and will not need to be upgraded. All remaining servers are running Win2K, including the internal IIS 5.0/SQL 2000 server, the two external IIS 5.0 servers, and an external SQL 2000 server.

The internal DNS is on two Sun Solaris Servers, a primary at the Home Office and a secondary at the Remote Office. The external DNS is also on two Sun Solaris servers, one on each DMZ segment. The DNS server on the DMZ segment at the Home Office is also the external mail relay running Sendmail. Additionally, the mail relay server is running Trend Micro's Viruswall product, which scans all incoming and outgoing email. The Viruswall product is also used to block all attachments that could potentially harbor malicious code. The existing internal DNS servers will be replaced by Microsoft DNS and the external DNS will remain unchanged.

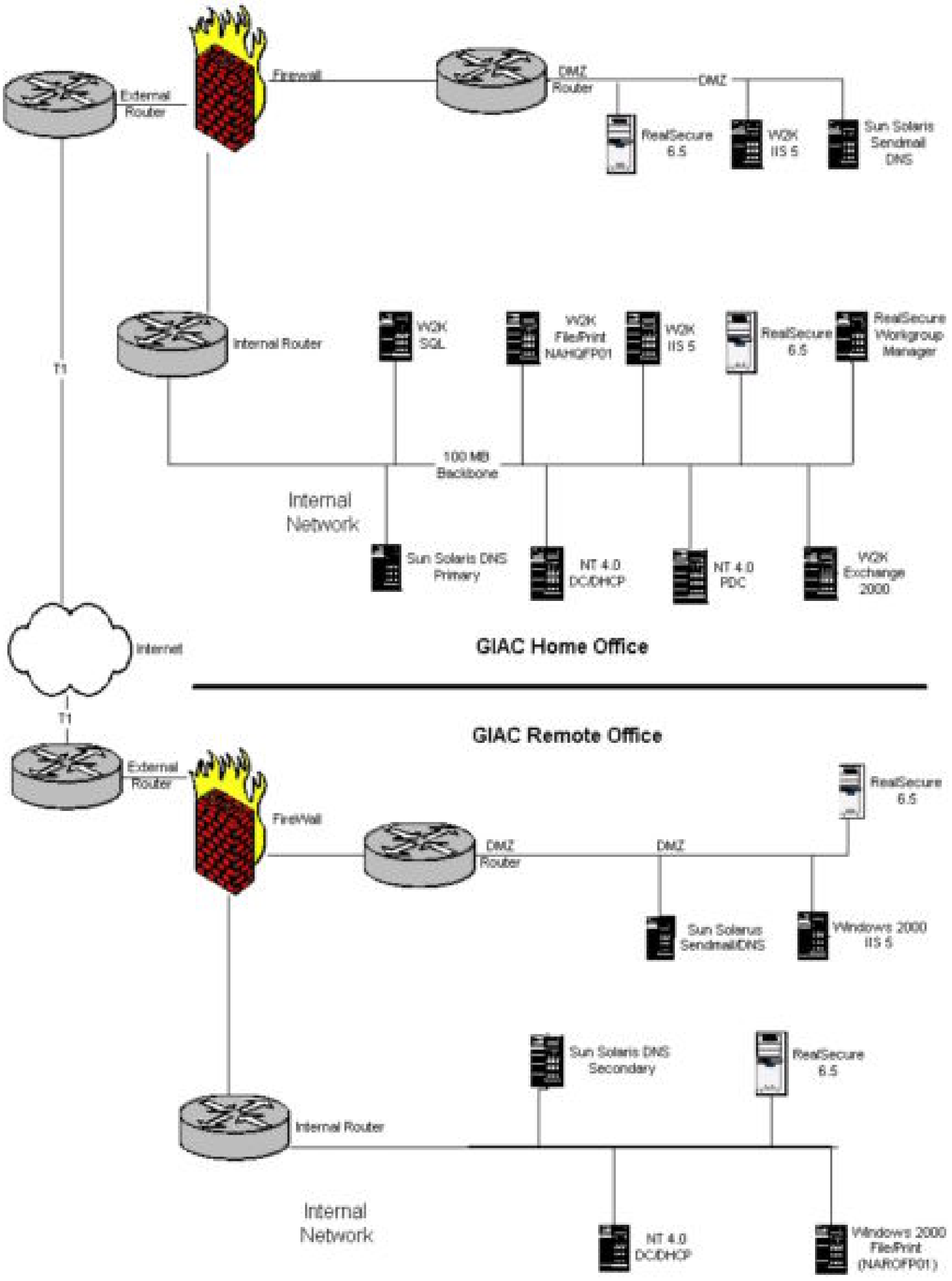


Figure 1 – Current Network Diagram

Chapter 2 – Active Directory Physical Design

The Windows 2000 Active Directory physical design includes specifications for the physical implementation of Windows 2000 and Active Directory on GIAC server platforms. The emphasis of this chapter is on elements necessary to implement an Active Directory infrastructure, including supporting Windows 2000 systems and services.

2.1 – Windows 2000 Server Software

For continuity and security, GIAC will standardize the product type, version and operating mode.

2.1.1 Product Specification

GIAC will implement the Windows 2000 Advanced Server product on all future server platforms. The current shipping version of Windows 2000 Advanced Server with Service Pack (SP) 2 will be used, although there are also many recommended "hotfixes" that must be applied in addition to SP 2 until Service Pack 3 is released. All fixed disks will be formatted with NTFS, for added file protection. Services like Simple Network Management Protocol (SNMP), Print Spooler, World Wide Web Publishing, FTP Publishing, Server, and Telnet should be disabled unless specifically needed.

All servers will be standardized on running McAfee's NetShield 4.5 anti-virus product with the latest service packs and hotfixes. This offers a layered anti-virus approach with Trend Micro scanning on the Firewall. The McAfee configuration will automatically update virus pattern (DAT) files using File Transfer Protocol (FTP). Scan engine, heuristics, file extensions to scan, update schedule, on-demand scan schedule and all other general settings will be determined by the most current recommendations from NAI.

Internet Explorer will be left the original version installed with the operating system on all servers, but the latest hotfixes and service packs will be applied.

The Administrator account is created by default when installing Windows 2000 and should be renamed for security purposes. GIAC will standardize on "Lemon" for the Administrator account name. The default account description will be deleted as well.
The Guest account is created by default when installing Windows 2000, but is disabled. GIAC will rename the Guest account also and standardize on "Lime" for the Guest account name. The default account description will be deleted as well.

2.1.2 Mode

An Active Directory domain can operate in either "Mixed" mode or Native mode. Mixed operating mode allows Windows NT 4.0 and Windows 2000 domain controllers to coexist on the network. Unfortunately the flexibility of Mixed mode does not allow the use of many Windows 2000 Active Directory features that GIAC Enterprises desires to utilize. Because the existing Windows NT 4.0 domain will be left as is and all the workstations are running Windows 2000, Active Directory will be implemented in Windows 2000 Native Mode. Some of Mixed mode limitations include:

- No automatic password filtering on domain controllers
- Nested groups are not supported.
- Mixed mode does not allow remote access by means of Windows 2000's access-by-policy administrative model.
- Universal Groups are not supported
- Same Windows NT 4.0 size limitations of computers, groups, and users.

Existing NT 4.0 objects (accounts, groups, servers, workstations) will be incrementally migrated to the new, parallel Windows 2000 environment. This will allow the new production Active Directory domain to be fully built, hardened, documented, and extensively tested before any production objects (accounts, groups, servers, or workstations) are migrated.

2.2 – Forest and Domain Design

Windows 2000 domains can be structured in a hierarchy of domains. The hierarchy of domains and sub domains within the same DNS namespace is referred to as a domain tree. An Active Directory forest is a collection of one or more Active Directory domain trees. Forests share a common Active Directory schema, configuration, and Global Catalog. There are many alternatives in Active Directory forest design, but GIAC will be using one of the simplest cases, where there is a single Active Directory forest that contains only one Active Directory domain. Since

Organizational Units (OUs) are the primary focus of security, administration, and delegation, multiple domains are no longer needed.

2.2.1 Production Domain

GIAC will use one Active Directory domain, "prophesy.com". An explicit external NTLM (NT 4.0 authentication protocol) 2-way trust will be created with "prophesy.com" and "giac01", the legacy NT 4.0 domain. There will be no replication between these domains and the trust will allow temporary transitive access both domains during the migration of the NT 4.0 objects, which will be limited to two weeks.

Although there will be Windows 2000 servers within the DMZ, there is no present need to create an Active Directory domain implemented outside the Intranet for three servers. Local security policies will be easier to manage for three servers than Group Policy, but an Active Directory implementation may be beneficial when GIAC grows and has more servers on the DMZ. Security policies for the DMZ will be discussed later.

2.3 – DNS Namespace

The Domain Name System (DNS) namespace defines how internal and external users visualize the structured relationship of GIAC computer resources. Since Dynamic DNS and Service (SRV) records replace WINS and Netbios names in Win2K, DNS is very important and requires careful planning. SRV records enables locating network services through DNS. Windows 2000 Active Directory domains have DNS names and exist in a structured topology. For security purposes, different internal and external DNS namespaces will be used, and each namespace will be implemented with separate and distinct DNS servers.

2.3.1 Internal

The internal DNS namespace is what GIAC users will see within the GIAC Intranet.

- The internal namespace will be registered to prevent any other company from using it and thereby increasing the potential for routing problems.
- The internal namespace is company-neutral, so as not to require a name change in the event of a merger, acquisition, or divestiture.
- The internal namespace will be separate and distinct from the external (Internet-viewable) namespace.
- The internal namespace shouldn't resolve to any external names in order to prevent possible confusion.

2.3.2 External

The external DNS namespace is what Internet users will see when accessing GIAC resources remotely and not using some form of remote access or tunneling technology. The external resources accessible to Internet users are not on the GIAC intranet but rather are isolated on a separate LAN called the DMZ. The external DNS namespace is not impacted by implementing Windows 2000 and will continue to be isolated on two Sun Solaris servers.

2.4 – Domain Controllers

Windows 2000 domain controllers (DCs) provide authentication services to network clients seeking to access a Windows 2000 Active Directory domain.

2.4.1 Placement

GIAC's domain (prophesy.com) will have three domain controllers: two at the main location and one at the remote location. (See Figure 3 for diagram) Even though both locations have secure facilities, the domain controllers will also be in secure racks, locked with limited access.

2.4.2 Configuration

For continuity purposes, the domain controllers will be on identical hardware with the same configuration (see table 1 for configuration). This will alleviate hardware and driver vulnerabilities, facilitate updating drivers, assist in troubleshooting, and ease in future upgrades.

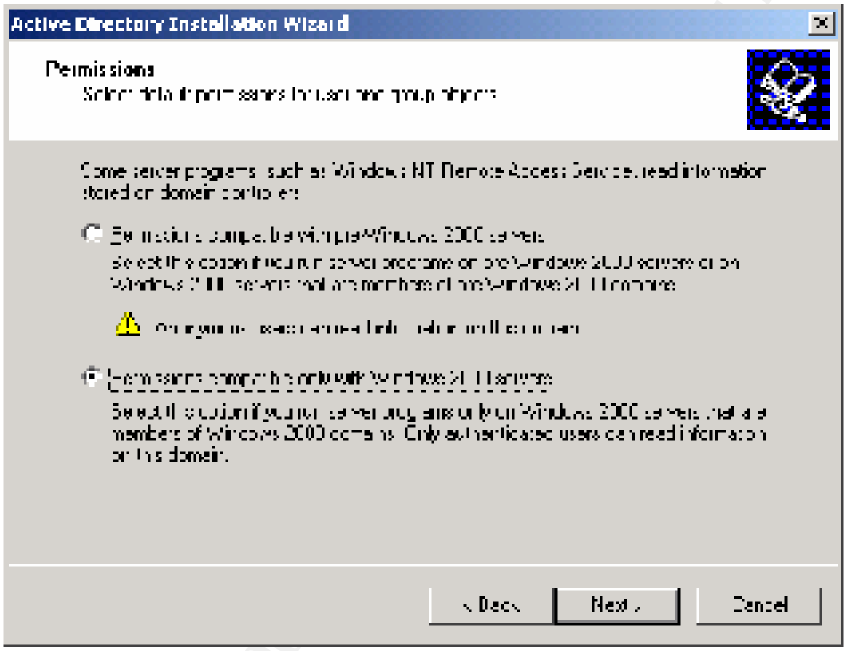
Server Hardware	Compaq Prolient DL 380
Ram	3 Gigabytes
Processor	2 Intel 1-Gigahertz Xeon 256k Cache
Hard Disks	4 - 18 Gig Ultra 3 10k SCSI Drives
Array Controller	Smart Array 5302
Array Configuration	2 – Raid 0 + 1 Mirror Sets
Network Interface	2 – 10/100 Ethernet Teamed NICs

Table 1 Server Hardware Configuration for Domain Controllers

The first domain controller configured will be NAHQDC01. Active Directory will be installed on NAHQDC01 by running DCPROMO.EXE from the command prompt. To ensure efficiency and tighten security, the following options will be selected during the installation:

- Select "Domain Controller for new domain" when prompted for Domain Controller Type.

- Select "Yes, install and configure DNS on this computer" when prompted for Configure DNS.
- "Permissions compatible only with 2000 servers" will be selected (see figure 2). The other option, "Permissions compatible with pre-Windows 2000 servers", allows anonymous users "read" access to information on the domain by nesting the "Everyone" group in the "Pre-Windows 2000 Compatible" access group.



Active Directory Installation Wizard

Permissions

Select default permissions for user and group objects.

Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.

○ Permissions compatible with pre-Windows 2000 servers

Select this option if you run server programs on pre-Windows 2000 servers or on Windows 2000 servers that are members of pre-Windows 2000 domains.

⚠ Anonymous users can read information on this domain.

● Permissions compatible only with Windows 2000 servers

Select this option if you run server programs only on Windows 2000 servers that are members of Windows 2000 domains. Only authenticated users can read information on this domain.

Figure 2 Permissions compatible setting

Also during Active Directory installation, a value for the Directory Services Restore Mode Administrator's password is granted. This password will be a robust password with more than 15 characters including special characters, numbers, and different case letters. Only a few key administrators will have access to this password. This password will be used to restore the Active Directory database from a backup and to protect access to "ntds.dit", the Active Directory database file stored on the server.

2.4.3 FSMO Roles

To prevent conflicting updates in Windows 2000, the Active Directory performs updates to certain objects in a single-master fashion, in which only one Domain Controller in the entire directory is allowed to process updates. Unlike NT 4.0, Windows 2000 extends the single-master model to include multiple roles and the ability to transfer roles to any domain controller. Currently in Windows 2000 there are five Flexible Single Master Operation (FSMO) roles:

- Schema Master: performs updates to the directory schema. Only one Schema Master is allowed per forest.
- Domain Naming Master: performs updates to the forest-wide domain name space. Only one Domain Naming Master is allowed per forest.
- RID Master: allocates pools of Relative Ids to each domain controller, which allow each new security principal object in a domain to be uniquely identified. Only one RID Master is allowed per domain.
- PDC Emulator: provides compatibility with NT 4.0 domain controllers; authoritatively synchronizes time; controls password changes, account lockout, and resource browse requests for down-level clients. Only one PDC Emulator is allowed per domain.
- Infrastructure Master: resolves cross-domain object references. Only one Infrastructure Master is allowed per domain.

The RID Master, Infrastructure Master, and PDC Emulator will be on the same domain controller (NAHQDC01). The Schema Master and Domain Naming master roles will be on the same domain controller that will also be the Global Catalog server (NAHQDC02). These two domain controllers will be at the main location. The third domain controller (NARODC01), located at the remote location, will act as a secondary server and be designated as an alternate site to host FSMO roles in case of catastrophic failure or disaster recovery. This third domain controller at the remote site will also be a Global Catalog server.

2.5 – Sites and Replication

Windows 2000 sites provide physical network topology information to Active Directory. Active Directory replication is organized around sites, but sites are not used for organizing the Active Directory structures such as domains and organizational units. The connectivity between the two offices is reliable and fast enough to have a single site, but to better manage replication and authentication traffic, we will divide the locations into two sites. Since the connections are fast and reliable, the default costs will be used for replication.

2.5.1 Replication

Due to the simple two-site design and sufficient network bandwidth, the default replication schedule setting “allow replication polling to happen throughout the seven-day schedule” will be used. The default replication interval setting will also be used “three hours when the schedule allows replication”. The replication transport setting “RPC-over-IP (for fast reliable links)” will always be used.

2.6 – IP Infrastructure

Windows 2000 provides an adequate level of services for supporting Internet Protocol (IP) services for GIAC. Windows 2000 will be used to provide DHCP, WINS, and DNS.

2.6.1 DHCP

Dynamic Host Configuration Protocol (DHCP) provides dynamic IP-address assignment for network clients. DHCP is an important network service for providing network address and configuration information to clients. DHCP will be configured on a file and print server at each location, NAHQFP01 and NAROFP01. Configuring DHCP on a domain controller is not recommended because the DHCP server updates its own records. A domain controller in the DNSUpdateProxy group leaves the domain controller's DNS records unprotected. (Fossen, Jason, 5.1 Windows 2000 Active Directory and Group Policy. Version 5.1.3, SANS Institute, November 13, 2001, page 105)

2.6.2 DNS

Domain Name System (DNS) provides Internet-standard name resolution in an IP-based environment. GIAC will implement a Windows 2000 Active Directory integration of Dynamic DNS on the Intranet only and leave the Solaris DNS intact on the DMZ. Once the migration is complete, the internal Solaris DNS servers will be retired. All three Domain Controllers will also be the DNS servers. Only internal addresses will be resolved with the internal DNS servers and will forward external queries to the Solaris DNS servers on the DMZ. Since DNS will eventually replace NetBios and WINS, inaccessible DNS servers or corrupted DNS records can severely disrupt network services. Dynamic updates will allow DNS records to be changed automatically when a client's IP address changes. Secure updates will be required to ensure the integrity of the DNS records. DNS will be additionally configured with the following settings:

- Require all zones to allow only secure dynamic updates.
- Disable all zone transfers.
- Enable the "Secure cache against pollution" option.
- Enable the "Netmask ordering" option.
- Enable logging for the Notify and Update activities under Logging, Desired activities to be logged.
- Set permissions on C:\winnt\System32\dns\Dns.log to Full Control for System and Administrators only, removing any other users or groups.

Requiring only secure updates will help prevent corruption and hacking by using Kerberos authentication to validate the updated record. This setting is under the “Allow Dynamic Updates?” in the DNS snap-in. By default, any client can change a record because non-secure updates are attempted first, no matter if the client can perform secure updates.

Disabling zone transfers will block malicious downloading of DNS records to determine servers IP addresses and what they host.

Enabling “Secure cache against pollution” will protect cache poisoning, which can overload the DNS server by handling a large number of bogus query responses.

Netmask ordering is mainly for network optimization.

Logging enabled for the Notify and Update DNS activities will log all notification messages received from other DNS servers and log all dynamic updates received from other computers. Setting permissions on this log will only allow Administrators and the local system to access the log.

2.6.3 Time Services

Time synchronization is critical for clients and servers, especially for clients communicating with the DHCP and DNS servers. Although Windows 2000 includes a native time synchronization service, a common time source is needed for synchronizing time on the Windows 2000 domain controllers. The domain controller NAHQDC01 will be synchronized with the US Naval Observatory (192.5.41.41) by using the Simple Network Time Protocol (SNTP) and the Net Time command. All the Windows 2000 clients and servers will synchronize their time from the PDC emulator.

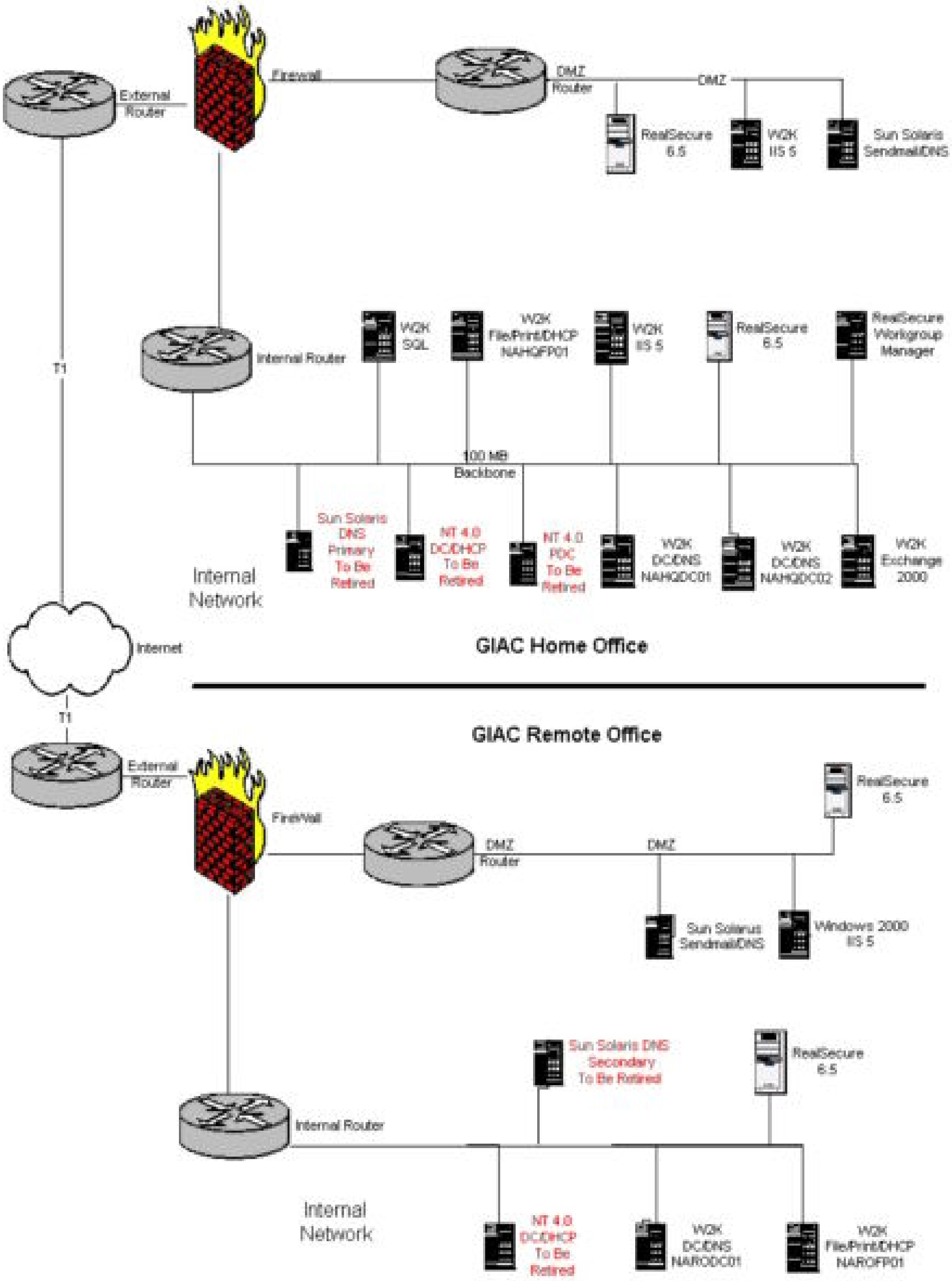


Figure 3 – New Active Directory Physical Design

Chapter 3 –
Active Directory Logical Design

The purpose of this section is to provide the logical design for a Windows 2000 Active Directory infrastructure at GIAC.

3.1 – Organizational Units

A Windows 2000 Active Directory Organizational Unit (OU) is a logical container used to hierarchically organize domain resources for the purposes of delegating administration, simplifying management of common resources, making searches more efficient, applying different group policies, as well as controlling what objects can be seen by various end users. OUs allow high-level administrators to delegate various User and Group administration tasks to localized administrators, such as adding users, changing passwords, or modifying group memberships.

OUs are generally created for the delegation of User and Group management tasks and the grouping of objects. OUs cannot be made members of security groups, nor can users be granted permissions to a resource because they reside in a particular OU. OUs provide a means of determining which Group Policy would be applied to sets of user and computer objects. Group Policy, through Group Policy Objects (GPOs), allows for the definition of desktop configurations associated with users and computers. GPOs are associated with sites, domains, and OUs. The Group Policy design for GIAC is described in a later section.

3.1.1 Design Strategy

Organizational Units will be used for delegating administration and enforcing policy. Since GIAC will be managed centrally, OUs are organized based on the type of object being managed. Lines of business will be introduced in lower layers. This will allow Group Policy Objects to be assigned centrally above delegated administration. For example, if you wanted to force a password policy centrally to all users not allowing lower level OU administrators to override the policy, a policy can be enforced at the top level users OU and No Override selected in the options.

GIAC will focus using Organizational Units to delegate administration, apply Group Policy, and hide objects. Delegation of administration is achieved through a combination of organizational units, per-attribute access control, and access control inheritance. Group Policy can be applied at the OU level, therefore any line of business requiring differing settings for their users of computers would need to create separate OUs to contain the respective objects. The most efficient way to hide an object or set of objects is to create an OU for those objects and limit the set of users who have the "List Contents" right for that OU.

Since users will not navigate the OU structure, the design wasn't created to appeal to end-users. Users can most efficiently query the global catalog to efficiently locate resources in the directory.

3.1.2 Structure

The following list presents the recommended tree structure for the domain, *prophesy.com*.

- **Home Office**- Computers and printers for the Home Office location will be placed in this OU. Since computer and printer administration and support is centralized by location, the local support staff for the Home Office will administrate this OU.
- **Remote Office**- Computers and printers for the Remote Office location will be placed in this OU. Again since computer and printer administration and support is centralized by location, the local support staff for the Remote Office will administrate this OU.
- **Users**- User accounts, sub-grouped by line-of-business (IT Administrators, Research and Development, Sales & Marketing, and Finance & Human Resources). A third-level OU can be created under the child OU's for even further refinement.
- **Enterprise Servers**- Computer accounts for enterprise-level servers will be placed in the appropriate second-level OU (e.g. database, web, file and print).
- **Domain Controllers**- Computer accounts for domain controllers will be placed in this OU.

Since user hardware is administrated by specific location, separate OU's were created for Home Office and Remote Office. GIAC will be able to delegate administrative powers of a location to the local hardware support staff without giving rights over the user accounts in that location. This will also become important if GIAC ever decides to outsource workstation and printer support. If there is a need to administrate a server locally by location instead of centrally, the computer account for the server can reside in the locations OU. For example if Marketing wanted to have their own application server and allow the local support staff at the Home Office to administrate it, the computer account could go in a server OU under the Home Office OU.

Organizing the users separate from the computers allows administrators to easily enforce Group Policy Objects to users centrally, not allowing administrators of child OU's to override. Organizing the four departments in separate child domains allows delegation of separate administration of these departments, allowing security precautions to be taken for interdepartmental protection.

All enterprise OU's will be separated and at the root to allow administrators to enforce Group Policy Objects to servers centrally. Separate child OU's can be created to further segment server administration. That way administrators of specific servers will only be able assign policy's to the servers they are responsible for – For example, not allowing administrators of web servers to affect settings of file servers. But for now the same administrators control all the enterprise servers.

The domain controllers will automatically be organized in the default OU "Domain Controllers". The default will be kept in order to apply domain controller specific Group Policy Objects. Domain controllers will require a different set of policies due to their importance and sensitivity.

OUs are relatively easy to change and do not impact the underlying physical Active Directory design or implementation. Think of the OUs as the logical organization of the directory that allows objects to be stored in a structured manner.

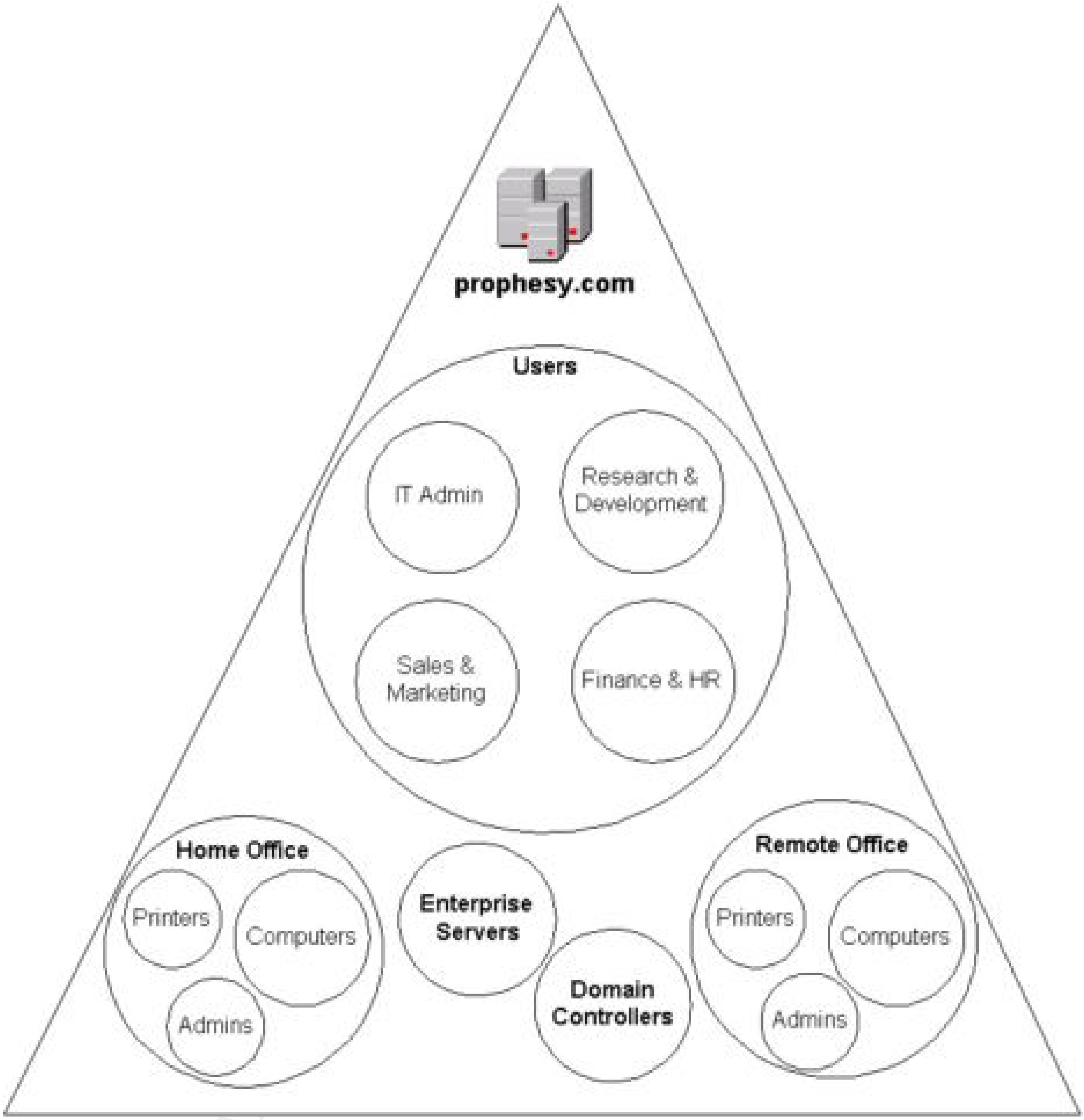


Figure 4 - Logical OU Design

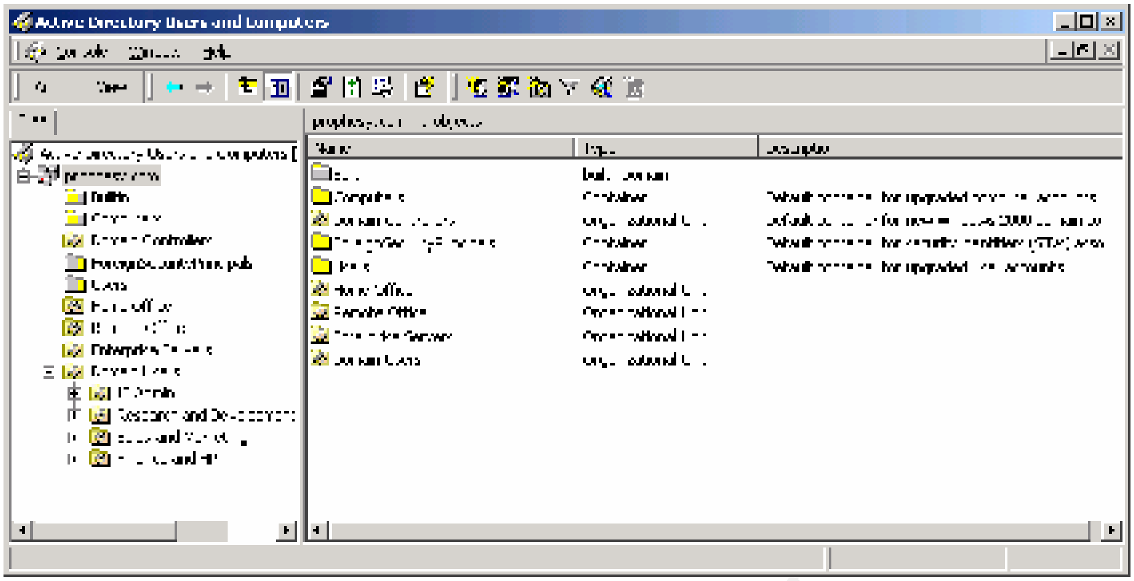


Figure 5 – Physical View of OU Configuration

3.1.3 Details

This section provides detailed information regarding the OU structure, including the top-level object-based structure, administrative delegation, methods of populating objects into the various OUs, and naming standards.

3.1.3.1 Object Functions

An object is the basic building block of the Active Directory database. These objects have a distinct, named set of attributes that represent a network resource. These objects are then going to be organized into classes, which are logical grouping of objects. Users, groups, and computers are examples of different object classes. The table below shows each top-level OU, the object type contained, and the purpose of the container:

OU Name	Object Type	Purpose
Home Office	OUs containing Computers and Printers	OUs containing all desktop and published print queues at the Home Office
Remote Office	OUs containing Computers and Printers	OUs containing all desktop and published print queues at the Remote Office
Users	User	Domain login accounts

Enterprise Servers	Computer	Infrastructure/Application server computer accounts
Domain Controllers	Computer	Domain Controller computer accounts

Table 2 - OU Type and Purpose

3.1.3.2 Population

Once the OU structure has been implemented, the individual OUs must be populated with objects. The following table identifies how the OUs will be populated:

OU Name	Source	Population Method
Home Office	Migration from existing NT 4.0 domain	Automated using third party tools
Remote Office	Migration from existing NT 4.0 domain	Automated using third party tools
Users	Migration from existing Exchange 2000 database	Automated using third party tools
Enterprise Servers	Administrator	Manual process
Domain Controllers	Default Configuration	Automatic

Table 3 - OU Source and Population Method

The selected Windows 2000 migration tool for the automated population will be BindView bv-Migrate.

3.2 – Group Policy

Being the most important security feature of Windows 2000, Group Policy is the primary tool for defining and controlling how programs, network resources, and the operating system behave for users and computers in an organization. Group Policy allows specification of a desired computer configuration at one time, and then relies on the Windows 2000 environment to enforce that desired configuration on all affected client computers. Group Policy specifies settings for groups of users and computers, including registry values, registry key permissions and auditing, NTFS permissions and auditing, startup/shutdown/logon/logoff scripts, manage user rights, manage group memberships, software installation, folder redirection, password policies, security settings, manage services, and manage users desktops.

This policy information is stored in Group Policy objects, which are linked to selected Active Directory containers: sites, domains, and organizational units. Each object then gets applied as part of the startup process or when someone logs on to the workstation.

3.2.1 Design Considerations

Group Policy is a powerful complex tool that needs some careful considerations. Keeping the design simple with the fewest number of Group Policy Objects will make administration much easier. Keep group related settings to a single Group Policy Object and delegate the administration. Plan and carefully test Group Policy Objects in a lab before deploying. Carefully document the design, changes, and any problems experienced including the date, time, and the administrator that made the changes.

All domain-wide account policies settings and other settings should be included in the Group Policy Object at the domain level. Too many Group Policy Objects can be an administrative nightmare, making it difficult to track policy settings, troubleshoot policy problems, and can limit the number of Group Policy Objects assigned to users and computers.

The PDC Emulator (NAHQDC01) will remain the Group Policy Manager.

3.2.2 Design

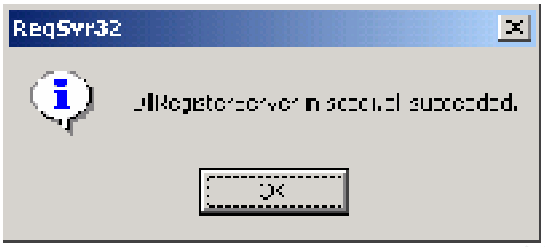
To simplify the Active Directory Design, only four Group Policy Objects were selected:

- Domain Policy
- Workstation Policy
- Server Policy
- Domain Controller

These were selected based on security templates from the National Security Agency. The templates can be downloaded from NSA's web site and is updated regularly. The following templates need to be downloaded and copied to C:\winnt\security\templates on NAHQDC01:

- w2k_domain_policy.inf
- w2k_workstation.inf
- w2k_server.inf
- w2k_dc.inf

Next, "sceregv1.inf" needs to be copied to C:\winnt\inf on NAHQDC01. To register the new security options on NAHQDC01, run "regsvr32 sceregv1.inf" from a command prompt. You should see the succeeded message in figure 6.



DllRegisterServer in scecli.dll succeeded.

Figure 6 – NSA "sceregv1.inf"

3.2.2.1 Domain Policy

Account policies apply at the domain level. This security policy is defined at the root of the domain and should be most restrictive. The modified template, "w2k_domain_policy.inf" from the National Security Agency, was chosen as a baseline for this level of security. To import this template, right-click on the Security Settings in the GPO/Import Policy and check the box "Clear this database before importing"; highlight w2k_domain_policy, and select Open. Some changes will be made to this security template for GIAC customization (see table 4).

Options	Recommended For	Customization
Message text for users attempting to log on	Workstations, Members Servers, Domain Controllers	HKLM\Software\Microsoft\Windows \CurrentVersion\Policies\System \LegalNoticeText = "See message title below"
Message title for users attempting to log on	Workstations, Members Servers, Domain Controllers	HKLM\Software\Microsoft\Windows \CurrentVersion\Policies\System \LegalNoticeCaption = "GIAC Enterprises Warning Statement"
Rename Administrator account	Workstations, Members Servers, Domain Controllers	Configure locally. Do not assign in Group Policy.
Rename Guest account	Workstations, Members Servers, Domain Controllers	Configure locally. Do not assign in Group Policy.

Table 4 - Customization to Domain Policy

Because of legal concern, a legal notice will be displayed to all users attempting to log on to any machine on the domain. This option was modified to display a GIAC customized warning statement from the Department of Defense (DoD), the following is the message text users will see when attempting to log on to Workstations, Member Servers, or Domain Controllers:

“This is a [GIAC Enterprise] computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized [GIAC] use. [GIAC] computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized [GIAC] entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this [GIAC] computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.”
(National Security Agency, “Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set”, pg. 95)
The message title will be displayed before the message text, identifying the legal message.

Renaming the administrator and guest account will take place at the time of server or workstation installation and will not be controlled by group policy.

The rest of the settings from the security template will be set according to Table 5. The security settings not configured are not included in Table 5.

Domain Policy Settings	
Policy	**Computer Setting**
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	12 characters
Passwords must meet complexity requirements	Enabled

Domain Policy Settings	Computer Setting
Policy	
Store password using reversible encryption for all users in the domain	Disabled
Account lockout duration	15 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	15 minutes
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes
Automatically log off users when logon time expires	Enabled

Table 5 – Domain Policy settings

The password policies will prevent users changing their password to previous passwords, force users to change their password every 90 days, not allow users to change passwords more than once a day, require passwords to be 12 or more characters, and enforce strong password requirements. Strengthening the passwords will make it difficult for brute force password cracking programs to crack the passwords and more difficult for someone to guess a password, making resources more secure. The complexity requirements require passwords to contain characters from three of four classes: uppercase letters, lower case letters, numbers, and special characters. The setting also will not allow users to make passwords the same as their logon name.

The account lockout settings will lock an account from logon if an incorrect attempt has been made three consecutive times within 15 minutes. If the account becomes locked, the account will be enabled after 15 minutes of being locked. This will help protect the account from password guessing programs cracking the password.

User and service ticket settings are for Kerberos Policy settings, which determine Active Directory authentication settings. Enforce user logon restrictions will not allow a service ticket to be issued if the user does not have the appropriate user right for that service.

Computer clock synchronization is to help Kerberos validate authenticity of tickets by setting the maximum number of minutes the Key Distribution Center and the clients clock can differ.

3.2.2.2 Workstation Policy

The Workstations Group Policy Object implements the portion of GIAC's security strategy that's controlled by user settings. This Group Policy Object is linked to Computers OU's and will apply to all Windows 2000 desktop and laptop systems at GIAC unless filtering is used to deny the policy to specific groups of computers.

The modified template, w2k_workstation.inf from the National Security Agency was chosen for a baseline for this level of security. To import this template, right-click on the Security Settings in the GPO/Import Policy and check the box "Clear this database before importing"; highlight w2k_workstation.inf and select Open.

Most of the NSA's modifications were kept on the Workstation Policy. One major benefit of this policy is the auditing settings. Success and failure will be audited in event manager for account logon events, account management, logon events, policy change, and system events. Directory service access, object access, and privilege use will be audited on failure.

Amount of idle time required before disconnecting session was set at 30 minutes to protect a workstation from being compromised if a user left without logging out.

Disable Media Autoplay is a recent addition that protects the system from auto running malicious code from any drives. By default, Windows 2000 auto runs any CDROM that is placed in the drive.

For all the specific settings in the Workstations GPO, see Appendix A.

3.2.2.3 Server Policy

The Servers Group Policy Object implements auditing policies and hardening changes to GIAC's Enterprise Servers. This Group Policy Object is linked to the Enterprise Servers OU and will apply to all Windows 2000 servers at GIAC unless filtering is used to deny the policy to specific groups of servers.

The modified template, w2k_server.inf from the National Security Agency was chosen as a baseline for this level of security. To import this template, right-click on the Security Settings in the GPO/Import Policy and check the box "Clear this database before importing"; highlight w2k_server.inf and select Open.

The servers will be configured to digitally sign the client and server communication when possible. The virtual memory pagefile will be cleared when the machine shuts down to prevent compromised data extracted from the file if the server is ever physically attacked. For specific settings in the Servers GPO see Appendix B.

Since there are servers on the DMZ that are not a member of the Active Directory, this security template will need to be manually applied to the DMZ servers. Once GIAC grows with more servers on the DMZ, it may be beneficial to create a separate DMZ domain and Active Directory to apply Group Policy Objects. Securing the DMZ servers with security templates is covered in the next section, Security and User Administration.

3.2.2.4 Domain Controller Policy

The Domain Controller Group Policy Object auditing policies and hardening changes to GIAC's Domain Controllers. This Group Policy Object is linked to the default Domain Controllers OU that is predefined in Windows 2000.

The modified template, w2k_dc.inf from the National Security Agency was chosen for a baseline for this level of security. This script was built to address the specific security concerns of domain controllers. To import this template, right-click on the Security Settings in the GPO/Import Policy and check the box "Clear this database before importing"; highlight w2k_dc.inf and select Open.

The Domain Controllers will have the same or more restrictive security precautions of the Servers. Only Administrators, Authenticated Users, and Enterprise Domain Controllers will be able to access the domain controller from the network. Bypass traverse checking will be set to authenticated users instead of just users. NTFS auditing will be used to monitor any failed attempts to access the NTDS and SYSVOL folders. Because all the Domain Controllers will be Windows 2000, the "Secure channel: Digitally encrypt or sign secure channel data (always)" and "Secure channel: Require strong session key" policies will be set to "enabled". For specific settings in the Domain Controller GPO see Appendix C.

3.2.2.5 Additional Considerations

Group policy will be used in other ways that will secure the network and departments. Delegation of control will assist in giving an administrator power over a specific location or a department, without giving the administrator rights over other locations or departments. This will be set at the OU level using the Delegation of Control Wizard.

File security will be assigned to the users home drives to only allow access by the user and administrator. Departmental folders will be protected by only giving rights to groups that require access to the specific folder.

Workstation settings in the Administrative Templates will be locked down on certain groups that do not need to make many changes to their workstation. This will aid in support cost, as well as security. Internet Explorer security settings under Windows Settings will be enforced from Group Policy, setting the Security Zones and Authenticode settings. The security settings will initially set to medium, but disable all downloading of Java applets, ActiveX controls, and scripting for the Internet Site Settings.

3.2.3 Script Policies

In Windows 2000 Group Policy, script policies offer four script types: startup, shutdown, logon, and logoff. Startup and shutdown scripts are part of the Group Policy computer configuration. Group Policy startup and shutdown scripts provide a mechanism through which you can define and apply common scripts to multiple computers.

3.2.3.1 Description of Script Policies

Logon and logoff scripts are part of the Group Policy user configuration. Group Policy logon and logoff scripts provide a mechanism through which you can define and apply common scripts to multiple users, not related to the logon script defined as part of a user's profile.

The computer runs startup scripts when it starts and shutdown scripts when it shuts down. Logon scripts run when a configured user logs on to the computer, and logoff scripts run when the user logs off, after all policy scripts have executed. Logon scripts always run after startup scripts and logoff scripts always run before shutdown scripts. Since logon scripts are the last to execute, they have the power to change or override settings from other scripts.

3.2.3.2 Scripting Language

Scripts can be developed in any language that Windows 2000 supports. Scripts can be written in VBScript, Jscript, PERL, Extensible Markup Language (XML)-based Windows Script (.ws) file. Since Microsoft's preferred language for scripting access to Active Directory is VBScript, GIAC will standardize on Windows Scripting Host (WSH) scripts in VBScript. This will give GIAC the ability to utilize many scripts already written.

Other than the sample Administration scripts found on the Windows 2000 Resource Kit, there are many script repositories available on several Internet sites. Group Policy is not needed to utilize most of the Administrative scripts found, however a machine with domain level administrative access will be needed for many of the scripts.

3.2.3.3 Script Policies Configuration

Script Policies will be enforced in the Domain Policy Group Policy Object at the Users Organizational Unit. These will be created through the properties under the Users OU in Active Directory Sites and Services. Expand the User Configuration tree and then expand the Windows Settings sub tree. Departmental specific drive mappings and settings will be applied at the appropriate lower-level OU under the Users OU. Initially a simple logon script will suffice, mapping the appropriate drives and applying any customized settings. This script will be named userslogon.vbs. Logoff, startup, and shutdown scripts will only be used as needed.

3.2.4 Software Distribution

Much of the software and Service Packs will be deployed through Group Policy. Active Directory can deploy software through group policy with Microsoft's Windows Installer feature. A package file with an .msi extension will be needed to deploy software and is usually included with today's software and Microsoft's service packs. Most of the software will be deployed through the Workstation Policy Group Policy Object, but the Server and Domain Controller policy may be used for certain service packs and hotfixes. Software can then be either Assigned or Published to computers or users. Below are descriptions of the different scenarios that can be applied:

- If "assigned" to a computer, the application will be installed when the computer boots up.
- If "published" to a computer, the application becomes available in the Add/Remove Programs Control Panel of the computer to which the policy applies and the application must be installed manually.
- If "assigned" to a user, the application will be installed when the user logs on.
- If "published" to a user, the application becomes available in the Add/Remove Programs Control Panel of the user to which the policy applies and the application must be installed manually.

3.2.4.1 Assigning Software to Workstations

To assign a software package to a group of computers at a particular site, simply select properties under the site's OU, browse to Computer

Configuration, and select Software Installation. By right-clicking the Software Installation icon and selecting New, you will be able to browse for the software package you would like to assign. When asked for the deployment method, select Assigned for the application to be forced to the Workstations. GIAC will assign all users the standard applications including Office XP Sp1, IE 5.5 Sp2, and McAfee VirusScan 4.5.1 Sp1. Departmental specific applications will be assigned at the departments child OU under Users. Service packs will be assigned by the Location's OU. Currently Service Pack 2 for Windows 2000 will be assigned.

3.2.4.2 Assigning Software to Servers

To assign a software package to a group of servers at a particular site, simply select properties under the Enterprise Servers Organizational Unit, browse to Computer Configuration, and select Software Installation. By right-clicking the Software Installation icon and selecting New, you will be able to browse for the software package you would like to assign. When asked for the deployment method, select Assigned for the application to be forced to the Servers. The current tested Service Pack will be assigned to the Enterprise Servers OU, which is Service Pack 2 at this time.

3.2.4.3 Assigning Software to Domain Controllers

GIAC will assign software to domain controllers to mainly enforce service packs and anti-virus software. To assign a software package to a group of domain controllers at a particular site, simply select properties under the default Domain Controllers Organizational Unit, browse to Computer Configuration, and select Software Installation. By right-clicking the Software Installation icon and selecting New, you will be able to browse for the msi enabled software package or service pack you would like to assign. When asked for the deployment method, select Assigned for the application to be forced to the Domain Controllers. The current tested Service Pack will be assigned to the Domain Controllers OU, which is Service Pack 2 at this time.

3.2.4.4 Publishing Software to Workstations

GIAC will not only assign service packs and anti-virus software to workstations, all the standard applications that GIAC loads on all workstations that support msi packages will be published. To publish a software package to a group of computers at a particular site, simply select properties under the site's OU, browse to Computer Configuration, and select Software Installation. By right-clicking the Software Installation icon and selecting New, you will be able to browse for the msi enabled software package or service pack you would like to assign. When asked for the deployment method, select Published for the application to be available in the Add/Remove Programs Control Panel of the computers in the selected OU.

3.2.4.5 Publishing Software to Servers

To publish a software package to all the servers, simply select properties under the Enterprise Servers OU, browse to Computer Configuration, and select Software Installation. By right-clicking the Software Installation icon and selecting New, you will be able to browse for the msi enabled software package or service pack you would like to assign. When asked for the deployment method, select Published for the application to be available in the Add/Remove Programs Control Panel of the server in the Enterprise Servers OU. Software published to servers will be optional applications that administrators may need that GIAC approves for servers.

3.2.4.6 Publishing Software to Domain Controllers

To publish a software package to all the domain controllers, simply select properties under the default Domain Controllers Organizational Unit, browse to Computer Configuration, and select Software Installation. By right-clicking the Software Installation icon and selecting New, you will be able to browse for the msi enabled software package or service pack you would like to assign. When asked for the deployment method, select Published for the application to be available in the Add/Remove Programs Control Panel of the domain controllers. Software published to servers will be optional applications that administrators may need that GIAC approves for Domain Controllers.

3.2.5 Administration

Windows 2000 Active Directory supports delegation of control for portions of the directory service. Three types of Group Policy tasks can be delegated in Windows 2000:

- Managing Group Policy links for site, domain, or OU
- Editing GPOs
- Creating GPOs

By default, authenticated users have both Read and Apply Group Policy permissions set to Allow. This means that users cannot modify the information in the GPO. Also by default, Domain Administrators, Enterprise Administrators, and the local system have full control permissions, without the Read and Apply Group Policy permissions. The default settings will be kept in order to protect the Group Policies and the permissions. With the appropriate rights a user or group could be excluded from running a Group Policy.

Permissions can also be used to selectively apply Group Policy to the users in a particular group, without having to configure multiple GPOs. An example would be, creating a GPO just for contractors without having to create a separate OU. This GPO could be applied to the main Users OU to ensure it would be applied over any other policies. After creating the Group Policy Object for contractors, simply remove the Read and Apply Group Policy permissions for Authenticated Users and add the Read and Apply Group Policy permissions for the Contractors group.

Chapter 4 – Security and User Administration

Previous sections provided specifications on how the Active Directory is to be deployed and initially configured. This chapter describes strategies for managing and supporting Active Directory in production.

4.1 – Access Control

The security of Active Directory objects is based on access control lists (ACLs). Components of Active Directory security include Security Principals, Security Identifiers (SIDs), and Security Descriptors.

Security Principals include users, security groups, services, and computers and are represented by Security Identifiers (SIDs). SIDs uniquely identifies the Security Principals and is never reused. The security information associated with an object is called a Security Descriptor. Security Descriptors contain Discretionary Access Control Lists (DACLs) and System Access Control Lists (SACLs). The DACL is an ACL that maintains data indicating which users have access to the object and the access permissions those users have. The SACL is an ACL used by the system to track events for auditing purposes

The entries in an object's ACLs are called Access Control Entries (ACEs). ACEs are added to the DACL of an object and specify permission settings for users and groups. ACEs in a parent object's security descriptor are passed to a child object's descriptor through inheritance. The following describes how to access the Object Security Properties in Active Directory:

- Select Start, Programs, Administrative Tools, and open Active Directory Users and Computers
- Select Advanced Features from the View menu.
- Right-click the object and select Properties.
- Select the Security tab in the Properties dialog box.

4.2 – Security Groups

Security groups can be used to control access to resources, define additional system rights, or to provide application access control. Since Windows 2000 is being implemented in native mode, all types of Windows 2000 groups and functionality will be available. Since only one domain will be supported, Universal groups will not be used.

GIAC will standardize on Global groups for organizing users, while using Domain local groups to provide access to resources. Nesting groups will be limited to three levels to provide better administration and management. All administrative accounts will be created in the IT Admin OU. Administrative accounts will be granted rights by placing them in the appropriate administrative global groups, not by direct rights assignment. When creating new Windows 2000 security groups, the following factors should be considered:

- Groups should be defined and used in a uniform manner.
- Redundant or overlap between groups should be avoided.
- Each group should have an owner.
- The purpose and lifetime of the group should be identified

4.3 – Auditing

Although the security templates automatically activate the recommended auditing policies, reviewing audit events is not automatic. Auditing is a critical piece in maintaining the security of the domain. At a minimum, a weekly task should be enabled to audit specific user, computer, group, and other objects that have security significance.

Events from the enabled auditing policies are recorded in the computer's Security Log in the Event Viewer. Review should include verification that the expected events are recorded, data can be analyzed and understood, and the amount of data is manageable. Filters can be used to simplify the audit process.
In addition to using Event Viewer, many debug log files can be used to audit events. Netsetup.log and netlogon.log are two very informative log files. Netsetup.log records attempts to join domains and records the results. Netlogon.log contains events when the Net Logon service is used.

4.4 – Securing DMZ Servers

Because the servers on the DMZ will be accessible from the Internet, great caution needs to take place to secure these servers from attack. Special Security Templates will be used to lock down the server that is specifically designed for IIS 5. The DMZ servers will have two network cards with a static valid IP visible to the outside and a non valid static IP connected to the internal network, both protected by a firewall and IPSec rules. Finally there will be other manual security precautions that will need to take place.

4.4.1 Security Templates

Because GIAC will not have an Active Directory domain in the DMZ, Security Templates will need to be manually applied. There are only two Windows 2000 servers on the DMZ's and both are IIS 5 Web Servers. GIAC will be using Microsoft's latest security template for IIS 5, Hisecweb.inf, to initially lock down the server. Refer to Artical Q316347 at http://support.microsoft.com/default.aspx?scid=kb;en-us;Q316347& to download the Hisecweb.exe. First run Hisecweb.exe and then copy the Hisecweb.inf file to C:\winnt\security\templates on the local server. Next from a command line, run secedit /configure /cfg "Hisecweb.inf" /db giac.sdb /overwrite. This will load the template into a new security database named giac.sdb. This process will need to be repeated on all DMZ servers each time a security setting is changed, or until an Active Directory domain is implemented on the DMZ.

4.4.2 IPSec Policies

IPSec policies will also be configured on the two DMZ servers. This will be used to secure communications to and from the outside client, as well as securing communications through the internal firewall. The external firewall will protect the DMZ servers for the most part, but if the firewall is compromised, the IPSec policies will add additional layer of protection. The only communications allowed through the internal firewall will be ports needed for SQL connections. Since the DMZ servers are not connected to a domain controller, two custom IPSec policies will need to be created on each server.

For the network card connected to the outside, create an Ip Security Policy from the IP Security Policies on the server. Run the Security Rule Wizard, select does not specify a tunnel, and assign it to the network connection to the outside. Configure the web server to Public key signature using a certificate from VeriSign. Block all ports except the ones absolutely needed for communication to the public. Block any IP addresses that are considered a threat from public awareness or past experiences.

For the network card connected to the inside, create an IP Security Policy on both the SQL server and the Server on the DMZ. A private key will be used for this communication that will only be used for these servers. Allow only the ports needed for the SQL communication and only allow communication on each others IP address. The SQL server will have two network cards as well, one just to communicate to the external web servers. The internal firewall will need to be configured to open the required ports just between the IP address of the SQL server and the two DMZ servers.

4.4.3 Other Considerations

The DMZ servers will need additional security considerations in addition to applying the templates. Since Group Policy won't be assigning software either, all service packs, post hotfixes, and anti-virus software will be manually installed. As with all the other servers, the Local Administrator and Guest account will be renamed with the Guest account disabled. The Local Administrator password will be unique to the server and at least 30 characters from all four classes: uppercase letters, lower case letters, numbers, and special characters. All unused services mentioned earlier will be disabled in addition to NetBios, Telnet, DHCP, and Terminal services.

Service pack 2 for Windows 2000 should already be applied with the default server build, but also apply the latest security rollup package, which is currently Windows 2000 Security Rollup Package 1 released January 2002. See Article Q311401 at **http://support.microsoft.com/default.aspx?scid=kb;EN-US;q311401**.

Download and run the latest IIS lockdown tool from Microsoft. The latest one now is version 2.1. See http://www.microsoft.com/technet/security/tools/locktool.asp for more information and download location.

Turn off unneeded features and block unneeded URL requests with the latest Urlscan Security Tool from Microsoft. The current version is 2.5 and available from http://www.microsoft.com/technet/security/tools/tools/urlscan.asp.

Run the latest cumulative patch for IIS 5 from http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32011.

Follow Microsoft's Secure Internet Information Server 5 Checklist, which is currently available from http://www.microsoft.com/technet/security/tools/chklist/iis5chk.asp.

4.5 – Administration Delegation

Administration delegation is one objective from creating OUs in Active Directory. This gives the ability to discretely control the scope of system administration, which increases overall security. GIAC will focus on centralizing administration of most system, server, account, and group operations, but there will be justification for some delegation. Fortunately Active Directory and the structure designed allow delegation to be secure and granular. It will be up to the core administrators to correctly delegate authority and responsibility of groups that require.

Appendix A – Workstation GPO Settings

Policy	Computer Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	12 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled
Account lockout duration	15 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	15 minutes
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Failure
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	Success, Failure
Access this computer from the network	Administrators,Authenticated Users,ENTERPRISE DOMAIN CONTROLLERS
Bypass traverse checking	Authenticated Users
Create a pagefile	Administrators
Enable computer and user accounts to be trusted for delegation	Administrators
Force shutdown from a remote system	Administrators
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Log on locally	Administrators Users
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	Administrators
files and directories	Administrators
Shut down the system	Administrators Users
Take ownership Restore of files or other objects	Administrators
Additional restrictions for anonymous connections	No access without explicit anonymous permissions

Policy	Computer Setting
Allow Automatic Administrator Logon	Disabled
Allow server operators to schedule tasks (domain controllers only)	Disabled
Allow system to be shut down without having to log on	Disabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	30 minutes
Audit the access of global system objects	Enabled
Audit use of Backup and Restore privilege	Enabled
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Disabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Disabled
Digitally sign server communication (when possible)	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Disable Media Autoplay	All Drives
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM
Number of previous logons to cache (in case domain controller is not available)	0 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Enabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled

Policy	Computer Setting
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Disabled
Send unencrypted password to connect to third-party SMB servers	Disabled
Shut down system immediately if unable to log security audits	Enabled
Smart card removal behavior	Lock Workstation
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled
Unsigned driver installation behavior	Warn but allow installation
Unsigned non-driver installation behavior	Warn but allow installation
Maximum application log size	4194240 kilobytes
Maximum security log size	4194240 kilobytes
Maximum system log size	4194240 kilobytes
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Shut down the computer when the security audit log is full	Enabled
Retention method for application log	Manually
Retention method for security log	Manually
Retention method for system log	Manually

Appendix B – Server GPO

Policy	Computer Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	12 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled
Account lockout duration	15 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	15 minutes
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Failure
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	Success, Failure
Access this computer from the network	Administrators,Users
Back up files and directories	Administrators
Bypass traverse checking	Users
Change the system time	Administrators
Create a pagefile	Administrators
Force shutdown from a remote system	Administrators
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Restore files and directories	Administrators
Shut down the system	Administrators
Take ownership of files or other objects	Administrators
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Allow Automatic Administrator Logon	Disabled
Allow system to be shut down without having to log on	Disabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before	30 minutes

Policy	Computer Setting
disconnecting session	
Audit the access of global system objects	Enabled
Audit use of Backup and Restore privilege	Enabled
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Disabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Disabled
Digitally sign server communication (when possible)	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Disable Media Autoplay	All Drives
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM
Number of previous logons to cache (in case domain controller is not available)	0 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Enabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Disabled
Send unencrypted password to connect to third-party SMB servers	Disabled
Shut down system immediately if unable to log security audits	Enabled
Smart card removal behavior	Lock Workstation
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled

Policy	Computer Setting
Unsigned driver installation behavior	Warn but allow installation
Unsigned non-driver installation behavior	Warn but allow installation

Appendix C – Domain Controller GPO

Policy	Computer Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	12 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled
Account lockout duration	15 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	15 minutes
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Failure
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit system events	Success, Failure
Access this computer from the network	Administrators,Authenticated Users,ENTERPRISE DOMAIN CONTROLLERS
Back up files and directories	Administrators
Bypass traverse checking	Authenticated Users
Change the system time	Administrators
Create a pagefile	Administrators
Enable computer and user accounts to be trusted for delegation	Administrators
Force shutdown from a remote system	Administrators
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Log on locally	Administrators
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Restore files and directories	Administrators
Shut down the system	Administrators
Take ownership of files or other objects	Administrators
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Allow Automatic Administrator Logon	Disabled

Policy	Computer Setting
Allow server operators to schedule tasks (domain controllers only)	Disabled
Allow system to be shut down without having to log on	Disabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	30 minutes
Audit the access of global system objects	Enabled
Audit use of Backup and Restore privilege	Enabled
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Disabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Disabled
Digitally sign server communication (when possible)	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Disable Media Autoplay	All Drives
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM
Number of previous logons to cache (in case domain controller is not available)	0 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Enabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Enabled
Send unencrypted password to connect to third-party SMB servers	Disabled

Policy	Computer Setting
Shut down system immediately if unable to log security audits	Enabled
Smart card removal behavior	Lock Workstation
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled
Unsigned driver installation behavior	Warn but allow installation
Unsigned non-driver installation behavior	Warn but allow installation

Appendix D – References

Casad, Joe, Windows 2000 Active Directory, Berkeley, California: Osborne/McGraw-Hill, 2000

Fossen, Jason, 5.1 Windows 2000 Active Directory and Group Policy. Version 5.1.3, SANS Institute, November 13, 2001

Haney, Julie M. Guide to Securing Microsoft Windows 2000 Group Policy, Version 1.1, National Security Agency, September 13, 2001

Haney, Julie M. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set, Version 1.1, National Security Agency, January 22, 2002

ISS Real Secure 6.5 Frequently Asked Questions, URL: http://documents.iss.net/literature/RealSecure/RS6.5ExternalFAQ.pdf

Make Your Windows Servers Secure, URL: http://www.microsoft.com/technet/security/tools/ChkList/wsrvSec.asp

Microsoft Windows 2000 Network Architecture Guide, Version 1.0, National Security Agency, April 19, 2001

Rice, David, Group Policy Reference, Version 1.0.8, National Security Agency, March 2, 2001

Sanderson, Mark and David Rice, Guide to Securing Microsoft Windows 2000 Active Directory, Version 1.0, National Security Agency, December 2000

Step-by-Step Guide to Internet Protocol Security, February 17, 2000, URL: http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp