Global Information Assurance Certification Paper

Designing a Secure Windows 2000 Network Infrastructure

Securing Windows
GCNT Practical Assignment v. 3.0
Option A

David Branscome
03/15/02

Introduction

GIAC Enterprises is an e-business that deals in the online sale of fortune cookie sayings.

GIAC is a small company consisting of a single office located in San Francisco. The office employs 200 people. The job functions of these employees can be broken down into essentially 5 groups – Corporate Executives, Human Resources, Finance and Accounting, Research and Development and Information Technology.

The company is a relatively new startup company, and as such, they were able to design their network infrastructure from the ground up. In order to provide an infrastructure which is stable and can be utilized in the future to conduct extensive amounts of e-business, all servers and workstations were purchased specifically to accommodate the Windows 2000 Server and Windows 2000 Professional operating systems.

Security and availability are the primary concerns of the IT staff, and fortunately, the CEO of the company, being a former CIO, agrees with those priorities. Therefore, considerable time and money was spent on the design and implementation of the GIAC Windows 2000 network, which includes a public web server running IIS 5.0 hosting the www.giacent.com corporate website, clustered Exchange 2000 servers for mail, clustered file and print servers, and redundant domain controllers to provide for consistent logon availability.

The varying requirements of the staff necessitate the granting of differing levels of access to the desktop and server systems.

Specifically, there are three levels of access to the systems:

Standard Users – Corporate staff, including Human Resources, Marketing and Sales, Finance and corporate executives are given this level of access.
Power Users - The Research and Development staff and IT staff members have user accounts included in this category.
Administrators – IT staff responsible for administering the servers have special usage accounts which are included in this category.

Within those groups, job functions at times require varying levels of security as well. The Human Resources, Finance and Accounting, and Research and Development staff members deal with highly sensitive materials, and as a result have much higher security requirements, both at the workstation and server level.

Human Resources – Staff members who handle confidential employee records, including reviews and payroll records, maintain data on a separate server with more restricted application level access to ensure security of those records and obviate the possibility of private data becoming public knowledge. Applications that are used to manage HR records are tightly integrated with Active Directory, and can therefore have permissions assigned at the enterprise level.

Finance/Accounting – The Finance and Accounting departments require security on the company financial records and the ability to control access to the financial databases is critical. Again, the application selected for use was chosen in part because of its tight integration with Active Directory, and can therefore be managed at the enterprise level.

Research/Development – The R&D staff members are working on highly confidential, proprietary information, which could have vast implications on the fortune cookie saying industry. Needless to say, their work must remain secure, as the future of the company hinges on their ability to design and develop in a secure environment. To that end, the server housing the Research and Development data must be secured using Active Directory permissions and other methods of access control.

These three groups, because of the critical nature of their work, maintain data on servers that are physically and logically separated from the standard e-mail and file/print servers.

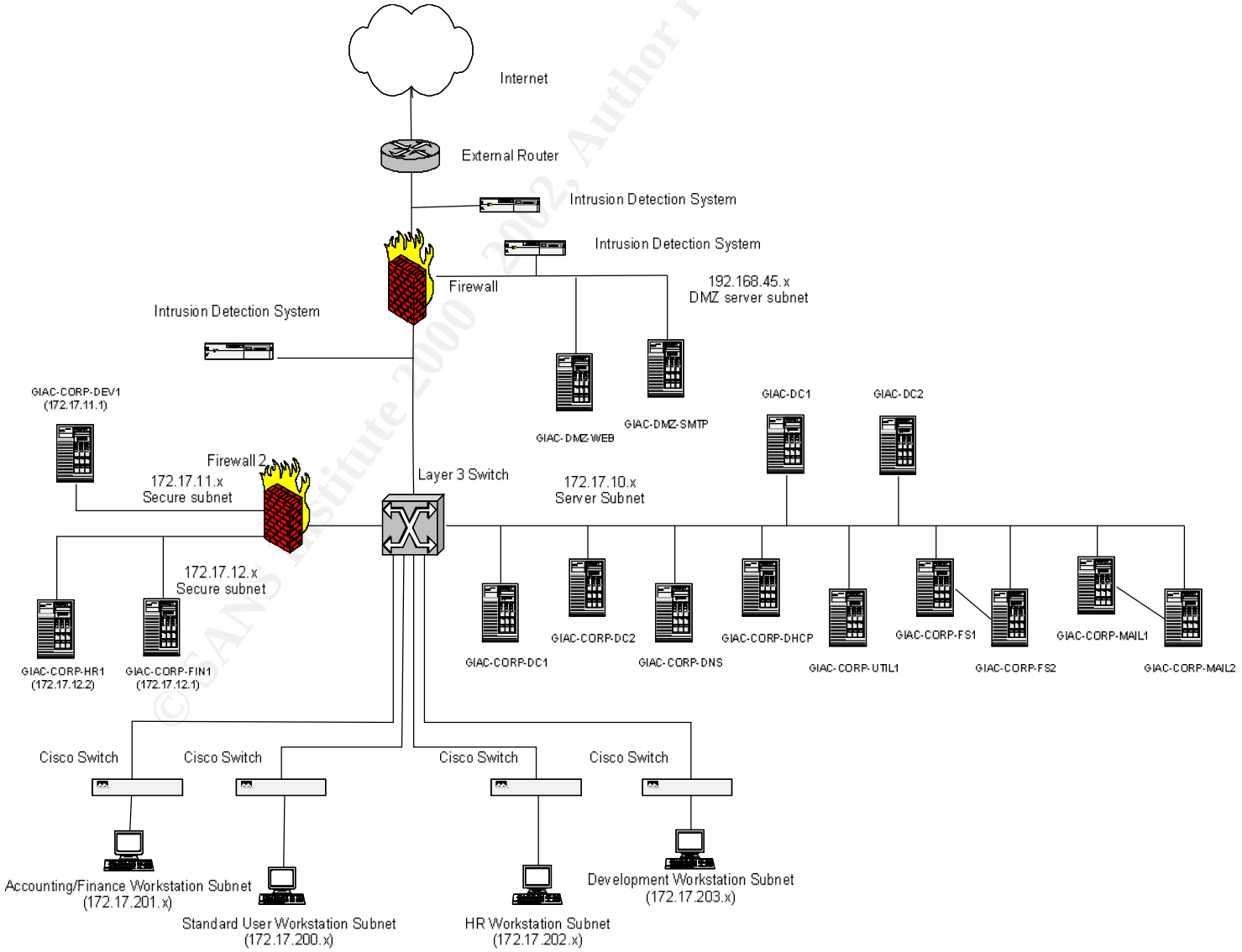
Additionally, IT personnel are divided into two separate groups with differing levels of network access, as outlined below.

Help Desk Personnel – IT staff members who provide desktop and application support to the user population are included in this group. This group has been delegated rights to change passwords, unlock accounts, modify group membership and specific field information for user accounts in the Standard Users and Power Users OU's in Active Directory.

Administrators – IT staff members who are responsible for all configuration changes on the servers, security management of the servers and design and builds of the servers are members of this group. Additionally, administrators have an account without elevated rights in the Power Users OU of Active Directory that is used for normal daily access to e-mail, file system and other standard access permissions to the network. The account with elevated permissions is utilized only when performing administrative functions.

GIAC Enterprises Network Configuration Overview

As indicated above, the GIAC Enterprises network is a single location. The overview of the network is shown in the diagram on the following page and described in detail on subsequent pages.



As indicated by the diagram, the GIAC network represents a contained domain model within a single physical site.

Working from the Internet towards the internal corporate network, the design is justified as follows:

The external router links the protected internal network as well as the DMZ to the Internet. This router is the first line of defense for GIAC Enterprises. It provides the first opportunity to permit or deny access to clients, servers and network services. This router acts as a screening filter, providing a relatively static set of controls against IP address spoofing, denial-of-service attacks, and connections to unauthorized services. Additionally, logs are kept on this router of traffic that is denied access to give network administrators the ability to identify potential weaknesses.

The next device is an Intrusion Detection System, configured to detect external threats. This is used to detect security breaches, provide real-time intrusion detection and notification, and provide response to unauthorized activity in order to block an intruder's attempts at penetrating the internal network.

The firewall in place represents an enforcer of security policy. Its three interfaces are for incoming traffic, access to the DMZ, and access to the protected, internal network. This firewall provides stateful packet filtering, which analyzes traffic based on IP address, port, direction of traffic and the state of the TCP or UDP session, and therefore is more valuable for analyzing the traffic than a standard packet filtering firewall. The firewall is configured to allow only SMTP and HTTP traffic into the DMZ as a security measure.

Within the DMZ, a second intrusion detection system provides another layer of protection from attack. Since the servers that reside on this network are exposed to the Internet, they are considered more vulnerable. It is therefore advisable to monitor the traffic going to and from these servers. The IDS can again provide alerts and responses to malicious attacks and other unauthorized activity, whether from an internal or external source.

The servers residing in the DMZ and their function will be described in detail later in the document.

The third IDS resides between the firewall and the layer 3 switch on the protected network. This provides an additional line of defense against attacks by monitoring traffic that has been able to pass through the internal firewall onto the protected network.

Next, the layer 3 switch is used to direct traffic on the internal network. Critical devices are directly attached to the collapsed core device, including each of the corporate servers, the second internal firewall protecting the subnets for the Development, Human Resources and Finance servers, and the switches which segment traffic to the 4 workstation subnets.

The internal firewall (Firewall 2) provides a layer of protection for the critical servers used by the Research and Development team, the Finance group and the Human Resources staff. The Research and Development server is isolated on its own subnet for two reasons:

1) The requirements for security on this server are high because of the critical business nature of the contents of the server. Any unauthorized access to the server represents a compromise of business-critical data and could be ruinous to the company.
2) From a network traffic perspective, putting this server on its own subnet is a good idea, as it would prevent any accidental broadcast storms that could be generated by a poorly written development application from causing disruption to either the Finance or HR servers on the other fire walled subnet, or to the other devices beyond the firewall.

The HR and Finance servers are behind the firewall as well to prevent unauthorized access to critical and confidential data.

The four workstation network segments coming off the Cisco switches attached to the layer 3 switch are, once again, designed as a security measure.

- An IP helper map will be defined on the Layer 3 Device that will allow DHCP requests from workstations on each of the 4 segments to be passed to the server, GIAC-CORP-DHCP. This DHCP server will have scopes defined that will allocate IP addresses based on the source network of the DHCP request.
- The workstations on the Standard User Workstation Subnet will receive IP addresses from the 172.17.200.x DHCP scope. Firewall 2 will then have access control lists defined to deny access to the firewalled subnets for workstations with IP addresses in the 172.17.200.x range. Workstations possessing IP addresses within that scope will be allowed access to all the servers on the 172.17.10.x subnet, however.
- The workstations on the Accounting/Finance Workstation Subnet will receive IP addresses from the 172.17.201.x DHCP scope. Firewall 2 will then have access control lists defined to allow access to 172.17.12.1 (GIAC-CORP-FIN1) for workstations with IP addresses in the 172.17.201.x

range. Workstations possessing IP addresses within that scope will also be allowed access to all the servers on the 172.17.10.x subnet.

- The workstations on the HR Workstation Subnet will receive IP addresses from the 172.17.202.x DHCP scope. Firewall 2 will then have access control lists defined to allow access to 172.17.12.2 (GIAC-CORP-HR1) for workstations with IP addresses in the 172.17.202.x range. Workstations possessing IP addresses within that scope will also be allowed access to all the servers on the 172.17.10.x subnet.
- The workstations on the Development Workstation Subnet will receive IP addresses from the 172.17.203.x DHCP scope. Firewall 2 will then have access control lists defined to allow access to 172.17.11.1 (GIAC-CORP-DEV1) for workstations with IP addresses in the 172.17.203.x range. Workstations possessing IP addresses within that scope will also be allowed access to all the servers on the 172.17.10.x subnet.

GIAC Enterprises Server Configuration

This section will describe in detail the configuration and security precautions taken on the servers on the GIAC Enterprises network. We will consider the roles of the servers, the reasons for their placement in particular locations on the network and pertinent details regarding their hardware and software configurations.

Physical Security

GIAC Enterprises' server room is secured using a biometric reader to verify identity using a fingerprint scan and a personalized PIN number that must be entered into the door locks to obtain access. Once inside the server room, each rack of servers is locked with a non-standard key. Each key is numbered and tracked individually.
Only administrators and operations staff members are issued PIN numbers and have keys to the server racks.
Each server CPU case is locked and cabled to the rack in which it resides.
Access to the server room is managed by an internal security department with software that automatically logs entry into the secured area. The security department monitors the server room with a 24-hour surveillance camera.
Each server is plugged into two different UPS units to provide for power fault-tolerance and to allow for a graceful power-down in the event of a power outage. The UPS' also have an attachment which monitors humidity and temperature and sends pager alerts to administrators when predefined thresholds are reached.
Backup tapes are stored in a secure room for a pre-defined period according to the type of backup (described later) and then stored offsite according to legal and business requirements for the specific data.

Standard Precautions

In line with Microsoft's Windows 2000 Server Baseline Security Checklist, the following steps are required on every server built.

- All disk partitions are formatted with NTFS
- The OS/2 and POSIX subsystems have been removed, including any related files and registry settings.
- All systems have the latest service packs and relevant hot fixes applied. Since, as a general rule, service packs (and often hot fixes as well) require

machine reboots, downtime for individual servers must be scheduled through the Change Management group, typically two days in advance. If especially critical hot fixes are identified, downtime can be approved on an emergency basis, but if systems are updated in the same week that security issues are identified, it is considered acceptable. To manage the constantly changing number of hot fixes required, Update Expert software from St. Bernard Software, Microsoft's QFECHECK utility (http://www.microsoft.com/downloads/release.asp?ReleaseID=27333) and Microsoft's HFCheck utility for IIS servers (http://www.microsoft.com/downloads/release.asp?ReleaseID=24168) are utilized.

- Obsolete directories have been removed from all servers. The directories that have been removed are:
    a. %systemdrive%\DOS
    b. %systemroot%\Cookies
    c. %systemroot%\History
    d. %systemroot%\Temporary Internet Files.

Server Specifications

DMZ Servers

The DMZ (Demilitarized Zone) is designed to restrict access to public giac.com servers from the Internet (considered to be an untrusted environment)

The two servers residing in the DMZ are not members of either the giac.com or corp.giac.com Active Directory domains, but rather, are stand-alone servers that are protected through the implementation of local security policies. These servers can only be administered through the local console or through an administrative workstation located on the internal network. The local policies for these devices will be discussed later.

Public IIS Web Server:
The public web server (GIAC-DMZ-WEB1) is available to Internet users via Port 80 (http). It serves up static content that is designed and tested on the internal network by the IT staff. It requires no direct access to any other servers in the enterprise.
Its hardware configuration is defined in the table below:

Server model	Compaq DL-380
Processors	P3 933 MHz/256K cache
Memory	256 Mb (2 Modules; 2 x 128)
Peripherals	Compaq NC3123 10/100 NIC
Other add-on components	None
Hard drives	2 x 18.2 Gb wide pluggable ultra 3 (10K RPM)
Hard drive configuration	One RAID 1 array with two physical drives; Two logical drives OS Partition (C:) 5 Gb,(5120 Mb) Data Partition (E:) uses remaining space

SMTP Mail Server: The mail forwarding server (GIAC-DMZ-SMTP) sends and receives from the internal mail server cluster all outbound SMTP mail. The backend servers have an antivirus program running on them that scans all incoming and outgoing mail for viruses.
Its hardware configuration is described below:

Server model	Compaq DL360 Model DL360R01
Processors	P3 933 MHz/256K cache
Memory	256 Mb
Peripherals	None
Other add-on components	None
Hard drives	2 x 36.4 Gb wide pluggable ultra 3 (10K RPM)
Hard drive configuration	One RAID 1 array with two physical drives; Two logical drives OS Partition (C:) 5 Gb, Data Partition (E:) uses remaining space

Internal Servers:

Domain Controllers:

Configuration for the domain controllers is described in the sections that follow since they have more complex roles on the network.

File and Print Servers: The file and print servers are set up in a clustered configuration to provide fault-tolerance and high-availability. The file and print servers are connected to a Storage Area Network via a SAN switch. The user profiles, home directories and departmental data reside on RAID-5 configured drives on the SAN. The log and quorum files reside on the SAN in a mirrored set RAID configuration. This configuration allows the IT staff to make configuration changes and apply service packs without incurring downtime. The file servers also run anti-virus software against the data on the Storage Area Network on a weekly basis as well as any time a file is accessed. Standard printers are defined on the virtual print server in the cluster and are made available to all users through Active Directory. Special printers, such as high-speed color printers and printers in the CEO's offices are restricted through Group Membership in Active Directory. The configuration of each server in the File Server cluster (they are identical) is described below:

Server model	Compaq DL380 Model DL380R01
Processors	P3 933 MHz/256K cache
Memory	1 GB
Peripherals	• Compaq NC3123 Fast Ethernet NIC PCI 10/100 WOL • Compaq NC6134 Gigabit NIC 64 PCI 1000SX • 2 x Compaq Fibre Channel Host Adapter PCI
Other add-on components	Compaq hot plug redundant power supply module
Hard drives	2 x 9.1 Gb wide pluggable ultra 3 (10K RPM)
Hard drive configuration	One RAID 1 array with two physical drives; one logical drive using full capacity

Exchange 2000 Servers: The Exchange 2000 mail servers are also set up in a clustered configuration to provide fault-tolerance and high-availability. They are connected to a Storage Area Network via a SAN switch. The mail data resides on RAID-5 configured drives on the SAN. Logs and quorum data reside on the SAN in a mirrored set RAID configuration. The Exchange servers also run anti-virus software that checks each incoming and outgoing mail message and it's attachments for viruses. The configuration of each server in the Exchange Server cluster (they are identical) is described below:

Server model	Compaq DL380 Model DL380R01
Processors	P3 933 MHz/256K cache
Memory	1 GB
Peripherals	• Compaq NC3123 Fast Ethernet NIC PCI 10/100 WOL • Compaq NC6134 Gigabit NIC 64 PCI 1000SX • 2 x Compaq Fibre Channel Host Adapter PCI
Other add-on components	Compaq hot plug redundant power supply module
Hard drives	2 x 9.1 Gb wide pluggable ultra 3 (10K RPM)
Hard drive configuration	One RAID 1 array with two physical drives; one logical drive using full capacity

Utility Server

The server GIAC-CORP-UTIL1 serves a multi-purpose role on the network. It is designated as the virus definition repository and is configured to continually check the anti-virus vendor's web site throughout the day to receive virus and engine updates and disseminate these updates to the clients on the network. (Each workstation also has a local anti-virus program loaded). As the central backup server with a fiber connection to the SAN, this server also performs

backups of the SAN data, and is configured with an attached DLT tape changer to back up multiple devices according to the backup schedule requirements. Its configuration is described below:

Server model	Compaq DL380 Model DL380R01
Processors	P3 933 MHz/256K cache
Memory	1 GB
Peripherals	• Compaq NC6134 Gigabit NIC 64 PCI 1000SX • Compaq Fibre Channel Host Adapter PCI
Other add-on components	Compaq hot plug redundant power supply module
Hard drives	2 x 9.1 Gb wide pluggable ultra 3 (10K RPM)
Hard drive configuration	One RAID 1 array with two physical drives; one logical drive using full capacity

Other Servers: Separate servers have been set up to provide DHCP and DNS services on the network. The Finance/Accounting, Human Resources and Development groups all have their own designated servers on the network for security reasons.
The DHCP and DNS servers have been "hardened" to restrict access to only the designated services that they will provide.
Access to the Finance/Accounting server (GIAC-CORP-FIN1), the Human Resources server (GIAC-CORP-HR1) and the Development server (GIAC-CORP-DEV1) is restricted through both Active Directory integration of the applications running on the servers, and through network level separation at the firewall.
The servers themselves all have the same basic hardware configurations, described below:

Server model	Compaq DL380 Model DL380R01
Processors	P3 1.0 GHz/256K cache
Memory	1024 Mb
Peripherals	Compaq NC3123 Fast Ethernet NIC 64 PCI 10/100
Other add-on components	Compaq hot plug redundant power supply module
Hard drives	4 x 18.2 Gb wide pluggable ultra 3 (10K RPM)
Hard drive configuration	Two RAID 1 arrays with two physical drives; one logical drive using full capacity

GIAC ENTERPRISES ACTIVE DIRECTORY

FOREST-GIAC.COM

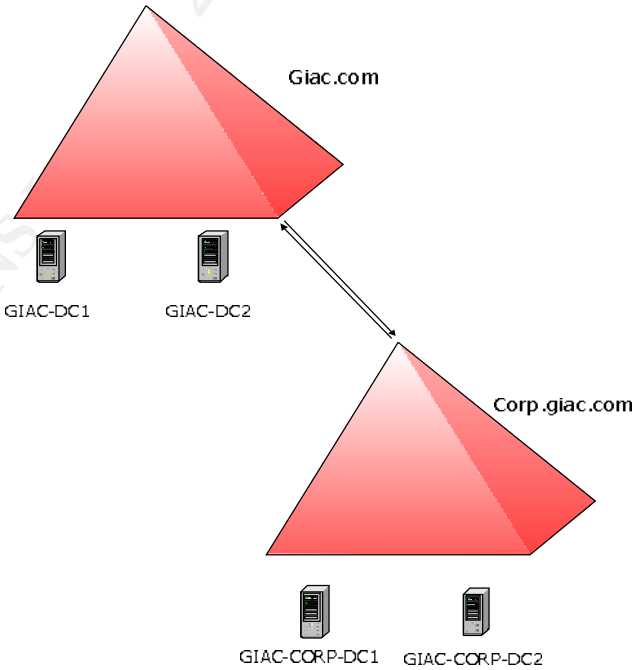
The GIAC Enterprises Active Directory consists of one forest, and therefore one schema. The giac.com forest was created when the server GIAC-DC1 was promoted to domain controller for the giac.com domain.

SITE-HQ

The GIAC Enterprises Active Directory consists of one site, to which all domain controllers belong. The site was created when the server GIAC-DC1 was promoted to domain controller. The original name of the site was DEFAULT-SITE-FIRST-NAME; it was renamed to HQ after GIAC-DC1 was promoted.

DOMAIN TREE – GIAC.COM

The GIAC Enterprises Active Directory consists of two domains in one tree: giac.com and corp.giac.com. Giac.com was the first domain built in the forest and is therefore the root domain. It was created with the promotion of GIAC-DC1 to the role of domain controller.
The relationship of the two domains in the tree and their domain controllers is shown in the following diagram:



Forest - Giac.com

PARENT DOMAIN – GIAC.COM

The giac.com domain is the parent domain in the Active Directory structure. It is an "empty domain" which serves as a placeholder for the child domain, corp.giac.com.

GIAC-DC1

GIAC-DC1 is the first domain controller in the forest. As such, when the server was promoted to domain controller it automatically became a global catalog server and took on the following forest-wide operations master roles:

- Schema Master
- Domain Naming Master

GIAC-DC1 is also the first domain controller in the domain. Therefore, when the server was promoted to domain controller it automatically took on the following domain-wide operation master roles:

- Relative ID (RID) Master
- PDC Emulator
- Infrastructure Master

Because GIAC-DC1 is the PDC emulator at the root of the forest, it is by default the Authoritative Time server for the enterprise. It is configured to gather time from an NTP time server on the Internet for all servers and workstations on the network.

Since global catalog server and infrastructure master are considered to be incompatible roles, the infrastructure master role was transferred to GIAC-DC2 after it was installed.

GIAC-DC1 is also the primary DNS server for the giac.com DNS domain and hosts reverse DNS lookups for the 172.17.x.x subnets. All Windows 2000 servers are configured to point to GIAC-DC1 as the preferred server for DNS resolution.

Communication with other servers in the forest is configured to be handled via IPSec. The local security policy on GIAC-CORP-DC1is configured to use only IPSEC to communicate with those servers.

The table that follows gives general hardware configuration details for the build of this server:

Server model	Compaq DL380 Model DL380R01
Processors	2 x P3 933 MHz/256K cache
Memory	512 MB
Peripherals	Compaq NC3123 Fast Ethernet NIC PCI 10/100 WOL
Other add-on components	Compaq wide ultra2 SCSI drive cage option kit Compaq hot plug redundant power supply module
Hard drives	6 x 36.4 GB wide pluggable ultra 3 (10K RPM)
Hard drive configuration	Three independent RAID 1 arrays with two physical drives in each; one logical drive per array using full capacity
OS version	Windows 2000 Server v5.0.2195
SP version	Service Pack 2

GIAC-DC2

GIAC-DC2 is a replica domain controller in the giac.com domain. It also acts as a DNS server for the giac.com DNS domain and hosts reverse DNS lookups for the 172.17.x.x subnets.
Since global catalog server and infrastructure master are considered incompatible roles, the infrastructure master role was transferred to GIAC-DC2

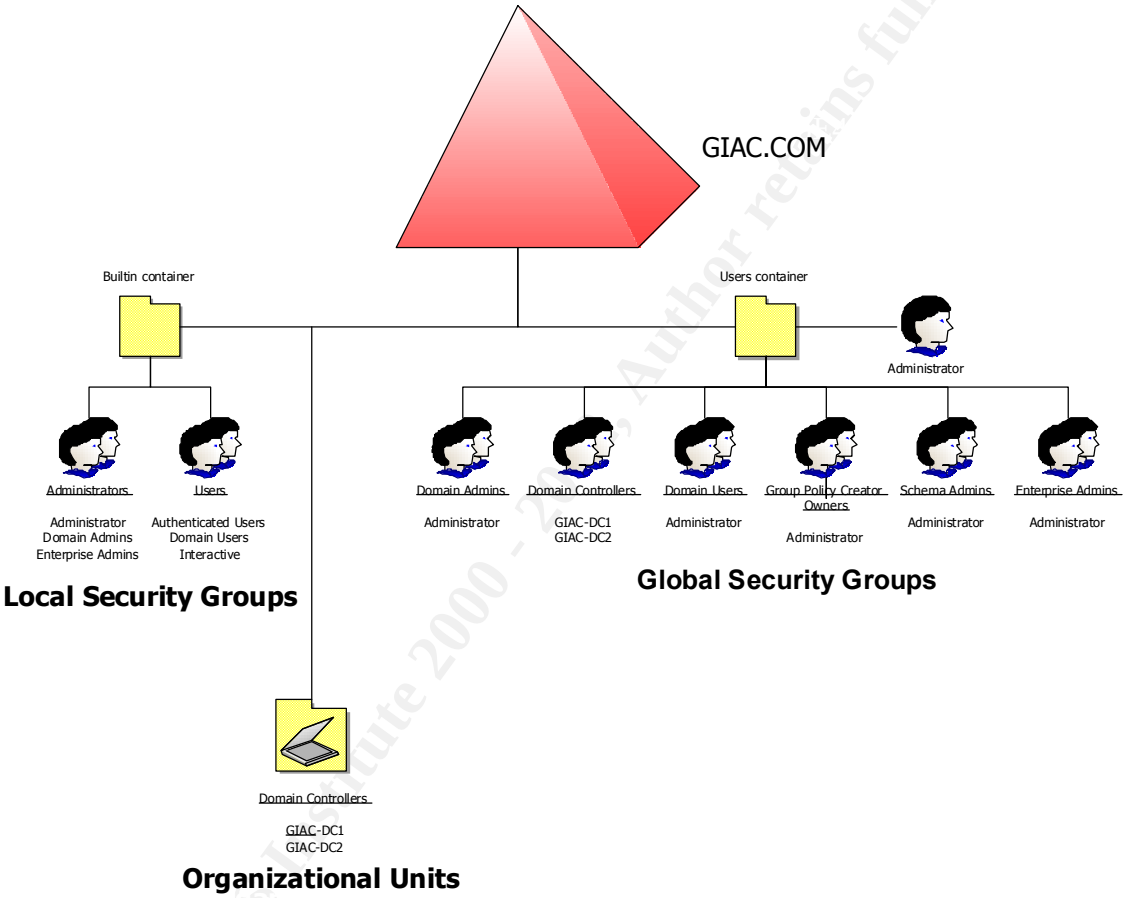
Communication with other servers in the forest is configured to be handled via IPSec. The local security policy on GIAC-DC2 is configured to use only IPSEC to communicate with those servers.

The table that follows gives configuration details for the build of this server:

Server model	Compaq DL380 Model DL380R01
Processors	2 x P3 933 MHz/256K cache
Memory	512 MB
Peripherals	Compaq NC3123 Fast Ethernet NIC PCI 10/100 WOL
Other add-on components	Compaq wide ultra2 SCSI drive cage option kit Compaq hot plug redundant power supply module
Hard drives	6 x 36.4 GB wide pluggable ultra 3 (10K RPM)
Hard drive configuration	Three independent RAID 1 arrays with two physical drives in each; one logical drive per array using full capacity
OS version	Windows 2000 Server v5.0.2195
SP version	Service Pack 2

DOMAIN STRUCTURE

The figure below illustrates the domain structure of giac.com. The Organizational Units and containers depicted below were automatically created by Active Directory when the GIAC-DC1 server was promoted to domain controller.



CONTAINERS

The following are built-in containers in the giac.com domain that contain no objects:

- Computers
- ForeignSecurityPrincipals

By default, all computer accounts other than domain controllers that are added to the domain are placed in the Computers container. However, the giac.com

domain does not contain any computer accounts other than domain controllers. Therefore, the container remains empty.

ORGANIZATIONAL UNITS

The only OU in the giac.com domain is the default Domain Controllers OU. This OU was automatically created when the GIAC-DC1 server was upgraded to be the first domain controller in the domain. All other domain controllers in the domain are automatically placed inside this container when they are created.

GROUP POLICIES

In the giac.com domain, group policy is applied only to the Domain itself and the Domain Controllers Organizational Unit.

Group Policy for the giac.com Domain

The default group policy object that is applied to the domain is called Default Domain Policy. This policy was applied to the domain automatically when the domain was created. The security portion of the policy was then modified to meet GIAC Enterprises' standards. Following are the settings that will be applied to the giac.com domain.

Domain Group Policy – giac.com Domain

Account Policies

Policy	Computer Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 Days
Minimum password length	12 characters
Password must meet complexity Requirements	Enabled
Store Passwords using reversible encryption	Disabled

These settings will have the following results:

- Windows will keep track of the users' last 24 passwords
- Users must reset their passwords every 90 days
- The minimum password age setting (1 day) will prevent users from quickly changing their password 23 times to return to the password previously used.

- The minimum password length and complexity standards ensure that users' passwords are at least twelve characters long and contain characters from three of the following groups – uppercase alpha, lowercase alpha, numeric and special characters.
- Passwords are not stored using reversible encryption.

Account Lockout Policy

Policy	**Computer Setting**
Account lockout duration	480 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	480 minutes

These settings will have the following effect:

- Since the root domain has a higher security requirement, the account lockout duration is set at 8 hours.
- The account lockout threshold is 5 invalid attempts.
- After the account is locked, the reset counter will only be unlocked after 8 hours.

The idea behind this is to prevent a potential hacker from guessing administrator passwords. If an attempt were made, after the 5th incorrect guess, the account would be locked out for 8 hours.

Kerberos Policy

Policy	**Computer Setting**
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

These are the recommended Kerberos policy settings and exist by default.

Group Policy for the Domain Controllers OU

The default group policy object that is applied to the Domain Controllers OU is called Default Domain Controllers Policy. This policy was applied to the OU automatically when the domain was created. The security portion of the policy was then modified to meet GIAC Enterprises' standards. This was accomplished by selecting a predefined Windows 2000 security template file, modifying the template file and importing it into the Default Domain Controllers Policy group policy object. Following are the steps required to complete this task.

DOMAIN CONTROLLER GROUP POLICY – giac.com Domain

The account policies, account lockout policies, and Kerberos policies are defined at the giac.com domain level and therefore are not defined here. Local policies are outlined below.

LOCAL POLICIES

Audit Policy

Policy	Computer Setting
Audit account logon events	Success, Failure
Audit account management events	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Not defined
Audit system events	Success, Failure

The audit policy is set to keep track of all major events on the domain controller. With the noted settings, we will log all successful and failed logons as well as any changes made to accounts on the system. Object access auditing is enabled, but does require that the individual objects have auditing enabled as well if we are to log events.

User Rights Assignment

Policy	Computer Setting
Access this computer from the network	Administrators Authenticated Users Enterprise Domain Controllers
Act as part of the operating system	None
Add workstations to domain	Administrators
Back up files and directories	Backup Operators Administrators

Bypass traverse checking	Authenticated Users
Change the system time	Administrators
Create a pagefile	Administrators
Create a token object	None
Create permanent shared objects	None
Debug programs	None
Deny access to this computer from the network	Not defined
Deny logon as a batch job	Not defined
Deny logon as a service	Not defined
Deny logon locally	Not defined
Enable computer and user accounts to be trusted for delegation	Administrators
Force shutdown from a remote system	Administrators
Generate security audits	Not defined
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	None
Log on as a batch job	None
Log on as a service	None
Log on locally	Administrators
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	None
Replace a process level token	None
Restore files and directories	Administrators
Shut down the system	Administrators
Synchronize directory service data	None
Take ownership of files or other objects	Administrators

As shown in the User Rights Assignment portion of the GPO, Regular users have very limited right on the domain controller. Domain users only have the right to access the computer from the network. The administrators do not have every right on the domain controller. By limiting the Administrators right to those that they need to do their jobs, you create a more secure system. Note that only the Administrators can shutdown the machine, manage security logs, take ownership of files and directories, and add workstations to the domain.

Security Options

Policy	Computer Setting
Additional restrictions for anonymous connections	No Access Without Explicit Permissions
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	15 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	Not defined
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 responses only\Refuse LM & NTLM
Message text for users attempting to log on	
Message title for users attempting to log on	
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
Rename administrator account	Larry Ellison
Rename guest account	Steve Jobs
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
Unsigned driver installation behavior	Warn but Allow Installation
Unsigned non-driver installation behavior	Warn but Allow Installation

Event Log Settings

Policy	Computer Setting
Maximum application log size	10,240 Kilobytes
Maximum security log size	10,240 Kilobytes
Maximum system log size	10,240 Kilobytes
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guess access to system log	Enabled
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Manually
Retention method for security log	Manually
Retention method for system log	Manually
Shutdown the computer when the security audit log is full	Enabled

The above table shows the settings for the event log portion of the GPO. The max log size is 10 MB and events have to be cleared manually when the logs become full. This will allow enough space to store multiple day's worth of events. It is recommended that the event logs not be overwritten to ensure that no important data is lost in the event of a security breach. Guest access is restricted to all logs for obvious reasons.

Services

Service Name	Startup	Permission
Alerter	Disabled	Configured
Application Management	Not defined	Not defined
ClipBook	Disabled	Configured
COM+ Event System	Not defined	Not defined
Computer Browser	Disabled	Configured
DefWatch	Not defined	Not defined
DHCP Client	Disabled	Configured
Distributed Link Tracking Client	Not defined	Not defined
Distributed Transaction Coordinator	Not defined	Not defined
DNS Client	Not defined	Not defined
Event Log	Not defined	Not defined

Fax Service	Disabled	Configured
Indexing Service	Not defined	Not defined
Internet Connection Sharing	Disabled	Configured
IPSEC Policy Agent	Automatic	Configured
License Service	Automatic	Configured
Logical Disk Manager	Not defined	Not defined
Logical Disk Manager Administrative Service	Not defined	Not defined
Messenger	Disabled	Configured
Net Logon	Not defined	Not defined
NetMeeting Remote Desktop Sharing	Disabled	Configured
Network Connections	Not defined	Not defined
Network DDE	Not defined	Not defined
Network DDE DSDM	Not defined	Not defined
NT LM Security Support Provider	Not defined	Not defined
Performance Logs and Alerts	Not defined	Not defined
Plug and Play	Not defined	Not defined
Print Spooler	Disabled	Configured
Protected Storage	Automatic	Configured
QoS RSVP	Not defined	Not defined
Remote Access Auto Connection Manager	Disabled	Configured
Remote Access Connection Manager	Disabled	Configured
Remote Procedure Call (RPC)	Not defined	Not defined
Remote Procedure Call (RPC) Locator	Not defined	Not defined
Remote Registry Service	Disabled	Configured
Removable Storage	Not defined	Not defined
Routing and Remote Access	Disabled	Configured
RunAs Service	Not defined	Not defined
Security Accounts Manager	Not defined	Not defined
Server	Disabled	Configured
Smart Card	Not defined	Not defined
Smart Card Helper	Not defined	Not defined
SMTPSVC	Automatic	Configured
System Event Notification	Not defined	Not defined
Task Scheduler	Automatic	Configured
TCP/IP NetBIOS Helper Service	Not defined	Not defined
Telephony	Disabled	Configured
Telnet	Not defined	Not defined
TermService	Disabled	Configured

The above chart shows the preferred settings for services settings of the GPO. As a means of increasing security, unneeded services are disabled on the domain controller.

Additional settings not addressed in the GPO

Disable Autorun on CD-Rom Drives	Hive: HKEY_LOCAL_MACHINE Key: System\CurrentControlSet\Services\CDRom Value Name: Autorun Type: REG_DWORD Value: 0
Restrict Null User access to Named Pipes	Hive: HKEY_LOCAL_MACHINE Key:System\CurrentControlSet\Services\LanManServer\Parameters Value Name: NullSessionPipes Type: REG_ MULTI_SZ Value: (list of pipe names permitted anonymous registry access)
	Hive: HKEY_LOCAL_MACHINE Key:System\CurrentControlSet\Services\LanManServer\Parameters Value Name: RestrictNullSessAccess Type: REG_DWORD Value: If this value exists and is set to 0, the NullSessionPipes value above is disregarded and null sessions are allowed to all pipes. Thus, in a secure system,RestrictNullSessAccess should either not exist or be set to 1. If this key does not exist, its value is assumed to be 1.
Restrict Null User access to Shares.	Hive: HKEY_LOCAL_MACHINE Key: System\CurrentControlSet\Services\LanManServer\Parameters Value Name: NullSessionShares Type: REG_ MULTI_SZ Value: (list of share names permitted anonymous registry access)
Remove the AEDebug Key.	Hive: HKEY_LOCAL_MACHINE Key: Software\Microsoft\WindowsNT\CurrentVersion\AEDebug Value Name: Debugger
Remove Administrative Shares.	Hive: HKEY_LOCAL_MACHINE Key: System\CurrentControlSet\Services\LanmanServer\Parameters Value Name: AutoShareServer Type: REG_DWORD Value: 0
Disable 8.3 Filename Creation.	Hive: HKEY_LOCAL_MACHINE Key: System\CurrentControlSet\Control\Filesystem Value Name: NTFSDisable8dot3NameCreation Type: REG_DWORD Value: 1

Removing the names of any named pipes makes those pipes inaccessible to anonymous users. Null user access to shares is also restricted. The administrative shares are disabled to remove them as a target for would be hackers.

On the following table are the registry permission settings that will be put in place.

Registry Keys	Audit	Administrator & System	Authenticated Users
HKLM\Software\	S & F	Full Control	Read
HKLM\Software\Classes\helpfile	S & F	Full Control	Read
HKLM\Software\Classes\.hlp	S & F	Full Control	Read
HKLM\Software\Microsoft\Command Processor	S & F	Full Control	Read
HKLM\Software\Microsoft\Cryptography	S & F	Full Control	Read
HKLM\Software\Microsoft\Driver Signing	S & F	Full Control	Read
HKLM\Software\Microsoft\EnterpriseCertficates	S & F	Full Control	Read
HKLM\Software\Microsoft\Non-DriverSigning	S & F	Full Control	Read
HKLM\Software\Microsoft\NetDDE	S & F	Full Control	Read
HKLM\Software\Microsoft\Ole	S & F	Full Control	Read
HKLM\Software\Microsoft\Rpc	S & F	Full Control	Read
HKLM\Software\Microsoft\Secure	S & F	Full Control	Read
HKLM\Software\Microsoft\SystemCertificates	S & F	Full Control	Read
HKLM\Software\Microsoft\Windows\CurrentVersion \Run	S & F	Full Control	Read
HKLM\Software\Microsoft\Windows\CurrentVersion \RunOnce	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\AEDebug	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\AsrCommands	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Classes	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Console	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\DiskQuota	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Drivers32	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Font Drivers	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\FontMapper	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\IniFileMappings	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\PerfLib	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ProfileList	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\SecEdit	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Svchost	S & F	Full Control	Read

HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Time Zones	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Windows	S & F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon	S & F	Full Control	Read
HKLM\Software\Policies	S & F	Full Control	Read
HKLM\System	S & F	Full Control	Read
HKLM\System\CurrentControlSet\Control\Services	S & F	Full Control	Read
HKLM\System\CurrentControlSet\Control\SecurePipeServers\Winreg	S & F	N/A	Everyone=None
HKLM\System\CurrentControlSet\Control\Session Manager\Executive	S & F	Full Control	Read
HKLM\System\CurrentControlSet\Control\TimeZone Information	S & F	Full Control	Read
HKLM\System\CurrentControlSet\Control\WMI\Security	S & F	Full Control	None
HKLM\Hardware	S & F	Full Control	Everyone = Read
HKLM\SAM	S & F	Full Control	Everyone = Read
HKLM\Security	S & F	Full Control	N/A
Hkey_Users (HKU)	S & F	Full Control	N/A
HKU\.Default	S & F	Full Control	Read
HKU\.Default\Software\Microsoft\NetDDE	S & F	Full Control	N/A

On the following pages are the File and Folder GPO settings for the Domain Controller OU. The Group Policy for this OU is designed to ensure that critical system files are not purposely or inadvertently deleted from the domain controllers. Enforcing these restrictions on the file system limits access to sensitive OS directories and files while allowing full functionality required by the administrators and the operating system itself.

Folder and File Permissions Settings

File System Object	User Group	Permissions	Inherit Method
%ProgramFiles%	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Read and Execute Full (subfolders and files) Full Control	Replace
%Program Files%\ResourceKit	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%	Administrators Authenticated Users CREATOR OWNER	Full Read and Execute Full (subfolders	Replace

	SYSTEM	and files) Full Control	
%SystemDirectory%\appmgmt	Admins Authenticated Users SYSTEM	Full Read and Execute Full Control	Propagate
%SystemDirectory%\config	Admins SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\dllcache	Admins CREATOR Owner SYSTEM	Full Control Full Control Full Control	Replace
%SystemDirectory%\DTCLog	Admins Authenticated Users CREATOR Owner SYSTEM	Full Control Read and Execute None Full Control	Propagate
%SystemDirectory%\GroupPolicy	Admins Authenticated Users SYSTEM	Full Control Read and Execute Full Control	Propagate
%SystemDirectory%\ias	Admins CREATOR Owner SYSTEM	Full Control Full Control Full Control	Replace
%SystemDirectory%\Ntbackup.exe	Admins SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\NTMSData	Admins SYSTEM	Full Control Full Control	Propagate
%SystemDirectory%\rcp.exe	Admins SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\regedt32.exe	Admins SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\ReinstallBackups			Ignore
%SystemDirectory%\repl	Admins Authenticated Users SYSTEM	Full Control Read and Execute Full Control	Propagate
%SystemDirectory%\repl\export	Admins Authenticated Users Replicator SYSTEM	Full Control Read and Execute Read and Execute Full Control	Propagate
%SystemDirectory%\repl\import	Admins Authenticated Users Replicator SYSTEM	Full Control Read and Execute Modify Full Control	Propagate
%SystemDirectory%\rexec.exe	Admins SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\rsh.exe	Admins	Full Control	Replace

	SYSTEM	Full Control	
%SystemDirectory%\secedit.exe	Admins SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\Setup	Admins Authenticated Users SYSTEM	Full Control Read and Execute Full Control	Propagate
%SystemDirectory%\spool\printers	Admins Authenticated Users CREATOR OWNER SYSTEM	Full Control Travers Folder, Read attributes, Read extended attributes, Create files, Create folders Full Control Full Control	Replace
%SystemDrive%	Admins Authenticated Users Replicator SYSTEM	Full Control Read and Execute Full Control Full Control	Propagate
%SystemDrive%\autoexec.bat	Admins SYSTEM Users	Full Control Full Control Read and Execute	Replace
%SystemDrive%\boot.ini	Admins SYSTEM	Full Control Full Control	Replace
%SystemDrive%\config.sys	Admins SYSTEM Users	Full Control Full Control Read and Execute	Replace
%SystemDrive%\Documents and Settings	Admins Authenticated Users SYSTEM	Full Control Read and Execute Full Control	
%SystemDrive%\Documents and Settings\Administrator	Admins SYSTEM	Full Control Full Control	Replace
%SystemDrive%\Documents and Settings\All Users	Admins Authenticated Users SYSTEM	Full Control Read and Execute Full Control	Propagate
%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson	Admins Authenticated Users CREATOR OWNER	Full Control Read and Execute (Subfolders and files only: Travers Folder, Create files, Create folders) Full Control (Subfolders and	Replace

	SYSTEM	files) Full Control	
%SystemDrive%\Documents and Settings\All Users\Documents \DrWatson\drwtsn32.log	Admins Authenticated Users CREATOR OWNER SYSTEM	Full Control Modify Full Control Full Control	Replace
%SystemDrive%\Documents and Settings\Default User	Admins Authenticated Users SYSTEM	Full Control Read and Execute Full Control	Replace
%SystemDrive%\IO.SYS	Admins Authenticated Users SYSTEM	Full Control Read and Execute Full Control	Replace
%SystemDrive%\MSDOS.SYS	Admins Authenticated Users SYSTEM	Full Control Read and Execute Full Control	Replace
%SystemDrive%\My Download Files	Admins Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write and Execute Full Control Full Control	Replace
%SystemDrive%\ntdetect.com	Admins SYSTEM	Full Control Full Control	Replace
%SystemDrive%\ntldr	Admins SYSTEM	Full Control Full Control	Replace
%SystemDrive%\Program Files\Resource Kit	Admins SYSTEM	Full Control Full Control	Replace
%SystemDrive%\System Volume Information			Ignore
%SystemDrive%\Temp	Admins Authenticated Users CREATOR OWNER SYSTEM	Full Control Read and Execute (This folder and subfolders: Travers Folder, Create files, Create folders) Full Control (Subfolders and files only) Full Control	Replace
%SystemRoot%	Admins Authenticated Users CREATOR OWNER SYSTEM	Full Control Read and Execute Full Control (Subfolders and files only) Full Control	Replace
%SystemRoot%\$NtServicePackUninstall$	Admins SYSTEM	Full Control Full Control	Replace

%SystemRoot%\CSC	Admins SYSTEM	Full Control Full Control	Replace
%SystemRoot%\debug	Admins Authenticated Users CREATOR OWNER SYSTEM	Full Control Read and Execute Full Control (Subfolders and files only) Full Control	Propagate
%SystemRoot%\debug\UserMode	Admins Authenticated Users SYSTEM	Full Control This folder only: Travers Folder, List folder, Create files Files only: Travers Folder, Write Data, Append data Full Control	Propagate
%SystemRoot%\NTDS	Admins SYSTEM	Full Control Full Control	Propagate
%SystemRoot%\Offline Web Pages			Ignore
%SystemRoot%\Program Files\Resource Kit	Admins SYSTEM	Full Control Full Control	Replace
%SystemRoot%\Program Files\Resource Pro Kit	Admins SYSTEM	Full Control Full Control	Replace
%SystemRoot%\regedit.exe	Admins SYSTEM	Full Control Full Control	Replace
%SystemRoot%\Registration	Admins Authenticated Users SYSTEM	Full Control Read Full Control	Propagate
%SystemRoot%\repair	Admins SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\ipconfig.exe	Admins DHCP Admins SYSTEM	Full Control Full Control Full Control	Replace
%SystemRoot%\system32\netsh.exe	Admins DHCP Admins SYSTEM	Full Control Full Control Full Control	Replace
%SystemRoot%\security	Admins CREATOR OWNER SYSTEM	Full Control Full Control (Subfolders and files only) Full Control	Replace
%SystemRoot%\Tasks			Ignore
%SystemRoot%\Temp	Admins Authenticated Users	Full Control This folder and subfolders: Travers Folder, Create files,	Replace

	CREATOR OWNER SYSTEM	Create folders Full Control (Subfolders and files only) Full Control	
c:\cmdcons	Admins SYSTEM	Full Control Full Control	Replace
c:\autoexec.bat	Admins Authenticated Users SYSTEM	Full Control Read and Execute Full Control	Replace
c:\boot.ini	Admins SYSTEM	Full Control Full Control	Replace
c:\config.sys	Admins Authenticated Users SYSTEM	Full Control This folder only: Execute File, Read data, Read attributes, read extended attributes, Read permissions Full Control	Replace
c:\ntbootdd.sys	Admins SYSTEM	Full Control Full Control	Replace
c:\ntdetect.com	Admins SYSTEM	Full Control Full Control	Replace
c:\ntldr	Admins SYSTEM	Full Control Full Control	Replace

ACTIVE DIRECTORY USER AND GROUP ACCOUNTS

The only user account that is active in giac.com is the built-in Administrator account. This is the only account that can be used to make forest-wide changes. For security purposes, this account has been renamed and a strong password applied to it; the password changes every 30 days and is maintained by authorized personnel. The only active group accounts in the domain are those automatically created by Active Directory during installation. These include the local groups Administrators and Users and the global groups Domain Admins, Domain Controllers, Domain Users, Group Policy Creator Owners, Schema Admins, and Enterprise Admins.

INACTIVE USER AND GROUP ACCOUNTS

The following are built-in user accounts in the giac.com domain that are disabled:

- Guest (disabled by default and renamed for security reasons)

- Krbtgt (disabled by default; special account that is not used to log in)
- TsInternetUser (disabled by choice for security reasons)

The following are built-in local security groups in the giac.com domain that either contain no user accounts or only disabled user accounts:

- Builtin\Account Operators
- Builtin\Backup Operators
- Builtin\Guests
- Builtin\Pre-Windows 2000 Compatible Access
- Builtin\Print Operators
- Builtin\Replicator
- Builtin\Server Operators
- Users\DNSAdmins
- Users\RAS and IAS Servers

The following are built-in global security groups in the giac.com domain that either contain no user accounts or only disabled user accounts:

- Users\Cert Publishers
- Users\DnsUpdateProxy
- Users\Domain Computers
- Users\Domain Guests

CHILD DOMAIN – CORP.GIAC.COM

The corp.giac.com domain is a child domain in the Active Directory structure. It serves as a context for the corporate office workstations and users. The two domain controllers that serve this domain are GIAC-CORP-DC1 and GIAC-CORP-DC2. The domain operation mode was changed from mixed mode to native mode after the installation of the domain controllers. The Domain Prep utility was run after the domain was created in order to prepare for the installation of Microsoft Exchange 2000 Servers in the domain.

GIAC-CORP-DC1

WIN-CORP-DC1 is the first domain controller in the domain. As such, when the server was promoted to domain controller it automatically took on the following domain-wide operation master roles:

- Relative ID Master
- PDC Emulator
- Infrastructure Master

GIAC-CORP-DC1 was also promoted to Global Catalog server. Since Global Catalog server and Infrastructure Master are considered incompatible roles, the Infrastructure Master role was transferred to GIAC-CORP-DC2.

GIAC-CORP-DC1 is a DNS server for the corp.giac.com DNS domain and hosts reverse DNS lookups for the 172.17.x.x subnets. Authority for this domain was delegated to GIAC-CORP-DC1 from the GIAC-DC1 server.

Communication with other servers in the forest is configured to be handled via IPSec. The local security policy on GIAC-CORP-DC1 is configured to use only IPSEC to communicate with those servers.
Below is the hardware configuration of the server:

Server model	Compaq DL380 Model DL380R01
Processors	2 x P3 933 MHz/256K cache
Memory	512 MB
Peripherals	Compaq NC3123 Fast Ethernet NIC PCI 10/100 WOL
Other add-on components	Compaq wide ultra2 SCSI drive cage option kit Compaq hot plug redundant power supply module
Hard drives	6 x 36.4 GB wide pluggable ultra 3 (10K RPM)
Hard drive configuration	Three independent RAID 1 arrays with two physical drives in each; one logical drive per array using full capacity
OS version	Windows 2000 Server v5.0.2195
SP version	Service Pack 2

GIAC-CORP-DC2

GIAC-CORP-DC2 is a replica domain controller in the corp.giac.com domain. GIAC-CORP-DC2 also acts as a DNS server for the corp.giac.com DNS domain and hosts reverse DNS lookups for the 172.17.x.x subnets. Authority for this domain was delegated to GIAC-CORP-DC2 from the GIAC-DC1 server.

GIAC-CORP-DC2 was also promoted to Global Catalog server.

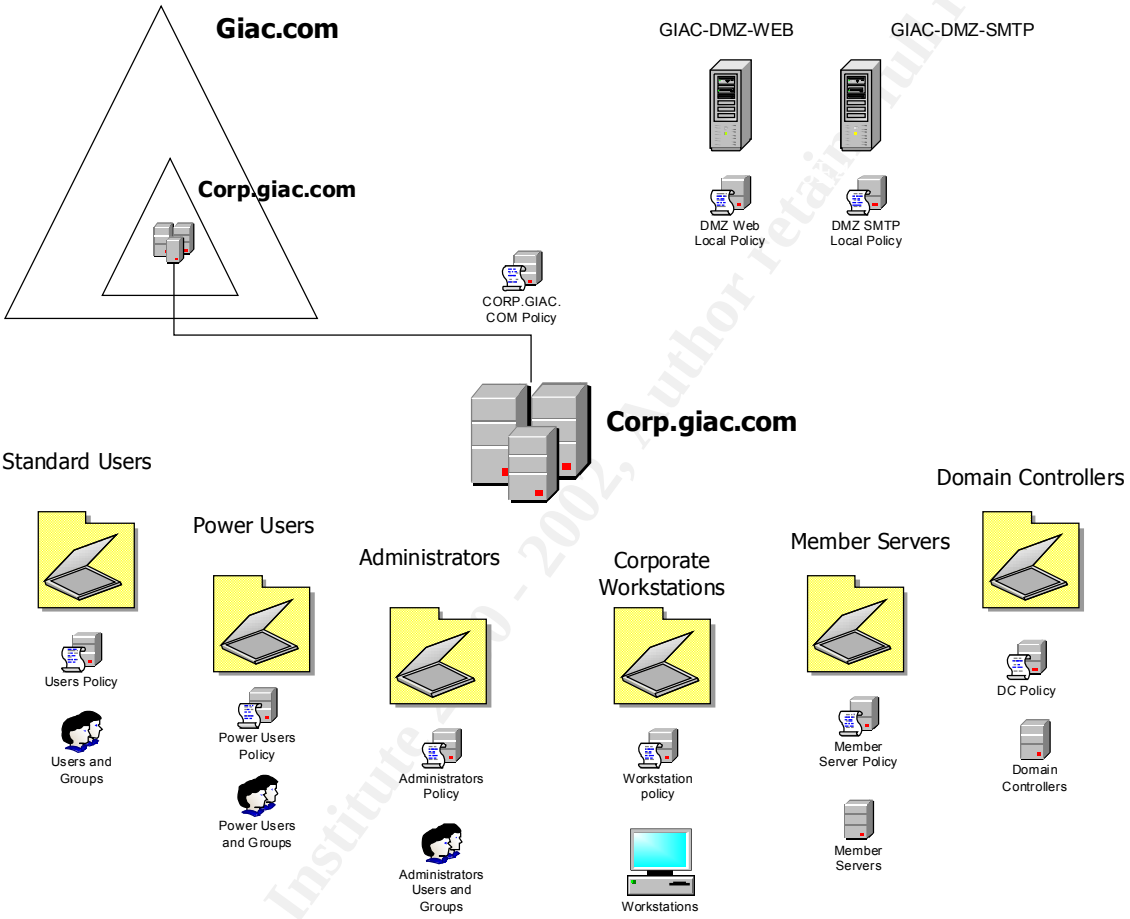
Communication with other servers in the forest is configured to be handled via IPSec. The local security policy on GIAC-CORP-DC2 is configured to use only IPSEC to communicate with those servers.

Below is the hardware configuration of the server:

Server model	Compaq DL380 Model DL380R01
Processors	2 x P3 933 MHz/256K cache
Memory	512 MB
Peripherals	Compaq NC3123 Fast Ethernet NIC PCI 10/100 WOL
Other add-on components	Compaq wide ultra2 SCSI drive cage option kit Compaq hot plug redundant power supply module
Hard drives	6 x 36.4 GB wide pluggable ultra 3 (10K RPM)
Hard drive configuration	Three independent RAID 1 arrays with two physical drives in each; one logical drive per array using full capacity
OS version	Windows 2000 Server v5.0.2195
SP version	Service Pack 2

Active Directory Diagram – corp.giac.com

Shown below is the Active Directory layout of the giac.com enterprise, detailing the corp.giac.com domain, its containers and OU's.



The intent behind the Active Directory design for GIAC Enterprises is to create a secure environment and to make administration of the environment as simple and logical as possible.

Default Domain Policy – corp.giac.com

A default domain policy exists at the corp.giac.com level. This policy basically defines user account policies, (including passwords), lockout parameters, and Kerberos Policies. They are not as stringent as the policies set for the giac.com domain because the policy would affect corporate user accounts. For example, the length requirement for passwords has been shortened and the password history threshold decreased.

Account Policies

Policy	Computer Setting
Enforce password history	8
Maximum password age	90 days
Minimum password age	1
Minimum password length	8 characters
Password must meet complexity Requirements	Enabled
Store Passwords using reversible encryption	Disabled

Account Lockout Policy

Policy	Computer Setting
Account lockout duration	480 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	480 minutes

Kerberos Policy

Policy	Computer Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Group Policy for the Domain Controllers OU

The default group policy object that is applied to the Domain Controllers OU is called Default Domain Controllers Policy. This policy was applied to the OU automatically when the domain was created. The security portion of the policy was then modified to meet GIAC Enterprises' standards. This was accomplished by selecting a predefined Windows 2000 security template file, modifying the template file and importing it into the Default Domain Controllers Policy group policy object. Following are the steps required to complete this task.

DOMAIN CONTROLLER GROUP POLICY – corp.giac.com Domain

Once again the account policies, account lockout policies and Kerberos policies are defined at the corp.giac.com domain level. The policies for the corp.giac.com Domain Controllers OU are identical to the settings defined in the giac.com Domain Controllers OU Group Policy, and therefore are justified for the same reasons.

Group Policy for the Member Servers OU

The security portion of this policy has been modified to meet GIAC Enterprises' standards from a predefined Windows 2000 security template file. The template was then imported into the Member Servers Policy group policy object. Following are the steps required to complete this task.

MEMBER SERVERS GROUP POLICY – corp.giac.com Domain

The following policies closely resemble the policy settings for the corp.giac.com domain controller OU, and therefore are justified for the same reasons.

LOCAL POLICIES

Audit Policy

Policy	Computer Setting
Audit account logon events	Success, Failure
Audit account management events	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Not defined
Audit system events	Success, Failure

The audit policy is set to keep track of all major events on the member servers. With the noted settings, we will log all successful and failed logons as well as any changes made to accounts on the system. Object access auditing is enabled, but does require that the individual objects have auditing enabled as well if we are to log events.

Shown below are the GPO settings that **differ** from the Domain Controller GPO settings defined previously in the document. All other settings for the Member Server OU group policy are considered to be identical to those defined for the Domain Controller OU group policy.

User Rights Assignment

Policy	Computer Setting
Access this computer from the network	Administrators Users
Bypass traverse checking	Users

Workstation OU Policy

On the following table are the User Rights Assignments and File and Folder GPO settings for the Workstation OU that **differ** from the settings defined on the corp.giac.com Domain Controller OU policy. Settings not explicitly defined below are considered to be identical to settings in the Domain Controller OU group policy.

User Rights Assignment

Policy	Computer Setting
Access this computer from the network	Administrators Users
Bypass traverse checking	Users
Enable computer and user accounts to be trusted for delegation	None
Log on locally	Administrators Users
Manage auditing and security log	Administrators
Remove computer from docking station	Administrators Users
Replace a process level token	None
Shut down the system	Administrators Users

Corp Admin OU Policy

On the following pages are the GPO settings for the Corp Admin OU. The Group Policy for this OU is less restrictive than the group policy in effect on the Power Users OU or the Users OU because the administrator accounts require greater flexibility and a higher level of access to the systems.

User Configuration	Setting
Windows Settings	
Internet Explorer Maintenance	
Programs	
HTML editor E-mail Newsgroups Internet Call Calendar Contact List	None Microsoft Outlook Microsoft Outlook None Microsoft Outlook Microsoft Outlook
Administrative Templates	
Windows Components	
NetMeeting	
Application Sharing	
Audio & Video	
Options Page	
Internet Explorer	(Configured via IEAK)
Windows Explorer	
Microsoft Management Console	
Task Scheduler	
Windows Installer	
Start Menu & Taskbar	
Add logoff to the Start Menu	Enabled
Gray unavailable Windows Installer programs Start Menu shortcuts	Enabled
Desktop	
Prohibit user from changing My Documents path	Enabled
Active Directory	
Active Desktop	
Control Panel	
Add/Remove Programs	
Display	
Printers	
Default Active Directory path when searching for printers	Enabled;LDAP://DC=corp,DC=giac,DC=com
Regional Options	
Network	
Offline Files	
Disable user configuration of Offline Files	Enabled
Synchronize all offline files before logging off	Enabled

Disable "Make Available Offline"	Enabled
Prevent use of Offline Files Folder	Enabled
System	
Don't display welcome screen at logon	Enabled
Logon/Logoff	
Limit profile size	Enabled; 30 MB
Group Policy	Not configured

Corp Power Users OU Policy

On the following pages are the GPO settings for the Corp Power Users OU. The Group Policy for this OU is less restrictive than the group policy in effect on the Users OU because the administrator's day-to-day logon accounts require greater flexibility and a higher level of access to the systems. The Research and Development User accounts and IT Help Desk staff accounts also exist in the Power Users OU.

User Configuration	**Setting**
Windows Settings	
Internet Explorer Maintenance	
Programs	
HTML editor	None
E-mail	Microsoft Outlook
Newsgroups	Microsoft Outlook
Internet Call	None
Calendar	Microsoft Outlook
Contact List	Microsoft Outlook
Administrative Templates	
Windows Components	
NetMeeting	
Application Sharing	
Audio & Video	
Options Page	
Internet Explorer	(Configured via IEAK)
Windows Explorer	
Microsoft Management Console	
Restrict the user from entering author mode	Enabled
Task Scheduler	
Windows Installer	
Start Menu & Taskbar	
Disable and Remove links to Windows Update	Enabled
Add logoff to the Start Menu	Enabled
Gray unavailable Windows Installer programs Start Menu shortcuts	Enabled
Desktop	
Prohibit user from changing My Documents path	Enabled

Active Directory	
Active Desktop	
Control Panel	
Add/Remove Programs	
Display	
Printers	
Default Active Directory path when searching for printers	Enabled;LDAP://DC=corp,DC=giac,DC=com
Regional Options	
Network	
Offline Files	
Disable user configuration of Offline Files	Enabled
Synchronize all offline files before logging off	Enabled
Disable "Make Available Offline"	Enabled
Prevent use of Offline Files Folder	Enabled
System	
Don't display welcome screen at logon	Enabled
Disable registry editing tools	Enabled
Logon/Logoff	
Limit profile size	Enabled; 90 MB
Group Policy	Not configured

Corp Users OU Policy

On the following pages are the GPO settings for the Corp Users OU. The Group Policy for this OU is a more restrictive policy to enable administrator to limit the ability of standard users to modify their system configuration. This is done because a reasonably managed environment can help to limit the number of trouble calls that Help Desk personnel must deal with on a daily basis, thus lowering the total cost involved in managing the network.

User Configuration	**Setting**
Windows Settings	
Internet Explorer Maintenance	
Programs	
HTML editor E-mail Newsgroups Internet Call Calendar Contact List	None Microsoft Outlook Microsoft Outlook None Microsoft Outlook Microsoft Outlook
Administrative Templates	
Windows Components	
NetMeeting	
Application Sharing	
Audio & Video	
Options Page	
Internet Explorer	(Configured via IEAK)

Windows Explorer	
Remove the Folder Options menu item from the Tools menu	Disabled
Remove File menu from Windows Explorer	Disabled
Remove "Map Network Drive" and "Disconnect Network Drive"	Enabled
Remove Search button from Windows Explorer	Disabled
Hides the Manage item on the Windows Explorer context menu	Enabled
Only allow approved Shell extensions	Enabled
Hide these specified drives in My Computer	Disabled
Prevent access to drives from My Computer	Disabled
Hide Hardware tab	Enabled
Disable UI to change menu animation setting	Enabled
Disable DFS tab	Enabled
No "Entire Network" in My Network Places	Enabled
Maximum number of recent documents	Disabled
Do not request alternate credentials	Enabled
Common Open File Dialog	
Hide the common dialog places bar	Enabled
Microsoft Management Console	
Restrict the user from entering author mode	Enabled
Restrict users to the explicitly permitted list of snap-ins	Enabled
Restricted / Permitted snap-ins	
Active Directory Users and Computers	Enabled
Task Scheduler	
Hide Property pages	Enabled
Prevent Task Run or End	Enabled
Disable Drag-and-Drop	Enabled
Disable New Task Creation	Enabled
Disable Task Delegation	Enabled
Disable Advanced Menu	Enabled
Prohibit Browse	Enabled
Windows Installer	
Disable media source for any install	Enabled
Start Menu & Taskbar	
Remove user's folders from the Start Menu	Enabled
Disable and Remove links to Windows Update	Enabled
Remove common program groups from Start Menu	Disabled
Remove Documents from Start Menu	Disabled
Remove Network and Dial-Up Connections from Start Menu	Enabled
Remove Favorites menu from Start Menu	Disabled
Remove Search menu from Start Menu	Disabled
Remove Help menu from Start Menu	Disabled
Remove Run menu from Start Menu	Disabled
Add logoff to the Start Menu	Enabled
Disable drag-and-drop context menus on the Start Menu	Disabled
Disable changes to Taskbar and Start Menu Settings	Disabled

Disable context menu for taskbar	Disabled
Do not keep history of recently opened documents	Disabled
Clear history of recently opened documents on exit	Disabled
Disable personalized menus	Enabled
Gray unavailable Windows Installer programs Start Menu shortcuts	Enabled
Desktop	
Hide My Network Places icon on desktop	Enabled
Hide Internet Explorer icon on desktop	Disabled
Do not add shares from recently opened documents to the My Network Places folder	Enabled
Prohibit user from changing My Documents path	Enabled
Disable adding, dragging, dropping and closing the Taskbar's toolbars	Disabled
Disable adjusting desktop toolbars	Disabled
Don't save settings at exit	Disabled
Active Directory	
Active Desktop	
Disable Active Desktop	Enabled
Control Panel	
Disable Control Panel	Disabled
Show only specified Control Panel applets	Enabled; accessibility options, add/remove programs, display, folder options, internet options, keyboard, mouse, power options, printers, regional options
Add/Remove Programs	
Disable Add/Remove Programs	Disabled
Hide the "Add a program from CD-ROM or floppy disk" option	Enabled
Hide the "Add programs from Microsoft" option	Enabled
Display	
Disable Display in Control Panel	Disabled
Activate Screen saver	Enabled
Screen saver executable name	Disabled
Screen saver timeout	Enabled
Printers	
Disable deletion of printers	Disabled
Disable addition of printers	Disabled
Default Active Directory path when searching for printers	Enabled;LDAP://DC=corp,DC=giac,DC=com
Regional Options	
Network	
Offline Files	
Disable user configuration of Offline Files	Enabled
Disable "Make Available Offline"	Enabled
Prevent use of Offline Files Folder	Enabled
Network and Dial-up Connections	
Prohibit deletion of RAS connections	Enabled

	Prohibit deletion of RAS connections available to all users	Enabled
	Prohibit connecting and disconnecting a RAS connection	Enabled
	Prohibit enabling/disabling a LAN connection	Enabled
	Prohibit access to properties of a LAN connection	Enabled
	Prohibit access to current user's RAS connection properties	Enabled
	Prohibit access to properties of RAS connections available to all users	Enabled
	Prohibit renaming LAN connections or RAS connections available to all users	Enabled
	Prohibit renaming of RAS connections belonging to the current user	Enabled
	Prohibit adding and removing components for a LAN or RAS connection	Enabled
	Prohibit enabling/disabling components of a LAN connection	Enabled
	Prohibit access to properties of components of a LAN connection	Enabled
	Prohibit access to properties of components of a RAS connection	Enabled
	Prohibit access to the Network Connection wizard	Enabled
	Prohibit viewing of status statistics for an active connection	Enabled
	Prohibit access to the Dial-up Preferences item on the Advanced menu	Enabled
	Prohibit access to the Advanced Settings item on the Advanced menu	Enabled
	Prohibit configuration of connection sharing	Enabled
	Prohibit TCP/IP advanced configuration	Enabled
	Prohibit deletion of RAS connections	Enabled
System		
	Don't display welcome screen at logon	Enabled
	Disable the command prompt	Enabled
	Disable registry editing tools	Enabled
	Disable Autoplay	Disabled
Logon/Logoff		
	Disable Task Manager	Disabled
	Limit profile size	Enabled; 90 MB
Group Policy		

Local Policy on DMZ Servers

On the following pages are the configuration settings for the web server, GIAC-DMZ-WEB and the mail forwarding server GIAC-DMZ-SMTP.

As noted earlier, the servers located in the DMZ are not part of the Active Directory. This will insure that the internal Active Directory cannot be compromised in any way even if an intruder accesses any of the servers in the DMZ.

Following is an overview of the steps taken to harden the DMZ servers through the use of local policies on servers that are not managed through the use of Active Directory group policies, along with a few of the most important security considerations for web servers placed in a DMZ.

The GIAC-DMZ-WEB web server provides static web content to Internet users regarding GIAC Enterprises. The GIAC-DMZ-SMTP mail forwarder

First, the Secure Microsoft IIS Server Security Template (hisecweb.inf) is applied to the **local policy** of the web server.

In order to maintain consistency with the servers that exist in Active Directory, all of the **domain level policies** that were defined in the corp.giac.com Active Directory domain have been mirrored on the local web server policies.

Other important considerations for a hardening a web server in your DMZ:

1. Shut off all unnecessary services. This will prevent all known and unknown vulnerabilities in unused services from being exploited. The following services should be turned off or disabled:
    i. Alerter
    ii. ClipBook Server
    iii. Computer Browser
    DHCP Client
    Distributed File System
    iv. Distributed Link Tracking Client
    v. Distributed Link Tracking Server
    vi. DNS Client
    vii. Fax Service
    viii. File Replication
    ix. FTP Publishing Services
    x. Indexing Service

xi. Internet Connection Sharing
xii. IPSec Policy Agent
xiii. Messenger
xiv. NetLogon
xv. NetMeeting Remote Desktop Sharing
xvi. Network DDE
xvii. Network DDE DSDM
xviii. Network Monitor Agent
xix. NNTP Service
xx. Print Spooler
xxi. QoS RSVP
xxii. Remote Access Auto Connection Manager
xxiii. Remote Registry Service
xxiv. Removable Storage
xxv. RunAs Service
xxvi. Server Service (except on SMTP server)
xxvii. Simple TCP/IP Services
xxviii. Smart Card
xxix. Smart Card Helper
xxx. SMTP Service (except on SMTP server)
xxxi. Task Scheduler
xxxii. TCP/IP NetBIOS Helper Service
xxxiii. Telnet
xxxiv. Uninterruptible Power Supply
xxxv. WMI
xxxvi. WMI Driver Extensions
xxxvii. Windows Time
xxxviii. Workstation Service

2. It has been verified that Iuser_machinename and Iwam_machinename are not part of any privileged groups.
3. The default web site has been deleted and a new default site created.
4. Indexing of the Scripts folder, directory browsing in the Site Property sheet and parent paths in scripts have been disabled.
5. Unnecessary application subsystems have been removed. None of these subsystems are typically used and could be used to exploit your system. To do this, remove the following registry keys:
   HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\Os2
   HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\Posix
   Delete the value named:
   HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\Os2LibPath
   Delete all the Sub-Keys underneath:
   HKLM\SOFTWARE\Microsoft\OS/2 Subsystem for NT\

6. As a means of protection against SYN flooding, the SynAttackProtect registry value has been changed:
   HKLM\SYSTEM\CurrentControlSet\Services\TcpIp\Parameters\SynAttackProtect=2
7. Internet printing has been disabled. All unused ISAPI filters and network bindings have been removed. The URLSCAN.DLL ISAPI filter has been installed and configured to reject requests which appear to be threatening or invalid.
8. Auditing has been enabled for all failed and successful attempts except for successful events in Directory Service Access, Process Tracking and System Events.
9. NTFS auditing has been enabled to log all failed actions by the Everyone group.

All other specific settings in line with the recommended configuration for web server security defined in Appendix F of the SANS course book "Securing Internet Information Server 5.0" have been implemented as well.

Windows 2000 SP2 has been installed and all of the latest updates and security patches have been downloaded from windowsupdate.microsoft.com and security.microsoft.com. The IIS Lockdown Tool has been used to protect against known vulnerabilities.

The firewall will limit outside Internet access to the DMZ by allowing only access to HTTP and SMTP traffic.

CONCLUSION

Implementing a secure network for even a smaller company is a complicated procedure, with far-reaching implications for the business if there is a connection to the Internet. Security procedures are implemented at every level, from physical site security, to hardware redundancy to ensure availability, to higher level operating system security.
Active Directory provides the framework within which extensive layers of security can be defined, but if these security measures are not carefully planned, or are layered too deeply, administration can become more complicated than the business requires. The ability to delegate rights for users to very specific fields of Active Directory objects can help with the administration of many tasks that were previously an administrator's responsibility.
This paper has outlined the most important settings required to configure a secure Windows 2000 based network, but there are many other Group Policy and network settings that could be utilized to leverage Active Directory's security capabilities. In addition to a well designed Active Directory and associated Group Policy settings, a secure Windows 2000 network requires:

- Company policies, known to the user population, that define what is considered "appropriate use" of company resources.
- Well-defined server and network change configuration policies to mitigate the possibility of unintentional downtime.
- Clearly defined and tested recovery procedures for disasters.
- Appropriate levels of physical site security.
- Vigilance on the part of security administrators to current threats.
- A documented and followed auditing practice (log reviews, etc).
- The creation of baseline server builds that represent secure, locked-down configurations of all the public and private servers within the organization.
- Disabling of **all** unnecessary services on GIAC Enterprises servers and workstations.
- Detailed documentation and testing of all network related devices and settings.
- Scheduled audits and penetration testing.

This is not meant to be a complete and exhaustive set of security measures for a Windows 2000 network. There are many other configuration changes that could be implemented on a network depending on business needs. However, for the network and the business model described, the measures taken in this paper are appropriate. They fit the security needs of the company and provide for high availability without creating an overly complex and unmanageable system for administrators.

References:

1. Fossen, Jason. (1 June 2001) Securing Windows 2000 (Books 5.1 – 5.5). SANS Institute; June 2001
2. National Security Agency. (April 19, 2001) "Microsoft Windows 2000 Network Architecture Guide" v.1.0 Security Recommendation Guides // National Security Agency, http://nsa1.www.conxion.com (5 February 2002)
3. National Security Agency. (January 22, 2002) "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set" v.1.1 Security Recommendation Guides // National Security Agency, http://nsa1.www.conxion.com (5 February 2002)
4. National Security Agency. (December 2000) "Guide to Securing Microsoft Windows 2000 Active Directory" v.1.0 Security Recommendation Guides // National Security Agency, http://nsa1.www.conxion.com (5 February 2002)
5. National Security Agency. (April 9, 2001) "Guide to Securing Microsoft Windows 2000 DNS" v.1.0 Security Recommendation Guides // National Security Agency, http://nsa1.www.conxion.com (5 February 2002)
6. Shawgo, Jeff, ed. Securing Windows 2000 Step by Step, Version 1.5. SANS Institute, 1 July 2001
7. Schmidt, Jeff. Microsoft Windows 2000 Security Handbook. QUE Publishing; August 2000; ISBN: 0-7897-1999-1.
8. Govanus, Gary; King, Robert. Windows 2000 Network Security Design Study Guide. Sybex; ISBN: 0-7821-2758-4.
9. Russel, Charlie; Crawford, Sharon. Windows 2000 Server Administrators Companion. Microsoft Press; January 2000; ISBN: 1-57231-819-8.
10. Microsoft Corporation. Windows 2000 Server Resource Kit. Microsoft Press; January 2000; ISBN: 1-57231-805-8.
11. Minasi, Mark.; Anderson, Christa; [and others]. Mastering Windows 2000 Server, 2nd Ed. Sybex; February 2000; ISBN: 0-7821-2774-6.
12. Microsoft Corporation. (2001) "Windows 2000 Server Baseline Security Checklist", Microsoft TechNet, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/w2ksvrcl.asp (9 December 2001)
13. Microsoft Corporation. (2001) "IIS 5.0 Baseline Security Checklist", Microsoft TechNet, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/iis5cl.asp (9 December 2001)

14. SANS Institute. (15 November 2001) "The Top Twenty Most Critical Internet Security Vulnerabilities: The Experts' Consensus", v.2.501, SANS Institute Resources, http://www.sans.org/top20.htm (10 December 2001)

15. Microsoft Corporation. (2002) "Windows 2000 Active Directory FSMO Roles (Q197132)", Microsoft http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q197132&

16. Microsoft Corporation. (2002) "FSMO Placement and Optimization on windows 2000 Domain Controllers (Q223346)", Microsoft http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q223346&