Global Information Assurance Certification Paper

GIAC Windows Security Administrator Practical

Windows 2000 Security for a Manufacturing Enterprise

Version 3.1
May 2002

By Jon M. Brage

October 8, 2002

GIAC Windows Security Administrator Practical
Part 1 – A Description of GIAC Enterprises

ABSTRACT

This is a practical for the GIAC Windows Security Administration Certification, Version 3.1 dated April 8, 2002 (Option 1). This practical outlines the design of a Windows 2000 Network for a fictional re-manufacturing business, called GIAC Enterprises.

GIAC Enterprises – A Description

GIAC Enterprises is an ISO 9001/9002 certified business that repairs, refurbishes and re-manufactures critical electro-mechanical infrastructure components (e.g., large electrical generation components, manufacturing equipment, etc.) for governments and businesses. Physically, GIAC Enterprises is located on a 10 building wholly owned campus. This campus is a gated facility employing physical security through guards and closed circuit television monitoring of the perimeter. Personnel can only access the campus guarded gates or via turnstiles activated only by using GIAC Enterprises badges swiped through a badge reader. All employees must wear their GIAC Enterprises badges at all times when on campus or when working at off-site locations in an official work capacity.

Business Operations

GIAC Enterprises repairs, overhauls and refurbishes critical complex electro-mechanical infrastructure components for governments and businesses either at the customer's site or within the GIAC Campus. All repair work is performed to written procedures and all deviations from original specifications are documented in writing. In order to conduct repairs in a cost effective, high quality, timely manner and create a profit for the stockholders, GIAC Enterprises has invested heavily in automated management and engineering information systems.

GIAC Enterprises consists of several organizational groupings and/or departments, each having differing needs for information systems. These groups are and their Information Technology needs are as follows:

1. The Accounting Department - This department uses an in house developed Oracle database used for financial management, budgeting and time keeping. This database has links to the Industrial Management System (IMS) databases. The IMS is an in-house developed Oracle database that provides for project management, resource projection (personnel and financial).

2. The Human Resources Department - This department uses commercial software to maintain personnel records. An in-house developed Oracle database, the Qualifications Tracking System (QTS) tracks personnel qualifications (to industry and customer standards). This database has links to the IMS databases.

3. The Quality Assurance Department - This department uses an in-house developed Document Management System (DMS) based upon web technology and an Oracle database. The department also performs research and development into the industrial processes used by GIAC Enterprises. To assist

in the performance of this function the department uses a Commercial Off-the Shelf (COTS) Statistical Analysis software package for in depth trend analysis.

4. The Engineering Department - This department uses the IMS to plan for the accomplishment of proposed and contracted projects. The department uses DMS to track and manage procedures issued to accomplish contracted projects. To support the writing of these procedures, COTS computer aided design (CAD) and Computer Aided Engineering (CAE) software (depending upon the customer requirements) is used. The Engineering Department uses a variety of proprietary software that original equipment manufacturer's (OEM's) developed to supports many of the components repaired by GIAC Enterprises. Additionally, the department places requisitions for materials and supplies using the Supply Department's Requisition Management System (RMS) databases. This department also performs some research and development in the course of preparing to the accomplishment of proposed and contracted projects.

5. The Sales and Marketing Department - This department uses the IMS databases to develop the initial cost estimates and planning in order to define and offer bids on work solicited by potential GIAC Enterprises customers.

6. The Production Department - This department uses the various CAD and CAE software and computer aided manufacturing software that supports their numerically controlled manufacturing equipment. Production also uses the Supply Department's RMS databases.

7. The Supply Department - This department uses in-house developed document control and inventory management software called the Requisition Management System (RMS) that uses web-based technology and an Oracle database. This software/hardware system tracks technical specifications for materials and services from the identification of need by the Engineering and Production Departments through the contracting cycle, receipt inspection, storage and eventually until it is used.

8. The Environmental Monitoring Department - This department uses several automated data collection instruments to monitor GIAC Enterprises compliance with environmental quality, health and safety regulations. Additionally, they access the RMS to track Material Safety Data Sheets for hazardous materials ordered and used by GIAC Enterprises.

9. The Software Development and Information Technology Department (SD/IT) - This department utilizes a large number of software development and system monitoring tools.

10. The Security Department - This department utilizes the QTS to track areas and systems that GIAC Enterprises personnel (and visitors) are authorized to access.

11. Management - Management uses the IMS, QTS, DMS and RMS to oversee the operations of GIAC enterprises.

12. Remote Users - This group comprises management, marketing, engineering, production personnel using GIAC Enterprises owned Laptops. These individuals require access to GIAC Enterprises information systems when off-campus. Access is through dial-in to the RAS server using intelligent secure tokens (SmartCards) for short-term situations. For longer term (or where contractually provided for) a dedicated VPN connection may be established.

Upgrading to Microsoft Windows® 2000:
Faced with an aging operating system that was approaching the end-of-life for support by Microsoft, GIAC Enterprises had to face upgrading to the next operating system. Management has decided to upgrade to Windows® 2000. Due to a limited budget and the complex integration of in-house developed information systems, Management decided to use a phased approach to implement Windows® 2000 across the enterprise. Management tasked the Software Development and Information Technology Department with formulating this strategy.

Design Basis

To properly design a network system, requires an understanding of the current state of information systems in an organization. Unless the organization is just starting, then the new design must be built upon the preceding environment.

GIAC Enterprise Network Design

The GIAC Enterprises network is comprised of two elements: a large campus and satellite installations at client sites. Figure 1 shows the layout of the network at the GIAC Enterprises main campus.

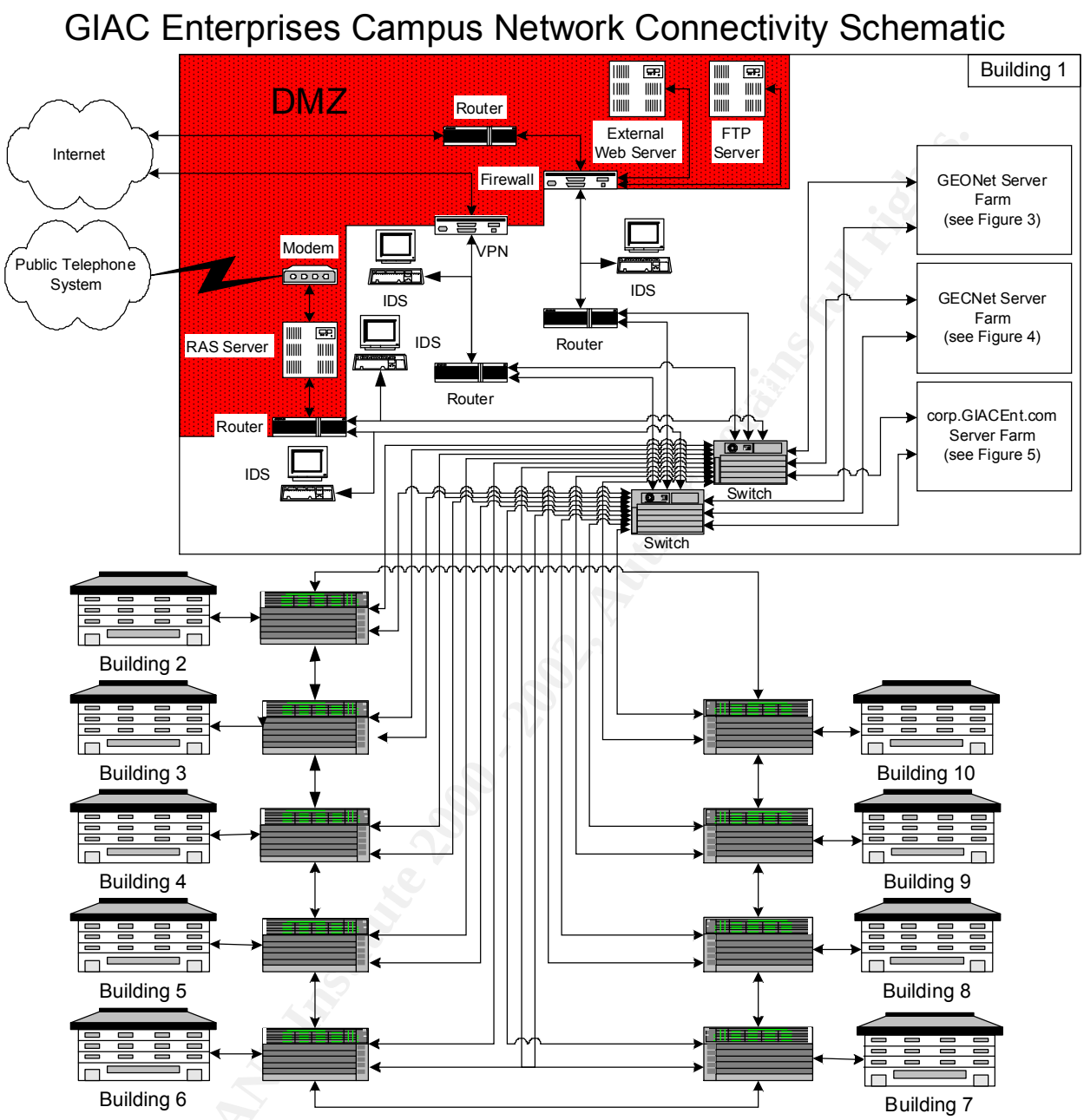


Figure 1

Note: Within the buildings of the main campus, hubs will connect to the building switch. From these hubs, clients, printers, plotters and other network aware devices (e.g., numerically controlled milling machines) are connected.

Figure 2 shows a typical client site installation.

GIAC Enterprises Network Installation at a Client Location

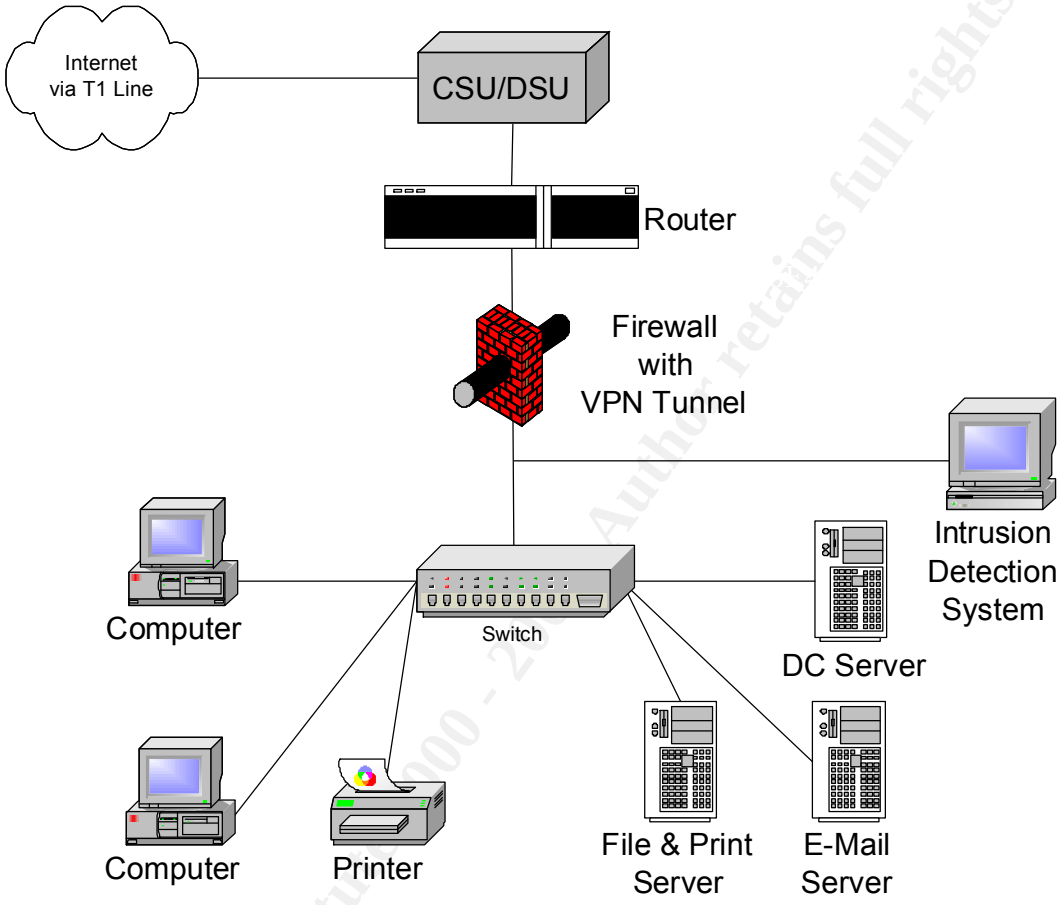


Figure 2

Figure 3 shows a detail of the GEONet Server Farm.

GIAC Enterprises GEONet Domain Server Farm

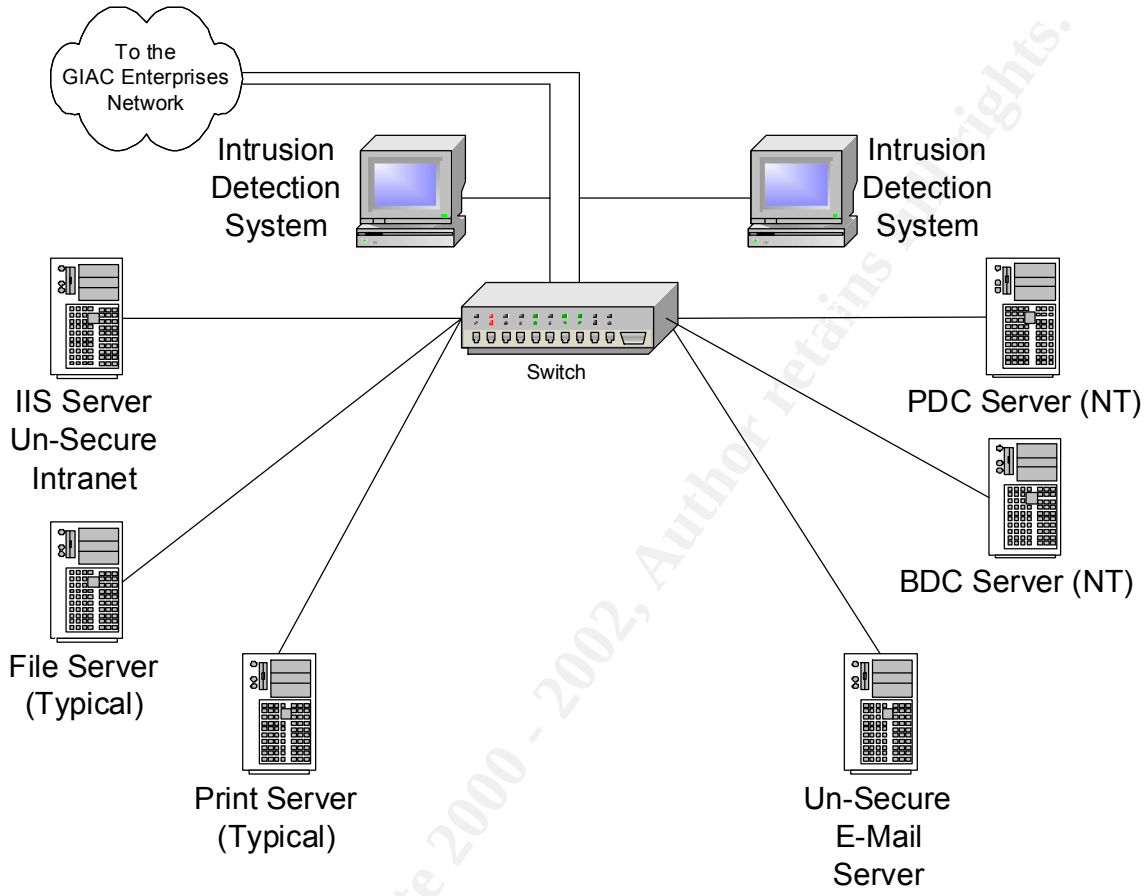


Figure 3

Figure 4 shows a detail of the GECNet Server Farm.

GIAC Enterprises GECNet Domain Server Farm

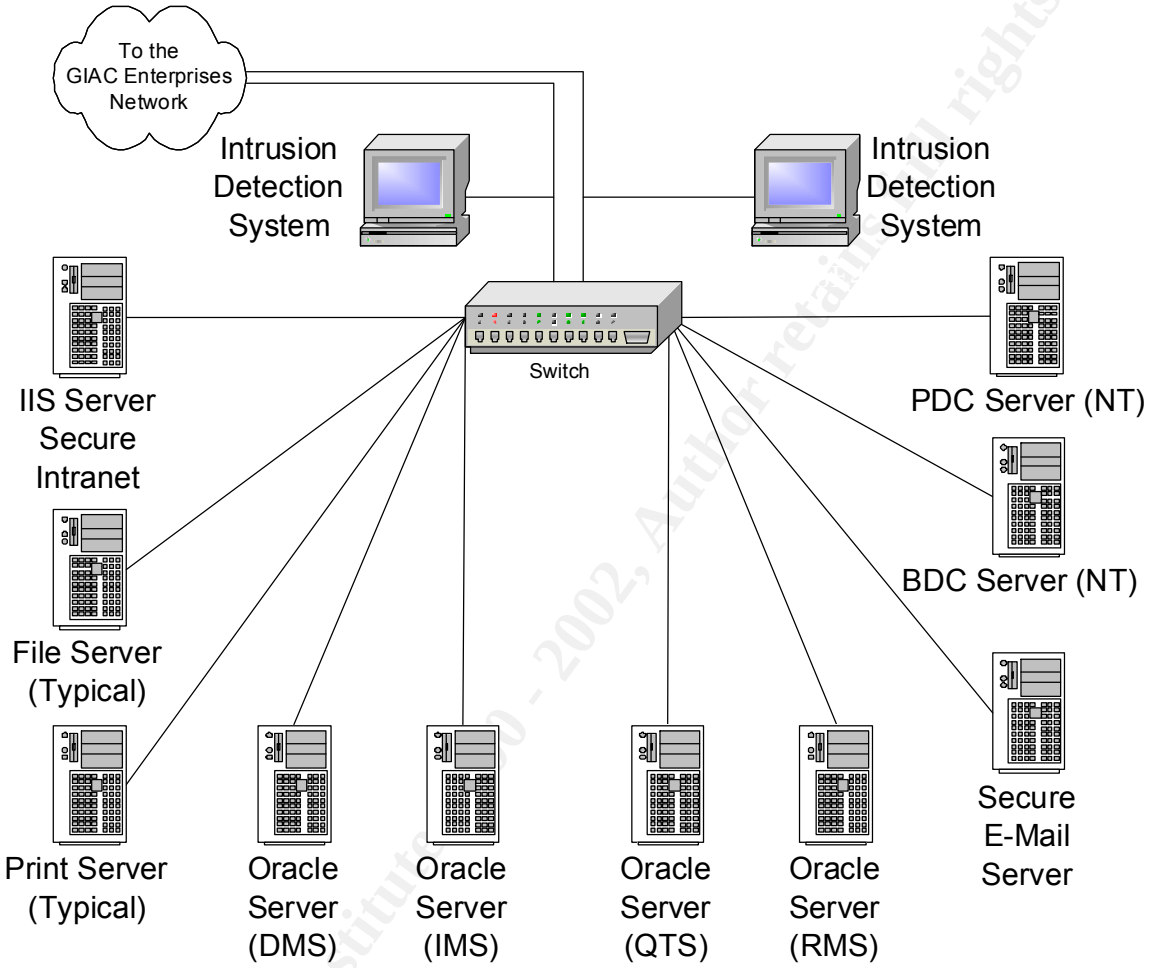
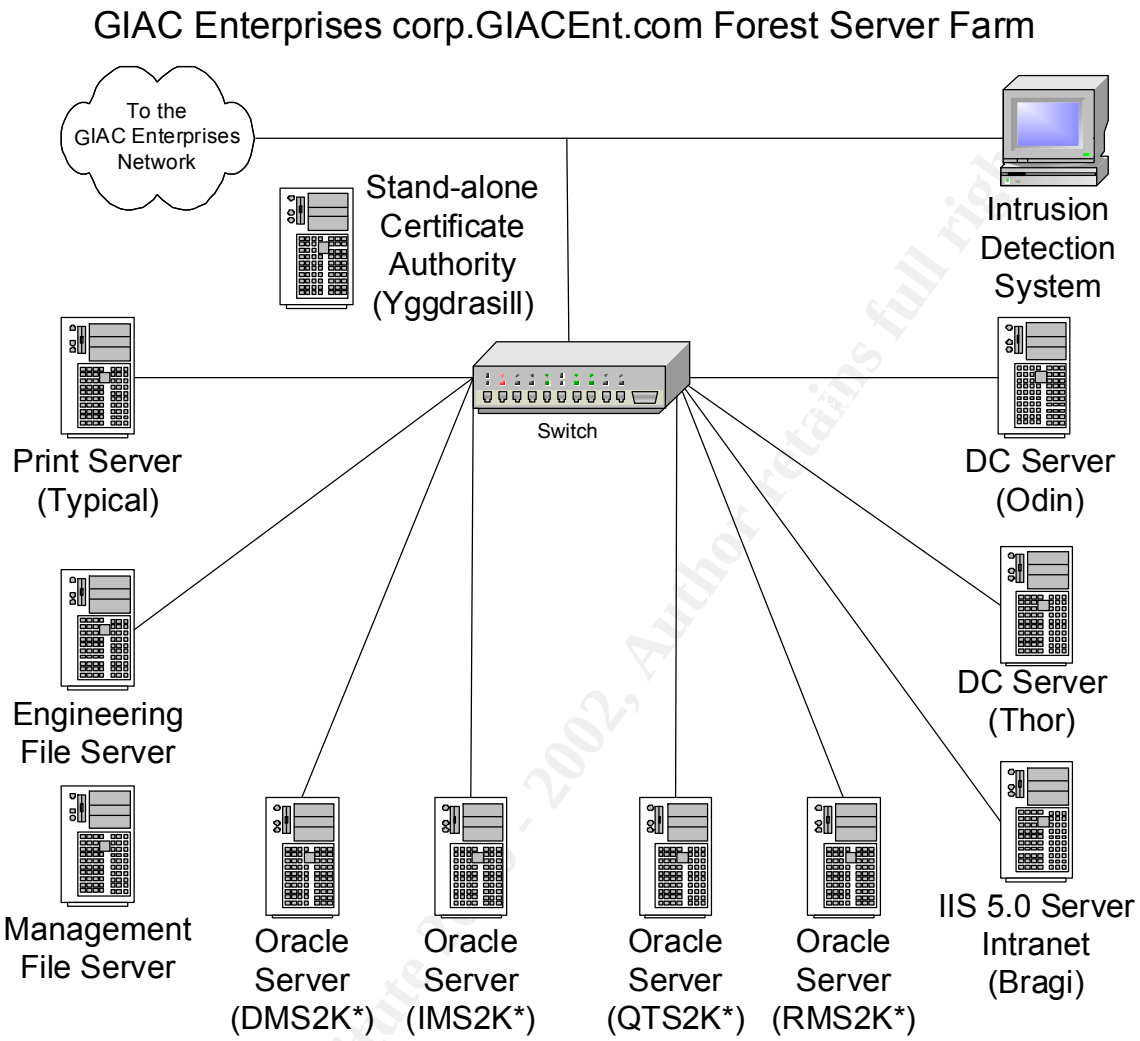


Figure 4

Figure 5 shows a detail of the GIAC Enterprises Windows 2000 Server Farm.



* - The Oracle servers are currently in development and test mode and are only available to SD/IT Programmers and Administrators.

Figure 5

Information Technology Description

The GIAC Enterprises Information Technology Infrastructure consists of workstations, laptops, printers, personal data assistants, servers, and other intelligent devices such as computer aided manufacturing equipment and inventory control devices. These devices communicate across a TCP/IP based network infrastructure that consists of 100Base-T (within buildings) and 100Base-FI (primarily between buildings). The network infrastructure connects through a demilitarized zone (DMZ) to the Internet via two T1 lines. Additional external access to the network is available through dial-in connections. A network operations center where the DMZ, primary switches and the server farms for the network are located is located in Building 6 as well as a testing network used to test proposed hardware, software and configurations. In Part 2, a further description of the

physical layout is provided. Figure (1) provides a schematic lay out of the infrastructure (Building 6 and the testing network are not specifically identified).

The primary operating system of the network was Windows NT® 4.0 (service pack 6a) supported with Simple Network Management Protocol (SNMP) for remote management of network devices. A demilitarized zone (DMZ) protects the network from the internet where the company's public web server and File Transfer Protocol (FTP) server are located. GIAC Enterprises uses a virtual private network (VPN) device via the second T1 line to establish secure links to critical business partners and clients. GIAC Enterprises uses a Windows NT® RAS server to allow dial-in access, also located in the DMZ. GIAC Enterprises has a class C Internet address and performs TCP/IP address translation at the DMZ. Internally, GIAC Enterprises operates using class B TCP/IP addresses.

The GIAC Enterprises had divided the network into two internally Windows NT® domains. Both Domains remain in use until the full migration to Windows 2000/XP has been accomplished. The first is the GIAC Enterprises Open Network (GEONet). This portion of the network comprises those Windows NT users that regularly interface with the public and/or the marketing of GIAC Enterprises. The second is the GIAC Enterprises Closed Network (GECNET). This domain is where information that the GIAC Enterprises Management has designated as business sensitive, financial, operations, proprietary, etc., (collectively called sensitive information) is processed. Both networks share the same infrastructure, but user accounts and workstations are set up to access only domain one at a time. GEONet trusts GECNet only. Both GEONet and GECNet trust the new Windows 2000 Domain.

GIAC Enterprises also runs a testing network does not connect to either the internal network or the Internet. GIAC Enterprises uses this network to test new software and the security of new commercial off the shelf software and hardware. This network was used to test the initial Windows 2000 Domain setup and the Group Policies,

Because GIAC Enterprises often performs repairs for the Department of Defense (DOD), the GIAC Enterprise information systems meet the DOD Trusted Computer Systems Evaluation Criteria security level of C2 and are certified and accredited to the DOD Information Technology Security Certification and Accreditation Process (DITSCAP).

Company personnel must be able to use the GIAC Enterprises information systems efficiently to translate a set of repair specifications into working procedures that will pass through the contracting, procurement, engineering and production stages of a project. GIAC Enterprises maintains critical information (i.e., information deemed proprietary or sensitive by the customer, original equipment manufacturer and or GIAC Enterprises management) in a secure manner during this process. GIAC Enterprises uses a combination of COTS products as well as in-house developed solutions in order to automate some or all of those business functions.

Minimum Personnel Requirements for Accessing GIAC Enterprises Information Systems:
GIAC Enterprises screens all employees upon hire for criminal background and United States citizenship. After hiring, certain employees may also receive government clearances in support of potential and active government contracts.

GIAC Enterprises grants subcontractors, business partners and customers' access to the company information systems based upon contractual need and Management's discretion. Such access and the minimum security provisions are set forth in the applicable contracts. As a minimum, individuals from these organizations must be United States citizens in order to receive a GIAC Enterprises information system user account.

Standard User Computing Resources:
In general, GIAC Enterprises provides all employees Office Automation software (Microsoft® Office 2000) for general communications, correspondence and documentation of work progress. All employees have network accounts on the GEONet domain. Electronic Mail is part of each user's account using Microsoft® Exchange/Outlook 2000. In addition, all employees have access to the GEONet Intranet web pages for keeping employees up to date on internal happenings with in the organization.

Personnel authorized by GIAC Enterprises Management to access GIAC Enterprises sensitive information receive accounts on the secure access domain, GECNet. These accounts come with an additional e-mail account (Microsoft® Exchange/Outlook 2000) using a separate mail server that is located on the GECNet Domain. The GEONet domain trusts the GECNet domain and the GECNet Domain does not trust the GEONet Domain.

When the applications of a department or grouping of users are ready to move to the Windows 2000 network, an organizational unit (OU) is developed within the GIAC Enterprises Windows 2000 Active directory. The OU's is set up with Group Policies to support the operational and security needs of the department or group. In some cases, sub-OU's may also be required. Once an OU is established and tested, the users from the group or department are setup with Windows 2000 accounts and their workstations and printers are upgraded and connected to the new Windows 2000 domain. Databases and in-house applications are migrated individually based upon the circumstances of each application. (and as applicable, sub-OU's)

Workstation and Servers on GEONet, GECNet, and the New Windows 2000 Domain:
Currently, all Windows NT workstations are members of both domains and the user selects which domain to log on to at login. All Windows 2000 workstations are members of the new Windows 2000 Domain and are added to the GEONet and GECNet Domains if needed to access legacy applications that have not migrated to the Windows 2000 servers. The GEONet and GECNet exchange servers shall not be moved to the Windows 2000 domain until the migration of all other GIAC Enterprises

information systems is complete. At that time, the e-mail servers are to be and upgraded to the latest version of Exchange and migrated to Windows 2000 network.

Access control lists protect data on file and internal web servers based upon management defined access policy. Company data is managed using databases developed in-house based upon roles that meet the management defined access policies. Auditing is performed on all databases data, file and web servers for unauthorized access and activity. All servers are located in one of two computer centers, called server farms. The Security Department controls and monitors physical access to the server farms. Only "authenticated" users may gain electronic access to the GIAC Enterprises information systems. GIAC Enterprises monitors the entrance to the DMZ and at the entrances to the GEONet and GECNet server farms for unauthorized access using intrusion detection systems.

Servers perform several roles and are configured as follows:

- Domain Controllers, used to provide access and security; Windows NT 4.0 and Windows 2000 Advanced Server
- Mail Servers, inter and extra communications, Exchange 4.0/Windows NT 4.0
- Database Servers, data management; Oracle 8.0 (various patch levels depending upon impact to database interconnectivity, interfaces and reporting designs)
- File/Print Servers, for data storage and printing; Windows NT 4.0/Windows 2000 Advanced Servers
- Web Servers (Internal and External), for data accessibility to internal and external users; IIS 4.0/Windows NT and IIS 5.0/Windows 2000 Advanced Servers
- File Transfer Servers, for data transmission ease; Windows NT 4.0
- Domain Naming Server, for Internet connectivity; Linux

All servers are configured with RAID 5 disk arrays and tape backup and currently are running the latest service packs, security role up packs and the latest (applicable) patches that have been evaluated for problems with interoperability of the various GIAC Enterprises applications.

General Data Processing Requirements:
In order to maintain a strong leadership position within their industry, GIAC Enterprises Management has adopted several information technology policies to protect GIAC Enterprises electronic information systems. Re-design of the company's information systems included consideration of these policies. These policies are as follows:

1. Data Availability, Integrity and Confidentiality
2. Security Awareness Training
3. Acceptable Use
4. Remote Users
5. Intrusion Detection

1. Data Availability, Integrity and Confidentiality - Data Availability, Integrity and Confidentiality are first in importance to GIAC Enterprises. If data is not available to those who need it, the business cannot function. If the data is not correct, therefore un-reliable, mistakes will happen and cause re-work and lost customer satisfaction, both of which affect the bottom line. If a loss of data occurs (loss of confidentiality) GIAC Enterprises' business reputation will suffer and possible legal action, both civil and criminal, can result. Again, loss of data confidentiality ultimately affects the bottom line. If GIAC Enterprises cannot design information systems that allows for the detection and notification of unauthorized access to GIAC Enterprises information, this directly affects the customer's confidence in our ability to protect their information and contracts can be lost or cancelled. If GIAC Enterprises cannot control the configuration of the deployed information systems, then it is not be possible to ensure the designed controls of the systems are properly working. Should uncontrolled elements be introduced into GIAC Enterprises information systems, it can no longer be assumed those systems are a controlled environment. Thus, the risk to the information processed by those systems will no longer be known or manageable.

2. Security Awareness Training - Security Awareness Training is of prime importance because people build and use and ultimately will compromise those information systems. The strongest policies, the best safes, the highest level of encryption are all worthless if people do not properly use and safeguard them. Therefore, making authorized users, system administrators, and Management aware of their role in the protection of GIAC Enterprises information is critical to the success of protecting this information.

3. Acceptable Use - Acceptable Use refers to what uses GIAC Enterprises information systems that the GIAC Enterprises Management considers acceptable. In order to conduct profitable business, GIAC Enterprises has built information systems to meet this end. The well being and morale of GIAC Enterprises employees directly affects the ability of GIAC Enterprises to be competitive, therefore GIAC Enterprises management recognizes the value in allowing some non-business related usage of GIAC Enterprises information systems. However, GIAC Enterprises has not provided these information systems for the sole use of employees. Misuse of company assets will affect the cost of doing business, the reputation of the company and possibly criminal and civil liability.

4. Remote Users – This is a term for personnel provided with portable information systems (laptops) when not at the GIAC Enterprises campus or satellite facility. These users may or may not also access the GIAC Enterprises information systems via dial-in. The need to support user access to the GIAC Information Systems when off-site, on travel, etc., is a fact of how GIAC Enterprises does business. To protect of GIAC Enterprises information that remote users carry on their company provided laptops and the secure transmission of that information is of prime importance. Transmission of company data or the security of that data

on those remote information systems directly affects the company's ability to maintain data Confidentiality. Therefore, GIAC Enterprises cannot afford to allow the interception of transmitted data or the access to that data if such a system is stolen.

5. Intrusion Detection - Intrusion Detection is the last major area of concern. It does not directly relate to the bottom line of the company. However, it is the primary tool used to determine if the information systems perform as designed and determines if anyone has had unauthorized access to company information systems (therefore had access to the data). Unless the company uses a measurable resource to determine if an unauthorized access has occurred to their information systems, the company has no way to protect itself from such an attack. Such an unrecognized attack can cause a loss of confidentiality, integrity and availability, thus loss of competitive edge, or civil and criminal liabilities.

Specialized Data Processing Requirements:
Remote site users and each GIAC Enterprises department require some specialized data/data processing capability. In general, these requirements are as follows:

1. The Accounting Department uses the Industrial Management System (IMS). IMS is an in-house developed collection of Oracle database used for financial management and time keeping.

2. The Human Resources Department uses commercial software to maintain personnel records and an in-house developed Oracle database, the Qualifications Tracking System (QTS). The QTS tracks personnel qualifications (to industry and customer standards). This database links to the IMS databases.

3. Management uses the IMS to provide for project management and resource projection (personnel and financial).

4. The Quality Assurance Department uses an in-house developed Document Management System (DMS) based upon web technology and an Oracle database. The department uses a COTS Statistical Analysis software package for in depth trend analysis.

5. The Engineering Department uses the IMS to plan for the accomplishment of proposed and contracted projects. The department uses DMS to track and manage procedures issued to accomplish contracted projects. To support the writing of these procedures, the department uses COTS computer aided design (CAD) and Computer Aided Engineering (CAE) software (depending upon the customer requirements). The Engineering Department uses a variety of proprietary software developed by original equipment manufacturer's (OEM's) to support many of the components repaired by GIAC Enterprises. Additionally, the department orders materials and supplies using the Supply Department's Requisition Management System (RMS).

6. The Production Department uses the various CAD and CAE software and computer aided manufacturing software that supports their numerically controlled manufacturing equipment. Production also uses the Supply Department's RMS.

7. The Supply Department uses the Requisition Management System (RMS). The RMS is an in-house developed system that uses web-based technology and an Oracle database. The Supply Department uses the RMS for controlling procurement documents and inventory management. This software/hardware system tracks technical specifications for materials and services from the identification of need by the Engineering and Production Departments through the contracting cycle, receipt inspection, storage and eventually until it is used.

8. The Environmental Monitoring Department uses several automated data collection instruments to monitor GIAC Enterprises compliance with environmental quality, health and safety regulations. The Department also uses the RMS to track Material Safety Data Sheets for hazardous materials ordered and used by GIAC Enterprises.

9. The Software Development and Information Technology Department utilizes a large number of software development and monitoring tools.

10. The Security Department utilizes the QTS to track areas and systems that GIAC Enterprises personnel are authorized to access.

11. Remote Users are defined as management, marketing, engineering, and production personnel using GIAC Enterprises owned Laptops. Remote Users require access to GEONet and/or GECNet when off-campus. Access is through dial-in to the RAS server using intelligent secure tokens (SmartCards) for short-term situations. For longer term (or where contractually provided for) a dedicated VPN connection may be established.

GIAC Enterprise Network Windows 2000 Design

SD/IT evaluated the original Windows NT 4.0 design of the GIAC Enterprises network infrastructure and determined the basic physical design was sound, thus restricted the redesign to those elements that would require replacement because of the move to a new network operating system. This strategy minimized the need for hardware replacement and primarily affected equipment that was nearing the end-of-life. This allowed for a minimization of impact on current the information technology budget.

SD/IT researched the possibilities for deploying Windows 2000. Basing their analysis on elements found in the Microsoft Windows® 2000 Deployment Planning Guide, the Microsoft Windows® 2000 Security Technical References, the National Security Agency Windows 2000 Guides, and general good practices and experience, the following are the design decisions for establishing a Windows® 2000 network for GIAC Enterprises:

1. A new domain (forest) shall be deployed named corp.GIACEnt.com. SD/IT chose corp.GIACEnt.com for the new domain name because it would become a sub-domain to the Internic-registered is the Domain Naming Service (DNS) domain name for GIAC Enterprises.
2. The existing Windows NT domains will remain in place and have limited trusts established between these two domains and the new Windows 2000 Forest.
3. Organizational units (OU's) will be created in corp.GIACEnt.com for each department and organizational group described above. The Group Policies for these OU's shall provide the same level of security (as a minimum) currently provided by the Windows NT GEONet and GECNet domains. SD/IT chose not to make separate domains (as was done in Windows® NT) since Windows 2000 domains do not provide a security function and replication concerns will not be an issue. These new OU's will serve as resource locations for organizational databases and file servers that will be access according to assigned user privileges.
4. The Active Directory shall be divided into several domains to mitigate replication of Active Directory data. Domains shall be created based of remote connectivity needs to off-site GIAC Enterprises operations and/or supplier and customer connectivity needs.
5. The Linux DNS server will remain in the DMZ and will continue to provide Domain Naming for GIAC Enterprises with relation to the Internet. A Windows 2000 domain controller will provide internal Domain Naming only.
6. The new network will provide certificate services for in-house document security and encryption. GIAC Enterprises will continue to rely upon a contracted certificate service for extra-network certificates.
7. SD/IT will move communities of users and their associated workstations and applications to the new domains rather than move the entire GIAC Enterprises all at once. This will allow for reducing the numbers of workstations that will require replacement to what can be handled within the current budgets. This also divides the numbers of legacy applications that must be reviewed and upgraded to Windows 2000 operability into manageable amounts. Additionally, the SD/IT organization can manage the time spent to develop detailed group policies applicable to the individual organizations as well as scripts to manage the software used by those organizations. This reason allows (and item 1 above), the new forest to be operated in "native" mode vice "mixed" mode from the start providing the full benefits of the new operating system fully to those organizations that migrate without having to wait upon the entirety of GIAC Enterprises.
8. The current VPN device will not be replaced. The current hardware will continue to provide security between sites. The Windows 2000 VPN capability shall be used as an additional layer of defense where it may be beneficial to security of the GIAC Enterprises information system and data.
9. The use of a dual e-mail system will continue. When the entire network of users has migrated to Windows 2000, the e-mail services shall be redesigned. SD/IT will then upgrade to the latest version of MS Exchange in order to use the Active Directory features of Windows 2000. By not converting at the outset avoids having to redesign an aspect of databases integrated with the e-mail servers in

addition to other Windows 2000 compatibility issues faced by the databases. This reduces the upfront complexity of the migration without increasing the level of support required for managing the current e-mail systems.

10. The encrypted file system (EFS) capability are used for remote users and remote sites where the potential for loss of company data is greatest. SD/IT shall also use EFS as a way to protect the most sensitive company data (i.e., data that needs be restricted from general user access and controlled distribution) using digital certificates and the IPSec capability.

New Servers and Their Functions

SD/IT planned the Windows 2000 Forest and tested its security prior to connecting it to any external resources, including the current Windows NT domains. All the Windows 2000 servers are high-end Intel processor platforms running Windows 2000 Advanced Server (service pack 2). All are equipped with RAID 5 arrays, and a minimum of 80 GB of drive space. Memory (hard disk and RAM) are sized to support the purpose of the server. All are equipped for tape backup of all data.

Server Name	Purpose	Comments
Odin	Domain Controller RID Master Domain Naming Master Global Catalog Master Schema Master	The first domain controller established.
Thor	Domain Controller Infrastructure Master Enterprise On-line Certificate Authority	The second domain controller.
Huginn	Unsecured E-mail Server	To be established after all the corporation upgrades to the Windows 2000 Forest. Huginn will replace the GEONet mail server.
Muninn	Secure E-mail Server	To be established after all the corporation upgrades to the Windows 2000 Forest. Muninn will replace the GECNet mail server.
Bragi	Intranet Web Server	Established after the Windows 2000 Forest is connected to the corporate network infrastructure.
Yggdrasill	Root Certificate Authority	Standalone server.
Database servers (various)	Databases	These servers accommodate corporate databases that have been upgraded to operate in the Windows 2000 environment. Once approved for the new environment, the production databases shall transferred over these servers.
File & Print Servers	Data repositories and Printing	To be added as groups migrate from the Windows NT environment to the new forest.

GIAC Enterprises Active Directory Design

The following is a description of the GIACEnt.com Active directory. The roles, purposes (network performance, administration and security) and reasoning for of each object is given below.

Figure 6 is a detail of the corp.GIACEnt.com Active Directory.

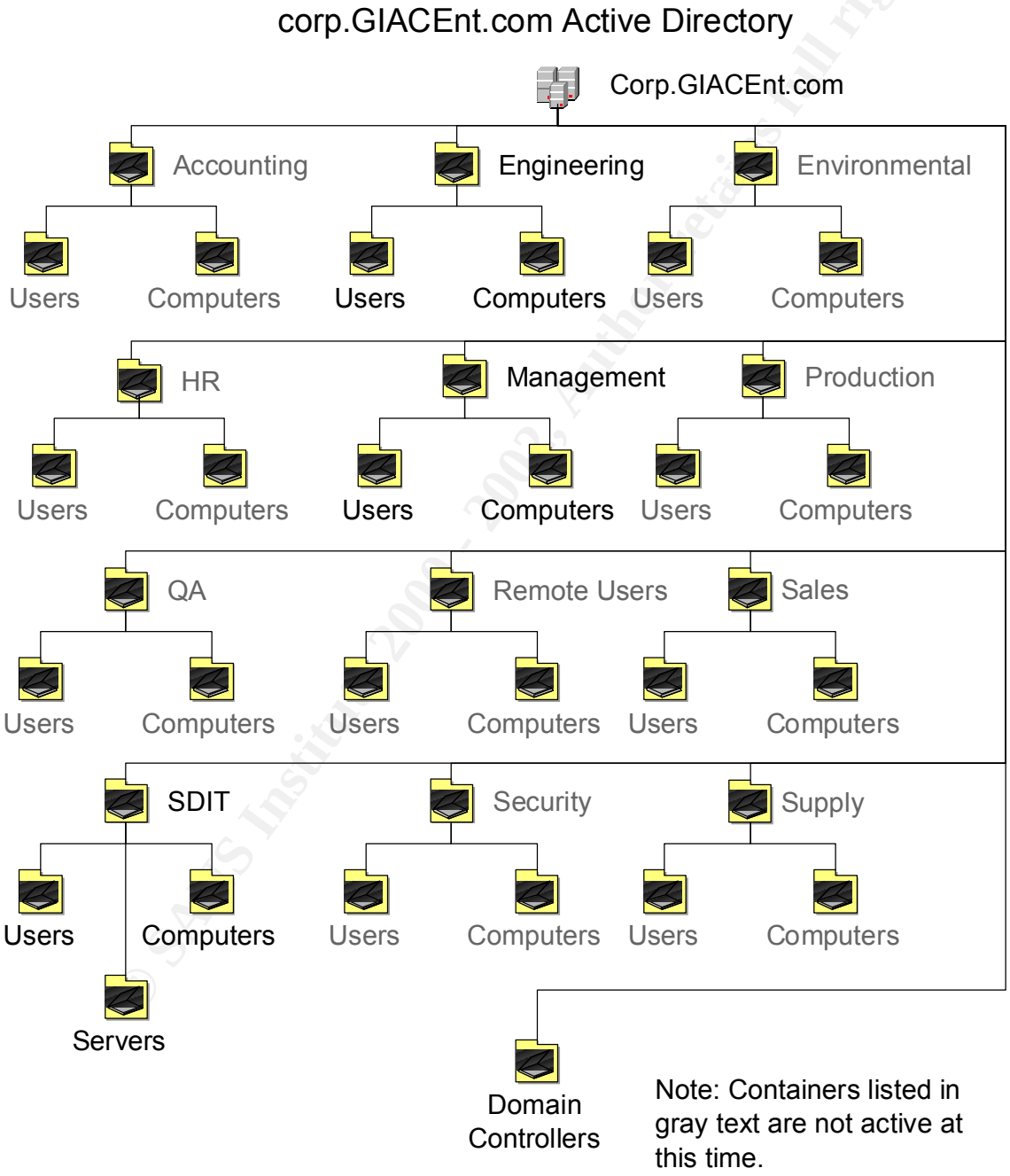


Figure 6

Active Directory Users and Computers

Built-In Containers

The following are containers are built-in to the Windows 2000 Active Directory.

Builtin – The pre-defined built in security groups.
Computers – The default container for upgraded computer accounts.
Domain Controllers – The default container for upgraded Windows 2000 Domain Controllers.
ForeignSecurityPrincipals – The default container associated with Security Identifiers (SIDs) associated with objects from external, trusted domains.

corp.GIACEnt.com Organizational Units

Because of the decision to migrate individual departments and logical groups of users to the new forest on a group-by-group basis, SD/IT established matching OU's. The purpose is to provide administration of these groups without interfering with the users, computers and policies that are already migrated. This also allows for the development of tailored policies for each organization, assisting the migration as well as meeting the operational needs and security of that group. Use of organizationally based OU's allows SD/IT to delegate the day-to-day administration functions to responsible individuals within an organization using specially designed Microsoft Management Consoles (MMC's) once the migration of the organization was completed.

Management (migrated) – This OU allows individuals defined as Management to access specifically defined organizational information and IT resources based upon a group policy. This allowed the development of group specific scripts and policies to assist in the migration of data and resources to the Windows 2000 Forest. This OU's primary purpose is to provide a framework for the secure access to organizational data and resources that Management has designated as requiring limited access based upon a strict need-to-know policy. The Group Policy for this OU provides the foundation of this added security. Information that Management has designated as "for Management only" is to be placed in shared folders that are located only in this OU. The Group Policy for this OU provides additional protections for these shared folders. SD/IT will not delegate the administration of this OU.

Accounting (currently migrating) – This OU allows for the grouping of users, databases, file and print servers that support the Accounting Department. This allowed the development of the department specific scripts and policies to assist in the migration of data and resources to the Windows 2000 Forest. Confidential financial information is to be placed in shared folders that are located only in this OU. The Group Policy for this OU provides additional protections for these shared folders. Once the migration of this organization is complete, SD/IT will delegate the day-to-day administration of this OU to the Accounting Department.

HR (awaiting migration) - This OU allows the grouping of users, databases, file and print servers that support the Human Resources Department. This allows for the development of the department specific scripts and policies to assist in the migration of

data and resources to the Windows 2000 Forest. Confidential personnel information is to be placed in shared folders that are located only in this OU. The Group Policy for this OU will provide additional protections for these shared folders. Once the migration of this organization is completed, SD/IT will delegate the day-to-day administration of this OU to the Human Resources Department.

QA (awaiting migration) - This OU allows the grouping of users, databases, file and print servers that support the Quality Assurance Department. This will allow for the development of the department specific scripts and policies to assist in the migration of data and resources to the Windows 2000 Forest. Confidential information on partner and supplier quality is to be placed in shared folders that are located only in this OU. The Group Policy for this OU will provide additional protections for these shared folders. Once the migration of this organization is completed, SD/IT will delegate the day-to-day administration of this OU to the Quality Assurance Department.

Engineering (migrated) - This OU allows the grouping of users, software, systems, databases, file and print servers that support the Engineering Department. This allowed for the development of the department specific scripts and policies to assist in the migration of data and resources to the Windows 2000 Forest. Data on confidential corporate processes and patents used by the Engineering Department is stored in shared folders that are located only in this OU. The Group Policy for this OU provides additional protections for these shared folders. SD/IT has delegated the day-to-day administration of this OU to the Engineering Department.

Sales (awaiting migration) - This OU allows the grouping of users, databases, file and print servers that support the Sales and Marketing Department. This will allow the development of the department specific scripts and policies to assist in the migration of data and resources to the Windows 2000 Forest. Additionally, confidential sales data is to be placed in shared folders that are located in this OU. The Group Policy for this OU will provide additional protections for these shared folders. Once the migration of this organization is completed, SD/IT will delegate the day-to-day administration of this OU to the Sales and Marketing Department.

Production (awaiting migration) - This OU allows the grouping of users, systems, databases, file and print servers that support the Production Department. This will allow for the development of the department specific scripts and policies to assist in the migration of data and resources to the Windows 2000 Forest. Confidential production information is to be placed in shared folders that are located only in this OU. The Group Policy for this OU will provide additional protections for these shared folders. Once the migration of this organization is completed, SD/IT will delegate the day-to-day administration of this OU to the Production Department.

Supply (awaiting migration) - This OU allows the grouping of users, databases, file and print servers that support the Supply Department. This will allow for the development of the department specific scripts and policies to assist in the migration of data and resources to the Windows 2000 Forest. Confidential contracting information is to be

placed in shared folders that are located only in this OU. The Group Policy for this OU will provide additional protections for these shared folders. Once the migration of this organization is completed, SD/IT will delegate the day-to-day administration of this OU to the Supply Department.

Environmental (awaiting migration) - This OU allows the grouping of users, databases, file and print servers that support the Environmental Monitoring Department. This will allow for the development of the department specific scripts and policies to assist in the migration of data and resources to the Windows 2000 Forest. Confidential environmental compliance information is to be placed in shared folders that are located only in this OU. The Group Policy for this OU will provide additional protections for these shared folders. Once the migration of this organization is completed, SD/IT will delegate the day-to-day administration of this OU to the Environmental Monitoring Department.

SDIT (migrated) - This OU allows the grouping of users, systems, file and print servers that support the Software Development and Information Technology Department. This allowed for the development of the department specific scripts and policies to assist in the migration of data and resources to the Windows 2000 Forest. Installation packages of software used to support the organization and sensitive network design and operations data is stored in shared folders that are located only in this OU. The Group Policy for this OU provides additional protections for these shared folders.

Security (awaiting migration) - This OU allows the grouping of users, databases, file and print servers that support the Security Department. This will allow for the development of the department specific scripts and policies to assist in the migration of data and resources to the Windows 2000 Forest. Confidential security information is to be placed in shared folders that are located only in this OU. The Group Policy for this OU will provide additional protections for these shared folders. Once the migration of this organization is completed, SD/IT will delegate the day-to-day administration of this OU to the Security Department.

Remote Users (awaiting migration) - This OU allows the grouping of users that require remote access to resources within the Windows 2000 Forest. This will allow for the development of group specific scripts and policies to assist in the security of remotely accessing to the Windows 2000 Forest. SD/IT will not delegate the day-to-day administration of this OU.

Second Level OU's – Beneath each OU (except for remote users) there will exist two other OU's and in some cases, a third level OU. These would be "Users", "Workstations" and where applicable, "Member Servers". This will allow SD/IT to detail the Group Policies for these roles. The SD/IT OU shall also have several other second level OU's in order to provide security and support for all the types of systems and users encountered only within the SD/IT organization. For example: "Programmers", "IIS

Servers", "Database Servers", "Programmer Systems", "Admin Consoles", etc. The GIACSite1 OU shall also have a second level OU for Domain Controllers.

Domains and Trusts

GEONet – SD/IT set up an explicit trust to the existing GEONet Windows NT domain. This provided migrated users access to resources and information that is not yet migrated. GEONet trusts the Windows 2000 Forest, but the Windows 2000 Forest does not trust GEONet.

GECNet – SD/IT set up an explicit trust to the existing GECNet Windows NT domain. This provided migrated users access to resources and information that is not yet migrated. GECNet trusts the Windows 2000 Forest, but the Windows 2000 Forest does not trust GECNet.

GIACSite1 – This domain is representative of an off-campus, semi-permanent GIAC Enterprises office. Such offices are equipped with a domain controller and a file/print server as a minimum (See Figure 2). These additional domains will allow SD/IT flexibility to use the security and operational structure of an existing Group Policy or to create new tailored Group Policies, etc., that meets the off-site office's needs. Use of separate domains for these off-site offices is primarily to reduce the replication of Active Directory data across limited bandwidth links. This Windows 2000 Domain is part of the Windows 2000 Forest.

Partner1 – This domain is representative of a corporate partner's domain. Establishing such links to partner domains will provide partners with continued access to GIAC Enterprises information systems as agreed to by GIAC Enterprises Management. The nature of these explicit trusts (one-way, two-way, or transitive) are based upon those agreements. These domains may or may not be part of the Windows 2000 Forest.

Customer1 - This would be a domain of a corporate customer. Establishing such links to customer domains will provide customers access to GIAC Enterprises information systems as agreed to by GIAC Enterprises Management. The nature of these explicit trusts (one-way, two-way, or transitive) are based upon those agreements. These domains will not be part of the Windows 2000 Forest.

Active Directory Sites and Services

Currently, SD/IT does not need the use of Sites as the first GIAC Enterprise offsite domain has not been established. When the first site is established, SD/IT will implement the use of Sites in order to reduce replication of Active Directory traffic across a limited bandwidth link.

Basic Group Policy for GIAC Enterprises

The following is the Group Policy established for all GIAC Enterprises Windows 2000 Domains. It encompasses the default Domain policy and the Domain Controllers Policy. SD/IT installs the Microsoft provided Security Templates designed for high security. Following this practice, all domain controllers will have the following security templates imported first: security.inf, DC security.inf, basicdc.inf, securedc.inf and the hsecdc.inf, and ocfiless.inf, (installed in that order; the templates are cumulative as noted in Reference 7, pg 1239). The Domain policy starts with the importing of the security setup templates: security.inf, compatws.inf, securews.inf, hisecws.inf, ocfilesw.inf and the notssid.inf (installed in that order). Unless otherwise noted, SD/IT has left the settings established by the templates.

Default Domain Policy - GIAC Enterprises decided to use the Microsoft Security Templates because the templates provide most of the necessary settings required to meet the Information Technology Policy of the corporation and industry best practices. GIAC Enterprises is required to conform to government standards in order to perform contracts for the government. Many government contracts require GIAC Enterprises to receive government information and use that information on the company's information systems. The following is the reasoning for using the changes to specific settings beyond what the Microsoft templates set up and where SD/IT made changes to those settings, why.

Computers

Software Settings

Software Installation – SD/IT uses this feature extensively to prepare over the network installation packages. However, SD/IT will not establish any of these packages at the Domain level in order to avoid bandwidth problems with remote site and remote user systems. Therefore, there are no settings here.

Windows Settings – Security Settings

Account Policies – Account policies are set to prevent unauthorized access to the system or data by someone who is trying to gain entry using an authorized user account to which they do not have the password for.

1. Password Policy – To meet government requirements to protect government information on company information systems, it is necessary to set minimum password complexity, age and protection. Setting these thresholds provides a measure of security against social engineering attacks and password cracking. SD/IT uses the Domain Group Policy to force all user accounts to have set password lengths, complexity and ages. The settings established by the Security templates ensure that all users will have complex passwords, forcing users to select good passwords that are not easily guessed or cracked. The passwords are forced to change frequently, minimizing how long a password that has been compromised can remain useful to the intruder. Old passwords cannot be conveniently revised by the user since there is a minimum time set for when the user can change their password. No changes were made to the template settings.

2. Account Lockout Policy – The settings established by the Security Domain templates ensure users accounts are not easily broken into. By establishing an upper limit on failed attempts within a set time, prevents accounts from being broken into by brute force attacks. Any time an account is locked-out could be evidence of an intruder. For this reason, the account lockout duration is set to zero thereby forcing the user to contact an administrator in the event of a lockout. This policy allows GIAC Enterprises to investigate all lockouts. No changes are made to the template settings.
3. Kerberos Policy - The Security templates do not set any Kerberos policy. Since GIAC Enterprises Windows 2000 network will rely on Kerberos Authentication and will connect to the Internet as well as to customer and partner networks, SD/IT chose to set the Kerberos Policy as an extra measure of security. Normally this extra measure is not necessary. However, should a compromise of a partner's or customers network occur or the GIAC Enterprises DMZ fails to prevent an intrusion, this additional security will help prevent such intruders from easily using the GIAC Enterprises network resources. The option to enforce the user's logon restrictions has been enabled so every time a system service is requested by a user, the system checks that the user has the right to use the service. The computer clock synchronization tolerance is set to prevent replay attacks. The policy also sets the lifetimes for service, user and user renewal tickets.

Local Policies – SD/IT uses Local Policies to set registry settings that they will apply to the entire domain. The settings established by the Security templates ensure auditing and security specific options are set across the Domain. The administrator and guest accounts are renamed so that hackers cannot attempt to gain access via known default accounts.

1. Audit Policy – no changes from the settings established by the templates.
2. User Rights Assignments –
    a. Access this computer from the network – "Everyone" removed. No anonymous users should be able to access any GIAC Enterprises system.
    b. Add workstations to a domain - Changed from none assigned to Administrators. Only SD/IT administrators are able to add workstations to the domain.
    c. Deny logon as a batch job - Changed from none assigned to Authenticated users. Only those accounts enabled in "Log on as a batch job" should be logging on using a batch job. This prevents the possibility of someone that breaks through the DMZ form being able to run batch jobs with out having successfully logged on also.
    d. Log on locally – only Administrators, backup operators and system accounts allowed. GIAC Enterprises does not use local accounts (except for remote users that use laptops). This is mainly to get users to rely on network resources for security and back up. Since there is insufficient staff to recover data stored on workstations should the system need to be rebuilt, the policy is not to use local accounts (except on laptops) as these would encourage the use of storing data locally.

e. Remove Computer from docking station – Change to Administrators and Remote Users only. Only users having laptops and administrators need this right, therefore based on the principle of least privilege, this right is set to only those who need it.

3. Security Options – A variety of options are detailed in this area, all dealing with various aspects of security. SD/IT has made a few changes to some of the settings set by the Security Templates. In general, the settings set by the templates provide for needed security and do not inhibit the manner in which GIAC Enterprises uses its information systems and follows the principle of least privilege. The following are those values that have been changed and why.
    a. Message text/title for users attempting to log on – The message text and title for users attempting to log on values are set to the GIAC Enterprises Information System Usage Policy statement.
    b. Rename administrator/guest account - The administrator and guest accounts are to be renamed to make it more difficult for hackers to attack the systems.
    c. Restrict floppy access to locally logged-on user only - GIAC Enterprises policy does not allow the use of Floppy drives as a measure of preventing importation of viruses or the removing of electronic files. Since local accounts are not used by SD/IT, this is an effective method of preventing general users from using the floppy drive on a workstation.
    d. Secure channel: Require strong (Windows 2000 or later) session key – SD/IT has left this at the setting set by the template (enabled). However, when the Windows 2000 systems are allowed to connect to customer and partner Domains, it may be necessary to change the settings for the "Secure Channel: Require strong (Windows 2000 or later) session key" based upon negotiated arrangements with these organizations.

Event Log – The settings for the event logs controls the size, retention method, and whether to shut down the system when the logs are full. They also determine guest access to all logs. Defining these settings here will set a domain wide policy. Since SD/IT has limit personnel to regularly review the event logs of network workstations, GIAC Enterprises employs active Intrusion Detection Systems (IDS's) through out the network for security. Primarily for this reason, no changes have been made to the settings set by the templates. Event logs are used primarily for determining the cause of problems called in by users or discovered by the IDS's. If a situation arises where SD/IT needs to establish system wide control of the Event Logs, then it can be done here. As it becomes apparent what size is needed for the security logs (based on actual usage data from GIAC Enterprises users) SD/IT will set the size of the Security logs for all systems in the Default Domain Policy.

1. Settings For Event Logs –
    a. Retain security log – Currently set to "Not Defined". SD/IT believes that 30 days are sufficient for purposes of tracking past security events. SD/IT has determined this would be sufficient to reconstruct any evidence if required beyond what the IDS could provide in the event of an actual intrusion. Since SD/IT does not want to have a rash of disabled systems every 30 days

because the log size was too small (based upon recommendations in the Windows 2000 Resource Kit) SD/IT will monitor the sizes of typical workstations as they are deployed to ensure the security log size is adequate for the 30-day period. Once the entire network has migrated to Windows 2000 and an overall optimal size has been determined, SD/IT will revise the policy.

b. Retention method for security log – Currently set to "As needed". When the size of the log has been determined that are sufficiently large for 30 days of security events, it are changed to "By days".

Restricted Groups – SD/IT does not intend to establish restricted groups at the Domain level for regular operations. Periodically, SD/IT will review group assignments and purge current groups using the Restricted Groups.

System Services – SD/IT has chosen to modify only a few of the settings set by the Security templates. Services that SD/IT disables or control as standard across the Domain are set here. Where selected users require these services, their accounts are assigned to special groups at the OU level and granted privileges to these services at that level. A typical situation is for users to be delegated the authority to administer the day-to-day IT duties for a department. The following are those values that have been changed and why.

1. Fax – Disabled. GIAC Enterprises policy is not to connect telephone lines (for any reason) to GIAC Enterprises systems.
2. IIS Administration – Not Defined. This are set within each OU to allow only IIS Administrators to use. Only selected individuals are to be authorized to publish to the GIAC Enterprises Web sites (internal or external).
3. Telephony – Disabled. GIAC Enterprises policy is not to connect telephone lines (for any reason) to GIAC Enterprises systems.
4. Windows Installer – Not Defined. This are set within each OU to allow only Administrators to use and shall be restricted to Administrators and those with delegated authority). Only authorized individuals shall be allowed to install authorized software packages set up and/or approved by SD/IT.
5. WWW Publishing Service – Not Defined. This are set within each OU to allow only IIS Administrators to use and shall be restricted to Administrators and those with delegated authority). Only selected individuals are to be authorized to publish to the GIAC Enterprises Web sites (internal or external).

Registry – SD/IT made no changes beyond those applied by the security templates.

File System - SD/IT made no changes beyond those applied by the security templates.

Public Key Policies – SD/IT has set up a Certificate Authority primarily to manage secure e-mail traffic, EFS, encrypted data recovery agents, IPSec and certification of corporate information (code signing and time stamping). SD/IT will establish a stand-alone Certificate Authority for these services. The following are the initial settings set for the Public Key Policy and why.

1. Encrypted Data Recovery Agents – This is set to a certificate issued by the GIAC Standalone Certificate Authority.
2. Automatic Certificate Request Settings – This is set for computers and domain controllers.
3. Trusted Root Certificate Authorities – This is set to trust the GIAC Enterprises stand-alone, Microsoft, the certificate authority contracted to provide GIAC Enterprises certificates for external business as a minimum.
4. Enterprise Trust – Internal Certificates issued for file recovery, code signing, etc., are listed in the enterprise trust.

IP Security Policies on Active Directory – The settings established by the security templates meets the current needs of GIAC Enterprises until the transition to a total Windows 2000 network is completed. At that time, SD/IT will evaluate system capability to employ IPSec within the enterprise. Until then, the mandatory use of IPSec is limited to the Remote Users and Management OU's, GIAC Enterprises Offsite Domains, partner and customer domains. The Group Policies for these domains will alter these settings (primarily clients will require IPSec). Note: SD/IT replaced the policies set up by the IPSEC Policy templates with duplicates in order to avoid potential problems with duplicate GUID numbers as is advised in Q232817. The Client Policy is "assigned".

Administrative Templates - GIAC Enterprises policies require high security and the SD/IT organization has limited personnel to administer the large network across a wide campus. Therefore, settings in these areas have been set to maximize general security and ease of administration.

Windows Components –

1. Net Meeting – Remote desktop sharing - Disabled. Prevents users from sharing their workstation resources or controlling their systems remotely. Where specific departments and GIAC Enterprises management allow, the settings may be changed in the OU Group Policy for that organization (e.g., Management).
2. Internet Explorer – IE represents a constant risk to the network as well as the GIAC Enterprises Acceptable Use Policy. Most settings for IE have been set to the most restrictive setting.
    a. Security Zones: Use only machine settings – Not Defined. This prevents a user from modifying the security zone for other users on the same system.
    b. Security Zones: Do not allow users to change policies – Enabled. This prevents users from changing security zone settings.
    c. Security Zones: Do not allow users to add/delete sites – Enabled. This prevents users from adding new sites to the security zones.
    d. Make proxy settings per-machine (rather than per user) – Enabled. This ensures all users on a particular machine have the same settings.
    e. Disable Automatic Install of Internet Explorer components – Enabled. This helps the system administrators maintain version control. Since GIAC Enterprises are using more and more web-enabled applications, this will assist in preventing them from "breaking" due to an automatic install of IE components when a user goes to a web site that wants to add the component.

   f. Disable Periodic Check of Internet Explorer software updates - Enabled. Since SD/IT will push out all software updates, this prevents extra traffic on the network.
3. Task Scheduler – No changes made.
4. Windows Installer – Generally, SD/IT will push out all software centrally. However, where an installation package can be built and made available to users without the need for elevated privileges, SD/IT wants the option of using this feature. Therefore, the Group Policy establishes the possibility while ensuring strict security.
   a. Disable Windows Installer – Enabled (For non-managed applications only). This allows SD/IT to select what can be deployed, especially for approved freeware, shareware or where licensing is adequate for all GIAC Enterprises systems (typically software bought under enterprise license agreements).
   b. Disable patching – Enabled. Used by SD/IT to prevent a loss of version control.
   c. Cache transforms in secure location on workstation – Enabled (Check to force settings on). This is set as a security measure to prevent malicious users or hackers from editing transform files used by Windows Installer that are left on the system.

System – Many settings could affect system performance and until SD/IT has a reason to need to configure these settings, they have been left "Not configured". Where setting could affect system security or make it easier to support, those settings have been changed. The following are those values that have been changed and why.

1. Disable Autoplay - Enabled (All drives). This prevents the autoplaying of all media inserted into removable drives, including CD-Rom drives, thus preventing unknowing installation of any software, etc.
2. Logon – All settings (except "Add the Administrators security group to roaming user profiles") were left as "Not configured". SD/IT will only change these settings after a base line of system performance has been established or if problems in system performance arise.
   a. Add the Administrators security group to roaming user profiles – Enabled. Enabling this will allow the auditing of roaming user profiles, especially in cases of internal user misconduct on the system.
3. Disk Quotas – This policy is to be used to discourage users from using local hard drives and to prevent a malicious user from systematically saving data to a local drive or removable media. All settings are "Enabled" except for the "Default quota limit and warning level" which is set to "Not configured". This setting will be established in the Group Policy for each organization's OU. The size allowed will depend upon the software needed by users in each organization and the disk space the software requires to operate efficiently. Since different organizations will have different software mixes, this cannot be set here.
4. DNS Client – set to "corp.GIACEnt.com".
5. Group Policy – Since most GIAC Enterprises users will not have time limits set for using computers, users can be left logged on (sometime with reason) for long

periods. SD/IT does want changes to Group Policies be added because even in this situation. Where the Group Policy settings will not support this policy, SD/IT has changed those settings as necessary to implement this policy. The following settings have been set to force Group Policy changes and the reasons why.

a. Disable background refresh of Group Policy – Disable. SD/IT wants Group Policy changes to propagate even if a user does not log out.
b. Apply Group Policy for computers asynchronously during startup – Not configured.
c. Apply Group Policy for computers asynchronously during logon – Not configured.
d. Group Policy refresh interval for computers – Not configured. This are set at the OU level as the operational needs of each organization may dictate different intervals.
e. User Group Policy loopback processing mode – Merge. The design of the Group Policies is to be additive, therefore local computer policy will not specify all settings, only those that differ or add to the Domain policy.
f. Registry policy processing – Not Configured. This has not been set even though there is a useful security purpose for this setting. Until all GIAC Enterprises organizations and their custom software and databases are fully migrated to the Windows 2000 environment, SD/IT cannot afford to set this policy for fear of breaking legacy applications.
g. Internet Explorer Maintenance policy processing – Enabled ("Do not apply during periodic background processing" is not checked). GIAC Enterprises does not yet have any Web enabled corporate applications, so SD/IT determined this to be the more secure setting.
h. Software Installation policy processing – Not Configured. This has not been set even though there is a useful security purpose for this setting. Until all GIAC Enterprises organizations and their custom software and databases are fully migrated to the Windows 2000 environment, SD/IT cannot afford to set this policy for fear of breaking legacy applications.
i. Security policy processing – Enabled ("Do not apply during periodic background processing" is not checked). System security is a priority to GIAC Enterprises, so SD/IT determined this to be the more secure setting.
j. IP Security policy processing – Enabled ("Do not apply during periodic background processing" is not checked). Since IPSec will play a role in the future of the network (once all of GIAC Enterprises is on Windows 2000 and when partner and customer agreements are set up to support IPSec), setting this as described will allow for the most rapid implementation of a new policy.
k. EFS recovery policy processing – Enabled ("Do not apply during periodic background processing" is not checked). Should a need to update this policy be required, it will allow this to be propagated quickly.
l. Disk Quota policy processing – Enabled ("Do not apply during periodic background processing" is not checked). Should changes be needed (e.g. if new programs are added and more space is required on the user's computer), this would allow them to propagate quickly.

6. Windows File Protection – Except for the "Specify Windows File Protection cache location" setting, all settings were left "Not Configured". The cache location was changed so that hackers would not know the location of protected files.

Network - Many settings could affect system performance and until SD/IT has a reason to need to configure these settings, they have been left "Not configured". Where setting could affect system security or make it easier to support, those settings have been changed. The following are those values that have been changed and why.

1. Offline files – GIAC Enterprises policy is not to encourage the use of local hard drives for storage. Specifically as an ISO 9001/9002 certified organization, GIAC Enterprises must control the revisions to procedures. Saving versions of these files for offline use would pose the threat of someone using an out-of-date procedure. For these reasons 3 settings have been configured:
    a. Disable user configuration of Offline Files – Enabled.
    b. Disable "Make Available Offline" – Enabled.
    c. At logoff, delete local copy of user's offline files – Enabled.

2. Network & Dial-Up Connections – "Allow configuration of connection sharing" so administrators cannot set up share dial-in connections on servers. This is an added security measure.

Printers – These values shall be set at the OU level if they are deemed necessary for operations and security.

Users

Software Settings

Software Installation – SD/IT uses this feature extensively to prepare over the network installation packages. SD/IT will not establish any packages at the Domain level in order to avoid bandwidth problems with remote site and remote user systems. Therefore, there are no settings here.

Windows Settings

Internet Explorer Maintenance – These settings have been set to meet the GIAC Enterprises Acceptable Use Policy, the proposed designs of GIAC Enterprises Web-based applications and the need to simplify the support of the network for the SD/IT staff.

Browser User Interface - These settings customize the Browser Interface (Title Bar, Animated Bitmap, Toolbar Buttons and Custom Logos). SD/IT removes the Messenger button through these settings.

Connection – These settings modify the way the Browser connects to the Internet, Automatic Browser Configuration, Proxy Settings and User Agent String. SD/IT uses these settings to ensure only the network is used to connect to the Internet through a defined proxy server. Additionally, a URL is provided where SD/IT can periodically have the client go to get updated settings for the browser.

URLs – These settings establish defaults for Favorites and Links, Important URL's and Channels. SD/IT uses this to configure a standard for Important Links (based on Intranet and Customer and Partner URL's) and forces the deletion of all Channels.
Security – These settings establish Security Zones and Content Ratings and the Authenticode Settings (Trusted Publishers certificates). SD/IT implements the Security Zones and Content Ratings based upon the the GIAC Enterprises Acceptable Use Policy (no profanity, nudity, etc.) and set Partner and Customer Web sites in to the Trusted Zone as directed by Management through these settings. Software Publisher certificates approved by SD/IT are also added and then locked out so a user can not add additional ones.
Programs – Used to set the Internet programs (e-mail client, HTML editor, etc.). SD/IT sets each to the standard GIAC Enterprises software used for each.

Scripts – The log on and log off scripts shall be set at the OU level so they may be tailored to the specific needs of the organizations.
Security Settings – Public Key Policies – SD/IT has set up the Enterprise Trust to list Internal Certificates issued that are standard across the enterprise. Others may be added for OU level usage.
Remote Installation Services – The defaults are acceptable and no changes are to be made.
Folder Redirection – Currently, SD/IT has no need to redirect these standard folders. After an organization (and all its standard applications) is moved to Windows 2000 and a baseline requirement is set up for each, SD/IT may utilize these options to enhance ease of support.

Administrative Templates - GIAC Enterprises corporate policy requires high security and the SD/IT organization has limited personnel to administer the large network across a wide campus. Therefore, settings in these areas have been set to maximize general security and ease of administration.

Windows Components –

1. Net Meeting – Disabled. Most Net Meeting user settings are set to disable functionality. This prevents users from using most of the features of Net Meeting until each organization develops a policy for its use. Where specific departments and GIAC Enterprises management allow, the settings may be changed in the OU Group Policy for that organization (e.g., Management).
   a. Internet Explorer – IE represents a constant risk to the network as well as the GIAC Enterprises Acceptable Use Policy. Most settings for IE have been set to the most restrictive setting.
2. Windows Explorer – Most settings do not affect the manner the security of the network. For those few that do, SD/IT has set those values. The following is a list of those changes and why.

a. Only allow approved Shell extensions – Enabled. Should a hacker manage to load their own shell utility, the Group Policy may possibly prevent it from being used.
b. No "Computers Near Me" in My Network Places – Enabled. Prevents a malicious user from doing a reconnaissance from a single computer.
c. No "Entire Network" in My Network Places – Enabled. Prevents a malicious user from doing a reconnaissance from a single computer.

3. Microsoft Management Console – These options are not configured at this level. They are configured at the OU level based upon the delegation of administration that SD/IT will use for each OU.
4. Task Scheduler – These settings are configured in the *Computer Configuration* folder.
5. Windows Installer – All settings were left "Not configured" except "Search order" where this was enabled and the URL source was deleted. This is an additional way to prevent the installation of software from sources external to GIAC Enterprises network. GIAC Enterprises policy dictates those users that need to download software (such as system administrators) will do so on standalone systems where it will not affect the network directly.

Start Menu & Task Bar – Most settings do not affect the manner the security of the network. For those few that do, SD/IT has set those values. The following is a list of those changes and why.

1. Disable and remove links to Windows Update – Enabled. SD/IT does not want the possibility of changing system components with out first reviewing the impact upon the systems and software the corporation runs. Enabling this aided this policy.
2. Remove Network and Dial-up Connections from Start Menu – Enabled. SD/IT does not want the possibility of users connecting telephone lines and using dial-up capability. Enabling this option supports this policy.
3. Add Logoff to the Start Menu – Enabled. Added as a convenience for the users.

Desktop – There are no settings configured here. These options have little effect on the manner SD/IT will support the network or have is insufficient security value. If there becomes a problem, SD/IT can revisit this policy.

Control Panel – There are no settings configured here. These options are set at the OU level consistent with security needs and the GIAC Enterprises acceptable use policy (particularly the "Add/Remove Program settings").

Network

1. Offline Files – These settings are configured in the *Computer Configuration* folder.
2. Network and Dial-up Connections – Most of the settings in this section that apply to users can be superceded by other settings elsewhere or are already superceded by other settings within the section. For these settings, most were left as "Not configured" to avoid confusion and conflicting with other Group Policy settings. The remainder of the settings affects the manner in which administrators can access Networking and Dial-up properties. These

settings are left as "Not Configured" and are set at the OU level and integrated with delegated administration of those OU's. The following are those settings that were configured and why.

a. Prohibit connecting and disconnecting a RAS connection – Enabled. SD/IT sets this as an additional measure to prevent the use of remote access capability.
b. Prohibit enabling/disabling a LAN connection – Enabled. SD/IT sets this as an additional measure of preventing users from mis-configuring their computers.
c. Prohibit access to the Dial-up Preferences item on the Advanced menu – Enabled. SD/IT sets this as an additional measure of preventing the use of Dial-In capability.

System – Many settings within this section can affect system performance and until SD/IT has a reason to configure these settings, they have been left "Not configured". Many other settings are also listed in *Computer Configuration* folder where that setting takes precedence. For many of the remaining settings, if it is determined to be in required, they are best set at the OU level as users in different organizations will require different settings. For those few settings where SD/IT evaluated that there could be an affect on system security or make it easier to support, those settings have been changed. The following are those values that have been changed and why.

1. Century interpretation for Year 2000 – Enabled (2049). Set for user convenience.
2. Disable registry editing tools – Not configured. SD/IT sets this setting at the OU level and integrates it with the delegation of system administration at those levels.
3. Logon/Logoff – no changes have been here for the reasons stated above.
4. Group Policy – no changes have been here for the reasons stated above.

Default Domain Controllers Group Policy

GIAC Enterprises selected to use the High Security Templates for domain controllers for the reasons detailed previously. The following explains the reasoning for using the specific settings and where they are changed from the settings in the templates and why. (Settings that were changed and noted above in the Domain Policy that are also in the Domain Controller Group Policy are not repeated if the settings are the same).

Computers

Software Settings

Software Installation – No changes from the Domain Policy.

Windows Settings – Security Settings

Account Policies – No changes from the Domain Policy.

Local Policies – No changes from the Domain Policy except as noted below.

1. Audit Policy – No changes from the templates.
2. User Rights Assignments – Deny logon as a batch job - Changed from none assigned to Administrators. Only these accounts are enabled in "Log on as a batch job" should be logging on using a batch job.
3. Security Options – Renamed Administrator/Guest Accounts –Used non-standard account names as an addition layer of protection from hackers.

Event Log – No changes from the Domain Policy.
Restricted Groups – No changes from the Domain Policy.
System Services – No changes from the Domain Policy except as noted below

1. IIS Admin – Set to Manual with rights to Administrators. When the GIAC Enterprises Intranet is moved to Windows 2000, this policy shall be changed to add an IIS Administrators group.
2. Windows Installer – Manual with rights to only Administrators.
3. WWW Publishing Service - Set to Manual with rights to Administrators. When the GIAC Enterprises Intranet is moved to Windows 2000, this policy are changed to add an IIS Administrators group.

Registry – No changes from the Domain Policy.
File System – No changes from the Domain Policy.
Public Key Policies – No changes from the Domain Policy.
IP Security Policies on Active Directory – No changes from the Domain Policy except the Secure Server Policy is "assigned".

Administrative Templates - No changes from the Domain Policy except as noted below.

Windows Components – No changes from the Domain Policy.
System – No changes from the Domain Policy except there are no "Disk Quotas" settings configured (including the "Disk Quota policy processing" in the Group Policy Folder).

User Configuration

Software Settings

Software Installation – No changes from the Domain Policy.

Windows Settings – No changes from the Domain Policy.

Administrative Templates – No changes from the Domain Policy.

Additional Group Policies – Management and Engineering

At the Domain level, several Group Policy settings are left for the OU level Group Policies to set because there are differences in how each organization uses the network that affects the security of the network and the support required by the SD/IT organization. The following is an example of two OU's.

Management – As described in Part 3, this OU will allow individuals defined as Management to access specifically defined organizational information and IT resources based upon a group policy. SD/IT will not delegate the administration of this OU. The following are Group Policy differences and additions established at this OU level:

Computers

Software Settings

Software Installation – All software that is widely used by management personnel are installed using installation packages.

Windows Settings – Security Settings

Account Policies – No changes or additions to the Domain Policy.

Local Policies –

1. Audit Policy – No changes or additions to the Domain Policy.
2. User Rights Assignments – No changes or additions to the Domain Policy.
3. Security Options –.
   a. Secure channel: Require strong (Windows 2000 or later) session key – SD/IT has left this as set by the template (enabled). When the Windows 2000 systems are allowed to connect to customer and partner Domains, it may be necessary to change the settings for the "Secure Channel: Require strong (Windows 2000 or later) session key" based upon negotiated arrangements with these organizations. Even at then, this key will remain enabled for Management OU computers as an extra measure of security.

Event Log – No changes or additions to the Domain Policy.

Restricted Groups – Periodically, SD/IT will review group assignments and purge current groups using the Restricted Groups. Membership in the Management OU groups is reviewed monthly due to the added sensitivity of the information available to the users of this OU.

System Services – No changes or additions to the Domain Policy.

Registry – No changes or additions to the Domain Policy.

File System - No changes or additions to the Domain Policy.

Public Key Policies – No changes or additions to the Domain Policy.

IP Security Policies on Active Directory – The Management OU is one of the few where SD/IT will implement IPSec on all systems assigned to the OU. All Management OU clients will require IPSec. The Management OU Security policy will "require security" for all IP traffic. This prevents internal users and external hackers from sniffing Management OU client and server traffic.

1. General Setting changes: The Master key Perfect Forward Secrecy is enabled.
2. Rule Setting changes: A filter list has been added for all IP traffic where all traffic requires security.

Administrative Templates –

Windows Components –

1. Net Meeting – Remote desktop sharing - Enabled. The Management OU Group Policy allows the sharing of their desktop environments. With the added security of IPSec, the risk presented here is mitigated sufficient to allow the added capability of Net Meeting.

System – Many settings here could affect system performance. Until SD/IT has a reason to configure these settings, they are left "Not configured". For those few settings where system security could be affected or it makes it easier to support the network, SD/IT has made changes. The following are those values that have been changed and why.

1. Disk Quotas – "Default quota limit and warning level" is enabled and set to 50 MB.
2. Group Policy – Group Policy refresh interval for computers – Enabled with a 90-minute interval and 30-minute random time added.

Network - No changes or additions to the Domain Policy.

Printers – No changes or additions to the Domain Policy.

User Configuration

Software Settings

Software Installation – No changes from the Domain Policy.

Windows Settings – No changes from the Domain Policy.

Administrative Templates –

Windows Components – No changes from the Domain Policy.
Start Menu & Task Bar – No changes from the Domain Policy.
Desktop – No changes from the Domain Policy.
Control Panel –

1. Add/Remove Programs
   a. Disable Add/Remove Programs – Enabled. This prevents users from adding programs via the Control Panel. This aids SD/IT in preventing

unauthorized software from being added to the network and promotes version control.

b. Hide Change or Remove Programs page – Enabled. This aids SD/IT in preventing unauthorized software from being added to the network thus promoting version control.
c. Hide Add/Remove Windows Component page – Enabled. This aids SD/IT in preventing users from altering the configuration of their systems, thus reducing operational problems caused by users and/or opening security threats to the client or network.
d. Disable Support Information – Enabled. This prevents users from having access to program support information including hyperlinks to support information on the Internet. In general, all users should go to the SD/IT Help Desk when problems occur. Disabling Support Information promote the likelihood that users will use the Help Desk instead of troubleshoot their systems. Allowing the use of Support Information when users do not have a full understanding of the system design can cause more problems and/or introduce a security risk to the client and/or network.

Network – No changes from the Domain Policy.
System – No changes from the Domain Policy.

Engineering – As described in Part 3, this OU will allow individuals in the Engineering Department to access specifically defined organizational information and IT resources based upon a group policy. SD/IT will delegate the administration of this OU. The following are Group Policy differences and additions established at this OU level.

Computers
Software Settings
Software Installation – All software that is widely used by engineering personnel are installed using installation packages.

Windows Settings – Security Settings
Account Policies – No changes or additions to the Domain Policy.

Local Policies – No changes or additions to the Domain Policy.

Event Log – No changes or additions to the Domain Policy.

Restricted Groups – Periodically, SD/IT will review group assignments and purge current groups membership by using the Restricted Groups. The membership to Engineering OU groups is reviewed biannually due to the added sensitivity of the information (research and development data) available to the users of this OU.

System Services – No changes or additions to the Domain Policy.

Registry – No changes or additions to the Domain Policy.

File System - No changes or additions to the Domain Policy.

Public Key Policies – No changes or additions to the Domain Policy.

IP Security Policies on Active Directory – The Engineering OU is one of the few locations where SD/IT will implement IPSec. Engineering personnel often must utilize computing resources that reside at non-GIAC Enterprises sites, often with sensitive information involved. Therefore, all Engineering OU systems will require IPSec when their communication leaves the Domain. As there is often research and development data handled by the Engineering Department, Engineering systems will be set to request IPSec for internal communications. This prevents internal users and external hackers from sniffing Engineering OU client and server traffic when that traffic involves research and development data that is to be stored only in approved network locations.

1. General Setting changes: The Master key Perfect Forward Secrecy is enabled.
2. Rule Setting changes: A filter list is added for all IP traffic (external to the DNS domain) where all traffic requires security and a filter for all IP traffic (internal to the DNS domain) where all traffic requests security.

Administrative Templates -
Windows Components – No changes or additions to the Domain Policy.

System – Many settings within this section could affect system performance. Until SD/IT has a reason to configure these settings, they are left "Not configured". For those setting where system security could be affected or it makes it easier to support the network, SD/IT has made changes. The following are those values that have been changed and why.

1. Disk Quotas – "Default quota limit and warning level" is enabled and set to 500 MB. Since many applications used by engineering personnel require large amounts of local disk use (e.g., finite element analysis software and computer aided modeling), this value has been set high.
2. Group Policy – Group Policy refresh interval for computers – Enabled with a 90-minute interval and 30-minute random time added.

Network - No changes or additions to the Domain Policy.

Printers – No changes or additions to the Domain Policy.
User Configuration
Software Settings
Software Installation – No changes from the Domain Policy.

Windows Settings – No changes from the Domain Policy.

Administrative Templates –
Windows Components – No changes from the Domain Policy.
Start Menu & Task Bar – No changes from the Domain Policy.

Desktop – No changes from the Domain Policy.
Control Panel –

3. Add/Remove Programs
    e. Disable Add/Remove Programs – Enabled. This prevents uses from adding programs via the Control Panel. This aids SD/IT in preventing unauthorized software from being added to the network and promotes version control.
    f. Hide Change or Remove Programs page – Enabled. This aids SD/IT in preventing unauthorized software from being added to the network and promotes version control.
    g. Hide Add/Remove Windows Component page – Enabled. This aids SD/IT in preventing users from altering the configuration of their systems, thus reducing operational problems for the user and/or opening security threats to the client or network.
    h. Disable Support Information – Disabled. This allows Engineering users to have access to program support information including hyperlinks to support information on the Internet. In general, all users should go to the SD/IT Help Desk when problems occur. Allowing users to troubleshoot their system problems with out a full understanding of the system design and settings can cause more problems and/or introduce a security risk to the client and/or network. However, the Engineering personnel often require support information for the engineering software used by the department when it is not functioning properly or as expected. Normally for this software, SD/IT is not sufficiently familiar with these software to do troubleshooting where the individuals using the software are.

Network – No changes from the Domain Policy.
System – No changes from the Domain Policy.

Because Group Policies cannot meet all security requirements for all situations, users and systems, GIAC Enterprises supplements the security of the network in some of the following ways.

Auditing – This administrative process helps to complete the security envelope in several ways. Performing reviews of domain controllers (daily), member server (at least weekly) and client audit logs (on a statistical basis) helps to answer questions concerning the health of the system. By performing these reviews, problems in system If the IDS's determine unusual activity, these logs aid in tracking down what happened. Group Policy does not serve to make these reviews, only to set their log file limits and accessibility. Review of the logs over time also provides trend analysis, thus assisting in fine-tuning system operations as well as system security.

Reviewing for New Vulnerabilities – This administrative process initiates the addition of new security measures for the systems when new vulnerabilities are discovered. Group Policies have no way to maintain a watch for new vulnerabilities. Therefore, SD/IT staff periodically reviews resources such as the SANS/FBI Twenty Most Critical Internet Security Vulnerabilities and subscribe to various computer security on-line newsletters and bulletin services.

Reviewing Patches and Software Upgrades – This administrative process is crucial to a large network that runs interconnected software systems and databases. Loss of version control means these systems have a high probability of losing that interoperability. GIAC Enterprises conducts its business through these systems. Loss of interoperability means delays and downtime for users who then cannot perform their work and this results in a loss of profitability to the corporation. Therefore, all patches and upgrades go through a rigorous testing before deploying onto the network. First, they undergo testing on the GIAC Enterprises test ring, and then undergo limited deployment (if possible) to systems within the SD/IT organization. Once the upgrades and patches pass that review, the patches can be installed manually. When large numbers of systems require the patches, Windows Installation packages are then developed and tested. Once these packages are tested, Group Policy can implement them across the network automatically.

Physical and Personnel Security – Group Policy only deals with the system. If there is no physical security, then any hacker can get direct access to the systems (i.e., steal or deny access to information). Personnel Security is important. If background checks are not done for new hires then internal system security is useless. There is no physical or system security if you hire the hacker who can then carry the system(s) off site without question and then hack the system at their leisure.

System Resources not managed by Active Directory – Not every piece of equipment is immediately going to be capable of interfacing with the Windows 2000 Active Directory, thus Group Policies have no effect on that equipment. Even after the completion of the conversion, some systems are to remain outside of the Windows 2000 environment.

The systems that are yet to be converted and those that will remain as they are will continue operations without the benefit of Group Policy.

GIAC Windows Security Administrator Practical
References

1. International Organization for Standards (ISO) 9001:2000, Quality Management Systems – Requirements; available on-line for purchase at http://www.iso.org/iso/en/CatalogueListPage.CatalogueList
2. International Organization for Standards (ISO) 9002:1994, Model for Quality Assurance in Production, Installation and Servicing; available on-line for purchase at http://www.iso.org/iso/en/CatalogueListPage.CatalogueList
3. Department Of Defense Standard 5200.28, Department Of Defense Trusted Computer System Evaluation Criteria, December 1985; available at http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html
4. Department Of Defense Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997; available at http://mattche.iiie.disa.mil/ditscap/DitscapFrame.html
5. Microsoft Corporation *Windows 2000 Server Deployment Planning Guide*, Redmond, WA: Microsoft Press, 2000.
6. Microsoft Corporation *Windows 2000 Security Technical Reference*, Redmond, WA: Microsoft Press, 2000.
7. Microsoft Corporation *Windows 2000 Distributed Systems Guide*, Redmond, WA: Microsoft Press, 2000.
8. National Security Agency Security Recommendation Guide: Windows 2000 Guides, 14 August 2002; available at http://nsa2.www.conxion.com/win2k/download.htm
9. Microsoft Corporation, Microsoft Knowledge Base Article - Q216899: Best Practice Methods for Windows 2000 Domain Controller Setup, available at http://support.microsoft.com/default.aspx?scid=kb;en-us;Q216899
10. The SANS/FBI Twenty Most Critical Internet Security Vulnerabilities (Updated) The Experts' Consensus Version 2.504 May 2, 2002 ©; available on their Web site: http://www.sans.org/top20.htm