Global Information Assurance Certification Paper

Designing a Secure Windows 2000 Infrastructure For GIAC Enterprises

By

Paul W. Rondorf

Table of Contents

Abstract

Global Information Automation & Computing (GIAC) Enterprises is an international computer hardware manufacturing company with offices in the United States (U.S.) and Canada. Information technology (IT) started as home grown networks in each of the three corporate locations almost 10 years ago. These isolated IT islands had little or no concern for security. The CEO and CIO of GIAC Enterprises noticed that competitors were taking advantage of recent advances in IT to expand their business and increase market share. GIAC was being left behind so the CEO and CIO hired me as a consultant. My job was to design a Windows 2000 (WIN2K) Active Directory (AD) Enterprise Network for GIAC Enterprises with security being paramount to a successful fielding of this new network. The three corporate locations could now share information in a secure, timely manner. GIAC also has an Internet presence and its secure e-commerce website is starting to take off. Salesmen and saleswomen also have a secure means of connecting into the GIAC network while traveling and meeting customers. The future looks bright for GIAC Enterprises as it just starts to leverage the wide range of capabilities the company's new WIN2K AD Enterprise Network.

Designing a Secure Windows 2000 Infrastructure for GIAC Enterprises
Paul W. Rondorf
GCWN, v3.1
4 April 2003

Introduction

Global Information Automation & Computing (GIAC) Enterprises is an international computer hardware manufacturing company with offices in the United States (U.S.) and Canada (See Figure 1). GIAC Enterprises specializes in the design, manufacture, and sale of ergonomic computer equipment. GIAC Enterprise's corporate headquarters (HQ) and United States (U.S.) offices are co-located in Nashville, Tennessee. Detroit serves as GIAC's manufacturing center. Winnipeg, Manitoba serves as the center of GIAC's Canadian Regional Office.

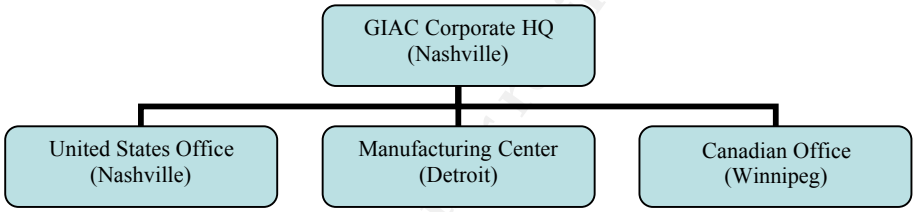

Figure 1: GIAC Organizational Structure

Corporate Headquarters contains the Human Resource (HR), Sales & Marketing (S&M), Finance & Accounting (F&A), and Purchasing Departments. The Manufacturing Center in Detroit contains GIAC's Research & Development (R&D) Department as well as Production and Shipping Departments. Regional Offices in Nashville and Winnipeg are primarily involved with sales so they each have a subordinate element of the Corporate Headquarters' Sales & Marketing Department. These Regional Offices also have small, local HR and F&A elements is residence to support the large sales staffs.

All GIAC locations have their own respective information technology (IT) departments which administer a local Windows NT4 domain. Each Windows NT4 domain has a Primary Domain Controller (PDC) and one Backup Domain Controller (BDC) and a file/print server. The NT4 domains at each GIAC location don't communicate with each other. Each location has approximately 400 Windows 9x, Windows NT4 desktop computers, or Windows 2000 desktop systems connected together over a local area network (LAN) for logon validation and file/print services. Neither Regional Office nor the Manufacturing Center has Internet connectivity. The Corporate Headquarters/U.S. Office has a Microsoft SQL Server v6.0 database server. Database administrators in the U.S. Office run queries for any corporate office and fax the results to the requesting office. GIAC has no consolidated email service.

The Chief Executive Officer (CEO) and the Chief Information Officer (CIO) realize that GIAC Enterprises hasn't used information technology (IT) very effectively up to this point in the company's existence. They want to change how GIAC uses IT in a number of ways. They've called me in to design and implement a secure Windows 2000 (WIN2K) network for GIAC Enterprises under the following conditions:

- The WIN2K network must be an enterprise network in which the disparate networks at the various company locations are merged so information can easily flow throughout the company.
- All Windows 9x and Windows NT4 desktops must be either upgraded to Windows 2000 Professional or replaced by desktops running Windows 2000 Professional.
- All GIAC servers will run Windows 2000 Server or Windows 2000 Advanced Server. Any server unable to run one of these variants of Windows 2000 Server must be replaced with a server running the appropriate version of Windows 2000 Server.
- Management of this new enterprise network must follow the centralized management and decentralized operations business model. IT policies are developed and tested by the IT Department at the Corporate Headquarters and then approved by the CEO/CIO. Decentralized execution comes next with the small IT Departments in each regional office and the manufacturing center implementing the IT policies.
- GIAC must build an Internet-based means of marketing products and services.
- The products GIAC wants to market over the Internet come directly from R&D's efforts to develop proprietary breakthroughs in ergonomic computer equipment.
- Sales & Marketing must be able to use the enterprise network to improve customer relations and customer management through the implementation of a customer database. The server(s) hosting this corporate database must be highly available.
- Sales & Marketing must also use the enterprise network to achieve the strategic business goal set down by the CEO of increasing GIAC Enterprise's online market share through a robust, highly available e-commerce initiative.
- Finance & Accounting and Human Resources want to use the IT services of this new enterprise network to improve internal accounting and employee records management. They also want to develop a web-based means for employees to check up on their respective personnel and finance records.
- The CEO and CIO want an enterprise electronic mail (email) messaging system with high availability built into the system.
- The CIO wants the internal DNS namespace and external DNS namespace to be different. The internal DNS server must also securely transfer DNS information.

- The CIO also to be able to seamlessly share files across the GIAC network.
- GIAC wants to support its large number of traveling sales people with virtual private network (VPN) support. These sales personnel will use a GIAC-supplied ISP account to establish an Internet connection and then VPN into the GIAC network.
- The CEO and CIO expect very rapid growth in their new web-based e-commerce business so they want to ensure adequate bandwidth is available to the Internet from the Corporate Headquarters. Funding for WAN connectivity is available as required.
- The CIO directs the implementation of Public Key Infrastructure (PKI) in order to enhance the security of key network services.
- The CEO and CIO feel security is of paramount importance to the GIAC enterprise network and should be implemented at all levels.

Network Design & Diagram

The GIAC WIN2K Active Directory (AD) enterprise network will have the following site design (See Figure 2):

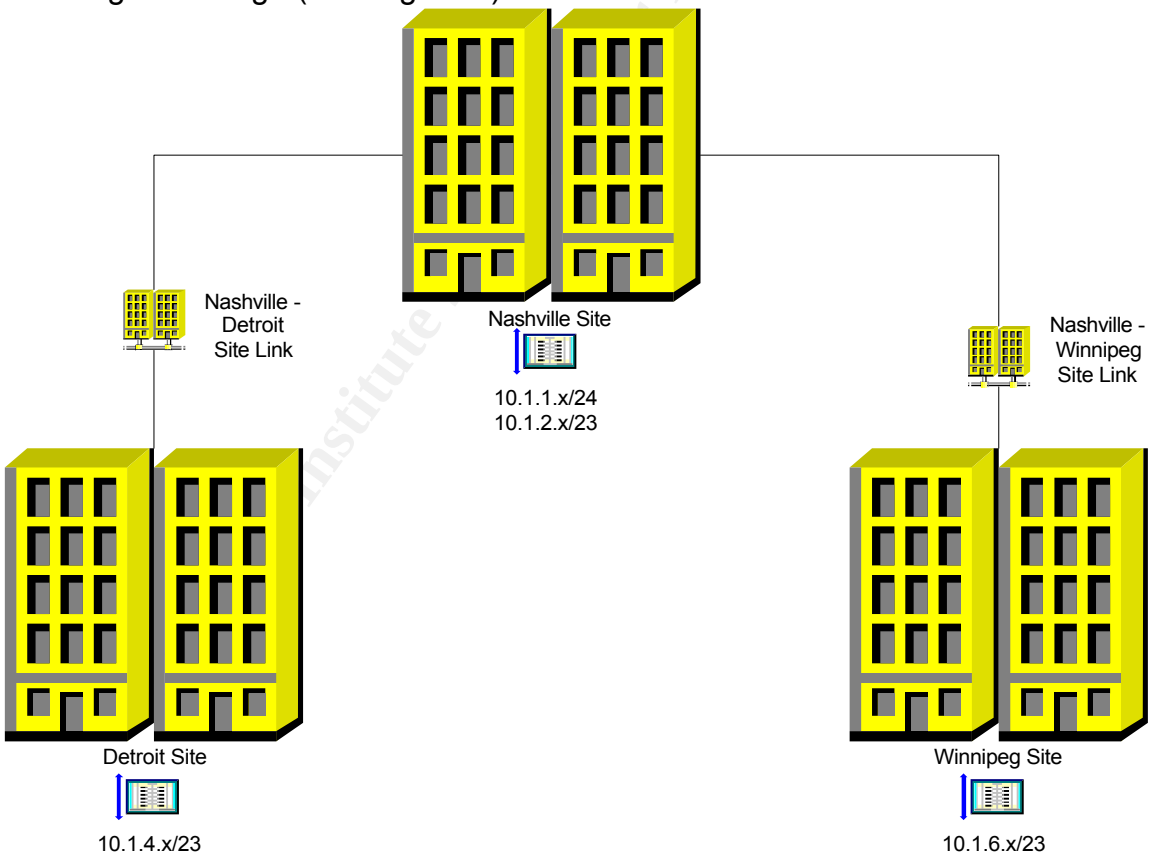

Figure 2: Site Design – GIAC WIN2K AD Enterprise Network

GIAC Enterprises will organize this WIN2K AD enterprise network into three sites: Nashville, Detroit, and Winnipeg. A site is defined as a group of one or more Internet Protocol (IP) subnets connected by high-speed links. The high-speed links in this environment are 100Mbps network connections at each GIAC site.

GIAC wants to organize its WIN2K domain architecture (See Figure 3) along the lines of a WIN2K AD root domain, **giac-ent.local**, and child domains company organizations at Nashville (**nashville.giac-ent.local**), Detroit (**detroit.giac-ent.local**), and Winnipeg (**winnipeg.giac-ent.local**).

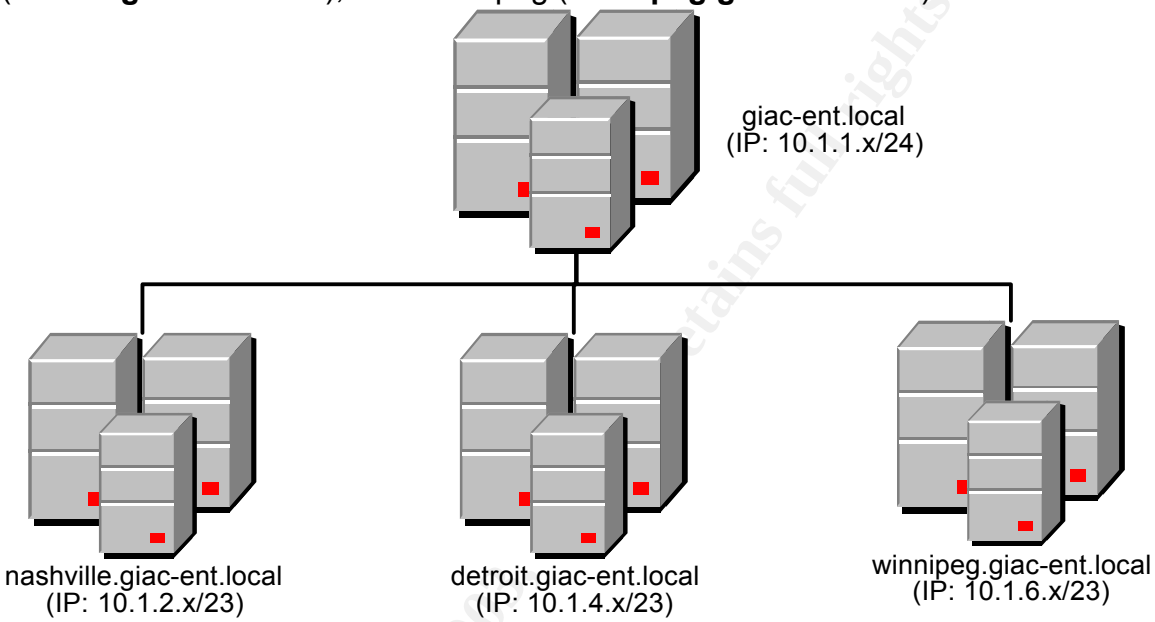

Figure 3: Domain Design – GIAC WIN2K AD Enterprise Network

Corporate Headquarters and the United States Office make up the Nashville site. The Detroit site contains the Detroit Manufacturing Facility. The Winnipeg site contains GIAC's Canadian Office. The Detroit and Winnipeg sites have dedicated T1 (1.544 Mbps) circuits connecting them to the Nashville Site (See Figure 4). The only connection the GIAC network has to the Internet is a T1 circuit from the Nashville site. The CEO of GIAC Enterprises authorized funding for these T1 (WAN) circuits in order to meet the requirement to have network connectivity between all corporate sites. LAN connectivity at each corporate site is Fast Ethernet (100Mbps) so LAN upgrades aren't required. GIAC also has a demilitarized zone (DMZ).

The Nashville site (Figure 5) contains two Windows 2000 (WIN2K) Active Directory (AD) native mode domains. The first WIN2K AD domain, **giac-ent.local** is the root domain. The second WIN2K AD domain, **nashville.giac-ent.local** is a child domain of **giac-ent.local**. The **giac-ent.local** domain is an empty WIN2K AD root domain contained in the GIAC CORPORATE HQ network. It only contains three WIN2K AD domain controllers which host the five Flexible Single Master Operation (FSMO) roles. Two of these five FSMO roles, Schema Master and Domain Naming Master, exist only in the root domain within a WIN2K AD forest.

- **Schema Master –** The domain controller holding this role (See Table 1) is the only domain controller that can perform write operations to the Active Directory's directory service. The schema defines which objects can be contained in the directory service and what attributes those objects can

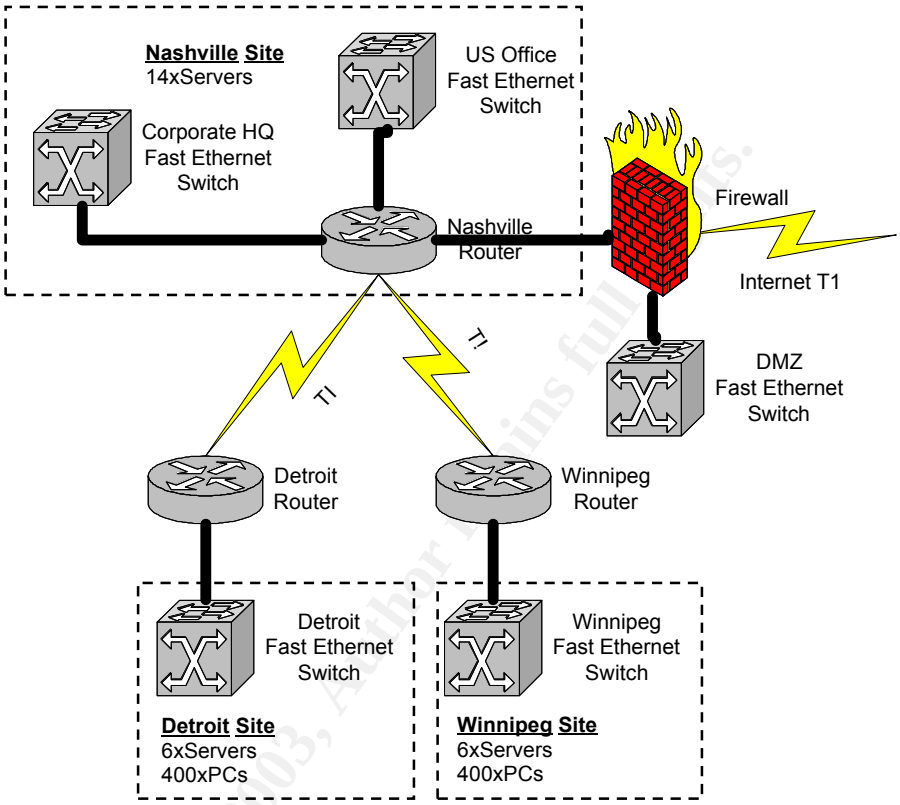

Figure 4: GIAC Enterprise WAN Architecture

have. A newly created WIN2K AD domain comes with a default schema which defines common network objects in the directory like users, groups, domains and computers. The schema is extensible in that new object classes and attribute types can be added to it. Members of the Schema Admins group have the rights needed to modify the schema the Active Directory Schema, a Microsoft Management Console (MMC) snap-in. Schema modification entails the creation of new classes and attributes, the modification of existing classes and attributes, and deactivation of existing classes and attributes. Schema modifications are irreversible and can cause extensive replication traffic throughout a WIN2K AD forest so they should be performed judiciously.

Schema Master/Domain Naming Master		
Fully Qualified Domain Name (FQDN)	**IP ADDRESS**	**WIN2K AD Domain**
GIAC-DC01.GIAC-ENT.LOCAL	10.1.1.2/24	GIAC-ENT.LOCAL

Table 1: Schema Master/Domain Naming Master

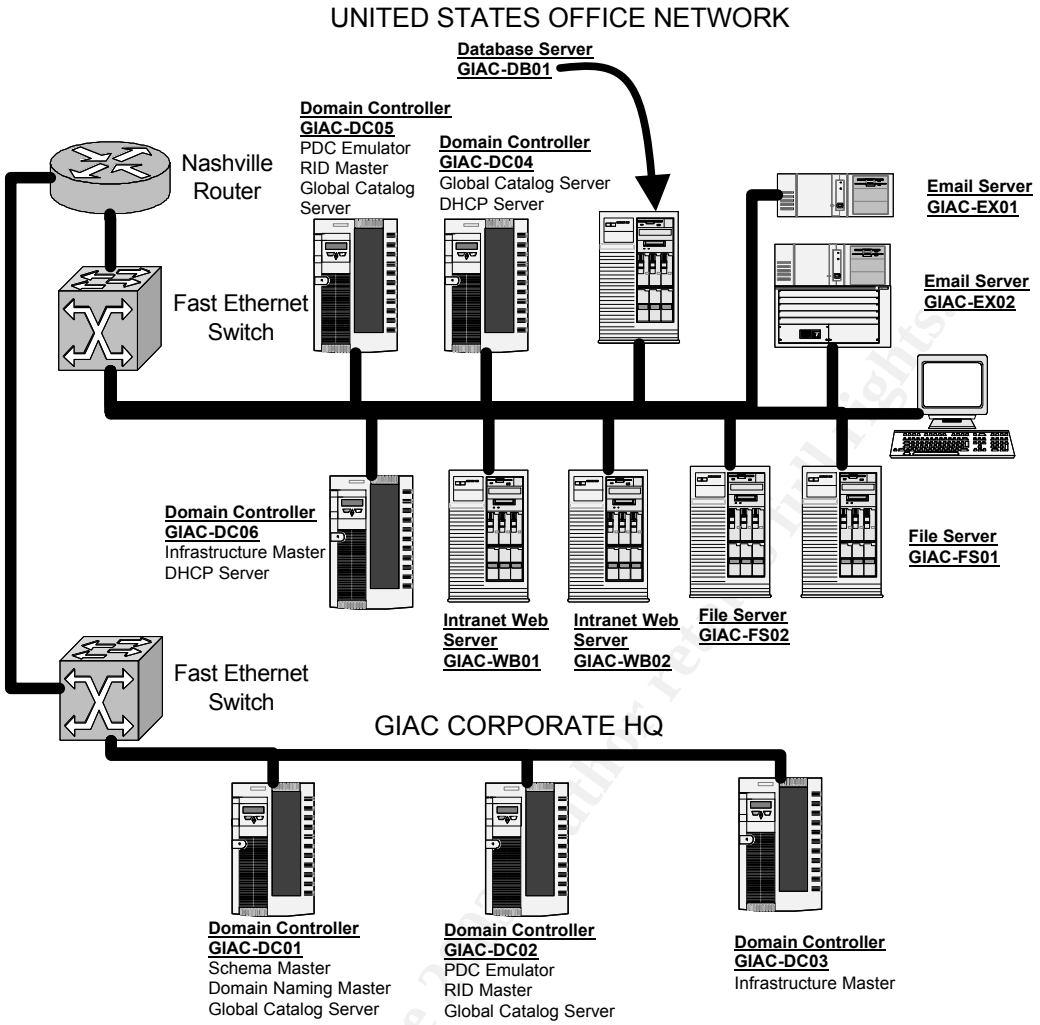

Figure 5: Nashville Site Network Architecture

- **Domain Naming Master –** the domain controller having this role (See Table 1) is the only domain controller in a WIN2K AD forest that can do the following:
    - Add new domains to the WIN2K AD forest.
    - Remove domains from the same WIN2K AD forest.
    - Add or remove cross-referenced objects to external directories.

  The other three FSMO roles; PDC Emulator, RID Master, and Infrastructure Master exist in each WIN2K AD domain within the forest.
- **PDC (Primary Domain Controller) Emulator –** The PDC Emulator (See Table 2) has a number of key functions in a native mode, WIN2K AD domain:
    - Password changes are sent preferentially to the PDC Emulator with other domain controllers querying the PDC Emulator if a password fails.
    - Group Policy Objects are still processed on the PDC Emulator by default.

  - The PDC Emulator preferentially processes account lockouts.

There are four WIN2K AD domains in the GIAC enterprise network so there will be four PDC Emulators.

- **Relative Identifier (RID) Master –** A security principal is an object in the Active Directory directory service of Microsoft Windows 2000 that can be assigned permissions and rights. A RID is given to each newly created security principal object (a user, group, or computer) created on any domain controller. Each domain controller has a pool of relative identifiers to draw from when creating these objects. A domain controller must contact the domain controller holding the RID Master role (See Table 2) for the domain when it needs to replenish its pool of relative identifiers. There are four WIN2K AD domains in the GIAC enterprise network so there will be four RID Emulators.

PDC Emulators/RID Masters		
Fully Qualified Domain Name (FQDN)	**IP ADDRESS**	**WIN2K AD Domain**
GIAC-DC02.GIAC-ENT.LOCAL	10.1.1.3/24	GIAC-ENT.LOCAL
GIAC-DC05.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.3/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-DC08.DETROIT.GIAC-ENT.LOCAL	10.1.4.3/23	DETROIT.GIAC-ENT.LOCAL
GIAC-DC11.WINNIPEG.GIAC-ENT.LOCAL	10.1.6.3/23	WINNIPEG.GIAC-ENT.LOCAL

Table 2: PDC Emulators/RID Masters

800xClient PCs

- **Infrastructure Master –** The Infrastructure Master (See Table 3) is responsible for resolving lookups between domains in a WIN2K AD forest. The Infrastructure Master is involved when a member from the **giac-ent.local** domain is given membership to a group in the **nashville.giac-ent.local** domain. It also updates the distinguished name (DN) and security identifier (SID) of objects that move between WIN2K AD domains. A good example being the moving of a user object from the **giac-ent.local** domain to the **nashville.giac-ent.local** domain. The Infrastructure Master must not be on the same domain controller as a Global Catalog server, but it should be in the same site as it is in the **giac-ent.local** domain.

Infrastructure Master		
Fully Qualified Domain Name (FQDN)	**IP ADDRESS**	**WIN2K AD Domain**
GIAC-DC03.GIAC-ENT.LOCAL	10.1.1.4/24	GIAC-ENT.LOCAL
GIAC-DC06.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.4/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-DC09.DETROIT.GIAC-ENT.LOCAL	10.1.4.4/23	DETROIT.GIAC-ENT.LOCAL
GIAC-DC12.WINNIPEG.GIAC-ENT.LOCAL	10.1.6.4/23	WINNIPEG.GIAC-ENT.LOCAL

Table 3: Infrastructure Masters

It is anticipated that the Infrastructure Master server in each WIN2K AD domain will have a good load placed on it due to a lot of anticipated changes being made due to cross-domain group memberships. Also, the Infrastructure Master must not be on the same domain controller as the Global Catalog server. However, it must be in the same WIN2K AD site as a Global Catalog server. There are four WIN2K AD domains in the GIAC enterprise network so there will be four Infrastructure Masters.

- **Global Catalog –** The role played by the Global Catalog server (See Table 4) in the GIAC WIN2K AD enterprise is also crucial. Global Catalog servers allow GIAC network clients to search for user, group, domain and computer objects located anywhere in the GIAC WIN2K AD forest. The

Global Catalog Servers		
Fully Qualified Domain Name (FQDN)	**IP ADDRESS**	**WIN2K AD Domain**
GIAC-DC01.GIAC-ENT.LOCAL	10.1.1.2/24	GIAC-ENT.LOCAL
GIAC-DC02.GIAC-ENT.LOCAL	10.1.1.3/24	GIAC-ENT.LOCAL
GIAC-DC04.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.2/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-DC05.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.3/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-DC07.DETROIT.GIAC-ENT.LOCAL	10.1.4.2/23	DETROIT.GIAC-ENT.LOCAL
GIAC-DC08.DETROIT.GIAC-ENT.LOCAL	10.1.4.3/23	DETROIT.GIAC-ENT.LOCAL
GIAC-DC10.WINNIPEG.GIAC-ENT.LOCAL	10.1.6.2/23	WINNIPEG.GIAC-ENT.LOCAL
GIAC-DC11.WINNIPEG.GIAC-ENT.LOCAL	10.1.6.3/23	WINNIPEG.GIAC-ENT.LOCAL

Table 4: Global Catalog Servers

Global Catalog is also essential to the ability of GIAC network users being able to log on to any of the GIAC WIN2K AD native-mode domains. The logon process in a GIAC WIN2K AD native-mode domain requires a check for universal group membership which entails querying a Global Catalog server. Universal groups contain members from any domain in the GIAC WIN2K AD forest. These universal groups can also be granted permissions to access resources in any domain within the WIN2K AD forest. The GIAC Global Catalog contains a listing of universal group membership for each GIAC user. GIAC's Global Catalog information is updated each time AD performs directory replication which is every 15 minutes, by default, in each WIN2K AD site. Users need fast, reliable access to the domain controllers hosting a copy of the Global Catalog in order to logon to their WIN2K AD domain in a timely manner. Therefore, it is important that each GIAC site have at least on Global Catalog server within the site. Fault tolerant requirements dictate that each WIN2K AD domain have at least two Global Catalog servers. All GIAC WIN2K AD domains: **giac-ent.local**, **nashville.giac-ent.local**, **detroit.giac-ent.local**, and **winnipeg.giac-ent.local** will have two Global Catalog servers.

The hardware configuration of each domain controller in the GIAC WIN2K AD enterprise will have 2x900MHz PIII CPUs, 1GB RAM, a Fast Ethernet (100MB) NIC, the Windows 2000 operating system installed on a RAID1 array of 18.2GB drives, the transaction logs in a second RAID1 array of 18.2GB hard

drives, and the Active Directory running on a RAID5 array of four 18.2GB hard disk drives. All domain controllers will apply Service Pack 3 since the Corporate Headquarters IT Office has cleared this software for installation after extensive lab testing.

The WIN2K AD domain operating on the US OFFICE NETWORK (Figure 3), **nashville.giac-ent.local**, has a number of additional key network services running on several additional servers which run either Windows 2000 Server or Windows 2000 Advanced Server. These key network services exist to meet the WIN2K AD requirements laid down by the CEO and CIO. A brief description with employment considerations follows:

- **Domain Name Service (DNS):** DNS is critical to the successful implementation and operation of any WIN2K AD enterprise network. It is the primary means by which key network services and resources are located in a WIN2K AD domain. Internal DNS within the GIAC WIN2K AD enterprise (See Table 5) will be AD-integrated. AD-integration of DNS

DNS Servers Fully Qualified Domain Name (FQDN)	IP ADDRESS	WIN2K AD Domain
GIAC-DC01.GIAC-ENT.LOCAL	10.1.1.2/24	GIAC-ENT.LOCAL
GIAC-DC02.GIAC-ENT.LOCAL	10.1.1.3/24	GIAC-ENT.LOCAL
GIAC-DC03.GIAC-ENT.LOCAL	10.1.1.4/24	GIAC-ENT.LOCAL
GIAC-DC04.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.2/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-DC05.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.3/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-DC06.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.4/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-DC07.DETROIT.GIAC-ENT.LOCAL	10.1.4.2/23	DETROIT.GIAC-ENT.LOCAL
GIAC-DC08.DETROIT.GIAC-ENT.LOCAL	10.1.4.3/23	DETROIT.GIAC-ENT.LOCAL
GIAC-DC09.DETROIT.GIAC-ENT.LOCAL	10.1.4.4/23	DETROIT.GIAC-ENT.LOCAL
GIAC-DC10.WINNIPEG.GIAC-ENT.LOCAL	10.1.6.2/23	WINNIPEG.GIAC-ENT.LOCAL
GIAC-DC11.WINNIPEG.GIAC-ENT.LOCAL	10.1.6.3/23	WINNIPEG.GIAC-ENT.LOCAL
GIAC-DC12.WINNIPEG.GIAC-ENT.LOCAL	10.1.6.4/23	WINNIPEG.GIAC-ENT.LOCAL

Table 5: DNS Servers

means that DNS zone data within each WIN2K AD domain is converted into directory objects within the WIN2K AD domain. These DNS directory objects are now replicated as part of the normal AD multimaster replication to every domain controller within the domain. Since each WIN2K AD domain within the GIAC enterprise has only one site, DNS changes are replicated every 15 minutes. AD-integration of DNS zone data also allows for secure dynamic updates by WIN2K clients. These WIN2K clients can only negotiate secure dynamic DNS updates using Kerberos with WIN2K AD domain controllers within their respective domains.

- **Dynamic Host Configuration Protocol (DHCP):** DHCP is a client-server protocol which dynamically assigns Internet Protocol (IP) addresses and IP configuration information to hosts on an internetwork. This child WIN2K

AD domain, **nashville.giac-ent.local**, has the DHCP service running on two DHCP servers, **GIAC-DC04** and **GIAC-DCO6**. System administrators will employ the 80 – 20 rule on these DHCP servers to provide a measure of fault tolerance. Each DHCP server will have the IP subnet for the US OFFICE NETWORK, 10.1.2.x/23, configured in a DHCP scope on each respective server. **GIAC-DC04** will exclude 20% of the IP addresses of its DHCP scope from being leased and provide IP address leases from the other 80% of the IP addresses available in the scope. **GIAC-DC06** will exclude 80% of the IP addresses from its DHCP scope and provide IP address leases from the other 20% of the IP addresses available in the scope. System administrators will ensure that the IP addresses available on each DHCP server don't overlap so the same IP address won't be leased from each DHCP server. The statically assigned IP address of each WIN2K server in the **nashville.giac-ent.local** domain will also be excluded from each DHCP server's scope. Default dynamic update options for a WIN2K DHCP client computer also apply. The DHCP client will register its own A resource record. The client will request that the DHCP server register its PTR resource record. The DHCP service only exists within the WIN2K AD child domains (See Table 6) since the three computers in the **giac-ent.local** root domain are all domain controllers with static IP addresses.

DHCP Servers		
Fully Qualified Domain Name (FQDN)	**IP ADDRESS**	**WIN2K AD Domain**
GIAC-DC04.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.2/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-DC06.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.4/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-DC07.DETROIT.GIAC-ENT.LOCAL	10.1.4.2/23	DETROIT.GIAC-ENT.LOCAL
GIAC-DC09.DETROIT.GIAC-ENT.LOCAL	10.1.4.4/23	DETROIT.GIAC-ENT.LOCAL
GIAC-DC10.WINNIPEG.GIAC-ENT.LOCAL	10.1.6.2/23	WINNIPEG.GIAC-ENT.LOCAL
GIAC-DC12.WINNIPEG.GIAC-ENT.LOCAL	10.1.6.4/23	WINNIPEG.GIAC-ENT.LOCAL

Table 6: DHCP Servers

- **Email:** Exchange 2000 (E2K) Server will provide GIAC's electronic mail service. E2K is a reliable, scalable messaging solution which integrates with WIN2K AD directory service. The **nashville.giac-ent.local** domain will host the E2K bridgehead server, GIAC-EX01.NASHVILLE.GIAC-ENT.LOCAL, and one two-node E2K cluster, GIAC-EX02.NASHVILLE.GIAC-ENT.LOCAL, for the 800 mailboxes of the GIAC Corporate Headquarters and the US Office. The E2K bridgehead server will have 2x900MHz PIII CPUs, the WIN2K and E2K software installed on a 36.4GB RAID1 array, 1GB RAM, and a Fast Ethernet (100MB) NIC. The **detroit.giac-ent.local** domain and the **winnipeg.giac-ent.local** domains will each have a two-node E2K cluster for the mailboxes of the 400 users in each domain. The E2K servers must run Windows 2000 Advanced Server in order to take advantage of Microsoft Cluster Service. These E2K servers are clustered in order to meet the requirement that GIAC's email service is highly available. Each node of the E2K cluster will

have 2x900MHz PIII CPUs, the WIN2K and E2K software installed on an 36.4GB RAID1 array, 1GB RAM, and a Fast Ethernet (100MB) NIC. The quorum disk and E2K transaction logs will be on separate 36.4GB RAID1 arrays. The E2K Information Store will be on a RAID 5 array of five (5) 36.4GB SCSI hard drives. The quorum and transaction log RAID1 arrays will be on a separate hard disk controller from the RAID5 array to prevent a disk input/output bottleneck. GIAC will also put a server in the Demilitarized Zone (DMZ) in order to provide web-based access to E2K. This "webmail" server, GIAC-EX03.NASHVILLE.GIAC-ENT.LOCAL, will run Outlook Web Access (OWA) and will be discussed later with other DMZ servers. The OWA server will have 2x900MHz PIII CPUs, the WIN2K and E2K software installed on an 18.2GB RAID1 array, 1GB RAM, and a Fast Ethernet (100MB) NIC. Table 7 lists the basic information about the E2K servers within the GIAC WIN2K AD enterprise network.

EMAIL Servers		
Fully Qualified Domain Name (FQDN)	**IP ADDRESS**	**WIN2K AD Domain**
GIAC-EX01.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.5/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-EX02.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.6/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-EX03.NASHVILLE.GIAC-ENT.LOCAL	210.28.44.2/24	NASHVILLE.GIAC-ENT.LOCAL
GIAC-EX04.DETROIT.GIAC-ENT.LOCAL	10.1.4.5/23	DETROIT.GIAC-ENT.LOCAL
GIAC-EX05.WINNIPEG.GIAC-ENT.LOCAL	10.1.6.5/23	WINNIPEG.GIAC-ENT.LOCAL

Table 7: Exchange 2000 Servers

- **Intranet Web Services:** GIAC will have two intranet servers (See Table 8) located in the US Office. R&D will use these intranet servers for internal collaboration on new product development as well as sharing product information with the GIAC sales force and corporate headquarters. Finance & Accounting and Human Resources will also use this intranet web server as a front end interface to accounting and employee record databases on the database server. Sales & Marketing will also use this front end – back end concept to build and access a customer service database. These intranet web servers will use network load balancing (NLB) in order to ensure high availability and fault tolerance. Each intranet server will have 2x900MHz PIII CPUs, the Windows 2000 Advanced Server and E2K software installed on an 18.2GB RAID1 array, all web content on a RAID5 array of 5x36.4GB hard disk drives, 1GB RAM, and a Fast Ethernet (100MB) NIC.

Intranet Web Servers		
Fully Qualified Domain Name (FQDN)	**IP ADDRESS**	**WIN2K AD Domain**
GIAC-WB01.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.8/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-WB02.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.9/23	NASHVILLE.GIAC-ENT.LOCAL

Table 8: Intranet Web Servers

- **Database Server:** GIAC's database server (See Table 9) will run Windows 2000 Advanced Server and SQL Server 2000 (SQL2K). The server hardware will have to be robust in order to support the database needs of R&D, Sales & Marketing, Finance & Accounting, and Human Resources. The system will have 6x900MHz PIII CPUs, the WIN2K and SQL2K software installed on an 36.4GB RAID1 array, transaction logs on a 72.8GB RAID1 array, the database on a 5x72.8GB RAID5 array, 4GB RAM, and a Fast Ethernet (100MB) NIC. This database server is centrally located in order to support all GIAC network clients as well as database queries from the web interface hosted on the intranet server cluster.

Database Server		
Fully Qualified Domain Name (FQDN)	**IP ADDRESS**	**WIN2K AD Domain**
GIAC-DB01.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.7/23	NASHVILLE.GIAC-ENT.LOCAL

Table 9: Database Server

- **File Servers:** A major goal of a GIAC WIN2K AD enterprise network was to be able to seamlessly share files across the enterprise network. We'll used Distributed file system (Dfs) to meet this requirement. Dfs allows file servers and network shares to be logically organized into a hierarchical structure called a Dfs directory tree. This type of organization makes it much easier to manage, locate, and access network resources. Any GIAC network user sees only what appears to be one server containing a hierarchical tree of resources, when these resources are really distributed across the six GIAC file servers (See Table 10). Users need make only one persistent network connection to the Dfs directory tree in order to access everything within the tree. Each WIN2K AD child domain of the **giac-ent.local** root will host a domain-based Dfs root from which we'll build the Dfs hierarchical structure for each respective domain. We created domain-based Dfs roots because these roots are stored in the domain partition of Active Directory and these roots support replication. Each file sever will have 2x900MHz PIII CPUs, Windows 2000 Server software installed on an 18.2GB RAID1 array, the Dfs shared folders/files on a RAID5 array of 5x36.4GB hard disk drives, 1GB RAM, and a Fast Ethernet (100MB) NIC.

File/Print Servers		
Fully Qualified Domain Name (FQDN)	**IP ADDRESS**	**WIN2K AD Domain**
GIAC-FS01.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.10/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-FS02.NASHVILLE.GIAC-ENT.LOCAL	10.1.2.11/23	NASHVILLE.GIAC-ENT.LOCAL
GIAC-FS03.DETROIT.GIAC-ENT.LOCAL	10.1.4.6/23	DETROIT.GIAC-ENT.LOCAL
GIAC-FS04.DETROIT.GIAC-ENT.LOCAL	10.1.4.7/23	DETROIT.GIAC-ENT.LOCAL
GIAC-FS05.WINNIPEG.GIAC-ENT.LOCAL	10.1.6.6/23	WINNIPEG.GIAC-ENT.LOCAL
GIAC-FS06.WINNIPEG.GIAC-ENT.LOCAL	10.1.6.7/23	WINNIPEG.GIAC-ENT.LOCAL

Table 10: File/Print Servers

The DMZ (See Figure 6) extends off the GIAC firewall and contains the servers listed in Table 11.

- **OWA Server:** The OWA server supports web-based email access. This server will use Secure Sockets Layer (SSL) to secure web communications over the Internet. SSL is a transport-layer protocol that provides three aspects of security:

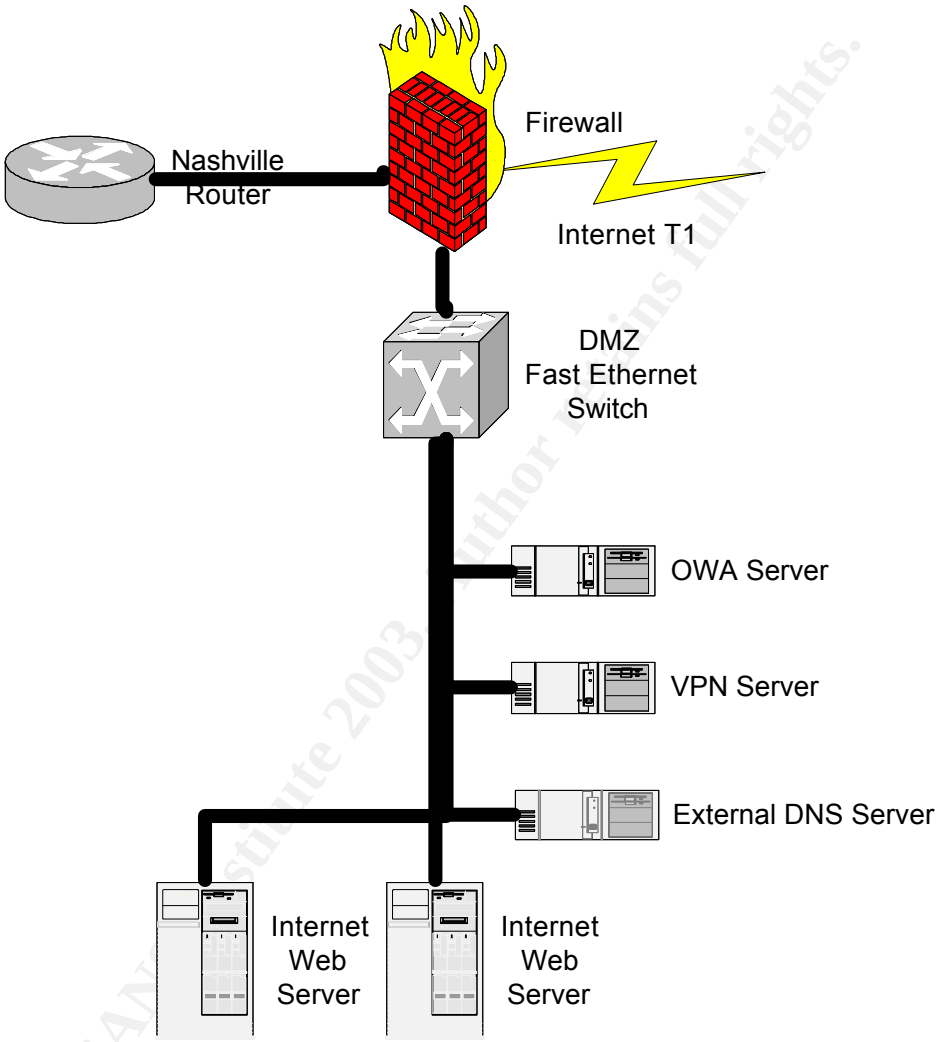

Figure 6: GIAC DMZ (Screened Subnet)

- **Authentication** – The message received is really from the individual listed as sending the message.
- **Confidentiality** – Protects the message by preventing unintended recipients from reading the message as it passes from sender to recipient.
- **Integrity** – Makes sure message content isn't tampered with while passing from the sender to recipient.

SSL uses public-key cryptography PKI encryption "for secure authentication and symmetric key encryption for encryption of transmitted information."[1] GIAC plans to obtain the certificate to support SSL on the OWA server from Verisign (http://www.verisign.com).

- **External DNS:** The CIO stated that the internal and external DNS and internal DNS namespace must be different. Hence, the external DNS namespace is **giac-ent.com** and the internal DNS is **giac-ent.local**. This external DNS server hosts the **giac-ent.com** primary zone. GIAC clients within the GIAC WIN2K AD enterprise locate resources using DNS. All DNS queries which the internal DNS servers can't resolve are forwarded to this external DNS server for resolution. The DNS server will have 2x900MHz PIII CPUs, Windows 2000 Server software installed on an 18.2GB RAID1 array, 3GB RAM, and a Fast Ethernet (100MB) NIC.
- **Virtual Private Network (VPN):** GIAC clients requiring remote access will use dial up access to a local ISP. Once they've established an Internet connection through the local ISP, they'll establish a VPN with this VPN server. All client computers establishing these VPN connections will be Windows 2000 Professional computers with Internet Protocol Security (IPSec) enabled. The VPN server (See Table 11) running the Routing and Remote Access Server (RRAS) to support the VPN service will have 2x900MHz PIII CPUs, Windows 2000 Server software installed on an 18.2GB RAID1 array, 2GB RAM, and a Fast Ethernet (100MB) NIC. The VPN server will be configured to only use the strongest encryption possible for the connection which is 3DES and will also be IPSec enabled. The client – server VPN connection will use Layer 2 Tunneling Protocol (L2TP) and IPSec. L2TP is the tunneling protocol that encapsulates Point-to-Point Protocol frames for transmission over the TCP/IP network transport. IPSec provides end-to-end data encryption and integrity at Layer 3, the IP layer, of the OSI model. End-to-end encryption means the connection from the VPN client to the VPN server will be encrypted.
- **External Web/E-Commerce Servers:** The CEO and CIO want to use the Internet to improve the web-based distribution of information about GIAC Enterprises and the wide range of ergonomic computer equipment it sells. The CEO wants to build on this web-based distribution of information

DMZ Servers		
Fully Qualified Domain Name (FQDN)	**IP ADDRESS**	**Function**
GIAC-EX03.NASHVILLE.GIAC-ENT.LOCAL	210.28.44.2/24	OWA
GIAC-NS01.GIAC-ENT.COM	210.28.44.3/24	External DNS
GIAC-VPN01.NASHVILLE.GIAC-ENT.LOCAL	210.28.44.4/24	VPN
GIAC-EXTWB01.GIAC-ENT.COM	210.28.44.5/24	Internet Web/E-Commerce
GIAC-EXTWB02.GIAC-ENT.COM	210.28.44.6/24	Internet Web/E-Commerce

Table 11: DMZ Servers

about GIAC Enterprise by also giving visitors from the Internet a means of purchasing GIAC products. The Sales & Marketing folks expanded upon this idea by stating the requirement for an E-Commerce website (https://estore.giac-ent.com). Design of this E-Commerce website must also scale to meet the expected growth and be highly available (fault tolerant). The two web servers we'll put in the DMZ will use network load balancing (NLB) to meet these scalability and fault tolerant requirements. We'll also obtain a PKI certificate from Verisign, a commercial certificate authority (CA), for the e-commerce website to secure the personal and financial information of all Internet customers. These NLB clustered web servers will also host the GIAC website, http://www.giac-ent.com. Each web server will have 2x900MHz PIII CPUs, Windows 2000 Server software installed on an 18.2GB RAID1 array, 2GB RAM, 3x36.4GB SCSI hard drives in a RAID5 array to host the wide range of web pages, and multiple Fast Ethernet (100MB) NICs to support both the general website, http://www.giac-ent.com, and the E-Commerce website (https://estore.giac-ent.com).

Active Directory (AD) Design & Diagram

A domain within the GIAC WIN2K AD forest serves as an administrative boundary for managing security principals. A security principal is an object within the WIN2K AD directory service that can be assigned permissions and rights. User, computer, and group objects are security principals. A domain performs the following important functions:

- **Authentication** – Security principals can be granted or denied access to network resources based on authentication. A user's logon attempt can only be authenticated within the domain that hosts the user's account.
- **Policy-based Administration** – The GIAC domains will use Group Policy Objects (GPO's) to standardize user and computer configurations.
- **Security Policies for User Accounts** – The security policies applied to GIAC domain user accounts can only be granted within a specific domain. These security policies are a password policy, account lockout policy, and Kerberos ticket policy.
- **Directory for Publishing Shared Resources** – AD is a place where services publish connection information about shared resources. A good example is the domain-based Distributed File System (Dfs) GIAC plans to deploy among the file servers within each domain.

GIAC plans to employ a dedicated, empty root domain (See Figure 3), **giac-ent.local**, managed by the small group of system administrators within the Corporate Headquarters IT Office. The child domains will be geographically based domains at Nashville, Detroit, and Winnipeg. All domains in the GIAC WIN2K AD enterprise will operate in native mode. GIAC going to native mode WIN2K domains enables the use of universal groups, group nesting, and Domain local groups

- **Universal groups –** can include members from any domain in the GIAC WIN2K AD forest and can be granted permissions for resources in any domain in the forest. Universal groups can contain user accounts, global groups, other universal groups, but they can't contain domain local groups. The Global Catalog lists universal group membership so it is a good idea to nest global groups inside universal groups to reduce network traffic due to global catalog replication. It is also a recommended practice to use global groups when their membership changes infrequently. Universal groups can grant users access to resources located in multiple domains by adding domain global groups to the universal group and assigning permissions for the resource to the universal group.
- **Group nesting –** Group nesting involves placing one group inside another group. The previous example of placing global groups from various domains in a universal group is a good example.
- **Domain local groups –** Domain local groups have a scope which is restricted to the local domain in which it is defined. This group provides users with access to network resources and assigns permissions to control these resources. You can add members from any domain in the forest to a domain local group.

GIAC decided to go with WIN2K child domains at Nashville, Detroit, and Winnipeg in order to retain more autonomy at these locations while still falling under an enterprise root domain for the implementation of enterprise-wide policies. This approach met the goal of designing the WIN2K AD enterprise according to the centralized management, decentralized operations business model.

Organizational Units (OUs) are containers within domains that can contain other OUs, users, groups, computers, and other objects. OUs form a hierarchical structure within a domain and are used to group objects together which have the same managerial requirements. There is no limit to the number of levels of OUs you can nest. However, it is a good idea to keep the OU organization as simple as possible while meeting managerial requirements in order to make administration and troubleshooting much easier.

Delegation of administration is another key goal of designing an OU structure. The general steps to delegation of administration through the use of OUs entail:

- Place the user or users having control into a group. Example: Local system administrator within the Sales & Marketing Department.
- Place the set of objects to be controlled into an OU. Example: All the Windows 2000 Professional desktops in the Sales & Marketing Department.
- Delegate administration of the OU to that group. Example: Delegate administration of the OU containing the Sales & Marketing desktops to Help Desk personnel from that WIN2K AD domain.

It was also the intent of Microsoft to minimize the number of administrators with high levels of administrative access by replacing Windows NT4 domains with

OUs. We'll minimize the number of administrators with high level administrative access, but retain domains at each of the major GIAC locations.

We decided to have GIAC's OU structure follow the corporation's departmental hierarchy. GIAC also wants to set up a standard set of OUs within each domain to simplify administration over the long haul. However, we must first address the OU organization within GIAC's empty WIN2K AD root domain, **giac-ent.local** (See Figure 7).

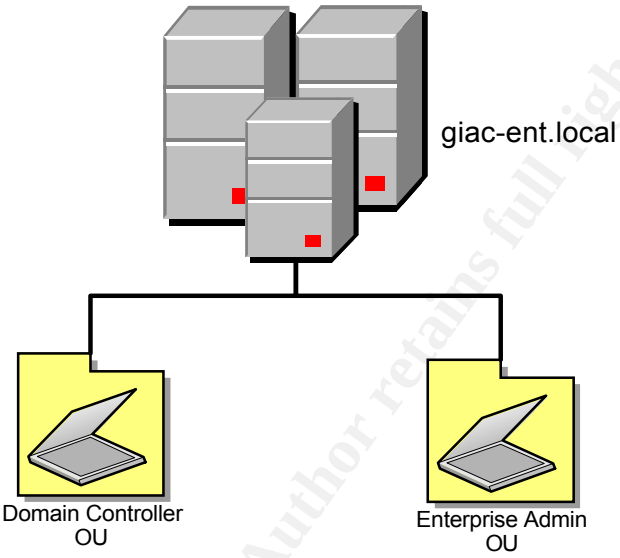

Figure 7: Root Domain OU Structure

This forest root domain will have only two OUs. The Domain Controller OU, created by default, contains three domain controllers: GIAC-DC01, GIAC-DC02, and GIAC-DC03 (See Figure 5).

The theme regarding system administrators and permissions is to only grant the system administrators the minimum permissions they need to do their respective jobs. A good example is the **Schema Admins** group. This group will contain a system administrator account only when the system administrator needs to modify the schema. Once schema modification is complete, the system administrator account performing the modification is removed from the **Schema Admins** group. Schema modification should occur only when absolutely necessary since replication resulting from schema modifications can be considerable. Protection of the Schema Admins group is another reason for implementing the empty enterprise root domain, **giac-ent.local**.

The very small number of system administrators from the IT Office of the Corporate Headquarters will have accounts in the Enterprise Admin OU. These root-level system administrator accounts in the Enterprise Admin OU will only be used to perform administrative actions at the enterprise root domain, **giac-ent.local**, level. They won't be used for everyday work activities.

It was my intent when developing the OU architecture within each domain to first create a standard set of OUs within each of the child domains of **giac-ent.local**. These standard OUs include both computer hardware OUs and user

account OUs. The standard computer hardware OUs are the Domain Controller OU, Member Server OU, PC OU, and the Printers OU. Each child domain will also have a Domain Admins OU and a Domain User OU serving as user account OUs. All OUs in each child domain will have an OU owner designated by the child domain owner of the domain in which they reside. OU owners can control delegation of administration tasks, how policies are applied to objects, and the creation and administration of subordinate OUs.

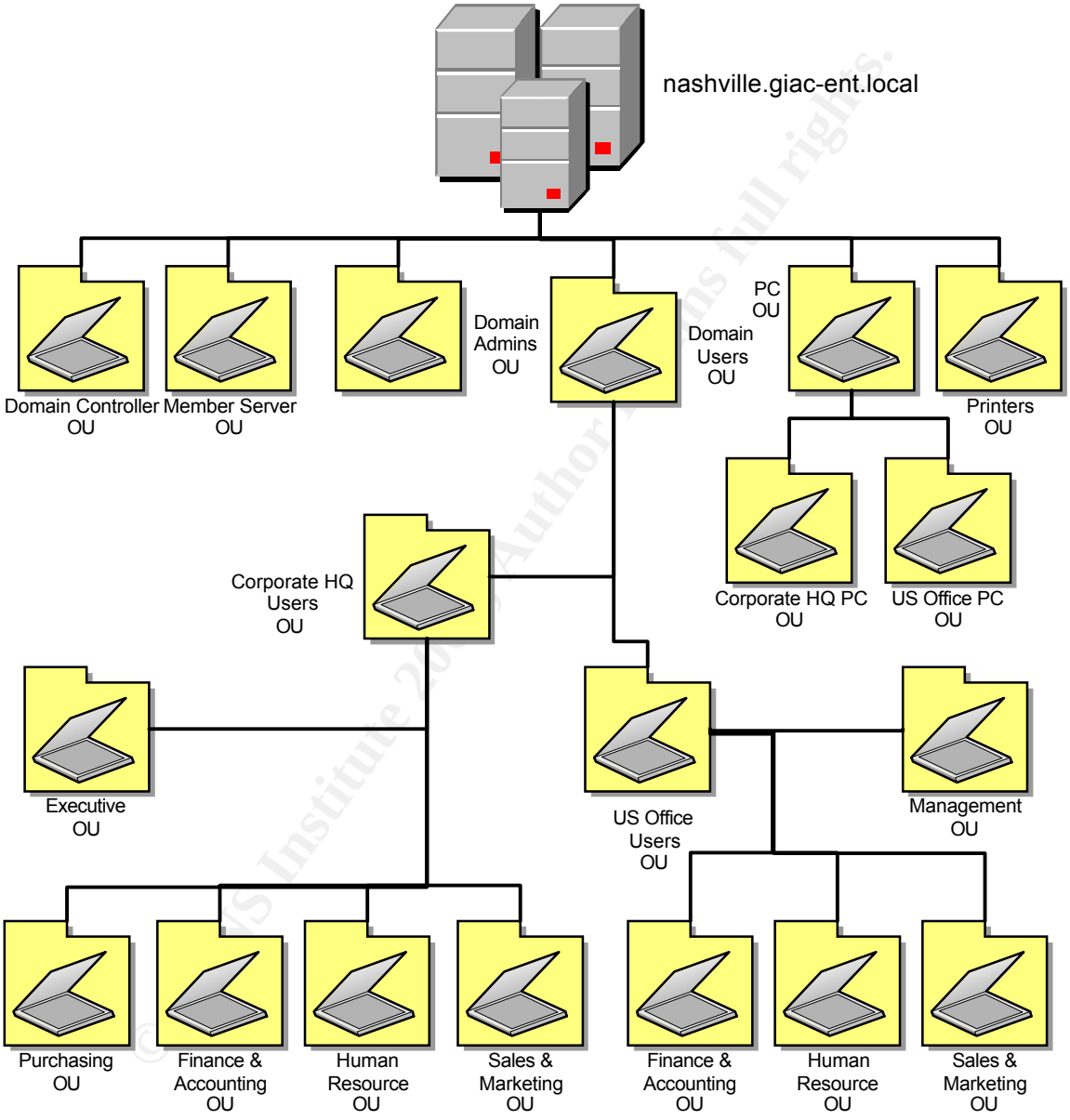

Figure 8: Nashville Domain OU Structure

The OU structure for **nashville.giac-ent.local** (See Figure 8) includes the standard hardware OUs and several variations within the Domain Users OU. The Domain Controller OU contains the three domain controllers of the **nashville.giac-ent.local** WIN2K AD domain. The Member Server OU contains two Intranet web servers (See Table 8), two File Servers (See Table 10), two

Email Servers (See Table 7), one Database Server (See Table 9), one VPN Server (See Table 11) in the DMZ, and one Email server (See Table 11) which is also in the DMZ providing OWA email access. The PC OU contains 400 WIN2K PRO desktops of the Corporate Headquarters in a sub-domain called the Corporate HQ PC OU and 400 WIN2K PRO desktops of the US Office in a sub-domain called US Office PC OU. The Help Desk Managers for the Corporate HQ and US Office Help Desks will be the owners of these sub-domains of the PC OU from **nashville.giac-ent.local**. These Help Desk Managers will handle the system administrative functions for the 400 PCs in their OUs. The Printers OU contains all printers in the **nashville.giac-ent.local** domain which will also receive administrative support from Help Desk personnel.

The Domain Users OU within the **nashville.giac-ent.local** domain is divided further into subordinate Corporate HQ User and US Office User OUs. Each of these subordinate OUs contain either an Executive or Management OU followed by Finance & Accounting, Human Resource, and Sales & Marketing OUs. The Corporate HQ OU also contains a Purchasing OU. Each of these user account OUs receives administrative support from their respective Information Management Officers (IMOs). IMOs are the first line-of-defense for user computer support requirements. If an IMO can't solve a user's problem, a call is placed to the Help Desk and a trouble ticket opened.

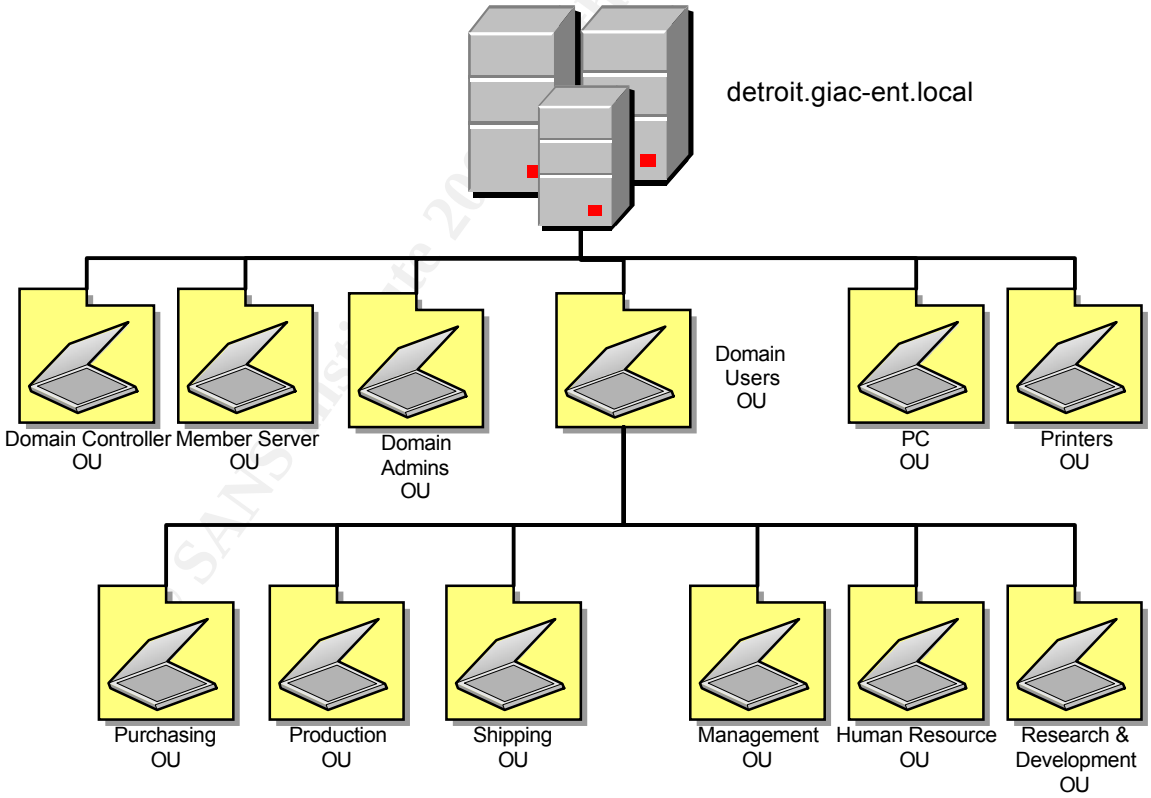

Figure 9: Detroit Domain OU Structure

The OU structure for the Detroit domain, **detroit.giac-ent.local**, is similar to Nashville site with a few exceptions. Since manufacturing is the main mission

of business operations in Detroit, there is no need for a Sales & Marketing OU. However, Research & Development plays a major role at this location so it has a separate subordinate user account OU for R&D. The user account OU also contains subordinate OUs for Purchasing, Production, and Shipping as well as Management and Human Resources. The user accounts OUs receive administrative support from their respective Information Management Officers (IMOs). IMOs are the first line-of-defense for user computer support requirements. If an IMO can't solve a user's problem, a call is placed to the Help Desk and a trouble ticket opened.

The standard hardware OUs: Domain Controller, Member Server, PC, and Printer OUs are also in residence. The Domain Controller OU contains the three domain controllers and no other computer objects. The Member Server OU contains two file servers (See Table 10) and an email server cluster (See Table 7). The PC OU contains 400 client PCs. The Help Desk Manager of the Detroit office is responsible for hardware support on these 400 desktops. The Help Desk Manager will also be the owner of these sub-domains of the PC OU from **detroit.giac-ent.local**. These Help Desk Managers will handle the system administrative functions for the 400 PCs in their OUs. The Printers OU contains all printers in the **detroit.giac-ent.local** domain which will also receive administrative support from Help Desk personnel.

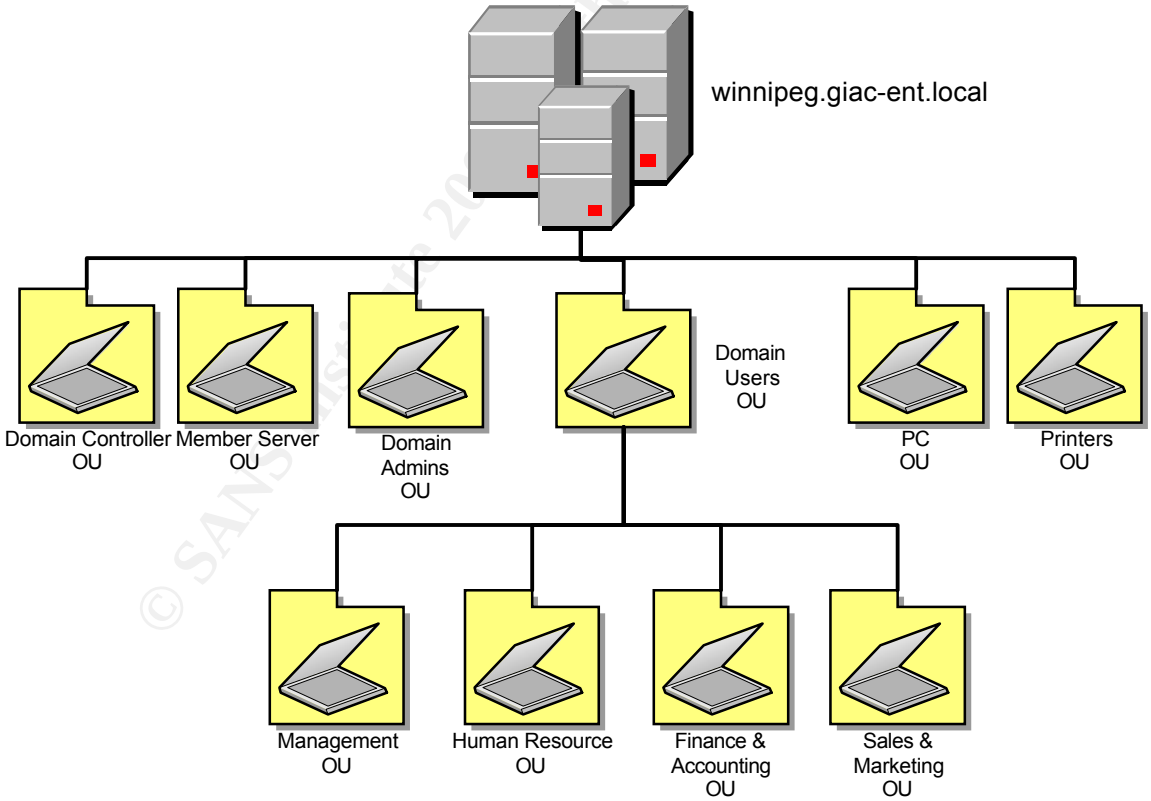

Figure 10: Winnipeg Domain OU Structure

Winnipeg's business operations center on the sale and marketing of GAIC products in all Canadian provinces. Therefore, the Sales & Marketing

subordinate user account OU contains the largest number of personnel. Subordinate user account OUs also exist for Management, Human Resources, and Finance & Accounting. Since each child WIN2K AD domain in the GIAC enterprise network uses AD-integrated DNS, every domain controller in the Winnipeg domain is listed in Table 5. The Domain Controller OU contains the three domain controllers of the **winnipeg.giac-ent.local** domain. The Member Server OU contains the Winnipeg's two file servers (See Table 10) and an email server cluster (See Table 7). The PC OU contains the 400 WIN2K PRO desktop computers which support daily business operations in the Winnipeg Office. The Manager of the Winnipeg Help Desk is the owner of the PC OU. Her handful of technicians provides support to the Winnipeg user population. If a user has a problem that a local Information Management Officer (IMO) can't readily solve, a call is placed to one of these Help Desk technicians for support. The Printers OU contains all printers in the **winnipeg.giac-ent.local** domain which will also receive administrative support from Help Desk personnel. The Domain Admins OU contains the system administration accounts of the two system administrators who perform all domain-level system administration tasks in the **winnipeg.giac-ent.local** domain. The two people functioning as system administrators only log in with their respective system administrator accounts when they have system administration tasks to perform. The rest of the time, they log in using an account with general user privileges. The lead system administrator is also the owner of the Domain Controller, Member Server, and Domain Admins OUs.

The life blood of any WIN2K AD forest rests with the prudent implementation of DNS and a sound replication plan. Performance is directly impacted by these two key features. Care has been taken when designing the GIAC WIN2K AD enterprise to ensure the timely access of resources by active directory integrating the DNS zones for each domain. Network clients can easily locate network resources by locating the service resource (SRV) record for the resource within DNS over 100Mbps LAN links. Keeping all the domain controllers for each domain on the same high speed LAN also removes any major replication issues. The Knowledge Consistency Checker (KCC), operating on each domain controller (DC), automatically generates a map of the replication topology within each domain. DC's use multimaster replication over this topology to push changes made on one domain controller to all domain controllers over 100Mbps LAN links. The responsibility for intersite replication between the sites in the GIAC WIN2K AD enterprise (See Figure 2) rests with the bridgehead servers within each site. Bridgehead servers are responsible for the physical act of transferring replication traffic between the GIAC WIN2K AD sites. This replication traffic will take place according to a schedule during off peak times of the day when activity on the T1 WAN links is low. Replication traffic from the Detroit and Winnipeg sites to the Nashville site will occur at 6:00 A.M., 12:00 P.M., 6:00 P.M., and 12:00 A.M.

Intrasite and intersite RP replication traffic between WIN2K AD domain controllers is unencrypted. Securing replication traffic between domain controllers within the same GIAC site and between domain controllers in different

sites is essential to meeting the CEO/CIO security requirement. We'll use Group Policies to mandate the use of all communications between domain controllers.

Group Policy and Security

Group Policies are a very powerful tool used within WIN2K AD domains to define the configuration of groups of users and computers. The Group Policy settings are contained in a Group Policy Object (GPO). The GPO provides GIAC system administrators with a very powerful tool for the management of the user and computer environment within the GIAC WIN2K AD enterprise. Security configuration is a key element of the user and computer environment GPOs support. In fact, Group Policies are the primary means by which GIAC Enterprises will implement security within its WIN2K AD enterprise network. However, Group Policies can also do a number of other things to include the following:

- Configure user profiles such as desktop settings, Start menu, and other common settings.
- Control user access to files and folders, user logon rights, and account lockout restrictions.
- Allow users to install software applications published in Active Directory directory service or to automatically install or upgrade applications on their respective computers.
- Redirection the location of folders from the Documents and Settings folder on a user's local computer to a network share.
- Assign scripts to do a number of different tasks like computer startup, shutdown, logon, and logoff events. WIN2K provides the ability to do most administrative action through either a GUI or script.

Group Policies are configured and assigned through the following steps:

1. Create and configure the settings of a GPO using the Group Policy snap-in for the Microsoft Management Console (MMC).
2. Assign or "link" the GPO to the appropriate site, domain, or OU.

Next, the newly created and linked GPOs are replicated by WIN2K AD to all domain controllers within the domain.

An object can have multiple GPOs applied which may conflict. If a conflict occurs, the "last policy written" rule applies meaning the last GPO created and associated with the object is the one that takes affect. WIN2K applies GPOs in the following order:

- First – local GPOs are applied.
- Second – WIN2K AD Sites
- Third – WIN2K AD Domains
- Fourth – WIN2K AD OUs

A Group Policy assigned at the site, domain, or OU affects computers or users at that level and in containers below it by inheritance. Two interesting exceptions to Group Policy inheritance are:

- **Black Policy Inheritance** – It is available on domains and OUs only. Administrators of lower-level containers like a subordinate OU can block the inheritance of Group Policies from upper level OUs or domains.
- **No Override (Enforce)** – Is a configuration option at the higher-level containers system administrators can use to enforce Group Policy on lower level containers.

In situations where both **Block Policy Inheritance** and **No Override (Enforce)** are set, the **No Override** option takes precedence. This fact allows system administrators to force policy on subordinate domains or OUs.

GIAC system administrators will also make every effort to simplify the implementation of GPOs throughout the enterprise. Too many GPOs applied to a user or computer object can severely hinder the timely logon of the user to the network. Troubleshooting also becomes an exacerbated process due to the need to look at multiple GPOs as part of the troubleshooting process.

The design of the GPOs within the GIAC WIN2K AD enterprise must strike the proper balance between functionality and security. The CEO and CIO want security implemented at all levels of the enterprise network. However, Information Technology must be used to expand GIAC's share of the ergonomic computer equipment market space. GPOs will meet these strategic goals. The

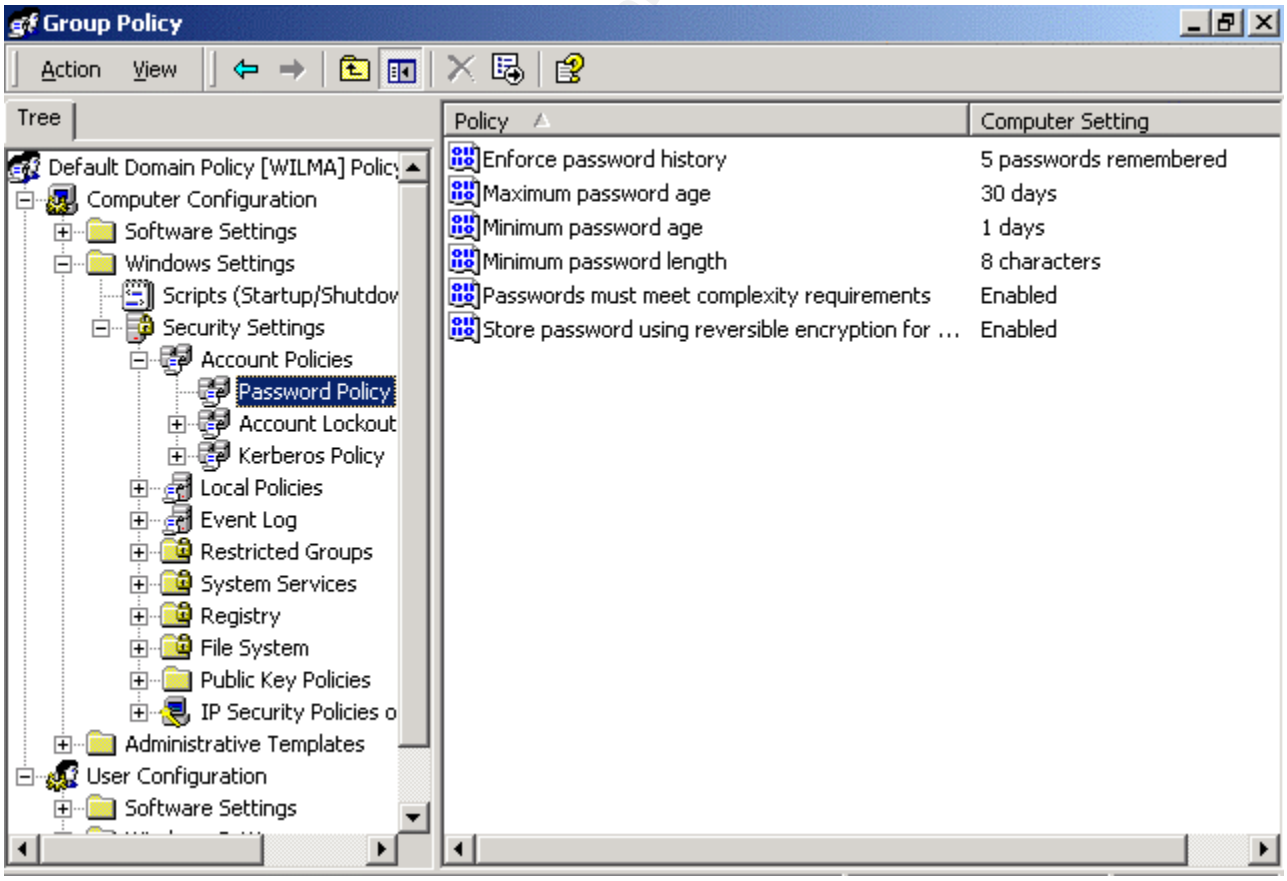

Figure 11: Default Domain Policy – Password Policy

first GPO we'll look at is the Default Domain Policy for the **nashville.giac-ent.local** domain. The default GPO for a domain, "is the only GPO on which you can configure password restrictions, lockout restrictions, Kerberos, the Encrypting File System (EFS), and Internet Protocol (IP) security settings."[2] The first part of the Security Settings – Account Policies deals with Password Policy (See Figure 11). We modified the following password security settings:

- **Enforce Password History –** AD stores the last 5 passwords of each user object. A user can't use the same password over and over again. A user must use 5 different passwords before he/she can reuse a password.
- **Maximum Password Age –** set at 30 days is the maximum amount of time a user can use the same password before he/she must change it.
- **Minimum Password Age -** set at 1 day is the minimum amount of time a GIAC user must keep his/her password before they're allowed to change it.
- **Minimum Password Length –** is set at 8 characters. GIAC users must use passwords that are at least 8 characters in length.
- **Passwords must meet complexity requirements** – is enabled. The 8 character password GIAC users create must have three of the following four types of characters:
    - Uppercase Letters
    - Lowercase Letters
    - Numbers
    - Special Characters (! @ # $ % ^ & * ( ) _ + ? > <)
- **Store all passwords using reversible encryption for all users in the domain –** is enabled. A copy of the user's password is stored with the user's account with a 3DES key derived from the master key of the domain controllers. We've enabled this option since all domain controllers are physically secured behind locked doors with limited access granted only to select individuals.

Password Policy can only be configured at the domain level.

Account Lockout Policy is configured next (See Figure 12).

- **Account lockout threshold –** a user failing to log on to the network 5 times will have his/her user account locked out.
- **Account lockout duration** – A user failing to log on to the network a specified number of times, 5 times in this example, will have his/her user account locked out for 30 minutes.
- **Reset account lockout counter after –** configured at 30 minutes is the maximum amount of time between bad logons that will still trigger account lockout when the threshold is reached.

The three log files viewable in the Event Viewer are the System, Security, and Application logs. The System Log records events pertaining to the performance of the Windows 2000 operating system. The Security Log records "authentication events, access to resources, invocations of user rights, and other

items of interest for intrusion detection and incident response."[3] The Application Log is a catch all place to log activity which software developers determine is

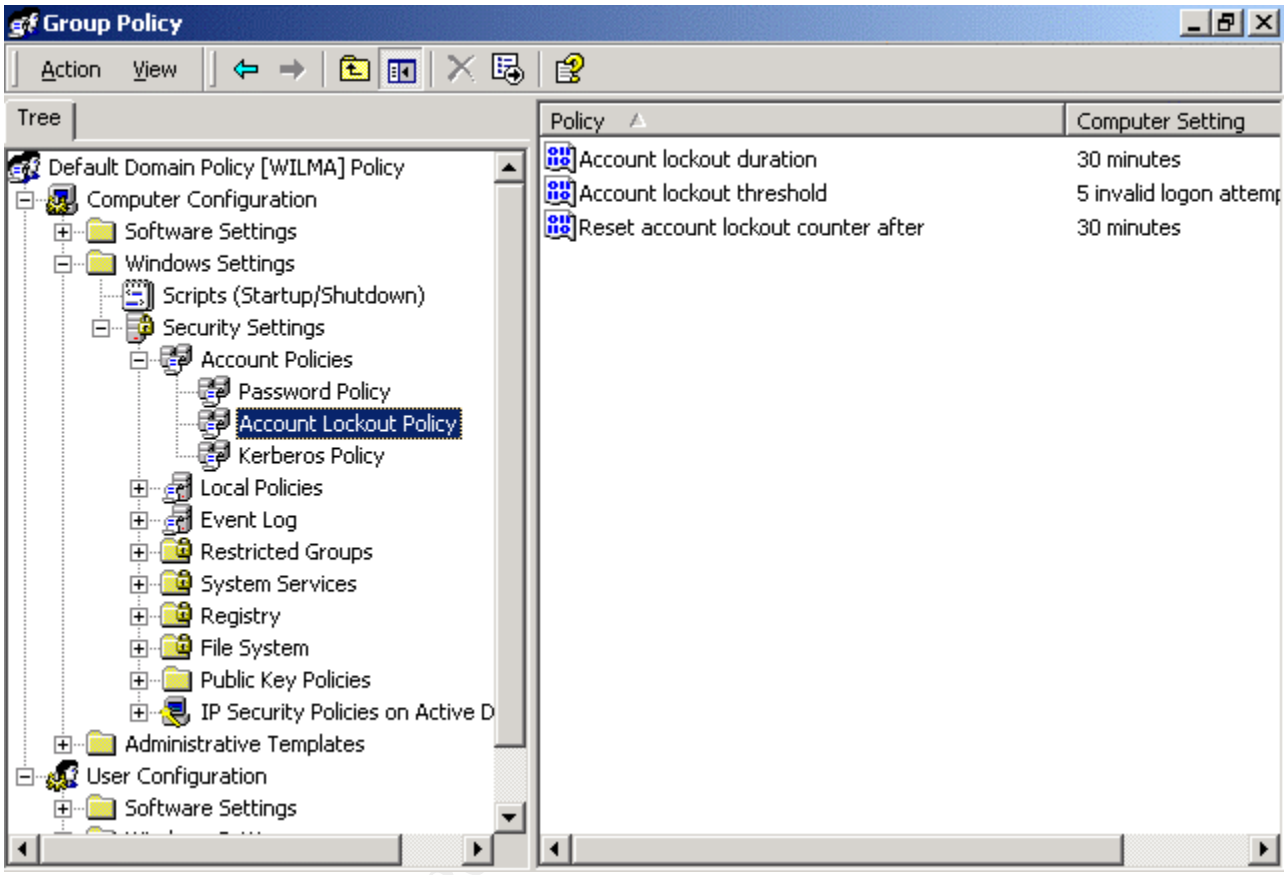

Figure 12: Account Lockout Policy

important to the development of their software products.

Auditing is an essential part of any WIN2K AD domain security program. It specifies which security-related events that will be recorded in the Security Log. Auditing Policy is set under Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy. System Administrators configured the following auditing policy for the **nashville.giac-ent.local domain**:

- **Audit Account Logon Events** (Success, Failure) – Logs successful and failed user logon attempts made to domain controllers.
- **Audit Account Management** (Success, Failure) – Logs the successful and failed user account management tasks like user account creation, account deletion, account modification, and group membership changes.
- **Audit Directory Service Access** (Success, Failure) – Logs successful and failed access to AD objects as defined by the SACL of each object. SACL stands for system access control list used by WIN2K for security control.
- **Audit Logon Events** (Success, Failure) – Logs successful and failed logon attempts. Too many failed logon attempts is a good indication of a

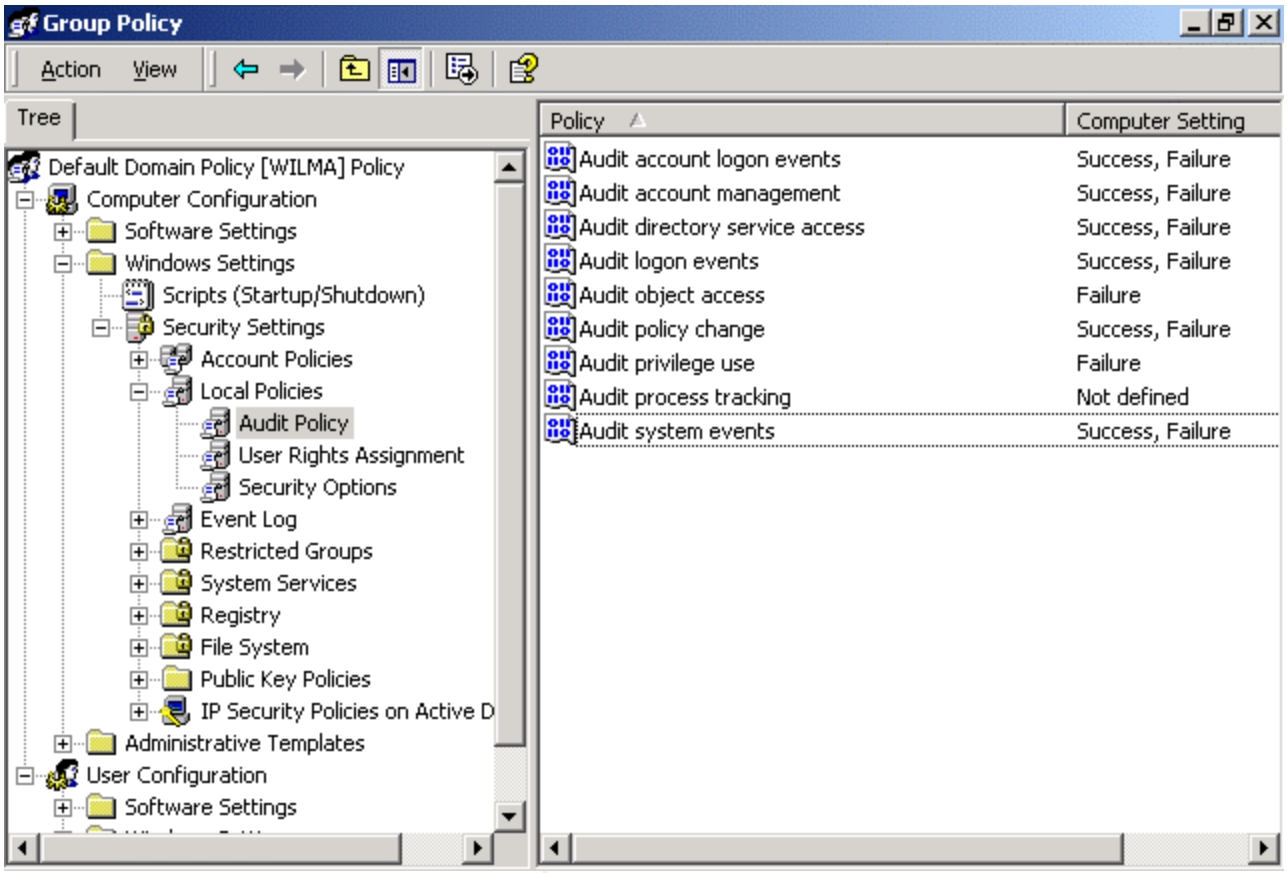

Figure 13: Audit Policy

possible hacking attempt on the domain from a workstation or server within the domain.

- **Audit Object Access** (Failure) – Logs failed attempts to access NTFS files, folders, registry keys, and shared printers. You must also configure the object (file, folder, registry key, shared printer) to audit some kind of access to it.
- **Audit Policy Change** (Success, Failure) – Logs successful and unsuccessful changes made to audit policies and user rights assignments.
- **Audit Privilege Use** (Failure) – Logs the failure of user rights on the machine like changing system time and taking ownership of an object.
- **Audit System Events** (Success, Failure) – Logs the successful and failed system-wide events like startup and shut down. Clearing of the System and Security logs is also recorded here. A ominous sign of something having gone wrong is an empty security log.

System Administrators of the **nashville.giac-ent.local** domain will also configure several security-related options under Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options (See Figure 14).

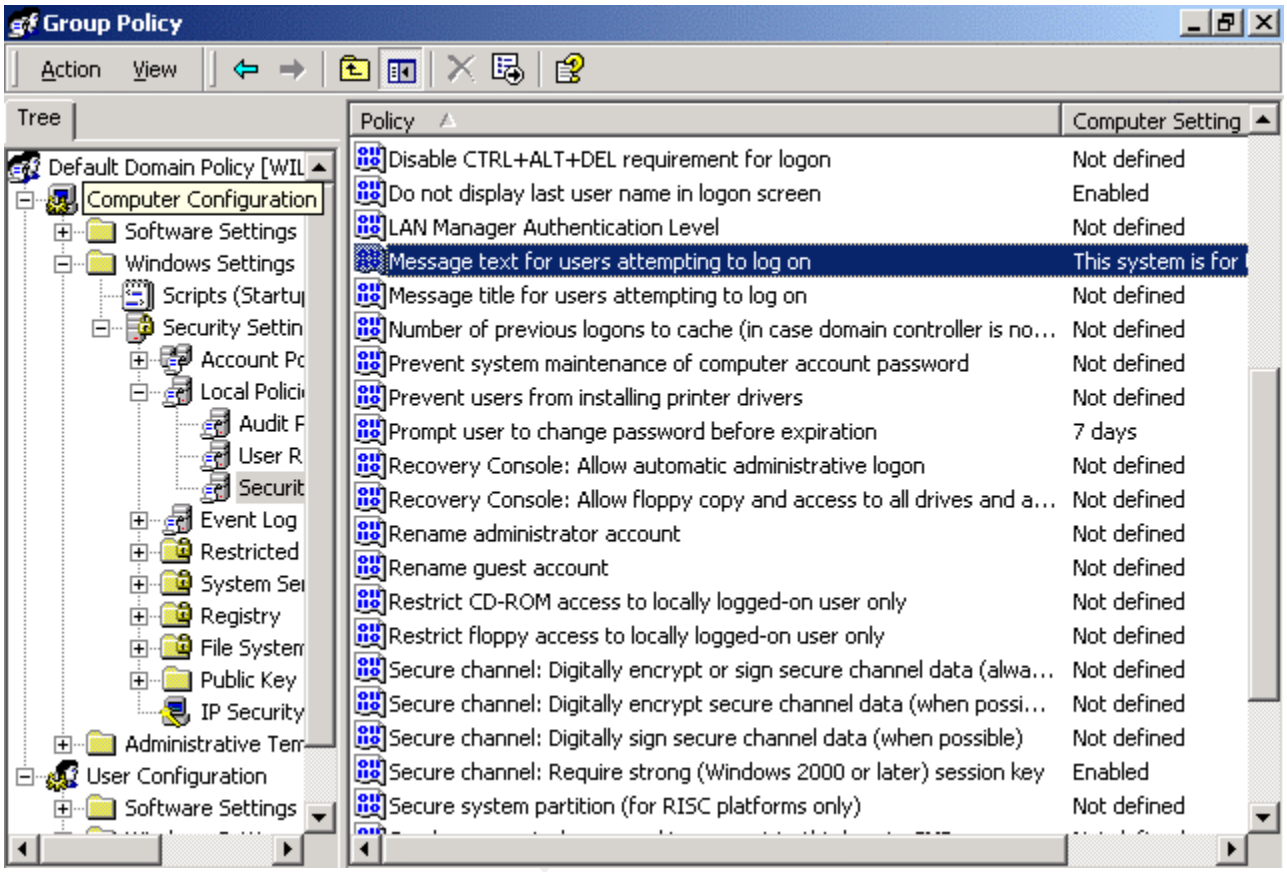

Figure 14: Event Log Policy

- **Do Not Display Last User Name in Logon Screen** – The user name of the last user logged into a system remains in the user name field by default when the next user logs into the system. Enabling this system removes the last users logon from the user name field. It is a low cost security configuration which denies a user name to a hacker.
- **Message Text for Users Attempting to Log On** – Text filled into the Computer Setting field of this security option will be displayed as a banner before a user logs on to the computer. Displaying this banner stating the computer is to be used for official GIAC business only and any activity on the system may be monitored is a good, cheap means of protecting GIAC Enterprises from possible legal action.
- **Prompt User to Change Password Before Expiration** – is configured to remind that user that his/her password will expire in 7 days. The user can choose to change his/her password at that time or wait another 7 days.
- **Secure Channel: Require Strong (Windows 2000 or later) session key** – The NetLogon daemon provides a wide variety of services within a domain which mainly travel on an RPC channel call the “secure channel.” One of the first things a member server or workstation does when it boots up is to establish a NetLogon secure channel to a domain controller. A

changed user password travels from the user's computer to the domain controller through a secure channel. Enabling this security option means all domain controllers in trusting/trusted domains must be WIN2K and all domain members must be WIN2K. All GIAC WIN2K AD domains are native mode domains, all member servers are WIN2K, and all clients run WIN2K Professional. Also, every WIN2K system has Service Pack 3 installed to support 128-bit encryption.

Hackers will often try to cover their tracks by either zeroing out the Event Logs after some malicious activity or running a script to fill up log files and hopefully overwrite their activities. It is imperative that Event Log files be configured according to a set standard across the board to hopefully preserve a record of any malicious activity so appropriate action can hopefully be taken against the intruder in the future. Event Logs are configured under Computer Configuration > Windows Settings > Security Settings > Event Log (See Fig 15).

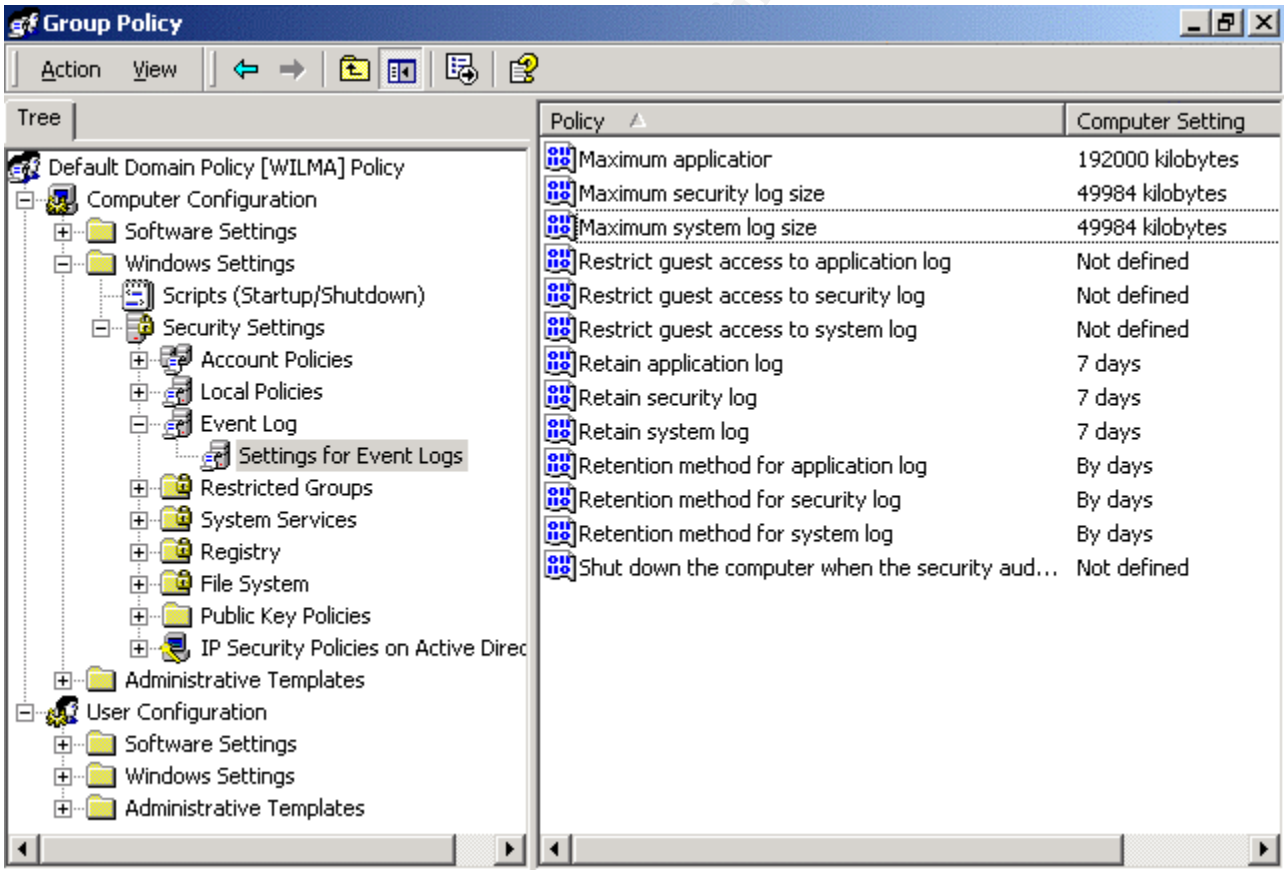

Figure 15: Event Log Policy

- **Log Size** – The default log size is 512KB which is much too small. The larger the size of a configured log, the more events it can hold. However, it is imperative that the proper balance be struck between log file size and

available hard disk space. Care must be taken that log files aren't configured to take up too much space and hinder system performance.

- **System Log & Application Log** – record events which are used by a security analyst to investigate Denial of Service (DoS) attacks. Figure 15 illustrates a maximum size of 49.9MB for both the System Log and the Application Log.
- **Security Log** – is the most important log file from a security perspective. It should be backed up and archived on a regular basis. It has a configured size of 192MB in this example.

We mentioned earlier how replication traffic is essential to the efficient operation of a WIN2K AD enterprise network. The problem with this fact of WIN2K AD operations is that both intrasite and intersite RPC (Remote Procedure Call) replication is unencrypted. The solution the GIAC system administrators came up with was to use IPSec (Internet Protocol Security) to provide end-to-end security for all replication between domain controllers within each child domain and to the GIAC root domain, **giac-ent.local**.

IPSec provides a number of advantages for network security in Windows 2000:

- **Authentication –** IPSec verifies the identity of a packet's original sender computer. WIN2K will automatically obtain IPSec certificates from the GIAC WIN2K Enterprise Certificate Authority (CA) with "computer auto-enrollment" enabled through Group Policy. Kerberos authentication can also be used.
- **Encryption –** strong encryption using 168-bit 3DES is available since all WIN2K systems have Service Pack 3 installed.
- **Integrity –** IP packets are verified that they haven't been tampered with through the use of MD5 or SHA-1 for integrity checking.
- **Packet Filtering –** static packet filtering is also available.
- **Transport to Applications and Services –** IPSec security is applied at the Network Layer (Layer 3) of the OSI Model so it is transparent to applications, services, and end users. Applications and services do not have to be upgraded or patched to make them IPSec-compatible.
- **Policy-Based Management –** IPSec can be centrally managed through Group Policies. System administrators have the flexibility to configure a separate set of IPSec policies for each OU within a domain if required.
- **Virtual Private Network (VPN) Support –** VPN is the ability of a remote user or router to connect to the GIAC network through the use of a secure encrypted channel.

Several issues exist with regard to WIN2K and IPSec. A hardware VPN/IPSec solution which companies like Cisco sell will provide better performance than a straight WIN2K VPN/IPSec solution. Interoperability of Microsoft's IPSec solution with other non-Microsoft IPSec implementations is also a possible point of contention. They don't seamlessly integrate. Also, the

use of IPSec places an additional load on the CPUs of each domain controller due the added encryption load. This additional load won't be a problem for the GIAC domain controllers since they have 2x900MHz PIII CPUs and 1GB RAM. However, smaller businesses could run into problems if they try to implement an IPSec-based solution on their existing WIN2K domain controllers if these systems are already near capacity. The best action to take would be to run a series of performance diagnostics on the domain controllers in question to determine CPU and RAM utilization before determining if an IPSec implementation will require additional hardware.

Despite these drawbacks to Microsoft's IPSec implementation within WIN2K, IPSec is still a viable solution to secure WIN2K AD replication traffic.

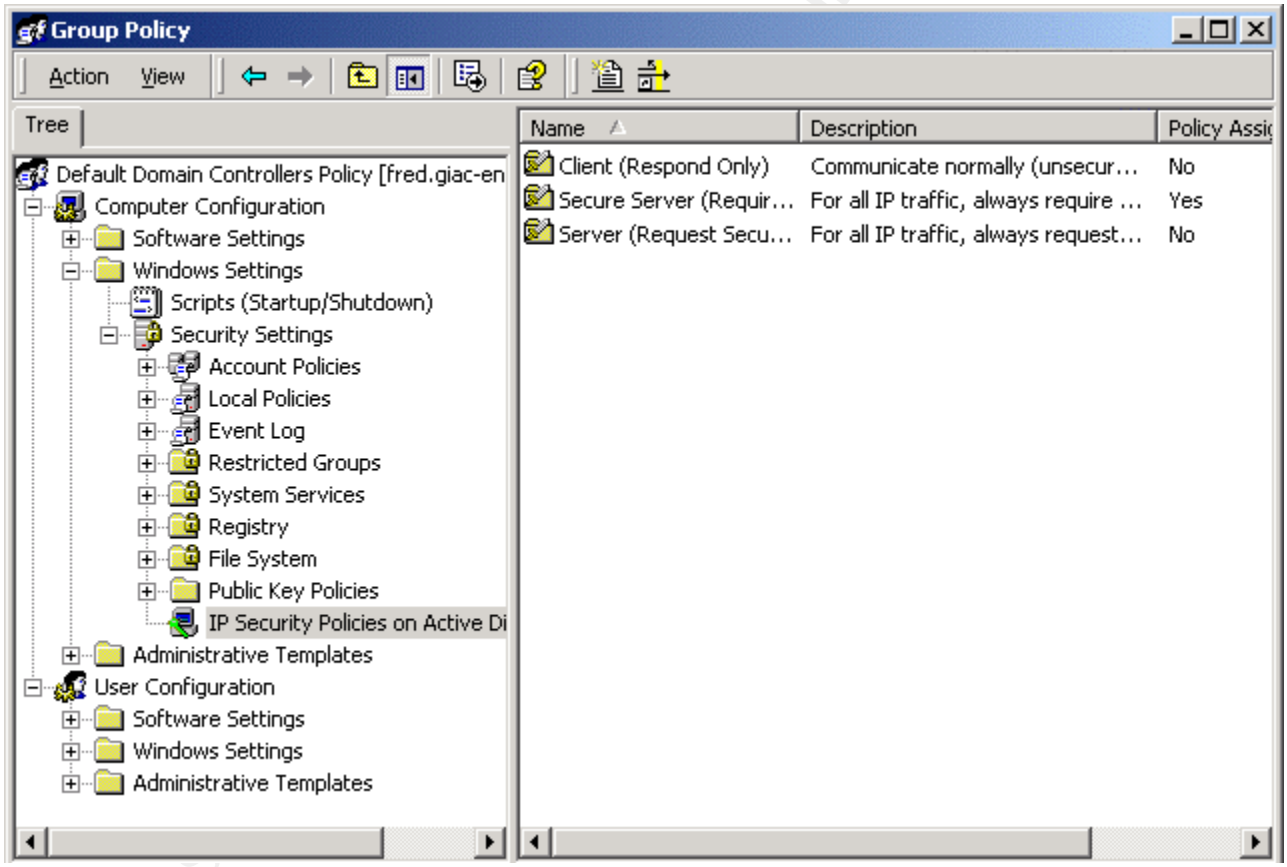

Figure 16: IPSec Group Policy – Domain Controllers

IP Security Policies on Active Directory provides three configuration options:

- **Client (Respond Only) –** A client normally communicates unsecured. Clients use the default response rule configured to respond to servers that request security. Only the requested protocol and port traffic with that server is secured.

- **Secure Server (Require Security) –** Always require security for all IP traffic using Kerberos trust. Unsecured communication with untrusted clients is not allowed.
- **Server (Request Server) –** Always requests security for Kerberos trusts for all IP traffic. Unsecured traffic is allowed with clients that don't respond to requests for secure communications.

The Default Domain Controller Policy (See Figure 16) for the **giac-ent.local** illustrates the assignment of the Secure Server (Require Security) option. Security Settings for the Default Domain Controllers Policy used the same configuration settings as the Default Domain Policy for passwords (See Figure 11), account lockout (See Figure 12), audit policy (See Figure 13), security options (See Figure 14), and event logs (See Figure 15).

The next task in the building of the GIAC WIN2K AD enterprise within the **Nashville.giac-ent.local** domain is the building of a support structure for the user, PC, and printer objects of the domain (See Figure 8). Support personnel comprise a Corp Help Desk, a US Help Desk, Corp HQ IMOs, and US OFF IMOs (See Table 12). The Corp Help Desk provides direct computer support to all PCs

Corp Help Desk	US Help Desk
Bob - TM Lead	Sue - TM Lead
Jim	Betty
Frank	Esther
Bill	Fannie
Corp-HQ-IMOs	**US-OFF-IMOs**
Sam	Kate
Tim	Matty
John	Gertrude
Luke	

Table12: Nashville Support Staff

within the Corporate HQ PC OU (See Figure 17). The Delegation of Control Wizard run on the Corporate PC OU (See Figures 18 & 19) specifies computer objects with Full Control permissions for the Corp Help Desk for the PCs in this OU. The Corporate HQ PC Help Desk personnel need this level of control since they're primarily responsible for the support to these 400 PCs.

The US Help Desk headed by Sue faces the same support mission for the 400 PCs within the US Office PC OU (See Figure 17). The Delegation of Control Wizard run on the US Office PC OU (See Figures 18 & 19) provides Full Control permissions for the US Help Desk on the PCs in this OU.

The US Help Desk also picked up the support mission for all the printers in in the Nashville domain. The Printers OU contains all these printers (See Figure 17). The Delegation of Control Wizard is run on the Printers OU this time (See Figure 20) with Full Control permissions given to the US Help Desk.

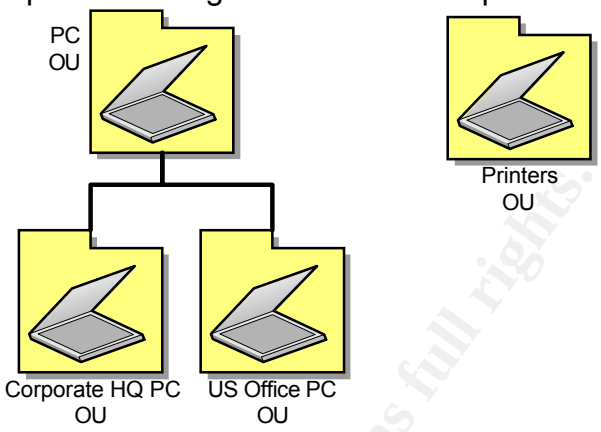

Figure 17: Nashville's PC OUs

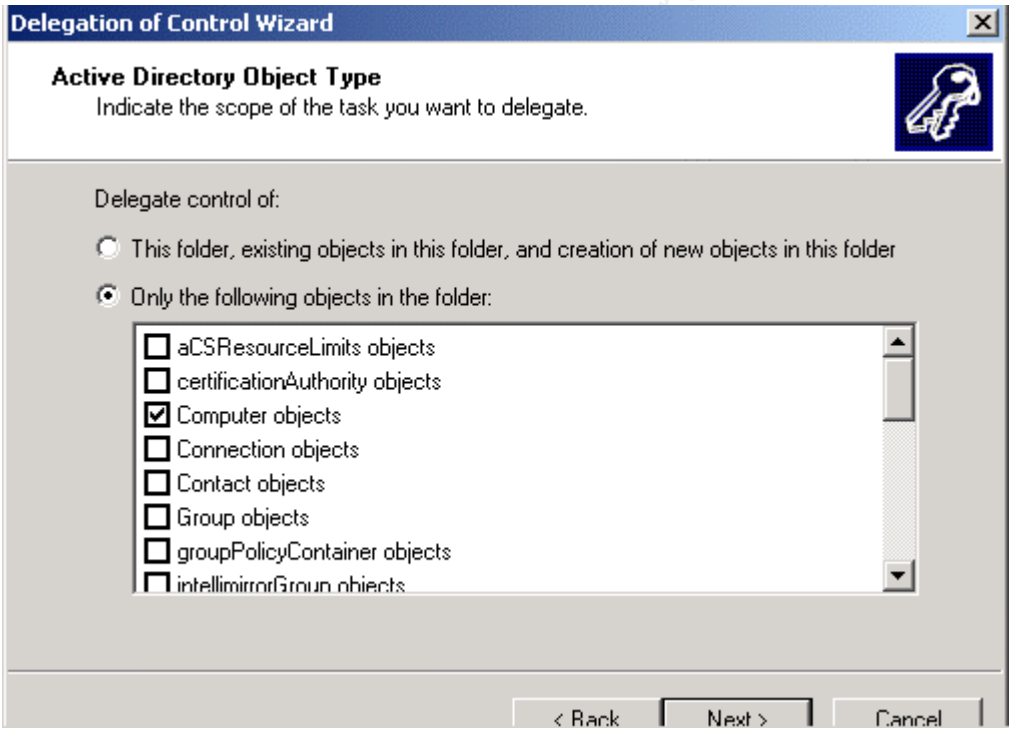

Figure 19: Delegation of Control Wizard – Computer Objects

A painstaking task which has plagued the two Help Desks since the days of the NT4 domains is resetting user passwords. Sue and Bob came up with the idea to delegate this menial task to selected individuals within the Corporate HQ Users OU and the US Office Users OU. Corporate IT Office system administrators approved the idea and the Nashville domain system

administrators create two groups, **Corp-HQ-IMOs** and **US-OFF-IMOs**, and populated these groups with users from the User OUs (See Table 12). Next, they ran the Delegation of Control Wizard another time to delegate the common task of resetting user passwords in their respective OUs to the individuals in these IMO groups (See Figure 22).

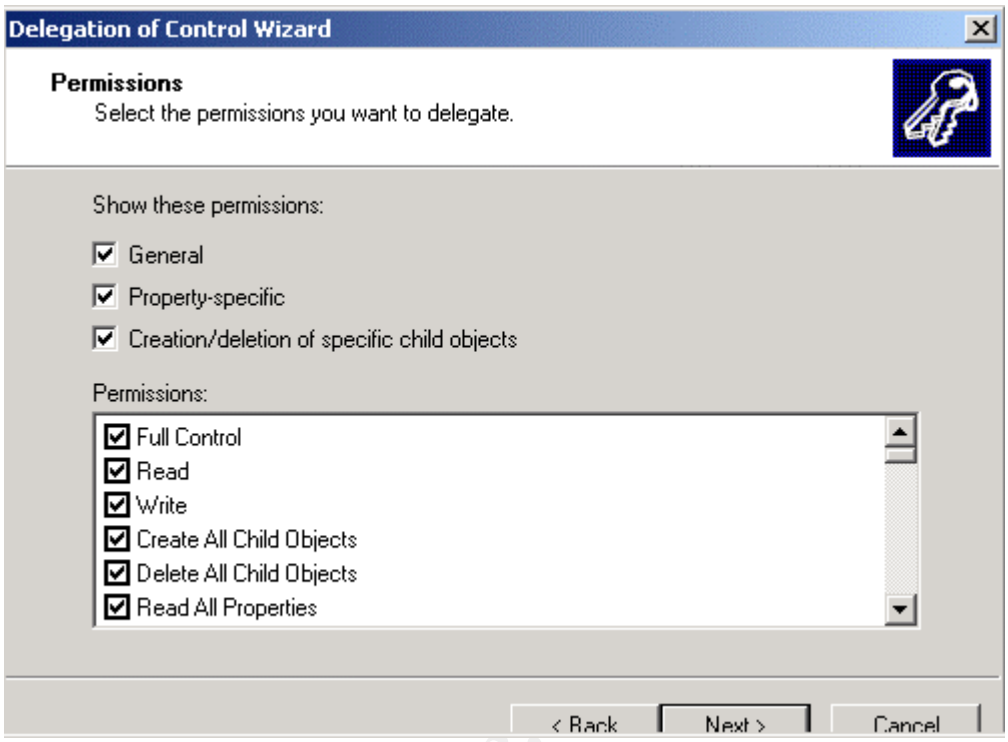

Figure 19: Delegation of Control Wizard – Computer Objects Full Control

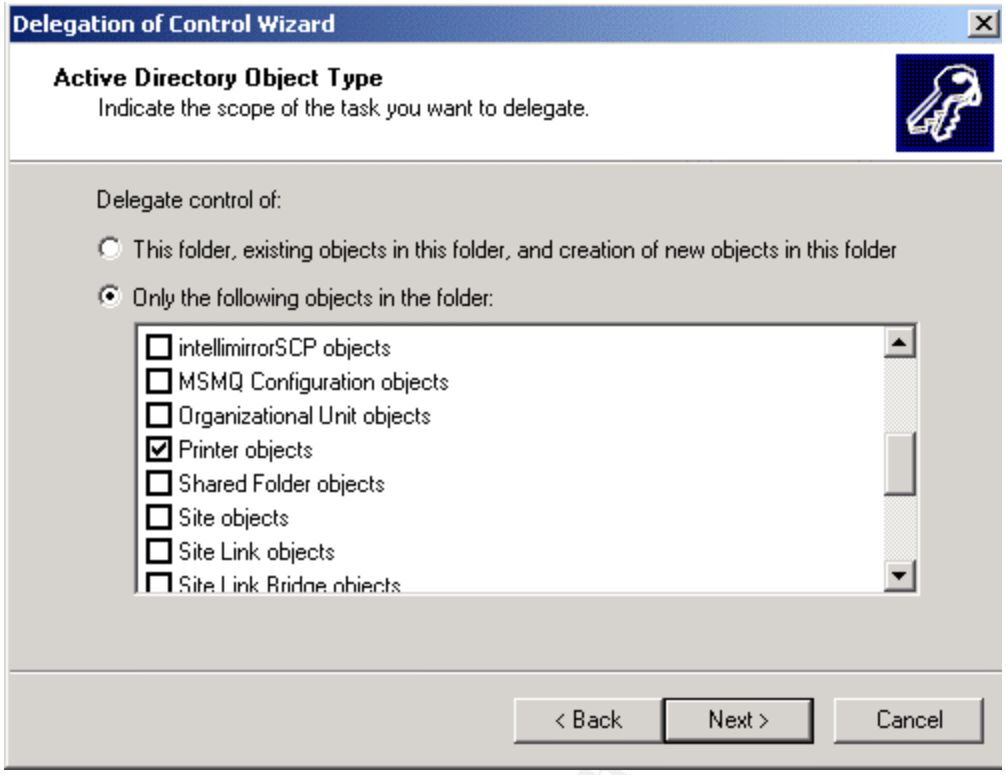

Figure 20: Delegation of Control Wizard – Printers OU

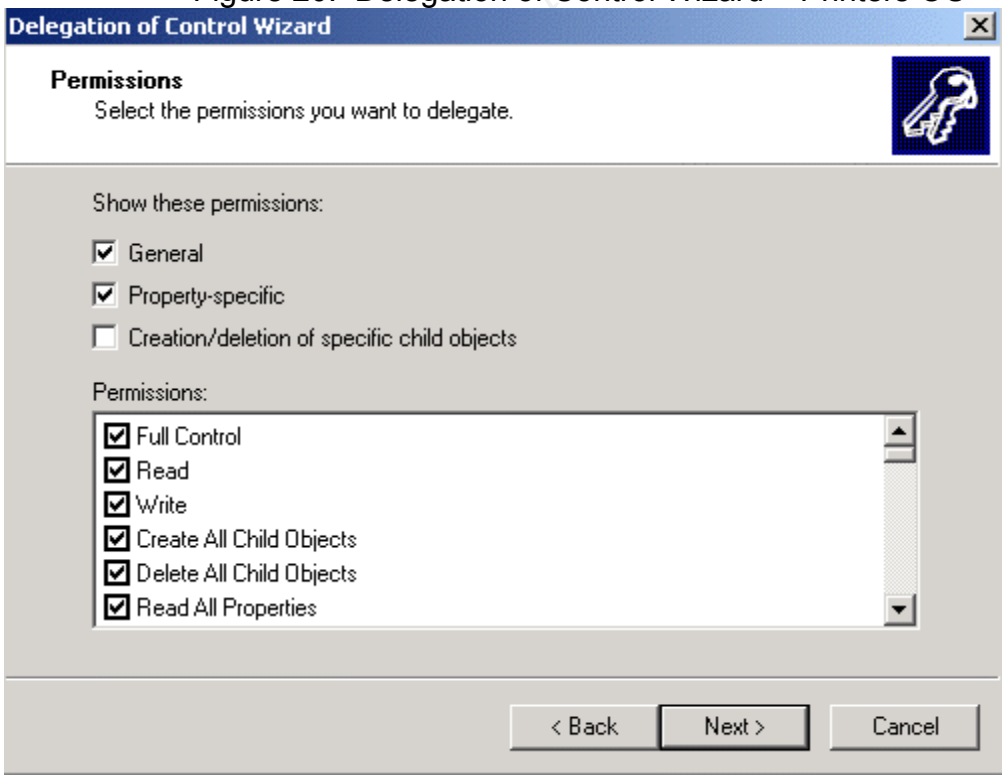

Figure 21: Delegation of Control Wizard – Printer Objects Full Control

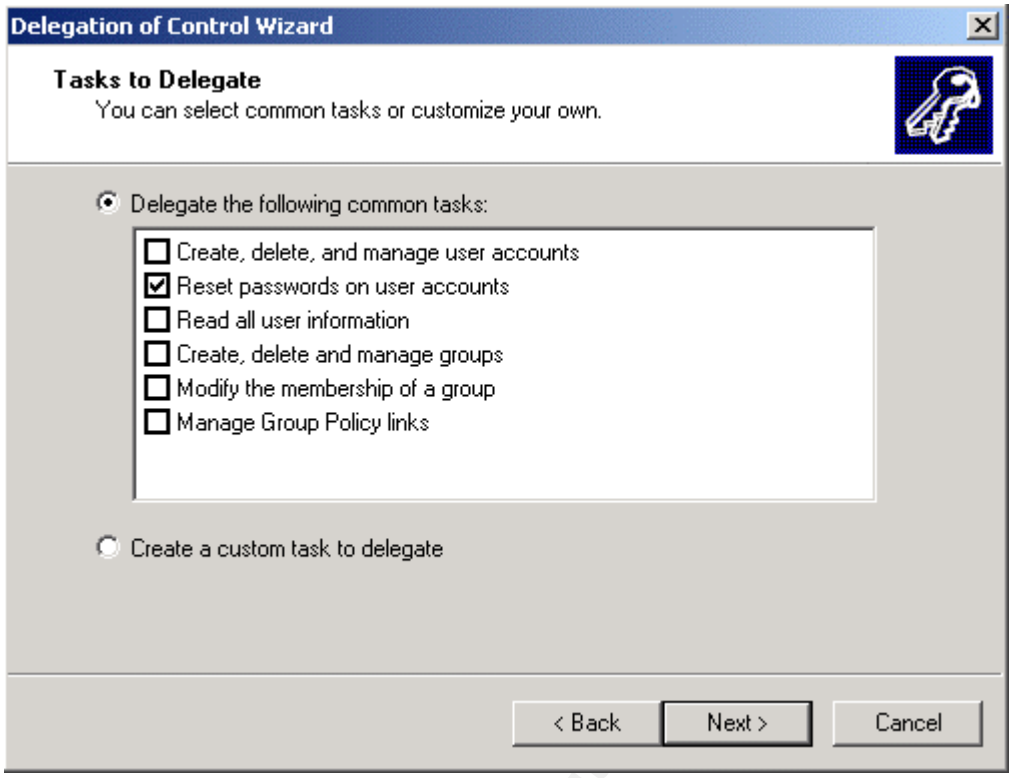

Figure 22: Delegation of Control Wizard – Printer Objects Full Control

Additional Security

Physical security was an area GIAC Enterprise all but ignored before the implementation of WIN2K AD and the building of the GIAC enterprise network. Companies often overlook the physical security of critical server hardware. Companies pour thousands of dollars into hardware and software yet they go cheap with regard to safeguarding the actual hardware once the software is installed and the system is operational. IT organizations should insist upon the proper physical security measures to ensure a secure operating environment for information systems they've spent so much time designing, purchasing, installing, and operating. Here are a few recommended physical security measures which will help:

- Locked rooms secured with combination locks, magnetic swipe cards, or even biometrics measures. Biometric devices include thumb or finger scanners or even retinal scanners.
- Surveillance cameras set up at strategic locations inside and outside the operational IT area.
- The number of administrators actually needing physical access to the server area is very small since we now have delegation of administration tools within Windows 2000.

- Terminal services are another alternative system administrators could possibly use to do their respective jobs while staying away from the server area.
- Use of a raised floor for the server area is also a preferred option. All ducting, cabling and power could run under the raise floor to free up more operational space.
- Sloppy system administration practices like leaving recovery disks on top of servers must be eliminated.
- More servers are now going the way of the rack mounted and server blade variety so they're easier to lock up. It is recommended that GIAC look into these types of servers as they life cycle replace their existing server systems.
- Off site storage is a must for backup tapes. Tapes must be rotated according to an agreed schedule and strictly accounted for at all times. The off site storage facility must be physically secured.
- All servers must be hooked up to an uninterrupted power supply (UPS) with the appropriate software installed and configured to allow for the graceful shut down of the system if main line power goes out.
- Extreme attention must be paid to physically securing every domain controller.

Conclusion

GIAC Enterprises is entering into a very exciting time in the company's history. The Windows 2000 Active Directory Enterprise Network is just starting to take off. This new network will reach out and touch all facets of GIAC's business operations. The result of such activity will be the generation of even more requirements. The WIN2K solution designed for GIAC Enterprises will scale to meet these new requirements while providing the security required GIAC's IT resources safe from harm. Building the enterprise network has carried with it many long hours and the future holds more of the same. However, it will be an interesting ride with dividends being paid in terms of increased productivity in a secure operating environment.

References

MS Windows 2000 Server Distributed Systems Guide. (Redmond, Washington: Microsoft Press), 2000.

Olsen, Gary. Windows 2000 Active Directory Design & Deployment. New Riders Publishing, 2001.

Abell, Roger, Herman Knief, Andrew Daniels, Jeffrey Graham, Windows 2000 DNS. New Riders Publishing, 2000.

Bragg, Roberta, Windows 2000 Security. New Riders Publishing, 2001.

Mitch Tulloch and Ingrid Tulloch. Microsoft Encyclopedia of Networking, 2nd ed, Redmond, Washington. Microsoft Press, 2002.

Moskowitz, Jeremy. Windows 2000 Group Policy, Profiles, and Intellimirror. Sybex Inc. 2001.

Fossen, Jason. **SANS Institute Track 5 – Securing Windows: 5.1 Windows 2000/XP Active Directory**, SANS Institute, 2002.

Fossen, Jason. **SANS Institute Track 5 – Securing Windows: 5.2 Windows 2000/XP Group Policy and DNS**, SANS Institute, 2002.

Fossen, Jason. **SANS Institute Track 5 – Securing Windows: 5.3 Windows 2000/XP PKI, Smart Cards and EFS**, SANS Institute, 2002.

Fossen, Jason. **SANS Institute Track 5 – Securing Windows: 5.4 Windows 2000/XP IPSec and VPNs**, SANS Institute, 2002.

Footnotes

[1] Mitch Tulloch, Ingrid Tulloch, **Microsoft Encyclopedia of Networking**, 2nd ed, Page 1019.

[2]Ibid, Page 535.

[3] Jason Fossen, **SANS Institute Track 5 – Securing Windows: 5.2 Windows 2000/XP Group Policy and DNS**, 2002, P. 107.

Last Updated: May 28th, 2017

Upcoming Training

SANS Cyber Defence Canberra 2017	**Canberra, Australia**	**Jun 26, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 06, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**