Global Information Assurance Certification Paper

Design a Secure Windows 2000 Infrastructure Without Limiting Your Networks Potential

Abstract
Microsoft's Windows 2000 was used for the network infrastructure of GIAC Enterprises, a fictitious company. The author assigned a possible line of business for GIAC and then designed its network around that business. Company size, physical location, and business needs were addressed. Migration to Active Directory did not include eliminating all stand-alone systems, although the same principles for securing Active Directory are applied to those machines as well. References with links to documents, some of which provide step-by-step implementation for key areas, have been included. The primary focus of this document is on the directory structure, and the methods used to secure the enterprise. Information regarding company operations, network layout, and services are included as well.

Brian Long
SANS GCWN
Practical Assignment
Version 3.1, Option 1

Table of Contents

Corporate Overview

Founded in 1974, GIAC Enterprises (GIAC) entered the business market as a manufacturer of utility consumption metering equipment (CME). Our customer base consists entirely of power, gas, and water companies, throughout the United States. Over the past several years, we have modified our line of strict mechanical units to now include a dedicated computer based system that reports on consumption and key operating areas specified by each utility line for field troubleshooting. Collective information from units deployed to specific areas provide companies with data for expansion and consolidation analysis. A significant corporate restructure was involved including the outsourcing of component manufacturing. GIAC still performs the final assembly of each unit.

Background

Product and program development revolves around the evolution in several key areas:

- The base design of the system unit and software which reports on both consumption of resources and CME health.
- Helping clients link their customer accounts database to our unit identifiers.
- Systems for customer data access and reporting.
- Unit troubleshooting utilities.

The CME calls into our facility once a week for reporting and obtaining updates. It may become necessary to initiate a connection with a CME in cases of troubleshooting from a field or office position, and/or on demand consumption reports. Most companies do not have, nor want to engineer, an infrastructure that will support this communication, which is why we host the connection service. Internet clients with SSL capable web browsers provide the method for our clients to access unit data at will. Our service, used in conjunction with wireless Internet capable notebook computers, provide field service personal the ability to trace problems from any location.

Although we have enjoyed quick adoption of our new CME line, continued success requires an environment full of resources and open to change. Our employees appreciate technology that is both current and functional. When our products were strictly mechanical units, we relied primarily on perimeter security and minimal network based intrusion detection. Now that our future depends on electronic trade secrets and the availability of customer data, we have a different attitude towards computer and network security. As a means of obtaining greater internal security and manageability without a significant increase in staff size, we recently migrated to Microsoft's Active Directory.

Operational Requirements

As with our product design models, we want technology that will enhance productivity and profitability. Prior to entering the design phase of our Active Directory (AD) environment, we read books on Windows 2000 and Exchange 2000. Microsoft's[*] website also provided an enormous amount of information including that which can be found in "Best Practices for Designing the Active Directory Structure."[†] It quickly became evident that the task at hand would be increasingly productive if we solicited input from executives and managers regarding areas that they have intimate knowledge of. This decreased the amount of assumptions made and provided management with general expectations for changes to come.

Flows and Staffing

It is imperative planners have an understanding of workflow in a security conscious AD environment. For us, the more information we obtained about what resources users "needed" to access, as opposed to what they thought they needed, the clearer our AD environment became. We learned that most user requirements differed beyond the department level.

Structure of Operations by Department[‡]

Business Operations

Positions: Chief Executive Officer (1), President (1), Chief Operations Officer (1), Chief Financial Officer (1), Chief Technology Officer (1), Executive Assistant (3).

Functions: Business review and strategic planning.

Sales and Marketing

Positions: Customer Account Manager (13), Outside Sales Rep (52), Sales Manager (3), Customer Service Manager (3), Customer Service Rep (17), Product Support Technician (35), Marketing Manger (1), Market Analyst (6).

Functions: Client acquisition and management. Product marketing. Market analysis. Assist customers with installation interface software. Customer satisfaction and support.

[*] The References section contains a complete listing of software and hardware vendors mentioned throughout this text.

[†] "Best Practices for Designing the Active Directory Structure" is a topic on Microsoft TechNet. The URL the topic points to is located in the References section.

[‡] The number of employees per position is in parenthesis ( ).

Research and Development

Positions: Product Manager (2), Senior Analyst (2), Analyst (4), Project Manager (3), Senior Developer (5), Developer (12), Product Specialist (4), Assembly Technician (10).

Functions: Develop new, and advance existing products. Ensure that products meet specifications and produce the functionality desired. Train customers on how to use services.

Finance and Human Resources

Positions: Controller (1), Accountant (2), Accounting Clerk (4), Human Resources Manager (1), Corporate Trainer (1).

Functions: Processing and accounting of internal finances and employee records. Internal end-user system and application usage training.

Business Administration

Positions: Office Manager (1), Office Supervisor (2), Administrative Assistant (8), Mail and Shipping Supervisor (1), Mail Clerk (4), Shipping Clerk (5), Operator/Receptionist (2).

Functions: Data entry for order processing and receivables. Process all incoming and outgoing mail. Telephone and visitor assistance.

Technical Services

Positions: Network Manager (1), Database Administrator (1), Desktop Administrator (2), Systems Engineer (1), Network Administrator (1), Systems Administrator (2).

Functions: Secure, install, and maintain all internal computer and network systems.

Other Design Considerations

Security

When it comes to network design and security, we (GIAC) did not invent the wheel. A more practical approach was for us to find proven methods and incorporate them into our environment. Few pieces of configuration information gained from research and experience were meant as hard-line, one size fits all, strategies. Enhancements to the ideas of others are often necessary to achieve a satisfactory result. In fact, we must continually evaluate and if appropriate, adjust configurations to ensure we are in compliance with the policies and principals set forth by the company and technology industry.

Some books and articles recommend designing network infrastructure around the written policies of the company. We [now] embrace that theory. Much of the principals and written policies regarding our computing environment were derived from successful communication between the technology staff and executive officers. The consciousness obtained from public resources and fee based conference material from the SysAdmin, Audit, Network and Security Institute (SANS)[*] and other institutions are invaluable for bridging communication. A fine example of the information available is the "The SANS Security Policy Project."[†] The project makes available written policy templates and other related resources.

Physical security was already addressed by all server systems and network hardware being locked in rooms with electronically controlled access. Backup media rotations are logged and include internal and off-site vaults.

Sampling of the technology based security concerns we addressed

- HIPAA compliance[‡]
- Personal data not under HIPAA
- Internet abuse
- Software installation and maintenance
- Current and future CME designs
- "Curious" users
- Internal and external attacks, including viruses/trojans
- Disaster recovery
- Secure communication

As we progress into the implemented architecture, it is worth noting that we set a goal to have end-user intervention be a last resort in security. Experience tells us that short of something an end-user has no way around, such as changing

[*] SANS home page http://www.sans.org/
[†] "The SANS Security Policy Project" website http://www.sans.org/resources/policies/
[‡] United States Department of Health and Human Services "Administrative Simplification" website http://aspe.hhs.gov/admnsimp/ -Link obtained from SANS.

passwords, user based controls would be ignored. This presented some significant hurdles in that we wanted to greatly refine internal security but still maintain a user friendly environment. Our design also had to take into consideration that users throughout GIAC were accustom to having local administrative privileges at their workstations. Testing was done to ensure that the "required" functionality of the computing environment, and flexibility to change the environment, was not hampered by limiting local permissions.

Platform Selection

GIAC takes full advantage of the Microsoft platform at the desktop and server levels. We have invested significant time and financial resources in ensuring the technical staff is fluent within a Windows environment. Similarly, our line of CME is based on Windows CE technology.

Budget

GIAC's network switches and routers, as well as a significant portion of our servers were no older than 2 years old when AD was implemented. This was in part, due to an initiative to upgrade our backbone to fiber and perform a rip-and-replace on the CAT5 going to the desktop in favor of CAT5e, in anticipation of a future move to voice over IP. We proposed moving the client systems off NT4 with an upgrade to Windows XP. This upgrade would enable leveraging more from Group Policy and take advantage of some additional features of XP, such as "System Restore" and "Driver Rollback". We already were on Microsoft's "Software Assurance" program so no additional software costs would be incurred. Everyone thought this was a fantastic idea, that was until we found that nearly every desktop system outside of the Technical Services and Research & Development departments had motherboards that were incapable of running XP. The costs for replacing motherboards, which involved downtime, as well as complete system replacement were weighed. In the end, it was more economical to replace the systems rather than deal with the downtime and costs associated with major hardware upgrades.

We did invest in additional servers to accommodate the number of Domain Controllers in our AD enterprise. Additional overhead and security concerns of having both building locations participate in the domain environment over the Internet motivated us to standardize on a firewall for each building that would allow a site-to-site Virtual Private Network (VPN) without working through vendor compatibility issues. Installation of Microsoft (MS) Exchange 2000, a dedicated network backup server, and MS ISA Server did require new machines as well. Running down the list of installed applications and services yielded no additional surprises. All were compatible (after updates) running on Win2k and/or XP with the exception of our voicemail system which we did not upgrade.

Backend Systems

All production servers run Microsoft Windows 2000 Server, Service Pack 3, with the exception of the voicemail system which is a standalone Windows NT4 Server, Service Pack 6a installation. Hardware is Dell branded with a minimum configuration of:

- Pentium III 800Mhz processor
- 256MB RAM
- Dedicated RAID 1 for operating system
- Dedicated RAID 1 and/or RAID 5 for each database installation, database logs, file storage, web server files, etc., where appropriate
- 2 power supplies

Servers with heavy loads may have multiple Intel XEON processors, increased RAM, hardware encryption capable NIC's, dedicated hard drive for virtual memory, and/or multiple RAID controllers. Servers that use "Windows Backup"[*] have a single internal or external tape drive. Servers that host backup services for domain members have an external tape array.

All servers in the lab run Windows 2000 Server or beta Windows Server 2003. Lab hardware is Dell branded and is comprised of single processor servers with 512MB RAM, and a single hard drive.

All systems and network equipment are protected by a facility wide UPS, consequently no individual system has a dedicated battery backup.

Client Systems

All lab, Technical Services, and Research & Development department workstations run Windows XP Professional, Service Pack 1, or Windows 2000 Professional, Service Pack 3. All other internal end-user machines run Windows XP Professional, Service Pack 1. Hardware is Dell branded.

Network Equipment

Routers, switches, and hubs are Cisco or Nokia branded. Network time server is a Symmetricom (formerly TrueTime) GPS based product. MUX units (not shown) are manufactured by Adtran.

[*] "Windows Backup" is in reference to the backup utility included with Microsoft Windows NT4 and Windows 2000.

Logical Network Diagram

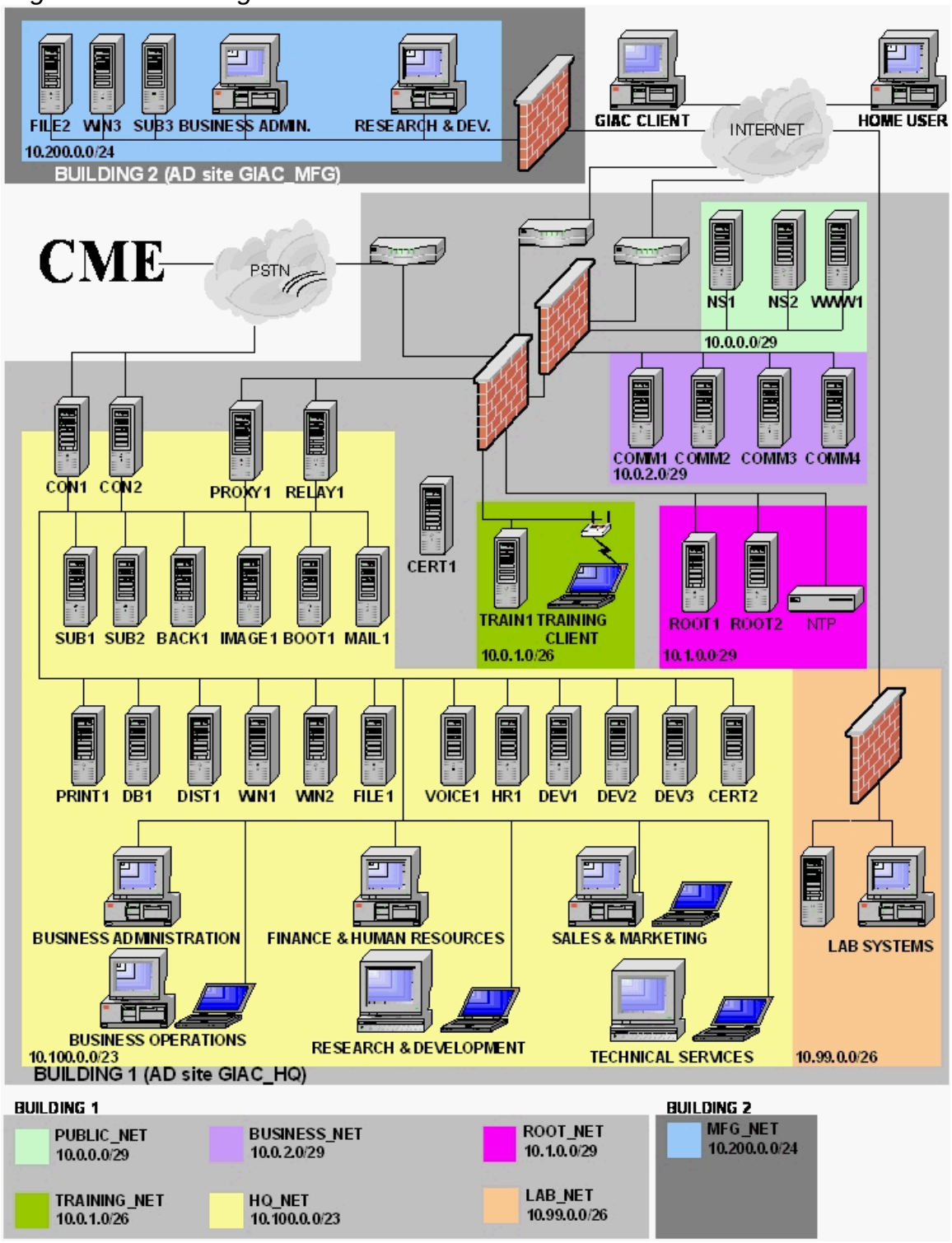

Figure 1

Network Segments

Each named network (see Figure 1) has been segmented by firewalls for all of the following reasons:

- Limit number of hosts scanned when performing internal sweeps.
- Separation by firewall policy and/or IPSec policy to allow/deny communication based on network address when reasonable.
- Firewalled segments provide a means of quickly isolating system groups from external networks (ie. isolate TRAINING_NET from the Internet without shutting down access to PUBLIC SERVERS).

Additional reasons for network separation are provided if appropriate.

PUBLIC_NET
DNS and web servers available for public access. Systems do not participate in AD. Located in BUILDING 1.

BUSINESS_NET
Web and database servers accessible to subscribers of GIAC's services. Systems do not participate in AD. Located in BUILDING 1.

ROOT_NET
Domain Controllers for the root AD domain giac.corp. NTP server provides time synchronization service for ROOT1 and all network hardware. Highly restricted and monitored segment as the Domain Naming Master and Schema Master reside on this segment. Located in BUILDING 1, site GIAC_HQ.

TRAINING_NET
Facilities for training GIAC employees as well as GIAC customers. Client machines are connected via wireless network which increased the need for segmentation. Systems do not participate in AD. Located in BUILDING 1.

HQ_NET
Internal server and client systems. Most participate in the AD child domain ops.giac.corp. Located in BUILDING 1, site GIAC_HQ.

LAB_NET
Isolated network that is only reachable by Internet connection or sneaker net. No production or proprietary information is stored on this network. It serves as a test environment for a variety of issues (patches, config. changes, connectivity, etc.). Located in BUILDING 1.

MFG_NET
Internal server and client systems that participate in the AD child domain ops.giac.corp. Located in BUILDING 2, site GIAC_MFG.

Systems Purpose

The following breakdown outlines the primary purpose(s) of each Windows server system named in Figure 1.

BACK1

Network backup services using Veritas Backup Exec. Backs up all domain member servers.

BOOT1

Remote Installation Services (RIS) and DHCP services for BUILDING 1.

Intermediate Certificate Authority fulfills certificate requests for general user and client needs. Provides a separation on types of certificates issued limiting exposure in the case this, or another, authority is compromised.[*]

CERT1

Offline root Certificate Authority. Not connected to network thus providing a cutoff point in the case of a subordinate (authority) being compromised. Uses Windows Backup.

CERT2

Intermediate Certificate Authority fulfills certificate requests for administrative, development, and core system needs. Archive for development designs and code. Provides a separation on types of certificates issued limiting exposure in the case this, or another, authority is compromised. Hosts roaming profiles for administrative accounts.

COMM1 & COMM2

Web servers that participate in round-robin (by virtue of firewall policy) for fulfilling requests made by GIAC customers. Not part of Active Directory. Uses Windows Backup.

COMM3 & COMM4

MS SQL Server 2000 systems that store data for GIAC's current service subscribers. All data is available for 2 years. Not part of Active Directory. Uses Windows Backup.

CON1

32 internal modems for initiating connections to CME units by GIAC personnel for troubleshooting purposes.

[*] Following recommendation of Chapter 12 in Microsoft's "Windows 2000 Server Deployment Planning Guide."

CON2
32 internal modems for initiating connections to CME units for on-demand reporting.

DB1
MS SQL Server 2000 that houses all of GIAC's current business records (customers, inventory, billing, etc.).

DEV1, DEV2, & DEV3
Systems used by Research and Development. Contain alpha and beta versions of delivery and reporting systems. Not AD members. Uses Windows Backup.

DIST1
Media archive for installable applications.

FILE1
General use file and profile server for employees working from BUILDING 1.

FILE2
General use file and profile server for employees working from BUILDING 2. RIS and DHCP services for BUILDING 2. Print server for BUILDING 2. Runs IIS to allow publishing of printers to Active Directory.

HR1
Storage for all employee data that is in electronic format and falls under the guidelines of HIPAA. Application server for payroll system which is outsourced and requires a modem for pay period transfers. Modem is set to dial out only.

IMAGE1
Controls optical storage array. All CME data and related customer information is permanently archived on write-once media. Network backup services using Veritas Backup Exec. Performs a weekly "copy" backup on Domain Controllers, online Certificate Servers, and portions of MS Exchange. This backup provides a means of recovering core authentication systems in the case of disaster and BACK1 becomes unavailable.

MAIL1
MS Exchange 2000 Server, Service Pack 3.

NS1 & NS2
Publicly accessible DNS servers. Contains only minimal "public" DNS entries that use a different name space from the internal enterprise. Also performs all Internet DNS queries for internal DNS servers.

PRINT1
Print server for BUILDING 1. Runs IIS to allow publishing of printers to Active Directory. Performs batch functions for CME data.

PROXY1
MS ISA server. Acts as proxy for outbound Internet traffic from HQ_NET and inbound/outbound traffic between HQ_NET and other GIAC networks. RADIUS authentication services for CME connections. The CME "user" database is stored locally. All CME's reuse one of 1000 randomly generated username/password combinations.

RELAY1
Gateway SMTP virus protection, distribution and update server for client and server installations of virus protection software.

ROOT1
Active Directory integrated DNS for the giac.corp domain. PDC Emulator Master, RID Master, and Infrastructure Master for giac.corp domain. Runs TrueTime software to communicate securely with NTP system. Is the master time source for all other Domain Controllers.

ROOT 2
Active Directory integrated DNS for the giac.corp domain. Global Catalog, Schema Master, and Domain Naming Master for the enterprise.

SUB1
Active Directory integrated DNS for the ops.giac.corp domain. Secondary DNS server for the giac.corp domain. PDC Emulator Master, RID Master, and Infrastructure Master for the ops.giac.corp domain.

SUB2
Active Directory integrated DNS for the ops.giac.corp domain. Secondary DNS server for the giac.corp domain. Global Catalog for the enterprise.

SUB3
Active Directory integrated DNS for the ops.giac.corp domain. Secondary DNS server for the giac.corp domain. Global Catalog for the enterprise.*

TRAIN1
Authentication services (Cisco Secure ACS) for wireless clients. Not AD member. Uses Windows Backup.

VOICE1
Voicemail server. Not AD member. Uses Windows Backup.

* Microsoft recommends at least one Global Catalog in each site. See "Global Catalog Replication" in Chapter 6 of Microsoft's "Windows 2000 Server Distributed Systems Guide."

WIN1 & WIN2 & WIN3
Management software from NetIQ. NetIQ and several other services we run on our network need the assistance of WINS which has been installed on these same systems.

Active Directory Design

GIAC choose a single tree, multiple domain environment.

Domain Hierarchy
The geographic location of GIAC requires only a single AD domain in that replication traffic can be easily sustained over the existing Wide Area Network (WAN) link. With that said, during the design phase of our AD structure a question was presented on the current and future ways clients are granted permission to the Business Client Servers. Consideration was given to abandoning the current client account authentication process that involved storing usernames and passwords in a SQL database, in favor of the control provided by AD. Storing these accounts in AD does pose a potential problem in that our internal password policy is strict. It is believed that from a customer standpoint, the strict password controls would be cumbersome. The debate over the client account authentication process continues. We had to take into consideration that if indeed the client accounts were moved to our AD environment, password policies could be used for political leverage.

Other issues regarding the domain hierarchy

- We did not want to overburden our site connection with the unneeded replication of changes made to the accounts of 50,000 utility workers.
- Company attorneys were concerned about possible legal ramifications of client accounts having a naming hierarchy that was below our corporate office domain; ie. a child domain of *name*.giac.corp would be *child.name.*giac.corp.
- There was a possibility that the service portion of GIAC would be split into a separate entity with GIAC being the parent organization.

To satisfy these potential issues we choose to implement two domains, with the child domain hosting all possible resources and accounts. This gives us the freedom to add another child domain for client accounts at any time without significant effort. Adding a child domain instead of another tree retains the administrative advantages that AD provides over NT4. The password security on any new child domain could be set as the company sees fit. The security risks involved with our having two domains are minimal as the root domain is well protected and fairly isolated. The other potential issues raised are also addressed with this domain model.

Replication of Domain Controllers

The site Default-First-Site-Name was renamed to GIAC_HQ* and is comprised of the network segments 10.1.0.0/29 and 10.100.0.0/23. ROOT1, ROOT2, SUB1, and SUB2 are located under GIAC_HQ. A second site named GIAC_MFG was created to speed users authentication at BUILDING 2. A single DC, SUB3, which is also a GC†, is on this segment (10.200.0.0/24). The sites are connected using RPC over IP transport on a single T1 (1.54Mbps) link. To aid in the integrity of this replication, a site-to-site VPN has been implemented using 3rd party (non-Microsoft) firewalls at both building locations.

Site Configuration

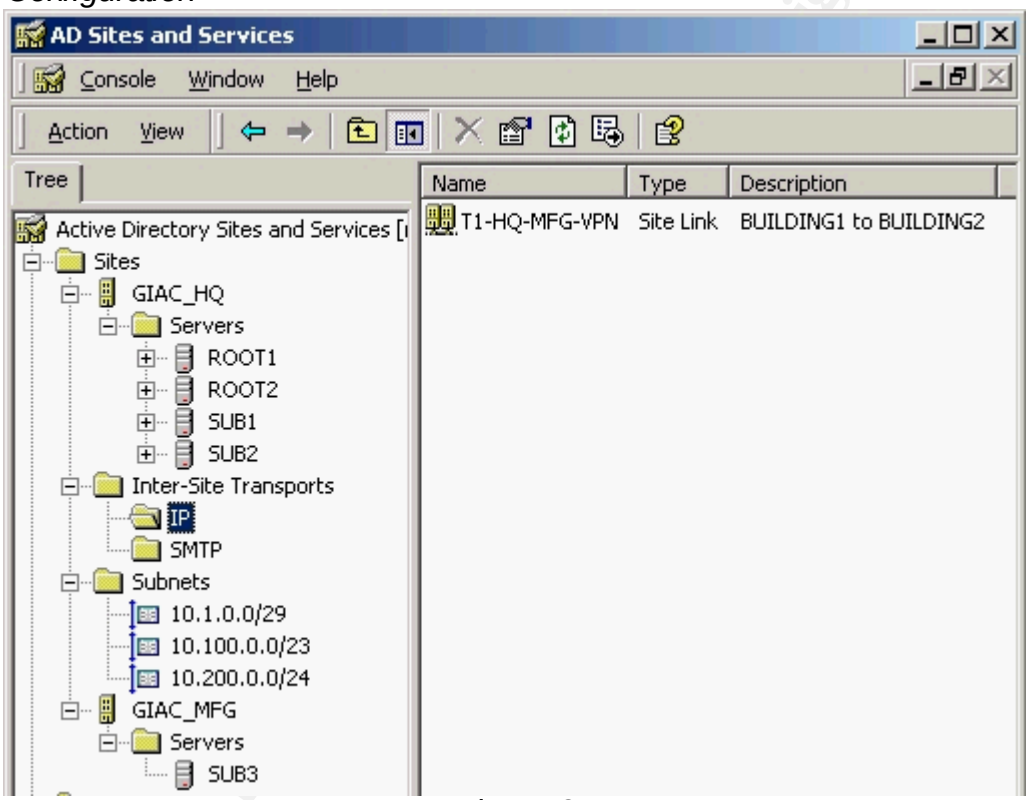

Figure 2

Site Naming Message

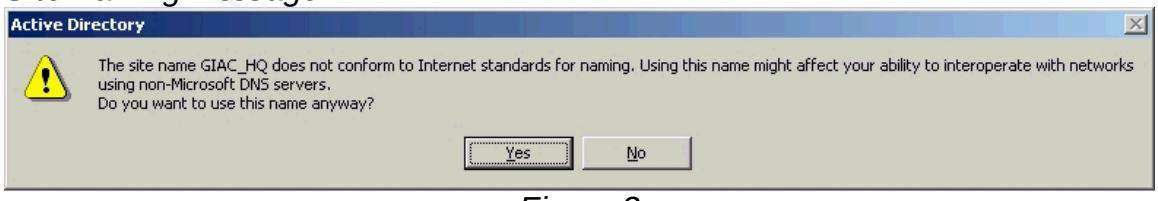

Figure 3

* Using the underscore "_" character generates a message warning that our naming convention may not work with non-Microsoft DNS servers – see Figure 3. We are not concerned with this as we only use Microsoft DNS.

† The AD rolls for each DC (ROOT1, ROOT2, SUB1, SUB2, and SUB3) can be found under their respective machine names on page 12.

Logical Active Directory Diagram[*]

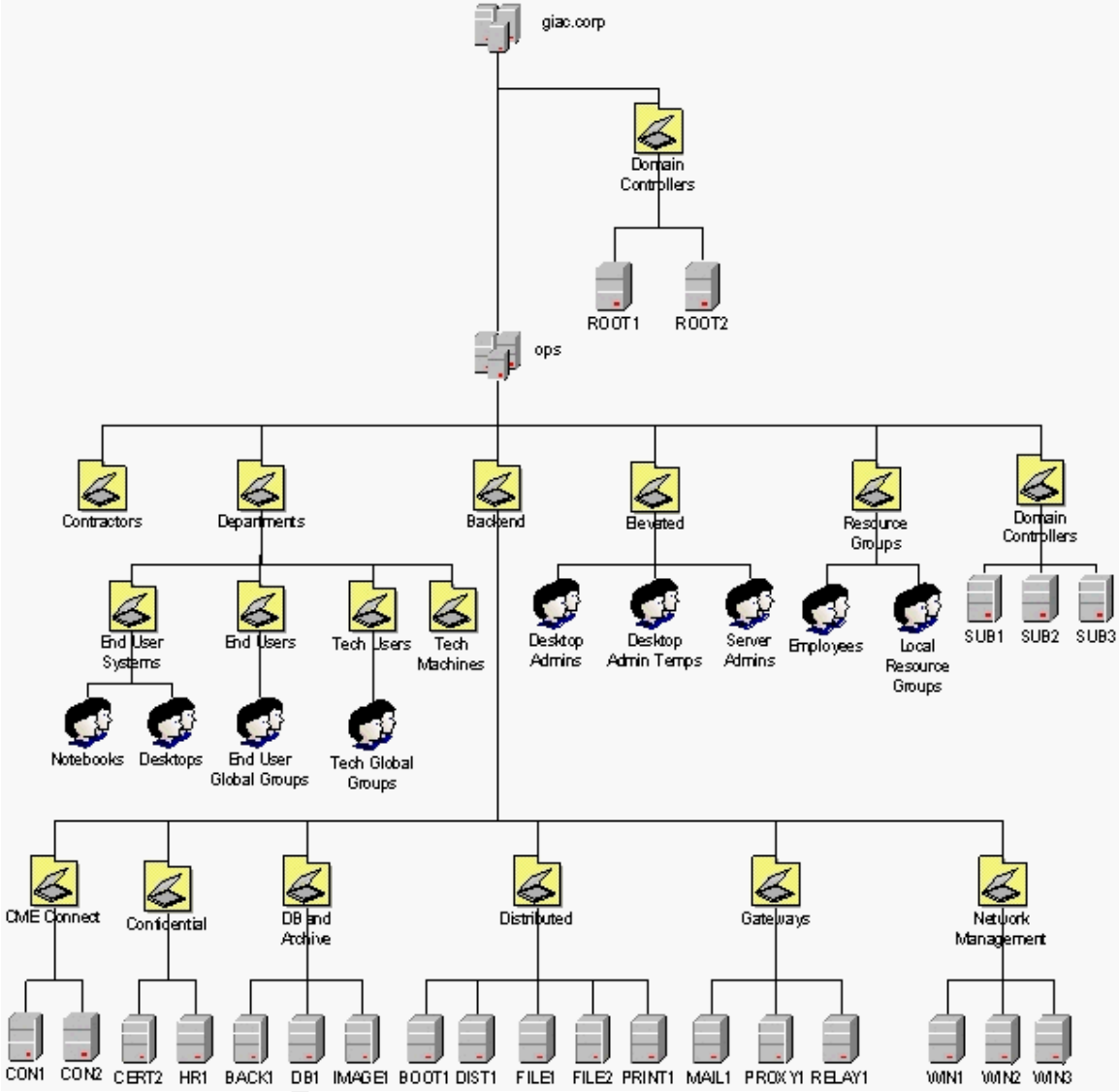

Figure 4

[*] Figure 4 contains the objects that play a part in the overall structure of our AD design and provides the foundation for group policies that are currently in force. Groups entitled "Local Resource Groups," "End User Global Groups," and "Tech Global Groups" are placeholders for many groups of that type (Global/Local).

Namespace
All DC's have the DNS service installed. Delegation of ops.giac.corp was assigned to SUB1, SUB2, and SUB3. The DNS servers in the OPS domain act as secondary (non-AD integrated) DNS servers for giac.corp. This enables us to limit DNS queries destined for the root domain to only the DC's from OPS. ROOT1 and ROOT2 use SUB1 and SUB2 as forwarders. All queries originating from inside out organization for resources outside of our enterprise are sent to the OPS DNS servers which utilize our public Name Servers as forwarders. These procedures, along with others mentioned later aid in ensuring DNS resolution inside our enterprise remains functionally correct.

The root domain giac.corp is predominantly empty. Since we do not have any down-level NT4 Domain Controllers (old NT4 domain was abandoned), the domain was original installed in Native Mode for the security benefit of removing the "Everyone" group from the "Pre-Windows 2000 Compatible Access" group. Although MS Exchange 2000 Server is installed in the OPS domain, we put the Exchange installation user in the root domain for isolation. The Exchange 2000 installation also created the "Exchange Domain Servers" and "Exchange Enterprise Servers" groups in this domain. The creation of service accounts required for management and security applications (backups, updates, monitoring) was performed as needed. All of these accounts and groups reside in the default container "Users".

The use of "Universal Groups" is limited to those automatically created. Group types can be changed easily should "Universal Groups" become needed in a larger capacity.

Following internal guidelines that only a limited number of individuals have access to the Domain Administrators account(s), and that standard accounts be used for non-administrative tasks, is fairly easy given the relatively small size of our Technical Service's department. The Systems Engineer and the Network Administrator both have two additional accounts. One is a member of ops.giac.corp/Elevated/Domain Admins and the other is a member of ops.giac.corp/Elevated/Server Admins. The two Systems Administrator's have an additional account that is a member of ops.giac.corp/Elevated/Server Admins. Only the Network Manager, Systems Engineer, and Network Administrator have access to the password book that contains the default enterprise accounts. Most of our administrative tasks are performed with scripts.[*] "Run as" is used when possible to elevate permissions as needed. Terminal Services, or a local console session is used for tasks that cannot be performed with "Run as." In cases where Delegation has been declared, failed attempts are audited.

[*] Eck, Thomas. "Windows NT/2000 ADSI Scripting for System Administration." Indianapolis: MTP. 2000.

Root Domain Organizational Units Detail[*]

giac.corp/Domain Controllers
Purpose: Default for Domain Controllers.
Contains: ROOT1; ROOT2

Child Domain Organizational Units Detail

ops.giac.corp/Contractors
Purpose: Holds user and computer accounts for vendors, consultants, or other outside parties that need temporary user and/or computer accounts on our network. The "Guest" (renamed) account is not used. Allows for stringent Group Policy enforcement without effecting general operations. Currently Empty.

ops.giac.corp/Departments
Purpose: Entry point for delegation of certain administrative tasks that apply to all employees as well as point of Group Policy inheritance.
Contains: OU: End User Systems; OU: End Users; OU: Tech Users; OU: Tech Machines
Delegations: Human Resources group and Desktop Admins group: Create, delete, and manage user accounts.

ops.giac.corp/Departments/End Users
Purpose: Point of Group Policy inheritance. Simplifies the administration of Group Policies related to users that do NOT regularly possess "Power Users" or greater privileges. Not all policies assigned to this OU should be applied to all users. Users that should not have policies applied are denied Read access to the policy based on group membership.
Contains: All employees that fit the afore mentioned criteria and the Global Groups that these users belong to.

ops.giac.corp/ Departments/End User Systems
Purpose: Point of Group Policy inheritance. Simplifies the administration of Group Policies related to computers that are NOT regularly used by individuals possessing "Power Users" or greater privileges. Not all policies assigned to this OU should be applied to all machines. Machines that should not have policies applied are denied Read access to the policy based on group membership.
Contains: Computers falling under the classification mentioned above. These systems are then inserted into either the Notebooks or Desktops group.
Delegation: Server Admins group: Full Control.

[*] The Organizational Unit (OU) details assume the default Security permissions unless modified under "Delegation".

ops.giac.corp/ Departments/Tech Users
Purpose: Point of Group Policy inheritance. Simplifies the administration of Group Policies related to users that DO regularly possess "Power Users" or greater privileges.
Contains: All employees that fit the afore mentioned criteria and the Global Groups that these users belong to.

ops.giac.corp/ Departments/Tech Machines
Purpose: Point of Group Policy inheritance. Simplifies the administration of Group Policies related to computers that ARE regularly used by individuals possessing "Power Users" or greater privileges.
Contains: Computers falling under the classification mentioned above.
Delegation: Server Admins group: Full Control.

ops.giac.corp/Backend
Purpose: Directory organization and a point of Group Policy inheritance to Server based systems other than Domain Controllers.
Contains: OU: CME Connect; OU: Confidential; OU: DB and Archive; OU: Distributed; OU: Gateways; OU: Network Management

ops.giac.corp/Backend /CME Connect
Purpose: Point of Group Policy inheritance for systems that contain modem banks for the purpose of dialing CME's.
Contains: CON1; CON2

ops.giac.corp/Backend /Confidential
Purpose: Point of Group Policy inheritance for systems that contain sensitive internal information.
Contains: CERT2; HR1

ops.giac.corp/Backend /DB and Archive
Purpose: Point of Group Policy inheritance for systems that contain backup, archive, and internal databases.
Contains: BACK1; DB1; IMAGE1

ops.giac.corp/Backend /Distributed
Purpose: Point of Group Policy inheritance for systems that contain general access information and services.
Contains: BOOT1; DIST1; FILE1; FILE2; PRINT1

ops.giac.corp/Backend /Gateways
Purpose: Point of Group Policy inheritance for systems that perform proxy and/or mail services.
Contains: MAIL1; PROXY1; RELAY1

ops.giac.corp/Backend/Network Management

Purpose: Point of Group Policy inheritance for systems that monitor network and system health and security.

Contains: WIN1; WIN2; WIN3

ops.giac.corp/Elevated

Purpose: Point of Group Policy inheritance for groups that have been granted elevated privileges. Desktop Admin Temps is used in cases when an end user account must have administrative privileges on the local machine to perform a specific task that either could/should not be assigned with Group Policy or are rare enough that modification/creation of a policy was not warranted. A script runs nightly to purge all members of the Desktop Admin Temps group to remove any users that were inadvertently left. This could be performed with Group Policy\..\Restricted Groups but we usually need the settings to survive several reboots.

Contains: The Global Groups: Desktop Admins, Desktop Admin Temps, and Server Admins. Individual accounts and Local Groups that are used for sensitive tasks and access, such as services that must be run under a domain account, and resources pertaining to trade secrets.

ops.giac.corp/Resource Groups

Purpose: Organization and administrative delegation for local groups that are assigned to resources in which managers and other trusted individuals regularly assign permissions.

Contains: Various groups and the group "Employees". "Employees" is a security group that is often used when assigning permissions associated with all GIAC employees in place of the Everyone group. This provides a more granular approach than substituting "authenticated users" for Everyone.

Delegation: Groups that contain managers and other trusted individuals from the End Users and Tech Users OU's have "Modify the membership of a group".

ops.giac.corp/Domain Controllers

Purpose: Default for Domain Controllers. Point of Group Policy inheritance.

Contains: SUB1; SUB2; SUB3

Group Policy

Policies were derived using the template indicated. The default Windows 2000 templates and files from the "Security Operations Guide for Windows 2000 Server" were used as a baseline. The following sections will detail the significant changes made to the templates and certain key policy items that are in the templates.*

Root Domain Group Policy

The "Default Domain Policy" is allowed to propagate to the Domain Controllers OU eliminating the need for an additional policy.
NOTE: "Resource Domain" type activity would render some of these policies intolerable.

Default Domain Group Policy

Applied to: giac.corp
Templates: baseline.inf, securedc.inf
Notes: Speed of policy processing is not a concern so both User and Computer portions are active. Neither No Override or Block Policy inheritance is required.

[Computer Configuration\Windows Settings\Security Settings\Account Policies\… …Password Policy]

- Enforce passwords remembered
  - 24
- Maximum password age
  - 5 days
- Minimum password age
  - 4 days
- Minimum password length
  - 15 characters
- Passwords must meet complexity requirements
  - Enabled
- Store password using reversible encryption for all users in the domain
  - Disabled

Rationale: Only the default (renamed) accounts and necessary service accounts exist in this domain. The accounts are set to have passwords that never expire, and "user can not change password." In turn, we have a written policy to change these passwords every 30 days. A strict password policy does not hamper administration. We have no need for DES, MAC UAM, or Digest authentication, nor do we use Exchange IM so storing passwords encrypted with DES is not necessary.

* Microsoft's "Security Operations Guide for Windows 2000 Server" and "Security Operations Guide for Exchange 2000 Server" were significant resources for building Group Policies.

[Computer Configuration\Windows Settings\Security Settings\Account Policies\…
…Account Lockout Policy]

- Account lockout duration
  - 0 (forever)
- Account lockout threshold
  - 1
- Reset account lockout counter after
  - 99999 minutes

Rationale: Although this lockout policy could be used for a denial of service attack, we believe the chances of a rouge administrator or any other party taking a third "guess" at a password on an account that locks out after the first attempt will be rare. Failed attempts are monitored by NetIQ Security Manager. Violations are immediately reported on and investigated.

[Computer Configuration\Windows Settings\Security Settings\Account Policies\…
…Kerberos Policy]

- Maximum tolerance for computer clock synchronization
  - 1 minute

Rationale: Specifies tolerance for time differences between client and server. Session timestamps within this range are treated as valid; defends against "replay attacks." The GPS based NTP server we have deployed is very efficient and allows us to run with a low value.

[Computer Configuration\Windows Settings\Security Settings\Local Policies\…
…Audit Policy]

- Audit * (All other than process tracking)
  - Success, Failure

Rationale: Performance hits related to heavy logging have proven to be negligible in this domain[*]. High levels of logging are preferred if/when issues arise. NetIQ Security Manager is used to consolidate logs and sort/filter as needed while troubleshooting.

[*] Setting "Audit process tracking" to Success, Failure can generate many events quickly.

[Computer Configuration\Windows Settings\Security Settings\Local Policies\…
…Security Options]

- Additional restrictions for anonymous
  - No access without explicit anonymous permissions
- Allow server operators to schedule tasks (DC's only)
  - Disabled
- LAN Manager Authentication Level
  - Send NTLMv2 response only\refuse LM
- Message text for users attempting to logon
  - warning of use violations and contact information
- Number of previous logons to cache
  - 0

Rationale: No down-level (earlier than Windows 2000) machines do/should communicate or authenticate with this domain.* Leaving profiles on the DC's may leave unwanted scripts and utilities that could be exploited.

[Computer Configuration\Windows Settings\Security Settings\Event Log\...
…Settings for Event Logs]

- Maximum log size (all)
  - 51200 kilobytes
- Retain log (all)
  - Not defined
- Retention method (all)
  - As needed

Rationale: Same as for Audit Policy.

[Computer Configuration\Windows Settings\Security Settings\...
…Restricted Groups]

- Cert Publishers, DNSUpdateProxy, Domain Admins, Domain Computers, Domain Controllers, Enterprise Admins, Schema Admins

Rationale: Given the domain composition, we could easily audit all groups. Our greatest concerns are protecting against non-owner DNS entries, rouge administrators, abuse of certificate issuance policy, and ability to change the Schema.

* Voicemail software is running on a Windows NT4 Server (VOICE1) however the server is stand-alone. The software's user authentication does not make use of Windows authentication.

[Computer Configuration\Windows Settings\Security Settings\...
…System Services]

- Non-essential services have been removed (at the machine) or disabled. Services that could be set to manual were changed accordingly. Windows Installer was handled here rather than under Administrative Templates.

Rationale: Running unnecessary services consumes resources and provides an avenue for exploits. Windows Installer options under Administrative Templates, with the exception of "Disable Windows Installer" applies to "Software Installation" packages in Group Policy. We do not install from Group Policy.

[Computer Configuration\Administrative Templates\Windows Components\…
…Internet Explorer]

- Make proxy setting per-machine (rather than per-user)
  - Enabled
- Disable Periodic Check for Internet Explorer updates
  - Enabled

Rationale: While it is assumed that any user that logs into machines in this domain can change this policy, Internet Explorer should only be used for reading local files on servers. These settings have been placed to serve as a reminder. Additional settings to make this happen are under the User Configuration portion of this policy.

[User Configuration\Windows Settings\Internet Explorer Maintenance\...
…Connection]

- Connection Settings have been made to Delete existing. Proxy has been set to a non-existent IP and non-standard port.

Rationale: Prevent Internet Explorer from reaching the Internet.

[User Configuration\Administrative Templates\Windows Components\...
…Internet Explorer\Internet Control Panel]

- Disable the *
  - Enabled

Rationale: Prevent Internet Explorer Settings from being easily changed.

[User Configuration\Administrative Templates\Control Panel\Display]

- Hide Screen Saver tab
  - Enabled
- Activate screen saver
  - Enabled
- Screen saver executable name
  - logon.scr
- Password protect the screen saver
  - Enabled
- Screen Saver timeout
  - 10 minutes

Rationale: Locks screen to prevent others from viewing and/or using session if machine is inadvertently left unattended and unlocked.

Child Domain Group Policy

Only deviations from the Root Domain Group Policy are addressed.

Default Domain Group Policy

Applied to: ops.giac.corp
Template: baseline.inf
Notes: To increase performance, the Computer and User portion of this policy have been split into two separate policies, with the unused portion of each policy being disabled. Neither "No Override" or "Block Policy inheritance" is required.

[Computer Configuration\Windows Settings\Security Settings\Account Policies\… …Password Policy]

- Enforce passwords remembered
  - 10
- Maximum password age
  - 45 days
- Minimum password age
  - 10 days
- Minimum password length
  - 10 characters

Rationale: Set to comply with written company password policy; policy reflects the maximum tolerance management believes the user community can handle.

[Computer Configuration\Windows Settings\Security Settings\Account Policies\… …Account Lockout Policy]

- Account lockout duration
  - 4 hours
- Account lockout threshold
  - 3
- Reset account lockout counter after
  - 30 minutes

Rationale: Set to comply with written password policy. Failed attempts are monitored by NetIQ Security Manager. All are recorded with failed administrator attempts are sent to engineers, failed user attempts are sent to the Help Desk mailbox.

[Computer Configuration\Windows Settings\Security Settings\Account Policies\… …Kerberos Policy]

- Maximum tolerance for computer clock synchronization
  - 3 minutes

Rationale: When client machines are powered off over the weekend we occasionally see time differences in excess of 2 minutes. This policy has been adjusted accordingly.

[Computer Configuration\Windows Settings\Security Settings\Local Policies\… …Audit Policy]

- Audit account logon events
  - Success, Failure
- Audit account management
  - Success, Failure
- Audit Directory service access
  - Failure
- Audit logon events
  - Success, Failure
- Audit object access
  - Success, Failure
- Audit policy change
  - Success, Failure
- Audit privilege use
  - Failure
- Audit process tracking
  - No auditing
- Audit system events
  - Success, Failure

Rational: Recommended values from baseline.inf. Adjustments are made if situations warrant changes (ie. when troubleshooting).

[Computer Configuration\Windows Settings\Security Settings\...
…Restricted Groups]

- Cert Publishers, DNSUpdateProxy, Domain Admins, Domain Controllers, Desktop Admins, Server Admins

Rationale: Same as root domain. Groups that reside only in root domain have been removed. Computers in this domain change to often to warrant auditing Domain Computers.

[Computer Configuration\Windows Settings\Security Settings\...
…System Services]

- These settings have been applied at the OU level.

Rationale: Changing services at this level (domain) has proved to be counterproductive.

[Computer Configuration\Windows Settings\Public Key Policies\...
…Encrypted Data Recovery Agents]

- Defined as a single, non-administrative account

Rationale: Limits exposure of who can recover encrypted files. Account is not used for any other purpose.

[Computer Configuration\Windows Settings\Public Key Policies\...
...Automatic Cert Req. Settings]

- Request created for computers allowing participation in IPSec

Rationale: Does not require user intervention for IPSec.

[Computer Configuration\Windows Settings\...
…IP Security Policies on Active Directory]

- Policies have been created and assigned from with this and other Group Policies.

Rationale: Ensures that: only approved ports are used, sensitive servers can only communicate with appropriate clients (such as HR1, DEV1, etc). Only 3DES and SHA1 are allowed when IPSec is required for communication.

[Computer Configuration\Administrative Templates\System\Logon]

- Delete cached copies of roaming profiles
  - Enabled

Rationale: Prevents snooping of profiles by users with elevated privileges.

[User Configuration\Windows Settings\Internet Explorer Maintenance\... …Connection]

- Connection Settings have not been changed at this level.

Rationale: The same restrictions set in the root domain have been applied to the Backend and Domain Controllers OU's. The Departments OU has different settings.

[User Configuration\Administrative Templates\Control Panel\Display]

- Screen Saver timeout
  - 20 minutes

Rationale: Provides a reasonable amount of time of computer inactivity (phone calls, document review, etc.) before locking the screen.

Organizational Unit Group Policy

Applied to: OU's of ops.giac.corp
Template: basicdc.inf, basicwk.inf, hisecws.inf, Exchange BackEnd Incremental, File and Print Incremental, IIS Incremental, Infrastructure Incremental
Notes: The remaining Group Policies that apply to Computer Configuration are incremental. The appropriate templates were modified for service needs, IPSecurity, and strengthening permissions on key executables/registry values based on the role of the systems inside the OU. Other significant changes for the System Configuration portion relating to sub-OU's of Departments and several User Configuration settings will still be discussed.

End User Systems Group Policy
[Computer Configuration\Administrative Templates\Windows Components\... …Internet Explorer]

- Security Zones: Do not allow user to *
  - Enabled
- Disable Automatic Install of Internet Explorer components
  - Enabled

Rationale: Prevents changes to company approved settings.

[Computer Configuration\Administrative Templates\Network\Offline Files][*]

- Enabled
  - Disabled

Rationale: Prevents desktop machines from using offline files to lessen administrative troubleshooting.

[*] The "Notebooks" group has been denied Read access to this policy.

[Computer Configuration\Administrative Templates\Network\Offline Files][*]

- Enabled
  - Not Configured
- Synchronize all offline files before logging off
  - Enabled
- Administratively assigned offline files
  - Set as needed

Rationale: Allows Notebook users (and administrators) to set offline files and ensures they are synchronized.

End Users Group Policy
[User Configuration\Windows Settings\Internet Explorer maintenance\...
…Connection\Automatic Browser Configuration]

- Settings are to automatically detect and configure browser settings every 120 minutes. The configuration URL and proxy have been provided.

Rationale: Allows internal systems to be configured appropriately yet enables Notebook computers to be reconfigured when away from the office.

[*User Configuration\Windows Settings\Internet Explorer maintenance\Security\...*
…Security Zones and Content Ratings]

- Set according to company policies.

Rationale: Ensures that zones are set according to company standards.

Additional Group Policy settings
Many options under the User Configuration of Group Policy for End Users and Tech Users have been set. Areas configured include:

- Other IE settings such as available menus, approved controls, cookie behavior, and favorites.
- Logon scripts for drive mappings and one time administrative tasks
  - Drive mappings vary by need so group permissions were used to control who could read each policy.
- Start menu items; again controlled by group permissions.
- Limits on control panel items.
- Printer locations and installation permissions.
- Folder Redirection
- Trusted Enterprise Certificate Trust List (CTL) for non-member servers is created using GIAC's internal root CA.

[*] The "Desktops" group has been denied Read access to this policy.

Concerns Not Addressed by Group Policy

With the seemingly limitless options available from within Group Policy, some areas are not available for configuration, others are easier addressed at the machine level. Some items that are regularly addressed on server and user objects, and have not previously been mentioned, are listed, followed by topics that require more clarification.

Servers

- Services that have logging ability that is not "on" by default are configured appropriately.
- When possible, log files are moved from their default location.
- IIS installations get stripped of the default site contents and URLScan* is applied.
- NTFS auditing is performed on \NTDS, \SYSVOL, service logs, and confidential directories.
- Vulnerability assessment is performed bi-weekly using NetIQ Security Analyzer. NetIQ Security Manager monitors key servers.
- NetBIOS is disabled on all interfaces that do not require its use.
- DC's have the NoLMHash key created to remove the LM hash as per Microsoft Knowledge Base Article 299656.
- TrendMicro Server Protect is used on all servers (OfficeScan runs on all clients) and configured to provide the maximum protection possible without degrading the system.
- SYSKEY.EXE is run on all Servers. Passwords are stored on floppy disks. One copy remains in the drive (ejected) the other in our vault.

Users

- Only service accounts that require impersonation are marked for delegation.
- "Account is sensitive and cannot be delegated" is checked if it can be done without loosing functionality.
- Terminal services and dial-up permissions are granted on a case by case basis.
- The profile path for any account that should not be allowed to logon locally is manually created and auditing enable. The account is then denied Read (NTFS) access to the path. The profile path is then listed in the account thus eliminating the possibility of it being used for a local logon.
- Logon hours are specified when feasible.
- "Log On To" is specified for accounts that are created under the Contractors OU. This feature does require NetBIOS.

* See Microsoft Knowledge Base Article "HOW TO: Configure the URLScan Tool" in the Reference section.

Training

Employees attend mandatory on-site, hands-on, computer instruction. Sessions include operating system basics, accessing and using network resources, applications tutorials (Office, etc.), application safety, Internet use and safety, and personal privacy protection. The material is presented by our Corporate Trainer, Executive Officers, and Technical staff. We try to keep the classes in 3 month rotations. GIAC provides funding for, encourages, and in the case of the Technical staff requires, employees to enroll in professional instructor led courses for in-depth training in these areas.

Software Maintenance

Patches on all Microsoft operating systems and Microsoft Office applications are kept up to date using St. Bernard's Update Expert. It is an internal policy that all patches be evaluated for relevance and if appropriate, verified in the lab prior to a company wide rollout. The patch process should not exceed 30 days from the date of first availability.

Local Computer Policies

The Remote Assistance feature included with Windows XP is very helpful in assisting users, particularly those that are not in the same building as our Technical staff. In order to allow an administrator to initiate the connection, as opposed to the user sending a request, you must modify the Group Policy on the local machine. It has been specified that only the Desktop Admins group can connect[*]. Desktop Admins and Desktop Admin Temps have been added to the local Administrators group on all systems in the End User Systems OU. The Server Admins group has been added to the local Administrators group on all servers for which this group has delegations assigned under an OU. These changes have been made on the base RIS images for servers and desktops, and on the base Symantec Ghost images for notebook machines.

We have eleven Windows 2000 Server, and twenty Windows XP installations, not including LAB_NET, that are not part of our AD environment. Policies were configured locally on each machine (or image) using the same principals applied to our AD policies.

Mobile Computers

Users often travel with their Notebooks which presents a potential problem in that we do not cache logons so access to a DC or a local account is required. Our firewall solution, with accompanying client software, provides the ability to establish a tunnel prior to commencing the logon process. Users that have access to an Internet connection are asked to use this method over the local account.

[*] See Microsoft Knowledge Base Article "HOW TO: Configure a Computer to Receive Remote Assistance Offers in Windows XP" in the Reference section.

Certificate Authority

Microsoft's implementation of Certificate Server provides a fairly inexpensive method for providing a Public Key Infrastructure (PKI). Authenticating Mobile Users, Secure Socket Layer (SSL) encrypted web site, Internet Protocol Security (IPSec), and code signing are some areas in which having a low cost PKI can be beneficial. While we do not intend to fully leverage all the uses of PKI at this time, Mobile Users, SSL certificates, and Encrypted Files Systems (EFS) were motivation enough for us to take on the endeavor. In order to avoid a total breakdown of the Certificate Trust List (CTL) in the event that a subordinate CA is compromised, CERT1 was installed as an Off-Network Root Authority. Two subordinate CA's were also installed with BOOT1 and CERT2 hosting these services. The root CA's Certificate Revocation List (CRL) is published (sneaker net) to BOOT1. We installed the CA's in our environment (Off-Network, multiple domains) by following the instructions found in Microsoft Knowledge Base Article 271386 "HOW TO: Install a Windows 2000 Certificate Services Offline Root Certificate Authority," and Microsoft Knowledge Base Article 281271 "Windows 2000 Certification Authority Configuration to Publish Certificates in Active Directory of Trusted Domain." It is important to note that if you wish to utilize Microsoft's Enhanced Cryptographic Service Provider (CSP) as we did, you must have at least the Microsoft High Encryption Pack and Windows 2000 Service Pack 1 installed (SP2 or higher will contain these packages).

DNS, DHCP, IP

The "QueryIpMatching" registry value that is used to check that the DNS server queried matches the one that replied, and "Secure cache against pollution" option used to discard additional records returned from domains that were not queried, are used on all DNS servers. Because Network Address Translation (NAT) is used for all servers accessible from the Internet, and we use several internal domains (Training, network equipment, etc.) we do have traditional DNS zones on our DNS (DC) servers. Zone transfers are required for proper operation thus they are only permitted to servers that are specified in the Name Servers tab. Transfers are only performed internally. The DHCP server configured so it will not update DNS for clients (only available if DNS zone is Active Directory-integrated) that are not capable of performing that function as we do not wish to support down-level clients. ACL's on DNS records for core systems and services are manually tightened. Scans for rouge IP's, services, and ports are run continually. We do have other network monitoring tools (SolarWinds, CiscoWorks 2000 LMS) but limit their use as their primary functions require SNMP, which we use sparingly. Border routers are ACL'd appropriately to keep internal address inside and protect against spoofing

Wireless Networking

Our Training Room has twenty dedicated notebook computers. Occasionally employees request authorization to use their assigned production notebook in this room. To limit the amount of cable strung across the floor, we swapped out Ethernet for wireless. As training often requires access to servers on our network and Internet access, security of the wireless network required special considerations. We elected to go with Cisco's Aironet line, which when coupled with their Cisco Secure ACS provides a fairly stringent authentication and encryption mechanism. Placing the ACS server, with its own user database, on the training network allows us to control access from the ACS and firewall.

References

Web Resources
1. "The SANS Security Policy Project."
The SANS Institute.
URL: http://www.sans.org/resources/policies/

2. "Administrative Simplification."
United States Department of Health and Human Services.
URL: http://aspe.hhs.gov/admnsimp/

3. Microsoft Corporation. "Best Practices for Designing the Active Directory Structure." Microsoft TechNet. URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/ad/windows2000/default.asp

4. Microsoft Press. "Windows 2000 Server Deployment Planning Guide."
Microsoft TechNet. URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/deploy/home.asp

5. Microsoft Corporation. "Windows 2000 Server Distributed Systems Guide"
Microsoft TechNet. URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/distsys/dsintro.asp

6. Microsoft Corporation. "Security Operations Guide for Windows 2000 Server"
Microsoft TechNet. URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/default.asp

7. Microsoft Corporation. "Security Guide Scripts Download."
Microsoft Corporation. URL:
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9989D151-5C55-4BD3-A9D2-B95A15C73E92

8. Microsoft Corporation. "Security Operations Guide for Exchange 2000 Server."
Microsoft TechNet. URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/mailexch/opsguide/default.asp

9. Microsoft Corporation. "New Registry Key to Remove LM Hashes from Active Directory and Security Account Manager."
Microsoft Product Support Services. URL:
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B299656

10. Microsoft Corporation. "HOW TO: Install a Windows 2000 Certificate Services Offline Root Certificate Authority."
Microsoft Product Support Services. URL:
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B271386

11. Microsoft Corporation. "Windows 2000 Certification Authority Configuration to Publish Certificates in Active Directory of Trusted Domain."
Microsoft Product Support Services. URL:
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B281271

12. Microsoft Corporation. "Using Security Templates."
Microsoft TechNet. URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prdd_sec_lqvj.asp

13. Microsoft Corporation. "Appendix F - Windows 2000 Security Configuration Templates for the Evaluated Configuration."
Microsoft TechNet. URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/W2kCCSCG/W2kSCGcf.asp

14. Microsoft Corporation. "Baseline Security Analyzer."
Microsoft TechNet. URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/mbsawp.asp

15. Microsoft Corporation. "How to Configure an Authoritative Time Server in Windows 2000."
Microsoft Product Support Services. URL:
http://support.microsoft.com/default.aspx?scid=kb;EN-US;216734

16. Microsoft Corporation. "HOW TO: Configure the URLScan Tool."
Microsoft Product Support Services. URL:
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B326444

17. Microsoft Corporation. "HOW TO: Configure a Computer to receive Remote Assistance Offers in Windows XP. URL:
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B301527

Printed and/or resources requiring purchase
1. King, Robert R. "Mastering Active Directory, Second Edition." Alameda: Sybex. 2000.

2. Manasi, Mark. "Mastering Windows 2000 Server, Second Edition." Alameda: Sybex. 2000.

3. Hipson, Peter D. "Mastering Windows 2000 Registry." Alameda: Sybex. 2000.

20. Redmond, Tony. "Microsoft Exchange Server for Windows 2000, Planning, Design, and Implementation." Woburn: Butterworth-Heinemann. 2001.

4. Fossen, Jason. "Active Directory, DNS and Group Policy." www.sans.org. 2001.

5. Fossen, Jason. "Windows 2000/XP PKI, Smart Cards and Encrypting File System." www.sans.org. 2001.

6. Fossen, Jason. "Windows 2000/XP IPSec, RRAS and Virtual Private Networking." www.sans.org. 2001.

7. Fossen, Jason. "Securing Internet Information Server." www.sans.org. 2001.

8. Boswell, Bill. Fossen, Jason. "Windows 2000/XP Scripting For Security and Auditing." www.sans.org. 2001.

9. Eck, Thomas. "Windows NT/2000 ADSI Scripting for System Administration." Indianapolis: MTP. 2000.

Companies and organizations that were mentioned by name or are related to a product identified:
1. Microsoft Corporation. URL: http://www.microsoft.com/
2. The SANS Institute. URL: http://www.sans.org/
3. Intel Corporation. URL: http://www.intel.com/
4. Dell Computer Corporation. URL: http://www.dell.com/
5. Cisco Systems. URL: http://www.cisco.com/
5. Nokia. URL: http://www.nokia.com/
6. Symmetricom. URL: http://www.symmetricom.com/
7. Adtran. URL: http://www.adtran.com/
8. NetIQ Corporation. URL: http://www.netiq.com/
9. St. Bernard Software. URL: http://www.stbernard.com/
10. Symantec Corporation. URL: http://www.symantec.com/
11. Solarwinds.net. URL: http://www.solarwinds.net/

Last Updated: May 25th, 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**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**