Global Information Assurance Certification Paper

GCNT Securing Windows - Practical Assignment
Version 3.0, Option 1

Submitted by: Chester Li

Title: Design a Secure Windows 2000 Infrastructure

I. FORWARD

This practical is written from the perspective of recommending and designing a guideline by an IT security consulting firm. ISI (Independent Security Inc) is recommending a design guideline for securing GIAC Enterprises' internal Windows 2000 and Active Directory infrastructure.

In this guideline, ISI first briefly introduces GIAC Enterprises' business background and its current network infrastructure. Then it outlines the reasons why GIAC is upgrading its internal network by listing some of the primary objectives a Windows 2000 infrastructure will provide that its current network Windows NT 4.0 could not otherwise provide. Further, ISI's proposed guideline will include three major areas of security and configuration recommendations: network design, Active Directory design, and finally, Group Policy and security.

Note: This practical does not include arguments to convince GIAC to migrate to Windows 2000. The migration plan has already been established by members of GIAC's management and systems administrator.

II. INTRODUCTION/SCENARIO

GIAC Enterprises is an e-business with online sales of fortune cookies sayings. GIAC Enterprises' office resides in one single office building located in downtown Savannah, GA. With only 10 employees, it is a small family startup business that was founded in 1995. GIAC's network has grown since it started its business from a single-server, multi-client without connections to the Internet and no presence on the web model. It has gradually evolved into today's multi-server, multi-client with direct T-1 connection to Internet, and a 24/7 e-business operation with web presence. Today, GIAC employs approximately 50 employees with most of its workforce involved with Research and Development's design labs.

GIAC Enterprise's Business Structure

Today's GIAC Enterprise's business structure is comprised of 4 major divisions:

- Research and Development
- Sales and Marketing
- Finance and Human Resources
- Information Technology

GIAC Enterprises Network Infrastructure

Today, with an already established web presence, GIAC Enterprises' network infrastructure is comprised of the following items:

- A CISCO 2600 series modular access router
- Two Pentium IV class, Windows NT 4.0 domain controllers – a primary and a secondary domain controller
- A Pentium IV class, Windows NT 4.0 public web server

- A Pentium IV class, Windows NT 4.0 mail server
- A Pentium IV class, Windows NT 4.0 file, print, application, database server
- A mix of Pentium III and IV class, Windows 9x[1] clients (workstation or laptop) and various network appliances (e.g.: printers, scanners, etc.) attached to the LAN.
- Internal network are fully switched, full duplex, 100 Mbps Ethernet network.

Each server is configured with raid-5 and redundant fan and power supplies to provide maximum fault tolerance. It has already been predetermined that the company has the following:

- No legacy enterprise hardware and software.
- All Pentium IV class servers both exceed and meet the hardware, memory, and disk space requirements.
- All Pentium III and IV class clients both exceed and meet the hardware, memory, and disk space requirements.
- Will be running in native mode in Windows 2000.

Windows 2000 Security Design Goal

As one of its 2002 fiscal year goals, GIAC Enterprises wants to migrate its internal Microsoft network infrastructure to Windows 2000 based on a memorandum written by GIAC's systems administrator the previous fiscal year. The systems administrator established the need for the internal infrastructure upgrade and also decided to contract ISI, a regional independent IT security consulting company, to provide a guideline to implement and secure GIAC's Active Directory and internal Windows 2000 network infrastructure.

After a 2 week time period of interviews, tests, inspections, and meetings of GIAC's different departments, ISI makes its recommendation. ISI agrees with GIAC's systems administrator's decision to pursue the internal infrastructure upgrade. Not only will Windows 2000 professional client workstations solve GIAC's biggest administrative headache - preventing users from installing unauthorized software, it also offers the security of Microsoft's NT file system (NTFS) v.5 and encryption file system (EFS). The real key benefits[2], of implementing Windows 2000 Directory Service in GIAC's internal LAN servers is twofold. First it offers the ability to administer group policy in a central location with ease, and secondly, it offers the ability to delegate administration authority.

ISI provided guidelines for three key issues.

- Network Design
- Active Directory Design
- Group Policy and security Design

III. NETWORK DESIGN

[1] Windows 98, 98 Second Edition, and Windows 95.

[2] Other features that can be available to GIAC Enterprises by implementing Windows 2000 Directory Services will not be included in this discussion because it is out of the scope of this assignment.

Data Center Location

All network servers are centrally located in one area of GIAC's building, the Data Center. Only GIAC IT staff has physical access to this area. Both internal network and DMZ network can be managed within the Data Center.

Infrastructure Setup

The current GIAC Enterprises Windows NT network infrastructure is simple but an efficient and capable design. GIAC deployed a small business, high performance CISCO 2600 series modular access router less than one year ago. This access router, model 2610 to be specific, was procured with optional 2 Ethernet port with component upgrades of: a) WIC-1DSU-T1[3] for WAN connection, and b) CISCO IOS feature set[4]. With the added component upgrades, the GIAC network infrastructure offered comprehensive protocols and services, including virtual private networking (VPN), firewall, encryption, and WAN optimization.

With VPN/Extranet access, GIAC's network can provide added security and reduce costs for remote access. The firewall, adds internal network security against intrusion especially when connecting to the Internet. The infrastructure also provides high performance application with L2TP encryption and data compression. Finally, with the added WIC, GIAC's network took advantage of CISCO's 2600 modular access router's capability for LAN segmentation. This would allow GIAC to separate a secure internal LAN from a perimeter LAN (Saunders, "Multi Service Access Solutions – CISCO 3600 Series and CISCO 2600 Series" pg. 12).

Because the CISCO 2600 modular access router technology is still relatively new and versatile, its life expectancy can last at least another two years, perhaps more. And the 2600 has ample capacity for future component upgrades. ISI does not recommend any changes to infrastructure backbone, therefore, the Windows 2000 Active Directory will be designed around this infrastructure.

Proposed Infrastructure Design and Upgrade Components

ISI recommends GIAC to fully utilize its CISCO 2610's router/firewall capabilities to segment the network infrastructure into three segments - internal network, DMZ network, and Extranet. See Figure 1 for proposed LAN segmentations. The router must be setup only to allow web and inbound email traffic through to the DMZ web server and mail relay server.

By setting router rules to direct web traffic to the DMZ web server, GIAC will reduce the risk and exposure to Microsoft IIS based or similar web based attacks, which might jeopardize the internal network.

[3] One port T1/fractional T1 with CSU/DSU
[4] Internet Operating System with IP/FW plus IPSec 3DES

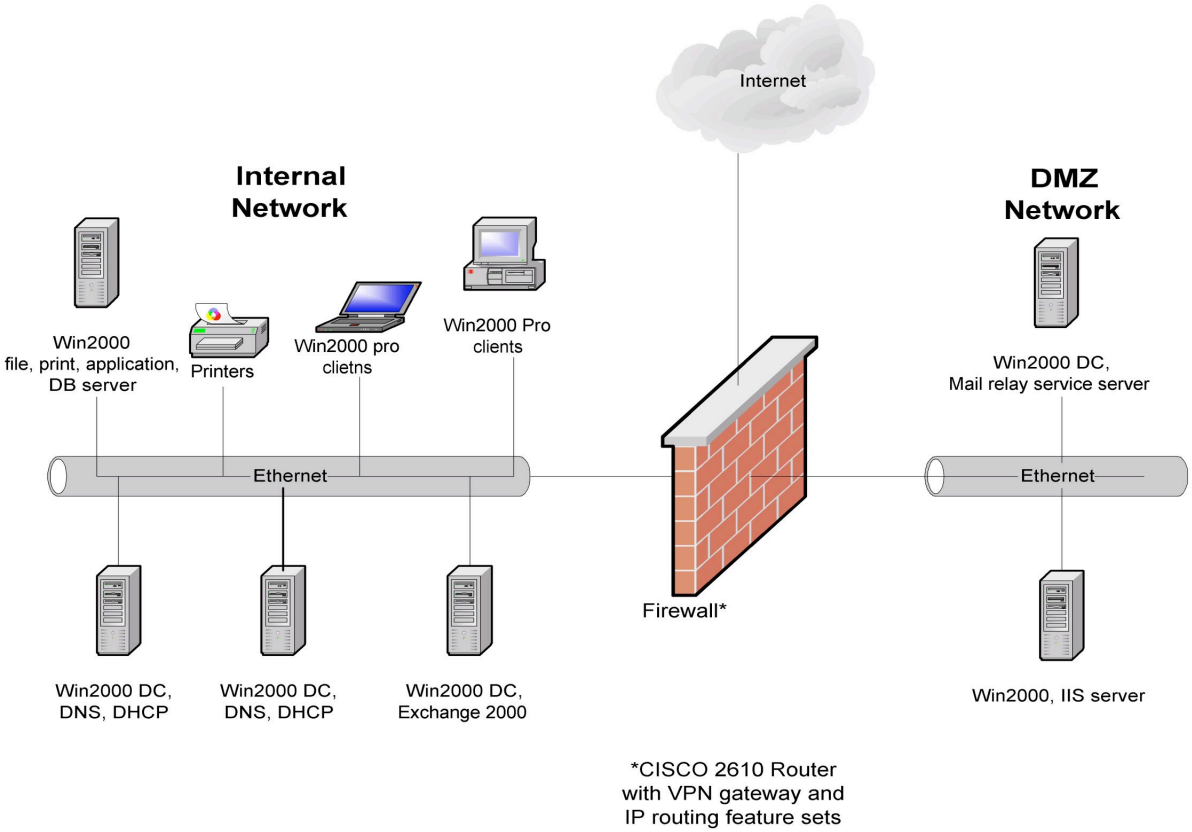

Figure 1: GIAC Enterprises network diagram.

By adding a mail relay server in the DMZ and setting router rules to direct all inbound email traffic to it, GIAC's network can significantly decrease its chance of getting email born worm/Trojan viruses by implementing a third party virus scanner[5]. With this configuration, "processed" email can then be routed to internal Exchange server and GIAC's employees can confidently open all their emails. Presently, GIAC's DMZ network does not run a DMZ area mail relay server, making it susceptible to email born virus attacks. It is for this reason that ISI recommends an external mail relay server in the DMZ for added security. See Table 1 for itemized present and proposed machine roles and their configurations.

Finally, the firewall must be configured with a rule to have a one way trust from the internal network to the DMZ. Ports 135 through 137 should be open for web access. Open all the MAPI ports for mail access and also open a conduit from the DMZ mail relay server to the internal Exchange server (port 25 only).

[5] Any virus detection program is only as good as its virus definition date. Therefore, it is up to the systems administrator to ensure the virus definition is up-to-date.

Machine Roles:	Present Configuration	Infrastructure Location	Proposed Upgrade Configuration
Router	CISCO IOS feature set	Firewall	No change
Server 1	WinNT 4.0 server, PDC, DNS	Internal	Win2000 DC, DNS, DHCP
Server 2	WinNT 4.0 Server, BDC, WI NS, DHCP	Internal	Win2000 DC, DNS, DHCP
Server 3	WinNT 4.0 Server, Exchange 5.5	Internal	Win2000 Server, Exchange 2000
Server 4	WinNT 4.0 Server, file, print, app, db	Internal	Win2000 Server, file, print, app, db
Server 5	WinNT 4.0 Server, IIS 4.0	DMZ	Win2000 server, IIS 5.0
Server 6	n/a	DMZ	Win2000 DC, Mail relay service
Clients (PCs and laptops)	Win9x	Internal	Win2000 Professional

Table 1: Present and proposed machines roles and configuration.

Apply The Latest Service Packs And Keep Informed of Updates

In addition to these modifications, all servers and clients (workstations and laptops) should have Windows 2000 service pack 2 and the latest hotfixes applied. ISI also recommends that all domain controllers and IIS go through Microsoft's Windows 2000 server and IIS baseline security checklist. Here are some of the more important steps listed in both baseline checklists:

- Disable unnecessary services
- Disable or delete unnecessary accounts
- Protect the registry from anonymous access
- Apply appropriate registry access control lists (ACLS)

To identify all the latest security vulnerabilities and holes in Windows 2000, GIAC's systems administrator must continually keep up-to-date with the latest critical security releases. GIAC's systems administrator should frequently visit security bulletin websites for information's pertaining to latest security issues. Some of the recommended security bulletin services are:

- Microsoft - <http://www.microsoft.com/security/>
- SANS Institute - <http://www.sans.org>

Finally, other than Windows 2000 and IIS baseline security checklists, Microsoft provides a wealth of security information[6] that will harden all GIAC's systems:

- Guides, Updates, and Tools
- Windows 2000 Professional Baseline Security Checklist
- Microsoft Personal Security Advisor
- HFNetChk

IV. ACTIVE DIRECTORY (AD) DESIGN AND DIAGRAM

[6] See a complete listing of Microsoft's Windows 2000 security tools, go to <http://www.microsoft.com/technet/treeview/default:asp?url=/technet/security/tools/tools.asp>

Designing Active Directory

By conducting an organizational analysis of GIAC's management team and IT department, ISI was able to determine the company's business and information technology needs and characterized GIAC's IT organization as a centralized IT organization. A centralized IT organization reports to a single individual and is usually the group responsible for all network and information services, although some day-to-day tasks may be delegated to certain groups or departments. (Microsoft Corporation, "Designing a Microsoft Windows 2000 Directory Services Infrastructure", Module 3, pg. 4.) There were definitely signs of interests within the management and IT teams to be able to enforce and delegate administrative authorities to other department within GIAC Enterprises. They wanted to implement delegated administrative authorities to both the Finance and Human Resources division and Research and Development division.

Because of these interests, ISI will recommend to design GIAC's Active Directory hierarchy based upon the departmental or organizational structure as shown in Figures 2 and 3. We will implement an organizational unit (OU) container called GIACgroup on the root of GIACEnt.giac.com to create a bases and starting point for GIAC's departmental OUs. See Figure 2. The purpose of this OU container is purely to separate the actual default domain policies that are security related and other user/computer related settings. In other words, GIAC will implement all default domain policies at the GIACEnt.giac.com root OU level. All remaining settings such as login scripts or desktop environment properties that are not necessary security related but must be inherited by all child OUs should be implemented at the GIACgroup.GIACEnt.giac.com OU container.

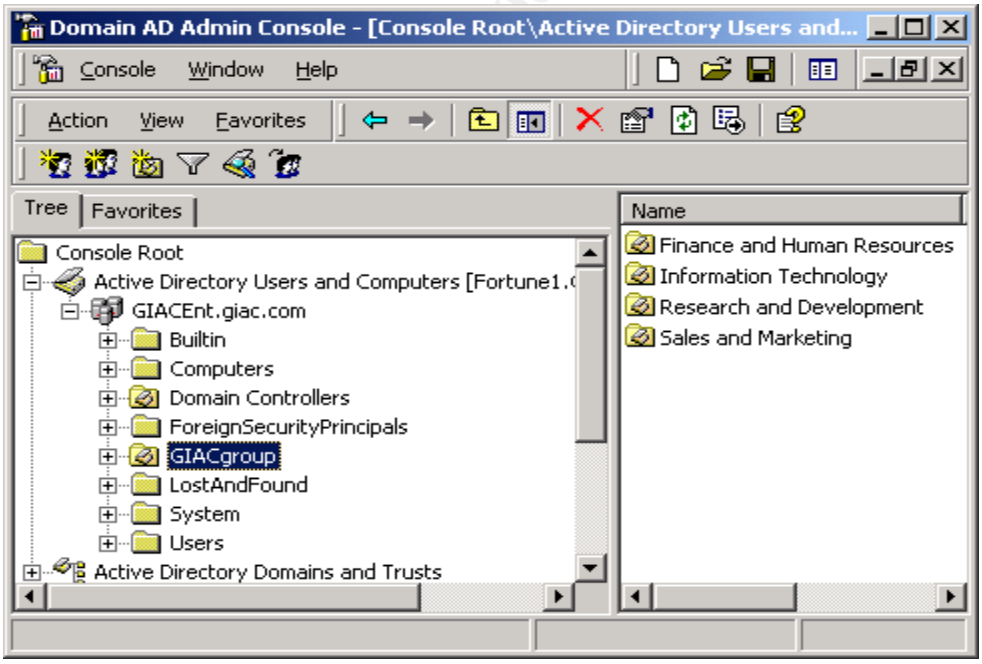

Figure 2: Creating a Top GIAC Hierarchical OU.

The advantages of designing OU hierarchy according to departmental or organizational structures are the following:

- More accurately reflects the business model
- Maintains current division/departmental autonomy
- Can accommodate mergers and expansions

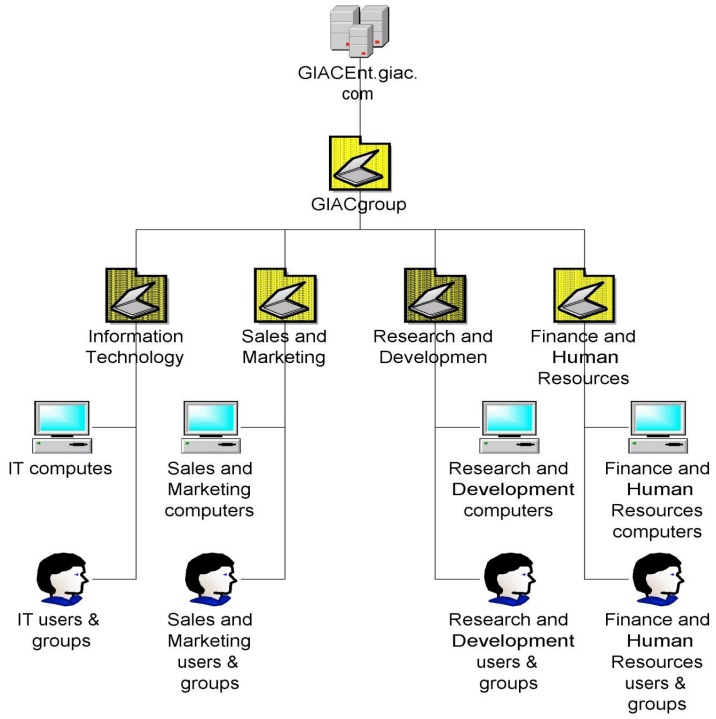

Figure 3: GIAC Enterprises Active Directory Diagram

On the other hand, the disadvantages of this design hierarchy are the following:

- Vulnerable to reorganizations
- May affect replication (Von Weltin, "Guide to Active Directory Design")

The disadvantage factors listed above are not part of the Active Directory hierarchical design considerations because GIAC Enterprises is in excellent financial standing. It does not have plans to acquire another organization and it does not have plans to expand considerably within the next five to seven years. Furthermore, GIAC's internal network design is a single forest, single domain Active Directory structure and since GIAC's Information Technology division would grow or expand in size proportionally in relation to the rest of the company, the effects of replication between sites or domain is ruled out.

Delegate Administrative Authority

With a departmental hierarchical Active Directory design, GIAC's systems administrator can now setup a "trusted" administrative delegate to manage Finance and Human Resource's OU's.

See Figure 4. With all the right authorization and setup, this individual can manage basically everything within this OU container. For example, the areas of interest are the following:

- Maintain User and Computer accounts
- Audit security logs
- Audit access resource logs
- Maintain security group membership

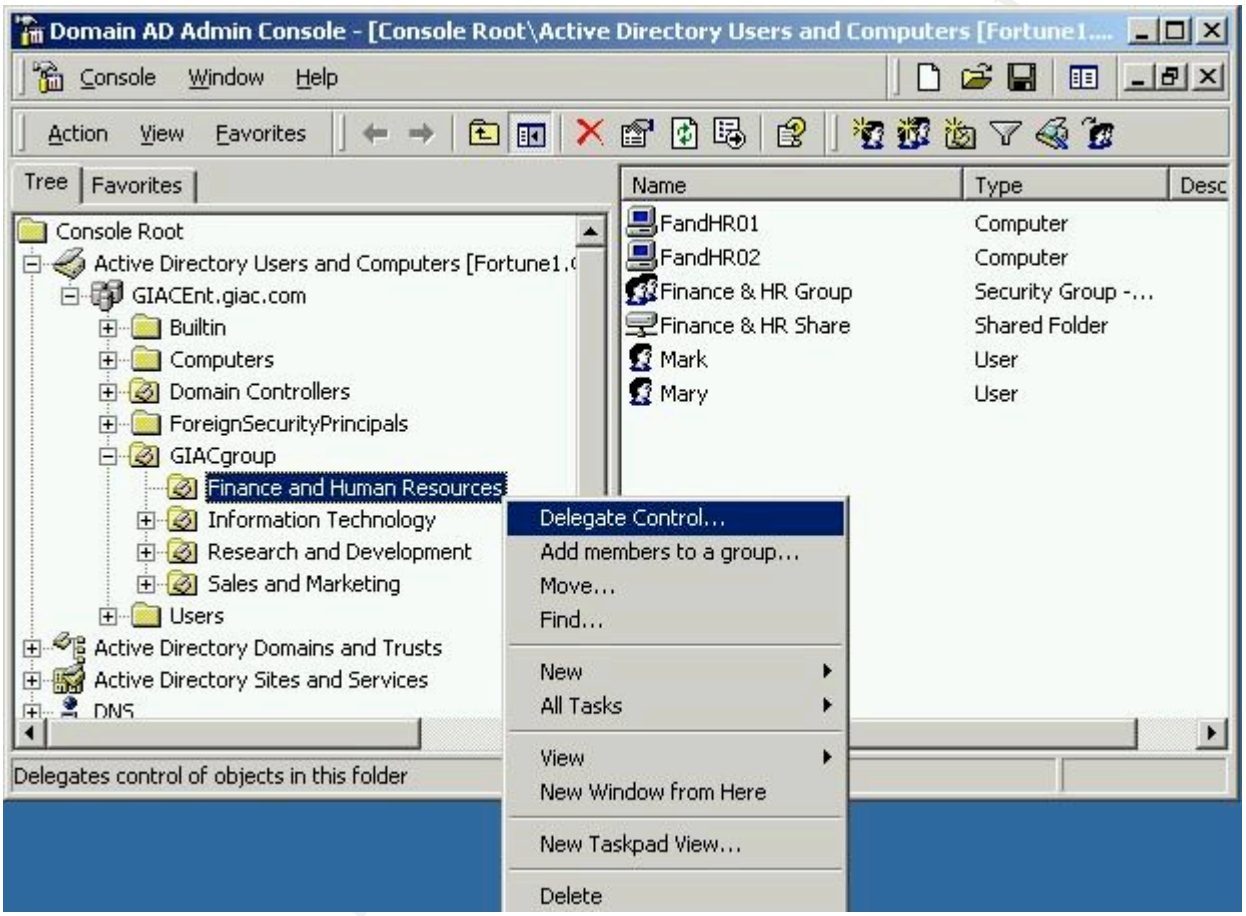

Figure 4: Delegating Administrative Authority for Finance and Human Resources OU.

For added control, instead of setting up administrative authority via Micrsoft's delegation control wizard, it is recommended that GIAC configure the user rights through the advanced option in Security tab of the OU in question. Through this method of administrative control, GIAC's systems administrator can provide specific controls over to the trusted agent.

ISI recommends implementing an E-mail alert service (through third-party software) to notify the trusted staff of any changes or modification to the OU structure and resource share security. This level of security can provide both the management and IT teams with the comfort and confidence of knowing that security will not be unknowingly breached.

As for Research and Development division, its needs in some way mirror the needs of the Finance and Human Resources division. Because of our hierarchical design, the systems administrator can replicate the same settings for Research and Development division as he did for Finance and Human Resources division and he can designate a trusted agent in this OU as well.

V. GROUP POLICY AND SECURITY

Using Active Directory to Manage Group Policy and Security:

By incorporating the Windows 2000 Active Directory into the company's internal infrastructure, GIAC can utilize its best feature/tool, the induction of Group Policy Editor through one of the Microsoft Management Console (MMC) snap-ins. The Group Policy Editor is a tool that extends the functionality of the System Policy Editor, which was first employed by Microsoft's Windows NT 4.0 operating systems. With the Group Policy Editor, the Windows 2000 systems administrator now can use the same technology he is accustomed to for configuring and managing user and computer settings from groups of computers and users. (McLean, "Windows 2000 Security Little Black Book," pg. 78)

The benefits of managing Group Policies through Active Directory are the following:

- Free of charge
- Already integrated with Active Directory services
- Allows for centralized management
- Is a simple integrated tool – MMC with snap-in
- Allows administration delegate control of OUs and Group Policy Objects (GPOs)
- Offers a wide range of implementation scenarios for an infrastructure of any size

Managing Group Policy Objects:

Group Policy settings are defined in a GPO that is applied to an Active Directory container. More than one GPO may be applied to the same container. An Active Directory container can be of a site, a domain, or of an OU. Figure 5 shows an example of how Group Policy may be applied to a container. Note – we will not be concerned with the site object in this scenario because GIAC's site perimeter equals to the domain Active Directory architecture perimeter.

Group Policies are processed in the order of local computer, site, domain, and then lastly the OU. The last Group Policy setting that gets processed (if the value is specified), supersedes any previous Group Policy if the values conflict, otherwise it inherits those settings. For example, if a local computer GPO specifies a setting to 'Enable', domain GPO specifies the same setting to 'Disable', and OU (to which the computer object resides in) specifies it to 'Enable', then the effective policy setting is 'Enable'. Or if local computer GPO specifies a setting to 'Enable', domain GPO specifies the same setting to 'Disable', and OU GPO does not specify a setting or 'Not Configured', then the effective policy setting is 'Disable'.

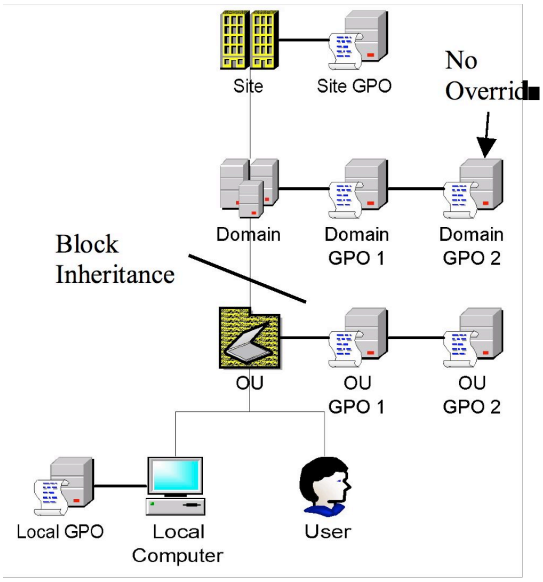

Figure 5: Example GPO applied to a site, domain, OU, and local computer. Note: When inheritance is blocked, GPO does not apply to child OU. Domain GPO 2 applies even through Block Inheritance setting.

GPO's within each container have processing order. GPO's are processed from the bottom up within an object. The latter GPO that is processed with a specified value assigned, supersedes its predecessor GPO if the values conflicts. Otherwise, it inherits the assigned registry value. As shown in Figure 5, both the Domain and OU objects contain more than one GPO. For example, let us say the GPO's in the Domain container are defined in the top to bottom order of the following: Domain GPO 1 is the top GPO and Domain GPO 2 is placed on the bottom of the processing order. If Domain GPO 2 specifies a setting to 'Enable' and Domain GPO 1 specifies it to 'Disable', then the effective policy setting is 'Disable'. If Domain GPO 2 specifies a setting to 'Disable', and Domain GPO 1 does not specify a setting or 'Not Configured', then the effective policy setting set by this Domain object is effectively 'Disable'.

Additional Controls in Group Policy Objects:

In addition to knowing the order of GPO precedence, there are also several GPO management methods that are important to Group Policy management. These management methods are:

- Filtering
- Block Inheritance & No Override
- Loopback Mode

Filtering: GPO filtering is used to exempt objects (users, computers, or security groups) from Group Policy through the access control list (ACL) editor. This method of GPO management offers GIAC better control over specific computers and users within a Group Policy. Because Active Directory can group computers together and classify them as a security group, systems administrators can now use the GPO filtering method to selectively filter out computers and users that belong to a security group to explicitly deny access to apply a GPO.

We'll see an example of this method of GPO administration later in the Organizational Unit Group Policy section in page 22.

Block Inheritance and *No Override*: Within a domain, GPOs are inherited from one Active Directory container to another. GIAC can use the Block Inheritance setting in the GPO to prevent the OU from inheriting Group Policy settings from a parent container. However, if the GPO of the parent container has the No Override setting enforced, then the Block Inheritance setting will have no effect. For example, in Figure 4, the OU has the Block Inheritance setting checked (enabled). None of the GPO's from its parent container (Domain) will be applied except for Domain GPO 2. Domain GPO 2 will go through the Block Inheritance property and enforce the Group Policy to all objects in its child containers. An excellent use of the No Override feature is GIAC's user password Group Policy. It should be enforced no matter who the person is.

Loopback: Loopback is a management feature that only applies Group Policy to a specific computer. It will allow GIAC's systems administrator to override existing Group Policy on a particular computer. Loopback is an excellent feature if you want the computer environment to be the same no matter which user logs on. (Microsoft Corporation, "Designing a Microsoft Windows 2000 Directory Services Infrastructure", Module 5, pgs. 12~14) Loopback is a good Group Policy strategy for deploying publicly used computers. It is recommended when you want a particular computer to behave exactly the same (or as expected – very strict) no matter what user logs on. This feature will not apply to GIAC's Active Directory structure for it does not contain or host public computers for users to access.

Computer Settings And User Settings:

Within each GPO, Group Policy may be applied to the Computer Configuration and User Configuration in that container. By configuring policies within the Computer Configuration node in Group policy, policies are applied to computers regardless of who logs onto them. When configuring in the User Configuration node, policies are applied to users regardless of which computer they logged onto.

Within each configuration of the GPO, you can specify settings for the following:

- Software Settings
- Windows Settings
- Administrative Templates

With Software Settings, GIAC's systems administrator can implement automated software deployment for applications that includes a .msi package. A software package can be made available in one of two states: assigned or publish. GIAC's systems administrator can assign an application when he wants everyone to have the application on his or her computer. For example, all users in the Accounting and Human Resources OU must have Microsoft Excel on their computers. The systems administrator can advertise Excel for the users in this OU. Note: assigned software does not actually get installed; rather, the application shortcut and file associations are planted on the computer via the GPO. The application will self-install upon first use. On the other hand, a published application can be made available to the user, but it is up to

each person to decide whether or not to install the application. As an example, GIAC's system administrator can have an in-house built database application published to every computer. GIAC staff can then use the Add/Remove Programs in the Control Panel to initiate the installation process.

Next, scripts and security settings can be managed in Windows Settings. There are four states of GPO script deployments. Group Policies can be specified in computer startup/shutdown or user logon/logoff states. Startup/shutdown scripts are executed with local system (or administrator) privilege and logon/logoff are executed with the same privilege of the logged in user. Windows 2000 supports various scripting languages: such as old school - CMD/BAT files, Perl, Java, and MS Visual Basic Scripts (VBScript). Security Settings include information about account, local, and event log policies. We will investigate further in the next section, specifically on GIAC's domain policy, domain controller policy, and OU policies for GIAC's Active Directory.

Finally, a wide range settings and controls (including the operating system, program, user, and desktop environment) can be managed through the Administrative Settings in a GPO. The manageable settings here are similar to those found in Windows NT 4.0 Systems Policy Editor. It contains all registry-based policy information. GPO policies enforced in the Computer Configuration node are merged into the HKEY_LOCAL_MACHINE (HKLM) portion of the system registry, whereas the User Configuration GPO policies are merged into HKEY_CURRENT_USESR (HKCU) portion of the registry.

As you can see, utilizing the Active Directory provides a wide range of administrative controls over client workstations on GIAC's network. However, the most important issues remain undisguised – Security Settings. We will now go back and focus our attention on implementing Windows security GPO settings for GIAC's network infrastructure. There are nine distinct security features within this container. These nine features are used to manage the following:

- Account Policies
- Local Policies
- Event Logs
- Restricted Groups
- Systems Services
- Registry
- File System
- Public Key Policies
- IP Security Policies on Active Directory

Of these nine GPO features, we will focus our attention on implementing account policies, local policies, and event logs on GIAC's default domain, default domain controller, and OU policies. The remaining GPO features, in some degree, are less important comparing to the three being discussed, therefore will not be included in this report. They will be considered as being not within the scope of this report. GIAC's systems administrator is advised to explorer these remaining GPO features in a future date.

Default Domain Policy:

The default domain policy affects all users and computers in GIAC's domain tree. Group Policies set at this OU are inherited by all its child OUs. ISI recommends implementing the following policies for the default domain policy Security Settings:

- **Account Policies:** This portion of the policy allows GIAC's systems administrator to manage user password requirements and controls of lockout actions.

Password Policy: Password policy controls the properties of user password. GIAC does not want to force its employees to change their password too often. It does want however, to require employees to adopt a long and complex password.

✓ Enforce password history	8 passwords remembered
✓ Maximum password age	90 days
✓ Minimum password age	5 days
✓ Minimum password length	8 characters
✓ Passwords must meet complexity requirements	Enabled

The rational behind recommending these settings is to enforce an eight password history with a 5 day minimum usage, which automatically forces a minimum of 40 days before the user is able to reuse his first password. This would discourage any effort to reuse an old password as quickly as possible. Also, these settings also enforce a maximum password age of 90 days for those that never want to change passwords. The most important aspect of a password is the combination of its length and complexity. Complexity in this case, requires that each password contain three of the four following requirements: upper or lower case letters, numerals, and symbols. By requiring GIAC's employees to exercise this policy, the chance of a successful brute-force password guesses are virtually eliminated.

Account Lockout Policy: This policy controls the account lockout actions when an invalid password is entered.

✓ Account lockout duration	30 minutes
✓ Account lockout threshold	5 invalid logon attempts
✓ Reset account lockout counter after	30 minutes

These recommended settings causes an account to be locked out after five invalid attempts. The rational of a 30 minute lockout period is to provide even more protection to an already solid protection with a strong password. Plus, 30 minutes seems to be a good balance between ensuring a secured environment and unhappy users waiting to be able to sign-on again. With the combination of a 30 minute lockout period and strong password, for a would-be hacker, it is not worth the time nor the effort.

- **Local Policies:** This portion of the policy manages audits/logging specifications, user access rights, and other security options.

Audit Policy: Audit policy specifies what events or circumstances should trigger a log.

✓ 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	Failure
✓ Audit system events	Failure

It is recommended for GIAC to audit failures on all events. Never let any failures go unnoticed. Otherwise, if something should occur, whether the security was breached or not, the company will never find out what happened.

User Rights Assignment: This policy specifies user/group control and access rights in a local workstation.

✓ Deny access to this computer from the network	ANONYMOUS LOGON
✓ Deny logon as a batch job	ANONYMOUS LOGON
✓ Deny logon as a service	ANONYMOUS LOGON
✓ Deny logon locally	ANONYMOUS LOGON

Most other settings in this portion of the policy should be revisited by GIAC's systems administrator. However, ISI recommends the above four policies should explicitly deny anonymous access to local computer. These settings can be a fail-safe measure for any missed configuration or potential security hole(s) outside of the Active Directory.

Security Options: This policy specifies all other security settings in a local workstation.

✓ Do not display last user name in logon screen	Enabled
✓ Additional restrictions for anonymous connections	No access without explicit anonymous permissions
✓ LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM
✓ Rename administrator account	<new admin account id>
✓ Rename guest account	<new guest account id>

It is recommended that GIAC erase the name of the last signed-on user off the logon screen. This policy introduces another variable in the password guessing game for a would-be hacker. Here, we are specifying no access to any resources without explicit permissions to anonymous logons. We will only need to run in NTLMv2 level authentication mode due to the fact that GIAC's network is a Windows 2000 exclusive network. Renaming the administrator and guest

account is not only recommended, it is also critical. Because these are default accounts, they are prime targets for attacks and must be changed.

- **Event Logs:** This portion of the policy manages event log specifications.

✓ Maximum security log size	5120 kilobytes
✓ Restrict guest access to application log	Enabled
✓ Restrict guest access to security log	Enabled
✓ Restrict guest access to system log	Enabled
✓ Retention method for security log	As needed

As a general rule of thumb, we always want to restrict guest access to everything. In this case, we are restricting entry to the application, security, and system logs. The remaining three recommended event log policies all pertain to the security log: its size, retention method, and what to do when log is full. We want a log file size large enough to collect all security data on all the computers in the domain. 5 MB will provide sufficient space for most circumstances. The security log retention is set to overwrite as needed, however the log size is large enough to accommodate most local computers.

Default Domain Controller Policy:

The default domain controller policy affects only DC's in GIAC's domain tree. ISI recommends implementing the following policies for the default domain controller policy Security Settings:

- **Account Policies:**

Password Policy:

✓ Enforce password history	16 passwords remembered
✓ Maximum password age	60 days
✓ Minimum password age	5 days
✓ Minimum password length	8 characters
✓ Passwords must meet complexity requirements	Enabled

Password policy for the domain controllers should be more restrictive then that of the default domain policy. Besides having the same minimum password length and meeting complexity requirements as the default domain policy, ISI is recommending a longer password history and a shorter maximum password age. The rational behind forcing a shorter password lifespan (60 vs. 90 days) and minimizing password reuse (16 vs. 8 password history remembered) is to provide maximum security assurances for GIAC Enterprise's data. It will ensure a shorter unauthorized access time for as long as it is not detected.

Account Lockout Policy:

✓ Account lockout duration	30 minutes
✓ Account lockout threshold	5 invalid logon attempts

✓ Reset account lockout counter after	30 minutes

We will keep the same settings as those set in Default Domain Policy because it is also relatively a good balance between security and lockout time even for DC's.

- **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	Failure
✓ Audit system events	Success, Failure

Once again ISI recommends auditing all failed events. Never let failures go unnoticed or uninvestigated. Auditing policy settings stay relatively the same except now GIAC systems administrator should also audit successes in 'Audit system events'. The addition of auditing success events in DC's will help in the administration and troubleshooting of problems.

User Rights Assignment: This policy specifies user/group control and access rights in a local workstation.

✓ Deny access to this computer from the network	ANONYMOUS LOGON
✓ Deny logon as a batch job	ANONYMOUS LOGON
✓ Deny logon as a service	ANONYMOUS LOGON
✓ Deny logon locally	ANONYMOUS LOGON

The User Rights Assignment policy will also remain relatively the same with the exception of three important policies below:

✓ Access this computer from the network	Administrators, Authenticated Users
✓ Add workstations to a domain	Administrators
✓ Log on locally	Administrators, Server Operators, Backup Operators

By default, the 'Everyone' group is included in Access this computer from the network and Log on locally policy. There is no reason for this group to do either. We will only allow users with Administrators, Server Operators, and Backup Operators credentials to log on locally. Finally, by default, Authenticated Users are included in the Add workstations to a domain policy. All

workstation user support is strictly to be an IT function in GIAC's network. Regular users are not granted permission to add workstations to GIAC's domain.

Security Options: This policy specifies all other security settings in a local workstation.

✓ Do not display last user name in logon screen	Enabled
✓ Additional restrictions for anonymous connections	No access without explicit anonymous permissions
✓ LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM
✓ Rename administrator account	<new admin account id>
✓ Rename guest account	<new guest account id>

The Security Options policy will remain the same with the same reasons discussed in the previous section.

- **Event Logs:** This portion of the policy manages eventlog specifications.

✓ Maximum application log size	2048 kilobytes
✓ Maximum security log size	10240 kilobytes
✓ Maximum system log size	2048 kilobytes
✓ Restrict guest access to application log	Enabled
✓ Restrict guest access to security log	Enabled
✓ Restrict guest access to system log	Enabled
✓ Retain application log	14 days
✓ Retain security log	21 days
✓ Retain system log	14 days
✓ Retention method for application log	By days
✓ Retention method for security log	Manually
✓ Retention method for system log	By days

Again, as a general rule, always restrict guest access. Even though in this case, we have already specified only users with Administrators, Server Operators, and Backup Operators credentials to log on locally, we will still specify explicit guest access to all logs. For GIAC's systems administrator, 14 days of log retention and overwriting events as needed should be sufficient for both application and system logs. If the logs are filled before the 14 day period, the oldest events will be overwritten automatically. Lastly, we will retain 21 days of the security log. The systems administrator must monitor this log and manually clear it periodically. We have not opted to suggest setting the 'Shut down system immediately if unable to log security audits', because a near maxiumum log size alert is not available in the Active Directory GPO or Windows 2000 OS. Shutting down critical systems like a DC is not an option with GIAC. Rather, third party software should be used send (E-mail or page) alert to GIAC's systems administrator if security size should near the maximum.

Organizational Unit Group Policy:

As discussed previously, the systems administrator can take advantage and utilize the Active Directory GPO's to desktop administrations responsibilities. Among those responsibilities, there are some examples the systems administrator is able to manage through GPO's. They are the following:

- Software deployment and installation
- Internet Explorer configuration and maintenance
- Desktop and Control Panel

Software deployment and installation can be used to install a .msi package to a specific OU. We will address this Active Directory GPO feature in detail later.

Two recommended policies - disabling users to access to Internet Explorer's Security and Advance pages can be found in:
User Configurations | Administrative Templates | Windows Components | Internet Explorer | Internet Control Panel:

- ✓ Disable the Security page Enabled
- ✓ Disable the Advance page Enabled

These two policies if set in GIACgroup.GIACEnt.giac.com OU will restrict all users in its child OU's from gaining access to the Security and the Advance tab of the Internet Properties windows dialog box.

Another important GPO that should be implemented at the GIACgroup OU is the screen saver configuration. See Figure 6. This GPO will also be inherited to all child OU's to provide additional security.
User Configurations | Administrative Templates | Control Panel | Display:

- ✓ Activate screen saver Enabled
- ✓ Password protect the screen saver Enabled
- ✓ Screen Saver timeout Enabled

Also whenever possible, if a GPO only contains either Computer or User Configuration settings, disable the unused node to decrease the Group Policy processing time. See Figure 7.

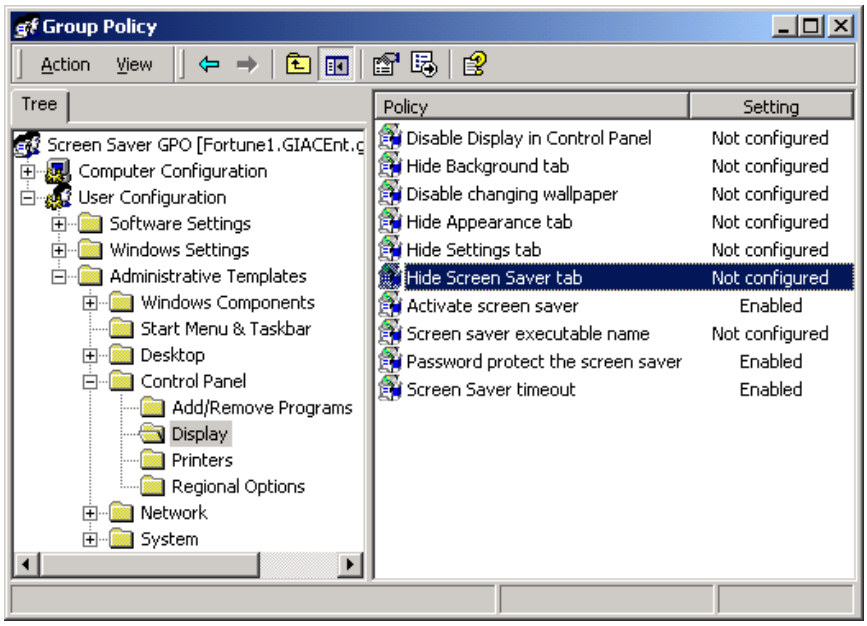

Figure 6: Screen Saver configuration for GIACgroup OU.

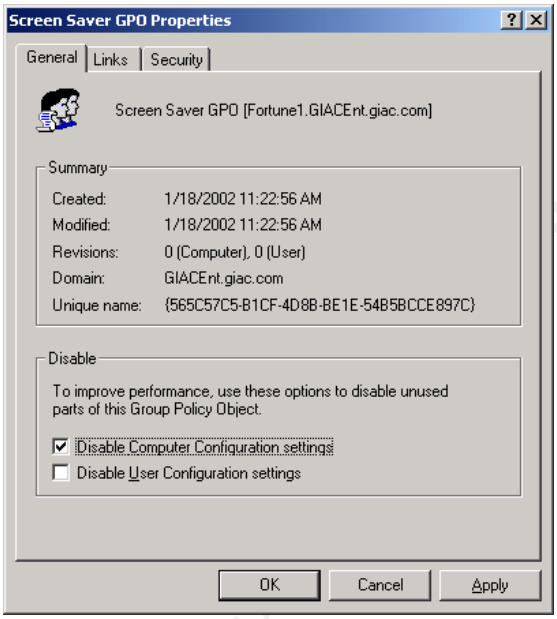

Figure 7: Disable unused node in a GPO to decrease Group Policy processing time.

Other useful Administrative Templates settings that should be implemented in the GIACgroup OU are:

To remove Run menu form Start Menu:
User Configuration | Administrative Templates | Windows Components | Windows Explorer:

- ✓ Remove "Map Network Drive" and "Disconnect Network Drive" — Enabled

To remove Run menu form Start Menu:
User Configuration | Administrative Templates | Start Menu & Taskbar:

- ✓ Remove Run menu from Start Menu Enabled

To disable registry editing tools:
User Configuration | Administrative Templates | System:

- ✓ Disable registry editing tools Enabled

All these other useful settings mentioned above will effect how the IT group is able to perform its duties when working in a Reach & Development OU because of how the Active Directory is structured. Refer to Figure 3. We can simply deny Apply Group Policy for the IT security group membership. See Figure 8 to see a representation of denying apply GPO to IT security group. Now, if one of the IT staff members are is logged onto any computers in any OU in the Active Directory, he/she has all the administrative access and tools to troubleshoot. There is another method of configuring the settings to achieve the same goal. It is the use of the Block Inheritance setting in the GPO. ISI chose not to use this method because it will introduce other problems for the proposed Active Directory structure setup. ISI suggests keeping Group Policies simple. Adding Block Inheritance adds another layer of complexity into Group Policy troubleshooting, testing, and documentation. For example, should the screen saver be applied to everyone, even members of the IT staff. Because the Screen Saver GPO and Disable Registry & CMD GPO are applied at the GIACgroup OU, even if block inheritance is at the IT OU level, you would still have to implement a link to the Screen Saver GPO at the IT OU level.

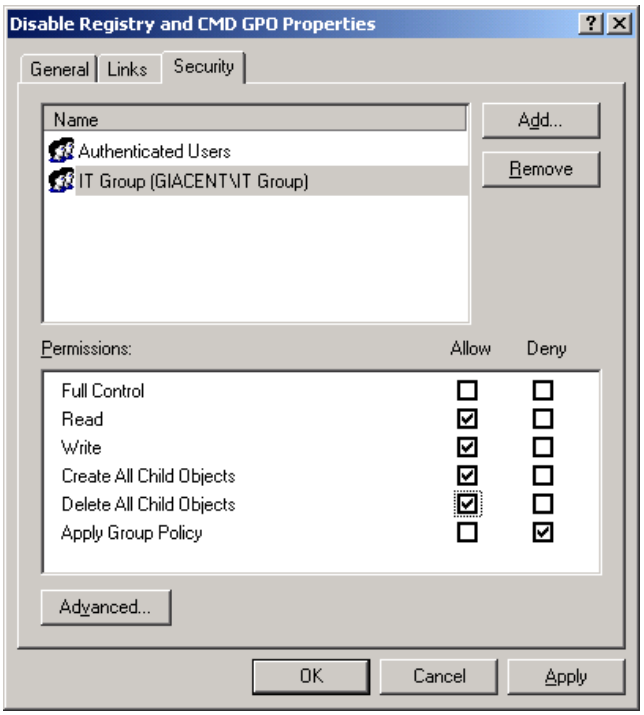

Figure 8: Denying Apply Group Policy Object to IT security group members.

Finance and Human Resources OU:

Being able to implement a "trusted" delegate to oversee administration of the Finance and Human Resources OU is one of the security interests that both GIAC's management and IT team were looking forward to. This appointed staff member would be an individual who works and directly reports to the Chief of Finance and Human Resources Division. This trusted administrative delegate would not be a full time IT staff member, rather, he would be given charged with the additional responsibilities of monitoring and managing this OU. He would be the one that watches out for Finance and Human Resources' best interests, both administrative and data integrities. As reported in the Delegate Administrative Authority in section IV, Active Directory Design and Diagram, we demonstrated the administrative authority delegation process to implement this kind of security.

Research and Development OU:

The Research and Development Division also wanted an administrative delegate for its division. Since its needs in some way mirror the needs of Finance and Human Resources, we will just note in this section that ISI recommended the same implementation procedure for the Research and Development Division as it did for the Finance and Human Resources Division.

All Research and Development computers must have MS Visio 2000 installed on it. We can create a 'Default R&D GPO' and assign MS Visio 2000 in Computer Configuration | Software Settings, right click on Software installation and select New | Package, to specify the path of the .msi file to complete this GPO. Refer to Figure 9. The next time the computer boots up, Visio program shortcut as well as all its file associations will be available to the users. Note, this .msi package can also be assigned to the User Configuration | Software Settings portion of the GPO.

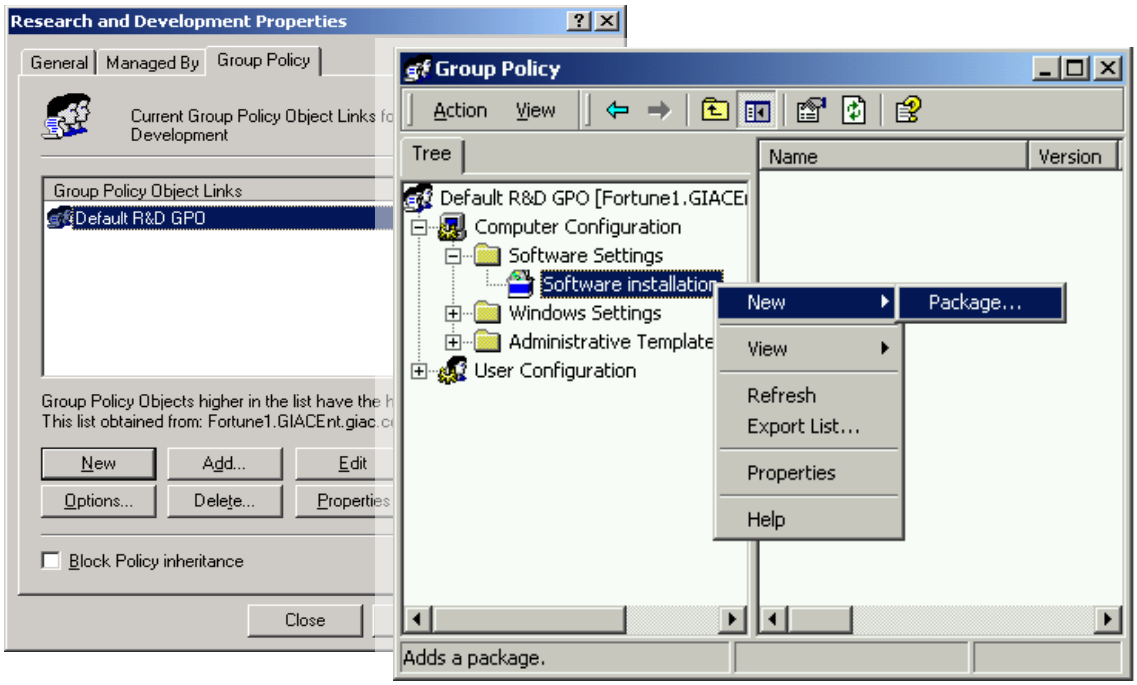

Figure 9: Assigning a software package.

Information Technology and Sales and Marketing OU:

There are currently no OU specific Group Policy requirements for these two OUs.

VI. SUMMARY

As demonstrated, GPO's can define the various components of the computer and user's environments in Active Directory at the site, domain, and OU objects. These components include Software Settings, Windows Settings, as well as Administrative Templates. All the manageable control that is provided by these settings can sometimes be overwhelming to an enterprise ready to implement Active Directory. However, with careful planning and fully understanding all the manageable settings and configurations of the Group Policies recommended by ISI, GIAC's IT division will be able to construct a secure internal Windows 2000 infrastructure for its employees.

After working extensively with all the departments and management levels within GIAC to find out their IT concerns and security problems, ISI recommends the following practices in managing Group Policy's. They are the following:

- Keep it simple. If possible, apply Group Policy at a top level where it will affect most of your users and computers. It would make troubleshooting Group Policy easier.
- Test and document the Group Policy plan. We cannot stress enough the importance of testing and documenting all Group Policy plans. Whenever possible, use an off-line test environment. Use the gpresult.exe command-line utility available from the Windows 2000 Server Resource Kit to check GPO settings in effect on that particular computer and the user who is logged onto the computer.
- Whenever possible, if a GPO only contains either Computer or User Configuration settings, GIAC should disable the unused node to decrease the Group Policy processing time. See Figure 7.
- Minimize the number of GPOs associated with users in domains or OUs. The more GPOs are applied to a user, the longer it takes to log on.
- Using the Block Policy Inheritance and No Override features sparingly. Routine use of these features makes it difficult to troubleshoot.

Finally, one very important factor of security not previously discussed here is that neither Group Policy related nor bulletproof passwords when it come to dealing with the human factor. With increasingly more software, hardware, ATM, office locks, and websites requiring passwords, people tend to write down passwords on a piece of paper instead of committing them to memory. This piece of paper can sometimes be easily found inside desk drawers or the password may be on a sticky note pasted on the monitor. No matter how secure your technical infrastructure may be or how long and complex the password is, security may be compromised because people make mistakes. This may be the biggest challenge in designing a secured infrastructure. If this is the roadblock, then consider taking the next step in the method of authentication technology:

- Smart cards

- Finger scan
- Voice scan
- Retina scan.

Each listed method of authentication are very different and has it's pro's and con's. Cost and compatibility may be a factor if GIAC is considering these alternative authentication methods. ISI recommends conducting a full business risk analysis to determine if there is a need to adopt one of these authentication methods.

VI. REFERENCES

Whiffen, Richard. Network Architect. Figure 1: GIAC Enterprises network architecture design.

Saunders, Jonathon, "Multi Service Access Solutions – CISCO 3600 Series and CISCO 2600 Series", URL:<http://www.CISCO.com/warp/public/cc/pd/rt/3600/prodlit/2636_pl.pdf>

Element K Journals, "Inside Microsoft Windows 2000", Volume 2, Number 1, January 2002

Designing a Microsoft® Windows® 2000 Directory Services Infrastructure
Microsoft Corporation, Material No: 1561BCP Microsoft®

McLean, Ian, "Little Black Book, Windows 2000 Security." Coriolis, 2000

Microsoft® Website, URL:<http://www.microsoft.com> (various)

Von Weltin, Alan, "Guide to Active Directory Design", September 11, 2000
URL:<http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/actdirds.asp>

Microsoft® Windows® 2000 Server Help Files (various)