Global Information Assurance Certification Paper

Secure Active Directory Design for GIAC Enterprises

GCWN Practical Assignment
Version 3.1 (revised April 8, 2002)

By
Charles J. Palmer

Table of Contents

Abstract

This paper discusses the design of a secure Active Directory infrastructure for GIAC Enterprises. This paper was written as part of a practical assignment for GIAC certification. The paper discusses many of the security improvements and implications of Active Directory. The discussion of Group Policy defines a policy to control workstations and users access to data on the network servers.

Introduction

Purpose of this paper

The design of a network and Active Directory are closely related. It is necessary to have an understanding of the network architecture to properly design the Active Directory structure. Additionally, understanding business needs is helpful in Active Directory design. With this in mind, the following sections will layout all of the different areas and how they interrelate to help with an effective rollout of Active Directory in this environment.

Description of GIAC Enterprises

GIAC Enterprises is an online fortune cookie publishing company based in Florida. They have a primary business office in Tampa, FL and a satellite office in the Chinatown section of San Francisco. The satellite site is connected to the home office with a 256KB fractional T1. The company has experienced a recent cash windfall when the owner played the lottery numbers printed on one of their fortunes and won the $250,000,000 lottery pot. This has resulted in a plan to upgrade the company infrastructure to Window 2000 on all servers and a standard desktop image of Windows XP with Office XP on all desktops. Additionally, the fractional T1 will be upgraded to full speed (1.54MBps). The existing servers are old and limited and will have to be replaced. Since most employees are not even on the network, a new domain will be created and built from the ground up. All employees will have a new desktop computer. An equipment list for the new network is as follows:

- 13 Compaq Proliant DL380 G2's w/ 2 1.4GHz procs, 1GB RAM
- 2 RA4100 Compaq SAN, 4TB and 1TB
- 150 Compaq Desktops, 2GHz, 256MB RAM, 40GB HDs
- 10 Compaq Laptops for management and IT staff
- Cisco Catalyst 6500 series backbone switch for main office
  - Gigabit attachment for all servers
  - Fast Ethernet switched to all desktops
- Cisco Catalyst 4000 series backbone switch for remote office
  - Gigabit attachment for all servers
  - Fast Ethernet switched to all desktops
- WAN cards will be installed to provide WAN connectivity between offices
- Cisco Router for T1 connection to Internet with room for growth

Existing equipment that will be reused is a recently purchased Cisco PIX Firewall that is installed on the Internet T1 that protects the company from direct access by Internet attached personnel. This will be retained in its current role and the configuration of the Cisco PIX firewall falls outside of the scope of this document.

The owner of GIAC Enterprises has retained my services to design and build their new Windows 2000 network. Some of the security requirements the owner has specified are as follows:

- Minimize the chance of information leakage both internal and external
- Provide standard desktop to all users minimizing ability to customize
- Users will not necessarily sit at same computer each shift
- Allow for 2 designated individuals in each office to be able to administer sites
- Owner wishes to limit access for overall control w/o having to deny Domain Admin level access to administrators
- Auditable Internet Access for employees based in the home office

Given these requirements, the following design will meet or exceed each of these requirements. The management will be involved for feedback during the design process to account for any changing network needs.

GIAC Enterprises has 3 major departments: HR/Finance, Research & Development, and Sales & Marketing.

HR/Finance is responsible for all of the companies accounting and personnel functions. Their data needs to be considered sensitive and unauthorized personnel should not have access to their data. All HR and Finance personnel are located in the Tampa Offices. They are on the ground floor of the 3-story building that comprises GIAC Enterprise's Tampa location. There are 20 associates that comprise the HR/Finance department including the Senior Vice President of HR/Finance.

The Research & Development department is located in the San Francisco offices of GIAC Enterprises. This office is located on the 2nd floor of the Hu Shor Da Di Chinese restaurant in Chinatown. There is a room on the second floor that has been reinforced and secured to function as the remote data center. This room will house the remote office backbone and network servers. The remainder of the floor is dedicated to the Research & Development department personnel. The R&D department consists of about 60 people including the R&D Senior Vice President. They are responsible for the development of the fortunes and lotto numbers for the fortune cookies. The restaurant downstairs is used as a test-bed for some of the fortunes as they are developed.

The Sales & Marketing department operates out of the Tampa, FL offices of GIAC Enterprises. They primarily work by phone sales and there is little travel involved. They gather contact information from the National Restaurant Registry. There are about 70 personnel in the S&M department. This is the most volatile department in the company. This is the department that does not have assigned desks and will be using different computers from day to day. They occupy the whole of the 2nd Floor and part of the 3rd Floor. The remainder of the 3rd Floor is made up of the datacenter and IT offices.

On the 3rd Floor of the Tampa Offices, half of the floor has been secured and setup as the primary data center for GIAC Enterprises. The datacenter has

all necessary environmental facilities as well as secured access and closed circuit cameras for monitoring. All surveillance tapes are stored offsite for a period of 3 years. There is an emergency generator capable of powering the datacenter and minimal external systems for a period of 3 days prior to needing a refueling. All backbone gear and server hardware are secured in the data center.

Figure 1 shows the physical network layout for GIAC Enterprises, Inc.

Network Design and Diagram

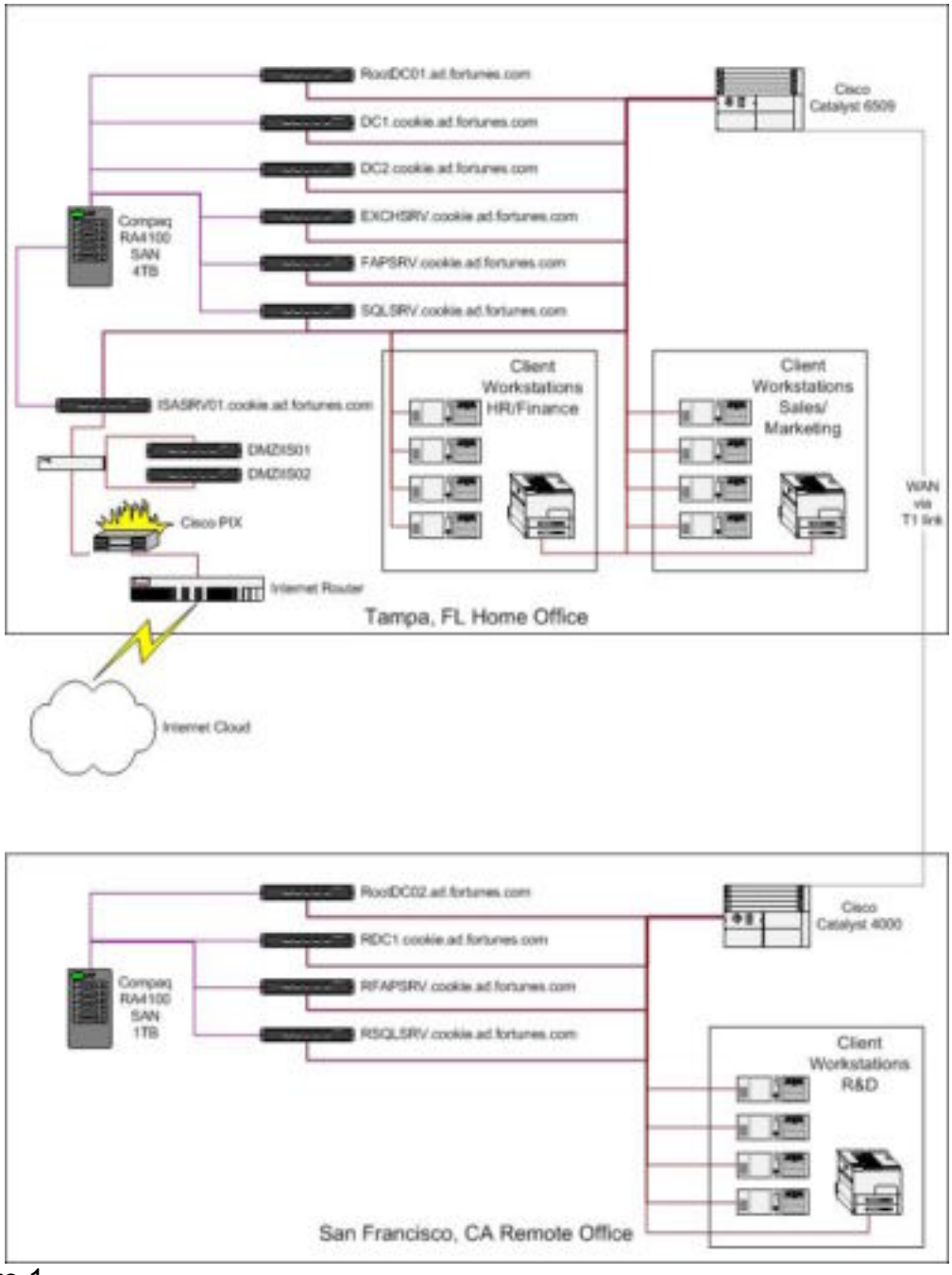

Figure 1

The network consists of two offices connected by T1 WAN connection. Each office can operate largely independent of the other office for short periods of time. Each site has its own core services with the exception of Email. Email is housed solely in the home office.

San Francisco Office

The San Francisco office can develop new fortunes and upload them to their local SQL database and the data will be synchronized on a regular basis back to the home office SQL server. They also have access to their local file server and domain controller for authentication.

Each server is configured with two local hard drives configured in a mirror arrangement for fault tolerance of the operating system. All data is stored on the SAN which is connected to the server via redundant fiber channel interfaces. Storage is allocated as follows:

SQL Server	300GB
File and Print	500GB
DC for Cookie	50GB
DC for Root	50GB

The additional 100GB's is held in reserve to be allocated where necessary. The servers, SAN, and backbone are all secured in the datacenter. Only the local IT representative and site manager have access to the datacenter. The surveillance tapes are shipped daily to the home office for archive. Nightly, critical data is replicated between the file servers and the SQL servers.

Tampa Office

The Tampa office is the primary office for GIAC Enterprises. Housed within the confines of the Tampa offices are the HR/Finance department on the 1st Floor, Sales & Marketing department on the 2nd Floor and part of 3rd Floor, and the Datacenter and IT services group on the remainder of the 3rd Floor.

The 1st floor houses the Reception Area that is staffed by HR, the HR Offices, and the Finance and Accounting functions. With the exception of the reception area, access to any other area of the building is restricted by badge access. All network connections on the 1st floor are terminated to the 3rd floor data center.

The 2nd floor houses the majority of the S&M department. Each person has a computer and a phone on their desk. Desktop computers provide them access to their contact management database and other tools necessary to perform their function. All network connections on the 2nd floor are terminated to the 3rd floor data center.

The 3rd floor houses the remainder of the S&M department and the IT offices and data center occupy the remainder of the floor. Only senior S&M employees are assigned desks on the 3rd floor. The data center is secured and only IT personnel and senior management have any access to the data center area. The area is protected with surveillance cameras and biometric access controls. There is a palm scanner and smartcard reader for entrance to the data center.

Within the data center, all network equipment is installed in a secured rack and the doors are locked. The servers and SAN are installed in 3 other racks. Each rack has its own UPS power source providing conditioned power to the

servers. Servers are balanced between the racks for fault tolerance where possible. All desktop network connections terminate in the datacenter in the back of the rack with the network equipment. Only currently active ports are enabled. All other ports are disabled and have to be enabled by IT staff to provide a live network connection. This is done to prevent anyone from connecting a computer at any unoccupied desk to collect network data.

Each server is configured with two local hard drives configured in a mirror arrangement for fault tolerance of the operating system. All data is stored on the SAN which is connected to the server via redundant fiber channel interfaces. Storage is allocated as follows:

SQL Server	1000GB
Exchange Server	1000GB
File and Print	1000GB
DC for Cookie	50GB each
DC for Root	50GB
ISA Server	50GB

The additional 800GB's is held in reserve to be allocated where necessary. The DMZ servers do not share anything with the internal network. They are each configured with 6 18.2GB hard disks in a RAID 0+1 configuration for maximum performance.

Active Directory Design and Diagram

The Active Directory design will mimic the setup of the company's sites and offices. It will consist of two site based on geography, Site Tampa, and Site SanFrancisco. Each department will have its own organizational unit. Within each OU, there will be four sub-OUs: Desktops, Users, Printers, and IT Staff. The layout of the domain can be seen in Figure 2 and the OU layout can be seen in Figure 3.

Each Departmental OU is setup with three sub OU's: Users, Computers, Printers. The Users OU has a sub OU named Unit Admins. Designated administrators within a unit are moved into this subcontainer. This OU is configure to Block Inheritance so that the unit administrators can troubleshoot machines without being locked down by the User Policies that prevent access to system tools. Additionally, any users that are in the Unit Admin subcontainer will also need to be added to the admin group for that subcontainer. Each OU will have a group defined and delegated as having administrative access to all users, computers and printers within that OU. The groups will be named after the department using the following criteria: OUAdmin_DeptName.

Since the owner of the company wishes to plan for future acquisitions and he likes to maintain control, the domain will be setup with an empty root design. The empty root will only have accounts for the owner, his son, and the Senior Vice President of IT. The root domain's NETBios name will be simply ROOT. The Fully Qualified DNS Name (FQDN) is AD.Fortunes.com. The primary domain for all users, computers, and other resources will be named COOKIE. The FQDN is COOKIE.AD.Fortunes.com. Each department will have designated personnel for the management of network equipment and personnel in the department on a day-to-day basis. The IT department maintains responsibility for long term planning and upkeep of the network resources as well as the day-to-day maintenance of cross-departmental resources.

FSMO Placement

With Windows 2000 and Active Directory, Microsoft made great strides in improving the flexibility of the network domains. The multi-master model provides a more robust and reliable infrastructure than the old single-master model. But, certain functions lend themselves to needing a single point of contact for control of these services. These services are known as the Flexible Single Master Operations (FSMO). The 5 FSMO services can be divided into two groups: Forest Wide and Domain Wide. The Forest Wide FSMO roles are the schema master and the domain naming masters. There is only one of each of these for the whole forest, regardless of the number of domains. These roles will be held by domain controllers in the first domain of the forest, known as the ROOT domain. The remaining 3 FSMO roles exist in every domain within the forest. These three roles are: infrastructure master, RID master, and the PDC emulator.

The domain controller with the PDC emulator role acts as an old style NT4 domain controller in mixed mode domains. Also, all password changes are preferentially communicated to the PDC emulator DC.

The RID master helps insure unique SID's throughout a domain. The RID is a Relative Identifier. Each domain controller communicates with the RID DC to get an allotment of RIDs to assign to domain objects. When their pool runs low, DC's will communicate with the RID master to get a fresh supply. In a static domain, the RID master could be unavailable for an extended period of time with little ill effect.

The Infrastructure master is responsible for ensuring that the global catalog server has the appropriate information. Because of this, in a multi-domain environment like ours, it is imperative that the Infrastructure master and Global Catalog server role not be held by the same DC.

The Domain Naming Master is responsible for the structure of the directory trees. A new domain cannot be added if the domain naming master is offline.

The Schema master is responsible for changes to the active directory schema. To modify the schema, a user needs to be a member of the Schema Admins group. Because changes to the schema should only be undertaken with significant planning, no users, including the Administrator account, should be members of the Schema Admins group.

Taking all of the FSMO roles into account as well as the need of Global Catalog servers, we will have the following division of schema rolls:

ROOT domain	
Schema	ROOTDC01
Domain Naming	ROOTDC01
PDC Emulator	ROOTDC01
RID Master	ROOTDC01
Infrastructure	ROOTDC01
Global Catalog	ROOTDC02 (GC for Remote Site)

COOKIE domain	
PDC Emulator	DC01
RID Master	DC01
Infrastructure	DC01
Global Catalog	DC02 (GC for Primary Site)

Certificate Services Architecture

With the owner's desire for security, it is necessary to implement IP Security for many of the applications. To facilitate this, a certificate services infrastructure is necessary. While a certificate services infrastructure is not absolutely necessary to use IP Security, it significantly improves the deployability of IP Security. Without a certificate services infrastructure, it would be necessary

to provide a shared secret key to all necessary machines. With the small IT staff and the comparative ease of implementing a certificate infrastructure, it is not cost effective to not implement one.

Since GIAC Enterprise does not need to issue certificates to persons external to the company for access, the need of an independent certificate authority like Verisign or Thawte is not cost justifiable. But, having a hierarchy of certificate servers is desirable since we would want multiple issuing servers all authenticated by the same root CA. With this in mind, we will be using one of the old company laptops to build an offline standalone root CA. This server will then issue certificates to the domain controllers that will host the issuing certificate services. (Fossen, 2002) This will allow the root CA to be maintained offline and stored in a fireproof safe. A backup of the private key will be made and stored at a different, secure location. The ROOT domain DC's will both run certificate services and will issue IP Security certificates to clients when requested. Additional certificate usage will be examined on an as needed basis. A diagram detailing the certificate structure can be seen in Figure 4.

IP Security Design

IP Security is a standards based technology that has been implemented in Windows 2000. Microsoft has provided a means to encrypt and/or authenticate data as it travels across the wire. The code for IP Security that is within Windows 2000 was a collaborative effort between Microsoft and Cisco. It adheres to the IP Security standards and provides a means to ease the implementation of a secure IP Security infrastructure. Group Policy provides a means of centrally managing the IP Security infrastructure and Group Policy settings will be discussed below.

The requirements for IP Security are founded in the need for securing access to the Accounting/Financial data as well as Personnel data. Also, to minimize the chance of leakage of corporate data, the data accessed within the Research and Development department should also be protected. Since all servers are running Windows 2000 and all clients are running Windows XP, it will be simple enough to implement an IP Security policy that will require secure communications between clients and servers, thereby limiting the access to the data to corporate systems. If an outsider were able to tap into the network infrastructure, they should not be able to retrieve any sensitive data since it will be encrypted on the wire.

Since all servers will be within the same routable network space and all systems will have a unique IP address on the network, there should be no issues with Network Address Translation.

Server Roles

When planning a network, it is ideal to provide a different machine for each different service that will be provided. This allows for minimal impact in the event of a problem with one application. Since it is rare to have a budget that will allow this, it is necessary to design servers with similar roles that do not conflict

with each other. It is a good practice to consolidate your WINS, DNS, and DHCP on one system. But, since DNS is a necessary component of your Active Directory infrastructure, the DNS service is typically on your domain controllers. Adding WINS to a domain controller is also a good option. But, DHCP is not a good choice from a security perspective in a migration environment. Since the DHCP service will register DNS records for clients that can not register themselves, by default, the DHCP server will be the owner of the DNS records, assuming Active Directory Integrated DNS zones. When a client is upgraded to a level that would allow it to register itself, problems result because the machine does not have access to its own record with Active Directory Integrated DNS, the client system generates an error message. This message can be overcome by adding the DHCP server's machine account to the DNSUpdateProxy group. Then, when the DHCP server registers a DNS name, it does not take exclusive control of the record. This is a security problem if the domain controller is hosting the DHCP service. When the DC registers itself with DNS, the DC's DNS records would then not be owned by the DC and there is the possibility of a rogue machine changing the DNS record of the DC. Therefore, it is best to avoid placing DHCP on a domain controller in a migration environment. In our environment, since all machines are starting out as Windows XP or Windows 2000, this is not a limitation with which we need to be concerned.

Other services that pair well are low volume services like certificate services. Unless you are in an environment where there is a high volume of certificates being issued, a domain controller is also a good choice for the placement of the certificate services. File and printing services are also good choices for teaming together on a single machine. In a Windows NT environment, it was common practice to put file sharing services onto domain controllers. The reasoning behind this was the fact that local groups created on a domain controller were shared amongst all of the domain controllers, thereby easing group maintenance. In Windows 2000, with the new class of group known as the Domain Local Group, this is no longer necessary. Domain Local Groups can be used on any domain member server or workstation to assign permissions to resources. This provides more flexibility than was provided in the NT4 domain environment.

Some services should not be combined with any other service. Two examples of this are Exchange Services and SQL services. Each of these should be given their own system for performance reasons.

With the above considerations in mind, servers will have the following distribution of server roles:

ROOTDC01	DC, Issuing Certificate Authority, DNS, WINS, DHCP
ROOTDC02	DC, Issuing Certificate Authority, DNS, WINS, DHCP
DC01	DC
DC02	DC
RDC01	DC
EXCHSRV	Exchange Services
FAPSRV	File and Print
RFAPSRV	File and Print
SQLSRV	SQL Services
RSQLSRV	SQL Services
ISASRV01	ISA Server (firewall and proxy mode)
DMZIIS01	IIS
DMZIIS02	IIS

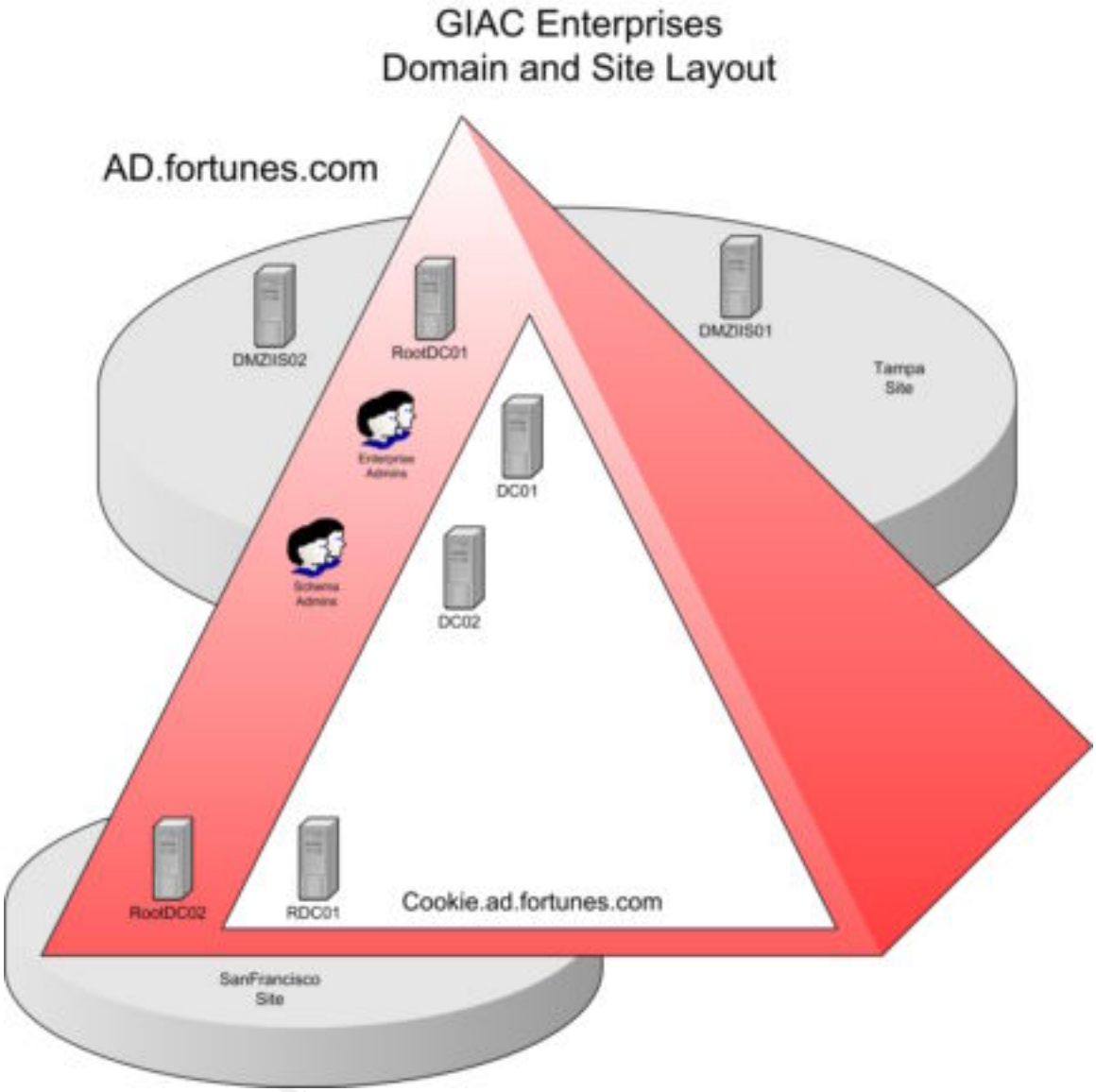

Figure 2

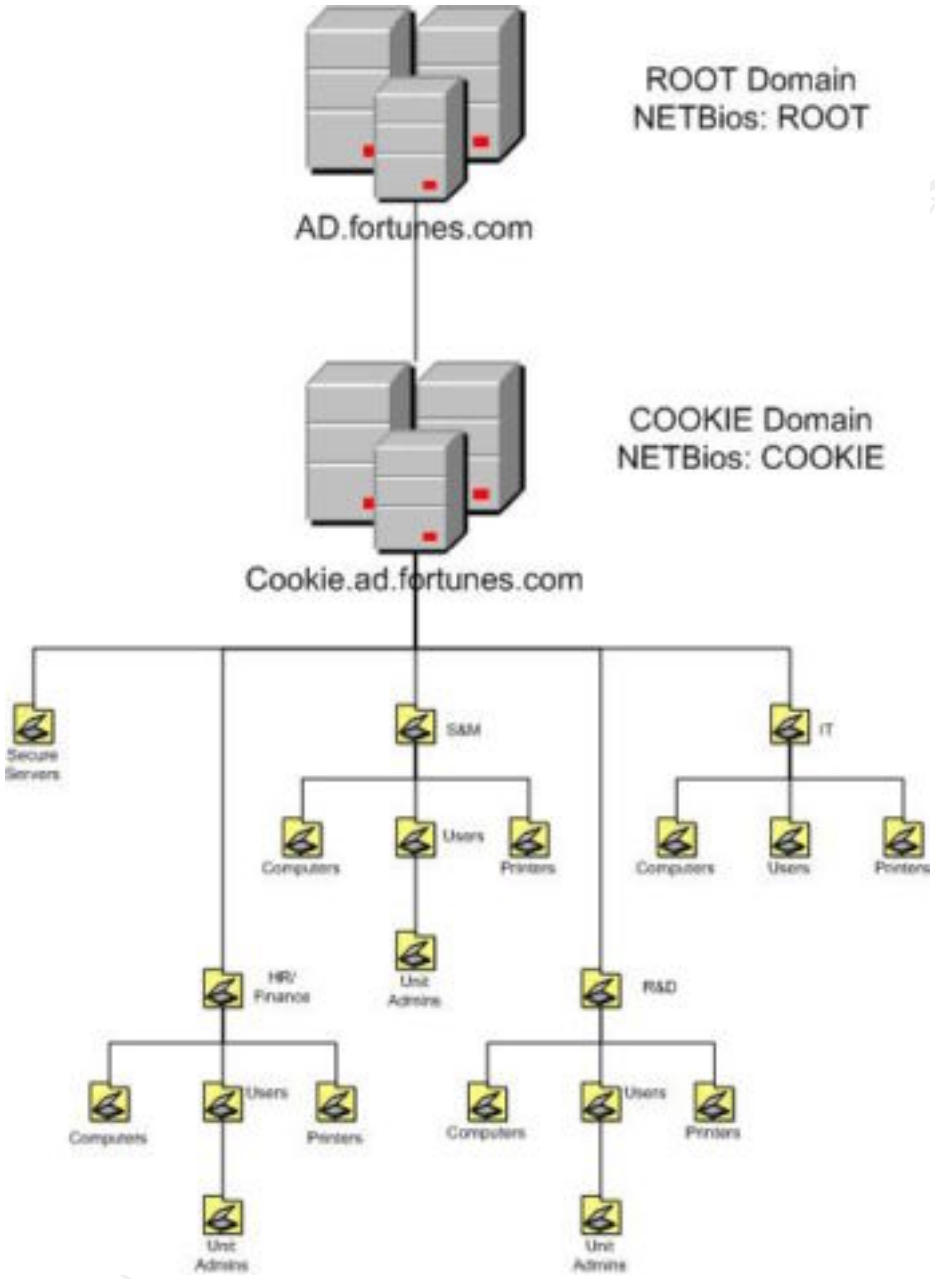

Figure 3

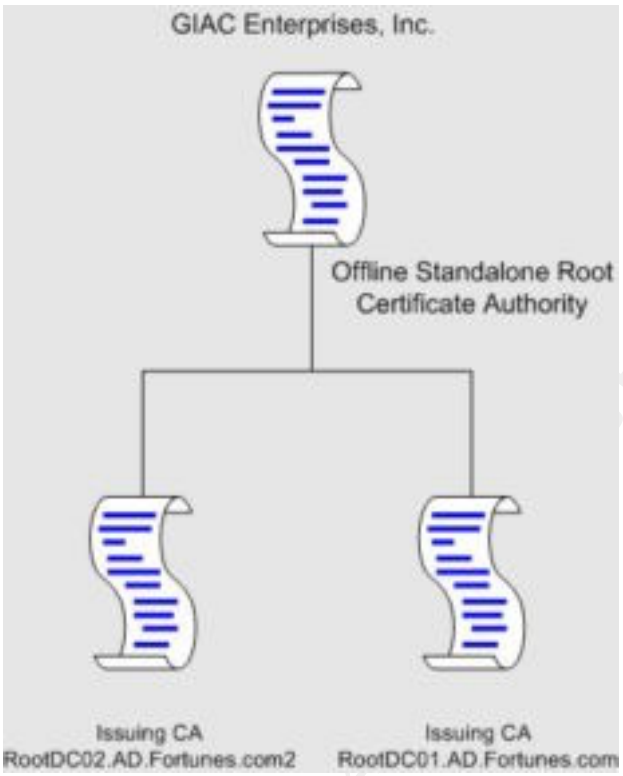

Figure 4

Group Policy and Security

Basic Group Policy

Background on Group Policy

Of all the features and advances in Windows 2000 over Windows NT 4, the one that provides the most advantage to network administrators is Group Policy. Group Policy provides security administrators with significantly more control over both servers and workstations from a central location than any previous built-in tool. While WinNT had NTConfig.pol and Config.pol to provide some central control of client machines, Group Policy brings this control to a whole new level. With Policy files, network systems were "tattooed" with the settings supplied by the policy file. Tattooing means that the settings were persistent regardless of who is logging on. This was problematic when administrators locked down systems for their users and then the administrator needed to log into the systems to fix something. Depending on what was locked down, the administrator may have been unable to troubleshoot the problem without first reversing the necessary tattoos. While some policy settings for Group Policy will tattoo a system, a large number will change on a per user basis.

The terms used by Jeremy Moskowitz to describe the new policies are Policies and Preferences. Preferences tattoo the system; Policies do not tattoo the system. Policies use a "non-sticky" portion of the registry to store their settings. Because of this, applications have to be written to support Policies. Otherwise, the only way to affect change on an application that is not aware of the Policy section is to use the old style preferences and tattoo the system. Policies are set on a user or computer basis in the following locations:

HKLM\Software\Policies
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies
HKCU\Software\Policies
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies

Any settings made in the above areas of the registry are considered non-sticky and do not tattoo the registry. If the setting is made anywhere else in the registry, it is sticky or persistent and it is classified as a preference. Additionally, Microsoft has provided more tools/documentation for customizing group policy than they did with the earlier system policies.

Knowing what we now know about group policy, there are a few other points that need to be kept in mind. The two default group policies are special when compared to any other user defined policy. Per Moskowitz, 2001, "These two policies are special. First, they cannot be easily deleted (though they can be renamed). Next, each default Group Policy object generated by the system contains a special property that doesn't quite act like the Group Policies that we

mere mortals can create." He goes on to describe the differences. The default domain policy is responsible for the Password Policy, Account Lockout Policy, and the Kerberos Policy. While you might try to set these settings in other user created policies, the Default Domain Policy takes precedence for these settings throughout the whole domain. Additionally, there are three other settings that can only be set in the Default Domain Policy:

Automatically Log Off Users When Logon Time Expires
Rename Administrator Account
Rename Guest Account

While technically, you could wipe out the Default Domain Policy and set another policy as having a higher precedence, thereby destroying the "special nature" of this policy, this is not recommended. (Moskowitz, 2001)

The Default Domain Controllers Policy has the special power that it will always affect domain controllers, no matter which OU to which the DC's might be moved.

Basic Domain Settings for Group Policy

Following the recommendations for setting up group policy as laid out in Moskowitz, 2001, we will define the Default Domain Policy special settings in the Default Domain Policy and create new policies for any additional settings that we will be using. Within the Default Domain Policy, we will define the password requirements, account lockout, and Kerberos.

Password Policy:

We will set Password Policy as laid out in the following table:

Policy Name	Setting	Explanation
Enforce Password History	12	Setting the password history to remember the last 12 passwords, when combined with the other settings results in an acceptably long period of time before the user would be able to go back to an old password.
Maximum Password Age	60 days	Requiring users to change their passwords is essential to good security, but security has to be balanced with the patience of users. Many users do not like having to change their password on a regular basis. Therefore, we are setting the maximum password age short enough to minimize the chance of a password being cracked before expiration and long enough that most users will accept changing their password.
Minimum	5 days	Setting this to 5 days requires a user to wait at

Password Age		least 5 days before trying to change their password again. This coupled with the password history of 12 would mean an absolute minimum of 60 days before a user to change their password back to what it was before they had to change it originally. Few users will have the patience and tenacity to actually go through this exercise for another brief 60 day period of using the same password. Also, 5 days is short enough that most users will become familiar enough with their new password that they will not want to change it until they are required to change it.
Minimum Password Length	7 characters	A setting of 7 characters was chosen because of the backwards compatibility feature of LANMAN hashes. Since Windows 2000 servers still store LM hashes along with the NTLM hashes, this makes the password more vulnerable to password cracking. The LM hash has been proven trivial to crack due to its smaller possible character set (not case sensitive) and the algorithm used to encrypt it. Once the LM hash is known, tools such as L0phtCrack can determine the NTLM hash in short order. See further discussion below.
Password must meet complexity requirements	Enabled	Enabling this setting requires the user to meet the complexity requirements as published by Microsoft in the "Security Operations Guide for Windows 2000 Server". These requirements are as follows: Minimum length of 6 characters (which we exceed) 3 of the 4 characters groups: uppercase, lowercase, Arabic numerals, punctuation. While it is not stated in this source, this setting is derived from the Windows NT 4 PASSFILT.DLL. If all of the functionality of PASSFILT has been transferred into this setting, it should also screen out any usage of the user name and full name as part of the password. This goes a long way in ensuring users have difficult to guess passwords.
Store password using reversible encryption for all user in the domain	Disabled	We will not be running any applications that require the password to be stored in a reversibly encrypted state. This setting severely undermines the security of the

		network and applications that require it should be avoided if possible. In the event that an application that requires this is necessary, this can be set on an account basis and only those accounts that need to use the applications passwords would then be stored in a reversible state. But, on a domain wide basis, this is a setting that should always be set to Disabled in a secure environment.

Further discussion on password length:

While there is a new registry key in Windows 2000 that will turn off the storage of the LM hash altogether, the use of this setting is not supported. It has not been thoroughly tested and it may break certain applications. Also, it does not actually clear out the LM hash that is already stored within the SAM or Active Directory. This could cause authentication problems down the road. It is better to control the user of the LM hash with the LMCompatibility registry key and the LM Authentication Security setting that will be discuss in more detail below. (Scambray & McClure, 2001)

Account Lockout Policy:

Account lockout goes hand-in-hand with the password policy. If you set a good password policy, but allow unlimited brute force attempts against the passwords, your network will not be secure very long. Account lockout policy sets limits on the number of attempts at typing an incorrect password before action is taken. The following settings will be used:

Policy Name	Settings	Explanation
Account Lockout Threshold	5 invalid attempts	The threshold determines the number of unsuccessful password attempts that can be made in the period of time defined below before the network account will be locked out. Offline brute force attacks, unfortunately, are not affected by this policy.
Reset Account Lockout Counter After	60 minutes	This is the time interval that the above defined number of invalid attempts will be track. If there are 5 invalid attempts within a 60 minute period, the account will be locked out for the duration defined below.
Account Lockout Duration	120 minutes	Lockout duration of 2 hours will severely hinder anyone trying to perform a brute force attack network. If a legitimate user mistypes their password and locks out their account, they will be able to contact their designated support person to have their account unlocked without waiting the full 2 hours.

Account lockout needs to be monitored on a regular basis by IT staff. Event log entries will be made on the domain controllers when an account is locked out. All domain controller event logs need to be check on a regular basis for event ID 539. If there are a large number of account lockout events for key accounts, action should be taken to investigate the source of the invalid attempts.

Kerberos Policy:

The Kerberos Policies as defined by Microsoft in the default settings are secure enough for our environment. We will be making no change to these policies.

Additional Default Domain policy settings:

Automatically Log Off Users When Logon Time Expires: While initially, we will not be setting hours to limit logon, we will Enable this setting to ensure that if we do decide to enable this option at a later date, this setting is already available for enforcing logon hours.
Rename Administrator Account: Since Administrator is a very well known account, it is prudent to take the extra step to rename the administrator account. Even though it is easy enough to determine the account name since the SID is a known constant, as part of a strategy of removing the low-hanging fruit, the administrator account name will be changed to GIACMIN as part of the Default Domain Policy.
Rename Guest Account: The guest account will be disabled, but for the same reasons as above, the guest account will be renamed FRED.

That completes the settings that will be set in the Default Domain Policy. We will now go through the settings that will be set specifically for the Domain Controllers.

Since the domain controllers receive all of the settings from the default domain policy, we will not be looking at any of those settings within the Default Domain Controller Policies. We will concentrate on the policies that matter most to domain controllers and their role in maintaining network security.

Audit Policy:

The audit policy determines what will be tracked and logged by the system. Audit events are written to the event log. The following settings will be used to determine what will be logged on the domain controllers:

Policy Name	Setting	Explanation
Audit account logon events	Success, Failure	Tracks successful and failed use of domain accounts to authenticate to network systems. This will provide a record of users authenticating to the

		domain.
Audit account management	Success, Failure	This will provide an audit trail for accountability of successful account modification. It will also track attempts by unauthorized users to modify accounts.
Audit directory service access	Failure	Failed attempts at accessing the directory service object that have their system access control list (SACL) defined will be recorded.
Audit logon events	Success, Failure	Auditing both success and failure is necessary as part of a good security policy. If only failure events were logged, there would be no record of a successful logon after multiple failed attempts. Also, being able to track the logon of legitimate users may be desirable in some environments. This will track where the user logged on as well as other pertinent information that could be useful in a post-attack analysis.
Audit object access	Success, Failure	This will allow the tracking of access to defined objects. By default, no objects are enabled for auditing. This can be enabled on a per file/registry entry basis. Highly sensitive files or registry keys can be configured for auditing and success and failure access events will be logged. Auditing both success and failure access of some files can result in significant logging activity. The items actually audited should be selected carefully and high volume files should not be audited at all, except in the highest security environments.
Audit policy change	Success, Failure	This will provide an audit trail of successful policy modification as well as unsuccessful attempts to modify policy by those not authorized.
Audit privilege use	Failure	This will track the unsuccessful attempt to use certain advanced privileges. Only failures are tracked because tracking success would result in an excessive amount of log entries.
Audit process tracking	Not defined	Tracking individual processes is a very resource intensive process. It should only be performed for troubleshooting reasons or when a system is under attack and detail tracking of what is being performed is desirable.
Audit system events	Success, Failure	Tracks the startup and shutdown times of systems. This is useful for auditing of system uptime for domain controllers.

User Rights Assignment:

User rights provide additional permissions to groups or individuals on a system. We will only discuss the ones that have been modified from the default below.

The following user right should not have anyone assigned the right by default on domain controllers:

Act as part of the operating system
Add workstation to domain
Create a token object
Create permanent shared objects
Debug programs
Deny access to the computer from the network
Deny logon as a batch job
Deny logon as a service
Deny logon locally
Generate security audits
Lock pages in memory
Log on as a service
Remove computer from docking station
Replace process level token
Synchronize directory service data

Modifications from default:

- In a default configuration, any authenticated user can add a workstation to the domain. There is a limit of only 10 machines per user, but this is a potential security vulnerability if any user can add computers to the domain. Therefore we removed the Authenticated Users group from this right.
- The administrators group has the ability to debug a program in a default configuration. Only developers need to debug programs and will rarely need to do so on a domain controller. Therefore, the administrators group has been removed from this right and no other accounts are granted this right.
- Since production domain controllers are not running on docked laptops, the ability to remove computer from docking station is unnecessary. Therefore, there is no need for any user to be assigned this right, not even the default Administrators group.

The following additional modifications will be made from the default:

- Everyone removed from 'Access this computer from the network' in favor of Authenticated Users
- Everyone group removed from 'Bypass traverse checking' leaving only Authenticated Users and Administrators

- Since only administrators should be shutting down domain controllers, only Administrators have the right to 'Force shutdown from remote systems' and 'Shutdown the system'. Server Operators, Backup Operators, Print Operators, and Account Operators have been removed from the default setting.

Security Options:

The following security options will be set specifically for the domain controllers:

Policy Name	Setting	Explanation
Additional restrictions for anonymous connections	No access without explicit anonymous permissions	Since all applications on our network are certified for Windows 2000, we do not want to allow any unnecessary information leakage.
Number of previous logons to cache (in case domain controller is not available)	0	Since this is a domain controller, it should not be unavailable if you are logging onto it. Therefore, we will be disabling cached logons.
Rename Administrator account	DomMaster	Renaming the domain level administrator account to a different name than any of the client machines.

All remaining settings will be inherited from the domain level.

Event Log Settings:

The retention time and size of the domain controller event logs will be different that the rest of the systems on the domain. These settings will be set as follows:

Policy Name	Setting	Explanation
Maximum application log size	102400	100MB of log data is sufficient with the archive actions that are defined below.
Maximum security log size	204800	200MB for security log data will allow for a sufficient number of events. Archives will be available of older entries if necessary.
Maximum system log size	102400	100MB of system log data is sufficient with the archive actions as defined below.
Restrict guest access for all three logs	Enabled	Any users with guest level access should not be able to view any of the event logs.
Retention method	As	Since events will be archived and the log

for all three logs	Needed	cleared on a regular basis, no data will be lost using the as needed setting.

A process will be put into place where all domain controller event logs will be dumped to file and cleared on a weekly basis. These files will then be imported into the SQL database for analysis, when necessary.

Custom Domain Computer Group Policy:

For all remaining domain wide settings a new group policy object will be created and linked to the domain. The Microsoft supplied template securews.inf will be used as a basis for all settings below where applicable. Any settings that are already defined in the Default Domain Policy will be set to Not Defined within this policy object. The User Configuration half will be disabled to allow for faster processing. The following configuration settings will be made for all network computers, except where overridden by a more specific policy.

Computer Configuration/Windows Settings/Scripts: A startup script and shutdown script will be defined. The script will check the current patch status on each computer and log any missing security patches in a central location for the IT department to examine. This may be refined to allow the installation of critical patches on shutdown of a computer. This script will utilize hfnetchk.exe and a centralized XML file. The output will be parsed to look for any discrepancies. An up-to-date version of the XML file will be downloaded on a daily basis to ensure that systems are checking against an up-to-date source. When Microsoft starts distributing MSI friendly patches, the Software Installation section will be utilized for installing patches after they undergo appropriate testing.

Computer Configuration/Windows Settings/Security Settings/Local Policies/Audit Policy:
All setting are per securews.inf except “Audit logon event” which is set to “Success, Failure” instead of just “Failure.”

Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options:
“Message title for users attempting to log on” will be set to “Important Notice from GIAC Enterprises”

“Message text for users attempting to log on” will read as follows:

> “The system you are accessing is the property of GIAC Enterprises, Inc. We reserve the right to audit any activities performed with this computer. These systems are provided to allow our employees the tools they need to perform their duties. Any unauthorized activity or logon is prohibited and any such activity discovered will be prosecuted to the full extent of the law. If you agree to the terms of this statement, you may click OK to continue your login.”

Policy Name	Settings
Secure Channel: Require strong (Windows 2000 or later) session key	Enabled
LAN Manager Authentication Level	Send NTLMv2 responses only\refuse LM & NTLM
Do not display last user name in logon screen	Enabled
Number of previous logons to cache (in case domain controller is not available)	3

Computer Configuration/Windows Settings/Security Settings/Event Log
All three logs size will be set to 5120KB. Since extensive auditing is not set on the individual workstations, these settings are primarily for troubleshooting issues with the workstation. The event logs will also be set to overwrite as needed.

All other settings for the computer section of the Custom Computer Domain Policy are per the securews.inf template.

Custom Domain User Group Policy

For the User section of the policy, only defined policies will be listed below. Most of these settings are locking down the desktop to minimize user customizations. The Domain Admins and Domain Account Operators (Custom group with Account Operator privileges, All OU Admin groups are members) groups will be denied the "Apply Group Policy" permission thereby allowing them to be unaffected by these lockdowns.

User Configuration/Windows Settings/Internet Explorer Maintenance/Connections: Proxy settings will be defined to use the corporate ISA server as their proxy server. Access to the Internet will be controlled by groups defined on the ISA server.

User Configuration/Windows Settings/Scripts(Logon/Logoff):
A logon script that maps the necessary network drives and printers for users will be assigned via the Logon Script setting. A Logoff Script will be assigned to perform cleanup of user temporary data from the computers.

User Configuration/Administrative Templates/Windows Components/Internet Explorer/Internet Control Panel:
The following settings will be set to Enabled:

- Disable the General page
- Disable the Security page
- Disable the Content page
- Disable the Connections page
- Disable the Programs page
- Disable the Advanced page

User Configuration/Administrative Templates/Windows Components/Windows Explorer:
The following settings will be set to Enabled:
- No "Computers Near Me" in My Network Places
- No "Entire Network" in My Network Places
- Removes the Folder Options menu item from the Tools menu
- Remove File menu from Windows Explorer
- Remove "Map Network Drive" and "Remove Network Drive"

User Configuration/Administrative Templates/Windows Components/Start Menu & Taskbar:
The following settings will be set to Enabled:
- Remove Run menu from Start Menu
- Add Logoff to the Start Menu
- Disable changes to Taskbar and Start Menu Settings
- Disabled personalize menus

User Configuration/Administrative Templates/Windows Components/Desktop:
The following settings will be set to Enabled:
- Hide My Network Places icon on the desktop
- Disable Active Desktop
- Disable all items

User Configuration/Administrative Templates/Windows Components/Control Panel:
- Disable Control Panel

User Configuration/Administrative Templates/Windows Components/System:
- Disable the command prompt
- Disable registry editing tools

Explanations

As you can see from the above, these settings are self-explanatory. They lock down the desktop of the average user to limit their ability to customize their environment. Coupled with the roaming user profiles that will be defined below in the Additional Security section, each user, regardless of which workstation they sit down at each day, will get a consistent user environment.

Additional Group Policy – Application and User Data Redirection

With the need to provide a means of providing a reliable backup option for user data, it is necessary to formulate a backup plan. Backing up each user's desktop is not feasible from a space standpoint. There is a large amount of repetitive information on each machine. All we want to backup is the data. With Group Policy, there is an easy means of performing this backup. We will redirect the user's My Documents folder to a network location. We will set the location by Organizational Units. Since we have setup our departmental organizational units such that they do not span sites, it makes it easy to choose a location that will be local and fast for the user. For the small number of users that travel between sites, we have the option of setting up file replication either with Windows 2000 or with the SAN technology that we have deployed to make the data available at both offices.

To accomplish this, we will create a new OU for each department that requires redirection. First, we need to establish a network location to store the data. On each File and Print Server we will create a directory named UserData and share it as UserData$. In the properties for the share set the Caching option to "Automatic Caching for Documents." This will cause commonly used files to be cached on the user's desktops to minimize network bandwidth and then automatically synchronize to the network on a regular basis. Then we create four new Group Policy Objects attached to each department's OU as follows:

FolderRedirection – IT
FolderRedirection – S&M
FolderRedirection – HR/Finance
FolderRedirection – R&D

Inside each new group policy object, we will navigate to **User Configuration/ Windows Settings/ Folder Redirection**. The way we are setup, we are able to use the 'Basic Redirection' option. We could also determine location based on groups as well. Under 'Folder Redirection', we select the 'My Documents' folder and open the Properties box. Within here, we select "Basic – Redirect everyone's folder to the same location" option. For the 'Target folder location', we input the following paths:

S&M	\\FAPSRV\UserData$\%username%
R&D	\\RFAPSRV\UserData$\%username%
HR/Finance	\\FAPSRV\UserData$\%username%
IT	\\FAPSRV\UserData$\%username%

This will cause the users 'My Documents' folder to be created under a folder that mimics the username. We will perform the same modifications for the 'Application Data' policy. This will cause all user data that is stored in either the 'My Documents' folder or in the 'Application Data' folder to be moved to a network location where it will remain. We can then include this location in the backup plan, thereby removing the need to backup each individual workstation.

Additional Group Policy – IP Security Implementation

Because of the sensitivity of the data within the HR/Finance systems and the value of the fortunes that are developed by the R&D department, it is necessary to secure access to the data. On the servers, we can lock down access by implementing NTFS permissions that limit access to only those who require access. This is a common practice and does not require extensive discussion. But, regardless of the efforts taken to secure data that is stored on the servers, in a default configuration, the data is transmitted over the wire in an unsecured way. All data is effectively clear text. With Windows 2000, Microsoft has provided the option of implementing IP Security to secure the data as it is transmitted on the wire. To do this, we will create custom policies and assign them to the servers and clients that deal with the sensitive network data. Since all of the data that the S&M department has access to is considered open information, it is not necessary to implement an IP Security policy for the S&M department. For the HR/Finance department, the personnel data and accounting data is considered crucial to the operations of the company and should be protected with IP Security. The fortunes that are generated by the R&D department are considered corporate secrets. Management wants this data protected in all media as best as is possible.

With this in mind, we need to implement an IP Security policy for communications between clients and some of the servers. The servers that contain the sensitive data are:

File and Print – FAPSRV, RFAPSRV

SQL – SQLSRV, RSQLSRV

To accommodate the application of IP Security polices through group policy, these servers will be placed in a different OU (Secure Servers) and a separate GPO will be applied to them.

To setup the IP Security rules, we will need to create two different Group Policy Objects: Client IP Security Settings and Server IP Security Settings. In the Client IP Security Settings policy, we will create a new IP Security Policy that will mimic the setup of the default Client (Response Only) rule. This is being done because it is recommended in Q232817 that this be done to avoid problems with duplicate GUID numbers in backing up and restoring policies (Fossen, 2000). This policy will then be linked to the R&D and HR/Finance OU. The Server IP Security Settings policy will be created the same as the Client policy with the only difference being that the new IP Security Policy will mimic the Server (Request Security) rule. This will cause any users that attempt to attach to these servers with the default response rule enabled to establish a secured connection. Therefore, any R&D or HR/Finance personnel that connect to these servers will establish a secure connection, but S&M or IT personnel who attach to the servers will not utilize IP Security. Since all users connect to the File and Print servers, but not all of them have information that requires IP Security to be enabled, the decision was made to not require IP Security for all connections, thereby minimizing the overhead on the File and Print servers. Additionally, IP Security offload network cards will be installed in the servers that are protected to help minimize the impact on processor time.

Additional Security – Roaming Profiles

You are probably wondering why I would classify Roaming Profiles as additional security. First, let me summarize my definition of security: the controlled access to data. Most people place the emphasis on the word controlled and I agree that control is a very important part of security. But the other part of my definition is "access to data." Yes, you have great control of data if the wrong people cannot gain access, but what about the right people? The data needs to be available to the personnel that require access to the data to perform their duties. Therefore, a key part of security is access to the data for the appropriate personnel.

With that being said, Roaming Profiles are a key part of access for users on GIAC Enterprises network. In Windows 2000, the profile is the repository for user data that is critical for accessing the tools they use to do their job. Above, we defined rules for separating the My Documents and Application Data from the profile. This was done so that rules could be put into place for allowing for Offline Files on this data. The features of a Roaming Profile already synchronize data and this method conflicts with the method used by Offline Files Synchronization Manager. (Moskowitz, 2001) Therefore, on each of the File Servers, we will create another directory named UserProfiles and share it as Profiles$. For the Caching properties for the share, set it to "Disallow Caching for Files of Any Type." Upon creation of each user, the appropriate file server will be specified for the profile path as follows:

\\FAPSRV\Profiles$\%username%
\\RFAPSRV\Profiles$\%username%

This will cause a folder to be created for each person to which they will be granted the necessary NTFS access. This will cause the profile that is created for each person to be stored on the network servers where they will be backed up and available for restore in the event of a company wide disaster. For those users that do not log into the same computer each day, their profile will follow them from computer to computer so they are presented with a common interface that they are familiar with. In the event of a hard drive failure in client machine, a user could sit down at another machine and get everything back the way it was before the crash except for any changes that had occurred since the last synchronization. This helps reduce the support burden on the limited IT staff since there is a means to restore a user to full functionality rapidly. Effectively, each workstation is little more than a dumb terminal as far as storing critical information, but you get the functionality of the computer performing all of the processing instead of offloading it to the server. If the IT staff employs RIS or some other means of deploying images to desktops, new images could be distributed and user settings restored in a rapid manner.

Additional Security – ISA Server Configuration

One of the requirements set out by GIAC management was to allow auditable Internet access for employees that are based in the Tampa office. With this in mind, a Microsoft Internet Security and Acceleration 2000 Server has been installed. Microsoft ISA Server is the latest version of Proxy Server. It incorporates the functionality of Microsoft Proxy and adds additional functionality that makes it a legitimate firewall. While the company already has a Cisco Pix firewall installed and management wants to continue to use that as their first line of defense and for controlling access to their IIS web servers, it is not the easiest means of auditing access by user or group. The Cisco PIX firewall has been configure to only allow outbound access by the ISA Server. The ISA server will provide the auditable access to the Internet that management requested. Microsoft ISA Server integrates with Active Directory and Windows 2000 groups. It also provides ample logging to meet the needs of management. The system will be setup as follows:

Access will be controlled by group membership
All access will be logged to files on disk
Log files will be imported into the SQL Servers on off hours

The ISA server is setup to deny access by default. Additional rules will be created that allow members of specified groups access to the Internet. At current, management does not want to place any limits on the access if the user is in the Tampa location. Therefore, initially there will only be one rule necessary for allowing web browsing. That rule will allow members of the group ISA_InternetAccess to have unrestricted web surfing. A protocol rule will be created that allows all IP traffic. Management will then need to examine the usage and determine if they wish to limit the usage of certain protocols like instant messaging and audio or video streaming. The protocol rules can then be modified to meet the needs as necessary. For any protocols, other than those that go through the web proxy, to work the firewall client will need to be installed on the clients since the Cisco PIX will only allow outbound access from the ISA Server. This client can either be installed on each client manually or pushed out by Group Policy as a Software Installation task.

We will enable logging on the ISA server and have it send data to file instead of direct ODBC logging. This is being done due to performance considerations on the recommendations of Tom & Deb Schinder in their book Configuring ISA Server 2000. (Schinder, 2000) The added overhead of the ODBC logging on both the ISA Server and on the SQL Server could cause a significant impact on the conduct of business. With the functionality provided by Microsoft SQL Server 2000 Data Transformation Services (DTS), we do not need to log directly through ODBC. Instead, we will log data to disk and then nightly, in off-production hours, we will use DTS to import the data into the SQL Database.

To create the DTS package, we will open SQL Enterprise Manager. We will create a new database for the ISA logs and use the scripts provided by Microsoft on the ISA Server 2000 CD to create the three tables that are necessary for the ISA logs. We will then create three DTS packages. We will

need to take an example of each logfile and name each a known name. In our case will name them IPPD.log, FWSD.log, and WEBD.log. We chose these names because it defines which log file we are dealing with as well as the log file format. We have chosen to use the ISA logfile format since it logs all fields, even if empty. It makes it easier for making the DTS package. Within each of the three packages we created, we will establish a connection to the SQL server with the ISA database as the default database. We will then define a text file as the source of the data and point each of the packages to a different source file. Then we create a transformation object from the text file to the database. In the transformation, we need to map the columns of the text file to the columns in the tables. For the cacheinfo column, a little modification is necessary. The table that is provided by Microsoft defines the cacheinfo column as a type Integer, but the text file has a hexadecimal number in this column. To facilitate the import of this data, a conversion of the data from hexadecimal to decimal integer is required. Once each package is created, save the package as a Local Package on the SQL server. Now you can create a fourth package that will be a driver for the other three. In this new package, you only need to add an ActiveX object to the package and then put the code that is provided in Appendix A into it. You should then save this package with a name like “ISA Log Import Driver.” This package can then be scheduled to run on a regular basis (daily) and all ISA logs will be imported into the SQL server database.

Once the data is in the database, reports can be created and published through a variety of methods included Access, Excel, and HTML. Managers can run the necessary reports on each user to see what access they have been using. The reports can then be used as the basis for removing non-business related protocols in problem cases.

Conclusion

We set out to design a secure implementation of Active Directory for GIAC Enterprises. The owner had a number of objectives that he wanted to be met. We will now restate those objectives and explain how we met them.

Objective	Met by
Minimize the chance of information leakage both internal and external	The implementation of a firewall and a proxy server minimizes the chance of leakage of data to the outside world. There is no wireless option implemented at current due to security implications. Internal information leakage is minimize with the application of IP Security to sensitive data, proper application of NTFS permissions on files and folders, and disabling unused ports to prevent the stealthy installation of data collection devices.
Provide standard desktop to all user minimizing the ability to customize	All client systems are installed from a standard image. Group Policy removes the ability for the users to customize but does not limit IT staff from troubleshooting any problems. Also, the use of Roaming Profiles and redirected Application and User data allows users to change machines on a regular basis and maintaining their standard environment.
User will not necessary sit at the same computer each shift	The use of Roaming Profiles and Application and User data redirection fulfill this requirement.
Allow for 2 designated individuals in each office to be able to administer sites	The implementation of groups with delegated authority to administer each OU and Unit Admin OU's that block policy inheritance will allow personnel to be designated as administrators. Membership in an OU is not necessary to administer the OU. Only membership in the group is necessary to administer OU resources. Additionally, if problems arise with Group Policy objects, the OUAdmins groups can be added to the list of groups that are denied access to Apply

	Group Policy Objects.
Owner wishes to limit access for overall control w/o having to deny Domain Admin level access to administrators	Since the design includes an empty root domain, user can be made Domain Admin of any of the sub-domains without having access to any other domain. Only a Domain Admin in the root domain can affect membership in the Enterprise Admin group by default. This will limit the need to give full administrative access to anyone that the owner does not want to grant the access.
Auditable Internet access for employees based in the home office	The implementation of an ISA Server and setting the Cisco PIX firewall to only allow the ISA Server out effectively restricts access to the Internet to those who are granted access through the ISA Server. Management can determine who should have Internet access and their user accounts can be made members of the ISA_InternetAccess group. Initially, only members of the Tampa site will be granted this access.

After reviewing the management requirements, we have met all of them. Additionally, we have implemented a secure Active Directory designed that allows for the flexible expansion of the company. Administration of users, computers, and printers can be easily delegated to Unit Administrators. This should allow GIAC Enterprises to grow and expand their market leadership in the fortune cookie business.

References

Riley, Steve “Using IP Security to Lock Down a Server” URL: http://www.microsoft.com/serviceproviders/columns/using_IP Security.asp (Aug 28 2001)

Minasi, Mark “Mastering Windows 2000 Server 3rd Edition” Sybex Inc. 2001

Moskowitz, Jeremy “Windows 2000 Group Policy, Profiles, and IntelliMirror” Sybex Inc. 2001

Scambray, Joel & McClure, Stuart “Hacking Windows 2000 Exposed” Osborne/McGraw Hill 2001

Schinder, Tom & Schinder, Deb “Configuring ISA Server 2000: Building Firewalls for Windows 2000” Syngress Publishing 2001

Additional sources of information not specifically reference in this document

Windows and .NET Magazine, Security Administrator, NSA Security Documentation, Hacking Exposed 3rd Edition, Microsoft Technet, Microsoft Resource Kit Documentation, and others.

Appendix A

Script used to drive the import of ISA log files into SQL 2000 Server using DTS

```
'**********************************************************************
'  Visual Basic ActiveX Script
'**********************************************************************
Function Main()
  DTSGlobalVariables("gvCurrentDate").Value = Date
  Dim fileRoot, currentDate, archivepath
  currentdate = DTSGlobalVariables("gvCurrentDate").Value
  fileRoot = DTSGlobalVariables("gvFilePathRoot").Value
  archivepath = fileroot & "\archive\"
  Dim strWebLog, strIPPLog, strFWSLog
  strWebLog = GetFileName ("WEBD", currentDate)
  strIPPLog = GetFileName ("IPPD", currentDate)
  strFWSLog = GetFileName ("FWSD", currentDate)
  Dim oFSO
  Set oFSO = CreateObject("Scripting.FileSystemObject")
  If (oFSO Is Nothing) Then
    'FileSystemObject had a problem opening
    Main = DTSTaskExecResult_Failure
    Exit Function
  End If
  Dim logFolderFiles, file
  Set logFolder = oFSO.GetFolder (fileRoot)
  For Each file In logFolder.Files
    Dim orgFile
    Select Case Left(file.Name, 4)
      Case "IPPD"
        orgFile = file.Name
        If orgFile = strIPPLog Then
        Else
          file.Name = "IPPD.Log"
          If runImportIPPD Then
            file.Name = orgFile
            file.Move archivePath
          End If
        End If
      Case "WEBD"
        orgFile = file.Name
        If orgFile = strWebLog Then
        Else
          file.Name = "WEBD.Log"
          If runImportWEBD Then
```

```
            file.Name = orgFile
            file.Move archivePath
          End If
        End If
      Case "FWSD"
        orgFile = file.Name
        If orgFile = strFWSLog Then
        Else
          file.Name = "FWSD.Log"
          If runImportFWSD Then
            file.Name = orgFile
            file.Move archivePath
          End If
        End If
    End Select
  Next
  Main = DTSTaskExecResult_Success
End Function

Function runImportIPPD
  On Error Resume Next
  runImportIPPD = False
  Dim oPackage
  Set oPackage = CreateObject("DTS.Package")
  oPackage.LoadFromSQLServer
"SMSSRV01","","","256",,,,"ISALogImportIPPD"
  If err.number = 0 Then
    oPackage.Execute
    If err.number = 0 Then runImportIPPD = True
  End If
  'Cleanup
  oPackage.Uninitialize()
  Set oPackage = nothing
End Function

Function runImportWEBD
  On Error Resume Next
  runImportWEBD = False
  Dim oPackage
  Set oPackage = CreateObject("DTS.Package")
  oPackage.LoadFromSQLServer
"SMSSRV01","","","256",,,,"ISALogImportWEBD"
  If err.number = 0 Then
    oPackage.Execute
    If err.number = 0 Then runImportWEBD = True
  End If
```

```
  'Cleanup
  oPackage.Uninitialize()
  Set oPackage = nothing
End Function

Function runImportFWSD
  On Error Resume Next
  runImportFWSD = False
  Dim oPackage
  Set oPackage = CreateObject("DTS.Package")
  oPackage.LoadFromSQLServer
"SMSSRV01","","","256",,,,"ISALogImportFWSD"
  If err.number = 0 Then
    oPackage.Execute
    If err.number = 0 Then runImportFWSD = True
  End If
  'Cleanup
  oPackage.Uninitialize()
  Set oPackage = nothing
End Function

Function GetFileName (logType,currentdate)
  Dim longDateString : longDateString = ""
  longDateString = longDateString & Year(currentdate)
  If Month(currentdate) < 10 Then longDateString = longDateString & "0"
  longDateString = longDateString & Month(currentdate)
  If Day(currentdate) < 10 Then longDateString = longDateString & "0"
  longDateString = longDateString & Day(currentdate)
  GetFileName = logType & longDateString & ".log"
End Function
```