Global Information Assurance Certification Paper

SECURING A FORTUNE

(Or how I designed a secure Windows 2000 Infrastructure for GIAC Enterprises)

Securing Windows GCNT Practical Assignment
Version 3.0, Option 1

Marc Westbrock
December 18, 2001

INTRODUCTION

GIAC Enterprises is one of the three leading providers of fortune cookie sayings. They have been providing the most interesting fortunes for years, but were slow to change. Having been around for a while, the owner was pretty set in his ways – "It's worked this way before, why not now?" His son has followed in his footsteps, but has kept up with the latest and greatest technologies and the power of the Internet, and finally 3 years ago convinced his father to enter the online world of e-business. They created a domain name, giacfortunes.com, and had their ISP host the web server.

Thanks to the son's idea, the company has grown to be a powerful online sales force, but their internal network infrastructure is still lacking. The current infrastructure is based on Windows NT 4.0 servers, with a mix of Windows 95 and 98 workstations, and only a couple of NT boxes. The Technology Services(TechSvc) department has been around for ages, and can do basic support, but are not up to speed on security and virus protection, much less installing patches and fixes. Their infrastructure was laid out wherever there was room, not making much use of a large room in the back. Each department had their own server, usually set up in an empty cubicle in their area, and the R&D group had one additional server for testing.

In early 2001, two things happened to change the direction of the company. First, the owner had a mild heart attack, and decided to retire and let his son run the business. Second, the dotcom fallout had started, and GIAC Enterprises' main e-business competitor, fortunes-r-us.com, was having difficulties with massive layoffs and the latest round of viruses. Even though they had the best-of-the-best software and computers, their IS department had been mostly laid off, and Code Red and NIMDA made it in. This decimated their network, leaving them with one functional server, and no web presence. Being located in the same city, GIAC Enterprises was quick to look at the bright side, and proposed a takeover. Fortunes-R-Us agreed, and I was brought in to create a new, secure, Windows 2000-based infrastructure to merge and update the two companies.

In the merger, all of the software owned by Fortunes-R-Us transferred to GIAC Enterprises. Being a dotcom company, they had all the best – 6 Compaq ML370 servers (only one up and running), 6 licenses for Windows 2000 Server, SQL Server 2000, Cisco routers and switches, and top-of-the line workstations, all running Windows 2000 Pro. Lotus Notes R5 was their e-mail client.

NETWORK DESIGN

To create a secure Windows 2000 network, it was decided to replace all NT servers with Windows 2000 servers, merge some departments onto shared resources, and rearrange departments so the Finance, Human Resources, Sales, and Marketing departments from both companies moved to the GIAC location. The R&D Department moved to the old Fortunes-R-Us location, connected to headquarters by a T1 line and Cisco 3640 routers at both ends. The website was brought in-house, onto a Windows 2000 Server running IIS 5.0, and set up behind a Cisco PIX 515 in a DMZ. ISP Internet access goes through another Cisco 3640. All servers were moved into the unused back room, and the door was fitted with a Proximity cardlock so only TechSvc staff have access. Racks were set up to secure the servers even further, especially the DMZ components - the PIX box, IIS server, and SMTP/DNS server. (Figure 1)

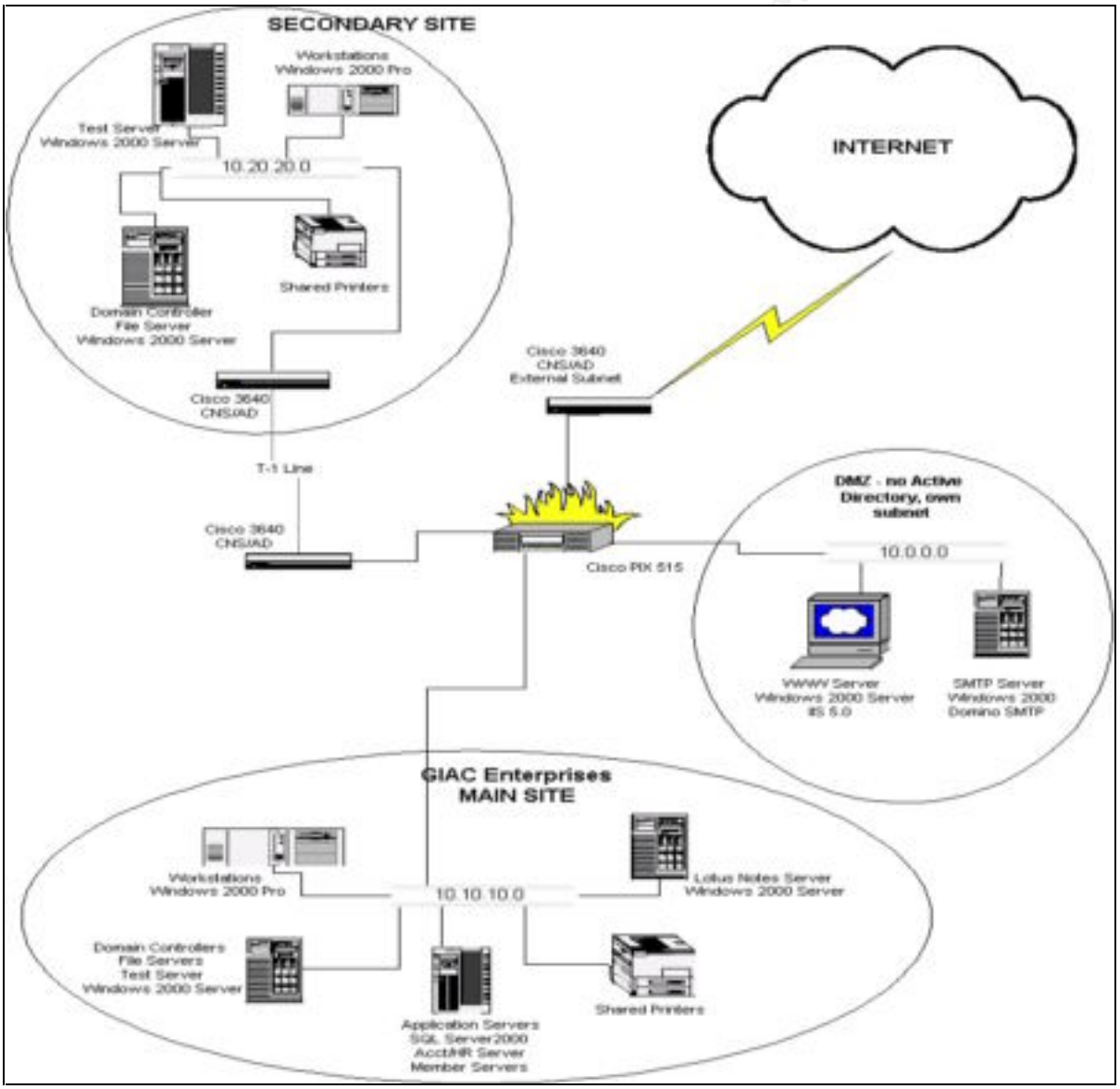

Fig. 1

The new infrastructure includes the following:

- 1 Lotus Notes member server at the main location.
- 1 IIS 5.0 server at the main location, and 1 SMTP/DNS mail routing server on the DMZ subnet. Both standalone, not included in AD layout.
- 2 file servers at the main location, as shown. Both are Domain Controllers.
- 2 Application servers, one running SQL Server 2000 for the Sales and Marketing database, and one running the Accounting and Human Resources programs. These are member servers, not DCs.
- 1 file server at the secondary (R&D) location. This is a Domain Controller.
- 2 test servers, one at each location. R&D checks their fortunes before going live, and TechSvc uses the other to test patches, fixes, etc. before applying to production servers.
- Shared printers as needed in each department.
- 2 Cisco 3640 routers connecting the 2 offices over a T1 line, and another Cisco 3640 connecting to the ISP for all Internet functions.

All servers are Compaq ML370 rackmounts, with 512MB RAM and a minimum of 3 SCSI drives in a RAID5 array. 2 additional drives are on the shelf for immediate hotswap replacement. 2 Intel NICs with IPSec offload capabilities are in each server, going to separate Cisco switches for redundancy. They are running Windows 2000 Server, with Service Pack 2 and the latest hotfixes.

All workstations are upgraded to Windows 2000 Pro to make full use of Active Directory and Group Policy (as described later). The chosen software is MS Office 2000 Professional and Lotus Notes R5 for email.

ACTIVE DIRECTORY DESIGN

Since these two companies were merging, and changing over to Windows 2000 Server, it was decided to do a mirrored migration. This would take care of any inconsistencies from the original NT network, and allow us to basically start from scratch, utilizing the best components of both networks. First, the 5 unused servers would have Windows 2000 Server installed. We would create the new forest and Active Directory structure, then move users over one by one to the new Windows 2000 domain. Once some of the other servers were freed up, those would be wiped out and built anew, as 2000 servers.

We will use the "empty root" approach to creating our Active Directory structure. This allows for future growth, and for ease of administration of the Schema. The root domain is giacfortunes.com, and the child domain is corp.giacfortunes.com. Explicit trusts will be set up between the old NT domains and the new 2000 domains until the migration is complete, then they will be deleted. Please note that the IIS web server is not included in the domain structure, since it will be on its own subnet in the DMZ and not part of any domain or forest. The Enterprise Admins and Schema Admins groups are created in the root domain and will not have any members assigned.

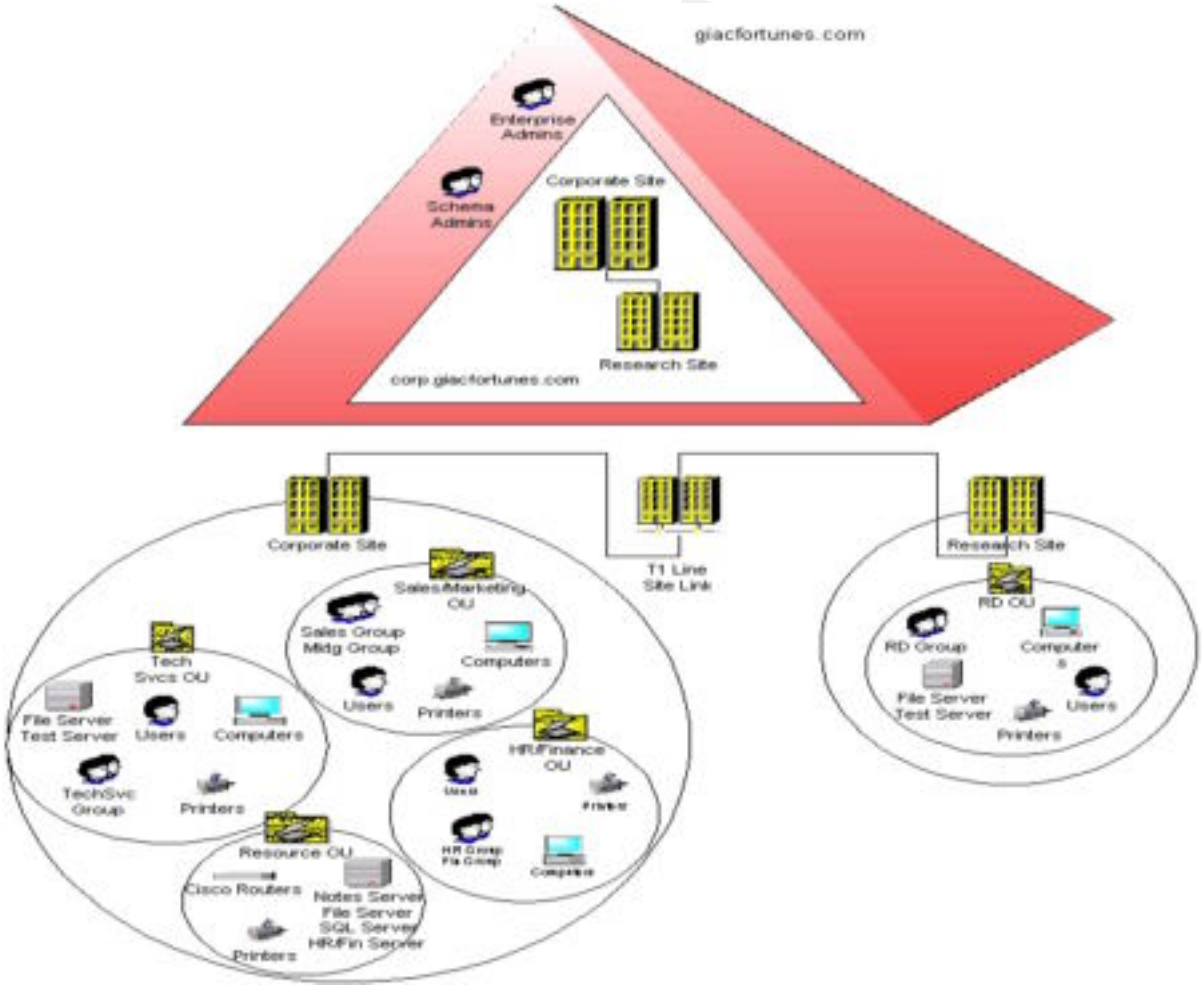

Fig. 2

Organizational Units
Each department will belong to an Organizational Unit (OU) within the domain. These OUs will hold a mixture of users, groups, computers, printers, and shared folders. There will also be a Resource OU to hold those resources that are shared among all departments. Following is a breakdown of the OUs created, and their specific components, within the corp.giacfortunes.com domain:

Research & Development OU	Users	Groups	Printers	Computers	File Server	Test Server
Sales & Marketing OU	Users	Groups	Printers	Computers		
HR & Finance OU	Users	Groups	Printers	Computers		
Tech Services OU	Users	Groups	Printers	Computers	File Server	Test Server
Resource OU	Printers	Notes Server	File Server	SQL Server	HR/Finance App Server	Cisco Routers

Note that the Sales & Marketing OU and the HR & Finance OU do not have file servers within them, and that their App servers are also located in the Resource OU. This is because they will be sharing a file server, and at different times other departments will need access to the application servers. Placing them all in the Resource OU also makes it easier for the TechSvc group to manage them, and control access with Group Policy. The three Cisco 3640 routers are running Cisco Networking Service for Active Directory (CNS/AD) and are also located in the Resources domain for administrative reasons.

The Tech Services OU has it own file server for holding images, program install files, and system administration utilities that we don't want others to have access to, and a test server for patches and upgrades. The Research & Development OU will need to administer its own file server and test server, and will be at their own site, so those servers were placed in that OU instead of the Resource OU. There is also a Domain Controllers OU that is built-in, and provides access to the Default Domain Controllers Policy that we will discuss later.

Configuring the Active Directory Replication
Since there will be at least one Domain Controller at each location, we will set the Active Directory to replicate between the two "sites." To configure this, we will need the "Active Directory Sites and Services" MMC snap-in. The first site has a default name of "Default-First-Site-Name" and will be changed to "Corporate." The second site is added by right-clicking Sites>New>Site and naming it "Research", and telling it which DC is at that site. (Fig. 3) Then click on Inter-Site Transports, right-click IP, and select New>Site Link. Name the link "T1 Line" and check that Corporate and Research show as the servers to link. Click OK. (Fig. 4)

To adjust the scheduling of the replication, we right-click on the "T1 Line" transport we just created and select Properties. The cost can stay as shown, and for the small amount of AD changes we will be making daily, the replication can stay at 180 minutes. To prevent replication from causing slowdowns during peak login traffic, click the

Change Schedule button, highlight the “8am to 9am” column and click “Replication Not Available”. Click OK twice.

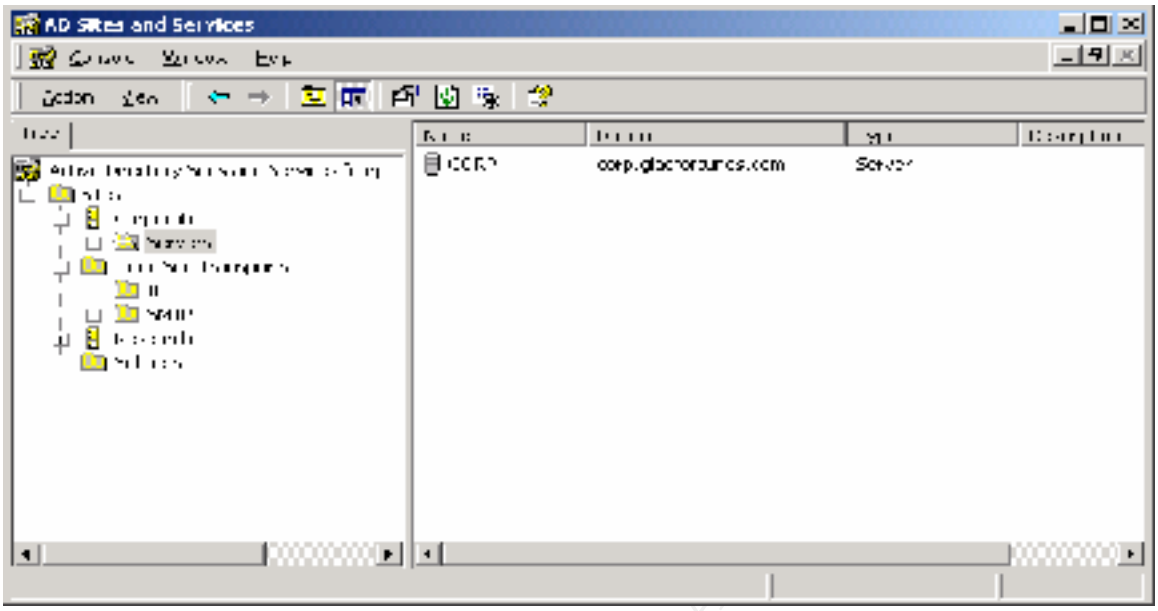

Fig. 3

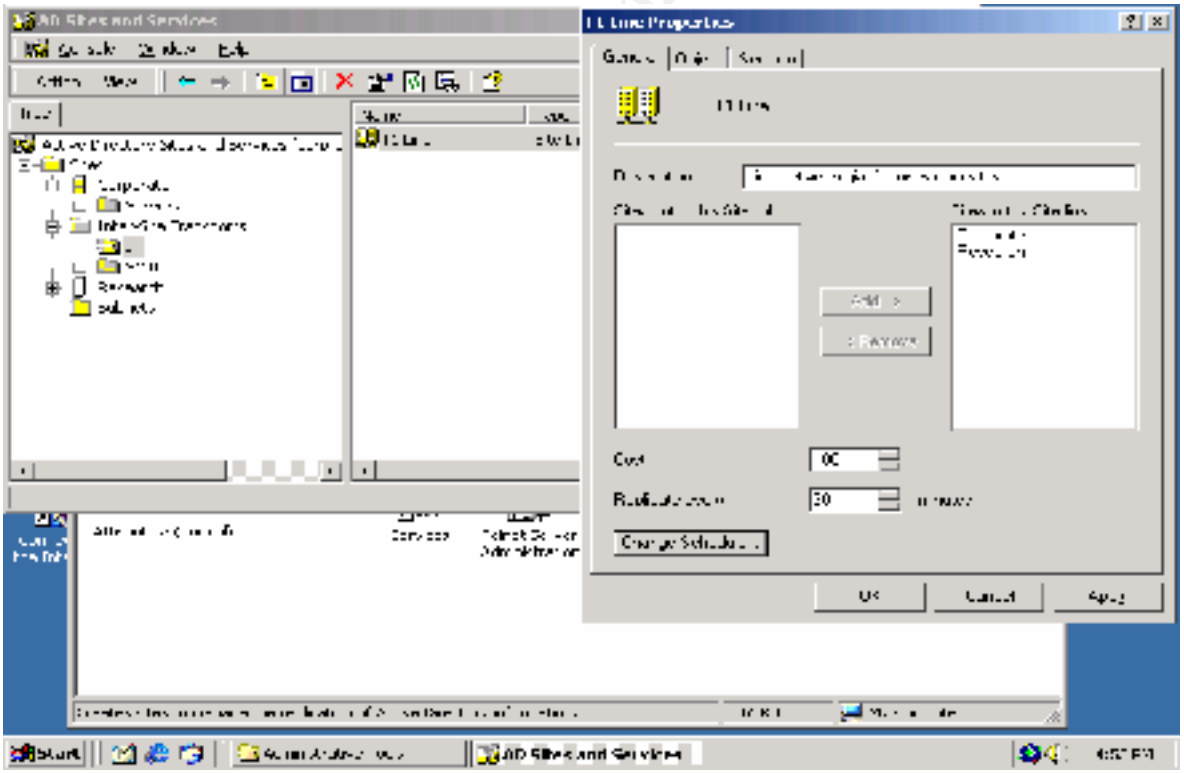

Fig. 4

Finally, to optimize various network functions so that computers and servers in a site look locally instead of over the WAN for each other, each site needs to be associated

with its subnet. This is done in the Subnets area under the “Active Directory Sites and Services” snap-in. (Fig. 5)

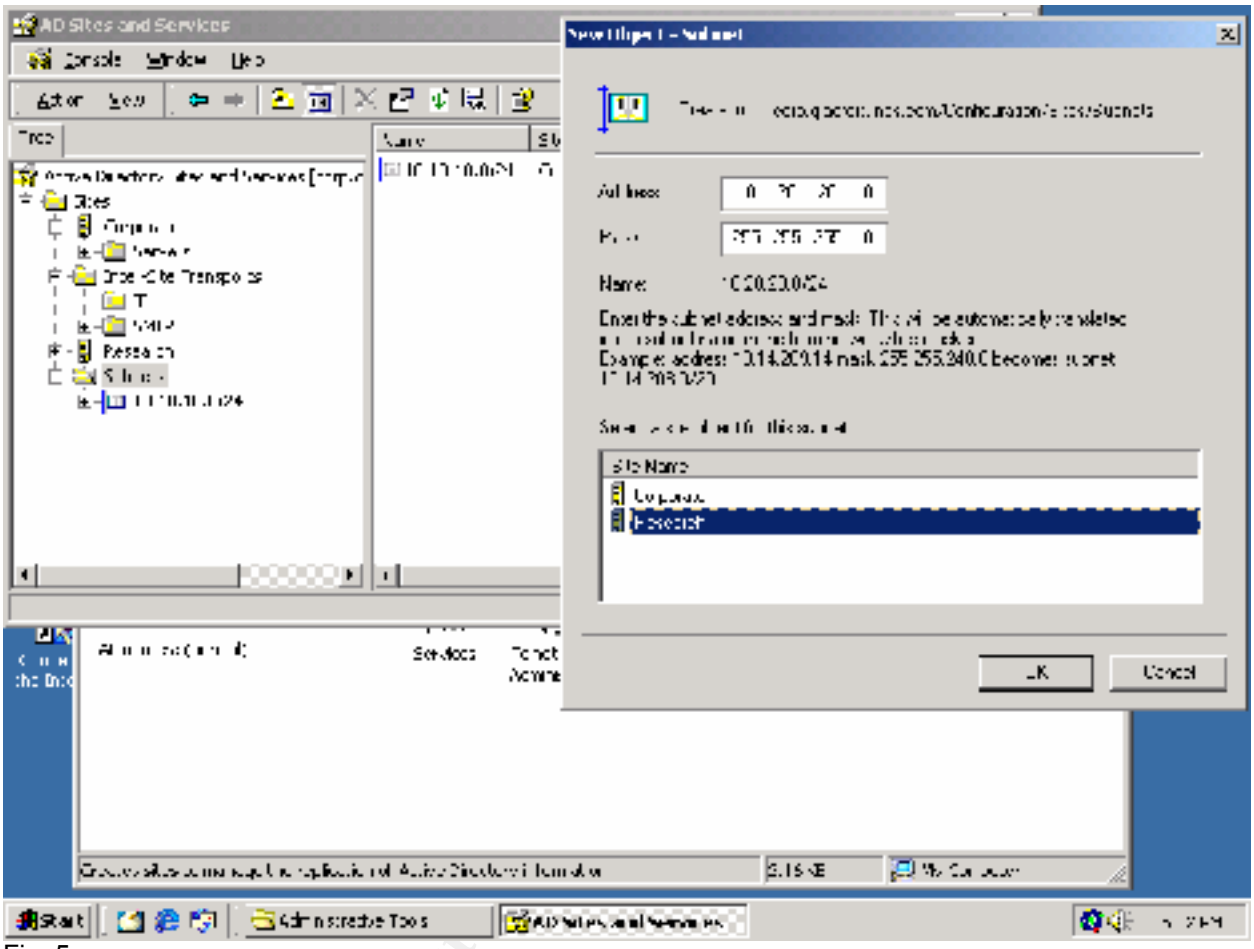

Fig. 5

We had to use the RPC-over-IP transport because both sites were part of the same domain. However, that would have been our first choice because we have a fast, reliable dedicated T1 line connecting the two sites, and RPC-over-IP is the best transport to use. If we had a slow, unreliable link and were in different domains, we would have used the SMTP transport instead.

There are many other settings within the Sites and Services Snap-in that can be used to further fine-tune replication. For now we will leave these as default, but if slow-downs occur frequently these settings may change.

GROUP POLICY AND SECURITY

The core of Windows 2000 security is Group Policy. With hundreds of security settings available, and the multiple levels of security needed in any company, it could get confusing fast, and often did in NT 4.0. However, Group Policy Objects (GPOs) make creating and applying security policies simple. Every computer or user in a GPO will be reconfigured as designated by that GPO, no matter how large your network is. Laptops, desktops, temp users, dial-up users, Administrators, all are affected when a Group Policy is applied to them.

Windows NT 4 had approximately 70 policies that you could set. Windows 2000 has around 550. The biggest advantage to Group Policy over NT4 System Policies is that the changes to the client workstation are not "tattooed" as they were in the NT4 days. "Tattooing" is Microsoft techno-slang for a permanent or persistent change. So when a user logs off (or the policy no longer applies), the "non-persistent" settings are wiped off. (Moskowitz, Windows 2000 Group Policy, Profiles, and Intellimirror, p. xvii)

Group Policy does not just affect basic settings like password preferences, etc., but also allows you to set group memberships, install applications, assign scripts for logon and logoff, auditing of files and folders, and even modify the registry! Plus much, much more.

Group Policy is broken into 2 sections. First is the Computer Configuration, which is applied to a computer when it boots up, and is the same no matter who sits at that computer. These settings do not follow you. For example, if you have a computer in a public place, you can have every file accessed audited, whether previous logons are cached to prevent unauthorized users from using the system without accessing the network, and whether the last user name is displayed in the logon screen. Computers not receiving that GPO can be more open, because access to the computer is already restricted to company staff only.

The second section is User Configuration. This applies to users whenever they log into the network, no matter what computer they are logged in at. The policy follows the user. You can have a temp employee who is limited to a certain printer, cannot change the background or screensaver, and cannot access the Internet. However, when that user logs off and you go log on, you can access everything that you could before.

You can create separate policies for Sites, Domains, and Organizational Units which will apply to all users and objects within those areas. If there is more than one GPO that applies, then they will follow an order of precedence as follows: (Fossen, 5.1-Windows 2000 Active Directory & Group Policy, p.123)

1. NT 4.0 System Policy
2. Local GPOs (stored locally, not in Active Directory)
3. Site GPOs
4. Domain GPOs
5. Organizational Unit GPOs (in nested order)

Since we are migrating to an all-Windows 2000 network, NT4 System Policies won't apply to our scenario. Local GPOs only apply to the computer where they are created, and since the Web Server and the SMTP/DNS server are not in Active Directory, each will have a local GPO. We have 2 Sites, but will not utilize Site GPOs because all objects at each location are in specific OUs also, so will get those policies applied. If we had multiple GPOs tied to a specific container, then we could specify the order that they are applied on the Group Policy tab on the Properties sheet of that container. So we will start with the Default Domain Policy, a built-in Group Policy.

Default Domain Policy

This policy covers every server and computer in the domain, including the Domain Controllers. The DC policy is applied after the Domain Policy, so changes shown here will apply to the Domain Controllers unless overwritten by an explicit entry in the Default Domain Controllers Policy.

The default Domain Policy can be accessed through the Active Directory Users and Computers Snap-in. Right-click on the domain (corp.giacfortunes.com) and choose Properties, then Group Policy. (Fig. 6) Click on Edit to begin configuration of the Default Domain Policy.

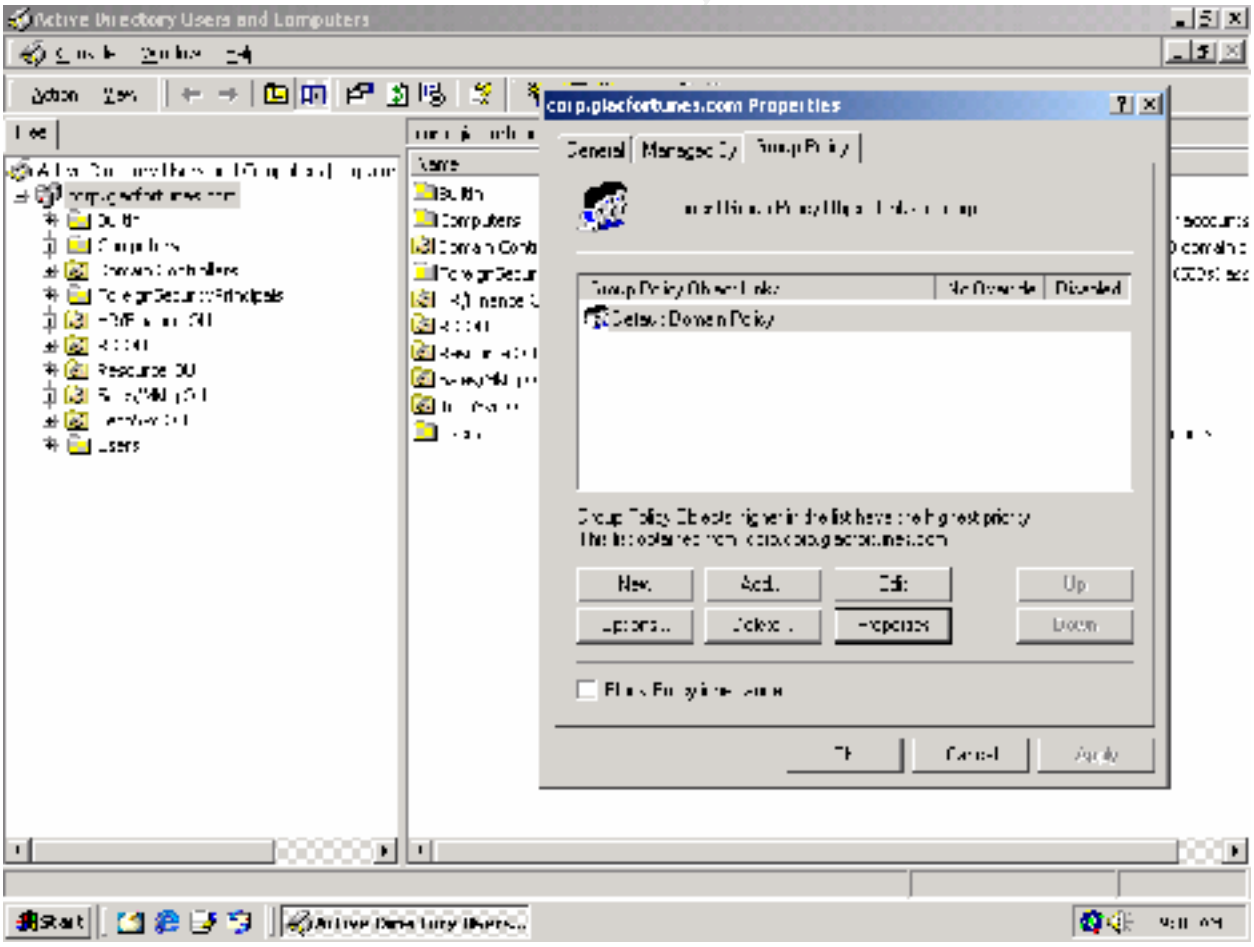

Fig. 6

We will not be showing the settings for every variable in the GPO, but will focus on the major entries or those we changed from default. First we will focus on the Computer Configuration section of the policy, then the User Configuration.

Computer Configuration

Software Settings>Software installation

Software Installation helps you specify how applications are installed and maintained within your organization. (MMC Help for Software Installation). We will not be using Group Policy to control automatic installation of software, so this section will be skipped.

Windows Settings>Scripts

In the Computer Configuration section, you can set Startup and Shutdown scripts to run each time a computer that receives the policy start or exits Windows 2000. We have no scripts that need to be used on any computers.

Windows Settings>Security Settings>Account Policies>Password Policy

Enforce password history	9 passwords remembered
Maximum password age	90 days
Minimum password age	5 days
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store passwords using reversible encryption…	Disabled

By remembering the last 9 passwords, users cannot keep using the same one or two passwords over and over again. They are required to change their passwords every 90 days, which helps cut down on trouble calls from users who don't change and get locked out, or forget what they changed it to, yet still keeps a level of security. The minimum password age of 5 days helps prevent users from changing their password 8 times in a row, to get back to the same password they used before. If they tried that, it would take them 45 days (9 remembered, x 5 days between changes) before they got back to the original password. By setting the password length to 8 characters minimum and having them meet complexity requirements (mix upper and lower case, use characters) makes the passwords more difficult to crack. Lastly, since we are not using Digest Authentication, we do not want to store passwords using reversible encryption.

Windows Settings>Security Settings>Account Policies>Account Lockout Policy

Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

After 3 invalid logon attempts, the user account will be locked for 30 minutes, then released. This allows users who recently changed their password a few tries to remember the new one, but if they get locked out and can't find an administrator to unlock them, they can still get back in after 30 minutes. If they enter the wrong password twice, then stop and wait for 30 minutes, the lockout counter is reset to 0 invalid logon attempts, giving them 3 more tries. Either way, after 30 minutes a user can get back in. This is a long enough delay, however, to deter most hackers who are trying to guess passwords, since they can only try 3 at a time before being locked out.

Windows Settings>Security Settings>Local Policies>Audit Policy

Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined (is for DC's only)
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Not Defined
Audit system events	Success, Failure

By enabling the auditing of account logons, you can see who has been trying to log in who may not have the rights, or a reason to, get onto the system. We are also auditing user or group accounts that have been created, renamed, deleted, or changed in any way. System events such as shutdowns and startups, access to the directory service, and changes to policy (user rights, audit policies) are also monitored.

Some of the audits are not required for member servers and computers, but unless there are log file space limitations, we will leave them turned on. Remember though, just enabling auditing does not mean that all files and objects WILL be audited. You still need to enable auditing on each and every object (registry keys and entries, files, folders, etc) that you want to log, so file size and items actually audited can be controlled that way.

Windows Settings>Security Settings>Local Policies>User Rights Assignment
(not all are shown, only important settings or those changed from default)

Access this computer from the network	Domain Users, Administrators
Add workstations to domain	(none)
Backup files and directories	Backup Operators
Change the system time	Administrators
Deny access to this computer from the network	(none)
Force shutdown from a remote system	Not Defined
Log on as a service	(none)
Manage auditing and security log	Administrator
Restore files and directories	Backup Operators
Shut down the system	Administrators, Authenticated Users
Take ownership of files or other objects	Administrators

Administrators and Domain Users are the only ones able to access this computer from the network for support reasons. No users can add workstations to a domain except for through Domain Controllers (configured later). 'Force shutdown from a remote system' is not defined here, it will be defined in the other policies. Both Administrators and Authenticated Users can shut down the systems when local to them. No user has the ability to 'Log On as a Service,' because this would give them full control of the system.

Only Administrators should be allowed to change the system time because it is important to Kerberos security that all times be synchronized (within tolerances). Audits would be difficult to follow from object to object without accurate times, and AD

synchronization between sites would fail. Also, only allow the Administrator to manage auditing and security logs, since others with this right could clear the logs to cover their tracks during attacks or illegal activity.

We gave the Backup Operators group rights to both 'Backup files and directories' and 'Restore files and directories.' If you need higher security, it is recommended to create a second group called Restore Operators and to separate the powers between the two. Make sure the same user is not listed in both groups because this defeats the purpose of creating separate groups. By doing this, we prevent giving one person the complete rights to read, copy, and restore files, which would allow them to get copies of private data, or to backup a virus or corrupt file and restore it over a good one, infecting or crashing your servers or corrupting your data.

Windows Settings>Security Settings>Local Policies>Security Options
(not all settings are shown)

Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (when possible)	Enabled
Do not display last user name in logon screen	Disabled
LAN Manager Authentication level	Send NTLMv2 response only/refuse LM & NTLM
Message text for users attempting to log on	This computer and all programs and data accessed therein are the sole property of GIAC Enterprises (giacfortunes.com). Any unauthorized or illegal use of these systems is punishable to the fullest extent of the law. By continuing past this point, you are signaling your acceptance of these terms of use.
Message title for users attempting to log on	READ CAREFULLY!
Number of previous logons to cache	3 logons
Recover Console: Allow automatic administrative logon	Disabled
Rename administrator account	Change name and description *
Rename guest account	Change name, leave disabled *
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Enabled

With so many topics to cover, I will break this down into a few paragraphs, loosely grouped. First, by settings additional restrictions for anonymous connections, we make sure that no user that accesses the network as a Null User can get more rights than explicitly set. Digitally sign client and server communication (when possible) allows for security of transmissions between servers and clients when supported by both ends. Unsecured transmissions can still occur with computers incapable of SMB signing, but

signatures will be used whenever possible. We also have enabled Secure Channel digital encryption and signatures (when possible) using strong session keys. This creates secure transmissions between servers to help prevent passwords, etc. from being stolen. Since we are one domain once the migration is complete, this will not have any interoperability issues.

Once we convert, every server and workstation will be Windows 2000, so we will only accept NTLMv2 authentication. This setting will be set at "Set NTLMv2 response only" until the migration is complete, then changed to "refuse LM & NTLM". The last user name can be displayed on the logon screen since most of the computers affected by this Domain policy are workstations assigned to specific users, and this helps ease-of-use. Other policies may change that setting (e.g. Domain Controllers). Also, when users do attempt to log on, they will receive a standard company message about unauthorized use. The last 3 logons will be cached in case a domain controller cannot be found, so the user can still access their local files.

Since the Administrator (and Guest) accounts are renamed, it is more difficult for someone to guess what name and password to use. This setting only applies to the Domain Admin account when set at the domain level, so this policy will cover all Administrator accounts. We used a name that follows our standard, a fake first-initial-last-name that we made up. The description for the renamed Administrator account was changed, and the renamed Guest account was left disabled so even if it was discovered, it could not be used. A new account was created with no rights and everything audited, and named Administrator with the same description as the original Administrator account, so we could watch for unauthorized attempts to access that account.

Windows Settings>Security Settings>Event Log>Settings for Event Logs

Maximum Application (System) log size	5MB
Maximum security log size	10MB
Restrict guest access to (app/security/system) log	Enabled
Retain Application/System log	15 days
Retain security log	15 days
Retention method for Application/System log	Overwrite as needed
Retention method for Security log	Overwrite as needed
Shut down the computer when the security audit log is full	Disabled

The Application and System logs are set the same: No Guest access, 5MB in size, retain for 15 days, and overwrite as needed. These two files do not grow as quickly as the Security log with the settings we have chosen. 15 days makes sure the data is covered by at least 2 weekly backups.

The Security log is set for 10MB due to all of the auditing we are doing. These settings will change drastically for the Domain Controllers, but the workstations and member servers do not require as much room. Retaining the log for 15 days makes sure the data is covered by at least 2 weekly backups. Finally, the system is not configured to shut down when the security log is full, since the log will overwrite itself as needed and will

never fill up. This setting changes for the Domain Controllers, since those are usually the targets of hacker attacks.

All server logs will be reviewed, archived, or cleared once a week to look for anything strange. Settings may change if unusual entries start to appear.

Windows Settings>IP Security Policies on Active Directory
IPSec will not be enabled on the internal network.

Administrative Templates>System>Group Policy

Group Policy refresh interval for computers	90 minutes
Group Policy refresh interval for domain controllers	5 minutes

The only Administrative Template settings we will enable are the refresh intervals, using their default settings. Every 90 minutes, even if a user bypasses or modifies a security setting, it will be re-enabled. If you make a change to Group Policy, every user will receive that change within 90 minutes if logged on, and automatically the next time they log on if not currently networked. This time interval is cut to 5 minutes for domain controllers, because of the importance of security on them.

That completes the Computer Configuration section. Since all of the users are in the same domain, we will also apply the majority of the standard User Configuration settings with the default Domain policy. Those settings will be modified where required by the OU GPOs that will apply later.

User Configuration
There are very few user settings to make – most of the major security is applied through the Computer Configuration section. The defaults will be left except as follows:

Administrative Templates>Windows Components>Internet Explorer

Disable Internet Connection Wizard	Enabled
Do not allows AutoComplete to save passwords	Enabled

Administrative Templates>Windows Components>Internet Explorer>Internet Control Panel

Disable the Content page	Enabled
Disable the Connections page	Enabled

By disabling the Connection Wizard and the Connections page, users cannot change what proxy server they are configured for. They also cannot have IE dial out through a local modem, bypassing proxy limitations and logs. Web access rights will be controlled by the proxy server itself. By disabling the Content page, users cannot change site ratings, or add or modify certificates that you have installed. Lastly, by not having AutoComplete save passwords, that is one less file that hackers can attempt to access to try to find out users' passwords, or if someone sits at another employee's desk, they cannot easily access secured web sites with pre-existing account information.

Administrative Templates>Start Menu & Taskbar

Disable and remove links to Windows Update	Enable
Add Logoff to the Start Menu	Enable
Disable personalized menus	Enable

Windows Update installs files and changes settings that we might not want changed, it is better if we test any updates first, then apply them ourselves to each station. Adding Logoff to the Start Menu makes it easier for users to access, and disabling personalized menus cuts down on the number of users who call for support because their "programs keep disappearing".

Administrative Templates>Control Panel>Display

Hide Screen Saver Tab	Enabled
Activate Screen Saver	Enabled
Screen Saver executable name	Enabled, thisone.scr
Password protect the screen saver	Enabled
Screen Saver timeout	Enabled, 1800 seconds (30 min)

Thanks to the Privacy Act and corporate standards, all stations are required to have a screen saver enabled, to have it password protected, and to activate in 30 minutes or less. By locking down all of these settings, we know that policy is being followed. If a user walks away from their machine for a shorter period of time and wants to lock their system from prying eyes, they have been instructed how to use CTRL-ALT-DEL/Lock Computer.

We also have set the screen saver to a specific one, to prevent users from loading their own screensavers, etc. We have also found that some screensavers interfere with background processing, or can lock up the system in the right circumstances. The screensaver chosen is a basic screensaver, tested with our programs, to prevent conflicts and lockups.

Administrative Templates>System>Group Policy

Group Policy refresh interval for users	Enabled, 90 minutes

This will reapply the User Configuration section of Group Policy every 90 minutes.

That concludes the User Configuration section, and the complete Default Domain Policy. Next we will look at the policies for the different Organizational Units, beginning with the Domain Controllers OU and the built-in Default Domain Controllers Policy. All settings in the next OU sections will be added on top of (or modify) the Domain GPO, so only settings that are very important or different will be covered.

Default Domain Controllers Policy

The default Domain Controllers Security Policy is applied after the Domain GPO for all Domain Controllers, no matter what OU they are placed in. To access the Default Domain Controllers Policy, right-click on Domain Controllers, choose Properties, then the Group Policy tab. Since we are setting the policy for the DCs themselves, we will

click on Properties, then check the box to Disable User Configuration settings. This will make processing of this policy faster.

Also, since some of the Domain Controllers are in other OUs besides the Domain Controller OU, we want to make sure that those policies don't overwrite the ones we expressly set. To prevent this, we click Options, then check the box for No Override. (Fig. 7) This prevents other GPOs set later from overwriting/replacing the settings made here.

If we were troubleshooting why multiple GPOs seem to be conflicting, we can check the other box (Disabled: the Group Policy Object is not applied to this container) and re-enable the GPOs one by one, to see where the problem occurs. This is especially handy if you have multiple policy objects linked to the same OU.

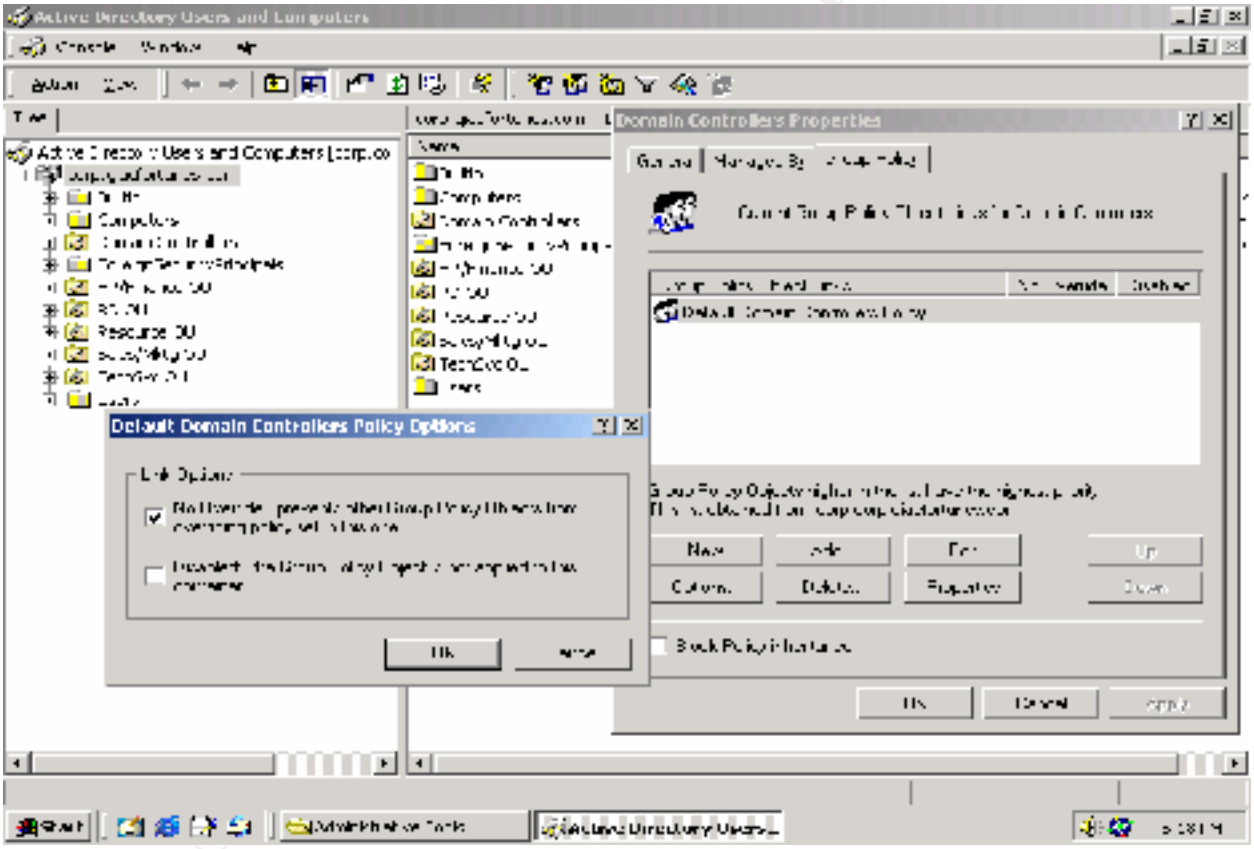

Fig. 7

We want the Domain Controllers to be very secure, because access to one of them can allow a hacker or user to make changes to the whole domain. We will not be changing all of the settings from default, but will show the settings that we chose for the major security topics, going from the top of the list down. Click on Edit to see the Group Policy screen. All of the following are found under Computer Configuration. Items in gray are different than the default Domain policy. However, all settings shown will be made to the DC policy, in case the default Domain policy changes in the future. This helps prevent

those changes from affecting the Domain Controllers unless specifically applied in this policy.

Windows Settings>Security Settings>Account Policies>Password Policy

Enforce password history	9 passwords remembered
Maximum password age	90 days
Minimum password age	5 days
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store passwords using reversible encryption…	Disabled

These settings remain the same as those for the default Domain Policy.

Windows Settings>Security Settings>Account Policies>Account Lockout Policy

Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

These settings remain the same as those for the default Domain Policy.

Windows Settings>Security Settings>Local Policies>Audit Policy

Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Not Defined
Audit system events	Success, Failure

Being a Domain Controller, you want to be aware of any changes that are made and by whom. The only difference with these settings is that Directory Service audits are for Domain Controllers only. Therefore, they are defined here. By auditing directory service access, we can see who is attempting or making changes to the Active Directory service. Remember, auditing still needs to be enabled for each object being audited before information will be logged. It is good practice to enable auditing on all system folders and important folders and files on Domain Controllers so you have more information available if your systems are compromised.

Windows Settings>Security Settings>Local Policies>User Rights Assignment
(not all are shown, only important settings or those changed from default)

Access this computer from the network	Domain Users
Add workstations to domain	Administrators
Backup files and directories	Backup Operators
Change the system time	Administrators
Deny access to this computer from the network	Administrators
Force shutdown from a remote system	(remove all)
Manage auditing and security log	Administrator
Restore files and directories	Backup Operators

Shut down the system	Administrators
Take ownership of files or other objects	Administrators

By denying Administrators access to this computer over the network, we are forcing them to be sitting at the computer to make major changes. This may seem a disadvantage to the administrators, but with all servers in a secure location, if the servers can be accessed over the network, then the physical security can be bypassed. However, even if a hacker steals an administrator account, they cannot do major damage to the comain controllers or the Active Directory. We also remove the ability to shut the domain controller down from a remote location, you must be physically there.

Only Administrators should be allowed to change the system time for the reasons mentioned in the default Domain policy. Also, only allow the Administrator to manage the logs, since others with this right could clear the logs to cover their tracks during attacks or illegal activity.

Windows Settings>Security Settings>Local Policies>Security Options
(not all settings are shown)

Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Allow server operators to schedule tasks	Disabled
Audit use of Backup and Restore Privilege	Enabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (when possible)	Enabled
Do not display last user name in logon screen	Enabled
LAN Manager Authentication level	Send NTLMv2 response only/refuse LM & NTLM
Number of previous logons to cache	0 logons
Recover Console: Allow automatic administrative logon	Disabled
Restrict CD-ROM (and floppy) access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Enabled
Shut down system immediately if unable to log security audits	Enabled

By auditing the use of the backup and restore privilege we can see who is “reading” files on the machine. Note that having this enabled will generate very large logs, so we planned accordingly in the Event Logs section later.

Digitally sign client and server communication (when possible) allows for security of transmissions between servers and clients when supported by both ends. Unsecured transmissions can still occur with computers incapable of SMB signing, but signatures will be used whenever possible. We also have enabled Secure Channel digital

encryption and signatures when possible using strong session keys. This creates secure transmissions between servers to help prevent passwords, etc. from being stolen. Since we are one domain once the migration is complete, this will not have any interoperability issues.

Since every server and workstation will be Windows 2000, we will only accept NTLMv2 authentication. As mentioned in the Domain Policy, this setting will be set at "Set NTLMv2 response only" until the migration is complete, then changed to "refuse LM & NTLM". To prevent anyone from trying to log in with previous usernames, we have set policy to not display the last logon name, and to not cache any previous logons. This way, you must know the correct Administrator logon name and password, it cannot be bypassed. Since the Administrator (and Guest) accounts are renamed in the Default Domain Policy (previously) it is more difficult for someone to guess what name and password to use.

Since the Administrators can only log onto the server locally (set in the User Rights section), we set the CD-Rom and floppy access to the locally logged-on user only. This way, if an administrative disk or CD is left in the drive, it cannot be used over the network by unauthorized personnel.

Finally, we have set policy to shut the system down immediately if it is unable to log security audits. The negative side of this is that the logs should be made as large as possible, and if the log fills up without an Administrator there to clear it, the server will shut itself down. This can be prevented by the Event Log settings we will discuss next.

Windows Settings>Security Settings>Event Log>Settings for Event Logs

Maximum Application (System) log size	5MB
Maximum security log size	500MB
Restrict guest access to (app/security/system) log	Enabled
Retain Application/System log	15 days
Retain security log	15 days
Retention method for Application/System log	Overwrite as needed
Retention method for Security log	Do not overwrite events
Shut down the computer when the security audit log is full	Enabled

The Application and System logs are set the same: No Guest access, 5MB in size, retain for 15 days, and overwrite as needed. These two files do not grow as quickly as the Security log with the settings we have chosen. 15 days makes sure the data is covered by at least 2 weekly backups.

The Security log is set so large (500MB) due to the logging of the Backup and Restore privilege, auditing of all logon events, not overwriting events, and the setting of Shut Down System Immediately if security log is full. The Security Log is set to 512KB by default, but it is recommended to expand the size as large as possible to prevent the system from shutting down in all but the most rare of circumstances. (SANS, Securing Windows 2000 Step-By-Step Guide, p.29) Setting it at 500MB gives us plenty of space

to compile log data on the all but the most intrusive attacks possible with our other policy settings.

If we would have the log set to overwrite events, and someone broke in, they could flush the log by sending repeating errors, overwriting any record of their break-in. In this case they could try that, but the DC would shut down, and the log would be intact when you brought it back up. Then you could see what caused the attack, how they got in, etc. Retaining the log for 15 days makes sure the data is covered by at least 2 weekly backups.

All logs will be reviewed, archived, or cleared once a week to look for anything strange.

The settings under User Configuration will not be used for the Default Domain Controllers Policy, and was disabled at the start of this section.

Site GPOs

We will not make use of Site GPOs since no OUs cover both sites, and all settings can be handled by the default Domain Policy, Domain Controllers Policy, or the separate OU Policies. Sites are only configured in this case for AD replication and network optimization.

Organizational Unit Policies

In our Active Directory structure, we created five OUs – Research & Development, Sales & Marketing, HR & Finance, TechSvcs, and a Resource OU for servers, printers, and routers. All of these OUs will already have the default Domain GPO applied, and all Domain Controllers have the default Domain Controllers Policy applied as shown above. The Domain GPO configured the settings at the minimum that would be required for the least-restrictive OUs, specifically the R&D and TechSvcs OUs. Therefore, those two OUs will not have additional GPOs created. The Resource OU has no users in it, only hardware, so it will use the Computer Configuration that was already created in both default GPOs.

This leaves us with 2 OUs that need additional restrictions. Since both units are made up of everyday users, with the same basic access needs, one Group Policy Object can be created and linked to both. This saves time and duplicate effort in administration. Another advantage to Group Policy is that you can create as many policies as you want, but they don't go into effect until they are linked to a site, domain, or OU. If you are currently using one GPO and wish to try some new settings, just unlink the original object, link to the new, and test. If there are unusual results, then switch back. Once the testing is done, then leave the OU linked to the new GPO and delete the old.

To work with an OU policy, just right-click on the OU, choose Properties, then Group Policy. You can create a New GPO by clicking New, then naming the object, or you can

Add a policy object that has already been created by clicking Add and choosing which object to link.(Fig. 8)

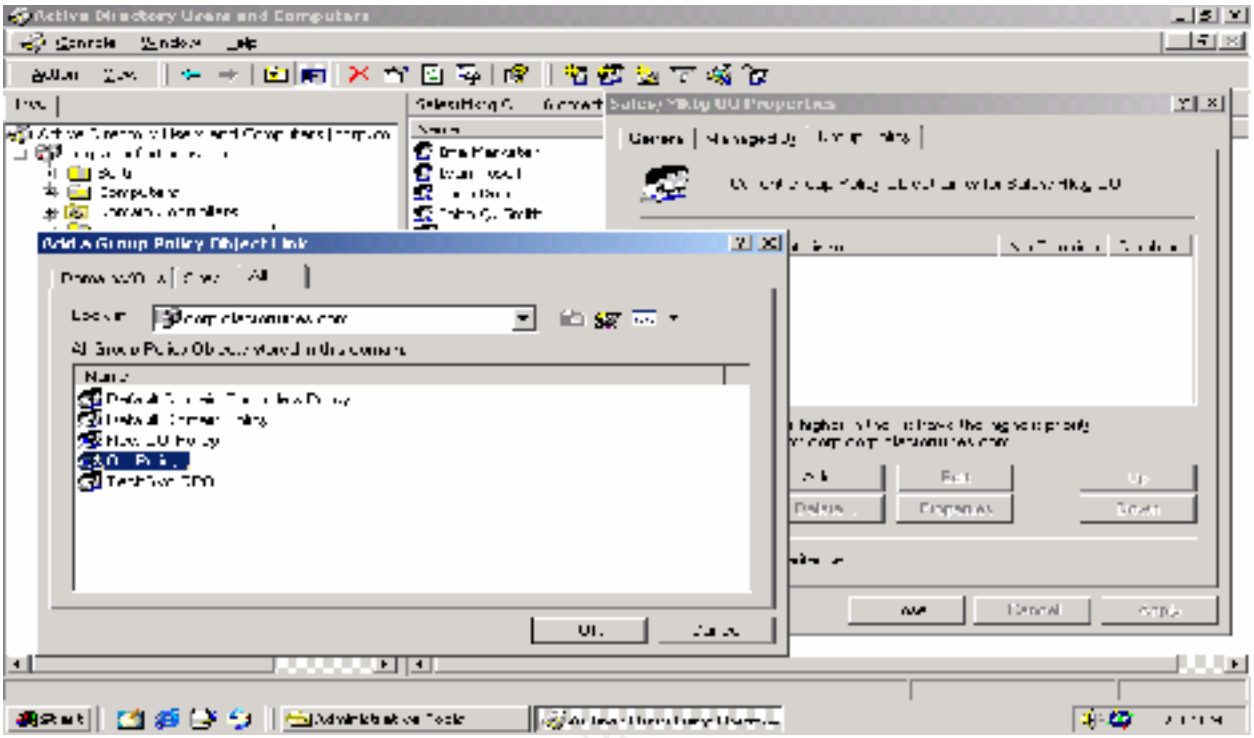

Fig. 8

Once the GPO is showing under the Current Group Policy Object Links section, it will be applied to that OU. (Fig. 9)

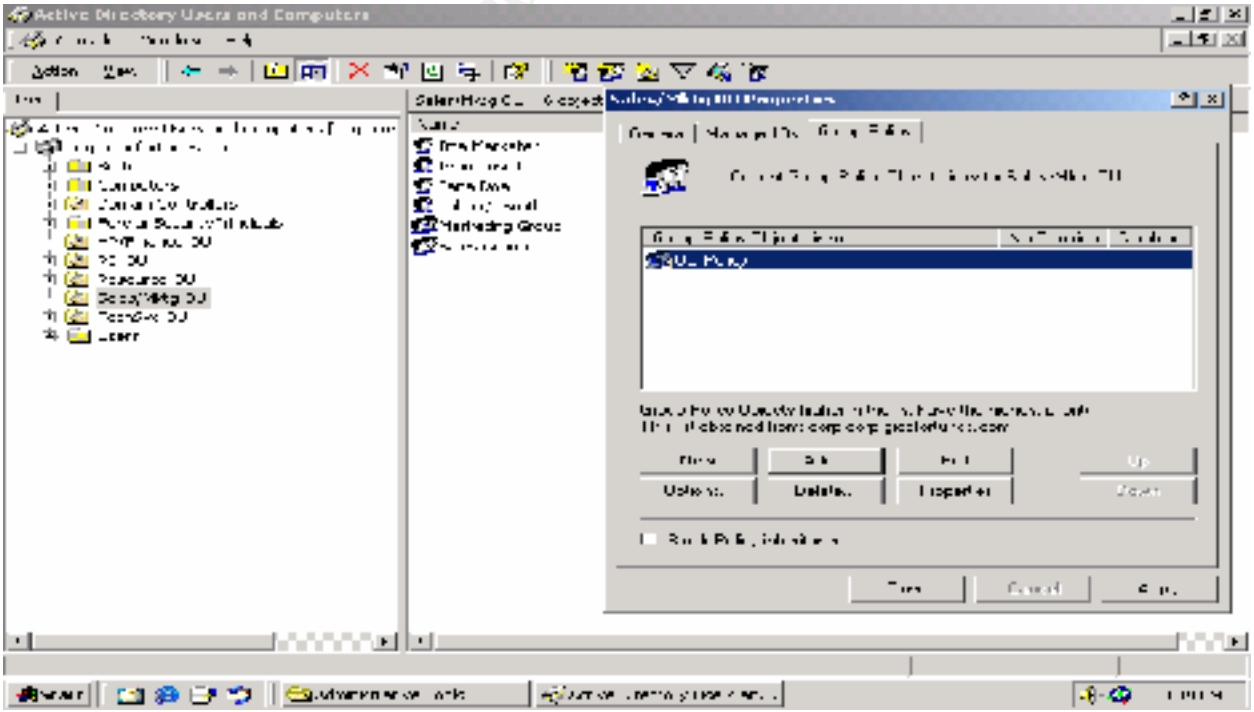

Fig. 9

You can also be more specific and set the GPO to only apply to certain users or groups within a domain, site, or OU. This is done under Properties, then choosing the Security tab. Only those groups or users with the Read and Apply Group Policy permissions will actually read and apply the settings. (Fig. 10)

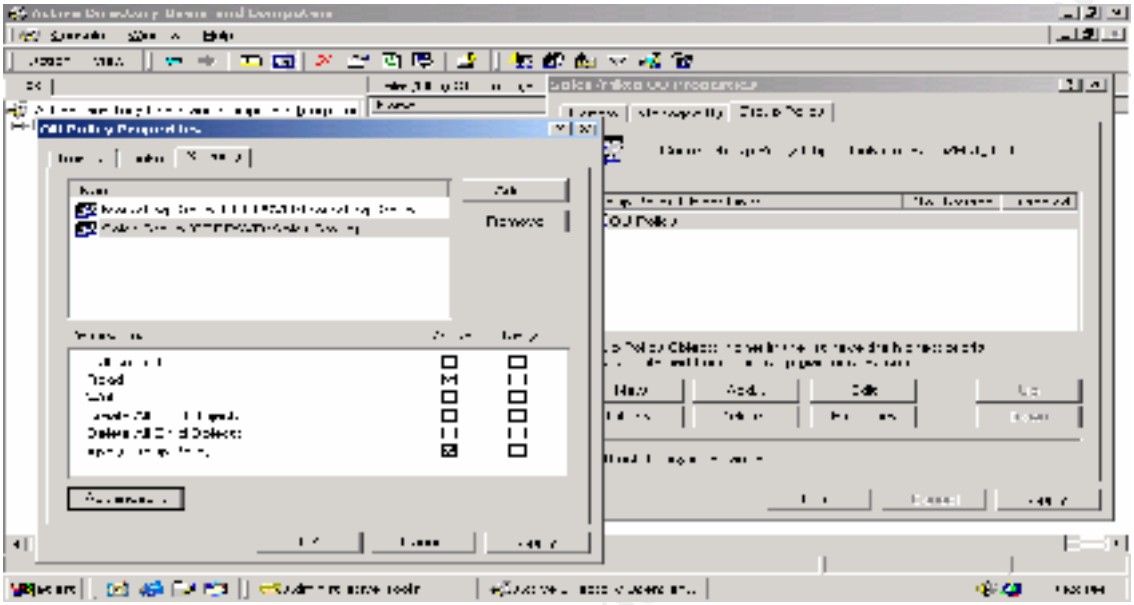

Fig. 10

Now that we have shown how we control who receives and processes the Group Policy Objects, we will show the OU Policy that was created for both the Sales & Marketing OU and the HR & Finance OU.

To create the new policy, click New, and name it Base OU Policy. Now, since this Policy is only going to be changing user settings, we will start by highlighting the name of the policy we just created, click Properties, and check Disable Computer Configuration Settings. This will help speed up the processing.

Next, click Edit. The Group Policy screen appears. All entries shown are under the User Configuration section of the chosen Policy. The settings shown are the changes or additions to the default Domain policy that is already applied.

Administrative Templates>Windows Components>NetMeeting
Since these two OUs do not need NetMeeting, and we don't want them using it without our knowledge, we can pretty much disable or prevent every aspect of the program. This way they won't be transferring files, or entering meetings on the Internet where they might open themselves and our network to attack.

Administrative Templates>Windows Components>Internet Explorer>Internet Control Panel

Disable the General page	Enabled
Disable the Security page	Enabled
Disable the Programs page	Enabled
Disable the Advanced page	Enabled

Since they will only be allowed general web browsing, all IE Properties pages will be disabled. The other two pages, Content and Connections, were disabled in the default Domain policy. Users with this policy can use the Internet, but cannot change their proxy settings, enable dialup access, or even where their temporary Internet files are stored and how long of history is kept. Their default web page is set to the corporate site, and cannot be modified through the Properties page.

Administrative Templates>Windows Components>Internet Explorer>Offline Pages

Disable channel user interface completely	Enabled

We do not want users receiving automatic Web site updates according to a channel provider's schedule. Since this takes place automatically, if one of those sites is hacked, damage could be done to our machines without any user knowledge until it is too late. The users receiving this policy only need to access specific Web sites for their daily business needs, so channels are not an option.

Administrative Templates>Windows Components>Internet Explorer>Browser menus
There is an option here to 'Disable Internet Options…menu option' that prevents users from accessing the Tools>Internet Options screen at all. This can be used to prevent users from even going to the Properties area of IE from within the program and can save some administration time (one setting instead of the 4 above for each page). However, this does NOT prevent users from modifying their settings by going to the Control Panel>Internet Options icon. Therefore, disabling each page is more secure. So no changes will be made to this section for our policy.

Administrative Templates>Windows Components>Microsoft Management Console

Restrict users to the explicitly permitted list of snap-ins	Enabled

These users do not need any access to the MMC or snap-ins, so the permitted list is blank, preventing use of MMC by anyone except TechSvcs or R&D staff.

Administrative Templates>Control Panel>Add/Remove Programs

Disable Add/Remove Programs	Enabled

Since all workstations will be imaged and software installed by the TechSvcs staff, we will disable this option in the Control Panel to hinder users from installing their own programs. This will not prevent them from running Setup in other ways, but it will stop most basic users from bringing games or software from home. When combined with the System setting of Disable Autoplay, they have to know how to start the install themselves.

Administrative Templates>System

Disable registry editing tools	Enabled
Disable AutoPlay	Enabled, on All Drives

Unauthorized users cannot make changes to the registry through regedit.exe and regedt32.exe, and AutoPlay on CDs and other drives is disabled, making it more difficult for novice users to install their own programs.

This concludes the configuration of Group Policy and security for the domain and OUs of corp.giacfortunes.com.

Other Security

One of the areas not covered in this paper is the DMZ. The settings to protect the Web Server and the SMTP/DNS Server from hackers, viruses, and trojan horses would take way too long to cover here. Suffice it to say that local policies will be created on each server, starting with the settings that can be installed using the hisecweb security template, and modified from there. Only required ports will be allowed access, from the Internet, through the PIX box, and onto the DMZ. Access will be controlled by the Cisco router, the PIX box, the local policy, IPSec settings, and finally with TCP/IP filtering that is built-in on the Intel network cards we are using.

If we were using IPSec policies internally, these could also be applied by Group Policy, but we didn't need that level of security since access to our internal network is screened so well. However, the TCP/IP filtering, if used, cannot be controlled by Group Policy and would need to be applied on a server-by-server basis.

CONCLUSION

Group Policy can accomplish a lot, but there are some things it cannot do. Users still need to be trained not to tell others their passwords, or use their anniversary or birthday, or write the password down on a sticky note. Administrator accounts need to be assigned long passwords, and changed frequently. If possible, third-party tools or add-ons should be used to allow the Administrator account to be locked out through intruder detection, to search the logs for unusual or unwanted activity, and to add a layer of Intrusion Detection that will notify you if anything funny is going on.

Administrative scripts also abound, and can do things not covered by Group Policy, such as make additional registry changes, dump log file data in different formats, change passwords, create users, and much more. Used wisely these can enhance your administrative powers.

Group Policy, when used correctly, is a very powerful tool that will help you manage and secure your network fairly easily. It can be used by itself, but when used in conjunction with other resources, you can virtually guarantee yourself a secure, stable network environment.

REFERENCES

Fossen, Jason. 5.1 Windows 2000 Active Directory & Group Policy. Version 5.0.2 SANS Institute, August 8, 2001

Fossen, Jason. 5.5 Windows 2000 Scripting and Security. Version 3.4. SANS Institute, August 22, 2001

Securing Windows 2000 Step-By-Step. Version 1.5. SANS Institute, July 1, 2001

Microsoft Windows 2000 Server Deployment Planning Guide. Redmond: Microsoft Press, 2000

McLean, Ian. Windows 2000 Security Little Black Book. Scottsdale: The Coriolis Group, LLC, 2000

Moskowitz, Jeremy. Windows 2000 Group Policy, Profiles, and Intellimirror. San Francisco: Sybex, 2001

Casad, Joe. Windows 2000 Active Directory – Network Professional's Library. Berkeley: Osborne/McGraw-Hill, 2001

Windows 2000 Server Resource Kit. Supplement 1. Redmond: Microsoft Press, 2001

Last Updated: July 28th, 2017

Upcoming Training

SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**