# Global Information Assurance Certification Paper

# SECURING WINDOWS 2000 FOR THE SMALL ENTERPRISE

**SECURING WINDOWS GCNT PRACTICAL ASSIGNMENT**

VERSION 3.0, OPTION 1



Carlin D. Carpenter
December 19, 2001

Introduction:

GIAC Enterprises sells fortune cookie sayings. Until recently they were an old line company with little on-line exposure. Twelve months ago, they made the strategic decision to move most of their processes to computer, and specifically to leverage the internet for their operations. GIAC Enterprises has its main office in New York City. The New York office has approximately 150 employees split among four departments:

- Research & Development (R&D)
- Sales & Marketing (SALES)
- Finance and Human Resources (FIN/HR)
- Information Technology (IT)

They also have a branch office in San Francisco that has approximately 30 employees. Mostly, they are the West Coast sales staff with 2 FIN/HR personnel and 2 IT personnel. Finally, the sales staff spends a significant amount of time on the road where they often need access to the firm's resources.

Both the R&D team and the FIN/HR team have sensitive data that should not be available to the other member of the organization. For the R&D team, this data is mostly trade secret information. As the fortune cookie saying industry is highly competitive, compromise of innovation data could prove devastating to GIAC Enterprises. FIN/HR's records contain private information about personnel that could expose the company to legal liability if it were compromised.

The firm did not have a coherent IT policy prior to this initiative. There were disparate workgroup networks, local managed and a few core services, namely web and mail. Leadership is committed to this new course for the company and is providing the necessary funding to baseline the network. All of the IT systems have been upgraded, standardized and networked. Since there is no legacy enterprise network to integrate, the decision was to implement a pure Windows 2000 solution. All workstations will be Windows 2000 SP2, and most servers will run Windows 2000 as well.

The president of the firm is especially interested in ensuring that the San Francisco office is included in the firm's advances. The West Coast operations have long been neglected by corporate, however, with a new Regional Vice President in place, they believe that they can quickly make significant gains in the region. They hope to double or triple the size of the West Coast office over the next several years.

Network Design:

In order to ensure security and access, the decision was made that all workstations and most servers would run the Windows 2000. The New York office will be connected to the Internet via a T1 and the San Diego office will use a 512Mbps symmetric DSL (SDSL) connection. These connections will provide Internet access as well as a VPN connection between the two sites. Mobile users will have commercial dial-up access to the Internet and from there to the VPN.

The New York office will use a CISCO PIX 515 firewall/VPN in conjunction with a CISCO 2500 series router. The San Francisco Office will use a CISCO PIX 506 firewall/VPN in conjunction with a CISCO 2500 series router. Mobile users will use CISCO Secure VPN Client software to allow them access through the firewalls. The 515 was chosen for the New York office in order to provide three interfaces: WAN, DMZ, protected. The 506 was selected as a less expensive alternative for the San Francisco office that did not require a DMZ.

The New York office will serve as the corporate data center. It will have two primary subnets, one fully protected and one DMZ. The DMZ will contain two servers, a web server running IIS 5 and a linux server acting as the public DNS server and the mail gateway. The IIS server will run Windows 2000 Server, SP2 with all hotfixes applied. The linux server will run Red Hat 7.1 with BIND 9.1.3 and qmail 1.03. The BIND server will be authoritative for GIAC Enterprises external services (www, ftp, mail) only. The ISP will provide a secondary DNS server for those addresses. qmail will act as a mail relay agent for the Exchange server. qmail is superior to sendmail for this task because qmail because of its smaller footprint, ease of configuration and the fact that it does have to run as root on the server.

Both boxes will have all unnecessary/unused services disabled or removed. Both machines will be configured with level 5 raids, dual power supplies, dual fans and be placed on uninterruptable power supplies for maximum reliability. The IIS server will not be part of the active directory architecture. As a single machine it should be easy enough to administer without the increased risk/headache of including it in the AD.

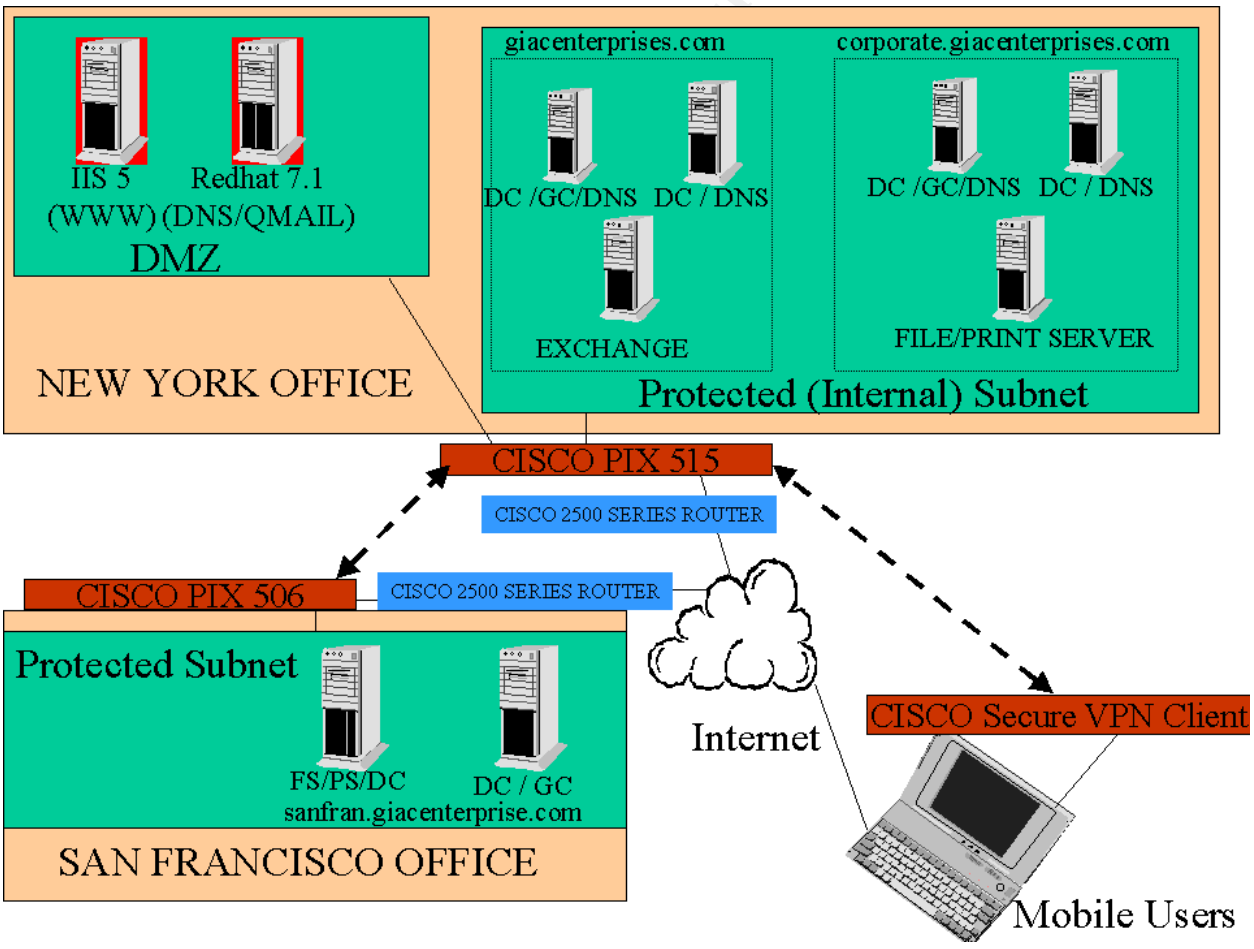
The firm has seen a significant amount of growth in its West Coast operations and is expecting that office to increase in size. The VP of West Coast operations was also concerned about a productivity loss if the VPN between the sites went down. Because of these two concerns, the decision was made that create two separate domains for the two sites. Both domains would be child domains of the giacenterprises.com domain.

The New York office (corporate.giacenterprises.com) will have two Domain Controllers that will also serve as internal Name Servers. One of these will also act a Global Catalog. The single corporate Exchange server will exist in New York. This decision

was made in order to simplify administration and reduce overall cost. The expected impact to San Francisco users is negligible. The firm will also maintain a centralized file and print server in the New York data center.

The San Francisco center (sanfran.giacenterprises.com) will have two servers, one will act as the DC/GC as well as an internal DNS server and one that will act as a DC/DNS as well as a file and print server. All servers will be configured with a level 5 raid, dual power supplies, dual fans and UPSs. Hard drives and power supplies will be hot-swappable. In addition all servers will be backed up to tape nightly. Desktop machines will not be backed up and users will be encouraged to store their files on the network.

All internal networks will be fully switchedh, full duplex 100 Mbps ethernet networks. In the New York data center the file/print server will have a 1 Gbps network adapter to the switch.



Active Directory Design:

As discussed earlier, there are two sites for GIAC Enterprises, one in New York and one in San Francisco. Although these two sites are fairly well connected, the decision was made to treat them as separate sites for system reliability concerns. Also remember that the machines sitting in the New York DMZ will not be part of the AD design.

The AD root domain will be giacenterprises.com. It will have two child domains, sanfran.giacenterprises.com and corporate.gaicenterprises.com. This geographical separation will facilitate organizational growth and it is a logical separation. The root domain will contain two domain controllers, one of which will act as a GC, the other will act as an Infrastructure Master, a Schema Master, and a Domain Naming Master.

As GIAC Enterprises is running a pure Windows 2000 environment (no NT 4 boxes in the network) all domain controllers will run in native mode vice mixed. Because there are no NT4 boxes in the network, there is no need for a PDC Emulator Master.

In each domain, whichever domain controller is not the GC will act as the RID Master and the Infrastructure master. This should prevent any condition of the Infrastructure master not detecting bad references.

Another advantage of breaking the network into three domains is that Group Policy Objects (GPOs) can be applied to Domains, Sites, and OUs. Conceivably this would have allowed for a single domain with New York and San Francisco being treated as Sites within the Domain. However, given the fact that the West Coast operations are expected to increase, there is the possibility that additional west coast satellite offices will open. By making each major office its own domain, smaller satellite offices under its cognizance can be identified by site and still allow establishment of GPO by business unit (West Coast vs. East Coast).

The other advantage three domains is that as the online presence grows, giacenterprises may wish to move the machines currently sitting in the DMZ to the AD. The giacenterprises.com root domain would be the ideal place for them to be inserted. Simply breaking the organization into two sites would have facilitated some of this, but would have required modification as the organization grew.

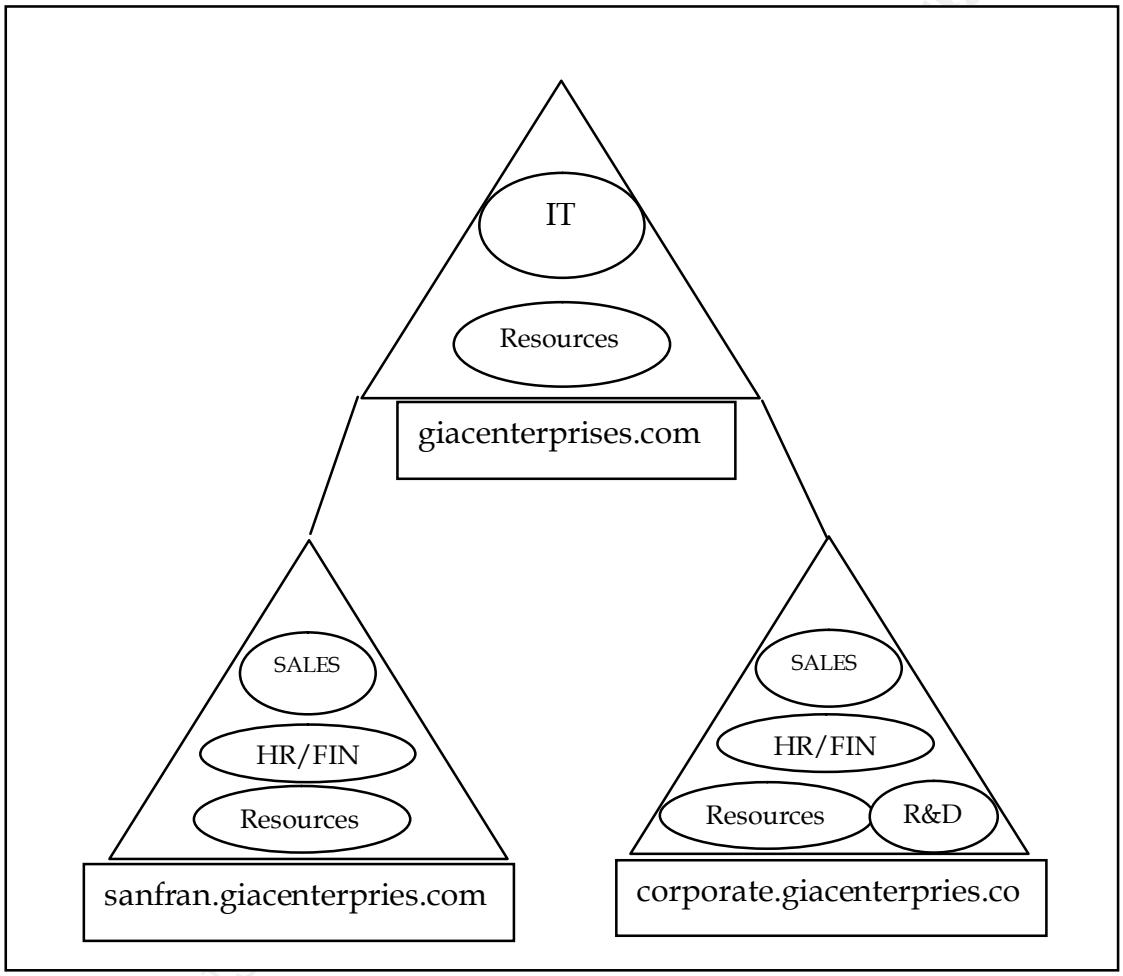
Organizational units will be broken down as follows:

-All IT personnel will be placed in an IT OU in the giacenterprises.com (root) domain.

-The the other three departments will have their own OUs in each of the other two domains.

-Each domain will have a Resource OU.

This organizational breakdown will have several advantages. First, it follows a logical break down of the organization. As each business unit has dedicated IT personnel assigned to support it, it allows specific IT personnel specific control over their realm of responsibility. Second, it is at a granular enough to allow specific control without being unnecessarily complicated.




Active directory layout

OU Contents by Domain:

**giacenterprises.com**

| **Resources** | **IT** |
|---|---|
| Exchange Server | IT Users |
| Domain Controllers | IT Groups |
| | IT Computers |
| | IT Printers |

**sanfran.giacenterprises.com**

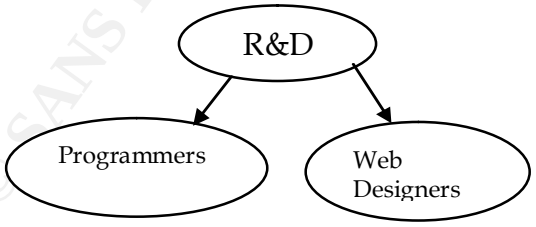
| Resources | SALES | FIN/HR |
|---|---|---|
| File/Print Server | Sales Users | FIN/HR Users |
| Domain Controllers | Sales Groups | FIN/HR Groups |
| | Sales Computers | FIN/HR Computers |
| | Sales Printers | FIN/HR Printers |
| | Sales Shared Folders | FIN/HR Shared Folder |

**corporate.giacenterprises.com**

| Resources | SALES | FIN/HR | R&D |
|---|---|---|---|
| File/Print Server | Sales Users | FIN/HR Users | R&D Users |
| Domain Controllers | Sales Groups | FIN/HR Groups | R&D Groups |
| | Sales Computers | FIN/HR Computers | R&D Computers |
| | Sales Printers | FIN/HR Printers | R&D Printers |
| | Sales Shared Folders | FIN/HR Shared Folder | R&D Shared Folders |
| | | | R&D Servers |

OUs maybe nested. That is, an OU can have a child OU that inherits its setting and then applies the child's settings on top of it. For example, if the R&D team had web design and programmers as two subsets, and the programmers required certain capabilities that we didn't want to open to all R&D, they could be placed in a child OU of the R&D OU.

Limited changes inside an OU could be accomplished using policy filtering, however that technique can be difficult to implement and tends not to scale well. Taking the above example another step, let's add that the web designers need access that we don't want the programmers or the rest of R&D to have either. Then by creating a child OU for each the web designers and the programmers, we can specify their capabilities specifically. In the end it would look like this:




Where the R&D GPO get applied to everyone who is part of the the R&D OU, and then the specific changes are made to the Programmers and Web Designers policies without changing the rest of the users.

Microsoft classifies OU models as either flat, narrow or deep. The determining factor is how many layers deep OU are nested. In our design, we are not currently implementing any nested OUs, therefore this design would be considered flat. A site

with OUs 1-2 deep would be considered flat. One with OUs 3-5 deep is narrow, and one with OUs more than 5 deep would be considered deep. (Olsen, "Windows 2000 – Active Directory Design & Deployment," 2001, p. 163) While they increase the ability to more granularly define policy there are trade-offs to OU nesting. Primarily is that they complicate the policy and increase troubleshooting when a policy does not respond as expected. Secondly, the more policies that have to be applied, the greater the load on the system and network.

Group Policy and Security:

Group policy is the evolution of NT 4's system policy and is the most compelling reason to migrate to Windows 2000 if you are still using NT 4. Group policy allows security configuration, software pushes, registry changes, etc to be controlled centrally and applied according to where the machine is and who is using it. Group policy objects can be managed through the Group Policy snap-in for the MMC or directly through the containers that they affect.

GPOs can be applied locally (defeats the purpose of centralized management), to entire domains, to sites or to organizational unit. Among these the precedence is LSDOU:

- Local
- Site
- Domain
- OU

With OU overriding the other three. This means is that if the site policy and the domain policy specify different values for the same setting, the domain policy takes effect. This behavior is modifiable using the No Override and Block Inheritance settings in the GPO.

As policies are processed, they are applied one by one, in the precedence order specified above. In other words, all of the Local settings are applied, the Site settings, then the Domain settings and finally the OU settings. A policy applied later will change a setting set by an earlier policy if it's specified, otherwise it inherits those settings. In order to prevent a setting from being changed once set, the Administrator must set the No Override flag on the policy. Likewise, if a local Administrator wants to not inherit a specific set of settings, but also doesn't want to specify the defaults for each item, he may simply set the Block Inheritance flag. If the No Override flag and the Block Inheritance flag are set at two different levels for the same setting, the No Override setting will be honored, the Block Inheritance flag will be ignored.

Although Local Group Policy Objects (LGPOs) were disparaged above, they do provide some usefulness. No, they can't be easily centrally managed, and yes, local administrator accounts can change them. However, they do provide a certain level of protection. If the machine is configured to allow cached logons (which will be disabled

in GIAC Enterprises), then the LCPO could be the only policy in effect if a machine were disconnected from the network and attacked. Cached Logons store a configurable number of previous logons and use that data to validate a potential user if the Domain Controllers are unavailable. This option provides for improved workstation uptime, especially if the network is unreliable.

In this case, there would be no way for the workstation to receive the AD GPO for that user, because the DCs could not be reached, even though the user was logged on. Therefore if cached logons are enabled and certain setting need to be maintained regardless, they should be specified in an LGPO. As an added measure, they could be restated in the Site or Domain policies, in case the LGPO gets modified. Remember that LGPOs have the least amount of precedence applied to them, therefore settings specified anywhere else will take priority.

Microsoft has defined 8 methods of deploying Active Directory

- Layered GPO design
- Monolithic GPO design
- Single-policy Type design
- Multiple-policy Type design
- Functional Roles design
- Team design
- User- and Machine-Specific design

(Olsen, p. 168 – 173)

Our GP will be centered on the Functional Role design. For a small, fairly homogenous organization, it is logical and secure. It will also facilitate migration to a User- and Machine-Specific design in the future if that becomes necessary. The latter is a choice for many because it allows very granular levels of control. However, it suffers from many of the shortcomings that a deep OU structure has, namely difficulty in troubleshooting and increased complexity.

Default Domain Policy:

Default Domain policy is applied to every user and computer within a particular domain. It is a very effective way of specifying a baseline level of security and configuration throughout a domain. Default domain policy is divided into two categories: computer configuration and user configuration. The setting we discuss in the section will be applied to all three domains.

Computer configuration policies apply to all computers in a particular domain, regardless of who logs into them. Options include:

- Software installation
- Scripts

- Password policies
- Auditing policies
- Log policies

Software installation is extremely powerful in that in greatly simplifies patches and new software deployment across the enterprise. Microsoft allows .msi files to be pushed to client, with a fully automated install routine. The machines can be time phased so that the entire network does not try to pull the file at the same time. If a particular piece of software does not come as a .msi there are utilities available that will allow the administrator to create one.

The next section is scripts. There are 5 basic types of scripts; Startup, Shutdown, Log On, Log Out and Legacy. (Olsen, p. 155) Legacy (personal log on) scripts are included for backward compatibility and migration support with NT4 systems. They will not be an issue for our network, as there is no legacy enterprise to worry about. Scripts can be very useful in controlling configuration of the machines. Most popular scripting languages are supported, including Java, Perl, and .bat files.

Scripts can be processed one of two ways, either synchronously or asynchronously. Asynchronous processing is the default. In synchronous processing the process that engaged the scripting (Startup, Logon, etc) is placed on hold until the script finishes processing. If a script is particularly lengthy or error prone, this can be very frustrating to the end user. In asynchronous the mode the script is started and the other process is allowed to continue. The disadvantage to this method is that the service or protection provided by the script may not be immediately available during the users session. As with most of the setting there is a security/convenience trade off in determining which mode you select. Another significant advantage to specifying scripts via GPO is the ability to maintain a centralized script repository for version control and testing.

GPO scripts have a Maximum Wait Time associated with them. It is configured just as any other GPO. The default is 600 seconds. This setting prevents a hung script, running in synchronous mode from locking the box. Unless you have a number of lengthy scripts, or ones that require data pulls from the network, I would recommend lowering this value to at most 300 seconds (5 minutes) if running synchronous scripts.

Next in the list is Security Settings. This section allows the specification of password requirements, logging auditing procedures. Proper configuration of this section in essential to a secure network therefore each will be discussed in detail.

Account Policies contains:

- Password Policy
- Account Lockout Policy

Password Policy options and recommended settings:

| | |
|---|---|
| Enfoce password history | 8 passwords remembered |
| Maximum password age | 90 days |
| Minimum password age | 5 days |
| Minimum password length | 8 characters |
| Password complexity requirements | Enabled |
| Store using reversible encryption | Disabled |

This policy controls the setting and use of a user's password. It forces users to change their password at least every 90 days and prevents them from recycling the last 8 passwords. If a minimum age were not set, some users would simply change their password 8 times in a row, ending up with the same password they started with. To avoid this, we set a minimum age. Users cannot reset their password more often then every 5 days, therefore it would take them 40 days before they could cycle through the required passwords. Also, in order to increase the difficulty in cracking or brute forcing a password, set the minimum length to 8 characters and the enable the complexity requirements.

By default, password complexity means the password must contain 3 out of the 4 following:

- Upper case letters
- Lower case letters
- Numbers
- Non-alphanumerics
  (Microsoft, "Windows 2000 Resource Kits", November 5, 2001).

Assuming the user chooses upper case, lower case, number for the combination, then each position would have 62 possibilities. Total number of possibilities 62^8 = really huge number. Actually in excess of 200 trillion. Again, really, really big.

Account Lockout Policy options and suggested settings:

| | |
|---|---|
| Account Lockout Duration | 15 minutes |
| Account Lockout Threshold | 5 invalid attempts |
| Reset Lockout Counter after | 15 minutes |

These settings cause an account to be locked out for 15 minutes after 5 invalid login attempts. The counter resets after 15 minutes. These setting were selected because coupled with the Password Policy set earlier, these should provide adequate protection without causing undue stress to the user. Even if they screw up their password, they are only locked out for 15 minutes, however if you are trying to brute force a password, 20 attempts an hour will not get you very far.

Local Policies control specifically who can do what to the computer and what will be logged. Its subcategories are:

- Audit Policy
- User Rights Assignment
- Security Options

Audit policy options and recommended settings:

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

These settings will log logon attempts (successful or not), changes to accounts, policies and system events. Log management is critical, as it is your eye into the system. Do you have a user trying to elevate their access? Or is a machine rebooting more often then it should? When deciding what to log, you have to weigh the importance of each piece of information because you will have to wade through all of it later when you do choose to look for something.

User Rights Assignments define specifically what users and groups can do what to a machine. In general the principal of least privilege should be exercised here. Do any of your users really need to access the computer over the network? Probably not. How about managing your auditing and security logs? Most definitely not. The other extreme is removing the users' ability to shut down the system. There are valid reasons for wanting to deny users this ability, however make sure yours is a good reason before taking such a basic function away.

Security options allows the setting of numerous security options within the domain, including Smart Card behavior, response to unsigned device drivers, etc. This section will address some of the more commonly set options.

| | |
|---|---|
| Do not display last user name in logon screen | Enabled |
| Lan Manager Authentication Level | Send NTLMv2 responses only |
| Number of previous logons to cache | 0 |
| Rename administrator account | Anything |
| Rename guest account | Anything |
| Shutdown system if unable to logon security audits | enabled |

These settings achieve several things. First the user name of the last user is not displayed in the logon screen. This protects usernames from being harvested by anyone who happens by a logged off computer. Secondly, since the network is comprised exclusively of Windows 2000 machines, there is no reason to authenticate anything other than LanMan 2, especially given the weaknesses of the other options. The third setting prevents access to the machine if the DC is not available. This prevents someone from removing the network connection and attempting to brute force a password. Rename the Administrator and Guest accounts to prevent easy attack. Both of those accounts are easily targeted, renaming them prevents, or at least complicates those attacks. Finally, shut the system down if it can not log what the user is doing.

Event Log settings specify the size and handling methodology for the event logs.

| | |
|---|---|
| Max application log size | 2048 k |
| Max security log size | 10240 k |
| Max system log size | 2048 k |
| Restrict guest access to application log | Enabled |
| Restrict guest access to security log | Enabled |
| Restrict guest access to system log | Enabled |
| Retain applications log | 15 days |
| Retain security log | 30 days |
| Retain system log | 15 days |
| Retention method for application log | Overwrite events as needed |
| Retention method for security log | Clear log manually |
| Retention method for system log | Overwrite events as needed |
| Shutdown computer when the security log is full | Enabled |

In general, these options create log files large enough to handle worthwhile data. They will hold between 2-10 Megs of data, for up to 30 days. The applications log and the system log will wrap around, clearing old data as required in order to ensure that the new events are logged. The security log will require manual clearing if it gets full before the expirartion date. Finally if the security log becomes full the machine will shut down. This is used in conjunction with the earlier setting that specified the machine would shut down if it was unable to write the security log. The purpose of this setting and the requirement that the security log be manually cleaned is to prevent someone from filling the log with innocuous but audited events in order to force it to overwrite some earlier illicit activity.

The importance of complete, detailed logging cannot be over emphasized. If you are broken into, the logs will likely be your only records of the events. Even worse if a machine has been compromised for a length of time longer than the amount of time you keep your logs, then you have no record of the original break in. This will greatly complicate system clean up and closing the hole they used to break in.

Default Domain Controller Policy:

Due to the nature of the two way transitive trusts between Domain Controllers in the same forest, it is absolutely imperative that all Domain Controllers be as secure as possible. Not only must they be kept physical secure (in a restricted access room, etc) they must also be configured securely. The basic configuration will be similar to the default domain policy, only more stringent.

Password Policy options and recommended settings:

| | |
|---|---|
| Enfoce password history | 8 passwords remembered |
| Maximum password age | 90 days |
| Minimum password age | 5 days |
| Minimum password length | 8 characters |
| Password complexity requirements | Enabled |
| Store using reversible encryption | Disabled |

Account Lockout Policy options and suggested settings:

| | |
|---|---|
| Account Lockout Duration | 15 minutes |
| Account Lockout Threshold | 5 invalid attempts |
| Reset Lockout Counter after | 15 minutes |

The password related policies are identical to those set in the default domain, because as discussed before, 200 trillion is a really big number.

Audit policy options and recommended settings:

| | |
|---|---|
| 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 | Failure |
| Audit process tracking | Success, Failure |
| Audit system events | Success, Failure |

For the Domain Controllers the number of activities logged has been increased. As there are only 6 DC in the entire enterprise, it is reasonable to expect that their logs would be reviewed daily for anomalies. Because of this and the increased security concerns for them the change is justified.

User Rights Assignment Options and Settings:

| | |
|---|---|
| Access this computer from the network | Administrators, Enterprise Domain Controllers |
| Backup files and directories | Administrators, Backup Operators |

| | |
|---|---|
| Change system time | Administrators |
| Log on locally | Administrators |
| Shut down system | Administrators |

Because Domain Controllers are a special case, it easier to define some of the User Rights setting for them than it is for a workstation. In short, limit access to the DC to administrators. No one else likely needs it. Be aware however that certain applications may require access to the DC, so monitor the system for errors and add users/groups as required.

Security Options:

| | |
|---|---|
| Do not display last user name in logon screen | enabled |
| Lan Manager Authentication Level | send NTLMv2 responses only |
| Number of previous logons to cache | 0 |
| Rename administrator account | anything |
| Rename guest account | anything |

Event Log settings specify the size and handling methodology for the event logs.

| | |
|---|---|
| Max application log size | 10240 k |
| Max security log size | 204810 k |
| Max system log size | 10240 k |
| Restrict guest access to application log | enabled |
| Restrict guest access to security log | enabled |
| Restrict guest access to system log | enabled |
| Retain applications log | 15 days |
| Retain security log | 30 days |
| Retain system log | 15 days |
| Retention method for application log | Clear log manually |
| Retention method for security log | Clear log manually |
| Retention method for system log | Clear log manually |
| Shutdown computer when the security log is full | disabled |

Coupled with the earlier increase in the number of events logged and desire not to have a Domain Controller shut down due to full logs, the maximum log file size has been increased and auto-shutdown of the machines disabled. Also, in order to force the daily review of the DC logs, all logs have been set to "clear log manually".

OU Policy

In domain policy, the emphasis was on machine configuration, in OU policy we will place the emphasis on user settings. The reason for this is not that there is no hardware in OU, quite the contrary as shown by the chart in the OU section. Nor is it because people are not in the domain, they must be as OUs are sub-elements of domains. I tend to break them this way because in my mind, most machines in an organization should

be fairly similar, whereas people tend to vary widely. These variations are in technically saviness, personalities, requirements, etc.

Because of these variations I prefer to emphasize the user settings in the OU section. Again most settings (likely all) can be applied at the local, site, domain, and organizational unit levels. As stated earlier, any conflicts are resolved in that order, LSDOU.

The needs and technical ability of the FIN/HR section and of the SALES section are similar, therefore you could expect them to have similar GPOs. Remember that GPOs do not control access to files or network resources, that is the function of User/Group Permissions and Access Control Lists (ACLs).

In general, the practice of least privilege should be followed, no user should have more capability than he needs to complete his job. However, it is a fine balancing act to not lock the machine done so tight that the user dreads using it.

FIN/HR GPO settings

The options for user configuration include:

- Software Settings
- Windows Settings
- Administrative Templates

Of primary interest will be Windows Settings and Administrative Templates. In Windows Settings the most useful setting for the FIN/HR OU is Folder Redirection. This setting allows certain standard folders to be pointed to somewhere other than the local hard drive. For example, the "My Documents" folder can be redirected to a folder on the file server. This is critical for two reasons.

1. The local machines are not backed up, therefore if it crashes and the users data was on it – problems.
2. If the user sits somewhere else, the files on that local machine would not be available to him, which was one the goals

Folder redirection does have some trade-offs:

1. If the file server is unavailable, so are the files. However, this is more than overcome by the increase in general availability
2. File discipline by user will become more important. One user having 1 gig of MP3s on a local machine with a 20-gig drive is not a huge problem. 150 users having 1 gig of MP3s each on the server would be a problem.
3. Similar to item 2, network bandwidth could become an issue if the network was not designed to handle this sort of traffic. File sizes will continue to

increase and big hard drive will get cheaper and cheaper, but pulling new cable is expensive.

Administrative Templates:

Administrative templates actually change the users' registry settings. This is a very powerful tool that permits system administrators to force certain software settings for increased security or automatic configuration. In order to truly understand the power of this, you have to remember that group policies are the composite of the settings for the Domain, Site, and OU and that they are re-applied at every log on. Every time someone logs on to a machine the registry could be edited depending out the GPOs in place.

This also means that if the registry can control it, so can Active Directory. Within administrative templates there are three possible settings; Enable, Disabled, Not Configured. Enabled turns the registry value "on", disabled turns it "off" and not configured means that it will use whatever is currently set in the registry. More correctly, Not Configured means that AD does not touch the setting at all.

The FIN/HR staff uses NetMeeting to talk to colleagues in the other office (New York or San Francisco), but management was concerned about abuse and the potential for accidental virus propagation.

The GPO for NetMeeting is below:

| | |
|---|---|
| Enable Automatic Configuration | enabled |
| Prevent adding Directory servers | enabled |
| Set the intranet support Web page | enabled |
| Prevent sending files | enabled |
| Prevent receiving files | enabled |

These settings ensure that application is automatically configured, can only call sites in the corporate Directory server and blocks sending or receiving files. An added benefit is the ability to set the support page address to help new users, thereby reducing trouble calls.

Another security concern is web access. The firm has launched a vigorous education campaign to ensure that users are fully aware of the dangers of malicious code and the potential legal problems that could arise from misuse of the web. However, as a back up they want a locked down version of Internet Explorer. Not every feature that is controllable should be set however, disabling the ability to change font settings may be nice from a consistency standpoint, but does little to help those whose vision is slipping.

Recommended settings:

| | |
|---|---|
| Disable external branding of IE | enabled |
| Disable changing Advanced page setting | enabled |
| Disable changing home page | enabled |
| Disable Internet connection wizard | enabled |
| Disable changing proxy settings | enabled |
| Disable changing ratings settings | enabled |
| Disable changing certificate settings | enabled |
| Do not allow auto-complete to save passwords | enabled |
| Disable reset web settings feature | enabled |

These setting center around two goals. The first is to prevent the user breaking the browser for either themselves or someone else who uses the same machine. The second goal is security. Disabling external branding really just comes down to providing a consistent desktop experience for your users. Disabling the Advanced page likewise provides for a consistent experience across machines in the enterprise by preventing users from changing the way links and content is displayed. This tab also allows the user to change certain security settings dealing with the way certificates are handled, another area where we would prefer they not play with.

The company has an intranet web page that is used to make company wide announcements as well as serve as a portal for IT information, acceptable use guidelines, sexual harassment information, etc. This is the preset home page, and management wants to ensure that the users see that page every time they start a browser, therefore the ability for users to change their home page should disabled.

All of the machines receive their internet access through the lan, therefore there is no reason to allow the user to the Internet Connection Wizard. The browsers are installed with the proxy settings pre-configured, no reason for users to change it. Nor should they be allowed to adjust the RSAC ratings limits configured during browser installation or change the setting for certificates.

The firm is also looking at moving more of its internal processes to a web interface. As they do, much of the software will require users to log in to use it. Because of this, allowing Password completion would be bad for corporate security.

GIAC Enterprise does not use active-x controls in any of their web applications. Therefore they have left all of the Administrator approved controls disabled, thereby not specifically allowing any active-x control.

In Windows Explorer:

| | |
|---|---|
| Remove "Map Network Drive" . . . | enabled |
| Only allow approved Shell extensions | enabled |
| No Computers Near Me . . . | enabled |
| No Entire Network . . . | enabled |

The Remove "Map Network Drive" setting prevents users from attempting to mount drives on their own. While this should not be an issue if all of the permissions are set correctly on the drives, it provides another layer of defense. It also reduces the likelihood of users trying "fix" their systems. If they need access to a drive that is not automatically mounting on log on, then they will notify the trouble desk and the problem can be rectified.

The "only approved shell extensions" is an added layer of defense against certain malicious code such as trojans that attempt to run as part of the Windows interface.

Turning off the Computers Near Me and the Entire Network icons in Network Neighborhood prevents users from casually browsing the network. The point with many of these settings is that if the user is specifically given an asset, they should not simply go out and try to find it. It is the principle of least privilege revisited. If they need it, they identify the requirement and it is added to log in. This step also prevent malicious users from performing reconnaissance against your network.

Start Menu & Taskbar recommended settings:

| | |
|---|---|
| Add Logoff to the Start Menu | enabled |

Useful tool to encourage user to log off when done.

Desktop Setting:

| | |
|---|---|
| Prohibit user from changing My Documents Path | enabled |
| Don't save settings at exit | enabled |
| Disable active desktop | enabled |
| Hide Active Directory folder | enabled |

The first setting is designed to prevent user from changing the mapped path for the My Documents folder that was set earlier. The next two settings are designed to ensure a consistent desktop appearance. Finally, the last setting is designed to prevent user from casually browsing the Active Directory.

Control Panel:

| | |
|---|---|
| Disable Control Panel | enabled |

This setting completely disables control panel access to the user. In most cases there is nothing in the control panels the users need to access. More than likely, any changes

that a user would make to a control panel would simply break something if the boxes were initially configured properly. If a scenario arises where users will need to change a control panel setting specific control panels may be enabled and disabled individually.

The System section contains several settings useful for controlling the security of the system, however in this case no specifics will be determined. One topic however has been the subject of some debate, which is disabling the task manager. This of course could be very useful if you want to prevent the user from viewing a list of all of the processes running on a particular machine. For example, if a piece of spyware has been installed it may show up in the task manager. The user could then identify it and disable (kill) it or, now aware that they are being monitored, modify their behavior to avoid the tool. It is also important to note that buggy software is still universally present. If a user cannot simply kill a run-away process using the task manager, it may well take the machine with it as it dies, potentially causing user to lose valuable data.

This is also where it is possible to force logon/logoff scripts to be hidden from the user and also where group policy refresh interval can be set. The ability to hide scripts can be useful if you a loading spyware or the like and do not wish to alert the users. The latter can be useful if you often change the group policy, or if you're experiencing problems you can set the policy to refresh every 30 minutes for example. The default value is 90 minutes with a random offset applied. The random offset is designed to facilitate load balancing the Domain Controllers. It is added or subtracted from the set value to create a window during which the workstation will update policy. For example, if the value is set to 90 minutes and the random offset is +/-15 minutes, then the actual update request would occur sometime between 75 and 105 minutes. This reduces the number of machines attempted to contact the server at any one time.

Adding Templates:

Perhaps one of the best features of Group Policy and the MMC is that it is extensible via templates. A new service or piece of software is installed and if a template is available, it can be loaded to the Microsoft Management Console. From there it can be used as part of a GP. For that matter, even if a template doesn't exist, you can write your own. However this is a tricky business, particularly if the keys are set in other than specific areas. Microsoft discourages the creation of custom templates. (Olsen, p. 177) However, if carefully applied, particularly with attention to clean up, custom templates open a whole new prospect for enterprise system control.
For example, the Office XP resource kit includes templates to configure the various aspects of the Office suite. The resource kit is available from Microsoft (http://www.microsoft.com/office/ork/xp/). Once it is downloaded, double-click on the installer to run it. Then open the group policy that you want to add the template to, in this case FIN/HR. Once in the policy right click on "Administrative Templates"

under "User Configuration" and select "Add/Remove Templates." When the dialog box opens, click "Add" and select the template you wish to add. In this case I am adding OUTLK10.ADM, the Outlook Template.

Now, when we go to the Administrative Templates folder there is a new template called "Microsoft Outlook 2002." Outlook has been the victim of some of the most notorious virii and worms of the last two years. This template will allow the mitigation of some of those problems.

Outlook Security settings:

| | |
|---|---|
| Prevent users from customizing attachment security settings | enabled |
| Allow access to e-mail attachments | enabled, but with no executables specified |

These two settings work together to prevent user from accidentally infected the network. The first setting prevents the user from changing the security settings and the second would prevent any extension not expressly permitted. That way it is possible to allow .ppt and .doc but not .vbs. Of course, this technique is part of a defense in depth strategy that also employs a virus scanner on the mail server and on the workstation.

Add the OFFICE10 template and gain more controls including:

| | |
|---|---|
| Disable VBA for Office Applications | enabled |

This prevents Visual Basic for Applications from running in Office applications. If you do not need VBA, disable it easily.

This marks a good point to revisit the importance of OUs and GPOs. Earlier, nine OUs were defined for GIAC Enterprises and only one has been discussed in detail. The specifics of what OUs get which policies is a function of user requirements, user experience and acceptable risk values. The VBA option is a perfect example of this concept. For argument's sake, supposed that FIN/HR needs VBA for some of their spreadsheet applications. Then that functional OU would have that VBA available, but if no other OU needed the functionality, it should be turned off.

Also, it would be wise at that point to ensure that the FIN/HR members were familiar with the risks associated with VBA and how to guard against them.

As another example, the R&D team often must test their new products using different browser and web settings as well as in different browsers or other software. Also, they are all very computer savvy. To configure their access the same way that you had the SALES team configured would mean endless trouble calls and reduced team efficiency.

Therein lies the true power of Active Directory and Group Policy Objects. We know that there are certain settings that should be the same for all (or at least most) users in a domain, such as password security settings. We set these in the Domain section. Then, as we get more and more specific, possibly moving through multiple nested OUs, the policy continues to refine itself. In the end there is a policy that specifically tailored to a particular type of user, that allow him to do his job wherever he happens to be sitting. He shouldn't have to be concerned about how to add a printer, or set the name of his mail server the first time he sits down at a new machine. It all comes with him combined with Site settings, Domain settings and Resource OU settings. If the AD has been designed and implemented properly, it will just work.

Finally, it is worth restating that just because an Administrator can change or lock a setting doesn't mean that they should. Remember that depending on the user's job in the organization, they may spend a significant portion of their day on that computer. If there is no company policy banning an action and no significant risk in allowing the action, why block it? If the user dreads using the machine then has the IT plan improved the efficiency of the organization or reduced it? It is essential to remember that the IT dependent exists to enable the organization. Too strict of an implementation may have other side effects as well. If users are denied what they consider to be basic functionality two events may happen.

First, those who are computer savvy will attempted to circumvent the policy. This could potentially regard less odious but more important portions of the policy breached, increasing the security risk to the system. Secondly, they will loudly complain. This is likely to increase tech support calls and may cause management to declare the implementation a failure.

Some may say that this stance violates the policy of least privilege. The response is that trivial services are not necessarily subject to least privilege. What is the corporate interest in preventing users from being able to set their wallpaper or font size, especially if it improves their ability to read the data and perform their function. If there is a valid reason, then force the setting; otherwise leave it alone.

Conclusion:
Active Directory and Group Policy Objects allow unprecedented control and customization of the enterprise. It is now conceivable to create a standardized workstation load, deploy it and maintain it across the enterprise with great consistency. Prior to this, machines would drift from the baseline to the point of being nearly unrecognizable within a year.

Not only does AD and GPO allow standardization and reduced maintenance time, but it also enables the end user to sit anywhere and have a consistent environment. This will reduce user frustration, reduce training time and boost productivity.

However, perhaps the greatest advantage is the increased security that comes from centralized management and active reconfiguration of boxes. Even if a user manages to change the configuration on a box, it will only be temporary. As soon as the GPO is reapplied, whether at logoff, startup, a time interval, or what ever, the system returns to its previously secure state. Couple with the ability to push critical hotfixes and patches, Windows 2000 is a significant improvement over NT 4.

Finally, no single feature will make a system secure. All network security relies on defense in depth. Some of the feature described in the GP section overlapped other applications or defenses. That is on purpose and as it should be.

## List of References


Bartock, Paul F., Jr. et al. "Microsoft Windows 2000 Network Architecture Guide." (Version 1.0, April 19, 2001) URL: http://nsa2.www.conxion.com/win2k/download.htm (October 15, 2001).

Haney, Julie M. "Guide to Securing Microsoft Windows 2000 Group Policy." (Version 1.1, September 13, 2001) URL: http://nsa2.www.conxion.com/win2k/download.htm (October 10, 2001).

Maione, Dennis. "MCSE Windows 2000 Server Training Guide." New Riders, 2000.

Mar-Elia, Darren and Sean Daily. "The Definitive Guide to Windows 2000 Group Policy." URL: http://www.fullarmor.com/ebook/read (September 28, 2001). Free registration required.

Microsoft. "Microsoft Support Knowledge Base." URL: http://support.microsoft.com/ (Various).

Microsoft. "Windows 2000 Resource Kits."
URL: http://www.microsoft.com/windows2000/techinfo/reskit/en-us/gp/504.asp (November 5, 2001).

Olsen, Gary L. "Windows 2000 – Active Directory Design & Deployment." New Riders, 2001.

Last Updated: May 23rd, 2017

# Upcoming Training


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