Global Information Assurance Certification Paper

Bruce M. Elliott
GCNT Practical Assignment (v.3.0) (August 2001)

Secure Windows 2000 Infrastructure – GIAC Enterprises

GIAC Enterprises - Assumptions

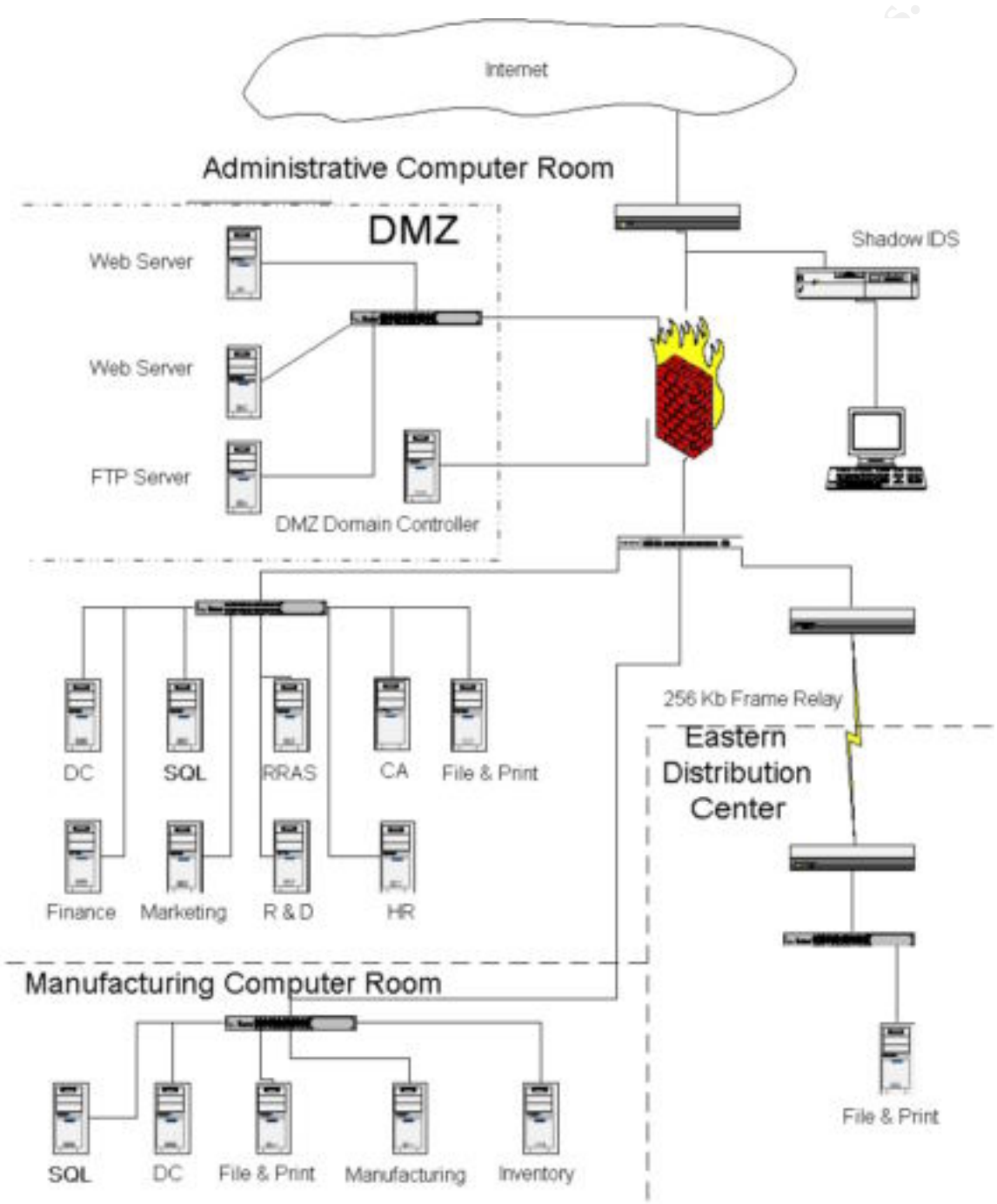
GIAC Enterprises is a Canadian company that operates out of two different geographical regions of the country. Its primary location houses the Administrative offices, Research and Development Department, Manufacturing Department, Warehousing, and a Western Distribution Center. All are located together on one large site located in a major city with good transportation links, and the availability of high order services. The Admin offices, Research and Development Department, Manufacturing Department, Warehouse facilities, and Western Distribution Center are all connected together on a high speed campus network of LANs.

GIAC Enterprises also has a separate Eastern Distribution Center located in another geographical region of Canada. The Eastern Distribution Center is the hub for all product distribution in Eastern Canada. It is connected to the company's main offices by a 256 Kb Frame Relay.

The western location houses both the Administrative offices and the Research and Development Department together in one building, with the Manufacturing Department and Warehousing located in a separate building adjacent to the main offices.

The Administrative offices encompass facilities for the Human Resources (HR) Department, the Sales and Marketing Department, the Finance and Accounting Department, and the Research and Development Department. GIAC Enterprises is fairly young company, with only two years of actual day-to-day operations. It does not have any legacy applications that require any older operating systems. All of the company's servers have been upgraded to Windows 2000 Server and all desktop systems have been upgraded to Windows 2000 Professional.

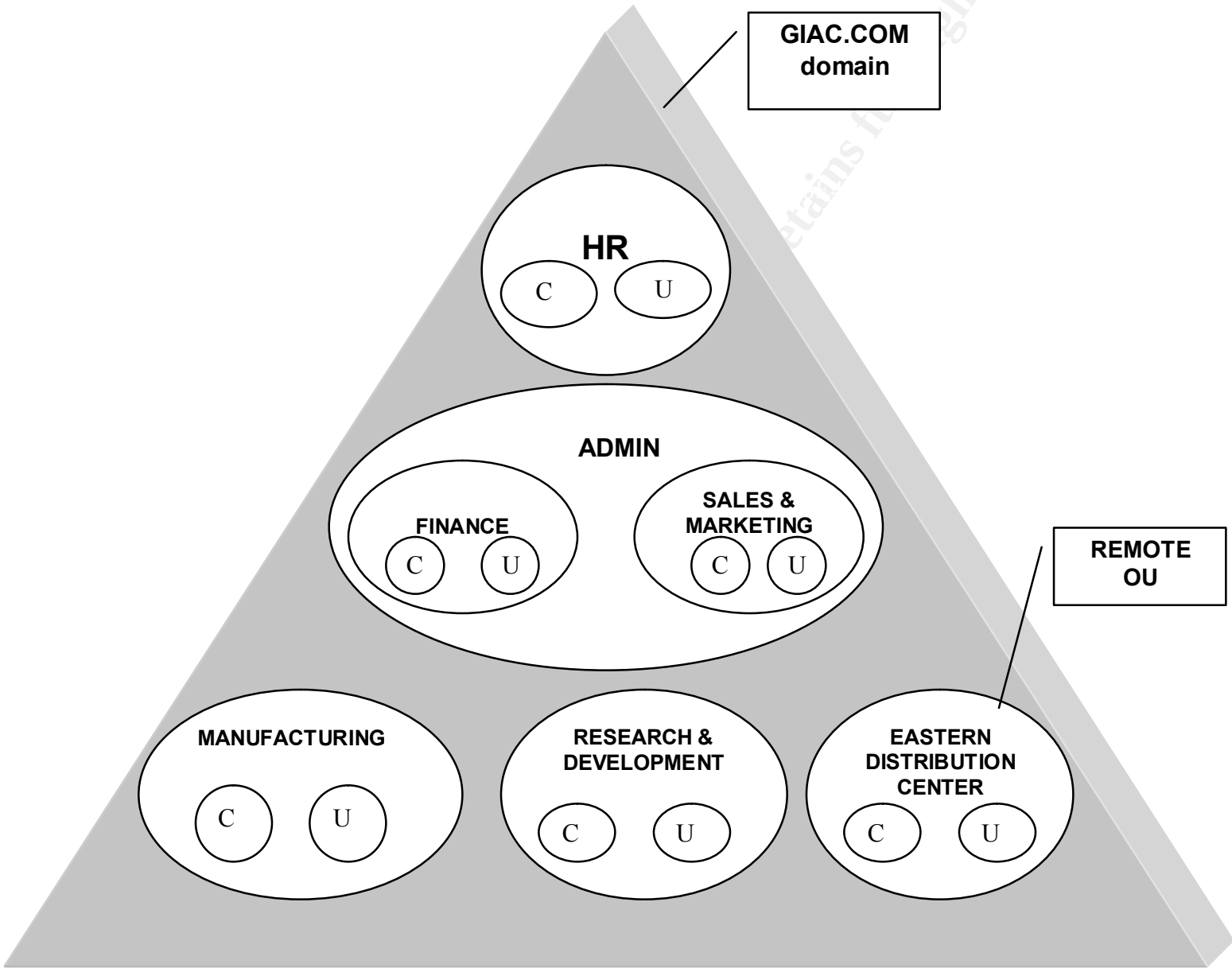
Network Design and Diagram



The corporate network has a single connection to the Internet. This connection is protected by a proxy firewall. The proxy firewall is designed with a DMZ , and in this DMZ two Web Servers, and an FTP Server are included to provide access to the publicly available systems. There is a second DMZ to hold a Domain Controller for authentication reference and to hold the Group Policy Objects that configure the DMZ based servers. Outside the firewall there is a Shadow IDS system to monitor the Internet connection for hostile traffic. This Shadow IDS system is kept on a private network for additional security.

The internal network is a 100 Mb switched network. There are three separate secured computer rooms, one for the Administration areas, a second one for the Manufacturing and Warehousing area, and the third one in the eastern Distribution center. The eastern Distribution center is connected with a 256 Kb Frame Relay link. There are two Domain Controllers, one is located in the Administration building's computer room and the second one is located in the Manufacturing Department's computer room. In the Administration Department's computer room there are separate servers for the Human Resources Department, the Finance Department, the Sales and Marketing Department, and the Research and Development Department. There is also a separate SQL server that provides central database support for all of the other servers, a certificate server to issue x.509 certificates for security and encryption, a general purpose file and print server for user files and print support, and an RRAS server that allows the sales representatives, conducting business in the field, to dial into the network to access existing orders, or enter new orders and to make enquiries. In the Manufacturing Department's computer room there are servers for inventory management, and manufacturing control, as well as a replicated SQL server for business recovery and performance and a file and print server. At this time there is only a file and print server in the computer room at the Eastern Distribution Center, although a domain controller could be located here in the future if staffing levels require it.

ACTIVE DIRECTORY TREE



LEGEND:

C = computers
U = users

The domain design for GIAC Enterprises is a single domain, within a single forest for ease of administration. The company is not large enough and it does not have enough geographical divisions to justify implementing additional domains plus the added administrative costs associated with a more complex structure.

There is a separate domain with an explicit one-way trust to the corporate domain that is not part of the forest. This specific domain is used to authenticate Employees and Partners against the Corporate domain controllers. This is accomplished via the trust with the inside domain when these users want to access secured Corporate information on the web or FTP servers from the Internet. The web and FTP servers are members of this separate domain and will get their group policies for their security configuration from this domain controller.

A number of Organizational Units have been created to provide for separate administrative functions and to protect data structures. Each top level OU is administered by a different individual, or individuals, in the Information Technology Department and the OU structure was created following the lines of responsibility within the Information Technology Department. In each top level OU there is a sub OU to hold users and another sub OU to hold computers for the department. The segregation of users and computers into their own sub OU allows for the creation of separate Group Policy Objects for both system startup/shutdown and user login/logoff, which should give better overall performance.

The Human Resources Department OU is designed to protect all information that is accessible to the Human Resources Department personnel working in this area. The requirement to protect all personal information falls under the jurisdiction of the Privacy of Electronic Information Act. Human Resources Department users would be placed in a sub OU for users and the computers located in the Human Resources Department would be placed into a sub OU for computers. There would be an Administrator for the Human Resources OU who would have full rights for this OU to create users, add systems, and create any other objects related to the users and systems in this OU, or any OU below the Human Resources Department OU.

There would also be a separate OU for the Research and Development Department. It is necessary to keep this OU separate because of the secretive nature of the work performed in this area. To ensure the growth and economic success of GIAC Enterprises the company must continuously carry out product research and the development of new products. Since this is where all of the company's new products and designs are created, they must be protected from outside interests. Again, users and computers will be segregated into their own sub OU. An individual who understands the unique security requirements of this

department and the special needs of the designers who work in it would administer this OU and each of the OUs below it.

The Finance and Marketing Departments have been combined into one OU as both of these departments will be administered by the same individuals. Data structures would be protected within this OU by NTFS rules.

Manufacturing, which includes the Warehouse and the Western Distribution Center, was set up as a separate facility with its own support staff and OU. They are in a separate building and have their own Information Technology support group, as the work in this area is quite different from the general office administration areas. As well, the Eastern Distribution Center has its own OU and a local Administrator; however, the administration duties are shared with the Administrator of the Manufacturing OU.

Domain controllers are situated in the computer rooms at the Administrative offices, and the Manufacturing Department. There is no domain controller at the Eastern Distribution Center because there is not enough staff located at that site to warrant it. Staff at this remote OU authenticate over the network. Should a larger contingent of staff later start working out of the Eastern Distribution Center this would create a performance issue that would need to be addressed. With more people at the Eastern Distribution site there would be extra authentication traffic and this remote OU would need its own domain controller so that it could do its own authentication. With the addition of a Domain Controller at the Eastern Distribution Center, domain synchronization traffic would have to be scheduled in off peak hours so as not to impact production work.

Group Policy and Security

In Windows 2000, client administration and configuration options are primarily done through Group Policy Objects. In this application an Active Directory Tree is used as the directory service used to manage the client administration and configuration. Consideration is given to the OU to which the user belongs, the type of work the user performs, where the work is performed, and the degree of confidentiality required[1].

Consideration needs to be given to a number of support issues. These issues will then determine what Group Policy rules need to apply.

---

[1] "Deployment Planning Guide, Windows 2000 Server, Part 6 Windows Professional/Client Deployment, Chapter 23 Defining Client Administration and Configuration Standards", pg. 827, Microsoft Corporation, July 1999

The following are some of the commonly occurring issues[2]:

- The top 10 support issues that reoccur and need to have their frequency reduced.
- Users attempts to change their configuration settings (e.g. video drivers) and options.
- Users attempts to add or remove applications (incorrectly) and break their configuration.
- Users attempts to install unauthorized software on their computers.
- Is client data secured, and does it need to be?
- Allowance of users to operate as local administrator on their computer.
- The amount of time spent by Help Desk personnel trying to fix broken configurations, with the result that they have to reinstall or reset the basic configuration.

The ability to establish a number of Group Policy Objects under Windows 2000 allows for better control of users and the delegation of administration tasks. It allows for IT administrative personnel to address support issues.

Some of the support issues that need to be regularly addressed in relation to Group Policy and Security are[3]:

- Who has authorization to create or change user or computer accounts, and how many user or computer accounts are routinely created or modified each month?
- Who sets the software standards and is responsible for their deployment?
- Who sets or updates passwords, and what are the requirements for password or authentication?
- Who handles the backup of servers, and user data, and how often? How often is data restored from backups?
- Are there service level agreements or other explicit service goals, and what are the criteria?

The service standards and goals set by IT determines how this Group Policy is used to administer users or clients. Group Policy settings are the primary method for enabling centralized change and configuration management. It

---

[2] "Deployment Planning Guide, Windows 2000 Server, Part 6 Windows Professional/Client Deployment, Chapter 23 Defining Client Administration and Configuration Standards", pg. 832, Microsoft Corporation, July 1999

[3] "Deployment Planning Guide, Windows 2000 Server, Part 6 Windows Professional/Client Deployment, Chapter 23 Defining Client Administration and Configuration Standards", pg. 834, Microsoft Corporation, July 1999

allows for the creation of specific desktop configurations, for specific groups of users and computers.

Domain Group Policy Set Up

There should be at least two Enterprise Administrators who have complete rights to the total Active Directory structure and all of its objects. When initially creating the top-level domain controller, select permissions compatible only with Windows 2000 server option. This would leave the Everyone group out of the NTFS permissions. For any application that fails with this removed, the Everyone group can be added in to that particular directory that that application uses. This would prevent null user session access to the servers.

It is important that the latest service packs and hot fixes are installed on all computers. Adding the .msi package file to the software installation area in either the domain Group Policy Object, or the OU Group Policy Object for computers can accomplish this task. That would ensure that the latest changes and fixes are installed.

Global groups would be set up to hold the users and computers for each department and the resources that need to be controlled, and access rights would be attached to domain local groups. For example, a group called RandD users would be setup to hold all of the users in the Research and Development Department and would be placed in the Users OU under the Research and Development OU. There could be additional nested global groups if there are discrete groups of users who have different security needs or require access to unique resources. Domain Local groups can be set up and can be applied to various resource objects, which can then be nested in the global groups who need access to these resources. Also in this example, a global group for computers would be set up to hold all of the computers in this area and placed in the Computer OU, under the Research and Development OU.

Group Policy Objects can be applied at the local level, site level, domain level, or the OU level. These levels are listed in the order of precedence that they are executed in, making the OU level the highest, as this is done last. Group Policy is initiated at the top-level domain, with global parameters that apply to all the objects in the domain, according to a top down order structure. The power granted is dependant on the OU administration structure. It is a top down structure in which later rules will supersede the top rules, unless forced inheritance is turned on. In those situations where forced inheritance is turned on it overrides all later rules. Forced inheritance is usually applied when establishing rules for password strength. Typically, the Administrator needs to

ensure that the strongest password rules apply when users are creating passwords, in order to ensure the best security against password cracking.

The rules set at the top level of the giac.com domain are password policies, account lockout policies, and Kerberos policies, as these all relate to account access policies that you don't want circumvented further down in the domain structure.

The Password Policy rules are:

- Enforced password history set to 6 passwords remembered.
    - This prevents someone from re-using the same passwords over and over again.

- Maximum password age set to 42 days.
    - This ensures that passwords are changed on a frequent basis.

- Minimum password age set to 7 days.
    - This prevents someone from changing their password frequently so as to get back to the favorite one that they had previously.

- Minimum password length set to 8 characters.
    - This ensures that both halves of the 14-byte password field have at least 1 character in them, to prevent the second half being null.

- Passwords must meet complexity requirements set to enabled.
    - This prevents someone from using a simple, easily guessed password.

- Store passwords using reversible encryption for all users in the domain set to enabled.
    - This is required for Digest Authentication for users authenticating from the Internet servers, or for SPAP and CHAP for dial up authentication using RRAS.

Account Lockout Policy rules are:

- Account lockout duration set to 30 minutes.
    - This is to provide a long enough lockout period to frustrate hackers, but not so long as to be difficult for users.

- Account lockout threshold set to 5 invalid logon attempts.
    - This is the number of password tries a user can make before the password locks. It is set high enough to allow a user who has forgotten his/her password, or who has recently changed his/her password to make a few invalid attempts before successfully logging on.

- Reset account lockout counter after set to 30 minutes.
    - This prevents invalid attempts from accumulating over an extended period of time.

Kerberos Policy rules are:

- Enforce user logon restrictions set to enabled.
- Maximum life time for service ticket set to 600 minutes.
- Maximum life time for user ticket set to 10 hours.
- Maximum life time for user ticket renewal set to 7 days.
- Maximum tolerance for computer clock synchronization set to 5 minutes.

    - These are all default rule values.

These rules should ensure the security of the users' passwords. This has to go hand-in-hand with educating the users on how to create secure passwords and keeping them secure. It is much easier to set the rules on creating and securing users' passwords than it is in gaining compliance across the board. Users generally have difficulty remembering their passwords and tend to write them down in obvious places, or try and circumvent the level of difficulty required when creating a new password. In addition, users will often give their passwords out to other employees when they will be absent and someone else needs to access their applications.

At the OU level, rules have to be set up so that the Administrator of the individual OU can administer all objects related to that OU and each lower level OU that they are responsible for, without them having the ability to access objects in any other OU.

Research and Development Department OU Set Up

Setting up the Research and Development Department's OU requires that the Property page for the OU be opened up. Select the Properties button, and add the Administrator under the Security tab. Give that Administrator Read, Write,

Create All Child Objects, and Delete All Child Object rights. To restrict access to the Research and Development OU, the Authenticated Users group needs to be removed from the Security tab and RandD users need to be added with Read and Apply Group Policy rights. It is imperative that only the Research and Development Department personnel have access to this OU. The groups for Domain Admins, Enterprise Admins, and System were left unchanged, with all their default rights intact. There is a tendency for the applications to fail if the System account is removed because the application may not have the necessary rights required for execution.

Next, there is the need to create the sub OUs under the Research and Development OU for the computers and users. Setting up the Research and Development Department's OU for computers and users at this sub level requires that the Property page again be opened up for both the computer and users OUs. The Properties button needs to be selected, and the Administrator needs to be added again under the Security tab for both the computer and users. Both the computer and user OU Administrator needs to be given Read, Write, Create All Child Objects, and Delete All Child Object rights as well. So as to again restrict access to the Research and Development OU, you need to again remove the Authenticated Users group from the Security tab for both the computers and users. Then the RandD users and computers need to be added to the Security tab with the rights to Read and Apply Group Policy. It is important to reiterate the need to ensure that only the Research and Development Department personnel have access to the computers and users OU. Again, all of the Domain Admins, Enterprise Admins, and System were left unchanged, so that all their default rights remain intact.

The Group Policy Object at the Research and Development OU level was left unchanged.

In the computers sub OU, under the Group Policy Properties tab you need to check the box to Disable User Configurations Settings. Then click the Edit button to open the current policy. Next, right click the Security Settings and select Import, and then select the BASICWK.INF import file to apply the basic security settings. Then again right click the Security Settings GPO name and select Import, and then select SECUREWS.INF import file to apply additional security settings. Under Account Policies the Password Policies and Account Lockout Policies remain not defined, as they were previously defined at the Domain level.

Local policies will be set on the computers in the sub OU.

The Audit Policy rules are:

- Audit account logon events set to Success, Failure.
    - This tracks both successful and failed logon attempts.

- Audit account management set to Success, Failure.
    - This tracks changes to existing accounts, and additions of new accounts.

- Audit logon events set to Failure.
    - This tracks attempts to logon to the network that have failed.

- Audit policy change set to Success, Failure.
    - This tracks any changes to policies.

- Audit privilege use set to Failure.
    - This tracks any attempted use of a privilege that has failed.

Under the User Rights Assignment, settings could be set to lockdown the desktop configuration and to set quotas on disk usage. At this time this is not deemed necessary in the Research and Development Department.

Security Options are the next consideration. These perform registry changes for well-known security issues, the most important of which are:

- Additional restrictions for anonymous connections set to Do Not Allow Enumeration of SAM Accounts and Shares.
    - This prevents null session enumeration of account names and shares.

- Automatically logoff users when time expires set to Enabled.
    - This is to prevent hackers from connecting to the network and using shares outside of the time allowed for the user's account that he has stolen.

- LAN Manager authentication level set to Send NTLM v2 Response Only / Refuse LM and NTLM.
    - This ensures stronger encryption of the credentials for the session.

- Number of previous logons to cache set to 0 logons.
    - This enforces any changes to domain policies so a person cannot logon using old rights.

- Send unencrypted password to connect to third party SMB servers set to Disabled.
    - This prevents clear text passwords from being exchanged on the network where they can be sniffed.

- Message text for users attempting to logon (logon banner).
    - This should be set to a statement about the LAN being private for company use and only authorized employees are allowed to logon. This makes a legal statement that can be used in court proceedings if data contained on these systems is used without company authorization.

- Rename administrator account.
    - The standard administrator account should be given a new name that does not indicate that this is in any way a special account.

- Rename guest account.
    - Because guest is common on all Windows systems it should be renamed to some other name and disabled.

The next area of configuration would be Event Logs. The following settings should be changed:

- Maximum application log size set to 5120 kilobytes.
- Maximum security log size set to 5120 kilobytes.
- Maximum system log size set to 5120 kilobytes.

    - All three logs should be set to sufficient size that they won't over write. The logs should be copied to a central secure server and then cleared on a regularly scheduled basis, preferably no longer than a week.

- Restrict guest access to application log set to Enabled.
- Restrict guest access to security log set to Enabled.
- Restrict guest access to system log set to Enabled.

    - No logs on the system should be accessible by guest to prevent hackers from using the guest account and then covering their tracks.

- Retain application log set to 7 days.
- Retain security log set to 7 days.
- Retain system log set to 7 days.

    - The logs should be copied to a central secure server more than once per week. The 7 day setting will be longer than the time period between the copying of the logs, thus preventing any log data loss. The sooner the logs are copied the more chance that hackers activities will be detected when the logs are reviewed.

- Retention method for application log set to By Days.
- Retention method for security log set to By Days.
- Retention method for system log set to By Days.

    - This option will not allow data to be over written that is less than the number of retained days, as defined above. You could also choose Manual option for these log files which would not allow over writing at any time. Either option requires the logs to be copied to a central secure server and secured on a regular basis.

- Shut down the computer when the security audit log is full set to Disabled.

    - For an extremely high security environment this could be set to shut the computer down if a hacker managed to fill the logs and hide what he was doing. In most environments this is not necessary.

Any services not required by the computers in this OU should be set to Manual.

The next consideration will be the user OU configuration. In the users sub OU, under the Group Policy Properties tab you need to check the box to Disable Computer Configurations Settings. Then click the Edit button to open the current policy. Select Scripts (Logon/Logoff) and copy the Logon Script to this location. The Logon Script would map commonly used drives for this group of users, as well as any special application configuration that is necessary for this group.

Under the System folder, the sub folder for Group Policy should be selected and the following rules applied:

- Group Policy refresh interval for users Enabled and set to 90 minutes, with a 30 minute random seed.
    - This would ensure that Group Policies when changed are kept up to date and applied to the user.

- Group Policy slow link detection Enabled and set to detect links under 500 kilobits (Kb.).
    - This allows better use of bandwidth with slow links.

- Group Policy domain controller selection Enabled and set with a value – "Use any available domain controller".
    - This allows the user to look for any available domain controller.

We now need to ensure that only the Research and Development Department users can access their directory structures and files, this is done by setting NTFS access control lists. Access control lists would prevent other areas from accessing the Research and Development Department's data. Create a Domain Local Group RandD rights to assign the file rights to. Go under the Research and Development OU and the computers sub OU, and open the Group Policy Object, select Files Systems under Security Settings, then right click on File Systems and select Add File. Next, select a top level directory that is to have access restricted to the members of this Research and Development group, and then click OK. Remove the Everyone group, and add the domain local group RandD rights, that was just created above. No other groups need to be added here, however, you can add the Domain Admins, and possibly the Enterprise Admins groups as a backup for control of these file systems. You would also need to add Backup Operators group, to allow centralized backup of the files in these directories. We would next select the RandD rights group, and give this group full control. They are given this level of access because they are a special, distinct autonomous unit within the company and their necessarily secretive activities affect both the product development and the bottom line revenue for the company. Repeat these steps for all other directories or files that are to be restricted to this Research and Development group.

Now, we move the RandD computers group and all of the computers that belong to this group into the Research and Development OU and computer sub OU, and we move the RandD users group and all the users that belong to this group into the Research and Development OU and users sub OU. Then, add the RandD rights group to the RandD users group. This enforces the policies we just completed on these computers and users.

Human Resources Department OU Set Up

The Human Resources Department also requires special consideration because of its need for confidentiality, under the Electronic Documents Privacy Act. The initial OU set up will be the same as for the Research and Development Department, including creating sub OUs for users and computers. The Administrator assigned to the Human Resources Department will need to be given all rights to the Human Resources OU and all objects within that OU. The same policy template rules that were used for the Research and Development Department will work here as well.

Local policies will be set on the computers in the sub OU.

The Audit Policy rules are:

- Audit account logon events set to Success, Failure.
- Audit account management set to Success, Failure.
- Audit logon events set to Failure.
- Audit policy change set to Success, Failure.
- Audit privilege use set to Failure.

It is also important to consider the Security Options due to the confidentiality of the role of the Human Resources Department. These Security Options perform registry changes, the most important of which are:

- Additional restrictions for anonymous connections set to Do Not Allow Enumeration of SAM Accounts and Shares.
- Automatically logoff users when time expires set to Enabled.
- LAN Manager authentication level set to Send NTLM v2 Response Only / Refuse LM and NTLM.
- Number of previous logons to cache set to 0 logons.
- Send unencrypted password to connect to third party SMB servers set to Disabled.
- Message text for users attempting to logon (logon banner).
- Rename administrator account.
- Rename guest account.

Event Logs also need to be configured. The following settings should be changed:

- Maximum application log size set to 5120 kilobytes.
- Maximum security log size set to 5120 kilobytes.

- Maximum system log size set to 5120 kilobytes.
- Restrict guest access to application log set to Enabled.
- Restrict guest access to security log set to Enabled.
- Restrict guest access to system log set to Enabled.
- Retain application log set to 7 days.
- Retain security log set to 7 days.
- Retain system log set to 7 days.
- Retention method for application log set to By Days.
- Retention method for security log set to By Days.
- Retention method for system log set to By Days.
- Shut down the computer when the security audit log is full set to Disabled.

The user OU configuration for the Human Resources Department also needs to be addressed. This would be done under the Group Policy Properties tab for the users sub OU. The same procedure used in the Research and Development Department's sub OU would be applied to this GPO. Copy a Logon Script to the script's location in the GPO. The Logon Script will map commonly used drives required for the Human Resources Department's users, plus any special application configuration that is necessary for this group.

It is imperative that we ensure that only the Human Resources Department users can access their directory structures and files. This is achieved by defining NTFS access control lists to prevent other areas from accessing their department's data. This is accomplished by going under the Human Resources Department's OU and the computers sub OU, and opening the Group Policy Object. Next, select Files Systems under Security Settings, right click on File Systems and then select Add File. Finally, since access would be restricted to only the members of the Human Resources group, a top level directory needs to be selected, followed by clicking OK. Because of restricted access, you need to remove the Everyone group, and add the HR Users group. No other groups need to be added. You need to select the HR Users group and give them full control. They are given this level of access because of the position they hold in the company, and the dealings they have with company's personnel and confidential, personal issues. Repeat these steps for all other directories or files that are to be restricted to the Human Resources group.

After this point, we would then move the computers that belong to this group into the Human Resources Department OU and computer sub OU. We also need to move the HR users group and all the users that belong to this group into the Human Resources Department OU and users sub OU. This permits the enforcement of the policies we just implemented on these computers and users.

Admin OU Set Up

This OU is a container OU for administrative purposes. It holds the OUs for both the Finance Department, and the Sales and Marketing Department. The administrators for these two groups would be given full admin rights at the Admin OU level and thus would be able to administer all OUs at the lower levels. This container OU is situated here to simplify the configuration and administration of the Finance and Sales and Marketing Departments, which will be administered by the same resources.

The Finance and Sales and Marketing OUs would be set up following the same procedural steps that were used in both the Research and Development Departments and Human Resources Department. The same security policy rules would be applied. NTFS settings do not need to be as stringent except for areas where confidential financial, or marketing plans are contained. The Everyone group should be removed from all high level directories, and if there are no other restrictions, should be replaced by the Authenticated Users group.

Manufacturing, and Eastern Distribution Center OUs Set Up

These two OUs are comprised of users and computers in the Manufacturing Department and the Eastern Distribution Center. Each OU would also have sub OUs for users and computers as described in the previous OU set up procedures. Different resources would administer each OU. There are two different styles of administration used; the Administrators of the Manufacturing OU have access to both the Manufacturing Department OU and the Eastern Distribution OU, and each OU below these. However, the Administrator of the Eastern Distribution Center OU only has access to the Eastern Distribution Center OU and each OU below this level.

The Manufacturing Department OU and the Eastern Distribution Center OU would each be set up following the same procedures as outlined for the Research and Development Departments and Human Resources Department. The same security policy rules would apply. Again, NTFS settings do not need to be as stringent except for confidential manufacturing designs. As well, the Everyone group should be removed from all high level directories, and if there are no other restrictions, should be replaced by the Authenticated Users group.

Other Domain Servers

There would be a Certificate Server to issue x.509 security certificates. This Certificate Authority would be signed with a publicly recognized Certificate

Authority such as Verisign so the certificates issued will be acceptable to public browsers and can therefore be used to identify the Corporate web site and secure e-business transactions with customers using SSL. Certificates would be used to identify the authenticity of the web site, as a private key to set up secure SSL sessions with on-line customers, for authentication on the web and FTP servers for sales employees and partners who need to access to secured information located there, to authenticate employees who dial into the RRAS server for access to the internal network, and file system encryption for sensitive documents such as employee records, marketing plans, designs, and manufacturing instructions. The company has been considering using smart cards in the future and the certificate server could also be used to load a certificate onto a smart card for logon authentication.

An RRAS server would be installed to handle employees on the road who need to dial in to access internal network facilities. The user would authenticate with an x.509 certificate and a VPN would be set up between the user and the internal network to protect the communications.

Secure Web Sites and Communications

"The Web site and browser have become the central mechanisms for open information exchange and collaboration on organizational intranets as well as on the Internet. However, standard Web protocols such as Hypertext Transfer Protocol (HTTP) provide limited security. You can configure most Web servers to provide directory and file level security based on user names and passwords. You can also provide Web security by programming solutions using the Common Gateway Interface (CGI) or Active Server Pages (ASP). However, these traditional methods of providing Web security are proving less and less adequate as attacks against Web servers become more frequent and sophisticated. You can use Internet Information Services (IIS), included with Windows 2000 Server, to provide high levels of security for Web sites and communications using standards-based secure communications protocols and standard X.509 certificates.

You can provide the following security for Web sites and communications:

- Authenticate users and establish secure channels for confidential encrypted communications using the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.

- Map user certificates to network user accounts to authenticate users and control user rights and permissions for Web resources based on users' possession of valid certificates issued by a trusted certification authority."[4]

Web Site Domain Set Up

Web and FTP servers would be set up in a protected DMZ that would allow both unauthenticated public access and authenticated Employee and Partner access to information contained on these servers. To allow authenticated access there would be a domain controller on a separate protected DMZ that has a one-way explicit trust with the domain controllers inside the network. This domain controller is not part of the corporate domain forest. There would be no users defined on this domain controller. It would only be used as an authentication path to the internal domain controllers. Install the latest Service Pack and Hot Fixes to ensure any known security weaknesses are addressed. Group Policy Objects would be set up to standardize the security on the web servers and FTP servers. This Group Policy Object would use hisecweb.inf as the template for security on all of these servers.

NTFS permissions need to be carefully set to ensure that visitors to the web and FTP servers can only go where they are intended to go. Remove the Everyone group from root level directories and give Administrators and System full control and apply this to all sub-folders and files. Set up auditing on the Everyone group for both failed and successful access attempts of all types. After IIS is installed, the default website (\Inetpub\wwwroot) should be moved to a separate disk from the Operating System (if this is not possible it needs to be installed into a separate partition). Disable all services not needed for the site to operate. Unbind NetBIOS and any other protocols leaving only TCP-IP as this is all that is needed on these servers. Set the registry value of HKEY_LOCAL_MACHINE \System\CurrentControlsSet\Services\Tcpip\Parameters SynAttackProtect to 2 to prevent resources being committed before a complete 3-way handshake and to reduce the number of SYN-ACK retries.

Create web site folders that do not follow the standard naming Microsoft uses. This would prevent worms that are looking for objects in standard places from finding their targets. Be sure not to give any folder both Write and Execute permissions as this would allow a hacker to upload any executable and then run it.

Remove support for Internet Printing by removing the 'printers' directory from web site directory structure. Also be sure to remove the Web-Based-Printing from the Group Policy Object that is controlling the setup of the web servers.

---

[4] "Deployment Planning Guide, Windows 2000 Server, Part 3 Active Directory Infrastructure, Chapter 11 Planning Distributed Security", pg. 425, Microsoft Corporation, July 1999

Unmap all unused ISAPI extensions as many of these have proven to have buffer overflow problems and be vulnerable to DoS attacks. Be sure to unmap the ISAPI extensions again whenever a Windows Component is changed using the Add/Remove Programs in Control Panel, as the default extensions will be replaced. Also remove any ISAPI Filters that the site would not be using.

References:

"Active Directory Users, Computers and Groups (White Paper)", Microsoft Corporation, February 2000

"Deployment Planning Guide, Windows 2000 Server", Microsoft Corporation, July 1999

Scambray, Joel, McClure, Stuart, and Kurtz, George. "Hacking Exposed - Second Edition", Osborne/McGraw Hill, 2001