Global Information Assurance Certification Paper

GIAC Enterprises Secure Active Directory Design

GCWN Version 3.1
Option 1 – Design a Secure Windows 2000 Infrastructure

Michael Greene
Sunday, January 16, 2005

Table of Contents

GIAC Enterprises Company Profile

For the past ten years, GIAC Enterprises has been a world leader in the finance sector. GIAC Enterprises specializes in providing investment capitol for companies interested in combining within the same industry to provide a more thorough market saturation and a better effectiveness in obtaining and using global resources. GIAC will not only fund profitable investments but provides internal consulting staff to optimize the transition in terms of reorganization, merger of management personnel, technical integration, and resource optimization.

GIAC Enterprises, founded in Chicago, IL, has grown to a multinational corporation. Typically, GIAC will open a new office in cities where there is financial support for start up companies to spawn and a potential consumer market to support new business. These qualifications tend to fit large cities with growth potential and an evolving interest in the quality of urban development. Once GIAC has a proven record of profitability in a geographic region, a major site will open in a location that has shown a supportive job market and superb quality of personnel to lead developmental interest within the corporation.

Corporate personnel such as Research and Development, Sales and Marketing, Finance, and Human Resources, each have a presence in all major and minor sites. In terms of the flow of business and transactional volume, each minor site reports to a major site and each major site reports to the Chicago site. Major sites support a minimum of 1,000 users and minor sites support an average of 100 users. Each minor, or branch site, is given technical resources to store user data locally, and the support personnel to support day-to-day activities. Any unresolved technical issues from minor sites are escalated to technical support personnel at major sites. Each major site hosts technical support staff, and the original site in Chicago is the primary source of leadership for the information technology department.

GIAC has grown to a global scope and has recognized the value in specialization of both people and resources. This has lead to an optimal consulting partnership between major sites so that new clients may be recognized and approached before growing beyond the state that would force a globalization effort to result in loss of jobs and costly resources. Contacts at minor sites are mostly responsible for sales and marketing within their local markets. Once an opportunity has been recognized, the accounts are researched, developed, and maintained primarily from major sites. To support these types of relationships, the company has formed swift lines of communication between sites but executives are concerned that the current level of security may be susceptible to compromise.

The management personnel at GIAC Enterprises are aware of the benefits from reinvesting profits within the company. While the current network infrastructure for the firm has been suitable to date, the developments in technology within the past 5-10 years have proven to increase collaboration and effectiveness in the work environment. An executive decision has been made to replace the current infrastructure with the latest proven technologies and the foresight in design methodology to allow infinite expansion and a convenient movement into future possibilities in the technology realm.

Standard Naming Conventions

In an enterprise environment such as that of GIAC Enterprises, it is important to establish clear-cut standards for naming conventions. The GIAC security model allows users and administrators to travel from site to site with ease, and keeps the same security permissions independent of geographic location. In order to organize Active Directory objects and simplify administrative tasks, all machines will be named with a standard prefix to designate site name. User accounts will not have this prefix because they are not site-specific.

Naming conventions will follow a strict abbreviation. The first two letter will designate the domain, associating either D,C, or W.

The next three letters from the name of the city where that site is located, or the nearest associated community, will prefix the name of each machine. In the event that a city is made up of two words, the first letter of the first word, and the first two letters of the second word will designate the name, to prevent multiple "new", "los", or "north" names, etc.

Chicago – CHI
London – LON
Los Angelos – LAN
Dallas - DAL
Denver - DEN
Seattle - SEA
Atlanta - ATL
New York - NYO
Guadalajara - GUA
Berlin - BER
Paris - PAR
Rome – ROM

Following the location will be a two-letter abbreviation to designate the role of the server. The standard for the two-letter abbreviation is loosely associated to make abbreviations less confusing. Any two letters may be used as long as they cannot be confused with a different role in the environment and clearly designate the intended role.

Domain Controller – DC
Distribution Server - DS
Disaster Recovery Server - BK
Mail Server – ML
File and Print – FP
Web Server – WB

Finally, the name will be appended with a two-digit number starting at 01 to make each name unique for roles that require more than one machine, so that names will follow as demonstrated below.

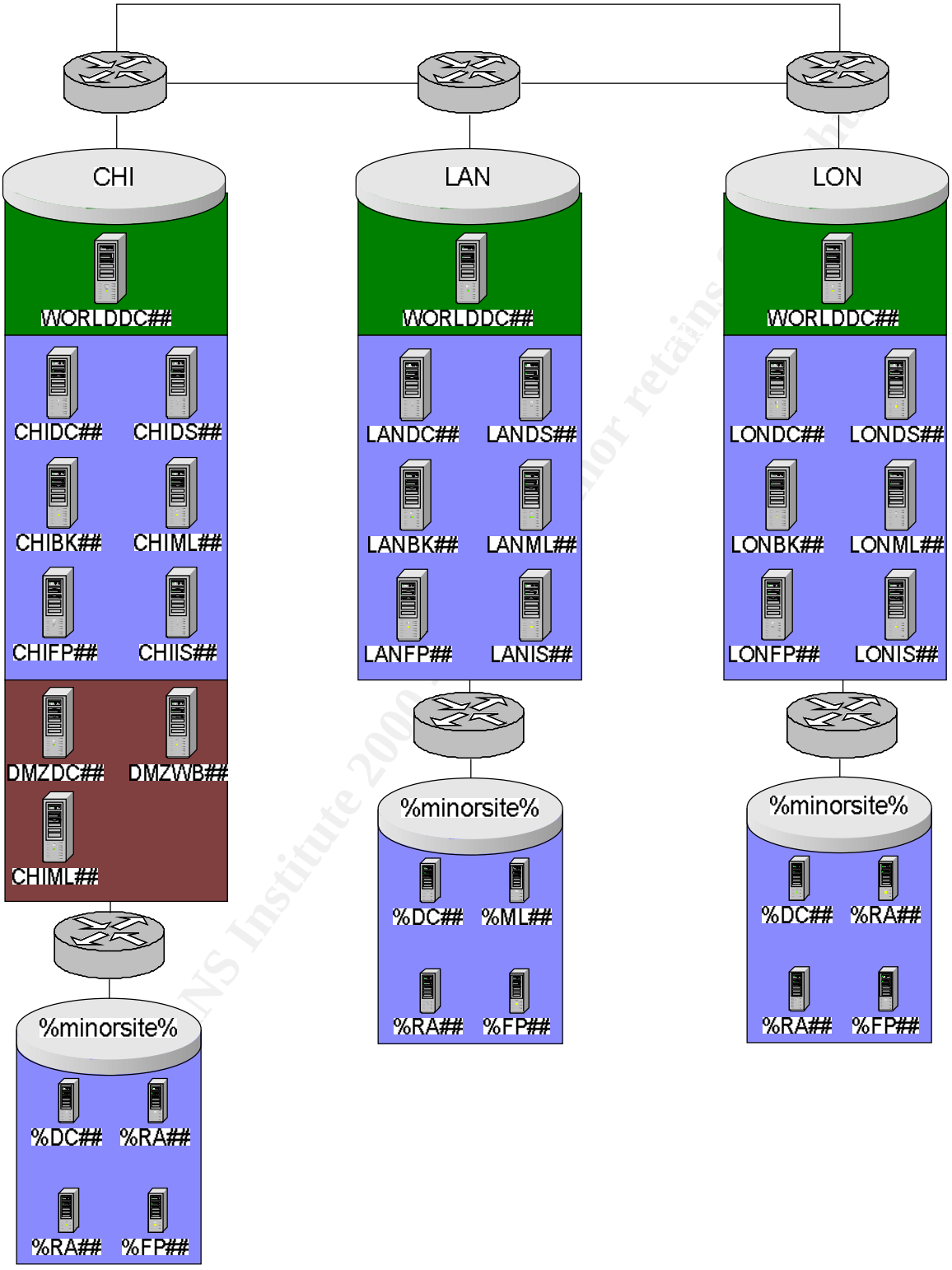
<domain><location><role><number>
Substituting "C", "CHI", "DC", and "01", the name becomes CCHIDC01.

The exception to this rule is the workstation naming convention, which is special because of the division of work groups in the enterprise and not geographic location. The two-digit role abbreviation will be doubled adding two letters to signify the role, two for the work group, and the name will be appended with six rather than two digits to compensate for the existence of more than 99 workstations in each group. The six digits will match the last six digits of the machine's serial number as labeled by the manufacturer.

Research and Development – RD
Sales and Marketing – SM
Finance and Human Resources – FH

<role><work group><number>
Substituting "WS", "RD", and "0001", the name becomes WSRD01.

Network Design and Diagram



Necessary Servers for Major and Minor Sites

Server placement is meant to satisfy the expectations for current throughput requirements and to provide conditions for growth. Each major site must support a minimum of 1000 users and each minor site must support an average of 100 users.

Minor sites are supported remotely by staff from Major sites. All servers at branch offices, except for file and print severs, will be in locked racks and local personnel will only be given access to administer help desk issues such as password resets, account management, backup maintenance, printer administration, etc. Each site will have a secure area with biometric authorization, backup power, cooling facilities, and fire prevention facilities.

Server Type	Major Site	Minor Site	DMZ
Active Directory Domain Controllers	3	1	1
Microsoft Exchange Servers	2 back end	1	3 front end
File and Print Servers	2	1	0
Microsoft Internet, Security and Acceleration Servers	5 (array)	0	0
Externally Accessed Web Hosting	0	0	3 w/NLB
Internally Accessed Web Hosting	5 w/NLB	0	0
Disaster Recovery Solution	5	Integrated with Mail Server, and Data Server	0
Distribution Server	1	Integrated with Domain Controller	0
Routing and Remote Access Servers	3	1	0
DNS	Integrated with Domain Controllers	Integrated with Domain Controller	2

Overview

The major sites are responsible for supporting a greater number of users and have functionality that is necessary for minor sites to maintain connectivity to the Internet. Both domain controllers and mail servers will need to replicate or relay data to minor site servers. Some servers, including distribution, file and print, and web servers, will be accessed routinely by users from minor sites.

The servers at minor sites will host authentication, mail, and data storage for a more limited number of users. The servers will be built and tested at major sites and then shipped to minor sites. The servers should only need to be "plugged in" once mounted at the minor site to function in their normal capacity. All support of these servers will be performed via terminal services from major sites. The support staff at minor sites will only be responsible for maintaining the local file and print servers. The domain controllers, mail servers, and RRAS servers at minor sites will only be physically accessible to local staff; the staff will not have rights to log on locally. In fact, the only function that local support staff is able to perform is the task of changing backup tapes nightly.

In terms of hardware, all servers will be ordered from the Dell Corporation and will be rack mounted in a secure location. A special room will be provided with construction considerations to provide a secure, fire resistant, and environmentally superior atmosphere. The specific hardware specifications of each server are outside the scope of this document, but will be appropriate for the role each server will play. All servers will have redundant components to prevent downtime due to hardware failure.

Active Directory Domain Controllers

Domain Controllers are responsible for storing user accounts and providing a point for network authentication. In addition, three other components, DNS, WINS, and Enterprise Certificate Authority, will be loaded one these machines. The Flexible Single Master Operations roles[1] will be distributed between the two machines at the Chicago site. One server at each major site and at each minor site will contain a copy of the global catalog. One domain controller will be placed at each major site to host the empty root WORLD domain. Each domain controllers for the WORLD domain will contain a copy of the global catalog. It is important to secure all domain controller machines as much as possible because local administrators of these machines are capable of gaining infinite access to the domain. Because of this, special group policies are set for these servers.

It is necessary to place three domain controllers at major sites and one at each minor site. This is to create a robust environment with fewer points of failure and lower network traffic across WAN links and to provide authentication for minor sites if the WAN connection should be broken.

Servers that support the DMZ will only be located in Chicago. One domain controller will be required to support Windows-integrated authentication for web applications and SQL integration. This domain controller will have to be locked down as much as possible to prevent domain admin access to attackers.

Domain Controller servers will host DNS and WINS for name resolution throughout the enterprise. The WINS servers will each be set to replicate with all other WINS servers in a push-pull partnership. The DNS servers will host typical Windows Active Directory DNS zones. Two servers will be set up in the DMZ that will not be part of any domain, but will host the external DNS zones for the domain.

These machines will be responsible for hosting the enterprise certificate authority. This machine will create certificates or host certificates that need to be trusted by domain machines. In addition to this machine, a stand alone certificate authority may be created offsite if a business need is later identified.

Microsoft Exchange Servers

Exchange servers provide mail, news, and instant messaging services for the network. Microsoft Exchange is a suitable application because it is meant to integrate with Active Directory and Windows 2000. Servers at major sites will be configured in a front end – back end setup. This provides a more robust solution because the servers configured as "front end" provide connectivity and perform transactions involved in mail services while the "back end" servers actually store data. This type of configuration provides better performance for users because fewer connections are made with the Exchange database(s). This also creates additional security because the front-end server will be hosted within the DMZ, and all information will be stored securely on back-end servers inside the network perimeter. An SMTP relay will be established in the DMZ with antivirus functionality to scan incoming and outgoing SMTP traffic for virus infection.

Servers at minor sites will not need the separated design because fewer transactions will occur on these machines. It is beneficial to have local servers at each minor branch to store mail for local users. This provides access to messages in the event the WAN connection is broken, and cuts down on WAN traffic because the transfer of mail and news data can be scheduled for replication during off peak hours.

[1] Microsoft White Paper, "*Active Directory Architecture*", Page

IPSEC will be used to secure the connections between these "front end" and "back end" servers. The general group policy for all servers will be used to lock down Exchange servers. In addition, Exchange is capable of operating using special service accounts, which should have extremely complex passwords set and stored in a secure off-site location. The Exchange database will be corrupted if scanned by most antivirus applications. With this concept in mind, the database and the "M:" drive, which Exchange creates to store information for web integration, must be excluded from real time protection and antivirus scanning. A special version of Norton Antivirus will be installed that is intended for integration with Microsoft Exchange. The "M:" drive should have NTFS permissions set on each folder that only allow access by the owner of messages stored in each folder.

File and Print

File and Print servers store all user data for every user on the network. To support this function the servers must have massive storage capabilities and processing power. The storage capabilities are necessary to store user profiles and corporate file stores. The processing power is necessary because EFS will be used to secure all data of sensitive nature and appropriate user data will be indexed. Certificates for EFS will be exported and stored in a safe place to prevent access to anyone but authorized staff from decrypting content. User home directories will be prestaged with the following hierarchy:

Indexed

Secure

    Indexed

User training will be required so that all users will take responsibility for placing resources in the appropriate stores. At the first level, only the "Secure" folder will be encrypted. This will cut down on processor time required to encrypt and decrypt files because users can store not-sensitive data in the "not secure" directories. In a similar fashion, under the "Secure" folder a second level is defined for indexed, encrypted files. Files under the "Indexed" portion of the hierarchy will be searchable and no directories will be searchable (for content). This will cut down on the time required to index files and will result in more efficient searches and better overall performance.

IPSEC will be used to encrypt the transfer of all data between File and Print servers and other machines. This will be configured in the group policy assigned to the servers OU and workstations OU, in addition to other policies already designed to secure servers in the GIAC environment. This encryption will include the PKI infrastructure so that certificates can be used to authenticate communications between machines and encrypt transfers.

Two servers of massive capacity will be placed at all major sites and one server with less capacity will be placed at each minor site. Minor sites will only store data for user profiles and corporate data only for the local office. All corporate data that involves more than one site will be stored at major sites. Storing as much data as possible locally cuts down on the transfer of sensitive data across WAN connections, cuts down on WAN traffic, and provides users access to most of their data in the event that a WAN link is broken.

ISA Configuration

Each major site will have an ISA array of five servers. These servers will share the workload of content filtering, caching, and access control. To allow for greatest functionality, the servers will be configured as the "both" role, allowing for both caching and firewalling capabilities and will have two network interface cards. The equipment hosting these services will need to be robust, as each server array is responsible for all Internet traffic from one major site and the respective minor sites.

The server will be setup with a "client address set" limited to appropriate subnets so that only computers with approved addresses (pending user authentication) will be allowed outbound access.

Clients will be automatically configured with proxy settings via DHCP. The firewall client will be transparently distributed to workstations. The firewall client will allow for a single sign on environment and will make it possible to monitor Internet access other than standard Web request logging.

ISA servers will also host an antivirus application from Trend Micro to scan incoming and outgoing HTTP and FTP traffic for virus infection.

These servers will be members of the servers OU, and thus will be locked down via the same group policy as all other servers. Although it is common practice to lock down ISA servers using extremely secure practices, these ISA servers will not have direct internet exposure and thus will be secured in the same fashion as every other server on the GIAC internal network.

Web Servers

Web servers in the GIAC environment will be divided by function. This includes "internal servers" which will only be accessible by users with direct (or VPN) access to the GIAC network. These web servers will host sensitive material including human resource and accounting applications. Internal web servers will be members of the CORP domain and will have special group policies designed to secure these servers in excess of the standard server policy. All communications will be secured using SSL when appropriate, and in addition, IPSEC will be used to encrypt communications between these and any other machines.

Internal web servers will only exist at major sites. Each major site will host seven "internal" web servers with network load balancing provided by Windows Load Balancing. The web servers will host content that is specific for each major site and the minor sites that are children of those sites. Much of the data includes corporate data that will be processed locally at major sites, so only the actual web pages and content that process data will need to be replicated to all sites when altered. This can be performed either manually, or if manual replication becomes a nuisance, DFS may be employed in the future.

External web servers either will be stand-alone or will be members of the DMZ domain. Group Policy will be used to lock down servers as much as possible in this domain and will be applied as local policies to external web servers that are not domain members. Because of the proximity to the Internet, these machines will be locked down using Microsoft and National Security Agency best practices for IIS 5.0 web servers. SSL will be used wherever necessary to encrypt communications.

Server placement for external servers is simple because they only exist in the DMZ, which is hosted at the Chicago site.

Backup Recovery

Backup recovery, or tape backup servers, will be placed at all sites. Three servers will be hosted at each major site due to the extensive amount of data that must be backed up. One server with dual tape drive integration will be responsible for backing up File and Print servers. Another server, also with dual tape drives, will be responsible for Exchange data. These two servers will need to run backups almost nonstop to maintain daily incremental backups of critical data. The third server will backup up system state data and business critical data from all other servers at major sites. This would include weekly or biweekly full backups of most servers.

At minor sites, the Exchange servers will contain tape drives and backup recovery applications to maintain daily backups of the mail server, nightly backups of system state data, and weekly full backups of the domain controller. The file and print server at minor sites will also contain tape drives that local support staff may use to backup user data as appropriate. Most likely, these servers will have daily incremental backups.

Distribution Servers

The distribution servers perform three similar and one unique function(s). The first is to store repackaged applications for distribution. Microsoft Systems Management Server will be installed and used to push out applications to all machines. Application distribution is outside the scope of this project except that the files and folders stored on the distribution folder should have access control set so that only the correlating application groups have read access. This security strategy prevents unauthorized installation of applications for users with low-level admin access.

In a similar manner, the server will host operating system images used for deployment of Symantec Ghost images via RIS (remote installation system). The Microsoft distributed file system (DFS) will be used for multi-master replication of application distribution files and operating system images to all other distribution servers in the environment.

The second function of these servers is to host the server component of Norton Antivirus Corporate Edition. This application will be used to provide virus protection to all machines in the GIAC environment. Live Update will be used to download virus definitions twice per day and the remote user function of this program will allow users to always access definitions from the server at the site with fastest connection.

The third function of these servers will be to host Microsoft Software Update Services. Patches, hotfixes, and service packs released by Microsoft for the Windows operating system will be downloaded to these machines. The Microsoft Software Update Service will be used to approve newly released updates after regression testing in a new environment. Updates will then be distributed using the functionality built in to the SMS value pack as discussed later in this document.

The fourth and final function hosted by the distribution server is to offer IP addresses through DHCP. It is beneficial for the same machine that hosts RIS functionality to also host DHCP services. The Exchange server at each minor site will host DHCP.

One of these servers will be placed at every major site. At minor sites, the distribution server will be combined with the domain controller on one machine. Minor sites will have secondary servers for SMS, Antivirus Live Update, and Software Update Service to prevent excess WAN traffic during peak hours.

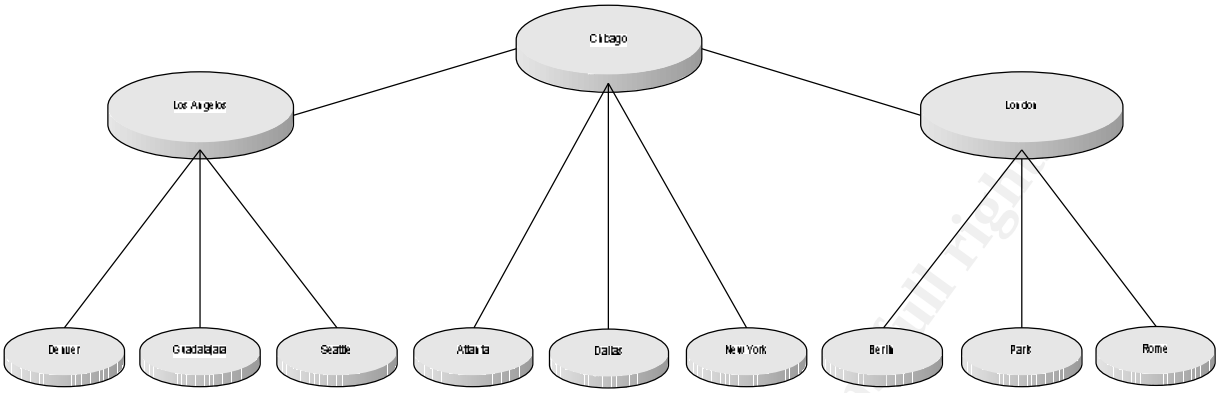
RRAS and IPSEC configuration

To meet client requirements, Microsoft RRAS will be used whenever possible to terminate incoming and outgoing VPN connections. These connections will be required to authenticate as the appropriate service account and the computer will have to negotiate the appropriate certificate authentication to create an IPSEC tunnel.[2] To prevent unmonitored transmissions, minor sites must first connect to a major site in order to communicate with any other source. This includes other major sites, other minor sites, or the Internet. Although each site will be responsible (in terms of cost) for a broadband connection to the Internet, all traffic to and from the site will be encapsulated and routed to a major site. This improves upon the cost of private connections and adds flexibility to prevent a single point of failure.

Because each minor site will rely on the VPN connection for connectivity, each site must have a server dedicated to Routing and Remote Access. The major sites will host three Routing and Remote Access Servers, one to maintain each VPN connection. Because all RRAS servers have direct Internet exposure (behind a hardware firewall), the servers must be configured as securely as possible using Group Policy, IPSEC, and Microsoft best practices.

[2] Systems and Network Attack Center (SNAC), National Security Agency; "*Microsoft Windows 2000 Network Architecture Guide*" , Page 6

Active Directory Design and Diagram



Major Sites

The network consists of multiple sites, with three main sites acting as central hubs. The ability for these sites to support connectivity for the branch offices is critical for business operations.

The hosting sites are located in:

Chicago, IL
London, England
Los Angeles, CA

Minor Sites

Branch offices consist of smaller operations and fewer users to support. These sites are connected to the main sites using virtual private networks. There are fewer users at remote sites and thus fewer servers in place to support operations. All servers at remote sites except File and Print will be administered by staff from major sites. Servers are placed at minor sites so that if the VPN connection was broken the site could function independently and would only lose Internet connectivity.

US Sites	International Sites
Atlanta, GA	Berlin, Germany
Dallas, TX	Guadalajara, Mexico
Denver, CO	Paris, France
New York, NY	Rome, Italy
Seattle, WA	

Forest Design

GIAC Enterprises has determined that it is most appropriate to maintain a single forest. A single forest environment will be used and internal security requirements will be based on Domains and Organizational Units.

Designing an environment with multiple forests creates additional administrative overhead for very little functional benefit.[3] Since the release of Windows 2000, it is on longer necessary to divide forests for security reasons. Division of domains and domain design including OU and group structure can resolve almost every issue associated with the need for separate forests. The only reason for GIAC to ever create a new forest would be if the schema in Active Directory needed to be unique for a future business requirement. The installation and integration of additional forests for reasons such as unique software and separate security models should be avoided whenever possible.

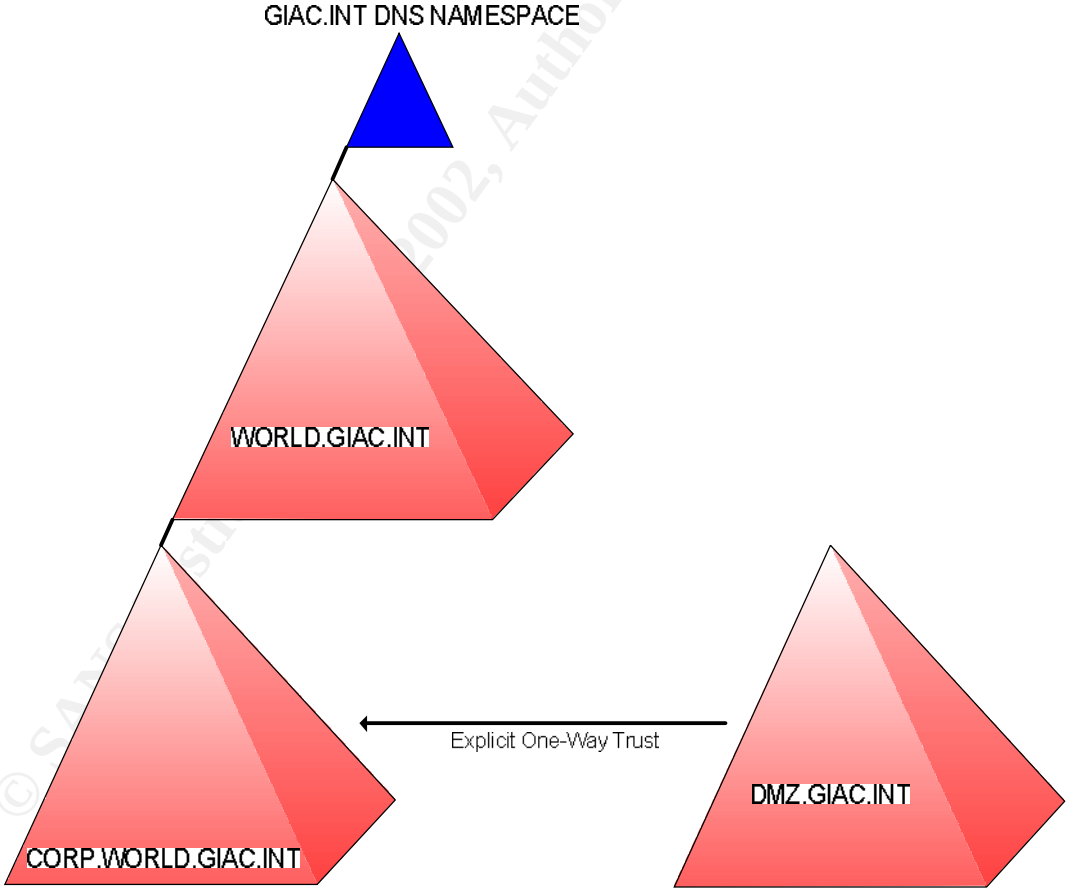
[3] Systems and Network Attack Center (SNAC), National Security Agency, "*Guide to Securing Microsoft Windows 2000 Active Directory*" , Page 19

Domain Design and Domain Controller Placement

The Domain is designed with a Forest Root domain (*world.giac.int*) and a Child Domain (*corp.world.giac.int*). The Root domain houses the Schema and configuration information, as well as the Forest FSMO roles and its own domain FSMO roles. If the root domain controllers were lost, the forest would no longer operate correctly. It is very important that there be at least two Domain Controllers for the root domain (minimum). It is recommended that one be kept offsite from the other and that they both be backed up Daily (and restore procedures are documented and tested).

Other advantages of an empty root domain include:

Fewer administrators can make forest wide changes
Easily replicated for forest backup (A small forest root domain can be easily replicated anywhere on your network to provide protection against geographically centered catastrophes.)
Never becomes obsolete (Since the root domain can never be retired, having an empty one guarantees it will not become obsolete since its only role is to be the forest root.)
Ownership easily transferred (If ownership of the root domain must be transferred it will not require any migration of data or resources.)



GIAC.INT

This domain will actually only be a DNS namespace. This provides flexibility for future projects and possibilities for expansion without the need to completely rebuild the internal network.

WORLD.GIAC.INT

This domain will serve as the empty root for GIAC Enterprises. The purpose of this domain is purely for security and for expandability of the network, very few objects will actually reside within the domain. One domain controller at each major site will collectively host this domain.

CORP.WORLD.GIAC.INT

This domain is the "working" domain for the GIAC network. All objects not in the empty root or DMZ will be a part of this domain. The users at each site must be able to log on to the network even if the WAN connection is not available. With this requirement in mind, one domain controller will be placed at each branch office, and two domain controllers will be placed at each major site, with the possibility of expanding the major sites to three servers if necessary.

DMZ.GIAC.INT

This domain will be set up for all servers in the DMZ. This domain will be at the same level as the CORP domain with a one-way trust relation ship. The DMZ domain will trust the GIAC.INT domain so that users in the GIAC domain can access the servers in the DMZ with their standard accounts. However, the GIAC domain will not trust the DMZ domain. One domain controller will host the DMZ domain from the Chicago location with very strict policies assigned to it and all child machines.

Trusts

A one-way trust will be configured between CORP.WORLD.GIAC.INT and DMZ.GIAC.INT. This will support authentication for development of web applications in the DMZ without the overhead of addition domain design and duplicate accounts.

The security model for the trust relationship inherently protects the internal domain from unauthorized access. The one-way trust relationship makes it possible for users in the internal domain with required permissions to access the servers in the DMZ using their standard user accounts.[4] However, if the servers in the DMZ are compromised by attackers, because the trust is only in one direction, the hijacked accounts from the DMZ.GIAC.INT domain will not have any rights to any internal domain.

Domain Time Server

By default, Windows 2000 clients and member servers synchronize with a DC in their domain, DCs synchronize with the PDC in their domain, and PDCs synchronize with the PDC in their parent domain. Thus, the PDC in the forest root domain is the authoritative timeserver for the forest and should be synchronized to an external time source.

The DC holding the PDC FSMO role for the forest root domain will be configured to synchronize with an external SNTP Server (time.nist.gov).

The following command, executed on the aforementioned DC, will provide this configuration: NET TIME /SETSNTP:time.nist.gov

[4] Systems and Network Attack Center (SNAC), National Security Agency, "*Guide to Securing Microsoft Windows 2000 Active Directory*" , Page 21

Organizational Unit (OU) Design

Active Directory will be organized using a design that is as secure and simple as possible. The organization is premised on the idea that user rights should flow between sites. This essentially means an administrator at any site should have equal rights at all sites. The hierarchy will begin with the original containers. The GIAC Users and GIAC Computers OUs are added to simplify administration by dividing object types. All objects of the respective types will be divided according to the need for variance in policy or "levels of security".

The objects in Active Directory will be divided according to levels of security, which will be Administrators, Service Accounts, and Users for the Users OU; and Services, Data, and Workstations, for the Computers OU. The workstations OU will be further broken out into work groups for increased security as discussed later.

Within each of these containers, a fundamental organizational structure will be created for container purposes to aid organization. These basic OUs will be Accounts and Groups. All account objects will be put into Accounts OUs and all group objects will be put into Groups OUs. This fundamental organizational structure will provide simplicity in security by optimizing the administrative effort required to securely delegate authority. Each branch of the OU structure will be configured with simple outline to make sense of account objects, group objects, and what security should be assigned to each division of security levels.

Major OU

Security Level

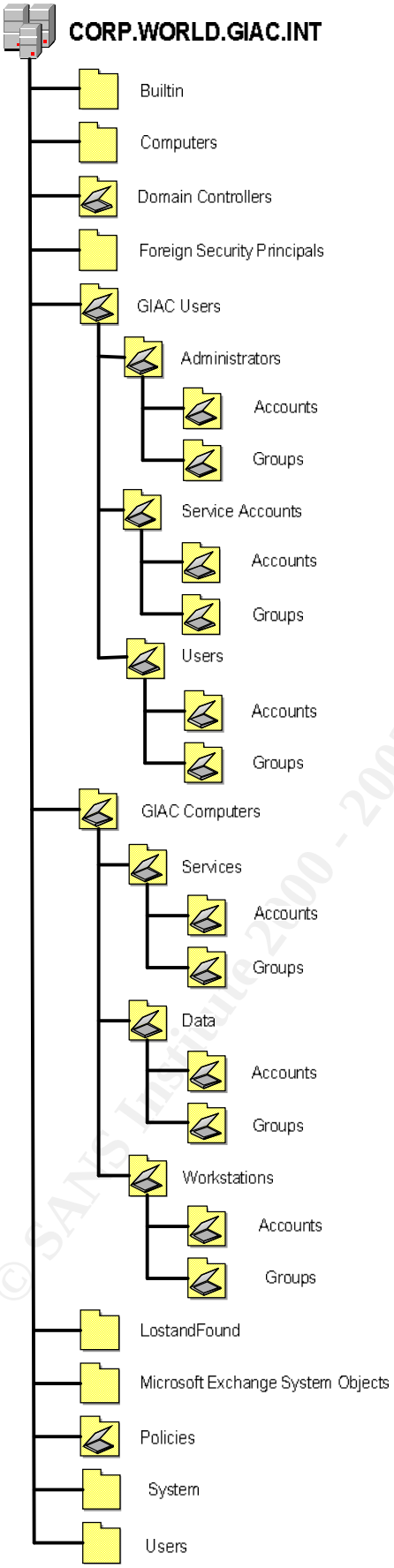
Accounts

Groups

Due to the distributed administration model, the ACL on each OU must be set so that appropriate user groups have rights. For example, all administrative accounts and groups will be in the Administrators OU, and so the ACL on this OU should be set to prevent user access. On a more granular scale, some groups, such as those for applications, and those for senior admin roles, will need to have access control set individually to prevent access by accounts within the same OU branch.

This presents a somewhat complicate OU model, but in the end, it will simplify security administration and prevent the creation of unnecessary groups and accounts out of convenience. Such objects often result in loosened security. For a visual breakdown of the OU structure, see the image on the following page.

The OU structure for the World and DMZ domains is not illustrated here nor is it elaborately discussed. That is because the organizational units and containers built in to Active Directory by default provide enough complexity to securely organize the objects required. The most complexity needed will be for the DMZ domain to have a DMZ Computers OU, with the fundamental accounts and groups OUs, where computer objects will exist in and groups may be created if required for special purposes. No additional objects must be created for either domain and so no discussion of either of these domains will continue here.



OU Design Description

The following describes each Organizational Unit not included in Active Directory by default installation. For additional detail, please see the "organizational unit structure" diagram.

GIAC Users

This OU contains all user objects. Policies applied to this OU must be appropriate for every account in the domain. To simplify administration, few policies should be applied at this level.

Administrators

This OU contains all accounts used to log on as local domain administrators and perform administrative functions. Policies applied here grant increased user rights, file permissions, while restricting chances of being hijacked through settings such as increased password security, and decreased time before lock out. The security on this OU will only allow Administrative accounts access.

Accounts

All administrative accounts will be in this OU.

Groups

All administrative groups will be in this OU. Some groups in this OU need more granular access control lists.

Service Accounts

Container for all accounts used to authenticate services. This OU is created to alienate service accounts and prevent unintentional change. Policies applied to this account may increase security as much as possible without conflicting with functions of the service accounts. Only Administrative accounts will be allowed to access this OU. At this time, there is no reason for a Groups OU within this container.

Accounts

All service accounts will be in this OU.

Users

Every user account in the GIAC domain will be placed within this OU. If a policy needs to be applied only to certain users, users will become members of global groups and the policy will be applied to the group in the Groups OU. Policies at this level should increase security as much as possible while allowing users to perform business critical functions. Remote Administrators will be able to identify users in their location by the abbreviations in naming standards. The access control applied to this container should allow read access to all authenticated users but only allow write access from the proper administrative accounts.

Accounts

All user accounts will be in this OU.

Groups

The groups in this OU are for many functional reasons. The first set of groups will be global security groups for granting access to resources within the domain such as printers, folders, and web sites. Security groups will include either global groups signifying a "Role" within the organization, or domain local groups signifying a "Task" and their names will be prefixed as such.

The second set of groups will be for application distribution and will have the prefix "APP". These groups will be correlated with collections in Systems Management Server. Members of APP groups will have applications automatically assigned to them. Access Control Lists should be assigned to this container, and to each respective group, to prevent users and unauthorized admin accounts from making themselves members of these groups.

The third set of groups in this OU is for site assignment and will be prefixed with the abbreviation "SITE". These groups are created to assign folder redirection in group policy.

The fourth and final group needed in this OU is to define work groups. These groups will be prefixed with the letters "WG" and will be named after their correlating workstation OU. By assigning users membership to these groups, administrators are essentially allowing them to log on to machines in that work group, and preventing users from accessing classified information stored in software installed on machines in other work groups.

GIAC Computers

This OU contains all computer objects with the exception of Domain Controllers. Policies applied to this OU must be appropriate for every server and workstation in the domain. To simplify administration, few policies should be applied at this level.

Services

All member servers that provide a service on the network will reside within this container. This includes Mail, Distribution, Web Host, SMS, Proxy, Routing, Backup, and Update. These servers are administered by staff from major sites only. Remote administrators have no rights on these machines. Group Policy should lock down these machines as much as possible without preventing functionality. Security should be assigned to this OU to allow read access to all users but only allow write access from the proper administrative accounts.

Accounts

All server accounts will be in this OU.

Groups

Any groups needed for specific policy assignment may be created here.

Data

This OU contains the servers that host file and print services at branch sites. These machines are administered by Remote Administrators and thus have different user rights (assigned using group policy) than "Services" computers. Group Policy assigned on these machines will be much like that of the "Services" OU plus the addition of IPSEC configuration. Security should be assigned to this OU to allow read access to all users but only allow write access from the proper administrative accounts.

Accounts
All data accounts will be in this OU.

Groups
Any groups needed for specific policy assignment may be created here.

Workstations

This container is only meant to simplify organization by setting apart workstation OUs from server OUs. At this time, no policies will be applied to this OU.

Research and Development

Policies applied to this OU will secure workstations from access by users not intended for this work group. User rights, Registry security, and File System security will be configured using group policy to only allow members of this group and administrators access to these machines. This will prevent users of other work groups from logging in to these machines and accessing software not intended for them. The groups associated with this work group will be created in the Groups OU under GIAC Users – Users. Access Control Lists should be assigned to this container and to each group to only allow read access to authenticated users and allow writable access to the proper administrative accounts.

Accounts
All workstation accounts will be in this OU.

Groups
These groups will be for application distribution and will have the prefix "APP". These groups will be correlated with collections in Systems Management Server. Members of APP groups will have applications automatically assigned to them. Access Control Lists should be assigned to this container and to each group to only read access to authenticated users and allow the proper administrative access.

Sales and Marketing

Policies applied to this OU will secure workstations from access by users not intended for this work group. User rights, Registry security, and File System security will be configured using group policy to only allow members of this group and administrators access to these machines. This will prevent users of other work groups from logging in to these machines and accessing software not intended for them. The groups associated with this work group will be created in the Groups OU under GIAC Users – Users. Access Control Lists should be assigned to this container and to each group to only allow read access to authenticated users and allow writable access to the proper administrative accounts.

Accounts
All workstation accounts will be in this OU.

Groups
These groups will be for application distribution and will have the prefix "APP". These groups will be correlated with collections in Systems Management Server. Members of APP groups will have applications automatically assigned to them. Access Control Lists should be assigned to this container and to each group to only read access to authenticated users and allow the proper administrative access.

Finance and Human Resources

Policies applied to this OU will secure workstations from access by users not intended for this work group. User rights, Registry security, and File System security will be configured using group policy to only allow members of this group and administrators access to these machines. This will prevent users of other work groups from logging in to these machines and accessing software not intended for them. The groups associated with this work group will be created in the Groups OU under GIAC Users – Users. Access Control Lists should be assigned to this container and to each group to only allow read access to authenticated users and allow writable access to the proper administrative accounts.

Accounts

All workstation accounts will be in this OU.

Groups

These groups will be for application distribution and will have the prefix "APP". These groups will be correlated with collections in Systems Management Server. Members of APP groups will have applications automatically assigned to them. Access Control Lists should be assigned to this container and to each group to only read access to authenticated users and allow the proper administrative access.

Policies

This OU is designed to have all policies within the domain assigned to it and disabled so that only the policy administrator (or other delegated individual/group) can create and manage policies while other groups or individuals have a central location to locate the policy for which they are looking.

Active Directory OU Security

WORLD.GIAC.INT

Each Root Level OU other than LostAndFound and System should be configured so that Authenticated Users access is removed (uncheck all boxes for this logical group). Delete Everyone from Builtin.

CORP.WORLD.GIAC.INT

Authenticated Users access to the following OUs should be removed (uncheck all checked boxes for Authenticated Users):

Admins

Policies

Builtin (Also delete everyone) –Authenticated Users should be configured for List object (this object) and read all properties (this object and all child objects)

Domain Controllers

Computers

Users

ForeignSecurityPrincipals

Special Active Directory Configuration Security

Authorizing DHCP Servers

As an Enterprise Administrator within Site and Services, under the services Node the NetServices folder should be configured to allow CORP\Domain Admins to have Full Control for "This object and all Child objects." Then CORP\Domain Admins will be able to Authorize DHCP Servers.

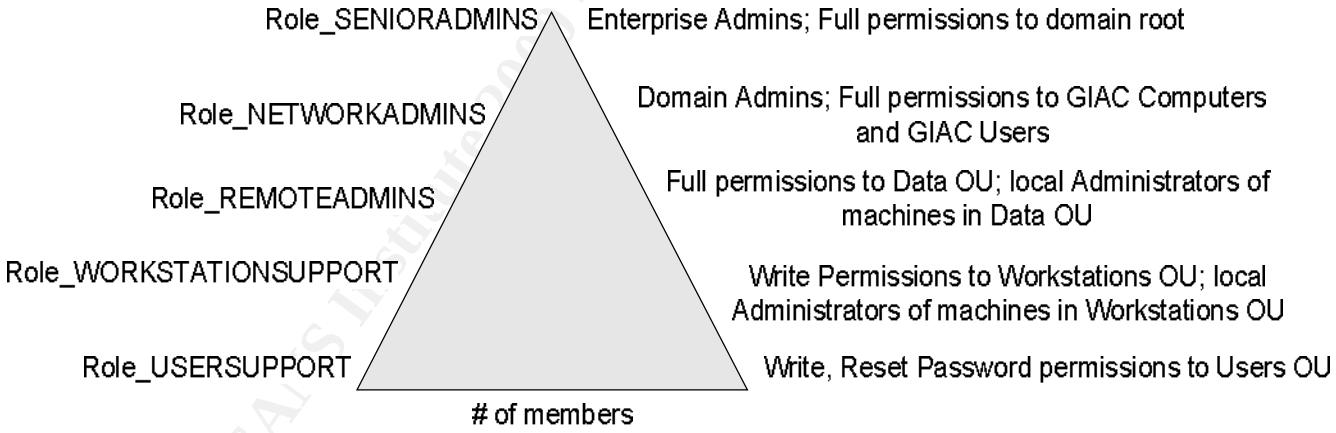
Active Directory Security Model Implementation

Domain security is set using Domain Root GPOs and through the administration of domain and OU permissions assignment. User rights and permissions will be assigned to OUs based on the appropriate task-based group. Each of the following groups will be assigned across all sites. This creates a universal environment where a support person at one site could remotely support another site in case of emergency.

To simplify administration[5], domain local groups will be assigned to resources and global groups will be put into local groups.[6] Local groups will be created with access in mind, such as "Task_<access level>_<resource>" and global groups will be named with roles in mind, such as "Role_<support function>. In the future, additional groups may be created to grant permissions for special cases such as to adding printers, imaging workstations, repackaging software, etc. In this model, if a user needs additional access to fulfill duties as a certain role in the environment, users can be added to global groups, automatically giving them access to appropriate resources.

The following details what groups will be created initially. Additional groups will be created as needed in the future. Unless specifically documented here, each of these groups will be in the GIAC Users – Administrators – Groups OU and will have security assigned to each of them to only allow read and write access from their own group, and each global group will have to be a member of the global group just below it in the security hierarchy. This will prevent admins from making themselves members of other groups with more administrative access and is only possible because the domain is in native mode.

Corp.World.Giac.Int Domain Security Hierarchy



[5] Microsoft White Paper, "*Active Directory Users, Computers, and Groups*",

[6] Systems and Network Attack Center (SNAC), National Security Agency, "*Guide to Securing Microsoft Windows 2000 Active Directory*" , Page 26

User and Workstation Objects

Help Desk

GLOBAL GROUP - Role_USERSUPPORT

This group is created for help desk personnel that are responsible for assisting users in day-to-day tasks. Help desk personnel will be able to reset users' passwords, modify user attributes, and unlock user accounts.

member of:

DOMAIN LOCAL GROUP - Task_RW_USERS_OU

At the Users OU, members of this group are given list contents, Read all properties, Write all properties, and Reset Password.

Workstation Support

GLOBAL GROUP - Role_WORKSTATIONSUPPORT

This group will be responsible for supporting all workstation machines. Users of this group will be able to perform administrative tasks on workstation objects in Active Directory and will be able to log in to workstation machines as local administrators. Typical tasks for this group will include deploying workstation images and installing software. This group is a member of the user support group, which allows staff to unlock accounts if needed during a testing procedure.

User rights are set using Group Policy to grant this group "create\delete computer objects". Restricted groups will be used in Group Policy to make these accounts members of the local Administrators group on all workstation machines. In addition, within the computer GPO for the domain controllers OU this group is assigned the right of "Add workstations to the Domain"

member of:

DOMAIN LOCAL GROUP – Task_RW_WORKSTATIONS_OU

On the Workstations OU, Read and Write permissions are granted to "this and all child objects". This group is also granted - Validated Write to Service Principal Name, Validated Write to DNS Host Name, and Reset Password.

Remote Admins

Global Group - Role_REMOTEADMINS

This group will be responsible for servers in the Data OU. The accounts in this group are intended for server support staff at minor sites. Members of this group will also be made members of the local Administrators group in all Data servers by using the restricted groups portion of Group Policy. This group will be a member of the workstation support group, which will allow members to perform additional administrative tasks for user and workstation objects if needed.

User rights are set using Group Policy to grant this group "create\delete computer objects". Restricted groups will be used in Group Policy to make these accounts members of the local Administrators group on all workstation machines. In addition, within the computer GPO for the domain controllers OU this group is assigned the right of "Add workstations to the Domain"

member of:

DOMAIN LOCAL GROUP – Task_RW_DATA_OU

On the Data OU, Read and Write permissions are granted to "this and all child objects". This group is also granted - Validated Write to Service Principal Name, Validated Write to DNS Host Name, and Reset Password.

Network Admins

GLOBAL GROUP - Role_SERVERADMINS

This group will support all CORP servers. This includes all machines in the SERVICES and DATA OUs. This group will support accounts for help desk staff and workstation support staff. Managing servers in the GIAC environment includes performing functions such as adding and removing server objects from Active Directory, managing services, disaster recovery, group policies for the GIAC Computers OU and all containers within, and delegating administration to Remote Admins. This group is a member of the remote admins group.

member of:

DOMAIN ADMINS - CORP domain

DOMAIN LOCAL GROUP - Task_RW_GIAC_COMPUTERS_OU

On the Computers OU, Read and Write permissions are granted to "this and all child objects". This group is also granted - Validated Write to Service Principal Name, Validated Write to DNS Host Name, and Reset Password.

DOMAIN LOCAL GROUP - Task_RW_GIAC_USERS_OU

At the GIAC Users OU, members of this group are given list contents, Read all properties, Write all properties, and Reset Password.

World.Giac.Int

World Admins

GLOBAL GROUP - Role_WORLDADMINS

This group will only be used when performing tasks on the WORLD domain. Administrative staff will log on to this account when modifying any configuration in the WORLD domain, therefore the number of personnel with accounts in this group will be limited. Additional group membership within the GIAC security hierarchy is not necessary because of membership to the Enterprise Admins group.

member of:

ENTERPRISE ADMINS in WORLD domain

DOMAIN LOCAL GROUP – Task_RW_WORLD_ROOT

This group is granted Read and Write permissions for "this and all child objects" for the CORP Domain.

Dmz.Giac.Int

Because of the trust relationship between the DMZ domain and the CORP domain, all groups assigned for the CORP domain will automatically have the same level of access in the DMZ domain. Therefore, no special groups will be needed to be created for the DMZ domain.

Basic Group Policy

Group policy is a powerful tool for configuring domain machines securely. Many policies are assigned to the GIAC domains to prevent users, either with good or bad intentions, from making changes to machines that would create weaknesses in the environment. Each setting is detailed in this section, but only settings that differ from the default settings are described.

World-DMZ Policies

These policies are assigned to the WORLD and DMZ domains. New policies should be created and assigned directly to the containers for which they are intended. For each policy, either the users or the computers portion should be disabled depending upon the objects for which it is assigned. The Computer Configuration portion of the policy should be disabled for polices applied to users, and likewise the users portion should be disabled for policies assigned to computers. To accomplish this, select the policy, click the button marked Options, and check the box for the unneeded configuration type. Once the policy is configured and applied the appropriate folder should be copied to a secure location in case it is later needed for an emergency restore. Each policy is stored in a folder named according to its GUID.

World-DMZ Domain Default Group Policy

Policies for the empty root domain must be fashioned in a more secure manner than those of a typical active directory domain. The policies applied here must take full advantage of what group policy has to offer to make this domain as secure as possible. A hijacked account in the empty root domain would have rights in every child domain because of the trust relationship. Even more noteworthy is the existence of Enterprise Admin Accounts in the empty root domain that are given the highest level of administrative privilege on all windows machines with domain membership. If a hacker were able to gain control of an account in Enterprise Admins, there would be no stopping would he or she could do. One of many benefits in the empty root domain design is the fact that there are no user objects in the empty root, and thus it may be secured to an extreme degree than what would be considered reasonable for most user functions.

Policy: SEC – USERS - Default

This policy will secure the WORLD and DMZ domains using the policies applied to users in Active Directory. There will not be any users created for the WORLD or DMZ domains. The proper groups will be given membership to the built in administrative groups within this domain. All settings here may restrict access as much as possible as long as administrative accounts are allowed to function in their normal capacity.

Software Installation

Windows Settings

Internet Explorer Maintenance

Scripts

Security Settings

Remote Installation Services

Each of these options should be set to "deny".

Folder Redirection

Administrative Templates

NetMeeting

There is not a business need for NetMeeting in the GIAC environment and thus all options to disable NetMeeting should be configured as such.

Internet Explorer

Windows Explorer

Microsoft Management Console

Task Scheduler

Windows Installer

Start Menu & Taskbar

Desktop

Control Panel

Network

System

Policy: SEC – Computers - Default

The default policy applied to the computers in the WORLD domain will need to lock down machines as much as possible to prevent them from being compromised. At the same time, these policies will apply to the domain controllers in the WORLD domain and thus must not restrict machines to the end that they may not function in their full capacity.

Software Installation

Windows Settings

Scripts

Security Settings

Account Policies

Password Policy

The password settings may be set to restrict passwords to an unreasonable extent because the accounts in the WORLD domain should rarely be used, and passwords should be well documented and stored in a secure location.

Account Lockout

These settings may also be set to an unreasonable extent, because the passwords set on this domain should be so complex that it would be very difficult to remember them without retrieving them from documentation every time they are entered. For this reason, there should rarely be any bad "guesses" for these accounts.

Local Policies

Auditing

All auditing features should be set to log both success and failure for every option.

User Rights Assignment

Right	Assigned to These Users
Access this computer from the network	Administrators, Authenticated Users
Act as part of the OS	
Add workstations to the domain	Administrators
Backup Files and dirs	Administrators
Bypass traverse checking	Authenticated Users
Change system time	Administrators
Create a pagefile	Administrators

Create a token object	
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	
Deny logon as batch	
Deny logon as service	
Deny logon locally	
Enable computers/users to be trusted for delegation	Administrators
Force shutdown of remote system	Administrators
Generate security audits	
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as batch job	
Log on as service	
Log on locally	Administrators
Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	
Replace a process level token	
Restore files and directories	Administrators
Shut down the system	Administrators
Synch dir service data	
Take ownership of files or other objects	Administrators

Security Options

Each of the settings in this group should be set to lock down machines as much as possible. To generalize the configuration of the settings in this group, each setting should be set to restrict unauthorized access, and should change default settings to make vulnerabilities less obvious to attackers. The only settings that should be left to default are to disable ctrl-alt-del at startup, and the shares that are given anonymous access.

Event Log

All event logs may be set to a maximum size of 1024 kilobytes, except the security log, which should be set to 3072 kilobytes. This is to prevent the security logs from being "flushed out" by standard hacker techniques. Guest access should be restricted from all logs. Retention method should be set to never allow overwrite. Of course, the event logs should be archived, but not cleared, by network support staff or a preconfigured script on a regular basis, so there should never be a fear of logs overwriting themselves.

Restricted Groups

This setting should be set to never allow accounts to become members of power users, to only allow the network administrators group from the CORP domain and the local administrator account to be members of the administrators group. This will prevent intruders from adding new local accounts.

System Services

Registry

The inf template available from the National Security Agency regarding Windows 2000 Domain Controllers should be imported after removing everything accept for the modifications to File System Security.

File System

The inf template available from the National Security Agency regarding Windows 2000 Domain Controllers should be imported after removing everything accept for the modifications to File System Security.

Public Key Policies

IP Security Policies

Administrative Templates

To generalize these settings, any policies applying to software applications may be set with utmost security. Any policies that apply to the operating system and network settings should be set to configure settings with the proper configurations for the network so that if settings on machines were changed, the correct settings would overwrite them when the policy is applied.

Policy: SEC – Domain Controllers - Default

This policy will secure the WORLD and DMZ domain controllers using the policies applied to users in Active Directory. There will not be any users created for the WORLD or DMZ domains. The proper groups will be given membership to the built in administrative groups within this domain. All settings here may restrict access as much as possible as long as administrative accounts are allowed to function in their normal capacity.

Software Installation

Windows Settings

- **Internet Explorer Maintenance**
- **Scripts**
- **Security Settings**
- **Remote Installation Services**
- **Folder Redirection**

Administrative Templates

- **NetMeeting**
- **Internet Explorer**
- **Windows Explorer**
- **Microsoft Management Console**
- **Task Scheduler**
- **Windows Installer**
- **Start Menu & Taskbar**
- **Desktop**
- **Control Panel**
- **Network**
- **System**

Policy: SEC – Computers - Default

This policy is applied to the domain controllers in the WORLD domain. The majority of group policy configuration is done at the domain root but the user rights, registry permissions, restricted groups, and file system permissions are important for assignment here.

Software Installation

Windows Settings

Scripts

Security Settings

Account Policies

Password Policy

Account Lockout

Local Policies

Auditing

User Rights Assignment

Right	Assigned to These Users
Access this computer from the network	Administrators, Authenticated Users
Act as part of the OS	
Add workstations to the domain	Administrators
Backup Files and dirs	Administrators
Bypass traverse checking	Authenticated Users
Change system time	Administrators
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	
Deny logon as batch	
Deny logon as service	
Deny logon locally	
Enable computers/users to be trusted for delegation	Administrators
Force shutdown of remote system	Administrators
Generate security audits	
Increase quotas	Administrators
Increase scheduling priority	Administrators

Load and unload device drivers	Administrators
Lock pages in memory	
Log on as batch job	
Log on as service	
Log on locally	Administrators
Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	
Replace a process level token	
Restore files and directories	Administrators
Shut down the system	Administrators
Synch dir service data	
Take ownership of files or other objects	Administrators

Security Options

The only settings applied here will be to digitally sign all communications.

Event Log

Restricted Groups

System Services

Registry

File System

Public Key Policies

IP Security Policies

Administrative Templates

Corp Default Domain Policy

The default domain policy for the CORP domain is much less restrictive than the policy set on the WORLD domain. This is because there will be users actively logging in to the CORP domain and the degree at which the WORLD domain is secured is much too restrictive for most users to function normally.

All policies applied to the CORP domain should be created at the Policies OU and assigned via link. [7] The policy should be disabled for the Policies container and the unneeded Configuration portion of the policy should be disabled by selecting the policy, clicking the button marked Options, and checking the box for either the users or computers configuration. Once the policy is configured and applied the appropriate folder should be copied to a secure location in case it is later needed for an emergency restore.

[7] Microsoft White Paper, "*Active Directory Architecture*"

Policy: SEC – USERS - Default

Software Installation

Windows Settings

Internet Explorer Maintenance

Scripts

Security Settings

Remote Installation Services

Folder Redirection

Administrative Templates

NetMeeting

There is not a business need for NetMeeting in the GIAC environment and thus all options to disable NetMeeting should be configured as such.

Internet Explorer

Windows Explorer

Microsoft Management Console

Task Scheduler

Windows Installer

Start Menu & Taskbar

Desktop

Control Panel

Network

System

Policy: SEC – Computers - Default

Software Installation

Windows Settings

Scripts

Security Settings

Account Policies

Password Policy

The password policies will apply an eight character length, 45 day minimum age, 5 day maximum age, 20 password history, and to require complexity. While these settings are complex, the password policies should be taken seriously and any users found leaving written passwords in obvious places should be seriously reprimanded. The help desk is available to reset forgotten passwords.

Account Lockout

Account lockout should be set reasonably to prevent brute force attacks but to allow users a threshold of five bad attempts in 30 minutes to prevent accidental lockouts. Once locked out, accounts must be manually unlocked by help desk personnel.

Local Policies

Auditing

All auditing features should be set to log failure for every option.

User Rights Assignment

Right	Assigned to These Users
Access this computer from the network	Administrators, Authenticated Users
Act as part of the OS	
Add workstations to the domain	Administrators
Backup Files and dirs	Administrators
Bypass traverse checking	Authenticated Users
Change system time	Administrators
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	Administrators

Deny access to this computer from the network	
Deny logon as batch	
Deny logon as service	
Deny logon locally	
Enable computers/users to be trusted for delegation	Administrators
Force shutdown of remote system	Administrators
Generate security audits	
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as batch job	
Log on as service	
Log on locally	Administrators, Authenticated Users
Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	
Replace a process level token	
Restore files and directories	Administrators
Shut down the system	Administrators
Synch dir service data	
Take ownership of files or other objects	Administrators

Security Options

Anonymous connections are not allowed to enumerate the SAM accounts or shares so that users not in the domain are denied access. All communications are to be digitally signed whenever possible. The standard built in accounts will be renamed appropriately and the last logged in username will not be displayed to prevent brute force attacks.

Event Log

Restricted Groups

System Services

Registry

File System

Public Key Policies

IP Security Policies

Administrative Templates

Policy: SEC – Domain Controllers - Default

This policy is applied to the domain controllers in the CORP domain. The majority of group policy configuration is done at the domain root but the user rights, registry permissions, restricted groups, and file system permissions are important for assignment here.

Software Installation

Windows Settings

Scripts

Security Settings

Account Policies

Password Policy

Account Lockout

Local Policies

Auditing

User Rights Assignment

Right	Assigned to These Users
Access this computer from the network	Administrators, Authenticated Users
Act as part of the OS	
Add workstations to the domain	Administrators
Backup Files and dirs	Administrators
Bypass traverse checking	Authenticated Users
Change system time	Administrators
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	
Deny logon as batch	
Deny logon as service	
Deny logon locally	
Enable computers/users to be trusted for delegation	Administrators
Force shutdown of remote system	Administrators
Generate security audits	
Increase quotas	Administrators
Increase scheduling priority	Administrators

Load and unload device drivers	Administrators
Lock pages in memory	
Log on as batch job	
Log on as service	
Log on locally	Administrators
Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	
Replace a process level token	
Restore files and directories	Administrators
Shut down the system	Administrators
Synch dir service data	
Take ownership of files or other objects	Administrators

Security Options

The only settings applied here will be to digitally sign all communications.

Event Log

Restricted Groups

This setting should be set to never allow accounts to become members of power users, to only allow the network administrators group and the local administrator account to be members of the administrators group. This will prevent unauthorized creation of local accounts.

System Services

Registry

The inf template available from the National Security Agency regarding Windows 2000 Domain Controllers should be imported after removing everything accept for the modifications to File System Security.

File System

The inf template available from the National Security Agency regarding Windows 2000 Domain Controllers should be imported after removing everything accept for the modifications to File System Security.

Public Key Policies

IP Security Policies

Administrative Templates

Additional Group Policy

Administrators OU Group Policy

Policy: SEC – ADMINISTRATORS - Default

This policy defines the settings for all policies applied to administrators accept for administrative templates. Administrative accounts should not be used for user type functions and thus options such as Internet Explorer Settings and Folder Redirection are unnecessary. The Remote Installation Service settings may be applied at this level because the settings apply to all administrators.

Software Installation

Windows Settings

Internet Explorer Maintenance

Scripts

Security Settings

Remote Installation Services

These options should be set to "deny" restarting setup or accessing tools, the settings for Automatic Setup and Custom Setup should be "don't care".

Folder Redirection

Administrative Templates

Policy: SEC – Administrators – %GroupName%

Only administrative templates are applied in this policy. The need for this policy is to disable administrative tools for accounts that do not have a business need for some options. The policies should be named according to group such as "SEC – ADMINISTRATORS – USERSUPPORT" and then the access control list on the policy should be set so that only the security group by that name, located in the Groups OU within the Administrators OU, is allowed read access and to apply the policy.

Administrative Templates

NetMeeting

There is not a business need for NetMeeting in the GIAC environment and thus all options to disable NetMeeting should be configured as such.

Internet Explorer

Windows Explorer

Microsoft Management Console

This group is the reason for assigning multiple policies to administrators. For all groups with less administrative responsibility than Network Admins "author mode" should be restricted. Further, the settings to explicitly restrict access to snap-ins should be enabled. For each group, only the snap-ins needed to perform tasks should be set to "enabled". This will act as an additional step in preventing unauthorized changes to Active Directory.

Task Scheduler

No accounts with administrative responsibility lower than Remote Admins will require the Task Scheduler and thus all settings to disable the feature should be configured as such.

Windows Installer

Start Menu & Taskbar

Desktop

Control Panel

Network

System

Policy: SEC – Service Accounts - Default

Now there should never be a reason for any user to log in to the domain as a service account. These accounts are only for programs that run on domain machines and require authentication to other places in the network. Therefore, the policies applied to this OU may be as restrictive as possible.

Software Installation

Windows Settings

Internet Explorer Maintenance

Scripts

Security Settings

Remote Installation Services

These options should be set to "deny" all functions.

Folder Redirection

Administrative Templates

NetMeeting

There is not a business need for NetMeeting in the GIAC environment and thus all options to disable NetMeeting should be configured as such.

Internet Explorer

Windows Explorer

Microsoft Management Console

For this setting at the top level, "restrict author mode" should be set to "enable". The settings to explicitly restrict access to snap-ins should also be set to "enable". This will act as an additional step towards preventing unauthorized changes to Active Directory, should a service account be hijacked by an unauthorized person.

Task Scheduler

No Service Accounts will require the Task Scheduler and thus all settings to disable the feature should be configured as such.

Windows Installer

Start Menu & Taskbar

Desktop

Control Panel

Network

System

Users OU Group Policy

Policy: SEC – Users - Default

The policy applied to the Users OU will span across all user accounts for GIAC enterprises and thus the settings must be applied selectively and with caution after extensive testing. The biggest reason for policies at the Users OU will be application distribution, logon and logoff scripts, and folder redirection. All applications will be packaged and deployed to users via the Software Installation portion of the user policy. For this reason, additional policies will be created based on the group name, as explained later.

Software Installation

Windows Settings

Internet Explorer Maintenance

Scripts

Scripts that run when users log on to or off the domain should be applied using this setting. If, in the future, there becomes a reason to have different logon or logoff scripts for certain users, a separate policy could be implemented and applied only to members of groups created for this purpose.

Security Settings

User accounts should be configured to trust the enterprise certificates necessary for SSL within the GIAC environment. This will prevent the user from being prompted to accept the certificate every time he or she loads the intranet site.

Remote Installation Services

These options should be set to “deny” all functions.

Folder Redirection

All folders listed here should be redirected to the local site for each group. The setting should be \\DFSROOT\USERS\%USERNAME%, with “servername” replaced according to the standard naming conventions to establish a redirection to the local file and print server. Groups created with names appropriate for each site are in the Groups OU in the Users OU within the GIAC Users OU. With this simplicity, if a user moves to a different site, his or her home directory may be moved to the file and print server at the new site and his or her account may be moved to the new group, and no other changes must be adjusted.

Administrative Templates

NetMeeting

There is not a business need for NetMeeting in the GIAC environment and thus all options to disable NetMeeting should be configured as such.

Internet Explorer

Windows Explorer

Microsoft Management Console

For this setting at the top level, “restrict author mode” should be set to “enable”. The settings to explicitly restrict access to snap-ins should also be set to “enable”. This will act as an additional step towards preventing unauthorized changes to Active Directory, should a service account be hijacked by an unauthorized person.

Task Scheduler

No user accounts will require the Task Scheduler and thus all settings to disable the feature should be configured as such.

Windows Installer

Start Menu & Taskbar

Desktop

Control Panel

The Control Panel may be restricted for user accounts. There is no reason for any user to ever access the control panel in the CORP domain, accept to use the add/remove programs applet, and the policy should be set to only allow use of the “appwiz.cpl”.

Network

All settings, except one, to prohibit user configuration of offline files and remote access connections may be set to do so. Users should never configure there own offline file settings or network configurations. The one setting that may be left at default is to allow users to initiate or close RAS connections from their machines. This setting will allow laptop users to dial in to the network when traveling.

System

The settings in the System folder add several unique security configuration opportunities to the domain. Domain users should never need to use the command prompt or registry editing tools and thus the policy may be configured to prevent this. Autoplay should be disabled. The setting for only run allowed Windows applications may be used to further restrict user’s ability to run harmful applications, but must be carefully examined to prevent too intrusive restriction. The setting may be applied because all applications in the GIAC environment are deployed using the Software Installation method in Group Policy and thus the executables should not be difficult to track.

Services OU GROUP POLICY

Policy: SEC – Services - Default

The Service OU will contain the accounts in Active Directory for all machines that are not domain controllers or file and print servers. Settings should be applied in group policy with caution, to prevent the chance of a policy settings preventing functionality.

Software Installation

Windows Settings

Scripts

Security Settings

Account Policies

Local Policies

Auditing

User Rights Assignment

Right	Assigned to These Users
Access this computer from the network	Administrators, Authenticated Users
Act as part of the OS	
Add workstations to the domain	Administrators
Backup Files and dirs	Administrators
Bypass traverse checking	Authenticated Users
Change system time	Administrators
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	
Deny logon as batch	
Deny logon as service	
Deny logon locally	
Enable computers/users to be trusted for delegation	Administrators
Force shutdown of remote system	Administrators
Generate security audits	
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as batch job	
Log on as service	ExServAcct, BackupExecServAcct,

	<additional service accounts>
Log on locally	Administrators
Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	
Replace a process level token	
Restore files and directories	Administrators
Shut down the system	Administrators
Synch dir service data	
Take ownership of files or other objects	Administrators

Security Options

Event Log

All event logs may be set to a maximum size of 1 Gigabyte. This is to prevent the security logs from being "flushed out" by standard hacker techniques. Guest access should be restricted from all logs. Retention method should be set to never overwrite logs. Of course, the event logs should be archived, but not cleared, by network support staff or a preconfigured script on a regular basis, so there should never be a fear of logs overwriting themselves.

Restricted Groups

This setting should be set to never allow accounts to become members of power users, to only allow the network administrators group and the local administrator account to be members of the administrators group.

System Services

Registry

The registry should have access control lists set in accordance with the security templates available from the National Security Agency for Windows 2000 servers. These may be obtained from the public NSA website. By removing everything except for the data needed for this section from the provided inf file, the settings may be imported rather than set manually. For specialized servers, permissions may be evaluated on a case by case basis.[8]

[8] Systems and Network Attack Center (SNAC), National Security Agency, "*Guide to Securing Microsoft Windows 2000 Group Policy*", Page 18

File System

The file system should have access control lists set in accordance with the security templates available from the National Security Agency. These may be obtained from the public NSA website. By removing everything except for the data needed for this section from the provided inf file, the settings may be imported rather than set manually. For specialized servers, specific directories should be evaluated on a case by case basis.[9]

Public Key Policies

The certificate trust list should be set to trust the enterprise certificates required for IPSEC and SSL communications.

IP Security Policies

IPSEC should be configured to respond with security for communications when authentication based on a trusted enterprise certificate is available.

Administrative Templates

[9] Systems and Network Attack Center (SNAC), National Security Agency, "*Guide to Securing Microsoft Windows 2000 Group Policy*", Page 18

Data OU Group Policy

Policy: SEC – Data - Default

This policy will be applied to all File and Print servers throughout the GIAC enterprise. This includes servers in both major and minor sites. The primary difference between this policy and the policy assigned to the Services OU is the User Rights assignment.

Software Installation

Windows Settings

Scripts

Security Settings

Account Policies

Local Policies

Auditing

All auditing features should be set to log failure for every option. Audit success for account management, policy change, privilege use, and system events. This is primarily to prevent brute force attacks, but also to log successful changes to identify the source of disasters.

User Rights Assignment

Right	Assigned to These Users
Access this computer from the network	Administrators, Authenticated Users
Act as part of the OS	
Add workstations to the domain	Administrators
Backup Files and dirs	Administrators
Bypass traverse checking	Authenticated Users
Change system time	Administrators
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	
Deny logon as batch	
Deny logon as service	
Deny logon locally	
Enable computers/users to be trusted for delegation	Administrators
Force shutdown of remote system	Administrators
Generate security audits	
Increase quotas	Administrators
Increase scheduling priority	Administrators

Load and unload device drivers	Administrators
Lock pages in memory	
Log on as batch job	
Log on as service	BackupExecServAcct – minor sites only
Log on locally	Administrators, Authenticated Users
Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	
Replace a process level token	
Restore files and directories	Administrators
Shut down the system	Administrators
Synch dir service data	
Take ownership of files or other objects	Administrators

Security Options

Event Log

All event logs may be set to a maximum size of 1 Gigabyte. This is to prevent the security logs from being "flushed out" by standard hacker techniques. Guest access should be restricted from all logs. Retention method should be set to overwrite all logs as needed. Of course, the event logs should be archived, but not cleared, by network support staff or a preconfigured script on a regular basis, so there should never be a fear of logs overwriting themselves.

Restricted Groups

This setting should be set to never allow accounts to become members of power users, to only allow the remote Admins and network administrators group and the local administrator account to be members of the administrators group.

System Services

Registry

The registry should have access control lists set in accordance with the security templates available from the National Security Agency for Windows 2000 servers. These may be obtained from the public NSA website. By removing everything except for the data needed for this section from the provided inf file, the settings may be imported rather than set manually.[10]

[10] Microsoft White Paper, "*Active Directory Architecture*"

File System

The file system should have access control lists set in accordance with the security templates available from the National Security Agency. These may be obtained from the public NSA website. By removing everything except for the data needed for this section from the provided inf file, the settings may be imported rather than set manually. Permissions for the folders used to store user and corporate data may be ACLed here if it becomes necessary later.[11]

Public Key Policies

The certificate trust list should be set to trust the enterprise certificates required for IPSEC and SSL communications.

IP Security Policies

IPSEC should be configured to require security for communications with authentication based on a trusted enterprise certificate.

Administrative Templates

The only settings within the administrative templates folder that will be applied are those in the "Disk Quota" section. Disk quota's should be enabled, enforced, and logged. Warnings should be sent. Quotas should not apply to removable media.

[11] Systems and Network Attack Center (SNAC), National Security Agency, "*Guide to Securing Microsoft Windows 2000 Group Policy*", Page 18

Policy: SEC – Research and Development - Default

This policy will apply to all workstations within the Research and Development OU. The primary differences between this and other workstation and server policies are the User Rights assignment. Policies assigned to this OU should prevent users other than those from the appropriate user group from access.

Software Installation

Windows Settings

Scripts

Security Settings

Account Policies

Local Policies

Auditing

All auditing features should be set to log failure for every option. Audit success for account management, policy change, privilege use, and system events. This is primarily to prevent brute force attacks, but also to log successful changes to identify the source of disasters.

User Rights Assignment

Right	Assigned to These Users
Access this computer from the network	Administrators, WORK – R&D
Act as part of the OS	
Add workstations to the domain	Administrators
Backup Files and dirs	Administrators
Bypass traverse checking	WORK – R&D
Change system time	Administrators
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	
Deny logon as batch	
Deny logon as service	
Deny logon locally	
Enable computers/users to be trusted for delegation	Administrators
Force shutdown of remote system	Administrators
Generate security audits	
Increase quotas	Administrators

Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as batch job	
Log on as service	
Log on locally	Administrators, WORK – R&D
Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	
Replace a process level token	
Restore files and directories	Administrators
Shut down the system	Administrators
Synch dir service data	
Take ownership of files or other objects	Administrators

Security Options

Event Log

All event logs may be set to a maximum size of 512 kilobytes. Guest access should be restricted from all logs. Retention method should be set to retain logs for 35 days and to shut down the machine before overwriting logs.

Restricted Groups

This setting should be set to never allow accounts to become members of power users, to only allow the workstation support group and the local administrator account to be members of the administrators group, and to only allow the WORK – R&D group to be members of the local users group.

System Services

Registry

The registry should have access control lists set in accordance with the security templates available from the National Security Agency. These may be obtained from the public NSA website. By removing everything except for the data needed for this section from the provided inf file, the settings may be imported rather than set manually.[12]

[12] Systems and Network Attack Center (SNAC), National Security Agency, "*Guide to Securing Microsoft Windows 2000 Group Policy*", Page 18

File System

The file system should have access control lists set in accordance with the security templates available from the National Security Agency. These may be obtained from the public NSA website. By removing everything except for the data needed for this section from the provided inf file, the settings may be imported rather than set manually.[13]

Public Key Policies

The certificate trust list should be set to trust the enterprise certificates required for IPSEC and SSL communications.

IP Security Policies

IPSEC should be configured to respond with security for communications when authentication based on a trusted enterprise certificate is available.

Administrative Templates

[13] Systems and Network Attack Center (SNAC), National Security Agency, "*Guide to Securing Microsoft Windows 2000 Group Policy*", Page 18

Policy: SEC – Sales and Marketing - Default

This policy will apply to all workstations within the Research and Development OU. The primary differences between this and other workstation and server policies are the User Rights assignment. Policies assigned to this OU should prevent users other than those from the appropriate user group from access.

Software Installation

Windows Settings

Scripts

Security Settings

Account Policies

Local Policies

Auditing

All auditing features should be set to log failure for every option. Audit success for account management, policy change, privilege use, and system events. This is primarily to prevent brute force attacks, but also to log successful changes to identify the source of disasters.

User Rights Assignment

Right	Assigned to These Users
Access this computer from the network	Administrators, WORK – S&M
Act as part of the OS	
Add workstations to the domain	Administrators
Backup Files and dirs	Administrators
Bypass traverse checking	WORK – S&M
Change system time	Administrators
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	
Deny logon as batch	
Deny logon as service	
Deny logon locally	
Enable computers/users to be trusted for delegation	Administrators
Force shutdown of remote system	Administrators
Generate security audits	
Increase quotas	Administrators

Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as batch job	
Log on as service	
Log on locally	Administrators, WORK – S&M
Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	
Replace a process level token	
Restore files and directories	Administrators
Shut down the system	Administrators
Synch dir service data	
Take ownership of files or other objects	Administrators

Security Options

These settings are configured in the policy assigned to the domain root. All settings in this policy may be left in the default state.

Event Log

All event logs may be set to a maximum size of 512 kilobytes. Guest access should be restricted from all logs. Retention method should be set to retain logs for 35 days and to shut down the machine before overwriting logs.

Restricted Groups

This setting should be set to never allow accounts to become members of power users, to only allow the workstation support group and the local administrator account to be members of the administrators group, and to only allow the WORK – S&M group to be members of the local users group.

System Services

Registry

The registry should have access control lists set in accordance with the security templates available from the National Security Agency. These may be obtained from the public NSA website. By removing everything except for the data needed for this section from the provided inf file, the settings may be imported rather than set manually.[14]

[14] Systems and Network Attack Center (SNAC), National Security Agency, "*Guide to Securing Microsoft Windows 2000 Group Policy*", Page 18

File System

The file system should have access control lists set in accordance with the security templates available from the National Security Agency. These may be obtained from the public NSA website. By removing everything except for the data needed for this section from the provided inf file, the settings may be imported rather than set manually.[15]

Public Key Policies

The certificate trust list should be set to trust the enterprise certificates required for IPSEC and SSL communications.

IP Security Policies

IPSEC should be configured to respond with security for communications when authentication based on a trusted enterprise certificate is available.

Administrative Templates

[15] Systems and Network Attack Center (SNAC), National Security Agency, "*Guide to Securing Microsoft Windows 2000 Group Policy*", Page 18

Policy: SEC – Finance and Human Resources - Default

This policy will apply to all workstations within the Research and Development OU. The primary differences between this and other workstation and server policies are the User Rights assignment. Policies assigned to this OU should prevent users other than those from the appropriate user group from access.

Software Installation

Windows Settings

Scripts

Security Settings

Account Policies

Local Policies

Auditing

All auditing features should be set to log failure for every option. Audit success for account management, policy change, privilege use, and system events. This is primarily to prevent brute force attacks, but also to log successful changes to identify the source of disasters.

User Rights Assignment

Right	Assigned to These Users
Access this computer from the network	Administrators, F&HR
Act as part of the OS	
Add workstations to the domain	Administrators
Backup Files and dirs	Administrators
Bypass traverse checking	WORK – F&HR
Change system time	Administrators
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	
Deny logon as batch	
Deny logon as service	
Deny logon locally	
Enable computers/users to be trusted for delegation	Administrators
Force shutdown of remote system	Administrators
Generate security audits	
Increase quotas	Administrators

Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as batch job	
Log on as service	
Log on locally	Administrators, WORK – F&HR
Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	
Replace a process level token	
Restore files and directories	Administrators
Shut down the system	Administrators
Synch dir service data	
Take ownership of files or other objects	Administrators

Security Options

These settings are configured in the policy assigned to the domain root. All settings in this policy may be left in the default state.

Event Log

All event logs may be set to a maximum size of 512 kilobytes. Guest access should be restricted from all logs. Retention method should be set to retain logs for 35 days and to shut down the machine before overwriting logs.

Restricted Groups

This setting should be set to never allow accounts to become members of power users, to only allow the workstation support group and the local administrator account to be members of the administrators group, and to only allow the WORK – F&HR group to be members of the local users group.

System Services

Registry

The registry should have access control lists set in accordance with the security templates available from the National Security Agency. These may be obtained from the public NSA website. By removing everything except for the data needed for this section from the provided inf file, the settings may be imported rather than set manually.[16]

[16] Systems and Network Attack Center (SNAC), National Security Agency, "*Guide to Securing Microsoft Windows 2000 Group Policy*" , Page 18

File System

The file system should have access control lists set in accordance with the security templates available from the National Security Agency. These may be obtained from the public NSA website. By removing everything except for the data needed for this section from the provided inf file, the settings may be imported rather than set manually.[17]

Public Key Policies

The certificate trust list should be set to trust the enterprise certificates required for IPSEC and SSL communications.

IP Security Policies

IPSEC should be configured to respond with security for communications when authentication based on a trusted enterprise certificate is available.

Administrative Templates

[17] Systems and Network Attack Center (SNAC), National Security Agency, "*Guide to Securing Microsoft Windows 2000 Group Policy*", Page 18

Additional Security

Hotfix checking, reporting, and deployment, with reinstallation after an overwrite

Microsoft operating systems are ideal for enterprise deployment and administration. The Microsoft Windows 2000 operating system is robust and user friendly, and is a perfect solution for the GIAC corporate network. As vulnerabilities are found in the Windows operating system, patches are released to correct issues that were overlooked at the time the operating system was released. When multiple hotfixes have been released and regression tested in enterprise production network, these hotfixes, as well as critical updates to improve the functionality of the operating system, are released in a compilation called service pack. The same is true for Microsoft software applications

Service Pack files can be extracted and built in to operating system images for deployment. At this time, the latest service pack is version 3, which was released In August of 2002. The installation of service pack three will install all hotfixes up to and including service pack three, so the previous releases need not be installed. By running the service pack with a –extract and then copying the files into the i386 directory of the Windows 2000 cd prior to creating the base RIS image, application deployment staff may surpass the need to deploy service pack three using the standard SMS methodology.

Service pack 3 is not the end of hotfix issuance for the Microsoft Windows 2000 operating system. A number of hotfixes have already been released with a naming context that indicates they will be included in service pack 4. Unfortunately, due to the critical nature of these hotfixes, it is not a practical opportunity to be patient and wait for the release of service pack 4 to distribute said hotfixes. Instead, each new hotfix must be installed on every machine in the environment as soon as possible after thorough regression testing on non-production machines.

Microsoft recently released, free of charge, two new tools to improve the distribution of hotfixes to a large-scale environment. The first was the Software Update Service, which allows system administrators to build their own Windows Update server, the internet resource for downloading and installing Microsoft hotfixes and updates. Unfortunately, because all networks are different and it is impossible for Microsoft to test hotfix interaction with all third party software, some hotfixes have been known to create problems when installed on production machines. The software update service provides administrators with a safe proxy for updates by downloading all newly releases hotfixes, but not making them available to network users for download until they have been approved by system administrators.

The second tool that Microsoft has provided, also for no cost, is the SMS value pack. The SMS value pack integrates with Systems Management Server 2.0 to streamline the process of distributing Microsoft updates. The tool uses the hfnetchk tool, originally developed by Shavlik Technologies, Inc., to scan Windows machines and determine which updates have already been installed, and which updates have not. It even scans versions of popular Microsoft software, such as SQL server and Internet Explorer, to determine if they are up to date. Hfnetchk is preferable to the active update windows components that are based on windows update technology. Only hfnetchk scans every file and registry setting to make sure hotfixes have not been overwritten by changes made to the computer after their installation.

The SMS value pack includes a tool to execute the hfnetchk scan across an enterprise network, and is capable of building a report based on this scan for hotfix distributing. The tool uses the systems management server technology to automatically install the software on every machine in the network transparently to users. The tool integrates another option called Qchain, which prevents the need for a reboot after individual hotfix installations. Based on the report generated by hfnetchk, SMS value pack creates a package for each machine, or groups of like machines, with specifically the updates those machines are lacking.

Software update service includes a client that, when incorporated into group policy, can be used to push out hotfixes as well. The active update component for Windows 2000 can automatically download and install updates from a software update service server at a specific time each day. The problem with the active update component is that it is based on the Windows update technology and not the hfnetchk technology. The SMS Value Pack specifically resolves the security issue of hotfixes being overwritten by changes to the operating system, such as adding new components, and no longer being effectively installed. Only hfnetchk and the SMS Value Pack can provide a thorough scan of every change that a hotfix makes and determine whether the changes made by the hotfix are still in effect. In addition to this critical factor, Microsoft has documented that because SMS centralizes administrative control of hotfix deployment and allows much more advanced administrative functionality such as generating reports on which machines have updates and installed and which do not, deploying using optimized bandwidth and scheduling, and support for user postponement until a more convenient time.

The integration of these two products creates an optimum environment. The SMS Value Pack tools have the capability of interfacing with the software update server to obtain regression-tested hotfixes. Using this method, the support staff providing the role as regression testers does not have to notify the SMS administrators which hotfixes to apply and which not to apply. Any hotfixes that the SMS Value Pack tools detect may be deployed because they have already been regression tested. This simple method streamlines distribution to the point of nearly eliminating points of failure.

Bibliography

Microsoft White Paper, "*Active Directory Architecture*", Copyright 2000 Microsoft Corporation http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ad/windows2000/deploy/projplan/adarch.asp

Microsoft White Paper, "*Active Directory Users, Computers, and Groups*", Copyright 2000 Microsoft Corporation, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ad/windows2000/maintain/adusers.asp

Systems and Network Attack Center (SNAC), **National Security Agency**, "*Guide to Securing Microsoft Windows 2000 Active Directory*" Report Number C4-056R-00, December, 2000, Version 1.0, PDF available at http://nsa1.www.conxion.com/

Systems and Network Attack Center (SNAC), **National Security Agency**, "*Guide to Securing Microsoft Windows 2000 Group Policy*" Report Number C4-007R-00, September 13, 2001, Version 1.1, PDF available at http://nsa1.www.conxion.com/

Systems and Network Attack Center (SNAC), **National Security Agency**, "*Microsoft Windows 2000 Network Architecture Guide*" Report Number C4-051R-00, April 19, 2001, Version 1.0, PDF available at http://nsa1.www.conxion.com/

Last Updated: May 27th, 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 Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**