Global Information Assurance Certification Paper

GIAC Enterprises Windows 2000 Network Design

By
Wayne Freeman
GCWN Practical Assignment Version 3.1
August 18, 2002

Introduction

GIAC Enterprises recent Initial Public Offering has sold out and they are now proceeding to implement the corporate network to support their online sales of fortune cookie sayings.

GIAC Enterprises is an E-Commerce sales organization which relies on a sales force supported by an E-Commerce enabled web site to generate income, and its Research and Development division to develop new and innovative products. Service and administration departments who oversee purchasing, human resources, accounting, and administration support the overall organization. GIAC is located in a single building, however the production and shipping departments are located in a separate location, which provides easy access to international shipping, and allows for the industrial nature of this process.

Due to the geographical dispersion of GIAC's customer base, online secure access to marketing, promotion, sales, and shipping information is critical. GIAC's sales force travel internationally to solicit new business and service clients as well as provide online sales information, support, and marketing such as email promotions. All sales closed are input through the corporate extranet from remote locations by the sales force, or directly input by clients through the secure area of the public web site. These orders are automatically logged into a database, where accounting and production then have access to the information to complete the order and billing process.

Senior management has asked us to design a secure Windows 2000 network taking advantage of the many benefits of Microsoft Windows 2000 and Active Directory.

Based on discussions with management and departmental interviews our fundamental approach to this network will be to obtain the securest possible network through a defense in depth strategy, while remaining as transparent as possible for the user. The primary goal is to support the Corporations business needs and goals as well as allowing for anticipated future growth while meeting GIAC's security needs.

Assumptions

The following assumptions have been derived from our detailed interviews and discussions with GIAC Enterprises Management as well as our review of their recently approved security policy,

- All servers will be housed in a physically secure location with restricted access and all necessary environmental controls
- GIAC Enterprises exists in two locations, the primary site occupies 3 floors, but secure external access will be needed for a select group of employees to this location. The second location is a production and

shipping facility across town in an industrial area and requires secure access to the primary site for email, inventory updates, and order processing.

- The entire organization will be on the Windows 2000 platform, including all desktops, laptops, and servers and will be running in native mode.
- All mainstream applications and will be Microsoft, including Office 2000, SQL Server 2000, Exchange 2000, and ISA Server
- The currently selected anti virus solution is the McAfee Total Virus Protection Suite and will be installed on all servers, desktops, and laptops.
- The external network connections are in place and consist of two T3 internet connections at the primary location, and a single T1 internet connection at the production facility.
- The server rooms and wiring closets in both locations are connected via fiber optic cable, and CAT 6 cabling runs from the wiring closets to the user's desktop.
- All cabling in the server rooms in both locations is fiber, with all servers having fiber network cards for connectivity
- All routers and switches will be Cisco with the exception of the remote access router which will be an Ascend 1800 Max.
- Network time synchronization will be managed through the Windows 2000 native time service, and will be obtained at four hour intervals from a US military time server. Accurate time across all machines in our network is critical for many reasons, the two most important being Kerberos authentication and event logging. Without consistent time across all our machines a timeline of activity would be flawed and the forensic evidence of an incident would be unreliable at best. It would also make us more vulnerable to such things as "replay" attacks. As GIAC Enterprises is located in the North American Mountain Time zone the following servers will be used:
    - Primary **navobs1.usnogps.navy.mil**
    - Secondary **navobs2.usnogps.navy.mil**
- All servers will be a 933Mhz dual processor with 1GB of ram and redundant power supplies.
- All servers will be installed with Adaptec hardware RAID cards, Ultra SCSI 3 with a transfer rate of 160MB/Sec and 10,000 RPM SCSI drives
- All servers will have a hardware RAID 1 configuration for their primary operating system drives and hardware RAID 5 array for their data drives. The number of disks in the RAID 5 arrays will differ depending on the server's role, but will be a minimum of five (allowing for 2 failed drives before risk of data loss).
- The Exchange 2000 and SQL 2000 servers will have a second RAID 1 setup to accommodate the logs and check files and will have quad 933Mhz processors and 4 GB of RAM
- The external and extranet web servers, external SQL 2000 servers, and the ACE (secure ID) server will all be clustered for fail over protection using Windows 2000 Advanced server.

- All servers will have their floppy drives, parallel, serial, and USB ports disabled in the BIOS and protected with a BIOS administrator password.
- All servers will be running current service packs and any hot fixes or security patches currently available
- All servers will be backed up using Veritas Backup Exec with the necessary agents that do not require a null session connection. All backups will require administrator level permissions including a password to run and to restore.
- All servers will be on Uninterruptable Power Supplies set to begin graceful shutdown after five minutes on battery power.
- The following Departments make up GIAC Enterprises:
    - Executive and Management
    - Research and Development
    - Sales and Marketing
    - Finance and Human Resources
    - Information Technology
    - Production and Shipping

Network Design

The following will outline our network design as detailed in Figure 1 and 2. GIAC Enterprises is a conventional and E-Commerce business, and as such must allow access to an external web site including electronic transactions involving credit cards and other highly confidential information. In order to be able to protect this sensitive information while providing external access, and secure access from the internal network to these servers we will implement a screened subnet architecture (DMZ). The DMZ will reside on a non-routable IP subnet (192.168.49.0/24) different from that of the internal network (172.16.10.0/24) and the production site network (10.20.30.0/24). All firewalls will use Network Address Translation (NAT). We have determined the network must be protected using defense in depth, while applying a least privilege approach to access control.

We have chosen to place our public DNS servers outside the firewall and we will secure them using the guidelines from the Systems and Network Attack Centers, Guide to Securing Microsoft Windows 2000 DNS[1], as well as SANS GIAC Security Essentials, Day 5, Windows Security[8]. We will also be installing Host Based Intrusion Detection (HIDS) on the DNS servers.

We will be using Microsoft Internet Security and Acceleration (ISA) Server in fully integrated mode for all of our firewalls. This effectively means we will be using a fully stateful Application Proxy Firewall. These firewalls can be centrally monitored and managed using a Microsoft ISA Server Console. The fully stateful nature of this firewall ensures that local and remote hosts remain isolated, and packets will also be forced to obey their protocol rules. This certainly doesn't mean we are fully protected and don't need any further security as an attack can conform to all protocol rules, but it is a good start to our defense in depth strategy. These firewalls also allow us a very granular level of control over what is allowed to enter our network. This includes being able to prevent streaming of

media files, prohibiting certain file types from being viewed, as well as performing other content filtering. Microsoft's ISA server also allows us to control bandwidth usage, restrict access times, and generate comprehensive management reports. At this point our network begins to diverge, with the DMZ needing to be dealt with separately during this discussion. Therefore we will first discuss the DMZ, and then we will expand on our internal network and production site.
Our DMZ will contain the following servers;

- Two Windows 2000 Advanced server machines running IIS5 in a cluster to serve GIAC Enterprises public web site.
- Two Windows 2000 Advanced server machines running IIS5 in a cluster to serve GIAC Enterprises extranet (Intranet accessible from outside the organization) site.
- Two Windows 2000 Advanced server machines running SQL2000 in a cluster to support GIAC Enterprises internal and external web sites.
- A front end Exchange 2000 Server used to provide web based and regular email to our users.

The two IIS5 machines hosting our external web site will be clustered using Microsoft's native clustering service, providing load balancing as well as redundancy. Due to the nature of GIAC Enterprises online business they need to achieve 99.9999% uptime, and the failover protection is absolutely necessary given this need. These standalone servers are in the DMZ to provide protection to our internal network by being able to separately control access to these machines, as well as being able to define tighter security and controls by effectively creating a bastion host type environment. The DMZ keeps outside users segregated from our primary internal network, allows delivery of services which may otherwise put our internal network at risk, and allows application of security that would potentially interfere with normal network operations.
The two IIS5 machines hosting our extranet site will also be clustered using Microsoft's native clustering service on Advanced Server, to provide load balancing as well as redundancy. Due to the nature of GIAC Enterprises business, access to this extranet site which will include the companies web site staging, internal employee information, as well as marketing material and related information needed by the sales force must be available 7/24. Although uptime expectations on this site are not as stringent as the external web presence, maintaining access to this information is still critical. These servers are in the DMZ for several reasons. We can provide significantly tighter access controls to these servers including Secure ID single use password authentication over SSL for our sales force needing to obtain marketing and sales information from an external location, or to input online sales orders. We can also concurrently allow internal network users access to this server without the need for secure ID authentication, and without allowing an external connection into our internal network.
The two SQL2000 servers will be providing business line data support to the external and internal web sites. They will be running on Windows 2000 Advanced Servers using Microsoft's native clustering support again to provide load

balancing and failover support. As these servers will be providing critical data necessary for the internal and external web sites they must maintain a 99.9999% uptime. Access to these servers will be heavily restricted. All web development has used encrypted COM+ objects to access data on the SQL servers so no passwords or user ID's needed to access data on these servers are directly accessible or travel over the wire in clear text. Having these servers and this data travel from the internal network would decrease performance as it would need to pass through the internal firewall, potentially open another security hole, and would need to be secured differently if they existed in the internal domain. In this regard the only data which will travel into our internal network will be "on change" SQL replication from the sales ordering system. This data will travel from the external SQL server to the internal SQL server, which maintains the ordering and shipping information.
The front end Exchange 2000 Server will be used to provide our travelling and remote users with access to web based email (OWA) as well as regular incoming mail which will be forwarded to the internal backend server. As OWA functionality will be provided via port 443, with a Server Certificate (SSL) and secure ID using IIS5 this does not require we open another port on our firewall as all other web servers also have the requirement for SSL. This front end server will simply take the request, securely pass this through the internal firewall, and provide the response to the client. All communication between this machine and the primary internal mail server will be on a secure channel, using MAC addresses and Kerberos for security. Its placement in the DMZ removes the need for another port open to the internet on our internal network.
Overall the DMZ area of our network is set up to be a highly protected area where we control and monitor external access to machines that need to be highly and widely available. This is not to say our internal network needs to be less dependable, or less secure, but our approach needs to differ slightly due to the nature of the access.

Our internal network will contain the following servers;

- Three Windows 2000 Server machines which will serve as our domain controllers.
- Five Windows 2000 Servers will be used to provide file and print services for the primary location.
- One Windows 2000 Server will be our mail server running Exchange 2000
- Two Windows 2000 Advanced Servers will be clustered to run an RSA ACE Server supporting our secure ID authentication (single use password)
- One Windows 2000 Server will be our internal SQL 2000 server
- One Windows 2000 Server will be our IAS Server
- One Windows 2000 Server will be our RRAS machine
- One Windows 2000 Server will be our security management machine running ISA server management console and our McAfee Anti virus Management Console

We have placed three domain controllers in the internal primary location network so we can separate the Flexible Single-Master Operation (FSMO) roles and provide the highest possible security for these critical machines. One server will be the PDC Emulator (not needed in our native environment), RID Master, internal DNS and will be a global catalog server. The second server will be the Schema Master, Domain Naming Master, and will also be a global catalog server. The third and final Domain Controller will only hold the Infrastructure Master role as a server not maintaining the global catalog should hold this role[4] (pg. 353). This machine will also be a second internal DNS server, KDC, and our DHCP. This setup also provides readily available DNS and DHCP for Kerberos functionality. All domain controllers will consist of our default hardware setup with a five-disk RAID 5 array. This configuration also provides redundancy and availability, but does increase some intrasite replication traffic. However with the gigabyte backbone this is not considered a significant problem.

Our file and print servers as well as all internal network servers except our Domain Controllers will all be maintained in the internal network, and will be placed inside the Network OU, within the Server child OU. This will allow us to apply a specific Group Policy to these servers, allowing the extra services needed to run on only these machines, control access to printers and data, as well as monitor access more closely. All file and print servers will be on our minimum hardware platform with five disks in their RAID 5 arrays.
Of the five file and print servers, one server will service Research and Development providing the ability for us to ensure we effectively control and restrict access. As this server will house product and development information that constitutes the firms highest value asset, it requires significantly more protection and monitoring. If someone were to damage, destroy, or steal this information it would cause significant harm to GIAC Enterprises. In this situation simply using a “least privilege” approach to access is not sufficient. We must focus significant defense in depth as well as least privilege on these corporate information assets. Failure to do this may result in these assets not being treated appropriately in a court of law relative to other corporate assets. Basically something this important to the company should be treated and secured accordingly. With this server in the internal network, within the Server Child OU will allow us to closely monitor and secure this data, including monitoring it with Host Based Intrusion Detection.
The second file and print server will be used by Human Resources. Due to the confidential nature of this information certain extra precautions will need to be taken to ensure compliance with any local, State, Provincial, or Federal privacy legislation. This server will house all of the HR Departments employee, payroll, benefits, and other related information. The HR Departments shared folders will reside here, and it will also be their print server. This will allow us to lock the machine down with a Group Policy as well as streamline resource access administration using our group structure.
The third file and print server will be used for the Finance Department and Executive and Management employees. Information relating to the corporation

will be maintained here, and a significant amount of it will likely be highly sensitive. Financial records, executive level data and planning information, as well as other data will be stored here. Again, the nature of this information requires extra protection and controls, and the separate server will allow us to closely control access using groups.
Our last two file and print servers will be used by the IT Department and Sales and Marketing. Although the information on these servers needs to be secured, it is not of the same confidential nature as that which will be stored on the other servers. This Sales and Marketing server will also be used to store and share information that needs to be available company wide, along with Sales and Marketing's departmental specific data.
The fact that all servers will also be print servers allows us to restrict access to certain printers, thereby allowing highly confidential documents to be printed to only certain printers by certain users. This will prevent a Human Resources user accidentally printing salary information to the Research and Development printers. We are also only allowing individual departments access to resources on their own server through the use of groups. This will assist in minimizing administration for resource access, and allows easier review of permissions if needed. It should also significantly decrease the potential for accidentally granting access to someone who shouldn't have it. The odds of a sales user getting put into an HR group are slim, and if someone changes specific permissions on a shared folder, and runs the access to all child objects the access will still stay within the specific department.
Although we could have easily combined servers to service more than one department, management elected to proceed in this manner to ensure future growth was being accommodated for as well as dealing with the least privilege access needs.
We will be setting up one server to handle our internal and internet based email services. This server will be running Exchange 2000, providing email, public folder access, mail distribution lists, and future support for instant messaging. This server is protected on the internal network in the Server Child OU - Network OU, and access to email will be provided through a front end Exchange 2000 server in the DMZ. This server is inside our network as the use of the Front End Exchange machine will effectively hide this machine from outside users, and allows us to protect our mailbox stores, public folder information, and distributions lists. Any email functionality for the web site will be programmed through NTSCDO or a third party programmatic interface. This email will travel from the Web server, to the front end Exchange machine, then to the primary Email server through the internal firewall. There will be no direct email from the companies web server. All incoming regular email will also be received by the front end exchange server and forwarded to the backend server, and outgoing email will come from this machine to the Front End server and then out. This server will also be running McAfee Groupshield and McAfee Webshield for Exchange server providing virus scanning of the message store, emails, and attachments. The hardware configuration of this machine will be that outlined in our assumptions for Exchange servers, with a ten disk RAID 5 array.

We will be using two Windows 2000 Advanced servers with our standard hardware and a 5-disk RAID 5 array in a cluster for our RSA Security ACE server to provide the Secure ID authentication needed for our external access. This authentication scheme will be used when accessing the extranet site from outside, as well as when users are accessing the internal network via a dial up connection. We decided to use a cluster setup for this server as significant issues arise if this server were to fail. These include not being able to access from an external location, and the users token can go into "next token" mode which would be confusing for users. It is highly unlikely that the load balancing of the cluster would ever be an issue, as usage should be relatively light. This server is located inside our network so we can apply very restrictive access policies and the management and issuing of new Secure ID cards can be controlled and monitored.

As we will provide dial up access to remote users we will be installing a RRAS server on one Windows 2000 server and another Windows 2000 server will be used as an IAS machine. These servers will be secondary authentication for access after a secure ID login and will provide the group policy and access restrictions for the remotely logged in user. All remote access policy will be controlled on the IAS server and access to this server will be controlled by group policy. Both of these machines will be our minimum hardware with five disk RAID 5 arrays. As we do not want dial up access to our DMZ this server will reside on our internal network.

To provide centralized management capability for the Information Technology department one Windows 2000 server will be set up to provide ISA Firewall, Anti virus, logging, and other security and network administration. This server will allow IT Administrative staff the ability to make changes, push out updates, and review and monitor the network and event logs. All network and DMZ servers will have their event logs downloaded into ASCII format onto this machine where they can then be imported into a spreadsheet for analysis. The Event log files will also be cleared from this centralized location. We will be using batch files and the dumpel.exe from the Windows Resource Kit[9] to pull out the logs in ASCII format and NTOlog utility available from Packetstorm Software[10] to remotely clear the event logs. McAfee Anti virus updates will be downloaded and automatically distributed to all servers and workstations as well as any patches or engine updates needed for the anti virus software from this server. IT administrators will also be able to manage the ISA firewalls from this console, including the ability to review all firewall log files, change rules, protocol handling, content filtering, and all other aspects of the firewalls needed administration. This server would be closely controlled, with access restricted to members of the IT administration group with security related responsibility. Due to the heavy use and volume of data on this machine it will have an eight-disk RAID 5 array.

Figure 1.

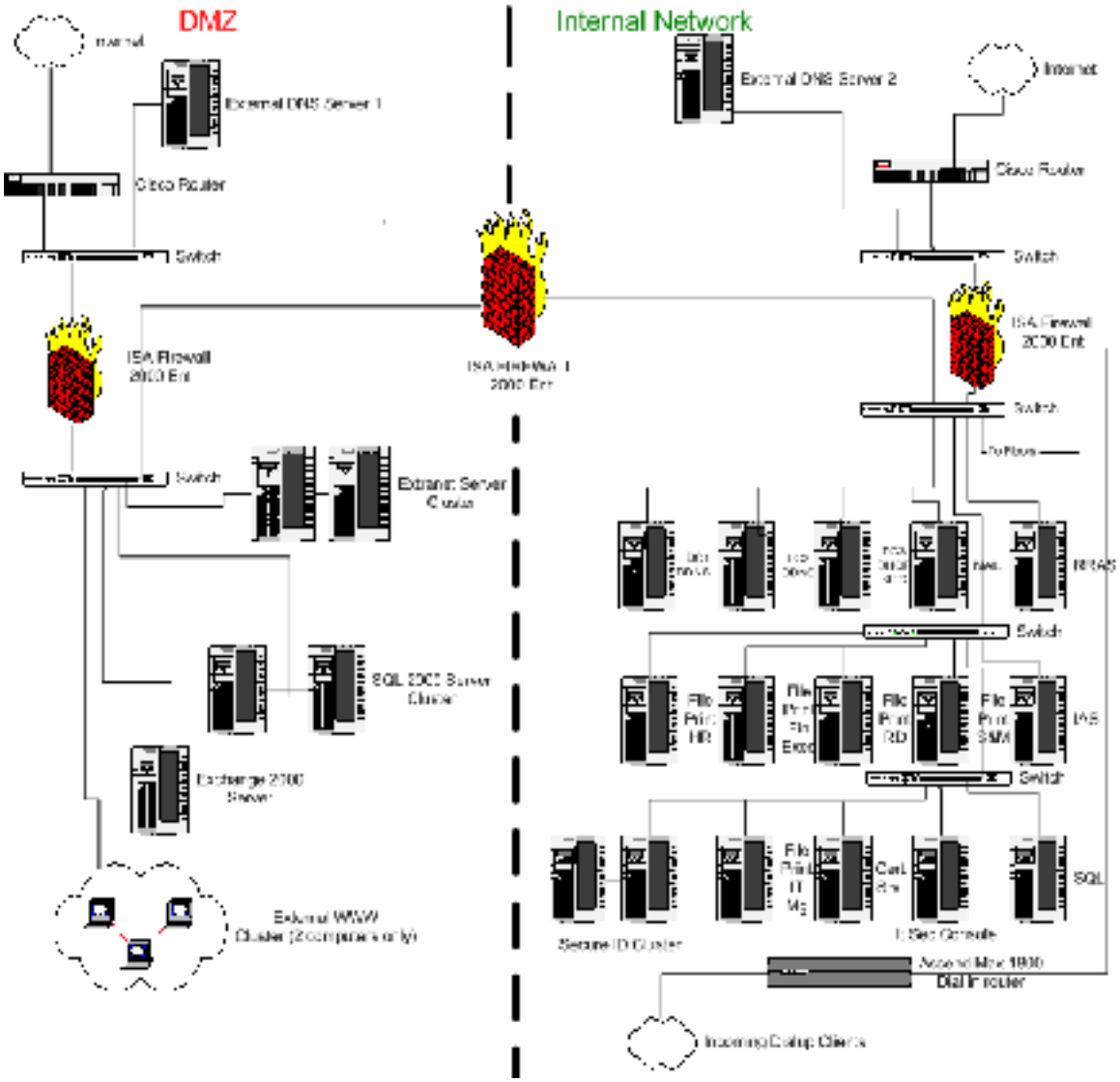
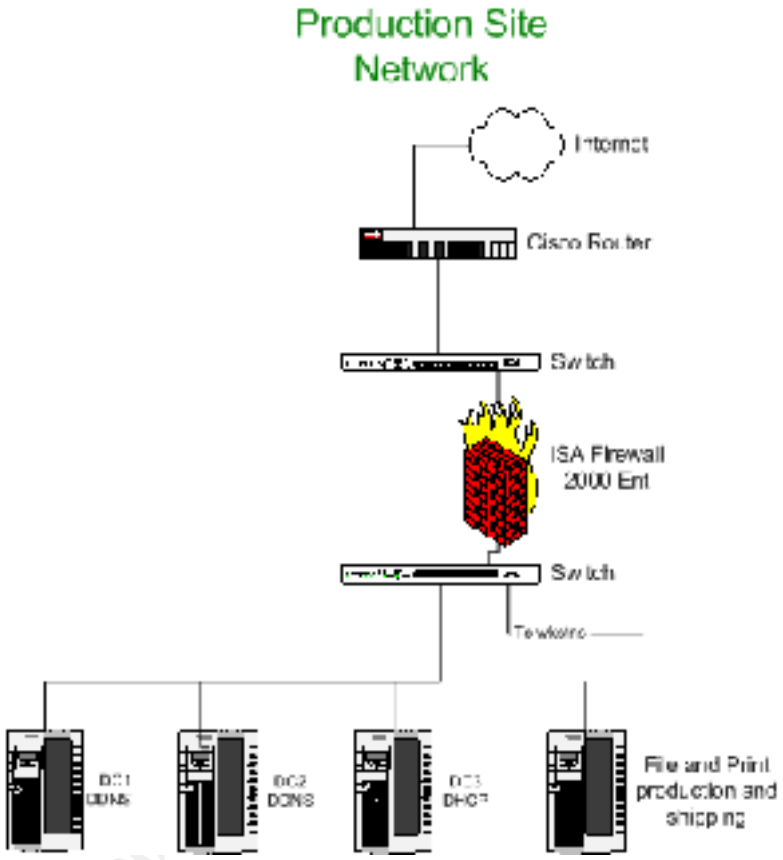


Figure 2.



Our production site network (figure 2) will contain the following servers, all of which will be our standard hardware setup with five disk RAID 5 arrays;

- Three Windows 2000 Server machines which will serve as our domain controllers.
- One Windows 2000 Server will be used to provide file and print services for the production site location.

The production and shipping site will be connected to our primary network via a VPN between the ISA firewalls located at the edge of each network. This will be a native Microsoft ISA server VPN using a 128 bit encrypted channel and MAC address authentication between servers. As our connection to the primary network is very reliable, with lots of bandwidth we do not have any replication concerns. We are placing three domain controllers in this site to provide redundancy and to minimize WAN traffic for authentication and name resolution. In the event the WAN link goes down, these domain controllers will allow this site to continue operation uninterrupted. In the event a domain controller crashes, we have redundancy. And in the event something in the primary site fails, users from that location would still be able to come across the WAN to resolve addresses for resources or authentication.

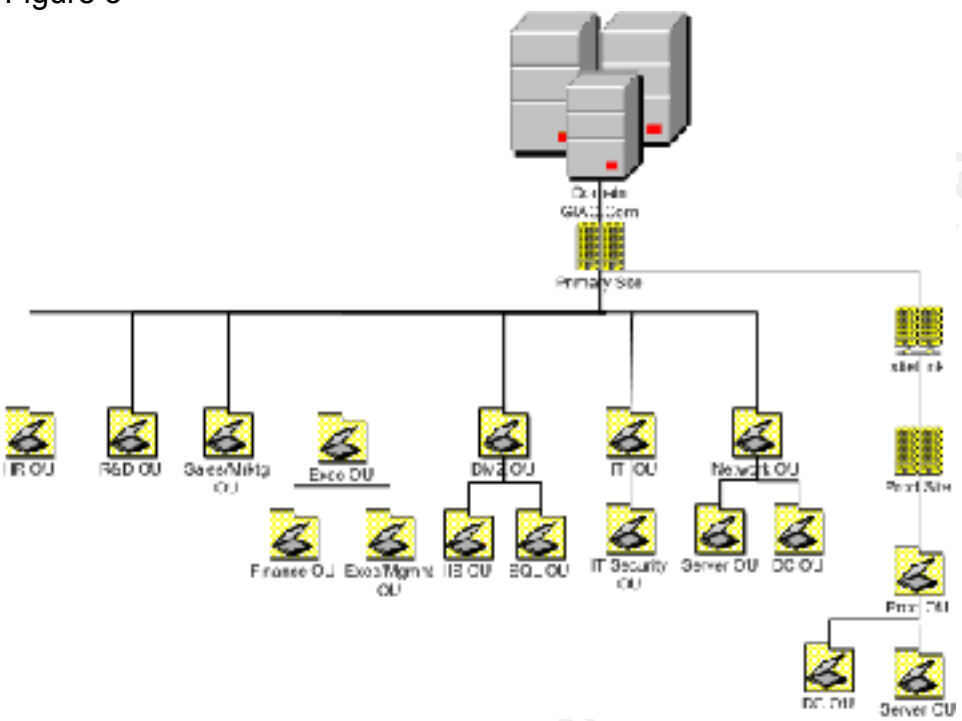
The three domain controllers will provide local authentication for users in the site, as well as local DHCP address assignments, DNS resolution for the site, and maintain a local copy of the global catalogue. The shipping and production file and print server will provide shared folder storage, print functionality, and access to specific data and applications needed for the users functions. It will reside in the server child OU in the production site so we can manage and secure it easily as well as decrease WAN traffic.

Active Directory Design

By far the most important part of designing a Windows 2000 network is in how the Active Directory is designed. The design can affect issues such as replication, access, and future expansion but more importantly the application of effective security and the minimization of administrative workload.
As domains are a management and security boundary, we have determined that GIAC Enterprises currently needs a single domain, two site network. As this is a new network, the domain will also be the root domain. Active Directory domains are used for the organization of resources, often geographically, but they can also be used within a single location. However, when multiple domains are used administration and security become separated, thereby increasing workload. You also cannot take a resource in one domain and add it to an Organizational Unit in another domain. This creates duplication of security policies, administration, and results in some performance issues. We must be careful not to confuse this with a DNS domain, which Windows 2000 actually uses very heavily, but to find resources, not organize them. As GIAC Enterprises grows, should they need to add a new office in another location, they could add another site, or a domain to the tree, depending on their needs. We can then assess implementations of Distributed File Sharing (DFS), and the use of Universal groups.
Organizational Units (OU's) help us to form a logical administrative grouping. By using OU's we can place like objects together and apply a security policy to the OU. Objects which can be placed in OU's are items like Users, Computers, Groups, Printers, Applications, File Shares, and other OU's to name a few. We have decided to use OU's within our domain to help with administration and security. The GIAC Enterprises Active directory design is shown in Figure 3.

The implementation of an Active Directory design begins when you run DCPROMO.exe on the first Windows 2000 Server to promote it to a domain controller. After promoting our first Server all server hardening, Service Packs, and hotfixes will be applied. This will be mandatory with all servers and is outlined in our assumptions, with server hardening detailed in the Security configuration area of this paper. When we promote our first server we will choose permissions which are "only compatible with Windows 2000 servers" during the DCPROMO Wizard. This will eliminate the possibility of "null user session" issues. We will also immediately change the server to Native mode prior to promoting any other servers or adding them to the domain. After promotion of the second and third servers to domain controllers the FSMO roles will be reassigned as outlined in our network design.

Figure 3



All OU's will be owned by the Domain administrator and delegation of OU administration to users outside the IT group will only be considered after the delegates have received appropriate training. We will therefore assume no authority delegation will occur at this time, but we will design our AD to accommodate this in the future. Delegation of authority to add, delete, or update objects in the OU's, or to change OU container properties such as policies will be controlled through groups.

Each OU will have a special group for authority delegation. We will create a user account with administrative privileges specific to each OU. This account will be added to the special group for its corresponding OU. This will give us an extra level of defense. Should a hacker gain administrative power over our production site server OU, they will not have the same administrative power over our domain controllers, IIS servers, or other critical machines. This also adds to our least privilege security at an administrative level.

Group policy can be assigned at several levels: Local, Site, Domain, and OU. Group policy, without any inheritance blocking or override restrictions will be applied in this order as well, with each progressive policy overriding the previous settings. Basically this means OU policy takes precedence over domain policy, and domain policy takes precedence over site policy. What we must keep in mind is that where block inheritance and no override settings conflict, no override will always win. We can also use what is called Group Policy Loopback, which involves two other settings called merge mode and replace mode, but these are

for very specific and unique situations, which we do not need to implement, and are beyond the scope of this paper. In our two site, single domain environment we will configure all of our security at the domain level and below, even though we could apply a policy to each of our sites, this would be redundant. Our altered default domain policy can accomplish the same security level as a site policy, and we will be using OU level policy for specific security settings. This will also help with performance as login times slow when you load another group policy. By eliminating the Site level policy we will eliminate the need to load the redundant settings and therefore save this time and traffic.

All servers other than those in the DMZ and our Domain Controllers will be placed in the Server Child OU under the Network OU as outlined in our AD plan so specific security settings can be applied. Servers in our DMZ as well as domain controllers will be in separate OU's to facilitate significantly higher security for these machines.

The following is a summary of the Organizational Units, their roles, purpose, and the logic behind them.

OU	Reasoning and Application
DMZ	This OU will house machines which will be available externally, and is designed to help segregate these higher risk machines from our internal network. We will be applying highly restrictive security settings to these exposed machines and control who has the authority to access and manage them. Direct access to our internal network will be avoided using this OU and the machines within it.
IIS and SQL Child OU's	These child OU's will allow us to apply the highly restrictive GPO's needed for critical servers resident in our DMZ. Our front end exchange server will reside in the IIS Child OU. By separating these servers we can be very specific on what runs on them, and also restrict internal access to them.
Network	Group and control servers and other network resources used within the domain for authentication and other functions critical to domain operation. This OU will allow us to separate our internal servers, and apply group Policies appropriate for the machines role within our domain.
DC Child OU (primary and production site)	This OU will allow us to apply a different and more restrictive GPO to these critical servers. We can ensure our DNS, DHCP, AD, and other critical network data is

	properly secured and access is restricted appropriately. This is effectively our authentication and network administration OU as all accounts, users, groups, and resources will be stored on these servers and access controlled here
Servers Child OU	This Child OU will allow us to restrict access to servers specific to departments and other specialized functions. Highly confidential information such as HR data and Financial information need to be closely monitored, and secured appropriately. The file and print servers for all departments will be objects here.
Departmental OU's (R&D, HR, Exec, Prod, Sales & Marketing)	These OU's are used to apply departmental specific restrictions and security to. It also allows us to use a least privilege approach more effectively. These OU's allow us to manage our users access, installed programs, updates, and roles more easily. Users changing departments can be moved to their new OU, as can their computers and then they receive the specialized policy, applications or anything else specific to that department.
Finance and Exec Child OU's	These child OU's are designed to allow us to properly secure access to the sensitive data which will be available to specific users who are members of these departments. Significantly closer monitoring and tighter controls are needed and this OU will allow us to streamline this ability. This OU is a result of the same logic as other departmental OU's, but its membership will have greater access to highly sensitive data which may be the target of corporate espionage or the like.
IT OU	Ability to apply and control administrative privileges for the domain and OU's. Will manage all other OU's through the use of groups. This OU is designed to allow the application of a much less restrictive policy for users and machines, while maintaining heavier restrictions for other users. Users in this area will have great powers relative to domain and site functions and access, but they also may need closer monitoring. Changes users in this group may be able to make could potentially effect our entire network, and access to the OU needs to be restricted separately from other OU's
IT Security Child OU	This child OU will contain the Management consoles, and ISA Firewall administration console. Only certain IT

Administration staff will have access. The nature of the applications and management tools available here require significantly tighter controls. This will allow us to control who can alter critical domain functions, and see information relating to overall domain activity, use, and performance.

Security Configuration and Group Policy

The effectiveness of our overall network security begins during the initial installation of our network hardware and operating systems. We will apply baseline security to every operating system, and then extra hardening will be applied to machines based on their anticipated roles within our domain or sites. This preemptive baselining also extends to our routers, switches, and any other hardware devices on our network. Even the best planned and implemented Active Directory structure and Group Policy is useless if your perimeter has not been appropriately assessed and secured. All decisions regarding this baseline hardening are derived from GIAC Enterprises Security Policy, which was previously developed, and has received Executive Management's approval. We will deal with the security baseline by progressing through our network, starting with our edge routers.

Router Security

Starting with our Primary Cisco routers, one will control access to the DMZ, one to the internal network, and one to the production site network. All routers will have twelve character, complex passwords (minimum 4 character sets) assigned to both user and privileged mode using Cisco's "secret" password convention so we have a none reversible MD5 hashed password. The same will apply to all five virtual terminals, and the console and auxiliary ports. Telnet will be disabled on the router's interfaces, and access will be required via console logon, no remote access will be allowed.

Egress and Ingress filtering will be set up on both routers, preventing address spoofing, and dropping all packets appearing to originate from non routable addresses, multicast addresses, and any invalid IP addresses. We would like to use Cisco's new AD functionality where the router can obtain its setup directly from Windows 2000 Active Directory however this functionality is still in development.

All routers will have the following disabled on all interfaces[11] (pg. 526-535):

- NTP (Network Time Protocol)
- UDP and TCP Small services
- CDP (Cisco Discovery Protocol)
- Finger Service
- Network Broadcasts (IP directed Broadcasts)
- IP redirects and unreachables
- IP Proxy ARP's
- SNMP Service

We will also be splitting GIAC Enterprises external IP address space between the three routers.
Our Ascend 1800 Max Router is a specialized hardware device that adds an extra level of control and security to our dial up functionality. This router has a bank of modems as well as multiple LAN ports. Incoming dial up connections are accepted, and then passed to our firewall, with a destination of our RRAS server. Our firewall will intercept this traffic and prompt for Secure ID authentication prior to allowing a connection to our RRAS server. Once the Secure ID authentication process is completed, the client will enter the Windows 2000 authentication process, with access and security controlled by policy on our IAS server.
This router requires setup on two levels, the modems and the actual router functionality.
All router configuration files will be backed up and stored on our IT security Management console, in a directory protected by NTFS and encrypted using native Windows 2000 EFS.

Switch Security

Each router will connect directly to a Cisco gigabyte switch. Our firewalls will be plugged into one port, and our external DNS will be plugged into another port on the DMZ and primary internal network routers. All switches will also have complex passwords which will be needed to effect any changes. All switch configuration must be done at the console level, telnet access will not be allowed. All other internal switches will be configured in an identical manner

Server Hardening

We will discuss this aspect of basic server security in two stages, the standard hardening that will be done on all servers, and then the additional hardening that must be done on specific machines.

- All servers will have NTFS on all partitions. All OS drives will be converted to NTFS during setup as this allows Windows 2000 to apply more effective and restrictive permissions to the file system than doing the conversion after installation.
- All unnecessary software and protocols will not be installed on any server. Specifically we will only install TCP/IP, and IIS will not be installed except on web servers and the front end exchange server.
- Unnecessary software will be removed. If necessary edit %systemroot% \inf\sysoc.inf and remove the “hide” reference (leaving the quotes) for the programs you want to uninstall. These items will then appear in the add/remove programs applet. DO NOT remove items you are not completely sure about.
- Remove any unnecessary certificates from the certificate store using the Certificate MMC snap-in.
- NetBIOS over TCP/IP will be disabled on the WINS page of TCP/IP properties. As we will have a native environment WINS will not be needed and NetBIOS over TCP/IP was used to support this functionality.

- Apply Service Pack 3, all current hotfixes and the high encryption pack. We recommend using Gravity Storm Software's Service Pack Manager 2000. They have just released a free version which will determine which hotfixes you need, including those for IE, Exchange versions, SQL versions, all versions of Windows NT, Outlook, ISA Server and others. The free version will not automate the download and installation of the hotfixes, but as a discovery tool it works well, and it has a good GUI interface. You can download this from http://www.securitybastion.com.
- Disable any unnecessary services based on the servers expected role using group policy. We have defined four roles - Users machines, Domain controllers, Servers, IIS/DMZ Servers. Our group policies will deal with each role. Namely the Default Domain Policy for user machines (as a result of blocking inheritance on some OU's this policy will apply only to user machines, not servers), Network Policy for Servers, Domain Controller Policy for our DC's, and Web Server Policy for our IIS/DMZ machines (with the exception of our external SQL machines which will have the Network Policy applied)
- Change the C:\ drive NTFS permissions to Administrators and System – Full Control
- Alter the pagefile settings so the minimum and maximum amounts are equal
- Run keymigrt.exe on the server to upgrade all private keys to 168 bit 3DES from 40 bit
- Set the permissions on the CMD.exe file in %systemroot%\system32\ to Administrators – Full Control. This file is often used during installation of programs (SQL for one) and removing it is not wise. Also Windows File Protection will replace this file if removed or renamed. Changing the permissions to Administrators – Full Control should have minimal effect as most installations or tasks need to be run under the Administrator account.
- Delete the guest account using delguest.exe
- Set a complex administrator password
- Use Passprop.exe to allow the administrator account to lockout. This forces an administrator to log on at the console to reset the lockout. It is also a good indication of an attempted or successful intrusion.
- Edit the registry and delete the DefaultPasswordKey if it exists, and ensure AutoAdminLogon is set to 0.
- Disable the Autorun feature for CD-Roms
- Disable Windows Scripting Host
- Create a new Emergency Repair Disk after all hardening is complete.
- Verify the \repair directory has its permissions set to Administrator - Full Control after the repair disk is done.
- Change the NTFS permissions on the Regedt32.exe and regedit.exe file to SYSTEM – Full Control, Administrators – Full Control
- Change the NTFS permissions on the Config.sys and autoexec.bat files to SYSTEM – Full Control, Administrators – Full Control, Everyone – Read and set the attributes on these files to read only

And finally a Security Policy will be applied. We will be using policies as outlined later in this paper on all servers. All servers will have specific policies. We will use the "block inheritance" option and then apply the specialized policy to the appropriate OU.

External DNS Servers

We have decided to use freestanding, bastion host external DNS servers sitting on each external connection. Both DNS servers will maintain identical zone records, but will not update each other. They will be standard zones, not Dynamic DNS. This will prevent both servers becoming polluted with bad zone data should hackers penetrate our defenses. These servers will also be used for resolution for our external facing firewalls. Both DNS machines will be standalone Windows 2000 servers, each in a separate workgroup. After OS installation, with all basic Server hardening and specific DNS server hardening[5] mentioned previously we will be applying a local security policy. As these servers are outside of our internal network we will not delve into specifics.

Web Server Hardening

The following steps are in addition to the above outlined basic server hardening. Due to the nature of web servers, as well as the addition of extra software certain special steps to minimize risk must be taken.

- Provided IIS was installed during the initial OS installation, appropriate patches would have already been installed. It is however a good idea to double-check at this point.
- Ensure your root directories for your web and FTP sites are on a different partition (the RAID 5 Partition) from your operating system. File traversal threats cannot cross between partitions.
- Alter the standard directory structure of the root directories for the web and FTP sites. For example use D:\public\shared\inetpub\ instead of the defaults. This will make it tougher for malicious scripts to find what they are looking for.
- Delete all unnecessary mappings. Most web sites do not need .htr, .idx, .idc, .printer, .htw, .rda, .idq, .cdx, .cer, .shtm, .stm and .shtml. Rule of thumb, if you don't use it, remove it. Multiple threats take advantage of these.
- Stop the default web site and create a new one for our external web
- Verify the following do not exist, and if they do delete the appropriate virtual sites and their corresponding directories;
    - IIS Samples
    - C:\inetpub\iissamples
    - IISSamples\SDK (subdirectory of above)
    - AdminScripts
    - C:\inetpub\AdminScripts
    - Help\IISHelp
    - C:\WINNT\help\iishelp

    - IISADMPWD (not installed by default on IIS5)
    - C:\WINNT\system32\inetsrv\iisadmpwd
    - MSADC\Samples
    - Printers
    - C:\WINNT\web\printers
    - C:\Inetpub\mailroot
    - C:\Inetpub\nntpfile
    - C:\WINNT\Help\mail
    - C:\WINNT\Help\news
- Alter your IIS server master properties to enable W3C extended logging, create a new log daily, and turn on all logging options
- Rename IUSR_MachineName and disable IWAM_MachineName accounts
- Reset the NTFS file permissions on C:\Winnt and the IIS root directory for the renamed IUSR_MachineName account to read. You need to uncheck the "Allow Inheritable Permissions from the Parent Object to propagate to this object" box and choose "copy" when prompted.
- Set permissions on all disk volumes on the machine to "No Access" for the renamed IUSR_MachineName account, then click the advanced button and check "Reset Permissions on all Child Objects". You must do this to ensure the parent and all child objects are properly configured.
- Test and apply the Web Server Security Policy template with the settings outlined later after blocking inheritance of the Default Domain Security Policy.

Front End Exchange Server Hardening

The front-end exchange server in our DMZ is our external mail server but also runs IIS5 to provide access to web based mail (OWA). Based on this the server will be hardened using the web server hardening techniques and the web policy template. All communication to the primary internal mail server will be done on a second NIC card, with private addressing, and MAC address restrictions to pass through the internal firewall. All external communication will be over SSL, with Secure ID authentication required for connection. Normal incoming and outgoing email will also follow this path, without the SSL and secure ID.

Firewall Hardening

Our firewalls will all be Microsoft Internet Security and Acceleration Servers (ISA). They will all be standalone machines, each in its own workgroup. This will not affect our ability to remotely monitor or administer these machines, but it does add an extra level of protection as they are not participating members in our Active Directory Network. Should an intruder compromise one of these machines, they still will not get to our accounts database, or any user credentials which would allow them easy access.

With the exception of all service packs and hotfixes, including the ISA Server Service Pack very little extra hardening needs to be done. Upon installation of ISA Server, the firewall immediately assumes control of all network connectivity,

and all local services. Any unnecessary services are stopped, all access through the firewall is blocked, and you must begin configuration to allow access.

Groups

One aspect of Windows security always has been the use of groups to control access to resources. In Windows 2000 this has not changed, but has actually been enhanced. To this end it is necessary for us to create groups to manage our users and other resources with less administrative overhead. Without a great deal of forethought and planning we could easily "build in" our own security risks when it comes to this aspect of our network. Groups are critical to the successful application of the "least privilege" theory of security. Without them we have a potential administrative and security nightmare.

Windows 2000 provides several different classes of groups that we can create depending on what we need to accomplish, Local, Global, and Universal. It also allows for two distinct varieties of these groups, namely security and distribution. Distribution groups are basically mailing lists. Security Groups are what we need to deal with at this time. Security groups allow us to manage access to resources. We can apply any Group Policy we want but without groups to control access we are left wide open to internal or external unauthorized access. The basic theory behind groups is this:

- We place individual user accounts into Global groups
- We create Local Groups and assign them access rights to resources
- We then place Global Groups and Universal Groups into Local Groups to allow the group members access to the resource controlled by the local group.

Based on this we need to create the following groups:

- Local Groups which should reflect our resources
  - Printer Group for each Departmental OU - Finance Printers, HR Printers etc
  - User Groups for each Departmental OU - Finance Users, Finance Managers, HR Users, HR Managers etc
  - Groups for other departmental specific access such as restricted directories, role based accesses etc
- Global Groups which mirror our departmental responsibility
  - User groups for each Departmental OU - Finance Bosses, Finance Supervisors, Finance Staff, HR Supervisors, HR Payroll, HR Benefits etc
  - Specialized Groups for certain, absolutely necessary reasons such as contractors, executive assistants and the like
  - Specialized groups will be created for the IT department, namely IT staff, IT Help Desk, IT Administrators, IT Security Administrators

The application of the groups will be very consistent, controlling access to resources and ensuring appropriate restrictions. For example, the Finance Printers Local group will be given Print Permission on all finance printers. The Everyone group will be removed, and the Finance area global groups will be added to the Finance Printers Local Group. Full control will be retained by the

Administrators group, and the manage printer permission will be held by Server Operators.

Group Policy

We will now move on to Group Policy and its use and application in our network. We will be using Group Policy at several levels, however as we have a multiple site, single domain network, we are applying group policy at the domain level first, and will not be applying any Site policies. We are taking this approach as the Site policies would be identical to the default domain policy, and would simply create extra administration with no added value. The first Group Policy applied will be the Default Domain Policy. There are two primary components to this policy, Computer Configuration and User Configuration. First we will deal with the Computer Configuration. Due to the design of our network, this policy will in effect be applied to users machines, as all servers will be in OU's with inheritance blocked and specialized policies applied.

We must ensure that this policy applies domain wide and provides the minimum acceptable security level. Less or more security will be applied, where needed at the OU level. We will be applying the "no override" option or the "block Inheritance" option to OU's as needed. The "no override" option prevents Policies applied at a level below the Domain Policy (IE:OU) from overriding the Default Domain Policy. The "Block Inheritance" option prevents the Default Domain Policy from being applied from the point the option is applied and to any child objects below that. This idea of "inheritance" and "override" become somewhat complex, especially when one delves into the area of conflicts. When designing the default domain policy we need to remember that if computer and user settings conflict, the user settings will apply as they are deemed to be more granular. When it comes to Site, Domain, and OU policy levels, the default is to apply the most specific level. So if we apply the default domain policy, then apply a specific security policy template to the DC child OU, the specific policy will override the Default Domain Policy. In this type of situation we will apply the block inheritance option, and then apply the specific security policy, ensuring we covered off what the default domain policy settings covered, if appropriate. We also could control the order in which these policies were applied, but that significantly complicates things now and in the future.

With these details clarified, we can now alter our Default Domain Policy to meet our needs based on GIAC Enterprises security policy and our overall approach to securing this network effectively.

We will begin with the Computer Configuration Component of the Default Domain Policy.

This area of the Default Domain Policy manages software, Windows, security, account policies, local policies, restricted groups, and system services. Many of these areas have sub categories requiring a great deal of thought when making policy decisions. All of these Computer area policy settings will affect user's computers, their behavior, and what tasks they can and cannot do, when they are done, and often how it handles certain situations. As previously mentioned all servers will have their own specialized GPO depending on the OU they are in.

These specialized GPO's will be altered for the specific needs with this Default Domain Policy being the baseline. We will now run through the subcategories with an explanation of what they do, why, and how it helps or affects our security, and our settings.

Default Domain Policy
Computer Configuration

Software - This option controls automatic software installation, level of user interaction, and other options. This option is used when assigning or publishing applications to specific users, groups, or machines. The concept and functionality of the Remote Installation Server (RIS) is beyond the scope of this paper, except to say one can automate service pack and patch updates, and perform upgrades using it's functionality. You can also control application security, what a user can install, and various other items. This setting can be used at a significantly more granular level, and should be used at the OU level to apply specific software to groups of users or departments. Service packs and patches should be installed by OU to minimize network traffic and minimize downtime should something go wrong. We will not be changing anything in this area.

Windows – This area defines computer shutdown and startup scripts used on the machines. This can be used to execute special utilities on startup or shutdown such as clearing the certificate cache, disconnecting secure sessions, and other like actions. We will be using scripts to run Kbinit on startup and KBDestroy on shutdown to initiate Kerberos functionality and clear the cache on logoff. This will make the Kerberos functionality transparent to the users.

Security Settings – Account Policy

Password Policies

Enforce Password History

This setting ensures a users password is unique when they are forced to change it by saving the last X number of passwords and ensuring the user enters something different. As most people use passwords consisting of things familiar to them such as children's names and birth dates this option, combined with the complexity requirement will prevent a hacker's paradise of easily cracked passwords. We will set this option to remember 24 Passwords

Maximum Password Age

This setting ensures users regularly change their passwords, which is important to help counter shoulder surfing and some aspects of social engineering. We don't want this to be too long as it would frustrate users, or too short as it would defeat its purpose. We will leave this setting at 42 Days.

Minimum Password Age

This security setting prevents passwords from being immediately changed to avoid the Enforce Password History requirement. If users are aware only 10 passwords are kept, they will change their password eleven times, and even use complex passwords, to keep a familiar password, thereby usurping our security. This is why we set this to 3 Days.

Minimum Password Length
We could force this setting to be a very long password to ensure they are more difficult to crack, but they would also be more difficult for our users to remember. Studies have shown humans can recall up to 7 characters accurately, so we have to decide between higher security and user frustration. We hope to minimize user problems, but to also provide a reasonable password length. We could force this setting to 14 characters, but most users have trouble with much shorter passwords. We have decided to use 8 characters to hopefully minimize user problems, but to also provide a reasonable password length.

Passwords must meet Complexity Requirements
This setting will help add strength to our passwords. With the requirement to use multiple character sets in the password the length concern is somewhat mitigated and should a hacker acquire our password database it will be more difficult to crack. Although a combined complex password of significant length is ideal (12 characters), it is not always reasonable based on the environment. This setting will be enabled and will help add strength to our passwords.
Store Passwords using reversible encryption
This is a risky setting to enable as it just makes a hacker's job easier. Not encrypting a password is just as risky as having the encryption reversible. By default this is disabled and as we do not foresee the need for digest authentication we will not change it.

Account Policies – Lockout
Account Lockout Duration
This setting determines if an account lockout is reset automatically, and how much time must pass before this occurs. We are setting this to 0 which means an admin must unlock the account. This prevents a hacker from using a tool like dumpsec to discover this reset period, then try password guessing knowing how may times they can try and how long they must wait between lockouts before they are able to try again.
Account Lockout Threshold
This setting ensures account lockouts occur after a set number of bad passwords are tried. This may be kind of a pain for users on occasion, but it counters some of the most common hacking attempts. We could set this fairly high to help minimize requests for password resets, but we need to balance this with security so we are going to set this to 3 attempts
Reset Account Lockout Counter after
Normally this item works in concert with the Account Lockout Duration setting, but we have set that to 0, so the account will never reset automatically. That leaves this setting to reset the counter after bad passwords are entered. If a user enters fewer bad passwords than the Account Lockout Threshold, and the period defined in this setting passes, the counter is reset and the previously entered bad passwords become irrelevant. To be safe we are specifying a relatively long

period of time as a deterrent. Hackers like to get things done fast and this will hopefully negate that. We are setting this item to 90 minutes. Note that this setting does not apply to screensaver password failures at the desktop.

Account Policies – Kerberos Policy

Kerberos authentication is used on a Windows 2000 network to authenticate clients and machines and in the process verify they have the right to log on locally to the machine or access the requested resource over the network. As an extra check it ensures that the user account requesting access to the resource is still active and valid. The overall process used by Kerberos is well beyond the scope of this paper, but we will cover off the basics as they relate to the settings controlled in this policy. We will be using Kerberos in our domain for authentication.

Enforce User Login Restrictions

This setting is what controls whether Windows 2000 performs the above outlined verifications and checks, and if it is mandatory or optional, if available. This item will be set to enabled as we want the extra authentication and non-repudiation provided by Kerberos. This will also add an extra level of security should a hacker penetrate our network as their ability to connect to servers will be restricted by this functionality.

Maximum Lifetime for a service ticket

This item defines the period of time a Kerberos Ticket can exist and be used until it becomes invalid. To minimize network traffic and streamline usage for users a ticket should have a lifetime at least equal to the organizations standard workday. Depending on an organizations scheduling it may be advantageous to extend this by a couple of hours as many people work longer than the basic workday. We are setting this option at the default, 10 hours.

Maximum Lifetime for a user ticket renewal

A ticket must be renewed if it is still needed after its lifetime expires. This setting allows us to provide a window for renewal past the set ticket lifetime if the user needs to continue using the ticket. This minimizes some network traffic as the renewal process is less intensive than issuing a new ticket. This setting is defined in days so we will set this to 1 day.

Maximum Lifetime for a user Ticket

This is the maximum time period a user ticket can be considered valid. If the ticket is not renewed it expires and the user must acquire a new ticket. This is technically known as the Ticket Granting Ticket (TGT). This is the total time a ticket can be used before it must be reissued. The default time is 10 hours, which is what we will leave this set at.

Maximum Tolerance for Synchronization of Computer Clocks.

This setting provides protection against certain attacks like the "replay attack" by ensuring times on systems are within specified tolerances. As Kerberos authentication includes a time stamp it is important that all machines have the same time. This does not have to be perfect, and this setting controls the allowable variance. As all machines will be receiving their time from the internal domain controllers we do not anticipate any significant variance problems. To minimize the potential for replay attacks we are setting this to 3 minutes.

Local Policies

Local Policies – Audit

This area of the policy defines what events we wish to audit and if we want to audit the specific event successes or failures. Not all auditing is controlled here, some specialized items actually must be turned on under Local Policy - Security options, but these are items we should be seriously considering as basic items to audit. One good example is auditing an account logon event, success or failure. As we are turning off the "show last logged on user" item, this audit log will give us the information about who has logged in and when. I can't think of any situation where you wouldn't want to turn on at least one or two of these items. We will be turning on the following settings.

Audit Account Logon Events	Success, Failure
Audit Account Management	Success, Failure
Audit Directory Service Access	Failure
Audit Logon Events	Success, Failure
Audit Object Access	Failure
Audit Policy Change	Success, Failure
Audit Privilege Use	Not Defined
Audit Process Tracking	Not Defined
Audit System Events	Success, Failure

Local Policy – User Rights Assignment

This area contains a very extensive list of options, all of which control rights, not permissions. Rights are generally considered more powerful than permissions due to the fact they generally relate to some basic operating system functionality. Items like loading and unloading device drivers, shutting down the system, logging on locally, and acting as part of the Operating System are contained in this area. The majority of the items are generally set at a reasonable level, or disabled, but some must be changed. Any item that grants the right to "everyone" should be closely assessed and more often than not changed. The authenticated users group is much safer and more secure than the everyone group, especially in this area. The majority of the other changes will likely be granting rights to administrators. To ensure we do not unknowingly provide server operators or other less privileged user groups with rights, which are inappropriate, we are assigning the majority of the rights to the administrators group. In most instances these rights will be used very rarely.

Due to the extensive list in this category we will only outline those items we will be changing

Change the system time	Administrators
Force Shutdown from a remote system	Administrators
Load and Unload Device Drivers	Administrators
Log on Locally	Administrators, Authenticated Users
Manage Auditing and Security Log	Administrators
Modify Firmware Environment Variables	Administrators
Restore Files and Directories	Administrators, Backup Operators

Shut Down the System Administrators, Authenticated Users
Take Ownership of files or other objects Administrators

Local Policy – Security Options
This area contains the options controlling what can be done on the machine, who can do it, and responses to certain actions. Items like a logon warning, who can install print drivers, who can access drives, and if communication is digitally signed between clients and servers.
Many of these options are important and should be closely reviewed. Due to the extensive list in this category we will only outline those items we will be changing.

- Additional restrictions for anonymous connections

-Do not allow enumeration of SAM accounts and shares – This prevents the enumeration of our SAM and other highly sensitive information

- Allow server operators to schedule tasks (domain controllers only)

-Disabled – We want to restrict scheduling of tasks to administrators to ensure they are closely controlled. Even though this applies to DC's only we want this set in our baseline policy to be safe.

- Allow system to be shut down without having to log on

-Disabled – Only Authenticated Users should be able to reboot machines

- Audit the access of global system objects

-Enabled – This adds to our audit trail by logging access to these objects.

- Audit use of Backup and Restore privilege

-Enabled – We want to audit this ability due to the security implications of this function

- Clear virtual memory pagefile when system shuts down

-Enabled – We want to ensure the page file is cleared on reboot as data in the page file could be accessed by a hacker and used inappropriately

- Digitally sign server communication (when possible)

-Enabled – This setting helps us protect ourselves from man in the middle and session hijacking attacks. The SMB communication will be authenticated and signed at the packet level. If the related authentication fails so does communication.

- Disable CTRL+ALT+DEL requirement for logon

-Disabled – We are disabling this as we want this process in place as it indicates an intention to actually sign on, and allows the use of the log on message

- Do not display last user name in logon screen

-Enabled – We want this in place so we do not reveal valid user names of administrators or other powerful accounts. We are logging logon events to monitor access to machines. Also leaving the user id showing on even a users machine allows a hacker to obtain half of what they need to penetrate our systems.

- LAN Manager Authentication Level

-Send NTLMv2 Response only/Refuse LM & NTLM – As we are not using any operating systems other than Windows 2000 we do not need to support downlevel LM and NTLM authentication

- Message text for users attempting to log on

-We are implementing a logon message for users to advise them of what may be occurring on the system (logging) and warning unauthorized persons not to access the systems. This can be helpful in court if needed as they were warned that we were logging what they were doing so cannot plead privacy violation as easily, and unauthorized persons are warned as well. This message requires the users click OK before they can proceed to the logon screen. This implies the warning has been read and agreement to the warning as presented.

  - This Computer System, data, and all attached peripherals are the property of GIAC Enterprises. Access to this computer system is restricted to those employees who have been granted explicit permission to do so by GIAC Enterprises. All access and activity on this computer system are subject to logging and review. Any unauthorized access or activity will be deemed an illegal act and will be prosecuted to the fullest extent of the law. By clicking OK you agree you have read and understand this warning and the inherent liabilities. If you are uncertain about your status regarding access to this system please contact the system administrator at sysadmin@GIAC.com.

- Message title for users attempting to log on

-This is just the title line for the above message.

  - GIAC Enterprises Restricted Access Computer System – Access subject to the below outlined Security Warning

- Number of previous logons to cache (in case domain controller is not available)

-0 logons – We are not allowing logons to be cached as they present a risk should a hacker access even a users machine. The hacker could extract the logon information, crack it and then have a level of access to our network.

- Prevent users from installing printer drivers

-Enabled – any driver can be a security risk, and printer drivers should be automatically installed on the users machine as all our printers will be network based. If we allow users to install drivers we risk infection, corruption, or worse.

- Recovery Console: Allow floppy copy and access to all drives and all folders

-Enabled – We want this enabled as a crashed machine may need new drivers, or we may need access to drives for troubleshooting purposes. In order to use this you will need to be logged on to the recovery console as an administrator.

- Notify users to change password

- 14 days. This will give the user the forewarning about an upcoming password change allowing them to be ready with a new complex password when the time comes.

- Rename administrator account

-Defined – as a basic security precaution we will rename the administrator account to something unremarkable and then create an account called administrator with minimal access.

- Rename guest account

-Defined – As above we will rename this account which is another hacker targeted account. Even though we are deleting the guest account, we are setting this to be safe. Guest account deletion is a manual process, and one could accidentally be added with a new machine.

- Restrict CD-ROM access to locally logged-on user only

-Enabled – anything that needs to be remotely accessed can be done via a network share with the appropriate NTFS permissions. There should be no reason to access a CD drive remotely

- Restrict floppy access to locally logged-on user only

-Enabled – As above, the reason to access a floppy drive remotely should be non-existent.

- Shut down system immediately if unable to log security audits

-Enabled – If a security logs fill it will be an excellent indicator that something is seriously wrong. We want the machine to shut down to prevent further damage or access and alert the administrators. We are setting our security logs to a fairly large size so this is likely a serious situation.

- Smart card removal behavior

-Lock Workstation – If we eventually use smart cards we want any machine to lock if someone takes their smart card out as they leave the machine. Leaving the machine open after the authentication media is gone is risky.

- Unsigned driver installation behavior

-Do not allow installation – Once again we do not want users to install any drivers we have not tested. We particularly do not want any unsigned drivers installed as they even present a greater risk, especially if they are from smaller or unknown organizations.

- Unsigned non-driver installation behavior

-Warn but allow installation – There is less risk to unsigned non-driver items, but we need to warn the user about his just to be cautious.

Local Policy – Event Log Settings

This area controls items such as the size of Windows event logs, access to these logs, how long we retain logs, and if they can be overwritten, or must be manually cleared. You can also have the computer automatically shut down if your security log fills.

We will be increasing all log sizes to ensure no entries are overwritten and all activity is available for forensic assessment if needed, as well as for troubleshooting purposes.

- Maximum application log size
  - 10240 kilobytes
- Maximum security log size
  - 20480 kilobytes
- Maximum system log size
  - 10240 kilobytes

We will be preventing any guest access to all our logs, which ensures only administrators can review or clear them. This helps prevent a hacker from covering their tracks.

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

Log retention is related to the retention method below. As we are not allowing the system to overwrite the log files we do not need to define these items.

- Retain application log
  - Not defined
- Retain security log
  - Not defined
- Retain system log
  - Not defined

We will be clearing our logs using scripts and utilities as previously outlined so we are setting these to prevent overwriting or stated another way, clear the logs manually.

- Retention method for application log
  - Do not overwrite events (clear log manually)
- Retention method for security log
  - Do not overwrite events (clear log manually)
- Retention method for system log
  - Do not overwrite events (clear log manually)

As above, should our large logs fill there will definitely be something going on that needs administrator intervention. We are setting this so our machine shuts down if our security log fills.

- Shut down the computer when the security audit log is full
  - Enabled

Restricted Groups

This area allows us to designate certain groups, which we want to prevent new users being added to without an explicit or administrative need to do so. You can also limit a user to a certain group, or control reverse membership IE: which groups the restricted group belongs to.
As we want to closely monitor who the members of these groups are we will be turning on these controls. We will however not be turning on the users group as it would significantly increase administration as this policy would have to be edited every time we added a new user to our domain.

- Administrators (will contain specific senior IT users)
  - OK
- Backup Operators (will contain no groups or users, defined to prevent addition of users or other groups)

        - OK
    - Guests
        - Not Defined
    - Power Users (will contain no groups or users, defined to prevent addition of users or other groups)
        - OK
    - Replicator (will contain no groups or users, defined to prevent addition of users or other groups)
        - OK
    - Users
        - Not Defined

System Services

This area allows us to ensure certain operating system services are either started or disabled. In some instances Windows will install the service and set it at Manual or Not Defined. Some of these services need to be disabled or they could create a security issue. A Manual setting means the service will start when needed, but will not run all the time. Automatic means the service usually starts on boot and runs constantly. Disabled means the service cannot start.

- Alerter — Defined - Manual
- Application Management — Defined - Manual
- ClipBook — Defined - Disabled
- COM+ Event System — Defined - Manual
- Computer Browser — Defined - Automatic
- DHCP Client — Defined – Automatic
- Distributed File System — Not Defined
- Distributed Link Tracking Client — Defined – Automatic
- Distributed Link Tracking Server — Defined - Manual
- Distributed Transaction Coordinator — Defined - Disabled
- DNS Client — Defined - Automatic
- Event Log — Defined - Automatic
- Fax Service — Defined - Disabled
- Indexing Service — Defined - Disabled
- Internet Connection Sharing — Defined - Disabled
- IPSEC Policy Agent — Defined - Automatic
- Logical Disk Manager — Defined - Automatic
- Logical Disk Manager Administrative Service — Not Defined
- Messenger — Defined - Automatic
- Net Logon — Defined - Manual
- NetMeeting Remote Desktop Sharing — Defined - Disabled
- Network Connections — Not defined
- Network DDE — Not defined
- Network DDE DSDM — Not defined
- NT LM Security Support Provider — Not defined
- Performance Logs and Alerts — Not defined
- Plug and Play — Defined - Disabled

- Print Spooler Defined - Disabled
- Protected Storage Defined - Automatic
- QoS RSVP Not defined
- Remote Access Auto Connection Manager Not defined
- Remote Access Connection Manager Not defined
- Remote Procedure Call (RPC) Defined - Automatic
- Remote Procedure Call (RPC) Locator Defined - Manual
- Remote Registry Service Not Defined
- Removable Storage Defined - Disabled
- Routing and Remote Access Defined - Disabled
- RunAs Service Defined - Disabled
- Security Accounts Manager Defined - Automatic
- Server Defined - Automatic
- Smart Card Not defined
- Smart Card Helper Not defined
- System Event Notification Defined - Automatic
- Task Scheduler Not defined
- TCP/IP NetBIOS Helper Service Defined - Disabled
- Telephony Defined - Disabled
- Telnet Defined - Disabled
- Uninterruptible Power Supply Not defined
- Utility Manager Not defined
- Windows Installer Not defined
- Windows Management Instrumentation Defined - Automatic
- Windows Management Instrumentation Driver Extensions Not defined
- Windows Time Defined - Automatic
- Workstation Defined - Automatic

Registry Settings

We will set the following registry keys using Group Policy:

- HKLM\System\CurrentControlSet\Services\Tcpip\Parameters and add the Value SynAttackProtect with a type of REG_DWORD and set the data to 2. This helps protect our machines from SYN Flood Attacks by timing out more quickly when the connection is left open and limiting some socket options.
- HKLM\Software\Policies\Microsoft\Windows NT\Printers\DisableWebPrinting we will set the Value to be 0x1. This disables web printing on your server. Deleting the virtual directory must be done as well. If this key does not exist this registry setting will create it.
- HKLM\System\CurrentControlSet\Services\lanmanserver\Parameters we will set the Value AutoShareServer with a type of REG_DWORD and set the data to 0. This helps protect our machines by removing the administrative shares.
- HKLM\System\CurrentControlSet\Control\FileSystem we will set the Value NtfsDisable8dot3NameCreation with a type of REG_DWORD and set the

data to 1. This change removes the undesirable backward compatibility to the old 8.3 file format.

Now on to the User area of the Default Domain Policy

User Configuration

Software Settings

This option controls automatic software installation, and is where you would place a new software package. The concept and functionality of the Remote Installation Server (RIS) and publishing applications is beyond the scope of this paper, except to say one can prevent users installing unauthorized software using it's functionality and manage who gets what applications.

Windows Settings

- Internet Explorer

This area controls the users Internet Explorer settings, including Browser User Interface, Connection settings, URL's, Security settings for zones, and Default Programs. Basically anything you may want to set in the Internet Explorers Options applet can be configured here. We will be leaving these set at their defaults.

- Scripts (logon/Logoff)

This setting controls the scripts we will run when users log on or off. We will have a script execute KINIT to initially log a user transparently into Kerberos in the domain. For the logout script we will run KDESTROY automatically to delete the Kerberos credential cache and prevent unauthorized reuse of a ticket.

- Security Settings

This area controls policies related to Public Key Policies and any enterprise trusts. We will be leaving these set at their defaults.

- Remote Installation Services

Client installation wizard settings can be controlled here. These are used in conjunction with Remote Installation Services and packages. We will be leaving these set at their defaults.

- Folder Redirection

These settings allow you to automatically redirect users folders to specific locations. You can control Application Data, Desktop, My Documents, My Pictures, and Start Menu items and storage locations. We will use this to map each users My Documents folder to their private share on the appropriate server.

Administrative Templates

These templates control a multitude of user settings. Due to the number of options we will be reviewing only some of the most useful and important items. Of the nine scripts which are available in Windows 2000 by default, only 4 of them are applicable in a new network, or an environment in which you are not doing migration from NT4. The scripts common.adm, Windows.adm, and Winnt.adm are all used for backwards compatibility with the systems policy editor in NT4. The scripts inetcorp.adm and inetset.adm are not used with Windows

2000. This leaves us with three templates to review and configure if we determine we need to. These are conf.adm, inetres.adm, and system.adm. For our default domain policy we will be using the system.adm template with the following alterations.

The first area is by far the largest, and deals with settings for Windows Components. Many of these items can be left at default, unless you want a very restrictive environment.

- Under the NetMeeting, Application Sharing, Audio & Video, and Option Page areas we will make no changes.
- Under the Internet Explorer area we will
  Enable the "Disable caching of Auto-Proxy scripts" option,
  Enable the " Disable changing Advanced page settings",
  Enable the " Disable Internet Connection wizard",
  Enable the " Disable changing connection settings,
  Disable changing proxy settings,
  Disable changing Automatic Configuration settings,
  Disable changing ratings settings,
  Disable changing certificate settings",
  Enable the " Do not allow AutoComplete to save passwords".

These settings will lock down IE so users cannot play with security related settings and most importantly that they do not save passwords in cookies on their machines. Users tend to use one password for their workstations and websites for ease of remembering, and if it is stored in clear text in a cookie a hacker could potentially extract it and then have access to our network.

- In the internet control panel options we will turn
  Disable the Security page,
  Disable the Connections page,
  Disable the Advanced page.

These settings will prevent users from messing around with security and connections such as trying to bypass a proxy server by changing the port.

- In the offline pages options we will make no changes.
- In the browser menu options we will make no changes.
- In the toolbars and Persistence behavior we will make no changes.
- In the Administrator Approved Controls area we will
  Disable Microsoft Chat, Microsoft Agent, Carpoint, Investor, and MSNBC.
- In the Windows Explorer area we will
  Disable the DFS tab and
  Set "No "Entire Network" in My Network Places" to on.
- In the Common Open File Dialog area we will make no changes.
- In the MMC area we will
  Restrict the user from entering author mode, but
  we will not define a list of explicitly permitted snap-ins.
- In the System Area – Group Policy

When considering the overall network security situation, one needs to consider changing the default refresh period for group policy which is set at 90 minutes, give or take 30 minutes of “randomization” for all computers except domain

controllers, which refresh every 5 minutes. This of course increases network traffic, and causes a reload of group policies, but if you make changes, have lots of power users like programmers who like to "play", reapplying your policies more often may be a valuable exercise. This is also valuable for high access or externally visible servers. We will change the default refresh time to 45 minutes

- All the remaining option will be set at their defaults.

This default domain policy will be applied to our entire network. All Organizational Units will inherit this policy unless we decide to apply a more restrictive policy, where we will use the block inheritance functionality. With this approach, and the nature of Group Policy we must ensure our more restrictive policies encompass everything in our default policy, unless there is a specific need to change anything. Based on this approach, all specialized Group Policy templates will be based on our Default Domain policy. The next policy we will define is our Domain Controller policy. We will start with the Default Domain Policy and alter it as needed to become our Domain Controller Policy. Following this approach we will only outline the changes we will make to the Default Domain Policy to define our Domain Controller Policy.

Domain Controller Policy (Default Domain Controller Policy)

Computer Configuration

Software

This will be left at the default

Windows

No changes in this area from our Default Domain Policy.

Security Settings – Account Policy

Password Policies

These policies apply domain wide, and as all logons and access to domain controllers will be done with domain accounts, we have set the Default Domain Policy quite restrictively so we will not change anything in this area.

Account Policies – Lockout

For the reasons noted above we will also not be changing anything in this area.

Account Policies – Kerberos Policy

No changes in this area.

Local Policies

Local Policies – Audit

We will be changing some of our logging, namely turning on more items to support closer monitoring of our domain controllers.

Audit Directory Service Access	Success, Failure
Audit Object Access	Success, Failure
Audit Privilege Use	Success, Failure

Local Policies – User Rights Assignment

For our Domain Controllers we need to define some further specific rights for certain groups as these machines contain some highly sensitive data.

Access this computer from the network	Administrators, Authenticated Users, Backup Operators, Power Users
Add Workstations to the Domain	Administrators, Server Operators
Create Permanent Shared Objects	Administrators
Enable Computer and user Accounts to be Trusted for Delegation	Administrators
Generate Security Audits	Administrators
Log on Locally	Administrators
Remove Computer from Docking Station	Administrators
Restore Files and Directories	Administrators, Backup Operators
Shut Down the System	Administrators
Synchronize Directory Service Data	Administrators

Local Policy – Security Options

Many of these options are important and need to be altered for our domain controllers. We must ensure the extra resources stored and services handled by a Domain Controller are as secure as possible We are forcing all communication with our DC's to be secure, signed, and encrypted.

- Digitally sign client communication (always)

-Enabled – Again, this setting helps us protect ourselves from man in the middle and session hijacking attacks. The SMB communication will be authenticated and signed at the packet level. If the related authentication fails so does communication.

- Digitally sign client communication (when possible)

-Enabled – Same as above

- Digitally sign server communication (always)

-Enabled – Same as above

- Secure channel: Digitally encrypt or sign secure channel data (always)

-Enabled – This extends the above protection for man in the middle and session hijacking attacks by adding encryption as well as forcing digitally signing the communication.

- Secure channel: Digitally encrypt secure channel data (when possible)

-Enabled

- Secure channel: Digitally sign secure channel data (when possible)

-Enabled

- Secure channel: Require strong (Windows 2000 or later) session key

-Enabled – We do not have anything less than Windows 2000 machines on our network so requiring this level of session key will work and add stronger security to sessions.

- Send unencrypted password to connect to third-party SMB servers

-Disabled - There is no reason we should have this type of server communication occurring on our network and to consider allowing any password to travel unencrypted is risky.

Local Policy – Event Log Settings
We will be applying the following settings to all domain controllers.
We will be increasing all log sizes to ensure no entries are overwritten and all activity is available for forensic assessment if needed, as well as for troubleshooting purposes.

- Maximum application log size
  - 20480 kilobytes
- Maximum security log size
  - 40960 kilobytes
- Maximum system log size
  - 20480 kilobytes

Restricted Groups
There will be no changes to this area.

System Services
This area allows us to ensure certain operating system services are either started or disabled. With our Domain Controllers some extra services need to be turned on automatically, or disabled. The Kerberos Key Distribution Center service is set to manual as this will run when needed on the DC which will be our KDC. We do not want this running on all DC's.

Alerter	Defined – Automatic
DHCP Client	Defined - Disabled
Distributed Transaction Coordinator	Defined - Automatic
Indexing Service	Defined - Manual
Kerberos Key Distribution Center	Defined – Manual
License Logging Service	Defined - Automatic
Net Logon	Defined - Automatic
NT LM Security Support Provider	Defined – Automatic
Remote Registry Service	Defined - Disabled
Uninterruptible Power Supply	Defined - Automatic

User Configuration
Software Settings
There will be no changes in this area
Windows Settings

- Internet Explorer

We will be leaving these set as they are in the Default Domain Policy.

- Scripts (logon/Logoff)

We will be leaving these set as they are in the Default Domain Policy.

- Security Settings

We will be leaving these set at their defaults.

- Remote Installation Services

We will be leaving these set as they are in the Default Domain Policy.

- Folder Redirection

We will be returning to their defaults as we do not want any personal drives automatically mapped when logged on to a domain controller. If necessary an administrator can manually map a needed drive, and then disconnect it when done.

Administrative Templates

- Under the NetMeeting, Application Sharing, Audio & Video, and Option Page areas we will make no changes.
- Under the Internet Explorer area we will
  Disable the "Disable caching of Auto-Proxy scripts" option,
  Disable the " Disable changing Advanced page settings",
  Disable the " Disable Internet Connection wizard",
  Disable the " Disable changing connection settings,
  Enable changing proxy settings,
  Enable changing Automatic Configuration settings,
  Enable changing ratings settings,
  Enable changing certificate settings",
  Enable the " Do not allow AutoComplete to save passwords".
- In the internet control panel options we will turn on
  Enable the Security page,
  Enable the Connections page,
  Enable the Advanced page.
- In the offline pages options we will make no changes.
- In the browser menu options we will make no changes.
- In the toolbars and Persistence behavior we will make no changes.
- In the Administrator Approved Controls area we will make no changes
- In the Windows Explorer area we will
  Enable the DFS tab and
  set "No "Entire Network" in My Network Places" to off.
- In the Common Open File Dialog area we will make no changes.
- In the MMC area we will
  not Restrict the user from entering author mode, but
  we will not define a list of explicitly permitted snap-ins.
- In the System Area – Group Policy
  We will be returning this to the default of no changes. By default Domain Controllers refresh Group Policy every 5 minutes
- All the remaining option will be set at their initial defaults.

Web server OU Security Policy

The following security policy will be applied to the IIS Child OU in the DMZ site to secure our externally facing IIS servers as well as our front end exchange server. As these servers are stand alone we need to make some changes.

Software

This will be left at the default

Windows
No changes in this area from our Default Domain Policy.

Security Settings – Account Policy

Account Policies – Password
All settings will remain the same except Minimum Password Length. We will set this to 12 Characters. As IIS uses a local account (IUSR_Machinename) for access this setting will force the extra password length, and the standalone nature of these machines allows us to alter this.

Account Policies – Lockout
We will be shortening the Account Lockout Threshold to 2 Attempts and the Reset Account Lockout Counter after setting to 180 Minutes. This will minimize the number of attempts a hacker can try before lockout, and extend the period before the counter resets to 3 hours.

Account Policies – Kerberos Policy
We will be disabling the user logon restrictions item as we do not need to enforce Kerberos on these standalone machines. We will handle any communication between servers, which should all be of an internal nature by using the settings in Security Options.

Local Policies

Local Policies – Audit

Audit Directory Service Access	Success, Failure
Audit Object Access	Success, Failure
Audit Process Tracking	Success, Failure
Audit Privilege use	Success, Failure

Local Policy – User Rights Assignment

Access this computer from the network	Administrators, renamed IUSR_MachineName account, Backup Operators
Create Permanent Shared Objects	Administrators
Enable Computer and user Accounts to be Trusted for Delegation	Administrators
Generate Security Audits	Administrators
Log on Locally	Administrators
Remove Computer from Docking Station	Administrators
Synchronize Directory Service Data	Administrators
Shut down the system	Administrators

Local Policy – Security Options

- Allowed to eject removable NTFS media

-Administrators

- Amount of idle time required before disconnecting session

-15 minutes

- Automatically log off users when logon time expires (local)

-Enabled

As communication to this OU will occur from external sources and internal users, we cannot force machines to use digital signing, but when the option exists (with inside users) we want to use it. On the server side, we want to force this as the

only servers communicating with these IIS and the Exchange 2000 Front End machine should be internal servers which will be capable of establishing these sessions. We also want to ensure when possible certificates are used once available.

- Digitally sign client communication (always)

-Disabled

- Digitally sign client communication (when possible)

-Enabled – Again, this setting helps us protect ourselves from man in the middle and session hijacking attacks. The SMB communication will be authenticated and signed at the packet level. If the related authentication fails so does communication.

- Digitally sign server communication (always)

-Disabled

- Secure channel: Digitally encrypt or sign secure channel data (always)

-Disabled

- Secure channel: Digitally encrypt secure channel data (when possible)

-Enabled – as above

- Secure channel: Digitally sign secure channel data (when possible)

-Enabled – as above

- Secure channel: Require strong (Windows 2000 or later) session key

-Enabled – We do not have anything less than Windows 2000 machines on our network so requiring this level of session key will work and add stronger security to sessions.

- Secure channel: Require strong (Windows 2000 or later) session key

-Disabled

- Send unencrypted password to connect to third-party SMB servers

-Disabled

- Strengthen default permissions of global system objects (e.g. Symbolic Links)

-Enabled

- Unsigned non-driver installation behavior
  -Do not allow installation

Local Policy – Event Log Settings

We want to increase our log sizes on the web servers and externally facing machines as they are the most likely to be attacked.

- Maximum application log size
  - 20480 kilobytes
- Maximum security log size
  - 40960 kilobytes
- Maximum system log size
  - 20480 kilobytes

Restricted Groups

No changes

System Services

Again, we need to enable or disable certain services due to the specific server's roles. Web servers do not need all the internal based items like Alerter, DHCP Client, Messenger, and task scheduler enabled, they also do not need to have server running as there should be no Named Pipe or RPC traffic for these machines. With remote registry service disabled a hacker will not be able to connect to the registry on these machines, nor can you install any program which must write to the registry with this disabled.

- Alerter — Defined - Disabled
- DHCP Client — Defined - Disabled
- DNS Client — Defined – Disabled
- IIS Admin Service — Defined - Automatic
- Messenger — Defined - Disabled
- Network Connections — Not defined
- NT LM Security Support Provider — Not defined
- Remote Access Auto Connection Manager — Defined - Disabled
- Remote Access Connection Manager — Not defined
- Remote Registry Service — Defined - Disabled
- Server — Defined - Disabled
- Task Scheduler — Defined - Disabled
- Uninterruptible Power Supply — Defined - Automatic
- Workstation — Defined - Automatic
- World Wide Web Service — Defined - Automatic

User Configuration and Administrative Templates

All settings will be the same as our default domain policy except we will be altering the Group Policy setting in the System Area. We will be setting the Group Policy refresh interval to 15 minutes.

Network OU Security Policy

The following security policy will be applied to the Network Child OU in the internal domain to secure our Network File servers and the critical data stores.

Software

This will be left at the default

Windows

No changes in this area from our Default Domain Policy.

Security Settings – Account Policy

Account Policies – Password

No changes in this area from our Default Domain Policy.

Account Policies – Lockout

No changes in this area from our Default Domain Policy.

Account Policies – Kerberos Policy

No changes in this area from our Default Domain Policy.

Local Policies

Local Policies – Audit

Audit Directory Service Access	Success, Failure
Audit Object Access	Success, Failure
Audit Process Tracking	Success, Failure

Local Policy – User Rights Assignment

Due to the extensive list in this category we will only outline those items we will be changing,

Access this computer from the network	Administrators, Authenticated Users, Backup Operators, Power Users
Add Workstations to the Domain	Administrators, Server Operators
Create Permanent Shared Objects	Administrators
Enable Computer and user Accounts to be Trusted for Delegation	Administrators
Generate Security Audits	Administrators
Log on Locally	Administrators, Server Operators
Remove Computer from Docking Station	Administrators
Shut down system	Administrators, Server Operators
Synchronize Directory Service Data	Administrators

Local Policy – Security Options

With these servers users will be connecting to their shares and other information so we need to define some other settings to manage this.

- Allowed to eject removable NTFS media

-Administrators

- Amount of idle time required before disconnecting session

-15 minutes

- Automatically log off users when logon time expires (local)

-Enabled

We will be enforcing all of these options for our network servers to ensure we have the most secure network communication to our servers possible.

- Digitally sign client communication (always)

-Enabled – Again, this setting helps us protect ourselves from man in the middle and session hijacking attacks. The SMB communication will be authenticated and signed at the packet level. If the related authentication fails so does communication.

- Digitally sign client communication (when possible)

-Enabled

- Digitally sign server communication (always)

-Enabled

- Digitally sign server communication (when possible)

-Enabled

- Secure channel: Digitally encrypt or sign secure channel data (always)

-Enabled

- Secure channel: Digitally encrypt secure channel data (when possible)

-Enabled

- Secure channel: Digitally sign secure channel data (when possible)

-Enabled

- Secure channel: Require strong (Windows 2000 or later) session key

-Enabled – We do not have anything less than Windows 2000 machines on our network so requiring this level of session key will work and add stronger security to sessions.

- Send unencrypted password to connect to third-party SMB servers

-Disabled - Again, there is no reason we should have this type of server communication occurring on our network and to consider allowing any password to travel unencrypted is risky.

- Strengthen default permissions of global system objects (e.g. Symbolic Links)

-Enabled

- Unsigned non-driver installation behavior

-Do not allow installation

Local Policy – Event Log Settings

- Maximum application log size
  - 20480 kilobytes
- Maximum security log size
  - 40960 kilobytes
- Maximum system log size
  - 20480 kilobytes

Restricted Groups

No Changes

System Services

Alerter	Defined – Automatic
DHCP Client	Defined – Disabled
Distributed Link Tracking Server	Defined - Automatic
Distributed Transaction Coordinator	Not defined
Indexing Service	Defined - Automatic
Print Spooler	Defined – Automatic
Remote Registry Service	Defined - Disabled
Removable Storage	Defined - Disabled
Task Scheduler	Defined - Automatic
Uninterruptible Power Supply	Defined – Automatic

User Configuration and Administrative Templates

All settings will be the same as our default domain policy except we will be altering the Group Policy setting in the System Area. We will be setting the Group Policy refresh period to 30 minutes.

We will be applying our Group Policies in the following way;

- We will be applying the Default Domain Policy to the entire domain and any sites.

- We will be blocking inheritance to our IIS Child OU in the DMZ and applying the Web Server Security Policy
- We will be blocking inheritance to our SQL Child OU in the DMZ and applying the Network Security Policy
- We will be blocking inheritance to our Primary network DC Child OU and applying the Domain Controller Policy
- We will be blocking inheritance to our Primary network Server Child OU and applying the Network Security Policy
- We will be blocking inheritance to our DC Child OU in the production site and applying the Domain Controller Policy
- We will be blocking inheritance to our Server Child OU in the production site and applying the Network Security Policy

To apply the above Default Domain Group Policies perform the following steps for each policy:

1) Open Active Directory, Users and Computers
2) Right Click on the Domain Controllers OU
3) Choose Properties
4) On the Group Policy Tab, click new
5) Type in the name you want to call this policy
6) Right click the policy name you chose above
7) Click edit
8) Expand the "Windows Settings" item
9) Right click Security settings
10) Select Import Policy
11) In the from dialog box navigate to the policy file (something.inf) you want to import
12) Double click the file to import it
13) Close group policy
14) Click close again
15) For the Domain Controller Policy force replication amongst your Domain Controllers, then reboot each DC, one at a time.
16) Review your event log to verify the policy was downloaded properly

To apply the above Specialized Group Policies perform the following steps for each policy:

1) Open Active Directory, Users and Computers
2) Right Click on the appropriate OU
3) Choose Properties
4) On the Group Policy Tab, click new
5) Type in the name you want to call this policy
6) Right click the policy name you chose above, choose block inheritance
7) Then click edit
8) Expand the "Windows Settings" item
9) Right click Security settings

10) Select Import Policy
11) In the from dialog box navigate to the policy file (something.inf) you want to import
12) Double click the file to import it
13) Close group policy
14) Click close again
15) For all other policies, force replication amongst your Domain controllers
16) Move each server into it's appropriate OU
17) Force the server to download the group policy using the secedit command
    At the command prompt C:\secedit /refreshpolicy machine_policy/
18) Review your event log to verify the policy was downloaded properly
19) Reboot each server, verify it restarts properly and the policy is applied.

NOTE: Occasionally some services will start before the group policy is applied the first time. To remedy this potential issue, reboot all servers a second time

All users and their computers will be placed in the appropriate Organizational Unit based on the department they work for. User accounts will be placed in the Global Group specific to the department and role within that department that the user is fulfilling. These global groups will then be placed in the Local groups on the departmental File and Print server specific to the users department.

Conclusion

Throughout this paper we have discussed various extra security implementations we felt would be necessary for securing this domain. Although we were limited in our ability to extrapolate on these items, what we did cover allows the idea of our comprehensive approach to defense in depth and least privilege to be understood.

Routers, Switches, Remote Access Devices, and firewalls are present in the majority of networks, which is why we addressed them. We chose to deal with these items within our paper to demonstrate the interrelationship of these devices and tools to the overall security of a network, and how they should be implemented to mitigate potential risks. We also discussed the implementation of Groups, a foundation on which one builds the "least privilege" access controls. Many other aspects of overall security from a Defense in Depth approach also could not be covered, however items such as a comprehensive backup strategy, disaster recovery, Intrusion Detection, and business resumption planning should not be discounted or forgotten. We also included in our network several items which we were unable to discuss as they have their own specialized implementations and could easily generate a full paper on their own. These items included Routing and Remote Access Servers (RRAS), Internet Authentication Servers (IAS), Certificate Servers, and Active Directory implemented firewall and router configurations.

One must remember, the best planned and designed network and Active Directory will need to be adjusted in one way or another after implementation. If one is lucky enough to be able to run a parallel network many of the bugs can be

ironed out with little user inconvenience, and the ability to roll back the last change is valuable. You also enjoy this flexibility when you are implementing a completely new network.

Unfortunately the reality of corporate life often does not allow us the luxury of extra high-end hardware for new domain controllers and other needed hardware. In these instances we need to plan a staggered approach to implementation, such as taking a server offline, rebuilding it to Windows 2000, and repeating this until enough are rebuilt and are stable enough to finally upgrade our NT4 PDC to an active Directory domain controller and progress from there.

No matter which way you look at it designing a Windows 2000 Active Directory network is not a simple task, daunting would be a more apt term. However with the appropriate planning, understanding what your network and users need to do, how the company's security policy applies to users, machines, and the network in general will get you well on your way to accomplishing this task. The most important thing to remember is designing an Active Directory network is not a mutually exclusive exercise, everything must be considered and accounted for in your planning, and then in your implementation. To exclude anything means the potential for significantly negative consequences, including security vulnerabilities, user aggravation, or network downtime.

Bibliography

1) Schein, Phillip G., Exam Cram, Windows 2000 Security Design Coriolis Group, 2000

2) Simmons, Kim, Buse, Jarret W., Halpin, Todd B., Exam Cram, Windows 2000 Network Design, Coriolis Group, 2000

3) King, Robert, Govanus, Gary, MCSE Windows 2000 Directory Services Design Study Guide, Sybex Inc, 2000

4) Rice, David C., Group Policy Reference, Systems and Network Attack Center (SNAC), National Security Agency, Version 1.0.8, March 2, 2001, Report #C4-053R-00

5) Stephens, Capt. Robin G., Guide to Securing Microsoft Windows 2000 DNS, Network Security Evaluations and Tools Division of the Systems and Network Attack Center (SNAC), National Security Agency, Version 1.0, April 9, 2001, Report #C4-050R-00

6) Walker IV, William E., Guide to the Secure Configuration and Administration of Microsoft IIS 5.0, Network Applications Team of the Systems and Network Attack Center (SNAC), National Security Agency, Version 1.1.4, June 19, 2001, Report #C4-057R-00

7) Pitsenbarger, Trent, Guide to the Secure Configuration and Administration of Microsoft ISA Server 2000, Network Applications Team of the Systems and Network Attack Center (SNAC), National Security Agency, Version 1.0.1, March 15, 2001, Report #C4-013R-01

8) SANS GIAC Security Essentials Course, Day 5 Hour 3, Windows 2000 Security, Hour 5, Windows Auditing, Hour 6, IIS Security

9) Microsoft Windows 2000 Resource Kit, Microsoft Press. http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp

10) Packet Storm Software, http://packetstormsecurity.org/NT/NTOtools2.zip

11) Anonymous; Maximum Security, Third Edition, SAMS Publishing, 2001

12) Microsoft's Secure IIS5 Checklist, http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/tips/iis5chk.asp

13) Microsoft From Blueprint to Fortress: A Guide to Securing IIS 5.0 http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/deploy/depovg/securiis.asp

14) Microsoft Prescriptive Guidance, Security Operations Guide for Windows 2000 Server, Microsoft Corporation, 2002

15) Haney, Julie M., Guide to Securing Microsoft Windows 2000 Group Policy, Network Security Evaluations and Tools Division of the Systems and Network Attack Center (SNAC), National Security Agency, Version 1.1, September 13, 2001, Report # C4-007R-01

Last Updated: July 28th, 2017

Upcoming Training

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