Global Information Assurance Certification Paper

SANS GIAC Certification

GCWN Practical v3.1

Date: 8 September 2002
Student: Jamie French

Option 1: Design a Secure Windows 2000 Infrastructure
Title: Employing the powers of Active Directory and Group Policy

Introduction

There are two goals set for this document. One is to design a secure Windows 2000 infrastructure primarily focusing on Group Policy. The second is to meet the Global Information Assurance Certification (GIAC), Certified Windows Security Administrator (GCWN) practical requirements for version 3.1, option 1.

This document is written from the perspective of a mid-sized fictitious company named GIAC Enterprises. Not unlike most real small to mid-sized businesses, budgets are limited, therefore I strove to come up with a plan that is conservative on budget, is geared primarily towards bridging the usability vs. security gap, and should not require on-the-fly design changes of significant proportions. Should changes need to be made, I have designed in compatibility for these changes without the requirement to re-design things from the ground up, and in areas where there may be need to apply change, I have tried to identify this for the reader so they are aware of it. It is my hope that this document will be useful to someone planning on designing a Secure Windows 2000 Infrastructure, as well as meeting the GCWN assignment 3.1 practical requirements.

Description of GIAC Enterprises

Mission Statement:

- Provide superior service and product offerings to the widget marketplace
- Maintain the highest of standards in support of our GIAC widget brand offerings
- Recognize and promote development of emerging markets where widgets may find new uses
- Enhance and offer customer education on the safe use of widgets
- Provide a strong and stable return on investment for GIAC Enterprises private share holders and employees
- Conduct widget research and development in order to stay ahead of competitor product life cycles

Organizational Business Units:

GIAC Enterprises (GIAC) is a midsize company employing 76 skilled professionals. The company's organizational chart breaks down into business units as displayed in the table below. Personnel are divided into the following business units:

Business Unit	# of Staff
Executive	3
Finance/HR	5
Sales HQ	34
Sales Branch	15

R&D	9
Marketing	7
InfoTech (IT)	3

Additionally, each business unit has one manager that belongs to an additional business unit comprised of the executives and managers.

Business Unit	# of Staff
Management	9

Operational Flow:

GIAC derives the majority of its revenue from patent royalties paid by other players in the widget industry. Business partners manufacture widgets on behalf of GIAC using our proprietary manufacturing designs. These widgets form GIAC's product line offerings. Sales consist primarily of bulk, repeat orders directly supported by sales staff through traditional sales practices (telephone) but also through e-commerce (approximately 30% of sales). GIAC widgets are in high demand as components in the manufacturing industry, requiring a less aggressive sales staff. Marketing is closely tied with both Sales and R&D. New sales result primarily through the success of the Marketing Business unit.

Management meets frequently to share information from their prospective Business units and maintain focus on the company's current and future goals.

New Needs Identified:

GIAC's core IT needs have not paralleled with offerings in the IT industry. Simple, mid-range workstations are required for day-to-day business applications throughout the entire Enterprise. As such the diversity of systems and applications present have not changed much. There are very few special circumstances for IT to consider. The redesign of infrastructure is intended mainly to enhance security and bring the network inline with the companies security policy, while additionally simplifying network manageability and performance.

- Recently, GIAC identified the need to place much higher emphasis on securing their IT infrastructure. The compromise of an internal system resulting in the harassment of management has occurred. The compromise took place at corporate Headquarters (HQ) by a disgruntled ex-employee of the Sales HQ Business unit. The current infrastructure consists of Windows9x hosts authenticating with NT4 domain controllers in two domains. While the full extent of damage caused by this incident cannot be ascertained due to the lack of evidence available, management has deemed it a priority to secure the business infrastructure to mitigate the possibility of far more serious security infraction possibilities in the future that might challenge the ongoing success of GIAC.
- GIAC opened up a sales office in the North East to meet demand and reduce the costs of conducting long-range business just 8 months ago. This Sales Branch is currently managed remotely. Management has expressed concern that some of the staff from this

branch (hereafter referred to as a site) may not be completely loyal to GIAC and more strict protocols need to be put in place to limit their access to GIAC HQ's computing resources.

- GIAC is expanding! While expansion is not fast, industrial sectors in the mid-west have expressed demand for GIAC widgets and expense forecasts predict that it would be more economically viable to open up a sales site in this area. Future plans include opening up another sales site in this region within one year.
- GIAC Management, excluding the Finance/HR manager, wish to enable remote access so that they can work from remote locations should the need arise. This has become an issue due to the fact that personnel are occasionally absent (sick, vacation, weekend etc.) and would like to accomplish a few tasks while at home. Sounds crazy but all management staff of GIAC are all shareholders of this privately held company and are truly interested in the best interests of GIAC's success.

Network Design and Diagram

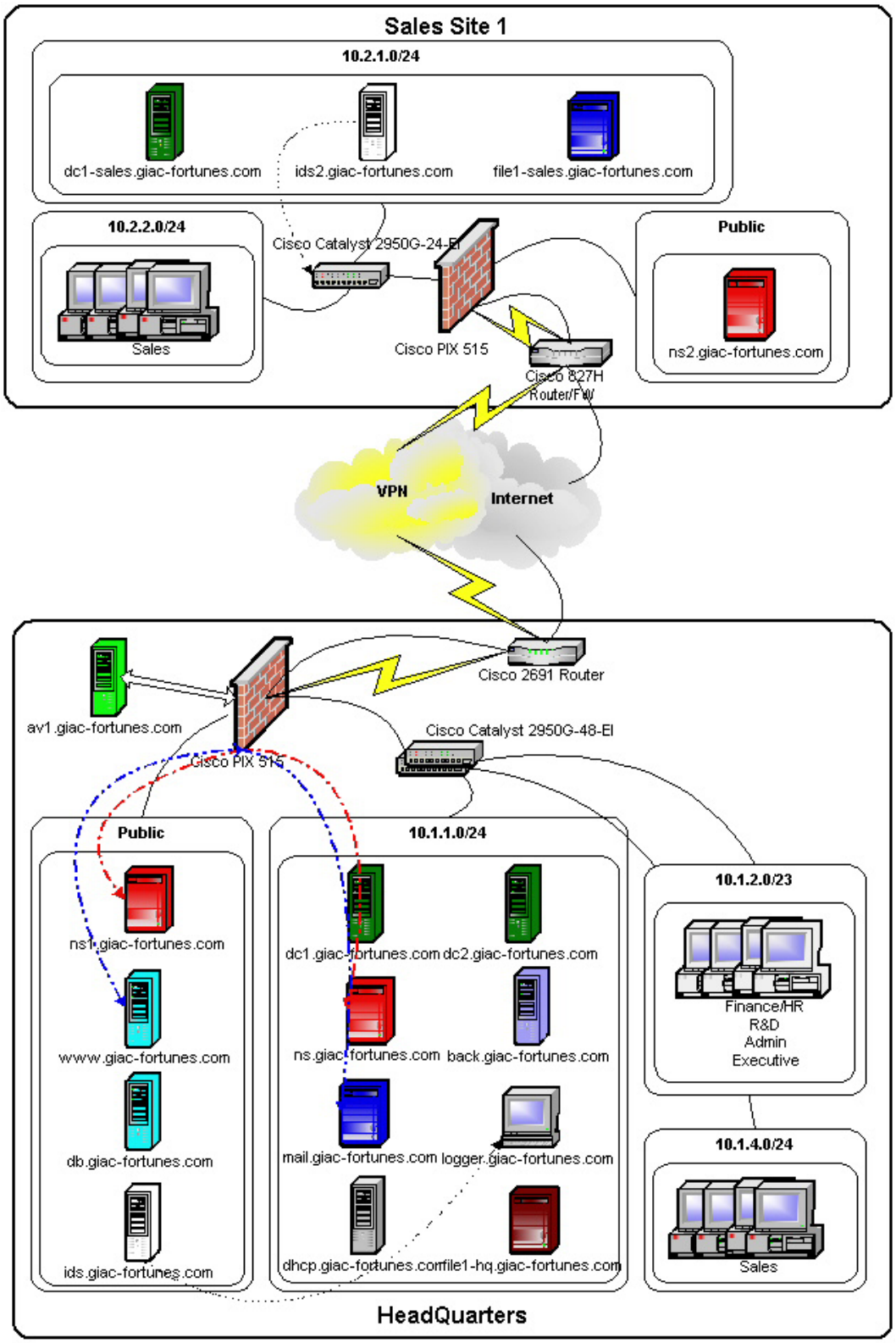


figure 1.1

Network Overview:

GIAC has a FastEthernet backbone at HQ and the Sales Site. Currently, neither site is switched, but both are firewalled effectively. Both sites will be switched using Cisco catalyst switches with the implementation of this proposed network design (figure above). Other challenges include Intersite Replication between HQ and the Sales site over a WAN link. GIAC manages all of its own computing infrastructure including publicly available services in-house. This presents, and will continue to present, quite a challenge for the three full-time IT staff. We are using NAT for our private internal addresses (RFC 1918) and implementing the VPN tunnel at the firewall. More detail will be provided in succeeding sections on the physical network configuration.

GIAC DMZ's:

Border Routers:	
HQ	Cisco 2691 Router
Sales	Cisco 827H ADSL Router/FW
Firewalls:	
HQ	Cisco PIX 515 3 Legs – Internet, DMZ, Internal FastEth Stateful, VPN Logging to syslog (Windows 2000* Logger running Kiwi SyslogGen2.0.1[1])
Sales	Cisco PIX 515 Same as HQ above
Switches:	
HQ	Cisco Catalyst 2950G-48-EI x 2
Sales	Cisco Catalyst 2950G-24-EI
Antivirus SMTP/FTP/HTTP Gateway:	
HQ	Windows 2000 Server* Interscan Viruswall**

Intrusion Detection:	
HQ	Windows2000 Workstation* Snort 1.8.7/MYSQL Output**
E-Commerce Backend DB:	
HQ	Windows 2000 Server* Oracle 9i**
Web/Mail Relay Server:	
HQ	Windows 2000 Server* IIS 5** HTP370 Raid (0+1) configured stripped and mirrored[2]
External DNS Servers:	
HQ	Windows 2000 Server*
Sales	Windows 2000 Server*

*all OS' are planned to be running the most current patch levels (IAW SecPol)
**all applications are planned to be running the most current patch levels (IAW SecPol)

Border Routers/Firewalls:

Public services offered in the DMZ's are segmented by PIX 515 firewalls respectively at both corporate locations. We are also employing NAT at both locations. Additionally the PIX's also implement the IPSec tunnels between both sites, tunneling our private. The PIX's are beefier machines with faster CPU's, have VPN accelerators, and are suited better to implement the VPN than our routers. The IPSec features of the Cisco routers will provide a redundancy backup should the FW implemented VPN fail. We are using ESP with 3DES

WEB/Mail Relay:
GIAC's one public IIS 5 server is intended to manage its entire web serving needs as well as handle any front-end e-commerce. It is located in the HQ DMZ. Transaction rates on the e-commerce site average about 75 per day. Average page views per day range about 2200. IIS also runs SMTP to proxy email for GIAC. A DNS alias has been created for the mail relay. The server is running on a dual Pentium III 933 box with a HPT 370 RAID interface configured in RAID modes 0+1 with 4 IDE drives of the same size. The IIS web services also support SSL connections for secure order processing. Servers in the DMZ are not part of the GIAC domain. More on this later.

E-Commerce Server:
Located in the HQ DMZ, this server is running Oracle9i on Windows 2000. Dynamic web pages submit orders to the database (DB) for processing. The DB handles the transaction, takes order information, updates inventory levels, and generates reports for the Marketing, Sales, and Finance staff. Payments are still invoiced via snail mail as orders are generally in large sums for large orders of 10,000 plus widgets with previously established clients. The DB is run on a separate system to enhance security and separate any client credentials from the web server. This adds another layer of security should the IIS server be compromised. It also enhances performance. The Oracle9i server is not publicly accessible (firewalled and local Group Policy).

Antivirus SMTP/FTP/HTTP Gateway:
An important piece in the security puzzle, this server will connect directly with the HQ PIX firewall and scan bi-directional traffic for malicious content. The intent is to protect GIAC's ingress/egress points from viruses, trojans, worms, mobile code, malicious active X and JavaScript etc. With this product in place, all SMTP/FTP/HTTP traffic will be scanned from HQ. The Sales site won't receive the exact same protection due to the fact that they are configured to access HTTP and FTP directly from their site, however, email enterprise wide will be protected.

External DNS:
These servers handle DNS resolution for GIAC's publicly available IP addresses. The primary DNS is located at HQ and the secondary DNS is located at the Sales Site. External DNS servers for each physical location process recursive resolutions for Internal DNS servers. This is the main security advantage to having an external server at each site. Having an external DNS server at each location also lowers bandwidth consumption from internal hosts. The Sales site, in this configuration, does not have to pipe across the Internet to reach an organizational DNS server. The other advantage is that should the HQ DNS server go down, persons trying to resolve external domain names will still be capable of doing so via the Sales sites external DNS server and vice versa.

Intrusion Detection Systems:
It took management a while to come around to the idea of capturing an audit trail based upon network packet signature matching, but they finally warmed up to the idea and we have approval to deploy Network Intrusion Detection Systems (NIDS). The system is running on older hardware with Windows 2000 workstation with dual NICS, one sniffing, unbound NIC and one out-of-band command and control NIC located on the internal network. The CAT5 cable

plugged into the DMZ has had the TX wires snipped. We are running Snort 1.8.7 in the HQ DMZ with the MYSQL output plug-in. Logs are forwarded to an internal Windows 2000 workstation (logger) running Kiwi Syslog Daemon Pro 7.0.2. Logs are then processed and written into a MYSQL 3.23.52 database installed on the loghost. More on the loghost later.

GIAC Internal:

Internal DNS/DHCP Server:	
HQ	Windows 2000 Server*
Domain Controllers:	
HQ	Windows 2000 Server* HTP370 Raid (0+1) configured stripped and mirrored
HQ	Windows 2000 Server* HTP370 Raid (0+1) configured stripped and mirrored
Sales	Windows 2000 Server* HTP370 Raid (0+1) configured stripped and mirrored DNS
Backup:	
HQ	Windows 2000* Veritas Backup Exec**
File Server:	
HQ	Windows 2000 Server*
Sales	Windows 2000 Server*

Mail Server:	
HQ	Windows 2000 Server* Exchange Server 2000**
Logger:	
HQ	Windows 2000* IIS 5** OfficeScan Server** Kiwi Syslog Daemon 7.0.2** MYSQL 3.23.52**
Intrusion Detection:	
HQ	Windows 2000 Workstation* Snort 1.8.7/MYSQL Output**
Sales	Windows 2000 Workstation* Snort 1.8.7/MYSQL Output**

*all OS' are planned to be running the most current patch levels (IAW SecPol)
**all applications are planned to be running the most current patch levels (IAW SecPol)

DNS/DHCP Server:
This dual-purpose box manages internal IP resolutions and forwards lookups for GIAC HQ. It has been configured to be authoritative for GIAC's internal IP's only. Requests for external resolutions are forwarded to the external DNS servers. Inbound requests from the Internet for our private addresses should never reach GIAC and if they do, ingress filtering will drop them at the internal FW leg. Ingress filtering between the DMZ network and internal network greatly limits the traffic allowed to pass (stateful, TCP 53 dropped etc.). Still further, requests from the DMZ DNS servers are rejected. GIAC DNS zones are integrated into AD unlike external servers. As such we are using multi-master replication to update DNS records between DC's. The internal DNS server also runs DHCP services, assigning address leases for select internal workstations.

Domain Controllers:

These are the blood and guts of GIAC's Windows 2000 secure infrastructure. Collectively they hold the Active Directory DB (ntds.dit), manage replication of the Global Catalogue (GC), hold the SAM database with user accounts and passwords, and without them, things would fall apart quickly. The following Flexible Single Master Operations (FSMO) are also running on DC1; GC, Schema Master (SM), and Domain Naming Master (DNM). HQ DC2 is running Relative Identifier (RID), PDC Emulator, and Infrastructure Master. The Sales site DC1-sales is running GC. Additionally, the Sales site is running internal DNS and DHCP services. It is configured in the same manner as the internal DNS and DHCP server for HQ. This is an important service for the Sales site. Without it, a DNS request might have to traverse the VPN tunnel 4 times (if the primary external DNS were down) before it would reach a GIAC external DNS server. This extra overhead is avoided by having a DNS server on-site. This also allows the site to continue with networked business relying on domain names should HQ's link be offline. All servers, including the DC's are physically secured and locked up in access-controlled rooms, with appropriate environmental controls. More on physical security later.

Logger:
PIX, router, event, and IDS logs are written to this box, which picks them up and writes them into a MYSQL DB. The logs are queried briefly on a daily basis to look for anomalous log events. Logging devices have been configured and tuned to reduce the number of false positives and monitor only events that directly affect GIAC computing resources (Group Policy audit policies help here). Should an incident (whether it's a misconfiguration or a security issue) occur in the future, we will be prepared to deal with it, having some evidence and valuable clues as to what happened so that we can take some reactive and corrective actions to mitigate the risk of repeat incidents. The logger is actually running a NIDS too, covering the server subnet in HQ. Generally we should only be seeing IPSec (Server IP Security Policy through Group Policy – covered later) traffic here so log events occurring will pose great interest.

Backup Server:
The backup server is located in HQ and is running Veritas Backup Exec. This server handles and backs up the Oracle databases from the DMZ host, in addition to files on the file server. In order to receive backups from Windows 2000 servers, accelerator agents will be installed. A little more on backup policy will be presented towards the end of the paper. It is important to note that both sites have scheduled backups to occur on different dates, during silent hours. The WAN link between the Sales site and HQ should be able to handle this load. This isn't the preferred configuration but finite monetary resources limit us. All backups are encrypted by the backup agent software and further encrypted when piped over the Internet through the VPN tunnel.

File Servers:
HQ and the Sales site both have file servers. These actually operate as print servers too. Both servers are operating with HPT370 controllers and 4 drives in RAID mode 0+1 with 120GB of storage available. Drives are cheap and data is priceless. The system hardware (i.e. motherboards with the built in controllers) was also quite cheap. They suit the needs of GIAC and have been functioning without event for over a year prior to this infrastructure upgrade. Separate volumes have been created on each site server so that permissions can be more finely managed (defense-in-depth).

Mail Server:
GIAC plans on using Exchange Server 2000 with SP3 to handle our corporate email needs. This server employs IMS to handle email forwarded to and from the SMTP proxy running in the DMZ. All users, including Sales site users must go through this email server to send and receive email, having access to TCP ports 25, 110, and 143 blocked by the sites Firewalls inbound and outbound.

Intrusion Detection Systems:
Similarly with the DMZ NIDS, both the HQ and Sales site NIDS are forwarding their logs to the loghost (logger). See DMZ description above for more information.

Active Directory (AD) Design and Diagram

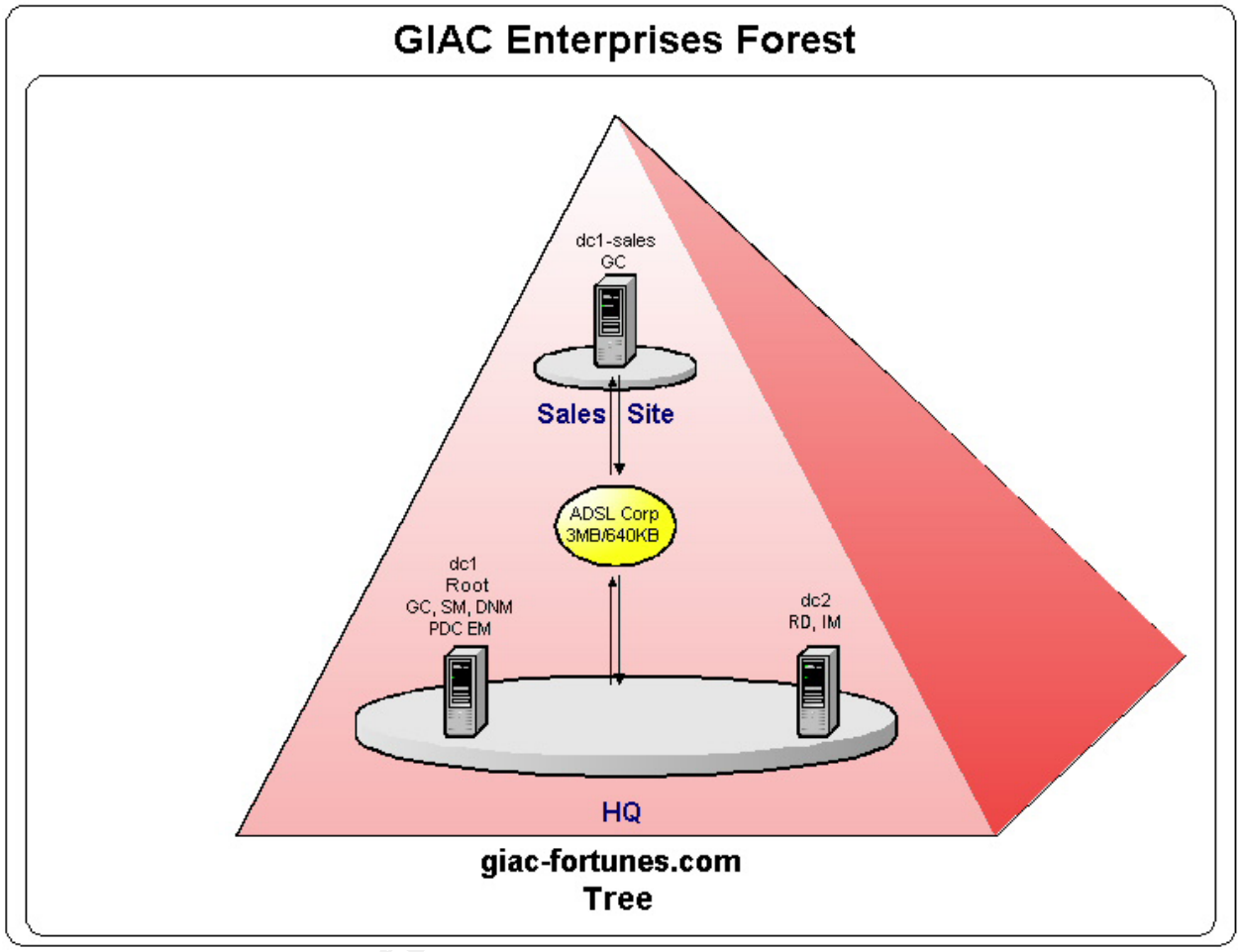


figure 1.2

Intro:

GIAC currently only has one remote site physically separate from HQ requiring a WAN link. The sales site has a slower corporate ADSL connection to the Internet (640K/3MB). AD Intersite Replication (Global Catalogue) will take place via RPC-over-IP transports over secure channel and further embedded in VPN tunnels implemented at the border routers.

Forest:

GIAC only requires one forest at this time. Some consideration was given into dividing up GIAC into more than one forest. We considered creating a forest for HQ the Sales site and yet another forest for the DMZ hosts. This however would bring the manageability of the infrastructure out of the scope deemed reasonably effective for three administrators and would also have required more capital expenditures for extra equipment. The threat vs. risk vs. cost assessment dictates that GIAC implement one forest in which resources are uniformly named

across the enterprise. A multi-domain set-up to cope with the possible shortcomings of our WAN connectivity were considered. Given the costs of maintaining and creating multiple domains (administrative, equipment), it was decided that should bandwidth become an issue, GIAC would return its leased ADSL router and upgrade services.

Trees:

The concept of having AD mirror DNS is fantastic. There are numerous naming standards in Windows 2000. When we are talking about trees, we are talking about DNS names and how resources are found using the well-known DNS naming conventions we are familiar with (i.e. www.giac-fortunes.com). This is referred to in Windows 2000 as a Domain Naming Context. The DNS root of GIAC's only tree is giac-fortunes.com. GIAC only requires one tree, as we should be able to handle all of our business with one domain name (giac-fortunes.com). The main purpose of trees is to reflect the DNS structure of an organization and provide a name mapping method for reaching sought resources. The Sales site uses the same domain name and thus is part of the same tree. Using this tree structure we can easily accommodate future organizational changes between the Sales site (and/or future sites) within the tree. If GIAC were concerned about the site being spun-off into a separate business (domain name change) then we would have pursued the concepts and possibilities of using separate trees in the forest or logically creating sites as new forests and then as new trees within these forests. This simply isn't practical given our scenario. A big benefit of having one tree also is that we can maintain one AD, schema, have one domain to administer. This in turn helps us effectively create and manage Group Policy successfully across the whole tree. If we were concerned about replication traffic, we would have given further consideration into making the Sales site a branch of the giac-fortunes tree.

Domains:

There is currently only one domain planned for GIAC. This domain spans two geographically separate sites, HQ and Sales. The concept of naming a domain that follows the DNS names of the organization was a welcome change from the NT domain model and was readily adopted by GIAC. It makes sense from a logical and administrative perspective to mirror the two. A drawback to naming the domain inline with the DNS naming scheme is that an attacker would be able to easily guess our internal naming scheme in AD. If they were able to access AD to make changes based upon this information however, it would likely be too little to late anyway. giac-fortunes.com has a dedicated T1 connecting to the Internet from HQ and a corporate ADSL 3Mbps/640Kbps connection from the Sales site. This is deemed to be a wide enough pipe to handle the current network load[3]. GIAC sales orders are not time critical and can be processed in batches, within a few days of the order being received. Should there be an outage above and beyond this period, Sites can manually relay business information via FAX or telephone. Taking into consideration that there are only fifteen staff members in this location we are planning on doubling up services on some servers. This isn't the optimal solution for security! Again, it comes down to the finite resources allotted. We have compromised and met the business requirements of GIAC (with management signing off on it).

We believe the domain design chosen is simplistic and will allow for the management of resources adequately through the use of a common schema, configuration, global catalogue

replication, group policy, and services may be accessed within the forest, up and down the tree, within the domain.

Sites:

As previously noted, GIAC has two sites and a strong business case to expect more sites in the future. GIAC has decided to employ RPC-over-IP transports for Intersite Replication. The Sales site contains its own Domain Controller with Global Catalogue services. This will greatly reduce the amount of inter-site traffic. Additionally, many Internet based services are available directly from each site, further reducing the amount of inter-site traffic (such as HTTP and DNS). Certain types of replication traffic (backup/sysvol) can be scheduled during low bandwidth time periods. Traffic is replicated over secure channel, through an IPSec VPN implemented at the border routers using 3DES and ESP. We currently do not have a redundant, higher cost link to ensure internal network connectivity via the VPN remains established should the lower cost link go down. We will revisit this topic in the near future however it is anticipated that the best management will budget for is dial-up or hopefully ADSL corporate (1.5MB/640KB) user connections (roughly $105/month for both) at each site.

Organizational Units (OU's):

Previously, OU's have been touched upon. Management required that some OU's be created to implement security measures as well to provide functionality deemed essential. Management understands division of authority concepts and appears to have employed them well through their initial design requirements. Group Policy and the level of granularity upon which controls may be implemented sold management on this infrastructure upgrade to Windows 2000 and has given GIAC piece of mind knowing that the dollars spent will pay off in dividends for quite some time.

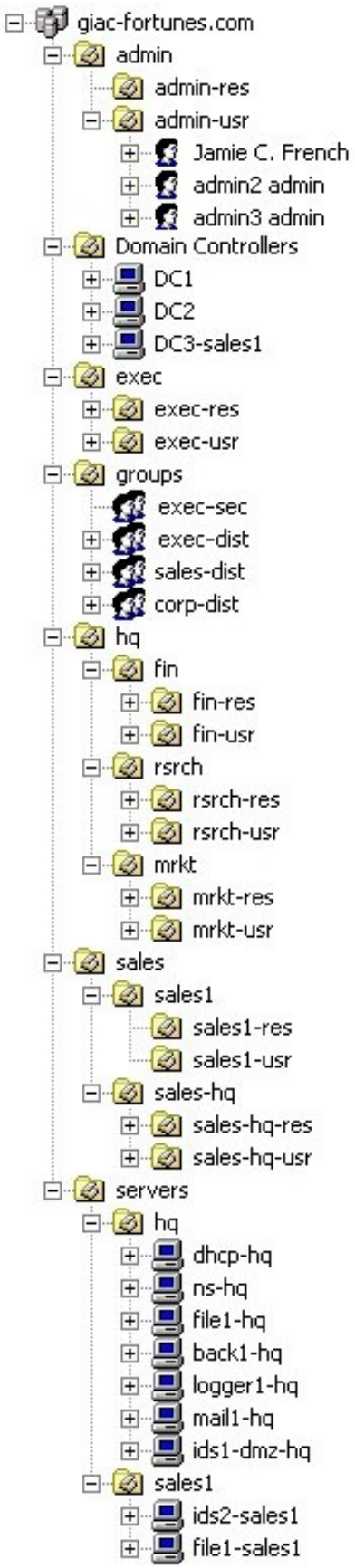
admin:

We have three administrators employed in the organization. Administrators are special users and as such have special requirements necessary to perform their job functions. It is important that we grant rights and privilege carefully when it comes to administrative tasks. This can be done effectively if we apply customized Group Policy to administrators and therefore we have placed them into a separate OU. If we need to add or modify administrative rights, we should not be confused and know exactly where to apply them using this orphan OU. The admin OU contains nested admin-res and admin-usr OU's.

Domain Controllers:

This default OU is slated for use. Domain Controllers are critical pieces of GIAC's IT infrastructure. Each DC is analogous to the King in a chess game; these resources require very fine oversight and strictly controlled access. If GIAC were to loose a DC to the dark side, we would have one heck of a mess to clean up (replication, access to ntds.dit etc.). It might be considered so critical that GIAC as a business would fold. As such we have prescribed DC's as belonging to their own OU for strict control. There are three domain controllers slated for GIAC. All will be running in Native Mode. We previously discussed some of the specifics relating to DC's.

exec:



Similar in needs to the admin OU, executives are grouped together into their own OU so that special Group Policy may be applied (allowing more rights and privilege). The ratio of executives to GIAC employees is relatively small. Coupled with their unique needs we have decided to place the decision makers into their own OU where these needs can be more tightly managed. The exec OU contains nested exec-res and exec-usr OU's. Business unit managers are also objects nested within this OU.

groups:

GIAC has a requirement for numerous groups. Distribution groups have been created for use with Exchange 2000. We are more concerned with security global groups and security local groups though. We have separated assets thus far in two distinct ways, 1) to aid in dividing privilege and access using a least privilege mentality, and 2) to mirror the corporate structure of GIAC as closely as we can to help us deploy departmental policy through Group Policy and security templates. We can further use security groups to ease administration in certain scenarios, while maintaining a high level of control.

We have the following groups in our AD design, within the groups OU:

1. Corporate distribution universal group (corp-dist)
2. Managers distribution universal group (exec-dist)
3. Managers security global group (exec-sec)
4. Sales distribution universal group (sales-dist)

Should we add another domain at some point, we might require universal groups, so it makes sense to create them at the beginning rather than global groups. This way we can add global groups to the universal groups and effectively distribute rights and privilege. Now, we'll skip right to the managers security global group. This group will allow us to grant more privilege to managers where necessary. Each business unit has a manager, therefore representation and someone with permissions to get specialized tasks done should be present within normal working schedules and rotations. One important issue has not been addressed by management and still awaits resolution. Like most organizations, there is a backup for primary position holders. This is true for GIAC as well. Each manager has a second in command (2IC) that requires a subset of the permissions the manager has. Management cannot decide upon a policy for the distribution of tasks to 2IC's. As such we will grant rights and privilege individually for these users within the OU structure for which they belong. Similarly,

we will delegate privilege where necessary for managers over AD objects in the respective OU's they manage.

hq:

This OU has numerous nested OU's. This OU contains the bulk of GIAC Business units; Finance, Marketing, and Research & Development. Within these nested OU's we have res and usr OU's respectively. Fairly generic policy will be applied to these OU's, relying mainly on default domain group policy. The Finance and Human Resources (HR) section of the company is small, employing five persons. At this point one might ask "why is GIAC designing their OU's like this? It doesn't seem efficient when one could just lump all users into an orphan users OU.". The answer is, if the organization grows we will have a design that is easily understood (both by veteran admins and newcomers alike). Major reorganization of the AD should not be required when we do expand. Thus we consider the concept of an OU with only a few resources in it now as a good idea. The fin OU contains two nested OU's; fin-res and fin-usr, which contain resources and users respectively. Marketing and R&D are separate too. Again, this helps mirror our internal business structure, making it easy for administrators to track down users and resources respective to their sections. They are within their own OU's so that Group Policy may be applied separately as required.

sales:

Previously, we identified that GIAC has two sites. Staff from both of these sites belongs to the sales OU. The design of this OU is meant to group together all sales related resources and users, while logically dividing these objects by physical locations. This is in part due to the fact that we want to keep a closer eye on Sales staff, as they tend to have a much higher turnaround with the company than other positions. Nested under sales is the sales-hq and sales1 OU's. Nested under these are sales resources (sales-hq-res, sales1-res) and users (sales-hq-usr, sales1-usr) respective to their locations. By keeping the Sales business unit under a similarly named OU, we are able to implement AD permissions and use inheritance in an efficient manner to compliment our organizational security policy through Group Policy.

servers:

This OU is designated for internal GIAC servers. Similar in scope to the default Computers OU, servers have been placed into their own OU for logically grouping and managing these assets, separate from workstation computers.

GIAC is taking a least privilege approach to security. This means that we are locking things down tightly and then granting rights and privilege where necessary. As such, exceptions to average access requirements will generally include special users or resources that require access to specific resources above and beyond the average. This method of assigning rights and privileges needs to be taken into consideration whenever design changes or additions are proposed. Using this concept, we will generally separate users that have special access requirements from those that do not. This means our Organizational Units will also logically mirror a similar approach, with servers, administrators, corporate executives, and managers all being separated into OU's or groups where we know specifically that objects inside have special requirements.

GIAC has created a base OU structure modeled closely to the organizational business unit structure. This aids in making administration easier and more efficient. A "keep it simple" approach was taken that allows for easy modification as GIAC expands. Logical groupings by department were created to support departmental policies (applied through Group Policy). Departmental OU's have nested OU's that separate users from other resources. Critical servers are maintained and administered through this OU.

Group Policy and Security

Probably the focal point of a Windows 2000 infrastructure from GIAC's perspective is Group Policy and its implementation through Group Policy Objects (GPO). The power of GPO's in managing resources and users is phenomenal. This feature weighed the heaviest in management's decision to implement a Windows 2000 infrastructure. Being able to administer the enterprise, securely and efficiently, through the fine-tuning of GPO's is key in our secure Windows 2000 design.

There are far too many configurable settings to discuss them all. We will be focusing on settings that will be changed from defaults and provide some reasoning for these changes. We will not be covering settings where the default is deemed to be acceptable. An example would be the Default Domain Kerberos Policy. We agree with Microsoft and the NSA that the default policy defined here is appropriate for our needs[4].

We will be using default policy as well as creating our own policies in this section. Security templates can be used, modified, and saved. When we're happy with our changes, we can import the templates into our new or default Group Policy. We can accomplish some versioning here and roll back changes to Group Policies should we make a mistake. Page 136 of the track 5.1 courseware describes this in more detail[5].

Default Domain Policy

GIAC is implementing one domain. The default domain policy will be applied to every object in the domain. As such we will not be fine tuning security within this policy but rather defining a baseline policy.

Password Policy:

The SANS consensus of the Twenty Most Critical Internet Security Vulnerabilities[6] places "accounts with no or weak passwords" as the second most common vulnerability applicable to all systems. GIAC Enterprises has developed a password policy that helps address this vulnerability. This policy will be applied across the Enterprise, through the default domain policy.

Password Policy	
\Root\Default Domain Policy\Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy	
References: http://www.labmice.net/Windows2000/Administration/password.htm[7] http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q147706&[8] http://support.microsoft.com/default.aspx?scid=kb;en-us;Q161990	
Enforce password history	3
We will keep track of the three previous passwords. When changing passwords, the new password may not match any of the 3 previously used.	
Maximum password age	60
Passwords may not remain the same for more than 60 days. If a password has not been changed within 60 days, the account will be locked and the user will have to send a request through their manager to a	

GIAC administrator or delegated password maintainer to reset their password. 60 days seems like a long time. Reasoning is that we don't want users to have to change their password too often, which will basically make them angry and more users will just start writing down their passwords in the usual places. We feel that 60 days gives the users a chance to maintain some stability with their passwords thereby remembering them, and should the password hashes fall into the wrong hands, will still provide only a limited window in which to break the secure channel encryption and then perform their brute force cracking. It would be much easier for a malicious user to circumvent password authentication using social engineering – which is discussed in the additional security section.

Minimum password age	3

We will not allow users to change passwords for 3 days after choosing a new password. This forces users to actually use new passwords and not to simply rotate through 3 passwords quickly to bypass password history policy.

Minimum password length	8

There are a lot of articles on the various methods employed by Microsoft to hash passwords, to compute the cracking speeds of various hardware platforms, and advice on the minimum length a password should be. This policy requirement is a little deceptive because the strength of password length really needs to be measured with consideration for the password authentication mechanism. An 8 character LanMan password hash is not equal to an 8 character NTLMv2 hash. Both passwords are eight characters long, but vary so drastically in terms of security that we feel it important to mention we will be modifying additional policy to require NTLMv2 authentication. For example, a 7 character LanMan hash (hashes are broken into 7 characters) which is limited to lowercase characters has a maximum of approx 587 billion (7^48 char) possibilities. An NTLMv2 password 8 characters long has approx 7.2 zillion (8^96) possibilities. We will be configuring Domain Controllers to only accept NTLMv2 authentication. Additionally, we will require passwords to be a minimum of 8 characters in length.

Passwords must meet complexity requirements	Enabled

According to Microsoft, enabling password complexity requires passwords to have the following attributes:

" 1. Passwords must be at least six (6) characters long.
2. Passwords must contain characters from at least three (3) of the following four (4) classes English upper case letters· English lower case letters· Westernized Arabic numerals· Non-alphanumeric ("special characters") such as punctuation symbols
3. Passwords may not contain your user name or any part of your full name"[9]

Methods of modifying these complexity rules was documented for NT4, however in Windows 2000 they appear to be implemented in the operating system security components and modification method documentation is sparse. We will therefore use the default complexity rules as they meet GIAC's Security Policy complexity requirements.

Account Lockout Policy:

Policy set here will dictate what happens to an account when login authentication credentials supplied via the Netlogon channel (over secure channel) do not match those in AD for the resource being authenticated.

There have been issues reported with lockout policy thresholds being exceeded too quickly, usually related to the number of login attempts recorded as multiple authentication mechanisms try to present credentials to a DC[10].

Account Lockout Policy
\Root\Default Domain Policy\Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy
References:

http://www.microsoft.com/windows2000/en/server/help/sag_rras-ch1_74.htm[11]

Account lockout duration	20 minutes
We are locking accounts for 20 minutes if the lockout criteria is met.	
Account lockout threshold	4 invalid logon attempts
We have set the invalid logon attempt value to 4. This value (4) is the criteria that must be met before an account will be locked out.	
Reset account lockout count after	20 minutes
After 20 minutes we will reset the counter. Thus if a user attempted to logon 3 times within 20 minutes and had failed on each attempt, after 20 minutes from the first attempt, the number of failed logons would be reset to zero.	

Auditing:

Audit trails are great for troubleshooting and detecting malicious activity. There are trade-offs however, and these are; disk space usage, network bandwidth usage, and the use of administrative staff time. GIAC tries to leverage the usefulness of audit trails while quantifying their use in realistic measures.

With this in mind, the following default audit settings have been configured for GIAC.

Audit Policy

\Root\Default Domain Controllers Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy
References:
http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=9633[12]

Audit account logon events	Failure
We want to see failed logon attempts authenticating with the Domain Controllers. We are not concerned with successful logons at the default domain policy level. Other GPO's will aid further in protect GIAC from malicious logon's using valid user accounts and credentials. Audit trails from other sources will provide clues to unauthorized successful logons.	
Audit account management	Success/Failure
We wish to track all events such as password changes. This should not generate large volumes of logs.	
Audit logon events	Success/Failure
We want to enable full logging for this event. Domain logon was previously covered. With this enabled we will capture any logons to servers such as the domain controllers.	
Audit object access	Failure
We will be using ACL's to manage objects. Auditing of successful events would generate logs above an acceptable level. We are interested in seeing failures denied by ACL's though.	
Audit policy change	Success/Failure
Well, we are definitely interested in any policy changes. This is a definite audit option we want full coverage of.	
Audit privilege use	Failure
By tracking failed attempts administrators can more closely identify where access to resources might be required. On the flip side we will also identify when illegitimate attempts to access objects fail.	
Audit system events	Success
We are interested in knowing when systems are restarted or event logs have been cleared. This audit trail will help administrators track down systems that are performing these types of actions outside of expected hours as well as identify when malicious activity is occurring on systems (such as the event log being cleared by someone other than one of the three administrators).	

User Rights Assignment:

Properly configuring user rights is an important part of our Enterprises security. If we don't adequately assign rights, access to critical files and functions may be obtained which could cause security infractions or even bring down the network!

User Rights Assignment	
\Root\Default Domain Policy\Computer Configuration\Windows Settings\Local Policies\User Rights Assignment	
References: http://www.microsoft.com/windows2000/techinfo/reskit/en/ProRK/prdd_sec_gqko.htm[13] http://support.microsoft.com/default.aspx?scid=KB;EN-US;q257346&[14] http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/acl_special_permissions.htm[15] http://www.microsoft.com/windows2000/en/datacenter/help/default.asp?url=/windows2000/en/datacenter/help/sag_SEconceptsUnPrivs.htm http://www.winnetmag.com/Articles/Index.cfm?ArticleID=20079[16]	
Access this computer from the network	Administrators, Authenticated users
We've decided that only members of Administrators and Authenticated users should be able to access any computers from the network. (we'll be disabling the Guest Group too)	
Add workstations to domain	Enterprise Admins
We don't want anyone adding workstations to the domain except one of the three full time admin users. We could easily have made this Domain Admins but it is possible that we might add administrative users or Domain Admins at branch sites in the future. This way, we won't forget and GIAC's policy will be enforced. Any new Admins will have to gain approval first and one of the two Enterprise Admins will have to add workstations.	
Back up files and directories	Administrators, Backup Operators
By allowing members of these two groups to backup files and directories, we are essentially allowing them the following rights (which grant privilege) over all file systems; "Traverse Folder/Execute File, List Folder/Read Data, Read Attributes, Read Extended Attributes, and Read Permissions"[17]. These are some pretty serious rights. Administrators will be required to fulfill the tasks related to backing up and restoring data for each respective site. We will also grant access to the Backup Operators built-in group. Users added to this group for their respective OU's can then manage their own backups as required. This may be assigned in the future to persons in pseudo administrative roles or to business unit managers.	
Change the system time	Administrators
There should be no need for users to modify the system time. Workstation systems will be running Window 2000 Professional or Windows XP Professional. Enterprise time synchronization takes place with the root DC, synchronizing off of its clock, which is kept in time by using net time from 3, stratum 3 time servers on the Internet (connection ACL's managed at the FW). As such, we only allow administrators to monkey with system time settings. We don't want audit logs to be out of sequence, nor do we want to mess up time sensitive authentication mechanisms such as Kerberos.	
Force shutdown from a remote system	Domain Admins
There are not to many reasons why we would want to allow employees of GIAC to remotely shutdown computers. As such, we will only grant the Domain Admins group the rights to perform this task.	
Logon Locally	Administrators
We have limited access to logon locally to any computer in the giac-fortunes.com domain to administrators. We will allow for users in various OU"s specific access to logon locally where required outside of the default domain policy.	
Manage auditing and security log	Administrators
No one except for administrators should have rights to clear audit trails. The fewer hands in the pie, the more solid a court case is likely to be. Chain of custody for the log files is critical. Unfortunately, this means that only administrators have rights to enable object access auditing. If we allow more groups to manage the security log, we lose the benefits of a tightly controlled auditing system. We have our hands	

tied on this one.	
Shut down the system	Administrators, Authenticated users
We've allowed administrators and authenticated users to shutdown systems. This setting applies to systems where a user is locally logged onto the domain. If they have physical access, its game over from a security standpoint so we may as well allow authenticated users this right. Many users do shutdown their workstations in the evenings, why not let them do it gracefully vice holding in their power buttons for 6 seconds or pulling power cordes ;-)	

Security Options:

Important settings are configurable through the Security Options portion of Group Policy. We will apply many settings across the entire domain through the default domain policy, generally focused on increasing security.

Security Options

\Root\Default Domain Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options	
References: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/588.asp[18] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/589.asp[19]	
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Simply put, unless the resource explicitly allows anonymous access, we are denying anonymous access.	
Amount of idle time required before disconnecting session	15 minutes
I recall issues with SAMBA file handles locking and having to release sessions manually. Makes sense that for Windows 2000 users, we don't want to maintain stale sessions. We mitigate the possibilities of session hijacking, poor user security practices (walking away from a machine during lunch) etc if we disconnect idle sessions after a set period of time. If the shared resource is required again, the user can simply log back in.	
Audit use of Backup and Restore privilege	Enabled
We want to know if backups are completed and if there has been any unauthorized activity related to the privileges granted to backup operators or administrators.	
Disable CTRL+ALT+DEL requirement for logon	Disabled
We want users to follow this key sequence to logon because this key sequence is difficult for trojanized logon capture programs to escape.	
Do not display the last user name in logon screen	Enabled
We will not display the user name of the last person logged in within the logon dialogue box. This forces an unauthorized person trying to physically logon to the network to guess the user names as well as the passwords, buying time through defense-in-depth processes.	
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM
We touched upon this previously in the password policy section. This is a very important setting. We are refusing to authenticate LM hashed passwords. All DC's in the GIAC domain are configured to only accept NTLMv2. All workstations and servers are configured to use NLTMv2.	
Message text for users attempting to log on	*see following
Logon message for users is as follows: "You are attempting to Logon to GIAC Enterprises computing resources. Unauthorized access is strictly prohibited. All sessions are logged and monitored."	
Message title for users attempting to log on	Attention - 注意- Atención - Aufmerksamkeit - Atenção
We are more concerned about unauthorized users and as such figure it would be prudent to list at least the title in a few languages. Historically, we have noted higher than average hacking attempts from persons who's primary language is not English. We're nice enough to at least display the title in multiple	

languages.	
Prompt user to change password before expiration	8 days
We give users a window of time in which to change their passwords. This helps lower the amount of password administration required for valid users. 8 days prior to expiration, users will begin receiving prompts to change their password. This range of days extends over a week, ensuring that users who are going away on holidays for a a business week will receive the message prior to their passwords expiring.	
Rename administrator account	mazakala
We have renamed the administrator account from the default. This removes this account as an attack vector using the well-known name, making brute force logon attempts much harder against the administrative account.	
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
The default for secure channel is to encrypt data when possible. By explicitly enabling this in the default domain policy, we will override any NT4, Local, or Site policy that specifies otherwise. Not entirely necessary but a fallback for the domain in case there are any misconfigurations elsewhere.	
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Similar to the above setting. The default is enabled. A little overhead is required but secure channel will then be authenticated and its payload integrity verified.	
Secure channel: Require strong (Windows 2000 or later) session key	Enabled
All GIAC assets are located within North America and are not subject to US encryption export controls. Domain controllers have been deployed with the strong encryption pack, allowing strong encryption keys. Further, all assets within the prescribed Windows 2000 design will be running Windows 2000 or newer operating systems from Microsoft. For internal sessions, 40bit is probably acceptable but why not use 128bit if it is available!	

Event Logs:

We'll be assigning a default event log policy for the domain. Basically, unless otherwise stipulated, every system will log up to 10MB for each of the 3 event logs and rotate them weekly. Critical boxes will be forwarding event logs to a central loghost. Further, critical boxes will also have their event logs backed up.

Event Logs	
\Root\Default Domain Policy\Computer Configuration\Windows Settings\Security Settings\Event Log\Settings for Event Logs	
References:	
Maximum application log size	10240 kilobytes
We will allow 10MB of data in the application log on all computers on the domain. The minimum hard drive size in GIAC workstations is 20GB. There is plenty of room for an application log this size. Keep in mind we are forwarding sensitive server logs to a central logging facility. Keeping logs at this size should not adversely affect system performance. If it does, we can tune down this size.	
Maximum security log size	10240 kilobytes
Same as maximum application log size above.	
Maximum system log size	10240 kilobytes
Same as maximum application log size above.	
Restrict guest access to application log	Enabled
We are disabling the Guest Group. This is a fallback just in case of a misconfiguration where the Guest Group is re-enabled at some point.	
Restrict guest access to security log	Enabled
Same as restrict guest access to application log above.	
Restrict guest access to system log	Enabled

Same as restrict guest access to application log above.	
Retain application log	7 days
We will retain logs for 7 days, after which older days will be overwritten. We are backing up files from critical servers and select workstations on a schedule, which will retain a duplicate of the logs that should match those on the central logging host (logger.giac-fortunes.com). If there are events on regular workstations, we'll have to get to them before the 7 day timeframe or before they reach 10MB in size.	
Retain security log	7 days
See retain application log above.	
Retain system log	7 days
See retain application log above.	
Retention method for application log	By days
See retain application log above.	
Retention method for security log	By days
See retain application log above.	
Retention method for system log	By days
See retain application log above.	
Shut down the computer when the security audit log is full	Disabled
We don't want systems to shutdown via the default domain policy when audit logs are full. It is unlikely that one of the administrators would not have noticed this event prior to it happening.	

Restricted Groups:

While we enjoy having guests drop by our offices, they have no business working on our computing resources. We will be restricting the guest group from accessing any resources on the GIAC domain.

Restricted Groups
\Root\Default Domain Policy\Computer Configuration\Windows Settings\Security Settings\Restricted Groups
References:
Guests
We have added the guest group. We will create a specific group for guests if we have any, assigning appropriate access and permissions at the time the user is added.

System Services:

Some services just should not be running unless you absolutely need them. By lowering the number of services running, you will cut down on possible attack vectors. The following services have been configured to increase security.

System Services	
\Root\Default Domain Policy\Computer Configuration\Windows Settings\Security Settings\System Services	
References: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=8383[20]	
Fax Service	Disabled
We are not running a fax service over the network. Old-fashioned faxes are used when necessary.	
FTP Publishing Service	Disabled
FTP services should be turned off on all hosts except where specifically enabled. We will know of and keep track of all FTP servers.	
IIS Admin Service	Disabled
We definitely do not want to run IIS services or the admin service unless we explicitly allow it. By	

disabling this service, we need not worry about domain systems sparking up a vulnerable web server or other unauthorized IIS services.	
Internet Connection Sharing	Disabled
We are not using Internet Connection Sharing. This is disabled. All connections to the Internet are centrally managed.	
NetMeeting Remote Desktop Sharing	Disabled
We are not running NetMeeting and have no need for this service.	
NT LM Security Support Provider	Disabled
Backwards support for NT4 is not necessary. All hosts in the GIAC domain are Windows 2000 or above.	
Simple Mail Transport Protocol (SMTP)	Disabled
Same as FTP. We don't want anyone starting an SMTP service unless explicitly allowed.	
SNMP Service	Disabled
We are not using SNMP to monitor systems. This can be disabled without adverse effect.	
SNMP Trap Service	Disabled
Same as SNMP Service.	
TCP/IP NetBIOS Helper Service	Disabled
GIAC is not running NetBIOS over TCP/IP. We are a Windows 2000 native domain and do not require NetBIOS. All communications required will use port 445.	
Telephony	Disabled
GIAC doesn't support telephony applications. We do not require this service.	
Telnet	Disabled
We do not require telnet for remote administration. This insecure protocol has been deemed as decommissioned by GIAC.	
Trivial FTP Daemon	Disabled
Why allow people to upload files to your systems without any authentication, or conversely download files. Bad idea. We don't want systems to run TFTP.	
Windows Time	Enabled
Time synchronization is important, especially in a Kerberos environment. We want consistent time on all of our computing assets. Logs will be sequential and ordered and Kerberos will work, allowing users to authenticate and gain access to the resources they need to work.	
World Wide Web Publishing Service	Disabled
Same as FTP. We don't want WWW services running unless we explicitly allow them.	

IP Security Policies on Local Machine:

Microsoft has implemented great functionality and powerful security policy may be implemented through IP Security Policies. We'll be employing some of this functionality on the default domain as well as other Group Policies.

IP Security Policies on Local Machine	
\Root\Default Domain Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\IP Security Policies on Active Directory	
References: http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp[21] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/robi/ro060500.asp[22]	
Server (Request Security)	Yes
The default policy will be implemented. ESP confidentiality via 3DES, integrity via SHA1, authenticating via Kerberos v5. This will force all servers to attempt communications with clients using IPSec for interoperability with all business units within GIAC. We will revisit implementing IPSec between all hosts after a trial with sensitive users (separate policy specified for the exec and hq OU's) to see if there are	

any performance issues.

Internet Explorer:

Domain wide, we have some Internet Explorer options that should be set. These are the following:

Internet Explorer	
\Root\Default Domain Policy\User Configuration\Administrative Templates\Windows Components\Internet Explorer	
References: Microsoft Windows 2000 Policy Explanation - Included in Windows	
Disable changing proxy settings	Enabled
GIAC Enterprises users do not currently have any reason to use external proxies. As such we will restrict users from configuring proxies for unauthorized purposes.	
Disable AutoComplete for forms	Enabled
This feature is often used for the combination of storing username and password for web-based authentication in the registry. For the protection of users, this has been disabled.	
Do not allow AutoComplete to save passwords	Enabled
see Disable AutoComplete for forms above.	

Group Policy:

We will replicate Group Policy for users at a desired interval. This will keep Global Catalogue updated and user specific policy fairly fresh.

Group Policy	
\Root\Default Domain Policy\User Configuration\Administrative Templates\System\Group Policy	
References: Microsoft Windows 2000 Policy Explanation - Included in Windows	
Group Policy refresh interval for users	Enabled
This has been set to 60 minutes with a 30 minute random variance. If we make a change via group policy, it should replicate out to users within 1.5 hours maximum without requiring a logoff/logon.	

Default Domain Controller Policy

As previously stated, domain controllers are the heart of a secure Windows 2000 design. We want to closely manage these servers and protect Active Directory and all assets managed through AD.

Some further reading on securing DC's is available from Microsoft at http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q216899&.

DC Audit Policy:

Variations from the default domain policy are necessary where the default policy is not appropriate for specific resources (grouped into different OU's). We have tightened certain policies up on domain controllers, starting with a more refined audit policy specific to DC's. We

can afford to turn on some of the logging features when they only apply to a few hosts, whereas enabling them for the whole domain would simply generate too many events.

Audit Policy	
\Root\Default Domain Controllers Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy References: http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=9633	
Audit account logon events	Success/Failure
We want to see all logon attempts authenticating with domain controllers. This will alert us to all access attempts and will also serve to help as an aid in troubleshooting.	
Audit directory service access	Success
We want this enabled on DC's. We can more finely configure which AD objects should be monitored and keep a log of what changed and when. Useful from a security perspective as well as an administrative one.	
Audit logon events	Success/Failure
We want to enable full logging for this event. Domain logon was previously covered. With this enabled we will capture any logons to DC's both locally and over the network. This is an important audit feature to be enabled on the DC's. All logon activity should be audited to alert us to unauthorized access. Also, should a change be made in error by an admin, we can check the times and user to know who is buying the next round of coffee after the problem is fixed (supported further by other audit policy).	
Audit object access	Success/Failure
We will be using ACL's to manage objects. Auditing of successful and failure events on DC's is a good idea for tracking object access as defined for each object. We will be monitoring things such as the registry keys and files.	
Audit policy change	Success/Failure
Well, we are definitely interested in any policy changes. This is a definite audit option we want full coverage of.	
Audit process tracking	Success/Failure
We are certainly interested in processes running on the DC's. Start and stop times for services and processes should be recorded.	
Audit system events	Success/Failure
Similar to the default domain policy. Additionally, we want to know when audit failures occur (like failure to clear an audit log).	

DC Event Logs:

Basically, we are enabling larger log files on the DC's because we've enabled more verbose logging and we don't want to lose logs prior to backup times should something be happening and nobody has noticed.

Event Logs	
\Root\Default Domain Controllers Policy\Computer Configuration\Windows Settings\Security Settings\Event Log\Settings for Event Logs	
References:	
Maximum application log size	204800 kilobytes
We will allow 200MB of data in the application log on DC's. We have 80GB of disk space total in a stripped and mirrored configuration. We can certainly handle keeping 200MB of data in the logs on DC's. Keep in mind we are forwarding sensitive server logs to a central logging facility. If system performance is impacted by keeping logs this size, we can tune down this size.	
Maximum security log size	204800 kilobytes
Same as maximum application log size above.	
Maximum system log size	204800 kilobytes

Same as maximum application log size above.

DC User Rights Assignment:

There are a few differences between the default domain policy and what we will support for DC's. We are restricting rights to administrators only, removing other groups.

User Rights Assignment	
\Root\Default Domain Controllers Policy\Computer Configuration\Windows Settings\Local Policies\User Rights Assignment	
References: http://www.microsoft.com/windows2000/techinfo/reskit/en/ProRK/prdd_sec_gqko.htm http://support.microsoft.com/default.aspx?scid=KB;EN-US;q257346&	
Access this computer from the network	Administrators
Administrators should be the only ones logging onto domain controllers over the network. As such, members of the Administrators Group are given this right.	
Back up files and directories	Administrators
By removing backup operators we are isolating the following rights (which grant privilege) over all file systems; Traverse Folder/Execute File, List Folder/Read Data, Read Attributes, Read Extended Attributes, and Read Permissions specifically to administrators. We don't want anyone except for administrators to have these rights on DC's.	
Shut down the system	Administrators
Administrators are the only persons with rights to shutdown Domain Controllers for obvious reasons. We don't want DC's being shutdown at all except when required, and then only when scheduled.	

Sales Policy

We are concerned about the staff in the Sales OU. The employee turnover in this OU is higher than anywhere else in the organization. They are also paid the least and more prone to conflict with management. One of the factors that encouraged management to consider deploying a Windows 2000 infrastructure was an incident where we suspect someone from the Sales business unit was harassing a manager after being dismissed. We wish to lock down users in this OU a little tighter than other OU's as a result.

Sales Event Logs:

The event logs for the sales OU are being set to 50MB. This will allow for larger log files should any of these employees be causing event logs to be generated. It is highly unlikely that they will produce logs this size as a result of the more restrictive policies applied. We would rather be safe than sorry, maintaining an audit trail to follow should something go wrong. We will be further exploring the viability of using Terminal Services for Sales staff before opening our next site[23].

Event Logs	
\Root\Sales Policy\Computer Configuration\Windows Settings\Security Settings\Event Log\Settings for Event Logs	
References:	
Maximum application log size	51200 kilobytes
We will allow 50MB of data in the application log on all Sales OU computers. We have plenty of storage room for a 50MB log. As per the default domain policy, we are forwarding sensitive logs to a central logging facility too.	
Maximum security log size	51200 kilobytes

Same as maximum application log size above.	
Maximum system log size	51200 kilobytes
Same as maximum application log size above.	

Sales IP Security Policies on Local Machine:

We're employing IP Security Policy to limit the IP addresses and services users in the Sales OU can communicate with.

IP Security Policies on Local Machine	
\Root\Sales Policy\User Configuration\Windows Settings\Security Settings\Local Policies\IP Security Policies on Active Directory	
References: http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/robi/ro060500.asp	
Client Sales	Yes
We have implemented specific IP Security Rules for the sales OU. Access has been granted to only the servers and service ports required for business use. Additionally, access to external services has been limited to only those required. This configuration layers defense-in-depth. Access to subnets such as 10.1.2.0/23 has been denied, restricting sales OU objects from accessing resources in this address range. Exceptions have been specifically configured for sales business unit managers so that they may perform their job functions. Further, the Cisco PIX's are used for additional firewalling.	

Sales Windows Explorer:

Locking down the file system and functionality of Windows is something I know will create a lot of unhappy sales users. Management has taken the stance that sales staff should only be allowed to access the services necessary to perform their jobs. This hopefully will increase productivity and profits. When this happens, management has decreed that a bonus will be paid to the sales users, followed by a raise. From a security standpoint, the IT staff supports this move. Sales staff prior to Windows 2000 deployment quite commonly spent their time downloading MP3 files via P2P applications installed without authorization, exchanged jokes via email (many of them executables which cause security concerns), and chatted with friends via IM applications. We will be closing this attack vector and monitoring NIDS logs. Spot checks will be performed on traffic (i.e. TCP port 80) to verify applications are not being tunneled. Locked down policy on these computers should severely inhibit unauthorized installation of software. Further, after signing the new Acceptable Use Policy (AUP), doing so will be grounds for termination.

Windows Explorer	
\Root\Sales Policy\User Configuration\Administrative Templates\Windows Components\Windows Explorer	
References: Microsoft Windows 2000 Policy Explanation - Included in Windows	
Enable Classic Shell	Enabled
We will be limiting members of the Sales OU from enabling active desktop. This is the primary reason for enabling the classic shell. We don't want active content to be executed on the users desktops.	
Removes the Folder Options menu item from the Tools menu	Enabled
By removing Folder Options we limit users from modifying file type extensions and associations. We also prohibit any other modifications that may have previously been made through the Folder Options menu.	
Remove "Map Network Drive" and "Disconnect Network Drive"	Enabled
We will be mapping the drives for users in the sales OU's at logon (including printers). There should be	

no need to map drives outside of those provided for the user. If there is, GIAC administrators will have to be consulted to fulfil the request.	
Hide these specified drives in My Computer	Enabled
Sales OU users will be prohibited from storing files locally on their computers. All files will be stored on the Sales sites specifically allocated file server. By hiding these drives, the users will not be able to access them through My Computer, Windows Explorer, and My Network Places. This not only supports backup policy, it helps ensure that the user does not access files stored locally. We are restricting all drives for the Sales OU.	
Prevent access to drives from My Computer	Enabled
This further prevents access to the Run dialogue box. Users will not be able to run programs that are not specifically displayed for them.	
Hide Hardware tab	Enabled
This will hide the hardware tab, prohibiting users from viewing hardware device configurations or from modifying these configurations.	
No "Computers Near Me" in My Network Places	Enabled
We are removing the "Computers Near Me" option and icons. By doing so users lists of network resources in Windows Explorer and My Network Places will be removed.	

Sales Start Menu & Taskbar:

More restrictive policies for the Sales users follow.

Start Menu & Taskbar	
\Root\Sales Policy\User Configuration\Administrative Templates\Windows Components\Start Menu & Taskbar	
References: Microsoft Windows 2000 Policy Explanation - Included in Windows	
Disable programs on Settings menu	Enabled
This removes Printers, Control Panel, and Network and Dial-up Connection folders from the start menu. Sales OU users cannot access these features.	
Remove Run menu from Start Menu	Enabled
We are prohibiting Sales OU staff from running unauthorized programs. By removing Run from the start menu we are further restricting users by disallowing them from starting programs from the command line.	

Sales Desktop:

We will disallow users from specifying an alternate path for their documents, supporting backup and lockdown policies.

Desktop	
\Root\Sales Policy\User Configuration\Administrative Templates\Windows Components\Desktop	
References: Microsoft Windows 2000 Policy Explanation - Included in Windows	
Prohibit user from changing My Documents path	Enabled
Self explanatory, we are not allowing users to circumvent our default domain policy by specifying a different location for their My Documents Path.	

Folder Redirection:

By specifying where users home directories are and redirecting their folders to central file servers, we can support our backup policies. We can also limit access to the local drives on users computers where necessary. Basically, if there is no need to touch the local drive, why should we provide access?

Folder Redirection
\Root\Sales Policy\User Configuration\Windows Settings\Folder Redirection
References: http://www.microsoft.com/windows2000/en/professional/help/default.asp?url=/windows2000/en/professional/help/Folder.htm[24] http://www.microsoft.com/windows2000/techinfo/reskit/samplechapters/dsec/dsec_pol_cxxv.asp[25] http://www.microsoft.com/WINDOWS2000/techinfo/reskit/en/Regentry/93508.htm[26]
Application Data
We will be keeping user specific folders on the specific sites file server. Applying this setting at the default domain level is acceptable, knowing that specific settings must be applied at the OU level for remote sites in order to specify the appropriate file server at that site. This requires the appropriate use of groups. Target: Advanced, sales-hq, \\file1-hq\home\%username% sales1, \\file1-sales\home\%username% Settings: Grant the user exclusive rights to Application Data, Move the contents of Application Data to the new location, Leave the folder in the new location when policy is removed. We will play with the prospects of modifying registry.pol to create home directories on file servers based upon the NT4 variable %homeshare% at a future time. This will tie in closely with user logon profiles, which would allow us to apply folder redirection at the default domain policy level.
Desktop
See application data for config.
My Documents
See application data for config.
Start Menu
See application data for config.

Exec Policy

We previously mentioned that there are a few business requirements for those in the exec OU. The users in this OU are in management positions and require a certain level of control over their respective OU's.

Managers will be delegated control over specific tasks within their respective OU. For instance the manager of the sales-hq OU will have create, delete, and manage user accounts/reset passwords on sales-hq. This will allow managers to perform administrative actions on their respective resources within AD.

Exec IP Security Policies on Active Directory:

We have a few specific IP Security Policies implemented to enable Sales Managers to access computers in the Sales OU's. Use of external services is less restrictive for users in the exec OU. All are considered as senior employees and all own substantial shares in the company. It is not in any of their best interests to be abusive of GIAC resources and all are considered to be competent enough to work without direct supervision. In case we are wrong, we'll have an audit trail to review from the FW and event logs.

IP Security Policies on Active Directory	
\Root\Exec Policy\Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Active Directory	
References: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/robi/ro060500.asp	
Client Exec	Yes
We have implemented specific IP Security Rules for the exec OU users. We are requiring all traffic between specific subnets to require security (IPSec). Traffic between the Sales OU subnet and the two business unit managers for the Sales sites has been specifically configured to request security, thereby allowing the managers to perform their jobs. Firewalling at the Cisco PIX's is relied upon for external service restrictions.	

A bit about DMZ Servers

We anticipate the majority of attacks against GIAC Enterprises resources will come from the Internet. Public servers in the DMZ are therefore the primary initial targets of external attacks and as such must be strictly configured, and monitored. Management is aware of the issues of having the DMZ computers operate as part of the domain. The following choices were considered:

1. Create another domain in the GIAC forest, adding more complexity to configuration and more physical assets to maintain and administer
2. Create a whole new Forest with a separate domain, adding a good deal of extra financial and administrative overhead
3. Run these DMZ servers in standalone mode, making administration more time consuming and for-going the benefits of domain wide Group Policy
4. Run the DMZ servers in a tightly controlled environment and have them participate in the current domain

There are many security related documents that advise against option number 4, as well as a plethora of examples of how such a configuration has failed. In cases where there were failures, almost all of them can be attributed to insecure administration of the DMZ hosts where access to other domain resources was available once the DMZ server was compromised. The key in making option 4 work is to limit access to the remainder of the domain. Management has dictated that we cannot add more physical resources to the network at this time. It simply isn't in the budget. This leaves us with only two options. Management has also stated that they wish to lower administration costs associated with DMZ hosts and prefer to have them managed primarily through GPO's. After much debate over the potential costs of recovery from a compromise of the DMZ and the potential for compromise of internal assets even if DMZ hosts were tightly controlled and a separate user account was used to administer these boxes outside of the regular admin groups (administrator, domain admins, enterprise admins etc.) we have finally convinced management to run the DMZ hosts in standalone mode. We can still apply Local Group Policy to these standalone servers. Future assets will be budgeted for, and the likely course of action will be a separate DMZ Forest and Domain. This isn't entirely viable with the number of DMZ servers right now but as GIAC expands and web based e-commerce picks up, it may become a more logical course of action.

Additional Security

Defense-in-depth:

I often think of computer security as a balancing act; trying to provide required business services without exposing assets to potential abuse. Many have come before that promised there was a one-stop-shop for your security woes. These solicitors have continuously been proven wrong. There are not too many products in the computer field that do not have a vulnerability associated with them. Taking a look at the CVE database hosted at http://icat.nist.gov, you hopefully will come to understand the point I'm trying to make here. The SANS Institute preaches defense-in-depth practices. The more defenses in place, supporting each other the better. If one should fail, your reaction time lessens. During the course of defenses being overcome by an abusive miscreant, alarms or stimuli triggers should be going off, alerting someone with the know how to deal with the situation, that there is indeed a problem. Through the use of Active Directory and Group Policy discussed above, we have implemented only a handful of the security measures available to us. It is time to look at some of these other defense-in-depth solutions that we can employ to support our overall security health.

Training and Awareness:

Probably one of the most effective countermeasures in blocking social engineering attacks is to educate employees of the consequences of a successful attack. Introduce some of the tactics that would be employed in subverting information or convincing users to perform the desired actions of the attacker. If users are trained to be wary of such threats, the likelihood of a successful attack is reduced. Along the same lines, training and awareness has gone the distance in preventing the spread of malicious code. Trojan and worm propagation vectors are almost stopped completely if users are trained not to "double click" attachments unless they are specifically expecting them, the attachment is from a known source, and the communication fits the profile of what is normal. GIAC Enterprises has a training and awareness program in place for its employees. Bi-annually, all employees attend a half-day seminar where security awareness is taught. A promotional awareness program also rewards employees who come forward with security concerns and suggestions with a monetary bonus, once per quarter. Another aspect of training and awareness is providing the necessary training for administrators to effectively manage the networks and resources. Sending the appropriate persons on quality training courses for certification, like SANS GCWN, is probably even more important (or at least equally important) than user training and awareness.

Enterprise wide Audit:

Having implemented a secure infrastructure is great! Making sure it is working and configured as we assume it is supposed to be is another story. Scheduled audits (scans) are performed on the Cisco PIX firewalls, confirming rules conform to policy. DMZ hosts are also poked and prodded to double-check their configurations. Any services, misconfigurations, vulnerabilities found are immediately addressed. This is on top of normal server maintenance. It doesn't take long to run an automated scanner such as Nessus[27] against the targets and browse through the reports. If there is a problem found, it can be queued by severity for follow-up action by one of

the administrators. Internal hosts receive the same type of attention; with workstations receiving a quick port scan and general Windows 2000 vulnerability scan. Auditing checklists are available online that others have prepared which help in identifying what to look for during audits of specific operating systems (OS)[28]. Further, we should be running some file integrity checkers on critical systems (eg. Tripwire[29]). Changes to system critical files would be an immediate tip-off that further action is required if we hadn't just rolled out a service pack or performed some system maintenance. The product would also provide a log of the changes to aid in troubleshooting, or in prosecuting an attacker.

Organizational Firewalls and Extended ACL's:

We are performing ingress/egress filtering on our routing and filtering devices. This goes great lengths in protecting assets. We not only protect our internal network from common denial of service attacks, we also restrict our network from use internally for the same types of attacks (allowing sane routing only). A default deny all policy is employed on Internet facing interfaces with only those services required being opened up. Further, stateful filtering is employed by the PIX. We trash most of the cruft coming in from the Internet right here. Highly effective additions in protecting our Microsoft Windows 2000 Secure Infrastructure![30]

Antivirus Gateway:

Educating users on virus threats isn't effective enough; at least we're not willing to place money on it. GIAC employees a proxy server that sits between the Internet and GIAC Enterprises, scanning for malicious code in all FTP/HTTP/SMTP traffic inbound or outbound of the HQ network. Through configuration options, we have opted to protect remote sites SMTP traffic through the gateway only. This cuts down drastically on Intersite traffic. We provided information on this gateway previously. [31]

Antivirus Software:

Well, why rely solely upon the gateway for protection. We also employ on-demand and on-access antivirus software at the desktop and scheduled on-demand scans on corporate servers. This protects the enterprise from malicious code introduced by internal users through software brought in on physical media or another hole in our antivirus strategy that we may have overlooked. Updates are incremental and the software is configurable and locked down to prevent tamper by users.[32]

Intrusion Detection:

Audit trails are important. From the infrastructure documented in previous sections, supported with group policy audit and event log policy, you've probably got the right impression. We are auditing heavily with the intent of prosecuting anyone that can be held accountable for causing harm to our business or employees. We take the matter of cyber-vandalism, threats against persons, abuse of our resources, and the loss of business very seriously. Currently we have three NIDS deployed. We are not currently covering all internal HQ subnets with the NIDS but we are auditing heavily and logging this to a centralized repository for correlation and protection of the logs. Previously we mentioned file integrity checkers should be installed on critical servers. Host Intrusion Detection Systems (HIDS), generally considered more functional than simple file integrity checkers, may also be employed in a similar fashion. Depending upon cost, these are products that should be considered as well.

Incident Handling and Response:

With all the effort we've put forth to secure our resources, it only makes sense to have a plan to deal with incidents and events that might occur. GIAC Enterprises needs to develop SOP's and action plans to deal with incidents, logically describing the courses of action that will take place. This is still being drafted and approved by management. Currently, administrators are rotated through on-call schedules and assigned a pager. Critical log and audit events trigger email that is routed to an external service provider who in-turn pages the administrator. Specific procedures will follow in policy.

Virtual Private Network:

Data between the HQ and Sales site is encrypted at the router and tunnelled between the two sites. Critical information thereby remains obscured to potential eavesdroppers. While we don't run grossly insecure protocols like telnet, and secure channel traffic is encrypted, we still do not want others to see what travels over our internal networks as it flows between sites over the Internet. We are employing a VPN to support our defense-in-depth practices.

Subscription Services:

Many information resources are published by sources that GIAC considers credible. These sources distribute late breaking news on various vulnerabilities and exploits as well as patch releases etc. First line defenses before vendors get to the punch are possible where we are able to determine our exposure. The administrators subscribe to numerous security mailing lists. Below are a few examples:

Cybernotes mailinglist[33]
SANS news product subscriptions[34]
Security Focus lists like focus-ms, vuln-dev, bugtraq[35]
Microsoft Security & Privacy Home webpage[36]
Incidents.org mailing list[37]

Backups:

We also employ incremental backups of important directories and files. Our backup policy includes a rotation schedule with removable media stored off-site in a bonded, environmentally controlled facility in a different physical location. Media is rotated weekly. In the event that archived files need to be recovered, we are able to go back two months, one week on-site and seven weeks off-site. Backup policy is very important to GIAC Enterprises. We cannot afford to lose important order information from our database, nor can we afford to lose important research, management documentation, business contracts, or accounting information. Come to think of it, we don't want to lose any data (including logs); hence we have a backup policy. We could cover disaster recovery in a separate section, however it is tied very closely with keeping off-site backups. There isn't much else to add to disaster recovery right now.

Hardware Redundancy:

Critical GIAC servers operate with RAID configurations. They are not hot swappable but data recover is possible. We keep a consumable supply of hard drives available as replacements should we lose one here and there. It happens so we had better be prepared for it. On average, we replace four drives per year on our servers due to hardware failures. Within an hour, a new

drive can be imaged and the server back up and in service. In a real pinch, we can reconfigure the RAID and run without redundancy until such a time that we can image a new drive. In this scenario, downtime averages 10 minutes.

Physical Security:

If we trusted every employee within GIAC we would probably be considered naïve. Even if all our employees were completely honest, could we trust that a stranger would not come in after hours and walk off with our data and assets? Again, probably not! We need physical security; locks, alarms, separation of assets based on value and criticality etc. GIAC Enterprises sites keep all servers in access and environmentally controlled rooms. No, these rooms don't have state of the art environmental controls, but they are air conditioned, humidity controlled, equipped with appropriate fire extinguishing systems[38], the door hinges are on the inside of the server rooms, the doors are metal reinforced, the locks are programmable combinations, the area between the foundation and raised floor is grated, and the partitioning walls extend up to the structural roof beyond the interior ceilings. We figure if someone with ill-intent gains physical access to a DC we are in big trouble. The current set-up is adequate given our current size.

Conclusion

Throughout this paper I have addressed the following requirements of the GCWN practical assignment version 3.1:

- I have considered the required departments, Research and Development, Sales and Marketing, Finance and Human Resources.
- I have provided a description of GIAC Enterprises business and the driving factors behind many of the decisions made.
- I have included a design with two geographically separated sites, including at least two domain controllers, a public IIS web server, electronic mail server, file server, and other key elements of the network.
- I have described Active Directory, including forests, trees, domains, sites, and OU's.
- I have described the default domain and default domain controllers group policy for the domain (modified from the default).
- I have described two other group policies and how they work with the default domain policy to increase security.
- And I have described additional security measures that should be considered and implemented to provide a layered defense-in-depth approach, working with group policy to secure GIAC Enterprises.

Through answering the above requirements, I believe we now have a network design that while not perfect, will provide a very good start during implementation. I have tried to be reasonable on budgetary expenditures while achieving a higher than average security posture. I have also allotted for the prospects of changes being made. In this sense things are a little modular in scope. No network design that I have seen in my previous experience is set in stone. Business requirements do change and newly addressable hardware does pop up on the network. I think I've provided some backwards compatibility for dealing with change.

It is my hope that this document will be useful to someone planning on designing a Secure Windows 2000 Infrastructure, and has met the GCWN assignment 3.1 practical requirements.

References

[1] Kiwi Enterprises, “Product Information – Kiwi Syslog Daemon”, 6 Sept 2002, http://www.kiwisyslog.com/products.htm#syslog

[2] EPOX Corp, “HPT370 UltraDMA-100 & RAID Setup Guide For EP-BX7+100”, http://www.epox.ru/support/mb/manual/upload/bx7+100-raid.pdf

[3] University of Pennsylvania, "Windows 2000 Active Directory database size and replication traffic between Domain Controller", http://www.upenn.edu/computing/group/win2k/references/replication.doc

[4] David Opitz, "Guide to Windows 2000 Kerberos Settings v1.1", Architectures and Applications Division of the Systems and Netowrk Attack Center (SNAC), 27 Jun 2001, http://nsa2.www.conxion.com/win2k/guides/w2k-16.pdf

[5] Jason Fossen, “Track 5 – Securing Windows – 5.1 Windows 2000/XP: Active Directory and Group Policy”, The SANS Institute

[6] The SANS Institute, "The Twenty Most Critical Internet Security Vulnerabilities - The Experts’ Consensus v2.504", 2 May 2002, http://www.sans.org/top20.htm

[7] LabMice.net, "Password Management in Windows 2000", http://www.labmice.net/Windows2000/Administration/password.htm

[8] Microsoft Knowledge Base Article - Q147706, "How to Disable LM Authentication on Windows NT", http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q147706&

[9] Microsoft Knowledge Base Article - Q161990, "How to Enable Strong Password Functionality in Windows NT", http://support.microsoft.com/default.aspx?scid=kb;en-us;Q161990

[10] Microsoft Knowledge Base Article - Q264678, "Increased Account Lockout Frequency in Windows 2000 Domain", http://support.microsoft.com/default.aspx?scid=KB;EN-US;q264678&

[11] Microsoft Corp, "Microsoft Windows 2000 Server Documentation - Account lockout", Microsoft Windows Server Documentation, http://www.microsoft.com/windows2000/en/server/help/sag_rras-ch1_74.htm

[12] Randy Franklin Smith, "Auditing Windows 2000", 20 Jul 2000, Windows & .NET Magazine Network, http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=9633

[13] Microsoft Corp, "Security - User Rights", http://www.microsoft.com/windows2000/techinfo/reskit/en/ProRK/prdd_sec_gqko.htm

[14] Microsoft Knowledge Base Article - Q257346, ""Access This Computer from the Network" User Right Causes Tools Not to Work", http://support.microsoft.com/default.aspx?scid=KB;EN-US;q257346&

[15] Microsoft Corp, "Microsoft Windows 2000 Server Documentation - Special permissions for files and folders", http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/acl_special_permissions.htm

[16] Mark Minasi, "Keeping Time with Win2K", Apr 2001, Windows & .NET Magazine Network, http://www.winnetmag.com/Articles/Index.cfm?ArticleID=20079

[17] Microsoft Corp, "Microsoft Windows 2000 Server Documentation - Privileges", http://www.microsoft.com/windows2000/en/datacenter/help/default.asp?url=/windows2000/en/datacenter/help/sag_SEconceptsUnPrivs.htm

[18] Microsoft Corp, "Secure channel: Digitally encrypt secure channel data (when possible)", MSDN Net, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/588.asp

[19] Microsoft Corp, "Secure channel: Digitally sign secure channel data (when possible)", MSDN Net, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/589.asp

[20] Zubair Alexander, "Windows Time Synchronization Service", 20 Mar 2000, Windows & .NET Magazine, http://www.winnetmag.com/Articles/Index.cfm?ArticleID=8383

[21] Microsoft Corp, "Step-by-Step Guide to Internet Protocol Security (IPSec)", Microsoft Windows 2000, http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp

[22] Microsoft Corp, "Robichaux on Security - June 2000", Microsoft TechNet, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/robi/ro060500.asp

[23] Microsoft Corp, "Terminal Services Features", 28 Oct 1999, Microsoft Windows 2000, http://www.microsoft.com/windows2000/server/evaluation/features/terminal.asp

[24] Microsoft Corp, "Folder Redirection", Microsoft Windows 2000 Professional Documentation, http://www.microsoft.com/windows2000/en/professional/help/default.asp?url=/windows2000/en/professional/help/Folder.htm

[25] Microsoft Corp, "Group Policy Storage", Microsoft Windows 2000, http://www.microsoft.com/windows2000/techinfo/reskit/samplechapters/dsec/dsec_pol_cxxv.asp

[26] Microsoft Corp, "ConnectHomeDirToRoot", http://www.microsoft.com/WINDOWS2000/techinfo/reskit/en/Regentry/93508.htm

[27] The Nessus Project Homepage, http://www.nessus.org

[28] Security Consensus Operational Readiness Evaluation; Prepared by Krishni Naidu, "Auditing Windows 2000", http://www.sans.org/SCORE/checklists/AuditingWindows2000.doc

[29] Tripwire Inc., "Tripwire for Servers; Assure the Integrity of Your Data", http://www.tripwire.com/files/literature/product_info/Tripwire_for_Servers.pdf

[30] The SANS Institute, "Cisco Anti-Spoof Egress Filtering", 23 Mar 2000, http://www.sans.org/dosstep/cisco_spoof.htm

[31] Trend Micro, "A Scalable, High-Availability Antivirus Solution: A High-performance, High-availability, Antivirus and Content Security Clustering Solution", http://www.trendmicro.com/download/whitepapers/isvw_clusters.pdf

[32] Trend Micro, "OfficeScan Corporate Edition", http://www.trendmicro.com/products/osce/

[33] National Infrastructure Protection Center, "CyberNotes", http://www.nipc.gov/cybernotes/cybernotes.htm

[34] The SANS Institute, "SANS Institute security digests", http://www.sans.org/newlook/digests/

[35] Security Focus Online, "Mailing Lists", http://online.securityfocus.com/archive

[36] Microsoft Corp, "Security & Privacy", http://www.microsoft.com/security/

[37] Incidents.org, Subscription Email Address, mailto:intrusions-subscribe@incidents.org

[38] Dupont Inc., "FE-13 for Total Flooding Agent Applications", http://www.dupont.com/fire/techinfo/fe13.pdf

[38] Microsoft Corp, “Windows 2000 Server Resource Kit Online Books”, Windows 2000 Resource Kit

[39] Microsoft Corp, “Resource Kit Group Policy Reference”, Windows 2000 Resource Kit

[40] Microsoft Corp, “MCSE – Designing a Microsoft Windows 2000 Directory Services Infrastructure”, Microsoft Press, ISBN 0-7356-1267-6

[41] Jason Lam, “Secure Windows 2000 network for GIAC Enterprises”, GIAC GCWN Certification

[42] Lenny Zeltser, “Designing a Secure Windows 2000 Infrastructure”, Apr 2002, GIAC GCWN Certification

[43] Jason Fossen, “Track 5 – Securing Windows – 5.2 Windows 2000/XP: PKI, Smart Cards and EFS”, The SANS Institute

[44] Jason Fossen, “Track 5 – Securing Windows – 5.3 Windows 2000/XP: IPSec and VPNs”, The SANS Institute

[45] Jason Fossen, “Track 5 – Securing Windows – 5.5 Windows 2000/XP: Scripting and Security”, The SANS Institute