Global Information Assurance Certification Paper

GIAC ENTERPRISES

"FORTUNES FOR THE FUTURE"

By: Lorna J. Hutcheson

Practical Assignment Version: 3.0

Implementing Active Directory with Defense in Depth

Table of Contents

Assignment 1: GIAC Enterprises Network Design and Diagram

Introduction

Background

GIAC Enterprises original network design comes from the work I did for my Track II certification (Firewalls, VPNS and Perimeter Security). I requested permission to use the design from Track II and have it carry over into this certification. I wanted to tie the two together and design my Active Directory structure based on my defense in depth network design. Permission was granted to approach it in this manner. As such, the basic overview and design concepts are based on the previous requirement and as such are more detailed.

Overview

GIAC Enterprises is a rapidly growing Internet startup company and as such has many concerns and needs. One of the major overall concerns is security. With their business being Internet based and starting out a small business, the need to get it right the first time is weighing heavy on everyone's mind. After all, this is the opportunity of a lifetime. It is important to design a security plan that protects them now and allows for expansion in the future. It is realized that initial costs may be high, but worth it in the long run. The following areas were causes of concern: customer access; suppliers being able to drop off their "fortunes for the future"; and their overseas partners who translate and then sale their cookies.

Assumptions

As stated before, it is very important that the first thing done when designing anything is information gathering. You have to understand and know the entire functionality of the system. If you don't know and understand this, chances are you will create a design that will not meet the overall security needs of the company or provide them with a way to expand. In essence, you will design yourself into a corner. Keep in mind the company hired you as the security expert. While they may know the basics of what needs to be protected, they are looking to you to validate this and ensure their company really is protected. The following are a sample of key questions to ask:

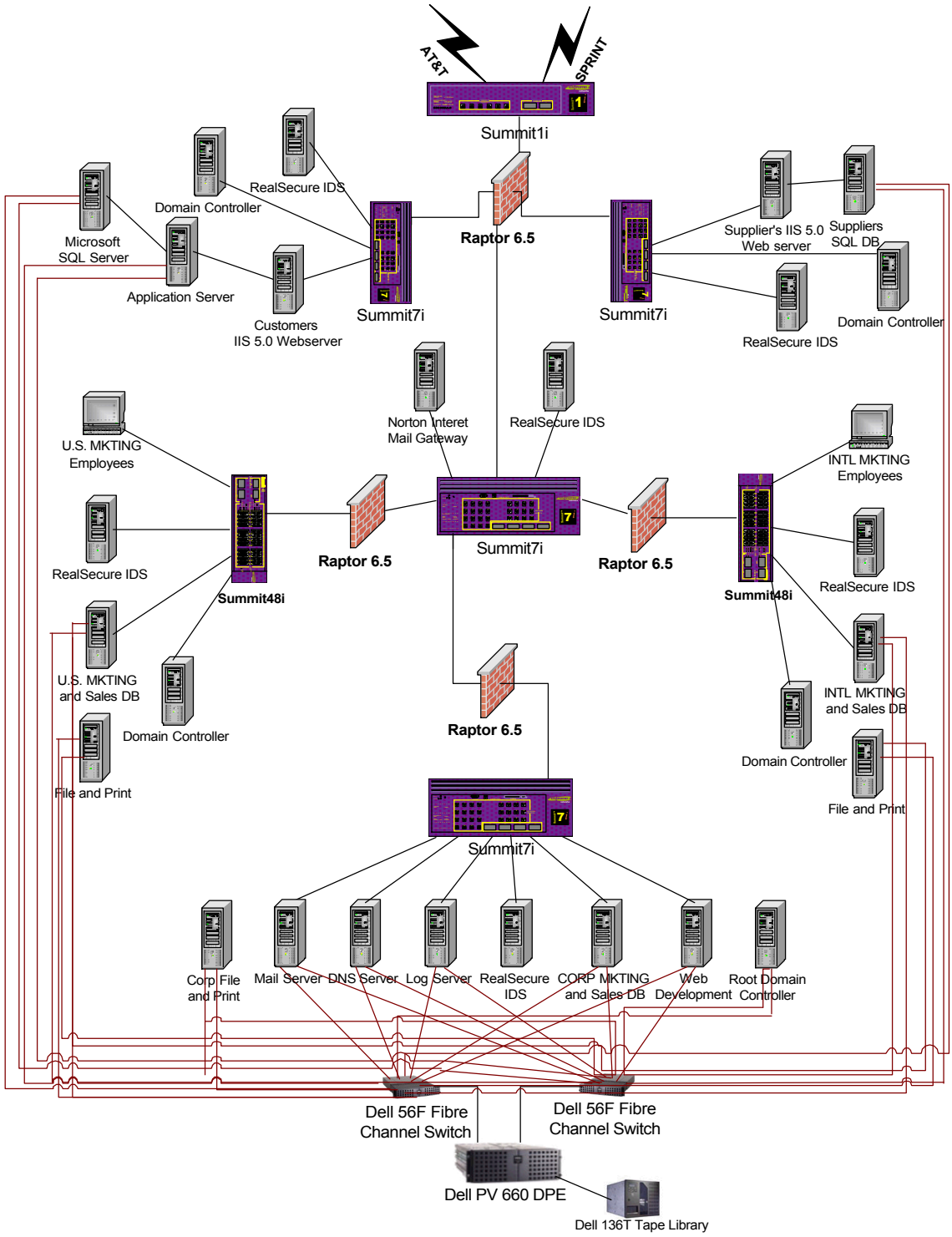
1. What does the organizational chart of the company look like? Who needs to talk to whom?
2. What is the current network design? What is already in place (servers, cabling, fiber, routers etc.).
3. What do they expect to look like in the next five years? Expansion is inevitable, and you need to know this to meet their growing needs.
4. Who manages what assets/personnel in the company?
5. Who is considered a trusted source outside of the primary firewall?

These are only a few of the questions that need to be answered to provide them with a secure system, capable of expanding. For the purposes of this exercise, these two

assumptions have been made:

1. Their defense in depth network design was approved and as such, it was realized that Microsoft's Windows 2000 architecture offered security benefits and greater ease of management.
2. Expansion in the future is going to be at an explosive rate.

GIAC Infrastructure



Overall Design

The previous diagram in shows the overall network design with security features implemented. Each of these features will be discussed later in greater depth. The design was developed to meet the requirements of GIAC Enterprises and to allow for growth and expansion in the future. Security needs not expressly stated by the company were taken

into consideration.

IP Addressing Scheme

The following addressing scheme will be used in this design. The routable IP addresses are fictious.

- Border Router:
  External Interface: 153.27.210.10/24
- Primary Firewall:
  External Interface: 153.27.38.20/24
  Internal Interface: 153.27.39.10/24
  Suppliers Services Network: 172.16.20.5/24
  Customers Services Network: 172.16.21.5/24
- Corporate Internal Router:
  External Interface: 153.27.39.15/24
- U.S. Marketing Firewall:
  External Interface: 153.27.39.25/24
  Internal Interface: 172.16.22.5/24
- International Firewall:
  External Interface: 153.27.39.20/24
  Internal Interface: 172.16.23.5/24
- Server Firewall:
  External Interface: 153.27.39.30/24
  Internal Interface: 172.16.24.5/24

Components Used

Firewalls

There is no way to discuss network security and not look at firewalls. Defense in depth demands some form of isolating off key systems within your organization. The majority of attacks/compromises are internal. This means finding a secure way of replicating active directory through a Firewall if you are going to have multiple domains and/or sites.

Hardware

Each of the firewalls is a Dell PowerEdge 2550 rack mountable system with dual processors. They have a RAID 5 configuration to ensure redundancy.

Implementation

Their operating system is Windows NT 4.0 workstation with Service Pack 6a. This was done to ensure the firewalls resided on a system different from the OS of the primary network and stay with an operating system that is proven under Raptor 6.5 with all of the latest service packs and hot fixes as required. There are three ways discussed in an article by Steve Riley to pass active directory replication. The first method is to open the firewall and let Remote Procedure Calls (RPCs) come and go at will. This is not a very safe

method, and if used, you probably should just get rid of the firewall. The second option is to only open the firewall some by static assigning RPC ports. This does require a registry hack on all of the AD servers and a reboot. The third option is using IPSec to pass network traffic between Domain Controllers. (Riley, 1)
To ensure that our systems stay secure and so as not to undo everything done by our defense in depth network design, we are going to use the third option and use IPSec. Since we will be promoting our domain controllers with the firewalls in place, we can not use Kerberos for the promotion phase as both computers have to be members of the domain. (Riley, 4) We will be using certificates of authority for IPSec, so we will need to have CA server as well. The following ports need to be opened on the internal firewalls. Mr. Riley provides an excellent table with the services and ports/protocols as seen below. (Riley, 5) For our purposes, we are only going to open for DNS, IKE and ESP and AH.

Service	Port/Protocol
DNS	53/tcp, 53/udp
PPTP establishment (if using PPTP)	1723/tcp
GRE, generic routing encapsulation (if using PPTP)	IP protocol 47
Kerberos3	88/tcp, 88/udp
IKE, Internet Key Exchange	500/udp
IPSec ESP, encapsulated security payload	IP protocol 50
IPSec AH, authenticated header	IP protocol 51

It is very important to remember that the only firewalls that will have these ports open are the U.S. Marketing, International Marketing and the server firewalls. The server firewall will be configured to talk to only the two domain controller's IP address's tied to their MAC address. Transparency has to be turned on in order for IPSec to not drop the packets. The U.S. Marketing, International Marketing firewalls will only be able to talk to the Root Domain Controller. Each of the above protocols will be created and tied only to rules for the Domain Controllers. They will NOT be opened up to allow unfettered access. It is critical that rules be put in place to deny the above traffic from the customer and suppliers services network interface card going to anywhere. The primary Firewall and all internal firewalls will be configured to deny the following services and ports as given to us in the SANS class, Track 5, Book 5.1 "Windows 2000: Active Directory and Group Policy" (Fossen, 25)

Port Number	Protocol	Description
3268	TCP	Global Catalog with LDAP
3269	TCP	Global Catalog with LDAP and SSL encryption
544	TCP	Kerberos KSHELL
464	TCP and UDP	Kerberos Passwords
88	TCP and UDP	Kerberos Secure Authentication
636	TCP	LDAP SSL

389	TCP and UDP	Lightweight Directory Access Protocol (LDAP)
137	UDP	NetBIOS query requests
138	UDP	NetBIOS query responses
139	TCP	NetBIOS Session (for SMB or CIFS)
135	TCP	RPC Mapper
445	TCP	SMB without NetBIOS (CIFS)
3389	TCP	Terminal Server
42	TCP	WINS Replication

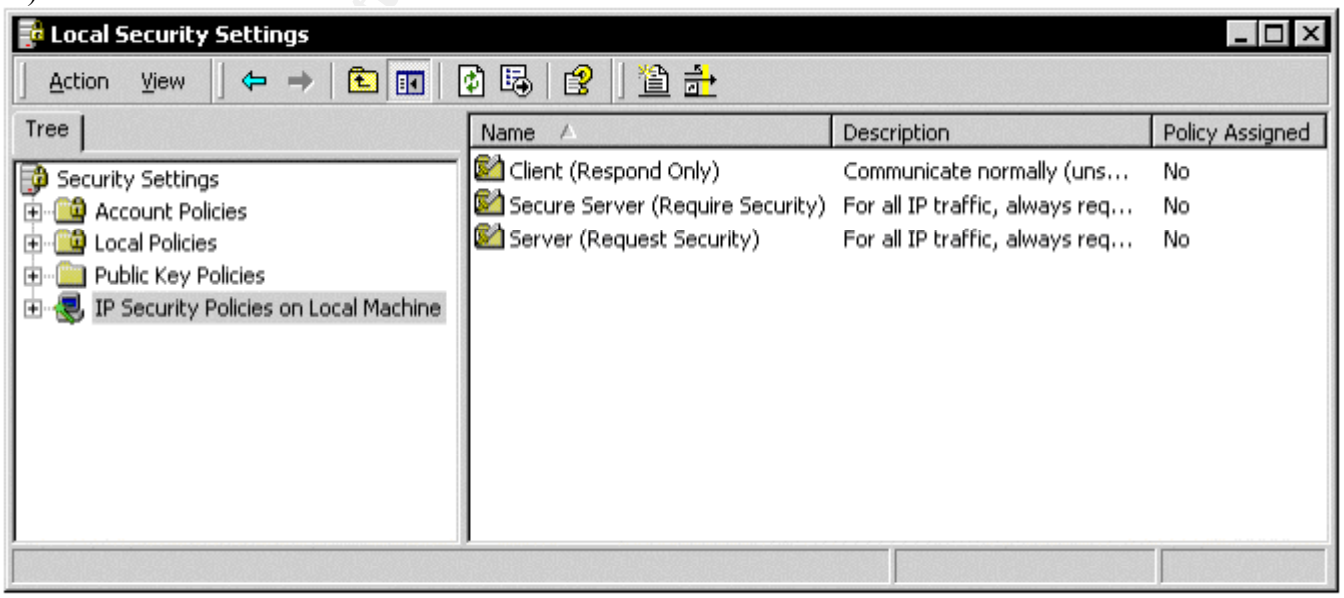
Domain Controllers

In the above design, there are five domain controllers. The root domain controller is located behind the server firewall. There is a domain controller behind the U.S. Marketing firewall and the International firewall. These three domain controllers are all part of the same tree. Each of the services networks, customers and suppliers, have a domain controller to help control the security and management of the services networks. However, the domain controllers are not part of the GIAC .org and do not replicate anything, hence they are each their own forest. All servers will have the latest patches and hot fixes applied.

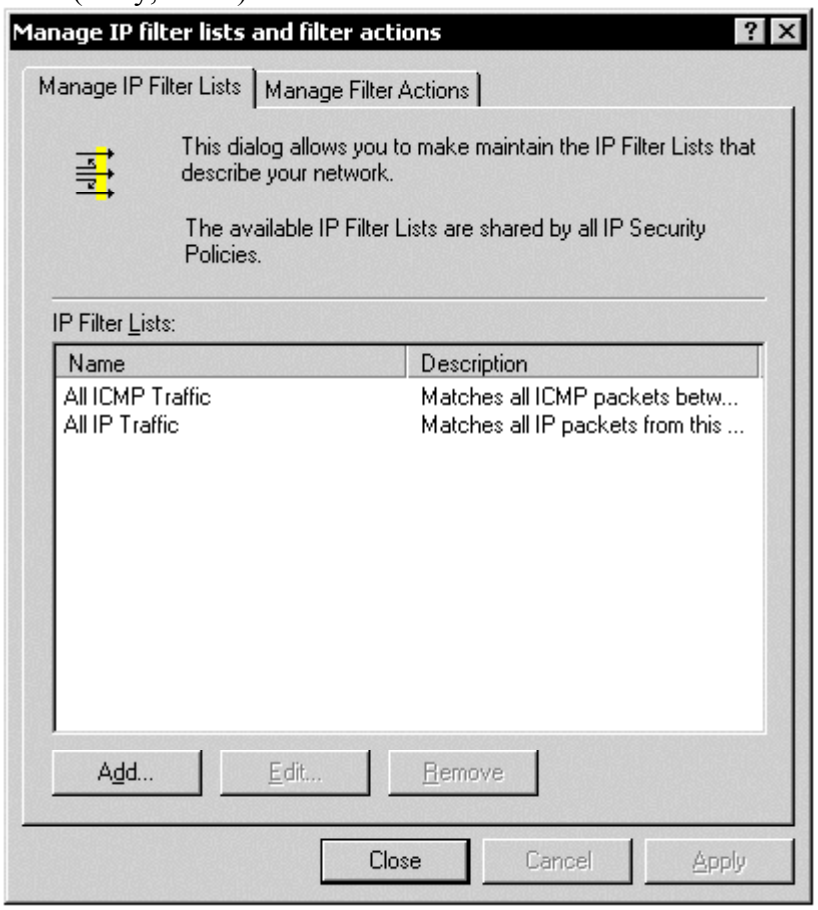
IPSec Configuration

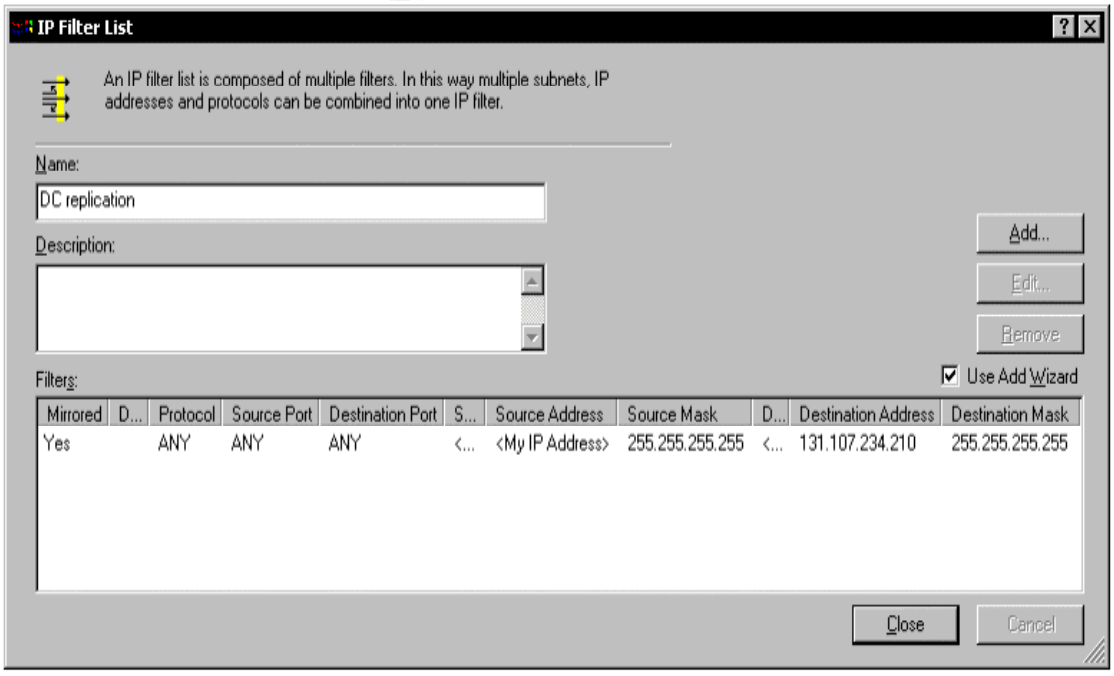
Mr. Riley provides an excellent tutorial on how to set up our Domain controllers to use IPSec on pages 11-18 of his article. The following is a short summary from his article and the same as was taught in the SANS course Track 5, Book 5.3.

1. Go to the local security settings and we will right click to manage a new filter. (Riley, 11)

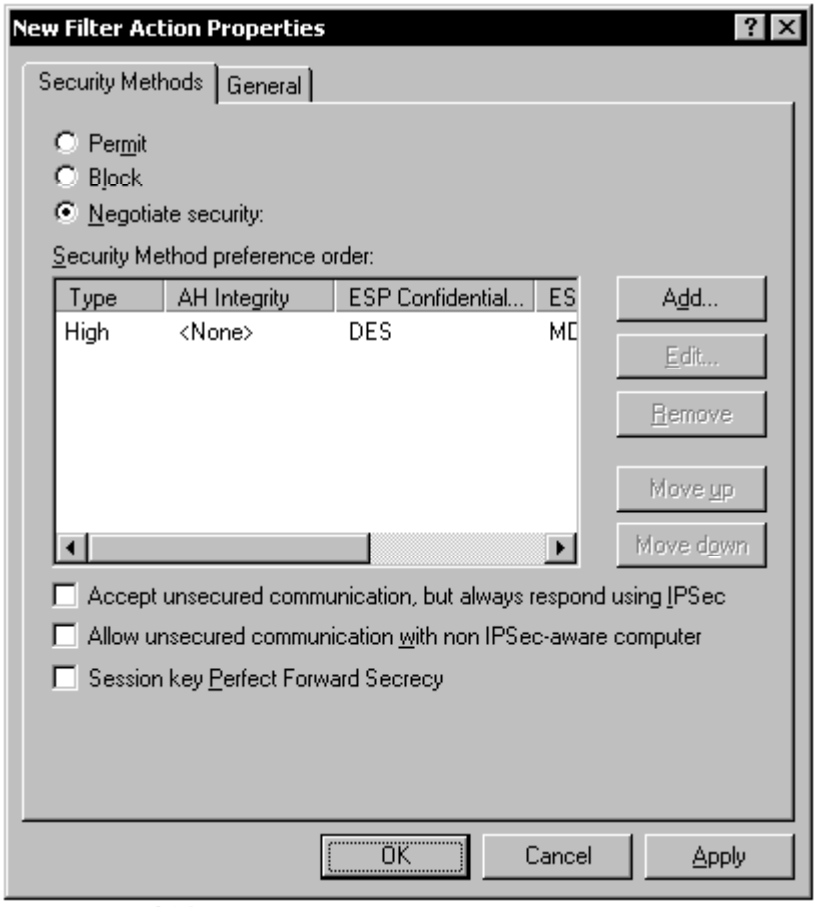


2. We now want to add a new filter. Make sure you choose the protocol as any to force all down the filter. (Riley, 12-13)

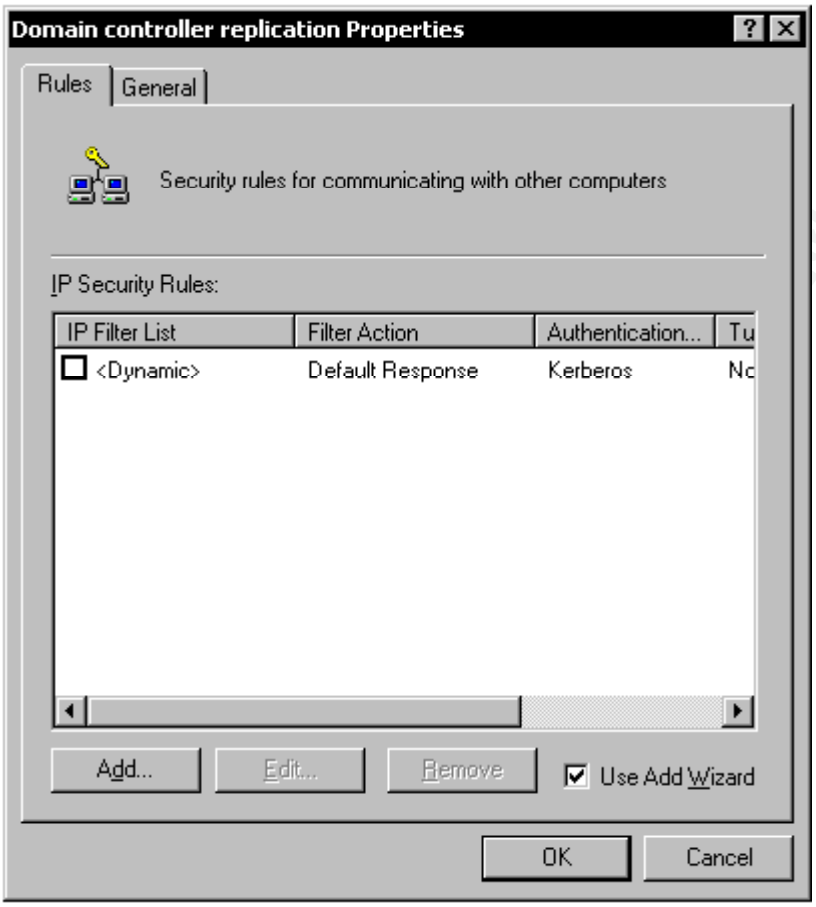




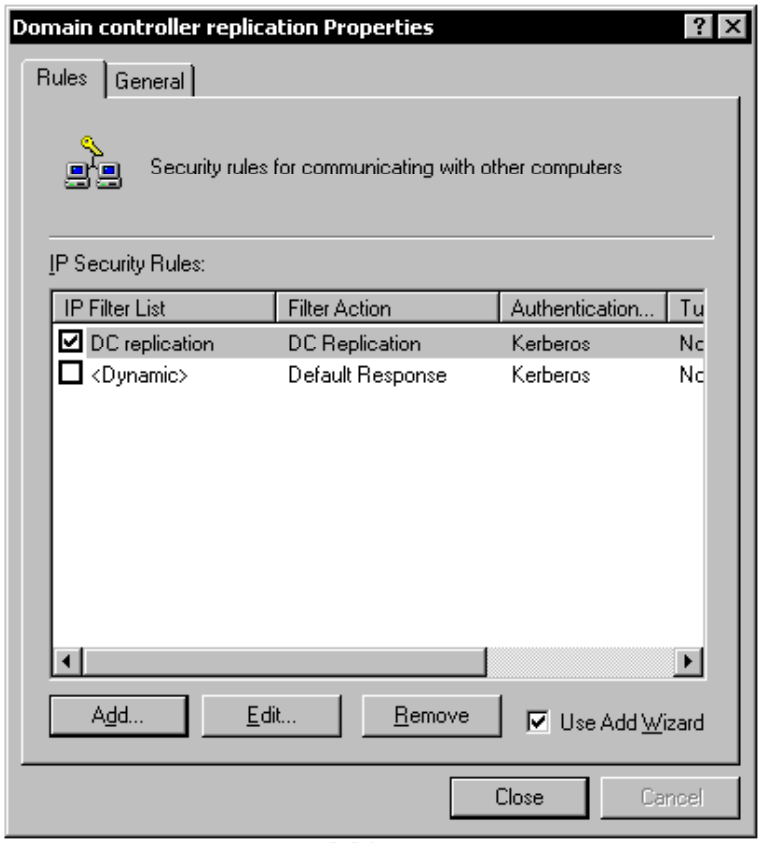
3. Now right click again and go to manage filter actions. It is here that we will tell it how to act. Choose the negotiate security, don't communicate with computers who don't support IPSec click High and select the edit properties check box. (Riley, 14)



4. Now right click and choose to create the security policy. Ensure the Activate the default response rule is clear and allow edits is checked. (Riley, 15)



5. Now click the add button and add a rule that does not specify a tunnel, select LAN and choose and authentication method. Select the IP filter and IP action you created previously and close the window. (Riley, 15)
6. The final step is to turn on the policy by assigning it. (Riley, 16)



Root Domain Controller

Hardware

The root Domain controller is a Dell 6450 with Quad Processors and will be a RAID 5 configuration to allow for redundancy and hot swappable drives. It also features two HBA cards to allow backup to a storage area network (SAN). This provides great speed in backup over the Fibre Channel.

Implementation

The root domain controller will be located behind the server firewall. Its primary role on the network is to control the entire active directory structure. As such, it is protected behind the server firewall where access is very restricted. It will replicate out to each of the other domain controllers the Schema, Configuration Naming Context (NC) and the Global Catalog. ALL replication will be done via IPSec between domain controllers as configured in the above example.

U. S. Marketing Domain Controller

Hardware

The Domain controller is a Dell 6450 with Quad Processors and will be a RAID 5 configuration to allow for redundancy and hot swappable drives. HBAs will not be used for backup of this server. It will be backed up by tape.

Implementation
The domain controller will be located behind the U.S. Marketing firewall. Its primary role on the network is to manage the U.S. Marketing section by enforcing security policy from the Root Domain controller and validating users on the network. It will control further defined group policy for the U. S. Marketing department. ALL replication will be done via IPSec between domain controllers as configured in the above example.

International Marketing Domain Controller

Hardware
The Domain controller is a Dell 6450 with Quad Processors and will be a RAID 5 configuration to allow for redundancy and hot swappable drives. HBAs will not be used for backup of this server. It will be backed up by tape.

Implementation
The domain controller will be located behind the International Marketing firewall. Its primary role on the network is to manage the International Marketing section by enforcing security policy from the Root Domain controller and validating users on the network. It will control further defined group policy for the International Marketing department. This department will have VPNs coming in from our overseas partners. ALL replication will be done via IPSec between domain controllers as configured in the above example.

Customers' Services Network Root Domain Controller

Hardware
The root Domain controller is a Dell 6450 with Quad Processors and will be a RAID 5 configuration to allow for redundancy and hot swappable drives. Backup will be done via tape drive.

Implementation
The root domain controller will be located on a services network off of the primary firewall. Its primary role on the network is to control the entire active directory structure of the customer's services network. . Because of the availability of the services network to anyone, it will NOT have any part to play with our internal network.

Suppliers Services network Root Domain Controller

Hardware
The root Domain controller is a Dell 2550 with dual Processors and will be a RAID 5 configuration to allow for redundancy and hot swappable drives. Backup will be done via a tape drive.

Implementation
The root domain controller will be located on a services network off of the primary firewall. Its primary role on the network is to control the entire active directory structure of the supplier's services network. . Because of the availability of the services network to anyone, it will NOT have any part to play with our internal network.

File and Print Server

Hardware

The File and Print Server is a Dell 6450 with Quad Processors and will be a RAID 5 configuration to allow for redundancy and hot swappable drives. It also features two HBA cards to allow backup to a storage area network (SAN). This provides great speed in backup over the Fibre Channel. The storage on the server will be the minimum as all storage for the File and Print server will be allocated on the SAN.

Implementation

Each of the departments will have their own File and Print server to put their data on. U.S. Marketing, International Marketing and Corporate will each have a File and Printer server. By each department having their own File and Printer server, we can eliminate having to transfer data over the network and each department would be kept isolate. We can control the storage in two different ways, each having their own SAN or using a joint SAN and keeping the systems completely separate. We are going to use the latter for our purposes. Further security will be defined by not assigning IP address to the Fibre Channel switches so that all management of them will be done via a direct connect. They will not be reachable from the network.

Public Web Server

Hardware

The Web server is a Dell 6450 with Quad Processors and will be a RAID 5 configuration to allow for redundancy and hot swappable drives. The public web server will only have a front end to which all users connect and a second machine will serve as a back end which holds the data. The back end database machine will have two HBA cards to allow backup to a storage area network (SAN). This provides great speed in backup over the Fibre Channel. The front end server is strictly to serve web pages.

Implementation

The web server will be located on the customers' services network off of the primary firewall. This web server will be accessible by everyone and will be hardened to help eliminate unwanted attacks. The ONLY functionality it will be supporting is HTTP and HTTPS.

Mail Server

Hardware

The mail server will be two Dell 6450 with Quad Processors and will be a RAID 5 configuration to allow for redundancy and hot swappable drives. Each server also features two HBA cards to allow backup to a storage area network (SAN).

Implementation

The mail server will be Microsoft Exchange server deployed using Microsoft cluster server. Since E-mail has quickly become the life blood of many organizations, all steps necessary will be taken to ensure that it is available at all times. Nothing will get

management's attention faster than being unable to send an email. As such, it is protected behind the server firewall where access is very restricted. We will also be employing a simple Norton Mail Gateway to screen incoming and outgoing email and attachments from viruses. This is also crucial to ensure the organization does not become infected with malicious code.

Assignment 2: GIAC Enterprises Active Directory Design and Diagram

Overview

The active directory design is one of the most time consuming and important parts of designing your Windows 2000 infrastructure. Everything else you do from Group Policy to administration duties will hinge on this design. This phase needs to be thought out in detail and the long term effects of it understood. The overall active directory design is presented below; however, it will be discussed in more detail.

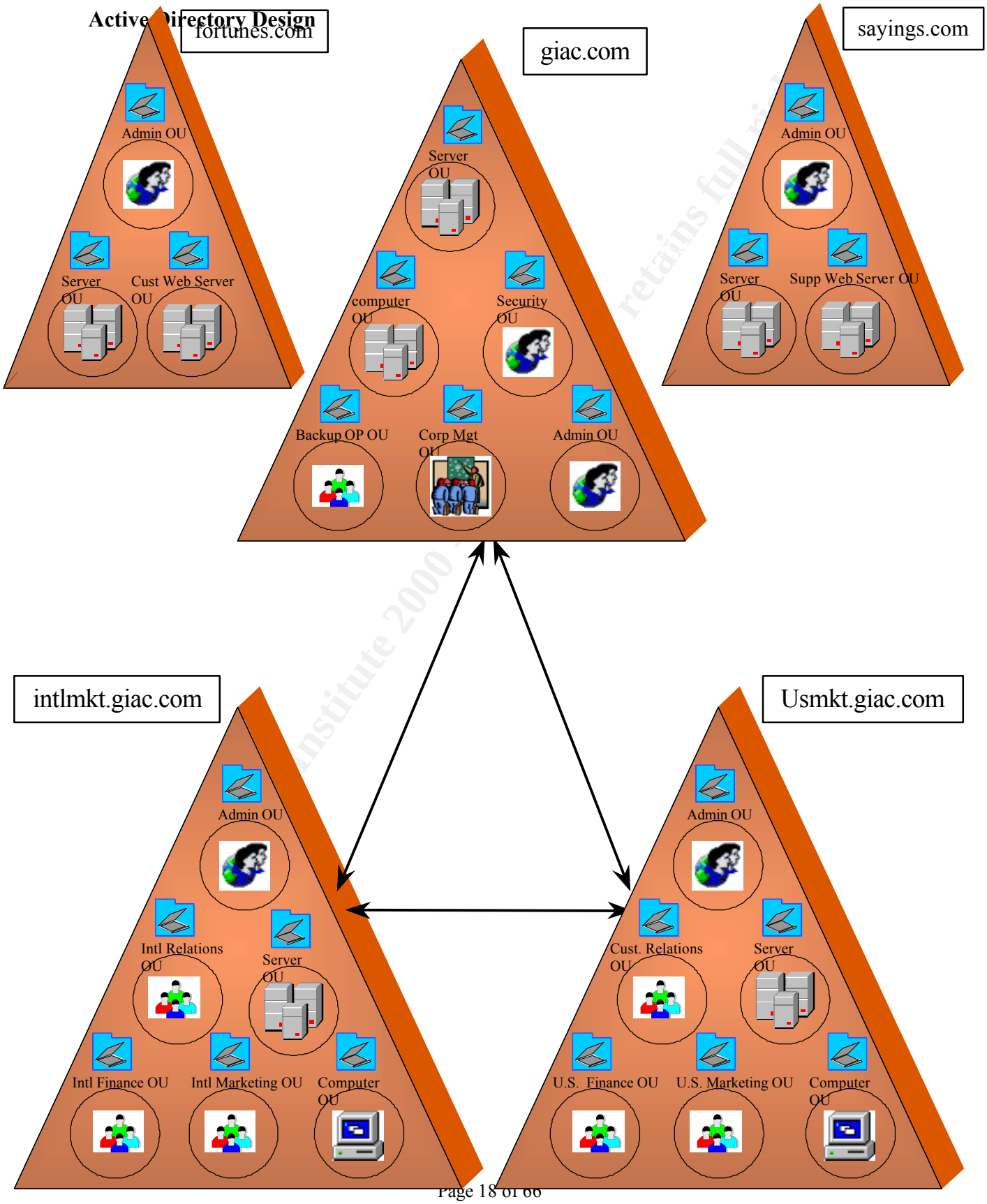
As a cursory overview, GIAC.com is the root domain. There are two additional child domains under GIAC.com called intlmkt.giac.com and usmkt.giac.com. This was done primarily for security reasons to be discussed later. Notice these follow a "complete trust" model. You will also see two other root domains: fortunes.com and sayings.com. Each of these is a root domain, one on each of the services network. Notice there are no trust arrows in either direction from either of these domains. This was done for security reasons as well which will be discussed shortly.

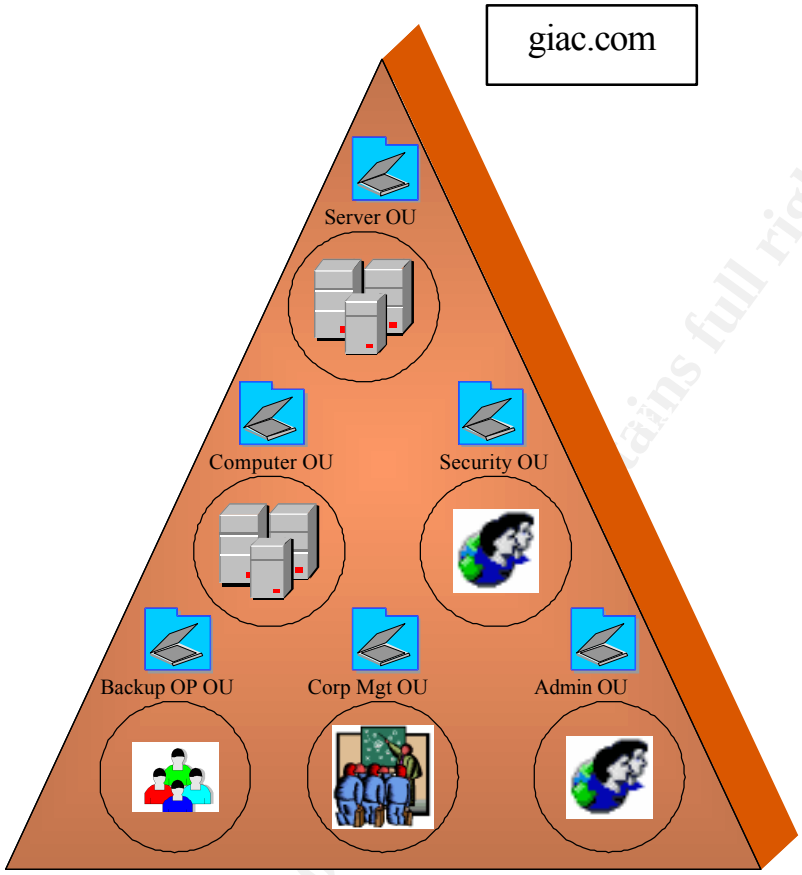
The Organizational Units (OUs) are represented under each domain by a different symbol. As opposed to trying to show all layers and intents of the OUs, the OUs were configured as an OU symbol (a folder) and an icon to represent the overall concept of what was in the OU. (Rice, Sanderson, Chapter 4: page 13) The OUs will be discussed in greater detail as each of the domains are looked at.

One of the primary guidelines for setting up the Active Directory infrastructure was the firewalls. Based on the locations of the firewalls, a clear picture was formed as to what should be kept in mind when separating off different sections/groups for security and administrative reasons. Because the network's defense in depth concept has already been designed and approved, it is extremely important not to undo what has been done. If the active directory was designed so that GIAC enterprises was all one big happy family, with no domains established, why put the firewalls in place? By separating out each of the fire walled areas as separate domains, I can enforce security policies tailored for each these areas and manage them with less chance for violating the defense in depth strategy.

Security Guidelines

We cannot over look the previously given security guidelines from our defense in depth friends and ensure we do not violate them. The primary rule of thumb is to be secure enough to protect the company, but still allow them to complete their mission. Only those protocols needed to complete the mission will be allowed through. Customers will be allowed access only to the Customer services network. Suppliers will be allowed into both the customer and the supplier services network. Any access into GIAC Enterprises will be by means of a VPN and then only to those resources that are required. Within GIAC Enterprises, access will be granted only to those resources required by the employees. It is with these guidelines, that we planned our Active Directory Structure.





GIAC.com was set up as the root domain for our active directory structure. This was done with several considerations in mind. I want to be able to safely protect the Active directory database. With the root domain controller sitting behind the server firewall, security was already set tight by the defense in depth plan and as such made a wonderful place to have the Active Directory database stored. You will see five primary OUs here and all will be discussed.

Server OU

The server OU will hold all of the servers to allow for centralized security and administrative management. Within the Server OU, nested OUs can exist to allow for more restrictive settings on particular servers if the need arises. Each OU will have a Group Policy Object (GPO) assigned to it. As such, the user configuration settings will be turned off to help reduce overhead of processing unused security settings.

Computer OU

The computer OU holds all of the computers other than the servers. This will allow for easier managing of the computers in the root domain. Within this OU will be nested OUs

as needed. The machines will start out with the same basic configurations assigned until such a time that more refinement is needed. This will enable us to manage, protect and audit all of the machines quicker and easier.

Security OU

The security OU will hold the members who are responsible for security in the security group. The purpose of the OU is to ensure that security team can do their job and have the correct permissions they need to do their job. Everything here would have a GPO to ensure what the security team could and couldn't do. They need specific software and abilities that others will not need. The members in this OU will be in universal group as well to have permissions and abilities in other domains for performing security functions. Within this OU there will be a

Backup OP OU

This OU will be administrator type folks whose only mission in life to handle the storage area network (SAN) and the backup and restoral of all critical systems. The responsibility of folks here will be to ensure all data is backed up and all of the off site storage requirements are met. As such, this OU was designed to apply permissions that limit as well as audit this group of people and their machines. The backup administrator is one of the most powerful rights a person can possess. As such, it needs to be monitored closely. This individual can copy any file as well as replace any file. Handling of the corporate databases requires extensive monitoring to ensure no compromise or espionage takes place.

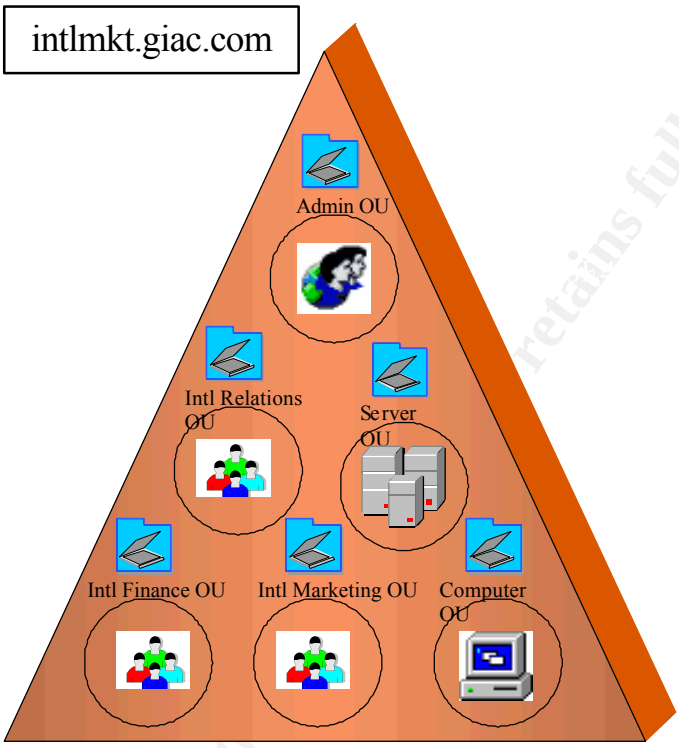
Corp MGT OU

This OU was developed for all of those folks at the corporate level who have a need to have accessed to other domains and/or entities. As such, they are going into an OU to allow us to give them the basic permissions they need and then allow us to tailor each and further define as needed. It will also put them in one location to allow more stringent auditing of their activities. They will also be assigned to a universal group to help facilitate this effort.

Admin OU

The admin group consists of all those individuals who have any rights administering any part of the root domain and/or other domains (i.e. enterprise/schema administrators). They will be broken down according to their roles on the admin team. There will be nested OUs with permissions for User management, Printer management, network management, server management, OU management etc. They will be divided if their job requires additional and/or fewer permissions.

Intlmkt.GIAC.COM Domain



The child domain of intlmkt.giac.com was created for one major reason and that was security. The original defense in depth plan called for a separation of the users from certain areas and these were made clear by the location of the firewalls. As such, we created separate domains of these areas to ensure they were autonomous from the other areas. Our users and resources are controlled within each domain. The domains are still controlled by the root domain. Now our users can be kept separated or they can be moved or given access anywhere in our forest.

Intl Relations OU

Our Intl Relations OU is a group of users whose role in life is to be a liaison with foreign nationals. As such, they are in constant contact and communications with foreign corporations. Because of their job, they require special software and access to limited amounts of information. As such, this group does not need the permissions as the rest of the domain. They will be locked down and given only what they need. They will also be monitored more closely for security concerns due to the nature of their job.

Admin OU

The admin group consists of all those individuals who have any rights administering any part of the child domain. They will be broken down according to their roles on the admin

team. There will be nested OUs with permissions for User management, Printer management, network management, server management, OU management etc. They will be divided if their job requires additional and/or fewer permissions.

Server OU

The server OU will hold all of the servers to allow for centralized security and administrative management. Within the Server OU, nested OUs can exist to allow for more restrictive settings on particular servers if the need arises. Each OU will have a Group Policy Object (GPO) assigned to it. As such, the user configuration settings will be turned off to help reduce overhead of processing unused security settings.

Intl Finance OU

The International Finance OU was created to manage all of the finance and specialized software. It was also created for security purposes and that was to ensure the Finance folks were locked down very tightly. Each of the international Finance folks is handling transactions from all over the world. As such, they require access to different resources, permissions, printers, servers etc. They will be configured according to their needs. They may be further broken down in the future by area if they need arises.

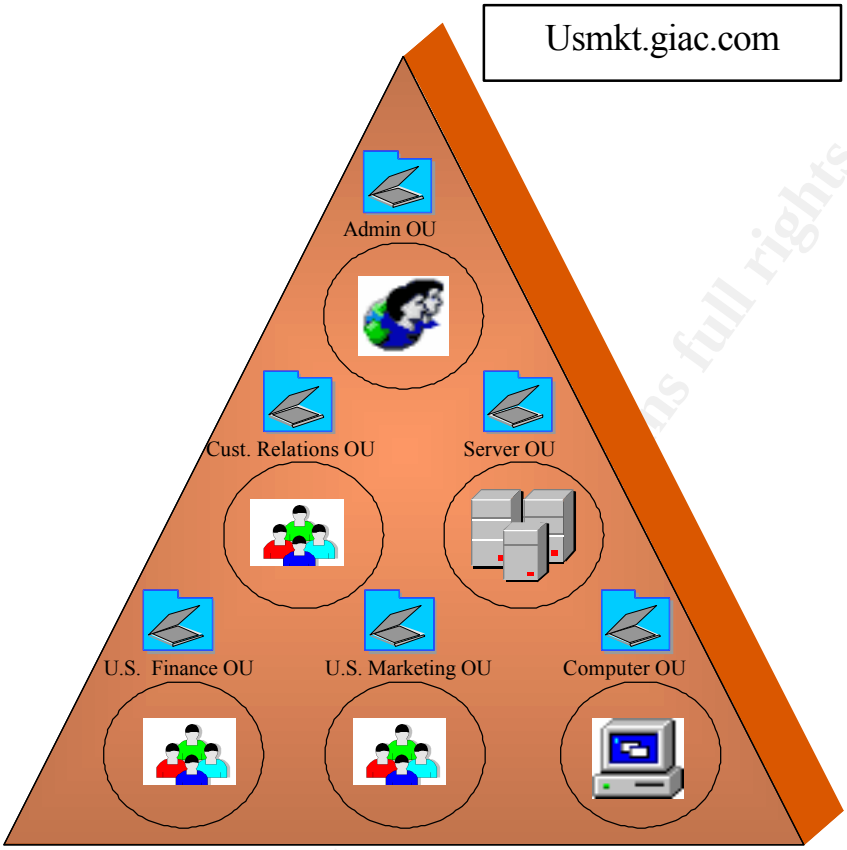
Intl Marketing OU

The international Marketing folks need to be able to reach out and touch everyone safely. They require their own tools, software and resources. The OU gives us that ability to more efficiently and securely manage it.

Computer OU

The computer OU holds all of the computers other than the servers. This will allow for easier managing of the computers in the root domain. Within this OU will be nested OUs as needed. The machines will start out with the same basic configurations assigned until such a time that more refinement is needed. This will enable us to manage, protect and audit all of the machines quicker and easier.

Usmkt.GIAC.COM Domain



The child domain of USmkt.giac.com was created for one major reason and that was security. The original defense in depth plan called for a separation of the users from certain areas and these were made clear by the location of the firewalls. It was felt very important for security to keep our international and U.S. departments completely separate. As such, we created separate domains of these areas to ensure they were autonomous from the other areas. Our users and resources are controlled within each domain. The domains are still controlled by the root domain. Now our users can be kept separated or they can be moved or given access anywhere in our forest.

Customer Relations OU

The customer relations group has the responsibility of customer service. They have different software and security needs. The do not need access to everything and as such will be restricted according to what they need. They will be monitored for security purposes.

Admin OU

The admin group consists of all those individuals who have any rights administering any part of the child domain. They will be broken down according to their roles on the admin team. There will be nested OUs with permissions for User management, Printer

management, network management, server management, OU management etc. They will be divided if their job requires additional and/or fewer permissions.

Server OU

The server OU will hold all of the servers to allow for centralized security and administrative management. Within the Server OU, nested OUs can exist to allow for more restrictive settings on particular servers if the need arises. Each OU will have a Group Policy Object (GPO) assigned to it. As such, the user configuration settings will be turned off to help reduce overhead of processing unused security settings.

US Finance OU

The U.S. Finance OU was created to manage all of the finance and specialized software. It was also created for security purposes and that was to ensure the Finance folks were locked down very tightly. Each of the U.S. Finance folks is handling transactions from all over the United States. As such, they require access to different resources, permissions, printers, servers etc. They will be configured according to their needs. They may be further broken down in the future by area if they need arises.

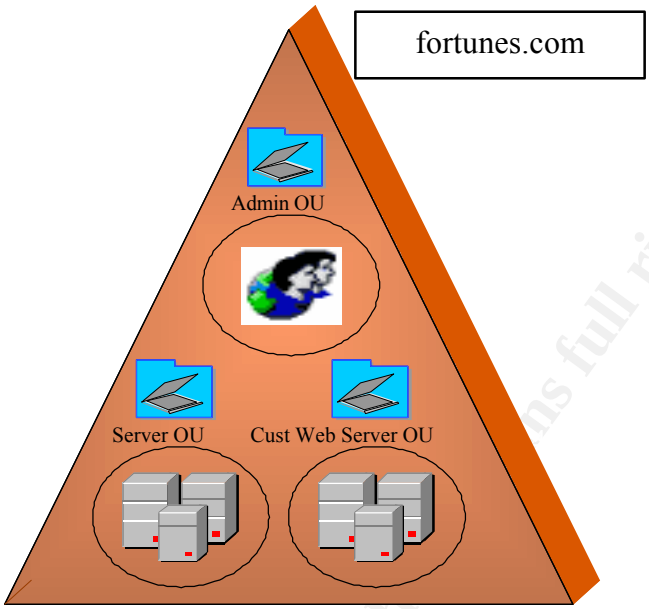
US Marketing OU

The U.S. Marketing folks need to be able to reach out and touch everyone safely. They require their own tools, software and resources. The OU gives us that ability to more efficiently and securely manage it.

Computer OU

The computer OU holds all of the computers other than the servers. This will allow for easier managing of the computers in the root domain. Within this OU will be nested OUs as needed. The machines will start out with the same basic configurations assigned until such a time that more refinement is needed. This will enable us to manage, protect and audit all of the machines quicker and easier.

fortunes.COM Domain



The fortunes.Com root domain is in a separate forest from the GIAC.com root domain. This was done for security purposes. When you look at the defense in depth design, the customer's web site and database was placed in a services network off of the primary firewall to ensure it was protected and monitored as well as isolating it from GIAC.com. This made sure good honest customers could come and go, but when bad guys came knocking, the rest of GIAC.com stayed safe. The configuration for fortunes.com was design with security in mind. The OUs were design to facilitate that.

Server OU

The server OU will hold all of the servers to allow for centralized security and administrative management. Within the Server OU, nested OUs can exist to allow for more restrictive settings on particular servers if the need arises. Each OU will have a Group Policy Object (GPO) assigned to it. As such, the user configuration settings will be turned off to help reduce overhead of processing unused security settings. Each server in the services network will only get the services it needs.

Cust Web Server OU

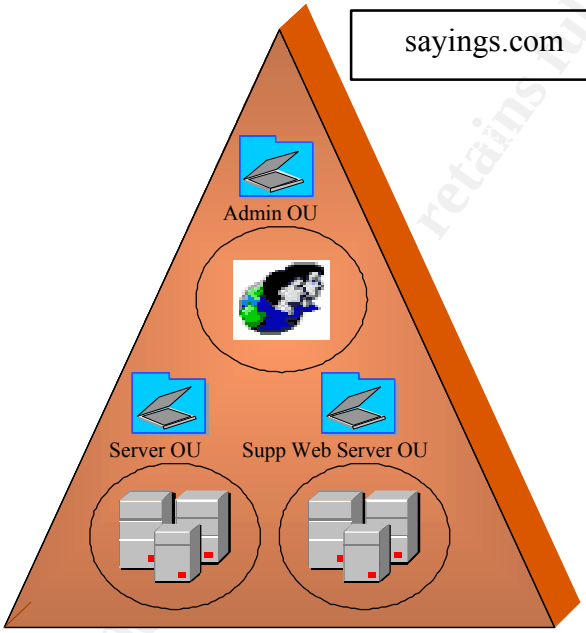
The customers' web server OU was designated by its self due to ensure it had the proper GPO assigned to it and was managed separately from the rest of the servers. It will be hardened down to a bastion host according to the practices recorded by the SANS Institute and monitored continually. (Fossen, Book 5.4)

Admin OU

The admin group consists of a select group of administrators who have been given rights to administer the fortunes.com root domain. They will be broken down according to their roles on the admin team. There will be nested OUs with permissions for User

management, network management, server management, OU management etc. They will be divided if their job requires additional and/or fewer permissions. There will be very limited administrators for this domain to ensure we don't get too many hands in the pot. If needs start to arise, a security group can be established. As of now, the logs will all be actively monitored by the security team.

sayings.COM Domain



The sayings.Com root domain is in a separate forest from the GIAC.com root domain as well as the fortunes.com. This was done for security purposes. When you look at the defense in depth design, the suppliers' web site and database was placed in a services network off of the primary firewall to ensure it was protected and monitored as well as isolating it from GIAC.com. This is further controlled by the firewall and ensures the security and safety of the GIAC.com. The configuration for saying.com was design with security in mind. The OUs were design to facilitate that.

Server OU

The server OU will hold all of the servers to allow for centralized security and administrative management. Within the Server OU, nested OUs can exist to allow for more restrictive settings on particular servers if the need arises. Each OU will have a Group Policy Object (GPO) assigned to it. As such, the user configuration settings will be turned off to help reduce overhead of processing unused security settings. Each server in the services network will only get the services it needs.

Supp Web Server OU

The suppliers' web server OU was designated by its self due to ensure it had the proper GPO assigned to it and was managed separately from the rest of the servers. It will be

hardened down to a bastion host according to the practices recorded by the SANS Institute and monitored continually. (Fossen, Book 5.4)

Admin OU

The admin group consists of a select group of administrators who have been given rights to administer the fortunes.com root domain. They will be broken down according to their roles on the admin team. There will be nested OUs with permissions for User management, network management, server management, OU management etc. They will be divided if their job requires additional and/or fewer permissions. There will be very limited administrators for this domain to ensure we don't get too many hands in the pot. If needs start to arise, a security group can be established. As of now, the logs will all be actively monitored by the security team.

Assignment 3: GIAC Enterprises Group Policy and Security

Overview/Goals

The purpose this requirement is to establish GIAC Enterprises security architecture and ensure it meets all of the security requirements. We will be establishing the default domain policy and the default domain controller policy in our architecture and validating it meets the criteria. The management at GIAC Enterprises, being a new E-commerce company and knowing their livelihood depends on the ability of the customers to make purchases 24/7, wants to ensure this will happen, but happen safely and securely. It is very important to them that they can protect their customers and themselves. With a vested interest in the overseas market, and in light of the attack on the World Trade Center and the Pentagon, concern has risen over staying secure. There have been many recent attacks on websites and the damage caused by Code Red alone (estimated cost $2.6 Billion), has management worried about attacks on their website. (Abreu, "New Year, New Web Attacks")

Default Domain Policy

It is extremely important to ensure that all of the default security settings are applied across the board to all desktop systems, laptops and servers alike. Further customization can be accomplished on a case by case basis. There are three major sources of information that can be researched to determine the best settings for your environment. The National Security Agency (NSA), Defense Information Systems Agency (DISA) (restricted access) and System Administration, Networking, and Security Institute (SANS) all have issued best practice solutions and guidelines. It is very important to remember that these are just guidelines. There is no one size fits all for anyone. They are all **guidelines**. This is very important to understand. When things become to set in stone, i.e. using xxx.xxx.xxx.1 as an IP address for a router, switch, PDC etc, you can open yourself up for vulnerabilities. Security has to be tailored to your environment, there is no one set template. The following settings are derived in conjunction with the Defense in depth design, the mission of GIAC enterprises and the active directory design. TEST, TEST, TEST all settings before implementation!! Don't just guess at what something does, FIND OUT! We will start with a restrictive policy at first and back out a little if needed.

1. The first thing to look at is the account policies. The options available and their recommendations are listed below:

Password Policy Options	***Domain Policy***

Enforce password uniqueness by remembering last x passwords **Reason:** To ensure users don't rotate around to their favorite password again and again.	24 passwords
Maximum Password Age **Reason:** Force the user to change their password to a new one.	4 months (Local login not allowed for users on network)
Minimum Password Age **Reason:** Force them to keep their password for a minimum period of time before requesting to change it. If you don't set this, they can change it over and over till they get back to the one they like.	90 Day
Minimum Password Length **Reason:** Force the users to use pass phrases and strengthen the passwords	12 Characters
Password must meet complexity requirements of installed password filter **Reason:** Force users to have a strong password and not one that will be cracked as easy by brute force or some other method.	Enabled
Store password using reversible encryption for all users in the domain **Reason:** Might as well store it in plain text if you use this one.	Disabled

2. Under Account Policies -> Account Lockout Policy are the lockout recommendations for the network:

Password Policy Lockout Options	***Domain Policy***
Account Lockout threshold **Reason:** A valid user should not take more than three times to log in.	3 invalid logon attempts

Lockout Account Duration **Reason:** I want the user to have to notify the network team and request permission to reset it. What if it isn't that person?	30 Minutes
Reset account Lockout count after **Reason:** Make sure it gives the user time to type in three attempts before resetting the count.	15 Minutes

3. On Windows 2000 systems you have the options for the following Kerberos Policy, which is only available if running Windows 2000 Servers for the domain controllers.

Kerberos Policy	***Domain Policy***
Enforce User Logon Restrictions: When this option is enabled, the KDC validates every request for a session ticket to ensure the user has the right to log on Access to services. **Reason:** Verify user credentials	Enabled
Maximum lifetime for Service Ticket: A "service ticket" is a session ticket. **Reason:** To ensure the session expires if not in use. (Remember this must be greater than 10 and less than the lifetime for a user ticket or it conflicts.) I set this to 10 hours for the server to match those users who work a long day and 2 hours on a laptop to force someone to reauthenticate.	120 Minutes
Maximum Lifetime for User Ticket: A "user ticket" is a TGT and must be renewed after this time. **Reason:** Use guidelines for your work day and plus it up 1 or 2 hours. For local, this should be much shorter since users aren't logging on there. If it's a bad guy, we don't want to give them all day to play.	2 Hours

Maximum Lifetime for User Ticket Renewal: This is the maximum lifetime of a ticket, No ticket can be renewed after this time. **Reason:** Limit the time before contact with the server has to be made.	7 Days
Maximum Tolerance for Computer Clock Synchronization: When the KDC clock off how many minutes from the client's clock, tickets are not issued for the client. **Reason:** This is a deterrent in Replay attacks. (Rice, David C and Sanderson, Mark J. "Guide to Securing Microsoft Windows 2000 Active Directory.")	5 minutes

4. Audits can consume enormous amounts of processor time and disk space. They should be chosen wisely.

Auditing Policy Options	***Domain Policy***
Audit Account Management: Tracks changes such as when accounts are created, changed, or deleted. **Reason:** You want to know when any user rights are elevated, changed etc. and make sure it was authorized and the account is a valid account.	Success, Failure
Audit Account Logon Events: Track logon events **Reason:** Who logged on where and when	Success, Failure
Audit Logon Events: Tracks users who have logged on or off, or made a network connection. Also records the type of logon requested (interactive, network, or service). **Reason:** Track failures to record possible unauthorized attempts to break into the system.	Success, Failure

Audit Directory Service Access: Monitor access to active directory. **Reason:** On workstations, no one is supposed to on locally and on servers, you want to monitor who get it. This is failures for normal activity however; I would switch this to success and failures if you suspect unwanted activity.	Failure
Audit Object Access :). **Reason:** Track unsuccessful attempts to access objects i.e. directories, files, and printers etc. However, remember to switch this to success and failures if you suspect unwanted activity	Failure
Audit Policy Change: Tracks changes in security policy **Reason:** You really want to know who changed it and why!	Success, Failure
Audit Privilege Use: Tracks unsuccessful attempts to use privileges. Privileges indicate rights assigned to Administrators or other power users. **Reason:** This can be massive if successes are monitored, however do this if you have anything suspicious.	Failure
Audit Process Tracking: Tracks process and what is running. **Reason:** Due to data generated, track this only if something suspicious occurs.	No Auditing
Audit System Events: Tracks events that affect the entire system or the Audit Log. **Reason:** **KNOW** what is going on your system. Don't just say I guess that was normal, **FIND OUT** the cause!	Success, Failure

5. The SCM Security Option section has many features. They can be modified in the registry, but it is recommended to use the SCM.

Security Attribute	***Domain Policy***

Additional Restrictions for Anonymous Connections **Reason:** You need to decide this for your network, we are operating in native mode and will use 2	No Access without explicit anonymous permissions
Administrator Automatic Logon **Reason:** Do not allow someone to logon automatically if they get access.	Disabled
Allow system to be shutdown without having to logon **Reason:** Make sure a user is at the keyboard and knows how to log on. If this is not disabled and access is gained, you can shut down machines remotely	Disabled
Audit the access of global system objects **Reason:** Know who is using your system!!!	Enabled
Audit use of backup and restore privilege **Reason:** Monitor this all power privilege and know when it used	Enabled
Automatically log off users when logon time expires **Reason:** Tailor this to the work hours of your company and make it a policy to request permission to be on the network past normal work hours.	Not Defined
Automatically log off users when logon time expires (local) **Reason:** Set this for local workstations, just as a security measure	Enabled
CD-ROM Autorun **Reason:** Turn it off to prevent malicious code from being executed knowingly or unknowingly.	Disabled
Clear virtual memory pagefile when system shuts down **Reason:** clear the data out of your system to protect it	Enabled
Default User Screen Saver Active **Reason:** Make sure the users have a screen saver come on to protect data when not at their desk or not in use	Enabled

Default User Screen Saver File **Reason:** We will use the logon.scr and force the users to log back on	logon.scr
Default User Screen Saver Password Protected **Reason:** Make sure this is enabled	Enabled
Default User Screen Saver Timeout Value **Reason:** This should be relatively short to help protect your data. Users get up and walk away with out locking the screen, you want it to lock very quick	300
Digitally sign client communication (always) **Reason:** We have a pure W2K environment, so we will require digital signatures	Enabled
Digitally sign client communication (when possible) **Reason:** Already selected the above	Disabled
Digitally sign server communication (always) **Reason:** Enable this since we have a pure W2K environment	Enabled
Digitally sign server communication (when possible) **Reason:** Already selected the above	Disabled
Disable CTRL+ALT+DEL requirement for logon **Reason:** Make the users press CTRL+ALT+DEL to help protect against Trojans that steal passwords	Disabled
Do not display last user name in logon screen **Reason:** This is 50% of the key needed to access your resources, make everyone type it in each time.	Enabled
Don't Save Dial-up Networking Password **Reason:** I just need physical access to your system if this is enabled. Make the users type it in everyone time, especially laptops!!!	Enabled

Enable Option to Delete Roaming Profile Cache **Reason:** Make sure you have this enabled, don't keep your cache and all your activities and files	Enabled
Generate 8.3 File Names **Reason:** Tailor it to your environment; we do not need it at GIAC enterprise.	Disabled
LAN Manager Authentication Level **Reason:** Base this on your environment	Send LM & NTLM - use NTLMv2 session security if negotiated
Message text for users attempting to log on **Reason:** What ever is appropriate for your organization, it should warn about unauthorized access etc, see your lawyer.	GIAC NOTICE
Message title for users attempting to log on **Reason:**	GIAC TITLE
Number of previous logons to cache (in case domain controller is not available) **Reason:** This gives anyone unauthorized access.	0 logons
Prevent system maintenance of computer account password **Reason:** Let the password alone	Disabled
Prevent users from installing printer drivers **Reason:** They could install something malicious, on purpose or by accident. This should be done only by the admin folks assigned to it.	Enabled
Prompt user to change password before expiration **Reason:** Give them time to get ready and think about a new one	14 days
Recovery Console: Allow automatic administrative logon **Reason:** Never allow this.	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders **Reason:** Have a better recover plan	Disabled

Rename administrator account **Reason:** Always and ensure you are logging on with separate accounts for all your administrators	Captain
Rename guest account **Reason:** Don't leave it the default name guest that everyone else does	Ted
Restrict CD-ROM access to locally logged-on user only **Reason:** Prevent access of your data from across the network	Enabled
Restrict floppy access to locally logged-on user only **Reason:** Prevent access of your data from across the network	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always) **Reason:** Always verify who's on the other end	Enabled
Secure channel: Digitally encrypt secure channel data (when possible) **Reason:** N/A	Disabled
Secure channel: Digitally sign secure channel data (when possible) **Reason:** N/a	Disabled
Secure channel: Require strong (Windows 2000 or later) session key **Reason:** We want to be sure and protect our data	Enabled
Secure system partition (for RISC platforms only) **Reason:** We do not use these at GIAC Enterprises	Not defined
Send unencrypted password to connect to third-party SMB servers **Reason:** Don't ever send your password in the clear	Disabled
Shut down system immediately if unable to log security audits **Reason:** This is key to stop unwanted attacks, but it can clue them they have been detected, lose data etc. We are going to shut down immediately	Enabled

Smart card removal behavior **Reason:** If the card is taken out, the user should be forced to put it back it and it have to be locked.	Lock Workstation

6. Event Log Settings

Event Log Settings	***Domain Policy***
Maximum application log size **Reason:** For the workstation, this will be set large enough to hold all of the information, but not take up too much room. The servers will be left at the max allowed to ensure they can collect everything	10048Kb
Maximum security log size **Reason:** This is set large enough to hold at least a month's worth of data before it is over written. The security logs will be rotated daily by scripts. Workstations will be kept for six months and servers for 1 year to ensure they are not needed.	10048Kb
Maximum system log size **Reason:** For the workstation, this will be set large enough to hold all of the information, but not take up too much room. The servers will be left at the max allowed to ensure they can collect everything.	10048Kb
Restrict guest access to application log **Reason:** No one should be allowed to access the logs and given the ability to modify or hide what they are doing. Only administrators should have access to this log	Enabled
Restrict guest access to security log **Reason:** No one should be allowed to access the logs and given the ability to modify or hide what they are doing. Only members of the security team should have access to this log	Enabled

Restrict guest access to system log **Reason:** No one should be allowed to access the logs and given the ability to modify or hide what they are doing. Only administrators should have access to this log	Enabled
Retain application log **Reason:** Workstations: we will have the logs over written every 30 days; all server logs will be kept and rotated.	30 days
Retain security log **Reason:** Workstations: we will have the security logs rotated off and stored for 6 months, all server logs will be moved off and kept for 1 year.	By days
Retain system log **Reason:** Workstations: we will have the logs over written every 30 days; all server logs will be kept and rotated.	30 days
Retention method for application log **Reason:** workstations will be over written every 30 days, servers will be scripted to rotate the logs for processing	By days
Retention method for security log **Reason:** Both will be manual and kept for 6 months for workstations and 1 year for servers (All data will be filtered for anomalies)	Manual
Retention method for system log **Reason:** workstations will be over written every 30 days, servers will be scripted to rotate the logs for processing	By days
Shutdown the computer when the security audit log is full **Reason:** If an event is taking place that is bad, we need to know and stop it; however, shutting down the system can get rid of valuable information in an investigation. The logs should be watched regularly for unauthorized access, but a real live person should make the call to shut the system down.	Disabled

Default Domain Controller/Workstation Policy

The policy for the Domain Controllers mirrors that of the default domain policy with few exceptions. At the same time, it is just as easy to look at local policy for each of the workstations to understand some of the differences between the two. It does provide a great comparison.

Password Policy Options	***Windows 2000 Workstation***	***Windows 2000 Server***
Enforce password uniqueness by remembering last x passwords **Reason:** To ensure users don't rotate around to their favorite password again and again.	24 passwords	24 passwords
Maximum Password Age **Reason:** Force the user to change their password to a new one.	4 months (Local login not allowed for users on network)	4 months (admin accounts changed every 90 days)
Minimum Password Age **Reason:** Force them to keep their password for a minimum period of time before requesting to change it. If you don't set this, they can change it over and over till they get back to the one they like.	90 Day	90 Day
Minimum Password Length **Reason:** Force the users to use pass phrases and strengthen the passwords	12 Characters	12 Characters
Password must meet complexity requirements of installed password filter **Reason:** Force users to have a strong password and not one that will be cracked as easy by brute force or some other method.	Enabled	Enabled
Store password using reversible encryption for all users in the domain **Reason:** Might as well store it in plain text if you use this one.	Disabled	Disabled

Under Account Policies -> Account Lockout Policy are the lockout recommendations for the network:

Password Policy Lockout Options	***Windows 2000 Workstation***	***Windows 2000 Server***
Account Lockout threshold **Reason:** A valid user should not take more than three times to log in.	3 invalid logon attempts	3 invalid logon attempts
Lockout Account Duration **Reason:** I want the user to have to notify the network team and request permission to reset it. What if it isn't that person?	30 Minutes	0/Forever
Reset account Lockout count after **Reason:** Make sure it gives the user time to type in three attempts before resetting the count.	15 Minutes	30 Minutes

On Windows 2000 systems you have the options for the following Kerberos Policy, which is only available if running Windows 2000 Servers for the domain controllers.

Kerberos Policy	***Windows 2000 Workstation***	***Windows 2000 Server***
Enforce User Logon Restrictions: When this option is enabled, the KDC validates every request for a session ticket to ensure the user has the right to log on Access to services. **Reason:** Verify user credentials	Enabled	Enabled
Maximum lifetime for Service Ticket: A "service ticket" is a session ticket. **Reason:** To ensure the session expires if not in use. (Remember this must be greater than 10 and less than the lifetime for a user ticket or it conflicts.) I set this to 10 hours for the server to match those users who work a long day and 2 hours on a laptop to force someone to reauthenticate.	120 Minutes	600 Minutes

Maximum Lifetime for User Ticket: A "user ticket" is a TGT and must be renewed after this time. **Reason:** Use guidelines for your work day and plus it up 1 or 2 hours. For local, this should be much shorter since users aren't logging on there. If it's a bad guy, we don't want to give them all day to play.	2 Hours	10 hours
Maximum Lifetime for User Ticket Renewal: This is the maximum lifetime of a ticket, No ticket can be renewed after this time. **Reason:** Limit the time before contact with the server has to be made.	7 Days	2 days
Maximum Tolerance for Computer Clock Synchronization: When the KDC clock off how many minutes from the client's clock, tickets are not issued for the client. **Reason:** This is a deterrent in Replay attacks. (Rice, David C and Sanderson, Mark J. "Guide to Securing Microsoft Windows 2000 Active Directory.")	5 minutes	Not Defined

Audits can consume enormous amounts of processor time and disk space. They should be chosen wisely.

Auditing Policy Options	***Windows 2000 Workstation***	***Windows 2000 Server***
Audit Account Management: Tracks changes such as when accounts are created, changed, or deleted. **Reason:** You want to know when any user rights are elevated, changed etc. and make sure it was authorized and the account is a valid account.	Success, Failure	Success, Failure
Audit Account Logon Events: Track logon events **Reason:** Who logged on where and when	Success, Failure	Success, Failure

Audit Logon Events: Tracks users who have logged on or off, or made a network connection. Also records the type of logon requested (interactive, network, or service). **Reason:** Track failures to record possible unauthorized attempts to break into the system.	Success, Failure	Success, Failure
Audit Directory Service Access: Monitor access to active directory. **Reason:** On workstations, no one is supposed to on locally and on servers, you want to monitor who get it. This is failures for normal activity however; I would switch this to success and failures if you suspect unwanted activity.	Failure	Failure
Audit Object Access :). **Reason:** Track unsuccessful attempts to access objects i.e. directories, files, and printers etc. However, remember to switch this to success and failures if you suspect unwanted activity	Failure	Failure
Audit Policy Change: Tracks changes in security policy **Reason:** You really want to know who changed it and why!	Success, Failure	Success, Failure
Audit Privilege Use: Tracks unsuccessful attempts to use privileges. Privileges indicate rights assigned to Administrators or other power users. **Reason:** This can be massive if successes are monitored, however do this if you have anything suspicious.	Failure	Failure
Audit Process Tracking: Tracks process and what is running. **Reason:** Due to data generated, track this only if something suspicious occurs.	No Auditing	No Auditing
Audit System Events: Tracks events that affect the entire system or the Audit Log. **Reason:** **KNOW** what is going on your system. Don't just say I guess that was normal, **FIND OUT** the cause!	Success, Failure	Success, Failure

In the User Rights Assignment section of the SCM: Right-click on the desired Attribute in the right frame, select Security.

Standard/Advanced User Rights **(All shaded areas represent advanced user rights)**	***Window 2000 Professional***	***Windows 2000 PDC and Member Servers***
Access this computer from Network **Reason:** Users have no need to access each other's workstations!	Administrators,	Administrators, users
Act as part of the OS **Reason:** Great damage could be done is someone could log on as the Operating system	(No one)	(No One)
Add workstations to the domain **Reason:** No one should be able to add a workstation with out proper authorization. Your network is only as secure as your weakest link.	(No one)	Administrators, account managers
Back up files and directories **Reason:** Keep this powerful privilege under control.	Administrators, Backup Operators,	Administrators, Backup Operators,
Bypass traverse **Reason:** Be careful of the restrictions set on these, you can stop some applications as well as your users.	Users Administrators	Users Administrators

Change the system time **Reason:** Users should never change their time, use a atomic clock, especially with Kerberos.	Administrators	Administrators
Create a pagefile **Reason:** Admin folks should handle this	Administrators	Administrators
Create a token Object **Reason:** No one should have this right, the system will handle it	No One	No One
Create permanent shared object **Reason:** We don't want our users sharing things out permanently and modifying their environment	No One	No One
Debug programs **Reason:** No one should be doing this.	No One	No One
Deny Access to this computer from the network **Reason:** Only as needed	No One	No One
Deny Logon as batch Job **Reason:** only as needed	No One	No One
Deny Logon as a Service **Reason:** only as needed	No One	No One

Deny Logon Locally **Reason:** This looks deceiving, however, if your users don't have a local account, they cannot log on.	No One	No One
Enable computer and user accounts to be trusted for delegation **Reason:** This should be done to match our active directory design.	No One	administrators
Force shutdown from a remote systems **Reason:** You don't want anyone shutting down your servers	Administrators	No one
Generate security audits **Reason:** This is up to the security team	No One	Security Group
Increase quotas **Reason:** Done as necessary	Administrators	Administrators
Increase scheduling priority **Reason:** Done as necessary	Administrators	Administrators
Load and unload device drivers **Reason:** Reserved for the admin group	Administrators	Administrators
Lock pages in memory **Reason:** You do not want to have pages data storage in this manner	No One	No One

Log on as a batch job **Reason:** NO ONE should do this	No One	No One
Log on as a service **Reason:** As needed per software package	As needed	As needed
Log on locally **Reason:** You are not allowed a local logon on domain controllers.	Administrators	NA
Manage auditing and security log **Reason:** security team only to ensure the integrity of the logs	security	security
Modify firmware environmental variable **Reason:** Only as necessary	Administrators	Administrators
Profile single process **Reason:** only as necessary	Administrators	Administrators
Profile system performance **Reason:** this should be by the admin team whose job is to monitor all of it.	Administrators	Administrators
Remove computer from docking station **Reason:** Only authorized people, doesn't apply to our servers	Administrators users	NA
Replace a process-level token **Reason:** This should be NO ONE	No One	No One

Restore files and directories **Reason:** Guard this privilege!! It should be only those in the backup operators group and administrators as a last resort	Administrators, Backup operators	Administrators, Backup operators
Shut down the system **Reason:** Make sure only admin can do this on the servers and ensure they have to log on first!!	Administrators, Authenticated users	Administrators, Authenticated users
Synchronize Directory service data **Reason:** Leave it alone and let the system handle it	No One	No One
Take ownership of files or other objects **Reason:** If it is not yours, you don't get to take ownership!! This should be audited!	Administrators	Administrators

The SCM Security Option section has many features. They can be modified in the registry, but it is recommended to use the SCM.

Security Attribute	***Windows 2000 Workstation***	***Windows 2000 Server***
Additional Restrictions for Anonymous Connections **Reason:** You need to decide this for your network, we are operating in native mode and will use 2	No Access without explicit anonymous permissions	Value of 2
Administrator Automatic Logon **Reason:** Do not allow someone to logon automatically if they get access.	Disabled	Disabled

Allow Server Operator to schedule tasks (Domain controller only) **Reason:** As needed	Not Defined	Not Defined
Allow system to be shutdown without having to logon **Reason:** Make sure a user is at the keyboard and knows how to log on. If this is not disabled and access is gained, you can shut down machines remotely	Disabled	Disabled
Allowed to eject removable NTFS Media **Reason:** Keep your data safe, only let administrator remove media	Administrators	Administrators
Amount of idle time required before disconnecting session **Reason:** if not in use, kill the session to prevent malicious behavior and just tying up your system	30 minutes	30 minutes
Audit the access of global system objects **Reason:** Know who is using your system!!!	Enabled	Enabled
Audit use of backup and restore privilege **Reason:** Monitor this all power privilege and know when it used	Enabled	Enabled
Automatically log off users when logon time expires **Reason:** Tailor this to the work hours of your company and make it a policy to request permission to be on the network past normal work hours.	Not Defined	enabled
Automatically log off users when logon time expires (local) **Reason:** Set this for local workstations, just as a security measure	Enabled	Enabled
CD-ROM Autorun **Reason:** Turn it off to prevent malicious code from being executed knowingly or unknowingly.	Disabled	Disabled
Clear virtual memory pagefile when system shuts down **Reason:** clear the data out of your system to protect it	Enabled	Enabled

Default User Screen Saver Active **Reason:** Make sure the users have a screen saver come on to protect data when not at their desk or not in use	Enabled	Enabled
Default User Screen Saver File **Reason:** We will use the logon.scr and force the users to log back on	logon.scr	Logon.scr
Default User Screen Saver Password Protected **Reason:** Make sure this is enabled	Enabled	Enabled
Default User Screen Saver Timeout Value **Reason:** This should be relatively short to help protect your data. Users get up and walk away with out locking the screen, you want it to lock very quick	300	300
Digitally sign client communication (always) **Reason:** We have a pure W2K environment, so we will require digital signatures	Enabled	Enabled
Digitally sign client communication (when possible) **Reason:** Already selected the above	Disabled	Disabled
Digitally sign server communication (always) **Reason:** Enable this since we have a pure W2K environment	Enabled	Enabled
Digitally sign server communication (when possible) **Reason:** Already selected the above	Disabled	Disabled
Disable CTRL+ALT+DEL requirement for logon **Reason:** Make the users press CTRL+ALT+DEL to help protect against Trojans that steal passwords	Disabled	Disabled
Do not display last user name in logon screen **Reason:** This is 50% of the key needed to access your resources, make everyone type it in each time.	Enabled	Enabled

Don't Save Dial-up Networking Password **Reason:** I just need physical access to your system if this is enabled. Make the users type it in everyone time, especially laptops!!!	Enabled	Enabled
Enable Option to Delete Roaming Profile Cache **Reason:** Make sure you have this enabled, don't keep your cache and all your activities and files	Enabled	Enabled
Generate 8.3 File Names **Reason:** Tailor it to your environment; we do not need it at GIAC enterprise.	Disabled	Disabled
LAN Manager Authentication Level **Reason:** Base this on your environment	Send LM & NTLM - use NTLMv2 session security if negotiated	Send LM & NTLM - use NTLMv2 session security if negotiated
Message text for users attempting to log on **Reason:** What ever is appropriate for your organization, it should warn about unauthorized access etc, see your lawyer.	GIAC NOTICE	GIAC NOTICE
Message title for users attempting to log on **Reason:**	GIAC TITLE	GIAC TITLE
Number of previous logons to cache (in case domain controller is not available) **Reason:** This gives anyone unauthorized access.	0 logons	0 logon
Prevent system maintenance of computer account password **Reason:** Let the password alone	Disabled	Disabled
Prevent users from installing printer drivers **Reason:** They could install something malicious, on purpose or by accident. This should be done only by the admin folks assigned to it.	Enabled	Enabled
Prompt user to change password before expiration **Reason:** Give them time to get ready and think about a new one	14 days	14 Days

Recovery Console: Allow automatic administrative logon **Reason:** Never allow this.	Disabled	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders **Reason:** Have a better recover plan	Disabled	Disabled
Rename administrator account **Reason:** Always and ensure you are logging on with separate accounts for all your administrators	Captain	Chief
Rename guest account **Reason:** Don't leave it the default name guest that everyone else does	Ted	Bill
Restrict CD-ROM access to locally logged-on user only **Reason:** Prevent access of your data from across the network	Enabled	Enabled
Restrict floppy access to locally logged-on user only **Reason:** Prevent access of your data from across the network	Enabled	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always) **Reason:** Always verify who's on the other end	Enabled	Enabled
Secure channel: Digitally encrypt secure channel data (when possible) **Reason:** N/A	Disabled	Disabled
Secure channel: Digitally sign secure channel data (when possible) **Reason:** N/a	Disabled	Disabled
Secure channel: Require strong (Windows 2000 or later) session key **Reason:** We want to be sure and protect our data	Enabled	Enabled
Secure system partition (for RISC platforms only) **Reason:** We do not use these at GIAC Enterprises	Not defined	Not defined
Send unencrypted password to connect to third-party SMB servers **Reason:** Don't ever send your password in the clear	Disabled	Disabled

Shut down system immediately if unable to log security audits **Reason:** This is key to stop unwanted attacks, but it can clue them they have been detected, lose data etc. We are going to shut down immediately	Enabled	Enabled
Smart card removal behavior **Reason:** If the card is taken out, the user should be forced to put it back it and it have to be locked.	Lock Workstation	Lock Workstation
Strengthen default permissions of global system objects (e.g. Symbolic Links) **Reason:** We need the global objects to have strong permissions. They have access to a lot of things.	Enabled	Enabled
Unsigned driver installation behavior **Reason:** Not all software manufactures are signing their drivers, especially other systems. We will allow it, but our GIAC policy says test first.	Warn but allow installation	Warn but allow installation
Unsigned non-driver installation behavior **Reason:** Not all software manufactures are signing their drivers, especially other systems. We will allow it, but our GIAC policy says test first.	Warn but allow installation	Warn but allow installation

Event Log Settings

Event Log Settings	***Windows 2000 Workstation***	***Windows 2000 Server***
Maximum application log size **Reason:** For the workstation, this will be set large enough to hold all of the information, but not take up too much room. The servers will be left at the max allowed to ensure they can collect everything	10048Kb	4194240Kb
Maximum security log size **Reason:** This is set large enough to hold at least a month's worth of data before it is over written. The security logs will be rotated daily by scripts. Workstations will be kept for six months and servers for 1 year to ensure they are not needed.	10048Kb	4194240Kb

Maximum system log size **Reason:** For the workstation, this will be set large enough to hold all of the information, but not take up too much room. The servers will be left at the max allowed to ensure they can collect everything.	10048Kb	4194240Kb
Restrict guest access to application log **Reason:** No one should be allowed to access the logs and given the ability to modify or hide what they are doing. Only administrators should have access to this log	Enabled	Enabled
Restrict guest access to security log **Reason:** No one should be allowed to access the logs and given the ability to modify or hide what they are doing. Only members of the security team should have access to this log	Enabled	Enabled
Restrict guest access to system log **Reason:** No one should be allowed to access the logs and given the ability to modify or hide what they are doing. Only administrators should have access to this log	Enabled	Enabled
Retain application log **Reason:** Workstations: we will have the logs over written every 30 days; all server logs will be kept and rotated.	30 days	Clear logs manually
Retain security log **Reason:** Workstations: we will have the security logs rotated off and stored for 6 months, all server logs will be moved off and kept for 1 year.	Clear logs manually	Clear logs manually
Retain system log **Reason:** Workstations: we will have the logs over written every 30 days; all server logs will be kept and rotated.	30 days	Clear logs manually
Retention method for application log **Reason:** workstations will be over written every 30 days, servers will be scripted to rotate the logs for processing	By days	Manual

Retention method for security log **Reason:** Both will be manual and kept for 6 months for workstations and 1 year for servers (All data will be filtered for anomalies)	Manual	Manual
Retention method for system log **Reason:** workstations will be over written every 30 days, servers will be scripted to rotate the logs for processing	By days	Manual
Shutdown the computer when the security audit log is full **Reason:** If an event is taking place that is bad, we need to know and stop it, however, shutting down the system can get rid of valuable information in an investigation. The logs should be watched regularly for unauthorized access, but a real live person should make the call to shut the system down.	Disabled	Disabled

Ensure that in the SCM template that all the settings for the registry are set to ignore all except those specifically mentioned.
The following table shows NSAs guidance on the setting of permissions for the registry and those for GIAC Enterprises: (Rice and Sanderson, "Guide to Securing Microsoft Windows 2000 Active Directory.") I cannot encourage you enough to thoroughly TEST the settings before applying them! They can have an adverse effect on software, devices etc!! (This comes from first hand experience!) Some of the recommended settings for GIAC Enterprises have been modified based on their needs and testing.

REGISTRY KEY	USER GROUPS	***NSA'S RECOMMENDED PERMISSIONS***	***GIAC Enterprises RECOMMENDED PERMISSIONS***
CLASSES ROOT\ Key and Subkeys **Reason:** It controls all of your software settings and functionality. All of your links are here for your DLLs as well.	Administrators Creator Owner System Users	Full Control Full Control (Subkeys only) Full Control Read Replace	Full Control Read, Execute Full Control (subkeys only) Read Replace

MACHINE\ **Reason:** Controls the configuration of the local machine. Critical to security for who has access	Administrators Creator Owner System Users	Full Control (This key only) Full Control (Child objects only) Full Control (This key only) Special (This key only)(Query, Set, Create subkey, Enumerate, Notify, Delete, Read perms) Propagate	Full Control (This key only) Full Control (Child objects only) Full Control (This key only) Special (This key only)(Query, Set, Create subkey, Enumerate, Notify, Delete, Read perms) Propagate
\MACHINE\SOFTWARE **Reason:** Controls the software on the local machine	Administrators Creator Owner System Users	Full Control Full Control (Subkeys only) Full Control Read Replace	Full Control Full Control (Subkeys only) Full Control Read Replace
\MACHINE\SOFTWARE\Microsoft\NetDDE **Reason:** Controls the shares for communication channels	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace
\MACHINE\SOFTWARE\Microsoft\ OS/2 Subsystem for NT **Reason:** Can allow a process to persist even across a login. There are several vulnerabilities dealing with this.	Administrators Creator Owner System	Full Control Full Control (Subkeys only) Full Control Replace	DELETE THE KEY
\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib key and subkeys **Reason:** Controls the performance monitor (See Microsoft's Q article Q226494)	Administrators Creator Owner System Interactive	Full Control Full Control Full Control Read Replace	Full Control Full Control Full Control Read Replace
\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\group policy Keys and subkeys **Reason:** Controls the group policy settings	Administrators Authenticated Users System	Full Control Read Full Control Propagate	Full Control Read Full Control Propagate

\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\installer **Reason:** Controls the installer for software packages	Administrators Authenticated Users System	Full Control Read Full Control Propagate	Full Control Read Full Control Propagate
\MACHINE\SYSTEM **Reason:** Controls all the system capabilities, drivers, etc	Administrators System Creator Owner Users	Full Control Full Control Full Control (Subkeys Only) Read Replace	Full Control Full Control Full Control (Subkeys Only) Read Replace
\MACHINE\SYSTEM\CurrentControlSet001 – 010 **Reason:** All the different configurations of the system	Administrators Creator Owner System Users	Full Control Full Control (Subkeys only) Full Control Read Propagate	Full Control Full Control (Subkeys only) Full Control Read Propagate
\MACHINE\system\CurrentControlSet\control\securepipeservers\winreg **Reason:** Controls remote system access to the registry	Administrators Backup Operators System	Full Control Read (This key only) Full Control Replace	Full Control Read (This key only) Full Control Replace
\MACHINE\system\CurrentControlSet\hardware profiles **Reason:** all the user profiles on the system	Administrators Creator Owner System Users	Full Control Full Control (Subkeys only) Full Control Read Propagate	Full Control Full Control (Subkeys only) Full Control Read Propagate
\USERS **Reason:** Users key of the registry, controls what they can and can't do	Administrators Authenticated Users Creator Owner System	Full Control (This key only) Read (This key only) Full Control (Child objects only) Full Control (This key only) Propagate	Full Control (This key only) Read (This key only) Full Control (Child objects only) Full Control (This key only) Propagate
USERS\.DEFAULT **Reason:** Default user profile	Administrators Creator Owner System Authenticated Users	Full Control Full Control (Subkeys only) Full Control Read Replace	Full Control Full Control (Subkeys only) Full Control Users: Read Replace

USERS\.DEFAULT\Software\ Microsoft\NetDDE **Reason:** Controls the shares for communication channels	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace

There are several files and folders that need to have their security settings modified. The following table shows NSA's recommendations (Rice and Sanderson, "Guide to Securing Microsoft Windows 2000 Active Directory.") and the ones for GIAC Enterprises. Folders and files not explicitly listed below are assumed to inherit the permissions of their parent folder.

- %SystemDrive% - The drive letter on which Windows NT is installed.
- %SystemRoot% - The folder containing the Windows NT operating system files
- %SystemDirectory% - %SystemRoot%\system32

FOLDER OR FILE	USER GROUPS	***NSA'S RECOMMENDED PERMISSIONS***	***GIAC'S RECOMMENDED PERMISSIONS***
%ProgramFiles% **Reason:** All of the software programs are there and it should not be modified easily.	Administrators Creator Owner System Users	Full Control Full Control (Subfolder and files only) Full Control Read Execute Replace	Full Control Full Control (Subfolder and files only) Full Control Read Execute Replace
%SystemDirectory% **Reason:** All of the system files and folders are here	Administrators Creator Owner System Users	Full Control Full Control (Subfolder and files only) Full Control Read Execute Replace	Full Control Full Control (Subfolder and files only) Full Control Read Execute Replace
%SystemDirectory%\dllcache **Reason:** All of the files for the OS controls are here. If someone replaced one or modified it could be very bad	Administrators Creator Owner System	Full Control Full Control Full Control Replace	Full Control Full Control Full Control Replace
%SystemDirectory%\GroupPolicy **Reason:** The effects of this being modified could alter your security settings or expose them.	Administrators Authenticated Users System	Full Control Read Execute Full Control Propagate	Full Control Read Execute Full Control Propagate

%SystemDirectory%\Ntbackup.exe file **Reason:** Runs the backup of all files as system	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace
%SystemDirectory%\rcp.exe file **Reason:** A form of the UNIX utilities that allow you to copy files	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace
%SystemDirectory%\Regedt32.exe **Reason:** Executable to run the registry editor	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace
%SystemDirectory%\repl **Reason:** Replication folder	Administrators System Users	Full Control Full Control Read Execute Propagate	Full Control Full Control Read Execute Propagate
%SystemDirectory%\repl\export **Reason:** Holds the replication folders/data for outgoing	Administrators Replicator System Users	Full Control Read, Execute Full Control Read Execute Propagate	Full Control Read, Execute Full Control Read Execute Propagate
%SystemDirectory%\repl\import **Reason:** Holds the replication folders/data for incoming	Administrators Replicator System Users	Full Control Modify Full Control Read Execute Propagate	Full Control Modify Full Control Read Execute Propagate
%SystemDirectory%\rexec.exe file **Reason:** Another UNIX type utility which lets you execute a command on another system	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace
%SystemDirectory%\rsh.exe file **Reason:** Let's you run a program on another system and view the outcome/results on yours	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace
%SystemDirectory%\secedit.exe **Reason:** Runs the security configuration manager	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace

%SystemDirectory%\spool\printers **Reason:** You can do a lot of data capturing and redirecting here.	Administrators Creator Owner System Users	Full Control Full Control (Subfolder and files only) Full Control Special (This folder and subfolders)(Traverse/ Execute, Read attribs, Read Ext Attribs, Create Files/Write Data, Createfolders/Append Data) Replace	Full Control Full Control (Subfolder and files only) Full Control Special (This folder and subfolders)(Traverse /Execute, Read attribs, Read Ext Attribs, Create Files/Write Data, Createfolders/Appe nd Data) Replace
%SystemDrive%\ **Reason:** Who has access to the system	Administrators Creator Owner System Users	Full Control Full Control (Subfolders and files) Full Control Read Execute Propagate	Full Control None Full Control Read Execute Propagate
%SystemDrive%\Documents and Settings **Reason:** Controls all of the users and their profile	Administrators System Users	Full Control Full Control Read Execute Propagate	Full Control Full Control Read Execute Propagate
%SystemDrive%\Documents and Settings\Administrator **Reason:** The administer profile and all of the administrator tools	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace

%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson **Reason:** Controls error handling	Administrators Creator Owner System Users	Full Control Full Control (Subfolders and files only) Full Control Traverse Folder, create files, create folders (Sub folders and files) Read Execute	Full Control Full Control (Subfolders and files only) Full Control Special (Subfolders and files only)(Traverse/Execute, Create files/Write data, Create subfolders/Append data) Special (This folder, subfolders and files)(Traverse/Execute, List folder/Read data, Read Attribs, Read Ext Attribs, Read permissions) Replace
%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log **Reason:** The system error logs	Administrators Creator Owner System Users	Full Control Full Control Full Control Modify Replace	Full Control Full Control Full Control Modify Replace
%SystemDrive%\io.sys **Reason:** Used during startup	Administrators System Users	Full Control Full Control Read, Execute Replace	Full Control Full Control Read, Execute Replace
%SystemDrive%\msdos.sys **Reason:** Used as part of the command prompt	Administrators System Users	Full Control Full Control Read, Execute Replace	Full Control Full Control Read, Execute Replace
%SystemDrive%\My Download Files **Reason:** Files that are downloaded and used by the users. IF this is the default location, no one should have access to it.	Administrators Creator Owner System Users	Full Control Full Control (Subfolder and files only) Full Control Read Write Execute Replace	Full Control Full Control (Subfolder and files only) Full Control Read Write Execute Replace

%SystemDrive%\System Volume Information **Reason:** All the information about your hard drive	Ignore	Ignore	Ignore
%SystemDrive%\Temp **Reason:** Used as a storage and retrieval place for software programs, unpacking etc.	Administrators Creator Owner System Users	Full Control Full Control (Subfolder and files only) Full Control Special (This folder and subfolders)(Traverse/ Execute, Create files, Create folders) Replace	Full Control Full Control (Subfolder and files only) Full Control Special (This folder and subfolders)(Traverse /Execute, Create files, Create folders) Replace
%SystemRoot% **Reason:** The key to your OS	Administrator Creator Owner System Users	Full Control Full Control (Subfolder and files only) Full Control Read Execute Replace	Full Control Full Control (Subfolder and files only) Full Control Read Execute Replace
%SystemRoot%\regedit.exe **Reason:** Older version before regedt32 to make registry changes	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace
C:\autoexec.bat **Reason:** a script file that can be executed on startup or any other time	Administrators System Users	Full Control Full Control Read Execute Replace	Full Control Full Control Read Execute Replace
C:\boot.ini **Reason:** Runs during startup and controls what OS gets booted	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace
C:\config.sys **Reason:** another system file used during startup	Administrators System Users	Full Control Full Control Read Execute Replace	Full Control Full Control Read Execute Replace

C:\ntbootdd.sys **Reason:** "When using the scsi() syntax in the BOOT.INI, Windows NT needs to load a SCSI device driver and uses that driver to access the boot partition. The SCSI controller driver is renamed NTBOOTDD.SYS and placed in the root of the system partition" (Microsoft Q article, Q178278)	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace
C:\ntdetect.com **Reason:** Controls the viewing of hardware/system information during bootup	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace
%SystemDirectory%\Secedit.exe **Reason:** This is the security editor	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace
C:\ntldr **Reason:** Used during bootup	Administrators System	Full Control Full Control Replace	Full Control Full Control Replace

Additional Security Practices

1. Install and run Passprop to eliminate unauthorized attempts at the administrator password. It does not lock it out at the console. For more information on PassProp, query on this key word

2. To fully prevent any OS/2 or POSIX based attacks, all registry keys dealing with these subsystems must be removed. Even if the subsystem executables have been removed form the %SystemRoot%\system32 folder, the subsystem could be reactivated if the registry keys still exist.

   Remove the following registry keys:

   Hive: HKEY_LOCAL_MACHINE
   Key: \System\CurrentControlSet\Control\SessionManager\Environment
   Name: Os2LibPath
   Entry: Delete Entry

   Hive: HKEY_LOCAL_MACHINE

Key: \System\CurrentControlSet\Control\SessionManager\Subsystems
Name: Optional
Entry: Delete Entry

Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Control\SessionManager\Subsystems
Name: OS2 and POSIX
Entry: Delete Entries for both OS2 and POSIX

Hive: HKEY_LOCAL_MACHINE
Key: \Software\Microsoft\OS/2 Subsystem for NT
Name: OS/2 Subsystem for NT
Entry: Delete entire key

REBOOT AFTER MAKING CHANGES (Make sure you tell users for the servers. You probably want to do this after hours.

3. There are several folder permissions that must be set manually. Several files related to the OS/2 and POSIX subsystems must be removed. The OS2 and POSIX subsystems in Windows 2000 can introduce security vulnerabilities to the operating system. Just query the internet on either subsystem and you'll have more information than you can read. Therefore, do a search and remove the following:
    a. os2.exe
    b. os2ss.exe
    c. os2srv.exe
    d. psxss.exe
    e. posix.exe
    f. psxdll.dll
    g. \os2 folder
    h. \%SystemDrive%\Dos folder

4. It is important to check file permissions on shared folders. By default, permissions on a share give the Everyone group Full Control; therefore, you must explicitly edit security permissions on shared resources to limit share access

5. Remote Registry access is controlled by applying permissions to the REGEDT32.exe. These permissions will also be assumed for remote registry access.

6. The following registry key will be added to help prevent SYN attacks:

Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Services\Tcpip\Parameters
Name: SynAttackProtect
Type: REG_DWORD

Entry: 2

7. The following registry key will be added to help save bandwidth: This is key with the firewall in place.

   Hive: HKEY_LOCAL_MACHINE
   Key: \System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\[Interface Name]
   Name: PerformRouterDiscovery
   Type: REG_DWORD
   Entry: 0

8. The following registry key will be added to disable IP routing:

   Hive: HKEY_LOCAL_MACHINE
   Key: \System\CurrentControlSet\Services\Tcpip\Parameters
   Name: DisableIPSourceRouting
   Type: REG_DWORD
   Entry: 1

9. The following registry key will be added to Stop ICMP redirects and possible other DOS:

   Hive: HKEY_LOCAL_MACHINE
   Key: \System\CurrentControlSet\Services\Tcpip\Parameters
   Name: EnableICMPRedirects
   Type: REG_DWORD
   Entry: 0

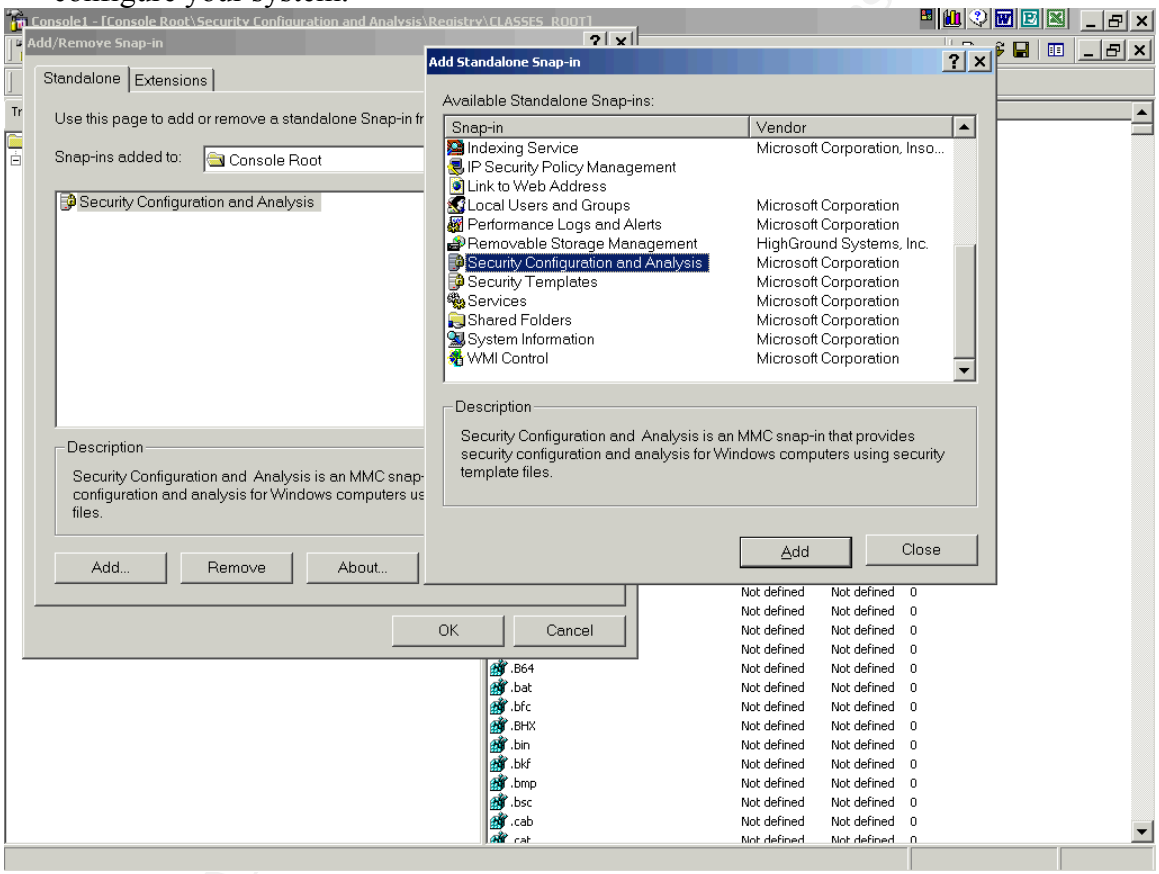
10. The following registry key will be added to disable 8.3 Filename creation:

    Hive: HKEY_LOCAL_MACHINE
    Key: \System\CurrentControlSet\Control\Filesystem
    Name: NTFSDisable8dot3NameCreation
    Type: REG_DWORD
    Entry: 1

11. **AN IMPORTANT NOTE!!!!!**  **When using permissions, the deny permissions take precedence over the allow permissions. Example, if a file is set to give the Administrators full control and the users group to deny all, then the administrators will not be able to get into it either. This is because the administrators are also a part of the user's group and the deny overrides everything else!!! BE VERY CAREFUL!!!**

GIACNT: Citation of Sources

12. Ensure all service packs and hot fixes have been tested and applied. Do not just install them because they came out. Read what they do and determine if you need to install it. It is important to track the order in which they were applied. They need to be removed in reverse order as they were put on the system.
13. The Security Configuration Manager (SCM) is included in the W2K interface. To access it, go to run and type MMC. You want to go to add/remove snapins and select Security Configuration Manager. This gives you another way to build templates and configure your system.



14. NSA has preset template for the SCM. This allows their setting recommendations to be applied to the system. Some of their settings are too restrictive and not practical under normal conditions. You cannot just apply a template or setting. You need to know what it is doing and ensure it will not disrupt your organization. It can be difficult to trouble shoot what went wrong.

15. Auditing is extremely important. We will be using W2K's built in feature for the desktop for this feature, however, the capability exists in NT. It is important to audit only what is necessary as it takes up a lot of resource time and space on the PC.

16. The right to perform backups, identified by users in the Backup Operators group, is one of the most powerful rights that administrators can assign. Backup operators are able to read and write to any file in the system, regardless of the rights assigned to it. **This right should be granted only when there is a clear need for it, even then, it should be limited to only a few trusted users.** Members of the Backup Operators group should have special logon accounts, not regular user accounts. Restrictions should also be set on the backup account, such as forcing the user to log on from a particular system only during appropriate hours.

17. The following is a list of account policies that should be implemented on the domain controllers:

    a. Remove group accounts. Only if necessary should this be in use. You CANNOT identify who it is with a group account.
    b. Set a password for the renamed Guest account and disable it. The built in guest account should be renamed and then also place a 14 character/numeric password on it. Even if the account was found and a hacker enabled it, they would still have to crack the password.
    c. Create a decoy "administrator" account. This provides a way of checking for attacks. Audit the fake administrators account. It should be a member of the guests or domain guests group, be disabled and have a long, complex password on it.
    d. Administrators should not be allowed to surf the web from a server.
    e. Ensure the daily policing up of the servers are done. As soon as users are gone, they need to be removed from the server.
    f. Local users should not exist on workstations. They need to be forced to authenticate through the domain.
    g. The built-in Guest account, Everyone group, Guests group, Domain Guests group will not have the right to access **this computer from the network.**
    h. The built-in Guest account, Everyone group, Guests group, Domain Guests group will not have the right to access **log on locally.**
    i. Individual and group accounts will not have the right to **act as part of the operating system.** If a program has the need to have this right or other special rights outside of these, it is important to document these accounts and identify them clearly. These accounts need to have passwords that are the maximum length, follow strong password rules and be kept in a secure container accessible only the ISSO.
    j. Finger is a TCP/IP utility used to obtain information about a user account via a remote system. It can leave the system open to denial of service attacks.

18. The following are a list of additional tools placed on the system to help with analysis and available only to the administrators:
    a. Cybersafe Log Analyst: Used to create and view reports in the event logs.

b. Internet Scanner from ISS:  This tool is included with the resource kit. DO NOT USE IT!!! It is broken. To load the scanner, use software purchased for that purpose. (RCERT, Fort Huachuca, Arizona)

Conclusion

In order to successfully support GIAC Enterprises, the Active Directory design had to support the needs of the company without violating the defense in depth network design. The overall concept of implementing an active directory infrastructure is not complicated, however what happens when you put up a couple of firewalls, and a router with a site on the other side? Suddenly it is not that simple anymore. With the advent of VPNs, the company boundaries have expanded and must keep up with the pace demanded. Securing and implementing an Active Directory infrastructure takes much planning and thinking up front, but will save you huge about of time and money later.

Citation of Sources

Abreu, Elinor Mills. "New Year, New Web Attacks." 26 December 2001. URL: http://abcnews.go.com/sections/scitech/dailynews/virusoutlook011226_wire.html (27 December 2001).

"Active Directory Architecture." 2 March 2000. URL: http://www.microsoft.com/windows2000/techinfo/howitworks/activedirectory/adarch.asp (29 December 2001).

"Active Directory Users, Computers, and Groups." February 2000. URL: http://www.microsoft.com/windows2000/techinfo/howitworks/activedirectory/adusers.asp (29 December 2001).

"Dell – PowerVault Storage Area Network." 2001. URL: http://www.dell.com/us/en/fed/products/seriers_sanet_storage.htm (18 September 2001).

"Events for Performance Monitor Extensions (Q226494)" 1 September 1999. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q226494 (6 January 2002)

"Everything You Need to Know about Network Security." 1999. URL: https://enterprisesecurity.symantec.com/content/TrialwareForm.cfm?PID=8535439&PDFID=32&PromoCode=SymEsForm&SSL=YES (28 August 2001).

Extreme Networks Quick Reference Guide. 2000.

ExtremeWare Software User Guide V6.1. April 2000.

Fossen, Jason. "Track 5 Securing Windows 2000." SANS Institute. 2001.

Longoria, Gerald. "Resolving Data Storage Demands with SANs." 2000. URL: http://www.dell.com/us/en/esg/topics/pwer_ps1q00-sans.htm (24 August 2001)

Northcutt, Stephen; Kessler, Gary; Pomeranz, Hal. Track 2—LevelTwo Firewalls, Perimeter Protection, and Virtual Private Networks. SANS Institute, 2001.

"PowerVault Storage Area Network (SAN) Version 4.05." April 2001. URL: http://www.dell.com/downloads/us/pvaul/san_405_infobrief.doc (24 August 2001).

Rice, David C and Sanderson, Mark J. "Guide to Securing Microsoft Windows 2000 Active Directory." National Security Agency. December 2000.

Riley, Steve "Active Directory Replication Over Firewalls." March 2001. URL: http://www.microsoft.com/Technet/ittasks/tasks/adrepfir.asp (13 December 2001).

"Security on IP Networks Countering Denial of Service (DOS) Attacks." URL: http://www.extremenetworks.com/technology/whitepapers/security.asp (24 August 2001).

"Step By Step Guide to Managing Active Directory." 9 February 2000 URL: http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/manadsteps.asp (29 December 2001).

Sunday, Larry. Information Assurance Raptor Management Console Firewall Training Class Part I and II. 2001.

Symantec Enterprise Firewall and Symantec Enterprise VPN Reference Guide Version 6.5. April 2001.

"Symantec Enterprise Firewall Formerly Raptor Firewall." April 2001. URL: http://enterprisesecurity.symantec.com/pdf/axentpdfs/sym_enterprisefw_factsheet.pdf?PID=8535439 (28 August 2001).

"With Cpqarray.sys, the Boot Partition cannot Extend Beyond 1023 Cylinders (Q178278)." 1 May 1998. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q178278 (6 January 2002)