Global Information Assurance Certification Paper

Design a Secure Windows 2000 Infrastructure

GCWN Practical Assignment

Presented to: SANS/GIAC
Version 3.1 – Option 1

Submitted by: Mason Karrer

8 November 2002

Table of Contents

List of Figures

List of Tables

1.0. Introduction

This document describes a secure Microsoft Windows 2000 Active Directory network for GIAC Enterprises. GIAC is a business specializing in the sale of online fortune cookie sayings.

GIAC Enterprises has two operational offices and several remote sales offices located worldwide. This document focuses on the design considerations for GIAC's internal network and is comprised of the following main elements:

Company Overview – A brief description of GIAC's various business units and departments. Included are the size of the departments and their basic computing requirements.

Network Design and Diagram – This section details GIAC's internal network. Included are the physical/geographical layout of GIAC's business centers, location of key servers and basic network architecture.

Active Directory Design and Diagram – Active Directory logical and physical network structures are offered here including a diagram. A brief explanation of the role of each logical object is also included.

Group Policy and Security Design – This section outlines the suggested Group Policy Objects to be created and the policy settings associated with them. The emphasis of this Group Policy design is on security.

2.0. Overview of GIAC Enterprises

GIAC Enterprises is a smaller corporation with approximately 100 employees. The main operational office is in Kansas with a research facility in Colorado and several remote sales offices located throughout the United States and abroad. The company is comprised of the following departments:

Department: Sales (In-house)
Location: Kansas
Employees: 30
Description: The in-house sales department is responsible for developing leads and generating business within the greater Midwest region. Although some travel is required these sales representatives will spend the majority of their time in the office.

Department: Sales (Remote)
Location: Kansas
Employees: 30
Description: The remote sales departments' focus is on both coasts and abroad. They typically work out of their homes and connect to the GIAC network via VPN over a broadband connection to the Kansas site. When traveling they will need to rely on dial-up if no broadband access is available.

Department: Marketing
Location: Kansas
Employees: 5
Description: The marketing department has little technical demand besides Apple hardware. Marketing employees typically require email, word processing and desktop publishing applications. Their work is stored on a general file server in a 'Marketing' share.

Department: Finance
Location: Kansas
Employees: 10
Description: Finance has a high technical demand including encryption and heavy printing loads. They are responsible for all accounts payable, receivable and payroll duties. The finance department resides in a physically restricted zone.

Department: Human Resources
Location: Kansas
Employees: 5
Description: HR is also in a physically restricted zone. However most HR records are stored on paper in locked file cabinets. The only technical requirements in HR are the ability to digitally sign and encrypt email and print securely.

Department: Research & Development
Location: Colorado
Employees: 10
Description: R&D is primarily responsible for delivering the fortune product to market. This is done via a web server that hosts the fortune cookie saying website. R&D has authored a software application for presenting the fortunes to customers. The software is proprietary and the source code must be protected as R&D is consistently striving to improve the product. R&D resides in a separate city and on a separate network. Their main requirements of the rest of the network are Internet and email.

Department: Technical Support
Location: Kansas
Employees: 10
Description: Technical Support (including the Help Desk) is responsible for all server and desktop administration. TS is also charged with maintaining 99.9% network uptime. While located in Kansas the employees of this department must be able to remotely connect to machines around the world for administrative purposes.

Department: Executive Staff
Location: Kansas
Employees: 7
Description: This department is comprised of the managers of the other departments and the president of GIAC. This department is unique because despite best security practices they insist on remaining exempt from certain requirements like tough passwords and other restrictions. They have been urgently discouraged against this practice; however since they are in charge (and ultimately responsible) they get what they want.

3.0. Network Design and Diagram

This section describes the network design. Included is a detailed logical diagram of GIAC's proposed network (Figure 3.1.)

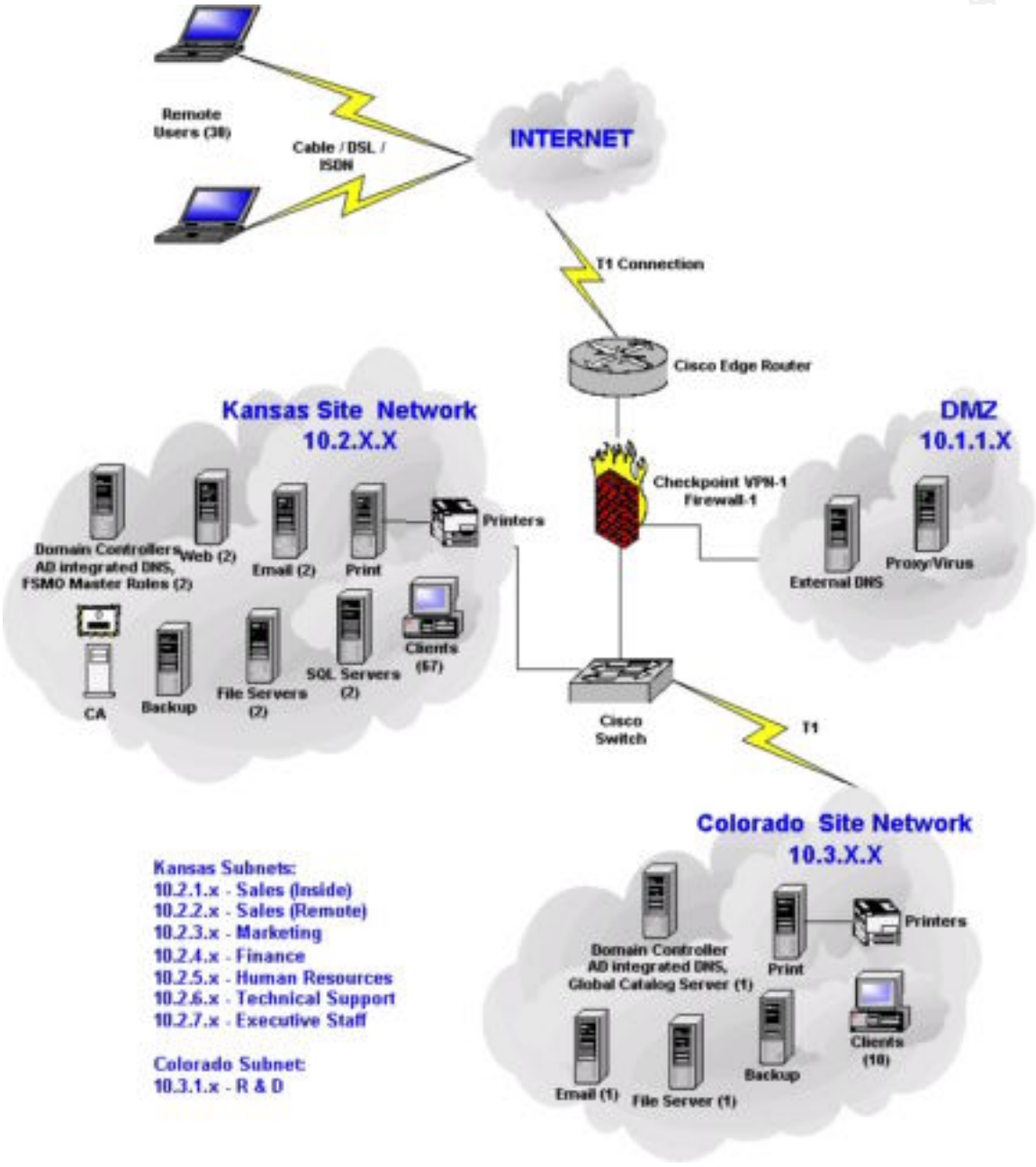

Figure 3.1 – GIAC Network Logical Diagram

3.1. Network Overview

The proposed network for GIAC is comprised of two physical sites (Kansas and Colorado.) All inter-office traffic is 100 Mbps Ethernet over Category-5 Cable. Plenum cable is used for extra fire retardation when needed. Two dedicated T1's are in place for Internet and WAN traffic respectively.

The Kansas site consists of an internal corporate network and a perimeter network also known as a DMZ (demilitarized zone). Kansas is also the sole gateway to the Internet. Two domain controllers in Kansas provide DC redundancy and share all FSMO (Flexible Single Master Operation) Master roles. An Intermediate Certificate Authority server along with various file, print, web and email servers also reside in Kansas.

A smaller branch office network for the Research and Development department is located in the Colorado site. File, print, email and backup servers are present along with a single domain controller configured as a Global Catalog Server. In the event that the WAN link between sites goes down the R&D employees will still be able to log on, access their files and print. Although they will not have email service per se, they will be able to work offline and synchronize their mail traffic with the Exchange server in Kansas once the WAN link is reestablished.

3.2. Network Subnets

Each department is assigned a unique subnet and each user within that department is assigned a static IP. Below is a reprint of each department along with its corresponding subnet.

Department: Sales (In-house)

Location: Kansas
Subnet: 10.2.1.x

Department: Sales (Remote)

Location: Kansas
Subnet: 10.2.2.x

Department: Marketing

Location: Kansas
Subnet: 10.2.3.x

Department: Finance

Location: Kansas
Subnet: 10.2.4.x

Department: Human Resources

Location: Kansas
Subnet: 10.2.5.x

Department: Technical Support

Location: Kansas
Subnet: 10.2.6.x

Department: Executive Staff

Location: Kansas
Subnet: 10.2.7.x

Department: Research & Development

Location: Colorado
Subnet: 10.3.1.x

3.3. Server and Workstation Overview

Note: 'Workstation' denotes in-house desktop PC's and remote laptops. All workstations feature the Windows 2000 Professional operating system with all service packs, patches and hotfixes applied. The reader can assume that all hardware is new and has enough processor speed, RAM and hard drive space that all normal desktop and network utilization requirements are easily handled.

Additionally,

- All servers reside in-house in a physically restricted space with separate air-handling and fire suppression systems.
- All servers are Compaq Proliant series and feature the Microsoft Windows 2000 Server operating system. Windows 2000 Advanced Server has been implemented wherever load balancing is required. (Compaq's are preferred because they are extremely reliable, easy to work on and readily available through GIAC's hardware vendor.)
- All systems are configured as RAID-5.[1]
- All disk drives (server and workstation) are formatted as NTFS.[2]
- All machines (server and workstation) are kept up-to-date with the latest service packs and patches.
- All web servers have been hardened using the IIS lockdown tool.[3]
- IIS has been removed from all servers not requiring it.
- All critical systems are backed up regularly to tape. Tapes are stored offsite at a secure location.

3.3.1. Server Inventory

Below is a list of all servers and their roles.

Kansas Servers

KS_BACKUP – Kansas Backup Server

KS_CA – Kansas Certificate Authority Server
- Intermediate (issuing) CA

KS_DC1 – Kansas Domain Controller
- Domain Naming Master
- Schema Master
- Global Catalog Server

KS_DC2 – Kansas Domain Controller
- PDC Emulator Master
- RID Master
- Global Catalog Server

KS_EMAIL1 – Primary Email Server
- Exchange 5.5
- Outlook Web Access (OWA)

KS_EMAIL2 – Secondary Email Server
- Exchange 5.5

KS_FINandHR – Finance and Human Resources (HR) File Server
- Finance and HR shares are restricted to respective groups

KS_PRINT – Kansas Print Server

KS_SandM – Sales and Marketing File Server
- Sales and Marketing shares are restricted to respective groups

KS_SQL1 and KS_SQL2 – Internal database servers providing online fortune requests from DMZ_WEB. All fortunes and online transaction data are stored on these servers. These servers are load-balanced for performance enhancement and are redundant. In the event that one of the servers is lost then all requests will failover to the operational server.

KS_WEB1 and KS_WEB2 – Web Servers – load balanced and redundant
- IIS 5.0

DMZ Servers

DMZ_DNS – External DNS Server

DMZ_VIRUS_PROXY – Company wide virus protection and proxy server
- Trend Micro Virus Scanner
- Microsoft ISA Server

Colorado Servers

CO_BACKUP – Colorado Backup Server

CO_DC1 – Colorado Domain Controller
- Global Catalog Server

CO_EMAIL1 – Primary Email Server
- Exchange 5.5

CO_PRINT – Colorado Print Server

CO_RandD – Research and Development File Server
- Restricted to R&D group

3.3.2. Domain Controllers and FSMO Master Roles

GIAC has three (3) domain controllers in total. Two are located in Kansas and one in Colorado. The Colorado DC is configured as a Global Catalog Server but does not fulfill any of the FSMO Master Roles. These are shared between the Kansas DC's in the following manor:

KS_DC1
- Domain Naming Master (one per enterprise)
- Infrastructure Master (one per enterprise)
- Schema Master (one per enterprise)

KS_DC2
- PDC Emulator Master (one per domain)
- RID Master (one per domain)
- Global Catalog Server (**not a FSMO Master Role**)

There is a maximum allowable of one per domain for the PDC Emulator Master, RID (Relative ID) Master and Infrastructure Master. Conversely there is a maximum allowable of one per enterprise for the Schema Master and Domain Naming Master.

These maximums are imposed as part of the Microsoft NT Architecture model. The following excerpt on Global Catalog servers comes from a SANS institute training manual (Reference 4, pg 37.)

"The Global Catalog is not a separate database from AD. Rather, some AD data is simply marked as being part of the catalog and some are not."

-And-

"Under normal circumstances, a native-mode user must be able to contact a GC server in order to log on…"

Thus at least one Global Catalog Server (GC) must be available for a user to log on to the network. Therefore one GC appears in each site for redundancy. Technically all DCs can be GCs but the bandwidth required for replicating this data between all DCs can quickly become overbearing.

It is desirable to share the FSMO roles in a certain fashion between multiple DCs. Specifically the Infrastructure Master should not also be a Global Catalog Server.

"This setup will cause the Infrastructure Master to never find bad references." (Reference 4, pg 39)

3.4. DMZ Equipment

The purpose of a DMZ is to separate the corporate LAN from other public servers (like those located on the Internet.) By erecting a DMZ a buffer zone is established that disallows traffic to flow directly from the Internet into the corporate network. The servers in the DMZ are not allowed to join the internal domain and therefore are unaware of the internal resources. In this manner they are unable to initiate sessions with machines on the LAN; only forward packets that were previously requested. Thus even if attackers subvert outward facing machines in the DMZ they cannot glean any information about the internal network. The DMZ machine(s) will likely need to be rebuilt if this occurs however.

Point of contention: It is argued that a true DMZ consists of machines that lie outside the firewall. However at GIAC the DMZ resides behind the firewall as a security measure. With this placement the firewall can be used as an initial shield thereby limiting the DMZ's exposure to unwanted traffic.

3.4.1. Domain Name System Services

DNS services are provided through Microsoft Windows 2000. Since GIAC is exclusively a Windows 2000 native environment Microsoft's Dynamic DNS service negates the need for separate WINS and NetBIOS. These services can then be disabled.

A separate (external) DNS server resides in the DMZ for all outward facing devices. This allows GIAC to host its own DNS records. In general this is how it works:

Allowable inbound traffic travels through the firewall for processing. The external DNS server performs a lookup for the destination address of the recipient and returns it to the sender which then properly addresses and sends the data payload. If the packet is destined for a machine on the DMZ (like a request from the Internet for a corporate web page) then the request is forwarded to DMZ_WEB. Otherwise it is forwarded to the firewall which performs NAT (network address translation) on the packet for processing by the internal DNS server and distribution to the appropriate destination. Outbound traffic works in an opposite fashion.

Note: NAT (Network Address Translation) is a method used to deliver packets from the outside world to internal network destinations without revealing anything about the internal network (RFC1631).[5] It works by 'hiding' all of the internal addresses behind an external address and then translating between the two. All internal addresses follow either the '10.x.x.x' or '192.168.x.x' subnet scheme. Neither of these subnets is routable on the Internet. By setting these subnets aside the same TCP/IP technology used to route packets on the Internet can be used to route internally thereby streamlining the data flow. It is much like receiving paper mail at an office. The sender of the letter only knows the street address not the exact location of the recipient within the business. The firewall "NAT'ing" a packet is like the mail room employee marking the letter with the floor, office number, etc. so it can be delivered to the recipient's office.

3.4.2. Antivirus and Proxy

GIAC utilizes a TrendMicro antivirus product. This product requires a dedicated server which automatically downloads current virus and spam pattern files. The machine sits on the DMZ and acts as a mail scanning gateway. When the firewall receives SMTP traffic it redirects it to the virus scanning device which inspects and cleans the message and then forwards it to the internal Exchange server for distribution.

Proxy services are provided via Microsoft's ISA Server configured as a forward proxy server. The proxy server provides content logging, web page caching and allows all internet users to utilize the same firewall port.

3.5. Firewalls, Routers and VPN

GIAC utilizes a dedicated T1 connection to the Internet and another dedicated T1 connection between Kansas and Colorado. All Internet traffic passes through the Kansas office which is protected by Check Point VPN-1/Firewall-1 running on Nokia 650 redundant hardware appliances. These same devices provide VPN connectivity. All unnecessary ports have been closed.

Routing service is provided by a Cisco router on the edge and a Cisco switch internally. Strong passwords have been chosen for all networking equipment and are changed every 30 days. Current firmware and patches are installed on all networking devices. Regular backups are performed on all routing tables and the firewall rulebase.

VPN connectivity is facilitated by the SecuRemote product from CheckPoint. This technology consists of a software client that connects over the Internet to the CheckPoint VPN-1/Firewall-1 appliance. A 128-bit encrypted session is established (through a 3-way handshake) and the user is allowed to authenticate to the Windows network via a pass-through authentication mechanism provided by CheckPoint.

3.6. Email Services

Email services are provided through Microsoft Exchange Server 5.5. There are two email servers located in Kansas and one in Colorado. One of the Kansas servers also provides Internet mail access via the Outlook Web Client (OWA) for users who are unable to access the network via VPN or dialup.

It is important that email servers are stable and secure as downtime is typically unacceptable. All service packs and hotfixes are applied to each server. IIS is required for OWA but can be removed from the other servers.

3.7. Print Services

Individual servers configured as Microsoft Print Servers are located in Kansas and Colorado. All printers are networked (local printers at GIAC are forbidden.) In this fashion 'File and Print' sharing can be disabled on all client machines. See Reference 6 for more information about configuring a Microsoft print server.

3.8. Certificate Services

A single Certificate Authority (CA) server exists on the GIAC network and is located in the Kansas site. Certain users require digital signatures and the ability to encrypt data. The machine is configured as an Intermediate (issuing) CA for this purpose. This can be done by navigating to control panel -> add/remove programs -> add/remove windows components and placing a check mark next to certificate services. The Certificate Wizard will guide the rest. See Reference 7 for more details.

The Root CA is a stand-alone machine used only to issue keys to the Intermediate CA. Afterwards the hard drive from the Root CA is removed and secured in a fireproof safe along with the private key. No issuing certificate from a trusted 3rd party (like VeriSign) has been purchased because it is cost prohibitive at this time. GIAC only requires certificate services internally. External requirements (like OWA and E-Commerce) have been outsourced and are discussed later.

Creation of a CA results in the creation of a Certificate Services local website that users can visit to request certificates. IIS is required on the server in order to host the website. As such some precautions need to be taken to protect the machine and the website. The IIS lockdown tool will be applied.

A Security Group called "Certificate Requesters" will be created and populated with members from the Finance and HR departments. This group will be used to grant permission to enroll for a certificate. See Reference 8 for instructions on assigning permissions.

The website may be modified by visiting the IIS MMC snap-in on the server. It is recommended that the website be set to require Integrated Windows Authentication in order to join (as opposed to anonymous access) - (Directory Security tab of website Properties.) Also under the Directory Services tab is the ability to Grant/Deny access based on IP subnet. The website will be set to 'Deny' access to all 'Except' the Finance and HR departments which are defined by network ID and subnet. (Recall that these departments require the ability to digitally sign and encrypt email and documents.)

Certificates are then issued by visiting the (http://*servername*/certserv) website and following the prompts. The expiration of the certificates will be set at two years. GIAC is still small enough that revocation of a certificate upon compromise can be accomplished in a short period of time.

3.9. Web Services

GIAC host a single site that displays both corporate information and the ability to buy fortunes online. GIAC's website resides on two separate servers with Windows 2000 Advanced Server and Windows Load Balancing Service (WBLS) enabled and the IIS Lockdown tool applied. The website files reside on a volume separate from the system volume.

3.9.1. Server Placement

The web servers at GIAC are not located in the DMZ. Instead they are members of the domain. This is a security trade-off in the name of simplicity. Joining the web servers to the domain simplifies server management since Group Policy can be used. The web servers are really middle-tier machines between external clients and back end database servers and this relationship is simplified within the domain.

In addition domain membership simplifies OWA for Exchange and duties performed by the backup server. IPSec AH is required for all communications except port 80 (HTTP) and port 443 (HTTPS.) The following features are also disabled: "Accept unsecured communication, but always respond using IPSec" and "Allow unsecured communication with non-IPSec-aware computers."

An alternative would be to create a separate DMZ domain with an explicit one-way trust. However this would complicate the network design by requiring a separate domain controller, etc.

3.9.2. SQL

SQL 2000 is implemented as the back-end responsible for providing database services to the customer interface for selling fortunes (located on the web servers.) The databases store the fortunes as well as certain customer and sales history data. There are two SQL servers at GIAC and both reside in the Kansas office. They are load-balanced and redundant. Access to them by the website front-end application is allowed through Windows Authentication via a specially created application service account (as opposed to SQL mixed security and SQL server logins.)

3.9.3. E-Commerce

The commercial side of GIAC Enterprises is outsourced to VeriSign primarily for simplicity. A link to buy appears on the GIAC fortune teller site that points to VeriSign's transaction network. All of this redirection is seamless and transparent to the customer. VeriSign provides GIAC with credit card transaction and recurring payment capability (for the fortune of the week subscribers) and detailed billing reports; all for a small monthly fee. (http://www.verisign.com/products/payment.html.)

3.9.4. Workstations

As previously stated all workstations (in-house and remote) are configured with the Windows 2000 Professional operating system. All service packs and hotfixes are consistently tested and applied. All remote sales laptops are equipped with Kensington locks which are hopefully used when the salespeople travel.

4.0. Active Directory Design

4.1. Active Directory (AD) Overview

The Active Directory GIAC is a single forest, single domain model running in native mode. (Figure 4.1) Active Directory namespaces can be called anything and do not need to match the Internet domain name. However the decision was made to trade-off the security benefits associated with this technique in exchange for simplified manageability. There are several benefits of single domain architecture, including:

- Ease of administration
- Increased performance
- Logon transparency when users travel between offices
- No trusts required

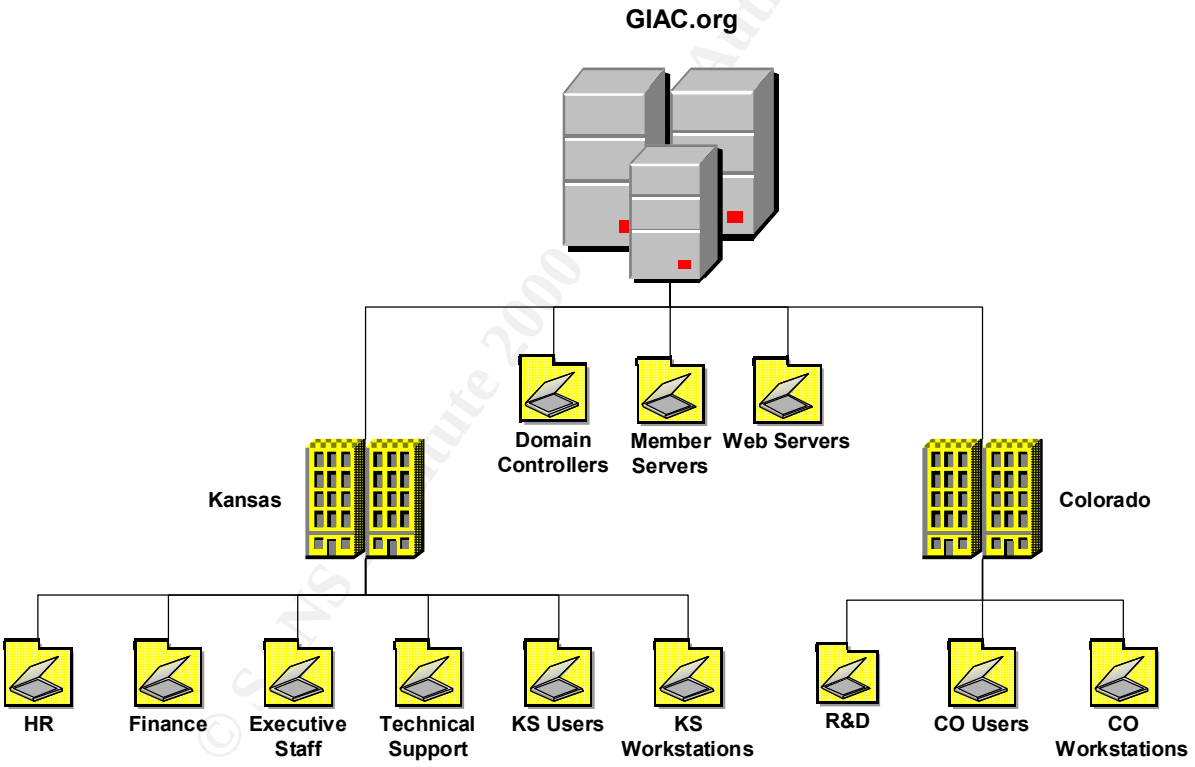

Figure 4.1 – GIAC Active Directory Logical Structure

4.2. Active Directory Sites and Replication

AD 'Sites' are intended to manage multiple physical locations within a single domain. This is more for network management and Active Directory replication then security; however Group Policy can be applied at the site level.

Microsoft defines a site as a collection of one or more subnets that are defined by the administrator. When you define subnets, they should be "well-connected" with high-bandwidth local area network (LAN) connections.[9] As such a site exists for each office (Kansas and Colorado.) A unique internal subnet is assigned to each; 10.2.x.x and 10.3.x.x respectively (10.1.x.x is the DMZ and is also located in Kansas.) The replication link between sites is configured to synchronize at an off-peak hour.

Since simplicity is one of the main goals in this design the question of using sites instead of OUs is raised. Colorado has very limited networking requirements none of which are really unique to that location. The staff could easily be organized into a single OU. A typical reason for using Sites is to aid in replication over slow links but there is a dedicated T1 between offices so that is not an issue either. So why define separate sites? The answer is simple: future growth.

Colorado only has ten employees and they are all in the same department. Well, almost in the same department. Actually there are nine developers and one administrative assistant. The admin does not require near the level of access that the developers do. Furthermore the marketing and sales staffs have seen market potential for some new products if GIAC can develop them. It has already been decided that all future growth in the R&D department will occur in Colorado. This means more administrative assistants and probably small sales, marketing and HR departments as well.

By defining the physical site structure in Active Directory now a supportive OU structure can easily be created beneath the Colorado Site when the need arises. This also maximizes the ability to leverage 'site specific' group policies if necessary.

Active Directory Sites are described in slight detail in the next few sections. References are named that can provide more details on Sites and Site management.

4.2.1. Site Creation[10]

Sites are managed via the "Active Directory Sites and Services" MMC snap-in. Once expanded, the snap-in will reveal three folders; 'Sites,' 'Inter-Site Transports,' and 'Subnets.'

A new site can be created by simply right-clicking on the 'Sites' folder, choosing 'New Site' and naming it appropriately. This must be done for both Kansas and Colorado. (It should be noted that no bridgehead server will be required as both sites reside behind the same firewall.)

4.2.2. Site Link Creation[11]

Once both sites are created a link must be established between them. Microsoft defines a Site Link as an object that typically represents two sites that are connected

physically by a wide area network (WAN) link. A Site Link can contain more than two sites but that does not apply to GIAC.

Expanding the 'Inter-Site Transports' link reveals two folders; 'IP' and 'SMTP.' GIAC only utilizes IP based links between offices. Right-clicking on the 'IP' folder yields the option to create a new link. A list of available sites appears on the left. 'Kansas' and 'Colorado' are then selected and 'Added;' this will move them to the right side of the dialog box and effectively create the Site Link.

Replication is set to occur every fifteen minutes and is available 24x7x365. Cost is not an issue since there are only two sites and one link between them.[12]

4.2.3. Subnet Creation

Each subnet in use at GIAC must be explicitly defined and associated with a Site. The following steps (taken from the MMC help file) describe how to create and associate a Subnet.

Open Active Directory Sites and Services.
In the console tree, double-click Sites.
Right-click Subnets, and then click New Subnet.
In Address, enter the subnet address.
In Mask, enter the subnet mask that describes the range of addresses included in this site's subnet.
Choose a site with which to associate this subnet, and then click OK.

4.3. Organizational Unit (OU) Hierarchy

The OU hierarchy is referred to as a hybrid model since mixed resource types (computer and user) reside on the same tier. This architecture was chosen for simplicity and ease of administration. Individual OUs are created only when necessary and there are as few as possible. The only built-in OU to be used is "Domain Controllers."

The following list describes each OU and its purpose:

Domain Controllers / Member Servers / Web Servers – These OUs exist to provide an extra layer of granularity for managing these special devices. The "Domain Controller" container is created automatically by Windows. (See section 4.4)

HR – Contains all Human Resources employees.

Finance – Contains members of the Finance department.

Executive Staff – Required to isolate the upper management from the rest of the company.

Technical Support – Created for increased security requirements pertaining to those with elevated network access.

KS Users – Contains all user accounts in Kansas not specifically assigned to another OU.

KS Workstations – Used for administration of computer accounts in Kansas.

R&D – Contains members of the Research and Development department.

CO Users – One staff member is not technically a part of R&D (secretary.) This organizational unit is intended for that employee and similar future employees.

CO Workstations – Used for administration of computer accounts in Colorado.

4.4. Default Organizational Units

Windows Active Directory automatically installs several containers by default. It is at the discretion of the network administrator whether or not to use them. Below is a list of built-in OUs and their purpose.

- Builtin – Contains several default security groups
- Computers – Not used.
- Domain Controllers – Contains all Domain Controller objects.
- Enterprise Groups – Contains all enterprise (highest level) security groups.
- ForeignSecurityPrincipals – Not used.
- Users – Not used.

4.5. Active Directory Administration, Performance and Security

As stated this AD architecture was chosen primarily for its simplicity. This makes AD more manageable; easing the administrative burden. GIAC's hardware is modern and powerful so no servers should encounter performance problems. However with respect to AD, performance should always be a design driver whether it is perceived as a future concern or not.

Along with performance is the issue of security. It is much easier to secure a simple system. Complicated AD structures make it exponentially more difficult to apply solid security settings via Group Policy.

4.6. Active Directory Security Groups

The following Security Groups were created to easily assign rights to required resources. These groups will be used in Group Policy, Network Share permissions, Certificate Enrollment Services, etc.

- Exec
  (Contains all Executives)
- Finance
  (Contains all members of the Finance Department)
- HR
  (Contains all members of the Human Resources Department)
- Marketing
  (Contains all members of the Marketing Department)
- R&D
- Sales Inside
  (Contains all members of Sales Department working in-house)
- Sales Remote
  (Contains all outside Sales staff)
- Tech Support
  (Contains all members of the Technical Support Department)

Additionally:

- Certificate Requesters
  (Contains all staff members approved for Certificate Enrollment)
- Desktop Support
  (Contains a portion of the Technical Support Department responsible for general desktop support and building new desktop machines. Members of the 'Account Operators' built-in group can add machines to the domain.

All user accounts should be a member of one or more of the aforementioned groups. All network administrators belong to the Domain Admins group.

5.0. Group Policy and Security

Group Policy is the primary means by which security is configured and applied in Windows 2000. Security settings can be applied to all or part of a domain through Group Policy. Any network object (user and computer accounts, printers, etc.) can be effectively managed through Group Policy. Additionally, Group Policy provides the ability to remotely install software and execute scripts.

5.1. Group Policy Basics

Group Policy is a critical component to securing a Windows 2000 environment. It is also a very powerful tool that can wreak total havoc on a network if misused. Therefore policies should be well conceived and tested prior to implementation. They should also be applied incrementally to limit any resulting damage. To view or modify the group policy for the domain (or any other object) simply add the 'Group Policy' MMC snap-in and choose the relevant policy.

Central to Group Policy is the Group Policy Object (GPO.) GPOs are stored at the domain level and affect users and computers contained in Sites, Domains, and Organizational Units. In addition each Windows 2000 computer has exactly one group of settings stored locally called the local Group Policy Object.[13]

Group Policy utilizes the parent-child relationship of AD containers to facilitate the inheritance of policies. Inheritance is easy to control via two features; "Block Inheritance" and "No Override." These features plus the ability to link GPOs provide the means to effectively manage the granularity of Group Policy.

The following is an excerpt from a SANS training manual on AD and Group Policy authored by Jason Fossen.[4]

> *GPOs are applied in the following order:*
> *NT 4.0 System Policy*
> *Local GPOs (stored on the machine, not in AD)*
> *Site GPOs*
> *Domain GPOs*
> *Organizational Unit GPOs (in nested order)*
> *An easy way to remember this is the acronym "4LSDOU."*

OU GPOs are applied in nested order: largest container down to smallest (inside) container holding the user or computer. If multiple GPOs are linked to a single container, e.g., a single OU, then they are applied in the order specified on the property sheet. Note that lower priority items are at the bottom of the list which means they will be processed first.

Additional information on GPO administration can be found at:
http://support.microsoft.com/default.aspx?scid=kb;en-us;q322143

5.2. Group Policy at GIAC

Group Policy contains a very large number of options that can be explicitly enabled or disabled or left undefined. Windows explicitly enables and disables some by default but leaves a large number undefined. Only the examples where GIAC's policies deviate from the standard "out-of-the-box" configuration are profiled here.

The two policies used most extensively are:

- Default Domain Policy
- Default Domain Controllers Policy

Some OU specific policies are used and all is explained further in the next sections.

5.3. Default Domain Policy

The Default Domain Policy is the first GPO to be applied and affects every user and computer on the domain. As with all GPOs it is comprised of two parts:

- Computer Configuration
- User Configuration

The Computer Configuration relates to settings applied to computers regardless of the user. It's first applied during the boot process. The User Configuration deals mainly with environment restrictions relevant to a specific user account. This usually involves forcing registry settings under the HKEY_CURRENT_USER section of a computer's registry wherever the user logs in.

The reader is reminded that the following subsections (5.3.x) relate only to the Default Domain Policy. OU policies, etc. are described later.

5.3.1. Computer Configuration

As stated above, Computer Configuration changes affect the machine regardless of who is using it. The Computer Configuration container is comprised of three child containers:

- Software Settings
- Windows Settings
- Administrative Templates

The following subsections describe specific Domain Level Computer Configuration settings applied at GIAC. They are listed in the same top-down order as they appear in the MMC snap-in.

5.3.1.1. Windows Settings/Security Settings/Account Policies

Several account policies are applied at the domain level. Namely the password, account lockout and Kerberos policies are defined here.

The password policy is straight forward. Each user must choose a password that is difficult to guess (complexity requirement) and change it periodically. Windows 2000 password policies are applied at the domain level by default since the password change ultimately occurs on the domain controller.[15] Table 5.1 shows the password policy settings.

Table 5.1 – Default Domain Policy: Password Policy

Policy	Computer Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 day
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store passwords using reversible encryption for all users in the domain	Disabled

Tantamount to the password policy is the account lockout policy. This policy guards against brute force attacks (password guessing) on network accounts. Notice the "Account Lockout Duration" setting is "0 minutes." This causes the account to stay locked out until an administrator physically unlocks it. Otherwise the account is locked out for the corresponding number of minutes only. (Table 5.2)

Table 5.2 – Default Domain Policy: Account Lockout Policy

Policy	Computer Setting
Account lockout duration	0
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	15 minutes

Kerberos is the preferred authentication process in Windows. Table 5.3 shows the policy settings which are the standard defaults.

Table 5.3 – Default Domain Policy: Kerberos Policy

Policy	Computer Setting
Enforce User Logon Restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

5.3.1.2. Windows Settings/Security Settings/Local Policies/Audit Policy

Auditing is important for tracking network access and usage. Forensic analysis of malicious activity depends on vigilant network auditing. Table 5.4 is taken from a SANS step-by-step Windows security manual.[16] It describes the various audit settings and recommendations.

Table 5.4 – Default Domain Policy: Audit Policy

Item	What it does (from TechNet)	Recommended
Audit account logon events	Logs both local and remote resource logons.	Success, Failure
Audit account management	Audits User accounts or Groups created, changed, or deleted. User accounts renamed, disabled, or enabled. Passwords set or changed.	Success, Failure
Audit Directory service access (For DC's)	Important for Domain Controllers. Audits access to the directory service.	Success, Failure
Audit logon events	Enables auditing of logon events.	Success, Failure
Audit object access	Enables auditing on base system objects.	Success, Failure
Audit policy change	Enables auditing of any changes to user rights or audit policies.	Success, Failure
Audit privilege use		None

Audit process tracking	Tracks program activation, handle duplication, indirect object access, and process exit.	No auditing Required. Good to monitor Virus behavior in a Development Environment.
Audit system events	Logs shutdowns and restarts for the local workstation.	Success, Failure

Part of configuring the Audit Policy is to specify the size and access to the logs. The following log sizes will be imposed for auditing activity on the network:

- Maximum application log size: 20,480 kB (20 MB)
- Maximum security log size: 51,200 kB (50 MB)
- Maximum system log size: 20,480 kB (20 MB)

Additionally all guest access to log files is restricted. The retention method for all logs is set to 'As needed' and the feature to shut down a computer when the log is full is 'Disabled.'

Several of these items will generate large amounts of log data. All servers at GIAC have at least 30GB of disk space or more so large log files are not perceived to be a problem. However the auditing of privilege use will not be enabled initially. Auditing privilege use will generate a log entry every time a user right is exercised. This is considered unnecessary at this time. In general, the account logon and modification and policy modification events should be logged at a minimum.

5.3.1.3. Windows Settings/Security Settings/Local Policies/User Rights Assignments

Table 5.5 lists the changes to the user rights portion of the domain policy. These changes apply to every user that logs onto the GIAC domain.

Table 5.5 – Default Domain Policy: User Rights Assignments

Policy	**Computer Setting**
Access this computer from the network	Authenticated Users
Add workstations to domain	Domain Admins, Desktop Support
Back up files and directories	Domain Admins
Bypass traverse checking	Domain Admins
Change system time	Administrators, Domain Admins

Policy	Computer Setting
Debug programs	Domain Admins, R&D
Enable computer and user accounts to be trusted for delegation	Domain Admins
Generate security audits	Domain Admins
Load and unload device drivers	Domain Admins, Desktop Support
Restore files and directories	Administrators, Domain Admins
Take ownership of files and other objects	Domain Admins

Only authenticated users can access other computers on the network. Administrative tasks like backing up and restoring files, taking ownership of files and objects and changing the system time are only allowed by the domain administrators.

The ability to add new machines to the network and load/unload device drivers is restricted to the domain administrators and desktop support staff (Desktop Support is responsible for rebuilding and distributing workstations.) The R&D department is allowed to debug programs in order to streamline the development process.

One other important setting to discuss is 'bypass traverse checking.' Traverse checking regulates the ability to browse child objects (file folders) without having rights to the parent object. This is a potential security risk and is restricted to the Domain Admins.

5.3.1.4. Windows Settings/Security Settings/Local Policies / Security Options

This area of Group Policy contains several specialized security options. Table 5.6 details the initial settings that will be applied at GIAC.

Table 5.6 – Default Domain Policy: Security Options

Policy	Computer Setting
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Audit use of backup and restore privilege	Disabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Enabled

Policy	Computer Setting
Digitally sign server communication (always)	Enabled
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 only \ refuse LM & NTLM
Message text for users attempting to log on	"Property of GIAC…Beware!"
Message title for users attempting to log on	"Property of GIAC…Beware!"
Rename administrator account	"Ne1469?"
Rename guest account	"#1GoodTimez"
Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Enabled

Additional restrictions for anonymous connections
Disallowing all but explicit anonymous access results in the removal of "Everyone" and "Network" from the anonymous users token; thus requiring that "Anonymous" be given explicit access to any required resources.[13]

Audit use of backup and restore privilege
Privilege use auditing has been disabled in the audit policy rendering the backup/restore privilege auditing feature unusable. So it has been disabled.[13]

Clear virtual memory pagefile when system shuts down
When this policy is enabled it causes the system pagefile to be cleared upon clean shutdown. Enabling this security option also causes the hibernation file (hiberfil.sys) to be zeroed out when hibernation is disabled on a laptop system. This ensures that sensitive information from process memory that might have made it into the pagefile is not available to an unauthorized user who has managed to directly access the page file.[13]

Digitally sign client communication (always)
The Windows 2000 Server Message Block (SMB) authentication protocol supports mutual authentication, which closes a "man-in-the-middle" attack; and supports message authentication, which prevents active message attacks. SMB signing provides this authentication by placing a digital signature into each SMB which is then verified by both the client and the server.[13]

Digitally sign server communication (always)
Enabling this option requires the Windows 2000 Server Message Block (SMB) server to perform SMB packet signing.

Do not display last user name in logon screen
When a user presses <CTRL><ALT><DEL> to logon, the field which normally displays the logon name of the last user will now be blank. This makes it more difficult for a hacker to guess valid login names (via social engineering.)

LAN Manager Authentication Level
Determines which challenge/response authentication protocol is used for network logons. Since all machines are Windows 2000, NTLMv2 protocol can be specified and the others neglected.

Message text for users attempting to log on
When enabled this option will display a message box directly after the user presses <CTRL><ALT><DEL> to logon but prior to the user actually logging on. The message box must be 'accepted' manually by pressing <OK> or the user will not be allowed to log on. The message contained within is a legal disclaimer alerting the user that they are logging onto equipment belonging to GIAC.

Message title for users attempting to log on
This is a companion to the previously mentioned option where the title of the message box may be specified.

Rename administrator and guest account
These are two distinct options but will be explained together. Hackers typically rely on default configurations for the majority of their exploits. Since it is widely known that all Windows 2000 Professional workstations come standard with 'Administrator' and 'Guest' accounts they will be renamed. The Guest account is then disabled. Furthermore a "honeypot" administrator account with no assigned rights will be created. Thus an attacker's efforts to exploit the default administrator account will be futile as the actual administrator account has been hidden and replaced with a false one.

Secure channel: Digitally encrypt or sign secure channel data (always)
When a Windows 2000 system joins a domain a computer account is created. Thereafter, when the system boots it uses the password for that account to create a secure channel with the domain controller. Requests sent on the secure channel are authenticated. Sensitive information (such as passwords) is encrypted but the channel is not integrity checked and not all information is encrypted.

If this policy is enabled all outgoing secure channel traffic must be either signed or encrypted. If this policy is disabled, signing and encryption are negotiated with the domain controller.

This option should only be enabled if all of the domain controllers in all the trusted domains support signing and sealing. Also if this parameter is enabled, "Secure channel: Digitally sign secure channel data (when possible)" is automatically enabled.[13]

Secure channel: Require strong (Windows 2000 or later) session key
All outgoing secure channel traffic will require a strong (Windows 2000 or later) encryption key. The reader is reminded that all DCs in the domain must support strong keys in order for this option to function properly.

5.4. Organizational Unit (OU) Policies

OU Policies are the last to be applied and therefore carry the most weight. OUs and OU policies are a perfect example of the power of Active Directory and the improvements in the Windows OS over NT4. OU policies at GIAC are used primarily to tweak inherited security settings (or block them entirely) and deploy software.

5.4.1. Default Domain Controllers Policy

Windows 2000 treats DCs differently than any other machine on the network. By default a Windows 2000 DC object is stored in the built-in "Domain Controllers" container. Windows 2000 also creates a separate GPO called "Default Domain Controllers Policy" and links it to the Domain Controllers OU. This policy will be used to further enhance the security of the DCs at GIAC.

It should be noted that DC objects in AD do not have to reside in the Domain Controllers container. That is simply where Windows stores them by default. If a DC computer object is moved it will pull certain settings from GPOs as long as they are linked to the domain container. All DC objects at GIAC will remain in the default container so this should not be an issue.[17] Furthermore the account policies (lockout, password and Kerberos) defined in the Default Domain Policy will apply to the domain controllers. As will 'Automatically log off users when logon time expires' and the renaming of administrator and guest accounts.

The primary threat that needs to be addressed at GIAC is the ability to physically access the DCs. All equipment resides in a locked room however too many people have the key. The budget would not allow for specialized cages or locking cabinets for the DCs so they will have to be protected another way. This is most easily facilitated by adjusting the Default Domain Controllers GPO to lock out the console.

Tables 5.7 – 5.8 show the domain controller policy enhancements.

Table 5.7 – DC Policy: User Rights Assignments

Policy	Computer Setting
Access this computer from the network	Administrators, Authenticated Users
Add workstations to the domain	Desktop Support, Domain Admins
Change the system time	Administrators, Domain Admins

Policy	Computer Setting
Log on locally	Domain Admins
Shut down the system	Domain Admins

Notice the last option to shut down the system. The author acknowledges that this option is useless if access to the server's power button is possible. However with a locking cabinet and open KVM interface; or if local log-on rights ever need to be granted to a lesser security group (like Account Operators) then this setting will be necessary.

Table 5.8 – DC Policy: Security Options

Policy	Computer Setting
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Enabled
Digitally sign server communication (always)	Enabled
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 only \ refuse LM & NTLM
Rename administrator account	"Long Random Name"
Rename guest account	"Long Random Name"
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Enabled
Unsigned driver installation behavior	Warn but allow installation
Unsigned non-driver installation behavior	Warn but allow installation

Enabling the settings in the previous two tables will make it extremely difficult to gain access to the DCs. The secure channel settings are part of a native 2000 environment. Disabling the ability to log-on locally and disabling access to the CD-ROM and floppy drives should prevent unauthorized console access.

5.4.2. Executive Staff OU Policy

The Executive Staff OU will have the "Block Inheritance" option flagged to block inherited policies. The executive staff refuses to maintain their passwords responsibly. The network security personnel do not relish the idea of finding new jobs so they are complying. By blocking inheritance the password policies defined on the domain will not filter down to the Executive Staff OU.

This is a double-edged sword as future Site or Domain policies that may apply to the executive staff will not be received. Instead those future polices will have to be specifically defined for this OU. Normally alternative settings could be defined in an OU GPO that would override the domain GPO. However the password policy is unique in that it is applied at the domain level and ignored everywhere else so a special concession must be made to management. This additional administrative overhead increases the complexity of the network which is undesirable. It is also why "management has its privileges."

5.4.3. Software Installation through Group Policy

This feature allows the administrator to quickly deploy/remove software to a group of machines. The "Software Settings" folder is the first container beneath the 'Computer Settings' object in Group Policy. The most important example at GIAC is the implementation of Windows Service Packs. OU-level policies are defined for software deployment to conserve bandwidth. Service packs can be large; to try to deploy one to the entire domain at once might overload the source server and/or completely congest the network. Using OU-level policies allows the deployment to easily be staggered over days/weeks and so on.

To deploy a service pack simply save it to a shared network folder (perhaps on a dedicated software deployment server or minimally used file server) and then point the Software Installation job at the original file. Avoid using a DC for software deployment. Group Policy will do the rest the next time each machine attaches to the network.

One important limitation of this feature is the acceptable format of the software installation file. All software packages pushed out via this feature must be in Microsoft Installer (.msi) format. Service Packs come standard in this format courtesy of Microsoft. Hotfixes and other 3rd party software do not and therefore must have custom .msi files created for them or be deployed another way.[18]

5.4.4. Startup/Shutdown Scripts

This feature is used at GIAC primarily for applying Windows hotfixes and modifying the registry. As stated previously the ability to automatically push software extends only to programs that have been converted to .msi format. However most hotfixes are delivered in the more traditional .exe format; therefore a different approach is required.

This is accomplished most easily by writing a small script designed to call the executable file and install it. Recalling that nearly the entire Windows operating system is scriptable the script execution feature in Group Policy is a great way to modify registry settings. Many extensive security settings (like removing the LAN Manager Hash) as well as adding or removing registry keys require modifying the registry directly.

Hotfixes and registry changes should be applied to computers not users. As such the 'Startup' portion of Group Policy is used (as opposed to Login/Logoff) when applying hotfixes and/or registry changes. All scripts are stored in the "\SYSVOL*domain_name*\SCRIPTS" folder located on each DC. The scripts container allows the administrator to force each computer to execute a script (preferably written in VBScript.) Multiple scripts can be defined for the same OU.

The script will automatically execute each time a computer connects-to or disconnects-from the domain. The Startup/Shutdown portion of Group Policy can be found in "Computer Configuration/Windows Settings/Scripts (Startup/Shutdown)." A startup script file defined here will execute each time the computer boots up and registers itself on the network but prior to a user actually logging in. A shutdown script defined here will execute after the user logs off but prior to the machine shutting down.

5.4.5. Logon/Logoff Scripts

Logon scripts are defined in the "User Configuration/Windows Settings/Scripts (Logon/Logoff)" portion of Group Policy. Each site has a unique logon script for the purpose of mapping drives and printers. The scripts are kept in the \SYSVOL*domain_name*\SCRIPTS subfolder located on each DC. VBScript is used at GIAC although Group Policy supports scripts written in almost any scripting language.

5.6. Additional Group Policy

Highlighted in this section are a few examples of customized policies used at GIAC. The reader is reminded that Group Policy options are nearly limitless.

5.6.1. Default Domain Policy: Screen Saver Policy

Screen savers are typically a headache for any network administrator. Besides screen saver hoaxes that result in viral infection many custom screen savers are resource hogs that may or may not be suitable for the work environment. Group Policy will be used at GIAC to regulate screen saver usage.

An additional benefit of this policy is the ability to force users to protect their screen savers with passwords and to force these screen savers to initialize after a certain period of inactivity. This can go a long way towards decreasing the social engineering threat due to a user leaving their workstation unattended but still logged

in. Table 5.9 outlines the domain-wide screen saver policy which can be defined at "User Configuration/Administrative Templates/Control Panel/Display."

Table 5.9 – Default Domain Policy: Screen Saver Policy

Policy	Setting
Activate Screen saver	Enabled
Screen saver executable name	"scrnsave.scr"
Password protect the screen saver	Enabled
Screen saver timeout (seconds)	600

Note: The screen saver must have a ".scr" extension. If the screen saver file is not in the %Systemroot%\System32 directory then the fully qualified path must be specified. If the screen saver executable does not reside on the client machine then the policy is ignored.

5.6.3. Sales OU Policy: Internet Favorites and Default Home Page

The sales manager has requested that all sales users be provided a list of standard websites that they need to visit frequently. In addition the sales manager wants the default home page changed to http://www.giac.org and does not want the sales staff to be able to change it. A single policy will be defined on the Sales OU called "Internet favorites and default home page."

Once created and linked to the Sales OU the list of preferred websites can be defined in Group Policy at: "User Configuration/Windows Settings/Internet Explorer Maintenance/URLs." The list of 'favorites' is entered under the "Favorite Links" container. The default home page is defined under the "Important URLs" container.

One other task must be performed namely removing the user's ability to change the default home page. This is done in the "User Configuration/Administrative Templates/Internet Explorer" container by enabling the option called "Disable changing home page settings."

5.6.4. Group Policy Templates

Templates are an easy way to apply multiple Group Policy settings at once. Some predefined templates are available by default.[19] Others are available from the Windows 2000 Resource Kit or 3rd parties such as the National Security Agency (http://www.nsa.gov.) They can also be created by manually changing the Group Policy settings on a single machine and then saving those settings to a template file that can be imported on any other machine on the network. In general,

- Templates are text-based .inf files stored in the \%systemroot%\Security\Templates folder.
- Templates are cumulative; thus when multiple templates are available (as in the case of domain controllers) the templates must be applied consecutively to achieve the desired effect.
- A template can be applied and then certain settings tweaked manually.
- All desired Group Policy changes may be performed manually and saved as a custom template instead of using a predefined template.

Two MMC snap-in tools are available for working with templates.

- Security Configuration and Analysis
- Security Templates

These tools are essentially GUI interfaces to the SECEDIT command. Using these GUI tools all analysis and template modification must be done on the local machine. Otherwise the SECEDIT command line utility can be used to deploy the templates to OUs, etc.

A more exhaustive discussion of templates is beyond the scope of this document. However an example can be made of the DCs. As mentioned above the Default Domain Controllers GPO was manually adjusted to meet the security criteria. An alternative would have been to import a template and apply it to the DCs. Windows makes available the following domain controller templates by default:

- Default domain controller (basicdc.inf)
- Secure domain controller (securedc.inf)
- Highly secure domain controller (hisecdc.inf)

These templates represent varying levels of security for domain controllers. All three could be applied to all domain controllers on the GIAC network (via the built-in Domain Controller OU and Default Domain Controller Policy.) In order to achieve the "Highly Secure Domain Controller" status the Default and Secure DC templates must be applied first.[20] The final result of applying these templates will be the assertion of several settings changes at once (some of which were discussed above.)

It is left to the reader to discover all the specific settings affected by applying these templates as they are many. Figure 5.1 shows a few of the differences (denoted by the "red circle – white X" symbols.) The "green check-mark" symbols indicate settings that will not change. This particular collection of settings shown in the figure is located in "Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options." Notice all 'Secure channel' options are enabled. Enabling these options is one of the main aspects of the 'hisecdc.inf' security template. The 'hisec' templates can only be applied to Windows 2000 domains operating in Native Mode.[20]

Policy	Database Setting	Computer Setting
Additional restrictions for anonymous connections	No access without explicit anonymous...	No access without expli...
Allow server operators to schedule tasks (domain controllers only)	Disabled	Not Available
Allow system to be shut down without having to log on	Disabled	Disabled
Allowed to eject removable NTFS media	Administrators	Administrators
Amount of idle time required before disconnecting session	15 minutes	30 minutes
Audit the access of global system objects	Disabled	Enabled
Audit use of Backup and Restore privilege	Disabled	Enabled
Automatically log off users when logon time expires (local)	Enabled	Enabled
Clear virtual memory pagefile when system shuts down	Enabled	Enabled
Digitally sign client communication (always)	Enabled	Disabled
Digitally sign client communication (when possible)	Enabled	Enabled
Digitally sign server communication (always)	Enabled	Disabled
Digitally sign server communication (when possible)	Enabled	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled	Disabled
Do not display last user name in logon screen	Enabled	Enabled
LAN Manager Authentication Level	Send NTLMv2 response only\refuse L...	Send NTLMv2 response ...
Message text for users attempting to log on		
Message title for users attempting to log on		
Number of previous logons to cache (in case domain controller is not av...	10 logons	0 logons
Prevent system maintenance of computer account password	Disabled	Disabled
Prevent users from installing printer drivers	Enabled	Enabled
Prompt user to change password before expiration	14 days	14 days
Recovery Console: Allow automatic administrative logon	Disabled	Disabled
Recovery Console: Allow floppy copy and access to all drives and all fol...	Disabled	Disabled
Rename administrator account	Not defined	Administrator
Rename guest account	Not defined	Guest
Restrict CD-ROM access to locally logged-on user only	Enabled	Enabled
Restrict floppy access to locally logged-on user only	Enabled	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled	Disabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Enabled	Disabled
Send unencrypted password to connect to third-party SMB servers	Disabled	Disabled
Shut down system immediately if unable to log security audits	Disabled	Not Available
Smart card removal behavior	Force Logoff	Lock Workstation
Strengthen default permissions of global system objects (e.g. Symbolic	Enabled	Enabled

Figure 5.1 – Hisecdc.inf Security Template Comparison

6.0. Additional Security Considerations

This section details additional measures designed to enhance the security at GIAC Enterprises.

6.1. Securing Outlook Web Access

This section will detail the steps necessary to secure Outlook Web Access (OWA) for Microsoft Exchange. OWA is a handy way for users to access email when they are out of the office and unable to dial-up directly. The OWA client is a web page designed to look like the normal Outlook client. Unfortunately, left unsecured this feature is a large security risk. By default an OWA session is transmitted in clear text and it is possible to re-invoke a session even after a user logs off. This is particularly dangerous when the user invokes OWA from an Internet kiosk or other public domain terminal.

The solution is to install a digital certificate and encrypt the OWA sessions over 128-bit SSL. (A similar process could be used to secure the online E-Commerce transactions associated with selling GIAC's fortune cookie sayings.)

6.1.1. Digital Certificate Basics

In order to encrypt OWA sessions a digital certificate is required. This certificate will be used each time somebody visits the OWA webpage. Therefore the certificate must be compatible with a variety of web browsers.

To ensure the most amount of functionality it is recommended to use a certificate provided by a trusted 3rd party, e.g., VeriSign (http://www.verisign.com), RSA (http://www.rsasecurity.com), etc., as opposed to generating one internally. If the Exchange server providing OWA is configured to disallow unencrypted sessions then the user will be unable to utilize OWA without installing the certificate in their browser. Many public domain workstations (like cyber-cafes and libraries) are locked down such that this is not allowed. Most browsers (like Microsoft IE and Netscape) however are preconfigured to trust certificates from certain 3rd party providers like VeriSign.

6.1.2. Obtain a Digital Certificate from VeriSign

VeriSign sells a variety of security services including digital certificates through their website. Before being issued a digital certificate a company must complete several steps to verify their credentials. This is the basis for VeriSign's ability to act as a trusted 3rd party. The following link will provide the reader with detailed instructions on how to prepare the Exchange server, buy the certificate and install it.[21]

Note: The server may either be a stand-alone machine in the DMZ or a domain member like KS_EMAIL1 from Figure 3.1. The budget at GIAC does not allow for a dedicated OWA server so the duties have been shared by an Exchange member server.

6.1.3. Automatically Redirect Traffic to SSL Port 443

After importing the digital certificate on the Exchange server the user will be able to invoke 128-bit encrypted SSL sessions over port 443. However, redirecting the traffic to this port is not done by default. Therefore anyone visiting the OWA website must know to type “HTTPS” as opposed to “HTTP”. This is an inconvenience to the user.

It is preferable to have the user automatically redirected to the secure site. This can be achieved in a variety of ways however at GIAC the ‘Error 403.4” web page method will be used. This is done by replacing the default ‘Error 403.4” page with a modified one containing scripting code to redirect the session. Reference 22 details the process.

Figure 6.1 on the next page shows the result of installing the digital certificate.

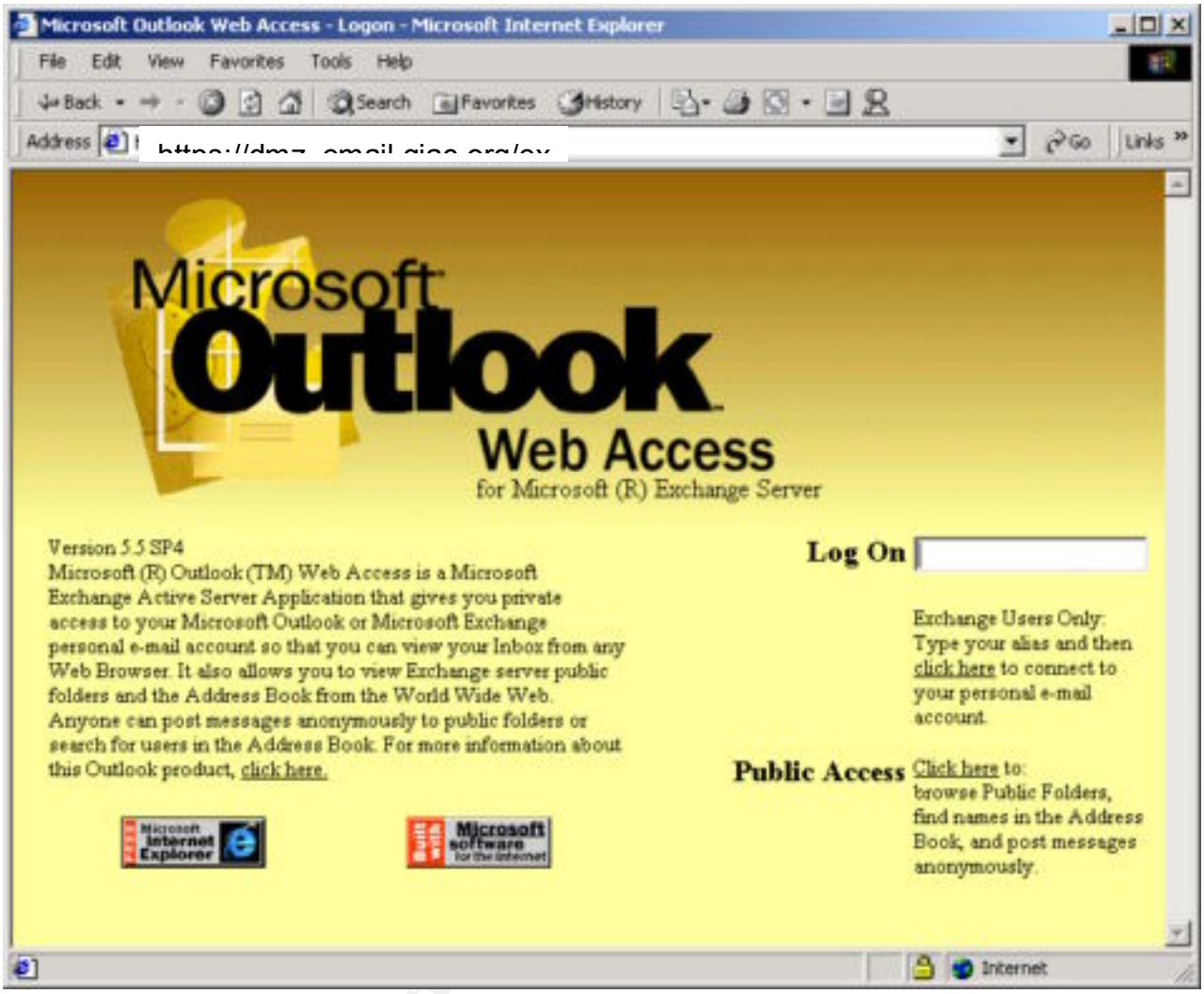

Figure 6.1 – Outlook Web Access Secure Site

Notice the yellow padlock near the bottom right corner symbolizing the session is SSL encrypted. The author apologizes for the lack of clarity in the figure.

6.2. Windows 2000 IPSec

Enabling IPSec can substantially increase the security posture of a network. It is argued that a properly configured IPSec network does not require a firewall. While this may be true a firewall will continue to be used at GIAC. The reader is reminded that IPSec is extremely verbose and complex. This section is a small glimpse of the functionality.

IPSec is implemented at the Network layer and…."protects not only the payload of a packet, such as email messages, but also port numbers, sequence numbers, session control flags, IP addresses, and other packet structures."[23]

IPSec is managed via the "IP Security Policies on Active Directory" MMC snap-in. This snap-in must be added manually to the console. Three default policies are included with Windows. They are:

- Client (Respond Only)
- Server (Request Security)
- Secure Server (Require Security)

The "Client (Respond Only)" policy tells network client machines to communicate without IPSec unless otherwise requested from the host server.

The "Server (Request Security)" policy causes computers to always request security for non-ICMP packets; but it will accept plaintext transmissions if the other host does not support IPSec.

The "Secure Server (Require Security)" policy will only send non-ICMP packets when those packets are secured with IPSec. Otherwise the sessions will fail.

These built-in IPSec policies will be used to get IPSec established on the network. Afterwards additional custom policies may be created as needed. However it is recommended that these three default policies be deleted and new ones created in their place. This is to avoid GUID problems related to backing up and restoring policies, etc. Microsoft has acknowledged this as a bug.[24] Therefore identical policies will be created from scratch and these three originals deleted.

Once the new policies are created they need to be enabled. IPSec can be enabled either on the local computer or through Group Policy. At GIAC the "Client (Respond Only)" policy will be enabled for the entire domain. This will act as a default IPSec response rule for every machine on the domain to use IPSec when requested to do so.

Recalling that OU policies overwrite the domain policy, the "Secure Server (Require Security)" policy will be assigned to the "Domain Controllers" and "Member Servers" OUs. This will cause all communication with DCs and member servers to be IPSec protected. Since GIAC has a Windows 2000 native domain and all servers and clients are Windows 2000 no internal sessions should fail.

Finally the "Server (Request Security)" policy will be enabled on the "Web Servers" OU. This will cause web sessions to use IPSec if possible but otherwise allow the session in cleartext. Recall that the web servers are middle-tier servers connecting to back-end SQL database servers. Since the SQL servers are contained in the "Member Servers" OU they will require IPSec encrypted sessions from the web servers. Thus all sessions between the web and database servers will always be protected.

7.0. Conclusions and Recommendations

7.1. Conclusions

Following these guidelines will yield a reliable, secure network for GIAC. The reader should consider the recommendations in this document as a minimum set of requirements. Many areas could be expanded upon. GIAC could benefit from many other additional technologies as the budget allows.

Since GIAC is an online business some consideration should be given to protection from Distributed Denial of Service (DDOS) attacks, Intrusion Detection Systems, and possibly a Layer-7 firewall or other Application Layer scanning device. Proper logging should aid in cost justification for any or all of these technologies. Furthermore if GIAC intends to bring the credit card transaction process in-house then all client information will need to be encrypted.

7.2. Recommendations

Security is a journey not a destination. There is always something else that can be implemented, tweaked or removed. The following subsections briefly describe some additional technology that could benefit GIAC.

7.2.1. Management and Staff Awareness

It is suggested that the top threat to any company is its own employee base. Either accidentally or on-purpose employees account for a majority of network incidents. A successful security initiative depends on many things but one of the most fundamental is upper management buy-in. They set the rules and tone of the company. If management says security is an important initiative then the employees will have no choice but to participate.

Good security is not the icing on the cake; it's the sugar in the mix. Getting an entire company to practice solid, secure computing techniques will go farther than any hardware appliance or piece of software. Most people are clueless when it comes to network threats and how to exploit them. Most overworked employees are completely disinterested. However they are usually willing and sometimes eager to learn new ways to use computers in their job; provided no added work is created for them.

Bundling network and computing efficiency with the security initiative can make implementing policy and procedural changes much easier. Training classes and "FYI" sessions will greatly increase company awareness and willingness to cooperate. Showing users that by learning a new way to compute they can save time and effort while making the company safer is motivational. It also makes them feel like they are part of a team working towards a common goal. This is exactly what a successful security initiative is all about: teamwork.

7.2.2. IDS, Honeypots and Log Analysis

Intrusion detection systems are a great tool for monitoring network traffic and detecting malicious activity. Several flavors are available depending on the requirements. Some IDSs can be bundled with a Honeypot system as well. A honeypot is a trap designed to lure hackers into subverting it while recording their steps in the process. Honeypot logs can provide a step-by-step record of the hackers' activity which may prove crucial when taking legal action.

A log analyzer would benefit GIAC considering the amount of logging being performed. Log analysis software can quickly scan myriad log files for specific events, signatures, etc. and concisely report the results.

7.2.3. Automatic patching

With the proliferation of Windows hotfixes administrators need a more efficient way to deploy them. Most administrators have neither the time nor resources to test and install every hotfix as it is released. Larger scale networks pose a real problem for timely and efficient hotfix management.

Products like UpdateEXPERT (http://www.updateexpert.com/) and Microsoft's Software Update Service (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q322365) will scan network devices for missing patches and automatically deploy them. Administrators have full control over times, dates, frequencies and whether or not to apply a patch at all.

7.2.4. Application Layer (Layer 7) Vulnerabilities

This is a relatively new area of concern. The focus is on Application Layer exploits (cross-site scripting.) Although a company may use a firewall, that firewall still allows traffic in, specifically port 80 (HTTP) traffic. SQL injection is one example of exploitation. For protection an Application Layer gateway scanning device (http://www.spydynamics.com) or a Layer 7 firewall that inspects all 7 packet layers is required.

8.0. References

1.) RAID-5
URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;Q100110

2.) NTFS
URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;Q100108
URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;Q300691

3.) IIS Lockdown tool:
URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp

4.) Fossen, Jason, Windows 2000/XP: Active Directory and Group Policy, Sans Institute, 2002.

5.) Network Address Translation (NAT)
URL:http://www.faqs.org/rfcs/rfc1631.html

6.) Print Services
URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/howto/fileprnt.asp

7.) Create a Certificate Server
URL:http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q313274&

8.) Configure CA to issue certificates
URL:http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q313274&

9.) Sites and Subnets
URL:http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q199174&

10.)Create and Configure an Active Directory Site:
URL: http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q318480&

11.)Create and Configure an Active Directory Site Link
URL: http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q316812&

12.)Configure Active Directory Site Link Replication
URL: http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q321253&

13.)Windows 2000 Group Policy Overview.
URL:http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/gpe_default.htm?id=1224

14.)GPO Administration
URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;q322143
URL:http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/575.asp

15.)Password Policies
URL: URL:http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/575.asp

16.)Securing Windows 2000 – Step by Step, Version 1.5, SANS Institute, 7/1/2001.

17.)Group Policy for Domain Controllers

URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q259576

18.)Create Third-Party Microsoft Installer Package (MSI)

http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q257718&

19.)Overview of Windows 2000 Default Security Templates

URL:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prdd_sec_umgs.asp

20.)Windows 2000 Templates must be applied incrementally

URL: http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q234926&

21.)VeriSign Digital Certificates for Outlook Web Access:

URL:http://www.verisign.com/support/site/secure/install.html

22.)Redirect OWA traffic to SSL encrypted secure site:

URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;Q298805

23.)IPSec Default Policies Should be Deleted

URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q232817

24.)Fossen, Jason, Windows 2000/XP: IPSec and VPNs, Sans Institute, 2002.