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: Matthew D. Arnold

12 March 2003

Table of contents

1.0 Introduction 3
1.1 Assumptions 3
2.0 Overview 3
3.0 Network Design and Diagram 4
3.1 Main Office Site 5
3.2 Warehouse Site 5
3.3 IP Scheme 6
3.4 Firewall 7
4.0 Servers and Client computers 7
4.1 Domain Controllers 8
4.2 External Web Server 9
4.3 Intranet Web Server 11
4.4 E-Mail Server 12
4.5 Database Servers 12
4.6 File and Print servers 12
4.7 Users computers 13
5.0 Active Directory Design 13
5.1 Forests 13
5.2 Domains 14
5.3 Recommended Design and Diagram 15
5.3 Organizational Units (OUs) 15
6.0 Group Policies 18
6.2 Default Domain Policies 18
6.3 Default Domain Controller Policies 21
6.4 External Web Server Policies 23
6.5 Task Based Workstation Group Policies 24
7.0 Additional Security Topics 25
7.1 Certificate Services 25
7.2 Remote Access 26
7.3 Encrypting File System (EFS) 26
7.4 Web based e-mail access 26
7.5 DHCP 27
7.6 Wireless 27
8.0 Conclusion 27
9.0 References: 28

1.0 Introduction

Bigger LAN Technologies (BLT) was engaged to design and implement a secure Windows 2000 network for GIAC Enterprises (GIAC) that will simplify operations, increase security, and provide ample room for growth. This document outlines the steps followed to secure the network.

1.1 Assumptions

This is a new implementation. No existing systems, equipment, or software are to be upgraded or considered. GIAC will provide any and all necessary communication links, network and power cabling. GIAC will provide any necessary computer systems (Servers, desktops, and laptops), backup devices, networking equipment. Servers and networking equipment will be placed within a temperature controlled server room with independent air handling and fire suppression systems in each site. Access to these rooms will be controlled through the use of third party card security systems. GIAC will provide all necessary software and licenses and will furnish any additional needed equipment or software.

2.0 Overview

GIAC Enterprises (GIAC) is a sandwich research and development company with approximately 300 employees. GIAC provides data analysis and research services for restaurants and food service supply companies. GIAC distributes surveys to food service professionals then enters the information that is collected into a database. The information in that database is then used to produce regional forecasts of sandwich consumption. The information contained within the databases is to be treated as client confidential.

Staff Requirements
BLT conducted interviews with relevant staff and developed this list of design requirements for the various departments.

Research & Development (R&D)– This group requires administrative access to internal and external websites and database servers. The second database server is solely for the use of the R&D staff. This group requires user access to fileserver2, and e-mail.

Sales and Marketing – This group requires administrative access to the external and user access to the internal websites. Remote access to e-mail and to certain folders and files contained on Fileserver1 is desired. This group requires user access to databases, fileserver2, and e-mail.

Finance and Human Resources – This group maintains the financial records, confidential employee and client information. Access to these records stored on Fileserver1 is to be restricted solely to these departments. Remote access to e-mail is desired. This group requires user access to internal websites, databases, fileservers and e-mail.

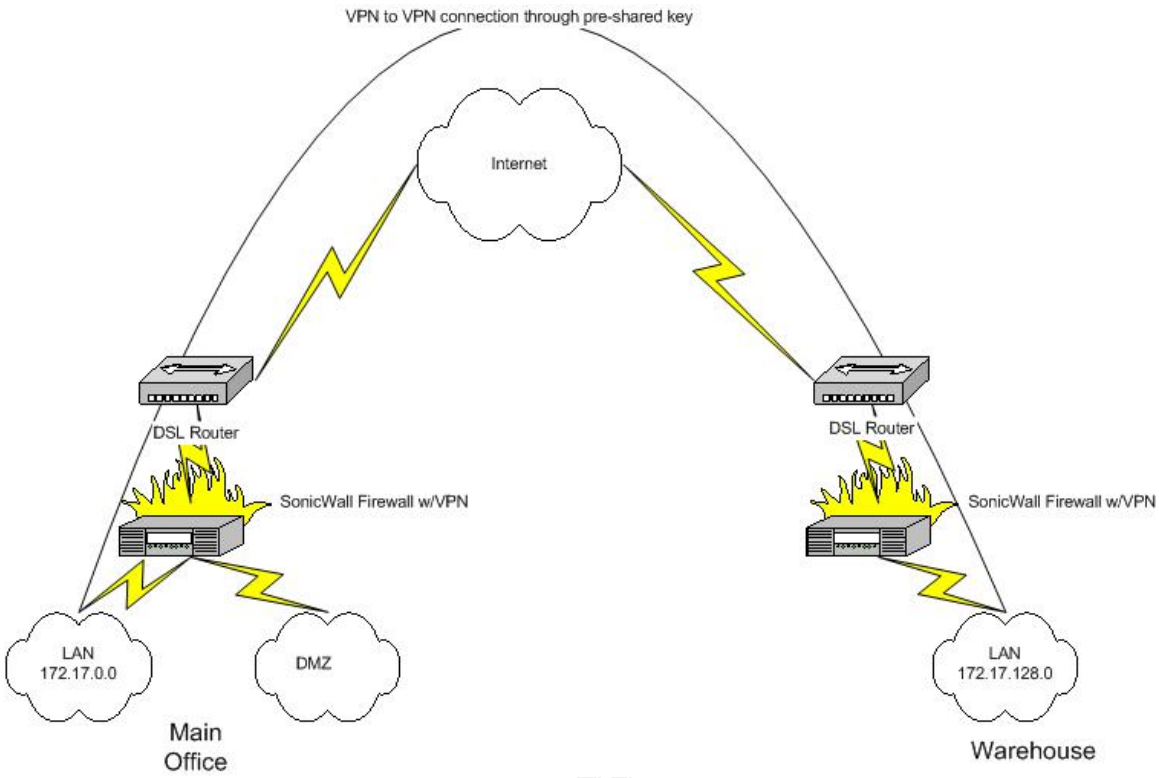
Executive – This group works in conjunction with the Sales, Finance and Human Resources groups. Administrative access to certain contents as it pertains to day-to-day operations of the company is required. Remote access to e-mail and to the files contained on Fileserver1 is desired. This group requires user access to internal websites, databases, fileservers, and e-mail.

Data Entry – This group requires user access to internal websites. This group is not to have access to the Internet, e-mail or be granted remote access to the network. This group requires user access to the intranet and user access to the databases.

Information Services – This group require administrative access to all GIAC internal and external servers. Remote access and remote administration to all network services and servers is desired.

3.0 Network Design and Diagram

GIAC has two offices, the main office and the warehouse. The close proximity of main office and warehouse to one another allows them to be connected through the use of high-speed (1.54Mbps) Symmetric Digital Subscriber Line (SDSL) connections. SDSL was selected because it provides the same speed upstream as downstream. A secure wide area network (SWAN) link has been established between these two sites crossing the Internet. The SWAN is a virtual private network (VPN) to VPN tunnel that allows two-way communication between the main office site and the warehouse site.



3.1 Main Office Site

The main office is located in Fairfax, Virginia. The main office houses approximately 200 employees and is the primary work location of the executive, administrative, marketing, and research & development group. The workstations in the main office location are general-purpose desktops with Internet connectivity.

3.2 Warehouse Site

The warehouse is located in Burke, Virginia. The warehouse houses approximately 100 employees and is the primary work location of the data entry employees. It is where surveys are received, sorted, logged, and then entered into the database. In addition to the data entry employees some management staff are located in the warehouse. The workstations in the warehouse location have no access to the Internet, and all web access is limited to the intranet. The data entry application they use is entirely web-based. A decision was made long ago to continue to purchase full PC's instead of implementing Terminal Services; this was to provide the company with the option to continue to work, through the use of a local Access database, in the case of any disaster.

3.3 IP Scheme

An IP address serves as an identifier for a computer or a device on a TCP/IP Network. GIACs internally assigned IP addresses will be using public IP addresses (Per RFC 1597 see references). Public IP addresses are specifically intended for use internally and are not owned by any company. Groups of these addresses are called classes, and the type of class determines the number of addresses that can be used (For example a class C subnet has 254 usable addresses). To allow for the two separate sites being connected via VPN the following network address scheme was used:

The Network address is:
172.17.0.0/17
Subnet Mask (The subnet mask is used to determine whether or not a host is local or remote, it also acts to define the number of hosts on a particular network)
255.255.128.0

This divides the single Class B into two subnets:
"Main" represents the physical location Main Office and the Active Directory Site of the same name. 172.17.0.0
"Warehouse" represents the physical location Warehouse and the Active Directory Site of the same name. 172.17.128.0

Each of these subnets provides 32766 IP addresses.

The following guide will be followed:

Default Gateways (The internal IP addresses of the Firewalls)
Main 172.17.0.1
Warehouse 172.17.128.1

Domain Controllers (Provide authentication) and DNS Servers (Provides host name to IP address resolution)
Main 172.17.30.1-10
Warehouse 172.17.130.1-10

File Servers (Stores users files in a centrally managed location on the network)
Main 172.17.40.1-10
Main 172.17.140.1-10

Web Server/SQL (Web servers provides access to data through a web browser and SQL is a server that hosts databases on the network for clients to access),
Main 172.17.50.1-10

Warehouse	172.17.150.1-10
Printers and other devices	
Main	172.17.60.1-254
Warehouse	172.17.160.1-254

DHCP (dynamically assigns IP Addresses and provides IP configuration information to clients)

DHCP Pool for Laptops	
Main	172.17.70.1-254
Warehouse	172.17.170.1-254
DHCP Pool for Desktops	
Main	172.17.80.1-254
Warehouse	172.17.180.1-254

3.4 Firewall

A firewall is a device on the network that prevents connections to your internal devices; it additionally can be used to monitor and control traffic between the internal (intranet) and the external network (internet). The firewall is configured to isolate the external IIS server into its own separate network called a DeMilitarized Zone (DMZ). The DMZ is a location on the network that can be reached through specific ports from the Internet and has limited access to the intranet. This acts as a one-way valve, providing access to resources from the Internet, but preventing users on the Internet from directly connecting to your internal network. The firewall is also configured to block most external ports, such as port 3389 (Terminal Services). External access to the internal network is only available through the use of VPN.

4.0 Servers and Client computers

BLT recommends that a total of eight servers be put into use throughout the enterprise. Two domain controllers to provide authentication, two web servers, two database servers, two file and print servers, and one e-mail server.

Default Hardware and Configuration
All servers are using a type of Hardware RAID (Redundant Array of Inexpensive Disks). RAID provides performance and redundancy. Two different types of RAID that are used in these configurations and RAID-1(a mirror set) and RAID-5 (a stripe set with parity).

RAID provides redundancy to data stored on hard disks. RAID-1 is a one to one copy of data across a minimum of two drives. RAID-5 takes the data and writes

it across a minimum of three drives additionally storing another copy of that data across all of those drives. The more drives you add to a RAID-5 set the more efficient the use of hard drive space.

All the servers are configured as follows:

- The servers are GIAC domain members.
- The servers are running Windows 2000 Service Pack 3.
- During the installation, the servers' hard drives were formatted as NTFS.
    - NTFS is a hard drive format that provides many security enhancements over FAT and FAT32. NTFS supports assigning permissions that allow administrators to restrict access to files and folders to specific users or groups.
- During the OS installation all additional components are removed. Following the OS installation the required components are added. For example on the Web Servers the IIS service is added after the OS installation.
- Following the configuration all servers are backed up nightly utilizing DLT Autoloaders.
- To safely shutdown the systems in the case of a power outage they are connected to a UPS (Uninterruptible Power Supply).
- To be able to limit the situations where you would need to be at the console to administer the servers, Terminal Services is installed in Remote Administration Mode.
- To prevent people outside of the organization from connecting to the servers via terminal services the port is blocked on the firewall.
- All servers are configured with anti-virus software.

4.1 Domain Controllers

Domain controllers store directory information, and provide authentication services to the domain. There are two domain controllers and both are global catalog servers. Global catalog servers store a replica of directory information that makes it possible for clients to logon to the domain. In this design one global catalog server is located in each site. This follows the recommendation of Microsoft that there be two global catalog servers to any single Exchange 2000 server. According to Microsoft's "*Exchange 2000 in six easy steps*" "As a general rule, at least one global catalog server should exist per Windows 2000 site*."*

Hardware and Configuration of Domain Controllers

- Each domain controller is configured with four hard drives, three configured as RAID-5 with one hot spare.
- Active Directory is in native mode, as there is no need to support NT 4.0 domain controllers in the domain.

- Active Directory Integrated DNS has been installed and configured on both servers. DNS has been configured to only allow secure updates to the GIAC.BIZ domain and Zone Transfers are enabled only to other name servers within the domain.
- The remote registry editing service is enabled, this service allows administrators to remotely look at event viewer logs on the servers, and to remotely stop and start services. Additionally it allows the registry to be manipulated remotely. While not a required service disabling this service on a domain controller is problematic.
- In order to support OWA (Outlook Web Access) being located in the DMZ and to prevent the default behavior of RPC dynamically using a port above 1024 for communications (The port selected for this is 49155). The following registry edit has been made on the domain controllers:

  HKEY_LOCAL_MACHINE\CurrentControlSet\Services\NTDS\Parameters
  Type: REG_DWORD
  Name: TCP/IP Port
  Value: 0000C003

4.2 External Web Server

The public website provides examples of the types of data gathered and analysis that can be produced and provides GIAC staff with access to Outlook Web Access (OWA). It provides contact information for potential clients, and a description of the company. It does not provide any information about the office network or internal e-mail addresses of individual staff. The public website has been placed within the DMZ of the main office.

Hardware and Configuration of the Public Web Server

- This server is configured with three hard drives, two configured as a RAID-1 with one hot spare.
- Three NTFS partitions are created:
  - OS
  - Exchange
  - Web directory (Inetpub)
- This server is located in the DMZ.
- This server hosts OWA (and therefore has Exchange 2000 installed) and the company's website.
- OWA is the only Exchange service the server will be providing; therefore the private and public folders have been dismounted and deleted.
- The remote registry editing service is disabled.
- The Client for Microsoft Networks is disabled.
- File and Print services are disabled.

- IISLockdown tool and URLScan secure the server.
- The following URLSCAN.INI file was used from Microsoft Knowledge Base Article "*IIS Lockdown and URLscan Configurations in an Exchange Environment*":

```
[Options]
UseAllowVerbs=1
UseAllowExtensions=0
NormalizeUrlBeforeScan=1
VerifyNormalization=1
AllowHighBitCharacters=1
AllowDotInPath=1
RemoveServerHeader=0
EnableLogging=1
PerProcessLogging=0
AllowLateScanning=0
[AllowVerbs]
GET
POST
SEARCH
POLL
PROPFIND
BMOVE
BCOPY
SUBSCRIBE
MOVE
PROPPATCH
BPROPPATCH
DELETE
BDELETE
MKCOL
[DenyVerbs]
[DenyHeaders]
If:
Lock-Token:
[DenyExtensions]
.asp
.cer
.cdx
.asa
.exe
.bat
.cmd
.com
.htw
.ida
.idq
.htr
.idc
.shtm
.shtml
.stm
.printer
.ini
.log
.pol
```

.dat
[DenyUrlSequences]
..
./
\
%
&

- An Anti-root kit application has been installed (Integrity Protection Driver.) That blocks any alteration to the kernel of the OS.
- Filter on Firewall between Internet and DMZ.
  - Set to block all external traffic to DMZ except for:
    - Port 80 (for serving websites) and Port 443 (for supporting secure access to websites)
- Filter on Firewall between DMZ and intranet.
  - Set to block all internal traffic between DMZ and Intranet except for:
    - Port 53 (DNS)
    - Port 80 (HTTP Traffic)
    - Port 88 (Kerberos Authentication)
    - Port 135 (RPC endpoint mapper Authentication)
    - Port 389 (Active Directory LDAP)
    - Port 3268 (Global Catalog LDAP)
    - Port 49155 (RPC service port)

- The web server requires an anonymous user account in order to provide access to public information on the website. In order to provide more security anonymous access is through a local account on the server as opposed to using a domain account.
- The default administrative shares on the server have been removed. This prevents people from trying to exploit them to gain administrative access to the web server.

4.3 Intranet Web Server

The intranet provides web access to the database server. Data entry users update information stored on the main office database server from the warehouse.

Hardware and Configuration of the Intranet Web Server

- This server is configured with three hard drives, two configured as a RAID 1 with one hot spare.
- Two NTFS partitions are created, this allows the OS to be installed on one partition isolated from the “Inetpub” directory on the second partition.
- This server is hosting the intranet web pages.

- This server is hosting the SQL front-end.
- The remote registry editing service is enabled.
- Client for Microsoft Networks is enabled.
- The File and Print services are disabled.
- The IISLockdown tool and URLScan secure the server.

4.4 E-Mail Server

The e-mail server provides e-mail, calendar, scheduling, and public folders to all non-data entry staff. It is located within the main office site.

- This server is configured with eight hard drives, two pairs configured as RAID 1, three configured as RAID 5 and one hot spare.
- The OS is installed on one RAID 1, the transaction log database is stored on the second RAID 1, and the Exchange Information Stores is stored on the RAID 5.

4.5 Database Servers

There are two database servers, the live production database and the development database. Both servers are located within the main office site.

- These servers are configured with eight hard drives, two pairs configured as RAID 1, three configured as RAID 5 and one hot spare.
- The OS is installed on one RAID1, the transaction log database is stored on the second RAID 1, and the databases are stored on the RAID 5.

4.6 File and Print servers

There are two file and print servers, one located in each site.

- These servers are configured with 6 hard drives, two configured as RAID 1, and three configured as RAID 5 and one hot spare.
- The file and print server in the main office is configured with separate partitions for Finance and Human Resources data.

4.7 Users computers

There are 240 users' desktop computers and 60 laptops within the organization. All computers in the warehouse location are desktops.

- All users computers are running Windows XP Professional SP1.
- All users computers hard drives have been formatted NTFS.
- Anti-Virus Software installed.
- XP Professional Office Suite installed.
- All other unnecessary services are disabled. (Telnet, Alerter, Messenger, etc)
- All unnecessary applications are removed. (Outlook Express, etc)

5.0 Active Directory Design

Active Directory allows GIAC to simplify management of users and resources. It also creates a secure and scalable infrastructure. In this section, BLT will provide definitions of Group Policy, forests, domains, and organizational units.

Group Policy Objects (GPO) allow administrators and users delegated the role of editing GPO's the ability to control the end users experience with Windows XP within the domain. It provides the ability to disable unnecessary services, to install applications, to redirect folders from the local computer to the network, to change what a user sees to set a default desktop, ultimately all of this is designed to lower the cost of supporting the equipment, by tightly regulating and controlling the applications installed on the workstation it provides a more homogenous environment, a user will be prevented from installing a piece of software that could render his computer unusable, a user would be prevented from purposefully or inadvertently damaging the system, a desktop could very readily be replaced from stock with little loss of productivity. Less time spent troubleshooting problems equates to less time at the users desktop.

5.1 Forests

A forest is a logical grouping of domains. The following definition is taken from Microsoft's "*Best Practice Design Guide*":

> *A forest is a collection of one or more Windows 2000 Active Directory trees, organized as peers and connected by two-way, transitive trust relationships. A*

single domain constitutes a tree of one domain, and a single tree constitutes a forest of one tree. Thus, a forest is synonymous with Active Directory — that is, the set of all directory partitions in a particular directory service instance (which includes all domains and all configuration and schema information) makes up a forest.

5.2 Domains

A domain is a logical grouping of users, computers, OUs (defined below), and other resources. The following definition is taken from Microsoft's TechNet, "*Windows 2000 Server Distributed Systems Guide, Chapter 1 - Active Directory Logical Structure*"

In Windows 2000, a domain defines both an administrative boundary and a security boundary for a collection of objects that are relevant to a specific group of users on a network. A domain is an administrative boundary because administrative privileges do not extend to other domains. It is a security boundary because each domain has a security policy that extends to all security accounts within the domain. Active Directory stores information about objects in one or more domains.

Domains can be organized into parent-child relationships to form a hierarchy. A parent domain is the domain directly superior in the hierarchy to one or more subordinate, or child, domains. A child domain also can be the parent of one or more child domains, as shown in Figure 1.

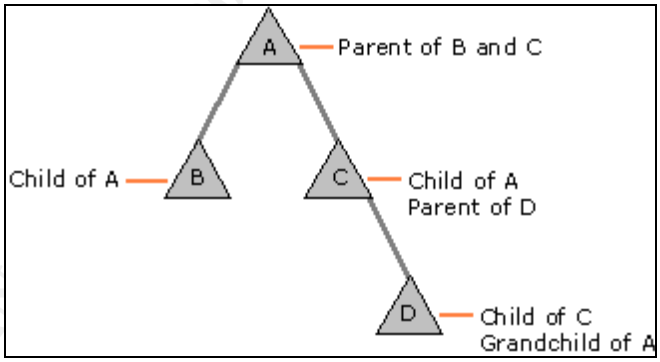


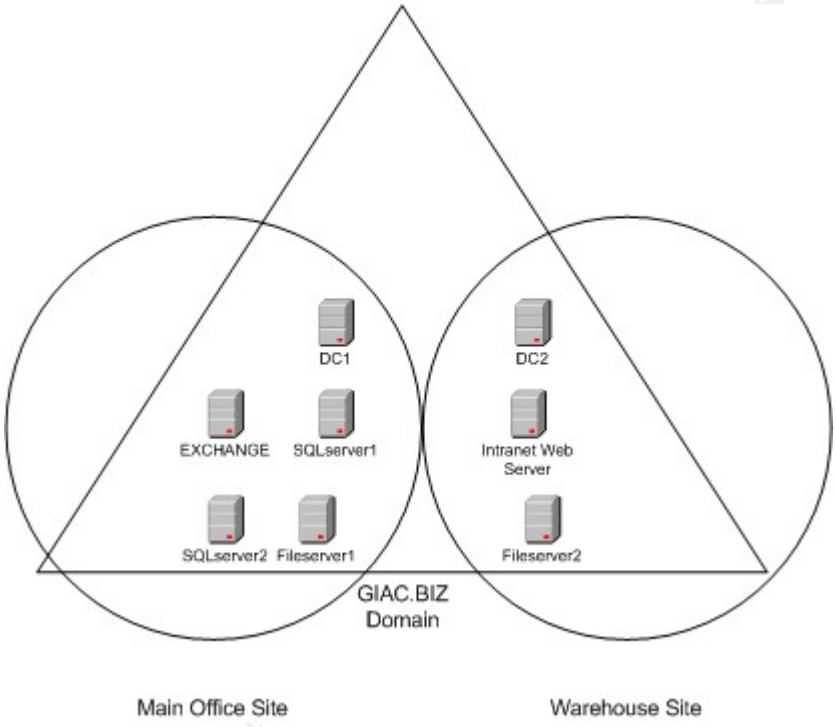
Figure 1

This hierarchical structure is a change from the flat domain structure of Microsoft Windows NT 4.0 and Microsoft Windows NT 3.51. The domain hierarchy of Windows 2000 allows you to search multiple domains in one query because each level of the hierarchy has information about the levels that are immediately above it and below it. This hierarchy information eliminates the need for you to know the location of a particular object in order for you to find it. In Windows NT 4.0 and earlier, you must know both the domain and the server where the object is located in order to find it.

5.3 Recommended Design and Diagram

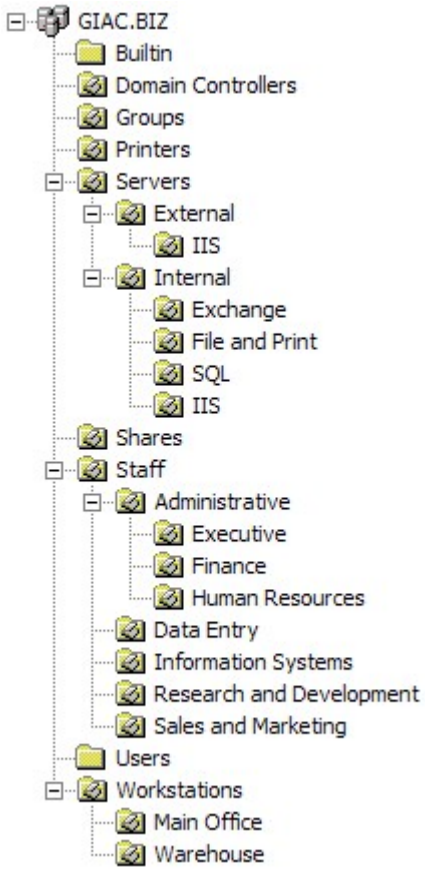
A Single Forest, Single Domain design as shown below is recommended. This design means fewer domain controllers are required to provide authentication and to replicate directory information.

Two Active Directory Sites are defined using the two subnets mentioned earlier in the IP Scheme section. DC1 is placed in the Main Office (Main) site and DC2 is placed in the Warehouse site.



5.3 Organizational Units (OUs)

An OU is a container of Active Directory objects (users, groups, computers, printers, and file shares) that can be managed as a single unit. The OU is the smallest unit within which you can delegate administrative and maintenance tasks. OUs appear as folders within the Active Directory Users and Computers utility.



The Organizational Unit Structure is modeled after the organization chart of the company.

- The Builtin Container contains default Windows 2000 group account objects.
- The Domain Controllers OU contains computer objects of Domain Controllers.
- The Groups OU contains group objects representing groups in use throughout the company. These groups are used to control access to resources on the domain.
- The Printers OU contains printer objects representing printers in use throughout the company.
- The Servers OU tree contains all the different types of servers within the organization these are initially divided into location OUs.
- The Internal OU contains OUs that designate the type of server being used internally without being accessible from the Internet.
    - The Exchange OU contains the computer object for the Exchange mail server.
    - The File and Printer OU contains the computer object for the file and print servers.
    - The SQL OU contains the computer object for the SQL Database servers.

    - The IIS OU contains the computer object for the Intranet Web server.
- The External OU contains OUs that designate the type of server being used externally-meaning these servers are accessible from the Internet.
    - The IIS OU contains the computer object for the Internet Web server.

The Shares OU contains folders that are accessible throughout the company.

The Staff OU contains OUs representing the five different departments.

- Administrative OU contains OUs representing the three different departments.
    - Executive OU contains user account objects-members of the Executive department.
    - Finance OU contains user account objects-members of the Finance department.
    - Human Resources OU contains user account objects-members of the Human Resources department.
- Data Entry OU contains user account objects-members of the Data Entry department.
- Information Systems OU contains user account objects-members of the Information Systems department.
- Research and Development OU contains user account objects-members of the Research and Development department.
- Sales and Marketing OU contains user account objects-members of the Sales and Marketing Department.

The Workstations OU tree contains all the different types of workstations within the organization. These are initially divided into location OUs.

- Main Office contains computer objects in use in the main office site.
- Warehouse contains computer objects in use in the warehouse site.

The Users container contains default Windows 2000 user account objects as well as service accounts in use throughout the organization.

Organization Units provide the ability to quickly assign Group Policy Objects (GPOs) based upon group membership. Verifying a user has been added to a particular group is no more intensive than seeing if they exist in the appropriate OU.

If any object (User, Computer, Printer, or Share) is placed within an OU, any GPO that is linked to that OU based upon the “Apply Group Policy” security permission is applied.

The Servers and Workstations OUs are designed to ease administration of GPOs, i.e. by placing a newly created/joined computer object within the Exchange OU, the Exchange Computer GPO is automatically assigned to it. (In this instance the system is going to be an Exchange server, so adding a windows

2000 server to the OU prepares the server for the installation of Exchange 2000 by applying security updates and making other configuration changes consistently).

This reduces the amount of time it takes to place a server into production. You assign the default password and account policies at the domain level, you can assign the policies that disable the "same" set of services at the "Server" OU level, you assign additional GPO's at the "internal" and "external" OU level, than the "Exchange" OU level has a much smaller GPO which applies only changes SPECIFIC to exchange servers.

The workstations are divided up by location. The majority of users are in the main office; the number of printers within each location is minimal. Printer assignments are accomplished on each workstation through a GPO linked to a VB Script that runs as a login script for the computer. The GPO runs against the computer account as though it were a user account. Then the printer is created regardless of which user logs onto the machine, effectively tying the printer to the computer.

6.0 Group Policies

Windows 2000 Active Directory includes two default GPOs. These GPOs are the Default Domain GPO and the Default Domain Controller GPO. From Microsoft's "*Step-by-Step Guide to configuring Enterprise Security Policies*"

> Account policies (password, lockout, Kerberos) are defined for the entire domain in the default domain GPO. Local policies (audit, user rights, and security options) for DCs are defined in the default DC GPO. For DCs, settings defined in the default DC GPO have higher precedence than settings defined in the default domain GPO. Thus, if you were to configure a user right (for example, Add workstations to domain) in the default domain GPO, it would have no impact on the DCs in that domain.

6.2 Default Domain Policies

Default Domain Group Policy Object

This policy applies to all objects in the domain. The domain security policy contains a consensus from both the Microsoft Common Criteria Security Policies and the National Security Agency (NSA) Domain Security Policy. What follows is a description of the policies and their settings.

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

Enforce Password History- Determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. Default is 1 this value is changed to 24 per NSA recommendations. Using a high number prevents users from reusing a small set of passwords for domain access.

Maximum Password Age- Determines the number of days that a password can be used before the system requires the user to change it. By default this policy is set to 42 days this value is changed to 90 per NSA recommendations.
This is to minimize problems associated with changing passwords, increasing the frequency of this policy leads to more administrative overhead in resetting passwords and the like.

Minimum Password Age- Determines the number of days that a password must be used before a user can change it. By default this policy is set to 0 this value is changed to 1 per NSA recommendations, Additionally this setting must be set to a value of more than 0 for the "Enforce Password History" setting to be effective. This is to enable "Enforce Password History" listed earlier in this section. Additionally prevents users from easily circumventing password history by changing their passwords repeatedly enable to quickly cycle through a list and reuse an old one.

Minimum Password Length- Determines the minimum number of characters a user account's password must contain. By default this policy is set to 0 this value is changed to 8 per Microsoft Common Criteria Domain Security Policy. Increasing the password length increases the amount of time necessary to "guess" a password through the use of "brute force" cracking tools.

Passwords Must Meet Complexity Requirements of the Installed Password Filter- Determines whether or not passwords must meet the following criteria:

Must not contain your user name or any part of your full name
Must contain characters from at least three of the following four types:

Character Types	Examples
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
Westernized Arabic numerals	0, 1, 2, ... 9
Non-alphanumeric characters (special characters)	$,!,%,^

Complexity requirements are enforced upon password change or creation.
By default this policy is disabled, this setting is changed to enabled per Microsoft Common Criteria Domain Security Policy.
This prevents users from using their user account with a number or special character on the end, thus forcing users to create difficult-to-guess passwords.

Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy

Account Lockout Threshold- Determines the number of failed logon attempts that will cause a user account to be locked out. By default this policy is disabled, this is changed to enabled after 5 attempts per High Security Microsoft Common Criteria Domain Security Policy.
Setting this number to 5 reduces the amount of time administrators spend resetting users accounts, additionally setting an account lockout threshold helps to thwart "brute force" attacks.

Account Lockout Duration- Determines the amount of time (in minutes) a locked out account remains locked out before automatically becoming unlocked. By default this policy is not defined, this is changed to 15 minutes per NSA Domain Security Policy.
Setting this to 15 minutes reduces the amount of time administrators spend resetting user accounts, additionally setting the duration helps to thwart "brute force" attacks.

Reset Account Lockout After- Determines amount of time (in minutes) that must elapse after a failed logon attempt before the bad logon attempt counter is reset to 0 bad logons. By default this policy is not defined, this is changed to 15 minutes per NSA Domain Security Policy.
See Account Lockout Duration for additional explanation.

Computer Configuration\Windows settings\Security settings\Local Policies\Security options

Do not display last user name in logon screen Enabled
Message text for users attempting to log on Enabled
Message is modified from "*Creating Login Banners*" by CIAC (see references):

"This computer system is the property of GIAC Enterprises. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, GIAC, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign.

By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or GIAC personnel.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these term and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning."

Message title for users attempting to log on Enabled
Title: "NOTICE TO USERS"

6.3 Default Domain Controller Policies

Default Domain Controller Group Policy Object

This security policy contains a consensus from both the Microsoft Common Criteria Security Policies and the NSA Domain Security Policy. What follows is a description of the policies and their settings.

Computer Configuration\Windows settings\Security settings\Local Policies\Security options

Additional restrictions for anonymous connections Set to “No access without explicit anonymous permission”	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Restrict CD-ROM access to locally logged-on user	Enabled
Restrict floppy access to locally logged-on user	Enabled
Send unencrypted password to connect to third-party SMB servers	Disabled
Strengthen default permissions of global system objects	Enabled

Computer Configuration\Windows Settings\Security Settings\System Services

Alerter	Set to Disabled
Clipbook	Set to Disabled
DNS Server	Set to Automatic
Fax Service	Set to Disabled
File Replication Service	Set to Automatic
Indexing Service	Set to Disabled
Internet Connection Sharing	Set to Disabled
Kerberos Key Distribution Center	Set to Automatic
Logical Disk Manager	Set to Manual
Logical Disk Manager Administrative	Set to Automatic
Messenger	Set to Disabled
Net Logon	Set to Automatic
Remote Procedure Call Locator	Set to Automatic
Remote Registry Service	Set to Automatic
Removable Storage	Set to Disabled
Routing and Remote Access	Set to Disabled
Simple Mail Transport Protocol	Set to Disabled
Smart Card	Set to Disabled
Smart Card Helper	Set to Disabled
Telnet	Set to Disabled
Terminal Services	Set to Automatic
Uninterruptible Power Supply	Set to Disabled
Utility Manager	Set to Disabled

Windows Management Instrumentation Driver Extensions Set to Manual
Windows Time Set to Automatic

Computer Configuration\Administrative Templates\Windows Components\NetMeeting

Disable remote desktop sharing Enabled
Prevents users from being able to setup NetMeeting and share the desktop.

Computer Configuration\Administrative Templates\Windows Components\Internet Explorer

Disable automatic install of Internet Explorer components Enabled
Disables the automatic installation of possible harmful components.

Computer Configuration\Administrative Templates\Windows Components\Task Scheduler

Disable new task creation Enabled
Prevents the creation of new tasks on the server.

Computer Configuration\Administrative Templates\System

Disable Autoplay Enabled
Prevents the CD Autoplay feature, which could launch scripts or applications.

Computer Configuration\Administrative Templates\System\Logon

Delete cached copies of roaming profiles Enabled
Prevents the system from maintaining a local copy of a users roaming profile.

Computer Configuration\Administrative Templates\System\Windows File Protection

Set Windows File Protection (WFP) scanning Enabled
Set to “At startup”
This will enable WFP to scan system software for changes every system startup. WFP only scans when the current user is a local administrator.

User Configuration\Administrative Templates\Windows Components\Internet Explorer

Do not allow AutoComplete to save passwords Enabled

Prevents the AutoComplete feature from saving passwords.

6.4 External Web Server Policies

External Web Server Group Policy Object

This security policy contains a consensus from both the Microsoft Common Criteria Security Policies and the NSA Web Security Policy. What follows is a description of the policies and their settings.

Computer Configuration\Windows Settings\Security Settings\System Services

Alerter	Set to Disabled
Clipbook	Set to Disabled
Distributed File System (DFS)	Set to Disabled
DNS Client	Set to Enabled
Fax Service	Set to Disabled
File Replication Service	Set to Disabled
Indexing Service	Set to Disabled
Internet Connection Sharing	Set to Disabled
Kerberos Key Distribution Center	Set to Disabled
Logical Disk Manager	Set to Manual
Logical Disk Manager Administrative	Set to Automatic
Messenger	Set to Disabled
Net Logon	Set to Automatic
NetMeeting Remote Desktop Sharing	Set to Disabled
NTLM Security Support Provider	Set to Disabled
QoS Admission Control	Set to Disabled
Remote Procedure Call Locator	Set to Disabled
Remote Registry Service	Set to Automatic
Removable Storage	Set to Disabled
Routing and Remote Access	Set to Disabled
Simple Mail Transport Protocol	Set to Disabled
Smart Card	Set to Disabled
Smart Card Helper	Set to Disabled
Telnet	Set to Disabled
Terminal Services	Set to Automatic
Uninterruptible Power Supply	Set to Disabled
Utility Manager	Set to Disabled
Windows Management Instrumentation Driver Extensions	Set to Manual

The following services are Exchange 2000 specific and will need to be set manually on the external web server:

Microsoft Exchange Event	Set to Disabled
Microsoft Exchange IMAP4	Set to Disabled
Microsoft Exchange Information Store	Set to Disabled
Microsoft Exchange Management	Set to Disabled
Microsoft Exchange Message Transfer Agent Stacks	Set to Disabled
Microsoft Exchange POP3	Set to Disabled
Microsoft Exchange Routing Engine	Set to Automatic
Microsoft Exchange Site Replication Service	Set to Disabled
Microsoft Exchange System Attendant	Set to Automatic

6.5 Task Based Workstation Group Policies

Task Based Workstation Group Policy Object

The task-based workstations located within the warehouse location are all running Windows XP. A GPO is assigned to the Warehouse workstations that limit them to only the applications and features needed to do a single task. Users are required to log off their systems when they are away from them. The Microsoft Office XP Suite is installed locally and use of MS Access and Internet Explorer is allowed.

Windows XP did not exist when Windows 2000 was first released. Enable to support the new additional Group Policy Options for XP Microsoft created a new administrative template that needs to be loaded before these changes can be made.

New specifically to Windows XP is the inclusion of software restriction policies that enable administrators to identify which applications that are allowed to run on the computers. It also allows for enhanced control of the Start Menu and the Taskbar.

User Configuration\Administrative Templates\Start Menu and Task Bar

Remove programs from start menu — Set to Enabled

This setting removes the Control Panel, Printers, and Network and Connection folders from Settings on the Start menu, and from My Computer and Windows Explorer. It also prevents the programs represented by these folders (such as Control.exe) from running.

User Configuration\Administrative Templates\Control Panel

Prohibit access to the control panel — Set to Enabled

This setting prevents Control.exe, the program file for Control Panel, from starting. As a result, users cannot run any Control Panel items.

User Configuration\Administrative Templates\System

Prevent access to the command prompt Set to Enabled

Run only allowed windows applications Set to Enabled
List contains: iexplore.exe and msaccess.exe
This setting allows the users to only run Internet Explorer and Microsoft Access on the workstations. It also prevents users from installing software.

User Configuration\Administrative Templates\System\Ctrl+Alt+Del Options

Remove lock computer Set to Enabled
This grays out the Lock Computer button when the user presses Ctrl+Alt+Del.

Note: This does not as it states on the Explain Tab prevent users from pressing the WinKey+L to lock the system. The following registry key has been added to the workstations to prevent the use of the Windows Key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ Keyboard Layout
Type: Binary
Name: Scancode Map
Value: 00 00 00 00 00 00 00 00 03 00 00 00 00 00 5B E0 00 00 5C E0 00 00 00 00

7.0 Additional Security Topics

Security within any organization is important; BLT believes that through defense in depth, the possibilities of breaches can be minimized.
The following Security guidelines were followed:

Perimeter security: The use of a firewall to prevent unauthorized traffic internally and externally.

Physical security: The locations of the servers provide access limited to IS personnel.

File and Share Level Security: The use of NTFS permissions and group memberships to restrict access to correct personnel.

7.1 Certificate Services

Incorporating certificate services into any security plan can be expensive, other consulting agencies recommend the use of third party certificate authorities to issue digital certificates that effectively guarantee that the computer connecting to your network has a valid certificate and are authorized on your network. BLT believes that the proper use of certificates can be accomplished inexpensively and securely through the use of a Windows 2000 Digital Certificate Server. BLT recommends that this server be used to issue strong certificates (1024 bit) only and that the system that is used is then disconnected from the network and stored in a secure offsite location. Alternately, if faster access is needed the removable hard drive of the server should be placed within the CSO (Chief Security Officer) fire safe.

7.2 Remote Access

Remote access will be secured through the issuance to each user a unique digital certificate, VPN with a random token generator (SecurID), and Kerberos password. This provides three tiers of security that will only require the user to provide a single password. A USB key-chain device will be issued to the user plugging that in to the USB port of their laptop or desktop machine will provide access to the digital certificate. The user will be issued instructions for the installation of the SonicWall client, and then provided with a SecurID card, a temporary password will be issued to the user, which upon successful connection to the network will prompt the user to change the password.

7.3 Encrypting File System (EFS)

EFS adds an additional layer of security on top of NTFS permissions. With EFS users can encrypt files or directories so that only they can open them. EFS does not require constant user interaction. After a folder is set as encrypted any files that are placed within the directory are secured. If the user cuts and pastes information to removable storage that is not formatted to NTFS the file is no longer encrypted.

7.4 Web based e-mail access

Exchange 2000 has a feature called Outlook Web Access (OWA). OWA allows users to connect to a web page to view their mail. Additionally it allows access to the Public Folders, Contacts, and Scheduling information.

The use of digital certificates and SSL (Secure Socket Layer) technologies, will enhance the security of their connection, SSL is an agreement between a client computer and a sever computer that the data sent between the two will be encrypted, the use of a digital certificate adds an additional layer, requiring the user to provide this virtual "ID" card to be allowed to connect to the server.

7.5 DHCP

Windows 2000 DHCP supports user specified and vendor specified option classes. Option classes allow administrators to group DHCP options for similar clients within a DHCP scope. The DHCP client needs to set a Class ID that matches one set up on the DHCP Server. This can be used to place Laptops on a separate subnet, or to point task-based workstations to a DNS that does not resolve IP addresses externally. To enhance security this could be used to lock-down DHCP by requiring that all clients have a Class ID specified, and if they do not issue them bogus information.

7.6 Wireless

Wireless networking is becoming increasingly popular with businesses; it provides the flexibility to carry your desktop throughout the office while maintaining network connectivity. Unfortunately it also means you're broadcasting your communication on the network in a 200 foot radius around your laptop. That means a criminal doesn't even need to physically touch your system in order to glean information from it. Another similar security problem is IR ports on both PDAs and Laptops, using tools people can connect to your device and read the information stored on it. To combat this type of problem, the Wireless Access Point (WAP)(the device that acts as a bridge between the wired network and the wireless network for the client) should not be placed in the internal network; it should be placed within the DMZ and treated exactly the same way a VPN user is treated. Users with Wireless cards will be required to logon to the network using VPN software. In addition the WAP will be configured with high encryption (WEP) and maintain a list of MAC addresses, for devices allowed to connect.

8.0 Conclusion

BLT has implemented and designed GIACs' network for growth and security. Windows 2000 and it components provides the basis for that. Through

the use of Active Directory and Group Policy, GIAC will be able to respond quickly to security threats, and easily administer its systems.

Network Administration

A single domain containing multiple Organization Units (OUs) provides opportunities to reduce time administering users and groups within departments. Administrators can choose to delegate authority over objects contained within OUs to other groups and/or users. Resetting passwords, changing group memberships, can be assigned to other staff members freeing up Administrators for other tasks. Fewer domains reduce the number of servers to backup, and maintain, which ultimately lowers costs.

Performance

This design provides the best performance because of its simplicity. The Organization Unit design is only four levels deep providing fast responses to queries. Replication takes less time to complete in this design. The Global Catalog servers, one in each site, mean users spend less time directly querying Active Directory for information.

Security

This design means there are fewer domain administrators maintaining fewer password policies, and monitoring fewer event logs. Two sites, each with its own domain controller, reduce the frequency of authentication traffic crossing WAN links. The use of Organizational Units linked with GPO's provides flexibility and consistency when applying security settings.

9.0 References:

"*Using Microsoft Exchange 2000 Front-End Servers*" by the Microsoft Corporation.
"*Microsoft Solution for Systems Architecture: Internet Data Center*" by the Microsoft Corporation.
"*Windows 2000 Active Directory*" by Alistair G. Lowe-Norris published by O'Reilly.
"*Microsoft TCP/IP for Windows 2000*" by Keith A. Powell published by PrimaTech.
"*Microsoft Windows 2000 Administrator's Pocket Guide*" by William R. Stanek published by Microsoft Press.
"*Securing Windows 2000 Step-by-step guide*" by the SANS Institute.
"*Creating Login Banners*" by United States Department of Energy and the CIAC.
"*RFC 1597*" by the Internet Engineering Task Force (IETF)

Last Updated: July 28th, 2017

Upcoming Training

SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**