Securing Windows
GCNT Practical Assignment

Tim Kwiatkowski

Design of a Secure Windows 2000 Infrastructure

Version 3.0

This paper will discuss the design of a secure Windows 2000 infrastructure for a fictitious company called "GIAC Enterprises". GIAC Enterprises is an e-business that deals in the design, development and online sale of Fortune Cookie sayings.

I will detail a proposed secure network design, Active Directory design and group policy security.

Background:

GIAC Enterprises has its main office in California and a Research and Development facility located in China. The GIAC Enterprises organization consists of the following departments:

Research and Development – The R&D group consists of psychics and engineers responsible for the design and development of new fortunes and the development of new innovative online fortune technologies.

Sales and Marketing – Responsibilities include customer relations and management, while increasing GIAC Enterprises share of the online fortune market.

Finance – Provides internal accounting functions.

Human Resources – Tracks all employee records and OSHA related issues.

Information Systems – The Information Systems department includes programmers, web developers, a network administrator and several desktop support employees.

Network Design and Diagram

The GIAC Enterprises network design is based on the guidelines outlined in the NSA "Microsoft Windows 2000 Network Architecture Guide" produced by the Systems and Network Attack Center (SNAC). This document can be found at: http://nsa1.www.conxion.com/win2k/guides/w2k-1.pdf.

The basic GIAC network consists of 2 segregated networks. The primary function of the network in the US Main Office is to provide the majority of network services to both sites, i.e. the public and test Web Servers, Mail services and domain administration. Although most server services are provided from the US network, a small File and Print server is located locally in the China Research and Development office to provide local file and print sharing.

Each site is linked via a dedicated T1 to the Internet. A Cisco PIX Firewall at each site provides secure site-to-site routed connectivity between each location.

Figure 1, is an illustration of the network configuration.

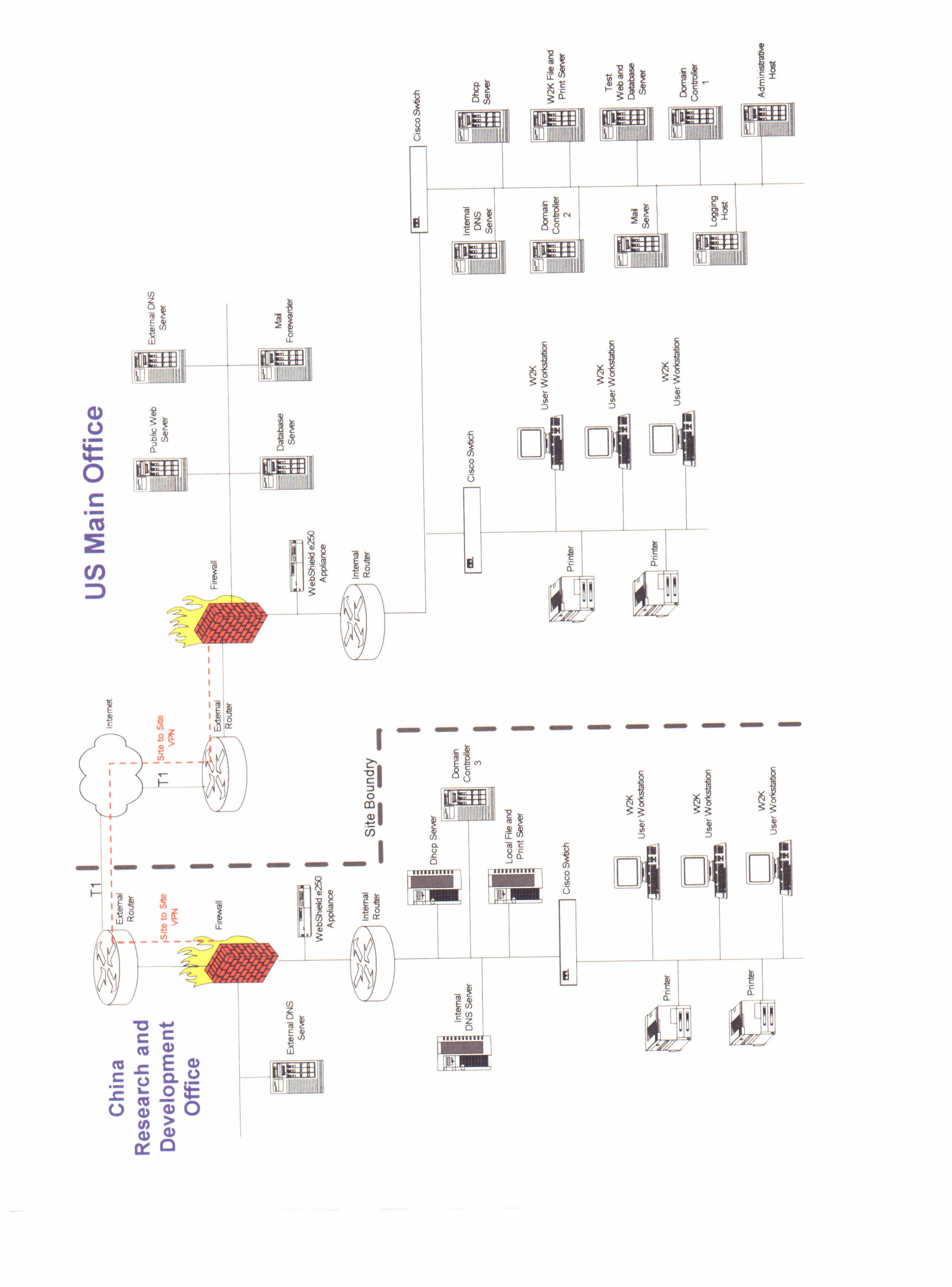

US Main Office
China Research and Development Office
Internet
T1
T1
Site to Site VPN
Site to Site VPN
External Router
External Router
Firewall
Firewall
WebShield e250 Appliance
WebShield e250 Appliance
Internal Router
Internal Router
Public Web Server
External DNS Server
Database Server
Mail Forewarder
Cisco Switch
Internal DNS Server
Dhcp Server
W2K File and Print Server
Domain Controller 2
Test Web and Database Server
Mail Server
Domain Controller 1
Logging Host
Administrative Host
Cisco Switch
W2K User Workstation
W2K User Workstation
W2K User Workstation
Printer
Printer
Site Boundry
External DNS Server
Internal DNS Server
Dhcp Server
Domain Controller 3
Local File and Print Server
Cisco Switch
W2K User Workstation
W2K User Workstation
W2K User Workstation
Printer
Printer

Figure 1

The following is an overview of the important aspects of the GIAC network configuration and notes on certain component functionality.

Routers and Firewalls

External Routers: This device provides the initial screening of incoming traffic to the internal networks. Each external router provides protection to the internal network from IP address spoofing, Denial of Service Attacks and connections to unauthorized services.

Each external and internal router is a Cisco 1751. All routers have Intrusion Detection logging enabled and save all of the IDS logged information to the Logging Host located on the internal US network.

Internal Routers: The internal routers in both the US and China provide an extra level of protection from *insiders* to the DMZ and the external routers and Firewalls.

As with the external routers, Intrusion Detection logging has been enabled and all logs are stored on the Logging Host.

Firewalls: There are 2 Firewalls (one in the US and one in China). Both Firewalls contain 3 network interfaces, one to the unprotected Internet, one for the DMZ and one for traffic routed to the local network. Each Firewall is a Cisco PIX (Private Internet Exchange) 515.

The Firewalls are configured to perform **Network Address Translation** (NAT), to preserve IP address space and prevent mapping of the internal networks from outside entities.

In addition, the Firewalls are setup to provide a secure IPSec based **site-to-site secure VPN connection** between the US and China sites.

Lastly, the Cisco PIX Firewalls provide "**Stateful Inspection**" of all inbound and outbound packets. Stateful Inspection intercepts packets at the network layer and creates a "stateful session flow table" within the Firewall to track each IP connection. Thereafter, all inbound packets are compared against the session flows in the connection table and are permitted through the Cisco PIX only if an appropriate connection exists to validate their passage. The connection object in the flow table is released once the connection is terminated.

The US Firewall only allows the following inbound services to the US DMZ:
SSL HTTP SMTP IPSec

The Firewall in China does not provide any inbound services to the China DMZ. The external DNS server is the only device required in the China DMZ.

Servers in the DMZ

The DMZ (Demilitarized Zone) is setup to protect public GIACNET.COM servers from an untrusted environment (i.e., the Internet).

All of the servers located in the DMZ are not part of the local Active Directory domain. They are all stand-alone servers that are protected via local security policies. These servers can only be administered via the administrative workstation located in on the internal network. The local policies for these devices will be discussed later.

Public Web Server and Database Server: The public web server is available to Internet users via Port 80 (http) and Port 443 (SSL).

The database server is a Windows 2000 server running Microsoft SQL Server 2000. The database contains static "fortune cookie sayings". The database is periodically updated via the Administrative Host Workstation.

Hardware Configuration: Compaq Proliant DL380, dual-PIII-1.2Ghz Processors, 1GB Memory, 3 - 36.4 GB Drives running in a RAID-5 configuration.

External DNS Server: This server resolves all DNS requests that cannot be fulfilled by the internal DNS Server. To protect the internal network, the external DNS server is the only DNS server that can resolve DNS queries made by the Internal DNS server to the outside network.

Hardware Configuration: Compaq Proliant DL360, PIII-1.2Ghz Processor, 512MB Memory, 2 – 9.1 GB Drives running in a RAID-1 configuration.

Mail Forwarder: The Mail forwarding server sends and receives from the internal Mail Server all outbound SMTP mail.

Hardware Configuration: Compaq Proliant DL360, PIII-1.2Ghz Processor, 512MB Memory, 2 – 9.1 GB Drives running in a RAID-1 configuration.

Internal Network Devices

All of the internal servers and workstations are members of the giacnet.com domain and are managed by Active Directory with Group Policies.

Domain Controllers: There are 3 domain controllers used by GIAC Enterprises, two in the US and one in the China research and development office. Domain Controller 1 is the master domain controller and the first one installed on the network. It serves as the schema master and it's use is primarily for domain administration purposes. DC2 and DC3 serve the purpose of facilitating user authentication requests at both sites.

Hardware Configuration: Compaq Proliant DL360, PIII-1.2Ghz Processor, 512MB Memory, 2 – 9.1 GB Drives running in a RAID-1 configuration.

WebShield e250 Appliance: Each site has a McAfee WebShield e250 network appliance installed behind the Firewall. This device will scan for viruses on all incoming SMTP, HTTP, FTP or POP3.

File and Print Servers: As mentioned earlier, each location (US and China) has a server dedicated to servicing file sharing and print queuing. All users Home drive directories are located on their local File/Print servers. In addition, all shared departmental data is secured via Group access to a share on the local servers. A common, company-wide share is available to anyone within the organization and is located on the US server.

In addition to servicing file and print functions, these servers are configured to download via FTP any virus engine and signature file updates from McAfee on a daily basis. This is simply an "at" job that runs once a day.

Hardware Configuration: Compaq Proliant DL380, dual-PIII-1.2Ghz Processors, 1GB Memory, 3 - 36.4 GB drives running in a RAID-5 configuration.

Internal DNS Servers: The internal DNS servers service all DNS requests for each site. This server is configured to resolve all external giacnet.com DNS requests via the external DNS server located in the DMZ (in both the US and China).

Hardware Configuration: Compaq Proliant DL360, PIII-1.2Ghz Processor, 512MB Memory, 2 – 9.1 GB Drives running in a RAID-1 configuration.

Other Servers: Separate servers have been setup to facilitate dhcp, e-mail and test web/database development. The dhcp and e-mail servers have been "hardened" to restrict access to only the designed services that they will provide. Access to the test web/database server is open only to the Information System developers, and Research and Development groups.

Hardware Configuration – DHCP Server: Compaq Proliant DL360, PIII-1.2Ghz Processor, 512MB Memory, 2 – 9.1 GB Drives running in a RAID-1 configuration.

Hardware Configuration – Test Web/Database Server: Compaq Proliant DL360, PIII-1.2Ghz Processor, 512MB Memory, 2 – 36.4 GB Drives running in a RAID-1 configuration.

Hardware Configuration – E-Mail Server: Compaq Proliant DL360, PIII-1.2Ghz Processor, 512MB Memory, 2 – 36.4 GB Drives running in a RAID-1 configuration.

Administrative Host, Logging Host and Workstations

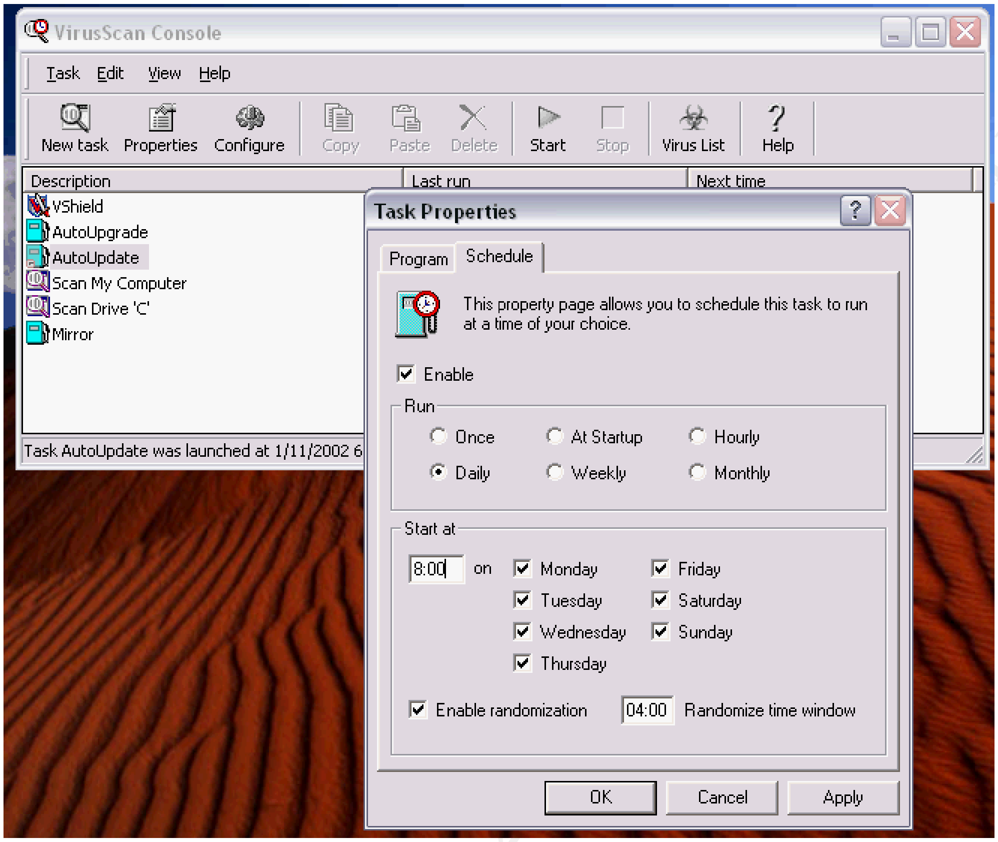
Administrative Host: The administrative workstation is a Windows 2000 professional workstation dedicated to administering the servers in the DMZ. This provides for auditing and tracking of changes to any of the servers in the DMZ. It is the only device that can be used to remotely access the DMZ servers from the internal network.

The Administrative host is also the only workstation that can update the content on the Public Web Server or Database Server in the DMZ. This access is controlled by an ACL on the Internal Router.

Logging Host: The logging host is the repository for all SYSLOG's generated on each of the routers and Firewall. This is a Windows 2000 workstation configured with a WinSyslog. WinSyslog is an enhanced SYSLOG server for Windows.

User Workstations: All user workstations are Windows 2000 Professional based PC's with W2K Service Pack 2 installed. There are approximately 200 Windows 2000 workstations on both campuses combined. The users on each PC are configured as members of the security level group "USERS", with the exception of the Information Systems developers, which require "POWER USER" group access to install and test new and innovative software applications. Only the 2 Network Administrators are configured as "ADMINISTRATORS" on any of the workstations.

Each user workstation is running McAfee AntiVirus software and setup to automatically check for and download any updated virus definition files and/or engine updates. These updated files are downloaded from the File and Print Servers.



Task AutoUpdate was launched at 1/11/2002 6

This property page allows you to schedule this task to run at a time of your choice.

☑ Enable

Run

○ Once ○ At Startup ○ Hourly
● Daily ○ Weekly ○ Monthly

Start at

8:00 on ☑ Monday ☑ Friday
☑ Tuesday ☑ Saturday
☑ Wednesday ☑ Sunday
☑ Thursday

☑ Enable randomization 04:00 Randomize time window

Active Directory Benefits

There are many advantages to using Microsoft's Active Directory domain model versus the old NT4 domain structure.

The important security benefits Active Directory provides in a Windows 2000 environment includes:

- **Centralized Management:** Active Directory allows for a centrally managed network of all users, computers and servers.
- **Group Policy:** Group Policies allows for central management of users, servers and workstation configurations. Policy based management defines access to computers and resources throughout an organization. Group policy definition can be setup as broad or as granular as your organization requires.
- **Kerberos Authentication:** Kerberos provides for fast secure authentication to network resources. Kerberos is the Internet standard security protocol for handling authentication of users or systems.
- **PKI:** Active Directory supports the use of Certificate Services to distribute x.509 certificates and public key infrastructure.
- **EFS:** Encrypted File System (EFS) support allows administrator and users to securely encrypt data.
- **Smart Card Support:** Active Directory's support of smart cards provides a tamper-resistant and portable to supporting domain logon.
- **Delegated Administration:** Active Directory allows Administrators to delegate a specific set of administrative privileges to appropriate individuals within the organization.

Active Directory Design and Diagram

Figure 2 is a diagram of the Active Directory design for the GIAC Enterprises Network.

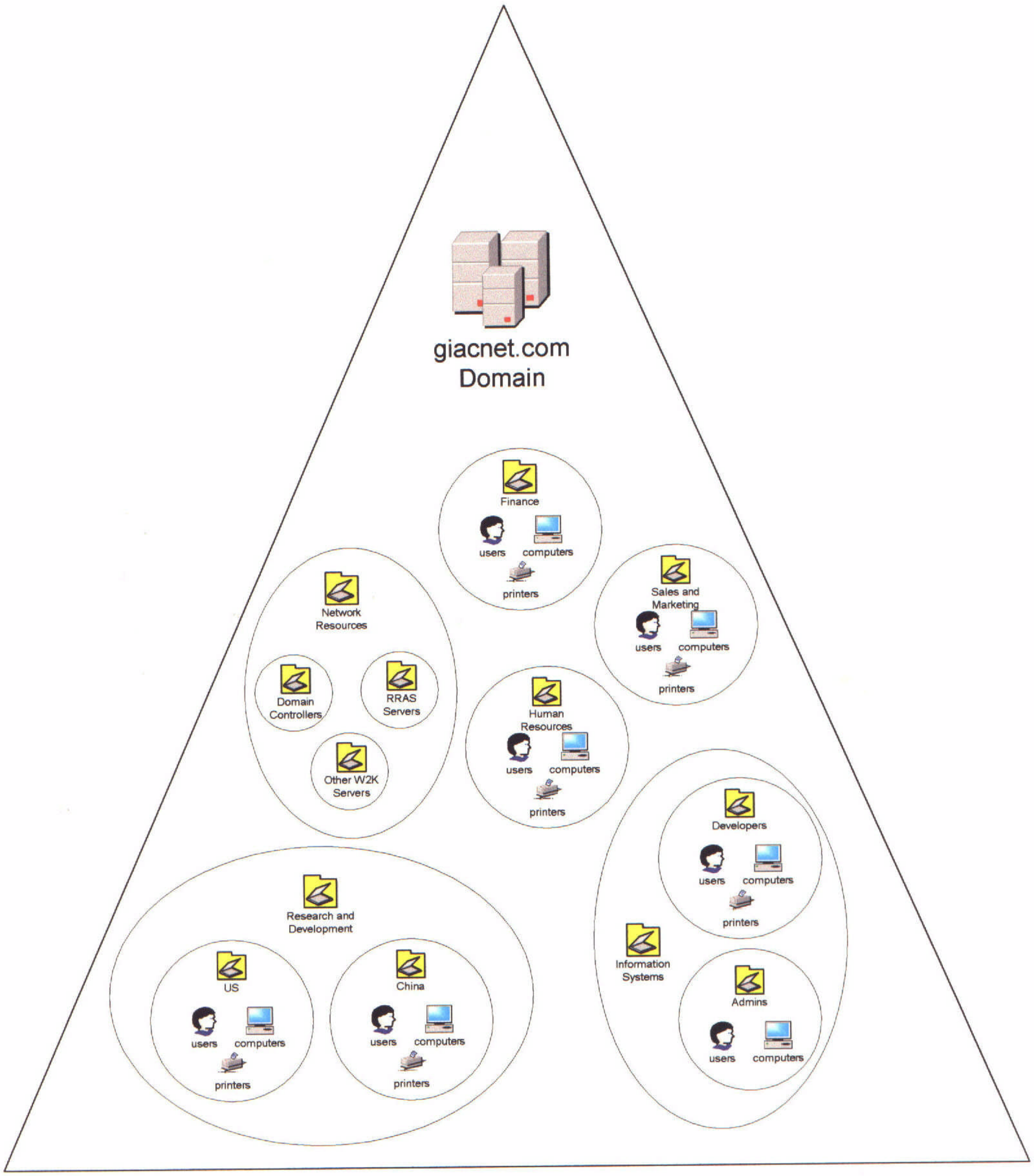


Figure 2.

Active Directory Structure Overview

The goal in setting up the Active Directory structure for GIAC Enterprises was to define organizational units that have unique Group Policy requirements and/or require delegation of management control. An attempt was made to minimize the number of organizational units while providing enough flexibility to apply unique Group Policies where appropriate.

We have chosen a single domain model for GIAC Enterprises. The Active Directory domain name for the GIAC Enterprises Network is giacnet.com.

Sites

Due to the differing geographical locations of the US and China local area networks, the giacnet.com Active Directory has been split into 2 "sites".

Microsoft defines a site as a collection of devices (servers, workstations and printers) that physically exist on a *fast* or "well connected" network. Active Directory servers within the same site communicate with no consideration to bandwidth between peers. The recommended minimum definition of a fast network is 1.5Mbs. Although each site is connected together via a secured T1 link through the Internet, the latency inherit to traffic travelling via the Internet may well degrade our actual throughput between the 2 locations to less than actual T1 speeds.

Sites exist to enable clients to find the nearest "well connected" network resources (i.e., Domain Controllers, DFS shares, etc). In addition, sites allow for the management of Active Directory data replication between Domain Controllers at each site. Several site replication parameters can be configured to optimize site replication traffic for remote sites connected by both fast and slower links.

The Windows 2000 service responsible for generating intra-site AD replication links between sites is know as the Knowledge Consistency Checker (KCC). The KCC will automatically create links between sites for your network only when an Administrator has specified that a set of sites should be connected. These links are configurable by the Administrator once they are created.

Creating and managing AD sites is performed with the "Active Directory Sites and Services" MMC add-in.

To create the China site for giacnet.com, we will load the MMC with the Active Directory Sites and Services add-in. Next, right click on the Sites folder and select New Site. We will now assign a name to the new site; in this case "China".

Once we have created the China site, we need to move the appropriate Domain Controller to the China site. To do this, open the "Default-First-Site-Name" site, select Servers and right click on the appropriate DC to be moved to the newly created China site. In this case, move GIAC-DC3 (China's Domain Controller).

Now we need to define IP subnets for each site. Right click the subnets folder and select New | Subnet.

Address	Mask	Site Name
192.100.1.1	255.255.255.0	China
192.100.2.1	255.255.255.0	Default-First-Site-Name

Lastly, we will need to create a link between these 2 sites. In the AD Sites and Services snap-in, open the Intra-Site Transports Folder and choose IP as the site transport. Given adequate bandwidth to support IP as an inter-site transport, we have opted not to use SMTP as the transport mechanism.

Right click the IP folder and select New Site Link. Select China and Default-First-Site-Name and click Add to create a new link between sites. Lastly, name the Site Link Object and click OK.

We will leave the default properties set for this site link. Those default properties include:

- **Cost**: That is a number representing the preferential use of one link over another. A lower cost number would indicate that a link is of higher bandwidth and thus a preferred path for replication traffic. Because we only have 2 sites and one link, the cost is irrelevant in this case.

- **Replicate Every**: Configures the number of minutes to perform replication across this link. Due to the size of the "pipe" between the two sites and the relatively infrequent AD updates anticipated, we will leave this setting at the default number of 180 minutes.

- **Schedule**: The schedule dictates the days of the week and hours of the day that AD replication will occur. Again, with relatively few AD updates anticipated, we will schedule our updates to occur anytime, 24 hours a day, 7 days a week.

Organizational Units

The top level Organizational Unit's include Finance, Sales and Marketing, Human Resources, Research and Development, Network Resources, and Information Systems.

The Finance, Human Resources and Sales and Marketing OU's will contain users, computers and printers for their respective departments. Due to the differing security and application requirements of each area, a separate OU was created for each department.

The Research and Development OU contains 2 sub-Organizational Units, one for the US R&D department and one for the China R&D department. Although they both perform similar functions for GIAC Enterprises, long-term, differing software application requirements dictate differing Group Policy configurations.

The Information Systems OU also contains 2 sub-OU's. One sub OU will be to manage and administer security for the application developers, the other for Network Administrators.

The last top level OU to be discussed is the Network Resources OU. This Organizational Unit is sub-divided into 3 separate OU's to effectively manage the common Network Resources:

- Domain Controllers
- Routing and Remote Access Servers
- All other Windows 2000 Network Servers

Single Domain Model

As noted earlier, the giacnet.com Active Directory is contained in a single domain. The following bullet points sum up the reasoning for this approach:

- Simplicity: GIAC Enterprises only consists of approximately 200 workstations and only a hand-full of servers. Once configured, there should be few daily changes to the AD. Replication traffic will be relatively low compared to larger and more complex AD implementations.

- No Legacy Support Requirements: This implementation was not an upgrade from a previous NT 4 domain. It was built from scratch and we did not have to face the difficulties of migrating from a possible multi-domain NT architecture.

- Adequate Bandwidth: Setting up AD site links along with ample bandwidth will allow for adequate single domain replication performance among the 2 sites.

- Single Domain Policy: A single domain policy could be implemented. There was no requirement to implement separate domain level policies for the different GIAC Enterprises departments.

  These domain level policy settings include:
  - Password Policies
  - Account Lockout Policies
  - Kerberos Policies

Creating the Active Directory Structure

To create the Active Directory structure for giacnet.com we must first login to the domain as a Domain Administrator.

Next,

- Load the Microsoft Management Console (MMC)
  START   Run   MMC.EXE

- Add the Active Directory Users and Computers snap-in
  Console   Add/Remove Snap-in…   Add…   Select Active Directory Users and Computers   Add   Close   OK

- Open the snap-in and right click on the giac.com domain, Select New   Organizational Unit

- Name your new OU

- Repeat for each top level OU

- To create any sub Organizational units, highlight the top level OU, right click and Select New   Organizational Unit

•

Group Policy and Security

Overview

Group Policies are used in an Active Directory to control domain users and computer settings via a central console. For example, a group policy can control settings for items such as security, software installation, registry settings, desktop “look and feel” and many, many other options.

Group policies can be applied to an entire domain, a specific group of users (organizational units) or both.

An important rule to understand when applying Group Policy Objects is the order of processing and precedence. From the lowest to highest precedence GP Objects are ranked as follows:

- Local GPO
- Domain GPO
- OU GPO containing the computer or user

It is also important to note that GPO settings are cumulative. In the event of a conflicting GPO setting, the order of precedence will apply. There are a few exceptions to this rule:

- Account Policy settings will always be provided by the Domain GPO. Attempts to change Account Policy setting at the lower OU level will be overridden by the Domain GPO.

- By setting the Block Policy Inheritance Checkbox in the OU GPO properties dialog box, or by setting the No Override option in the GPO properties dialog box, you will prevent inheritance of GPO’s from parent containers. These features should be used with caution. They add a level of complexity to your Group Policy structure and make troubleshooting difficult.

GIACNET.COM Domain Policy

We will start with setting the Group Policy at the domain level. First, open the Management Console (Start Run MMC).

Next, open the Active Directory Users and Computers snap-in, right click on giacnet.com and select Properties. Select the Group Policy Tab. Make sure Default Domain is the group policy assigned to the domain object and click Edit. From here we can update the domain group policy.

Following is a summary of the Group Policy settings for the Default Domain Policy:

Computer Configuration
  Windows Settings
    Security Settings
      Account Policies

Password Policy

Enforce password history: 24 passwords

This setting will prevent a user from re-using a password. By setting this value to 24 a user will not be able to use an old password until 24 other password changes have been made to his or her id.

This is the maximum setting possible. By keeping this setting at its maximum, it will be as close as we can get to keep end users from re-using old passwords.

Maximum password age: 90 days

This will require a user to change their password at least once every 90 days.

Forcing a user to change their password every 90 days seems reasonable. I feel 60 days seems to short of a time and 120 days seems to long of a time to wait for a password change.

Minimum password age: 1 day

This is the minimum amount of time to wait after a password has been changed and a new password can be set.

This will prevent users from changing their password to something and then changing it again (24 times, based on the Enforce password history setting) to their original password.

Minimum password length: 12 characters

This dictates the minimum length of the password.

12 characters may seem excessive for a password length, but it

encourages users to create long, hard to guess passwords that can be easier to remember by using a phrase or long acronym.

Password must meet complexity requirements: Enabled

Enforces strong password requirements. A strong password must contain at least 3 of 4 type of character classes: upper case characters, lower case characters, numbers or at least one special character. Special characters include: !@#$%^&*()-.?.

This setting, along with a password length of 12 characters, will insure that a password can withstand a “dictionary” attack. In addition, brute force password cracking programs, such as l0pht crack would take a considerable amount of time to crack a 12 character “strong” password.

Store passwords using reversible encryption for all users in the domain: Disabled

Determines whether passwords are stored using a two-way hash.

Although this feature is required for legacy NT4 support, in our environment, it is not needed. With this option enabled, passwords would be easily obtained using commonly available cracker tools. It would be equivalent to storing password in clear-text.

Account Lockout Policy

Account lockout duration: 15 minutes

This is the amount of time a user will be prevented from attempting a new logon attempt after the account lockout threshold has been met.

This will keep a cracker from continuously attempting to logon to a user workstation. 15 minutes appears to be an adequate “wait time” to frustrate someone attempting unauthorized access.

Account lockout threshold: 3 invalid logon attempts

The number of invalid logon attempts before a logon id is locked out for the account lockout duration.

If a user cannot logon successfully in 3 attempts, they have surely forgotten their password. In that case, they should call the helpdesk and have their password reset. If someone is not authorized to access the workstation, after 3 missed logon attempts, they will be prevented from subsequent logon attempts until the account lockout duration expires.

Reset account lockout after: 15 minutes

Sets the number of minutes before the invalid logon count is reset.

This is really a "belt and suspenders" setting to support the other 2 Account lockout policy setting. It is a good practice to keep this setting at it's maximum (15 minutes) to further discourage password cracking/guessing attempts.

Kerberos Policy

Enforce user logon restrictions: Enabled

Enables the Key Distribution Center (KDC) to check if the user requesting a service ticket has "Log on Locally" or "Access this Computer from the Network" right on the machine running the requested service. If the user id does not have the appropriate user right, a service ticket will not be issued. A service ticket is a Kerberos mechanism for providing access to network services.

Without enabling this setting, there would be a remote possibility that a disabled user accounts ticket could be "hijacked" before the maximum lifetime for a user ticket (10 hours) expires. This is the default setting.

Maximum lifetime for a service ticket: 600 minutes

The number of minutes that a Kerberos service ticket is valid. This is the default setting.

Maximum lifetime for a user ticket: 10 hours

Determines the amount of time that a ticket-granting-ticket is valid before a new one needs to be acquired or an old one renewed. This is the default setting.

Maximum lifetime for user ticket removal: 7 days

This sets the maximum number of days that the users ticket-granting-ticket can be renewed. This is the default setting.

Maximum tolerance for computer clock synchronization: 5 minutes

This is the maximum number of minutes of time that can differ between the Key Distribution Center (on the domain controller) and the client machine clock. This is the default setting.

Although all of the Kerberos settings discussed above are Microsoft default settings in Windows 2000, I thought it was important to discuss them for 2 reasons:

1. To provide a basic understanding of what they do.
2. Identify that **Administrator's should be careful when changing any of these settings**. This is best described as stated in the O'Reilly book, "Windows 2000 Active Directory":

   > *"The primary thing to remember about configuring Kerberos is that the default is good. Only about a half dozen items can be changed in Kerberos on Windows 2000. Unless there is some specific reason to change one of the parameters, you should leave the parameters alone."*

In addition to the account policies, we will set some additional Local and Event Log Policies at the domain level. This will insure minimum security is applied to servers and workstations if these settings are not defined in a Policy at the OU level. The following is an overview of the most important settings:

Computer Configuration
  Windows Settings
    Security Settings
      Local Policies
        Audit Policy

Audit account logon events: Success, Failure
Audit logon events: Success, Failure
Audit privilege use: Failure
Audit system events: Success, Failure

Logging has been enabled to track the most important security related events without "going over-board" and trying to log everything. If you decide to log too many events, it makes it very difficult to sift though the logged data for useful information.

The event logs can be used to track security breaches. An even better use and more proactive approach is to review your logs for unauthorized logon or privileged access *attempts* before they become *security breaches*.

Computer Configuration
Windows Settings
Security Settings
Local Policies
Security Options

Additional restrictions for anonymous connections: No access without explicit anonymous permissions.

This setting has been chosen to secure anonymous access to all workstations and servers. Although this limits access from applications to the Browser list, this should not pose a problem for any of the currently running GIAC applications. In addition, since we have all Windows 2000 workstations and servers at both locations, setting this option should not pose any additional problems.

Warning; be careful when setting this value in a mixed NT 4.0 and Windows 2000 environment. In a mixed environment, this setting will cause undesirable results on the NT 4.0 workstations. See Microsoft Knowledge Base article, Q246261, for additional information.

Disable CTRL+ALT+DEL requirement for logon: Disabled

This will insure the user must press CTRL+ALT+DEL to logon to any workstation or server. Although new for Win9X users, Windows NT users should be acquainted with this requirement. It provides a subtle level of security by not leaving the logon screen displayed.

Do not display last user logon name in logon screen: Enabled

This very important setting hides the last logged on user name from someone attempting to access the machine locally. This makes a valid user name one more piece of information that a potential intruder needs to identify before attempting to access the machine.

LAN Manager Authentication Level: Send NTLMv2 response only\refuse LM & NTLM

We have chosen to use NTLMv2 as it is the strongest of the 3 authentication mechanisms in a Window 2000 environment. Support for the weaker challenge/response authentication mechanism, LM & NTLM, is not required because we lack any legacy W9x for NT systems that would require this support.

Rename Administrator Account: XyZ10Ad43dsa4
Rename Guest Account: dfGrt12uisj45

> It is a very good idea to rid your system of the default user ids. In our case, we have renamed our Administrator and Guest account to obscure names. Another good measure is to change the password on these 2 accounts to a strong, obscure password. Note: User names are not case sensitive, although they display in the case they were created.

Computer Configuration
  Windows Settings
    Security Settings
      Event Log
        Setting for Event Logs

Maximum Application Log Size: 20MB
Maximum Security Log Size: 20MB
Maximum System Log Size: 20MB
Restrict Guest Access to Application Log: Enabled
Restrict Guest Access to Security Log: Enabled
Restrict Guest Access to System Log: Enabled
Retention Method for Application Log: Manually
Retention Method for Security Log: Manually
Retention Method for System Log: Manually

> As noted earlier, using the event logs for pro-active security monitoring will be very helpful. These registry settings insure that:
>
> There will be ample room to store the logged data.
> Access to the event logs by a Guest user is restricted.
> The event logs never overwrite them-selves, preserving the log data.
> The logs can only be cleared manually.

Computer Configuration
  Windows Settings
    Security Settings
      System Services
        Routing and Remote Access: Disabled

> By disabling Routing and Remote Access services, we can be sure a general user will be running this service on a local workstation. We

have a separate OU setup that will be used in the future to support RRAS servers. This setting will be enabled in the Group Policy on the RRAS Servers OU.

This is only a summary of the baseline settings for Group Policy at the domain level. Most of these settings were derived from policy recommendations by the NSA in the documents:

- Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set http://nsa1.www.conxion.com/win2k/guides/w2k-3.pdf.
- Group Policy Reference http://nsa1.www.conxion.com/win2k/guides/w2k-4.pdf.

General User OU Group Policy

The General user Group Policy applies to all OU's, except any OU in the Network Resources OU. This includes the following Organizational Units:

Finance OU	Sales and Marketing OU
R&D US OU	R&D China OU
IS Developers OU	IS Admins OU
Human Resources OU	

For each of these Organizational Units, a separate Group Policy has been created based on the Microsoft High Security .INF file.

To create these policies, from the Active Directory Users and Computers MMC snap-in:

- Right Click on the Desired OU to be configured and select Properties.
- Click the Group Policy Tab, and Select New. Name the new Group Policy. In this Example, assume we are working with the R&D China OU. Name the Policy GP_R&D_China.
- Click Edit to bring up the Group Policy Configuration Window.
- Open the Windows Folder, Right click on Security Options and Select Import Policy. Select the hisecws.inf file (High Security Workstation) and Click Open.
- Lastly, close the Group Policy Configuration Window and Close the OU Properties Windows. Now we have assigned the Microsoft High Security default Group Policy to the R&D China OU.

Repeat these actions for the remaining OU's to assign this same policy to them.

In doing this, we have a simple, consistent starting point from which to customize General User OU's based on their ongoing requirements. For the most part, the customizations should be minimal.

This also provides a unique Group Policy for each OU, which we can use to distribute individual departmental specific applications or create departmental specific logon/logoff scripts. These departmental applications may require changes to the individual OU policy.

Following are several examples of departmental OU policy changes that have been required:

Human Resources OU: The HR department has asked that their Internet Explorer Home page defaults to www.HotJobs.com, so they can begin their day searching for new employees and reviewing resumes. To accommodate this, the following change was made to the Group Policy for the Human Resources OU:

User Configuration
  Windows Settings
    Internet Explorer Maintenance
      URLs
        Important URLs
Customize Home Page URL: http://www.hotjobs.com

Finance OU: Finance runs a financial consolidation software application called Hyperion Enterprise. This legacy application requires write access a file called HypSettings.ini stored in the %windir% directory (c:\winnt in this case). As Finance users do not have write access to any files in this directory, we can use Group Policy to give users in the Finance OU explicit access to read and write to this file, first edit the Finance OU Group Policy and drill down to:

Computer Configuration
  Windows Settings
    Security Settings
- Right Click File System and Select Add File…
- Drill down to **C:\WINNT\HypSettings.ini**, Click OK
- Remove the Everyone group. Click Add and add the **GP_Finance_group**. (*This is a Security group containing all of the members of the Finance department. Setup of Security Groups will be discussed shortly*)
- Give this group **Modify, Read & Execute, Read, and Write** permissions.
- Click OK, OK.

Sales and Marketing OU: All of the Sales and Marketing users have a need to have an application installed on all of their PC's. The

application is called MarketCast. This application allows the Sales and Marketing users to forecast their Sales and Marketing activities based on data collected from other companies in the fortune cookie sayings business. We will use the Sales and Marketing OU GPO to distribute this application to all Sales and Marketing users.
To start, open the Sales and Marketing GPO for editing and Drill down to:

User Configuration
  Software Setting
- Right Click Software Installation and select New | Package…
- Find the network share containing the .MSI file to install the software application.
- When prompted to select the deployment method, select Assigned. This will assign the application to the user. In addition this application will be advertised to the user when they login to any computer.

These are only a few examples of how the separate Group Policy Objects can be tailored at the Organizational Unit to support each department's unique requirements.

Network Resources Group Policies

The Network Resources OU is setup to house all common infrastructure related workstations and servers.

This OU consists of 3 Sub-OU's: Domain Controllers OU, RRSAS Servers OU and the Other W2K Servers OU. It is at this sub-OU level that we will setup the Group Policies.

The Domain Controllers OU Group Policy will be configured with the Microsoft High Security Domain Controller .INF (hisecdc.inf).

The Other W2K Servers OU Group Policy will be configured with the Microsoft High Secure Server or Workstation .INF (hisecws.inf).

Although we have not implemented Remote Access to the giacnet.com network, we have setup an Organizational Unit for future RRAS servers. Remote access to giacnet.com will be implemented at a later date. Knowing that, we have configured an OU and Policy for RRAS.

To configure this setting, Open the RRAS Group Policy Object and configure:

Computer Configuration
  Windows Settings
    Security Settings
      System Services
        Routing and Remote Access: Automatic

Local Policies for the DMZ Servers

As noted earlier, the servers located in the DMZ are not part of the Active Directory. This will insure that the internal Active Directory cannot be compromised in any way even if an intruder accesses any of the servers in the DMZ.

To illustrate, we will review the **local policy** and hardening of the Public Web Server. **This is not intended as a comprehensive overview of IIS Web Server hardening**. The intent is to present an overview of the benefits of using the **local policy** on non-Active Directory connected servers, along with a few of the most important security considerations for web servers placed in a DMZ.

The Public Web Server provides Active Web Pages to outside Internet users and requires access to the database server in the DMZ. Other than the Administrative Host located within the Active Directory domain, no other user or server should have access to the DMZ web or database servers.

First, we apply the Secure Microsoft IIS Server Security Template (hisecweb.inf) to the **local policy** of the Web server.

Although, hisecweb.inf is a good starting point for local policy security, we have mirrored all of the **domain level policies** that we set in the giacnet.com Active Directory. This provides us with a consistent baseline policy for all servers, whether they are part of the Active Directory or configured using a local policy.

Other important considerations for a hardening a web server in your DMZ:

1. Shut off all unnecessary services. This will prevent all known and (more importantly) unknown vulnerabilities in unused services from being exploited. For example:
    Computer Browser

DHCP Client
FTP Publishing Services
Alerter
Messenger
NetLogon
Telnet
…etc.

2. Remove unnecessary application subsystems. None of these subsystems are typically used and could be used to exploit your system.

To do this, remove the Registry Keys:
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\Os2
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\Posix

Delete the Value Named:
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\Os2LibPath

Delete all the Sub-Keys underneath:
HKLM\SOFTWARE\Microsoft\OS/2 Subsystem for NT\

3. Protect against SYN Flooding. This registry value will reduce the retransmission of SYN-ACK retries and requires a full 3-way TCP handshake to be completed before cache memory is committed to this socket connection. Change this Value:
HKLM\SYSTEM\CurrentControlSet\Services\TcpIp\Parameters\SynAttackProtect=2

Another important consideration is running the Microsoft IIS Lockdown Tool from the Microsoft at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/locktool.asp.

By using this tool, we can insure the most common IIS vulnerabilities are restricted and accounted for. This includes installation of the Microsoft URLScan Tool. URLScan integrates with IIS to screen all incoming URL request to insure that only valid URL requests are sent to the Web server.

In addition, the latest Windows 2000 Server Service Pack (in this case SP2) has been installed and all of the latest updates and security patches have been downloaded from windowsupdate.microsoft.com and security.microsoft.com.

The Firewall will limit outside Internet access to the DMZ by allowing only access to http, https, IPSec and SMTP.

The Firewall is also configured to allow internal IP access to any device in the DMZ **only from** the Administrative Host workstation. All other internal user workstation IP access has been restricted to the http and https ports.

Group Security Settings

In addition to Group Policies, we needed to setup Security Groups for each department within GIAC Enterprises. Security Groups will provide 2 functions:

1. Restricting access to browsing resources only available within each department's Organizational Unit. All users will still have access to browse resources in the "Other W2K Servers" OU.

2. Providing a directory access security on the File Server. For example, we can create a common directory on the File Server for the Finance users and restrict access to that common directory via a Security Group.

The following Security Groups will be setup:

Functional Organization	**Security Group Name**
Finance	GP_Finance
Human Resources	GP_Human_Resources
Sales and Marketing	GP_Sales_Marketing
Research and Development	GP_Research_and_Development
IS Developers	GP_IS_Developers
IS Admins	GP_IS_Admins

First, we will restrict browsing (read) access to all of the OU's except for the Other W2K Servers OU. From the MMC, load the Active Directory Users and Computers Add-in, right click on the OU to be restricted and select Properties.

Next, click the Security tab and locate the Authenticated Users group. Deselect the Allow Read Permission and click OK.

This opertion should be performed on all Organizational Units except for the Other W2K servers OU.

We are now ready to create the Functional Organization Security Groups.

We will start with the Finance Security Group. Right click the Finance OU and select New   Group.

Group Name: GP_Finance
Group Scope: Global
Group Type: Security

Next, open the Finance OU, right click on the GP_Finance group and select Properties. Click the Members tab and add each of the Finance OU users to the GP_Finance Security group. Click OK when complete.

Repeat this operation for the remaining Functional Organization OU’s and users.

Lastly, we will assign read access to the appropriate OU for each of our newly created Security Groups.

We will start again with Finance. Right click on the Finance OU and click Properties. Select the Security tab and click Add. Find the GP_Finance Group and Click Add, then OK. This Security Group will automatically be assigned Read Access to this OU. Click OK to close the OU properties window.

Repeat this operation for the remaining Functional Organization OU’s .

To test the Security Group settings, we can login as a user in the Finance OU and GP_Finance Security Group, open My Network Places, browse the giacnet.com Active Directory and we’ll only see the Finance OU and the Network Resources OU. By opening the Network Resources OU, we will only see the Other W2K Servers OU.

Conclusion

This paper outlines the most important and critical settings required to configuring a secure Windows 2000 based network. Numerous additional Group Policy and network settings would be required to complete a secure network configuration. In addition to a well designed Active Directory and closer review of the Group Policy settings, a secure Windows 2000 network requires:

- Written “appropriate use” user policies.
- A documented and followed auditing practice (log reviews, etc).
- Building secure and lock-down configurations of all the public and private servers within your organization.
- Disabling of **all** unnecessary services on the GIAC Enterprises servers and workstations.
- Implementation of smart-cards for authentication.
- Implementation of IPSEC and Certificate Services.
- Detailed documentation and testing of Router and Firewall Configurations.
- Scheduled audits and penetration testing.

Windows 2000 with Group Policy is a very useful tool in securing and managing your Windows 2000 network. No other Network OS directory service offers this much flexibility and functionality in a Windows 2000 network environment.

References

NSA Microsoft Windows 2000 Network Architecture Guide
http://nsa1.www.conxion.com/win2k/guides/w2k-1.pdf

NSA Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set
http://nsa1.www.conxion.com/win2k/guides/w2k-3.pdf

NSA Group Policy Reference
http://nsa1.www.conxion.com/win2k/guides/w2k-4.pdf

Microsoft IIS Lockdown Tool
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/locktool.asp

Cisco's PIX Firewall and Stateful Firewall Security
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/tech/nat_wp.htm

The WinSyslog Product
http://www.winsyslog.com/en/Product/

WebShield e250 Appliance
http://www.mcafeeb2b.com/products/webshield-eapp250/default.asp

Lowe-Norris, Alistair, Windows 2000 Active Directory, O'Reilly & Associates, 2000

Fossen, Jason, Securing Internet Information Server 5.0 Workbook, sans.org, 2001