Global Information Assurance Certification Paper

GIAC Certified Windows Security Administrator (GCWN)
Practical Assignment
Version 3.2 Option 1

AD Design, Group Policy and Audit for SANS Co. and GIAC Enterprises merger

Alexei Galkine

October 2003

1. Introduction

This paper is a practical assignment for the SANS GIAC Certified Windows Administrator (GCWN) program. It consists of the following three major parts.

The first part, Domain Design, presents a merge scenario for two Windows 2000 networks with extensive Active Directory infrastructures. These networks belong to SANS Co. and GIAC Enterprises (both fictional companies) which have merged in order to expand their markets and to consolidate operations. Design of the SANS Co. network and Active directory infrastructure was done by the author. Design of the CIAC Enterprises network and infrastructure was developed earlier by Jason Lam (http://www.giac.org/practical/Jason_Lam_GCWN.pdf). The proposed merge solution is designed to meet the companies' business goals and allow existing customers to deal with both parts of the new company seamlessly. At the same time, the new infrastructure should maintain a suitable level of network security and ensure interoperability and consolidation of IT overheads.

The second part, Security Policy and Tutorial, describes the Group Policy design for the newly-merged system, explains implementation of the Group Policy and demonstrates the results of the Group Policy implementation.

The third part, Audit, discusses methods of auditing the merged system, including gathering and managing Event Logs and checking critical settings.

One of the general assumptions made in this paper is that all domain controllers are Microsoft Windows Server 2003 and all Active Directory Domains and Forests operate in the "Windows Server 2003" mode. The Lab setup and tests are based on Microsoft Windows Server 2003. Although, at present, most companies have Windows Server 2000 based infrastructure, I believe it is more important and valuable to research Windows Server 2003 behaviour and features.

2. Domain Design

This chapter introduces the Active Directory (AD) infrastructures of SANS Co. and CIAC Enterprises (both fictional companies) and proposes a solution for the merge of the two AD infrastructures. The proposed merge scenario is designed to meet the companies' business goals and maintain a suitable level of security for the new Active Directory infrastructure.

2.1 Introduction

SANS Co. was established several years ago in New York, USA. Their success in the market is based upon the quality of their products and support services as well as aggressive marketing. Initially USA-based, the company expanded to two new markets: Europe (based in UK) and Australia. In order to maintain high standards of support services and still to be able to retain relatively low costs, the company opened a call centre in India. Development and Production remained in the USA. Overseas departments consist only of marketing, support and local HR subdivisions. Were very successful in developing new markets and gaining customers' trust, SANS Co. overlooked the significance of e-commerce and on-line sales. Their current Web representation is only informative. Recent market research showed that on-line sales were the most promising way of developing the business. Therefore SANS Co. was determined to merge with GIAC Enterprises, a smaller company which operated in the same market but with years of e-commerce experience.

GIAC Enterprises works in the same market as SANS Co., but produces a different range of products. The company is located in Boston, USA. Over the years GIAC Enterprises has been selling on-line and has proved to be successful in the e-commerce business. GIAC Enterprises was willing to explore new markets, but were blocked by the high cost of setting up the support infrastructure. The merger with SANS Co. deemed to be a possible method for GIAC Enterprises to resolve this problem.

The merge scenario will result in

- an extended product range, based on the current product ranges of the two companies
- a united Web representation and an e-commerce Web site based on the experiences of GIAC Enterprises
- enlarged infrastructure, utilising the SANS Co. product support infrastructure for the extended product range.

2.2. SANS Co. Infrastructure and AD Design

2.2.1 SANS Co. Active directory structure

The current AD infrastructure of SANS Co. consists of a single AD forest with two trees and five domains. The forest root domain is called sans.org, and it is an AD

domain in the head office in New York. This domain is a root domain for the main sans.org AD tree. The sans.org AD tree also encompasses the uk.sans.org, au.sans.org and in.sans.org AD domains, which represent the UK office, the office in Australia and the call centre in India respectively. The second AD tree is a single domain tree called sans.com. This is a domain for SANS Co. DMZ. The domain consists of SANS IIS web servers, bastion hosts and external DNS and mail servers.

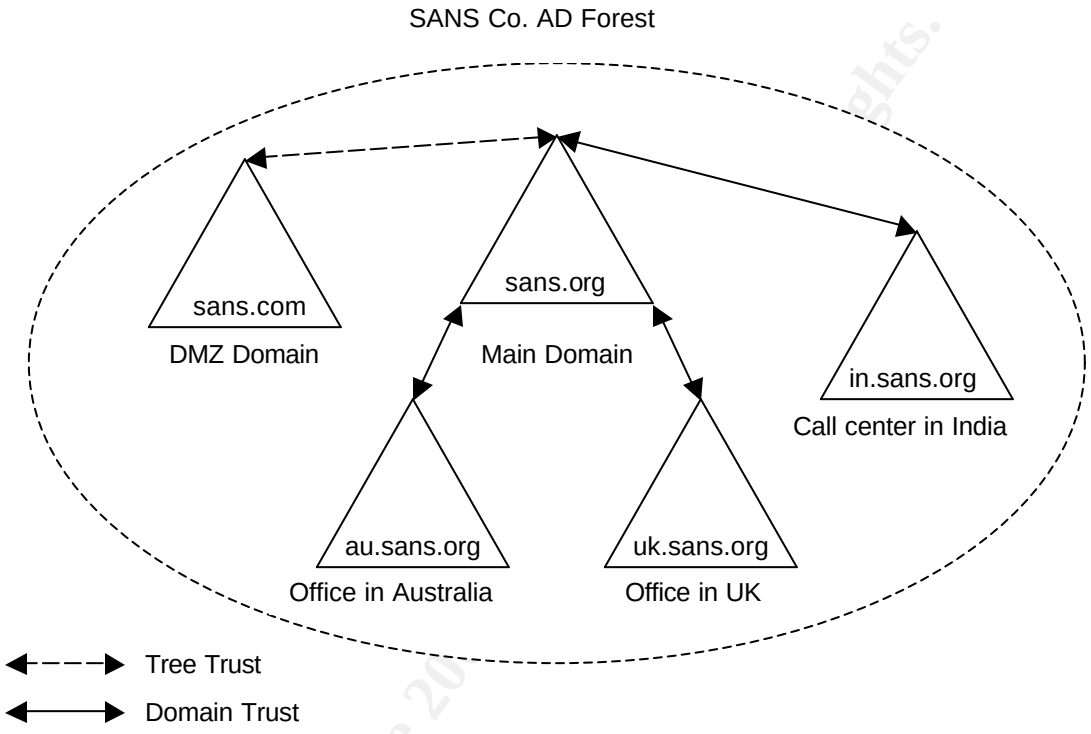

Figure 1 SANS Co. Active Directory Structure

The main (sans.org) AD tree comprises four domains, one for each geographical location. This infrastructure allows simplified administration of "locale" settings, which are usually set domain-wide. It also provides flexibility in complying with local laws related to privacy, encryption, reporting, audit and accounting.

Three of the domains are secondary domains (au.sans.org, uk.sans.org and in.sans.org) and are bound up with the forest root domain (sans.org) by transitive bidirectional trust. There are no direct trusts between the secondary domains. The secondary domains bear one particular function, such as a local sales department or a call centre. Primary company resources (R&D, production and the main marketing and sales departments) are concentrated in the main office and are covered by the main domain (sans.org). Therefore, the main domain is the only important resource for the secondary domains. As each of the secondary domains has a transitive trust to the main domain, they can access each others resources. When a user from one of the secondary domain needs to

log on to another secondary domain, the authentication process follows the Kerberos Referral Path. A direct sharing of the resources between the secondary domains is a rare occasion, and since the Kerberos Referral Path is not long (only one domain in between), it was decided not to increase complexity by having shortcut trusts between the secondary domains.

Delegation of rights and security inside the domains are based on Organizational Units (OUs). The main domain has Human Resources (HR), Accounting, Marketing, Production, R&D and Support UOs. The Australian and UK domains have HR, Accounting, local Marketing and Support OUs. The call centre in India has only HR, Accounting and Support OUs. Assigning a separate AD OU to each organizational department allows them to implement different security policies for every department. This structure is advantageous as it respects functional differences of the departments.

DMZ domain (sans.com) is a high security domain, the main purpose of which is to represent the company on the Internet. The domain consists of an IIS web server, an external E-mail server and an external DNS server. The domain represents a segregated AD tree which is bound with the main tree (sans.org) by the default inter-tree AD trust (Figure 3)[1]. Since the default inter-tree AD trust is transitive and bidirectional, the access to and from DMZ tree is restricted based on AD Universal security groups. It is configured so that only the members of one user group responsible for administering machines in DMZ and maintaining the web context has access to the DMZ AD tree.

2.2.2. SANS Co. Network Design

All of the SANS Co. offices are connected to each other by a VPN over the Internet. Each office has two firewalls: a main firewall and an internal firewall. The main firewalls separate the internal networks and the DMZs. The DMZs for the overseas offices are very small and consist only of external DNS servers and remote access bastion hosts. The DMZ in the main office also includes an external web server and an external mail server. The internal firewalls provide VPN links between the offices.

2.3. GAIG Enterprise AD infrastructure

2.3.1. Introduction

Design of the GIAG Enterprise's network and Active Directory infrastructure is documented in (http://www.giac.org/practical/Jason_Lam_GCWN.pdf). This chapter provides a short description of the network and the Active Directory infrastructure and highlights aspects important to the merge.

[1] The default trust is the one which is created automatically when adding a new AD Tree into an AD Forest. This trust cannot be removed or modified through a GUI. How is modified the default trust will be described later

2.3.2. Description of GIAC Enterprises

GIAC Enterprises (GIAC-E hereafter) is an e-business. GIAC-E generates most of its revenue through its web site (giac.org).

GIAC-E internal structure consists of four departments:

- Research and Development
- Sales and Marketing
- Finance and Human Resources
- IT and operations

The Sales and Marketing Department is located in the satellite office "SANS Tower Office"; the other three departments are located together in the main office "GIAC Building Office".

The machines within the GIAC-E network are configured as followed:

- Workstations run Windows 2000 Operating System
- Internal servers run Windows Server 2003 OS
- External Web servers are Windows 2003 Advanced Servers with Internet Information Server (IIS)

GIAC-E has an Active Directory infrastructure.

2.3.3. The GIAC-E Network

The GIAC-E network infrastructure is presented in Diagram 1.

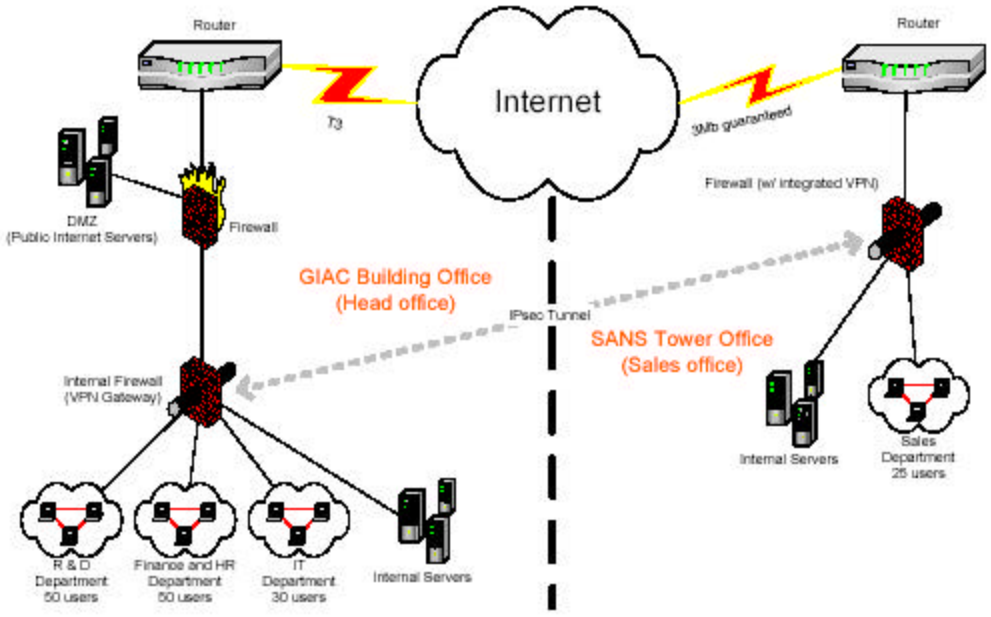

Diagram 1 GIAC-E Network Diagram

The Head Office and the Sales Office are connected by a VPN over the Internet. Public web servers are segregated into a DMZ via the main Firewall. Internal Firewalls separate departments' networks; provide a VPN link to the Sales Office; and translate network addresses (NAT).

GIAG-E Head Office (Diagram 2) has two principal structural elements: the DMZ and the GIAG-E internal network. The DMZ consists of five public web servers running in a load balancing schema, a backend database server, a mail relay server, an external DNS server and a dedicated Domain Controller (DC). The internal network includes two domain controllers, file and print servers, an internal DNS server, a mail server and a DHCP server.

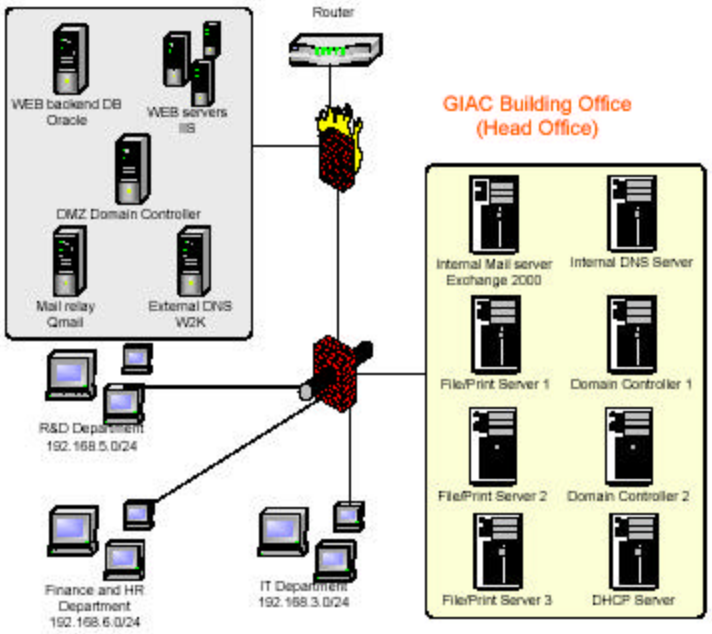

Diagram 2 GIAC-E Head Office Structural Diagram

GIAC-E Sales office (Diagram 3) has its own domain controller and a set of servers. The Domain Controller in the Sales Office is constantly synchronised with the domain controllers in the Head Office.

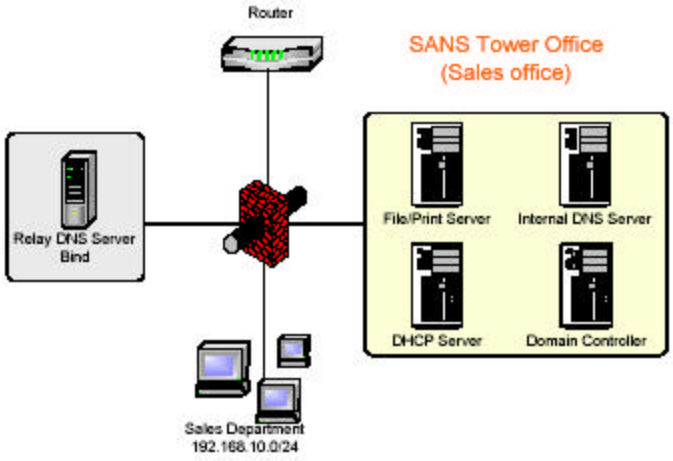

Diagram 3 GIAC-E Sales Office Structural Diagram

2.3.4. GIAC-E Active Directory Structure

GIAC-E has two Active Directory forests within the organization. One forest (giag.org) is dedicated to the DMZ, while the other (ad.giac.org) supports the internal networks. The two forests are completely isolated. There are no trusts between the forests. Every employee from the IT and Production department, who needs access to the DMZ receives a sets of credentials separate from the credentials for the internal networks. Each forest is a single domain forest. Like the forests, the domains are completely separated; there are no trusts between domains.

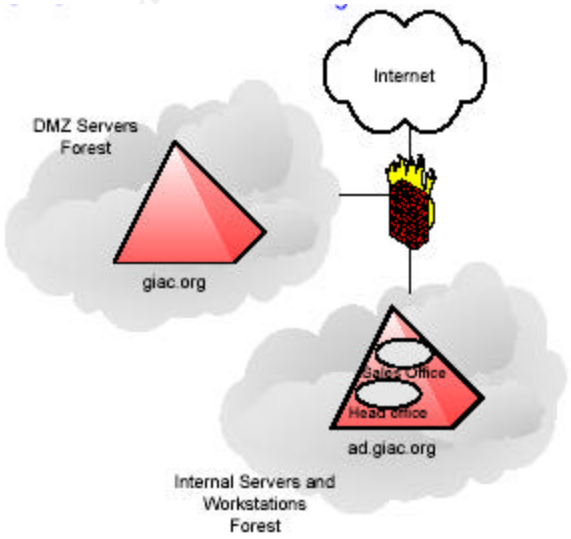

Diagram 4 GIAC-E Active Directory Structure

The name of the DMZ domain is “giac.org”, and the name of the internal domain is “ad.giac.org”. The domain names imply a parent and child relationship between them. However, as was mentioned above, in the GIAC-E Active Directory implementation, the domains are not bound by any trust.

The giac.org domain (DMZ domain) consists of external web servers, a backend database server and administrators accounts.

The ad.giac.org domain (Internal domain) contains all the non-Internet serving hosts and internal user accounts. Workstations, internal servers and users across the two locations are members of this domain. Logical structuring, administration of the domain and right delegation is performed at organization unit (OU) level.

GIAC Enterprises is located in two offices bound by a high speed VPN connection. One site was configured for each location. Replication between sites was configured to use TCP/IP protocol.

Each domain, the DMZ domain and the internal domain, has its own domain-wide group policy. In addition, a dedicated policy is assigned to almost every OU inside the domains.

The DMZ domain includes 3 OUs, one is dedicated to the web servers, another to the database servers and the third to the database administrators (diagram 3).

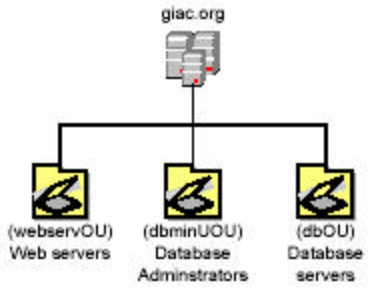

Diagram 5 DMZ Domain OU Design

The Web servers OU consists of 5 web servers. The web servers are configured identically through Group Policy.

The Database Administrators OU includes only database administrators’ accounts. There is a Group Policy to control their desktops and accounts.

The Database servers OU consists only of the backend database server. A special policy is assigned to this OU.

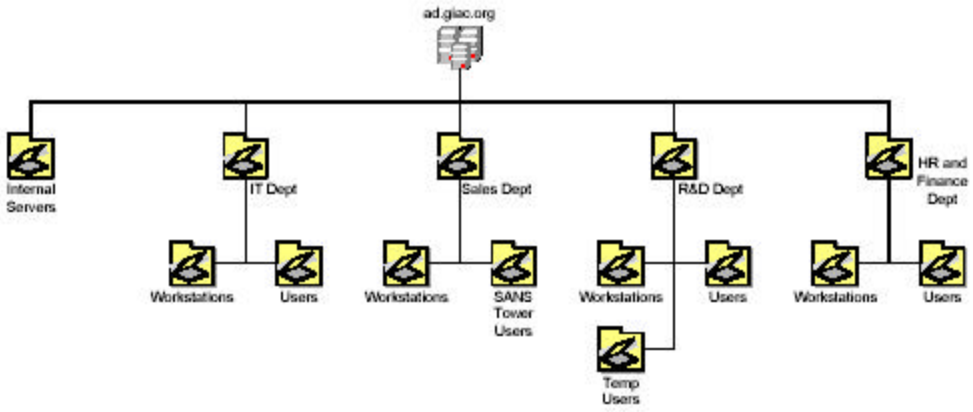

Diagram 6 Internal Domain OU Design

The internal domain OU structure (Diagram 6) reflects GIAC Enterprises' actual organization structure. The top level OUs represent the departments. Each department has the rights to implement its own Group Policy.

2.4. Merge Scenario

The two companies, SANS Co. and GIAC-E, have merged into a new company called GS. GS will have the extended product range of combined GIAC-E and SANS Co. product ranges. It will also use the SANS Co. sales network and support infrastructure for the GIAG-E product line and the GIAG-E e-commerce web site to sell SANS Co. products. The ultimate goal is to have a common interface with customers on all levels: web representation, sales and support.

2.4.1. Requirements for the GS IT infrastructure

The business goals of the merge present the following requirements for the GS IT infrastructure:

1. Common web representation. There should be a single group created to maintain external web servers. The group will consist of members of staff from both companies. They will maintain the companies' external web servers (in the DMZ domains) from their current offices.
2. Sharing of information between the companies' main offices, the R&D and the production divisions.
3. Integration of the GIAC-E production with the SANS Co. sales network. Resources in the GIAC-E production and R&D divisions should be available to the SANS Co. main office and the overseas sales offices, and vice versa.
4. Extension of the SANS Co. product support infrastructure to facilitate GIAG-E products. Resources should be shared between GIAG-E and the SANS Co. call centre.
5. Maintain or tighten security.

2.4.2. Merged Network

Since both companies already have a VPN setup, linking SANS Co. and GIAC-E offices implies adding new VPN links to the existing firewalls.

DNS name resolution is enabled across the AD domains of the two companies in order to:

- allow users or computers in one company to locate a resource (for example, an Exchange server, file share, or service) that is hosted on a computer located in the other company.
- allow users or computers to locate a domain controller in a different forest for the purpose of authenticating to a resource in that forest.
- allow a domain controller in one domain to locate a domain controller in a different domain to build an AD trust.

DNS servers in SANS Co. offices are configured to forward queries ending with ad.giac.org and giag.org suffixes to GIAC-E DNS servers. DNS servers in GIAC-E offices are configured to forward queries ending with sans.org and sans.com suffixes to SANS Co. DNS servers.

2.4.3. Merged AD Infrastructure

In order to address the business needs of the GS Company, the AD merge scenario was implemented as shown in Figure 2 “Merged AD Infrastructure”.

GIAG-E has advanced web representation which includes an e-commerce web site. The e-commerce web site is built on several IIS web servers in a load balancing schema and backend database. SANS Co, on the contrary, has a very simple web representation. It is based on a single IIS web server, and there is no supporting infrastructure for building an e-commerce web site. Therefore, it was initially decided to use GIAC-E’s web infrastructure as a basis for the united web representation. The SANS Co. web server will be assimilated by the GIAC-E web infrastructure. In the first phase, the content of the SANS Co. web servers will be transferred to the GIAG-E servers. Then the web server will be moved from the SANS Co. DMZ domain (sans.com) to the GIAG-E DMZ domain.

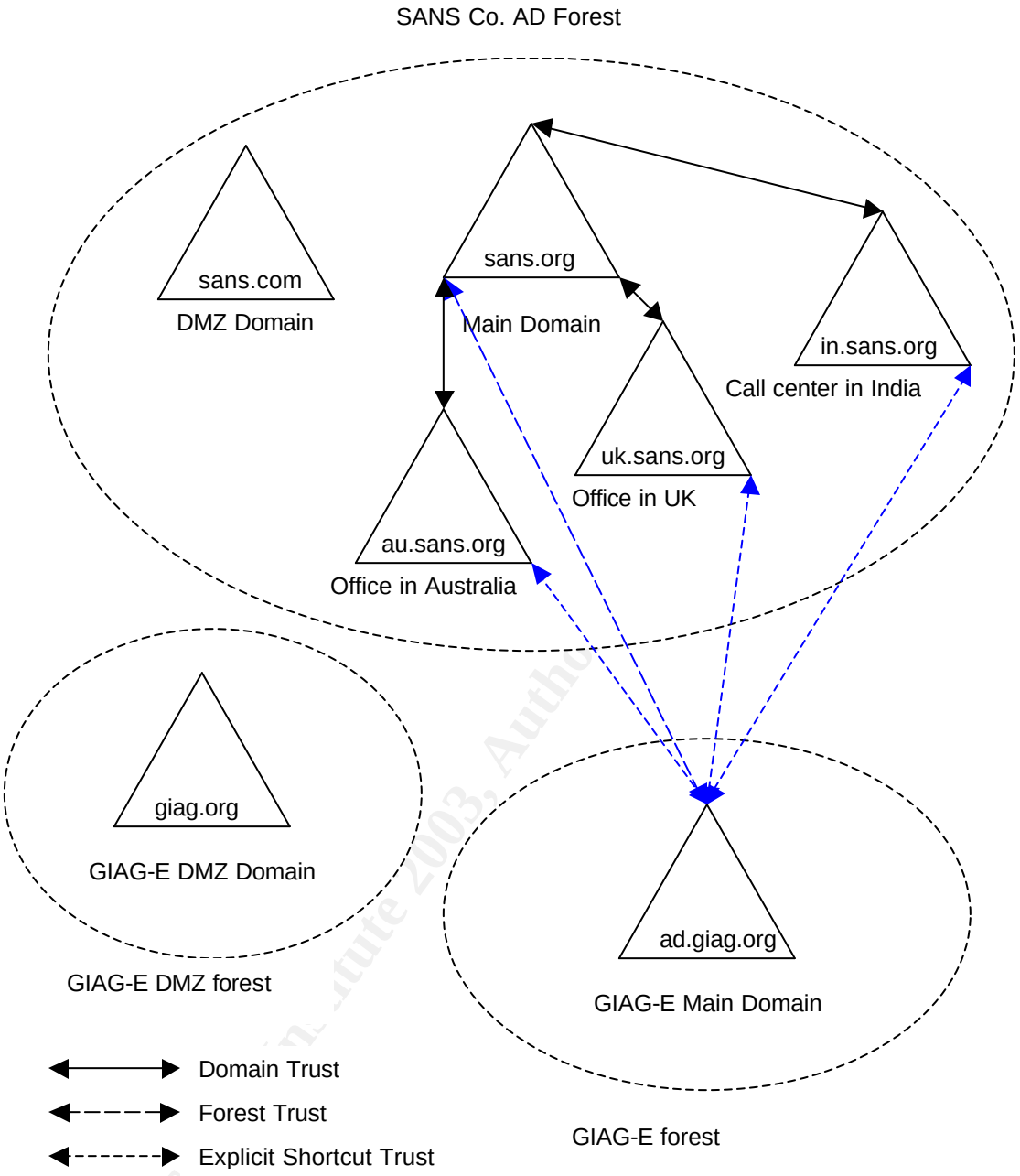

Figure 2 Merged AD Infrastructure

It was also acknowledged that having a separate forest for the DMZ domain is a securer solution than having a separate AD tree. Having a separate AD tree for a DMZ is not secure enough, due to the fact that trees within a forest are bound by transitive trust relationships and replicate AD information with each other. If one of the DCs in the DMZ is compromised, the other DCs within the same forest will become vulnerable. The only way to isolate DCs completely and prevent a single compromised DC from exposing the whole network, is to have two totally

separate forests, one for the DMZ and one for the main network. Having two forests makes administration more difficult. A set of explicit trusts would seem to be a way of simplifying administration and giving access to the web servers for web administrators from both companies, but it defeats the whole idea of isolation and requires opening ports on the firewall, which, in turn, makes the whole system more vulnerable. Therefore, the GIAG-E DMZ domain (giag.org) will have no trust relationships with any other domain. In order to allow access to the giag.org domain for SANS Co.'s web administrators, new accounts will be created in the giag.org domain. In order to tighten the security of the SANS Co network, a decision was made to break trust between the sans.com and the sans.org AD trees and then examine the possibility of separating sans.com via an isolated AD forest. Segregation of the sans.org DMZ domain into a separate AD forest requires thorough planning, but it is not technically, since there are only a few machines and a few administrative user accounts in the domain and, as was not the case with previous versions of Windows Server, demotion and promotion to Domain Controller does not require a reinstallation of the server.

The trust between the sans.org and the sans.com AD trees was created automatically by dcpromo wizard when the sans.com domain was added to the network. This is a transitive two-way trust which cannot be removed or modified using the GUI, as is shown in Figure3.

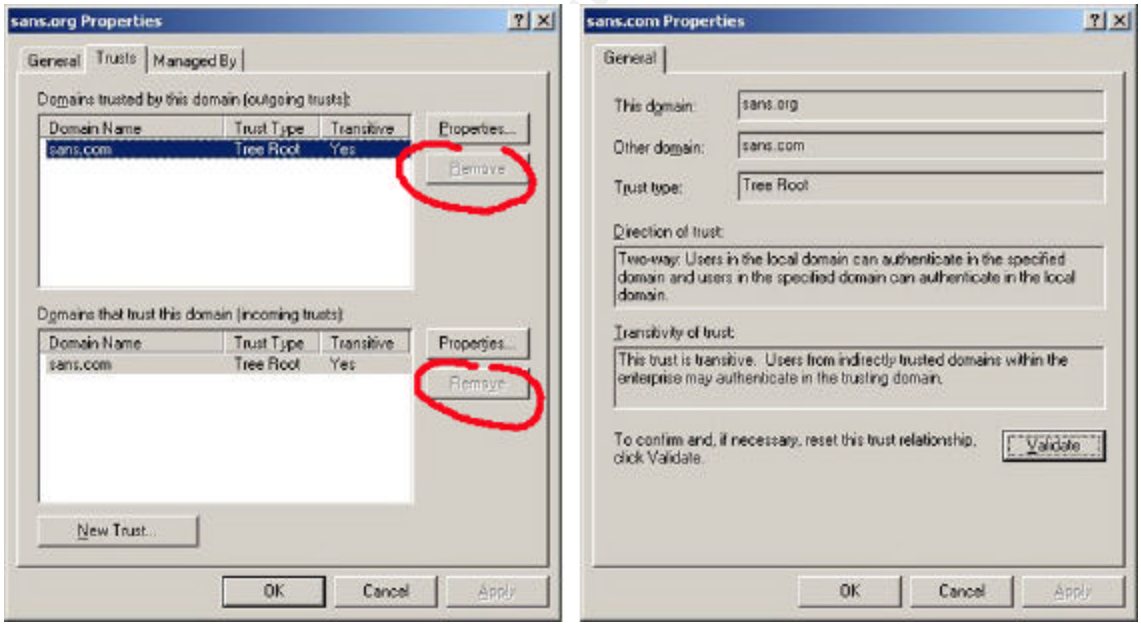

Figure 3 Default Forest Trust in SANS Co network

However, this trust is not immutable and can be altered with the help of the command line tool *netdom* which comes as a part of the Support Tools from Windows Server 2003 CDROM. The example below shows how the *netdom* tool can be used to see and modify trusts.

```
C:\>netdom query /domain:sans.org trust
Direction      Trusted\Trusting domain                    Trust type
=========      =======================                    ==========

<->      sans.com
Direct

The command completed successfully.


C:\>netdom trust sans.com /Domain:sans.org /remove /twoway
The command completed successfully.


C:\>netdom query /domain:sans.com /direct trust
Direction      Trusted\Trusting domain                    Trust type
=========      =======================                    ==========

The command completed successfully.
```

Removal of the default trust between the sans.org and sans.com forests practically isolates the sans.com domain. Users and administrators from the sans.org domain will not be able to connect to sans.com domain any more, thus local administrative accounts for responsible users will be created in the sans.com domain. For security reasons, these accounts will be different from the accounts in the sans.com domain.

In order to share information between the companies' main offices, the two primary domains, sans.org and ad.giag.org, were bound by Forest Trust[2]. Forest trust became available in Windows Server 2003; available options for creating a forest trust are shown in Figures 4 and 5.

[2] AD Forest Trust available only in Windows Server 2003
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_levels.asp

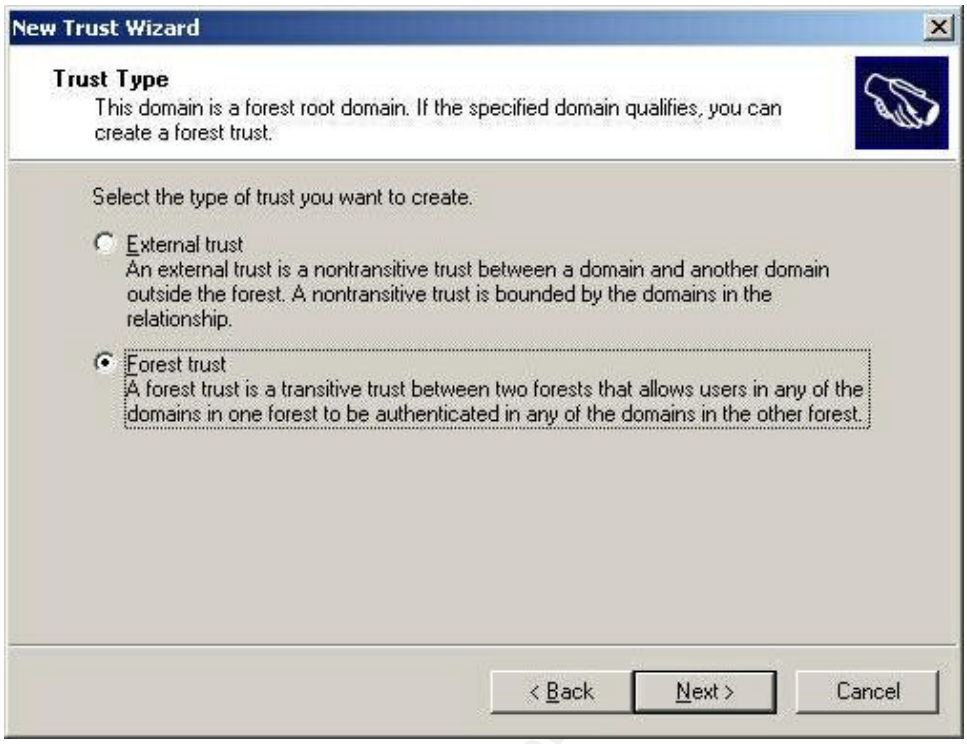

Figure 4 Creating Forest Trust

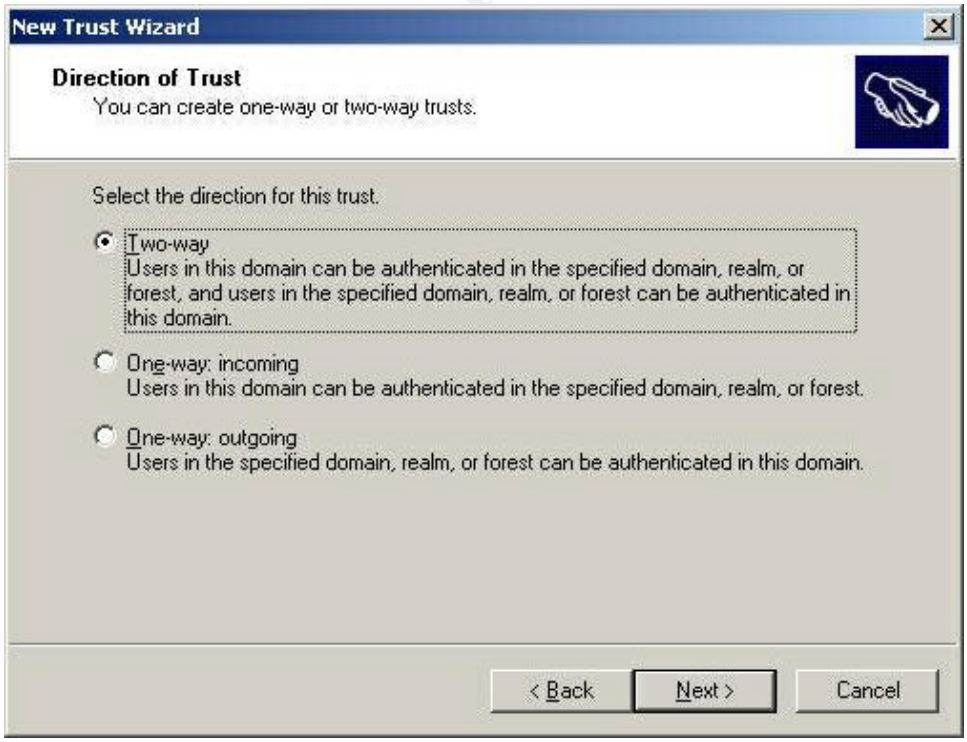

Figure 5 Available Forest Trust Types

The two forests (sans.org and ad.giac.org) are linked with a two-way forest trust, which forms a transitive trust relationship between every domain in both forests. This means that simply by creating the forest trust, we allow sharing of resources not only between SANS Co. and GIAC-E main domains, but also with the SANS Co. overseas sales offices, the SANS Co. call centre and GIAC-E main office. Therefore, the forest trust allows us to meet most of the requirements for GS IT infrastructure. It also provides the following benefits:

- Simplified Administration
    - The number of external trusts necessary to share resources across the two forests is reduced to one. This simplifies management of resources across the forests.
    - Complete two-way trust relationships between every domain in one forest and any domain in the other forests
    - Flexibility of administration. Administrative tasks can be unique to each forest, or applied across all forests.
- Transparency for users
    - Use of user principal name (UPN) authentication across two forests
    - Synchronizing data across forests. Global address lists (GALs) and objects can be integrated across forests using Microsoft Metadirectory Services (MMS). Common data types that need synchronisation across forests include:
        - GALs (Exchange)
        - Public folders
        - Directory objects

      Synchronizing this data across forests will help end users view address lists and other data in the same way as they view this information within their own forest.
- Security
    - Use of Kerberos V5 authentication protocols to improve the trustworthiness of authorization data transferred between forests.
    - By default, forest trusts in Windows Server 2003 Active Directory enforce SID filtering. SID filtering is used to prevent attacks from malicious users who might try to grant elevated user rights to another user account[3].

Although the forest trust allows the call centre and the overseas sales offices access ad.giag.com domain, the authentication process should follow the

[3] Microsoft Security Bulletin MS02-001 Trusting Domains Do Not Verify Domain Membership of SIDs in Authorization Data

Kerberos Referral Path in order to authenticate a user from one of the sales offices or the call centre in the ad.giac.org domain. This means that an authentication request will first be sent to the sans.org domain, and then the sans.org domain will request authentication in the ad.giac.org domain on behalf of the user. Since the offices are geographically very far apart and linked by a VPN over the Internet, an authentication process though the Kerberos Referral Path may take a long time. Therefore, for the practical reason of having an acceptable authentication speed, bidirectional explicit trusts were created between the ad.giag.org and uk.sans.org, au.sans.org and in.sans.org domains.

3. Security Policy and Tutorial

This chapter explains how Group Policy will be managed and applied across the forests. Although some of the principles of building a Group Policy are given, the complete design of a Group Policy is not provided. Designing a Group Policy is an extensive task, large enough to warrant a paper of its own. Also, it has been thoroughly covered already in the papers written for practical assignment version 3.1[4]. Only a fraction of a Group Policy for an IIS is be presented and used to demonstrate how the Group Policy is applied, how it can be tested and how it affects systems behaviour.

3.1 Group Policy Design and Management

One of the business needs related to the SANS Co and GIAC-E merger is to have a homogeneous IT environment and a uniform security setting across the whole network. The second goal is to centralise, simplify and minimize network management efforts.

In order to meet the business needs, a Group Policy that meets the merged company's standards has to be designed and applied across the two AD Forests. This Group Policy must be managed centrally.

Group Policy Objects (GPOs), which provide administrative control over users and computers, can be applied to a domain, an organizational unit (OU) or a site within the same forest. In GS's AD infrastructure, sites correspond directly to the domains, so it would be excessive to apply GPOs both to domains and to sites. Therefore, in the implementation we are discussing, assignment of GPOs at the site level was not used. In the SANS Co. AD Domains and in the GIAC-E Domain, OUs correspond to the business functions (departments), which means that a homogeneous infrastructure is already in place. In order to ensure identical settings, GPO objects will be designed for every type of OU (HR, accounting, marketing, production, support, R&D). These GPOs will reflect business function-oriented settings. Company-wide settings will be applied to the AD Domains.

When designing GPOs for OUs or the global GPO, Best Practices will be taken into consideration. Papers for the Practical Assignment version 3.1 and policy templates, available from Microsoft and various other organizations specialising in security, can be used as a basis. For example, to create a global GPO, NSA's *w2k_domain_policy.inf* template was used. The template was imported into the global GPO using the Group Policy Object Editor. It contains only a few settings (see Listing 1), but these are the only settings we want to deploy organization-wide. The rest of the settings vary from department to department and, therefore, will be assigned to OUs.

[4] GIAC Certified Windows Security Administrator (GCWN) Practical Assignment Version 3.1 (revised April 8, 2002) http://www.giac.org/GCWN_assign_31.php

```
; (c) Microsoft Corporation 1997-2000
; Security Configuration Template for Security Configuration Editor
;
; Template Name:        W2k Domain POLICY.INF
; Template Version:     05.00.DR.0000
;
; Revision History
; 0000  -           Original
; May 2001 - SNAC version 1.0
; November 2001 -
;           Changed the line "RequireLogonToChangePassword = 1" to
;           "RequireLogonToChangePassword = 0" under the [System Access]
;           section. This line is an artifact from Windows NT 4.0 templates and could have
;           adverse effects on a user's ability to change password at first logon. If you have
;           experienced this problem, please reapply this corrected inf file, or, via a
;           text editor, create and apply an inf file with only the following lines:
;           [Unicode]
;           Unicode=yes
;           [System Access]
;           RequireLogonToChangePassword = 0

;
;           NOTE: This setting does NOT appear when the template file is viewed graphically in
;           the MMC.

[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 12
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 15
LockoutDuration = 15
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 1
ClearTextPassword = 0
[Kerberos Policy]
MaxTicketAge = 10
MaxRenewAge = 7
MaxServiceAge = 600
MaxClockSkew = 5
TicketValidateClient = 1
[Registry Values]
[Profile Description]
Description=NSA Enhanced Security for Windows 2000 Domain Policy. Contains only account policies and one security option.
```

Listing 1 NSA Security Template

It is not possible to apply the same Group Policy Object to users and computers in multiple forests. Uniform settings can be deployed through identical Group Policy objects which are applied to the domains, organizational units, or sites in different forests. The Group Policy Management Console (GPMC)[5] makes it possible to manage Group Policy across multiple forests by importing and copying Group Policy Objects across forests. Figure 6 demonstrates how The Group Policy Management Console can be used to manage GPOs in different forests. The GS Global Policy was first created in the ad.giac.org domain and then copied into the sans.org domain. Now the sans.org domain has an exact replica of the global policy, and therefore settings across the forests will be identical.

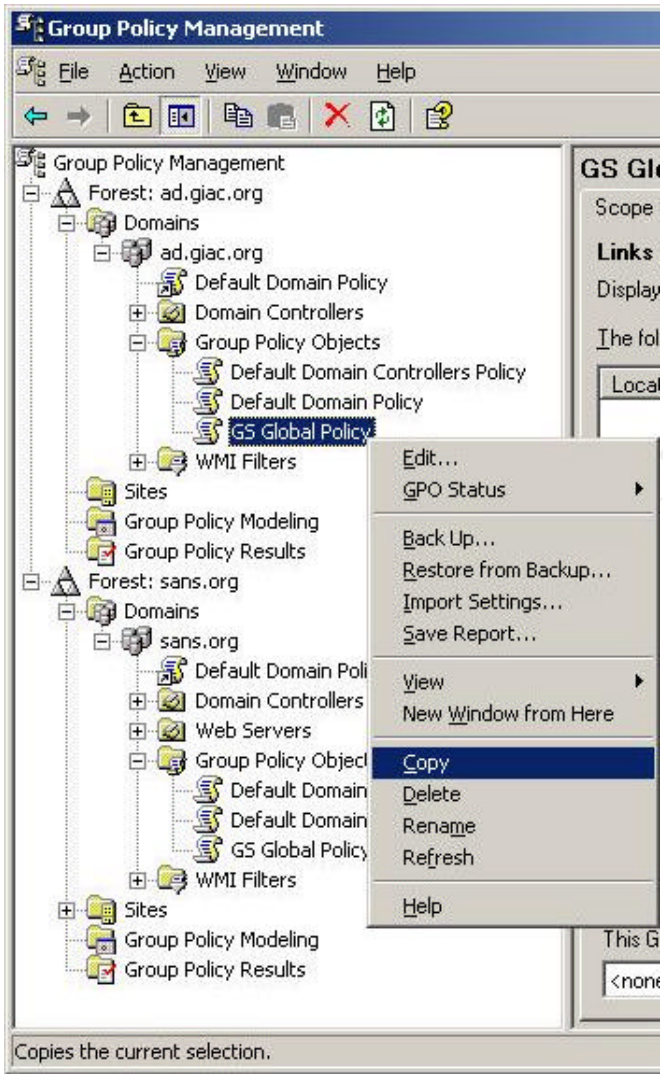

Figure 6 Using Group Policy Management Console to manage different forests

In order to manage multiple forests, the administrator has to have appropriate rights. The GS will assign an administrator to manage Group Policy and will delegate to him the rights to manage GPOs in both forests. In order to deploy identical settings across the company, the administrator will design GPOs, create them in one of the forests and then copy the GPOs to the second forest.

It is not possible to synchronise GPOs in different forests and domains. After the deployment, if there is a need to modify the Group Policy, the original GPO and its replica(s) have to be edited separately in order to maintain consistency.

A Group Policy for the GS will be designed, deployed and managed centrally by a dedicated administrator. GPOs will be configured in one of the domains and then copied to the others, which will ensure identical settings in all the domains.

[5] The Group Policy Management Console (GPMC) works only on MS Windows Server 2003 and MS Widows XP, but can be used to manage Windows Server 2000

Company-wide settings will be applied to the domains; departments' specific settings will be applied to the Organizational Units.

3.2. Tutorial

This tutorial shows application of the GPO to the GS internal IIS web server and testing of the GPO's settings. The two other tests check the server's functionality. At the end of the tutorial, an evaluation of the Group Policy is provided. The selected IIS server contains web pages for the Human Resource department. Some of the information is private and so cannot be disclosed. Therefore, although it is an internal web server, security requirements are high and are very close to the requirements for a web server in DMZ. In order to access the HR pages, the user has to provide identity information and a certificate issued by GS Certification Authority (CA). In the tutorial only a fraction of a GPO is considered. Although it is not a complete GPO, the selected settings make it possible to show the application of security settings and the centralized management of the server's settings and audit parameters.

3.2.1. Group Policy for IIS

The basis for the tutorial is a default installation of MS Windows Server 2003 with IIS 6.0. The server is a member server of the sans.org domain. Apart from being a web server, the server performs no other functions. By default, in Windows Server 2003 a universal set of services gets installed and activated. There are a significant number of services; most of them are not related to the web server function. Every service that is running not only consumes system resources, but can also make the server more vulnerable. Consequently disabling services that are not required makes the system more secure, faster and more stable. As an example, from a list of the first twenty two services (alphabetical order) shown in Figure 7, fourteen services are running. Half of these running services can be disabled without affecting the web server functionality.

The following services can be disabled:

- Computer Browser. DNS is used to find computers on the network.
- Distributed file system. The server does not act as a DFS root and does not host any DFS links.
- DHCP Client. The server has fixed IP address.
- Error Reporting Service. The service sends error reports to Microsoft, but a server that stores sensitive information should not send out any data.
- Help and Support. The server does not act as a Help and Support Centre.
- File Replication Service. The server is not a Domain Controller and does not host any DFS replicas.
- Automatic Updates. The servers are unique systems optimized for a specific role; therefore updates will be done manually in a controlled manner.

These amendments were implemented in the GS Web Servers GPO, which is shown in Diagram 7.

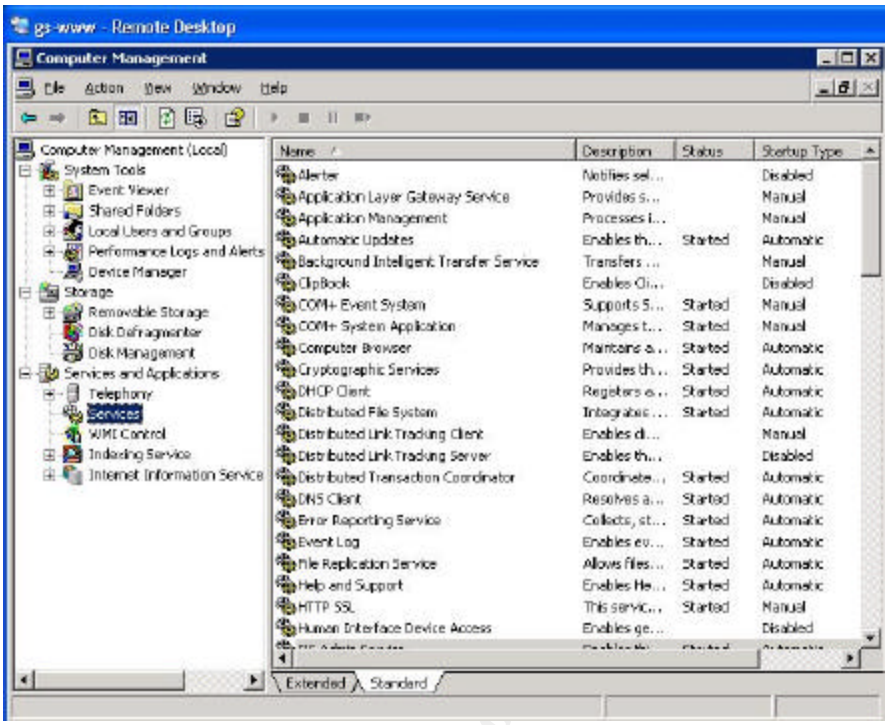

Figure 7 Services installed by default

Another issue that needs to be considered is access to the server. By default, as it is shown in Figure 8, the local Users group has rights to log on locally. The Users group, by default, includes the Domain Users group, which means anyone in the company can go to the server's console and log on. Even if the server room has substantial physical security, the tightening of the security settings should never be considered an excessive precaution. Because the membership and rights of local groups cannot be managed through Group Policy, the "Allow Logon Locally" right cannot be changed through a GPO without damaging the server's functionality. A safe way is to use the "Deny Logon Locally" right. Corresponding Group Policy settings are presented in Diagram 8.

As mentioned, the company's policy is to use certificates to access HR pages. The IIS server is configured to use SSL, and a server-side certificate is installed (shown in Figure 10). The certificate was issued by GS's own Certification Authority (CA)[6].

[6] In a real case, GS's own certificates would be the only ones installed on the server. Because the system used in the test lab is also used for other purposes in addition to emulating the GS IIS server, the other certificates have been conserved.

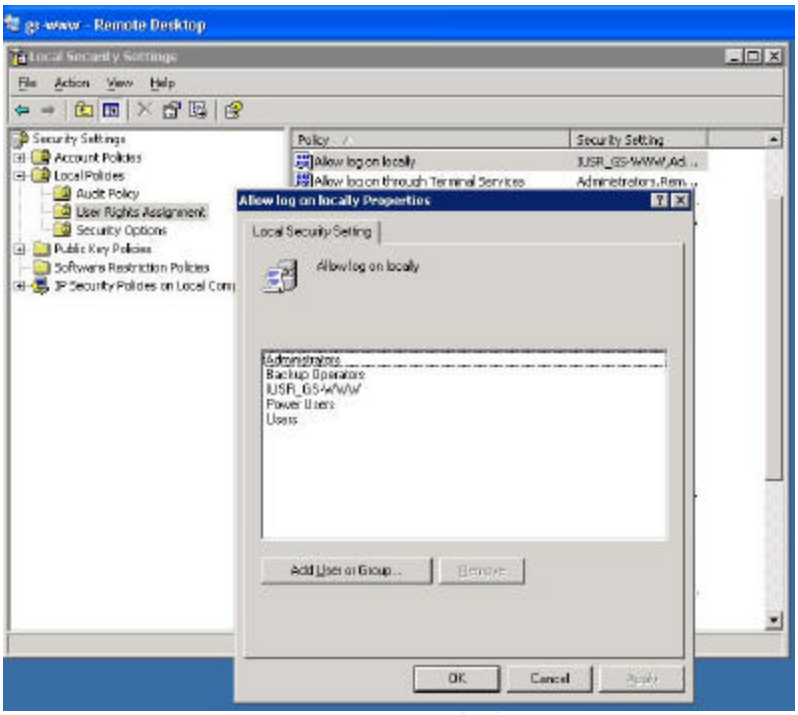

Figure 8 Default access rights

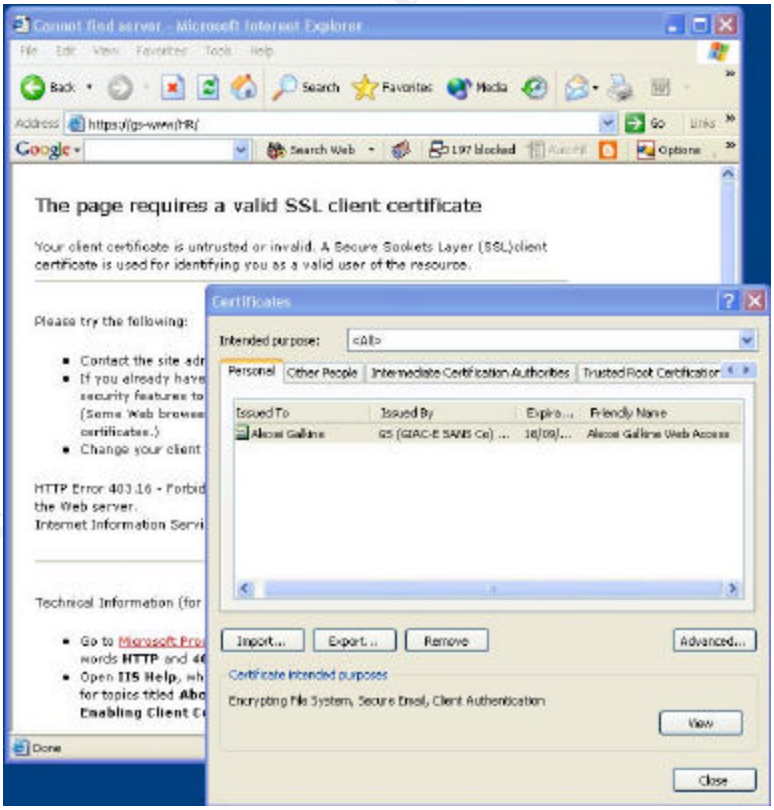

Figure 9 IIS server does not recognize the certificate

It appears that even if a user has a valid GS certificate, the IIS server does not accept it (see Figure 9). By default, the server did not trust GS CA. As shown in Figure 10, the GS CA certificate was not installed as trusted and was not present in the Trusted Root Certification Authorities list. Distribution of trusted root certificates can be done centrally through Group Policy. Diagram 7 demonstrates GPO settings for distributing the GS CA root certificate as trusted.

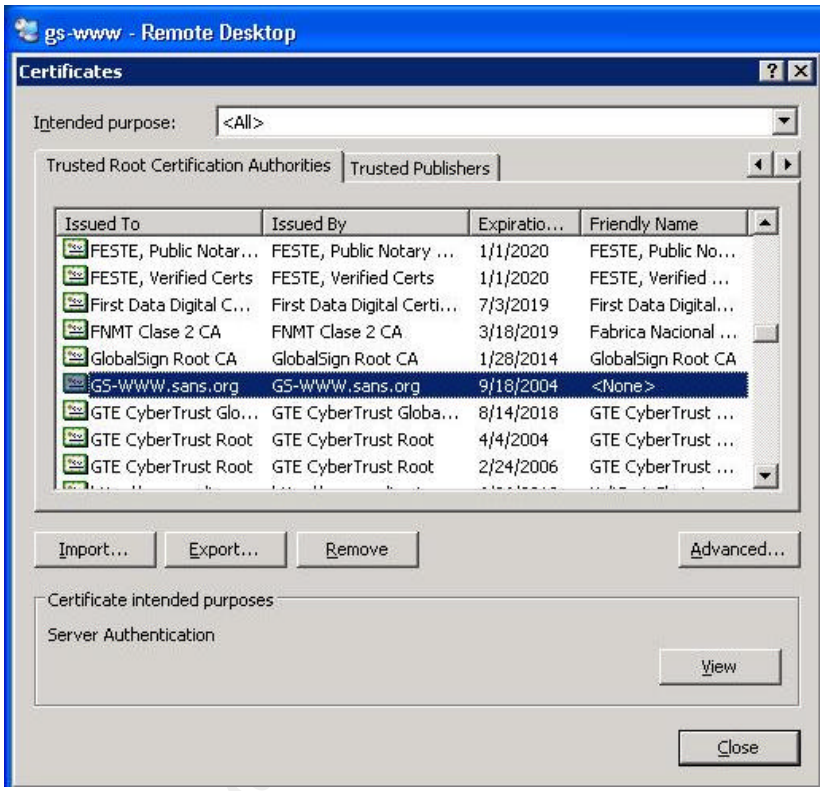

Figure 10 The Certificates installed on the IIS

All the settings were put together in the one GPO (see Diagram 7). In addition, the audit setting for logon events was configured. This audit setting will allow testing of the application of the Group Policy settings. Diagram 7 presents the resultant GPO for the GS internal web server.

GS Web Servers GPO

Data collected on: 9/19/2003 6:50:19 PM

General

Computer Configuration (Enabled)

Windows Settings

Security Settings

Local Policies/Audit Policy

Policy	Setting
Audit logon events	Success, Failure

Local Policies/User Rights Assignment

Policy	Setting
Deny log on locally	SANS\Domain Users, BUILTIN\Guests

System Services

Computer Browser (Startup Mode: Disabled)

Distributed File System (Startup Mode: Disabled)

DHCP Client (Startup Mode: Disabled)

Error Reporting Service (Startup Mode: Disabled)

Help and Support (Startup Mode: Disabled)

File Replication Service (Startup Mode: Disabled)

Automatic Updates (Startup Mode: Disabled)

Public Key Policies/Autoenrollment Settings

Public Key Policies/Encrypting File System

Public Key Policies/Trusted Root Certification Authorities

Properties

Certificates

Issued To	Issued By	Expiration Date	Intended Purposes
GS (GIAC-E SANS Co) CA	GS (GIAC-E SANS Co) CA	9/19/2008 12:06:18 AM	<All>

User Configuration (Disabled)

No settings defined.

Diagram 7 GS Web Servers GPO

3.2.2. Applying the Group Policy

A Group Policy Object called "GS Web Servers GPO" was created in the sans.org domain using the Group Policy Management Console. In the Group Policy Object Editor the GPO was configured with the settings explained above. After this had been configured, the GPO was linked to the "Web Servers" Organizational Unit of which the targeted web server is a member. From this moment the GPO can be applied to the server by one of the following methods:

- The Group Policy can be applied by restarting the server.
- The Group Policy can be refreshed in the background. The interval at which Group Policy is refreshed is defined by a refresh interval value and an offset interval value. By default Windows 2000-based systems use 90-minute refresh intervals[7]. To avoid the performance degradation that can occur if many Windows 2000-based computers request a group policy refresh from domain controllers at one time, a random offset interval is added to the refresh interval to determine the total amount of time between group policy application cycles. The default offset interval for Windows 2000-based computers is 30 minutes. Replication of Group Policy between domain controllers can also add a delay to the Group Policy refresh process.
- Application of the Group Policy can be enforced by the *gpupdate*[8] command line tool.

In the test lab I used the *gpupdate* command on the web server to get results immediately. In reality, since the *gpupdate* command can trigger the Group Policy refresh process on a remote system, it can be used in a script which enforces group policy update on a set of servers. This allows the administrator to apply new settings on all servers in a domain via a simple script. This can be done as soon as the settings have been defined. The second (default) approach is to wait for a background refresh to occur. The administrator can configure refresh intervals to suit company needs. The administrator should take into account that short refresh intervals add load to the domain controller, and long refresh intervals cause delay in applying security settings.

3.2.3. Testing the Group Policy security settings

After applying the group policy to the server, the following changes are expected on the system:

- The seven services (Computer Browser, Distributed File System, DHCP Client, Error Reporting Service, Help and Support, File Replication Service, Automatic Updates) are not running, and they are disabled
- A domain user is refused log on to the server's console and a security audit event is logged

[7] For domain controllers, the default refresh interval is 5 minutes and default offset interval is 0.
[8] *secedit* on Windows 2000-based systems

- The GS (GIAC-E SANS Co) certificate appears in the Trusted Root Certification Authorities list

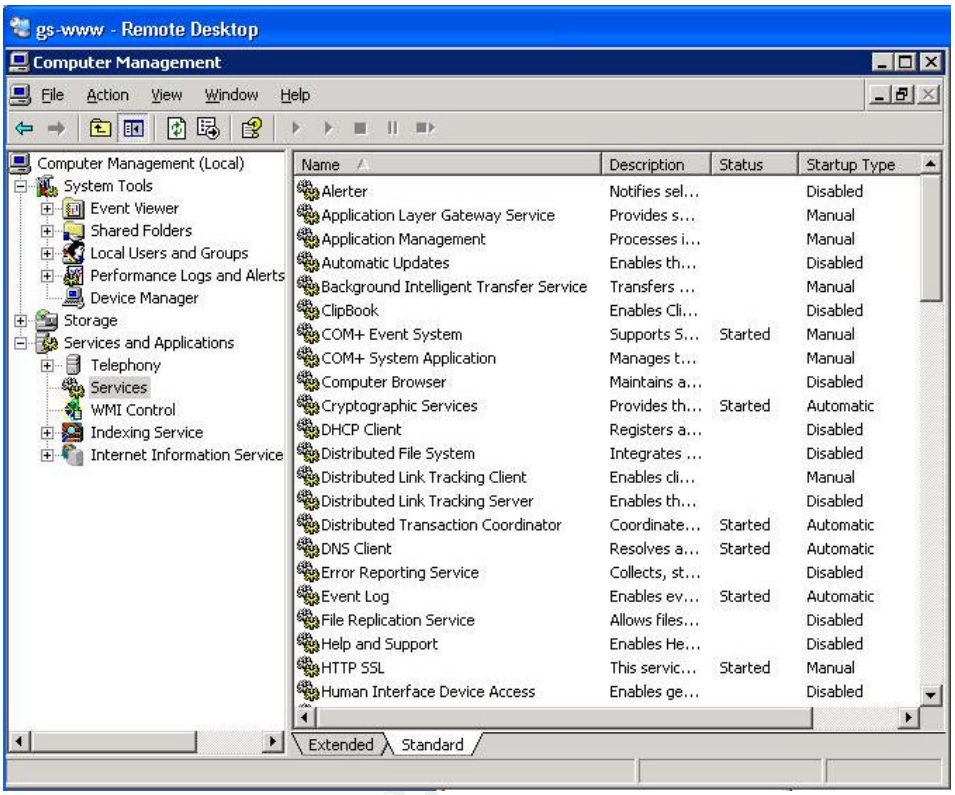

Figure 11 Microsoft Management Console. Running Services

Status of the services can be verified in the Microsoft Management Console. As shown in Figure 11 the services are not running and they are disabled.

I attempted to log on to the server's console with the Domain Users' credentials. I was denied access to the server and a corresponding security audit event appeared in the security log. The security audit event message is presented in Figure 12.

As expected, the GS (GIAC-E SANS Co) root Certificate appeared in the Trusted Root Certification Authorities list on the server, which is shown in Figure 13.

The test of the group policy security setting showed that the group policy was applied correctly. The new settings meet expectations, and the server behaves as expected.

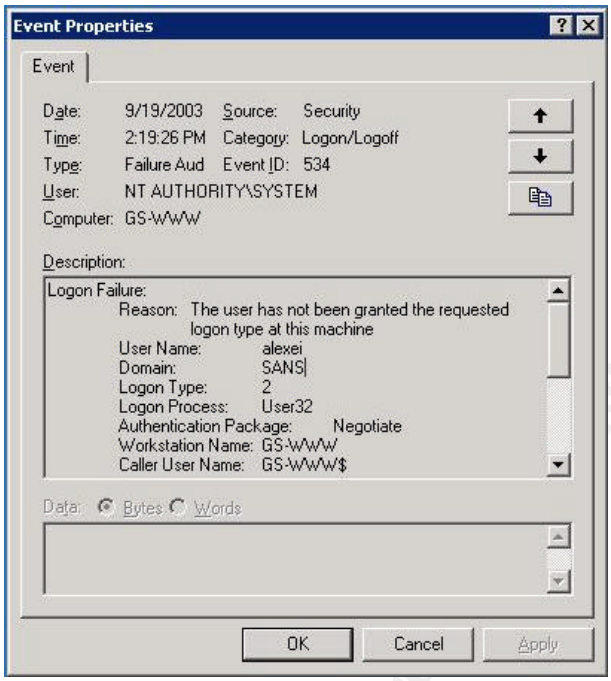

Figure 12 Security audit event message

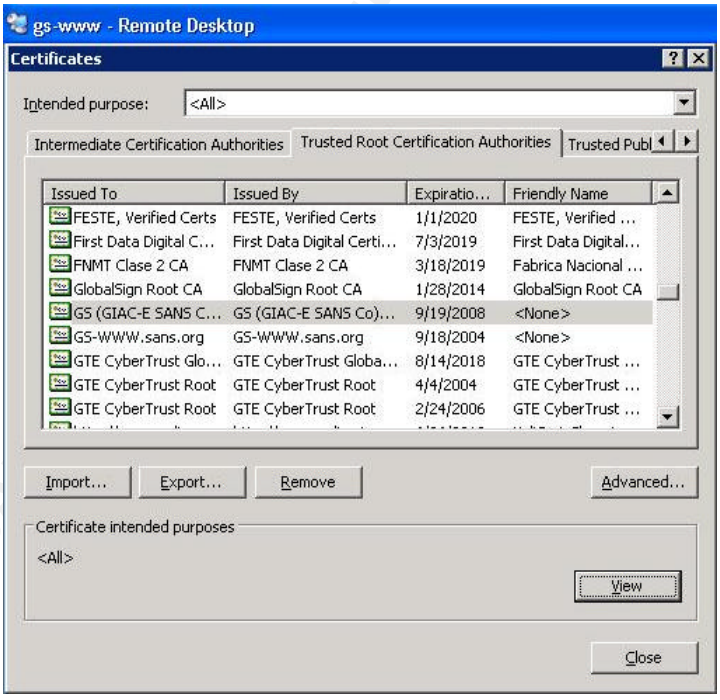

Figure 13 Trusted Root Certification Authorities list

3.2.4. Testing functionality of the system

The function of the server is to provide HTTP access to the GS internal web site. Some pages are published for everyone, others have sensitive information and require a GS (GIAC-E SANS Co) certificate and certain user credentials for access.

The server's functionality was tested from a standalone system, which gives a clear view of the moment when the server requests user credentials. As Figure 14 shows, the main page is displayed to everyone with no control over user credentials. Thus the result of the first test was considered positive.

Figure 14 Password and certificate are requested when accessing the secure pages

During the second test, a user tried to access the secure pages. When accessing the Human Resource Pages (the secure pages) the user has to provide adequate logon information and a certificate. Figure 14 shows that the logon window appears when clicking on the Human Resource Pages link. As was shown earlier in Figure 9, the user has the required certificate. Therefore, he is granted access to the pages, which is shown in Figure 15.

Figure 15 Access to the secure pages was granted

The tests of the system functionality showed that the server functions as expected. The application of the Group Policy does not affect the system's functionality.

3.2.5. Evaluation of the Group Policy

The Group Policy applied to the tested Intranet web server is a sum of the global GPO applied on the domain level and the GS Web Server GPO applied to the Web Servers Organizational Unit of which the tested server is a member.

The global policy defines Kerberos, lockout and authentication security settings. The GS Web Servers GPO disables unnecessary services, enhances audit settings, distributes the trusted root certificate and defines user rights. In total the Group Policy raises the security level of the system significantly and brings it up to the GS company requirements. Application of the Group Policy does not adversely affect the server's functionality. Therefore the Group Policy is considered as adequate.

The Group Policy does not cover the entire range of security settings. Further improvements can address the following areas:

- Event Log settings
- Redefining default IIS root directories
- Disabling unused subsystems
- Hardening TCP/IP parameters
- Securing access to IIS server files and operating system tools

Some of these settings can be configured using the default GPO template, while others require the creation of new administrative templates.

When the Group Policy was designed, the assumption was made that the web servers did not perform any other function. In reality, these servers can be used

for multiple functions, such as a secondary DFS root or to act as a Help and Support Center. In this case the GS Web Servers GPO has to be softened in order to comply with all the functions. This will automatically soften security settings on all the servers in the Web Servers OU regardless of their functions. This issue can be resolved by adding one more sublevel of OUs and defining GPOs based on the secondary function or by configuring the remaining server's specific security settings manually or via Security Templates.

The advantage of the proposed Group Policy is that all the security settings are managed and controlled centrally.

4. Audit

This chapter discusses methods of auditing GS (GIAC-E\SANS Co) network. At present, when networks consist of hundreds of servers and thousands of computers, administrators are unable to monitor the state of networks by checking each system status on an individual basis. Therefore automated audit systems become an essential part of any modern computer network. The general purpose of an audit system is to notify the administrator of any abnormal system behaviour or abnormal state and to provide this information in a timely manner and with sufficient information to allow the administrator to take prompt action. A good audit system provides an overview of the network as a whole, as well as the state of individual components. It detects changes in the system and deviations in system behaviour and reports them to the administrator. In a large network, an audit system is the only way to ensure that all system components are secure and functioning properly.

The requirements of the GS audit system are as follows:

- **Ubiquitous**. The audit system should monitor all the components and aspects of the network including the servers and workstations in the main networks, the machines in DMZ, other devices such as switches and UPS, each operating system and any running applications. It should be able to inform the administrator through a variety of methods: an audit system console, e-mail, or by a message on a mobile phone (SMS)[9].
- **Manageable**. The audit system should be easy to deploy, maintain and control. It must be flexible and adjustable to company specific needs. It should be possible to update, extend and modify the audit system centrally.
- **Self-controlled**. The audit system does indeed audit the network, but how can one be sure that the audit system works properly and there are no gaps? Who audits the audit system? The audit system should be able to audit itself. To audit itself, it should use various methods of collecting information. Having different audit methods allows the use of one method to report the state of other methods.
- **Forensic capture and later analysis**. It might be that an intrusion into the system or a system behaviour deviation is detected some time after its occurrence[10]. This may happen due to a flaw in the audit system, a

[9] An interesting method of notifying the administrator was presented at the SAGE LISA 2000 conference in the referred paper "Peep (The Network Auralizer): Monitoring Your Network With Sound" by Michael Gilfix and Alva L. Couch. The main idea was to represent system state by a set of sounds. Practical appliance of this method is disputable, but it is certain that the fastest way to alert the administrator is to produce a sound.

[10] The recent example is the crack of the GNU ftp site (http://ftp.gnu.org/MISSING-FILES.README). "The machine appears to have been cracked in March 2003, but we only discovered the crack in the last week of July 2003."

talented attacker, or simply a human factor: in a saturated flow of information, some information can get overlooked. Therefore, the system should archive collected information in case it is needed for later analysis or for litigation.

- **Automated**. The audit system should analyse audit events, send alerts, generate reports and archive audit data automatically. It should be possible to generate reports on demand.

4.1. Audit Plan

When defining an audit plan, the first question to answer is what we want to audit. For an internal network with Active Directory infrastructure, a set of audit parameters will include the following:

- Logon Events (failures) and account lockout
- Use of the Privileged Accounts
- Account creation and Deletion
- Active directory changes
- Reboots
- Computers overload
- File system and registry security settings
- Service pack and patch level
- Virus Scanner state

Some of these audit parameters are configured by default, for example reboot events are written into the System Log. Audit of other parameters could be configured through Group Policy. This was demonstrated in the chapter "Security Policy and Tutorial" under the "Group Policy for IIS". In order to audit the file system and registry security settings, the service pack and path level and the virus scanner state we must write scripts. For example, a script for checking the file system settings can run the *secedit* command to check the current state against a predefined security database; analyse the output and send an alert if a mismatch is detected.

The audit parameters can be divided into two categories: audit of actions and audit of state. An action can occur at any time, therefore actions have to be audited continuously, and the administrator should be notified of a malicious action as soon as possible. Appropriate methods of notification are e-mail, message on a mobile phone (SMS) and message to the audit system console. The state of a computer does not often change. Therefore, an audit of the state can be done by generating reports on a weekly basis. The purpose of these reports is to detect weak spots by showing if something was overlooked in the computer settings or whether all the applications are functioning properly. For example, the service pack and patch level reports show if all the computers were updated when deploying a security path. Virus scanner reports show if the virus

scanner is up-to-date on all the computers. The administrator should be able to generate reports on demand.

When setting up audit parameters, the frequency of the audit and the methods of notifying the volume of generated information need to be considered. Most of the audit events can simply be written into log files and archived; a review and analyses are done only if needed. Some events indicate potential danger and must be notified to the administrator immediately. Failure to log on to a desktop system is probably a mistyped password, but if it happens several times it becomes suspicious. If the number of failed logon attempts exceeds the limit defined in the group policy, the account will be locked. The administrator needs to know this and to check who is trying to log on to the computer, therefore this event should be reported immediately. Another example of an audit event which requires instant notification is a reboot of a server.

Log files from desktops and servers will be archived on a regular basis (daily). The log files will be copied to a central location and backed up on a tape. To ensure that no audit events are lost, the log files retention policy should last at least as long as two archiving intervals. The size of the log files should be big enough to hold all audit events for the retention period. The size of the log files and the retention policy are configured centrally in Group Policy. The values of specific parameters can be defined by monitoring the log files at the initial phase of deploying the audit system.

4.2. Audit System

It is always a challenge to get financing for systems not directly involved in production, such as a backup system, an audit system, an intrusion detection system and different security subsystems and tools. In the case of the audit system, commercial solutions are often complicated, inflexible and poorly automated. They often do not cover all areas, and they produce reports in a visually attractive, but impractical form. Active Directory has a potential for building a centralized audit system. Therefore GS designed its own audit system based on Active Directory, free tools and internally developed scripts.

The audit system consists of the following parts:

- Syslog Server
- Startup and shutdown scripts
- Daily security audit AT job
- Weekly reports

Syslog Server

Purpose	Yearly notification of malicious activities.
Method of installation	Installation of the syslog service is a part of the default installation for all GS computers.

Performed tasks	Real time analysis of logged events from all computers in the network. Sending alert messages when a dangerous event is detected.
Description[11]	Syslog service on a computer pushes records from local log files to a syslog server. The server writes the events into a consolidated log file. Then a script is used to filter the log file for important events. If such an event is detected, the script displays it on the console and sends an alert (e-mail).

Startup and Shutdown Scripts

Purpose	Yearly notification of shutdown and reboot events.
Method of Installation	Automatic, through Group Policy. The scripts are located on a network share on a server.
Performed tasks	• Send e-mail about shutdown/reboot • Check if the Virus scanner is installed and functions properly • Check if daily security audit AT job is installed
Description	Unplanned reboot of a desktop or a server indicates abnormal system behaviour and can be caused by a virus or intruder. Some viruses can gain administrator's rights after reboot. Therefore close monitoring of these events is necessary.

Daily security audit AT job

Purpose	Audit condition of computers. Report divergences from a predefined state.
Method of Installation	As a part of default installation for all GS computers
Performed tasks	• Copies local log files to a central location for archiving • Checks file system and registry security settings • Checks if the Virus scanner is installed and functions properly
Description	The script is executed from a network share.

[11] Application of the Unix Syslog to a Windows 2000 Network was described in the paper "Logging Windows 2000 Events With Unix Syslog" by Eric Yurick http://www.giac.org/practical/Eric_Yurick_GCNT.zip

	Therefore, it is easy to update and manage. Checking file system and registry security settings is done with the *secedit* command line tool. S*ecedit* is an example of a tool that can only be run locally. That is why we need a script which runs locally in our audit system. This script also allows us to perform audit tasks on all computers in the network simultaneously, and so the audit takes the minimum time to complete.

Weekly Reports

Purpose	Provide overview of the network state.
Method of Installation	Installed and run on one machine. The scripts query information on the computers over the network.
Performed tasks	• Virus Scanner update report • Overview of installed service packs and patches • Check if the Daily security audit AT job is installed on all computers
Description	Report-generating scripts are run as an AT job on the administrator's workstation or on a server. An example of a report script is shown in Appendix A. The script reports the virus scanner engine version and the virus definition file version. From the report, it is easy to detect if the virus scanner is out-of-date on any of the computers.

By writing several scripts, using free tools (syslog) and using the potential of Active Directory, a comprehensive audit system was developed. The system uses various audit methods: locally executed script, startup and shutdown scripts, centrally executed scripts and syslog. The diversity of the methods allows the monitoring of one method through another, and therefore the audit system ensures its own integrity. The system sends yearly notification of dangerous activities, monitors configuration of computers and provides reports with an overview of the network condition.

Appendix A – Virus Scanner Update Report

```
' ******************************************************
'Script Name: vs_update_report.vbs
'Version: 1.0
'Author: Alexei Galkine
'Last Updated: 23/07/2003
'Purpose:  This script checks virus scanner (McAfee VirusScan)
'update status. The script retrieves list of the computers in the OU
' in the DOMAIN and query every computer in the list for version of
' the virus definition file. The script retrieves list of the computers from the
' specified domain controller.
'Usage: cscript vs_update_report.vbs OU_name DOMAIN_name DC_name
' ******************************************************

On Error Resume Next

Dim i
Dim sComputer

' AD query related

Dim sPDC
Dim sOU
Dim sDomain
Dim sSQLquery
Redim aComputers(0)

' Registry Query related

Const HKLM = &H80000002
Const sKeyPath = "SOFTWARE\Network Associates\TVD\Shared Components\VirusScan Engine\4.0.xx"
Dim aValueName(2)
aValueName(0) = "szEngineVer"
aValueName(1) = "szDatVersion"
aValueName(2) = "szDatDate"
Dim aValue(2)
Dim iPadding

‘ read command line parameters
sOU = WScript.Arguments.Item(0)
sDomain = WScript.Arguments.Item(1)
sPDC = WScript.Arguments.Item(2)

        WScript.Echo ""
        WScript.Echo "============================================================="
        WScript.Echo "   Domain: " & sDomain
        WScript.Echo "    OU: " & sOU
        WScript.Echo "-------------------------------------------------------------"
        WScript.Echo "Computer Name  Engine Ver.    DatFile Ver.   Dat File Date  "
        WScript.Echo "-------------------------------------------------------------"


        ADSI_getComputers sOU, sPDC, sDomain, aComputers
```

```
        i = 0
        For Each sComputer In aComputers

        sComputer = aComputers(i)

        Err.Clear
        Set oReg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\" &_
                                    sComputer & "\root\default:StdRegProv")

        If Err.Number = 0 Then
                oReg.GetExpandedStringValue HKLM, sKeyPath, aValueName(0), aValue(0)
                oReg.GetExpandedStringValue HKLM, sKeyPath, aValueName(1), aValue(1)
                oReg.GetExpandedStringValue HKLM, sKeyPath, aValueName(2), aValue(2)
        Else
                aValue(0) = "no info"
                aValue(1) = "no info"
                aValue(2) = "no info"
        End if

        iPadding = 15 - Len(aValue(0))
        aValue(0) = aValue(0) & Space(iPadding)
        iPadding = 15 - Len(aValue(1))
        aValue(1) = aValue(1) & Space(iPadding)
        iPadding = 15 - Len(aValue(2))
        aValue(2) = aValue(2) & Space(iPadding)
        iPadding = 15 - Len(sComputer)
        sComputer = sComputer & Space(iPadding)
        Wscript.Echo sComputer & aValue(0) &  aValue(1) & aValue(2)

        i = i+1
        Next

        WScript.Echo "------------------------------------------------------------"
        WScript.Echo "  Total computers: " & i
        WScript.Echo "============================================================="
        WScript.Echo ""

Wscript.Quit()

'*****************************************************************************
'  ADSI_getComputers - gets list of computers in OU
'*****************************************************************************

Sub ADSI_getComputers(Byval sOU, Byval sPDC, Byval sDomain, ByRef aComputers)

   On Error Resume Next

   Const ADS_SCOPE_SUBTREE = 2

        Dim i

        sSQLquery = "Select Name from 'LDAP://" & sPDC & "/ou=" & sOU & ",DC=" & sDomain & _
                                    ",DC=sonytel,DC=be' where objectClass='computer'"

        ' Wscript.Echo sSQLquery
```

```
Set objConnection = CreateObject("ADODB.Connection")
Set objCommand = CreateObject("ADODB.Command")

objConnection.Provider = "ADsDSOObject"
objConnection.Open "Active Directory Provider"

Set objCOmmand.ActiveConnection = objConnection

objCommand.CommandText = sSQLquery

objCommand.Properties("Page Size") = 1000
objCommand.Properties("Timeout") = 30
objCommand.Properties("Searchscope") = ADS_SCOPE_SUBTREE
objCommand.Properties("Cache Results") = False
Set objRecordSet = objCommand.Execute
objRecordSet.MoveFirst

i = 0
Do Until objRecordSet.EOF
Redim Preserve aComputers(i)
aComputers(i) = objRecordSet.Fields("Name").Value
i = i+1
objRecordSet.MoveNext
Loop

End Sub
```

Example of the report

```
==========================================
  Domain:  SANS
   OU:  HR
------------------------------------------------------------------------
Computer Name  Engine Ver. DatFile Ver.   Dat File Date
------------------------------------------------------------------------
MUSKRAT         4.2.60       4.0.4294       9/18/2003
SEAL            4.2.60       4.0.4294       9/18/2003
……
ELAND           no info      no info        no info
QUOLL           4.2.60       4.0.4294       9/18/2003
…….
QUOKKA          4.2.60       4.0.4292       9/10/2003
IMPALA          4.2.60       4.0.4294       9/18/2003
------------------------------------------------------------------------
  Total computers: X
==========================================
```

References

1. Jason Lam, “Secure Windows 2000 Network for GIAC Enterprices”, GCWN Practical Assigment vesion 3.1 URL: http://www.giac.org/practical/Jason_Lam_GCWN.pdf
2. Jason Fossen, “Windows 2000/XP Active Directory”, www.sans.org, 2003
3. Jason Fossen, “Windows 2000/XP Group Policy and DNS”, www.sans.org, 2003
4. Jason Fossen, “Securing Internet Information Server”, www.sans.org, 2003
5. Jason Fossen, “Windows 2000/XP Scripting for Security”, www.sans.org, 2003
6. Eric Yurick, “Logging Windows 2000 Events With Unix Syslog”, GCWN Practical Assigment Version 2.1b URL: http://www.giac.org/practical/Eric_Yurick_GCNT.zip
7. Microsoft Corporation, “Multiple Forests Considerations”, White paper, 6/9/2003, URL: http://download.microsoft.com/download/0/2/6/026ee2e2-e06d-4660-b9db-6926fd200ed9/Multiforest White Paper.exe
8. Microsoft Corporation, “Establishing Interforest Authentication”, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/dsscc_aut_hirq.asp
9. Microsoft Corporation, “Forest Trusts”, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/x_c_foresttrusts.asp
10. Microsoft Corporation, “Windows Server 2003 Security Guide”, URL: http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en
11. Microsoft Corporation, “Security Bulletin MS02-001 Trusting Domains Do Not Verify Domain Membership of SIDs in Authorization Data”, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-001.asp
12. Microsoft Corporation, “HOW TO: How to Modify the Default Group Policy Refresh Interval”, URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;203607
13. Microsoft Corporation, “Planning and Implementing Federated Forests in Windows Server 2003”, Microsoft TechNet Article, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/security/fedffin2.asp
14. Microsoft Corporation, “Windows Server 2003 Resouces”, Microsoft TechNet Articles, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsnetserver/evaluate/cpp/reskit/adsec/part1/rkpdsefl.asp