Global Information Assurance Certification Paper

Dana Clark

GIAC Windows Security Administrator (GCWN) Practical Assignment
Version 3.2

SANS Co / GIAC Enterprises Secure AD Integration

Domain Design, Group Policy Development and Audit Requirements of a Merged Enterprise

Table of Contents

Abstract

This paper describes the secure integration of Active Directory (AD) Infrastructure for the fictional SANS Co. and GIAC Enterprises. SANS Co. is an industry leading developer of military simulation games for the domestic personal computer (PC) market. GIAC Enterprises is an industry leading developer of online computer games. With the growth and maturity of the online gaming market continuing at a steady rate, executives at SANS Co. envision a merger with GIAC Enterprises as a natural fit to enable the company to enter the lucrative multi-player online gaming space. As each company has significant successful public "brand" awareness it is very important to maintain each public entity to ensure continued success.

As a result of the merger between SANS Co. and GIAC Enterprises, a team of highly qualified infrastructure and security professionals has been assembled to manage and implement the secure integration of both company's AD infrastructure. Both companies use the Windows 2000 operating system as a server standard and Windows XP as the desktop, workstation and mobile standard. As both companies have well established AD implementations, the executive team has mandated that both AD forests shall remain intact to minimize initial merger impact to existing personnel. A future project may be initiated to integrate both AD infrastructures into a single AD forest but the immediate concern is to take steps to ensure a successful merger. The primary goals of the current integration project are as follows:

- Enable secure interoperability between AD infrastructure of both SANS Co. and GIAC Enterprises in a manner seamless to users.
- Consolidate IT administration functions of both SANS Co. and GIAC Enterprises into a single functional unit.
- Integrate World Wide Web systems and infrastructure while allowing existing customers to access both parts of the new company.

This paper will discuss the AD design of both SANS Co. and GIAC Enterprises prior to merger activities, including domain structure and current organizational site functions. The secure integration details of the AD infrastructure of the merged company will be described in detail with particular emphasis on the resultant security policy including effects the security policy has on the corporate intranet services. Finally, an audit plan of the merged AD infrastructure of SANS Co. and GIAC Enterprises will be presented to show the long term viability of the AD design.

1.0 SANS Co. Active Directory Infrastructure Design

SANS Co. AD infrastructure is an AD forest comprised of a root domain (SANSCO.NET) with three domains based on primary business function. The "Empty Root" AD forest model was selected to allow SANS Co. to expand globally in the future. As many countries have laws that may affect or restrict how IT infrastructure is deployed and secured, the "Empty Root" model allows for the flexibility required in this regard. Only the resources required to manage the forest are contained in the root domain. The three current domains are as follows:

- **OPS.SANSCO.NET** – The OPS domain is the domain used for the majority of business functions within SANS Co. and contains users, computers, printers and servers. The majority of SANS Co. infrastructure resides in the OPS domain including the SANS Co. Exchange 2000 E-Mail system. The business units within this domain include Executive Management, Sales and Marketing, and Information Technology teams.

- **HR.SANSCO.NET** – The Human Resources domain contains users, computers, printers and servers specific to Human Resource functions such as recruitment, payroll, benefits, training and employee relations. This domain is considered a highly managed, highly secure environment due to the sensitivity of data used by the HR group and the intense competition for talented developers in the highly lucrative gaming market.

- **RD.SANSCO.NET** – The Research and Development domain contains users, computers, printers and servers specific to game development, programming and quality assurance. As the activity within this business unit is core to the company's success it is also treated as a highly managed, highly secure environment in order to maintain and protect proprietary development processes, program code, and other intellectual property.

In addition to the core AD infrastructure, SANS Co. also utilizes a standalone forest, SANSCO.COM, to house the company's Demilitarized Zone (DMZ) for World Wide Web (WWW) services and other external services such as Domain Name Service (DNS) and E-Mail gateway. SANSCO.COM is considered a high security domain with extensive security services and systems to protect it from exploitation. The SANSCO.COM domain has no trust relationship with the SANSCO.NET forest.

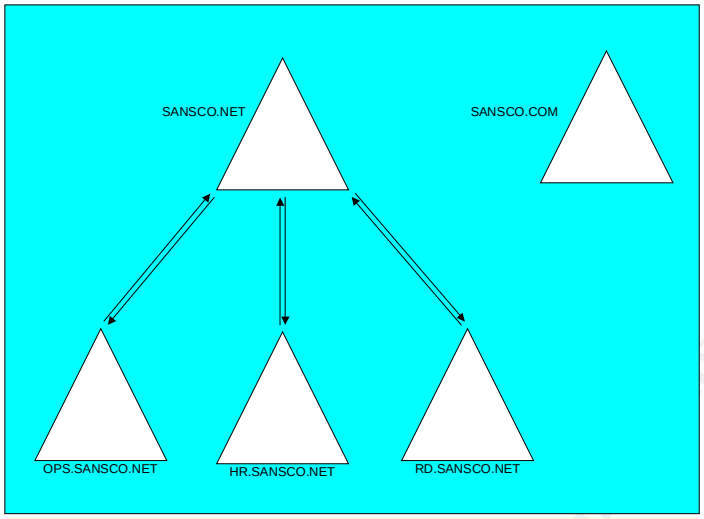

Figure 1 - SANS Co. Active Directory Domain Structure

1.1 Site and Network Design

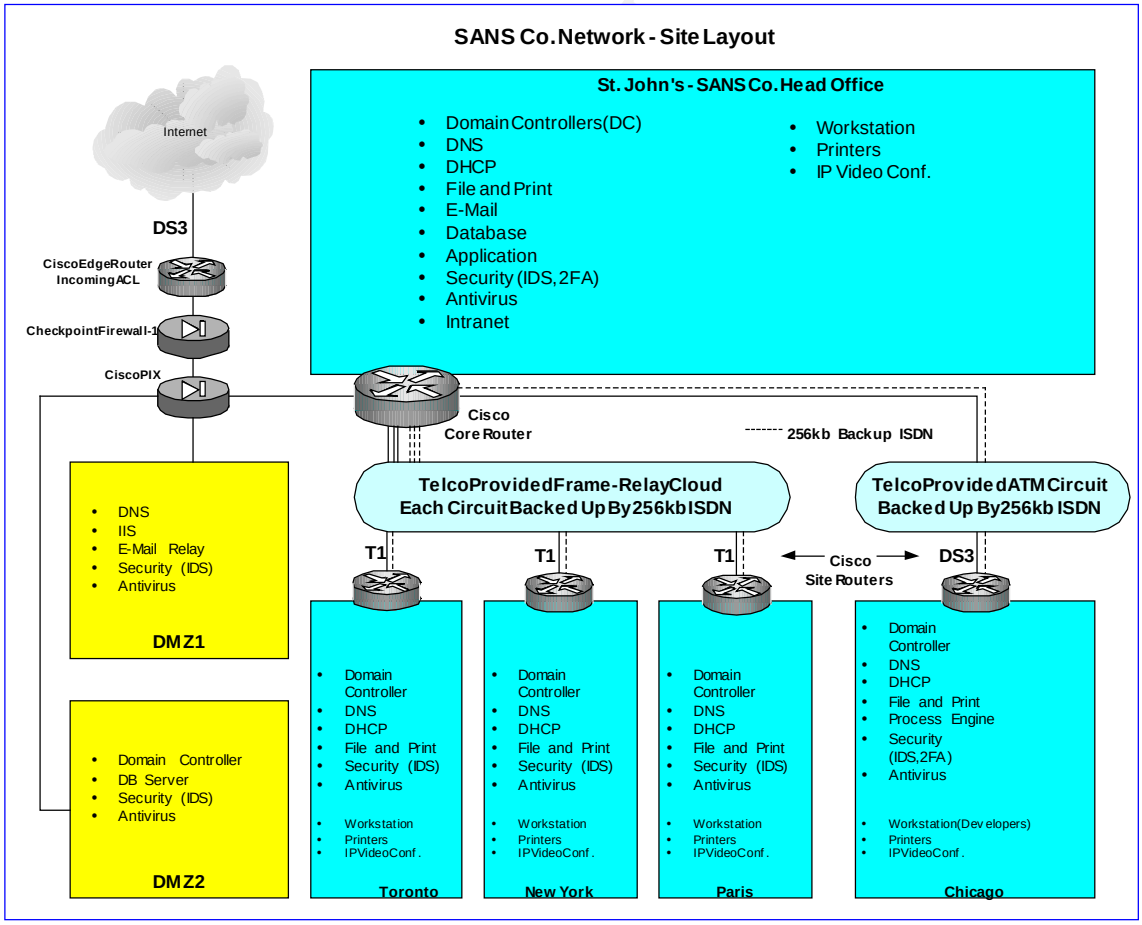

Figure 2 – SANS Co. Site and Network Design

SANS Co. head office is located in St. John's, Newfoundland, Canada which includes the company's Executive, Human Resources and Information Technology teams. The company has sales offices in Toronto, New York, and Paris as well as a significant research and development centre located in Chicago.

Each geographic location represents an AD site within the SANS Co. AD structure with the St. John's site acting as the hub in the hub and spoke site topology deployed at SANS Co. Each site within SANS Co., with the exception of Chicago, is connected using fully utilized T1 frame-relay WAN circuits with 256 Kbps ISDN data circuits used as redundant backup in case of failure of the primary circuit. The research and development site in Chicago is connected to the head office in St. John's utilizing a DS3 data circuit (45 Mbps) to facilitate enhanced product evaluations and presentations to the company's executive team. This site data circuit is also backed up with a 256 Kbps ISDN circuit for basic network redundancy. As communications to the Chicago research and development site is by its very nature sensitive and highly confidential, all communications traversing the circuit is encrypted in a VPN tunnel utilizing a 256-bit AES[1] hardware based encryption feature with Cisco routers.

The DMZ forest SANSCO.COM is located at SANS Co. head office in St. John's, Newfoundland, Canada and is connected to the Internet via a DS3 data circuit to the Internet service provider (ISP). The ISP provides diverse fiber path into the Sans Co. computing facility and also offers significant diversity in its metropolitan fiber mesh network in St. John's to assure communications to the ISP head end. SANS Co. practices "Defense in Depth[2]" to protect the DMZ and in particular, the internal network from external exploitation. In addition to firewall rules, Access Control Lists (ACL) are in place to control ingress traffic through the edge router as well as ACL's to control both ingress and egress traffic through the core router.

Ethernet connectivity within each site is provided by the use of Cisco Catalyst class switches. Each site network runs gigabit Ethernet for the backbone and server interfaces with dedicated 100 Mbps connectivity to each workstation through distribution Catalyst switches in each office area.

1.2 Organization Units

The root domain SANSCO.NET contains only two organizational units (OU), Domain Controllers and Administrators. The Domain Controllers OU contain all the domain controllers for the forest and are rigidly controlled and secured. The Administrator OU contains the user objects for "Enterprise Administrators".

[1] AES, http://csrc.nist.gov/CryptoToolkit/aes/
[2] Brooke Paul, http://www.networkcomputing.com/1214/1214ws1.html

To ease the implementation of standard company security policies, each functional domain within the SANSCO.NET forest has common organizational units; computers, users, administrators and printers (Figure 3).

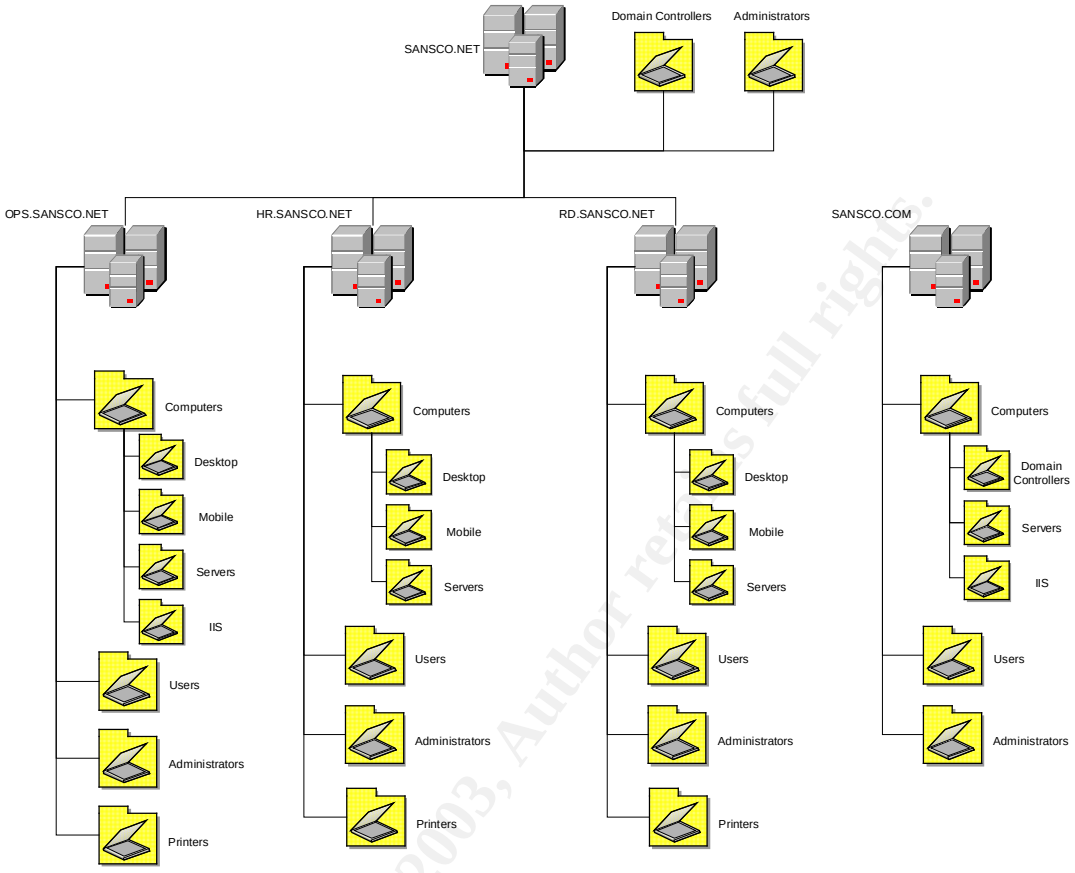

Figure 3 – SANS Co. Active Directory OU Design

1.3 SANS Co. Miscellaneous Security and System Integrity Considerations

1.3.1 Computing Facilities and Server Hardware

All servers within SANS Co. are physically secured in access-controlled facilities with redundant environmental equipment and uninterruptible power supplies. All servers and facility equipment are SNMP manageable and are monitored by a network monitoring system. All faults are reported to IT response personnel who carry pagers 24X7X365.

All servers are built and configured utilizing high availability options such as redundant power supplies, fans, network interface cards (IPSec cryptographic offload capable), and memory. All servers have a minimum of two processors and use redundant hardware based array controllers. All arrays are configured as either RAID 1 (mirrored) or RAID 5 (distributed parity) depending on the

function of the server. All arrays of the same type share a hot standby disk to quickly recover to full RAID status in the event of a failure.

1.3.2 Enterprise Security Systems

First line intrusion detection is enabled through the use of network intrusion detection systems by Enterasys. Network taps are installed in all segments of the network including the external interface of SANS Co.'s edge router and the DMZ. ISS RealSecure Host based intrusion detection systems are deployed on all servers to detect unauthorized traffic and access on SANS Co. servers. All critical detections are passed to the network monitoring system and reported to information security personnel for investigation and action.

Antivirus protection is provided by the Symantec Antivirus Gateway scanning all incoming and outgoing traffic through the SANS Co. DMZ. This includes all incoming and outgoing SMTP, FTP, and WWW traffic. SANS Co. protects all internal assets from virus exploitation by installing Trend Micro antivirus software on all Servers, E-Mail systems, and workstations including mobile computers. The systems are scheduled to check for and download new virus pattern files on an hourly basis and notify information security personnel via the network monitoring system should a virus outbreak occur. Using different vendors for antivirus systems internally and externally offers the maximum protection against infection and subsequent internal outbreak.

1.3.3 Mobile Computing Security

All mobile computers used at SANS Co. utilize the offline file capability provided by Windows XP and synchronize with the network file servers upon connection to the network. As the mobile computers are considered highly managed, security has been set to only allow users to write files to the documents and settings folders (i.e. Offline files). The documents and settings directory along with temporary file locations on the mobile computer are encrypted using the Windows XP encrypting files system (EFS). Users of mobile computers connect to the network when out of the office using the Cisco VPN client utilizing IPSec and SecurID two factor authentication (2FA).

1.3.4 Administrator Security

All administrative users are required to authenticate to the network using a proximity logon device, XyLoc from Ensure Technologies, as well as their password for two factor authentication (2FA). The XyLoc card automatically locks the administrator's workstation when they physically move away from the perimeter of the authentication device. Administrative authority to manage user accounts, printers, servers, and workstations is delegated to accounts located in each of the SANS Co. domains in the administrator OU. The delegated

administrator accounts are only granted the administrative controls required to perform specific administrator functions.

1.3.5 Domain Security

The SANS Co. root domain contains only the objects required to administer and operate the entire domain. These objects include the administrator's accounts (Enterprise Administrators) and the domain controllers for the SANSCO.NET forest. All SANS Co. domain controllers are configured to use IPSec 3DES encryption when they communicate with each other to ensure that AD replication is secure from end to end.

The HR domain is considered a high security environment due to the type of sensitive information processed. All users in the HR domain are also required to authenticate to the network using a proximity logon device, XyLoc from Ensure Technologies, as well as their password for two factor authentication (2FA). The XyLoc card automatically locks the user's workstation when they physically move away from the perimeter of the authentication device. In addition, all computers and servers are configured to use IPSec when communicating with HR specific servers running sensitive HR applications, but fall back to clear text when communicating with general purpose servers in the OPS domain. Security policy for HR domain computers and servers is significantly more restrictive than general computers and servers in the OPS domain. User and services auditing is significantly more comprehensive in the HR domain. Specific security policy for each domain will be discussed in detail later in this document.

The RD domain is also considered a high security environment due to the sensitive proprietary data used in the development of new games. All users in the RD domain are also required to authenticate to the network using a proximity logon device, XyLoc from Ensure Technologies, as well as their password for two factor authentication (2FA). The XyLoc card automatically locks the user's workstation when they physically move away from the perimeter of the authentication device. In addition, all computers and servers are configured to use IPSec when communicating with sensitive applications and services residing on RD servers, but will fall back to clear text when communicating with general purpose servers in the OPS domain. Security policy for RD domain computers and servers is significantly more restrictive than general computers and servers in the OPS domain. User and services auditing is significantly more comprehensive in the RD domain.

The DMZ forest SANSCO.COM is an obvious high security environment and is protected by several means already mentioned in this document. This includes multiple firewalls in the "defense in depth" network design, network and host based intrusion detection systems, and antivirus systems. Security policy for SANSCO.COM DMZ servers is significantly restricted and will be detailed later in this paper. All communications between IIS servers and database servers in the split DMZ will be encrypted using IPSec.

1.3.6 IIS Security

IIS Server security is of particular concern with special emphasis placed on the IIS servers located in the DMZ. The following security measures are taken when configuring IIS servers:

- Web site content files are located on a separate drive than the operating system, program files, and administrative scripts.
- All sample, help, and IIS administration files are deleted after IIS is installed.
- The latest service packs and hot fixes with implications for IIS are immediately applied once verified through proper change control measures.
- IIS Write and Execute permissions are never applied to folders accessible to anonymous users.
- All unused ISAPI Extensions and HTTP Verbs are unmapped.
- All unneeded ISAPI filters are removed.
- URLSCAN.DLL is installed and configured to reject all unauthorized requests and change the server description in the header line of the server response to “Generic HTTP Server”.

1.4 GIAC Enterprises Active Directory Infrastructure Design

The AD infrastructure design for GIAC Enterprises is well documented in GIAC practical assignment by Edmundo Farinas and can be found at the following location:

http://www.giac.org/practical/GCWN/Edmundo_Farinas_GCWN.pdf

GIAC Enterprises AD design is comprised of a single AD forest, GIACENTERPRISES.COM, consisting of three OU’s called SPUSERS, REGUSERS, and TEMPS. The OU SPUSERS contains users required for the research and development (RD) teams within GIAC Enterprises. The OU REGUSERS contains users required for Sales & Marketing, HR, Finance, IT, and Quality Assurance (QA) departments. The TEMPS OU is used specifically for users of outside contractors and temporary interns. The following OU’s have been added to the top level of GIAC Enterprises and applicable AD objects are moved to enable easy application of common GPO’s:

- Administrators: GIAC Enterprises Administrator Accounts

- Domain Controllers: GIAC Forest Domain Controllers
- Servers: Regular Security Servers
- High Security Servers
- Computers: Regular Security Computers
- High Security Computers
- High Security Mobile Computers

GIAC Enterprises head office is located in Chicago (Site 1) with a branch office located in Toronto (Site 2). The head office houses the RD, Sales & Marketing, HR, Finance, IT and QA departments while the Toronto office has a small contingent of Sales & Marketing and HR personnel.

Since the document by Edmundo Farinas was written, GIAC Enterprises deployed Exchange 2000 services due to problems with the previous POP3 E-Mail implementation. GIAC has also upgraded the desktop operating system to Windows XP for all users with Windows 2000 professional workstations.

1.5 GIAC Enterprises / SANS Co. Active Directory Infrastructure Integration

As both GIAC Enterprises and SANS Co. currently do business in common cities (Chicago and Toronto), the executive team decided to move GIAC personnel into SANS Co. facilities as there was adequate physical space available and SANS Co. network and security infrastructure was far superior to that of GIAC Enterprises. This move simplified network requirements and offered equal network security to both operating organizations without changing daily operational activities and procedures for each group. Network separation for GIAC and SANS Co. at each site was realized with the implementation of virtual local area networks (VLAN).

The information technology function for both GIAC and SANS Co. has been centralized in the St. John's site with local support personnel located in each office with specific expertise to service personnel located at each site (i.e. RD personnel in Chicago).

In order to enable cross-forest resource access between the GIACENTERPRISES.COM and SANS Co. sub domains (OPS, HR, and RD), the following activities have been completed:

- Enable name resolution across forest boundaries. Configured DNS secondary zones between each forest DNS to allow zone transfers (Figure 4), and therefore name lookups of resources between forests.

- Create two external one-way, non-transitive domain trusts[3] (Figure 5) between GIACENTERPRISES.COM and each SANS Co. sub domain (OPS.SANSCO.NET, HR.SANSCO.NET and RD.SANSCO.NET).

- Create global groups for cross-forest resource access and add these global groups to corresponding universal groups.

- Create domain local groups containing appropriate universal groups and apply security to resources to provide cross-forest access.

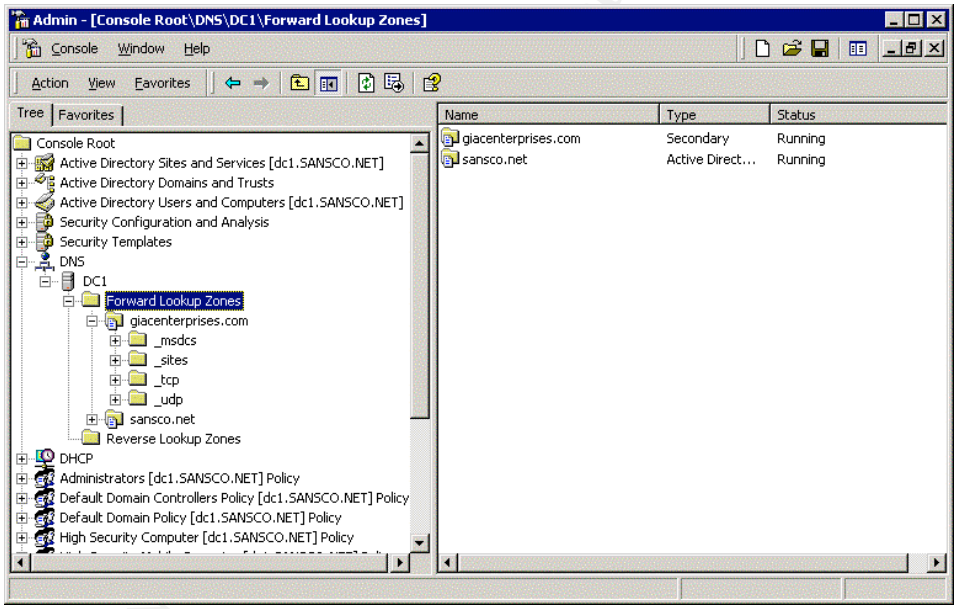

Figure 4 – DNS Secondary Zone Configuration

[3] Microsoft Knowledge Base Article - 309682

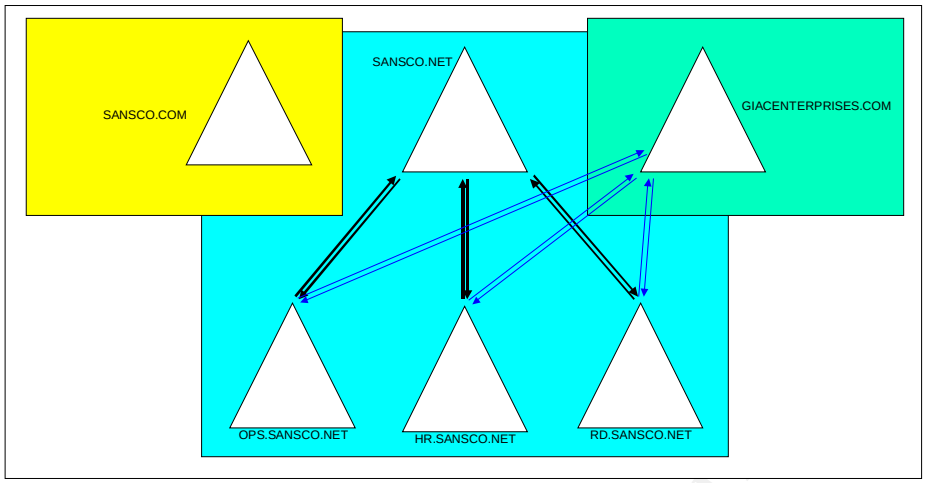

Figure 5 - SANS Co. / GIAC Active Directory Domain Trusts

In order to maintain efficient operation, interoperability and administration of the GIAC Enterprises AD infrastructure among all locations of the combined company, GIAC AD sites were expanded to include all sites (St. John's, New York and Paris) and domain controllers built and placed in sites new to GIAC Enterprises.

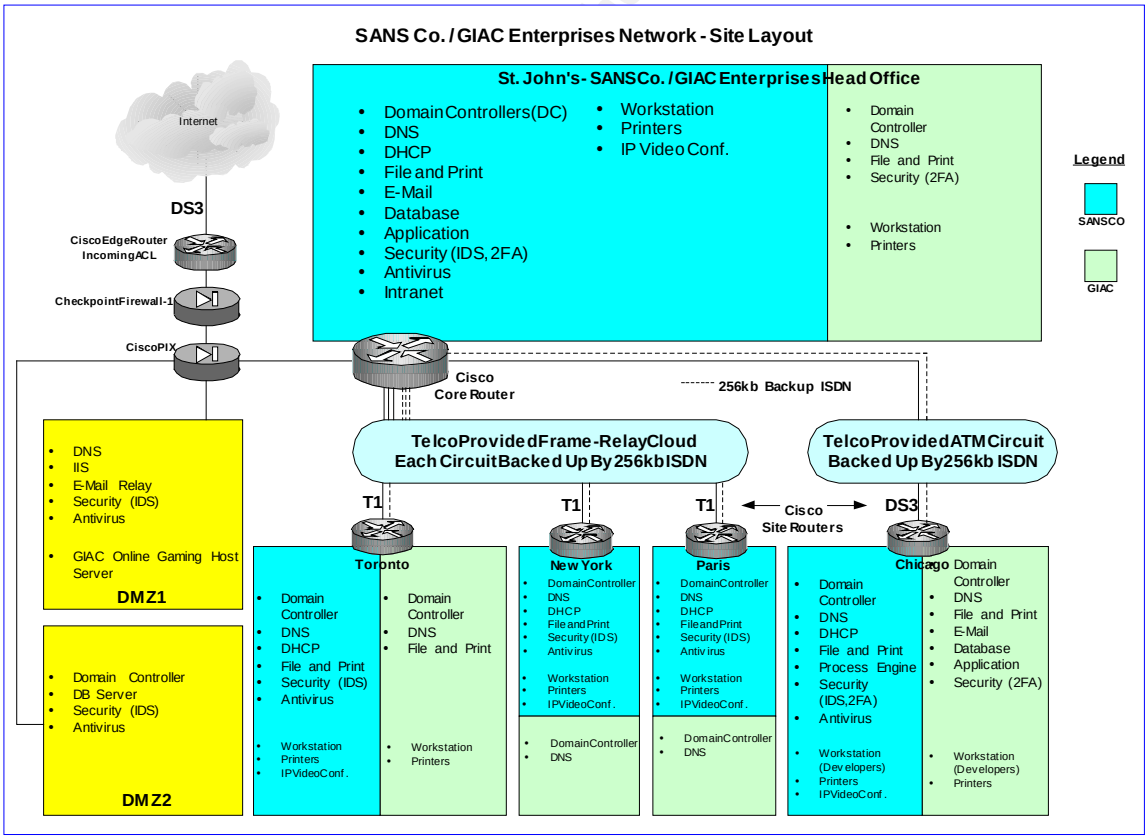

Figure 6 – SANS Co. / GIAC Merged Site and Network Design

1.6 Common DMZ Services for SANS Co. / GIAC Enterprises

All services formally located in GIAC Enterprises DMZ in Chicago have been moved to the St. John's location and included in the SANSCO.COM DMZ forest. The St. John's DMZ has more than adequate bandwidth (DS3) to handle the external facing services required for both public entities such as DNS name resolution, E-Mail relay, corporate WWW and FTP services. GIAC online gaming host servers have also been moved to the St. John's DMZ to save costs and to improve maintenance and update efficiency of the GIAC online gaming host servers.

SANS Co. outsources its public DNS services to ALLDOMAINS.COM Delta DNS service to provide fail-safe DNS resolution for external facing services located in the DMZ such as WWW, FTP and E-Mail relay. Only systems required for public interaction are configured in the Delta DNS service. With the addition of the public GIAC services including the online gaming servers, DNS changes were scheduled and staged to provide virtually no down-time during the physical transition of services to SANS Co. facilities and at the same time maintaining the two separate public identities of the merged organization as mandated by the executive team. A local DNS server is operating in the DMZ to satisfy SANSCO.COM AD requirements as well as providing internal DNS servers with DNS name caching and DNS forwarding capability.

1.7 SANS Co. / GIAC Enterprises Miscellaneous Security and System Integrity Considerations

Sans Co. / GIAC does not create common "Universal" groups to provide administrative functions to both forests. Administrative functions are always performed using an administrative account belonging to the forest where the change is occurring. The purpose of this separation is meant to prevent cross-forest compromise in the unlikely event that an administrative account is breached in either AD forest.

One of the issues with maintaining separate forests for use by Sans Co. and GIAC Enterprises is Microsoft Exchange 2000 interoperability. Natively, it is very difficult to provide all users visibility to the global address lists (GAL) of both Exchange systems as well as free and busy calendaring information across forests. Sans Co. / GIAC implements the Microsoft Identity Integration Server 2003 (MIIS) to perform near real-time synchronization of mail enabled objects in each forest including all mail attributes for users, distribution lists, and calendar free / busy information. The implementation of MIIS provides users of both organizations with a common view of E-Mail services regardless of which system they reside.

2.0 Security Policy Implementation Using Group Policy Objects

The SANS Co. and GIAC AD infrastructures will be managed separately but consistent security policies and procedures will be expected to be used whenever possible. To accomplish consistent security across both AD forests, the development of enterprise standard AD group policy definitions and templates is critical for success. Sample templates and security recommendations from SANS[4], the National Security Agency (NSA)[5], and Microsoft[6] will be used as a starting point to developing each computer group policy object. Each setting will be evaluated and tested for operational acceptance in the SANS Co. and GIAC AD environment.

Group policies are applied to AD objects in a specific order of precedence (Local Computer, Site, Domain, and OU) and are applied at different levels of interaction with the AD (Computer Boot, User Logon, and updates at scheduled intervals). With this in mind, high level security policy is applied at the default domain and sub domain level with specific policies applied to OU containers. In order to keep GPO development and implementation as simple as possible to operate and troubleshoot, Sans Co. and GIAC GPO's will only be applied at the Domain and OU levels with no GPO's applied at the sites. In order to improve logon performance Sans Co. / GIAC will disable all user configuration settings at the higher level domain GPO's (Figure 8) as these policy settings only apply to computer policies. As well "Group Policy Slow Link Detection" is enabled for all mobile users (500 Kbps bandwidth or less) so only critical settings (Security Settings, ADM Registry Values, EFS Recovery Policy, and IPSec Policies) are applied when accessing the network remotely. This prevents the remote connection from being saturated by group policy updates while working out of the office.

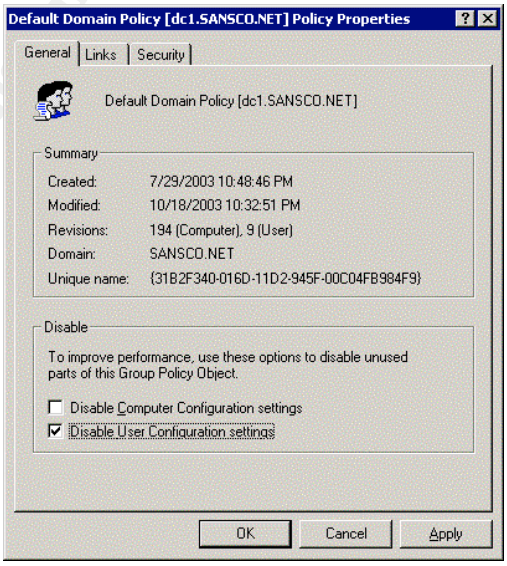

Figure 7 – Disabling User Configuration at Domain GPO

[4] Securing Windows 2000 Step by Step Version 1.5
[5] http://www.nsa.gov/snac/index.html
[6] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/secwin2k/default.asp

In the Sans Co. / GIAC AD environment, only “Enterprise Administrators” will have permissions to edit and deploy GPO’s. All GPO’s will have access control lists (ACL) applied to them in order to enforce this administration policy with the remaining users having “read” and “apply group policy” permissions.

In order to record, deploy, and maintain the desired security policy settings for Sans Co. / GIAC, a security template will be defined for each standard group policy object. A security template is simply an ASCII text file with an .INF extension that contains all security settings for a GPO in a single file. The “Security Templates” MMC snap-in is used to create and edit each security template in a graphical representation.

Once a security template is defined, it can be applied to a GPO by following a few simple steps; right click on the “Security Settings” option within “Computer Configuration: Windows Settings” and select “Import Policy” (Figure 9). Select the appropriate security template to apply to the group policy object. As a standing procedure, Sans Co. / GIAC always backs up the security settings using the same process as importing a security policy but selecting the export policy and saving the security policy to a template backup folder.

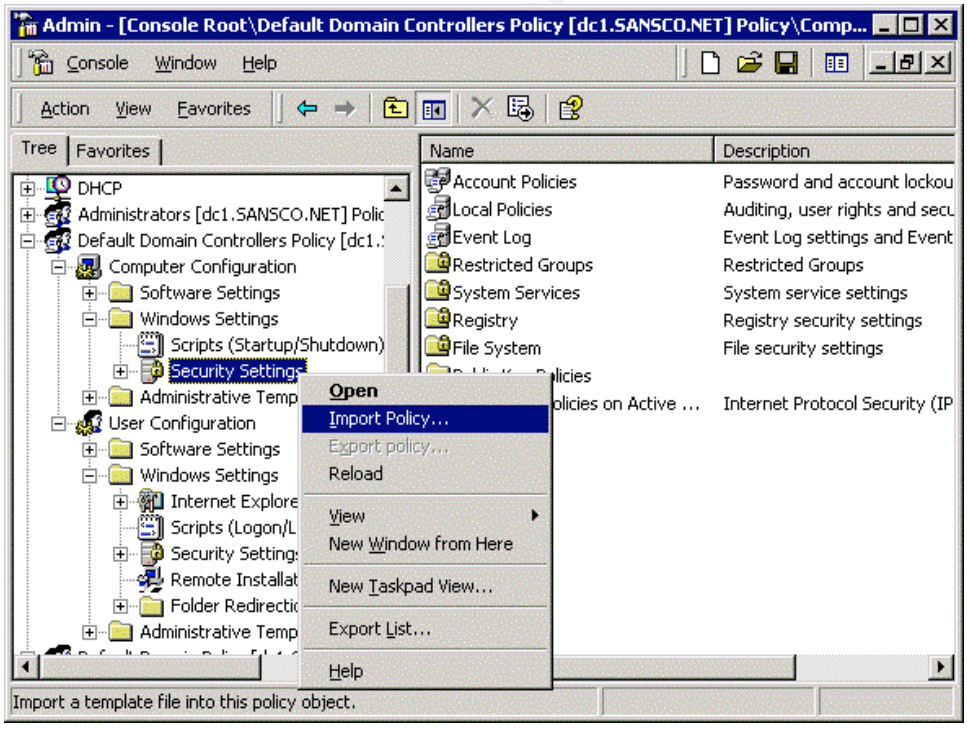

Figure 8 – Importing a security policy into a Group Policy Object

The following standard group policy object's (GPO) will be defined for application to both AD forests:

- Default Domain
- Default Domain Controllers
- Standard Servers
- High Security Servers
- IIS Servers
- Standard Computer
- High Security Computer
- High Security Mobile Computer
- Administrators
- Standard Personnel

As the bulk of security on a Windows network is determined by its password and account lockout policies[7], only these setting will be included in the domain group policies and described in detail. The remaining GPO's will be listed and only the settings pertinent to this paper will be described in detail.

The Default Domain GPO is defined as follows:

Account Policies: Password Policy

Policy	Description	Setting
Enforce Password History	Number of password remembered. Prevents user from reusing passwords.	24 passwords remembered
Maximum Password Age	Age of password before a password change is forced.	30 days
Minimum Password Age	Age of password before a password change is allowed. Prevents a user from cycling through password changes to make the password the same as previous password.	1 day
Minimum Password Length	Minimum number of characters required for password. Sans Co. / GIAC users trained to use "Passphrases" rather than typical passwords.	14 characters
Passwords Must Meet Complexity Requirements	Must use three of four of the following character groups (Upper case alphabetic, lower case alphabetic, numeric, special characters). Complexity makes it harder to crack using password cracking tools.	Enabled
Store Passwords using Reversible Encryption for all Users in the Domain	Ability to store passwords using a reversible encryption algorithm. Required for many authentication methods such as Radius.	Enabled

[7] Windows 2000 / XP Group Policy and DNS (Track 5) Course Guide, Page 81, SANS Institute

Account Policies: Account Lockout Policy

Policy	Description	Setting
Account Lockout Duration	Period of time an account is locked out when account lockout threshold is exceeded. Prevents various password crack attempts.	0 minutes
Account Lockout Threshold	Number of logon attempts before an account is locked. Prevents various password crack attempts.	5 invalid logon attempts
Reset Lockout Counter After	Period of time before the lockout counter is reset after the first failed logon attempt. Prevents various password crack attempts.	240 minutes

At Sans Co. / GIAC, account policies are taken very seriously and are applied and enforced at the very top level of the GPO's in use. The Default Domain GPO affects every object within the AD manageable by group policies, which makes it the logical place to address the largest security concern. Passwords are required to be changed every thirty (30) days and users are trained to use passphrases rather than traditional passwords for maximum password protection. This measure, along with a very stringent account lockout policy combines to protect the organization from all but the most determined unauthorized account user.

The Default Domain Controller GPO, which is applied to all forests is almost entirely adopted from the NSA security template **W2KDC.INF** which is the template titled "NSA Enhanced Security for Windows 2000 Domain Controllers". The major change to the template is the requirement to enforce digital encryption of the secure channel and to require strong session key for the secure channel. Another minor change to the template is the message text and title for users attempting to log on (banner) is customized for Sans Co. / GIAC (Figure 9).

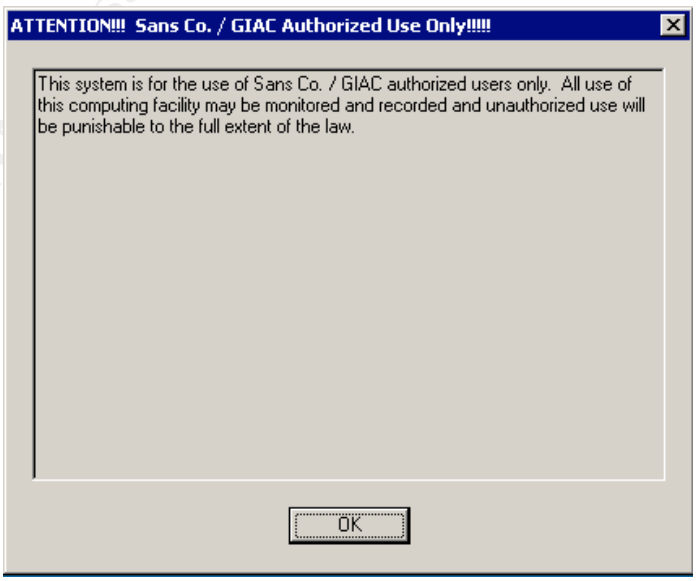

Figure 9 – Logon Text Banner

The Standard Servers and High Security Servers GPO's are based on the NSA security template **W2K_SERVER.INF** which is the template titled "NSA Enhanced Security for Windows 2000 Member/Stand-Alone Servers". The primary difference between the two is that the high security servers have the IP Security Policies on Active Directory set to Enable Policy on Secure Server to ensure secure communication with all clients. As well, the message text and title for users attempting to log on (banner) is customized for Sans Co. / GIAC. The Standard Servers GPO is applied to the Servers OU in the OPS domain while the High Security Servers GPO is applied to the Servers OU in the HR, RD, SANSCO.COM (DMZ) and GIACENTERPRISES.COM domains.

The IIS Servers GPO is applied to all IIS OU's and is based on Microsoft's **HISECWEB.INF** with the following exceptions:

- The Password and Account Lockout policies are left undefined as the default domain policy more than adequately addresses these items.

- The Event Log Settings are significantly enhanced by setting each log size to 4194240 kilobytes and retention setting for log files to be set to manual. The IIS server is also set to shutdown in the event that the security event log is full.

- The IP Security settings to encrypt all traffic between IIS servers and backend database servers. This is particularly important between IIS servers in DMZ 1 and database servers in DMZ 2.

- Disable options for "Web-Based Printing"

- File System permissions on IIS logs, Metabase Controls set for access to Administrators and System only

Both the Standard Computers and High Security Computer GPO's are based on the NSA Windows XP security template **WORKSTATION.INF** which is the template titled "NSA Enhanced Security for Windows XP Workstations". The primary difference between the two is that the high security computers have the IP Security Policies on Active Directory set to Enable Policy on Client which enables secure communications with servers that request it as is the case for specific servers in the RD, HR domains.

The high security mobile computer GPO is also based on the NSA Windows XP security template **WORKSTATION.INF** and is nearly identical to the high security computer GPO except that the use of offline files and the synchronization of such files are enabled as well as EFS configuration for all mobile computers. As well, significant file system permissions are applied to each computer to prevent users from writing files to any locations other than "Documents and Settings" and temporary folder locations.

The standard personnel GPO is a custom configured policy based on the operational and security requirements of Sans Co. / GIAC. The settings in this GPO are derived from "User Configuration" settings only and the "Computer Configuration" settings are disabled to improve user logon performance. The settings in this GPO are too numerous to detail individually but the following are listed to highlight the type of settings required for system integrity, security and user control:

- Disable user ability to change security and configuration options for Internet Explorer
- Disable user use of Task Scheduler
- Disable use of Windows Update
- Disable Active Desktop
- Disable access to the Control Panel
- Disable ability to Add / Remove Programs
- Disable user configuration of offline files
- Disable access and modification of LAN connection properties
- Disable user use of Registry Tools
- Disable user use of Task Manager
- Application of standard user logon scripts

The Administrator GPO is a custom configured policy based on the operational and security requirements for the performance of the Sans Co. / GIAC delegated IT administrator role. The top level "Enterprise Administrators" do not have a GPO applied to them through the Administrators OU in the SANSCO.NET root domain but the Administrator accounts in each of the sub domains (OPS, RD, HR) have the Administrator GPO applied to them. This enables "Enterprise Administrators" the ability to delegate specific tasks to the sub-domain administrators and to lock down the AD tools that they do use in day to day administration. Again, the settings in this GPO are too numerous to detail individually but the following are listed to highlight the type of settings required for system integrity, security and administrative user control:

- Enable the use of Task Scheduler
- Enable access to the Control Panel
- Enable ability to Add / Remove Programs

- Enable access and modification of LAN connection properties
- Enable administrator use of Registry Tools
- Enable administrator use of Task Manager
- Restrict use of Microsoft Management Console snap-ins to allow only the specific function tools delegated to sub-domain administrators
- Restrict administrative users from entering MMC author mode
- Application of Administrator logon scripts

It is important to note that all AD administrative changes are extensively audited and logged through the default domain controller GPO regardless of level of authority.

2.1 Application of Group Policy Objects

Group policies are applied to AD objects through the “Active Directory Sites and Services” and “Active Directory Users and Computers” MMC snap-ins. At each site, domain, or OU the group policy can be applied through the properties option. Group policies can be selected or created through the group policy interface (Figure 10) and be set to block policy inheritance from higher level GPO’s or conversely they can be set for no override by lower level GPO’s.

Sans Co. / GIAC computer group policies are set to automatically update every 90 minutes with a 30 minutes variance to ensure randomization of timing between computers. As with any change to the Sans Co. / GIAC environment, AD reconfiguration and group policy development is thoroughly tested in a non-production environment prior to implementation in the live production environment. Individual computers can be set to force immediate group policy updates with the use of the SECEDIT /refreshpolicy command. This is especially useful for testing the application of new group policy settings in a lab environment to perform quality assurance procedures on all group policy changes.

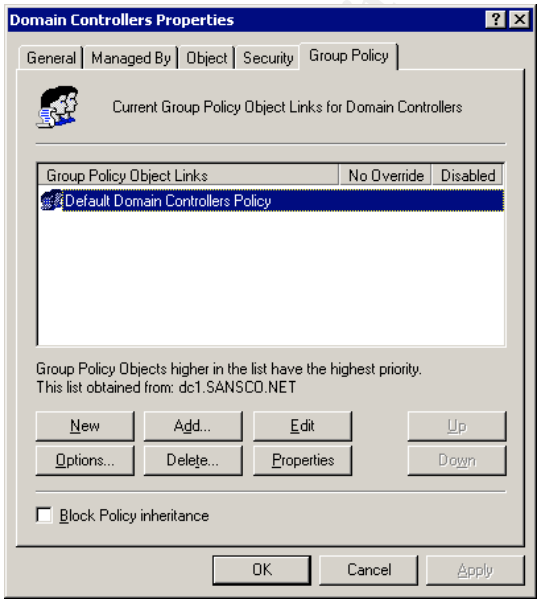

Figure 10 – Applying Group Policy

2.2 Testing Group Policy for Desired Functionality

Once all group policies were defined and applied in the Sans Co. / GIAC lab environment, they were tested to ensure system behavior was consistent with the desired results of the group policies. To demonstrate this, the lab version of the company's Intranet server (IIS1) was tested for operational acceptance. The Security Configuration and Analysis tool was used to ensure that the defined group policy settings were actually applied to the server. To do this the appropriate security template was selected for import into the tool and compared to the actual server settings (Figure 11).

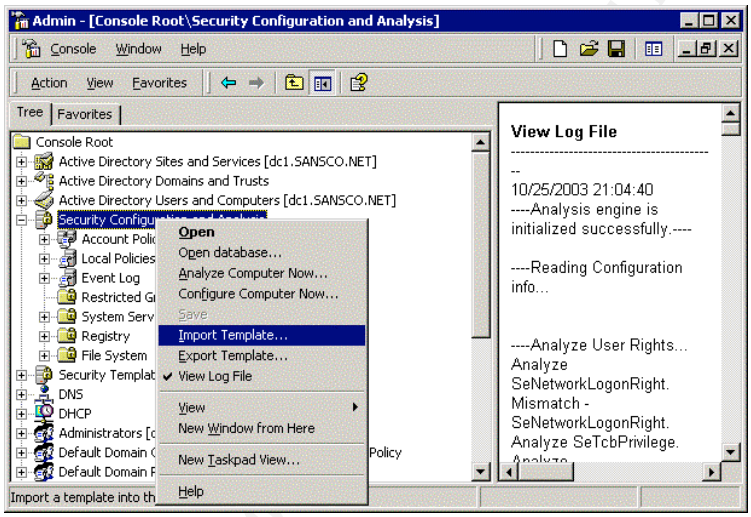

Figure 11 – The Security Configuration and Analysis Tool

It was confirmed that the server received and applied the GPO as shown by the relevant event log entry (Figure 12). Indications that the GPO is functioning as designed is evidenced by being able to browse the base Intranet page on server IIS1.SANSCO.NET (Figure 13) and observing the appropriate properties applied to the event logs of the IIS server (Figure 14).

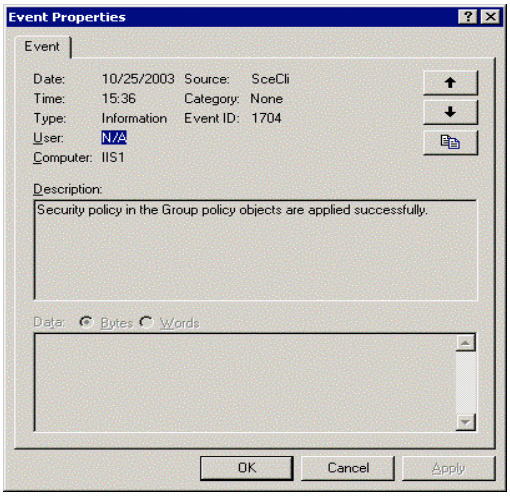

Figure 12 – Successful Application of Policy

Figure 13 – Sans Co. / GIAC Intranet Access

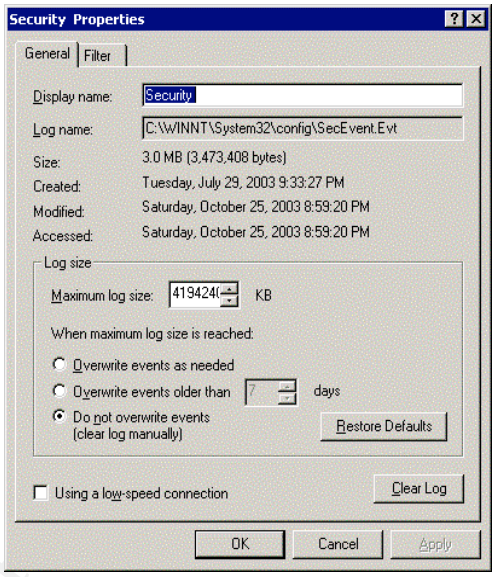

Figure 14 – IIS1 Event Log

Further indications that IP security settings within the GPO are operating correctly are the inability to PING, FTP or Telnet to the Intranet server IIS1 (Figure 15).

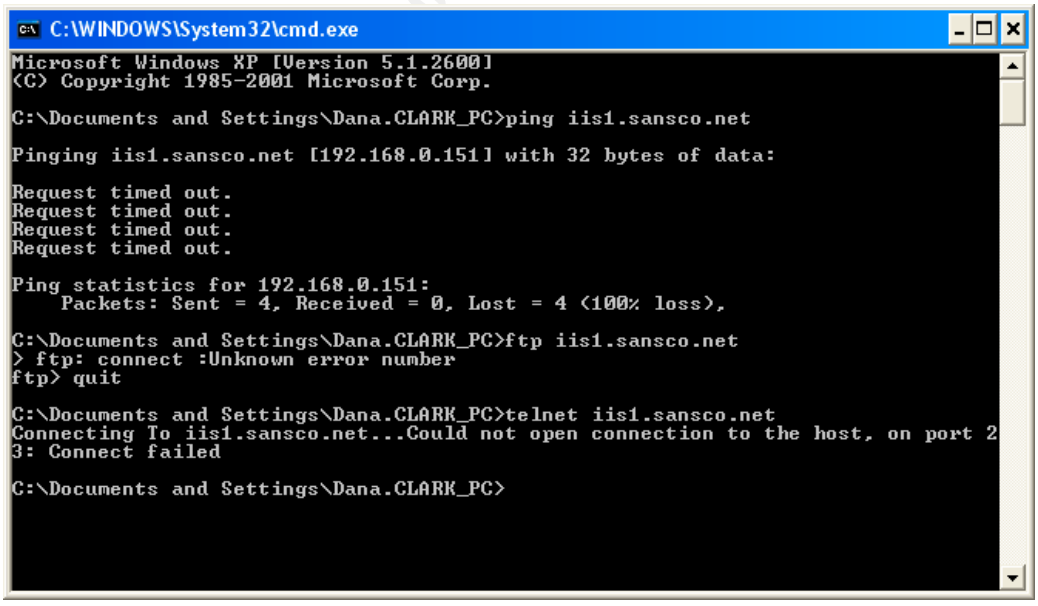

Figure 15 – GPO Blocked Traffic to IIS Server

2.3 Evaluation of the Sans Co. / GIAC Group Policy Implementation

The group policy design for Sans Co. / GIAC generally worked well when placed into operation with only a few exceptions. The decision to only apply GPO's at the domain and OU levels simplified application, testing, maintenance, and troubleshooting of policy issues. The operation of servers such as the Intranet server IIS1.SANSCO.NET continued unimpaired by the application of the group policy while at the same time enforcing desired security configurations included in the design of the group policies.

One area where the group policy had a negative impact was in the use of service accounts. Sans Co. / GIAC installed a new network monitoring system soon after the implementation of group policies. This new system relied on dedicated service accounts with non-expiring passwords to operate. As a result of the application of group policies, these accounts soon began to expire passwords according to the setting in the default domain policy which eventually led to the network monitoring system failing. To mitigate this issue it was decided to create another OU specific to services accounts and apply group policy to allow these accounts to continue running with no password expiration. To further mitigate security exposure that introduces, each account was configured to run only on the computers that required it.

3.0 Audit Plan for GIAC Enterprises / SANS Co.

The development and implementation of a functional, highly secure AD infrastructure is simply the first step in the management and operation of an AD based computing environment. In the natural evolution of system environments, change is the one constant that is guaranteed. In order to manage service delivery and change within the organization, while at the same time adhering to defined security policy and definitions, a comprehensive audit plan is required to ensure the proper checks are in place to maintain the security policy. Sans Co. / GIAC uses the ITIL[8] (IT Infrastructure Library) framework as its process basis for IT service management including change management and security management processes. A key component of the ITIL framework is the continuous assessment of security risk in all aspects of IT service delivery.

The audit plan for Sans Co. / GIAC Enterprises is comprised of three tiers:

- Tier 1 – System Configuration Confirmation: The process of ensuring all systems placed into production meet or exceed established configuration and security guidelines. This is primarily provided through the application of group policies and confirmed by procedural assessment prior to introduction of the system into the production environment.

- Tier 2 – System Operations Management: The process of monitoring and evaluating production systems for indications of unauthorized configuration change and early detection of attempts to compromise system security. This includes real time, scheduled and ad-hoc system assessment through the evaluation of system logs as well as full system evaluations and reporting to uncover anomalies affecting system integrity and security.

- Tier 3 – External Audit and Review: The process of engaging external professional audit firms to perform full system and procedural audits to ensure established controls and procedures are in place and being performed as designed.

3.1 Tier 1 Audit Activities

Tier 1 audits are primarily performed by dedicated information security personnel (Division of duties is important!) using the Security Configuration and Analysis tool available with Windows 2000. Identical group policies that will be applied in the production environment are applied in the test lab and an evaluation is performed to ensure the resultant group policy is in line with the policies previously defined and accepted by the organization. In addition, the Microsoft

[8] http://www.itil.co.uk

Baseline Security Analyzer[9] (MBSA) is used in conjunction with Microsoft's Software Update Service[10] (SUS) to evaluate each system to ensure that all approved service packs and hotfixes are applied.

3.2 Tier 2 Audit Activities

Tier 2 audit is the process of managing and responding to daily activities (including exceptions) within acceptable guidelines and norms. Sans Co. / GIAC utilizes Aelita Intrust and Enterprise Directory Reporter[11] to perform a number of very import security review operations in an automated manner. These products allow for consolidation and archival of all system event log files, IIS logs, database logs, Cisco network equipment and firewall logs. Rules are written to detect log file entries that would indicate system integrity issues, security configuration issues, and penetration attempts. When high priority log entries are detected, the system sends an urgent notification to information security personnel to investigate. Sans Co. / GIAC also uses custom visual basic scripts to perform auditing on servers. One script checks all server disks for suspicious files on a nightly basis and writes an event Log entry to the server if any are found. A second script checks each IIS server on an hourly basis for hacking attempts and writes an event log entry to the server as well as sending an urgent notification to information security personnel if any attempts are found. The custom visual basic scripts are scheduled for run on each server's task scheduler.

The Enterprise Directory Reporter also generates and sends weekly reports to information security personnel on the following items:

- Domain user accounts with administrator rights
  Lists all domain users with administrator or delegated administrator rights.
- Domain users with identical passwords
  A user with the same password indicates password sharing and presents the possibility of unauthorized access to resources.
- Unused user account report
  Stale accounts are a security risk if left enabled on the network. This report identifies stale accounts so system personnel can remove them.
- Disabled user account report
  Disabled accounts are often activated by accident and pose a security risk.
- AD object management report
  Lists all AD administrative activities including user accounts, domains, computers, local and global groups, devices, services, printers, shares, and user rights.

[9] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsahome.asp
[10] http://www.microsoft.com/windowsserversystem/sus/default.mspx
[11] http://www.aelita.com/products/default.htm

- Server services report
  Listing of all services installed on each server and the status of each.

The Microsoft Baseline Security Analyzer (MBSA) is also used in conjunction with the Software Update Service (SUS) to evaluate all servers to ensure that all approved service packs and hotfixes are applied. This evaluation is performed on a monthly basis by dedicated information security personnel.

As described earlier, Sans Co. / GIAC also uses network and host based Intrusion Detection Systems (IDS) to detect unauthorized traffic and access on SANS Co. networks and servers. All critical detections are passed to the network monitoring system and reported to information security personnel for investigation and action.

3.3 Tier 3 Audit Activities

Sans Co. / GIAC utilizes the services of industry recognized security audit professionals (third party consultants) to perform full system and procedural audits on a yearly basis. It is always good practice to have an independent review completed on system controls and procedures to ensure they are being performed and operated as designed.

The second aspect of the external audit review is to compare the results of the audit and benchmark them against industry standards and generally accepted "Best Practices" such as those published by the SANS Institute. The desired result is not only a detailed report on findings but also the generation of a "Gap Analysis" and recommendations report to assist Sans Co. / GIAC to work toward and attain "Best in Class" IT security operations across the enterprise.

References

National Institute of Standards and Technology. "Advanced Encryption Standard". December 4, 2001. http://csrc.nist.gov/CryptoToolkit/aes/

Brooke, Paul. "Building an In-Depth Defense". July 9, 2001. Network Computing Online. http://www.networkcomputing.com/1214/1214ws1.html

Microsoft Corporation. "HOW TO: Set up a One-Way Non-Transitive Trust in Windows 2000" June 4, 2003. Microsoft Knowledge Base Article – 309682. http://support.microsoft.com/default.aspx?scid=kb;en-us;309682

SANS Institute. "Securing Windows 2000 Step by Step". Version 1.5 July 1, 2001.

National Security Agency. "Security Recommendations". November 25, 2002. http://www.nsa.gov/snac/index.html

Microsoft Corporation. "Microsoft Solution for Securing Windows 2000 Server" Februrary 5, 2003. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/secwin2k/default.asp

Fossen, Jason. SANS Institute. "Track 5 – Securing Windows: Windows 2000 / XP Group Policy and DNS" June 8, 2002. Page 81

Office of Government Commerce. "IT Infrastructure Library" June 12, 2003. http://www.itil.co.uk

Microsoft Corporation. Microsoft Baseline Security Analyzer Product Information. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsahome.asp

Microsoft Corporation. Software Update Service Product Information http://www.microsoft.com/windowsserversystem/sus/default.mspx

Aelita Software. Intrust, Enterprise Directory Reporter Product Information http://www.aelita.com/products/default.htm