

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Benjamin J Schmitt
GIAC Certified Windows Security Administrator (GCWN) Practical Assignment
Version 3.2 (revised March 24th, 2003)

Assignment Option 1 – SANS Co/GIAC Enterprises AD Consolidation

Title: SANS/GIAC Enterprises Active Directory Merger – Design, Security Policy, and Auditing Practices

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of contents

Abstract....3
Introduction....4
SANS Co. Active Directory Network Design and Implementation....5
SANS Co. Network Topology....7
SANS Co. Forest Site Topology/Policy....7
GIAC Enterprises Active Directory Network Design and Implementation....10
GIAC Enterprises Network Topology (Previous Documentation)....11
GIAC Enterprises Network Topology (Current)....13
GASSANIC AD Integration Design....17
Customer Access to Company Resources....20
Creation of an Enterprise Intranet....22
Inter-forest authentication via Kerberos and a federated Forest trust....23
OU structure, reflecting business needs and security considerations.....24
Security Policy and Tutorial....26
GASSANIC Authentication Standard....27
Group Policy Application....31
Auditing....36
Appendix A – Event Log Harvest Tool....39
References:....42
"Introduction to Group Policy in Windows Server 2003: White Paper" 24 April 2003 URL:....43
"Administering Group Policy with the GPMC: White Paper" 7 April 2003 URL:...43

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Abstract

Microsoft Windows provides a managed, secure and extensible network infrastructure based on its Active Directory technology. Active Directory is the heart of a secure directory services infrastructure in Windows 2000/2003 operating systems. Active Directory (AD) is the replacement for the NT 4.0 SAM database located on NT 4.0 Domain Controllers. AD is the combined services, protocols and standards driven from a central database running on Windows server platforms.

Active Directory has made quantum leaps in the Microsoft network operating system offering since the release of Windows 2000. Active Directory has many new features, including integrated DNS, LDAP, Kerberos, IPSec, PKI, Group Policy as well as significant and powerful delegation of authority.

A new offering from Microsoft is Windows Server 2003, the most recent release and upgraded version of Active Directory. While Windows Server 2003 is an incremental upgrade from Windows 2000 server, significant improvements have been made. New benefits offered include support for inter-forest trusts, an Active Directory Migration Tool (ADMT), enhanced PKI features, IIS 6, improved system performance, Group Policy Management Console (GPMC), shadow copy restore, enhanced DFS and Enterprise UDDI Services.

This document will discuss the domain structures, security policy, group policy and auditing practices of the new company which has been formed. SANS and GIAC have merged into a new company, aptly named GASSANIC. The first section will highlight AD structures including physical and logical network topologies of both forests. The structure and its changes will be made to facilitate the creation of an Inter-forest trust, the effective solution to join the mature AD infrastructures of each company. The second section will cover the group policy design. This design will reflect business needs while implementing the necessary security for these networks. The third and final section will discuss auditing of the new network. Auditing will include, but is not limited to, Event Log correlation, performance data, anti virus data, group membership and checking of critical settings.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Introduction

This paper describes the Active Directory consolidation of SANS Co. and GIAC Enterprises, two major telecommunication providers in North America. In order to expand markets, consolidate operations and leverage current IT operations, the two companies will merge, most notably, each companies extensive Active Directory infrastructure.

SANS Co. is an ILEC (Incumbent Local Exchange Carrier) wire line Telecommunications provider. SANS Co. currently serves 29 states throughout the US and is comprised of brick-and-mortar Telcos located in primarily rural areas. As an ILEC, conservative business practices, stable access line growth, positive cash flow and a commitment to delighting customers have put a premium on customer service and a reliance on a stable and secure network. SANS Co. is a Windows 2000 Active Directory Integrated network with selective services utilizing Windows Server 2003. SANS Co. is headquartered in Langley (McLean) VA with a remote call center located Chicago, IL.

GIAC Enterprises is a Wireless Telecommunications provider serving more than 4 million customers in 25 states. GIAC Enterprises is an aggressive business capitalizing on the latest in wireless cellular technology. The company invests millions annually to update and enhance technology. The GIAC telephony network is currently under a monumental overhaul converting its current TDMA network to the latest in cellular technology, digital CDMA 1xRTT. GIAC Enterprises is a distributed company, headquartered in Fort Meade, Maryland with call centers in Roswell, NM, Boston, MA, Manitowoc, WI, Burbank, CA and Denver, CO. GIAC Enterprises is a Windows 2000 Active Directory Integrated network with advanced rollouts of Windows Server 2003.

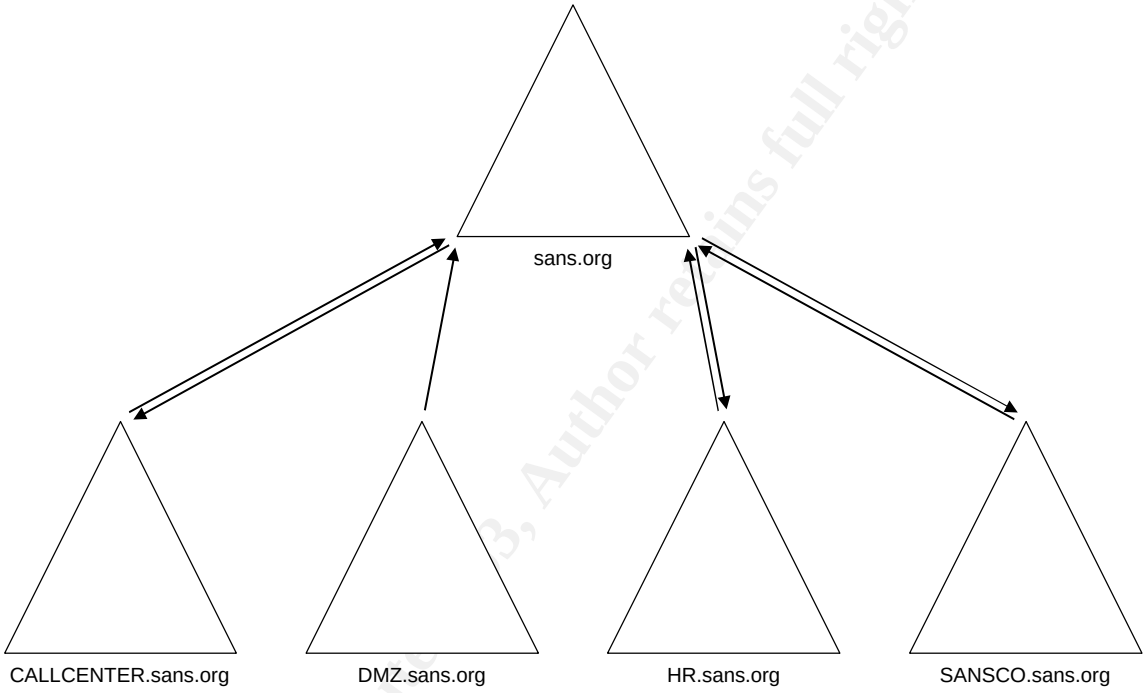
Current economic conditions, increased ROC targets, constrained IT budgets and increased competition have driven management to assess opportunities in the pursuit of “doing more with less”. This has resulted in the consolidation of the two companies in an effort to build synergy between business units. The new company is called GASSANIC and will rely heavily on the successful integration of both company’s established AD infrastructures. As AD infrastructures are to be integrated, corporate management has formed an Enterprise Governance Council (EGC) to strategically align the IT efforts of the new company through AD integration.

Inter-forest trusts are of particular interest to SANS Co. and GIAC Enterprises. Both corporations have established Active Directory infrastructures which make the migration of one forest into another an infeasible task. The goal is to develop trusts between the two companies to ensure interoperability, consolidate IT efforts and allow existing customers to access both parts of the new company via the Internet. This work will be driven, authorized and approved by the newly formed EGC.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

SANS Co. Active Directory Network Design and Implementation

The current AD design for SANS includes a single AD forest with four domains. The four domains are: CALLCENTER, a domain comprised of a remote call center located in Chicago, DMZ, a DMZ domain for SANS IIS web presence and bastion hosts, DEV, a development and test domain and HR, a highly secure domain dedicated to Human Resources. The SANS AD Forest layout and domains are shown below:



The current SANS forest is comprised of 1 root domain (sans.org) and 4 domains within it.

The CALLCENTER domain is a remote call center. This site is geographically located far from headquarters and the SANS ATM network. This connection is VPN-based requiring secure communications over the Internet. The CALLCENTER domain is comprised of the remote call center's users, computers, printers and an associated domain controller to reduce AD replication and help overcome bandwidth constraints. The CALLCENTER domain is connected to the internet via 1 SDSL connection, providing 1.5 MB of available bandwidth. The single SDSL connection provides exceptional performance over other Internet connections of similar capacity at a significant cost savings. Domain replication traffic will limited to a subset of the AD database; the global catalog.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The DMZ domain is a domain consisting of IIS 5 web servers, Exchange 2000 mail servers and Windows 2000 Terminal Servers. The IIS web servers provide the corporate web presence, customer portal, and externally-facing applications such as Outlook Web Access (OWA) and Terminal Services Web Client access. Exchange 2000 mail servers function as the corporate mail servers. Exchange, bundled with Outlook 2002 on corporate desktops allows for IMAP-based email on client workstations throughout the enterprise. Windows 2000 Terminal Services provides a wealth of functionality to remote users via RDP access to a terminal session. Applications delivered to the terminal server environment include Outlook, Internet Explorer (corporate intranet), Microsoft Office XP and user-profile related applications (Visual Studio, CRM, etc). This is a high security domain with bastion hosts, custom security templates and required secure communication.

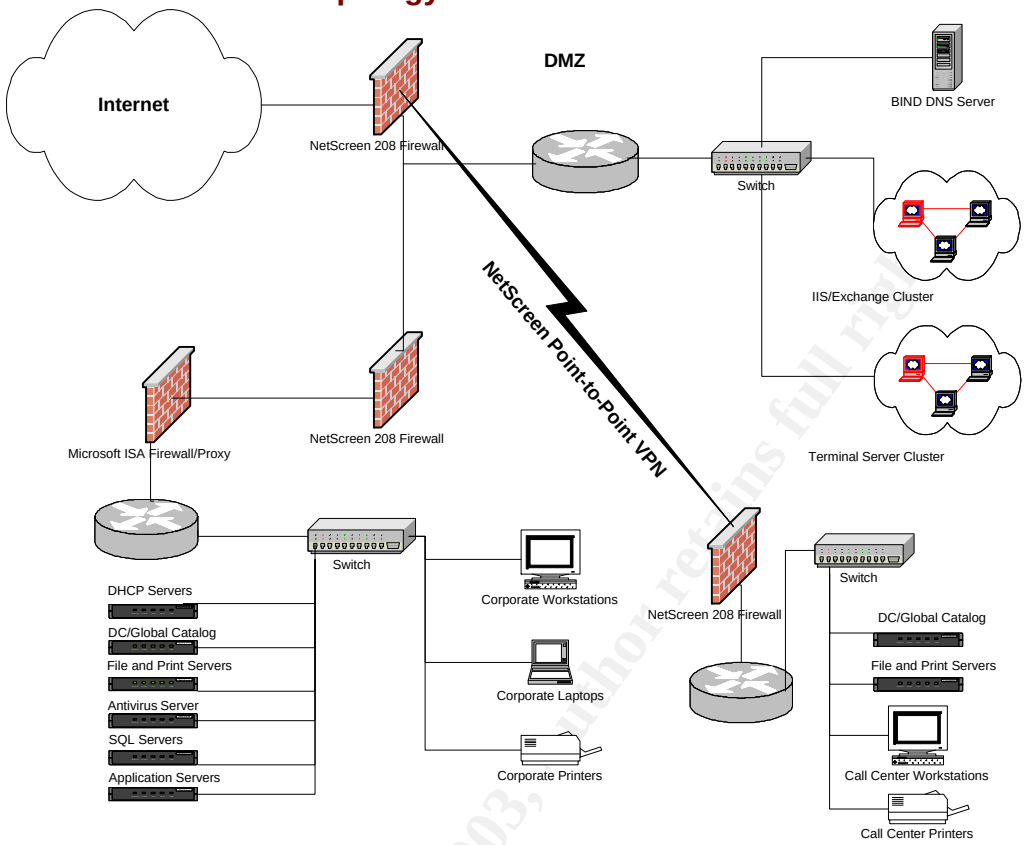
The HR domain is a high security domain for the Human Resources department at SANS. This domain consists of users, computers and resources related to the payroll, compensation, benefits, training, procurement and employee relations sub departments. This domain is highly managed, audited and secured. AD replication is secured, IPSec secures employee records databases, custom security templates are applied, EFS is used on workstation and laptop local storage and an enhanced authentication standard is required.

The SANSCO domain consists of SANS Co. users, computers, printers and AD components. The bulk of the SANS Co. users are members of the SANSCO domain (approximately 80%).

Internet Connectivity for the SANS Co. corporate network is via an OC-48 long-haul backbone fiber connection to its upstream provider, Cable and Wireless. This provides the necessary bandwidth to power the corporate web presence, email, VPN connection to the remote site as well as the Terminal Services cluster. Additionally, the connection is sized for growth as a future offering may include web hosting and ISP services. The connection between the remote call center and the corporate network is a single SDSL connection. This connection is capable of 1.5 MBPS and provides the necessary internet and AD site connectivity over a NetScreen point-to-point VPN.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

SANS Co. Network Topology



The SANS Co. domains are administered from its corporate headquarters in Langley, (McLean) VA. The root domain, sans.org, is a container domain which holds only those resources necessary to maintain and administer it. The current technical direction calls for a Single Forest – Empty Root model for SANS Co. This design supports future opportunities of collaboration between the potential new business units while allowing each business unit the flexibility to design, manage and support its own domain. The Empty Root is the core infrastructure that will facilitate the business units' ability to leverage its expertise and experiences while maintaining autonomy. This is a strategic direction for the Windows platform that provides the foundation for extensibility, management and growth.

SANS Co. Forest Site Topology/Policy

A site is a set of well connected (LAN speeds or greater) IP subnets. A site topology is created by identifying areas of high connectivity as a site and the WAN connection between the sites as a site link. Active Directory will automatically generate a replication topology between domain controllers in

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

different sites. By defining sites by the LAN/WAN topology, communication between domain controllers will avoid the WAN (VPN) link, when possible. This will be achieved by strategic placement of domain controllers to limit replication to global catalog traffic. The root forest site will be located centrally in Langley, VA and will act as a holder for the 4 sub domains which comprise the SANS Co.

The following security policies govern the use and administration of the root domain:

- The root domain will have no user or computer accounts except for those necessary to maintain the root domain itself. User and computer accounts are to be created in the SANS Co. sub domains within the empty root. User and computer accounts necessary to maintain the root domain will be approved by the SANS Co. IS Security Function and the EGC.

- Authority will be delegated to OUs and OU Administrators within AD. Only a select group (Critical support personnel) will be members of the Domain Administrators group. This group will be approved by the SANS Co. IS Security Function and the EGC.

- Permissions and auditing will be set on the Schema Administrators and Enterprise Administrators group. Scheduled scripts will check (every 5 minutes) for group members and alert the SANS Co. IS Security Function of changes.

- Physical security for core Domain Controllers is especially important due to AD multi-master replication. Domain Controllers (DCs) must be kept in locked, access-controlled rooms. DC access will be limited to Terminal Services rather than physical access.

- The RID Master and PDC emulator roles will be assigned to the same physical DC. This DC will be highly monitored as this machine is critical to AD. Host based IDS (Tripwire) will be installed on FSMO Masters.

The following security policies govern the use and administration of the CALLCENTER domain:

- Physical security to the pair of Domain Controllers is especially important due to AD multi-master replication. Domain Controllers (DCs) must be kept in locked, access-controlled rooms. DC access will be limited to Terminal Services rather than physical access.

- Authority will be delegated to the OU level for this remote site. A select group (remote staff approved and delegated the proper authorities) will

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

assist with CALLCENTER domain administration. Group membership will be approved by the SANS Co. IS Security Function.
- All traffic over the VPN will be encrypted. The latest NetScreen firewall units are capable of 256-bit hardware AES encryption. The point-to-point VPN will use preshared keys, managed by the EGC and require 128-bit AES encryption.

The following security policies govern the use and administration of the DMZ domain:

- The DMZ domain is a highly regulated and locked down domain for the segregation and maintenance of bastion hosts. The perimeter NetScreen firewall will only allow the following ports inbound: 53, 80,443 and 3389. This will limit inbound traffic to DNS, HTTP, HTTPS and Terminal Services (RDP).

- Require IPSec on all DMZ hosts and drop all TCP port 3389 packets which do not originate from the LAN. The exception to this rule will be an Administrative Terminal Server which is Internet accessible.

- The Terminal Server desktops will be highly locked down to non-privileged accounts.

- IDP will monitor the DMZ and notify the SANS Co. IS Security Function of alerts.

- Communication to other domains within the SANS Co. Forest will require IPSec.

The following security policies govern the use and administration of the HR domain:

- The HR domain is a highly security domain. Password complexity is enabled and maximized for all accounts in this domain.

- Communication to other domains within the SANS Co. Forest will require IPSec.

- Auditing of the HR domain is significantly more complex than other domains. Custom log correlation and reporting tools are used to routinely audit user activities.

The following security policies govern the use and administration of the SANSCO domain:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

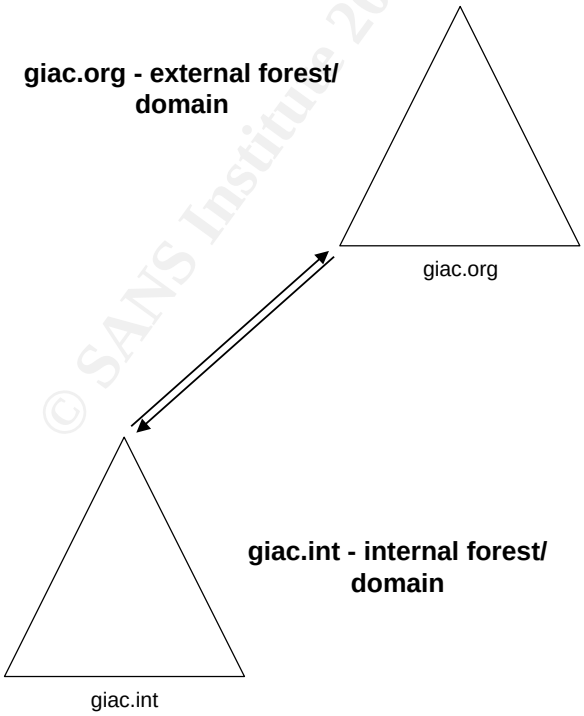
- The SANSCO domain is the largest domain in the sans.org forest. While concessions have been made to accommodate the productivity and flexibility of users, industry security best practices are still used. These details will be discussed further in the Group Policy and Tutorial section of this paper.

GIAC Enterprises Active Directory Network Design and Implementation

The current AD design for GIAC Enterprises is documented in a GIAC certification practical. It can be found at the following URL: http://www.giac.org//practical/GCWN/Erik_Weinmeister_GCWN.pdf

As GIAC Enterprises is a dynamic and changing corporation, additional sites have been added at the following locations: Boston, MA, Manitowoc, WI, Burbank, CA and Denver, CO. These sites are complete replicas of the Roswell, NM site, complete with workstations, network equipment and staffing.

The Active Directory design for GIAC Enterprises is for 2 forests, and single domain within each forest. Previous documentation lists 2 sites; this has since been updated to account for 6 sites, the 4 new sites mirror replicas of the Roswell, NM site. The GIAC Enterprises AD Forest layout and domains are shown below:



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The current GIAC Enterprises external forest is comprised of 1 domain (giac.org) as well as another internal forest with 1 domain within it as well. The giac.int is the internal domain for the GIAC Enterprises internal forest. GIAC.INT was chosen in an effort to not conflict with external naming standards. The important distinction is between domain and forest contents and purpose. The giac.com forest and domain combination is purely for external DNS and email/web presence. The members of this forest and domain combination are extremely limited. The giac.int internal forest/domain combination contains the users, computers and objects associated with the business workings of this wireless company. This paradigm can be considered an outershell of externally-facing services (external forest/domain) with a soft center comprised of the inner workings of giac (internal forest/domain).

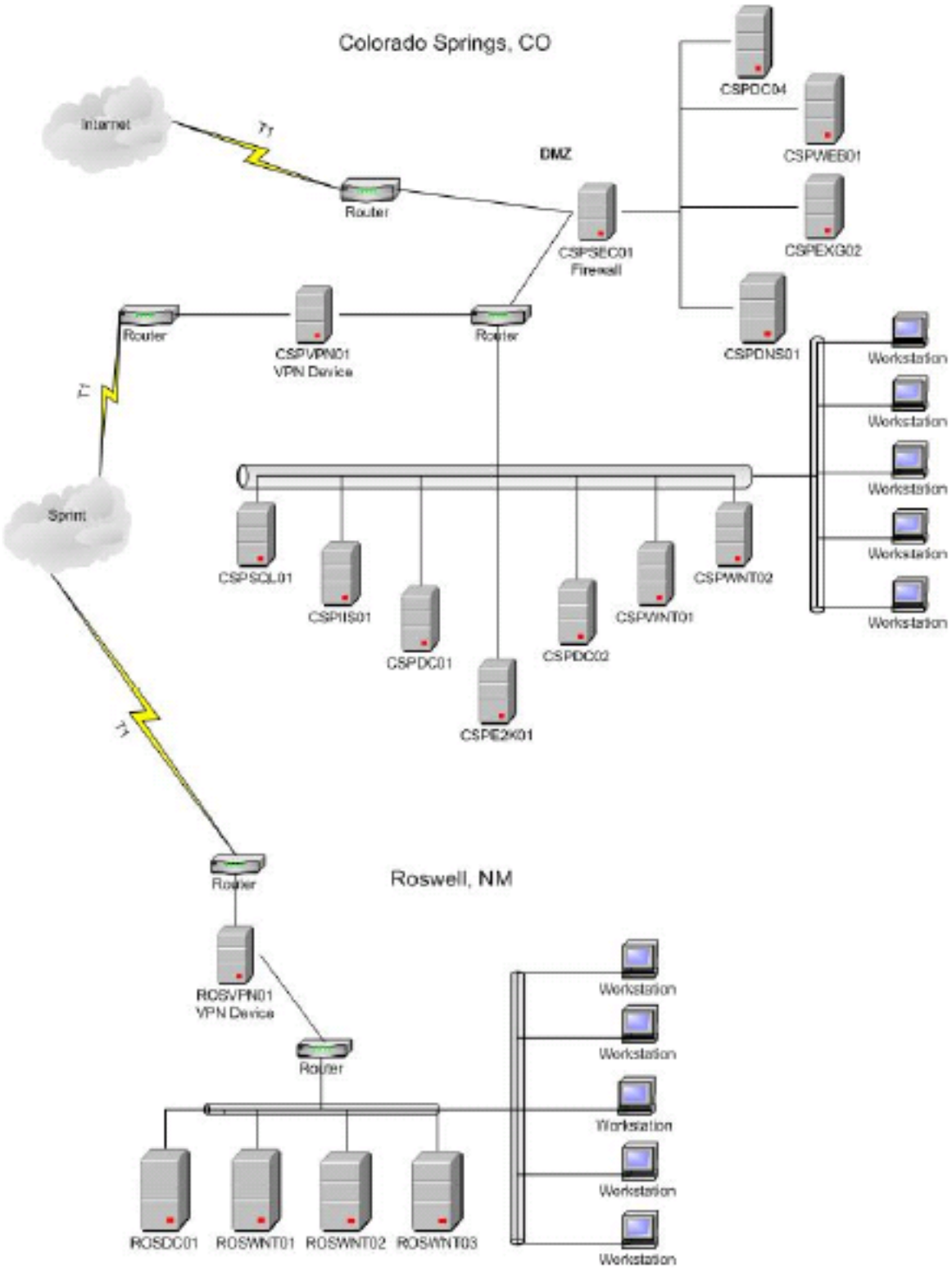
This single internal forest domain environment consists of 6 sites, each with exceptional connectivity. The sites are dictated by their respective geographic locations. The sites are, in no particular order: Colorado Springs, CO, Roswell, NM, Boston, MA, Manitowoc, WI, Burbank, CA and Denver, CO. Each site now has the same connectivity to each other as GIAC Enterprises has leveraged its telephony network to include data. Thus, all sites are connected via DS3 lines with an upstream Internet connection of OC48 provided by MCI WorldCom in Ford Meade.

GIAC Enterprises, being a fluid, dynamic and progressive organization has decided to leverage thin client technology via Citrix MetaFrame XP. Thus, the remote sites are merely geographic separations – the well connected sites, via their DS3 lines are simple separated by distance. The currently AD infrastructure of one domain is extended only by the addition of user accounts and resources to handle increased functionality.

GIAC Enterprises Network Topology (Previous Documentation)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



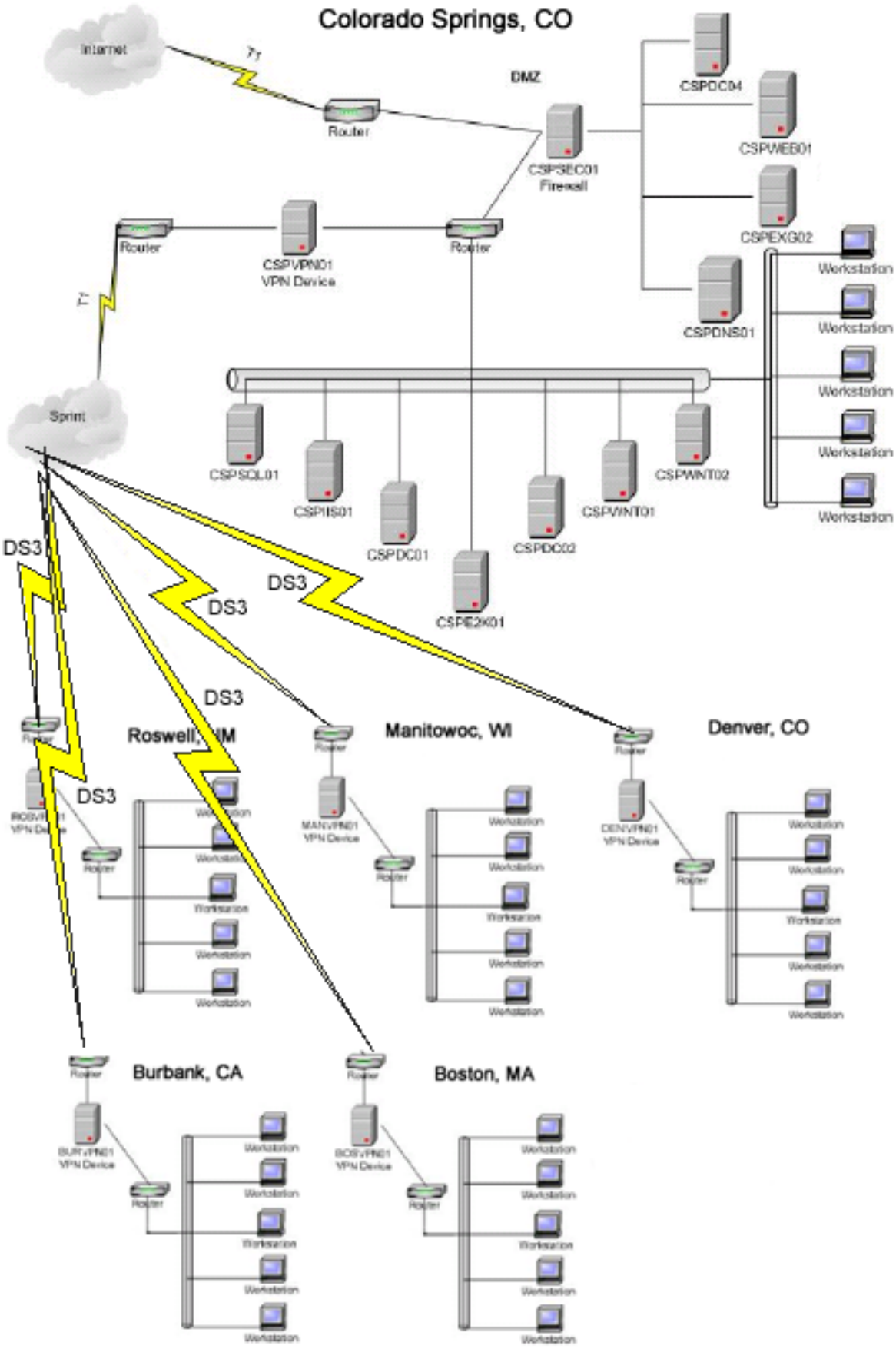
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The previous AD implementation of GIAC Enterprises accounted for 2 forests (external and internal) each with one domain but did not leverage Terminal Services and Citrix. As additional remote sites have been added to the internal forest/domain, this model has changed. The original model is shown below. It accounts for the same Colorado Springs, CO site with SQL Servers, Exchange, AD Domain Controllers, File and Print Servers, Web services and Anti Virus. However, it also accounts for a remote site without Terminal Services and Citrix and as a result, reflects additional domain controllers, file and print servers as well as a backup server. This can and will be reduced solely to the network infrastructure to provide the necessary protocols and connectivity to allow for a base, secure operating system (Windows XP) with central management from Colorado Springs via AD and Group Policy.

GIAC Enterprises Network Topology (Current)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

GIAC Enterprises Forest Site Topology/Policy

The GIAC.org root domain will consist of a pair of domain controllers and no trust will be established. The password policy will be changed to reflect the root domain policy of the SANS Co. root domain per EGC mandate. The root forest site will be located centrally in Fort Meade, MD and will act as a holder for its single sub domain which comprises only the externally facing components of GIAC Enterprises.

The following security policies govern the use and administration of the root domain within the GIAC.org forest:

- The root domain will have no user or computer accounts except for those necessary to maintain the root domain itself. User and computer accounts are to be created in sole sub domain within the empty root. User and computer accounts necessary to maintain the root domain will be approved by the GIAC Enterprises IS Security Function and the EGC.

- Authority will be delegated to OUs and OU Administrators within AD. Only a select group (Critical support personnel) will be members of the Domain Administrator group. This group will be approved by the GIAC Enterprises IS Security Function and the EGC.

- Permissions and auditing will be set on the Schema Administrators and Enterprise Administrators group. Scheduled scripts will check (every 5 minutes) for group members and alert the GIAC Enterprises IS Security Function of changes.

- Physical security for core Domain Controllers is especially important due to AD multi-master replication. Domain Controllers (DCs) must be kept in locked, access-controlled rooms. DC access will be limited to Terminal Services rather than physical access.

- The RID Master and PDC emulator roles will be assigned to the same physical DC. This DC will be highly monitored as this machine is critical to AD. Host based IDS (Tripwire) will be installed on FSMO Masters.

The following security policies govern the use and administration of the root domain within the GIAC.int internal forest:

- The internal domain will contain all user and computer accounts except for those necessary to maintain the root domain of the external forest.

- Authority will be delegated to OUs and OU Administrators within AD. Only a select group (Critical support personnel) will be members of the Domain

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Administrator group. This group will be approved by the GIAC Enterprises IS Security Function and the EGC.

- Permissions and auditing will be set on the Schema Administrators and Enterprise Administrators group. Scheduled scripts will check (every 5 minutes) for group members and alert the GIAC Enterprises IS Security Function of changes.

- Physical security for core Domain Controllers is especially important due to AD multi-master replication. Domain Controllers (DCs) must be kept in locked, access-controlled rooms. DC access will be limited to Terminal Services rather than physical access.

- Citrix is the main means of communication in this internal domain. Citrix client, server, and network security flow will together provide the security for this internal forest. Client workstations will be kept "thin" with a minimum OS installation with only those services running that are necessary to provide Citrix connectivity and AD management.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

GASSANIC AD Integration Design

As stated previously, AD infrastructures are to be integrated via the strategic direction of the new GASSANIC Corporation. Management support of this venture is provided via the Enterprise Governance Council (EGC) with the deliverable of Enterprise AD integration via a Transitive, Cross-Forest Kerberos Trust. This is a new feature in Windows Server 2003, thus, there will be a required upgrade to Windows Server 2003 prior to this new trust being put into place.

Simple external trust relationships will require extensive management and does not take advantage of new AD features. Additionally, authentication across forests will require trusts between every domain in one forest to every other domain in the other forest with no granularity of trust. Effectively, every user in the forest would need to be trusted or no users are to be trusted.

The goal is to federate the SANS Co. and GIAC Enterprises Active Directory forests with a single trust relationship which will enable near seamless authentication and authorization across both forests. This is to be achieved by using Selective Authentication, the ability to allow only specific users or groups to authenticate across the single, federated trust.

Given the nature of the new GASSANIC Corporation, its efforts both externally (customers) and internally (employees) need to be strategically aligned. The integration requirements are:

- Seamlessly provide customer access to resources from both companies via the Internet and Web Services

- Jointly market both wire line and wireless products to customers of the new GASSANIC Corporation. This effort will lead the development of marketing, product and customer service strategic support tools by teaming with internal and external partners to successfully achieve long term profitability, customer retention and growth.

- Allow for employee awareness, directory access, policies and procedures, time entry and expense reimbursement via an Enterprise Intranet.

- Require inter-forest authentication via Kerberos and the federated Forest trusts. This will be managed by Enterprise Administrators from both companies, driven and approved by the EGC.

- A uniform OU structure to reflect business needs while taking into account security considerations.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The process of implementing the AD Forest integration will a two phase effort and will require the collaborative efforts of both companies to achieve the end objectives listed above.

The first step will be to align Windows server platforms and perform upgrades to Windows Server 2003 and its corresponding DNS infrastructure across both enterprises. Windows 2000 does provide for External Forest trusts but lacks the following critical functionality:

- Support for Top Level Names
- DomainInfo for each domain
- Full Kerberos V5 Support (Critical for secure authentication and granular application of security controls across forest boundaries)
- Implicit and Explicit UPN (User Principal Name) logons.

Per the direction of the EGC, both companies have upgraded all AD domain controllers to Windows Server 2003. The companies DNS infrastructure also must be able to support this upgrade and changes will, at this point, not need to be made. There are 3 distinct requirements of Windows Server 2003 DNS which are accounted for in both companies AD infrastructures:

1. A network connection must exist on the server/servers which AD is being upgraded and is configured with a DNS server to query for domain names. Both companies currently meet this requirement. The SANS Co. network does relay on BIND servers in its DMZ for external DNS resolution, however, the BIND servers are merely forwarders for the internal Windows dynamic DNS. The BIND servers are aware of the internal Windows DNS and are aware that they are authoritative for sans.org, SANSCO.sans.org, DMZ.sans.org, HR.sans.org and CALLCENTER.sans.org names. GIAC Enterprises meets this requirement as it currently is 100% Windows dynamic DNS capable.
2. The verification of DNS resource records, specifically, the required service resource records (SRV) and matching address resource records (A). Both companies also meet this requirement and their records, gathered from nslookup on the appropriate DCs, are listed below:

SANS Co. DNS Resource Records

Role	SRV resource record
Forest Domain DC	_ldap._tcp.dc._mcdcs.*sans.org*
Child Domain DC	_ldap._tcp.dc._mcdcs.*sansco.sans.org*
Child Domain DC	_ldap._tcp.dc._mcdcs.*callcenter.sans.org*
Child Domain DC	_ldap._tcp.dc._mcdcs.*hr.sans.org*
Child Domain DC	_ldap._tcp.dc._mcdcs.dmz.*sans.org*

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

GIAC Enterprises DNS Resource Records

Role	SRV resource record
Forest Domain DC	_ldap._tcp.dc._mcdcs.*giac.org*
Forest Domain DC	_ldap._tcp.dc._mcdcs.*giac.int*

3. DNS must support dynamic updates and supports the service resource record (SRV). Both companies AD infrastructures currently support dynamic DNS for their appropriate and authoritative DNS zones.

The second step will be the creation and implementation of the federative, cross forest trust between each companies AD infrastructure to combine resources into the GASSANIC corporation. This trust will enable corporate synergy while maintaining reasonable security controls through Selective Authentication.

Prior to the creation and implementation of this trust, connectivity must be established to provide the transport mechanism of data between Forests. This connectivity requires a trust relationship be made within the GIAC Enterprise (internal to external with selective authentication). Given the established AD infrastructures and bandwidth requirements, a VPN connection between forests may not provide the necessary stability and throughput necessary to provide the feature rich needs of both enterprises. Large web services infrastructures, video conferencing over IP and possible VoIP technologies have made the EGC look at a leased/dedicated network solution.

Per many discussions, meetings and debates, the EGC and its technical networking contacts have decided to utilize an OC-48 Synchronous Optical NETwork (SONET) ring. The ring topology of the new GASSINAC SONET ring continually monitors service quality, detects any failure or degradation and automatically self-heals around a point of failure via a protect path to ensure uninterrupted transmission flow. Rerouting is accomplished within 50 milliseconds allowing for adherence to strict uptime requirements. This circuit is capable of meeting today's needs while providing the infrastructure to support voice, data and video transmission channels in one cost-effective, high-capacity channel.

The four objectives of this new trust, riding on top of its new SONET ring, along with its implications are listed and described below.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Customer Access to Company Resources via Web Services/ Marketing of joined products to customers of the new GASSANIC Corporation

SANS Co.

SANS Co. previously maintained its corporate web presence via the FDQN of http://www.sans.org. This corporate site provided the primary interface for SANS Co. customers. Its areas are focused on customer service by providing residential products and services, business products and services, account management, ISP portal (email, account statistics) and the latest in announcements and FAQ.

The www.sans.org website is a tiered application, consisting of IIS 5 web servers providing the presentation layers (HTML/XML), and SQL 2000 servers functioning as the backend database for this dynamic website. This technology is provided via ASP.NET and the Microsoft .NET Framework. As this is a dynamic website with a database backend, net features, links and content are easily added.

The sans.org website will leverage the new corporate synergy by providing GIAC Enterprises cellular technology to its current wire line customers. The current ASP.NET driven website will include GIAC Enterprises products in its offering by merging content via a replication schedule across forests. Once the forest trust is in place, database content will be refreshed daily so as to provide a dynamic means of GIAC Enterprises product offerings. Additionally, HTTP links will allow for specific details not replicated to be explained via the GIAC Enterprises website, www.giac.org.

GIAC Enterprises

GIAC Enterprises previously maintained its corporate web presence via the FQDN of http://www.giac.org in its external forest/domain. This corporate site provided the primary interface for GIAC Enterprise customers. The business model of GIAC Enterprises is customer focused but relies heavily on its ability to provide all customer service actions via the telephone and its corporate website. As such, the corporate website of GIAC Enterprises is housed by a third party, ASPMEBABY.com. This vendor performs the programming and maintains the infrastructure necessary to power GIAC's mission critical website. This is achieved via multiple independent connections to Tier 1 Internet access

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

providers to maintain and balance Internet traffic. Fully redundant OC-48 SONET Rings provide an uninterruptible telecommunication infrastructure.

The GIAC website is also powered by ASP.NET and Microsoft IIS5 servers. Current development work has touched on IIS6 but the core infrastructure is comprised of IIS5 servers running on Windows 2000 Advanced Server.

The backend of this large site is a large Sun Fire V880 server running Solaris 9 and Oracle 9i release 2. This decision was made so as to build a bulletproof or, in Oracle speak, "Unbreakable" website capable of immense network and processing load. Outstanding performance is delivered by the powerful Sun server featuring 8 UltraSPARC III processors; 64 GB of RAM and an attached DMX SAN for lightning fast disk I/O.

The decision not to utilize Microsoft SQL Server was made based on Oracle's price and cost benefit as the hidden losses of downtime and security overhead are mitigated through this outstanding database/operating stack.

The outsourcing of this giant task has allowed for a relaxed posture between GIAC forests (giac.org and giac.int), thus, allowing for an interforest-trust to be established within GIAC prior to the joining of the SANS.org AD forest. As the outer shell of GIAC contains merely the services (SMTP/DNS, etc) to provide external connectivity, selective authentication allows for this trust to limit internal GIAC communications to be externally resolved in an approved and secure manner.

Interoperability with the SANS Co. website is made through database replication between the SQL Server databases on the SANS Co. networks and the Oracle backend of the GIAC Enterprises website. Given the current lack of SANS Co. web expertise on this scale of complexity, size and management, this site will continue to be housed with ASPMEBABY.com with the future strategic direction of bringing this site in-house as additional corporate consolidation continues. Future developments also include a single corporate web presence. Until that time, the sans.org and giac.org domains will continue to highlight each company's corporate offerings and the offerings of its new partners via content and product offering synergy driven by database replication and linking. This is made possible by the inter-forest (GIAC-SANS) trust.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Creation of an Enterprise Intranet

The creation of the GASSANIC Corporation requires the collaborative effort of all business units in creating a central Intranet capable of delivering employee awareness, directory access, policies and procedures, time entry and expense reimbursement.

GIAC Enterprises does not currently utilize an extensive corporate intranet while SANS Co. does have the infrastructure to house this new corporate asset. The new Enterprise Intranet will be housed in the DMZ domain of the sans.org forest but will be accessible to all members of both forests via the newly created inter-forest trust.

Included materials for the new GASSANIC Corporation include the new employee handbook and its accompanying digital signature application for new employees, shared directory access for documents, the new web-based time entry application and the enterprise employee expense reimbursement application. These applications will also utilize ASP.NET and have ties into enterprise databases located on Microsoft SQL servers.

The intranet is integral to the success of the new GASSANIC Corporation merger. It will allow for the rapid dissemination of data, provide the latest company news and help to facilitate a shared knowledge base of new corporate procedures and changes.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Inter-forest authentication via Kerberos and a federated Forest trust

The joining of multiple forests in different corporations is a challenging feat given resource management and connectivity between sites. These possible roadblocks have been removed by the EGC by two very important Enterprise decisions.

Precise and accurate resource management is paramount to sound security practice across forests. The EGC has been created to help facilitate alignment across both company forests by the creation of a new enterprise security policy and oversight committee to approve and guide decisions within the new GASSANIC Corporation. These security policies and their applications will be discussed further in this paper.

Connectivity between sites is another barrier that was broken with the help of the EGC with the implementation of the sizeable SONET ring now joining the two networks. This negates the need for firewall configuration and rule set to allow for Netlogon, RPC Endpointmapper, Kerberos Authentication (inbound/outbound), Inbound and Outbound DACL lookups.

The new federated forest trust has been created and utilizes Selective Authentication. Thus, the authentications that occur across the trust do not work automatically. Administrators must enable authentication explicitly in conjunction with the appropriate DACLs. This process is required by both forest administrators for proper authentication to occur. Selective Authentication will be discussed further in this paper.

© SANS Institute 2003, Author retains full rights.

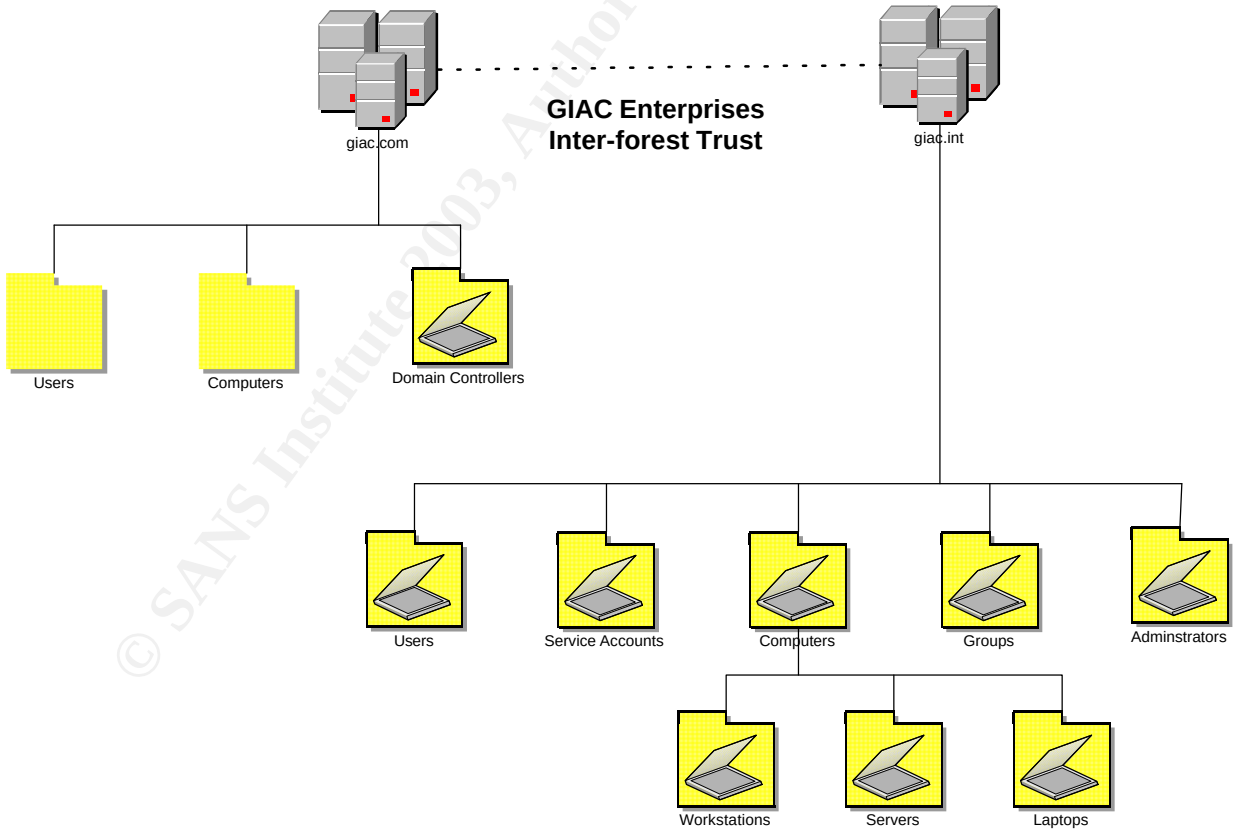
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

OU structure, reflecting business needs and security considerations.

An OU structure plan generally follows a business organization structure but should follow these guidelines in its creation:

- OUs are created to delegate administration.
- OUs are created to hide objects.
- OUs are created for the application of Group Policy.
- OU structures are created to minimize impact of change after deployment.

Given the structure of the new GASSANIC Corporation, the EGC along with the appropriate experts of the GASSANIC IS Security Function personnel have constructed the following OU structures, based on current and future Enterprise business and administration needs. The GIAC Enterprises OU structure is as follows:

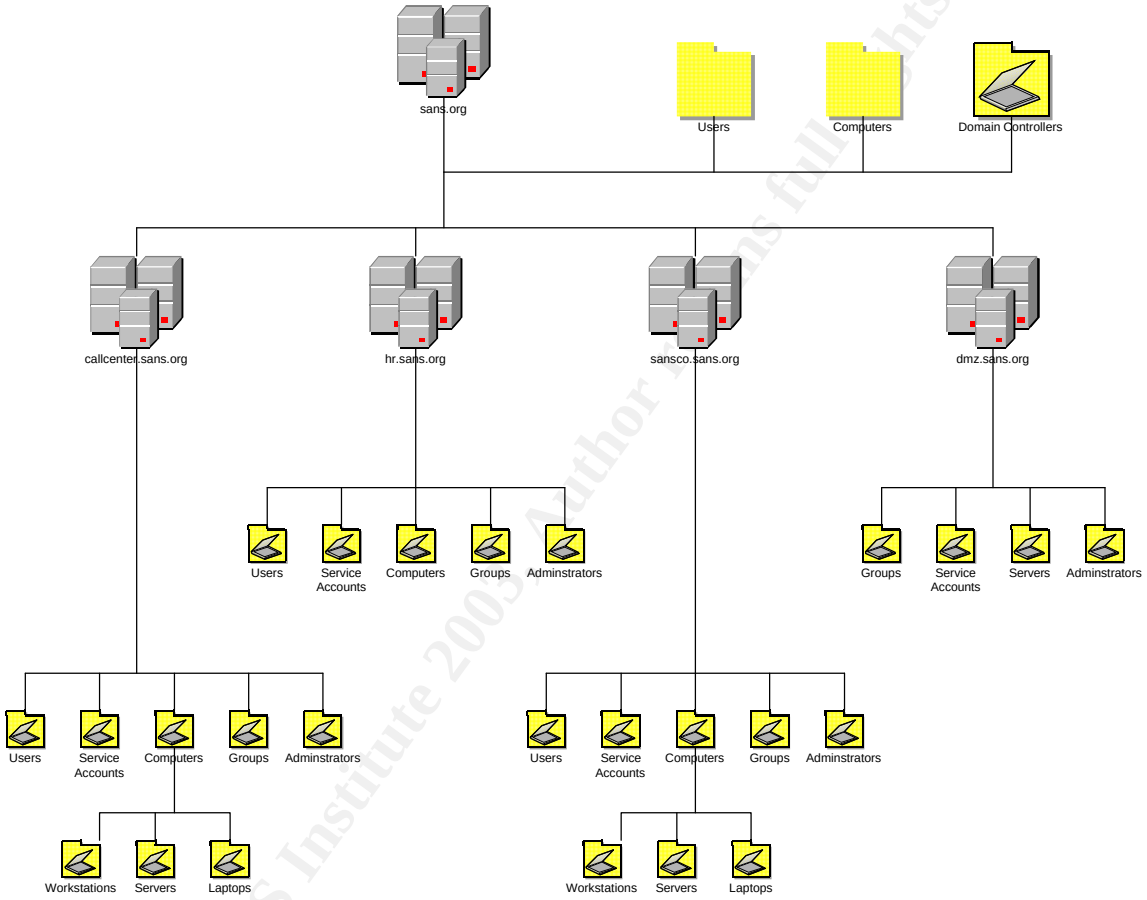


© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

This OU structure allows for both administrative delegation based upon sub domain administrators and service account OUs as well as accounts for Group Policy application.

The SANS Co. OU structure is as follows:



This OU structure allows for both administrative delegation based upon sub domain administrators and service account OUs as well as accounts for Group Policy application and site-based/domain-based segregation.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Security Policy and Tutorial

A sound AD infrastructure requires the utilization of Group Policy and Security Templates throughout the Enterprise. Given the established AD infrastructures and device disparity, an Enterprise-wide application of Group Policy and Custom Security Templates will help to ensure conformity to company security policy, mitigate risk and keep the network safe.

The EGC has identified that Forest Group Policy must have congruence among the 2 joined Forests and their respective trusted forests. The introduction of the inter-forest trust has effectively joined the networks. While the networks now share authentication, resources and interoperability, they also share the same vulnerabilities. The Security Policy for the GASSINAC Corporation has taken into account the separate AD forests and will serve to align the security efforts in a directionally correct manner. The policy, outlined below, will apply to both forests with exceptions to the policy made only by the EGC.

The Forests must implement a sound authentication policy as the basis of the inter-forest trust is Kerberos authentication via Selective Authorization.

Authentication is the process used to identify a user before allowing access to a system. This standard applies to all multiple user systems or devices used at the GASSANIC Corporation. New systems, major revisions of existing systems and AD must use this standard as a template for implementing a system authentication process.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

GASSANIC Authentication Standard	
Password Encryption:	Strong encryption of passwords is required while password is stored or transmitted is required. Kerberos, NTLMv2 and 3DES, will be utilized along with proper Syskey configuration in the joined Forests.
Password Caching:	Passwords are to reside only in the password database. Authentication credentials, user IDs and passwords are not to be cached by any system for use for future login, after logout. Kerberos, with properly configured ticket parameters, will negate the caching of passwords.
Centralized authentication	Centralized authentication will be used via AD. These systems will employ replicated databases.
Authentication Server Fault Tolerance:	AD's Multi-Master configuration and server RAID configurations will allow for a reasonable amount of fault tolerance and redundancy to ensure that the function of authorization remains available throughout both forests.
Automated user authentication:	When automated user authentication is necessary, a service account from the proper OU and group must be used and should not be associated with any special or privileged authorities.
Failure response:	Authentication systems shall employ fail-closed type processing.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The application of these settings is best suited for Group Policy distribution of Security Templates. Security Templates are the combined knowledge and settings of the following policies:

- Password Policy
- Account Lockout Policy
- Kerberos Policy
- Audit Policy
- User Rights Assignment
- Security Options
- Event Log Settings
- Restricted Groups
- System Services
- Registry Key Permissions
- File System Permissions

Security Templates are ASCII text files with an associated .INF extension. They can be easily edited using any text editor or via an MMC span-in named "Security Templates". The beauty of Security Templates is not only to easily enforce a consistent set of security options but to also provide for an effective auditing against this template. This will be discussed further in the Auditing section of this paper.

The combined effort of the GASSANIC IS Security Function personnel as well as the EGC has created customizes security templates based on the following devices:

- AD Domain Controllers
- Member Servers
- IIS Web servers
- Mobile Devices
- Default Workstation
- Highly Secure Workstation/Server
- Secure Terminal Server

The IIS Web Server template will be highlighted but not included in this paper. The IIS Web Server INF file is well over 17 pages in length.

Group Policy is not limited to Security Templates as it can also provide for many other management facilities. Group Policy allows for registry manipulation, application distribution, script assignment, IPSec and PKI settings, profile

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

management, Internet Explorer and RIS options. Additionally, Windows Server 2003 provides many new enhancements to Group Policy. New features include:

Group Policy Management Console (GPMC)	The GPMC MMC snap-in provides a central and unified view of GPOs, sites, domains, and OUs across an enterprise. It allows for reporting, Resultant Set of Policy (RSoP), backup and restore options for GPOs, enhanced User Interface in the Group Policy Object Editor, scriptable interfaces and support for cross-forest trusts.
WMI Filters	WMI Filtering provides additional granularity and what-if analysis of selected GPO targets.
New Group Policy Settings	Over 200 new policy settings are provided

The implementation of Group Policy is predicated by the creation of GPOs and the target OUs, sites and domains.

Per direction of the EGC, Group Policy will be applied at a base domain level with specific domain policy layered for a resultant set of policies based upon domain function.

Default Domain GPO (to be applied to all domains within both forests) consists of the following:

-Account Policies > Password Policy > Maximum Password Age: 90 days
-Account Policies > Password Policy > Minimum Password Age: 1 day
-Account Policies > Password Policy > Minimum Password Length: 8 characters
-Account Policies > Password Policy > Password history: 12 passwords remembered
-Password Policy > Password Must Meet Complexity Requirements
-Limit Local Accounts With Blank Passwords To Console Logons Only: Enabled
-Account Lockout Policy > Account Lockout Threshold: 5 attempts
-Account Lockout Policy > Account Lockout Duration: 15 hours
-Account Lockout Policy > Reset Account Lockout: 15 minutes
-Display A Logon Banner With A Legal Notice: Enabled, Corporate legal personnel to create
-Require Screensavers With Passwords
-Additional Restrictions For Anonymous Connections: Do not allow enumeration of SAM accounts and shares
-Network Access: Allow Anonymous SID/Name Translation: Disabled
-Audit Account Logon Events (Success, Failure)
-Audit Account Management (Success, Failure)
-Audit Directory Service Access (Success, Failure)
-Audit Logon Events (Success, Failure)
-Audit Object Access (Failure)
-Audit Policy Change (Success, Failure)
-Audit Privilege Use (Failure)
-Audit Process Tracking (Not Defined)
-Audit System Events (Success, Failure)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

-Event Log > Log Size: 500 MB
-Event Log > Wrapping Options: Overwrite Events Older Than 200 Days

Group Policy will also help to secure other unique areas of the joined forests by application to the following GPOs: hr.sans.org and dmz.sans.org.

The HR GPO consists of the default domain GPO settings and Highly Secure Workstation/Server Security Template as well as the following:

-Account Policies > Password Policy > Minimum Password Length: 16 characters
-Account Policies > Password Policy > Password history: 24 passwords remembered
-Account Lockout Policy > Account Lockout Duration: 200 hours
-Account Lockout Policy > Reset Account Lockout: 180 minutes
-Domain Member: Digitally encrypt or sign secure channel data (always): Enabled
-Domain Member: Require strong session key: Enabled
-Public Key Policies > Secure Server (Require Security): Policy Assigned

- The DMZ GPO consists of the default domain GPO settings, the Highly Secure Workstation/Server Security Template and the IIS Web Server Template as well as the following:

-Account Policies > Password Policy > Minimum Password Length: 10 characters
-Account Policies > Password Policy > Password history: 24 passwords remembered
-Account Lockout Policy > Account Lockout Duration: 200 hours
-Account Lockout Policy > Reset Account Lockout: 180 minutes
-Domain Member: Digitally encrypt or sign secure channel data (always): Enabled
-Domain Member: Require strong session key: Enabled
-Public Key Policies > Secure Server (Require Security): Policy Assigned
-IPSec Filters > IPSec filters the following ports: 21, 23 and 25

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Group Policy Application

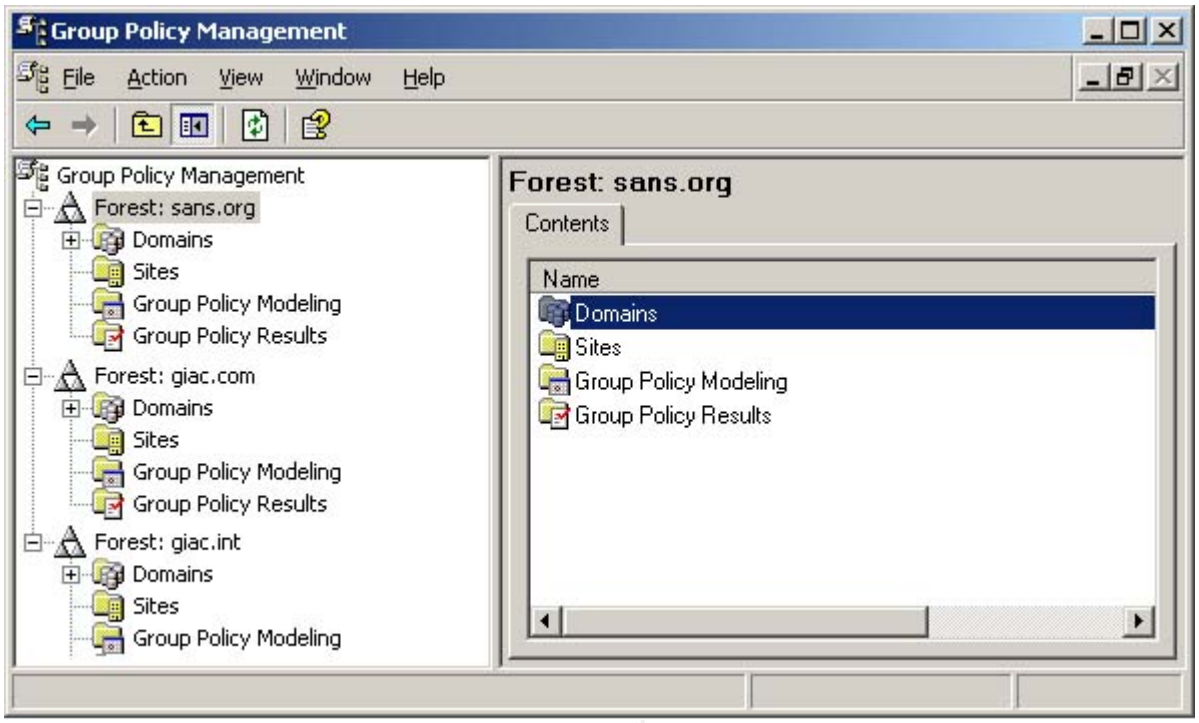
These Group Policies will need to be applied in both forests to provide a uniform level of security settings across the new GASSANIC enterprise. The recent upgrade to a pure Windows 2003 AD infrastructure has provided the capability of enhanced group policy application through the new Microsoft Group Policy Management Console (GPMC). This new tool provides a new UI, backup and restoration of Group Policy, Import/Export and copy/paste capability of GPOs, simplified management of Group Policy Security, reporting, Resultant Set of Policy (RSoP) and new scripting capabilities. The GASSANIC Corporation will focus on the management of multiple forests and the new scripting capabilities.

The new Group Policy settings, as outlined above, have been approved by the EGC and management/application of these settings will occur on both forests. As the SANS Co. forest is currently managing a more complex AD infrastructure, the management of both forests GPOs will be performed by the proper, authorized administrators located in SANS Co. Forest. This will be enabled via Selective Authentication across forests.

The GPMC is the frontline tool for the GASSANIC Corporation's Group Policy application in the new Enterprise network. The new inter-forest trust allows for Selective Authentication of Enterprise Administrators (with proper permissions/DACLS) to manage the Group Policy of both forests.

© SANS Institute 2003, Author retains full rights.

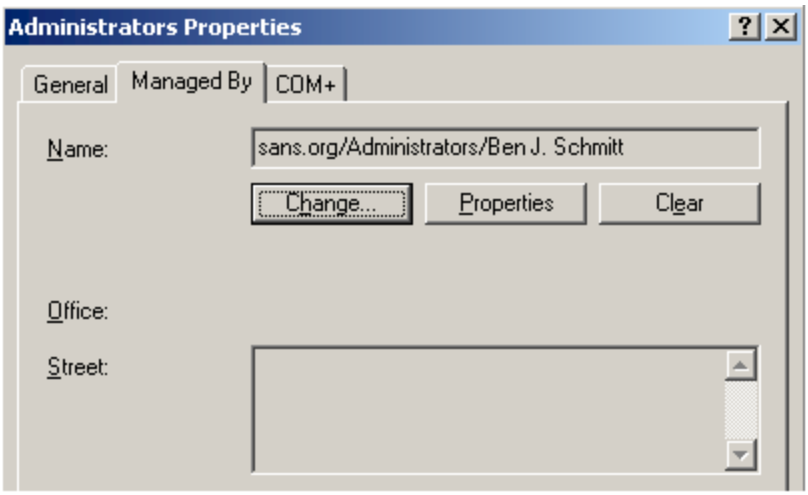
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



The sans.org, giac.org giac.int forests will be joined as they have a currently have a two way trusts between forests. However, the GPMC can be used with one-way trusts as well as forests with no trusts.

The GPMC uses a domain controller connection specific to the target domain. This includes all OU, GPOs, security principals and WMI filters. The GPMC requires that a domain controller be chosen for operations to be performed for all sites in a forest, or in the case of the GASSANIC Corporation, both forests. Within each domain controller connection, the GPMC will provide a view similar to the Active Directory Users and Computers MMC snap-in, including a policy-based view of Active Directory and its associated Group Policy components. This view can effectively associate and implement Group Policy settings across both forests including GPO creation and scope, linking GPOs, Security Filtering, WMI Filters, Inheritance, delegation, reporting. The Group Policy actions performed are by the Enterprise Administrator, Ben Schmitt.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

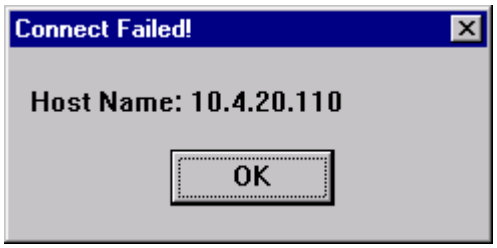


Testing of an IIS server and the application of Group Policy is a sound exercise given the heavy reliance on web services during this corporate merger. A web server in the dmz.sans.org domain will serve as the test subject. As discussed earlier, the DMZ GPO consists of all default domain GPO settings, the Highly Secure Workstation/Server Security Template and the IIS Web Server Template as well as increased password, lockout, domain membership and public key settings. These new settings, approved by the EGC, will first be "tested" via the Group Policy Modeling Wizard. This will help to determine the impact of the Group Policy application by the findings of the resultant set of policy. The process identifies the target device, policy settings for user or computer information, possible simulation for slow network connections, changes to security group membership, WMI Filters for users and computers. The result is a HTML report with a wealth of computer and user configuration information. This information, bundled with extensive testing will allow for successful application of security settings while not interfering with general business process.

The DMZ GPO is selected via the GPMC and the target domain of DMZ.sans.org is selected. For the initial test, only the SANSWEB001.dmz.sans.org IIS server is selected as this is a test and development server with a default install of Windows Server 2003 with IIS 6. It currently is configured with the "out of the box" IIS Security Template and the default domain policy. For testing purposes, the setting chosen is SMTP. SMTP services are installed on the SANSWEB001.dmz.sans.org IIS server and enabled, listening on port 25, IP address of 10.4.20.110. A telnet to port 25 was

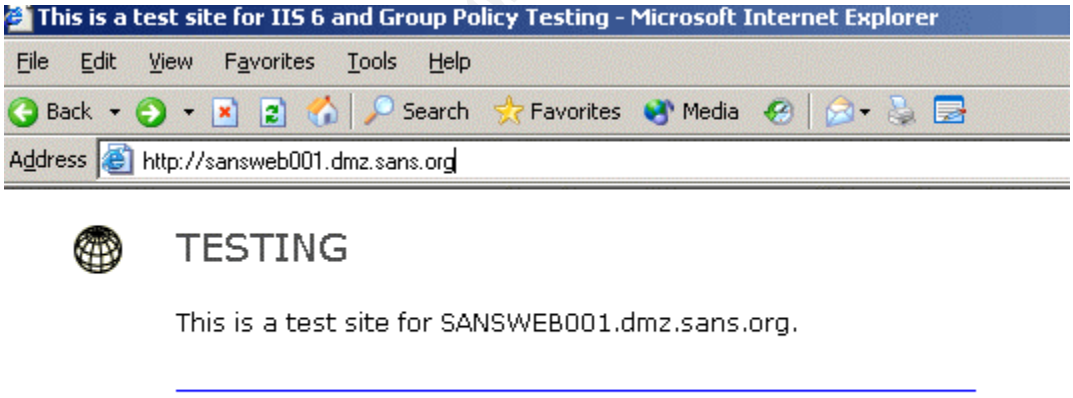
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

initially successful, however after the application of Group Policy, the server did not respond on that port:



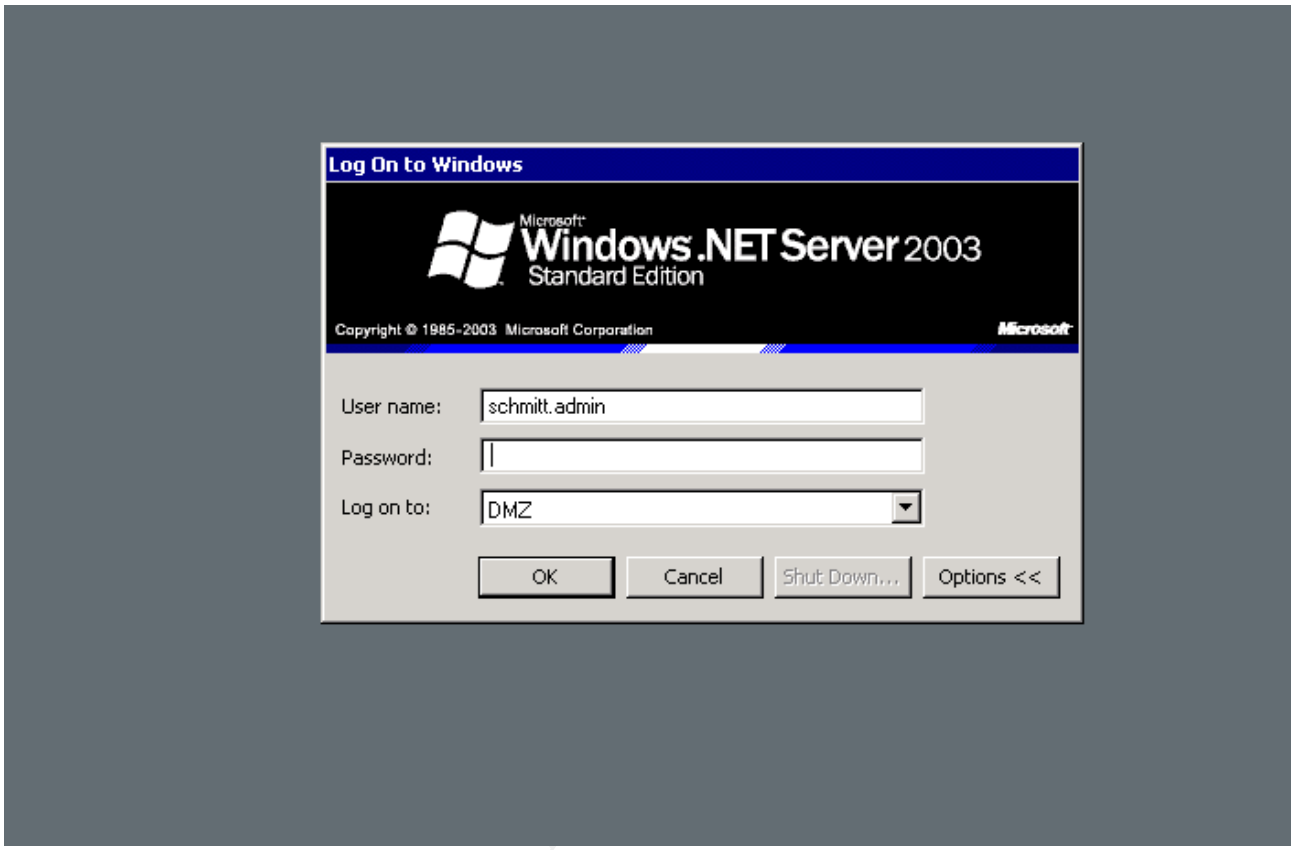
The goal of Group Policy application is to secure the target device while allowing for successful functionality. IIS is a core means of functionality to the GASSANIC Corporation. Two tests will be performed to certify that core functionality is not lost since Group Policy application.

The default web services scripting language is ASP (Active Server Pages). Prior to Group Policy application, web files with an .asp extension were mapped to the ASP parser and executed on the server end to produce dynamic web content. A simple test.asp page was created to ensure ASP execution and file association was not lost. The test page was put into the main site's root and it successfully executed prior to the application of Group Policy. The strict Group Policy for this server was applied. A web session via Internet Explorer was initiated and the default website viewed. The output of this simple test page was successful and is listed below:



Another core function of the web servers is Terminal Services access. The IIS servers are located in a DMZ with a one-way trust. Ports are filtered as this is a highly secure environment. Consequently, Terminal Services and RDP file transfer are critical to the IIS infrastructure. Prior to the application of Group Policy, Terminal Server access was successful. Subsequent to the Group Policy Application, Terminal Services was again initiated and was successful. The results of this test are shown below:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Overall Group Policy evaluation was successful – this did not come as a surprise. Extensive testing and user of the Resultant Set of Policy tool demonstrated the effects of security template and Group Policy application. The templates used were tested extensively via local template application on IIS6 beta copies of Windows Server 2003. These templates were perfected and honed to provide the specific security functions given the web infrastructure.

The Group Policy application on a Forest-wide level did not go without event as the HR domain did encounter challenges. IPSec no longer worked in the secure database application which houses sensitive employee relations data. After the policy application, it was realized that the IPSec policies were no longer applied and needed reapplication. These settings have now been reintegrated into the HR domain Group Policy set and are also audited to ensure secure communications. Additionally, the password length requirement of 16 characters proved to be too difficult given the password complexity requirements. This setting was reduced to 10 characters to accommodate the user's needs.

The application distribution mechanism, SMS, also encountered some problems after the application. SMS 2.0 is driven by many service accounts. Unfortunately, these service accounts are extremely difficult to change given their extensive use within the SMS infrastructure. These accounts are necessary and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

given the extreme workload required to change them to adhere to the password change policy of 90 days; these accounts were added to another OU and are set to be changed every 360 days. This is in the hope that SMS 2003 can be integrated into the network prior to that expiration date. Additionally, risk was mitigated by requiring 16 character passwords which also meet the password complexity requirements.

© SANS Institute 2003, Author retains full rights.

Auditing

Auditing of the new GASSANIC Corporation is paramount to the long term monitoring, maintenance and health of the new Forest trust. Enterprise Security posture must not be sacrificed by the modification or introduction of changes which may compromise security. The EGC has tasked the GASSANIC IS Security Functions with performing routing audits to ensure uniform and consistent security throughout the new Enterprise network.

The Enterprise Audit plan, from a high level, will cover industry best practices in the collection, retention, interpretation and corrective action execution of this plan. The plan will include:

- Event Log retention, access, correlation and review
- Naming Conventions
- Password Resets, lockouts and expirations
- UserID creation
- Antivirus
- Privileged Account use
- File, directory, share and registry permissions
- The use of trust relationships

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Security Patches/Hot fixes
- Remote Access
- Change Management
- IDS/IDP reports
- Malware/Spyware installation
- AD database changes

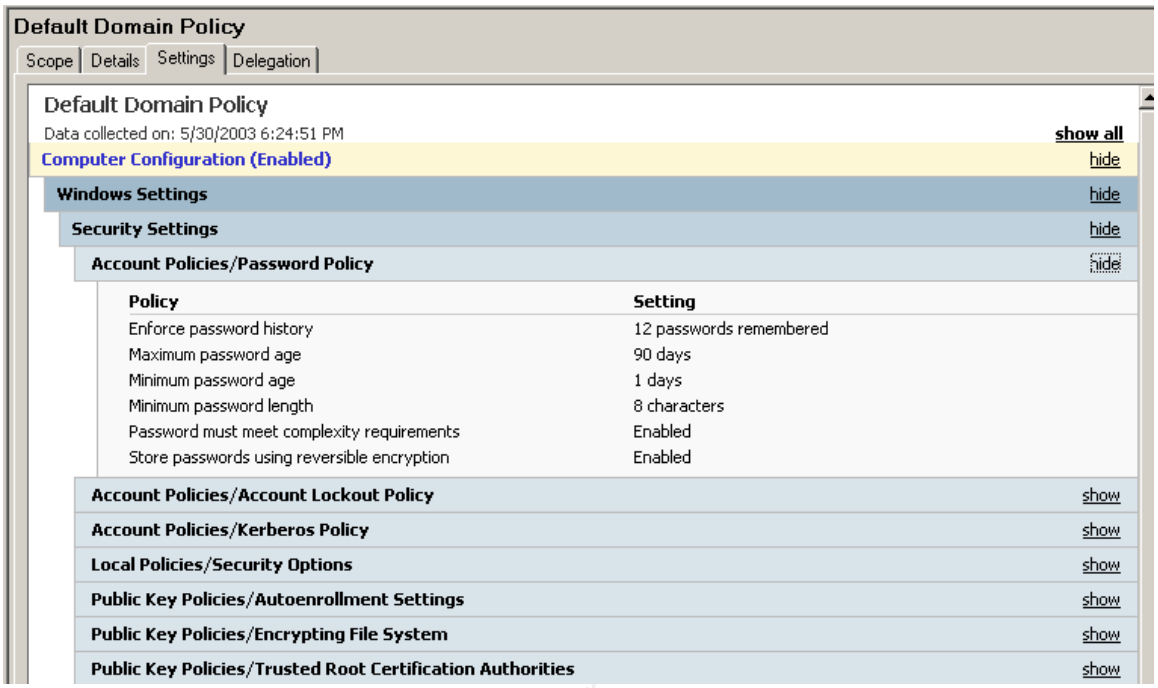
Event log retention is provided by stringent log file size requirements (500 MB per log) and the daily harvesting of these logs. Custom scripting in perl helps to dump the appropriate system events into a central database for reporting purposes. This script connects to all Windows network devices nightly and collects event log entries for application, security and system logs. Once this data has been collected, it is then imported into a SQL database for reporting purposes. Canned queries, ad hoc queries and significant events flags are routinely processed providing an accurate and timely snapshot of Enterprise-wide events. The perl script, which functions as a wrapper for the dumpevt.exe resource kit tool can be found in Appendix A.

Naming conventions, password resets, lockouts, expirations, userID creation, trust relationships and AD database changes are monitored by a third party tool, Pedestal Software's Intact™. Intact directory Services detects changes to LDAP-compliant databases, such as Active Directory. Pedestal Intact can effectively detect attribute and distinguished name changes, additions and deletions, as well as schema modifications. Intact will carefully monitor the Schema and Enterprise Administrators group memberships and report on additions. These reports will coincide with EGC approved changes as well as provide notification of possible breaches and changes that have not been approved. Additionally, Intact contains a behavior-based learning mode to detect unauthorized changes that have not been expressly identified.

Antivirus is critical to providing the current status of security threats to the newly joined forests. Central administration and reporting of malicious code provides a coordinated, proactive defense against the many possible vectors of virus introduction. McAfee EPO (ePolicy Orchestrator) provides this facility via a robust offering enterprise reporting, allowing for outbreak tracing, location of unprotected systems and overall antivirus posture. EPO is managed via a central console with its backend database stored on a SQL server. EPO has many predefined reports with exports available in HTML, Microsoft Word or Crystal Reports output. Additionally, ad hoc queries are available. Configuration of EPO allows for cross firewall protection and real time alerts and updates.

In addition to Intact and McAfee EPO reports, the GPMC tool allows for forest-wide reporting of GPO settings. The HTML reports are available in the settings tab of any GPO or GPO link and easily show all settings at a glance with expandable settings views. These reports will be reviewed regularly by the EGC and the appropriate IS Security personnel.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Auditing is an iterative process and automated auditing is a large component of the GASSANIC Corporation's security model. Daily reports are sent to GASSANIC IS Security Function members that correlate the information gathered by the above mentioned methods as well as for alerts generated by custom scripts. These scripts, run from a monitoring server, maintain uptime reports, service information and the membership of the Enterprise Administrators and Schema Administrators groups. All scripts are written in perl and run through the perl interpreter. This tool is provided by Active State and is distributed via SMS 2.0. SP3.

SMS 2.0 SP3 also generates reports of software installations, usage and removal. Aside from a powerful software distribution tool, SMS performs software audits for license compliance, the installation of unsupported software and effective metering for employee productivity data reviewed by the HR departments.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix A – Event Log Harvest Tool

```
#! usr/bin/perl
use Win32::Process;
use Win32::EventLog;

open (SERVLIST, "serverlist.txt");
while (defined ($server = <SERVLIST>)){
    chomp ($server);
    DumpEvt($server);
}

sub DumpEvt{

        # Run dumpevt.ext, dump the logs, and name it with the current month, day, year,
        # computer name and sec or app or sys
        #
    # Declare local variables
    my @evt = qw (APP SEC SYS);
    $tstamp = Stamp();

    # Define necessary variables
    $executabl= "L:\\dumpevt\\dumpevt.exe";
    $param1 = "/reg=local_machine";
    $param3 =  "/computer=$server";
    foreach $evt(@evt){
        $param2 = "/logfile=$evt";
        $folder = "L:\\event_logs\\$server\\$evt\\";
        $param4 = "/outfile=".$folder.$tstamp.".txt";
        $srvfldr = "L:\\event_logs\\$server\\";
        $file = $folder.$tstamp.".txt";
        $param = $param1 . " " . $param2 . " " . $param3 . " " . $param4;
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
        if(! -d $srvfldr){
            mkdir($srvfldr) || die "Cannont create $srvfldr\n";
            mkdir($folder) || die "Cannont create $folder\n";
        }
        elsif(! -d $folder) {
            mkdir($folder);
        }

        if (! `$executabl $param`){
            Log_event(503, "Process did not completed successfully",$executabl);
        }
        else{
            if (-e $file){
                Log_event(113, "Process completed successfully",$executabl);
            }
            else{
                Log_event(113,  "Process completed successfully with no log
changes",$executabl);
            }
        }
    }
}

sub Stamp{
## Setup for time stamp on report

    my ($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst) = localtime(time);
    $year = $year + 1900;
    $mon++;

    if($mon == 1){
        $mon = "Jan";
    }
    elsif($mon == 2){
        $mon = "Feb";
    }
    elsif($mon == 3){
        $mon = "Mar";
    }
    elsif($mon == 4){
        $mon = "Apr";
    }
    elsif($mon == 5){
        $mon = "May";
    }
    elsif($mon == 6){
        $mon = "Jun";
    }
    elsif($mon == 7){
        $mon = "Jul";
    }
    elsif($mon == 8){
        $mon = "Aug";
    }
    elsif($mon == 9){
        $mon = "Sep";
    }
    elsif($mon == 10){
        $mon = "Oct";
    }
    elsif($mon == 11){
        $mon = "Nov";
    }
    elsif($mon == 12){
        $mon = "Dec";
    }
    if($mday < 10){
        # If Day of Month is < 10, pad it with a zero to yield a two-digit  number
        $mday = "0".$mday;
    }
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
    $stime = $mday . $mon . $year;
}

sub Log_event{

    # Initiallize local variables.
    my %event;
    my $event_type;
    my $event_cat = 7;                      # Refers to Detailed Tracking    category.
    my ($event_id, $event_string, $event_data) = @_;
    my ($event_log);
    my $script_name;


    # Load name and path of current script, strip the path, leaving only the    script
name.
    $script_name = $0;
    $script_name =~ s/.*\\//g;

    # Determine event type. Exit if the event id is out of scope.
    if($event_id < 100){
        die "Invalid Event ID (EventID < 100)";
    }elsif($event_id > 699){
        die "Invalid Event ID (EventID > 699). $!";
    }else{
        # Error codes starting with a 1 or 2 are informational
        if($event_id =~ /^[12]/){
            $event_type=EVENTLOG_INFORMATION_TYPE;
        # Error codes starting with a 3 or 4 are warnings
        }elsif($event_id =~ /^[34]/){
            $event_type=EVENTLOG_WARNING_TYPE;
        # Error codes starting with a 5 or 6 are fatal errors
        }elsif($event_id =~ /^[56]/){
            $event_type=EVENTLOG_ERROR_TYPE;
        }
    }

    # Define a hash with eventlog info
    %event=("EventID" => $event_id,
            "Strings" =>    "Script=$script_name;Category=$event_cat;;$event_string",
            "Data" => $event_data,
            "Category" => $event_cat,
            "EventType" => $event_type);

    # Write to the event log.
    $event_log = new Win32::EventLog("Scripts",$server) || die $!;
    $event_log->Report(\%event) || die $!;
}
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References:

Microsoft TechNet Article “Planning and Implementing Federated Forests in Windows Server 2003” URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/security/fedffin2.asp

Microsoft Product Support Services, Support Webcasts “Restructuring, Migrating, and Upgrading Domains to Windows .NET Server 2003” URL:
http://support.microsoft.com/servicedesks/webcasts/wc102902/WC102902.ppt

Microsoft TechNet Articles “Windows Server 2003 Resouces” URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsnetserver/evaluate/cpp/reskit/adsec/part1/rkpdsefl.asp

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Microsoft TechNet Article "DNS requirements for installing Active Directory" URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_dns_und_dcpromo_requirements.asp

Microsoft TechNet Article "Verifying DNS before installing Active Directory" URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_DNS_Chk_new_forest.asp

Microsoft TechNet Article "To verify DNS registration for domain controllers using the nslookup command" URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_DNS_tro_VerifyDomainSrvLocRRs.asp

"Introduction to Group Policy in Windows Server 2003: White Paper" 24 April 2003 URL:
http://www.microsoft.com/windowsserver2003/techinfo/overview/gpintro.mspx

Windows 2000 Resource Kit "Designing the Active Directory Structure" URL:
http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/deploy/dgbd_ads_irnw.asp

"Administering Group Policy with the GPMC: White Paper" 7 April 2003 URL:
http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx

Jeff Shawgo, et al. "Securing Windows 2000: Step By Step" The SANS Institute.2001

Fossen, Jason; Windows 2000/XP Scripting for Security, 2002

Fossen, Jason; Windows 2000/XP Group Policy and DNS, 2002

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Fossen, Jason; Windows 2000/XP Active Directory, 2002

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.