Global Information Assurance Certification Paper

Acquisition of GIAC Enterprises by SANS Co.

"There's A Fortune To Be Made"

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

Submitted by: Erik P. Gilreath
Submitted on: June 14, 2004

Table of Contents

0.0 Abstract

The year is 2004 and SANS Co., having made it through the dark times of the recent recession, is looking to expand its operations. No one thought a company that specializes in making "Inspected by" tags for retail stores would ever survive.

SANS Co. is based in Grand Rapids, Michigan. They are a small organization of approximately 1,000 employees with factories in the Michigan cities of Grand Rapids, Lansing, and Detroit. They are considered to be at the top of the list for retailers needing "Inspected by" labels. They have a stellar reputation of quick turn around and impeccable quality with reasonable rates. However, they were feeling the pinch of the recession like everyone else and were scrambling to come up with a way to capitalize on their existing business processes.

Then, one Friday afternoon, the two founders of SANS Co. went to a local Chinese restaurant for lunch. After finishing their meal of Moo Shoo Pork they reached for the customary fortune cookie that came with the bill. They cracked open their cookies, in search of an inspirational fortune inside, when they came to a sudden realization: if people like getting fortunes in cookies, why wouldn't they like them in suits, shirts, even underwear packages? People will start opening their underwear and not throw away the "Inspected by" papers but rather find out what good fortune their newly purchased undergarments will bring!

Wanting to "hit the ground running" with this new idea, SANS Co. went in search of an organization that already had the fortune saying business and infrastructure in place. They found a match in GIAC Enterprises.

GIAC Enterprises, located in Schaumburg, IL, was struggling in the competitive market of fortune cookie fortunes, but was considered one of the best in the business. With their R&D department combined with the manufacturing prowess of SANS Co. the founders of SANS Co. figured they couldn't lose.

GIAC Enterprises already had an existing Active Directory infrastructure in place. Full documentation of the GIAC Enterprises Active Directory design can be found at http://www.giac.org/practical/Dennis_Depp_GCNT.doc[1]. SANS Co. didn't have the IT staff to handle full control of the GIAC Enterprises computing environment, so it was decided to leave the GIAC Enterprises IT staff in place but allow the SANS Co. IT staff to manage the environment and have the final say in IT policy design, implementation, and maintenance.

The purpose of this document is to discuss in detail the domain design of SANS Co. and the configurations that have been made to allow interoperability between the two organizations. It will then lay out a group policy design to be adopted by

[1] Depp, Dennis. "Security Plan for GIAC Enterprises." GCNT Practical Assignment Version 3.0. 30 Jan. 2002. <http://www.giac.org/practical/Dennis_Depp_GCNT.doc>. (7 April 2004).

the two organizations, and explain how the group policy will be deployed and document the application of the group policy on an IIS server from SANS Co. An explanation of auditing the environments and long term maintenance of the security plan will also be discussed.

1.0 Domain Design

Being a progressive company, SANS Co. jumped onto the Windows Server 2003 bandwagon as soon as the technology became available. They liked the better security and manageability as well as the improved group policies and the Group Policy Management Console.

The Active Directory design and implementation at SANS Co. was very important to the owners of the company. They wanted a design to meet the current needs of the organization that was flexible enough to allow for future growth and needs.

This rest of this section will cover the Active Directory design and infrastructure of SANS Co. in depth. It will also describe the connectivity between SANS Co. Active Directory forest and the GIAC Enterprises Active Directory forest, detailing all trusts and delegation between the two with an emphasis on the interoperability and management of the forests.

1.1 SANS Co. Active Directory Specifics

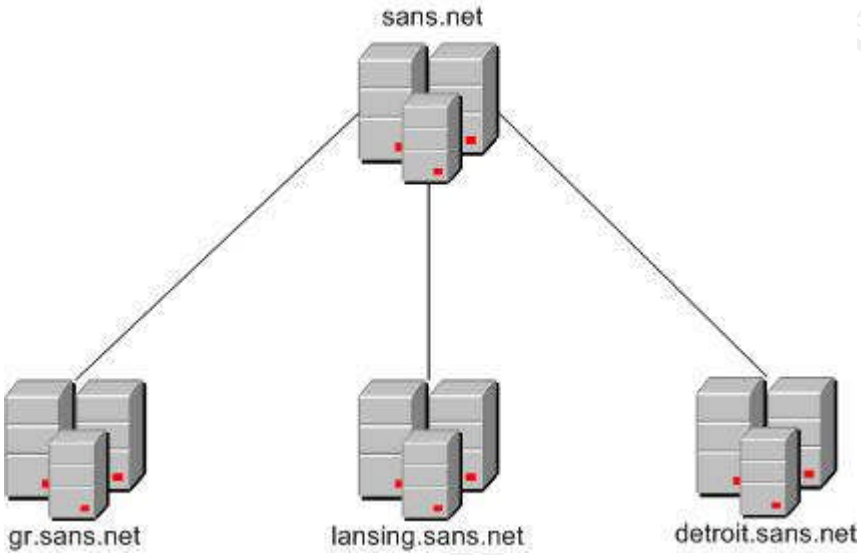
The SANS Co. Active Directory is a single Active Directory forest that contains four domains. The forest and all domains are running at a Windows Server 2003 Functional Level. The top level forest root domain is sans.net and is located at the headquarters in Grand Rapids, Michigan. It was decided to use a dedicated root domain for security, possible changes in organizational structure and to pre-empt any political issues of one domain being a subordinate domain to another regional domain. Being a dedicated forest root domain means that the domain does not contain any user accounts other than the basic service accounts and it does not represent any specific location in the organization.

The root domain of an organization is the first domain that is created when Windows 2003 is originally installed and Active Directory is first configured. By default it contains all Flexible Single-Master Operation (FSMO) roles and contains the two most powerful groups of the entire forest: the Enterprise Admins and Schema Admins groups. The Enterprise Admins group has full control of all domains in the enterprise while the Schema Admins group is the only group in the forest that is allowed to make modifications to the Active Directory schema. Because of the power of these groups, their membership is very limited. Use of the rights of these groups have to be approved by the owners of SANS Co. to prevent unauthorized modifications to the schema or abuse of the privileges held by these groups. In using the dedicated root domain, Domain Admins of the subordinate domains have full rights to their own

domains but not to any of the other domains. Therefore, Domain Admins in one domain that cannot make changes to a different domain.

There are three subordinate domains of sans.net. The first is gr.sans.net and it is located at the Grand Rapids, Michigan headquarters. The second and third subordinate domains are lansing.sans.net and detroit.sans.net which are housed in the Lansing, Michigan and Detroit, Michigan locations respectively. A graphical representation of the domain configuration is shown in Figure 1:

Figure 1: SANS Co. Active Directory Domain Diagram



In Windows 2003, all domain controllers are considered equal for the most part. That means that when a change of some kind is requested, the changes can occur at any domain controller and the changes will then replicate to all other domain controllers in the domain. The process of replicating these changes and handling any conflicts that arise is called multi-master replication and is part of the Active Directory multi-master model. A multi-master enabled database, such as Active Directory, provides the flexibility of allowing changes to occur at any domain controller in the enterprise, but it also introduces the possibility of conflicts that can potentially lead to problems once the data is replicated to the rest of the enterprise[2]. However, there are certain instances where it is better to just prevent conflict. In answer to this there are five FSMO roles:

[2]Microsoft Corporation. "Microsoft Knowledge Base Article – 197132." Windows 2000 Active Directory FSMO Roles. 05 Apr. 2004 <http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132>. (16 May 2004).

1. Schema Master
2. Domain Naming Master
3. PDC Emulator
4. RID Master
5. Infrastructure Master

The first two roles listed above are forest-wide roles while the other three roles are domain-wide roles. That means that in an organization with four domains, there will be one Schema Master, one Domain Naming Master, four PDC Emulators, RID Masters, and Infrastructure Masters.

The Schema Master role controls all changes to the Active Directory schema. Any schema change has to go through the Schema Master server to prevent conflicting changes to the schema happening at the same time.

The Domain Naming role controls any changes to the name-space forest wide. Any new domains or removal of domains goes through the Domain Naming master.

The PDC Emulator role varies slightly depending on the Domain Functional Level that the domain is running in. When running in compatibility mode, the PDC emulator acts as the Windows NT primary domain controller. This means that it processes all password changes and then replicates the changes to Windows NT 4.0 BDCs. When running in Server 2003 Domain Functional Level, the server still gets preferential treatment regarding passwords and gets the first notification of a password change from any other domain controller. The PDC Emulator also acts as the time source for all other domain controllers in the domain.

The RID Master role is responsible for the distribution of blocks of relative IDs (RIDs) to the other domain controllers in its domain. Every user, group, or computer object that is created in a domain is assigned a unique security ID (SID). The SID is made up of the domain SID, which is identical for any SID created in the domain and a RID which makes the SID unique.

The Infrastructure Master role is responsible for keeping track of objects from other domains. For example, if you have a domain group that is made up of users from multiple domains, and one of the members of the group that is from a different domain gets renamed, the Infrastructure Master would be responsible for updating the user's name in the domain group in the local domain with the new name.

SANS Co. decided to use two domain controllers per domain. The domain controllers for sans.net and gr.sans.net are housed at the Grand Rapids location. The domain controllers for lansing.sans.net and detroit.sans.net are housed at their respective locations. Figure 2 is a table containing a listing of all the domain controllers for the organization, their IP address and special roles that they hold:

Figure 2: Server Listing

Root Domain - Domain Controllers		
SANS-DC-01	172.30.5.10	Schema Master / Domain Naming Master / GC
SANS-DC-02	172.30.5.11	PDC Emulator / RID Master / Infrastructure Master
SANS-CA-01	172.30.5.12	Certificate Authority

Grand Rapids Domain Controllers		
GR-DC-01	172.16.5.10	PDC Emulator / GC
GR-DC-02	172.16.5.11	RID Master / Infrastructure Master
GR-DHCPWINS-01	172.16.5.12	DHCP / WINS

Lansing Domain Controllers		
LAN-DC-01	172.17.5.10	PDC Emulator / GC
LAN-DC-02	172.17.5.11	RID Master / Infrastructure Master
LAN-DHCPWINS-01	172.17.5.12	DHCP / WINS

Detroit Domain Controllers		
DET-DC-01	172.18.5.10	PDC Emulator / GC
DET-DC-02	172.18.5.11	RID Master / Infrastructure Master
DET-DHCPWINS-01	172.18.5.12	DHCP / WINS

Having a minimum of two domain controllers per domain allows for fault tolerance in the case of a major failure to a domain controller. This makes it so that the system will be available to end users as much as possible. In the case of a catastrophic failure of one of the domain controllers resulting in the machine never coming back on-line, the missing FSMO roles could be seized by the remaining domain controller and then transferred to a new domain controller in the future. Also, if the system shows signs of being overburdened, additional domain controllers can be added in the future to spread the load further.

As can be seen in Figure 2 above, the FSMO roles are balanced between servers at each location. Notice that the Global Catalog server is not on the server holding the Infrastructure Master role. The Infrastructure Master role should be held by a domain controller that is not a Global Catalog server. If the Infrastructure Master role is hosted on a Global Catalog server, cross-domain object references in that domain are not updated, and a warning to that effect is entered in that domain controller's event log[3].

Each location has a Global Catalog server. The Global Catalog server stores a local, full, writable domain replica (all objects and all attributes) plus a partial, read-only replica of every other domain in the forest[4]. This makes it possible to

[3] Penton Media, Inc. JSI FAQ. "JSI Tip 3654." Don't locate the Infrastructure Master and Global Catalog on the same server in a multi-domain forest. <http://www.jsiinc.com/SUBH/tip3600/rh3654.htm>. (16 May 2004).
[4] Microsoft Corporation. "Technologies Collections – Active Directory Collection." Microsoft Windows Server 2003 Technical Reference.

search for an object in the entire Active Directory forest without having the request get passed from domain controller to domain controller until the object is found. Since the Global Catalog server has a partial copy of all objects from all domains in the forest, it can respond to the requests.

The dedicated root domain has the default OU layout that was created when Active Directory was installed and wasn't modified because it does not contain any accounts. Every other domain in Active Directory has the same OU structure configuration as one another and has been customized to improve the ease of management of the domain. The OU structure is designed around the need to assign group policies to the objects contained in the OUs. There will be a general Default Domain Policy that will apply to all objects and then OU level group policies will be assigned to refine the Default Domain Policy.

The first added OU is named Domain Users. This OU contains all of the basic users and groups that are members of the domain. Because none of the domains are very large, this configuration works well. If in the future there is significant growth at the sites, or there is a need to assign different group policies to various groups of people, the OU structure can be modified to accommodate subordinate OUs underneath the Domain Users OU. This would allow different groups of users to be assigned different group policies or to delegate authority of a specific OU to allow additional rights to be given to a group of users. At this time, all users receive the same group policy, so subordinate OUs are not required.

The second OU is named Management Users. This OU contains all management users and groups. Every domain administrator user will have a normal user account that they use for day to day activities and a separate management account that is used strictly for domain administration tasks. This way, if a domain administrator's user account is compromised somehow, or the workstation that they are working on gets compromised, the malicious application will have limited rights and not full administrative rights. In addition, we can apply a different group policy to the administrative users than the regular users to allow the administrative user greater access to various servers and workstations.

The third OU that is available is for servers. This OU has three separate subordinate OUs: Web Servers, Application Servers, and Citrix Servers. This design is so that different group policies can be applied to the different server types. For example, the Web Servers OU will have a highly restrictive group policy assigned to it where as the Citrix Server OU will have a group policy with loopback processing enabled. This will be discussed in greater detail in the group policy configuration section of this document.

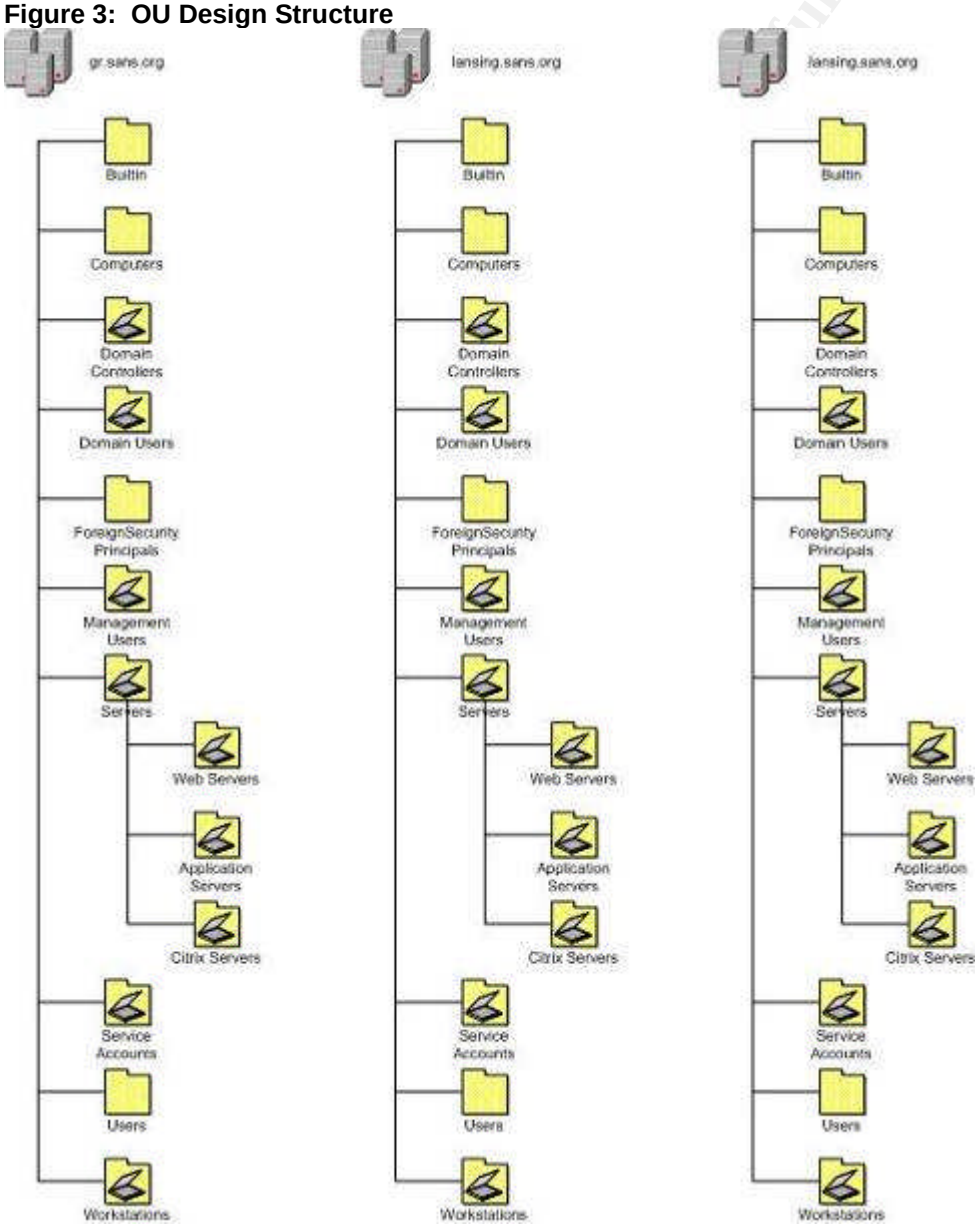
<http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/techref/en-us/w2k3tr_ad_over.asp>. (16 May 2004).

The fourth OU is the Service Accounts OU. It will contain all service accounts and groups. These would be backup software agent accounts or MOM agent accounts. Any service that requires an account to be configured for the service to work would be in this OU.

The fifth OU is the Workstations OU. This OU contains all workstations in the domain. Once again, if the need arises to apply different group policy configurations to different groups of workstations, subordinate OUs can be created to accommodate this. At this time, all workstations receive the same group policy so subordinate OUs are not required.

A diagram of the Active Directory OU design structure is shown in Figure 3:

Figure 3: OU Design Structure



1.2 Infrastructure

The infrastructure of any network is extremely important. It makes up the foundation of the network and if it is unreliable then no matter how robust and redundant the rest of the network is, everything will be perceived as unstable. Therefore, SANS Co. decided on using Cisco for its entire network infrastructure.

A uniform IP numbering scheme is also used. It was decided to use the 172.X.X.X/16 private IP range. That allows for IP addresses to range from 172.16.1.1 – 172.31.255.255[5] which allows for a great deal of flexibility when assigning IP ranges.

Each domain has been configured with its own subnet:

- gr.sans.net = 172.16.X.X
- lansing.sans.net = 172.17.X.X
- detroit.sans.net = 172.18.X.X
- sans.net = 172.30.X.X

The allocation of IP addresses at each location follows a standardized scheme to make it easier for administration and use of the network. Figure 4 outlines the standardization:

Figure 4: IP Address Allocation Standard

Device	Start IP Address	End IP Address
Networking Devices	172.XX.1.1	172.XX.4.254
Servers	172.XX.5.1	172.XX.9.254
Printers	172.XX.10.1	172.XX.14.254
Workstations	172.XX.15.1	172.XX.29.254

This addressing scheme allows a lot of room for expansion in the future if the locations increase in size. It also allows a lot of flexibility in assigning IP address based on building, floor, or department if it is decided.

All locations are connected by a T1 (1.536Mbps[6]) connection to the Internet. Each T1 routes out to the Internet through a Microsoft ISA server and a Cisco PIX 506E firewall. The PIX is configured so that all communications between the Grand Rapids, Detroit, and Lansing sites are secured using 168-bit Triple Data Encryption Standard (3DES) VPN tunnels running from PIX to PIX[7]. There are a

[5] Fosh Australia Pty Ltd. "Private IP addresses for use on internal networks." Vicom Technology – VICOM Internet Gateway FAQ's / Text. <http://www.fosh.com.au/Fosh/Support/vi/privateip.html>. (16 May 2004).
[6] Microsoft Corporation. "Wide Area Systems and Services – What's Cooking With T1 Bandwidth?" Microsoft Tech Net. 15 Jun. 1997. <http://www.microsoft.com/technet/prodtechnol/winntas/evaluate/featfunc/cmpt1.mspx>. (16 May 2004).
[7] Cisco Systems. "Cisco PIX 506E Security Appliance." Cisco PIX 500 Series Firewalls. <http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b13.html>. (16 May 2004).

total of three tunnels: Grand Rapids to Lansing, Grand Rapids to Detroit, and Detroit to Lansing.

The ISA Server is configured as both a firewall and a proxy server. All Internet traffic passes through the ISA Server. If a proxy server is not configured in the user's browser, they will not be able to connect to the Internet. In addition, SANS Co. workstations are configured with the Microsoft Firewall Client that allows for better monitoring of web activity and pass-through authentication of the user's login information.

The PIX routers are configured to limit incoming and outgoing traffic. The traffic is limited to web and secure web traffic (HTTP and HTTPS) being allowed in and out to anyone and SMTP traffic only going in and out from the Exchange server. This is shown below in Figure 5:

Figure 5: PIX Router Allowed Protocol List Permit	**From**	**To**	**Direction**	**Notes**
TCP 25	any	172.30.5.13	in/out	Allows SMTP traffic to and from the Exchange Server only
TCP 80	any	any	in/out	Allows HTTP traffic in and out
TCP 443	any	any	in/out	Allows HTTPS traffic in and out
TCP 1494	any	172.16.5.10	in/out	Allows Citrix ICA traffic to and from the Citrix Server only

In addition, there is an IPSec Security Policy on Active Directory in place that requires secure communication between the domain controllers from the different sans.net domains. The policy is configured based on subnet mask to limit it to server to server communication only. The IP Filter List configuration is listed in Figure 6:

Figure 6: IPSec Policy Filter List

Source	Destination	IP Address	Subnet Mask	IP Protocol Type	Mirrored
My IP Address	A specific IP Subnet	172.16.5.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.16.6.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.16.7.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.16.8.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.16.9.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.17.5.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.17.6.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.17.7.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.17.8.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.17.9.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.18.5.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.18.6.0	255.255.255.0	any	yes

My IP Address	A specific IP Subnet	172.18.7.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.18.8.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.18.9.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.30.5.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.30.6.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.30.7.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.30.8.0	255.255.255.0	any	yes
My IP Address	A specific IP Subnet	172.30.9.0	255.255.255.0	any	yes

In the future, if any new offices are built and new IP addresses added, they will have to be included into this filter list.

Each location has a Layer 3 switch which allows for the configuration for various VLANs. There are five common VLANs configured at each location. The configured VLANs are listed in Figure 7:

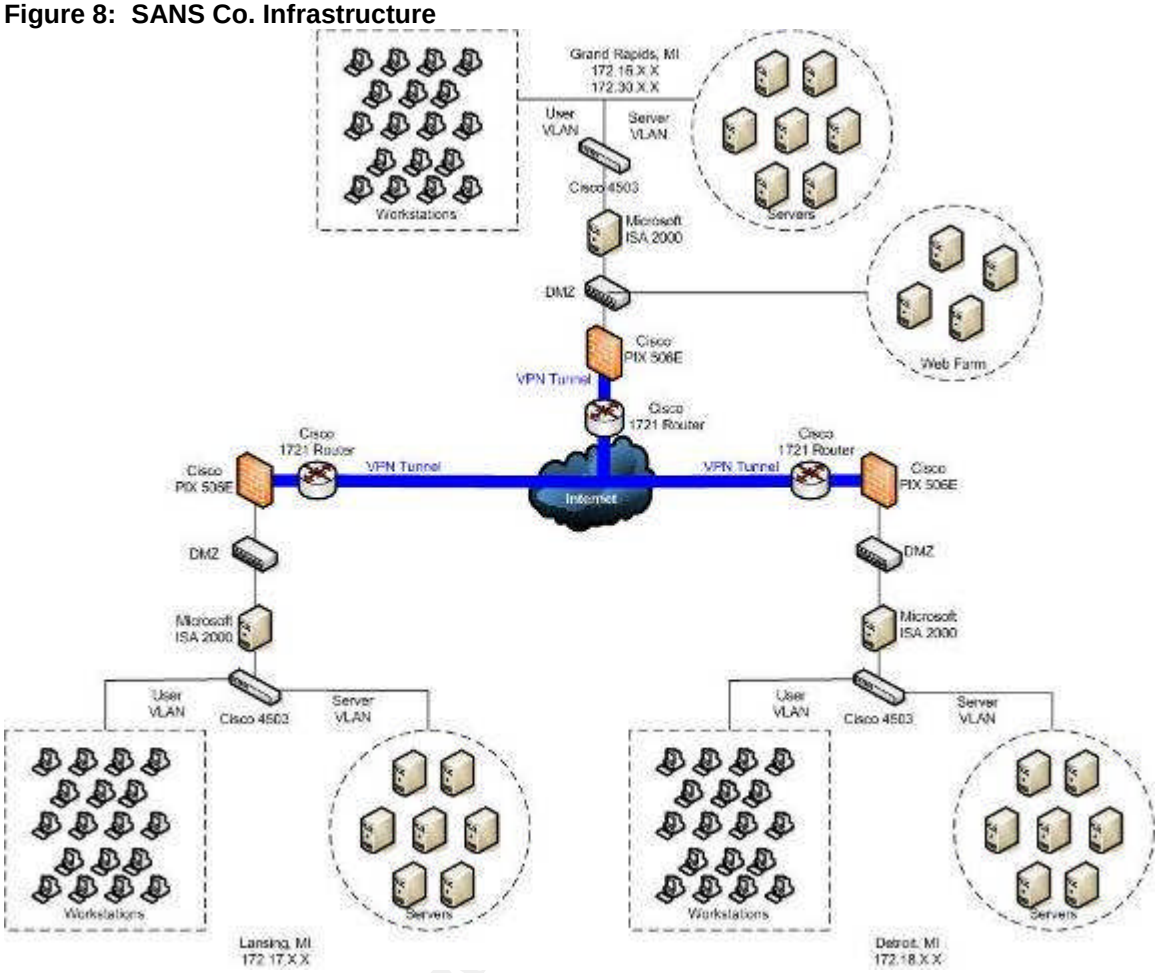
Figure 7: Common VLAN Configuration

VLAN #	VLAN Name	Purpose
VLAN1	MGT	Cisco Management
VLAN2	NET	Networking Devices
VLAN3	SVR	Servers
VLAN4	PTR	Printers
VLAN5	USR	Workstations

This VLAN configuration allows for better segmentation of network traffic. Also, the Grand Rapids location has an additional VLAN for the sans.net servers.

Figure 8 is a graphical representation of the entire network infrastructure:

Figure 8: SANS Co. Infrastructure



Physical access to the servers is also part of the infrastructure. Each location has a secure, climate controlled room with a fire suppression system. Access to the room is by key card only and all access is logged. In addition, each location has a video surveillance system that can be used to verify that a person who was logged as having swiped their card for access into the data center really was the person who entered.

1.3 Site Configuration

The configuration of Active Directory sites plays an important role in controlling replication traffic over WAN links. A site is typically configured in relation to the actual network topology. Microsoft defines the Active Directory site as "a collection of one or more well-connected Internet Protocol (IP) subnets."[8] It is the definition of "well-connected" that is the key to deciding how to configure sites. For SANS Co. purposes, Active Directory Sites well-connected is defined as a minimum connection speed of 10Mbps.

[8]Holme, Dan and Thomas, Orin. Upgrading Your Certification to Microsoft Windows Server 2003. Redmond: Microsoft, 2004. 1-41.

Because the three locations of SANS Co. are linked together by T1 connections, each location will be configured as an individual site. Grand Rapids Active Directory Site will contain the 172.16.X.X and 172.30.X.X subnets. The Lansing site will contain the 172.17.X.X subnet and the Detroit site will contain the 172.18.X.X subnet. Replication between the sites will occur only during the off-hours of 8:00pm – 6:00am and can be forced at other times if necessary. All traffic will be secured from server to server using the IPSec policy that is in place.

1.4 Hardware

As stated earlier, Cisco is the vendor of choice for all networking infrastructure. This includes routers, switches, and hardware firewalls. Cisco 1721 routers are being used for connecting to the Internet. The Cisco PIX 506E is used as the external firewall and as the first layer of defense. A generic hub is used as the DMZ. Once inside, all traffic routes through the Cisco 4503 core switch which is the backbone for all traffic at each location. The wiring closets all use Cisco Catalyst 2950 24 port switches.

SANS Co. was able to work out a deal with Dell and so all workstations and servers are Dell. All servers have a minimum RAID5 configuration, dual XEON processors, redundant power supplies and 2GB of RAM. Other configurations exist based on the needs of the server.

All workstations are a minimum of a Pentium 4 with 512MB of RAM and a 20GB hard disk. As with the servers, more powerful configurations exist based on the needs of the user.

In the data centers, power is provided by Liebert NX UPS systems.

1.5 Network Services

SANS Co. uses several networking services to allow for the seamless use of the computing environment by end users and to assist in the management of the network by administrators.

Each location has a DHCP/WINS server that provides IP addresses for user workstations and WINS services. In addition, each location has DNS services installed on the domain controllers. All DNS zones are active directory integrated zones. The Grand Rapids, Lansing and Detroit DNS servers contain the DNS zone records for their respective domains and forward all other requests to the sans.org DNS servers.

Exchange 2003 is the e-mail system in use and the mail servers reside at the Grand Rapids office. All users connect to the mail system using the Microsoft Outlook 2003 client.

There is a domain Certificate Authority (CA) that is configured in the sans.org domain that provides certificates for all domain computers. The CA is housed on the SANS-CA-01 server.

Software deployment is handled by Microsoft Systems Management Server 2003. This allows the deployment of software packages to workstations whether a user is logged in or not. It also assists in patching and support. This is discussed further in the Audit section of this document.

1.6 Web Farm

SANS Co. has a small web farm that allows customers to check on orders placed and to allow them to place additional orders. It also houses the Citrix Web Interface web server for remote access into the environment using Citrix MetaFrame XP Presentation Server. The web farm servers are part of the gr.sans.org domain and are contained in the Web Servers OU to allow for tighter configuration of the servers through group policy. All of the web servers are running Windows Server 2003 Web Edition.

The web farm is physically based in the Grand Rapids office and sits on the DMZ behind the Cisco PIX firewall. All web servers have a Verisign SSL eCommerce certificate on them to allow secure SSL communications for sensitive data. Verisign was selected because of the availability of their root certificate in most browsers.

The web servers are managed using Dell Remote Access Cards. They are hardware devices that allow full control of the console, even if the server is powered off. All traffic from the web servers to the internal network is blocked by the Microsoft ISA Server except for 80, 1494 and 5001 traffic. The port 80 and 1494 traffic is configured to only route to the internal Citrix servers and the 5001 traffic is required to allow access to the remote access cards.

1.7 GIAC Enterprises Overview

GIAC Enterprises was running a Windows 2000 environment at the time of acquisition which worked well for the simple single domain model. The Windows 2000 environment contained a single site and a single domain, GIAC.Net.

The GIAC.Net OU design had three main OU levels defined:

- Hardened Enclave
- R&D Enclave
- Main User Enclave

The Hardened Enclave contains the GIAC.Net web server and e-mail gateway. Because the objects in this OU are accessible from the Internet, they are locked down heavily using group policies.

The R&D Enclave is the location of all users and computers that are used to create and maintain the fortune cookie sayings. Because of the sensitive nature of the information that is stored and wanting to prevent any leaks, the R&D Enclave restricts access to all users and computers using group policies and IPSec policies.

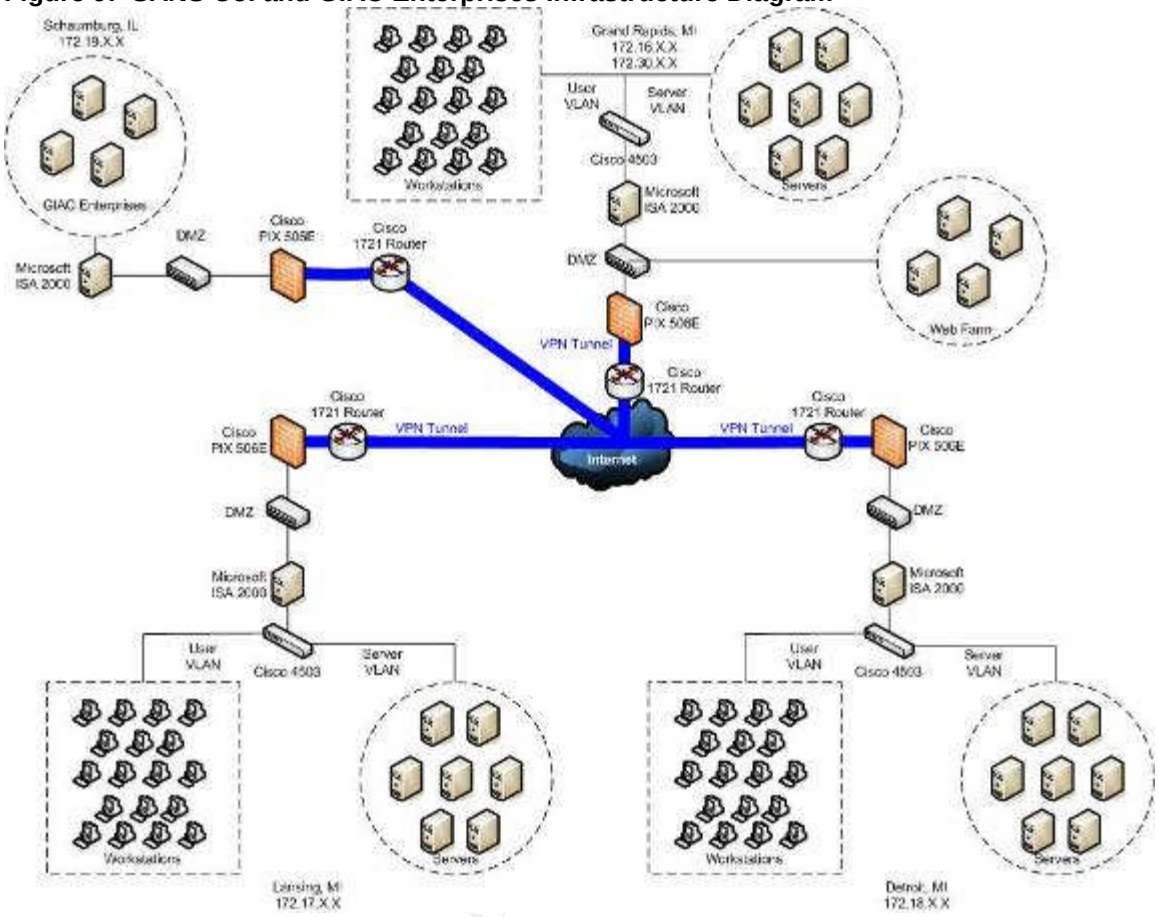
The Main User Enclave contains all other users and computers for the organization. There are group policies and IPSec policies applied to this OU and sub OUs but they are not as restrictive.

It was decided by SANS Co. management to send a team of engineers over to GIAC Enterprises and work with the IT Staff there to upgrade all servers to Windows Server 2003 for the increased performance, security and reliability that it offers. They also raised the forest functional level and domain functional levels to Windows Server 2003 as well. In configuring GIAC Enterprises in this way, SANS Co. was able to take advantage of the Forest Trust capabilities of Windows Server 2003.

1.8 SANS Co. and GIAC Enterprises Trust

Before any trust relationships could be created, physical connectivity between the two organizations needed to be established first. GIAC Enterprises was using a Cisco PIX 506E for its firewall duties so it was configured as part of the SANS Co. VPN mesh. A Microsoft ISA Server was also added so that the DMZ configuration would match the configuration at all of the SANS Co. locations. In addition, the GIAC Enterprises active directory controllers were added to the IP Filter list so that they could communicate with the SANS Co. active directory controllers. Figure 9 shows the updated infrastructure:

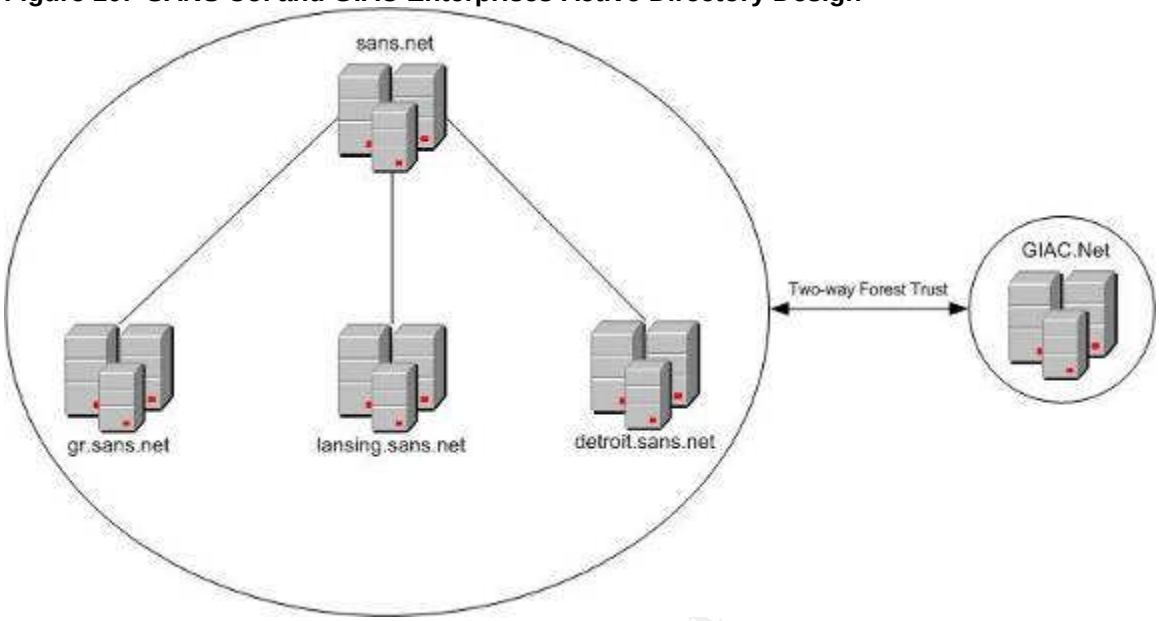
Figure 9: SANS Co. and GIAC Enterprises Infrastructure Diagram



With connectivity in place and both organizations running at Windows Server 2003 Forest and Domain functional levels, a two-way forest trust was created between sans.net and GIAC.Net using the Windows Server 2003 New Trust Wizard.

A two-way forest trust creates a transitive, two-way trust relationship between two forests. This allows administrators to be able to configure access to resources to users and computers in either forest. Because it is a transitive trust, it extends to all domains in both forests. The two-way forest trust is also easier on the end users because they can logon using their universal principal name (UPN) to authenticate across forests. It also allows for the use of Kerberos and NTLM authentication protocols across the forests. Figure 10 shows the updated Active Directory design of the SANS Co. and GIAC Enterprises forests:

Figure 10: SANS Co. and GIAC Enterprises Active Directory Design



Once the forest trust was created, the Domain Administrators group from sans.net was delegated control of the GIAC.Net domain. This was done to allow sans.net IT Staff to be able to administer the GIAC.Net domain. It was also decided to modify the GIAC.Net domain OU structure to reflect the SANS Co. OU structure as defined in Figure 3 above.

After the creation of the two-way forest trust and delegation of authority had been completed, the SANS Co. IT Staff started working on the creation of the group policies to be assigned to SANS Co. and GIAC Enterprises so that the SANS Co. security policies were being adhered to.

2.0 Security Policy

Security of the various computers and servers in SANS Co. and GIAC Enterprises is handled via group policy. Group policy allows for the centralized configuration and management of computer and user settings that can then be applied across the various domains and forests. A group policy can be defined at the following levels:

- Local – Group policy configured on the local workstation
- Site – Group policy configured on an Active Directory Site
- Domain – Group policy configured on an Active Directory Domain
- OU – Group policy configured on an Active Directory OU

Group policies are applied in the order: Local, Site, Domain, Parent OU, Child OU. This means that group policies configured at an OU level can override

group policies configured at the Domain level. Also note that OUs can be nested and that the lowest nested OU will be the last group policy to be applied.

There can be an exception to the group policy application order through the use of the Block Inheritance and No Override options that are available. The Block Inheritance option is assigned at the Site, Domain or OU level and blocks the inheritance of all parent group policies. This is typically used in cases where a higher level group policy that is assigned, a Default Domain Policy for example, that is too restrictive. By setting the Block Inheritance at an OU the Domain Group Policy will not be applied.

The No Override option is configured in a Group Policy Object (GPO) and forces the application of the group policy that is being assigned by the GPO. This includes the application of the group policy even to containers that are configured with Block Inheritance. In addition, the No Override option does not allow a group policy configured at a lower level to change the setting that is being applied by the group policy. Because of the power and unintended consequences of using the Block Inheritance and No Override functions, they should be used only when absolutely necessary. To ease troubleshooting of group policies and group policy assignments, it is better to try and use Site, Domain and OU design to get the correct group policies assigned rather than change the normal application of a group policy by using the Block Inheritance and No Override options.

SANS Co. has taken the approach to assign group policy configurations that will apply to most all computers and users at the domain level and then assign more restrictive group policies at the OU level to refine the configuration of the group policies as needed to enforce the SANS Co. security plan while addressing the functionality needs of the users and computers in the various OUs.

Management of the group policies will be done using the Group Policy Management Console. The Group Policy Management Console allows for ease in seeing what attributes of a group policy are set, running users or computers through a “What If” simulation to show what group policies will be a applied to a computer or user if they are moved to a different OU and it allows for managing of group policies and group policies across forests. Group policies cannot be linked across forests but using the Group Policy Management Console, it is possible to copy group policies across forests so that consistency of group policies can be maintained.

The rest of this section will cover in depth the configuration of the group policies being applied to SANS Co. and GIAC Enterprises.

2.1 Group Policy Configuration

SANS Co. is responsible for approving all Active Directory group policies. As stated previously, the philosophy of the organization is to apply a broad based policy at the domain level and to use OU level policies to fine tune configurations as necessary. All domains have the same group policy applied to them. This was accomplished by creating the Default Domain Policy and using the Backup and Import features of the Group Policy Management Console to copy the default domain policy after it is finalized and to import it into the other domains and into the GIAC.Net forest.

The Default Domain Policy is based on the Microsoft Secure Workstation policy template that is included in the Microsoft Windows Server 2003 default installation[9]. The policy has been modified as necessary to fit the environment.

2.1.1 SANS Co. Local Group Policy

Local group policies are not configured on any SANS Co. workstations or servers. All group policies will be deployed from Active Directory.

2.1.2 SANS Co. Site Group Policy

Site group policies are not currently being used by SANS Co. All group policy configurations will happen at the Domain or OU level.

2.1.3 SANS Co. Default Domain Policy

This section will lay out the Default Domain Policy that is implemented for all domains in the SANS and GIAC organizations. The section contains several figures containing the configured settings with a description of the settings beneath each figure.

Figure 11: Default Domain Policy – Password Policy

Policy	Computer Setting
Enforce password history	24 passwords remembered
Maximum password age	45 days
Minimum password age	5 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

[9] Microsoft Corporation. "Predefined Security Templates." Microsoft Windows Server 2003 Standard Documentation. <http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/sag_SCEdefaultpols.asp>. (12 June 2004)

The purpose of this portion of the policy is to ensure that passwords are not easily compromised. The default setting of 24 passwords remembered was kept. This setting, when combined with the minimum password age of 5 days means that the least amount of time before a user could reuse a password is 120 days.

Maximum password age was bumped up to 45 days just because the group policy designers liked the number 45 more than the number 42.

Minimum password length was left at 8 characters and deemed secure enough when used with the complexity requirements. The complexity requirements, as described by the Microsoft Windows Server 2003 Documentation, require that the password adheres to the following rules:[10]

- Not contain all or part of the user's account name
- Be at least six characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A though Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)

Users are however, strongly encouraged to use pass phrases which are easier to remember and not difficult to create to fulfill length and complexity requirements. An example pass phrase would be: Long passwords can be fun! That password is greater than 8 characters, contains upper and lowercase characters and a non-alphabetic character to fulfill the complexity requirements, all the while being very easy to remember and type.

The storing of passwords using reversible encryption will not be allowed. There are no applications that require reversible encryption to be enabled and because it is a significant security concern if implemented.

Figure 12: Default Domain Policy – Account Lockout Policy

Policy	Computer Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Account lockout policies are always a difficult decision to make. Ideally you would like to make sure that if someone is trying to brute force guess at a password, that after so many attempts the account is locked and has to be unlocked by an administrator. However, if you are the administrator, you get

[10] Microsoft Corporation. "Password must meet complexity requirements." Microsoft Windows Server 2003 Enterprise Documentation. <http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/504.asp>. (12 June 2004)

tired of unlocking 30 accounts every Monday morning because users bumped their Caps Lock key or getting called in the middle of the night when a night shift employee leans on the keyboard. In addition, a simple denial of service attack can be done by routinely attempting to log in and locking out an important account. After much haggling, the policy stated in Figure 12 was deemed adequate.

Essentially, a user gets five attempts to type their password correctly. If they don't succeed in those attempts, their account will be disabled for 30 minutes and then they get to try again. Proper monitoring should catch anyone trying to brute force attack someone's account and five attempts should be plenty for someone who is actually going to remember their password.

Figure 13: Default Domain Policy – Kerberos Policy

Policy	Computer Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Kerberos is the authentication method that is in use for both SANS Co. and GIAC Enterprises. It provides for fast and secure authentication and access to resources in all domains.

User logon restrictions being enforced means that the user account will be checked, on every resource request, that it is still active and authorized to access the resource that is being requested. This prevents an account that has been disabled, while the account was logged in, from having access to resources that it shouldn't.

The setting of the maximum lifetime for service ticket limits the amount of time that a session ticket that has been issued is valid. Once the ticket expires, a new ticket will need to be requested and issued from the Key Distribution Center. This has been set to 10 hours.

The setting of the maximum lifetime for user ticket refers to the user's Ticket Granting Ticket. The value configured is the number of days that a user's Ticket Granting Ticket can be renewed. The Ticket Granting Ticket is what a client presents to a target principal when authenticating to that principal, where the principal is any computer, person, service or thing that can engage in a Kerberos authentication exchange.[11]

The maximum lifetime for user ticket renewal is the number of days that a user's Ticket Granting Ticket may be renewed. After this time has elapsed, a new ticket

[11] Fossen, Jason. Windows 2000/XP/2003 Active Directory. (SANS Institute, 2003) 39.

must be exchanged with the principal for authentication. This has been left at the default setting of seven days.

The maximum tolerance for computer clock synchronization is the maximum variation of minutes that Kerberos tolerates between a client's clock and the principal running Kerberos. This is done to prevent replay attacks. Replay attacks are where attackers replay authentic network exchanges that they capture off the wire to cause the server to allow them access to the system.[12] The default setting of five minutes was kept.

Figure 14: Default Domain Policy – Audit Policy

Policy	Computer Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not defined
Audit logon events	Failure
Audit object access	No auditing
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	No auditing

Auditing is an important part of any security policy. In the event of a breach, you need to be able to look back and see what has happened. Therefore, auditing is enabled on all computers by default.

Audit account logon events audits each time the computer is used to validate the logging on or off of a user. This allows you to see who has authenticated or attempted to authenticate to the server or workstation. The policy is configured to log all successful and unsuccessful logons.

Audit account management audits all account management on a computer. This encompasses the creation, modification or deletion of all users and groups and the setting or changing of a password. This allows you to see if there were changes made to users or groups on a computer. A common practice of hackers is to create new users and add them to the local administrator group on compromised systems. The policy is configured to log all successful and unsuccessful management attempts.

Audit logon events audits user's logging on and off of the computer. This allows you to see who has logged on or attempted to log on to the computer. The policy is configured to log failures only.

[12] Microsoft Corporation. "Setting Clock Synchronization Tolerance to Prevent Replay Attacks." Microsoft Windows Server 2003 Deployment Guide. <http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dsscc_aut_qwwi.asp>. (12 June 2004)

Audit policy change audits all changes to user right assignments, policies, audit policies and trust policies. This allows you to see if any user account had their privileges elevated or if auditing was changed. The policy is configured to log all successful and unsuccessful management attempts.

Audit privilege use audits each time a user exercises a user right. This allows you to see who did what or attempted to change something. The policy is configured to log only unsuccessful attempts.

Audit object access, audit process tracking and audit system events have been disabled at this level but can be enabled at specific OUs in other group policies.

Figure 15: Default Domain Policy – Security Options

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Shut down system immediately if unable to log security audits	Disabled
Devices: Allow undock without having to log on	Disabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled
Devices: Restrict floppy access to locally logged-on user only	Disabled
Devices: Unsigned driver installation behavior	Warn but allow installation
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Disabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Disabled
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Message text for users attempting to log on	The information on this workstation and ...
Interactive logon: Message title for users attempting to log on	Attention!!! Please Read...
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons
Interactive logon: Prompt user to change password before expiration	14 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled

Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	Not Defined
Network access: Remotely accessible registry paths	Not Defined
Network access: Remotely accessible registry paths and sub-paths	Not Defined
Network access: Restrict anonymous access to Named Pipes and Shares	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Not Defined
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Enabled
Network security: LAN Manager authentication level	Send NTLMv2 response only\refuse LM
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	No minimum
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	No minimum
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Not Defined
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Not Defined
System objects: Default owner for objects created by members of the Administrators group	Not Defined
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled
System settings: Optional subsystems	Not Defined
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Not Defined

The Security Options section is where the foundation of the organization security is laid. Looking at the Account settings, the Guest account on all computers will be disabled and if there are any accounts with a blank password, they will only be allowed to be used from the computer's keyboard

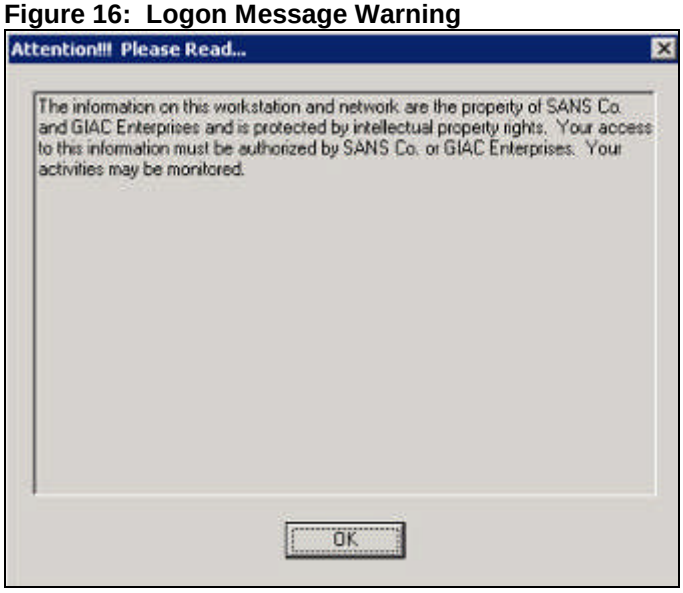
The audit section disables the auditing of the access to global system objects and the use of the backup and restore privilege. It also does not shut down the computer if it is unable to log security audits. This is to limit the amount of logging that is done. On sensitive systems, these settings will be modified accordingly.

Under the devices section, the configuration requires that a user be logged in to a docked workstation to undock it. It also only allows Administrators to format and eject removable NTFS media and allows access to the CD-ROM and floppy to both a logged in user and a network user at the same time. Finally, it will allow the installation of an unsigned driver but will warn the user and require the user to accept the risk.

In the Domain member section the computer is configured to digitally encrypt and sign secure channel data when possible but is not required to do so. This allows for secure traffic unless the workstation or server it is communicating with doesn't support it. The machine account password is also configured so that it is changed every 30 days.

In the Interactive Logon section, the last logged in user name will not be displayed and the user will be required to press Ctrl+Alt+Del to get to the login screen. This prevents someone from getting a known username just by walking up to a workstation and the Ctrl+Alt+Del makes sure that the logon is communicating by secure means. The users will also see the following when attempting to logon to a workstation or computer:

Figure 16: Logon Message Warning



The banner prevents unauthorized users from saying that they didn't know they weren't allowed to access the computer. Users will also have 10 logons cached if unable to connect to a domain controller and a domain controller is not required to be contacted to unlock a workstation. Users will be prompted 14 days before their password expires to change their password. Smart cards are not required to logon but if one is used, the workstation will be locked if it is removed.

The Microsoft network client section configures the computer to digitally sign communications when possible but does not require digitally signed communications. This also allows computers to talk to one another as securely as they can. User connections will be disconnected when a client's logon hours expire.

Under the Network access section, anonymous SID/Name translation has been disabled and anonymous enumeration of SAM accounts or shares has been disallowed. This prevents anonymous users from enumerating SIDs and from getting a list of domain accounts and shares. In addition, the Everyone group permissions do not apply to anonymous users.

In the Network security section, the LAN Manager hash value is not stored on the next password change. Because the LAN Manager hash is weak and easily compromised, it is not stored. Also, the force logoff when logon hours expire is enabled so that logon hours are enforced. Finally, LDAP client signing is required to negotiate signing when making LDAP calls.

The Recovery Console section does not allow an automatic administrative logon to the recovery console. This is so that if the server is brought up in recovery mode that the administrator password is required to have access to the console. Also, access to all drives or copy from a floppy is not allowed.

In the Shutdown section, the Clear virtual memory pagefile on shutdown is disabled. None of the workstations or servers are configured for dual boot so this should not be an issue.

In the System objects section, require case insensitivity for non-Windows subsystems and strengthen default permissions of internal system objects are both enabled. This allows case insensitive communication with non-Windows systems and increases the security on the default discretionary access control lists for objects.

Figure 17: Default Domain Policy – Event Log

Policy	Computer Setting
Maximum application log size	16384 kilobytes
Maximum security log size	16384 kilobytes
Maximum system log size	16384 kilobytes
Prevent local guests group from accessing application log	Enabled
Prevent local guests group from accessing security log	Enabled
Prevent local guests group from accessing system log	Enabled
Retain application log	7 days
Retain security log	7 days
Retain system log	7 days
Retention method for application log	By days
Retention method for security log	By days
Retention method for system log	By days

This section configures the event log settings. All event logs are configured the same: 16MB in size, not accessible by the local Guests group and allow the overwriting of events that are more than seven days old. This allows administrators to go back at least a week to review entries and allows for enough room to not have the log fill up except in the event of some sort of serious issue.

Figure 18: Default Domain Policy – Windows Components \ Net Meeting

Setting	State
Disable remote Desktop Sharing	Enabled

This setting prevents users from sharing out their desktops while using NetMeeting.

Figure 19: Default Domain Policy – Windows Components \ Internet Explorer

Setting	State
Disable Automatic Install of Internet Explorer components	Not configured
Disable Periodic Check for Internet Explorer software updates	Enabled
Disable showing the splash screen	Enabled
Disable software update shell notifications on program launch	Not configured
Make proxy settings per-machine (rather than per-user)	Not configured
Security Zones: Do not allow users to add/delete sites	Not configured
Security Zones: Do not allow users to change policies	Not configured
Security Zones: Use only machine settings	Not configured

These settings configure how Internet Explorer runs. The policy turns off the periodic checking of Internet Explorer updates so that the version all computers are running can be controlled. It also disables the splash screen strictly for cosmetic purposes.

Figure 20: Default Domain Policy – Windows Components \ Windows Update

Setting	State
Configure Automatic Updates	Enabled
No auto-restart for scheduled Automatic Updates installations	Enabled
Reschedule Automatic Updates scheduled installations	Enabled
Specify intranet Microsoft update service location	Enabled

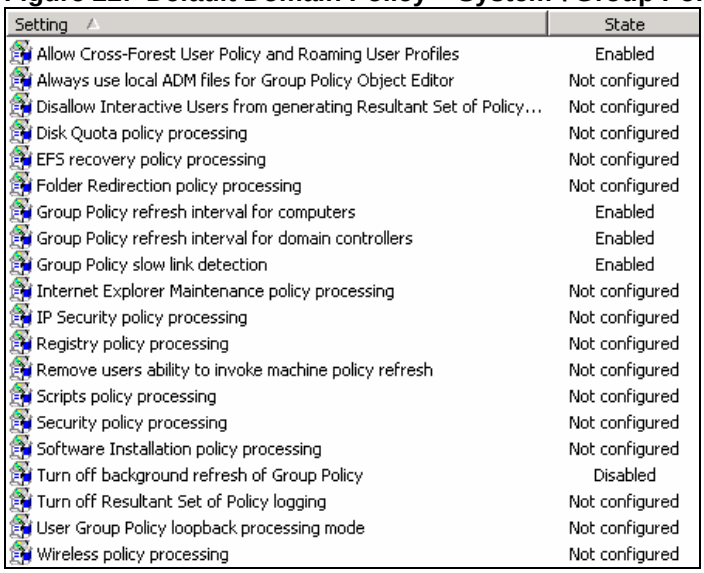
This section deals with the configuration of Windows Update. It configures all computers to use Windows Update but does not auto-restart any computers after updates have been applied. It also reschedules any missed updates five minutes after logging in. The final option specifies http://susserver as the local intranet site for getting updates. Each location has its own SUS server that downloads updates from the Internet. There is a DNS entry at each location for susserver that points to the local server. This allows for updates to be applied to all workstations running over the local network and not having all workstations connect to the Windows Update service across the Internet to download patches.

Figure 21: Default Domain Policy – System \ Logon

Setting	State
Always use classic logon	Not configured
Always wait for the network at computer startup and logon	Not configured
Do not process the legacy run list	Not configured
Do not process the run once list	Enabled
Don't display the Getting Started welcome screen at logon	Enabled
Run these programs at user logon	Not configured

This section of the policy disables the run once list and doesn't display the Getting Started welcome screen. The run once list is a hiding place for Trojans and is disabled to prevent it from being used for malicious reasons. Not displaying the Getting Started screen is done strictly for aesthetic reasons.

Figure 22: Default Domain Policy – System \ Group Policy



Setting	State
Allow Cross-Forest User Policy and Roaming User Profiles	Enabled
Always use local ADM files for Group Policy Object Editor	Not configured
Disallow Interactive Users from generating Resultant Set of Policy...	Not configured
Disk Quota policy processing	Not configured
EFS recovery policy processing	Not configured
Folder Redirection policy processing	Not configured
Group Policy refresh interval for computers	Enabled
Group Policy refresh interval for domain controllers	Enabled
Group Policy slow link detection	Enabled
Internet Explorer Maintenance policy processing	Not configured
IP Security policy processing	Not configured
Registry policy processing	Not configured
Remove users ability to invoke machine policy refresh	Not configured
Scripts policy processing	Not configured
Security policy processing	Not configured
Software Installation policy processing	Not configured
Turn off background refresh of Group Policy	Disabled
Turn off Resultant Set of Policy logging	Not configured
User Group Policy loopback processing mode	Not configured
Wireless policy processing	Not configured

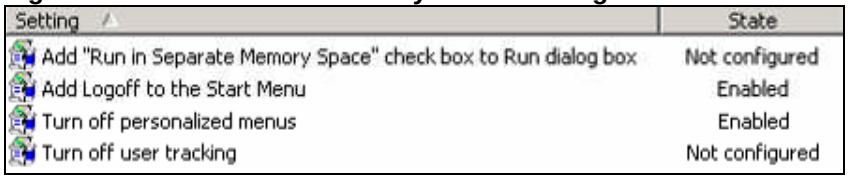
Cross-Forest User Policy and Roaming User Profiles allow users to login across forests and have user-based policy processing, roaming profiles and user object login scripts function. This has been enabled.

Group policy refresh interval is how often the computers refresh their group policy from the domain while the computer is in use. These updates happen in the background. Computers are configured to update their group policy every 90 minutes with a random offset of 30 minutes so all workstations don't attempt to refresh at the same time. Domain Controllers are configured to refresh their policies every 5 minutes. This is so any changes made to computer group policies will take effect even if the machine is not rebooted.

The group policy slow link detection is the network speed that a computer needs to be running to be considered a slow link. Some policies can be quite large and should not be deployed over a slow link like a dial-up connection. This setting is configured to consider any connection of less than 500Kbps a slow link.

Turn off background refresh of group policy is set to disabled. This ends up meaning that background refresh is enabled so that group policies are updated in the background.

Figure 23: Default Domain Policy – User Configuration \ Start Menu and Taskbar



Setting	State
Add "Run in Separate Memory Space" check box to Run dialog box	Not configured
Add Logoff to the Start Menu	Enabled
Turn off personalized menus	Enabled
Turn off user tracking	Not configured

These are the only User settings that are configured in the Default Domain Policy. The Logoff button is being added to the Start Menu so users can logoff

without accidentally shutting down. Also, personalized menus are being disabled so that all menu choices will be shown to the users.

2.1.4 SANS Co. OU Group Policies

This section will outline the key OUs where group policies are being applied. The OUs that have settings in addition to the Default Domain Policy are:

- Domain Controllers
- Domain Users
- Citrix Servers
- Web Servers

Below is listed the Default Domain Controllers, Domain Users and Web Servers policies to show how differences are applied.

Default Domain Controllers Policy

Figure 24 lists the settings enforced on Domain Controllers. It is a slightly more restrictive environment than the Default Domain Policy, which is to be expected.

Figure 24: Default Domain Controllers Policy

Access this computer from the network	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone
Act as part of the operating system	
Add workstations to domain	NT AUTHORITY\Authenticated Users
Adjust memory quotas for a process	BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Allow log on locally	BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Account Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Back up files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Bypass traverse checking	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone
Change the system time	BUILTIN\Server Operators, BUILTIN\Administrators
Create a pagefile	BUILTIN\Administrators
Create a token object	
Create permanent shared objects	
Debug programs	BUILTIN\Administrators
Deny access to this computer from the network	
Deny log on as a batch job	

Deny log on as a service	
Deny log on locally	
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators
Force shutdown from a remote system	BUILTIN\Server Operators, BUILTIN\Administrators
Generate security audits	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Increase scheduling priority	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Print Operators, BUILTIN\Administrators
Lock pages in memory	
Log on as a batch job	
Log on as a service	NT AUTHORITY\NETWORK SERVICE
Manage auditing and security log	BUILTIN\Administrators
Modify firmware environment values	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators
Profile system performance	BUILTIN\Administrators
Remove computer from docking station	BUILTIN\Administrators
Replace a process level token	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Restore files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Shut down the system	BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Synchronize directory service data	
Take ownership of files or other objects	BUILTIN\Administrators

Domain Controller: LDAP server signing requirements	None
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Microsoft Network Server: Digitally sign communications (always)	Enabled
Microsoft Network Server: Digitally sign communications (if client agrees)	Enabled

You will notice above that Domain Controllers do require all secure channel data to be digitally encrypted or signed. Also, all communication is required to be digitally signed to prevent man-in-the middle attacks.

Domain Users Policy

There were only a few additions made to the Default Domain Policy for the Domain Users OU. Figure 25 lists the settings that are configured in the Domain Users group policy:

Figure 25: Configured Domain Users Policy

Offer Remote Assistance	Enabled
Solicited Remote Assistance	Enabled
Do not add shares of recently opened documents to My Network Places	Enabled
Remove the Desktop Cleanup Wizard	Enabled
Prevent access to registry editing tools	Enabled
Prompt for password on resume from hibernate / suspend	Enabled
Do not allow AutoComplete to save passwords	Enabled

Internet Explorer Help menu: Remove “Tip of the Day” menu option	Enabled

The main purpose of this group policy is to refine the user’s experience and secure things a little more. The workstations are not completely locked down because of difficulties in allowing users to be able to complete their work so a compromise was made to leave the workstations a little more open.

A key point of the Domain User Policy is that Remote Assistance is enabled but only Domain Admins can perform remote assistance. This allows the Domain Admins to remotely assist users by controlling their computers.

The group policy also does not add shares for any recently opened documents to My Network Places to prevent the shares from being easily accessed by someone else sitting at the computer. Also, access to registry editing tools is being prevented. End users should not be poking around in the registry anyways, so this functionality was disabled. In addition, users can not save any passwords for websites with the AutoComplete feature of Internet Explorer once more so that if someone else is sitting at the computer they will not have easy access to potentially confidential material.

Web Servers Policy

The Web Servers Policy needs to be the most aggressive group policy because of the fact that the web servers are accessible from the Internet. There is a defense in depth philosophy being applied starting with the outside firewall, going through the ISA server and then using group policies to finely hone the security being applied to the web servers. There are a variety of web applications being hosted from simple, static web pages, sites for customers to place and review orders and a web server to allow Citrix access into the network using the Web Interface product.

The Default Domain Policy serves as a good foundation for locking down the web servers, however because of the exposure the web servers have it was decided to build on the Default Domain Policy by using the Microsoft Secure Internet Web Server template that is available in the Windows 2000 Resource Kit[13]. That template was then tweaked to provide the configuration that was deemed appropriate. Figure 26 lists the main modifications and important settings that resulted:

Figure 26: Configured Web Servers group policy

Local Policies \ User Rights Assignment	
Access this computer from the network	Everyone
Act as part of the operating system	
Add workstations to domain	BUILTIN\Administrators

[13] Microsoft Corporation. “Windows 2000 Server Resource Kit Tools.” Windows 2000 Resource Kit Overview. http://www.microsoft.com/windows2000/techinfo/reskit/rktour/server/S_tools.asp. (12 June 2004)

Adjust memory quotas for a process	BUILTIN\Administrators, NT
Allow log on locally	Web Server Admins, BUILTIN\Administrators
Back up files and directories	BUILTIN\Backup Operators, BUILTIN\Administrators
Bypass traverse checking	Everyone
Change the system time	Web Server Admins, BUILTIN\Administrators
Debug programs	BUILTIN\Administrators
Force shutdown from a remote system	Web Server Admins, BUILTIN\Administrators
Increase scheduling priority	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Administrators
Manage auditing and security log	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators
Restore files and directories	Web Server Admins, BUILTIN\Administrators
Shut down the system	Web Server Admins, BUILTIN\Administrators
Take ownership of files or other objects	BUILTIN\Administrators

Local Policies \ Security Options

Audit: Audit the use of Backup and Restore privilege	Enabled
Audit: Shut down system immediately if unable to log security audits	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Shutdown: Clear virtual memory pagefile	Enabled

Local Policies \ Event Log

Maximum application log size	262144 kilobytes
Maximum security log size	262144 kilobytes
Maximum system log size	262144 kilobytes

Restricted Groups

Administrators, Web Server Admins

System Services

Alerter	Disabled
ClipBook	Disabled
DNS Server	Disabled
Indexing Service	Disabled
Messenger	Disabled
NetMeeting Remote Desktop Sharing	Disabled
Remote Access Auto Connection Manager	Disabled
Remote Access Connection Manager	Disabled
Telnet	Disabled
Terminal Services	Disabled
Terminal Services Session Directory	Disabled
Themes	Disabled
Windows Audio	Disabled
Windows Image Acquisition (WIA)	Disabled

The User Rights Assignments have been configured to restrict access to the server for most things that would only need to be done by an administrator. To allow the web server to function properly, a couple of the options were configured

to allow access to the Everyone group, but that was just to allow access to the server and to traverse directories.

Under the Security Options section, the policy enables auditing of the backup and restore privilege to make sure that unauthorized backups or restores aren't taking place. It also restricts access to the CD-ROM and floppy drives to the locally logged-on user only. This prevents a rogue IT person from inserting a CD or floppy and connecting to the machine from a remote workstation and executing an application.

The event log settings were changed slightly to allow for a larger maximum size. This makes it more difficult for a hacker to cause a denial of server attack by filling the logs. It also makes it harder for a hacker to cover their tracks. Because disk space is not an issue, reserving 256MB per log is fine.

The restricted groups feature allows you to define and enforce who should be a member of specific groups. This feature locks down the group membership of the specified groups to the users and groups listed. It prevents unauthorized additions to the listed groups as well. The Administrators and Web Server Admins groups are defined as restricted groups and have memberships configured as needed.

The listed system services are not required for running any of the web services and to reduce the attack footprint they have been disabled.

In addition to the above settings, the Microsoft Secure Internet Web Server template locks down many registry keys and system files to secure the system even further.

2.2 Group Policy Validation Methods

For testing of group policies, an IIS server running Citrix Web Interface has been selected. Citrix Web Interface is a web application that allows authentication to the Citrix environment and the launching of Citrix applications from the web page.

The Web Interface application takes a user's login credentials, passes them to a back-end Citrix server for authentication and receives back a list of applications that are available for the user. It then displays to the user their available applications. The user then clicks on one of the available icons and an ICA session is started with the Citrix server.

There are several ways to verify that the group policies are being applied. The few that will be used for this example are:

- Receive the initial banner warning message
- Verify that the last logged in user is not displayed

- Attempt to login to the system as a non-administrative user and fail
- Check that all services that were flagged as disabled are disabled
- Run the RSOP.MSC command to see what policies are being applied

After verification of the group policies, I will then prove functionality of the web server still exists by logging into the Citrix Web Interface as a normal (non-administrative) user and launching a Citrix application.

I expect to see policies being applied by the Default Domain Policy, Domain Users Policy and the Web Servers Policy. I also expect to be able to log in to the Citrix Web Interface, receive the list of applications for my user and be able to launch any of the applications. To prove that the group policies are working but not affecting the web server, I will provide screenshots of the following:

- Logon banner with warning text
- Logon box with no user name
- Failed login attempt as a normal user
- Listing of disabled services
- A sampling of the RSOP.MSC results that shows multiple policies applied
- Web Interface application listing with a running Citrix application

2.3 Group Policy Application

The machine group polices are applied at startup and then get refreshed every 90 minutes with a 30 minute offset. Because the policies don't change frequently, this was considered to be adequate.

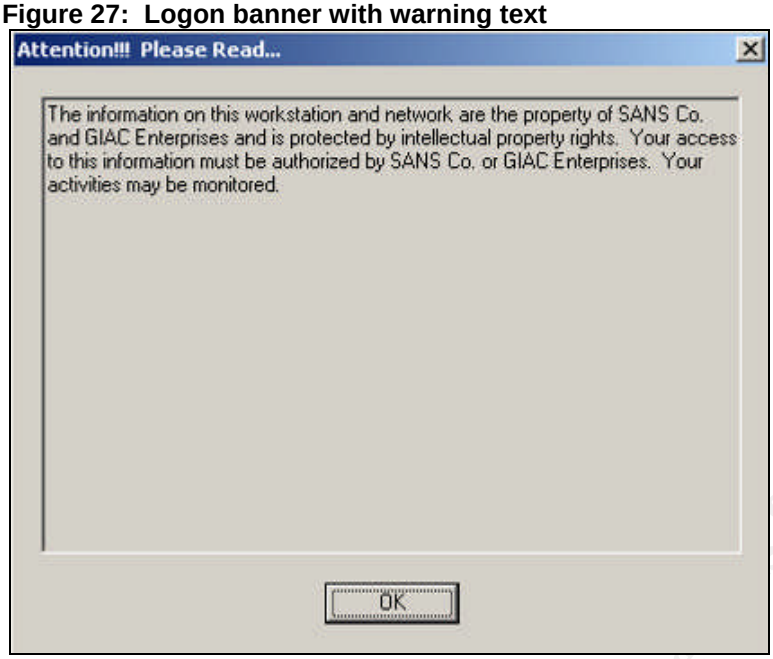
User policies are applied at login and also refreshed every 90 minutes with a 30 minute offset. As with the machine policy, the policies don't change that often and this time frame was considered adequate.

The command line tool GPUpdate can also be used to refresh the group polices. When used with the /Force switch it applies all polices that have changed. One thing to note is that the GPUpdate tool can also be run against a remote workstation to force a group policy update through a script if needed.

2.4 Group Policy Functionality Testing

The group policies did apply properly and the Web Interface application worked flawlessly. When first logging in to the server I received the initial banner with the warning text. Figure 27 shows the complete banner:

Figure 27: Logon banner with warning text

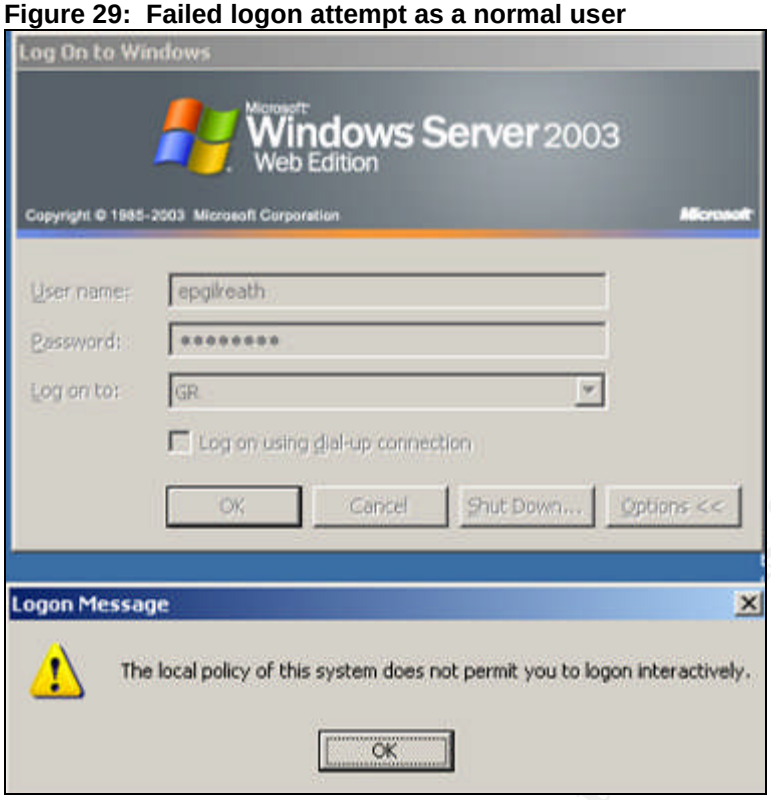


I then cleared the message and found that the logon box did not display any name. Figure 28 shows the logon box:

Figure 28: Logon box with no user name

I then attempted to logon with the "epgilreath" user account. That account is a member of the Domain Users OU in gr.sans.org. When attempting to login I received an error stating that I was not allowed to logon. Figure 29 shows the login attempt and error:

Figure 29: Failed logon attempt as a normal user



I then logged in successfully as a member of the local Administrators group. After logging in I verified that the services that were configured as disabled were indeed, disabled. Figure 30 shows the disabled services:

Figure 30: Listing of disabled services

After verifying the services, I ran RSOP.MSC from the run command to list the policies that were being applied. I verified that the policies from the Default Domain Policy, Domain User Policy and the Web Servers Policy were being applied. Figure 31 shows samples displaying all three policies being applied:

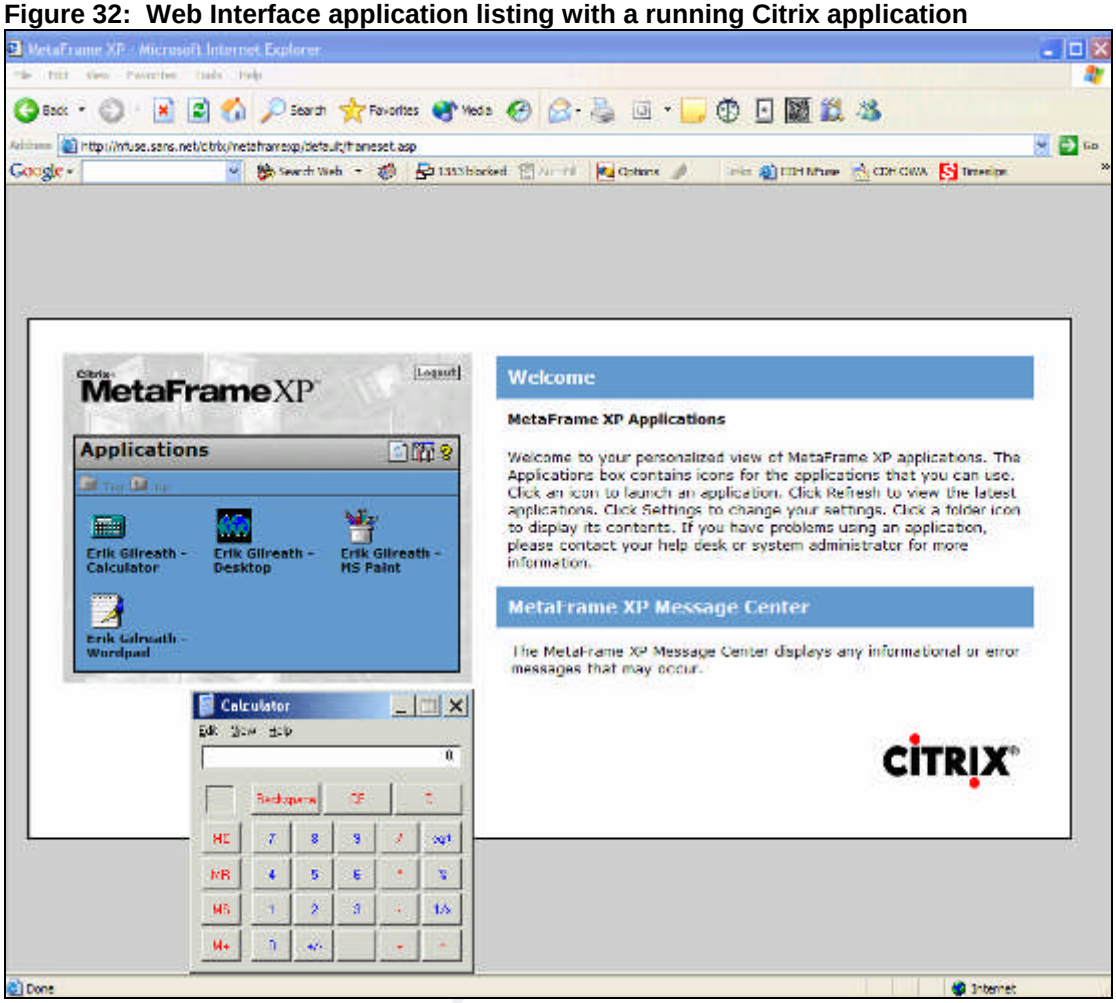
Figure 31: Sampling of RSOP.MSC results

Policy	Computer Setting	Source GPO
Accounts: Administrator account status	Not Defined	
Accounts: Guest account status	Disabled	Default Domain Policy
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Default Domain Policy
Accounts: Rename administrator account	Not Defined	
Accounts: Rename guest account	Not Defined	
Audit: Audit the access of global system objects	Disabled	Default Domain Policy
Audit: Audit the use of Backup and Restore privilege	Enabled	Web Servers Policy
Audit: Shut down system immediately if unable to log security audits	Enabled	Web Servers Policy
Devices: Allow undock without having to log on	Disabled	Default Domain Policy
Devices: Allowed to format and eject removable media	Administrators	Default Domain Policy
Devices: Prevent users from installing printer drivers	Not Defined	
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled	Web Servers Policy
Devices: Restrict floppy access to locally logged-on user only	Enabled	Web Servers Policy
Devices: Unsigned driver installation behavior	Warn but allow installation	Default Domain Policy
Domain controller: Allow server operators to schedule tasks	Not Defined	
Domain controller: LDAP server signing requirements	Not Defined	
Domain controller: Refuse machine account password changes	Not Defined	
Domain member: Digitally encrypt or sign secure channel data (always)	Disabled	Default Domain Policy
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	Default Domain Policy
Domain member: Digitally sign secure channel data (when possible)	Enabled	Default Domain Policy
Domain member: Disable machine account password changes	Disabled	Default Domain Policy
Domain member: Maximum machine account password age	30 days	Default Domain Policy
Domain member: Require strong (Windows 2000 or later) session key	Disabled	Default Domain Policy
Interactive logon: Do not display last user name	Enabled	Default Domain Policy
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	Default Domain Policy

Setting	State	GPO Name
Do not add shares of recently opened documents to My Network Places	Enabled	Domain Users Policy
Remove the Desktop Cleanup Wizard	Enabled	Domain Users Policy

Finally, I logged into the Citrix Web Interface and launched an application to verify that the web server was functioning properly. Figure 32 is a screen shot showing the Web Interface page displaying the available applications and the Citrix application Calculator running:

Figure 32: Web Interface application listing with a running Citrix application



2.5 Group Policy Evaluation

As was documented in section 2.4, the group policies are being deployed correctly and still allowing the application to run as expected. Being able to lock down the server through group policies allows changes to be made easily across many computers so it is a very efficient way to lock down systems.

I feel that the designed group policies are strong enough to accomplish what they are designed to do, that is to keep the systems protected from malicious attacks. At this point there are no special applications requiring any modifications to the group policies, but modifications could easily be handled through the creation of additional OUs and application of a slightly modified group policy.

One note about group policies though, you need to make sure to have a good test lab environment to be able to accurately and thoroughly test all group policies before deploying them. With the great power of group policy comes the great responsibility to use it wisely. If you are not careful, you could easily

disable an entire organization accidentally. Remember to test, test, test – then deploy.

3.0 Audit

Auditing is an important, yet frequently overlooked part of a network environment. Usually, once everything is in place you are so happy that everything is working that you forget that it might fail some day. Or worse, that it might fail because someone intentionally breaks it. Auditing allows you to monitor the systems and be aware when something is either about to fail or has just failed. It allows you to be proactive and not necessarily reactive in the network environment.

SANS Co. thought long and hard about what auditing system to implement. They wanted to be able to monitor all systems, however they did not want to flood the engineers and help desk staff with so much data that things got missed, or even worse, ignored all together. They needed to be able to monitor infrastructure (routers, switches, etc…), servers, workstations, and Active Directory. They needed applications that were flexible, robust yet didn't raise an alarm to people with every little change to the environment. With that in mind, an auditing strategy was created to describe what events would be monitored and audited.

The audit strategy consists of the following:

- Physical access – this covers access into buildings, server rooms and wiring closets through use of card readers. Card readers will log all uses. Video surveillance will be used in locations where it is deemed necessary.
- Network devices – gathering of SNMP logs, monitoring of systems and hardware status to verify systems are on-line and responsive.
- Servers – monitoring of event logs, installed applications, performance metrics and hardware status.
- Workstations – monitoring of event logs, installed applications and hardware status.
- Active Directory – monitoring of overall Active Directory health.

The following software packages will assist in achieving the auditing plan:

- Microsoft Operations Manager 2000 (MOM)
- WhatsUp Gold
- Microsoft Systems Management Server 2003 (SMS)
- Dell Open Manage

The remainder of this section will discuss how the use of the above applications will achieve the stated audit strategy.

3.1 Event Log Management

SANS Co. wanted to consolidate logs as much as possible to avoid sending large quantities of data across the Internet pipes. It was decided to use MOM to gather various event logs and to maintain a MOM server at each location. This would allow the logs for all to be gathered at each location and backed up.

A scheduled SMS job is run on all workstations to copy their event logs to a central location and backed up nightly. The job keeps a total of 3 days of logs in the central storage for ease of access if a log needs to be reviewed.

The Cisco PIX, routers and switches run MOM agents that are being used to monitor the infrastructure logs and performance so that all the information is gathered together in one spot.

3.2 Performance Data

It is important to be able to monitor and track the performance of various systems. However, the SANS Co. IT staff is made up of people who specialize in different areas. They include the following groups:

- Server Team
- Workstation Team
- Infrastructure Team

Because of the diversity between groups, each team does not really know or use the tools that the other teams use. MOM is a great utility for the Server Team because it lets them know what's going on with the servers and Active Directory. However, it gives the Workstation and Infrastructure teams more information than they really need to do basic monitoring of their systems. That is why WhatsUp Gold and SMS are used.

3.2.1 Server Team

The Server Team relies heavily on MOM for auditing and monitoring of the server and Active Directory environment. MOM does a great job of gathering information and is highly customizable so that alerts can be sent when certain thresholds are met. So when a domain controller is running at 95% processor utilization for 20 minutes, someone can be notified and react accordingly.

There are alerts that have been configured in the MOM system to let the Server Team know when there are problems or pending problems with servers or Active Directory. These alerts are reviewed on a quarterly basis to see if additional alerts need to be added or current alerts need to be adjusted or removed. MOM is also monitoring the infrastructure systems and there are rules associated with the Infrastructure Team for the infrastructure devices.

The Server Team also uses the Dell OpenManage software on all the servers to report SNMP data to local OpenManage servers at each location. This allows the local Server Team to monitor the hardware health of each server at their location and to be alerted if a drive is failing, a power supply needs replacing or any other hardware ailments.

3.2.2 Workstation Team

The Workstation Team primarily uses SMS for the monitoring of workstations. SMS is a powerful tool that allows the Workstation Team to inventory, monitor, deploy applications to and even remote control workstations. SMS is also used to deploy Microsoft Office Updates and Windows Updates that aren't handled by the Microsoft SUS servers.

3.2.3 Infrastructure Team

The Infrastructure Team receives alerts from MOM and uses MOM for data collection, however, they rely most heavily on WhatsUp Gold for current health of the infrastructure environment. Each data center has a large monitor with a network diagram showing the network infrastructure environment using WhatsUp Gold. If any location becomes unresponsive, the system changes from green to yellow to red and emits a siren sound to alert the infrastructure team. The graphical representation is a powerful method to easily see the health of the network.

MOM is used for gathering performance data and traffic patterns and some of the Infrastructure Staff is trained on using MOM to review the gathered data and to assist in creating the various thresholds for alerts to be sent. As with the Server Team, the alert rules are reviewed on a quarterly basis and changes are made as needed.

3.3 Security Reviews

SANS Co. has some pretty bright people on staff, however they can't handle all aspects of security. That is why it was decided to have an independent security review completed every six months at each location. These reviews consist of a vulnerability analysis both external and internal, search for unauthorized wireless access points, hubs and switches, as well as make recommendations based on best practices. The SANS Co. IT staff take the recommendations and secure the environment as much as possible while still allowing all users and applications to function.

4.0 Summary

As was shown in this paper, SANS Inc. started with a firm, robust infrastructure with their partnership with Cisco. They built on that by installing Dell workstations and servers running Windows XP and Windows Server 2003 respectively. They took the time to configure a flexible Active Directory environment and locked down the system using group policies. They will continue to monitor and audit the environment to ensure a secure network.

By taking care to design a solid, robust environment and watch it closely, SANS Co. and GIAC Enterprises' fortune sees a long and fruitful computing future ahead of them, inspected by MOM.

5.0 References

1. Depp, Dennis. "Security Plan for GIAC Enterprises." GCNT Practical Assignment Version 3.0. 30 Jan. 2002. <http://www.giac.org/practical/Dennis_Depp_GCNT.doc>. (7 April 2004).
2. Microsoft Corporation. "Microsoft Knowledge Base Article – 197132." Windows 2000 Active Directory FSMO Roles. 05 Apr. 2004 <http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132>. (16 May 2004).
3. Penton Media, Inc. JSI FAQ. "JSI Tip 3654." Don't locate the Infrastructure Master and Global Catalog on the same server in a multi-domain forest. <http://www.jsiinc.com/SUBH/tip3600/rh3654.htm>. (16 May 2004).
4. Microsoft Corporation. "Technologies Collections – Active Directory Collection." Microsoft Windows Server 2003 Technical Reference. <http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/techref/en-us/w2k3tr_ad_over.asp>. (16 May 2004).
5. Fosh Australia Pty Ltd. "Private IP addresses for use on internal networks." Vicom Technology – VICOM Internet Gateway FAQ's / Text. <http://www.fosh.com.au/Fosh/Support/vi/privateip.html>. (16 May 2004).
6. Microsoft Corporation. "Wide Area Systems and Services – What's Cooking With T1 Bandwidth?" Microsoft Tech Net. 15 Jun. 1997. <http://www.microsoft.com/technet/prodtechnol/winntas/evaluate/featfunc/cmpt1.mspx>. (16 May 2004).
7. Cisco Systems. "Cisco PIX 506E Security Appliance." Cisco PIX 500 Series Firewalls. <http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b13.html>. (16 May 2004).
8. Holme, Dan and Thomas, Orin. Upgrading Your Certification to Microsoft Windows Server 2003. Redmond: Microsoft, 2004. 1-41.
9. Microsoft Corporation. "Predefined Security Templates." Microsoft Windows Server 2003 Standard Documentation. <http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/sag_SCEdefaultpols.asp>. (12 June 2004)
10. Microsoft Corporation. "Password must meet complexity requirements." Microsoft Windows Server 2003 Enterprise Documentation. <http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/504.asp>. (12 June 2004)
11. Fossen, Jason. Windows 2000/XP/2003 Active Directory. (SANS Institute, 2003) 39.
12. Microsoft Corporation. "Setting Clock Synchronization Tolerance to Prevent Replay Attacks." Microsoft Windows Server 2003 Deployment Guide. <http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dsscc_aut_qwwi.asp>. (12 June 2004)
13. Microsoft Corporation. "Windows 2000 Server Resource Kit Tools." Windows 2000 Resource Kit Overview. http://www.microsoft.com/windows2000/techinfo/reskit/rktour/server/S_tools.asp. (12 June 2004)