Global Information Assurance Certification Paper

SANSGIAC
Enterprise Consolidation

Arnold H. Buursink
GCWN Practical Assignment
Version 3.2, Option 1
January 2 , 2004

ABSTRACT

SANS Co. has recently received substantial funding through a profitable public offering to expand their operations throughout the United States. SANS Co. finalized the acquisition of GIAC Enterprises and is in the process of merging the IT infrastructures of the two companies. Both companies rely heavily on the Microsoft operating system for both client and server side operations. The first section of this paper will examine the effects of merging the existing Microsoft forests and domains. The second section will discuss the implementation of security policies in an effort to standardize and centralize security across the merged companies. The last section will cover the need for a system auditing plan to keep administrators and managers informed of possible security breaches, system failures or improper configurations.

Table of Content s

Table of Figures

1 SANS GIAC Merger

1.1 OVERVIEW

SANS Co. (SANS) is a popular brewery with a significant market share within the mid Atlantic states. SANS is located in the valley of the Shenandoah Mountains and employs 200 persons. SANS manages the business operations from the company headquarters while the actual beer production is done at a separate nearby facility. Having completed five strong years of profitable growth, SANS made a strategic initiative to offer public stock in an effort to fund additional expansion. After a successful public offering, SANS was able to purchase the struggling GIAC Enterprises (GIAC). GIAC, a national beverage distributor, has lost most major contracts due to poor management and problems with its distribution chain. In negotiations with SANS, GIAC was able to have the deal look more like a merger than an acquisition.

GIAC employs 1,250 persons throughout its 5 distribution cente rs and owns a fleet of 50 trucks. GIAC will offer SANS immediate distribution channels throughout the remainder of the US. Some GIAC senior management positions will be rep laced by SANS executives who will join the existing 200 staff members at the SANS company headquarters. GIAC former contracts department will bear the greatest loss, as all positions will be dissolved.

As the two companies merge, special considerations ne ed to be taken into account when aggregating information systems. Because of management 's desire to leverage existing systems across company borders, security to protect proprietary data will become a top priority. The following sections will discuss the s ecurity measures required to allow SANS and GIAC to merge resources.

1.2 SANS INFRASTRUCTURE

SANS has achieved success through competent and energetic management that strives for excellence in all aspects of its business. SANS is headquartered in Harrisonburg, Virginia. 150 persons work at the co mpany headquarters with the remaining 50 working 10 miles away at the Elkton, Virginia brewing plant. All SANS technical support staff are located at the Harrisonburg office complex.

1.2.1 Network Design

The SANS network i nfrastructure uses private IP addressing for internal workstations and servers. Subnets are depicted in Figure 1-1. The Harrisonburg facility incorporates Foundry Ne tworks Fast Iron series switches on each of the three f loors, providing 100 Mbps to the des ktop. Each floor switch has a fiber uplink to a Foundry Big Iron core switch creating a SANS 1 Gbps backbone. Also attached to the core switch is another Foundry Big Iron gigabit switch providing connectivity to the servers.

Because of service problems, SANS headquarters is connected to the Internet via redundant, d edicated T1 lines. Separate ISP s provide the leased lines in an effort to increase fault tolerance. A Cisco PIX 515E firewall protects the internal network and forms the demilitarized zone (DM Z). DMZ's are commonly known for the portion of a

corporate network that has been segregated and made available to the Internet. The firewall also allows remote users to connect to corporate resources through IPSec tunnels.

The Elkton office is linked to the Internet via a single 256 Kbps SDSL connection. A Cisco PIX 506E firewall protects the Elkton internal LAN and creates a 3DES VPN with SANS headquarters.

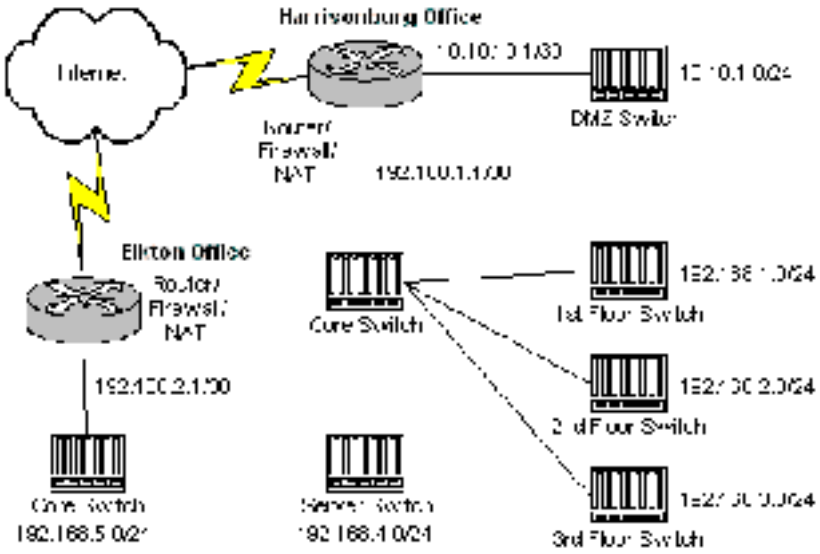


Figure 1-1 Network Diagram

Server host names are registered in Windows 2003 Active Directory Integrated DNS. DNS zone delegation is consistent with the domain structure. Client host names are registered in DNS through DHCP with dynamic updates. In order for DHCP clients to become the owner of DNS records at a later time, SANS administrators added the DHCP server to the DNSUpdateProxy global group. With the DHCP server added to the global group, new records will not have an owner until the first time they are modified. Following best practices, the DHCP server has been installed on a pair of Windows 2003 member servers rather than a domain controller. DHCP relay agents have been installed on all internal subnets. SANS has had problems with employees connecting personal, non-secure, systems to the corporate network. To solve the problem, all IP addresses have been reserved and require an administrator to issue a lease to an approved MAC address.

1.2.2 Domain Structure

SANS recently upgraded all servers to Windows 2003 and is currently running the Windows 2000 native domain functional level. After testing has been completed to verify that the domain controllers are operating as expected, the domain functional level will be raised to Windows 2003 on all domains. Thereafter, the forest functional level will also be raised to Windows 2003.

A separate Active Directory (AD) site has been established containing subnets from the Elkton office. An IP based site link has been configured and will utilize the existing VPN tunnel to transfer traffic securely. AD replication has been limited to evening hours between 5pm and 8am. In the event that password changes at the

Elkton office are made during non-replication hours, authentication requests will be forwarded to the domain controller holding the PDC emulator Flexible Single Master (FSMO) role located at headquarters.

SANS is comprised of four domains. Figure 1-2 depicts the domain layout. The top-level root domain (*sans.com)* does not contain any employee user or computer accounts and is strictly utilized for schema and forest modification. The user accounts are split between three child domains, the marketing/sales domain *(ms.sans.com)*, the R&D/Production (RDP) domain (*rdp.sans.com*) and the Corporate/HR domain (*chr.sans.com*). Aside from the empty root domain, the current domain structure is a direct reflection of the previous NT 4.0 architecture. No attempts where made to consolidate domains when the systems were upgraded mainly because the network administrators did not have a strong understanding of group policies and delegation.

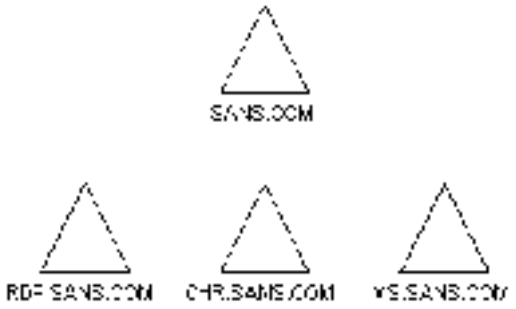


Figure 1-2 SANS Domain Structure

The FSMO holders are spread over various domain controllers located at SANS headquarters. The schema master and domain naming master roles are both located on a single (sans.com) root domain controller. The same domain controller also hosts the domain based roles that include; relative ID master (RID), PDC emulator and infrastructure master. The remaining three child domains only host domain based roles. Each domain has two controllers. Following Microsoft best practices, the PDC emulator and RID master as hosted on one and the infrastructure master is hosted on the other. Since all domain controllers host the global catalog (GC), there is no need to separate it from the infrastructure master role. The Elkton office has its own domain controller that only holds the GC. To ensure that the FSMO roles are properly distributed, Administrators use Ntdsutil.exe. (3)

SANS network administrators rely heavily on AD to centralize administration and impose security restrictions. The Organizational Unit (OU) structure is consistent across domains to reduce administration. The OU structure is illustrated in Figure 1-3. OU's were architected to coincide with the deployment of group policies. SANS has imposed domain level security policies on the three child domains. The domain policies control security settings that are applied to all objects within the domain. They are high-level settings that set the overall security standard for the domain. The ms.sans.com and chr.sans.com domains have similar domain policies. However, the rdp.sans.com domain has a slightly different policy that places more stringent requirements on password length. The higher password settings for rdp.sans.com are not mandatory, but are simply a result of carrying over the previous NT 4.0 password settings, which were haphazardly set by administrators of that domain. Some of the settings imposed at the domain level include: password restrictions;

account lockout settings; restrictions on who can access the computer from the network and locally; renaming of administrator and guest accounts; event log configuration settings; warning banners that are displayed at logon; auditing settings; restricted services; and modifications to registry and folder permissions. More detailed settings are discussed later in this paper. At the server OU level, multiple policies have been created that are more in line with the functions of the objects within the OU. The policies implement best practice lock down methods for the various types of server functions. For example, the Intranet IIS OU will implement security settings that prevent malicious users from modifying web content or using web servers as a gateway to the corporate network. The Citrix OU has a desktop lockdown policy, which prevents users from modifying system settings. Settings for the lockdown policy can be found in Section 1.2.3. The remaining group policy is attached to the Staff Members OU. Its primary function is to facilitate the deployment of applications.

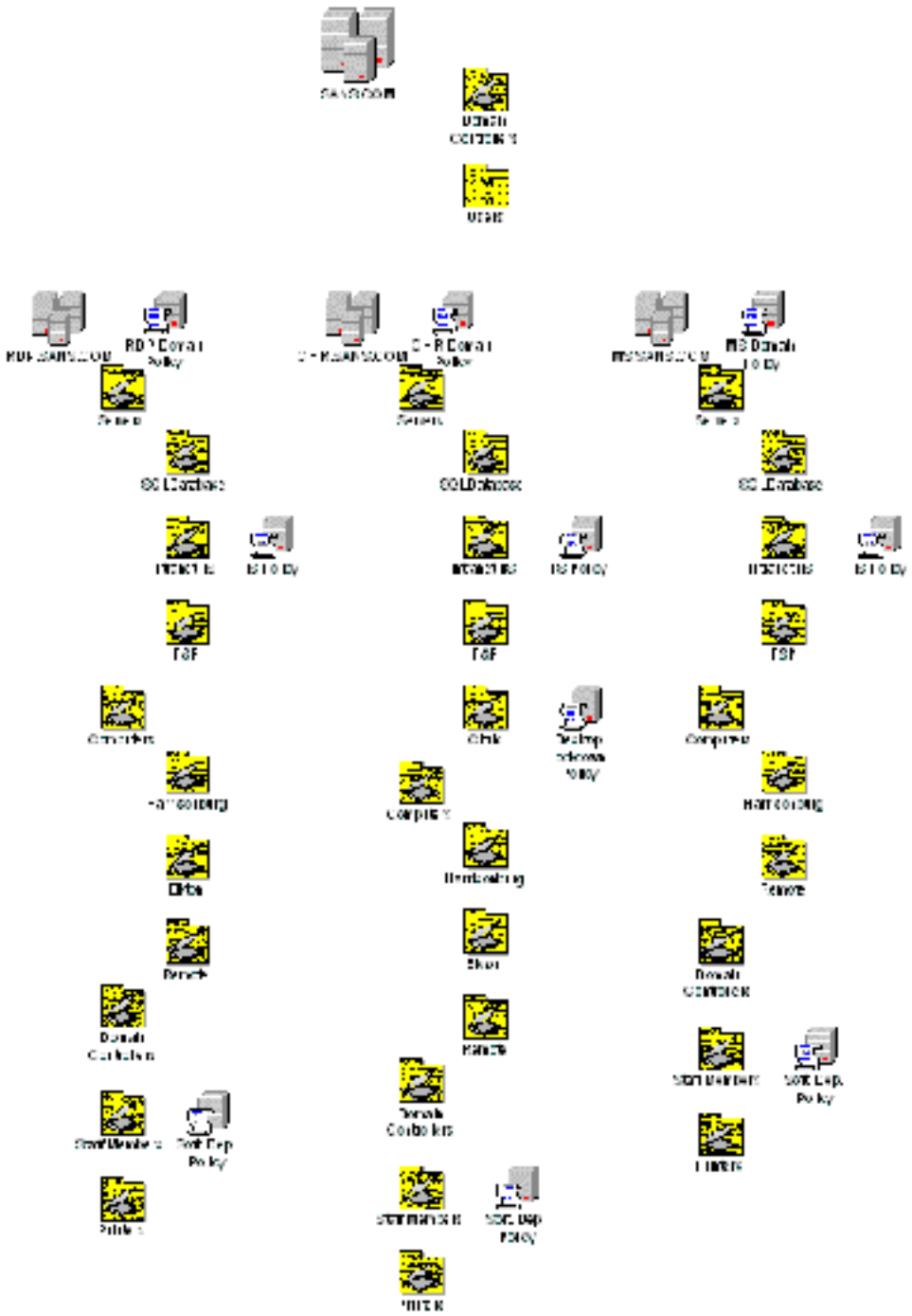


Figure 1-3 SANS OU Structure

Given the similarity in OU and Group Policy structures, SANS is considering a consolidated architecture that would combin e the three child domains. The consolidation is *not* scheduled to take place prior to the merger with GIAC. There are no distinct requirements that necessitate having separate domains. The usual reasons for having multiple domains, including political and u ser policy, do not exist within the SANS organization. Roles previously held by lower level domain administrators could be delegated to the appropriate Active Directory containers. Consolidating the computer and user objects will not have an adverse effect on overall security as the current settings are very similar between domains. Creating a single domain will relieve a great deal of administrative overhead necessary to

maintain multiple domains and security policies. Figure 1 -4 illustrates what the consolidated domain will look like. The domains are consolidated into a single internal.sans.com domain. This domain will remain a child of the sans.com empty root domain. All servers are consolidated into like kind OUs. The computer o bjects are placed in OU s based on physical location. Administrators reviewed the variations between the server group policies and modified the consolidated one according to the company's security policy. The users are separated by job function, much like what was done previously . Instead of a single Software Deployment Policy, multiple policies are created for each business segment

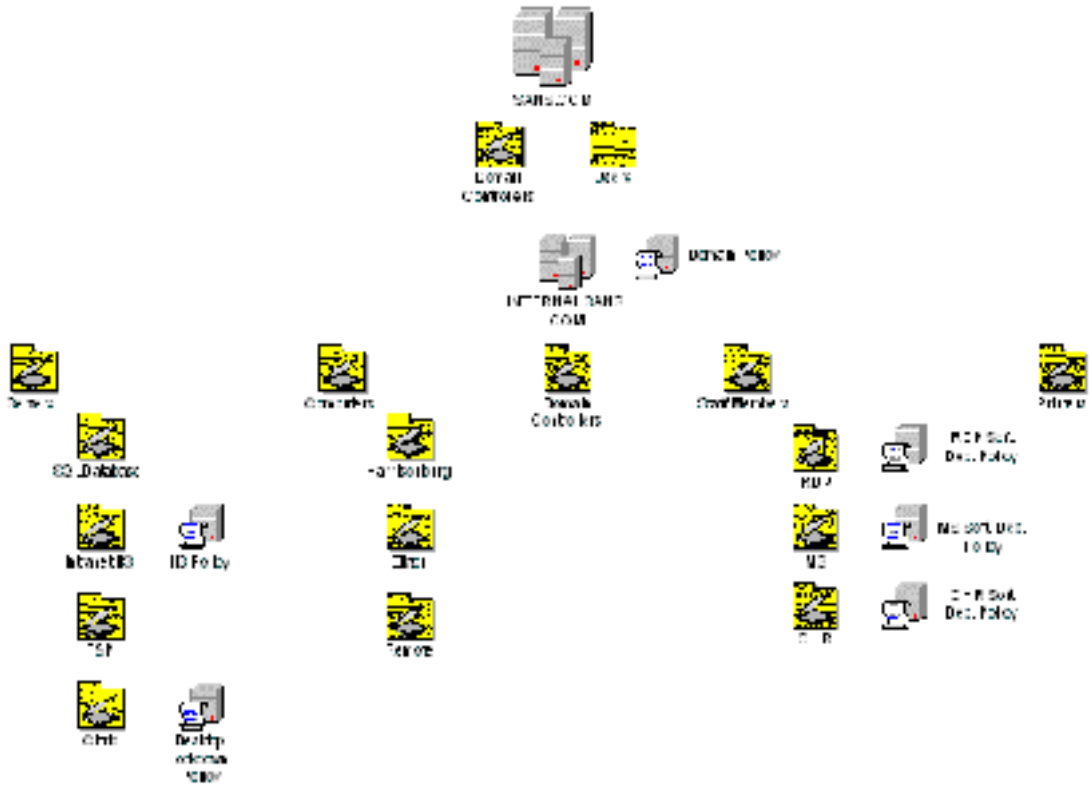


Figure 1-4 Proposed OU Struc ture

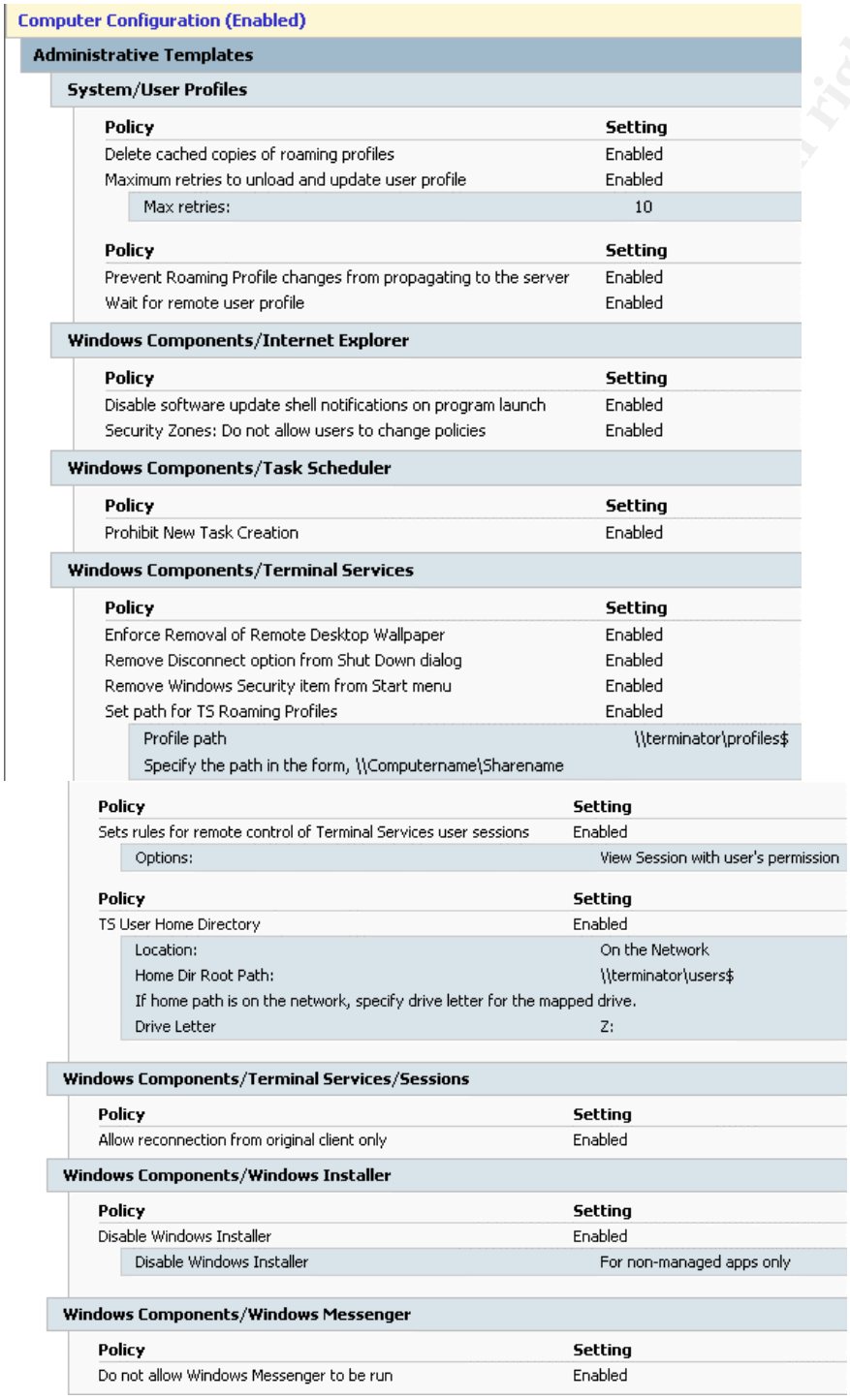
SANS chose not create a separate forest for the DMZ. All systems w ithin the DMZ are standalone Windows 2003 servers. Given the small number of servers within the DMZ, security policies are applied manually to each server and monitored through a third party utility discussed later in this paper. To protect communication w ithin the DMZ, all traffic is transmitted using IPSec. Name resolution for DMZ servers is performed by two external DNS servers configured on Sun Solaris boxes using BIND. The external DNS does not contain records of internal hosts.

1.2.3 Clients

All SANS emp loyees utilize thin clients with embedded Windows XP and the Citrix ICA client to acces s corporate applications. The limited operating system significantly reduces the cost necessary to secure and update local workstations. SANS uses a version of embedded XP that was modified by an external company. The modified version includes all binaries necessary to implement policy based security configuration. The thin clients have a Netscape web browser and ICA client

installed. Applications are published only to th ose users who require them and are accessed using Citrix Program Neighborhood shortcuts located on the desktop and Start menu.

The five Citrix Metaframe servers supporting client applications are “locked down” and secured using Group Policies. All Metafr ame servers are place in a separate OU so that more stringent security and desktop settings can be easily implemented and modified. To prevent the policy from being applied to systems administrators the “Apply Group Policy” setting within the properties d ialog box is set to Deny. The security p olicy settings are detailed in F igure 1-5.



Computer Configuration (Enabled)

Administrative Templates

System/User Profiles

Policy	Setting
Delete cached copies of roaming profiles	Enabled
Maximum retries to unload and update user profile	Enabled
Max retries:	10

Policy	Setting
Prevent Roaming Profile changes from propagating to the server	Enabled
Wait for remote user profile	Enabled

Windows Components/Internet Explorer

Policy	Setting
Disable software update shell notifications on program launch	Enabled
Security Zones: Do not allow users to change policies	Enabled

Windows Components/Task Scheduler

Policy	Setting
Prohibit New Task Creation	Enabled

Windows Components/Terminal Services

Policy	Setting
Enforce Removal of Remote Desktop Wallpaper	Enabled
Remove Disconnect option from Shut Down dialog	Enabled
Remove Windows Security item from Start menu	Enabled
Set path for TS Roaming Profiles	Enabled
Profile path	\\terminator\profiles$
Specify the path in the form, \\Computername\Sharename	

Policy	Setting
Sets rules for remote control of Terminal Services user sessions	Enabled
Options:	View Session with user's permission

Policy	Setting
TS User Home Directory	Enabled
Location:	On the Network
Home Dir Root Path:	\\terminator\users$
If home path is on the network, specify drive letter for the mapped drive.	
Drive Letter	Z:

Windows Components/Terminal Services/Sessions

Policy	Setting
Allow reconnection from original client only	Enabled

Windows Components/Windows Installer

Policy	Setting
Disable Windows Installer	Enabled
Disable Windows Installer	For non-managed apps only

Windows Components/Windows Messenger

Policy	Setting
Do not allow Windows Messenger to be run	Enabled

User Configuration (Enabled)

Windows Settings

Folder Redirection

My Documents

Setting: Basic (Redirect everyone's folder to the same location)

Path: \\terminitor\documents$\%USERNAME%\My Documents

Options

Grant user exclusive rights to My Documents	Enabled
Move the contents of My Documents to the new location	Enabled
Policy Removal Behavior	Leave contents

Administrative Templates

Control Panel

Policy	Setting
Prohibit access to the Control Panel	Enabled

Desktop

Policy	Setting
Hide Internet Explorer icon on desktop	Enabled
Remove Properties from the My Computer context menu	Enabled
Remove Properties from the My Documents context menu	Enabled
Remove Recycle Bin icon from desktop	Enabled

Desktop/Active Desktop

Policy	Setting
Disable Active Desktop	Enabled
Disallows HTML and Jpg Wallpaper	

Network/Network Connections

Policy	Setting
Prohibit access to properties of components of a LAN connection	Enabled

Start Menu and Taskbar

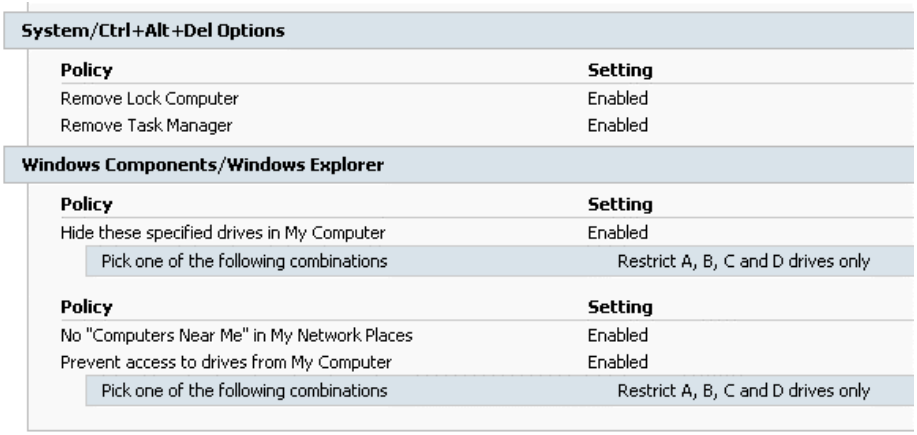
Policy	Setting
Add Logoff to the Start Menu	Enabled
Clear history of recently opened documents on exit	Enabled
Remove and prevent access to the Shut Down command	Enabled
Remove common program groups from Start Menu	Enabled
Remove links and access to Windows Update	Enabled
Remove Network Connections from Start Menu	Enabled
Remove Run menu from Start Menu	Enabled

System

Policy	Setting
Don't display the Getting Started welcome screen at logon	Enabled
Prevent access to registry editing tools	Enabled
Prevent access to the command prompt	Enabled
Disable the command prompt script processing also?	Yes

Policy	Setting
Run only allowed Windows applications	Enabled

List of allowed applications
BigSales.exe
calculator.exe
excel.exe
netscape.exe
winexplorer.exe
winword.exe



System/Ctrl+Alt+Del Options	
Policy	**Setting**
Remove Lock Computer	Enabled
Remove Task Manager	Enabled
Windows Components/Windows Explorer	
Policy	**Setting**
Hide these specified drives in My Computer	Enabled
Pick one of the following combinations	Restrict A, B, C and D drives only
Policy	**Setting**
No "Computers Near Me" in My Network Places	Enabled
Prevent access to drives from My Computer	Enabled
Pick one of the following combinations	Restrict A, B, C and D drives only

Figure 1-5 Citrix Server OU Group Policy

Individuals accessing applications on Citrix servers are relegated to User level security privileges and are not able to modify most of the Windows environment. All Metaframe servers utilize McAfee Virus Scan for virus detection. All SANS servers including the Citrix Metraframe servers are updated and patched using Patchlink.

Internal workstations connect directly to Citrix Metaframe servers utilizing a full ICA client installed on the local thin device. To accommodate traveling users, SANS has implemented a DMZ. It provides a web based Citrix application portal that allows traveling employees to access applications from any Internet enabled device through a 128-bit SSL connection. The x.509 certificate utilized for the SSL connection was obtained from Entrust, a widely trusted Certificate Authority, with public keys already configured in the latest releases of Netscape web browser. The DMZ consists of two Windows 2003 standalone servers running IIS and Citrix NFuse Elite. The recently upgraded servers allow SANS to take advantage of new security features within IIS 6.0. Some of those features include IIS being installed by default in a "locked down" state and only presenting dynamic pages if explicitly configured to do so. In addition, IIS worker process runs in a low-privileged user context by default. IIS 6.0 also prevents anonymous users from overwriting web content. Additional information on the new features within IIS 6.0 can be found in a document entitled "Technical Overview of Internet Information Services (IIS) 6.0", available from Microsoft's web site (7).

Currently, SANS employs their primary ISP to provide all email services. Users access email through Netscape mail clients using the IMAP protocol. SANS hopes to implement their own Microsoft Exchange environment, relieving the need for outsourcing. Management hopes to leverage scheduling and collaboration features within Exchange across the SANSGIAC enterprise.

1.3 GIAC INFRASTRUCTURE

GIAC's network architecture is considerably more distributed then SANS. GIAC employees are located at various distribution plants around the country. For the purposes of this paper, the network design for GIAC will be obtained from GCWN Practical Assignment "Design a Secure Windows 2000 Infrastructure" by John M. Shaw (http://www.giac.com/practical/GCWN/John_Shaw_GCWN.pdf)(6). Only the portions that are relevant to this paper will be utilized.

GIAC presented a great acquisition option for SANS, because it already possessed several remote distribution centers around the U S. Due to its distributed architecture, GIAC requires additional network management and security consideration. Figure 1 - 6 outlines GIAC's current physical network architecture. GIAC company headquarters is located in Kansas City (KC), Missouri and hosts t he company's executive management, Delivery Management Services (DMS), human resources, sales, accounting and information technology staff. A second site in Sta mford, Connecticut acts as a redundant facility in the event KC loses communication.

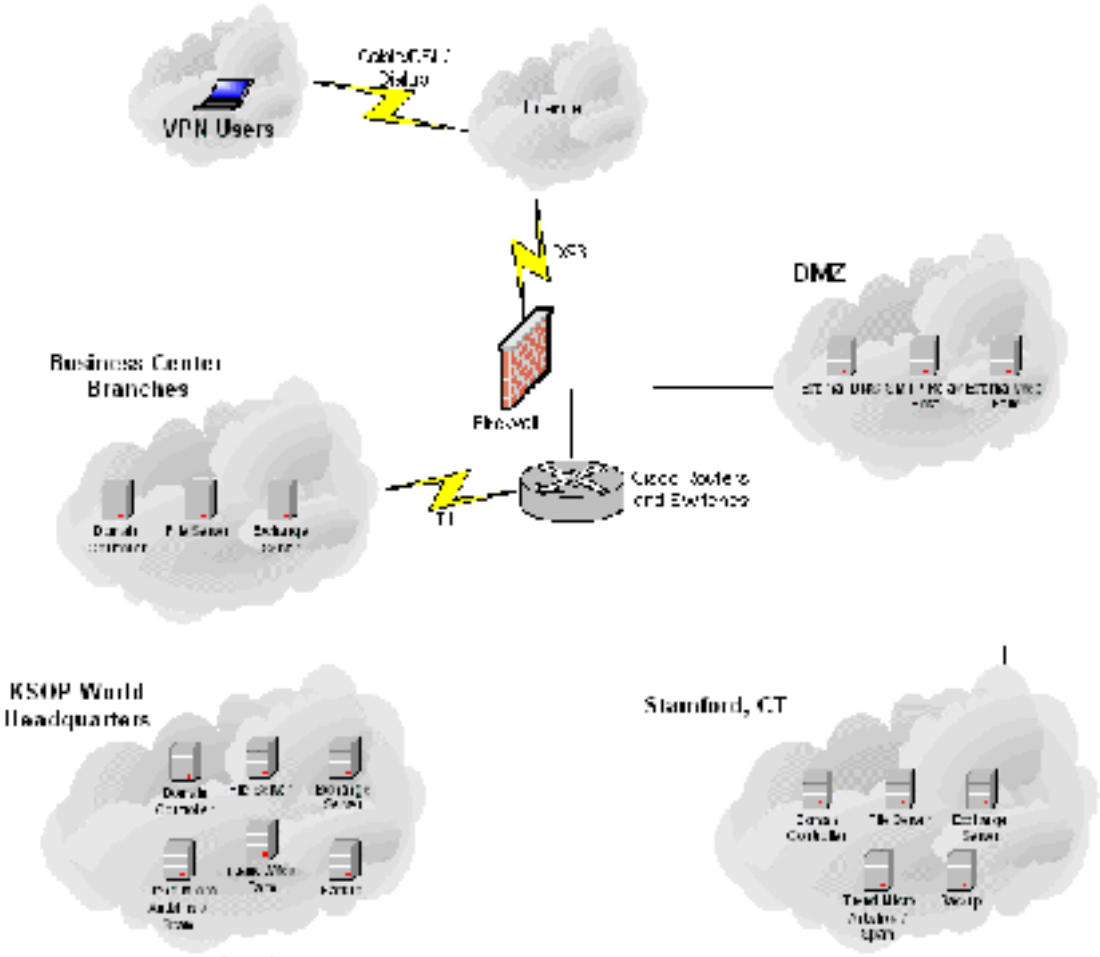


Figure 1-6 GIAC Network Diagram

1.3.1 Network Design

There are currently 15 branch offices around the country that function as bottling and distribution plants. In order to provide the freshest taste possible, SANS prefe rs that the pasteurization and bottling process occur at the closest possible point to its distribution area. Therefore, t hese plants are being converted to accept and pasteurize the bottled beer that is delivered from the SANS brewery. The branch office accesses the corporate network through a dedicated T1 connection that feeds into the core router. The computerized systems offer the branch offices three core values. The first two are email and file storage. The remaining system is a centralized Delivery M anagement System (DMSys) located at headquarters. DMSys tracks production, supply and delivery of whatever product GIAC is distributing.

A DMZ has been established to provide remote access to GIAC email services. The DMZ is directly connected to the GIAC Netscreen firewall to segment traffic. A DS3 connection from GIAC headquarters allows connectivity to the Internet. The 15 branch offices also use this bandwidth to access the Internet. Remote users can access resources, mainly email, in the DMZ through a VPN connection.

1.3.2 Domain Structure

GIAC recently migrated from NT4 to Windows 2000. Because of a long migration process that was frequently interrupted by heated political debates, the choice to migrate directly to Windows 2003 was rejected. GIAC has been configured with an empty root domain as well as a single child domain for user and computer accounts. The domain and OU structure is depicted in Figure 1-7. The following group policies have been implemented: a domain group policy which is applied to the northamerica.com domain; a domain controller group policy which is applied to the domain controllers OU; and a desktop configuration group policy which is applied to desktop OU. Further details on the settings of each group policy are specified within John Shaw's paper.

There are two domain controllers belonging to the empty root domain in KC with an additional one in Connecticut. The child domain has three domain controllers in KC, two in Connecticut and one in each of the branch offices. The global catalog is configured on each of the branch office DCs as well as two out the three KC DCs. All FSMO roles have been distributed over the five DCs at headquarters (root and child). In order to accommodate some additional user object fields, GIAC has made considerable modifications to the Schema. GIAC's Information Technology department has developed several Group Policies to enforce GIAC information technology security policies. Other Group Policies maintain workstation continuity in an effort to lower support costs.

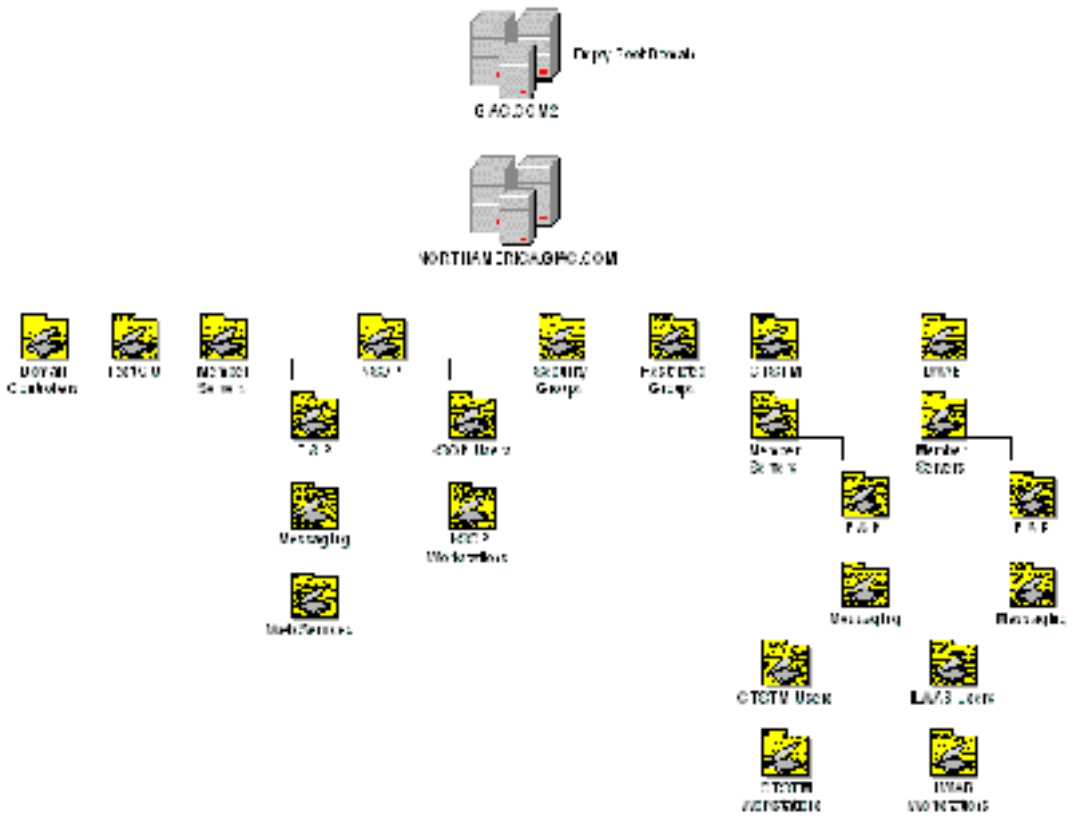


Figure 1-7 GIAC OU Struc ture

Corporate email services have recently been upgraded from Exchange 5.5 to Exchange 2000. The contact information from the Exchange 5.5 database was migrated to Active D irectory so user object information could be maintained. Remote users access their email through Outlook Web Access (OWA) installed on the IIS web servers located within the DMZ.

1.3.3 Clients

Corporate clients access GIAC network resources from Windows 2000 w orkstations located at the various locations. Workstations are configured with the standard Office 2000 suite, DMSys, MS Explorer 6.0 and McAfee's antiviral software. All applications are installed and maintained using Active Directory group policies. Addi tional applications are deployed to respective departments based on OU. Employees are assigned User level rights on all workstations in order to prevent unwanted manipulation of the operating system in addition to being able to install malicious applicatio ns. Norton Antivirus has been installed to protect the systems from malicious code.

1.4 THE MERGER

GIAC was able to retain most of its company structure in the acquisition negotiations. One of the contract stipulations required the name GIAC be appended to S ANS forming the new name SANSGIAC Incorporated. Aside from the cosmetic changes incurred by the companies as they go through the merger process, physical and operational changes must be implemented as well. Through the merger , SANS will continue to create recipes, brew the beer and sell the product. GIAC will be

responsible for pasteurization, bottling and distribution across the US. Physical location will not change at this time. Future consideration will be made to consolidate the corporate offices.

The consolidated IT landscape must coincide with the company's new mission. Systems access must be made available to all necessary employees across the previously imposed boundaries. There are four major systems that require access by employees throughout the SANSGIAC organization.

The first system is email. SANS has implemented Exchange 2003 to replace the outsourced solution. The new exchange site has been established in the chr.sans.com domain. SANS users still access email through their web browser using OWA. To meet managements requirement to be able to view calendar free/busy information across organizations, SANS implemented Microsoft Identity Integration Server (MIIS). MIIS can synchronize calendar and contact information between the two Exchange sites and forests. The second system is File Sharing. Given that SANS already has a large Storage Area Network in place, scaling storage needs to accommodate future growth is best done at the company headquarters. The third system is GIAC's DMSys, which tracks the production and distribution of orders. All members of the rdp.sans.com domain need to be able to access this system. The last system, BIGSales, is used by the sales and marketing department for sales orders and purchasing. An outside consulting firm has been tasked to develop an API that allows information to flow from BIGSales to DMSys. The API will allow orders entered into BIGSales to automatically form a record in DMSys. This prevents GIAC employees from having to reenter the information.

1.4.1 Network Infrastructure

The most obvious change will be the company's external domain name. The new consolidated name will be sansgiac.com. SANS original DNS servers, within its DMZ, will handle all external resource name resolution requests, including those for GIAC. GIAC's web servers will continue to provide user's access to OWA and the new company public web site. SANS external web environment will continue to provide remote users access to necessary Citrix applications.

Connectivity between the two sites was established using redundant leased T1 lines. Each line was acquired from a separate ISP. The original plan was to send traffic between the two organizations over a VPN connection. Given that a dedicated line fell within budget, the decision was made to create a dedicated connection. Having a dedicated line also eases the firewall requirements, as traffic between the sites is mostly trusted. In the event of a primary link failure, a VPN could still be established to return connectivity in the interim. SANS and GIAC core router tables were adjusted to reflect the additional network.

Employees will continue to access the Internet through their existing external connections. Given the geographical separation between the offices, it became more cost effective to provide access in this manner. Firewalls will remain in place at the corporate edge, managing all inbound and outbound traffic. Traffic between GIAC and SANS will be regulated by ACL's within the core router.

In an effort to minimize administrative overhead, GIAC's network infrastructure will gradually be upgraded with Cisco components where they do not currently exist.

Also, a Netscreen firewall will be placed at the SANS perimeter to replicate the one at GIAC. In order to achieve centralized control and monitoring of all systems, the consolidated SANSGIAC IT management staff felt it was necessary to standardize on manufactures for like components, which would allow consistent monitoring and reporting across the enterprise.

1.4.2 Systems Accessibility

Due to the modifications that were made to each organization's individual schema, consolidating the two forests was not an ideal solution. Instead, management felt maintaining the current architecture and creating forest trusts would be more appropriate.

As is the case with many organizations going through a merger, SANS and GIAC are not utilizing the same network operating system. SANS operating environment is based on Windows 2003 Active Directory and GIAC is based on Windows 2000. Because of the differences in operating levels, careful thought must be made to trust implementations between the two organizations. At this time, there are no plans to upgrade GIAC to Windows 2003 prior to completing the merger. In addition, since the proposed SANS domain consolidation will not be implemented prior to the merger, systems accessibility must be architected using the current environment.

Since both SANS and GIAC are not at a Windows 2003 forest functional level, the ability to create cross-forest trusts is not an option (8). Cross-forest trusts are a new addition to Windows 2003. They allow administrators to create a transitive trust relationship at the forest root level. With a forest trust, all domains in one forest trust all domains in the trusted forest. Forest trusts can be one or two way depending on the circumstances. In the case of SANSGIAC, the possibility to create cross-forest trusts is not possible. Instead, administrators must create explicit one or two-way external trusts between individual domains. Shortly after the merger is complete, progress will be made to upgrade all domains within GIAC to Windows 2003. After the upgrades have been completed, the domain and forest functional levels will be raised to Windows 2003. In addition, the current trusts will be replaced by a two-way cross-forest trust at the root level. The current plan is to coordinate the GIAC Windows upgrade with SANS domain consolidation.

The trusts implemented for SANSGIAC are outlined in Figure 1-8. In order to determine which domains should trust each other without giving up unnecessary access, each system was analyzed to determine the required level of trust. The first system considered was email. To accommodate the synchronization being performed by MIIS, a two way trust was establish between the chr.sans.com domain and the northamerica.giac.com domain. Second, the primary file stores that require access by all SANSGIAC employees are also contained within the chr.sans.com domain. Since a trust already exists, no additional configuration is needed. Third, GIAC employees require access to the BIGSales database located in the ms.sans.com domain. To accommodate this requirement, a trust was created that makes northamerica.giac.com a trusted domain of ms.sans.com. In the future a two-way trust will be configured to allow the API to function properly. Last, members of the research and production team will need to access the DMSys application. To make this possible rdp.sans.com will become a trusted domain of northamerica.giac.com. GIAC employees will be able to access the BIGSales application through a Citrix terminal session initiated from a web browser. The

DMSys client will be loaded on the Citrix servers to allow RDP employees to access that system.

Figure 1-8 Trust Relationships

Establishing trust relationships opens an organization to greater threats. In the case of SANSGIAC, upper level network administrators have been consolidated in an effort to promote the application of best practices and lessons learned across organizational boundaries. However, management wanted to retain the lower level systems administrator structure since these employees possessed a great deal of institutional knowledge and would be best suited to remain in their current positions. The result is that system administrators granted domain admin privileges for their respective domain do not have the same privileges in other domains.

To alleviate some of the threats associated with creating trusts, Microsoft has introduced SID filtering. SID filtering helps to combat Elevation of Privilege attacks. Should a malicious GIAC administrator obtain the SID information of an account with high access levels in one of the SANS domains, they could potentially add that SID information to an account in the GIAC domain. The SID information can be obtained by capturing network traffic, looking specifically for the SID's of known powerful accounts. Once the malicious person has acquired the SID information from the account in the SANS domain, they can append the SID History attribute of the GIAC account. This can be done using tools such as ADSI Edit. Now this modified GIAC account could access resources on the SANS domain wherever the sniffed account has privileges. SID filtering prevents this threat from becoming a reality. From the perspective of the trusting domain, SID filtering compares the SID of the incoming security principal to the domain SID of the trusted domain. If the account security principles include SID's from domains other then the trusted domain, the additional domain SID's are removed. (4)

The use of SID filtering becomes an issue if access is being granted to domain resources through the use of SID history. This usually occurs if accounts have been migrated from one domain to another without the ACL's being updated to reflect the change in domain membership. Since the SANSGIAC domains do not require the use of SID History, this will not become an issue. In addition, problems can occur if Universal groups are used and the Universal group was not originally created in the trusted domain (8). As an example, if a universal group was created in a hypothetical

non-trusted GIAC domain, the group could not be used to grant access to SANS resources even if the accou nts within the group are from a trusted GIAC domain. When the universal group attempts to access resources in the SANS domain, SID filtering will remove the domain SID from the Universal group, rendering the group ineffective.

Implementing SID filtering i n the SANSGIAC environment will require different steps from each side of the trust. From SANS point of view, every external trust that is created will have SID filtering enabled by default. All domain controllers running Windows 2003 and Windows 2000 SP4 or later will exhibit this behavior. However, domain controllers running Windows 2000 SP3 or earlier will have to manually enable this security component. Using Netdom.exe is the recommend method for enabling SID filtering. Below is an example to illustrat e the use of the Netdom utility for the ms.sans.com domain (1).

Netdom trust GIAC **/domain:** ms.sans.com **/quarantine:** yes **/user:** administrator **/pas:** abc

This step will need to be repeated for the rdp.sans.com domain.

The Netdom utility is part of the Windows 2000 Resource Kit. It allows administrators to create, remove and monitor trust relationships. In addition it can be used to add/remove computer objects to the domain and synchronize system time. When using Netdom to establish SID filtering, the */quarantin e* switch is used. This can either turn on or off SID filtering simply by stating yes or no after the option. The */domain* switch denotes the trusting domain. The /user and /pas switches specify the administrators user name and pass word necessary to impl eme nt the change.

The SANS and GIAC OU structure and group policies will remain intact throughout the merger. However, after the merger is complete SANS will consolidate domains and GIAC will upgrade to Windows 2003. Once this is complete, administrators can begin to implement the same group policies to both the internal.sans.com domain and the northmamerica.giac.com domain. The idea is to globally enforce the company's security policies from single group policy templates. After the merger, upgrade and consol idation is complete, the following group policies will exist:

- *Domain group policy* – The policy will be the same in both SANS and GIAC child domains. The policy settings are discussed in Section 2. GIAC will no longer have a Domain Controller group policy because the domain controller will apply the settings inherited from the Domain group policy. (domain and domain controller settings will be the same)

- *Citrix group policy* – The policy will be applied to both the SANS and GIAC Citrix Server OU. The primary function of this policy is to "lock down" the Citrix user environment. The settings will be taken from the original SANS Citrix group policy discussed earlier in this paper.

- *Intranet IIS group policy* – The policy will be applied to the IIS OU in both organizations. The settings will be created from the NSA IIS security guide. The settings for this policy have not yet been determined.

- *Software deployment group policy* – The policy will be applied to each user OU based on job function in both Organizations. Since most applications

are accessed through a Citrix client, the policy will only be used if newer version of a particular application needs to be installed (ex. Netscape).

1.4.3 Clients

SANSGIAC will continue to be a proponent of server based computing. GIAC will begin to replace all workstations with dumb terminals. A separate GAIC Citrix server farm will be established in order to publish the required applications. Having all SANSGIAC applications available through Citrix provides a great benefit to employees who travel between the various SANSGIAC locations. They will be able to access their personalized set of applications from any terminal throughout the company. In addition, moving GIAC towards server based computing fosters the growth of a homogeneous computing environment.

The only persons moving physical location will be senior management personnel and some senior IT staff. To accommodate these users, a northamerica.giac.com domain controller will be installed at the Harrisonburg office complex. The DC will be placed in a separate site to minimize replication traffic and increase the speed of client logon.

1.4.4 Conclusion

The end result of the SANSGIAC merger will enable employees from both organizations to access resources in each other's forests. Additional access will not be necessary for the DMZ domains. Only the SANS DMZ requires authentication for Citrix Metaframe access, which directs the authentication request to the individual resource. By merging the IT landscape between SANS and GIAC, the new company benefits from the seamless sharing of existing network resources, significantly reducing cost. Although employees from both organizations will have to get used to using the new applications and transition to a new email system, the overall transition has not impacted core business practices.

The structure of the organization, specifically the network structure, will dictate how trusts should be established. If a single group of administrators manages all forests, greater trust can be expected between external domains. Windows 2003 cross-forest transitive trusts is a great solution for merging organizations that also completely consolidate their network support operations. Regardless, creating external trusts brings an increased security risk and must be carefully planned.

SANSGIAC is also making great efforts to standardize on technologies and vendors. Standardizing a large organization reduces cost and improves the ability to secure systems. Determining security requirements for multiple different technologies requires a great deal of diversified knowledge and time to implement. With a homogeneous environment, planning, implementing and monitoring become much simpler.

2 SANSGIAC Security Policy

In an effort to standardize SANSGIAC network operati ng system (NOS) security, systems administrators plan to utilize Microsoft group policies and security templates. Group policies allow administrators to designate registry -based policy settings, security settings, software installation, scripts, folder re direction, Remote Installation Services, and Internet Explorer maintenance. Group policies can be implemented from a central location using the Group Policy Management Console MMC. Group policies can be applied to various Active Directory containers includ ing; sites, domains and Organizational Units. SANSGIAC is in the process of creating policy standards that can be deployed throughout the organization in an effort to standardize the enterprise infrastructure.

2.1 DEFINING THE GROUP P OLICY

Many government ag encies and contractors that work on government related projects are required to abide by a certain set of reg ulations. For exa mple, health care and insurance companies must abide by new security measures, known as HIPAA, in an effort to protect confidentia l patient information. Companies must meet certain security and process requirements in order to be deemed HIPAA compliant. SANSGIAC is not required to abide by these types of regulations. The security policy established by SANSGIAC information technology leadership group states that the production environment must meet the security standards set forth in the Microsoft Common Criteria Security Guide (MCCSG). This is an internally generated policy. In areas where the MCCSG does not provide adequate documen tation, additional information will need to be obtained. The primary source of this information will be the NSA Security Guidelines located online at http://www.nsa.gov/snac/index.html . The NSA guidelines specify greater detail in securing IIS, DHCP, DNS and other Windows services. The final group policy should be able to be applied in both SANS and GIAC Windows 2003 domains.

2.1.1 Configuring the Template

The security template settings can be viewed by using t he Security Configuration and Analysis (SCA) Snap -In. Within the SCA snap -in, settings can be analyzed against the current configu ration as illustrated below in F igure 2-1.

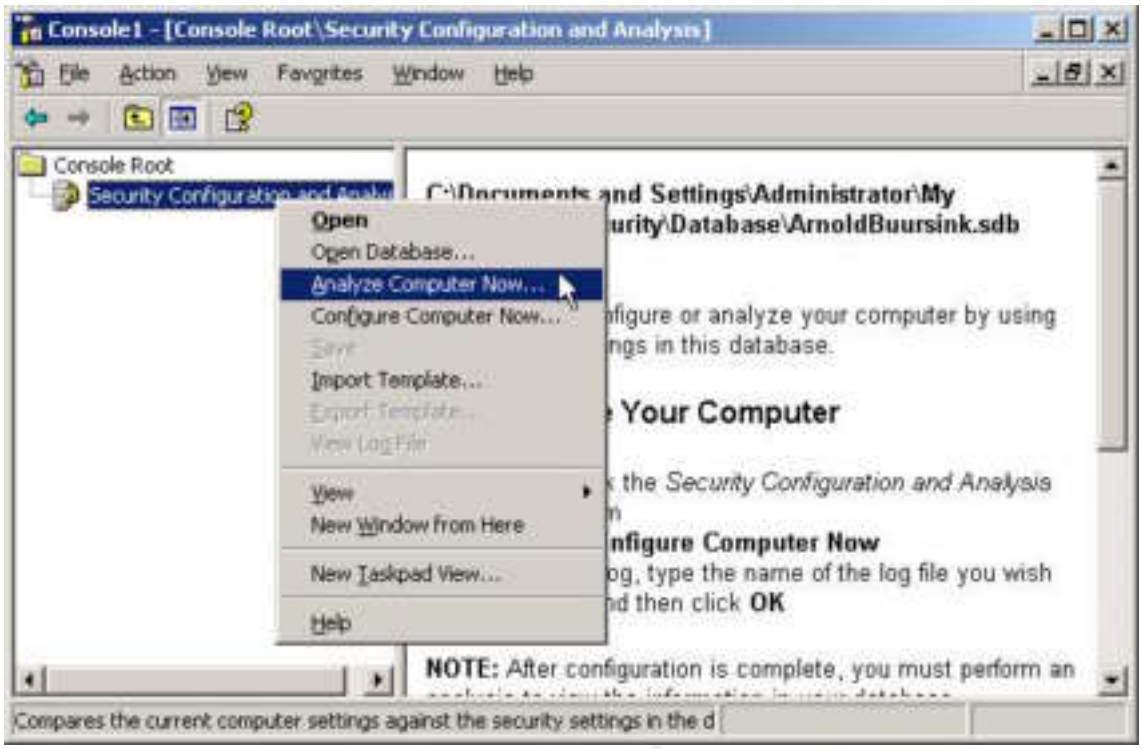


Figure 2-1 Analyze Computer

The analysis process will compare the local computers settings against the template and capture the results in a database file. This SCA database can be discarded at a later time. It only captures the settings of the system being analyzed (2) . Figure 2-2 illustrates how the analysis is presented. Settings that do not match those within the database are marked with an error symbol. This indicates that the current settings are either not defined, weak, or too strong. Since this is a Windows 2000 template applied against a Windows 2003 server, some of the settings will come up as being weaker than the current configuration. Microsoft has increased its "out-of-the-box" security settings within Windows 2000. Looking at the positives, settings that match the database are marked with a green check and only require further attention if the settings should be entirely omitted. Settings that are not defined in the template have no markings. They will simply show as Not Analyzed.

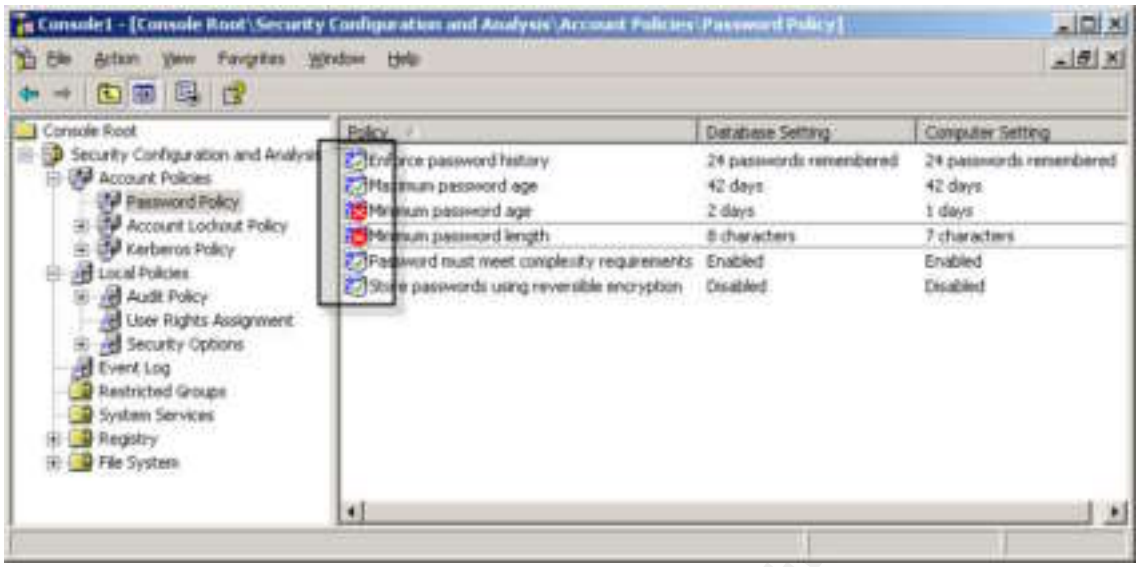


Figure 2-2 Policy Analysis

The next step is to go through the settings and determine whether the settings should be modified or left as is. Generic security settings found in publicly available templates are a good place to start the security policy process. However, they should be carefully sculpted to meet user expectations and company policy. After the security settings have been properly adjusted, they may be exported to a new template file. At this point administrators can use the new template file to import the settings into a group policy. Figure 2-3 illustrates how a security template can be imported.

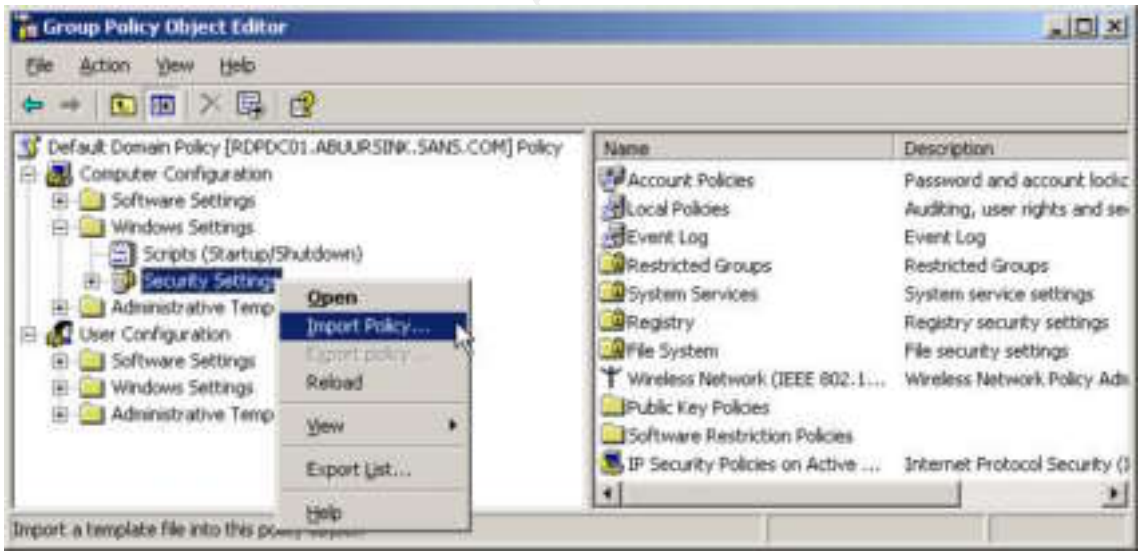


Figure 2-3 ImportPolicy

2.1.2 Group Policy Settings

Below are the final settings that comprise the SANSGIAC Domain Group Policy. The settings were captured using the Resultant Set of Policies (RSoP) MMC Snap-In. RSoP is a new utility that is part of Windows 2003 which allows administrators to view how a group policy will impact a particular system. RSoP is especially helpful to determine what effect multiple policies at various levels will have on a system.

Initially RSoP was run in planning mode. Planning mode simulates how a group policy would impact a designated server without actually applying the policy. Group Policy Management Console is also a useful tool to get reports about a particular policy. GPMC will only tell us what the current settings are for a single policy. The figures below illustrate the results presented by RSoP run against the SANS intranet web server. Policies marked with an error symbol will not be applied on a windows 2003 server. This is most likely because the service, file, or registry key does not exist. All settings determined by the SANSGIAC Domain Group Policy show the source as being Arnold_Buursink.

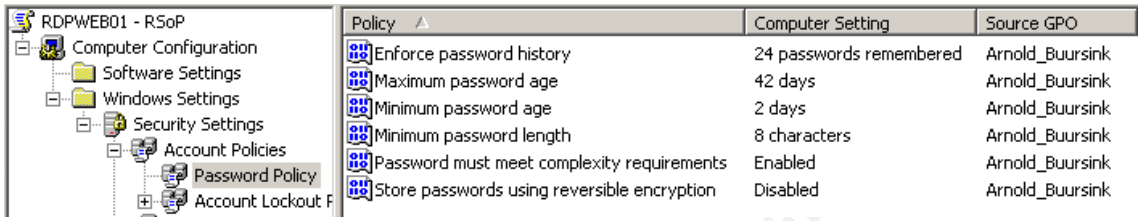


Figure 2-4 Password Policy

Minimum password age was increased from 1 day in the Windows 2003 settings to 2 days in the template. This setting prevents users from repeatedly changing their password to revert back to their previous password. The password length was increased to 8 characters to match the template. The RDP domain currently requires 25 characters for passwords. After the security risks where analyzed, managers did not feel that a pass phrase was necessary. Instead, with a consolidated domain and a single domain group policy, RDP users can revert back to 8 character passwords. The template also requires that passwords meet complexity requirements. Complexity requirements force users to specify at least three of the following four characters; upper and lowercase letters, symbols and/or numbers.

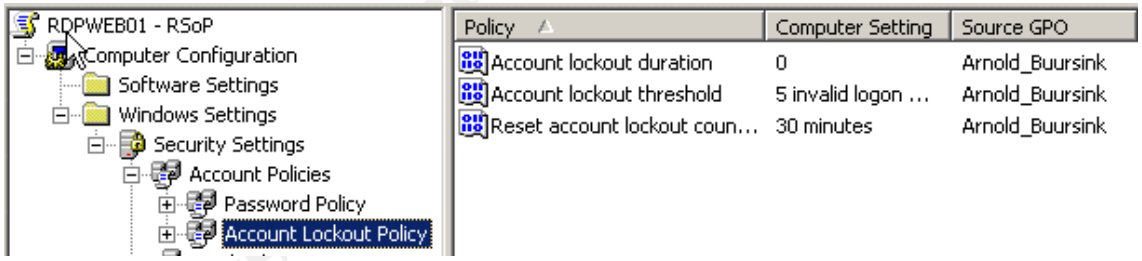


Figure 2-5 Account Lockout Policy

The account lockout duration has been set to zero, forcing an administrator to unlock the account. Setting an account lockout threshold will combat against brute force attacks which allow an attacker to continually guess passwords. The account lockout threshold works on all accounts *except* for the Administrator account. Additional attention must be given to this account to further protect it. As a general rule of thumb, organizations should not use the Administrator account for daily management activities. If a strict “no use” policy is enforced, auditing and alerting is possible should any malicious person attempt to use the account. For example, if a person attempts to guess the Administrator password, system auditing will capture the failed logon events. An alert could then be issued to the appropriate persons if more then 5 failures occur within a 24 hour period of time using event management scripts or applications. Section 3.1 will further discuss event monitoring and alerting.

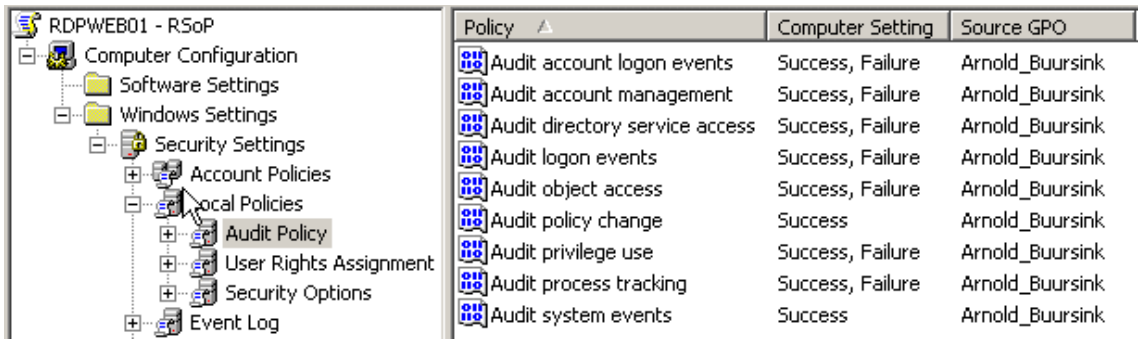


Figure 2-6 Audit Policy

Template settings increased the level of auditing to include failures for most settings. Auditing failures will allow event -monitoring services to notify administrators of any potential problems. For security purposes, auditing object acce ss and account management will go a long way. Object access allows administrators to specify at the file level what resources should be monitored for access. This would be useful if managers wanted to monitor who was accessing sensitive financial records. Account management and logon events will alert administrators if accounts are being modified or attempting to logon to systems.

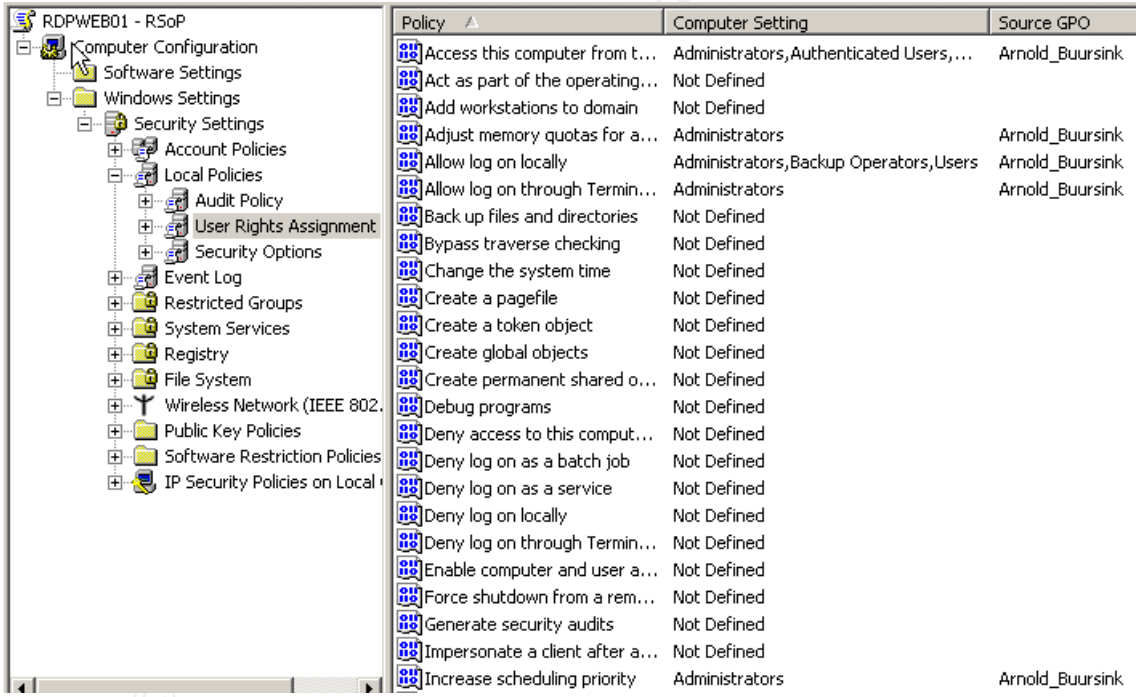


Figure 2-7 User Rights Assignment

The User Rights Assignment for “Access th e co mputer from the network” and “Allow log on locally” were removed from the template so that each machine can maintain its own access control list. This setting will likely be set on more granular group policies, as some systems should have more stringen t requirements for logon and network access. The Microsoft template also changed user rights on some system functions, allowing only an administrator to perform the action.

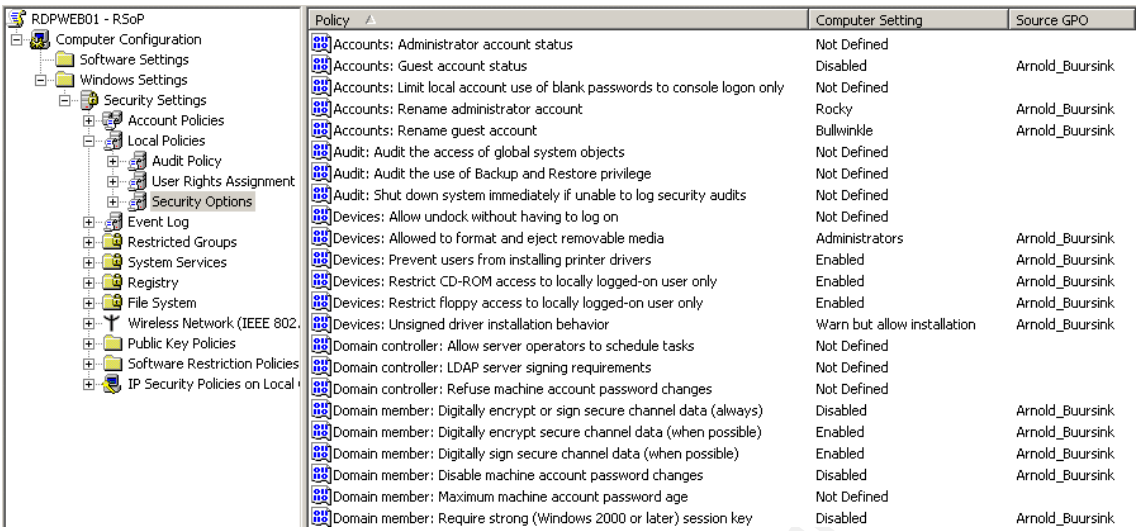


Figure 2-8 Security Options

Within the security options, the guest account has been set to disabled. To prevent a malicious user from attempting to guess common accounts, the administrator and guest account have been renamed. Making this change at the domain level keeps the naming conve ntion simpler for administrators. For additional security, a “honey pot” account named administrat or co uld be created. This account acts as a decoy and would have no privileges within the domain. Attackers would have little luck attempting to manipulate sy stem resources with the new administrator account. Careful attention must be given to remove the description field for the old Administrator account.

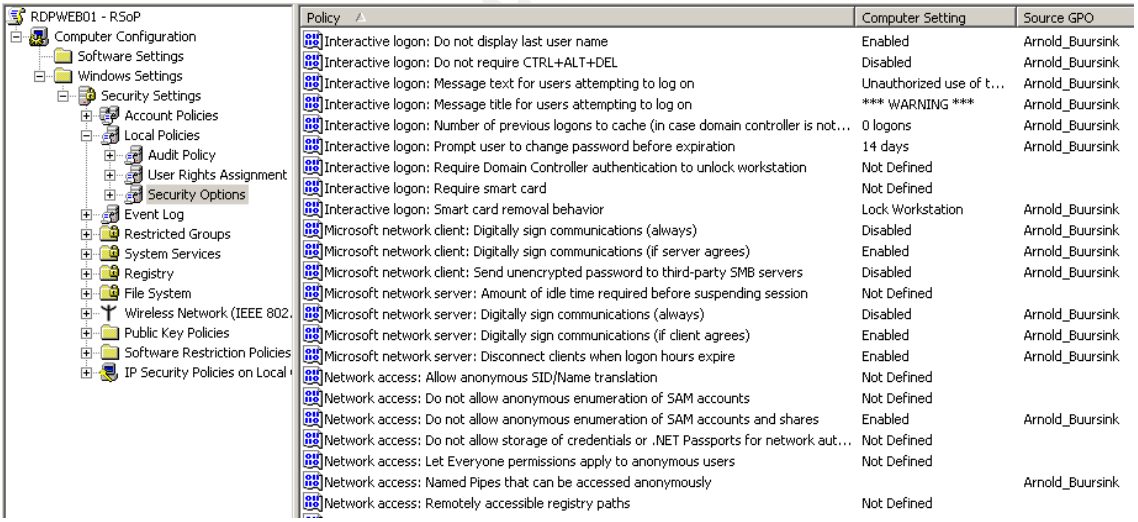


Figure 2-9 Security Options Continued

The setting will however be included within the Server Group Policy. “Do not allow anonymous enumeration of SAM accounts and shares” is disabled to prevent malicious users from locating common SID’s. Even if a common account has been renamed, the SID still remains the sam e. In the case of the administrator account it will always end in 500. If anonymous enumeration is enabled, a malicious person could determine what the administrator account has been renamed to.

Figure 2-10 Security Options Continued

The Security Option setting “Shutdown:Clear virtual memory pagefile” was removed from the template because it was determined that this settings caused workstations to take a prolonged period of time to shut down. This setting w as altered because the security benefits were not in line with the users expectations. In addition, automatic logon of the administrator account within the recovery console is disabled. This prevents unwanted administrative access to system resources.

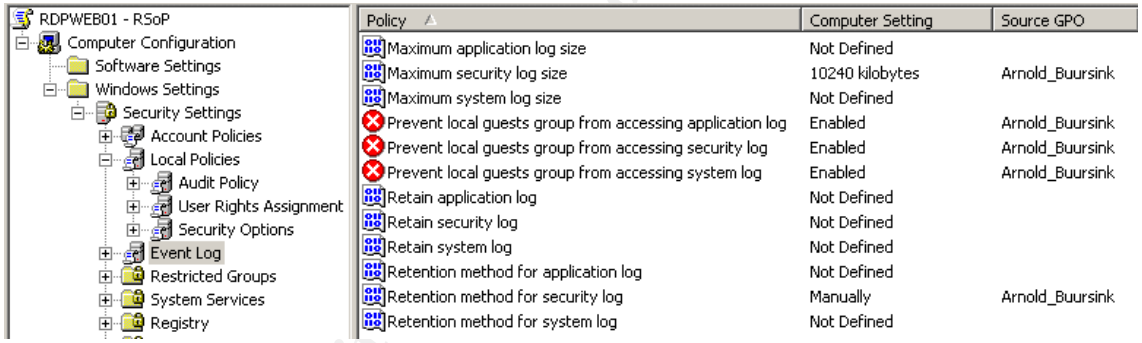


Figure 2-11 Event Log

The setting for “Maximum security log size” was increased to reflect the setting found on Windows 2003 servers. In addition the security log will be archived on a weekly basis. The polic y specifies that the security log will not be overwritten until the archive process is complete.

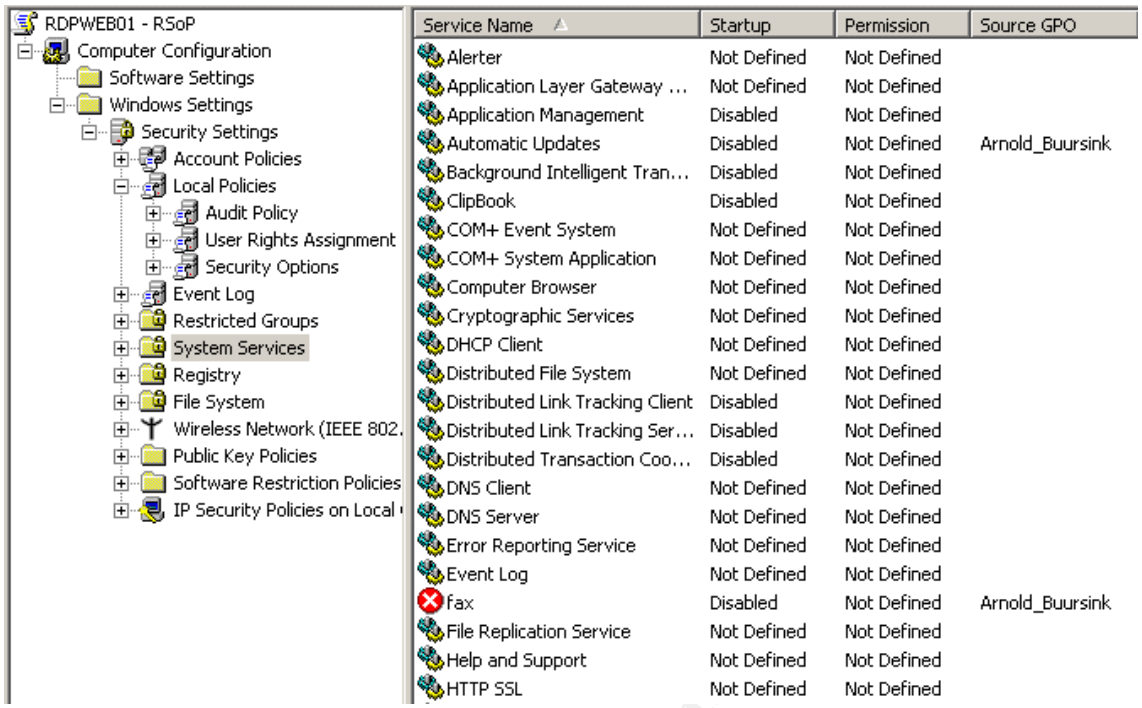


Figure 2-12 Services

Since SANSGIAC utilizes Pacthlinks Patch Management Server to update systems, the Windows Automatic Updates service has been disabled. Patchlink acts much like Windows Automatic Update but allows administrators to approve patches before they are distributed. Patchlink also tests the patches to verify that they are stable. In house testing against the local environment is always recommended. Microsoft also provides a similar type of product called Software Update Server (SUS). SUS will only perform updates on Windows operating system. Patchlink adds the ability to update various operating systems and some common applications such as MS Office.

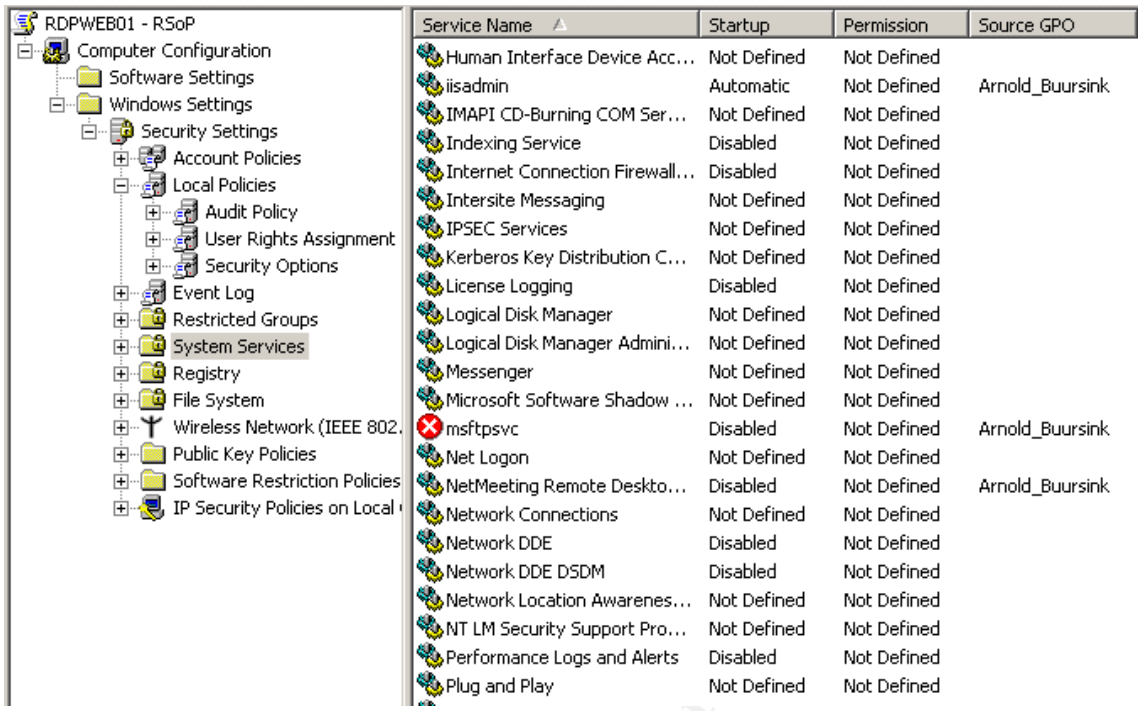


Figure 2-13 Services Continued

SANSGIAC mandates that no user be allowed to share network resources without explicit permission. To acco mmodate this requirement, Internet Connection Sharing is set to “Disabled”. Along the same lines, the desktop sharing feature within NetMeeting has also been disabled. Task Scheduler is disabled by default on Windows 2003 servers but not on Windows 2000. The setting has been left out o f the domain policy but will be added to the computer’s policy. Task Scheduler could allow attackers to run executables under elevated privileges without the user’s knowledge.

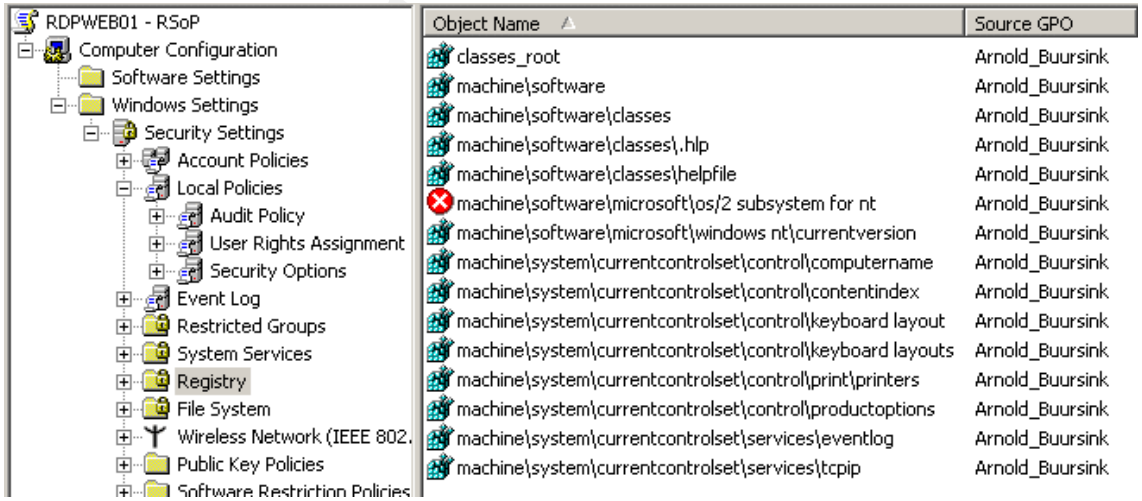


Figure 2-14 Registry

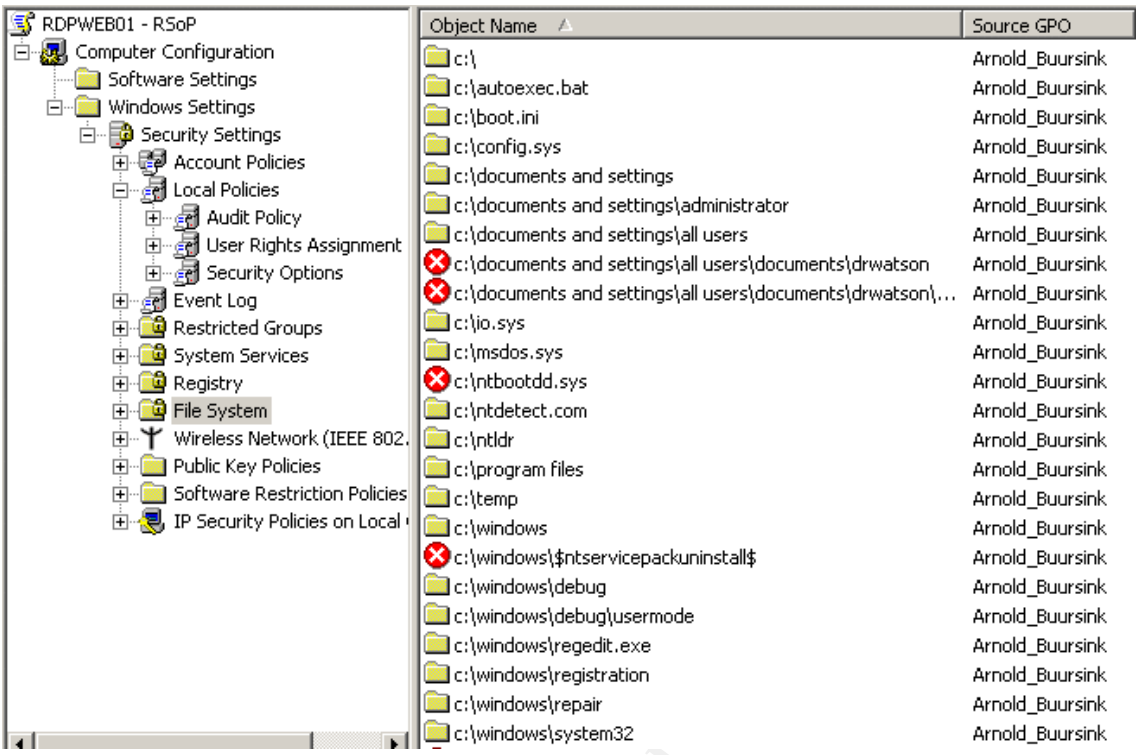


Figure 2-15 Folders

The remaining portion of the policy also addresses permissions on several files and folders within the File System. It is possible that the increased security level will cause applications to stop functioning. Some applications require writing to a log file commonly found in the Program Files folder, where most applications are installed by default. The template prevents Users from writing to this folder. However, many applications designed for Windows 2000 or greater have changed the location of these log files. In the future as SANSGIAC starts to incorporate wireless devices into the enterprise, additional policies can now be specified with Windows 2003. This is a very useful function to quickly configure systems for the appropriate wireless settings.

2.2 GROUP POLICY APPLICATION

The SANSGIAC domain security settings will be deployed as a group policy at the domain level. The domain group policy does not incorporate all potential policy settings. However, it incorporates the minimum security settings that should be applied to all objects within the domain. Additional settings should be enforced at lower OU levels. Applying additional GP settings at the various down level OUs allows administrators to granularly assign policies to systems based upon their function. Once the policies have been established, if a machine changes roles, it can simply be placed in the appropriate OU and receive the relevant settings.

Administrators must take order of precedence into account when deploying group policies. Local security policies are the first to be applied by a computer system. If a Site Group Policy has been created, its settings will then take precedence. The site policy is followed by the domain policy and then the OU policies. The lowest OU policy takes the greatest precedence and has the ability to negate earlier settings. In

addition, administrators can choose not to have a policy apply to certain OU's or even certain users or c omputer objects.

Conducting configuration management through group policies allows administrators to maintain the same settings across all like systems. Since the policies are modified from a central location, the requirement to visit each machine is eliminate d. This not only reduces administrative costs, but ensures that all systems can be centrally secured if security threats are discovered.

The domain group policy created earlier in this section is first applied to a mock domain that resembles SANSGIAC arch itecture. Rather than having potential problems occur in a production environment, it is always sound practice to first deploy group policies in a test environment. The SANSGIAC Domain Group Policy was applied to the rdp.sans.com test domain to simulate i ts impact. This paper will examine the impact of the domain group policy on the rdp.sans.com IIS intranet web server. Only the domain group policy will be applied until it is determined that the policy is stable. The domain policy will propagate down to t he web server's container and be applied to the IIS web server.

Since organizations computing environments have the potential to change frequently, policies must be adjusted to conform. SANSGIAC group policies will be evaluated on a quarterly basis to re flect any changes in technical requirements or organizational structure. The evaluation team will consist of primary IT management staff. The evaluation team must approve all changes that fall outside of the quarterly review cycle. Group policy modificatio ns will be audited to ensure unauthorized users do not inadvertently spread changes throughout the organization. Section 3.1 will discuss auditing and event monitoring in further detail.

2.3 TESTING POLICY CONFI GURATION

It is important to verify the functiona lity of group policies after they have been created. SANSGIAC uses GSX Server from VMWare to create their test environment. With VMWare, administrators are able to rapidly standup several virtual servers within a single host operating system. Each virtual server has the same functionality as a standard stand -alone server. The virtual test environment will include a domain controller from the rdp.sans.com domain and a replica of the SANS IIS intranet web server.

There are two approaches to testing the pol icy. The method first is to use the RSoP to determine the policies impact. RSoP will allow administrators to simulate policy settings for select users and computers. This is important when determining what settings are applied based on the objects location with the OU structure. The seco nd method is to implement the policy in a test environment. It is not recommended to test the policy in a production environment. At times, administrators will not have access to a test environment and should rely on RSoP fo r best effort testing. Since SANSGIAC has a lab environment available, it will be the location of choice for testing the policy.

The first step in the deployment process is to apply the group policy at the domain level. Since the intranet web server is pa rt of the domain, the policy settings should propagate. Once the group policy is applied, the intranet web server is rebooted.

Rebooting the server will ensure that computer settings are applied. With the computer online, the system is analyzed to determin e if the settings took hold.

For the purpose of this paper, only certain settings will be examined to ensure the operation of the security policy. However, all settings should be verified to ensure the effectiveness of a particular policy. Below are sever al figures that show the remaining test results.

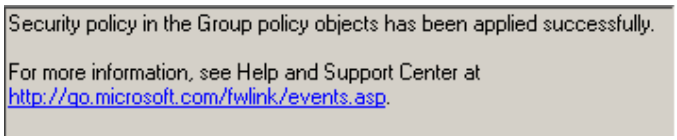


Figure 2-16 Policy Applied Event

The Application log was checked to verify that the group policy had been applied successfully. As noted above, the group p olicy objects were applied successfully.

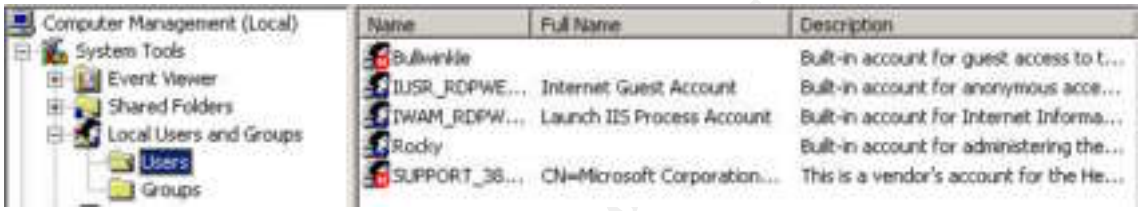


Figure 2-17 User Policy Test

The guest and administrator accounts have been renamed successfully. However the description should be removed so that it does not bec ome obvious that the account has been renamed.

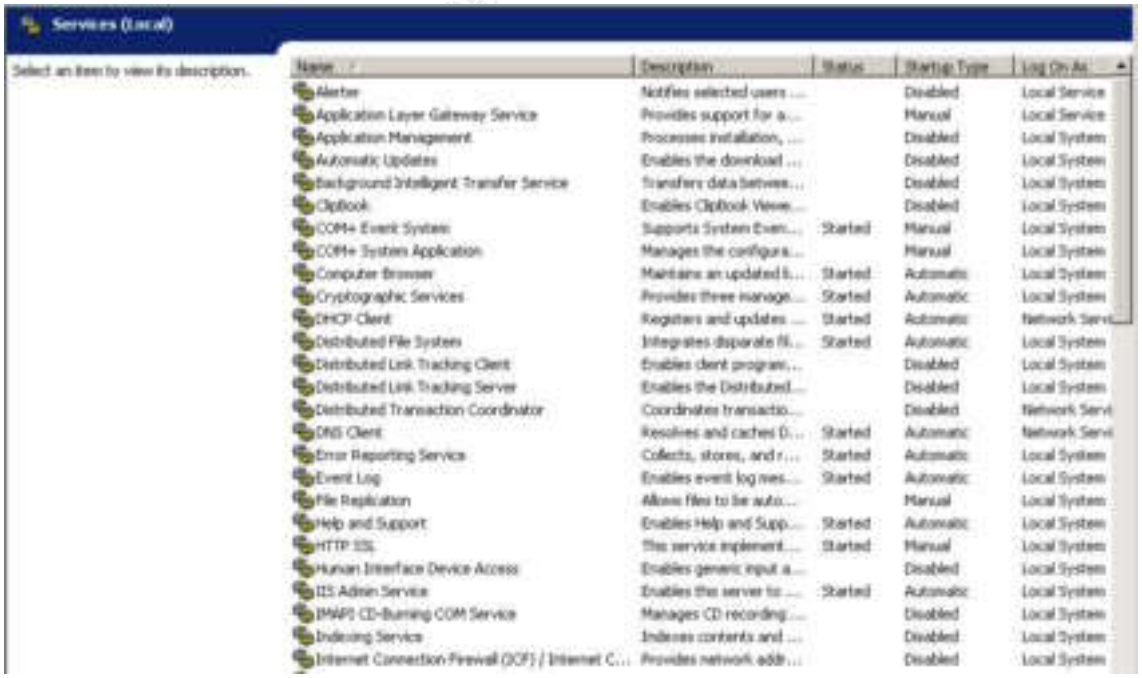


Figure 2-18 Service Po licy Test

Local services successfully show the automatic update services as being disabled. In addition, the Internet connection sharing service has been disabled.

Figure 2-19 Security Policy Test

After accessing a designated folder with a known invalid account, the security logs successfully registered a failure audit.

Overall, it appea rs that the policy has imposed its settings successfully on the intranet web server. As mentioned previously, additional testing will be performed to verify that all settings are applied. There are instances where settings can be set at the computer or use r level within the group policy. At times, the setting will only be properly applied if it is specified within the correct portion of the policy.

2.4 TESTING SYSTEM FUNCT IONALITY

Once the application of the group policy has been verified, additional test shou ld be conducted to determine that the SANSGIAC Domain Group Policy does not diminish the functionality of the SANS intranet web servers located within the rdp.sans.com domain.

The IIS web server's host dynamic content related to daily company announcemen ts and calendaring. Various employees regularly update the content by editing text files that are later called by active server pages. Testing should verify that users can access the web content and that employees are able to modify the text files. Access to the text files is being granted through the use of a group named Web Content Admin. In addition, administrators should verify that web services can be restarted and that that administrative functions have not been lost. Testing will be conducted on a virtual IIS server that is an exact duplicate of the production system.

The initial test will confirm that the web services can be restarted.

The test failed because the World Wide Web Publishing Service is dependent on the IIS Admin service, which has been disabled in the domain group policy. To rectify the problem, a web server group policy will be applied to the Web Server OU enabling the IIS Admin service.

Next, to test access to the intranet web site, Internet Explorer was launched from a workstation and the browser was pointed to the intranet URL. The page displayed without any errors. A non administrative user account was used for this test.

The final test had a user within the Web Content Admin group modify the text files from a workstation co mputer. The user was able to modify the content and the changes were successfully displayed in the browser.

Initial testing shows that the policy needs to be supported with additional policies in order to prevent unwanted results. Although the server appe ars to function properly, administrators must carefully monitor the system when the policy is applied in a production environment. Appropriate time should be allotted between the applications of policies in order to easily determine which policy caused pro blems.

2.5 EVALUATION

The SANSGIAC domain level policy is effective in providing general, enterprise security settings. However, most organizations will require policies to be set at a more granular level. Active Directory allows administrators to group like systems into Organizational Units. Policies that reflect the requirements of the systems within each OU can then be defined. SANS administrators should place the intranet IIS server within a web OU, and then apply appropriate security policies. There are several organizations including NIST and NSA that publish security templates which outline industry recognized settings for securing specific types of systems including; email, web, databases, etc.

The SANSGIAC domain security policy effectively secures en terprise resources. The goal is to create a policy that secures the operating system but not necessarily the secondary applications that run on these systems. The final policy meets all recommendations set forth by the MCCSG. The policy appropriately reduc es the security risks of any computer that is a member of the domain. However, it is possible that this policy does not appropriately address all needed security settings within Windows 2003 because the security template was designed to secure Windows 200 0. There are c urrently little publicly available Windows 2003 security templates from reputable security sources. It would have been more appropriate to implement a Windows 2003 security template, rather then having to modify a template created for an olde r operating system. The primary weaknesses in the policy are related to the security of specific applications like SQL and IIS. As previously mentioned, separate group policies should be created to secure these systems.

Aside from the problems with the W eb Publishing Service, the policy does not appear to create any functional problems. However, the testing done at this point is not sufficient to draw an accurate conclusion. Additional testing should be performed on other types of systems to determine if the policy will adversely affect system functionality and performance. Should a problem be discovered, such as the Web Publishing Service, down level policies can be modified to adjust the current settings. Because of the order of precedence, these down le vel policies will determine the final setting. Adjusting the policy at a lower level prevents the changes from being applied to all systems and potentially opening these systems to unwanted vulnerabilities.

3 Systems Monitoring and Auditing

3.1 MONITORING REQUIREMENTS

Systems monitoring and auditing is a crucial capability of any enterprise network. Most organizations will fall into two categories when it comes to the approach taken to monitoring. The first reacts to problems reported by the User community and then systematically goes through local event logs to determine the cause of the problem. The second establishes a proactive means of event evaluation and notification from a central location. Most companies will strive to achieve the later, but may come up short because of monetary and labor constraints.

Incorporating scripts is a great way for companies to monitor events if funds are not available to purchase a commercial-of-the-shelf (COTS) product. Scripts can be written from scratch or obtained through knowledge exchange sites on the web. Scripts can provide administrators with consolidated event logs gathered from enterprise systems. In addition, they can be modified to send alerts based upon event ID's or the frequency of occurrence in a given period of time. Windows Management Instrumentation (WMI) interface can be incorporated into scripts to dump event log data on remote system in near real-time. In addition, *DumpEL.exe* found on the Windows 2000 Resource Kit has the ability to dump event logs to an ASCII text file. The text files can later be parsed to display only the pertinent information. Although scripts provide some organizations with all the needed functions, many still long for additional functionality and reporting capabilities.

COTS products present administrators with a rapid method of implementing system monitoring functionality. Many products are able to consolidate event logs from various types of systems including servers, workstations, routers/switches, and storage devices. The systems do not necessarily need to be from the same manufacturer or revision level. This is critical in heterogeneous computing environments. Some monitoring applications require the installation of remote clients that report the information back to a central server while other applications simply query the system directly.

SANSGIAC follows industry best practices when it comes to monitoring its active directory infrastructure. Earlier in section 2, the SANSGIAC Domain Group Policy was modified to audit several key services.

- *Account management* is set to monitor when accounts are deleted created or modified. This is important should a malicious user attempt to add themselves to a more powerful global or local group.

- *Directory services access* allows administrators to specify what portions of the AD structure they wish to audit. Individual object SACL's must be modified to specify what events should be audited. In the case of SANSGIAC, auditing is configured for modification of organizational units, group policies and schema.

- Auditing successful *system events* will let administrators know when the system time has been changed, when an audit log was cleared or the last time a system was rebooted.

- Auditing *logon event* failures is configured for everyone and warns administrators of attempts to access secured resources. Auditing failures can be a great form of intrusion detection. To prevent malicious persons from successful launching a security log denial of service attack, the security policy is not set to shut do wn the computer is the security log is full.

- *Object access* auditing has been set to only track fil e deletions by everyone in the *c:\winnt* and *c:\program* files folders.

Staying on top of the large amounts of information event monitoring produces can be a daunting task. SANSGIAC has segmented the process of auditing and monitoring into the following three functions.

- *NOS Event Filtering, Notification, and Consolidation* – This segment is responsible for monitoring Windows events including Active Directory management. The systems administration team is responsible for this segment.

- *NET Event Filtering, No tification, and Consolidation* – This segment is responsible for monitoring firewalls, routers, switches and LAN/WAN connectivity. The network operations tea m is responsible for this se gment.

- *Change Management* – This segment is responsible for doc umenting and regulating the modifications made to group policies, schema, security group membership, firewalls and application version. IT management is responsible for this segment.

3.2 EVENT FILTERING, NOT IFICATION AND CONSOL IDATION

In an effort to stay on top of all the events created by the various audit logs, SANSGIAC has implemented NetIQ Security Manager Suite. NetIQ's product is one of many event consolidation a nd alerting tools on the market. Security Manager provides the added benefit of not only consolidating Windows events, but also being able to monitor events from various types of routers a nd antivirus products. Security Manager can alert administrators when virus definitions are out -of-date or if fire wall configurations are noncompliant. SANSGIAC will take advantage of the capability to work with Microsoft security policies and determine if computers are properly configured. If not, an alert is sent to the appropriate persons or group. Another added benefit is the ability to correlate events from various sources to alleviate false positives. For example, if one server looses network connectivity an event would be created and send an alert to a network engine er. Network Monitor will determine whether this is an isolated incident or a network wide issue by examining the events from other systems. If no other systems report network connectivity problems, the event is posted as a single incident rather then a net work wide issue. This can significantly reduce troubleshooting and resource allocation time.

SANSGIAC will use Security Manager to continually monitor all production servers. At this time workstations and dumb terminals will not be monitored. An agent is installed on each server that continually monitors the application, system and security log. On servers containing the DNS and DHCP services, the respective logs

will be monitored as well. The term monitored is used because it is a near real time process. Every event that occurs passes through a filter. Depending on the filter rules, the event is ignored or an action is triggered. Every Monday, Wednesday and Friday morning, at 5 am, the entire event log is sent to the central computer. The backend SQL data base stores events for future reporting and analysis. The process of storing the events within a database will also clear the individual audit logs, preventing the need to manually backup and clear each log. In between event log dumps, events that meet the agents filter requirements are sent to the central computer in real time. This allows alerts to be sent in a timely manner. This is a large distinction between passive and active monitoring solutions.

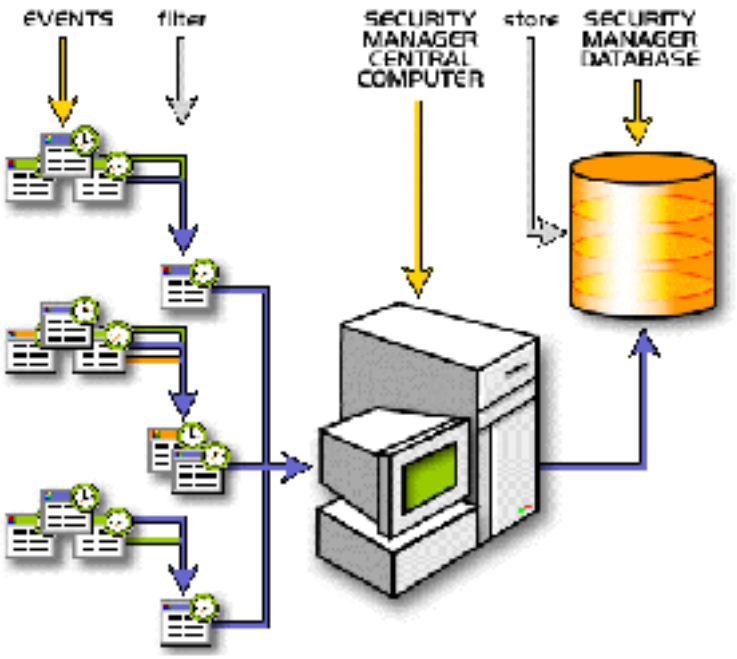


Figure 3-1 Image reproduced, with permission, from NetIQ Security Manager Demo (5)

Within the Security Manager Incident Management Console, in-depth information can be obtained about incidents that have been triggered by the system's event filters. The Alert Description gives administrators a quick synopsis of the problem in addition to offering a possible cause. This type of information is invaluable in freeing up senior administrators and allowing junior staff to manage day-to-day operations. The console will also display any issued alerts and denotes where the event originated. Figure 3-2 illustrates a sample incident where Security Manager identified a system which did not have an antivirus product installed. In this case the filter was looking for the Norton Antivirus product.

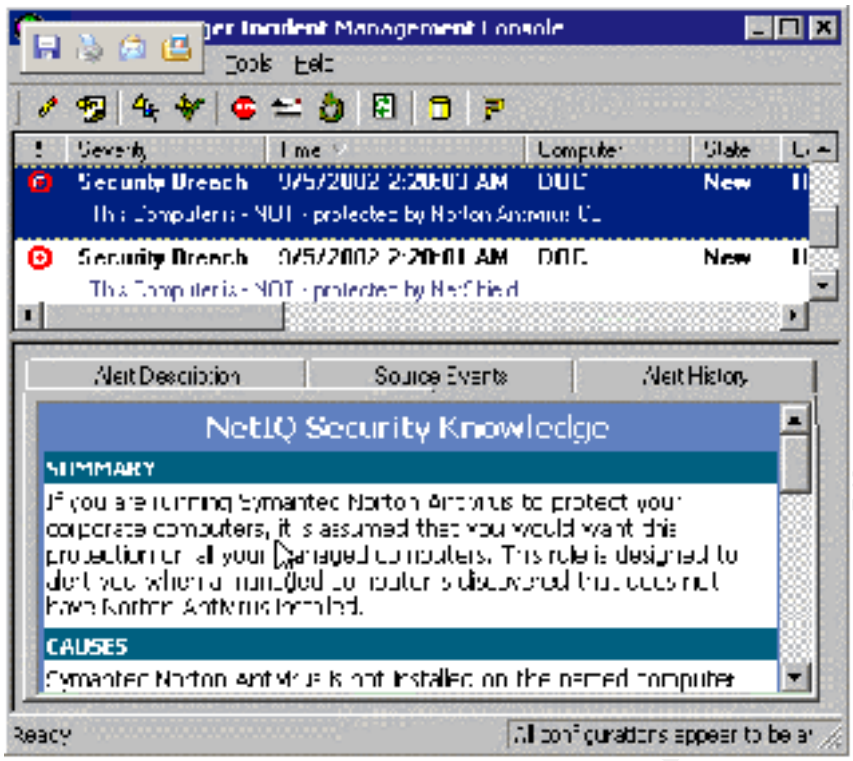


Figure 3-2 Image reproduced, with permission, from NetIQ Security Manager Demo (5)

The following filters have been applied to all agents:

- *Failed logon for Administrator account* – The filter is triggered should the decoy or renamed administrator account post 5 failed logon attempts. The systems administration team will be sent a pager alert.
- *Elevation of Privileges* – The filter is triggered any time an account is either added to the local or domain Admins group. The senior network engineer is sent an email notification.
- *Successful Modification of Group Policies* – The filter is triggered any time a group policy is successfully modified. The senior network engineer is sent an email notification.
- *System Service Halted* – The filter is triggered should any service stop or fail to restart. The systems administration team will be sent a pager alert.
- *Network Connectivity Lost* – The filter is triggered when any network adapter looses connectivity. The network operations team will be sent a pager alert.
- *Group Policy Not Applied* – The filter is triggered when a group policy fails to successfully apply itself to the local machine or user. The senior network engineer is sent an email notification.
- *Firewall Rules Modification* – The filter is triggered when a firewall rule has been modified. The senior network engineer is sent an email notification.

- *Old Virus Definition* – The filter is triggered when a system reports a virus definition with an age exceeding 30 days. The systems administration team is sent an email notification.

Additional triggers will be applied, as they are needed. In situations where a notification would have been useful, a filter should be created an applied to the appropriate system.

SANSGIAC creates formal audit reports on a weekly basis. Audit reports are made available Monday mornings to the Change Management segment for evaluation. The following reports are provided:

- *Virus Definition Revision Level* – This report lists all systems that are currently two or more virus definition revisions behind.
- *Virus Encounters* – This report lists the top 20 systems reporting virus incidents.
- *Firewall Configuration Modification* – This report details any modifications made to the firewall.
- *Security Group Members* – this report lists the members of the following groups: Domain Admins, Enterprise Admins, Schema Admins, DNSUpdateProxy, DnsAdmins.
- *Inactive Accounts* – This report lists all accounts that have expired or have not been used in over 90 days.
- *Weak Password* – This report lists all accounts that do not meet the high security password requirements.

3.3 CONCLUSION

Utilizing automated event monitoring tools reduces the requirement of performing repetitive analytical tasks. Cost plays a major factor in obtaining software such as Security Manager. In many organizations, these tools are thought of as luxury rather than a necessity. However, those that lack even the simplest scripts or automation processes fail to effectively react to security breaches and configuration errors. With new vulnerabilities appearing at ever growing rates, IT managers must consider the potential financial impact of not proactively monitoring the computing enterprise.

References

1. "Accessing Resources Across For est Trusts", http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/x_c_forestauthentication.asp , Microsoft Corp.

2. Fossen, Jason. "Securing Windows: Track 5 Course Materials", 2003, SANS Institute.

3. "FSMO Placement and Optimization on Windows 2000 Domain Contro llers", http://support.microsoft.com/default.aspx?scid=kb;EN -US;223346 , Microsoft Corp.

4. Policht, Marcin. " Exploring Windows 2003 Security: SID Filtering and Software Restriction Policies", http://www.serverwatch.com/tutorials/article.php/2241151 , July 2003.

5. "Security Manager Product Tour", http://www.netiq.com/products/sm/default.asp , NetIQ Corp.

6. Shaw, John W. "Design a Secure Windows 2000 Infrastructure", http://www.giac.com/practical/GCWN/John_Shaw_GCWN.pdf), SANS Institute.

7. "Technical Overview of In ternet Information Services (IIS) 6.0", http://www.microsoft.com/windowsserver2003/docs/IISoverview.doc , April 2003, Microsoft Corp.

8. "When to create External Trusts", http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/domadmin_concepts_explicit.asp , Microsoft Corp.

9. "Windows 2000 Common Criteria Security Configuration Templates", http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/issues/W2kCCSCG/W2kSCGc4.asp , Microsoft Corp.

Last Updated: May 29th, 2017

Upcoming Training

SANS Cyber Defence Canberra 2017	**Canberra, Australia**	**Jun 26, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 06, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**