



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

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

## Interested in learning more?

Check out the list of upcoming events offering  
"Securing Windows and PowerShell Automation (Security 505)"  
at <http://www.giac.org/registration/gcwn>

# "SANS and GIAC Together Again"

GIAC Certified Windows  
Security Administrator  
(GCWN)

Practical Assignment  
Version 3.2 Option 1

Submission Date:  
4/24/2004 10:41 PM

Don Murdoch, CISSP  
GCUX, GCIH, GCIA,  
MCSE, MCSD

SANS Online in  
conjunction with Mary  
Washington College

## Table of Contents

<b>INTRODUCTION.....</b>	<b>1</b>
<b>DOMAIN DESIGN .....</b>	<b>2</b>
EXISTING TECHNOLOGY AT EACH COMPANY.....	2
MERGER GOALS .....	2
SANS Co. DOMAIN DESCRIPTION.....	3
Demographic Population - Main Office (Maryland).....	4
AD OU and Group Structure - Maryland Office.....	5
Demographic Population - Manufacturing Office (Colorado) .....	5
AD OU and Group Structure - Colorado .....	6
Demographic Population - Florida Research/Development Office .....	6
AD OU and Group Structure - Florida .....	7
Demographic Population - Japan Manufacturing Office.....	7
AD OU and Group Structure - Japan .....	8
NETWORK INFRASTRUCTURE DETAILS .....	8
WINDOWS 2000 AD GROUP DETAILS .....	10
GIAC ENTERPRISES DOMAIN DESCRIPTION .....	11
GIAC Enterprises Description.....	11
GIAC Enterprises Active Directory Structure.....	12
GIAC Enterprises Network Infrastructure.....	13
MERGED DOMAIN DESCRIPTION .....	13
MERGING THE DOMAINS.....	14
Phase One - Establish Consistent DNS Environment.....	14
Phase Two - Establish AD Trusts .....	16
Phase Three - Establish Groups.....	22
Phase Four - Establish IIS Servers .....	23
Future Plans.....	23
<b>SECURITY POLICY AND TUTORIAL.....</b>	<b>25</b>
SECURITY CONTROLS .....	26
BASIC DMZ NETWORK CONFIGURATION .....	27
DMZ Domain AD Structure .....	29
DOMAIN WIDE GROUP POLICY (DDP) .....	30
DEFAULT DOMAIN CONTROLLER GROUP POLICY .....	35
WEB SERVER CONFIGURATION .....	36
IIS Server Installation Specific Details .....	36
GENERAL SERVER HARDENING .....	37
WEB SERVER GROUP POLICY DESIGN .....	38
GROUP POLICY TESTING.....	40
GROUP POLICY EVALUATION .....	44
VMWare 4.0 Disconnect.....	45
USER TESTS .....	45
AUDITING WITH MBSA.....	47
<b>ACTIVE DIRECTORY DOMAIN AUDIT.....</b>	<b>49</b>
GATHERING INFORMATION - ROUND ONE .....	50
GATHERING INFORMATION - ROUND TWO .....	51
System Revisions to Elky's Scripts.....	52
Highlights of the Audit System.....	53
System Build Information .....	54

Active Directory Support .....	54
EXAMPLE PROCESSED OUTPUT .....	55
GATHERING PERFORMANCE DATA .....	57
CHECKING SECURITY SETTINGS .....	57
<b>EPILOGUE .....</b>	<b>60</b>
<b>REFERENCES .....</b>	<b>61</b>
GIAC Practical Papers .....	61
Books and Magazine Articles .....	62
Web sites and Web Articles .....	62
<b>APPENDIX A: GPMC RESULTS FOR DMZDC0 .....</b>	<b>64</b>
<b>APPENDIX B: GPMC RESULTS FOR DMZWEB1 .....</b>	<b>74</b>

## List of Figures

Figure 1: SANS Co. Domains.....	4
Figure 2: corp.sans.com Maryland OU Structure .....	5
Figure 3: co.corp.sans.com Colorado OU Structure.....	6
Figure 4: fl.corp.sans.com OU Structure .....	7
Figure 5: jp.corp.sans.com OU Structure .....	8
Figure 6: SANS Co. Network Addresses.....	9
Figure 7: GIAC-E Inner Domain Organizational Units .....	12
Figure 8: corp.sans.com DNS Tests .....	15
Figure 9: SANS DNS Server Configuration .....	16
Figure 10: Merged Domain Trusts.....	17
Figure 11: SANS Trusting GIAC.....	18
Figure 12: Cross Domain Permissions .....	23
Figure 13: Controls Model .....	26
Figure 14: Basic Firewall Network Configuration.....	28
Figure 15: OU's in the DMZ.....	29
Figure 16: DMZ AD Structure .....	29
Figure 17: Default Domain Policy .....	31
Figure 18: Domain Controller Group Policy .....	35
Figure 19: GPCM for DMZDC0 .....	43
Figure 20: GPMC for DMZWEB1 .....	44
Figure 21: Example Successful Logon Audit.....	46
Figure 22: Example Logon Failure Audit .....	46
Figure 23: MBSA on the DC .....	47
Figure 24: MBSA on a Web Server .....	48
Figure 25: MSInfo32 XML Command Output .....	51
Figure 26: Elky's Audit System Illustrated .....	52
Figure 27: Startup GPO .....	55
Figure 28: Audit Summary.....	56
Figure 29: Detailed Audit Report for DC0.....	56
Figure 30: SCAT Analysis of Domain Controller .....	58

Figure 31: SCAT Analysis of IIS Server ..... 58

© SANS Institute 2004, Author retains full rights.

## Introduction

---

There are three sections in this paper. The first section discusses two Active Directory domains from two companies that are merging – SANS Co. and GIAC Enterprises. Second, there is a security policy and tutorial for one of the merged domains IIS servers. The third section is devoted to auditing the two merged domains using the system developed by Steve Elky, and the details of implementing that system.

© SANS Institute 2004, Author retains full rights.

## **Domain Design**

---

There are two domains that are being merged - SANS and GIAC Enterprises. Both companies want to merge the AD domains in a manner designed to support the business goals of the merged company. During the merger negotiations, the IT staff determined that they would not merge one of the Active Directory forests into the other. Therefore, a strategy of allowing users in each domain to make use of resources in the other domains needs to be implemented. This strategy is implemented with inter domain trusts. These trusts will be developed and deployed on this network so that users of various parts of the network will be able to use resources that are appropriate to their job function.

### ***Existing Technology at Each Company***

---

The existing domains for SANS Co. and GIAC Enterprises are based on Windows 2000 and Windows 2003, respectively. Historically, many sites that have extensive Active Directory networks don't adopt the newest technology immediately, preferring to rather wait for an initial service pack to be released. With the merger of the two companies, new requirements for future grow, and additional budget the company will implement a Windows 2003 based domain for its new web infrastructure.

### ***Merger Goals***

---

There are several goals and objectives that must be achieved when merging the two forests. Each goal is listed below.

- People from the appropriate departments from either network need to be able to access common resources (shares, printers, and applications).
- Consistent application of an overall security policy, which will be expressed as Windows 2000 Active Directory Group Policy. As the forests are merged, a consistent companywide set of Group Policy objects (GPO's) will be defined. During this process, some existing group policy objects may be renamed if necessary to provide a consistent naming structure for all GPO's.
- Unified Web presence. Both companies have similar product lines, and the merged company to have a consistent Web presence which allows different product lines and services to be presented in a unified fashion for the customer.
- Centralized security. Ultimately, security management of the various domains within the merged forests must be handled centrally. This means to a central security and administrative team must have sufficient rights to effect the security configuration of the entire network structure should the need arise.
- Decentralized user management. Centrally managing users across multiple domains which span physical sites and time zones is not likely to result in high user satisfaction - and user management would end up

being cumbersome. With this in mind, there must be a primary and secondary person who can create and manage user accounts for individual domains within the network structure.

### ***SANS Co. Domain Description***

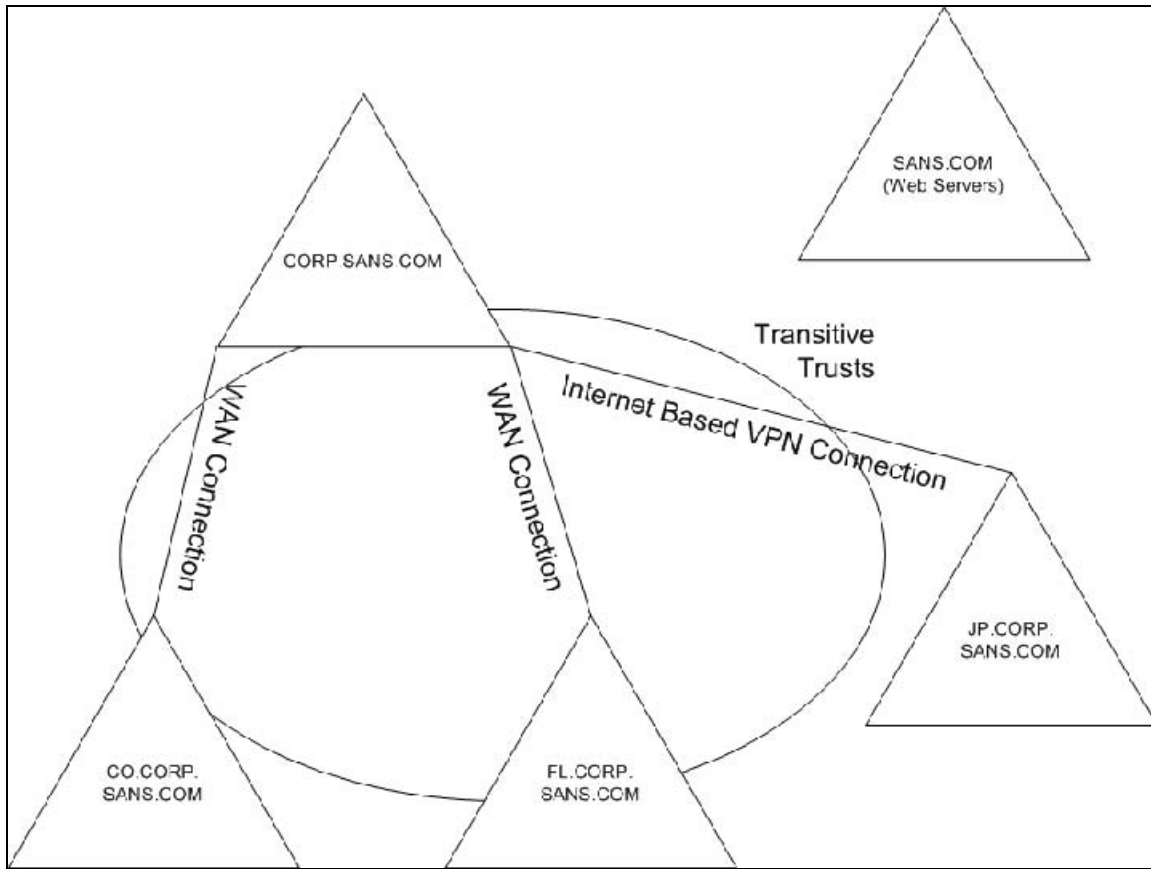
---

SANS Co, is a manufacturer of security hardware and software with four geographical locations. Their main headquarters facility is in Maryland which has the main "corp.sans.com" AD domain. The primary R&D center is in Florida with the AD domain name "fl.corp.sans.com". There are manufacturing facilities in Colorado and Japan with the domain names "co.corp.sans.com" and "jp.corp.sans.com", respectively. The company maintains its web server farm in a completely isolated domain named "sans.com" at the Maryland facility.

SANS Co. "grew up" from a Windows NT based domain model where each location installed its own NT domain. SANS Co. migrated from NT 4.0 to Windows 2000 AD, and in the process formed the parent / child based domain structure. The main "corp.sans.com" domain was installed first, and each of the child domains joined the parent forest as sub domains.

The four domains that are underneath corp.sans.com all maintains standard Active Directory transitive trusts. The web server domain, "sans.com", does not actually trust any of the main corporate domains - meaning that this domain is not a parent to corp.sans.com, or part of the trust scheme. The IT team and made this decision under the premise that it is a compromise within the Web support domain that this type of boundary would make it much more difficult for an attacker to learn information about the main corporate domains. Remote management of the Web domain is accomplished with Terminal Server sessions and firewall rules that the allow staff on the corporate domains to make connections to the Web domain, but not the inverse.





**Figure 1: SANS Co. Domains**

This illustration shows the SANS Co domains and the default trust relationship between the various domains. The "sans.com" DMZ network has IIS web servers and is not trusted by the main domain structure.

### **Demographic Population - Main Office (Maryland)**

**Research and Development:** The R&D department (about 60 people) is the primary department that is responsible for new product development and improving current products. Occasionally R&D hires some temporary workers to help test products, which normally involves making temporary use of the network.

**Sales and Marketing:** This department (about 20 people) is responsible for business development and frequently travels, thus requiring remote access into the network. Several of the staff needs to maintain content on the corporate web site as the company works on its marketing efforts.

**Finance:** There are three people in the finance department who manage the day to day cash and credit management operations of the company.

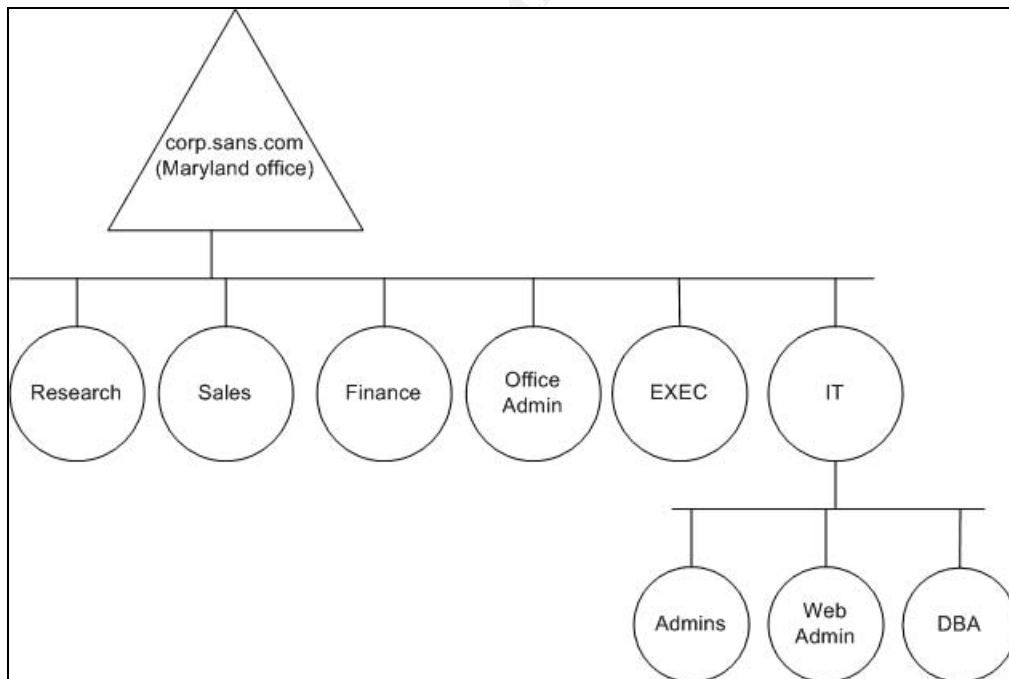
**Admin/Support:** Collectively, there are six people who support general administration for the company - shipping/receiving, receptionist, office manager, several part time general office clerks who support various people.

**Executive:** There are four executives in the company - CEO, CFO, COO/CIO, and the CTO/ISSO. These people are supported by two executive secretaries.

**IT Operations:** There are nine people who support IT operations - three system administrators who maintain the IT/IS environment and also who rotate taking helpdesk calls, two database developers/administrators, and four web content developers who maintain the IIS servers. The web content developers usually support the sales and marketing staff. Management of the domain(s) is directed by this group, meaning that the parent organization drives and directs policies for the parent and child domains.

### **AD OU and Group Structure - Maryland Office**

Below is an illustration of the OU structure for the Maryland location. Not shown in the illustration is a "Workstation" OU which has the PC's for the appropriate department.



**Figure 2: corp.sans.com Maryland OU Structure**

### **Demographic Population - Manufacturing Office (Colorado)**

This office has departments which support company manufacturing operations.

**Manufacturing Operations:** This department has seven managers and about fifty full time assembly operators and product packagers. Managers have PC's and perform a variety of computer tasks while the remaining staff have access to some kiosk PC's in the break room for Internet access (at lunch!), reading email, and access to Office applications.

**Sales:** There are four sales people based out of this office.

**Office Support:** There are a few people who generally support the facility - a receptionist/office clerk, HR generalist, a local system administrator, and a secretary for the divisional VP.

### AD OU and Group Structure - Colorado

Below is an illustration of the OU structure for the Colorado location. Not shown in the illustration is a "Workstation" OU which has the PC's for the appropriate department.

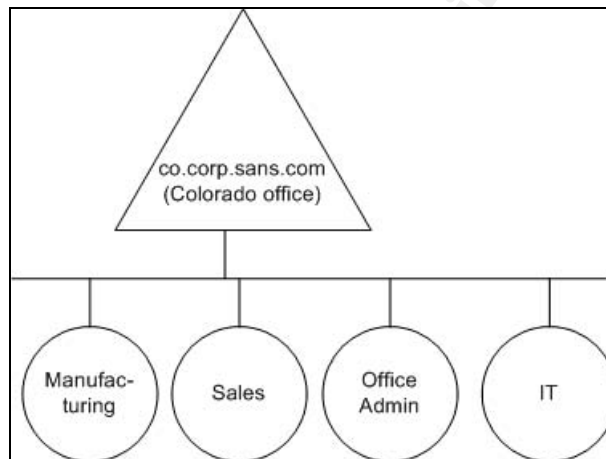


Figure 3: co.corp.sans.com Colorado OU Structure

### Demographic Population - Florida Research/Development Office

This office only has a few departments.

**Research and Development:** Functionally about the same as Maryland's, with about 50 people. This staff mainly consists of both hardware developers, software developers, documentation writers, and a few managers.

**Executive:** There is one VP for Florida operations who fills the COO/CTO role. He is supported by one secretary.

**Sales:** There are two sales people based out of this office.

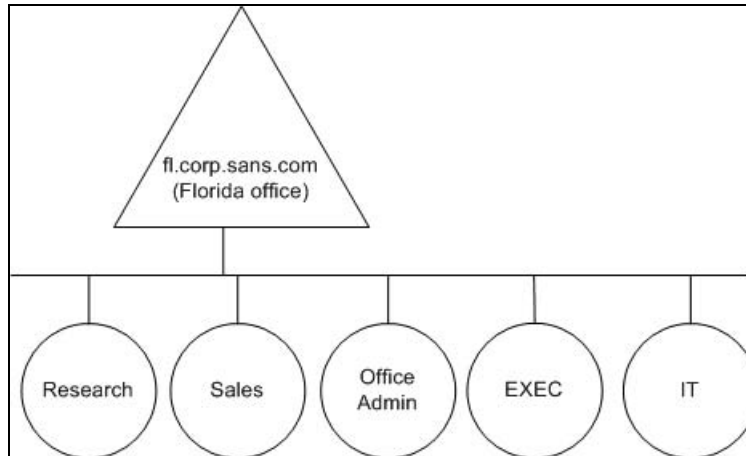
**Office Support:** There are a few people who generally support the office - a receptionist/office clerk, a local system administrator, HR generalist, and a secretary for the divisional VP.

**IT:** There is a single person who maintains the IT infrastructure in this location.

### **AD OU and Group Structure - Florida**

---

Below is an illustration of the OU structure for the Florida location. Not shown in the illustration is a "Workstation" OU which has the PC's for the appropriate department.



**Figure 4: fl.corp.sans.com OU Structure**

### **Demographic Population - Japan Manufacturing Office**

---

This office has departments which support company manufacturing operations and business operations specific to the Japanese economy.

**Manufacturing Operations:** This department has seven managers and about fifty full time assembly operators and product packagers. Managers have PC's and perform a variety of computer tasks while the remaining staff have access to some kiosk PC's in the break room for Internet access (at lunch!), reading email, and access to Office applications.

**Sales and Marketing:** There are four sales people based out of this office. There are two part time people who produce documentation in Japanese for company products, and occasionally people with other language skills perform translation services.

**Office Support:** There are a four people who generally support the facility - a receptionist/office clerk, finance person, HR generalist, and a secretary for the divisional VP.

**IT Operations:** There are five people who support IT operations - two system administrators who maintain the IT/IS environment and also who rotate taking helpdesk calls, one database developers/administrator, and two web content developers who maintain the IIS servers. The web content developers usually

support the sales and marketing staff and are conversationally fluent in English and Japanese.

### AD OU and Group Structure - Japan

Below is an illustration of the OU structure for the Japan location. Not shown in the illustration is a "Workstation" OU which has the PC's for the appropriate department.

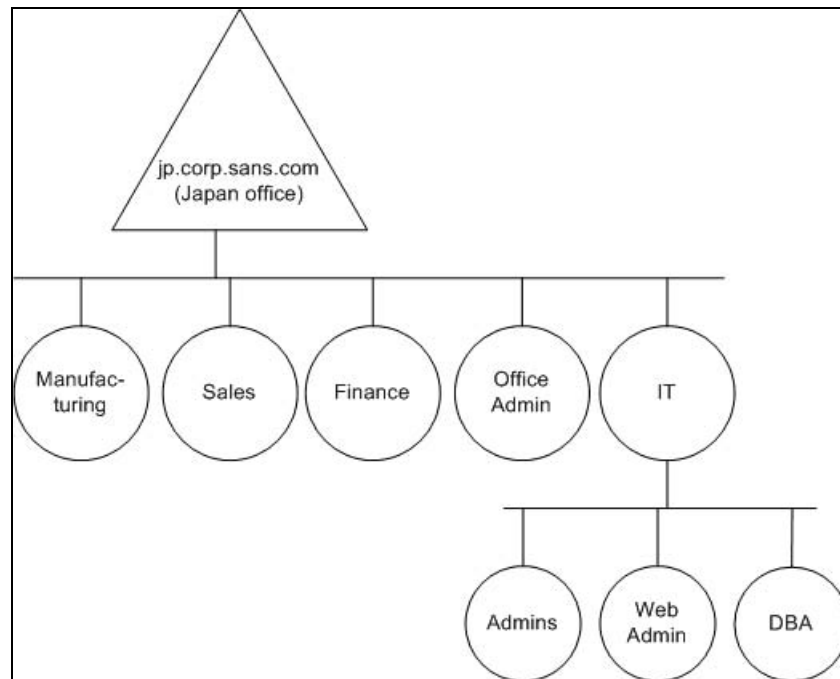


Figure 5: jp.corp.sans.com OU Structure

### Network Infrastructure Details

SANS Co. has several internal networks that it needs to manage. Early in the companies' development SANS standardized on the 192.168.X.X private IP address space, allocating four (4) Class C<sup>1</sup> networks for each office location. This plan allowed for a variety of configurations - different networks for servers and workstation and, segmented workstation networks being two. By using this method of address allocation general network management is much easier, as well as keeping track of systems on the network. The IP addressing scheme in use at SANS is shown in the next figure.

The various CONUS<sup>2</sup> locations on the network are connected via normal T1 leased lines. The OCONUS<sup>3</sup> site, Japan, has a L2TP/IPSec based VPN

<sup>1</sup> A Class C network has a 24 bit network mask. Since an IP Ver. 4 address is 32 bits long, eight bits are allowed for host addresses. Given that 0 for a host number corresponds to the network number, and given that 255 for a host number is the broadcast address, there is room for 254 distinct hosts on each of the Class C networks.

<sup>2</sup> CONUS: CONTinental UNITED States

connection. This connection is implemented using Cisco 3000 series routers with a router to router based VPN. SANS Co. preferred using a hardware based solution for establishing the VPN since it meant that there was an additional layer of security between the Windows servers and networks at each end. SANS implemented this design as a defense in depth measure - by using different VPN and IPsec technology an attacker needs to violate the integrity of the Cisco hardware and then is faced with penetrating the Windows domain's security measures.

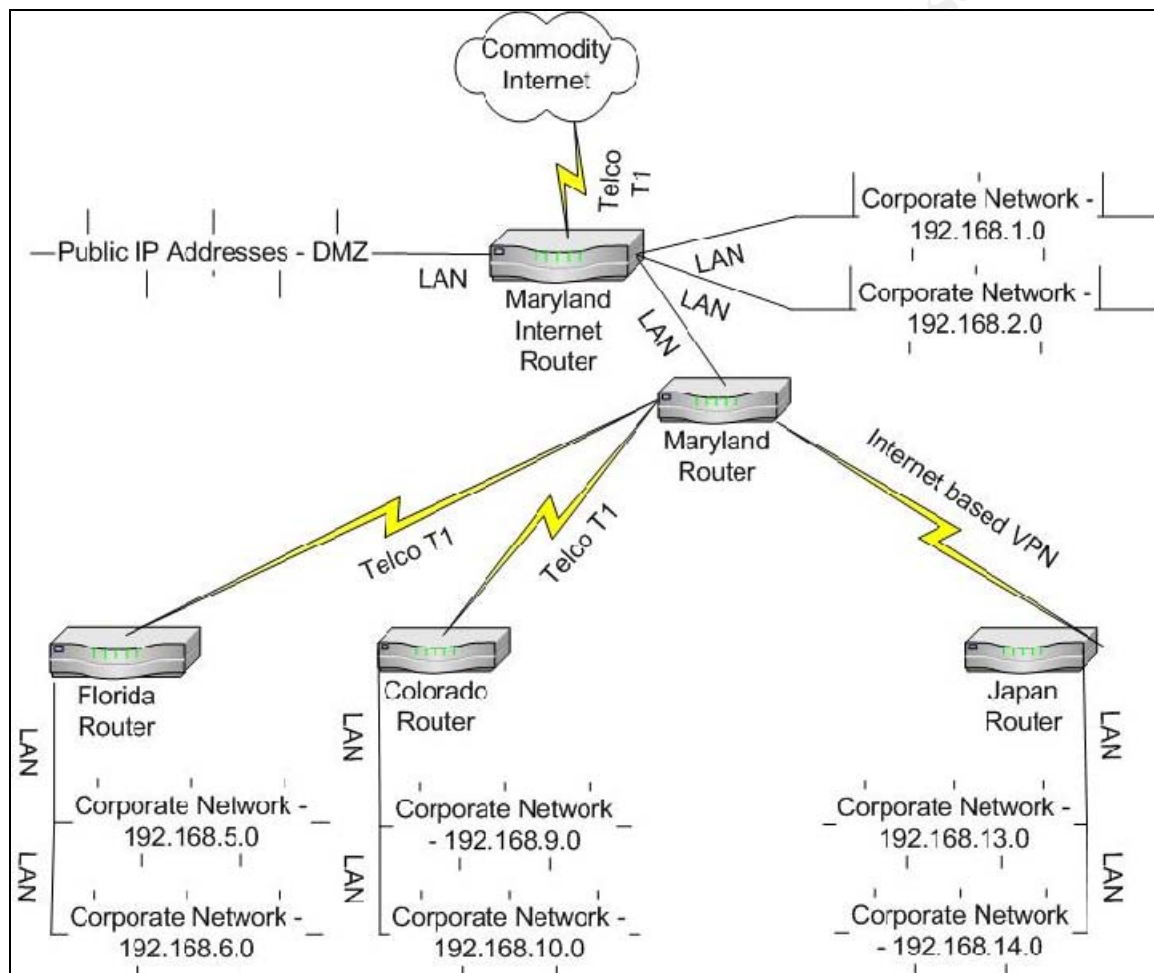


Figure 6: SANS Co. Network Addresses

Each location (MD, CO, FL, and JP) has similar hardware, by function, on site. Below is a list of the basic type of network servers with configuration details at each location.

- Domain Controller One
  - Dual processor system with at least 1 GB RAM and RAID 5 Ultra SCSI storage

<sup>3</sup> OCONUS: Outside CONUS.

- Global Catalog server
- Primary DNS server for the site
- DFS share for users home directories
- FSMO<sup>4</sup> roles of PDC Emulator and Relative ID Master
- DHCP server<sup>5</sup> with 70% of the DHCP scope configured
- Print server functions
- Domain Controller Two
  - Dual processor system with at least 1.5 GB RAM and RAID 5 Ultra SCSI storage
  - Global Catalog server (for redundancy)
  - Secondary DNS server for the site
  - FSMO role of Infrastructure Master
  - DHCP server with 30% of the scope (fault tolerant configuration)
  - Local Exchange server
  - Print server functions

SANS Co. installed Exchange (a messaging and groupware application platform) on the secondary domain controller primarily due to cost. It was much less expensive to provision a server that had a little more capability (larger disk and more memory) than it was to provision a server just for Exchange. SANS Co. also isn't adverse to putting a few functions on a single server, provided there is sufficient resource (CPU, memory, and disk) as this is an overall cost savings in hardware, operating system licenses, cabling, and switch ports.

### ***Windows 2000 AD Group Details***

---

SANS Co. is sensitive to general domain administration. In order to implement the principle of least privilege and wherever possible, the principle of separation of duties, SANS Co. has implemented these rules:

- Persons charged with Windows system administration login with a normal user account and use the Windows RunAs feature to run various administrative tools. The supervisor account is the same as their user account with the suffix "adm" - this makes reading logs and other event information easier.
- There is only one person in each domain who owns an account<sup>6</sup> in the Enterprise Admins and Schema Admins group - these groups have extra capability in the domains and are guarded with some care.

---

<sup>4</sup> FSMO: Flexible Single Master Operations. Active Directory has five (5) specific roles that are assigned to various servers in a domain. In any domain where there are multiple domain controllers the FSMO functions must be distributed to different systems - they cannot all be on one server. The Domain naming master and the Schema Master are at the main Maryland site, as there can only be one server with this role in an AD forest (Microsoft support articles 324801 and 197132).

<sup>5</sup> It is considered a security risk to have DHCP on the same server as DNS because of the ownership of records in DNS. If there were sufficient budget, SANS would separate out the function. Given that the environment is a well controlled corporate environment, SANS Co.'s IT staff thought that this was an acceptable risk.

- The HR director has delegated authority to change passwords - this person has "skin in the game", is usually at work, and would be informed if a person quits (or is terminated). Therefore, SANS Co. decided that it is acceptable for the HR director to have the ability to change a user's password.
- DBA's are not Domain Administrators, as they need supervisory access to the RDBMS and not complete supervisory access to the operating system or server. Some are members of the Server Operators group - they may need to actually reboot the server on occasion.
- Helpdesk staff have delegated authority to change users passwords, create accounts, and reset account lockout status, as this is a job function. There is also a software install account which is in the local administrators group on workstations so that Helpdesk staff can install software and make other administrative changes necessary for users to run various applications on the system. The password is site specific, changed monthly, and only known by HelpDesk staff.

### ***GIAC Enterprises Domain Description***

---

*The GIAC Enterprises Active Directory and network infrastructure is based on Jason Lam's GCWN practical assignment<sup>7</sup>. This section discusses his Active Directory design as the basis for the GIAC Enterprises network.*

### **GIAC Enterprises Description**

---

GIAC Enterprises (GIAC-E) is an eCommerce based company that manufactures products and is heavily dependant on its web presence for sales and customer support. There are four main departments at GIAC-E, described below.

**Research and Development:** This department develops new products for the company. There are about 50 full time people, and up to 10 part time people may be working in the department at any one time.

**Sales and Marketing:** This department is responsible for all of the companies' business development efforts and has about 50 people. This department is based in a satellite office, about 20 miles from the main office. The satellite is connected to the main network by a WAN connection.

**Human Resources and Finance:** Internal accounting is handled by this 25 person department.

---

<sup>6</sup> Owning an account means that the person (the employee) has and uses a specific account which is associated with that person.

<sup>7</sup> URL: [www.giac.org/practical/Jason\\_Lam\\_GCWN.pdf](http://www.giac.org/practical/Jason_Lam_GCWN.pdf). Mr. Lam's practical was chosen because of its' illustrations and good description of the company.



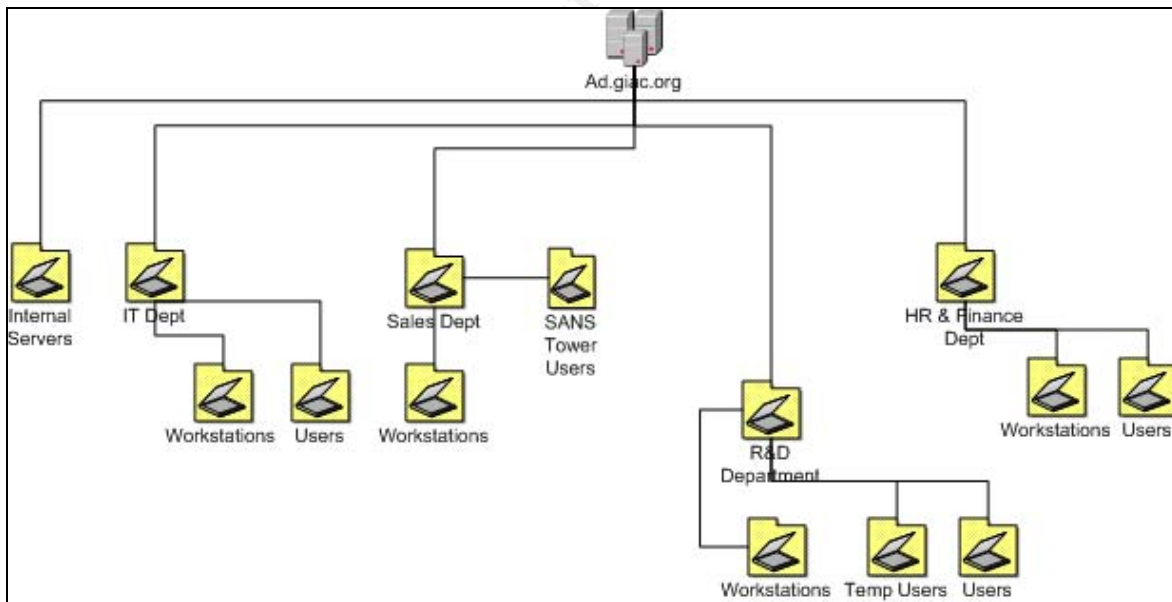
**Operations and Information Technology:** This department supports the web site and is under stress to keep a high server uptime. Servers and all IT infrastructures are maintained by this department.

### GIAC Enterprises Active Directory Structure

There are two Active Directory forests at GIAC-E. One servers the main company network, and the second is a small, isolated domain that supports the web servers in the DMZ. These AD forests are not connected (they do not share a trust relationship) and two forests provide a strong logical boundary. Staff who require access to the DMZ based domain are assigned credentials as appropriate in support of their job function.

The DMZ domain uses the "giac.org" namespace and the internal domain uses the "ad.giac.org" namespace. Neither domain has a child domain. Each major department described above is implemented as an Organizational Unit (OU). The internal domain does not support any Internet based functions, as these are all served from the DMZ domain.

There are several OU's in the GIAC-E internal domain which support the business groups defined above. Graphically, the domain's OU structure is illustrated in the next figure.



**Figure 7: GIAC-E Inner Domain Organizational Units**

The DMZ domain has three OU's to support its function:

- **webservOU**: This OU has the five web servers in the DMZ.
- **dbminOU**: Staff who are database administrators are in this OU.
- **dbOU**: The single RDBMS server is in this OU.

The web servers and the database server are separate so that Windows CCM features can be used to apply service packs and updates to the different systems on different schedules.

### **GIAC Enterprises Network Infrastructure**

---

At the workstation level, GIAC-E uses the following environment:

- Workstations use Windows 2000.
- Servers and domain controllers use Windows 2003.
- The external web servers use Windows 2000 Advanced Server, specifically for its support of Network Load Balancing (NLB), and IIS 5.

There are two main portions of the GIAC-E network. The main headquarters office has the majority of the staff and computer systems. The satellite office has enough servers (including a domain controller) and infrastructure to support the sales staff. Both offices are connected with a Virtual Private Network (VPN) over common Internet connections. At the main headquarters office there is a separate firewall which protects the DMZ network (where the web servers are) and the main corporate network from the Internet.

The DMZ network has five IIS servers running on Windows 2000 Advanced Server which is configured to support Network Load Balancing (NLB). There is also a messaging server and a database management system support server.

### ***Merged Domain Description***

---

The new company, "SGC"<sup>8</sup> (for SANS GIAC-E Corporation), is made up of the two companies merging. With the merger there will be an expanded product line, a larger sales force, more IT staff, and (unfortunately) some redundancy in some of the operational groups (HR and finance). The newly formed company will revamp its web presence in order to provide a single catalog, an integrated customer database (merged from each company), and more consistent credit terms.

There are several requirements that must be met in the merged environment. These include:

- Consistent, single web site (catalog, customer database, order handling, and invoicing).
- Web management should be handled by one group, meaning that they are unified and consistent in how they update content, the product catalog, and the overall tools that are used.
- Groups from the original two companies who have similar job functions need to be able to access all company resources related to that job

---

<sup>8</sup> This acronym should not be confused with the headquarters for a popular science fiction show which should be entering its eighth season on the SciFi channel. Note that the domain name "SGC.COM" is taken, so the merged company had to choose "SANSGIACCRP.COM", which was available as of April 1, 2004.

function. For instance, both sales groups need access to common sales resources.

- Improve security such that both sides have the same or higher levels of security (don't lower either company standards).
- Maintain a level of decentralized administration by making use of AD's delegation of authority.

Once the networks and domains are merged several technical issues need to be resolved. These include:

- DNS based name resolution.
- Consistent VPN settings for remote users and remote networks.
- Users need to be able to logon in either location.
- Ability to build and maintain trusts between the two independent domains.
- Consistency in the application of group policy.

### ***Merging the Domains***

---

The first phase in the merger is to establish trusts between the various SANS domains and the GIAC-E domain. This is accomplished by building trusts. The second phase is to merge the web servers - actually to eliminate one set (GIAC's) set of web servers and to have only one set of web servers that provide the overall Internet presence.

### **Phase One - Establish Consistent DNS Environment**

---

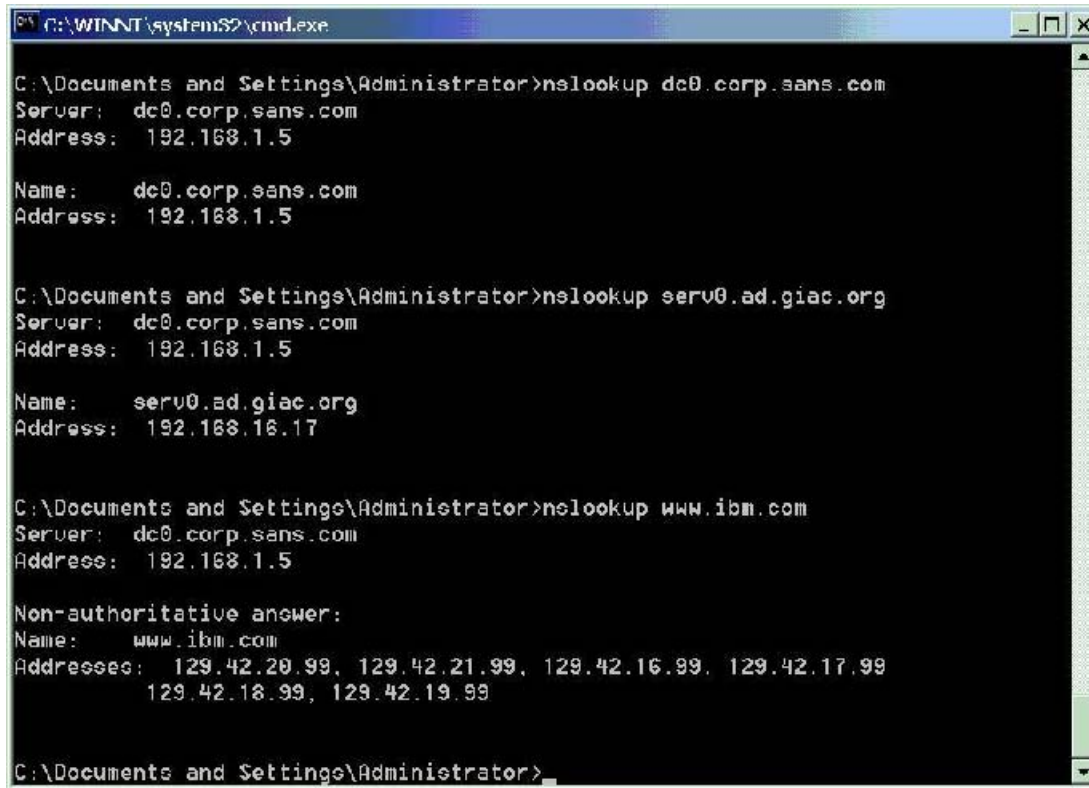
It is absolutely critical that a proper DNS environment be configured before any Active Directory trusts are built. Windows 2000 makes extensive use of DNS; without a properly updated dynamic DNS system in place proper Windows 2000 operation is next to impossible in a routed network. In order to achieve a contiguous DNS space, IP addresses were reviewed. GIAC needed to restructure its DNS configuration so that the site could fit into SANS model. IP addresses were changed from 10.X.1.X/24<sup>9</sup>- 10.X.4.X/24 to 192.168.16.0/24 to 192.168.19.0/24.

After the IP address change settled in, the SANS DNS server was configured as a secondary for the GIAC DNS server. By making this configuration change servers in the SANS network can locate servers in the GIAC network via a recursive DNS lookup because local domain DNS servers are configured to forward DNS requests to their parent DNS domain server. A secondary reverse lookup zone was also configured so that reverse lookups can properly occur. Once the DNS servers were configured, DNS queries were tested - with satisfying results - as shown in the next screen capture. There are three specific tests run from a client in the "corp.sans.com" domain. First, an `nslookup` test to show that the primary DNS server can be reached. Second, another `nslookup`

---

<sup>9</sup> This particular IP address notation is called "Classless Internet Domain Routing" (CIDR). The /24 syntax means that the IP address has a 24 bit subnet mask. Here, the 10.X.X.X private IP address space is subnetted out to function like a class C network.

test to show that the primary DNS server can resolve addresses (as a secondary) for the GIAC domain. Third, basic forwarders are tests (DNS server points to the local ISP) to make sure that the system is properly configured after it has had new information added to it.



```
C:\WINNT\system32\cmd.exe

C:\Documents and Settings\Administrator>nslookup dc0.corp.sans.com
Server: dc0.corp.sans.com
Address: 192.168.1.5

Name: dc0.corp.sans.com
Address: 192.168.1.5

C:\Documents and Settings\Administrator>nslookup serv0.ad.giac.org
Server: dc0.corp.sans.com
Address: 192.168.1.5

Name: serv0.ad.giac.org
Address: 192.168.16.17

C:\Documents and Settings\Administrator>nslookup www.ibm.com
Server: dc0.corp.sans.com
Address: 192.168.1.5

Non-authoritative answer:
Name: www.ibm.com
Addresses: 129.42.20.99, 129.42.21.99, 129.42.16.99, 129.42.17.99,
          129.42.18.99, 129.42.19.99

C:\Documents and Settings\Administrator>
```

Figure 8: corp.sans.com DNS Tests

In addition to the DNS lookup information, a screen capture of the DNS console is provided to show how the dc0.corp.sans.com DNS server is configured to be a secondary server for the "ad.giac.org" domain.

© SANS Institute

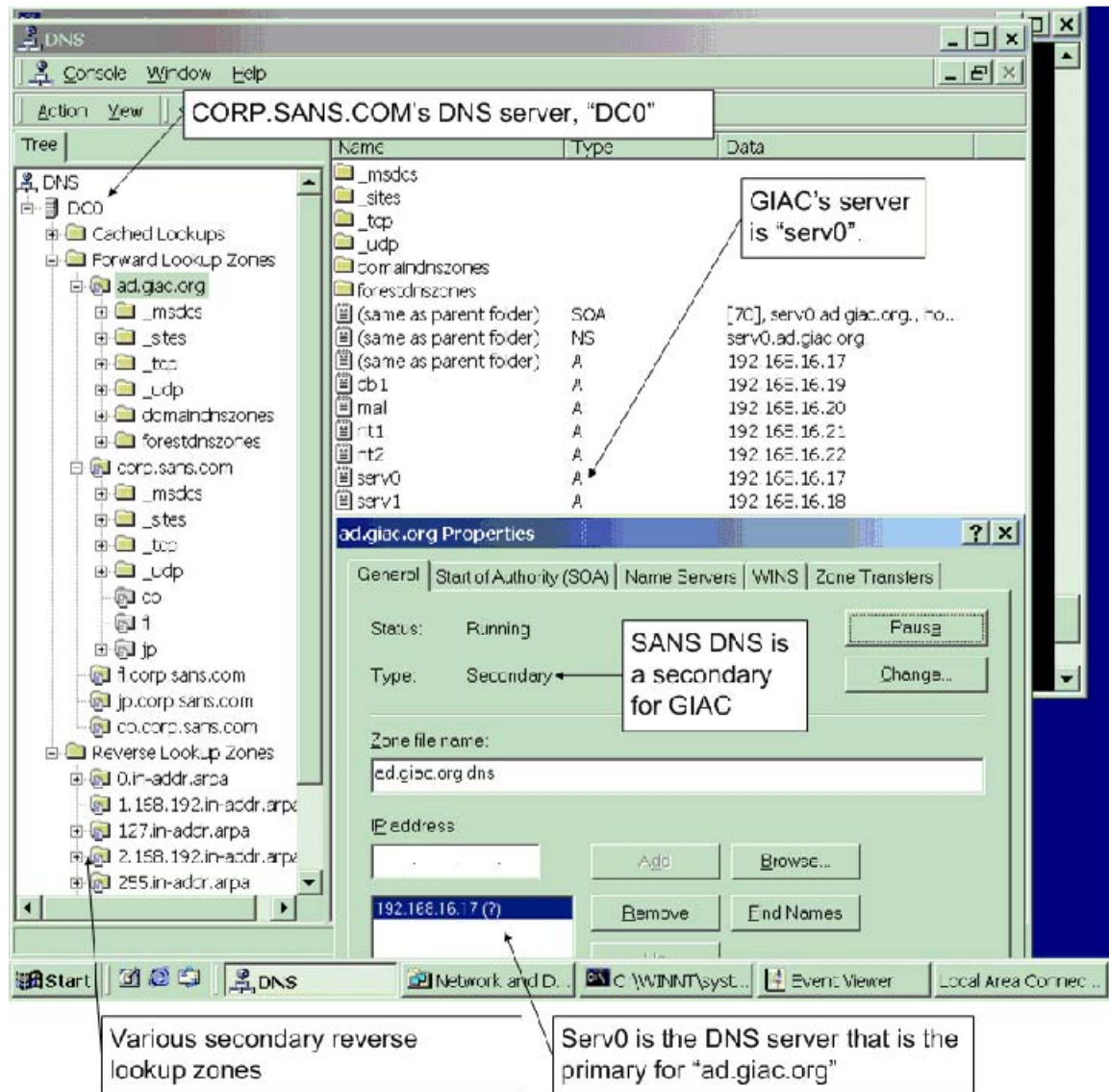


Figure 9: SANS DNS Server Configuration

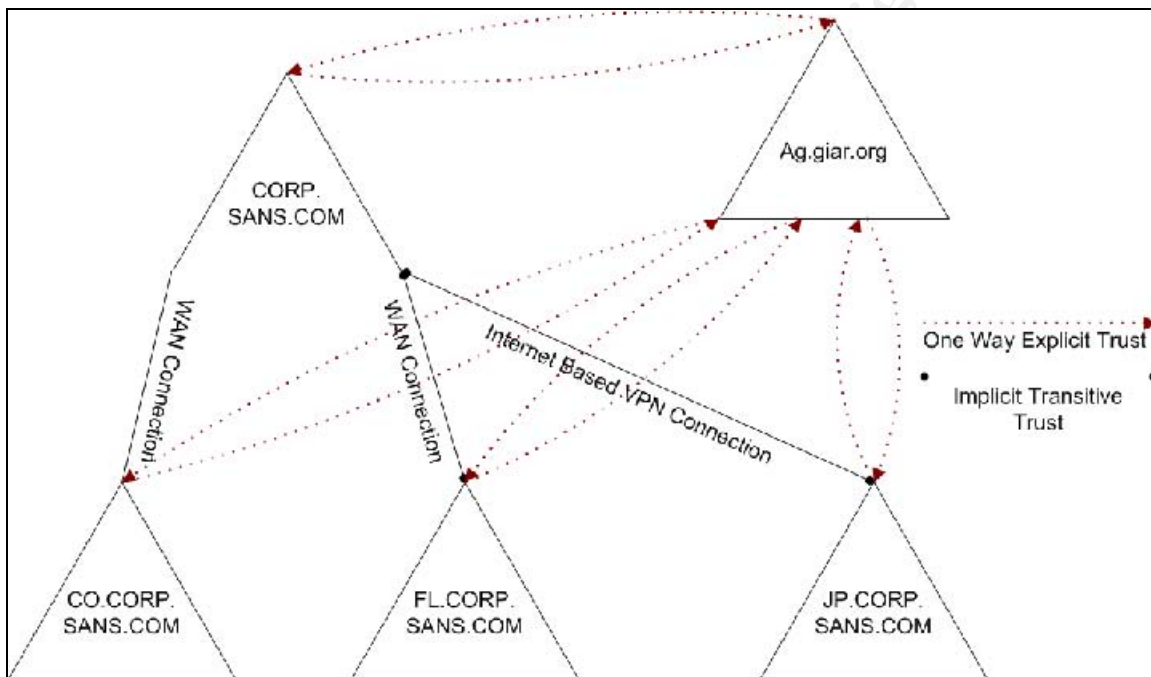
## Phase Two - Establish AD Trusts

Users in the SANS domains need to be able to access resources in the GIAC-E domains, and vice-versa. The security mechanism for allowing a user to authenticate to resources in another domain is called a *trust*. Historically, there are two sides to trusts in the Microsoft domain based networking world. First, there is the *trusting* side, and second there is the *trusted* side.

In this case, when a trust relationship is established between SANS and GIAC, users from SANS can log on to the SANS domain and then access resources (shares, printers, and applications) in the GIAC-E domain - without having to enter a username and password. In this specific example, SANS is the *trusted* domain and GIAC-E is the *trusting* domain. GIAC will trust SANS that the user is a legitimate user. In order for the converse to be true, GIAC needs to trust

SANS. Note that in order for users to have access to resources they need to be granted permissions - as they normally would in the domain itself. In the various user interfaces where permissions can be set other domains will not appear unless a trust relationship exists.

Trust relationships are built between the domains by using the Active Directory Domains and Trusts console snap in, with the trusts illustrated in the next figure. This procedure is described in the Microsoft support article "HOW TO: Set up a One-Way Non-Transitive Trust in Windows 2000"<sup>10</sup>. Here, the same procedure is used twice - once in each direction of the trust.



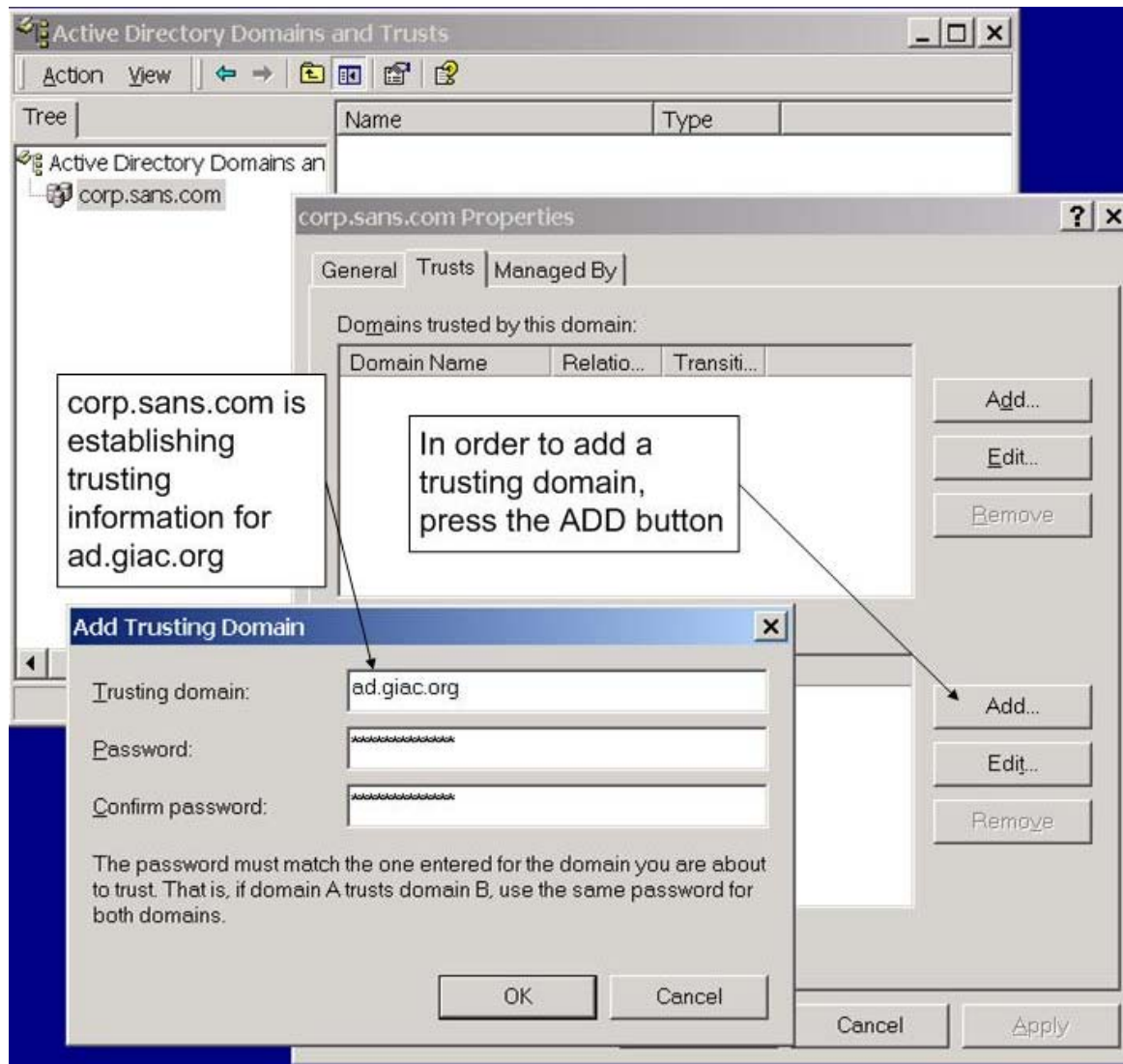
**Figure 10: Merged Domain Trusts**

Creating the trust is a straight forward process, as outlined in these steps below. These steps establish a trust between the "corp.sans.com" domain and the "ad.giac.org" domain, and are illustrated in the next figure.

1. In the "trusted" domain - from "corp.sans.com" - open up the Active Directory Domains and Trusts console.
2. Click "Add" in the "Domains that trust this domain" pane.
3. In the dialog box, enter the name "ad.giac.org" as the "trusting" domain.
4. Enter the agreed upon strong password (as an example, "as23fg76\$%#@ui90") twice in the dialog and press OK.
5. Next, enter in the name / password of an administrative user in the trusting domain - "ad.giac.org" - that can complete creating the one way trust.

<sup>10</sup> URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;309682&Product=win2000>



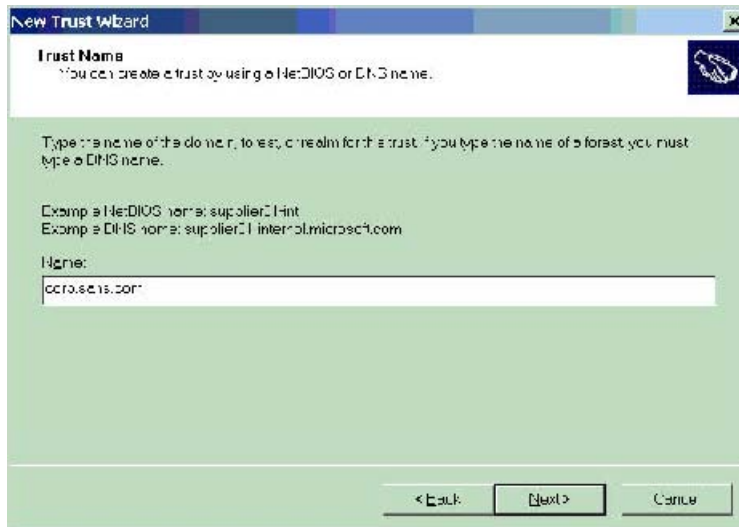


**Figure 11: SANS Trusting GIAC**

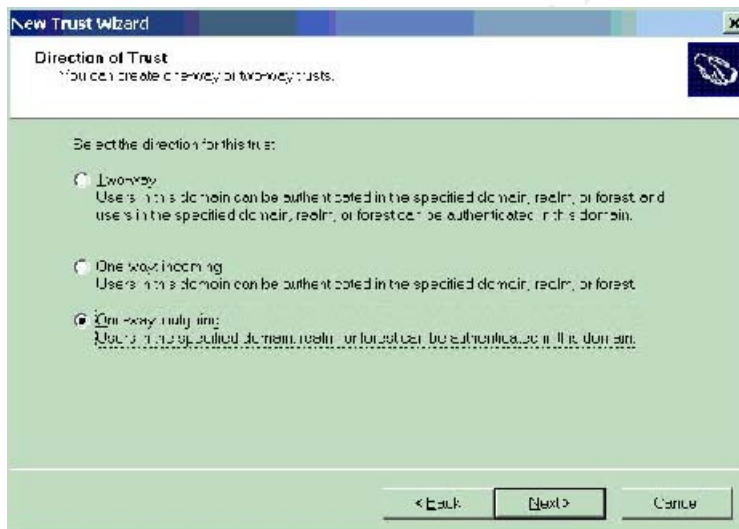
The procedures to create the second half of the trust in Windows 2003 are outlined below<sup>11</sup> (as adapted from a Microsoft Knowledge base article).

1. Open Active Directory Domains and Trusts.
2. In the console tree, right-click the domain that you want to establish a trust with, and then click Properties.
3. Click the Trusts tab, and then click New Trust to start the New Trust Wizard and click Next.
4. On the Trust Name page, type the DNS name or NetBIOS name of the domain, and then click Next.

<sup>11</sup> These procedures come from Microsoft Support article 816301. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;816301>

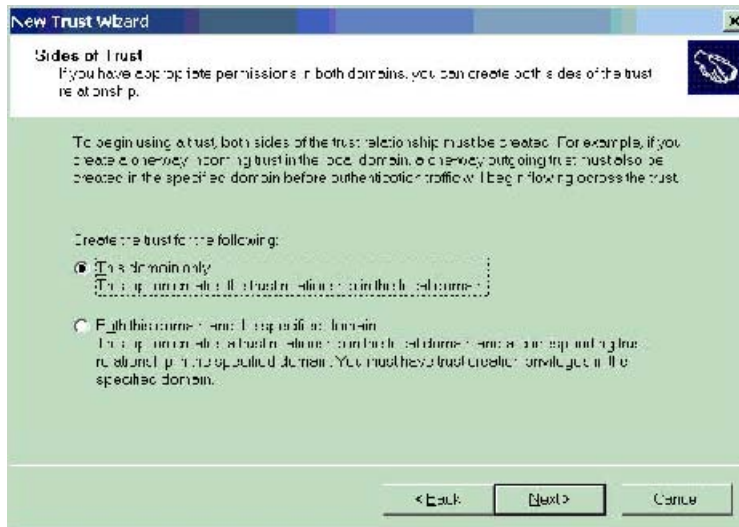


5. On the Trust type page, click External trust, and then click Next.
6. On the Direction of Trust page, create a "One way outgoing" trust, and then click Next.

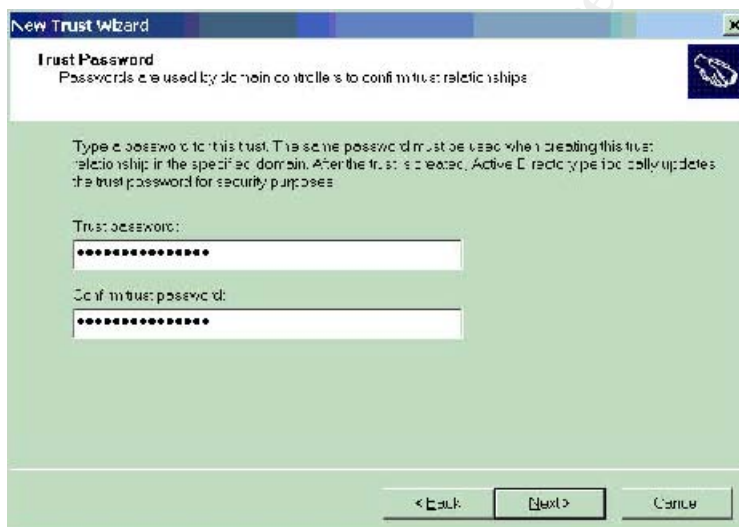


7. On the "Sides of Trust" page, select "This Domain only", and then click Next. This option is chosen because the other side of the trust exists already.

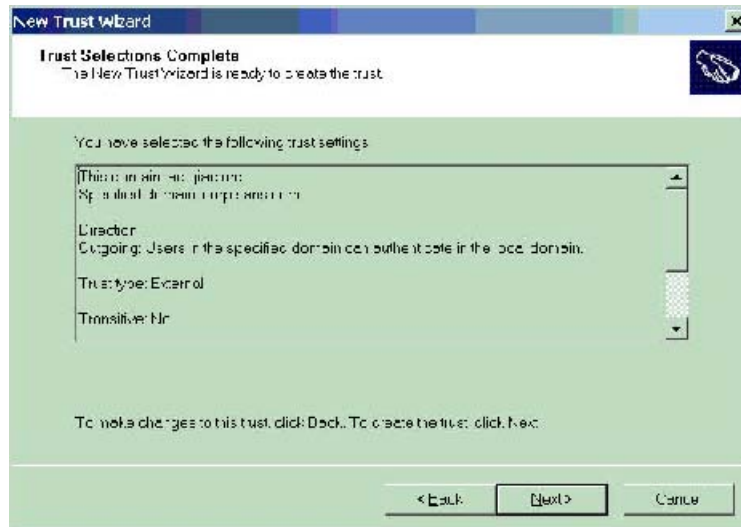




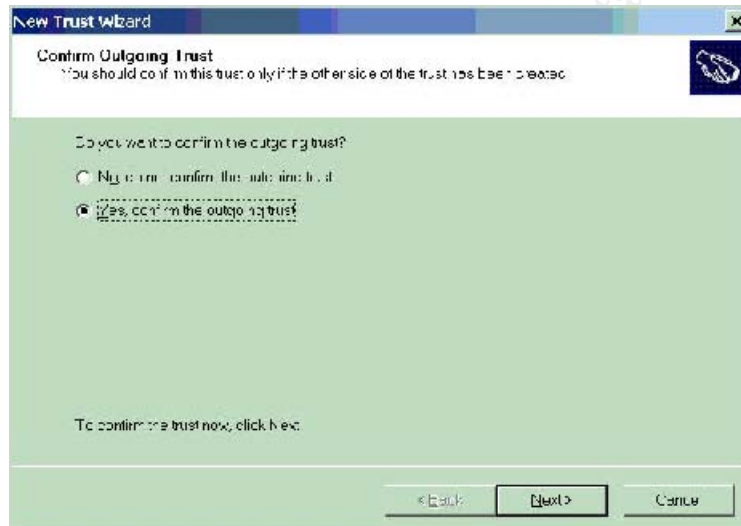
8. On the Trust Password page, enter in the trust password from above, and then click Next.



9. Next, the Trust Selection Complete dialog appears. Click Next.



#### 10. On the Confirming Outgoing Trust.



11. After the trust is confirmed (a popup appears and indicates whether the trust was successful or not), the trust can be validated. This is a good step to perform, as it reconfirms that the trust is actually working as a username and password needs to be entered which is actually checked against the other domain.



Over time, as needed, the domain trust can be verified by using the Active Directory Domains and Trusts tool, reviewing the properties, and clicking on "Verify" (Windows 2000) or "Validate" (Windows 2003).

### Phase Three - Establish Groups

In order for the various domains to allow for proper identification of people based on role and location the merged companies decided to rework group naming conventions. By having consistent names for the various groups administrators can better control access to network resources (BackOffice applications, shares, NTFS file systems, and printers).

The naming convention follows the patten of:

LC\_Role\_Postion.

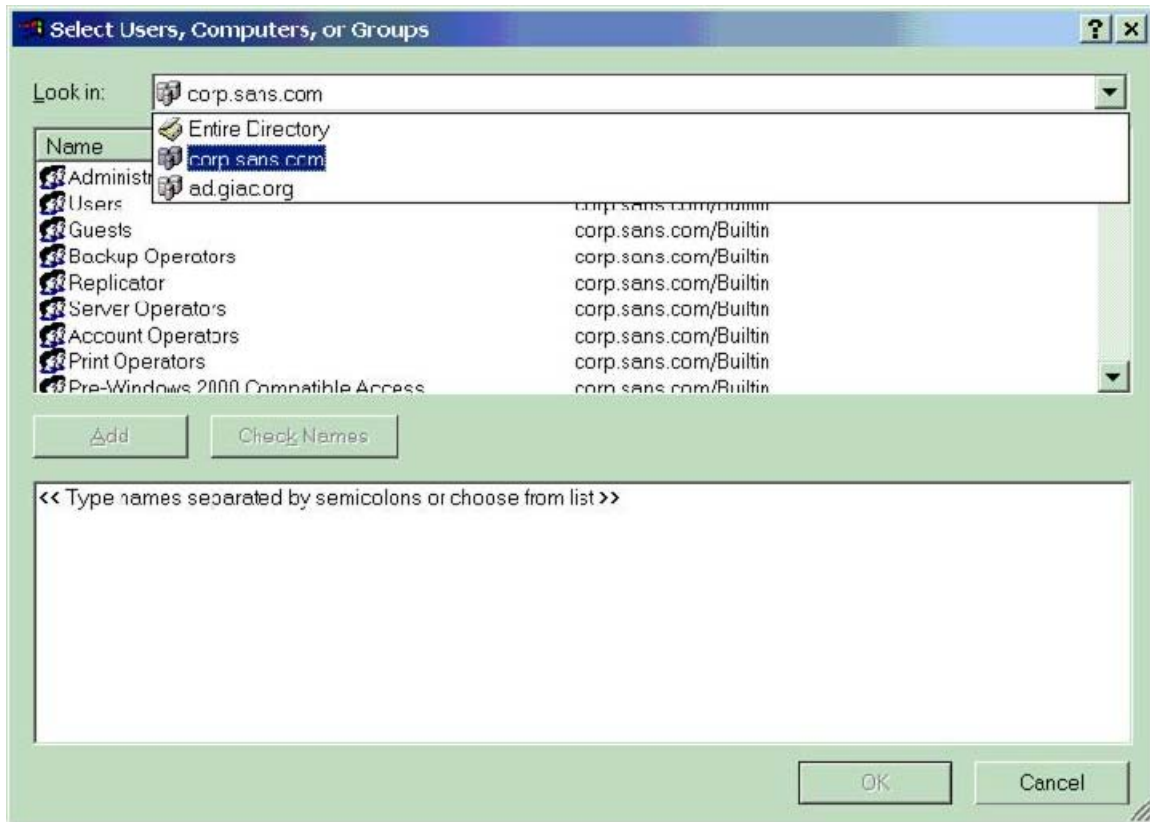
Where:

- LC - Location code (MD, CO, JP, FL, GC), where GC stands for GIAC.
- Role - This is a one or two capitalized word that indicates the department.
- Position - This is one of three options - Staff, Manager, or Temp.

Examples:

- MD\_Sales\_Managers: This group is for the managers of the Sales department from the Maryland location.
- FL\_OfficeAdmins\_Staff: This group is for the Florida general office staff.
- GC\_Research\_Temp: GIAC Research and Development department's occasional temporary workers.

Once groups are established, users in different domains can be added to shares, printers, and BackOffice applications. An example is shown in the next screen capture. The naming convention is shown as well as two of the domains (only one trust exists at this point):



**Figure 12: Cross Domain Permissions**

Once this sequence is complete - creating, verifying trusts, group names, and cross domain permissions - the same process is completed for each of the remaining domains with GIAC-E (ad.giac.org).

## Phase Four - Establish IIS Servers

The best that the merged company has to offer is GIAC's Windows 2003 based IIS servers. IIS 6 and Windows 2003 have better security features than IIS 5 and Windows 2000, so it makes good sense to build on the experience. This is the subject of the next major section.

## Future Plans

Once the domains are integrated and the web servers are fully integrated, then the SANS domain will be upgraded to Windows 2003<sup>12</sup>. Once the SANS domain

<sup>12</sup> Forest Trusts are discussed in the Resource Kit documentation for Windows 2003: URL: <http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en->

is upgraded a "Forest Trust" can be setup for the two domains. Forest trusts have several advantages<sup>13</sup>.

1. Eternal trusts are not needed - one single trust is all that is required.
2. Trusts that are complete and two-way everywhere in both forests.
3. Login authentication with User Principle Names (UPN's).
4. A feature called "SID Filtering", which helps to prevent users from attempting to scrumptiously gain elevated access privileges in the domain.

---

<sup>13</sup> Forest trust features are described in the online resource kit, URL:  
[http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/x\\_c\\_forestrusts.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/x_c_forestrusts.asp)

## Security Policy and Tutorial

---

What, exactly, is a "security policy?" After some research, this quote from Karen Guglielmo has this to say about security policies:

"In business, a security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets. A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change."<sup>14</sup>

This section describes the security policy for the newly merged companies' Active Directory network, and then its implementation on an externally facing customer support IIS based web server. Where possible the security policy will be implemented with Group Policy Objects.

The overall security policy statements that the merged IT departments developed are as follows:

- Systems will be managed following the principle of least privilege, which means a user will have the minimum rights to accomplish a task.
- Where feasible, access to resources will be defined by a user's role in the organization.
- Individual accountability on systems will be maintained.
- Systems - particularly systems with are exposed to the Internet - will be hardened to a level that enhances system security but does not significantly impair usability.

Further, the merged IT departments developed several additional policy statements governing server and desktop security. Implemented procedures are based on these policies.

- Enforce a consistent minimum security policy for every system in the domain.
- Maintain high server and desktop uptime.
- Protect servers and desktops from accidental damage wherever feasible.
- Preserve audit information for all systems periodically.
- Provide a high degree of desktop security.

One of the main concerns that both companies have is allowing proper access to departments on both of the original networks.

---

<sup>14</sup> Karen Guglielmo is a site editor for SearchCIO.com. URL:  
[http://whatis.techtarget.com/definition/0,,sid9\\_gci887248,00.html](http://whatis.techtarget.com/definition/0,,sid9_gci887248,00.html)

## Security Controls

There are three controls that can be applied to information systems - administrative controls, physical controls, and technical controls. The relationship between these controls is expressed in the next figure:

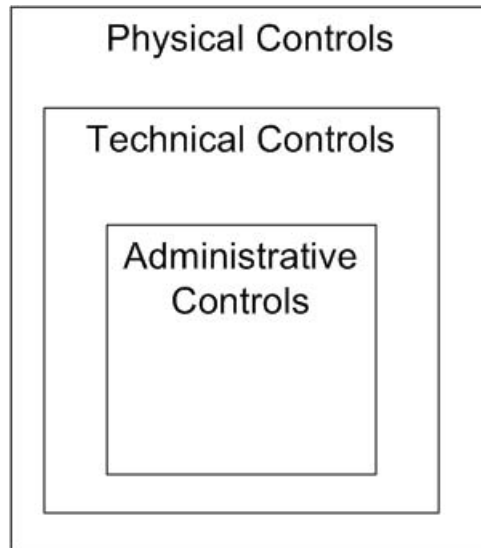


Figure 13: Controls Model<sup>15</sup>

SANS Co. doesn't have a traditional data center - a card based access controlled system, standalone HVAC, raised floor, concrete walls, taller than average ceilings, water sensors below the floor, positive air pressure, etc. Rather, what SANS Co has done is reconfigured a second floor interior room to have many of these features on a smaller scale. For instance, there are pushbutton cipher locks on the door, supplemental A/C, manual switchover electrical to an external generator, and upgraded the sprinklers to 165 degree activation points. These are the extent of physical controls that SANS Co. could afford.

SANS Co. does have good administrative controls in the form of written policies<sup>16</sup>. Policies include:

- Internet Access - must be for business purposes
- Computer use - must be for business purposes with occasional off hours personal use with permission.
- Physical - users logout nightly, lock their screens when away from the system, and safeguard media.
- Email - users must present a professional appearance and not disclose any sensitive data as email is not a secure medium.

<sup>15</sup> This specific illustration, which may come from a variety of sources, is attributed to Shon Harris in the "CISSP All In One Pep Guide, 2e".

<sup>16</sup> An excellent supplemental text on this topic is "Writing Information Security Policies" by Scott Barman.

- Viruses, worms, and Trojan horses - if a user has any reason to believe that their computer is "infected", immediately disconnect the system from the network, save data locally, and search for assistance.
- Administrators - any person who is granted supervisory or administrative access to the network or an information system on the network must not abuse their authority and privilege - violation of this policy may be a firing offense on the first violation.

Technical controls are what most of this section is about. These are controls that are implemented in a given information system and are designed to insure that a system is used properly. Physical controls are usually barriers that are designed to keep systems protected, like fences, locks, and fire control systems. Administrative controls are law, ethics, policies and procedures that are designed to guide behavior.

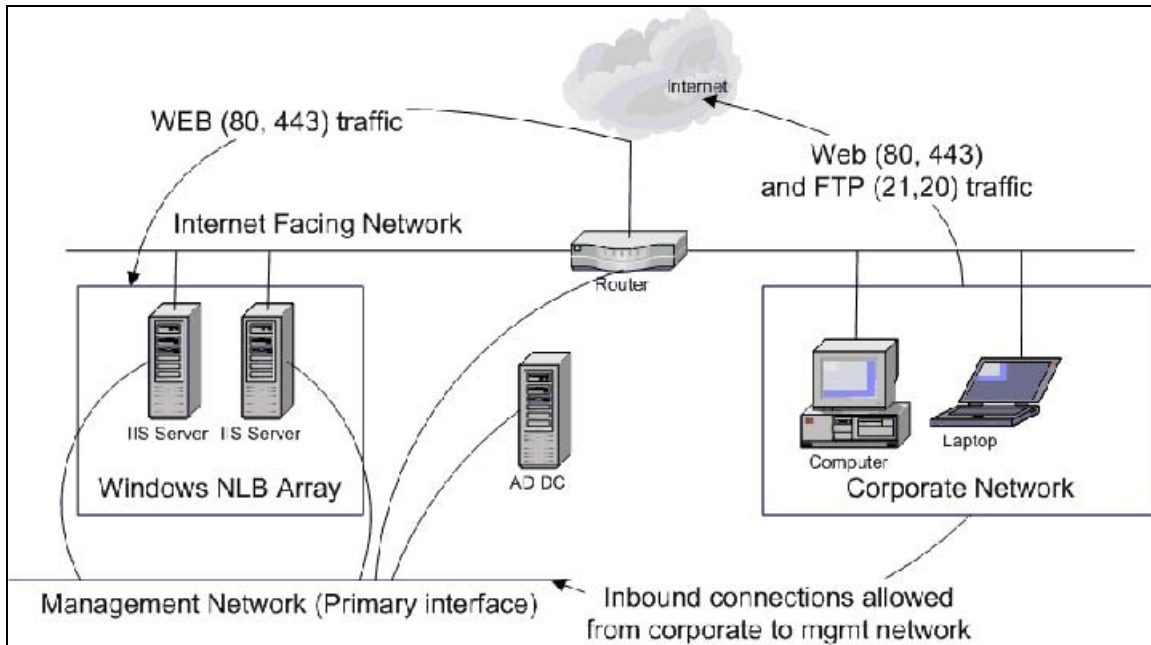
The technical controls that are implemented under the Windows 2000/XP/2003 operating systems here are:

- Group Policy Object (GPO's) in Active Directory
- File system permissions implemented in NTFS
- Group membership implemented in Active Directory
- Extended event auditing
- Authentication and authorization for some areas of the web site as administered by IIS

### ***Basic DMZ Network Configuration***

From a network management perspective, the Internet facing Web servers will be located on a segment away from the main corporate network (often called a DMZ or perimeter network). This network will have limited input and output (traffic flow) which is intended to support the web servers. In the next figure it can be seen that inbound web traffic is allowed into the IIS servers. Traffic that is for the corporate network is allowed into the web server network, including traffic for Windows Terminal Server (port 3389). General outbound traffic is allowed for web browsing and file transfer for the main corporate network. This illustration is a general one - there are a variety of other applicable rules that aren't shown here for simplicity sake (network addressing is on another figure).





**Figure 14: Basic Firewall Network Configuration**

There are some particular details that need to be followed in order to make this configuration work (based on practical experience from configuring a network like the one above<sup>17</sup>).

- The basic operating system is installed and patched before it is connected to the network. Instead of using a physical adapter, the MS Loopback adapter is used - this allows the system to function normally without actually being connected.
- Once the basic operating system is installed, the system is connected to the domain using the management network as the primary interface.
- Once the system is installed and updated, then install the secondary NIC.
- Bind IIS to the secondary NIC (in the Internet Services Manager snap in).
- The firewall only allows management style traffic to the management network from the corporate network.
- The firewall actually requires four (4) network adapters - logical networking and tinkering with switch configurations is not advised.
- The only systems connected to the Internet (through the firewall) are the IIS servers - other support servers in the DMZ domain are only connected to the management network.
- Rule ordering in the firewall is sensitive to network order and configuration - traffic needs to be routed to the DMZ, then from the corporate network,

<sup>17</sup> These details actually come from two real life installs on production networks. One was based on Windows NT 4.0 Enterprise edition (using WLBS) that was upgraded to Windows 2000 (including NLB), and the second was a straight Windows 2000 installation.

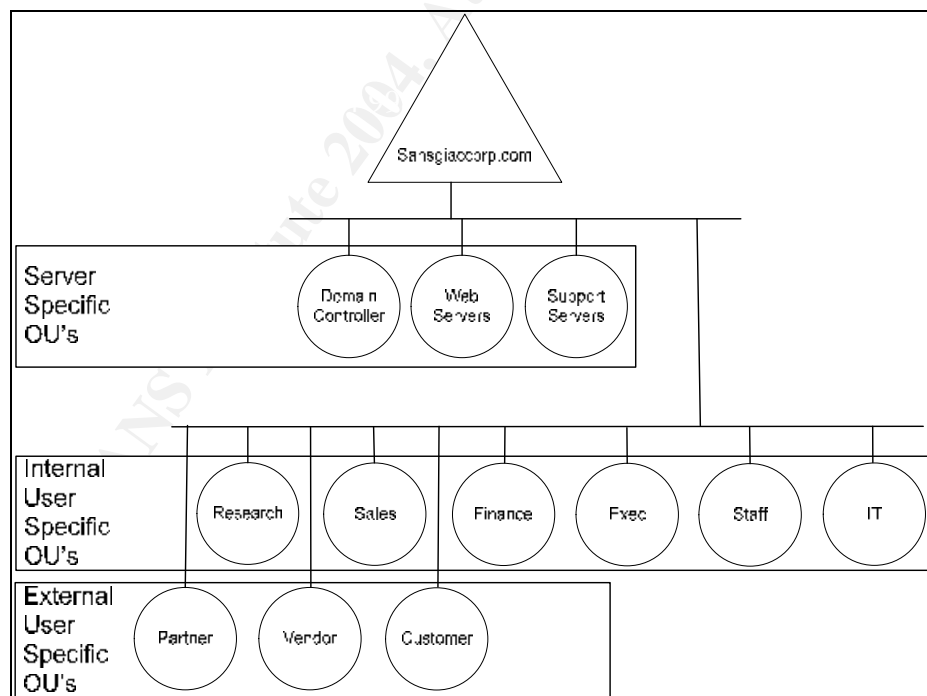
and then to the DMZ from the corporate network. Based on rule ordering performance is occasionally impacted.

## DMZ Domain AD Structure



The AD within the DMZ is designed to support two roles - control GPO assignment to servers in the domain and to provide enough support structure for the limited amount of users who will access the domain remotely. The user OU design is somewhat simplified from the existing AD domains, primarily because these are the groups of people that will access the domain. There are two OU's for people non-employees: Partners and Vendors. Partners are other companies that SANS-GIAC has as collaborators - companies and individuals who are in business with the company. Vendors are companies that sell services, Below is an illustration of the DMZ AD structure.

**Figure 15: OU's in the DMZ**



**Figure 16: DMZ AD Structure**

Layered on top of the OU structure is a group structure that mimics the one established for the main internal domains:

### LC\_Role\_Postion.

Where:

- LC - Location code - always set to SGC.
- Role - This is a one or two capitalized word that indicates the department.
- Position - This is one of two options - Staff or Manager.

Examples:

- SGC\_Sales\_Managers: This group is for the managers of the Sales department.
- SGC\_OfficeAdmins\_Staff: This group is for the general office staff.
- SGC\_Research\_Staff: GIAC Research and Development.

For third party companies that need access to the web site the same model is used. Instead of the "role" being a department the name of the company is used and its shortened enough to make sure that its clear what the company is. For instance, one business partner is named Gould and Lord Systems Enterprises. For this business partner the shorter name "GouldSystems" is used.

These groups are used to establish NTFS permissions for various parts of the web site when parts of the site need to be secured for group access. Also, by following this established convention for group membership adoption of more sophisticated web based collaboration tools such as Microsoft SharePoint Server is simplified - the site has an existing name and group membership method that maps neatly to these types of products. Furthermore, when users access the DMZ through Terminal Server sessions NTFS permissions on resources can be enforced.

### ***Domain Wide Group Policy (DDP)***

---

Windows 2000/2003 has a policy that can be implemented domain wide - this group policy object policy is applied to all server and workstation systems in the domain. There is another policy for all domain controllers discussed below. By configuring one GPO for the entire domain a baseline of group policy settings can be applied without having to tailor settings to individual organizational units within the domain unless necessary. SGC will implement a domain wide GPO by using the "Default Domain Policy" (hence, DDP), taking a conservative approach in settings in the DDP. It is possible to set some of the GPO options in the DDP that may cause some problems in the domain - thus, settings in the DDP GPO are designed to protect the entire domain and not to interrupt service while maintaining consistency in the domain. The settings implemented here will be *additive* to the IIS Web Server settings discussed below.

The DDP affects these Account policies:

- Password Policy
- Account Lockout Policy
- Kerberos Policy

The DDP affects these Local policies:

- Audit Policy
- User Rights Assignment
- Security Options
- Event Log
- Restricted Groups
- System Services
- Registry
- File System
- IP Security Policies on Active Directory
- Public Key Policies

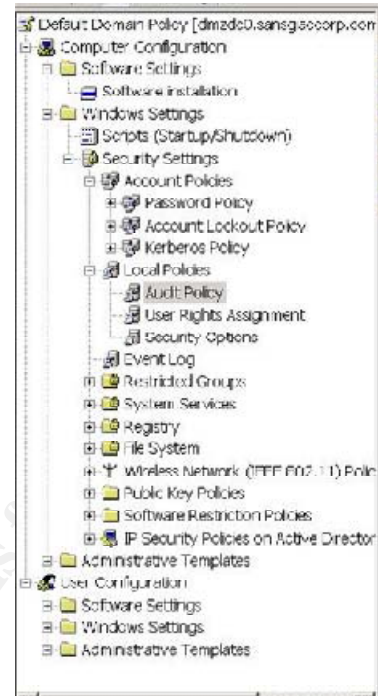


Figure 17: Default Domain Policy

For the SANS GIAC DMZ domain, several of the DDP settings that are in use are listed below and shown in accompanying screen captures and discussion. Note that these settings are *domain wide* - they are designed to establish a minimum security posture for all systems in the DMZ domain. An additional set of GPO's will be applied to the web servers. By using the DDP and an Organizational Unit GPO general security for the entire domain is established and then specialized security for particular computers is established.

While there are security templates for Windows 2000, there are no NSA security templates for Windows 2003. Over time, hopefully, there will be a template developed.

These settings are found in the DDP GPO under the path (see the above figure). Below are specific setting organized in the DDP. The actual configuration of the setting is in **bold**.

### Computer Configuration \ Windows Settings \ Security Settings.

#### Account Policies \ Password Policy:

Enforce password history	<b>24 passwords remembered</b>
Maximum password age	<b>30 days</b>
Minimum password age	<b>1 days</b>

Minimum password length	<b>8 characters</b>
Password must meet complexity requirements	<b>Enabled</b>
Store passwords using reversible encryption	<b>Disabled</b>

These settings are designed to protect login accounts on the network. The minimum password length is longer than default, and the maximum password age shorter than default.

### **Account Policies \ Account Lockout Policy:**

Account lockout duration	<b>30 minutes</b>
Account lockout threshold	<b>5 invalid logon attempts</b>
Reset account lockout counter after 30 minutes	<b>(enabled)</b>

The account lockout threshold is longer than default - given the physical security of the environment this isn't a major issue for interactive logins. Given the account lockout duration, it would be possible to make about 700 password attempts over a typical weekend before getting noticed. Password complexity requirements should prevent a password from being guessed.

### **Local Policies \ Audit Policy**

Audit account logon events	<b>Success, Failure</b>
Audit account management	<b>Success, Failure</b>
Audit directory service access	<b>Success, Failure</b>
Audit logon events	<b>Success, Failure</b>
Audit object access	<b>Success, Failure</b>
Audit policy change	<b>Success</b>
Audit privilege use	<b>Success, Failure</b>
Audit process tracking	<b>Not Defined</b>
Audit system events	<b>Success, Failure</b>

These settings are designed to record detailed information about system usage (thus supporting the accountability requirement from above). It's important to realize that the Audit object access setting doesn't enable auditing - rather it allows for auditing to be performed if auditing is requested in a SACL<sup>18</sup> on a given object.

<sup>18</sup> SACL: System Access Control List. A SACL contains the list of groups and users for which auditing (recording of an action or attempted action) on an object are recorded.

## Local Policies \ User Rights Assignment

Here, the majority of settings are "Not Defined". Below is the list of settings that are defined for the DDP – these settings are designed to enforce basic rules for all servers on the domain and supercede basic Windows 2003 defaults.

Access this computer from the network	<b>Administrators, Authenticated Users</b>
Allow log on locally	<b>Backup Operators, Authenticated Users, Administrators</b>
Manage auditing and security log	<b>Administrators</b>

For instance, by default, more groups can access the computer from the network – by specifying that "authenticated users" and "administrators" have the rights listed we are insuring that a user must be positively authenticated. Also – the only group that should manage the security log is the Administrators group.

## Local Policies \ Security Options

Accounts: Rename administrator account	<b>rdanderson</b>
Accounts: Rename guest account	<b>atapping</b>
Devices: Allowed to format and eject removable media	<b>Administrators</b>
Devices: Unsigned driver installation behavior	<b>Warn but allow installation</b>
Interactive logon: Do not display last user name	<b>Enabled</b>
Interactive logon: Message text for users attempting to log on	<b>This SGC system is restricted to authorized users, and uses. Individuals attempting unauthorized access will be prosecuted. Unauthorized users terminate access now! Clicking indicates your acceptance monitoring and auditing by SGC.</b>
Network access: Do not allow anonymous enumeration of SAM accounts	<b>Enabled</b>
Network access: Do not allow anonymous enumeration of SAM accounts and shares	<b>Enabled</b>
Network access: Do not allow storage of credentials or .NET Passports for network authentication	<b>Enabled</b>

Network access: Named Pipes that can be accessed anonymously  
(none listed)

Network access: Restrict anonymous access to Named Pipes and Shares  
Enabled

Network access: Shares that can be accessed anonymously  
(none listed)

Network access: Sharing and security model for local accounts  
Classic - local users  
authenticate as  
themselves

Network security: Do not store LAN Manager hash value on next password  
change  
Enabled

Network security: Force logoff when logon hours expire  
Disabled

Network security: LAN Manager authentication level  
Send NTLMv2 response  
only\refuse LM

Network security: Minimum session security for NTLM SSP based  
(including secure RPC) clients  
Require message  
integrity,  
Require message  
confidentiality,  
Require NTLMv2 session  
security, Require 128-  
bit encryption

Network security: Minimum session security for NTLM SSP based  
(including secure RPC) servers  
Require message  
integrity, Require  
message  
confidentiality,  
Require NTLMv2 session  
security, Require 128-  
bit encryption

These settings are designed to establish a minimum security profile for general network access, devices, and console access to the system. For instance, the network access settings are designed to harden connectivity over the LAN. Renaming the administrator and guest account help to protect these two default accounts. And there is a strong warning banner on the system.

## Security Settings \ Event Log

Retain application log	14 days
Retain security log	14 days
Retain system log	14 days
Retention method for application log	By days
Retention method for security log	By days
Retention method for system log	By days

These settings are designed to protect the event history. There is also a set of settings for controlling the maximum size of the event log – since these are not configured, the system will retain information for 2 weeks.

### ***Default Domain Controller Group Policy***

Domain Controllers have their own GPO. In order to make sure that the DC's process audit logon events similar settings for the DCGPO<sup>19</sup> need to be applied. The DCGPO was also edited (configured), and the auditing settings were configured. These are shown in the next screenshot, along with the GPMC report of the applied policy settings.

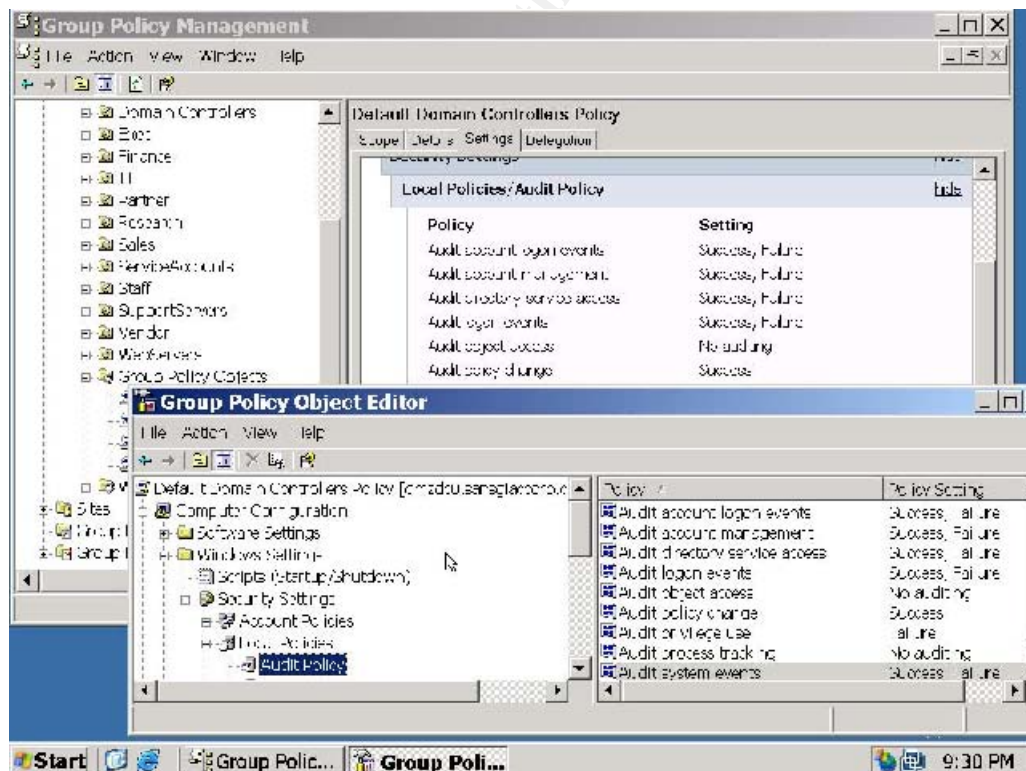


Figure 18: Domain Controller Group Policy

<sup>19</sup> DCGPO: Domain Controller Group Policy Object



---

## **Web Server Configuration**

---

For the merged web presence (SANS + GIAC), the company has decided to build a new Active Directory domain named "sansgiaccorp.com" (for "SANS GIAC Corporation"). Mechanically speaking, they will purchase three new servers - one for an AD domain controller and two that will run IIS. As the new environment is brought up equipment will be migrated from the existing web environments to support the new environment. For instance, GIAC won't need to have several IIS servers in their NLB array once there is a functioning catalog and ordering system available. As usage decreases for GIAC's web server array, servers will be brought out of the array, disks will be scrubbed with a US DoD compliant disk formatting tool, reinstalled, and brought into the SGC array.

---

## **IIS Server Installation Specific Details**

---

There are a variety of components which are installed with IIS 6. Microsoft has changed the setup and configuration of IIS such that it is much easier to control services/components under IIS. Each major grouping below follows a major functional grouping in the IIS configuration dialogs.

### Application Server Subcomponents

- Application Server Console - Disabled, as the IIS Server Manager provides this function.
- ASP.NET - Enabled, as the site will actually use ASP.NET applications.
- Enable network COM+ access - Enabled (required by IIS).
- Enable network DTC access - Disabled, as database access is via ADO connections and the site isn't doing two phase commit operations.
- Internet Information Services (IIS) - Enabled.
- Message Queuing - Disabled (not used by the site).

### IIS Subcomponents

- Background Intelligent Transfer Service (BITS) - Disabled, as the site is not planning on using this service.
- Common Files - Enabled (required).
- FTP Service - Enabled, as the site plans to distribute a variety of data using FTP such as catalog pages and product literature.
- FrontPage 2002 Server Extensions - Disabled.
- Internet Information Services Manager - Enabled, as it is needed to manage IIS.
- Internet Printing - Disabled.
- NNTP Service - Disabled, as the site is not supporting news groups.
- SMTP Service - Disabled.
- World Wide Web Service - Enabled (required).

### Message Queuing Subcomponents

- Since MQMS is disabled above, the five (5) components for MSMQ are also disabled.

### World Wide Web Service Subcomponents

- Active Server Pages - Enabled, as the site has a significant investment in ASP pages and hasn't upgraded everything to ASP.NET (ASPX pages).
- Internet Data Connector - Disabled.
- Remote Administration (HTML) - Disabled, as managing an IIS server over the web is ill advised.
- Remote Desktop Web Connection - Disabled, as access via Terminal Server is accomplished by the Win32 client from authorized desktops on the corporate network.
- Server – Side Includes - Disabled, as the site does not use these types of web pages.
- WebDAV - Disabled, as the site doesn't want to use HTTP as a transport mechanism for file / application updates.
- World Wide Web Service - Enabled.

### ***General Server Hardening***

---

There are a number of tasks that are normally performed to harden a server. Microsoft has recently published a Windows Server 2003 Security Guide<sup>20</sup> which has 12 chapters on installing and configuring Windows 2003 for security. Chapter 8 specifically deals with hardening IIS servers.

Major task groups in server hardening include:

- Use hardware that provides a necessary level of redundancy<sup>21</sup>.
  - Mirrored boot / operating system drives.
  - RAID 5 based data drives.
  - Cluster hardware (if it can be budgeted).
- Minimal installation - install the necessary components (discussed above).
- Apply service packs / patches and keep them updated over time.
- Apply an applicable security template to the system.
- Disable unnecessary services. Examples include:
  - Computer Browser.
  - DHCP Client.
  - Internet printing for IIS.
  - Web Distributed Access and Development for IIS.
- Restrict access to potentially dangerous files / applications on the system.
  - Example: Set the permissions on FTP.EXE and TFTP.EXE such that they cannot be used, but Microsoft System File Protection won't reinstall the program(s).
- Limit access to the system.

---

<sup>20</sup> This Guide can be found on the Microsoft web site:

<http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.msp>

<sup>21</sup> One of the critical tenants or elements in the information security world is the C-I-A triad (Confidentiality, Integrity and Availability). Redundant hardware, such as mirrored or RAID 5 disks, supports the Availability leg of the triad.

- Example: Change the TCP/IP settings so that NetBIOS is not used. For the configuration here and in the illustration, unbind additional components from the Internet facing NIC (File and Print Sharing, Client for Microsoft Networks).
- Run analysis tools on the system once it is up and running.
  - IIS Lockdown Wizard.
  - Center for Internet Security Benchmark Analysis (interpreting the data carefully, as there isn't a Windows 2003 specific template yet).
  - Run the Microsoft Baseline Security Analyzer (discussed later).

### ***Web Server Group Policy Design***

Based on several sources a consolidated group policy design will be implemented on the IIS servers. This group policy will be linked to the "WebServers" Organizational Unit in the domain so that the settings herein are only associated with the web servers. Note that by default the domain controllers get their settings from the Domain Controllers Organizational Unit - so there should be no conflict with the DC's. Specific details on the GPO items are listed below.

Sources include:

- Microsoft's guide referenced above.
- SANS GCWN curricula (several sections).

This GPO configures the system services which run for IIS servers in the WebServers OU. By setting a list of services and enforcing that configuration the "threat plane"<sup>22</sup> is minimized.

### **Security Settings \ System Services**

Alerter	<b>Disabled</b>
Application Layer Gateway Service	<b>Disabled</b>
Application Management	<b>Disabled</b>
Automatic Updates	<b>Disabled</b>
Background Intelligent Transfer Service	<b>Manual</b>
ClipBook	<b>Disabled</b>
COM+ Event System	<b>Automatic</b>
COM+ System Application	<b>Automatic</b>
Computer Browser	<b>Automatic</b>
Cryptographic Services	<b>Manual</b>
DHCP Client	<b>Disabled</b>
DHCP Server	<b>Disabled</b>
Distributed File System	<b>Disabled</b>
Distributed Link Tracking Client	<b>Disabled</b>
Distributed Link Tracking Server	<b>Disabled</b>

<sup>22</sup> The term "threat plane" essentially means the attack surface of a given system or application. In this context the threat plane is reduced that a standard Windows 2003 system because the number and type of systems services is significantly reduced. Further, the GPO enforces the rule by default for servers in the OU.

Distributed Transaction Coordinator	Manual
DNS Client	Automatic
DNS Server	Disabled
Error Reporting Service	Disabled
Event Log	Automatic
File Replication Service	Disabled
FTP Publishing Service	Automatic
Help and Support	Disabled
HTTP SSL	Automatic
Human Interface Device Access	Disabled
IIS Admin Service	Automatic
IMAPI CD-Burning COM Service	Manual
Indexing Service	Disabled
Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)	Disabled
Intersite Messaging	Disabled
IPSEC Services	Manual
Kerberos Key Distribution Center	Disabled
License Logging	Disabled
Logical Disk Manager	Manual
Logical Disk Manager Administrative Service	Manual
Messenger	Disabled
Microsoft Software Shadow Copy Provider	Disabled
Net Logon	Automatic
NetMeeting Remote Desktop Sharing	Disabled
Network Connections	Manual
Network DDE	Disabled
Network DDE DSDM	Disabled
Network Location Awareness (NLA)	Manual
NT LM Security Support Provider	Automatic
Performance Logs and Alerts	Automatic <sup>23</sup>
Plug and Play	Automatic
Portable Media Serial Number Service	Disabled
Print Spooler	Automatic
Protected Storage	Automatic
Remote Access Auto Connection Manager	Disabled
Remote Access Connection Manager	Manual
Remote Desktop Help Session Manager	Disabled
Remote Procedure Call (RPC)	Automatic
Remote Procedure Call (RPC) Locator	Manual
Remote Registry	Automatic
Removable Storage	Manual
Resultant Set of Policy Provider	Disabled
Routing and Remote Access	Disabled
Secondary Logon	Disabled
Security Accounts Manager	Automatic
Server	Automatic
Shell Hardware Detection	Disabled
Smart Card	Manual
SNMP Service	Disabled
SNMP Trap Service	Disabled
Special Administration Console Helper	Disabled

<sup>23</sup> Initially, this was set to "Disabled", but testing proved that it was a needed service (discussed later in the paper).

System Event Notification	Automatic
Task Scheduler	Disabled
TCP/IP NetBIOS Helper	Automatic
Telephony	Disabled
Telnet	Disabled
Terminal Services	Automatic
Terminal Services Session Directory	Automatic
Themes	Disabled
Uninterruptible Power Supply	Automatic
Upload Manager	Disabled
Virtual Disk Service	Automatic
VMware Tools Service	Automatic
Volume Shadow Copy	Manual
WebClient	Disabled
Windows Audio	Disabled
Windows Image Acquisition (WIA)	Disabled
Windows Installer	Automatic
Windows Internet Name Service (WINS)	Disabled
Windows Management Instrumentation	Automatic
Windows Management Instrumentation Driver Extensions	Manual
Windows Time	Automatic
WinHTTP Web Proxy Auto-Discovery Service	Disabled
Wireless Configuration	Disabled
WMI Performance Adapter	Manual
Workstation	Automatic
World Wide Web Publishing Service	Automatic

This section of the group policy object is designed to configure certain services to run on the web servers by default. Here, there are a variety of services that are disabled which are either a) not needed or b) represent some sort of risk. For example, the Wireless Configuration service isn't needed – the network is hard wired. The SNMP service – as a technology – implements weak security by using a plain text community string as its only real authentication mechanism. Further, SNMP is known for consuming extra bandwidth.

## ***Group Policy Testing***

There are several GPO's in the DMZ domain. In order to make sure that they are being applied correctly there are at least two tools available - the services list (what is running on the system) and the Group Policy Management Console (GPMC). The GPMC tool allows an administrator to see (in great detail, as will be shown) tremendous detail on the application of group policy to various OU's in the domain. By using the GPMC Group Policy Results wizard the OU can be selected and the net results of the group policy are shown (after a few minutes...)

First, check the services lists on both systems. There should be a larger services list on the domain controller. On one of the domain controllers, run the command: "net start" to see the list of services running on the system:

These Windows services are started:

Automatic Updates

COM+ Event System  
Computer Browser  
Cryptographic Services  
DHCP Client  
DHCP Server  
Distributed File System  
Distributed Transaction Coordinator  
DNS Client  
DNS Server  
Error Reporting Service  
Event Log  
File Replication Service  
FTP Publishing Service  
Help and Support  
HTTP SSL  
IIS Admin Service  
Intersite Messaging  
IPSEC Services  
Kerberos Key Distribution Center  
Logical Disk Manager  
Net Logon  
Network Connections  
Network Location Awareness (NLA)  
NT LM Security Support Provider  
Plug and Play  
Print Spooler  
Protected Storage  
Remote Access Connection Manager  
Remote Procedure Call (RPC)  
Remote Registry  
Secondary Logon  
Security Accounts Manager  
Server  
Shell Hardware Detection  
SNMP Service  
System Event Notification  
Task Scheduler  
TCP/IP NetBIOS Helper  
Telephony  
Terminal Services  
VMware Tools Service  
Windows Internet Name Service (WINS)  
Windows Management Instrumentation  
Windows Time  
Wireless Configuration  
Workstation  
World Wide Web Publishing Service

The command completed successfully.

On one of the IIS servers, run the same command again, and see the list of services.

These Windows services are started:

COM+ Event System  
COM+ System Application  
Computer Browser  
DNS Client  
Event Log  
FTP Publishing Service  
HTTP SSL  
IIS Admin Service

Net Logon  
Network Connections  
Network Location Awareness (NLA)  
NT LM Security Support Provider  
Plug and Play  
Print Spooler  
Protected Storage  
Remote Procedure Call (RPC)  
Remote Registry  
Security Accounts Manager  
Server  
System Event Notification  
TCP/IP NetBIOS Helper  
Terminal Services  
Terminal Services Session Directory  
Virtual Disk Service  
VMware Tools Service  
Windows Management Instrumentation  
Windows Time  
Workstation  
World Wide Web Publishing Service

The command completed successfully.

Based on the lists it is shown that are several services running on the domain controller that are not running on the IIS server.

Next, use the GPMC to see the evaluated policy in both OU's (the Domain Controllers OU and the WebServer OU). Below is a summary screen of the domain controller (DMZDC0).

© SANS Institute 2004, All rights reserved. Author retains full rights.

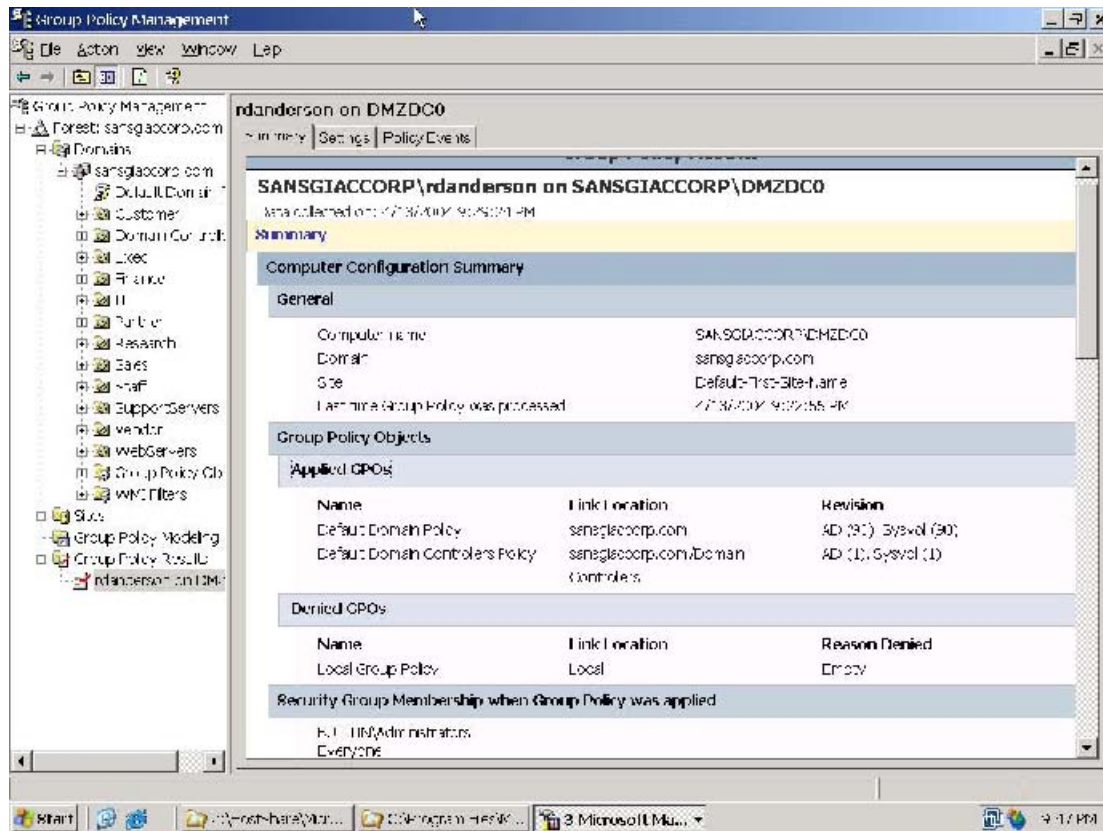


Figure 19: GPCM for DMZDC0

This is a summary screen that really doesn't show the group policies being used - the report (from the settings tab) shows a great deal more. This report is shown in Appendix A: GPMC for DMZDC0. In the summary list below the report shows that a variety of settings are applied, all from the Default Domain Policy.

Turning attention to the web servers, an example screen capture of the GPMC shows that a variety of system services are disabled. Focus within the GPMC is on the System Services report area and shows that the "Alerter" service is disabled - this setting was defined in group policy, confirmed in the services list (above), and then shown in the screen capture.

By comparing Appendix A with Appendix B it can be shown that the Web servers GPO was applied in many places - particularly the system services.



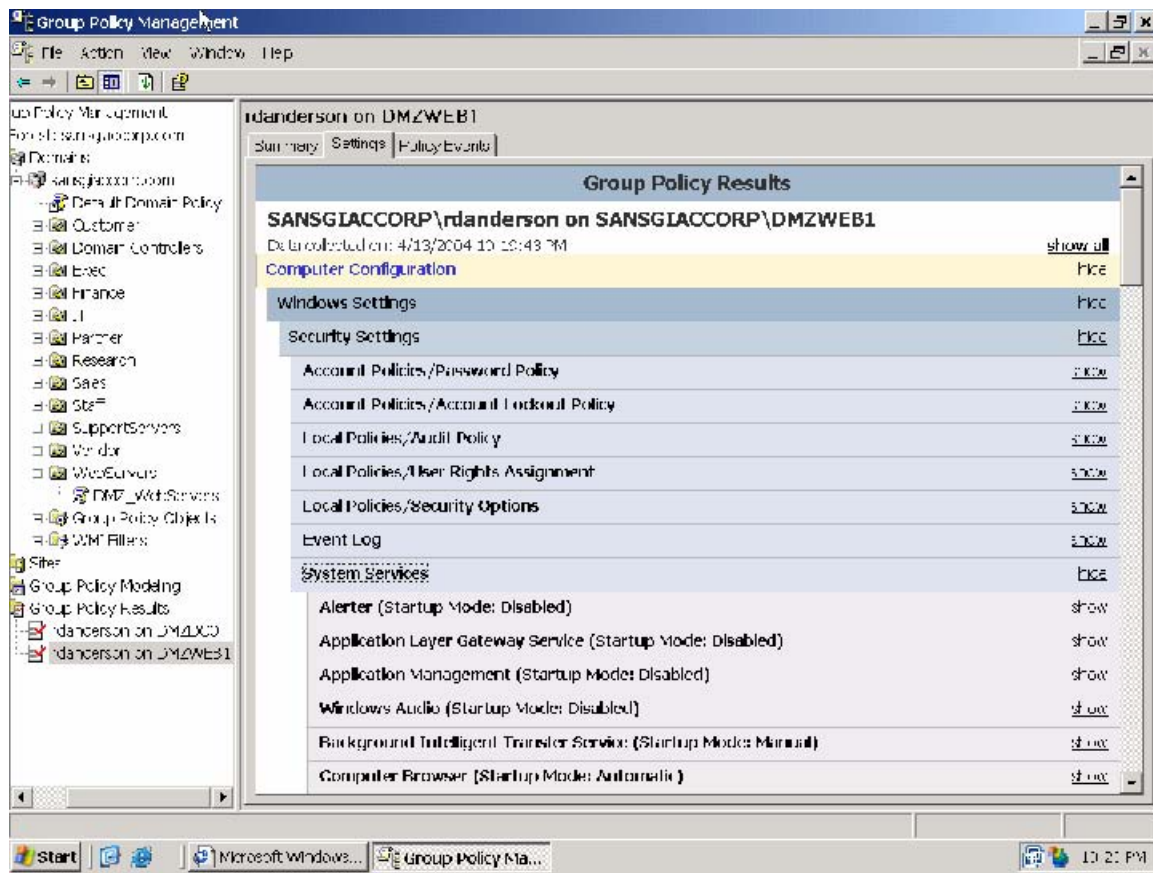


Figure 20: GPMC for DMZWEB1

## Group Policy Evaluation

After using and deploying this initial set of GPO's and using the GPMC tool some pro's and con's were discovered.

### Pro's:

- The IIS servers, from a system services point of view, are well hardened in the sense that unneeded services are disabled as per the GPO.
- The system is employing a specific GPO to the web servers - this demonstrates that the GPO's are being applied in the domain, and if other web servers are installed.
- The layered GPO's - the DDP and the OU specific GPO - establish a minimum stance for domain security.

### Con's:

- Some services were actually needed on the IIS server. The Performance Logs and Alerts service was needed in order to start and run the logman command (discussed later in this paper). Also, the "Wireless configuration" service should never be used on a DMZ network - this service should be disabled in the DDP.

- As originally designed there are no user settings for Group Policy. This was an initial oversight, and should be corrected<sup>24</sup>. These settings are applicable as the web servers are managed remotely with Windows Terminal Server Edition connections. Examples of user policies include:
  - Internet Explorer settings
  - Folder redirection
  - Desktop settings
  - Control Panel settings

---

## VMWare 4.0 Disconnect

Like many GIAC students, VMware 4.0 was used to run multiple virtualized operating systems on a few PC's/ The WebServer GPO was too restrictive in sharing files between the Guest OS and the Host OS under VMware 4.0. One of the network settings interfered with the ability to mount the Host share drive. The difficulty reveals that VMware 4.0 is making use of a weaker security model than the WebServer GPO caused to become apparent. In order to deal with this problem, I used the Active Directory Users and Computers console, moved the IIS server to the "SupportServers" OU and then used the "gpupdate /target:computer" command to force a new policy to be applied. After a few minutes I could use the mapped drive from the Host to the Guest operating system. By moving the virtualized system back to its proper OU and reissuing the gpupdate command the problem reappeared.

---

## User Tests

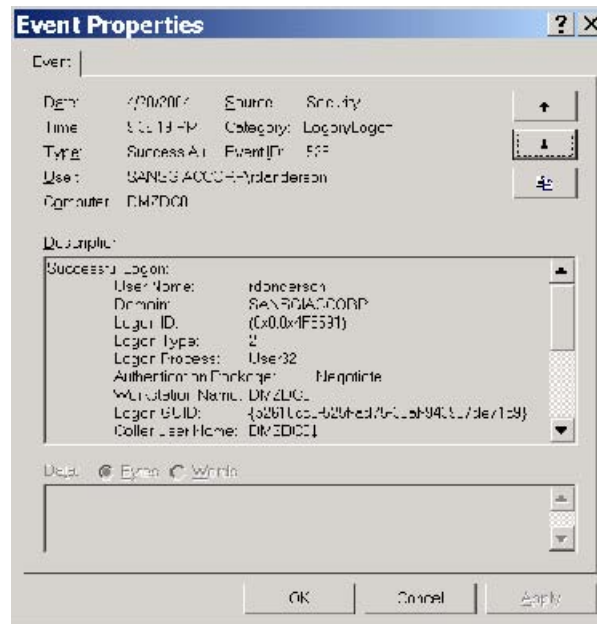
A few tests can be executed on the system to make sure that it is operating.

First, can an administrator run the `logman` commands cited below under Performance Monitoring? Initially they could not. Because the "Performance Logs and Alerts" service was marked Disabled, these commands fail. In order to fix this error, the startup parameters of this service should be set to "Automatic" in the WebServers Group Policy object.

Second, are logon attempts logged (successful and failure)? Yes, they are, as can be seen in the success and failure audits shown below.

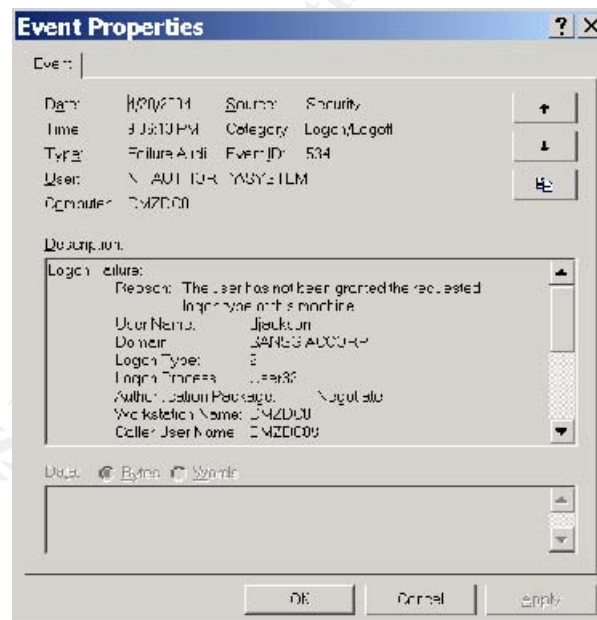
---

<sup>24</sup> Note: I specifically decided not to reedit and to change the original GPO configuration. Rather, after thinking about the overall structure I decided that it was a better answer for the GIAC practical assignment that I should express this fact.



**Figure 21: Example Successful Logon Audit**

In this event the user "rdanderson" (a high ranking administrator) is allowed to logon to the domain controller.

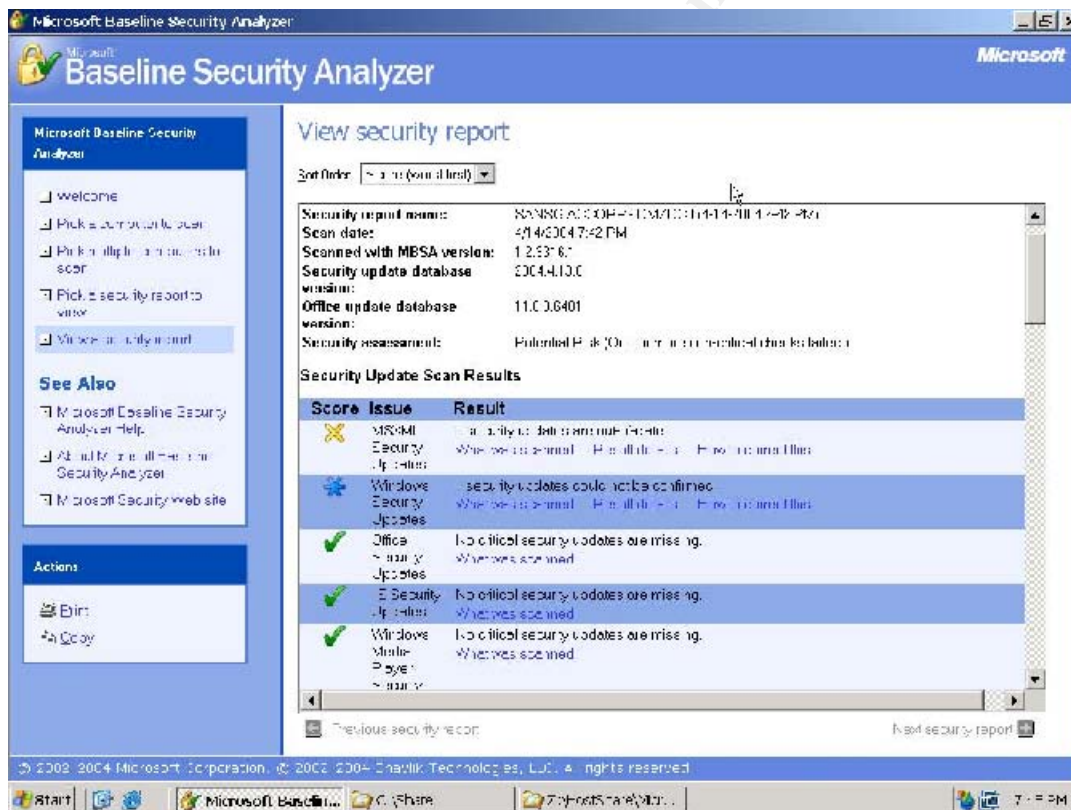


**Figure 22: Example Logon Failure Audit**

In this event the user "djackson" (a low ranking non-administrator) is *not* allowed to logon to the domain controller.

## Auditing with MBSA

Microsoft offers the MBSA<sup>25</sup> tool which performs scans and assessments against remote or local systems (by name or IP). MBSA checks for issues with a variety of common Microsoft products - Windows 2000/XP/2003, Office, SQL Server, Exchange, and Internet Explorer. MBSA puts a good quality security assessment into the hands of the user. MBSA provides an assessment and uses a list of system configuration characteristics and update from Microsoft by comparing a system against a frequently updated digitally signed XML file. The assessment provides information that an end user can actually use to keep a system updated and better secure a system - assuming they are willing to do a little reading and have sufficient rights on the system. There are two example screenshots of the MBSA. The first one, taken on the domain controller, shows that the system is almost current with respect to patches and updates after a visit to [windowsupdate.microsoft.com](http://windowsupdate.microsoft.com). The second screenshot is before a visit any updates were applied.



### Figure 23: MBSA on the DC

<sup>25</sup> MBSA can be downloaded from Microsoft:  
<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>



Figure 24: MBSA on a Web Server

© SANS Institute 2004, Author

## Active Directory Domain Audit

---

What is auditing? According to Webster's New Collegiate Dictionary, an audit is "a formal or official examination and verification of an account book; a methodical examination and review." Translating this definition to Information Technology - and in particular Microsoft's Active Directory, the working definition for SANS-GIAC is:

"A formal or official examination and verification of the use of Active Directory, the computer systems, and the computer network".

There are several characteristics of an effective audit system: Understandable, consistent, reliable, auditable itself, actionable, and universal. Specifically, these criteria mean:

- Understandable - the system should gather sufficient information that can communicate to users. As an example, the system should record details about an event and not just an event number. Here, the system needs to be able to show if the event relates to state or to action.
- Consistent - the system should produce similar information from similar circumstances.
- Reliable - the system should "work", and if the system isn't "working" that very fact indicates a condition warranting investigation.
- Auditable itself - a system knowledgeable person should be able to look over the audit system and be able to prove that if the audit system reports an event that the reported event really stems from a properly matched occurrence.
- Actionable - the system should provide sufficient information to know who, what, when, and where an event occurred.
- Universal - Where possible, the system should monitor all critical components.

With this working definition in mind, auditing for the network is implemented by monitoring:

- Event logs for servers
  - Application
  - System
  - Security
- Login and account login processes (Security log)
- System events (System log)
- Web server usage (IIS log)
- Application server log records (SQL server log file, or a similar log from a RDBMS)
- Firewall log records (as posted to a log server)

## ***Gathering Information - Round One***

The first implementation of auditing for the web server domain was implemented with a set of scripts designed to collect event logs from the systems. Over time, the domain administrators found that this system was unwieldy - they were only capturing event logs and basic system information.

Data collection command script flow:

1. Run the "net view /domain:sansgiaccorp" to get the list of computers in the domain.
2. From each computer, query the "AuditData\$" share and collect information.
  - a. System event log info
  - b. Application event log info
  - c. Security event log info
  - d. Msinfo32 output

On each system at 1 AM a Perl program runs that constructs a batch file which runs several commands. One of the principle functions of the control program is to calculate "yesterday", as "yesterday" is a command line parameter for the eventquery.vbs program invocations. Examples of these commands is shown below:

```
cscript c:\winnt\system32\eventquery.vbs /l application /fi "Datetime
gt 04/17/04,12:00:00AM" /fo CSV /fi "type eq warning or type eq error"
> %COMPUTERNAME%.20040417.APP.TXT
```

```
cscript c:\winnt\system32\eventquery.vbs /l system /fi "Datetime gt
04/17/04,12:00:00AM" /fo CSV /fi "type eq warning or type eq error" >
%COMPUTERNAME%.20040417.SYS.TXT
```

```
cscript c:\winnt\system32\eventquery.vbs /l security /fi "Datetime gt
04/17/04,12:00:00AM" /fo CSV /fi "type eq warning or type eq error" >
%COMPUTERNAME%.20040417.sec.TXT
```

Some example output is below from the first query (warnings or errors from the system log):

```
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.
```

```
"Type","Event","Date Time","Source","ComputerName"
"Warning","12","4/17/2004 6:50:32 PM","W32Time","DMZDC0"
"Warning","3019","4/17/2004 5:17:54 PM","MRxSmb","DMZDC0"
"Warning","3019","4/17/2004 5:17:34 PM","MRxSmb","DMZDC0"
"Warning","3019","4/17/2004 5:17:33 PM","MRxSmb","DMZDC0"
"Warning","3019","4/17/2004 5:17:31 PM","MRxSmb","DMZDC0"
"Warning","3019","4/17/2004 5:17:30 PM","MRxSmb","DMZDC0"
```

The real downside to this system is that the event ID must be correlated with the event list, by log type. There are a variety of sources for event log information - there is even a spreadsheet that can be downloaded from Microsoft which has details on the event ID itself.



Example of the msinfo32.exe output, in XML format (shown in IE) is next:

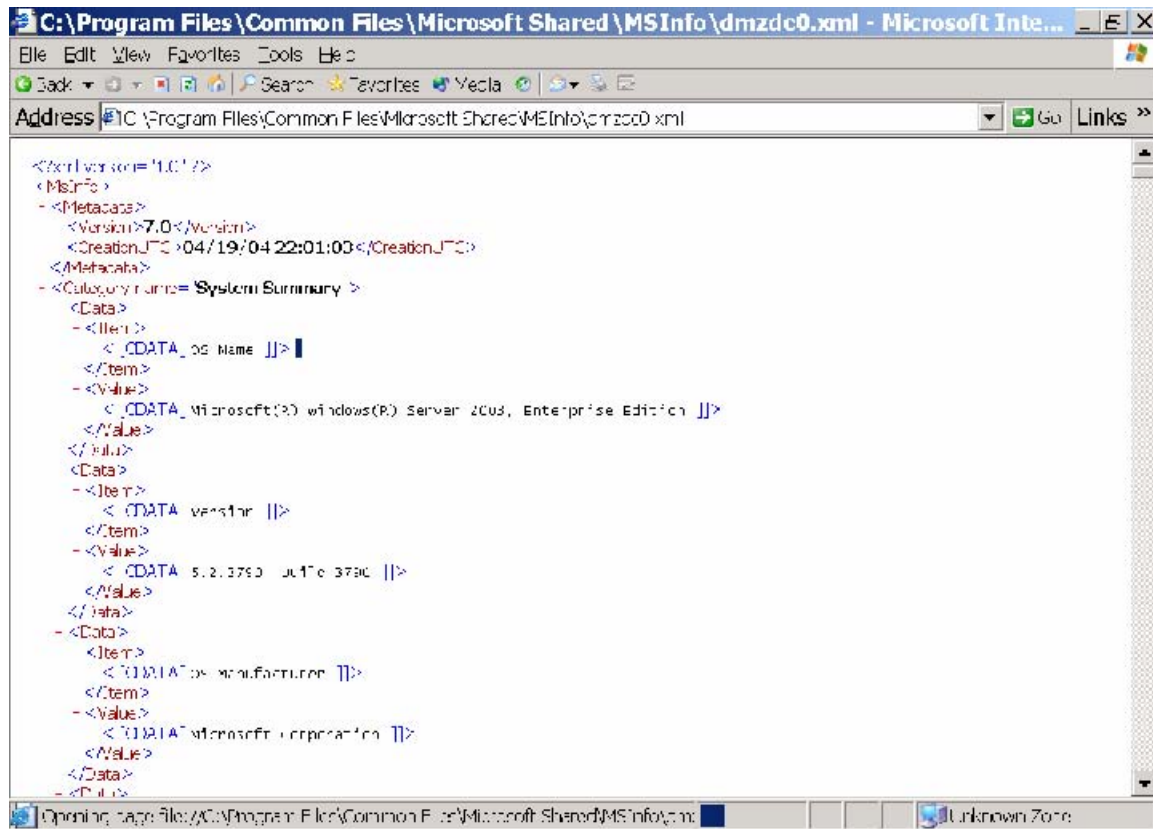


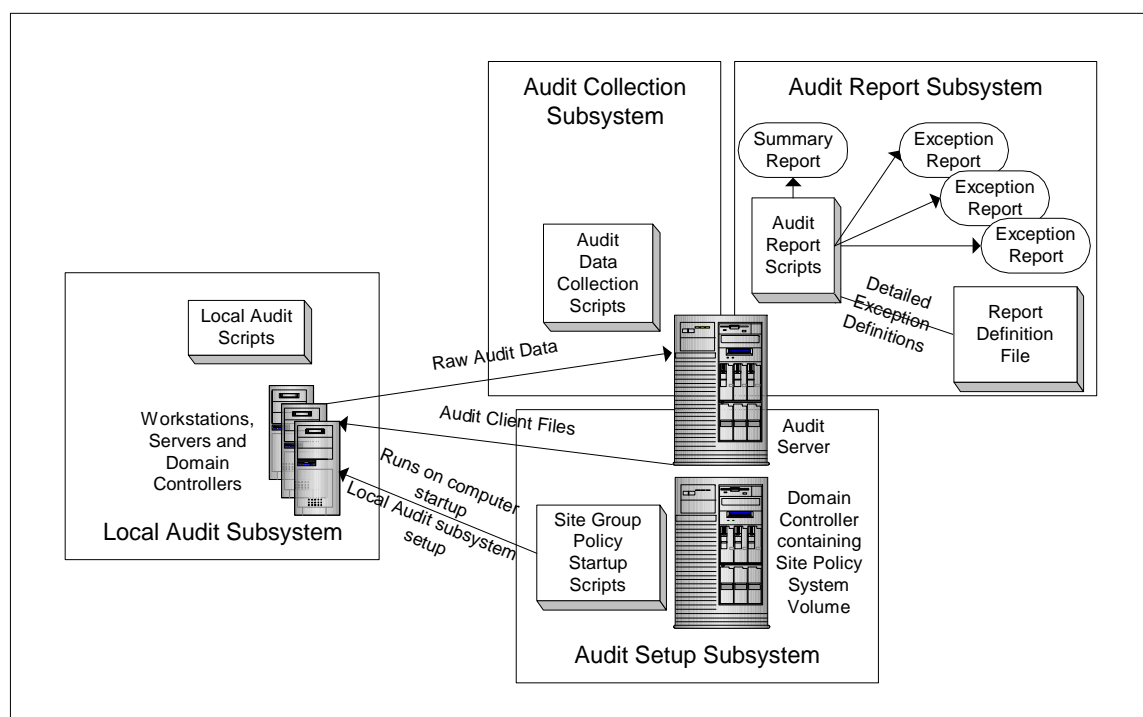
Figure 25: MSInfo32 XML Command Output

## Gathering Information - Round Two

In its research to determine how to better audit the network, SANS GIAC needed to implement tools that can monitor better and smarter. The IT staff found Steve Elky's audit system, which is posted on the SANS web site at:

[http://www.sans.org/resources/auto\\_audit.php](http://www.sans.org/resources/auto_audit.php). This audit system has numerous components that aid and assist greatly in the audit process. Below is an illustration from Elky's practical assignment, a description of the audit system, details on making the code work and how it is implemented on the network.





**Figure 26: Elky's Audit System Illustrated**

Elky's system, at its heart, is an automated way of running the "secdit" program and checking the system against a security template based on the system type (Security Templates are discussed later). This system has three main parts to its operation. First, on individual systems a script runs that compares the system's configuration against a base template. Before the template is checked, the system downloads the current template point from the "AuditScripts" directory - therefore any changes would be checked within 24 hours. Second, a server based process constructs a list of systems in the domain and writes a batch file for retrieving the data. The batch file checks to see if there is an audit file, and if there is it downloads the file. Third, the audit system works through the collected output data and processes it, producing HTML based reports (shown below) of systems which are in conformance or out of conformance with the templates.

### System Revisions to Elky's Scripts

There are a number of scripts in Elky's system. Each script was reviewed and modified for the network.

Script Name	Description <sup>26</sup>
site.cmd	Check for proper audit files and configure the Windows 2000 Task Scheduler to run the audit collection script. Debugging: In order to debug the script, the "CACLS"

<sup>26</sup> Some of this information is paraphrased From Elky's practical.

	command was commented out. Also, the domain name needed to be changed to match the environment.
y-with-crlf.txt	Provides affirmative input to commands that prompt for Y/N with a carriage return/linefeed. Debugging: This file needed to be created; it wasn't with the package.
attest.pl	Check the Windows 2000 Task Scheduler configuration to make sure that the audit script is properly configured.
recordfqdn.pl	Generates the DNS name of the machine into an output file. The output file is used by another script.
checktracking.pl	Creates the machine-tracking file on the Audit server if none exists.
subinacl.exe	Resource kit utility to set ACLs on shares. Debugging: needed to be added to the auditscripts distribution point.
collect.pl	This script generates the command file "getdata.cmd" batch. Debugging: this script incorrectly generated the file name output and needed to be modified to construct the proper file name (in time stamp format).
getdata.cmd	This command file actually goes and collects the audit system data.
auditreport.pl	This program parses the output data as collected from the various collection points.
audit*.inf	Security templates needed to be created from the base templates provided with Windows 2003.

## Highlights of the Audit System

There are some highlights in Elky's system that should be emphasized.

First, the commands to get data from the "site.cmd" file:

```
IF NOT EXIST C:\HIDDEN\AUDIT\localaudit.cmd (copy /y
"\\dmzdc0.sansgiaccorp.com\auditscripts\localaudit.cmd "
C:\HIDDEN\AUDIT) > NUL 2> NUL
...
CACLS C:\HIDDEN\AUDIT /G SYSTEM:F sansgiaccorp\AuditCollect:F /D
EVERYONE < y-with-crlf.txt > NUL 2>NUL
```

The first command checks to see if there is a local file, and if not it updates the local system with correct files. The "site.cmd" is added to the domain group policy as a "startup" script - therefore whenever any system that is part of the domain starts it runs this batch file. The second command changes the attributes on the files - this is an important security consideration, as regular users should not be allowed to see the directory contents.

The next file of interest is the "collect.cmd" batch file. This file is generated every day, and it does is responsible for collecting the `secedit` output from the enrolled systems back to the collection point.

```
XCOPY /Z /Y /V \\dmzdc0\HIDDEN$\2004-04-17-dmzdc0.raw  
\\dmzdc0.sansgiaccorp.com\auditlogs  
TYPE \\dmzdc0\HIDDEN$\dmzdc0.log >>  
"\\dmzdc0.sansgiaccorp.com\auditlogs\machinelist\dmzdc0.log"
```

These commands are used to retrieve raw output data (from the template processing) and the log data. By collecting the raw data using a time stamped format there is a record of the last time that the `secedit` command was executed.

## System Build Information

---

IT staff deploys Windows 2000 and Windows XP using a automated tools. Examples include Symantec Ghost and Microsoft Remote Installation Services. In order for Elky's audit system to be used, these changes were made to the system build process:

- Active State's ActivePerl was installed on the servers, and incorporated into system images for workstations. The system path needed to be updated to point to perl.exe.
- The Task Scheduler was setup to run under the "Local System Account" account. Specifically, in the Control Panel | Administrative Tools | Services applet, change the entry on the Log On tab for the Task Scheduler service to be Local System Account and check the Allow Service to Interact with Desktop option.
- Many of the scripts use the "C:\HIDDEN" directory. For the initial system build, this directory was created and its attributes set with the `attrib` command: "`attrib +s +h c:\hidden`". Under Windows Explorer, the folder is shown in pastel yellow, indicating to the average user that this is a system directory.
- The subsystem depends on an appropriate environment variable, `%MACHINEROLE%` - this was set on system images, and added to existing servers.

## Active Directory Support

---

Active Directory was configured to support startup/shutdown script "`site.cmd`". This setting in the Default Domain Group Policy object insures that each system in the domain will (eventually!) participate in the audit system.

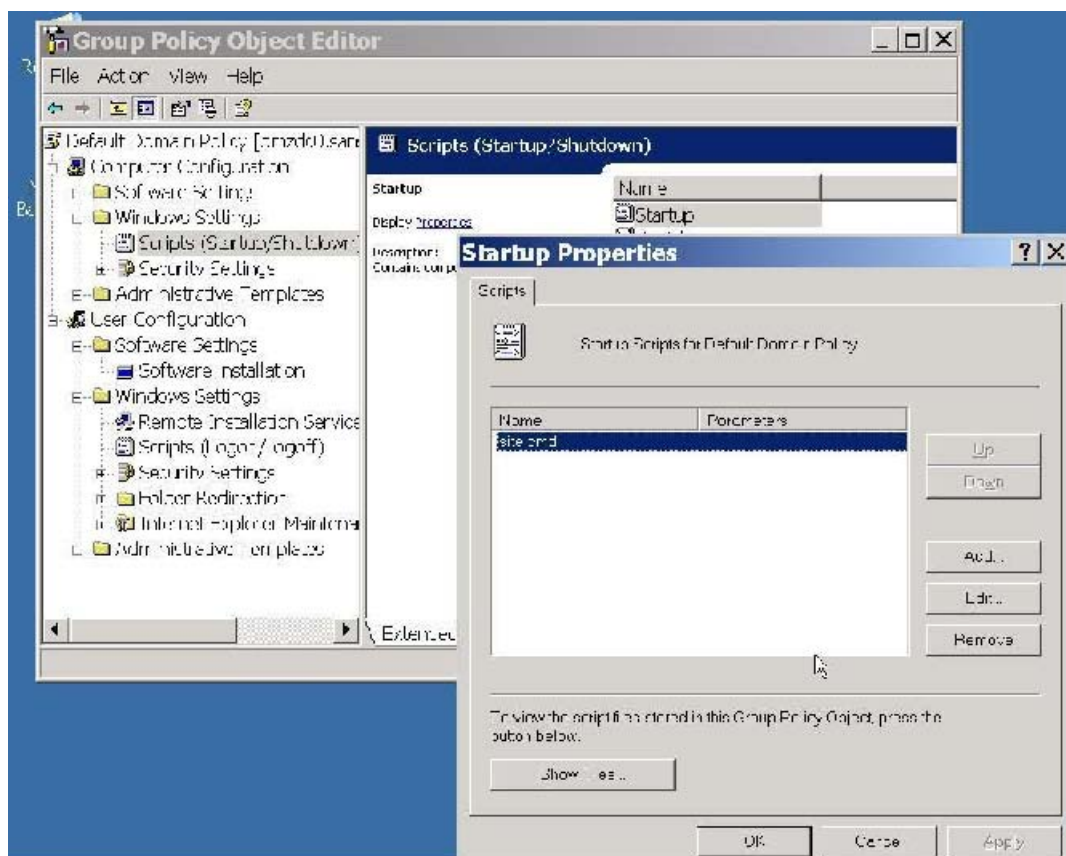


Figure 27: Startup GPO

### ***Example Processed Output***

In order to provide sample output, the default Microsoft provided security templates were used on the system. Elky's weren't used, as they were developed for Windows 2000.

Elky's system uses three templates - audit\_dc.inf, audit\_server.inf, and audit\_workstation.inf. These templates are based on the securedc.inf, the securews.inf, and the securews.inf (no, that's not a type-o) template files, respectively.

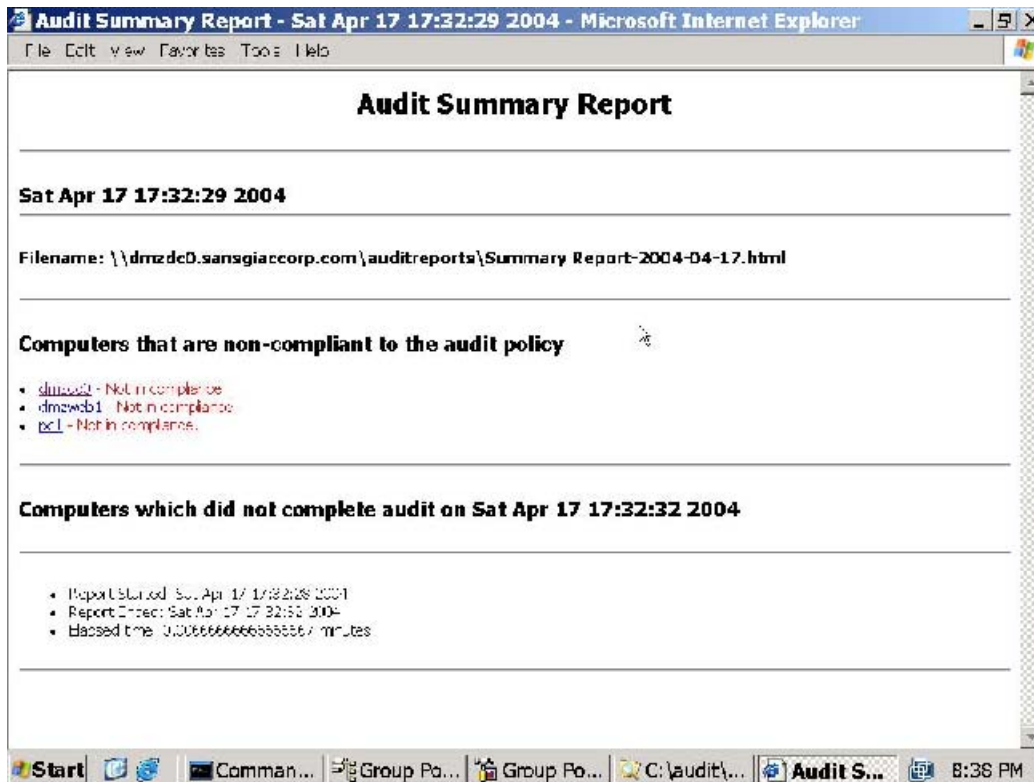


Figure 28: Audit Summary

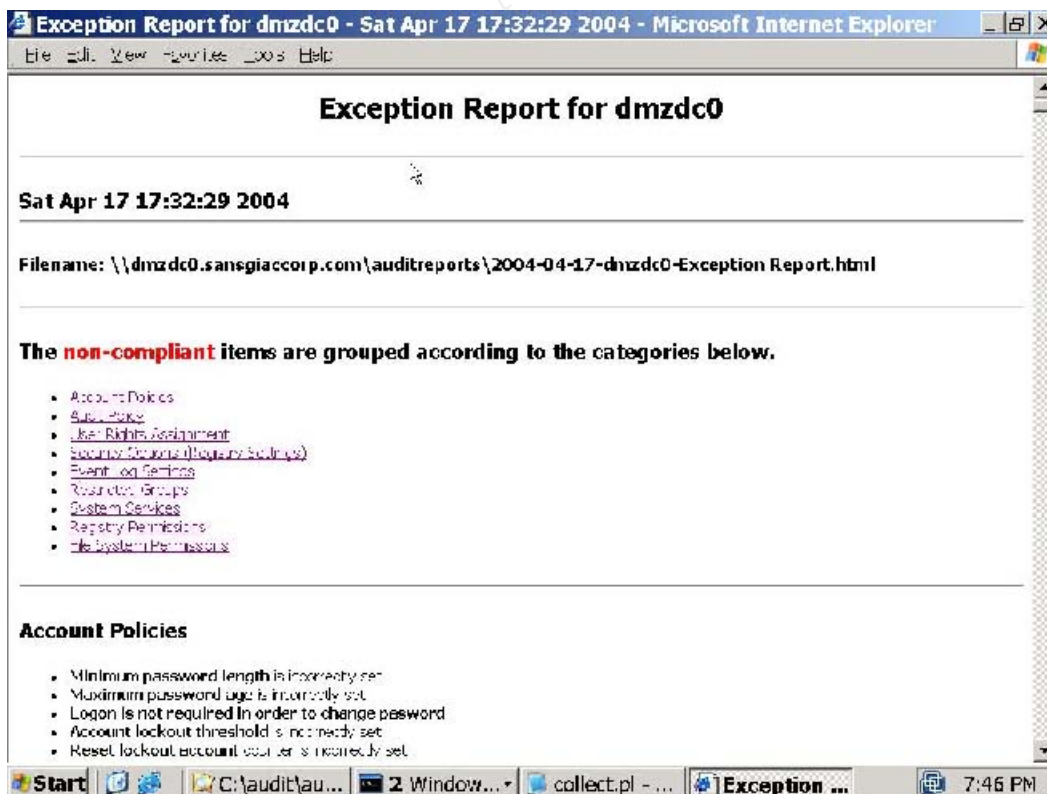


Figure 29: Detailed Audit Report for DC0

Why are all three systems showing up in the report? The template files used in evaluating the systems were not *applied* to the systems - this shows a fundamental benefit and a flaw to the auditing process. The benefit is that an automated system checked the security and configuration of the system against a known baseline - the template. The flaw is that a different set of criteria were used to audit the system that was used to initially configure the system. Auditing, in this case, is a double edged sword.

### ***Gathering Performance Data***

---

On the servers in the DMZ daily performance data will be collected by using the built in "Performance and Maintenance" facility. This system allows for an administrator (the user setting up data collection must be in this group) to collect data every day. Different performance counters are added to the daily job using the Schedule feature. Essentially, each week, an administrator will reset several jobs (one per day) that work with the logman facility.

Example:

```
Logman create counter daily_perf_log -b 4/11/2004 00:10:00 -e 4/17/2004
23:55:00 -r -v mmddhhmm -c "\Processor(_Total)\% Processor Time"
"\Memory\Available bytes" -si 00:15 -o "c:\perfhistory\daily_log"
Logman start daily_perf_log
```

### ***Checking Security Settings***

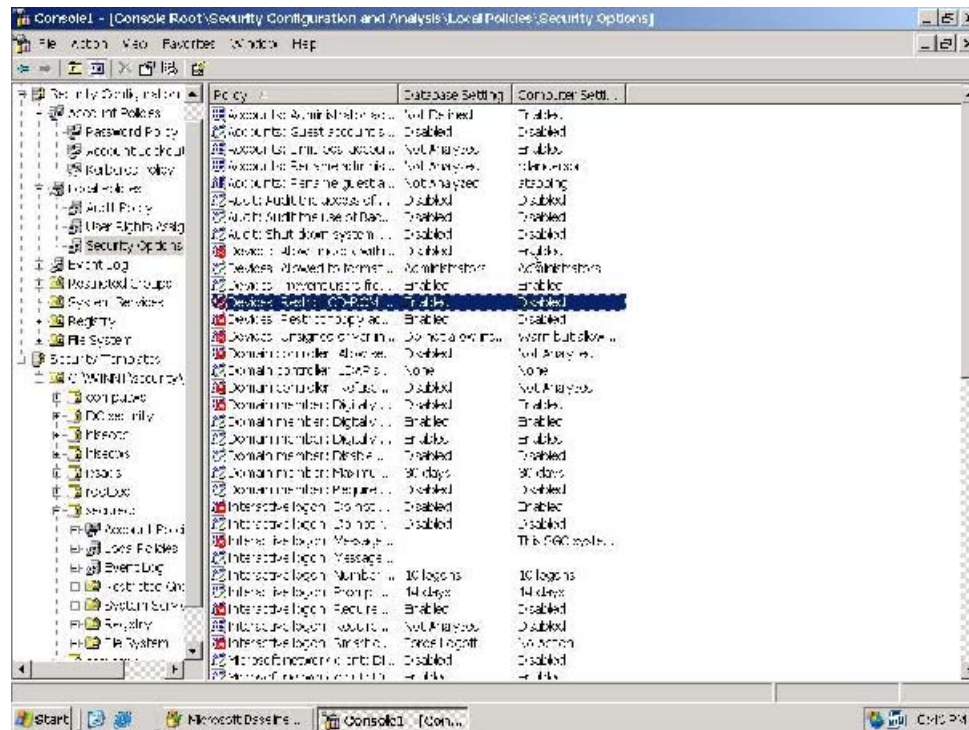
---

There are a variety of tools available for auditing systems. One of the more reputable tools is the Center for Internet Security benchmark and scoring tool. Unfortunately, this tool hasn't been updated for Windows 2003. Therefore testing of the DMZ domains will be performed with the Microsoft Security and Configuration Tool (SCAT) - this is the tool that Elky's system automates.

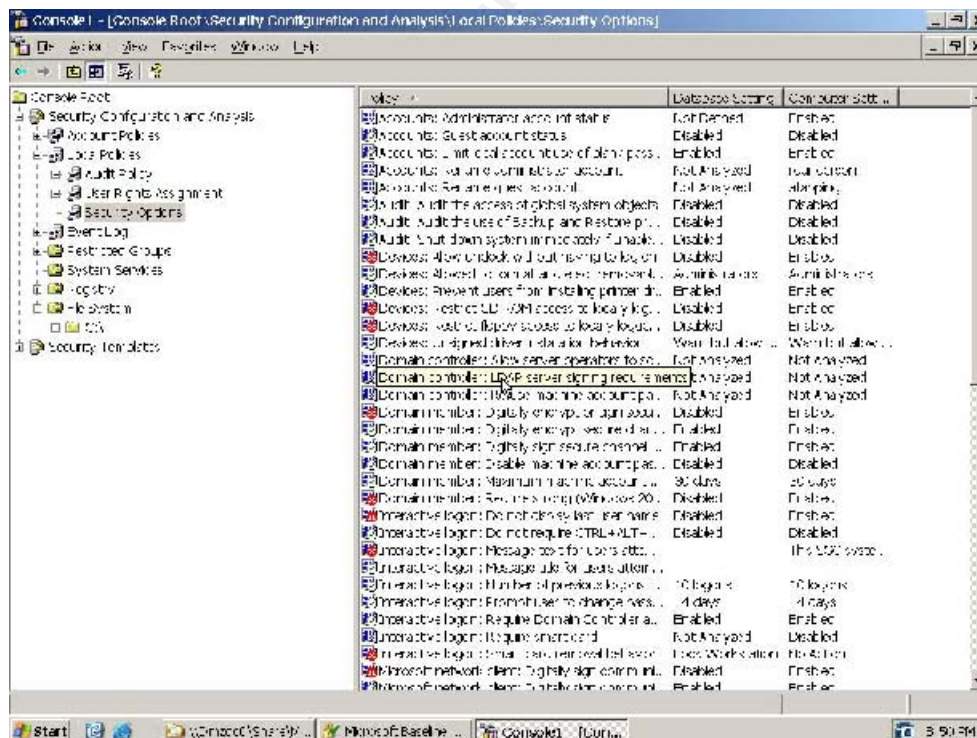
SCAT is used in a three step process. First, a database is created and a base template is used to compare the current state of the system against the template. SCAT analyzes the system against the configuration template. At this point the database can be saved and reused later if need be - or for the more daring the database can be auto *applied* against the system. The system can be compared against the database over time, as need be, in order to detect changes.

The first screen capture is for the domain controller. The analysis performed by the SCAT is based on the "securedc.inf" file, and is focused on the security settings node. Note that the system was *checked* against the template - the template was not *applied* to the system. The second screen capture is for an IIS server in the WebServers OU. This analysis was done against the "hisecws.inf" file - which isn't exactly for web servers, but a good starting point.





### Figure 30: SCAT Analysis of Domain Controller



### Figure 31: SCAT Analysis of IIS Server

Reading the analysis provided by the SCAT tool isn't quite as obvious as one might think in first glance. The red X's may be misinterpreted. For example, the "Restrict CD Rom" option is set to "Enabled" in the securedc.inf template, but "Disabled" in the hisecws.inf template. Further, based on the systems position in the domain, and the group policy that is being applied, the system may or may not conform to the template. One might think that there is an IIS server specific template - checking the IIS 6 Resource kit page doesn't show one<sup>27</sup>.

Essentially the SCAT tool can do a very good job of comparing system security against a baseline - the difficulty here is to determine what baseline.

---

<sup>27</sup> URL: <http://www.microsoft.com/downloads/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&DisplayLang=en>



## Epilogue

---

There are definitely some things I would do differently if I had the time.

First - I would have configured VMware to support a totally virtualized network - I actually used three real routers with four network interfaces between them and a Cisco switch configured with four VLANs to provide a real network.

Second - I would have used my name in some of the domain configuration as required in the practical. Oops.

Third - I would have implemented PKI for supporting an IPSec based network - taking extra time to establish Elky's auditing material put me way over my personal limit on this project.

Fourth - I would have read and reviewed Elky's material much earlier in the process. I decided to use this material after the first and second major sections were nearly done - implementing someone else's codebase was a great idea, and an excellent example of using the SANS community to its fullest. However, since there was a significant investment in time in setting up a test lab, getting screen shots, deploying a DDP and a WebServers GPO - well, I would have preferred to develop a better security template ahead of time, and used that in lieu of the default INF files in order to implement Elky's system.

Fifth - I would have chosen a different GIAC practical. Lam's stuff is fine, but the match between the two organizations wasn't that great.

Lastly - I think I would have liked to explore something different than Option One. Perhaps the security implications and use of Netware 6.5 and ZenWorks for automated system management in a non Microsoft AD system. I decided that this wasn't a great idea - the course is about AD, not NetWare. And someone had just finished their practical on integration with Services for UNIX - which I had bought about a week before so I could use it! Drat!

---

## References

---

A variety of references were used in preparing this paper. They are separated out below based on related categories.

### GIAC Practical Papers

---

These papers were of great guidance and practical value in preparing this document. It is my personal habit to download and keep the practicals that I actually consulted in one subdirectory on my system - various bits and pieces from these esteemed colleagues may have inadvertently crept into my practical. If there is a missing citation, please accept my apologies.

Brunswick, Arnold. "GCWN Practical Assignment" Jan 2, 2004. URL: [www.giac.org/practical/Arnold\\_Brunswick\\_GCWN.pdf](http://www.giac.org/practical/Arnold_Brunswick_GCWN.pdf) (Mar 29, 2004).

Doyle, Joseph. "Implementing and Securing the Merger of SANS Co. and GIAC Enterprises". Aug 21, 2003. URL: [www.giac.org/practical/GCWN/Joseph\\_Doyle\\_GCWN.pdf](http://www.giac.org/practical/GCWN/Joseph_Doyle_GCWN.pdf) (Mar 29, 2004).

Elky, Steve. "Automated Auditing in a Windows 2000 Environment". August 13, 2001. URL: [www.giac.org/practical/Stephen\\_Elky\\_GCNT.zip](http://www.giac.org/practical/Stephen_Elky_GCNT.zip) (Apr 19, 2004).

Galkine, Alexei. "AD Design, Group Policy and Audit for SANS Co and GIAC Enterprises merger". Oct 2003. URL: [www.giac.org/practical/Alexi\\_Galkine\\_GCWN.pdf](http://www.giac.org/practical/Alexi_Galkine_GCWN.pdf) (Mar 22, 2004)

Garden, Jay. "Design, Secure and Audit the Combined SANS Co & GIACE Windows 2000 Network" July 2003. URL: [www.giac.org/practical/GCWN/Jay\\_Garden\\_GCWN.pdf](http://www.giac.org/practical/GCWN/Jay_Garden_GCWN.pdf) (Mar 20, 2004)

Lam, Jason. "GCWN Practical". July 27, 2002 URL: [www.giac.org/practical/Jason\\_Lam\\_GCWN.pdf](http://www.giac.org/practical/Jason_Lam_GCWN.pdf) (Mar 20, 2004)

Lui, Willie. "Giac Certified Windows Security Administrator (GCWN) Practical". 10 Jul 2003. URL: [www.giac.org/practical/Willie\\_Lui.pdf](http://www.giac.org/practical/Willie_Lui.pdf) (Apr 19, 2004)

LeVeque, Vincent. "Certified Windows Security Administrator", Oct 2, 2003. URL: [www.giac.org/practical/GCWN/Vincent\\_LeVeque\\_GCWN.pdf](http://www.giac.org/practical/GCWN/Vincent_LeVeque_GCWN.pdf) (Mar 13, 2004)

Partridge, Richard. "Windows 2000 Vulnerability Analysis, Discovery and Patch Management". Nov 5, 2003. URL: [www.giac.org/practical/GCWN/Richard\\_Partridge\\_GCWN.pdf](http://www.giac.org/practical/GCWN/Richard_Partridge_GCWN.pdf) (Apr 18, 2004)

Poulin, Martin. "Windows and UNIX Interoperability". 23 Jul 2003. URL: [www.giac.org/practical/GCWN/Martin\\_Poulin\\_GCWN.pdf](http://www.giac.org/practical/GCWN/Martin_Poulin_GCWN.pdf) (Mar 13, 2004)

---

**Books and Magazine Articles**

---

Harris, Shon. CISSP Certification All In One Exam Guide, Second Edition. McGraw Hill Osborne, New York. 2003. Pp. 58 - 59, 68 to 72, 614.

Fosson, Jason. SANS GCWN Curricula, offered online. Jan 2004. Numerous references and chapters.

Guglielmo, Karen. "Learning Guide: Security Policy Primer", Mar 20, 2003. URL: [http://whatis.techtarget.com/definition/0,,sid9\\_gci887248,00.html](http://whatis.techtarget.com/definition/0,,sid9_gci887248,00.html) (Mar 26, 2004)

---

**Web sites and Web Articles**

---

Elky, Steve. "Automated Auditing in a Windows 2000 Environment" Aug 13, 2001. URL: [http://www.sans.org/resources/auto\\_audit.php](http://www.sans.org/resources/auto_audit.php) (Apr 4, 2004).

Microsoft Corporation. support.microsoft.com. "HOW TO: Set up a One-Way Non-Transitive Trust in Windows 2000 (309682)". 11/5/2003. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;309682&Product=win2000> (Mar 22, 2004).

Microsoft Corporation. URL: [http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/sag\\_ADtrustVerify.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/sag_ADtrustVerify.asp) (Mar 22, 2004).

Microsoft Corporation. "Active Directory Documentation". URL: [http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/x\\_c\\_forestrusts.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/x_c_forestrusts.asp) (Mar 22, 2004).

Microsoft Corporation. "Support Webcast (transcript)" Oct 11, 2001. URL: <http://support.microsoft.com/default.aspx?scid=%2Fservicedesks%2Fwebcasts%2Fen%2Fwc101101%2Fwct101101.asp> (Mar 22, 2004).

Microsoft Corporation. "HOW TO: Create an External Trust in Windows Server 2003" 12/18/2003. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;816301> (Mar 31, 2003)

Microsoft Corporation. "Windows Server 2003 Security Guide", April 2003. URL: <http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx> (Apr 1, 2003)

Microsoft Corporation. "Domain Security Policy in Windows 2000". 11/4/2003. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;221930&Product=win2000> (April 2, 2003)

Microsoft Corporation. "Group Policy Application Rules for Domain Controllers" 11/4/2003, URL: <http://support.microsoft.com/default.aspx?kbid=259576> (April 2, 2003)

Microsoft Corporation. "IIS 6.0 Resource Kit Tools". URL: <http://www.microsoft.com/downloads/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&DisplayLang=en> (Apr 14, 2004).

© SANS Institute 2004, Author retains full rights.

## Appendix A: GPMC Results for DMZDC0

Group Policy Results		
SANSGIACCORP\ rdanderson on SANSGIACCORP\ DMZDC0		
Data collected on: 4/13/2004 9:29:24 PM		
Summary	Error! Hyperlink reference not valid.	
Computer Configuration Summary Error! Hyperlink reference not valid.		
General Error! Hyperlink reference not valid.		
Computer name	SANSGIACCORP\DMZDC0	
Domain	sansgiaccorp.com	
Site	Default-First-Site-Name	
Last time Group Policy was processed	4/13/2004 9:22:56 PM	
Group Policy Objects Error! Hyperlink reference not valid.		
Applied GPOs Error! Hyperlink reference not valid.		
Name	Link Location	Revision
Default Domain Policy	sansgiaccorp.com	AD (90), Sysvol (90)
Default Domain Controllers Policy	sansgiaccorp.com/Domain Controllers	AD (1), Sysvol (1)
Denied GPOs Error! Hyperlink reference not valid.		
Name	Link Location	Reason Denied
Local Group Policy	Local	Empty
Security Group Membership when Group Policy was applied Error! Hyperlink reference not valid.		
BUILTIN\Administrators Everyone SANSGIACCORP\IIS_WPG BUILTIN\Pre-Windows 2000 Compatible Access BUILTIN\Users BUILTIN\Windows Authorization Access Group NT AUTHORITY\NETWORK NT AUTHORITY\Authenticated Users NT AUTHORITY\This Organization SANSGIACCORP\DMZDC0\$ SANSGIACCORP\Domain Controllers NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS		
WMI Filters Error! Hyperlink reference not valid.		
Name	Value	Reference GPO(s)
None		

**Component Status** Error! Hyperlink reference not valid.

Component Name	Status	Last Process Time
Group Policy Infrastructure	Success	4/13/2004 9:26:40 PM
EFS recovery	Success (no data)	4/10/2004 4:07:26 PM
Registry	Success	4/10/2004 4:07:16 PM
Security	Success	4/10/2004 4:07:26 PM

**User Configuration Summary** Error! Hyperlink reference not valid.

**General** Error! Hyperlink reference not valid.

User name	SANSGIACCORP\rdanderson
Domain	sansgiaccorp.com
Last time Group Policy was processed	4/13/2004 9:08:12 PM

**Group Policy Objects** Error! Hyperlink reference not valid.

**Applied GPOs** Error! Hyperlink reference not valid.

Name	Link Location	Revision
Default Domain Policy	sansgiaccorp.com	AD (1), Sysvol (1)

**Denied GPOs** Error! Hyperlink reference not valid.

Name	Link Location	Reason Denied
Local Group Policy	Local	Empty

**Security Group Membership when Group Policy was applied** Error! Hyperlink reference not valid.

SANSGIACCORP\Domain Users  
 Everyone  
 BUILTIN\Administrators  
 BUILTIN\Users  
 BUILTIN\Pre-Windows 2000 Compatible Access  
 NT AUTHORITY\INTERACTIVE  
 NT AUTHORITY\Authenticated Users  
 NT AUTHORITY\This Organization  
 LOCAL  
 SANSGIACCORP\Group Policy Creator Owners  
 SANSGIACCORP\Domain Admins  
 SANSGIACCORP\Schema Admins  
 SANSGIACCORP\Enterprise Admins

**WMI Filters** Error! Hyperlink reference not valid.

Name	Value	Reference GPO(s)
None		

**Component Status** Error! Hyperlink reference not valid.

Component Name	Status	Last Process Time
Group Policy Infrastructure	Success	4/13/2004 9:08:13 PM
<b>Computer Configuration</b> Error! Hyperlink reference not valid.		
<b>Windows Settings</b> Error! Hyperlink reference not valid.		
<b>Security Settings</b> Error! Hyperlink reference not valid.		
<b>Account Policies/Password Policy</b> Error! Hyperlink reference not valid.		
Policy	Setting	Winning GPO
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	8 characters	Default Domain Policy
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy
<b>Account Policies/Account Lockout Policy</b> Error! Hyperlink reference not valid.		
Policy	Setting	Winning GPO
Account lockout duration	30 minutes	Default Domain Policy
Account lockout threshold	5 invalid logon attempts	Default Domain Policy
Reset account lockout counter after	30 minutes	Default Domain Policy
<b>Account Policies/Kerberos Policy</b> Error! Hyperlink reference not valid.		
Policy	Setting	Winning GPO
Enforce user logon restrictions	Enabled	Default Domain Policy
Maximum lifetime for service ticket	600 minutes	Default Domain Policy
Maximum lifetime for user ticket	10 hours	Default Domain Policy
Maximum lifetime for user ticket renewal	7 days	Default Domain Policy
Maximum tolerance for computer	5 minutes	Default Domain Policy

clock synchronization

**Local Policies/Audit Policy** Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
Audit account logon events	Success	Default Domain Controllers Policy
Audit account management	Success	Default Domain Controllers Policy
Audit directory service access	Success	Default Domain Controllers Policy
Audit logon events	Success	Default Domain Controllers Policy
Audit object access	No auditing	Default Domain Controllers Policy
Audit policy change	Success	Default Domain Controllers Policy
Audit privilege use	No auditing	Default Domain Controllers Policy
Audit process tracking	No auditing	Default Domain Controllers Policy
Audit system events	Success	Default Domain Controllers Policy

**Local Policies/User Rights Assignment** Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
Access this computer from the network	Everyone, SANSIACCORP\IUSR_DMZDC0, SANSIACCORP\IWAM_DMZDC0, Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS, Pre-Windows 2000 Compatible Access	Default Domain Controllers Policy
Act as part of the operating system		Default Domain Controllers Policy
Add workstations to domain	Authenticated Users	Default Domain Controllers Policy
Adjust memory quotas for a process	LOCAL SERVICE, NETWORK SERVICE, SANSIACCORP\IWAM_DMZDC0, Administrators	Default Domain Controllers Policy
Allow log on locally	SANSIACCORP\IUSR_DMZDC0, Administrators, Backup Operators,	Default Domain Controllers Policy



	Account Operators, Server Operators, Print Operators	
Back up files and directories	Administrators, Backup Operators, Server Operators	Default Domain Controllers Policy
Bypass traverse checking	Everyone, Administrators, Authenticated Users, Pre-Windows 2000 Compatible Access	Default Domain Controllers Policy
Change the system time	Administrators, Server Operators	Default Domain Controllers Policy
Create a pagefile	Administrators	Default Domain Controllers Policy
Create a token object		Default Domain Controllers Policy
Create permanent shared objects		Default Domain Controllers Policy
Debug programs	Administrators	Default Domain Controllers Policy
Deny access to this computer from the network	SANSGIACCORP\SUPPORT_388945a0	Default Domain Controllers Policy
Deny log on as a batch job		Default Domain Controllers Policy
Deny log on as a service		Default Domain Controllers Policy
Deny log on locally	SANSGIACCORP\SUPPORT_388945a0	Default Domain Controllers Policy
Enable computer and user accounts to be trusted for delegation	Administrators	Default Domain Controllers Policy
Force shutdown from a remote system	Administrators, Server Operators	Default Domain Controllers Policy
Generate security audits	LOCAL SERVICE, NETWORK SERVICE	Default Domain Controllers Policy
Increase scheduling priority	Administrators	Default Domain Controllers Policy
Load and unload device drivers	Administrators, Print Operators	Default Domain Controllers Policy
Lock pages in memory		Default Domain Controllers Policy
Log on as a batch job	LOCAL SERVICE, SANSGIACCORP\IUSR_DMZDC0, SANSGIACCORP\IWAM_DMZDC0,	Default Domain Controllers Policy

	SANSGIACCORP\IIS_WPG, SANSGIACCORP\SUPPORT_388945a0	
Log on as a service	NETWORK SERVICE	Default Domain Controllers Policy
Manage auditing and security log	Administrators	Default Domain Controllers Policy
Modify firmware environment values	Administrators	Default Domain Controllers Policy
Profile single process	Administrators	Default Domain Controllers Policy
Profile system performance	Administrators	Default Domain Controllers Policy
Remove computer from docking station	Administrators	Default Domain Controllers Policy
Replace a process level token	LOCAL SERVICE, NETWORK SERVICE, SANSGIACCORP\IWAM_DMZDC0	Default Domain Controllers Policy
Restore files and directories	Administrators, Backup Operators, Server Operators	Default Domain Controllers Policy
Shut down the system	Administrators, Backup Operators, Server Operators, Print Operators	Default Domain Controllers Policy
Synchronize directory service data		Default Domain Controllers Policy
Take ownership of files or other objects	Administrators	Default Domain Controllers Policy

**Local Policies/Security Options** Error! Hyperlink reference not valid.

**Accounts** Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
Accounts: Rename administrator account	rdanderson	Default Domain Policy
Accounts: Rename guest account	atapping	Default Domain Policy

**Devices** Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
Devices: Allowed to format and eject removable media	Administrators	Default Domain Policy

	Devices: Unsigned driver installation behavior	Warn but allow installation	Default Domain Policy	
	<b>Domain Controller</b> Error! Hyperlink reference not valid.			
	<b>Policy</b>	<b>Setting</b>	<b>Winning GPO</b>	
	Domain controller: LDAP server signing requirements	None	Default Domain Controllers Policy	
	<b>Domain Member</b> Error! Hyperlink reference not valid.			
	<b>Policy</b>	<b>Setting</b>	<b>Winning GPO</b>	
	Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Default Domain Controllers Policy	
	<b>Interactive Logon</b> Error! Hyperlink reference not valid.			
	<b>Policy</b>	<b>Setting</b>	<b>Winning GPO</b>	
	Interactive logon: Do not display last user name	Enabled	Default Domain Policy	
	Interactive logon: Message text for users attempting to log on	This SGC system is restricted to authorized users, and uses. Individuals attempting unauthorized access, will be prosecuted. unauthorized, terminate access now!, Clicking indicates your acceptance monitoring and auditing.	Default Domain Policy	
	<b>Microsoft Network Server</b> Error! Hyperlink reference not valid.			
	<b>Policy</b>	<b>Setting</b>	<b>Winning GPO</b>	
	Microsoft network server: Digitally sign communications (always)	Enabled	Default Domain Controllers Policy	
	Microsoft network server: Digitally sign communications (if client agrees)	Enabled	Default Domain Controllers Policy	
	<b>Network Access</b> Error! Hyperlink reference not valid.			
	<b>Policy</b>	<b>Setting</b>	<b>Winning GPO</b>	

Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	Default Domain Policy
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled	Default Domain Policy
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Enabled	Default Domain Policy
Network access: Named Pipes that can be accessed anonymously		Default Domain Policy
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	Default Domain Policy
Network access: Shares that can be accessed anonymously		Default Domain Policy
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	Default Domain Policy

**Network Security** Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
Network security: Do not store LAN Manager hash value on next password change	Enabled	Default Domain Policy
Network security: Force logoff when logon hours expire	Disabled	Default Domain Policy
Network security: LAN Manager authentication level	Send NTLM response only	Default Domain Controllers Policy
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled	Default Domain Policy
Require message integrity	Enabled	

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Allow users to encrypt files using Encrypting File System (EFS)	Enabled
---	---------

<b>Certificates</b>	Error! Hyperlink reference not valid.
---------------------	---------------------------------------

Issued To	Issued By	Expiration Date	Intended Purposes	Winning GPO
Administrator	Administrator	4/3/2007 8:53:43 PM	File Recovery	Default Domain Policy

For additional information about individual settings, launch Group Policy Object Editor.

<b>Public Key Policies/Trusted Root Certification Authorities</b>	Error! Hyperlink reference not valid.
---	---------------------------------------

<b>Properties</b>	Error! Hyperlink reference not valid.
-------------------	---------------------------------------

<b>Winning GPO</b>	[Default setting]
--------------------	-------------------

Policy	Setting
Allow users to select new root certification authorities (CAs) to trust	Enabled
Client computers can trust the following certificate stores	Third-Party Root Certification Authorities and Enterprise Root Certification Authorities
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Registered in Active Directory only

<b>User Configuration</b>	Error! Hyperlink reference not valid.
---------------------------	---------------------------------------

No settings defined.
----------------------

© SANS Institute

## Appendix B: GPMC Results for DMZWEB1

### Group Policy Results

#### SANSGIACCORP\ rdanderson on SANSGIACCORP\ DMZWEB1

Data collected on: 4/13/2004  
10:19:43 PM

**Summary** Error! Hyperlink reference not valid.

**Computer Configuration Summary** Error! Hyperlink reference not valid.

**General** Error! Hyperlink reference not valid.

Computer name	SANSGIACCORP\DMZWEB1
Domain	sansgiaccorp.com
Site	Default-First-Site-Name
Last time Group Policy was processed	4/13/2004 10:14:01 PM

**Group Policy Objects** Error! Hyperlink reference not valid.

**Applied GPOs** Error! Hyperlink reference not valid.

Name	Link Location	Revision
Default Domain Policy	sansgiaccorp.com	AD (90), Sysvol (90)
DMZ_WebServers	sansgiaccorp.com/WebServers	AD (183), Sysvol (183)

**Denied GPOs** Error! Hyperlink reference not valid.

Name	Link Location	Reason Denied
Local Group Policy	Local	Empty

**Security Group Membership when Group Policy was applied** Error! Hyperlink reference not valid.

BUILTIN\Administrators  
Everyone  
S-1-5-21-2184914993-3854961186-316308027-1002  
BUILTIN\Users  
NT AUTHORITY\NETWORK  
NT AUTHORITY\Authenticated Users  
NT AUTHORITY\This Organization  
SANSGIACCORP\DMZWEB1\$  
SANSGIACCORP\Domain Computers

**WMI Filters** Error! Hyperlink reference not valid.

Name	Value	Reference GPO(s)
None		

**Component Status** Error! Hyperlink reference not valid.

Component Name	Status	Last Process Time
----------------	--------	-------------------

Group Policy Infrastructure	Success	4/13/2004 10:16:16 PM
EFS recovery	Success (no data)	4/10/2004 5:28:10 PM
Registry	Success	4/10/2004 5:27:56 PM
Security	Success	4/13/2004 10:16:16 PM

**User Configuration Summary** Error! Hyperlink reference not valid.

**General** Error! Hyperlink reference not valid.

User name	SANSGIACCORP\rdanderson
Domain	sansgiaccorp.com
Last time Group Policy was processed	4/13/2004 9:16:01 PM

**Group Policy Objects** Error! Hyperlink reference not valid.

**Applied GPOs** Error! Hyperlink reference not valid.

Name	Link Location	Revision
Default Domain Policy	sansgiaccorp.com	AD (1), Sysvol (1)

**Denied GPOs** Error! Hyperlink reference not valid.

Name	Link Location	Reason Denied
Local Group Policy	Local	Empty

**Security Group Membership when Group Policy was applied** Error! Hyperlink reference not valid.

SANSGIACCORP\Domain Users  
 Everyone  
 BUILTIN\Users  
 BUILTIN\Administrators  
 NT AUTHORITY\INTERACTIVE  
 NT AUTHORITY\Authenticated Users  
 NT AUTHORITY\This Organization  
 LOCAL  
 SANSGIACCORP\Group Policy Creator Owners  
 SANSGIACCORP\Domain Admins  
 SANSGIACCORP\Schema Admins  
 SANSGIACCORP\Enterprise Admins

**WMI Filters** Error! Hyperlink reference not valid.

Name	Value	Reference GPO(s)
None		

**Component Status** Error! Hyperlink reference not valid.

Component Name	Status	Last Process Time
Group Policy Infrastructure	Success	4/13/2004 9:16:03 PM

**Computer Configuration** Error! Hyperlink reference not valid.



**Windows Settings** Error! Hyperlink reference not valid.

**Security Settings** Error! Hyperlink reference not valid.

**Account Policies/Password Policy** Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	8 characters	Default Domain Policy
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy

**Account Policies/Account Lockout Policy** Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
Account lockout duration	30 minutes	Default Domain Policy
Account lockout threshold	5 invalid logon attempts	Default Domain Policy
Reset account lockout counter after	30 minutes	Default Domain Policy

**Local Policies/Audit Policy** Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	Default Domain Policy
Audit account management	Success, Failure	Default Domain Policy
Audit directory service access	Success, Failure	Default Domain Policy
Audit logon events	Success, Failure	Default Domain Policy
Audit object access	Success, Failure	Default Domain Policy
Audit policy change	Success	Default Domain Policy
Audit privilege use	Success, Failure	Default Domain Policy
Audit system events	Success, Failure	Default Domain Policy

**Local Policies/User Rights Assignment** Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
--------	---------	-------------

Access this computer from the network	Authenticated Users	Default Domain Policy
Allow log on locally	Administrators, Authenticated Users, Backup Operators	Default Domain Policy
Allow log on through Terminal Services	Remote Desktop Users, SANSIACCORP\rdanderson	DMZ_WebServers
Deny log on through Terminal Services	SANSIACCORP\atapping, SANSIACCORP\SUPPORT_388945a0	DMZ_WebServers
Generate security audits	LOCAL SERVICE, NETWORK SERVICE	DMZ_WebServers
Load and unload device drivers	Administrators	DMZ_WebServers
Manage auditing and security log	Administrators	DMZ_WebServers
Modify firmware environment values	Administrators	DMZ_WebServers
Perform volume maintenance tasks	Administrators	DMZ_WebServers
Take ownership of files or other objects	Administrators	DMZ_WebServers

**Local Policies/Security Options** Error! Hyperlink reference not valid.

**Accounts** Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
Accounts: Guest account status	Disabled	DMZ_WebServers
Accounts: Limit local account use of blank passwords to console logon only	Enabled	DMZ_WebServers
Accounts: Rename administrator account	rdanderson	Default Domain Policy
Accounts: Rename guest account	atapping	Default Domain Policy

**Audit** Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
Audit: Audit the access of global system objects	Disabled	DMZ_WebServers

	Audit: Audit the use of Backup and Restore privilege	Disabled	DMZ_WebServers
	<b>Devices</b> Error! Hyperlink reference not valid.		
	<b>Policy</b>	<b>Setting</b>	<b>Winning GPO</b>
	Devices: Allowed to format and eject removable media	Administrators	DMZ_WebServers
	Devices: Prevent users from installing printer drivers	Enabled	DMZ_WebServers
	Devices: Restrict CD-ROM access to locally logged-on user only	Enabled	DMZ_WebServers
	Devices: Restrict floppy access to locally logged-on user only	Enabled	DMZ_WebServers
	Devices: Unsigned driver installation behavior	Warn but allow installation	DMZ_WebServers
	<b>Domain Member</b> Error! Hyperlink reference not valid.		
	<b>Policy</b>	<b>Setting</b>	<b>Winning GPO</b>
	Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	DMZ_WebServers
	Domain member: Digitally encrypt secure channel data (when possible)	Enabled	DMZ_WebServers
	Domain member: Digitally sign secure channel data (when possible)	Enabled	DMZ_WebServers
	Domain member: Require strong (Windows 2000 or later) session key	Enabled	DMZ_WebServers
	<b>Interactive Logon</b> Error! Hyperlink reference not valid.		
	<b>Policy</b>	<b>Setting</b>	<b>Winning GPO</b>
	Interactive logon: Do not display last user name	Enabled	DMZ_WebServers
	Interactive logon: Do not require CTRL+ALT+DEL	Disabled	DMZ_WebServers

	Interactive logon: Message text for users attempting to log on	This SGC system is restricted to authorized users, and uses.Individuals attempting unauthorized access, will be prosecuted.unauthorized, terminate access now!, Clicking indicates your acceptance monitoring and auditing.	Default Domain Policy
	Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled	DMZ_WebServers
	<b>Microsoft Network Client</b>	Error! Hyperlink reference not valid.	
	<b>Policy</b>	<b>Setting</b>	<b>Winning GPO</b>
	Microsoft network client: Digitally sign communications (always)	Enabled	DMZ_WebServers
	<b>Network Access</b>	Error! Hyperlink reference not valid.	
	<b>Policy</b>	<b>Setting</b>	<b>Winning GPO</b>
	Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	DMZ_WebServers
	Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled	DMZ_WebServers
	Network access: Do not allow storage of credentials or .NET Passports for network authentication	Enabled	DMZ_WebServers
	Network access: Let Everyone permissions apply to anonymous users	Disabled	DMZ_WebServers
	Network access: Named Pipes that can be accessed anonymously		DMZ_WebServers
	Network access: Restrict anonymous	Enabled	DMZ_WebServers

access to Named Pipes and Shares		
Network access: Shares that can be accessed anonymously		DMZ_WebServers
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	DMZ_WebServers

**Network Security** Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
Network security: Do not store LAN Manager hash value on next password change	Enabled	DMZ_WebServers
Network security: Force logoff when logon hours expire	Disabled	Default Domain Policy
Network security: LAN Manager authentication level	Send NTLMv2 response only\refuse LM	Default Domain Policy
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled	Default Domain Policy
Require message integrity	Enabled	
Require message confidentiality	Enabled	
Require NTLMv2 session security	Enabled	
Require 128-bit encryption	Enabled	
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Enabled	Default Domain Policy
Require message integrity	Enabled	
Require message confidentiality	Enabled	
Require NTLMv2 session security	Enabled	
Require 128-bit encryption	Enabled	

**Shutdown** Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
--------	---------	-------------

	Shutdown: Allow system to be shut down without having to log on	Disabled	DMZ_WebServers
	Shutdown: Clear virtual memory pagefile	Enabled	DMZ_WebServers
	<b>System Settings</b> Error! Hyperlink reference not valid.		
	<b>Policy</b>	<b>Setting</b>	<b>Winning GPO</b>
	System settings: Optional subsystems		DMZ_WebServers
	<b>Event Log</b> Error! Hyperlink reference not valid.		
	<b>Policy</b>	<b>Setting</b>	<b>Winning GPO</b>
	Retain application log	14 days	Default Domain Policy
	Retain security log	14 days	Default Domain Policy
	Retain system log	14 days	Default Domain Policy
	Retention method for application log	By days	Default Domain Policy
	Retention method for security log	By days	Default Domain Policy
	Retention method for system log	By days	Default Domain Policy
	<b>System Services</b> Error! Hyperlink reference not valid.		
	<b>Alerter (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.		
	<b>Winning GPO</b> DMZ_WebServers		
	<b>Permissions</b> No permissions specified		
	<b>Auditing</b> No auditing specified		
	<b>Application Layer Gateway Service (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.		
	<b>Winning GPO</b> DMZ_WebServers		
	<b>Permissions</b> No permissions specified		
	<b>Auditing</b> No auditing specified		
	<b>Application Management (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.		
	<b>Winning GPO</b> DMZ_WebServers		
	<b>Permissions</b> No permissions specified		
	<b>Auditing</b> No auditing specified		

	<b>Windows Audio (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Background Intelligent Transfer Service (Startup Mode: Manual)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Computer Browser (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Indexing Service (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>ClipBook (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>COM+ System Application (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Cryptographic Services (Startup Mode: Manual)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	

	<b>Distributed File System (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>DHCP Client (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>DHCP Server (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Logical Disk Manager Administrative Service (Startup Mode: Manual)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Logical Disk Manager (Startup Mode: Manual)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>DNS Server (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>DNS Client (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	



	<b>Error Reporting Service (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Event Log (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>COM+ Event System (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Help and Support (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Human Interface Device Access (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>HTTP SSL (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>IIS Admin Service (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	

	<b>IMAPI CD-Burning COM Service (Startup Mode: Manual)</b>	Error! Hyperlink reference not valid.
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Intersite Messaging (Startup Mode: Disabled)</b>	Error! Hyperlink reference not valid.
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Kerberos Key Distribution Center (Startup Mode: Disabled)</b>	Error! Hyperlink reference not valid.
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Server (Startup Mode: Automatic)</b>	Error! Hyperlink reference not valid.
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Workstation (Startup Mode: Automatic)</b>	Error! Hyperlink reference not valid.
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>License Logging (Startup Mode: Disabled)</b>	Error! Hyperlink reference not valid.
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>TCP/IP NetBIOS Helper (Startup Mode: Automatic)</b>	Error! Hyperlink reference not valid.
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	

	<b>Messenger (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>NetMeeting Remote Desktop Sharing (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Distributed Transaction Coordinator (Startup Mode: Manual)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>FTP Publishing Service (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Windows Installer (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Network DDE (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Network DDE DSDM (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	

	<b>Net Logon (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Network Connections (Startup Mode: Manual)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Network Location Awareness (NLA) (Startup Mode: Manual)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>File Replication Service (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>NT LM Security Support Provider (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Removable Storage (Startup Mode: Manual)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Plug and Play (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	

	<b>IPSEC Services (Startup Mode: Manual)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Protected Storage (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Remote Access Auto Connection Manager (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Remote Access Connection Manager (Startup Mode: Manual)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Remote Desktop Help Session Manager (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Routing and Remote Access (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Remote Registry (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	

	<b>Remote Procedure Call (RPC) Locator (Startup Mode: Manual)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Remote Procedure Call (RPC) (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Resultant Set of Policy Provider (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Special Administration Console Helper (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Security Accounts Manager (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Smart Card (Startup Mode: Manual)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Task Scheduler (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b>	
	Type	Name Permission

Allow	BUILTIN\Administrators	Full Control	
Allow	NT AUTHORITY\SYSTEM	Full Control	
Allow	NT AUTHORITY\INTERACTIVE	Read	

**Auditing**

Type	Name	Access	
Failure	Everyone	Full Control	

**Secondary Logon (Startup Mode: Disabled)** Error! Hyperlink reference not valid.

**Winning GPO**

DMZ\_WebServers

**Permissions**

No permissions specified

**Auditing**

No auditing specified

**System Event Notification (Startup Mode: Automatic)** Error! Hyperlink reference not valid.

**Winning GPO**

DMZ\_WebServers

**Permissions**

No permissions specified

**Auditing**

No auditing specified

**Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS) (Startup Mode: Disabled)** Error! Hyperlink reference not valid.

**Winning GPO**

DMZ\_WebServers

**Permissions**

No permissions specified

**Auditing**

No auditing specified

**Shell Hardware Detection (Startup Mode: Disabled)** Error! Hyperlink reference not valid.

**Winning GPO**

DMZ\_WebServers

**Permissions**

No permissions specified

**Auditing**

No auditing specified

**SNMP Service (Startup Mode: Disabled)** Error! Hyperlink reference not valid.

**Winning GPO**

DMZ\_WebServers

**Permissions**

No permissions specified

**Auditing**

No auditing specified

**SNMP Trap Service (Startup Mode: Disabled)** Error! Hyperlink reference not valid.

**Winning GPO**

DMZ\_WebServers

	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Print Spooler (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Windows Image Acquisition (WIA) (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Microsoft Software Shadow Copy Provider (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Performance Logs and Alerts (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Telephony (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Terminal Services (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Themes (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers



	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Telnet (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Distributed Link Tracking Server (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Distributed Link Tracking Client (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Terminal Services Session Directory (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Upload Manager (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Uninterruptible Power Supply (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Virtual Disk Service (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers

	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>VMware Tools Service (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Volume Shadow Copy (Startup Mode: Manual)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Windows Time (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>World Wide Web Publishing Service (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>WebClient (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>WinHTTP Web Proxy Auto-Discovery Service (Startup Mode: Disabled)</b> Error! Hyperlink reference not valid.	
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Windows Management Instrumentation (Startup Mode: Automatic)</b> Error! Hyperlink reference not valid.	

	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Windows Internet Name Service (WINS) (Startup Mode: Disabled)</b>	Error! Hyperlink reference not valid.
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Portable Media Serial Number Service (Startup Mode: Disabled)</b>	Error! Hyperlink reference not valid.
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Windows Management Instrumentation Driver Extensions (Startup Mode: Manual)</b>	Error! Hyperlink reference not valid.
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>WMI Performance Adapter (Startup Mode: Manual)</b>	Error! Hyperlink reference not valid.
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Automatic Updates (Startup Mode: Disabled)</b>	Error! Hyperlink reference not valid.
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	
	<b>Wireless Configuration (Startup Mode: Disabled)</b>	Error! Hyperlink reference not valid.
	<b>Winning GPO</b>	DMZ_WebServers
	<b>Permissions</b> No permissions specified	
	<b>Auditing</b> No auditing specified	

[Public Key Policies/Autoenrollment Settings](#) Error! Hyperlink reference not valid.

Policy	Setting	Winning GPO
Enroll certificates automatically	Enabled	[Default setting]
Renew expired certificates, update pending certificates, and remove revoked certificates	Disabled	
Update certificates that use certificate templates	Disabled	

[Public Key Policies/Encrypting File System](#) Error! Hyperlink reference not valid.

[Properties](#) Error! Hyperlink reference not valid.

Winning GPO [Default setting]

Policy	Setting
Allow users to encrypt files using Encrypting File System (EFS)	Enabled

[Certificates](#) Error! Hyperlink reference not valid.

Issued To	Issued By	Expiration Date	Intended Purposes	Winning GPO
Administrator	Administrator	4/3/2007 8:53:43 PM	File Recovery	Default Domain Policy

For additional information about individual settings, launch Group Policy Object Editor.

[Public Key Policies/Trusted Root Certification Authorities](#) Error! Hyperlink reference not valid.

[Properties](#) Error! Hyperlink reference not valid.

Winning GPO [Default setting]

Policy	Setting
Allow users to select new root certification authorities (CAs) to trust	Enabled
Client computers can trust the following certificate stores	Third-Party Root Certification Authorities and Enterprise Root Certification Authorities
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Registered in Active Directory only

[User Configuration](#) Error! Hyperlink reference not valid.

No settings defined.