



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>

Certified Windows Security Administrator (GCWN)
Practical Assignment Version 1.0
Option 1 –Securing a Windows 2000 Network with Group Policies
Jennifer L. Fountain

© SANS Institute 2003, Author retains full rights.

TABLE OF CONTENTS

| | | |
|---------------------|--|----|
| 1.0 | Introduction | 3 |
| 2.0 | Company Overview | 3 |
| 2.1 | TSC Overview | 3 |
| 2.2 | GE Company Overview | 4 |
| 3.0 | Network and System Overview | 4 |
| 3.1 | TSC Network and Systems | 4 |
| 3.2 | GE Network and Systems | 8 |
| 4.0 | Active Directory Overview | 10 |
| 4.1 | TSC Active Directory Infrastructure | 10 |
| 4.2 | GE Active Directory Infrastructure | 14 |
| 4.3 | TSC and GE interoperability | 15 |
| 5.0 | Group Policy Overview | 17 |
| 5.1 | Creating Workstation Security Policies | 17 |
| 5.2 | Testing Group Policy Settings | 24 |
| 5.3 | Test the System functionality | 34 |
| 5.4 | Apply the Group Policy | 35 |
| 5.5 | Evaluate the Group Policy | 36 |
| 6.0 | Auditing the Active Directory Infrastructure | 37 |
| 7.0 | Conclusion | 43 |

1.0 Introduction

The following document will outline the network and security design of the Sans Company and GIAC Enterprises (GE). This paper will discuss the merger of the Sans Company and GE. Both the Sans Company (TSC) and GE have their own web presence, Active Directory infrastructure and IT support staff. First, both companies' network and Active Directory infrastructures will be described. Next, an explanation of how TSC and GE created interoperability with their existing Active Directory and network infrastructure while maintaining their individual web presence for existing clients will be provided. In addition, the group policy applied to workstations will be reviewed. Also demonstrated will be the testing methods used by IT staff to ensure functionality while not interfering with existing applications. Finally, this document will describe the auditing procedures and practices, such as centralized logging and auditing tools, to ensure the group policies are functioning and adhering to company standard network and system security.

2.0 Company Overview

2.1 TSC Overview

TSC, founded in 1994, is a software company that develops one of the top selling inventory software packages on the market, STORIT. STORIT is a web-based application that runs on Internet Information Server (IIS) and uses a MS SQL database for its data storage. TSC develops smaller applications, such as customer service software, but STORIT is the company's most popular application. As sales grew, TSC opened offices in California, Canada, UK and Sweden. The corporate office, located in Philadelphia, PA, contains Human Resources, Finance and Accounting, Sales and Marketing, Customer Service, Research and Development and Information Technology departments. The west coast office, located in Silicon Valley, California, contains Human Resources, Sales and Marketing, Research and Development, Information Technology and a Customer Service department to answer calls for their west coast customers. The UK and Canada offices, located in London, England and Montreal, Canada, respectively, are small offices with approximately 150-200 employees handling Human Resources, Sales and Marketing, Research and Development, Information Technology and a Customer Service department to answer call for Canadian and UK clients. The office in Sweden is employs approximately 50 employees. The office contains Human Resource, Sales and Marketing, Information Technology and a Customer Service department to answer calls for the Sweden clients. To expand their market share in software, TSC acquired GE, a small company that develops ordering, fulfillment and billing software. Adding the ordering, fulfillment and billing package to its already established inventory software will prove to be very lucrative for TSC.

2.2 GE Company Overview

GE is a small software company with approximately 500 employees. GE develops a software package, EasyOrder, which assists its customers with product ordering, fulfillment and billing. Similar to STORIT, EasyOrder is a web-based application which runs on IIS and uses a MS SQL database for data storage. GE also offers online ordering and billing for companies that need to outsource this function. To facilitate this task, GE has a customer call center in Blackburg, Virginia employing 100 people who process orders for the current clients. GE's corporate office is located in Hampton, Virginia where all departments are housed including Human Resources, Finance, Accounting, Sales, Marketing, Information Technology and Research and Development.

3.0 Network and System Overview

3.1 TSC Network and Systems

The TSC network consists of six components: corporate local area network (LAN), the west coast office LAN, UK LAN, Canada LAN and Sweden LAN and the production Demilitarized Zone (DMZ) located in the corporate office. Each location has a Virtual Private Network (VPN) connection to each remote site via Routing Remote and Access Server (RRAS) except for the corporate and California offices. Those offices share a dedicated T1 connection between them.

When configuring the US offices, IT Management required the networks to be designed similarly to eliminate any unknown performance issues. The bulk of the company's sales is generated by the US offices; therefore, communication between the two sites needed to be secure, redundant and fast. The backbone of the US offices LAN has been designed with a Cisco switch and several Cisco 48 port switches. All servers connect directly to the core switch. Workstations and printers connect to the 48 port switches, which have a gigabit uplink to the core switch. The perimeter routers at both locations are Cisco routers. The perimeter router in the corporate office has been configured for load-sharing and fault tolerance accomplished by Border Gateway Protocol (BGP) using two local Internet Service Providers (ISP). Fault tolerance was a requirement to ensure web server access to clients and potential clients was not interrupted. The connection between the east and west coast office was completed with a dedicated T1 and the inclusion of an ISDN backup in case of failure. The routers service both local and the wan routes. For their firewall, they installed a Cisco PIX with six interfaces. The Service DMZ, where all web servers and backend SQL databases reside, hangs off the third interface of the firewall and all machines connect to multiple Cisco switches for redundancy purposes. For remote connectivity, both locations have installed several RRAS servers configured for VPN connectivity for remote offices. They have also installed and configured RRAS servers with modems for traveling salespeople. The public

interface of the RRAS connects to the fourth interface of the firewall and the private interface is connected to the DMZ hub. The RRAS server with modems is connected to the DMZ switch. As a result, all access and data can be filtered by the firewall and logged to the Syslog server. The sixth interface of the firewall is currently disabled but may be used for future development projects.

The Canada, Sweden and UK network are designed similarly; they have several Cisco 24 port switches, Cisco routers and Cisco PIX firewall. All servers, workstations and printers connect to the switches. Their firewalls are configured with only three interfaces with the option to expand later. For VPN connectivity to remote sites and remote access, they use Microsoft RRAS server.

TSC uses a private IP address space, 10.10.40.0/23 (PA - Corp), 10.10.50.x/23 (CA), 10.10.60.0/24 (Canada), 10.10.70.0/24 (UK Office) and 10.10.80.0/24 (Sweden Office), for internal devices and uses NAT to translate to a public IP address space. All Cisco devices authenticate against a Microsoft IAS RADUIS and standard security requirements for all Cisco devices, such as patches and Access Control Lists (ACLs), are assumed.

As for system configurations, TCS offices use Compaq Proliants for servers and Dell desktops and laptops for their workstations. All servers run Windows 2000 and all client workstations run Windows 2000 or XP. Microsoft's recommends that there be at least one domain controller at site and at least one domain control configured as a global catalog (24). Therefore, all locations are configured with two domain controllers configured as Global Catalogs and installed with Domain Name Servers (DNS) configured as Active Directory integrated zones and service all DNS requests for clients. Site replication links for all domain controllers are configured to use the IP (RPC) transport. A redundant inter-site site link, SMTP transport, was created to replicate between domains controllers in case the IP transport is not available. The SMTP transport will only work with domain controllers in different domain, so an SMTP transport is not used for domain controllers in the same domain. Keeping in mind that replication traffic may not be encrypted; all traffic over the IP transport travels over an IPsec (Internet Protocol Security) session, which travels through the VPN connection between each site (ref 10 and 12). The SMTP site link uses s/mime, which is already encrypted so only the RPC site link travels over the IPsec tunnel (ref 12). TSC administrators used information outlined in Microsoft articles Q224196 (ref 26) and Q179442 (ref 25) to assist them with this task. TSC's Active Directories infrastructure will be discussed in more detail later in this document. TSC uses Exchange 2000 for their messaging system at all locations. Each server has been configured as a local bridgehead that delivers local mail via the VPN connection and all other mail through their public connection. TSC has a Public Key Infrastructure (PKI) for encryption of web sites, email, file and the SMTP replication transport. In accordance NSA and SANS recommended specifications, the root server has been configured as a stand-alone root and remains currently offline (ref 4 and 12). The production

servers are configured as enterprise subordinate Certificate Authority (CA). A similar design was configured for the DMZ; however, the subordinate CA servers are stand-alone servers. Each remote site supports at least two file servers. The corporate and west coast offices have at least four file servers. To make it easier for users to access file servers, TSC has incorporated Distributed File System (DFS) into their network. They chose to use a domain DFS root because shares are automatically published to Active Directories and they could take advantages of the replication feature (13). Each site maintains at least two SQL servers that store customer data, such as orders and billing information. Customer service uses the company's problem tracking application to record problems. The issue is then routed to R&D, where they try to recreate the problem. The corporate and west coast offices incorporated three SQL servers and IIS Web servers used to recreate customer issues and further develop new products. All problem resolutions are published to the intranet server which all customer service employees use as a problem solving tool prior to entering a new ticket. The intranet servers (IIS 5.0), where employees at all sites can retrieve important company documents and search the problem knowledgebase, are located in the corporate office. All locations have two DHCP (Dynamic Host Configuration Protocol) servers configured in the 80/20 model to ensure reliability and redundancy (7). Microsoft describes the 80/20 model as one server configured with at least 80% of the IP addresses and the second configured with the remaining 20%. All locations have two print servers for load balancing and redundancy. The corporate and west coast office direct all web traffic through Internet Security and Acceleration (ISA) proxy servers. This configuration was implemented to increase security due to the size of both offices.

The Production DMZ segment, located at the corporate office, contains the servers that are core to the external business. In the DMZ, there are four production web servers running IIS 5.0, two external DNS servers to resolve for the internal DNS Servers, two external SMTP servers to deliver mail to the internal servers, three production backend database servers running Microsoft SQL 2000, ISA proxy configured to reverse proxy Outlook web access and external IIS servers and two RRAS servers for modem users and to establish VPN connections to the remote locations. The DMZ SQL servers have been configured to replicate online order information with the Internal SQL servers. The firewall was configured to only allow SQL replication data from the DMZ server to the internal SQL server. In addition, IPsec was configured to encrypt all replication data and to ensure that only the external SQL servers can initiate a connection to the internal SQL servers. The private interfaces of the RRAS servers have been placed in the DMZ to service traveling users with high-speed connections and modem users.

(See illustration 1.0 and 2.0 for detailed design layouts for all locations.)

Illustration 1.0: Corporate and West Coast Network Design.

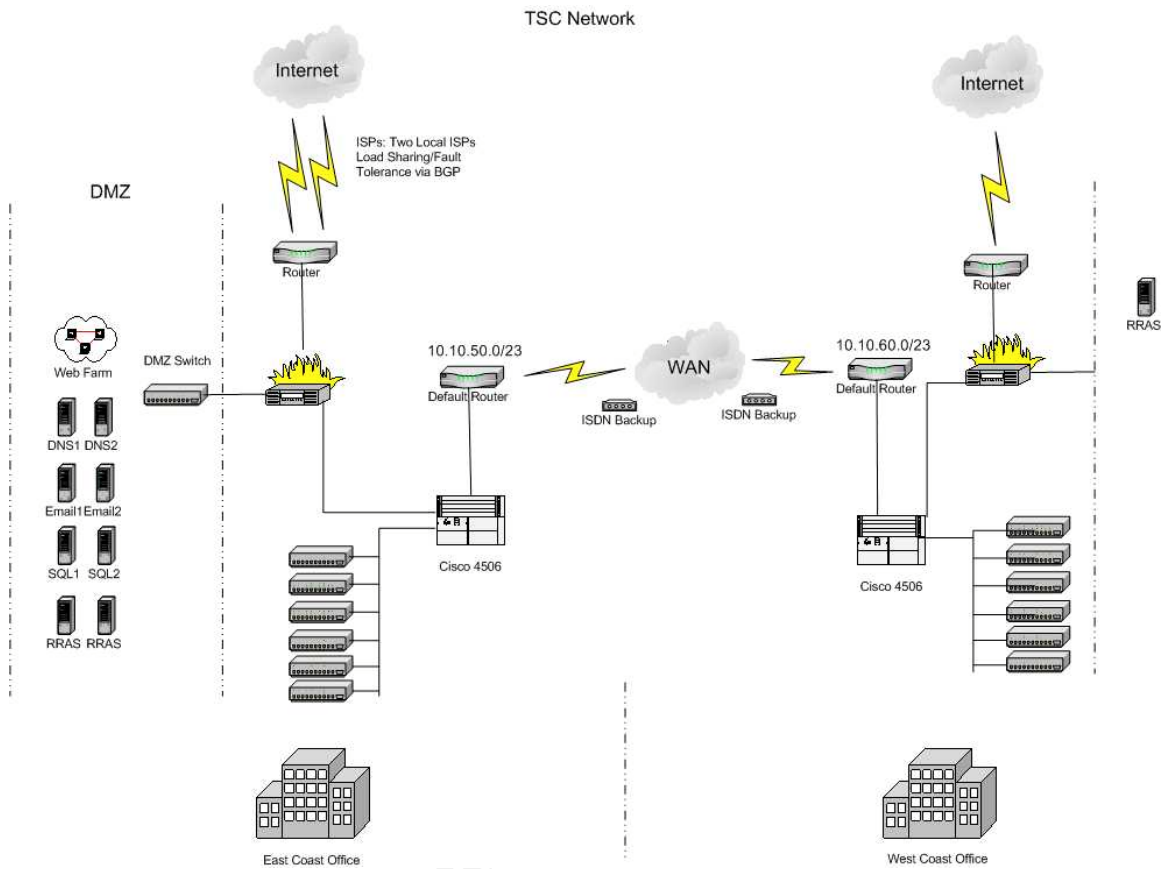
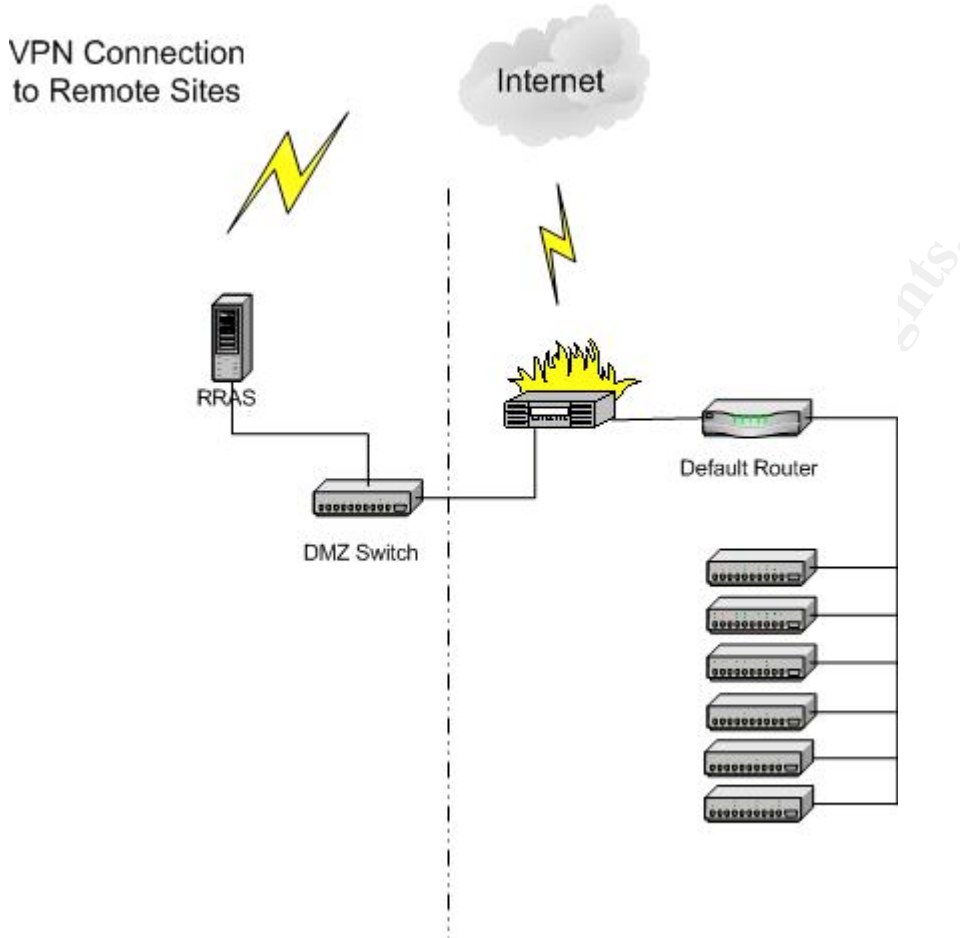


Illustration 2.0: Remote Offices Network Design.

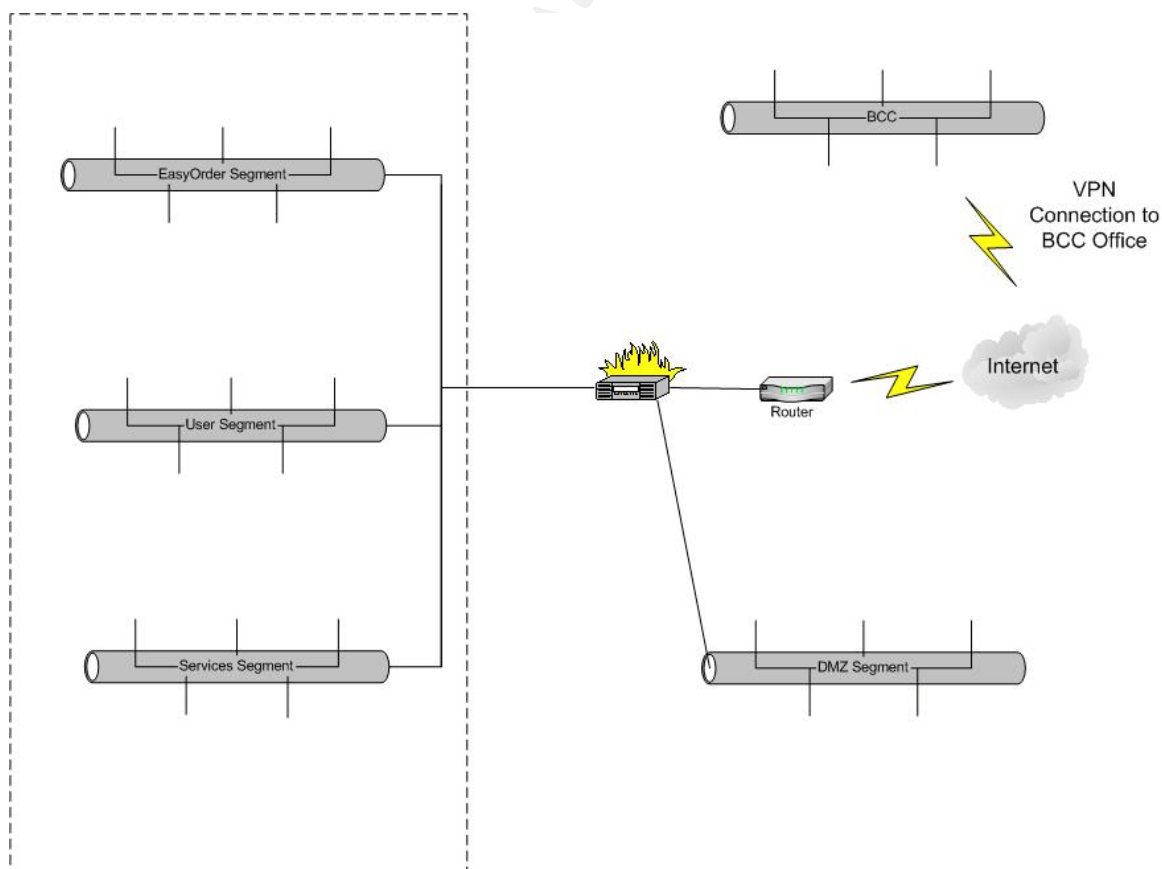


3.2 GE Network and Systems

The GE network consists of three components: the DMZ, the local area network (LAN) and Call Center LAN. GE's configured their LAN into three separate segments: the EasyOrder Segment, the User segment and the Services segment (1). The EasyOrder segment contains the hosts that maintain the company's outsourcing division. IIS servers and backend database servers that support clients' websites reside in this segment. Due to the sensitivity of customer data, only BCC staff and operational employees have access to this segment and access controls are implemented to regulate protocols permitted to access servers. The user segment contains all user workstations. The DHCP server, print server and second domain controller are located in this segment. The service segment provides core network functionality to the company. Access controls are in place to ensure only allowed network traffic to flow into this segment. The internal email server, the root domain controller, intranet IIS servers, RRAS servers that initiate the VPN connection to the BCC location, files

servers and application servers exist in this segment of the network. The network is configured in this manner to increase security and performance for each segment. GE also uses a private IP address space, 10.x.y.z, and uses NAT to translate to a public IP address space. The network backbone consists of a Cisco gigabit switch and Cisco 10/100 switches. All servers connect directly the gigabit switch and clients connect to the 10/100 switches. GE uses a Cisco router for the perimeter router and a Cisco PIX for their firewall. Similar to TSC, GE has a redundant internet connection to ensure internet connectivity at all times. The DMZ segment hangs off the third interface of the PIX firewall and contains the company websites and customer websites. In addition, external mail servers, RRAS servers and DNS servers exist in the DMZ. GE uses Windows 2000 Routing and Remote Access (RRAS) for VPN connectivity between their Hampton office and BCC office and remote access for traveling employees. The network at the Blackburg Call Center is very small and consists of several Cisco 10/100 mbps switches as the backbone. Connectivity to the Hampton office is configured through a RRAS machine and all internet access is directed through the GE corporate network. All workstations are Windows 2000 or XP. All Cisco devices authenticate against a Microsoft ISA RADUIS. Standard security requirements for all Cisco devices, such as patches and ACLs, are assumed.

Illustration 3.0: GE Network Design.



4.0 Active Directory Overview

4.1 TSC Active Directory Infrastructure

A single domain infrastructure is recommended for most organizations; however, TSC has three international locations where local laws on privacy and encryption differ from that of the US (ref 2 and 15). Therefore, to maintain compliance with their local laws, TSC implemented a multi-domain Active Directory infrastructure. TSC chose to run their Active Directory infrastructure in native mode for the following reasons:

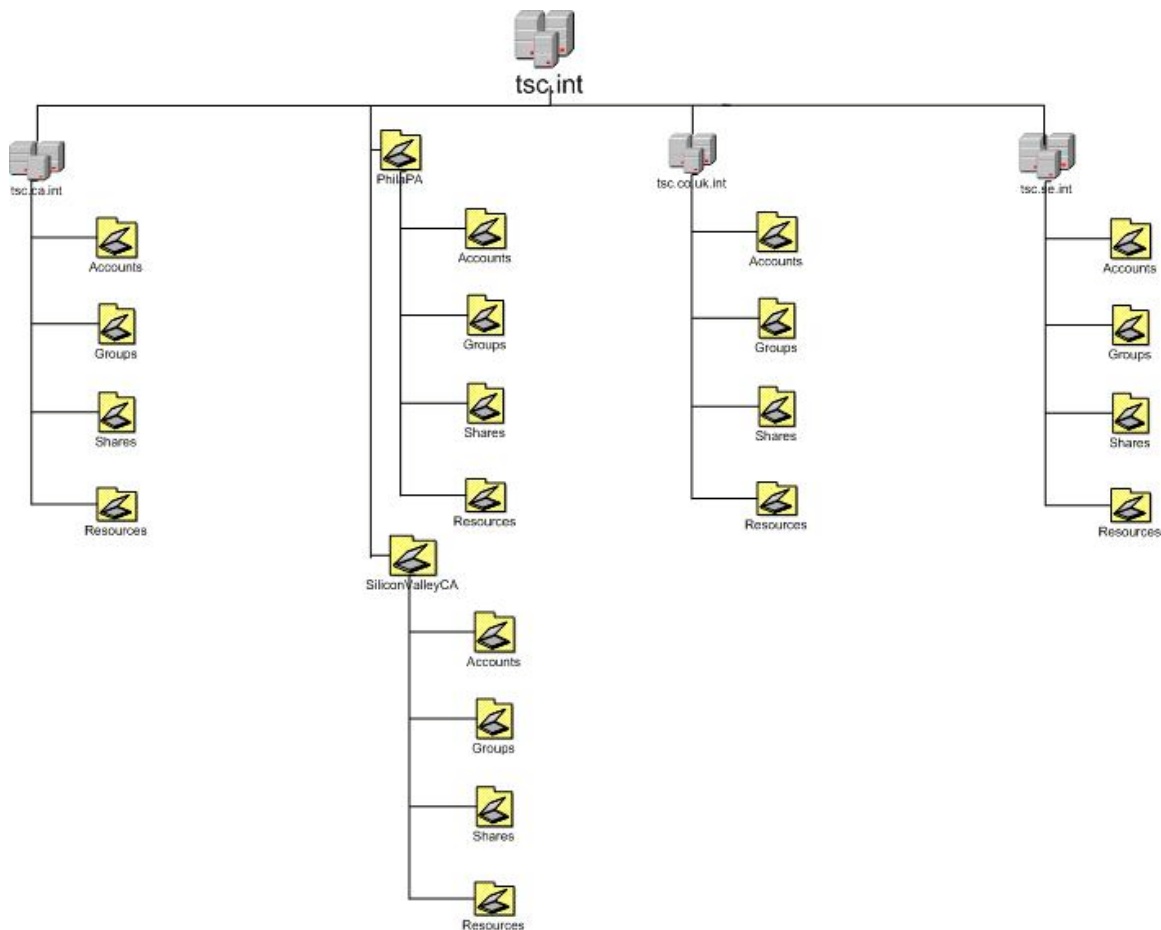
- They need to support backward compatibility with an NT 4 domain,
- They do not want be haunted with security weaknesses that are inherent with NT4 domains
- They wanted to take advantage of security features only supported in native mode (ref 14).

TSC's public domain spaces are tsc.com, tsc.ca, tsc.uk.co and tsc.se. The private domain spaces are tsc.int, tsc.ca.int, tsc.uk.int and tsc.se.int where int indicates internal. Microsoft recommends differentiating your internal from your external devices to secure internal devices from outside resources (ref 2 and 10). In accordance with this recommendation, they chose to use a private namespace instead of their public namespace.

Each domain has four top-level organizational units (OU): accounts, groups, shares and resources. Since the corporate and the California office shared the same domain, two OUs, PhilaPA and SiliconVaCA, were designed to contain the accounts, groups, shares and resource child OUs. See illustration 4.0 for a detailed look at the TSC active directory structure.

Illustration 4.0: Overview of TSC AD design.

© SANS Institute



TSC designed their OU structure so they did not exceed three levels deep as recommended by Microsoft (ref 10).

- accounts OU:
 - sensitive
 - untrusted
 - it_dept
 - rd_dept (does not exist in the Sweden domain.)
 - hr_dept
 - cs_dept
 - sales_dept
 - market_dept.
 - finacct_dept (only exists in the PhilaPA OU)
- groups OU:
 - security OU
 - distribution OU
- shares OU
 - DFS shares
- resources OU
 - file_servers OU

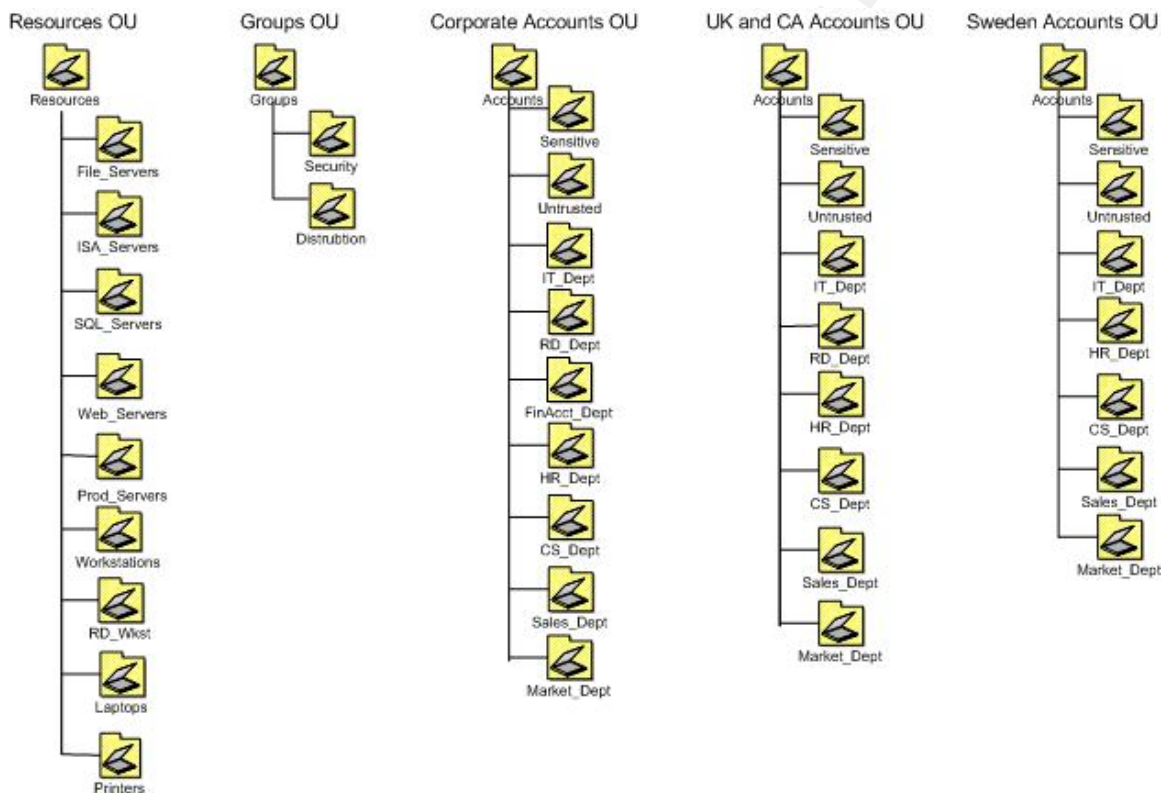
- isa_servers OU
- sql_servers OU
- web_servers OU
- prod_servers OU
- workstations OU
- laptops OU
- rd_workstations OU
- printers OU

See below for a more detailed description of OUs and child OUs.

| OU Name | Child OU | Description | GPO |
|-----------|--------------|--|-----------------|
| Accounts | | | Global_Acct_GPO |
| | Sensitive | OU where sensitive users such as domain admins or CEO accounts are placed. | Sensitive |
| | Untrusted | OU where "untrusted" users such as consultants or accounts that are being monitored. | Untrusted |
| | IT_Dept | OU where IT users are placed. | IT_GPO |
| | RD_Dept | OU where R&D users are placed. | |
| | FinAcct_Dept | OU where Finance and Accounting users are placed. | |
| | HR_Dept | OU where Human Resource users are placed. | |
| | CS_Dept | OU where Customer Service users are placed. | CS_GPO |
| | Sales_Dept | OU where Sales users are placed. | |
| | Market_Dept | OU where Marketing users are placed. | |
| Groups | | | |
| | Distribution | All Distribution Lists are stored in this OU | |
| | Security | All Security Groups are stored in this OU | |
| | | | |
| Shares | | File shares published in this Domain | |
| Resources | | | |
| | File_Servers | All File servers are placed in this OU. | FS_GPO |
| | ISA_Servers | All ISA servers are placed in this OU | ISA_GPO |
| | SQL_Servers | All SQL servers are placed in this OU | SQL_GPO |
| | Web_Servers | All Web servers are placed in this | IIS_GPO |

| | | | |
|--|--------------|---|----------|
| | | OU | |
| | Prod_Servers | All misc. production servers are placed in this OU. | Prod_GPO |
| | Workstations | All workstations are placed in this OU. | WK_GPO |
| | Laptops | All laptops are placed in this OU. | LP_GPO |
| | RD_Wkst | Special OU for R&D Workstations | RD_GPO |
| | Printers | All printers are published to this OU. | |

Illustration 5.0: Detailed Overview of TSC OU Layout.

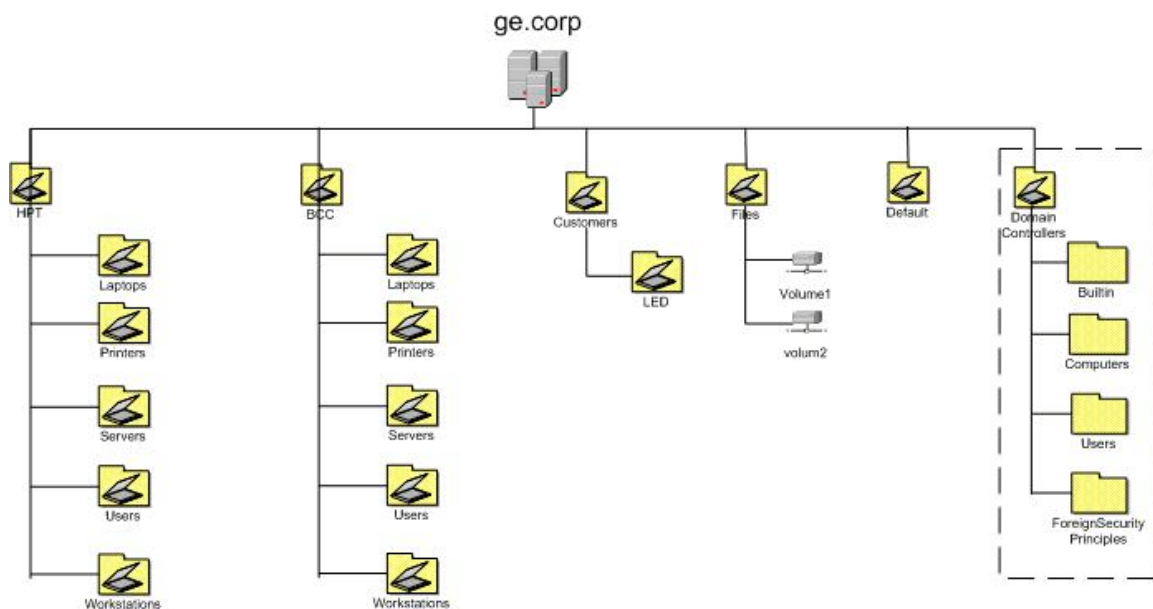


Each location has its own IT support staff; however, IT Management is located in the corporate office. Along with the domain admins and enterprise admins groups, special admins groups were created for each location: Canada_Admins, Sweden_Admins, UK_Admins, Corp_Admins and CA_Admins. The local admins are members of their local domain admins group and have delegated permissions to reset and unlock user accounts on the Accounts OU in other domains. This is valuable for when any TSC employee travels to remote offices. The Corp_Admins group is the only member of enterprise admins group, which means they have full control of all domains.

4.2 GE Active Directory Infrastructure

GE has implemented a single domain Active Directory Infrastructure (1). Their IT management and support staffs are centrally located in the Hampton office. Only a small support staff exists in the BCC office. GE's public namespace is giacenterprises.com and internal namespace is ge.corp. GE uses this method for security and ease of differentiating between internal devices and external devices. Each location has two DC's installed with DNS configured as Active Directory-Integrated zones. This was done for redundancy and reduced maintenance. For the same reasons as TSC, GE is running Active Directories in native mode. The AD infrastructure is broken into two main site organization units (OU): HPT and BCC. Under these site OUs, children OUs exist for laptops, printers, servers, users and workstations. On the BCC OU, administrative capabilities such as creating users and resetting passwords were delegated to the BCC IT staff. GE has also created a 'clients' and 'files' OU. By creating an OU for each new client, it makes it easier to delegate control to existing IT staff and centralize administration. In addition, by creating new OUs for new clients, the existing infrastructure will not be disrupted. By creating an OU for disk volumes, GE anticipated performance improvement on directory queries for file shares. For addition security and management, Administrative groups are broken into four admin groups, Domain, workstation, server and bcc admins. Domain admins have full control of all directory objects. Workstation admins have local administrative rights of desktops and laptops, permissions to add workstations to the domain and rights to change passwords for the users OU. Server admins can perform most domain/server administrative task but cannot modify the schema or group policies. BCC admins are permitted to add users and workstations to the BCC OU, unlock accounts and troubleshoot and/or administrator file, print and DHCP functions. Please see Illustration 6.0 for an overview of the GE Active directory infrastructure. Both TSC and GE have an Active Directory forest in their DMZ but are beyond scope of this paper and will not be discussed.

Illustration 6.0: GE AD Design.



4.3 TSC and GE interoperability

Migrating to one forest is not an option because both companies have an established network and active directory infrastructure. In addition, both companies have a web presence and any downtime would incur major company and client losses. Therefore, the decision to establish two-way trusts between domains has been made to create company interoperability. In addition, some modifications to IT staff will be made to consolidate IT overhead.

Let's review the TSC and GE IT infrastructure: TSC has an IT staff at all four locations but IT management is located in the corporate office. GE has IT management and staff at their corporate locations and a small IT staff at the BCC locations. In order for IT Management to work together more efficiently, the GE management staff will be relocated to TSC corporate office in Pennsylvania while keeping the existing non-management IT support staff at the HPT and BCC Location. Each location will have senior support staff that follows direction from the corporate office and modifies the active directories infrastructure accordingly.

The goal is to create interoperability without causing any downtime for either company and maintaining the web infrastructure without interruption for existing clients. In order to facilitate this task, a dedicated T1 connection was installed to connect GE and TSC corporate and west coast offices. Due to the limited access needed to the TSC foreign sites, a VPN connection, configured to only activate upon request, was established. Two-way trusts between the ge.corp and tsc.int domains were created. A standard DNS zone for each respective domain was created in the others DNS server. Administrators followed the

procedures outlined in Q Article 280061 to export and import the records in DNS to the new zone created in each domain.

Illustration 7.0: Snapshot of the trust configuration between domains.

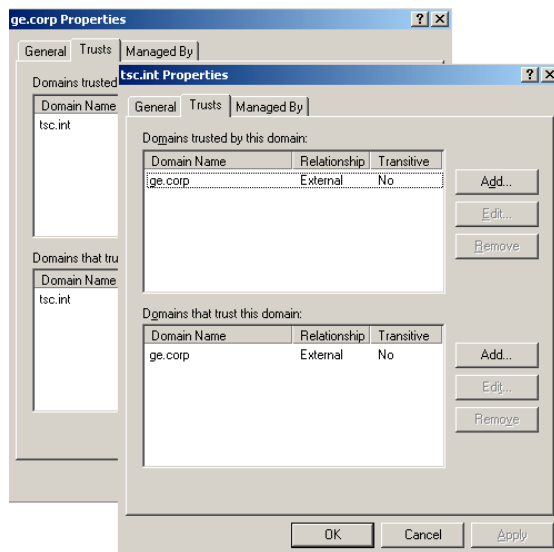
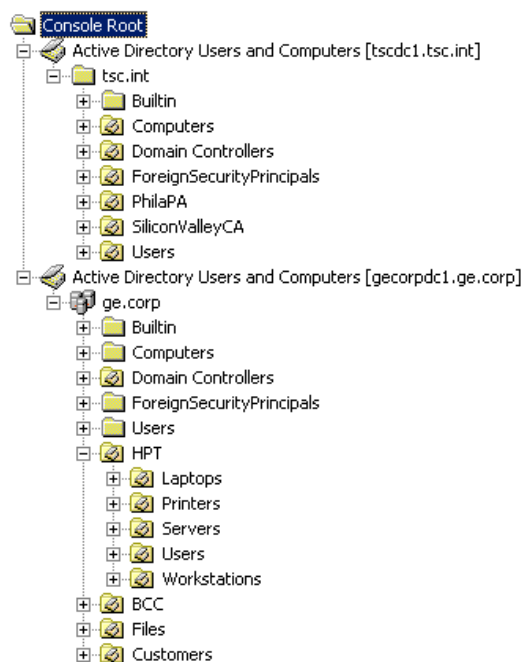


Illustration 8.0: Snapshot of the both domains in one mmc snap-in.



Two global groups, bcc_admins and hpt_admins, were created in each TSC domain. Four global groups, corp_admins, sweden_admins, canada_admins and uk_admins, were created in the ge.corp domain. HPT and BCC admins remained domain admins for their domain but only had delegated permissions to change passwords and reset accounts in TSC domains. The other admins in the

TSC domain had the same delegated permissions in the ge.corp domain as they have established currently in the TSC domain. Corporate admins will remain the only group that is allowed to modify the group policies. Any changes to the standard policy already in place must be approved by IT management prior to modification. More information about group policy standards and approval processes are discussed in the next section.

The web infrastructure at both companies will not be moved or changed so there will be no interruption during the transition period. TSC Corp admins will maintain the TSC web infrastructure while GE Corp admins will maintain the GE web infrastructure. There are no plans in the future to create a trust between the DMZ domains.

5.0 Group Policy Overview

To maintain system security efficiently and most affectively, TSC and GE deploy group policies. Group policies are defined for the function the machine performs, such as domain controller, email (exchange), file, print, DHCP, ISA, IIS, SQL servers or user workstation. The scope of this paper is about workstation security so only the workstation group policy will be discussed. The policy creation process consists of several phases. In the following sections, I will illustrate the entire group policy process.

5.1 Creating Workstation Security Policies

Administrators review policy templates created by National Security Agency (NSA), Microsoft and the Center for Internet Security (CISecurity) (ref 4, 5, and 6). Each template is examined with the Security Configuration and Analysis MMC snap-in and settings that are consistent with their security design are recorded. The security and configuration analysis tool provides a detailed overview of the changes the new policy will have on the existing local policy. Most of the settings in the group policy baseline reflect NSA's template because it was most consistent with their security standards. A few changes were made or added and are outlined below:

- An IPSec policy was assigned to encryption terminal server, SQL and email traffic.
- Netmeeting desktop sharing was disabled according to company policy no one is to remote control their machine from home without approval from IS.
- Internet sharing was disabled on TSC/GE workstations.
- TSC and GE use Software Update Server (SUS) to keep workstations up-to-date and implemented via group policy.
- Administrators disabled Automatic Install of Internet Explorer components because rogue ware could be downloaded by unsuspected users.

- Internet Explorer updates are delivered via SUS so administrators disable the periodic checks for Internet Explorer software.
- Administrators avoided giving local administrative rights to typical users. They do make an exception for R&D users due to the nature of their job.

See below for complete outline of the computer group policy baseline.

Computer Configuration Group Policy (setting not altered were omitted)

| Computer Configuration | | | | | | |
|------------------------|--|--|--|--|----------------------|--|
| | | | Software Settings | | | |
| | | | Windows Settings | | | |
| | | | Scripts (Startup/Shutdown) | | | |
| | | | Security Settings | | | |
| | | | Account Policies | | | |
| | | | Password Policy | | | |
| | | | Enforce password history | | 24 | |
| | | | Maximum password age | | 90 | |
| | | | Minimum password age | | 1 | |
| | | | Minimum password length | | 24 | |
| | | | Passwords must meet complexity requirements | | enabled | |
| | | | Store password using reversible encryption for all users in the domain | | disabled | |
| | | | Account Lockout Policy | | | |
| | | | Account lockout duration | | 15 | |
| | | | Account lockout threshold | | 3 | |
| | | | Reset account lockout counter after | | 15 | |
| | | | Local Policies | | | |
| | | | Audit Policy | | | |
| | | | Audit account logon events | | success, failure | |
| | | | Audit account management | | success, failure | |
| | | | Audit directory service access | | not audited | |
| | | | Audit logon events | | success, failure | |
| | | | Audit object access | | failure | |
| | | | Audit policy change | | success, failure | |
| | | | Audit privilege use | | failure | |
| | | | Audit process tracking | | not audited | |
| | | | Audit system events | | success, failure | |
| | | | User Rights Assignment | | | |
| | | | Access this computer from the network | | administrator, users | |
| | | | Back up files and directories | | administrator | |
| | | | Bypass traverse checking | | users | |
| | | | Change the system time | | administrator | |
| | | | Create a pagefile | | administrator | |

| | | | | | | | |
|--|--|--|--|--|--|---|---|
| | | | | | | Deny access to this computer from the network | guest |
| | | | | | | Deny logon locally | guest |
| | | | | | | Force shutdown from a remote system | administrator |
| | | | | | | Increase quotas | administrators |
| | | | | | | Increase scheduling priority | administrator |
| | | | | | | Load and unload device drivers | administrator |
| | | | | | | Manage auditing and security log | administrator |
| | | | | | | Modify firmware environment values | administrator |
| | | | | | | Profile single process | administrator |
| | | | | | | Profile system performance | administrator |
| | | | | | | Restore files and directories | administrator |
| | | | | | | Shut down the system | administrator |
| | | | | | | Take ownership of files or other objects | administrator |
| | | | | | | Security Options | |
| | | | | | | Additional restrictions for anonymous connections | no access without explicit anonymous permission |
| | | | | | | Allow system to be shut down without having to log on | disabled |
| | | | | | | Allowed to eject removable NTFS media | administrator |
| | | | | | | Amount of idle time required before disconnecting a session | 30 minutes |
| | | | | | | Audit the access of global system objects | enabled |
| | | | | | | Audit use of Backup and Restore privilege | enabled |
| | | | | | | Automatically log off users when logon time expires | enabled |
| | | | | | | Automatically log off users when logon time expires (local) | enabled |
| | | | | | | Clear virtual memory pagefile when system shuts down | enabled |
| | | | | | | Digitally sign client communication (always) | disabled |
| | | | | | | Digitally sign client communication (when possible) | enabled |
| | | | | | | Digitally sign server communication (always) | disabled |
| | | | | | | Digitally sign server communication (when possible) | enabled |
| | | | | | | Disable CTRL+ALT+DEL requirement for logon | disabled |
| | | | | | | Do not display last user name | enabled |

| | | | | | | | |
|--|--|--|--|--|--|---|---|
| | | | | | | in logon screen | |
| | | | | | | LAN Manager Authentication Level | send NTLMv2 response only\refuse LM & NTLM |
| | | | | | | Message text for users attempting to log on | This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials. |
| | | | | | | Message title for users attempting to log on | --- WARNING --- |
| | | | | | | Number of previous logons to cache (in case domain controller is not available) | 0 |
| | | | | | | Prevent system maintenance of computer account password | disabled |
| | | | | | | Prevent users from installing printer drivers | enabled |
| | | | | | | Prompt user to change password before expiration | 14 days |
| | | | | | | Recovery Console: Allow automatic administrative logon | disabled |
| | | | | | | Recovery Console: Allow floppy copy and access to all drives and all folders | disabled |
| | | | | | | Rename administrator account | tslocaladm |
| | | | | | | Rename guest account | tslocalgst |
| | | | | | | Restrict CD-ROM access to locally logged-on user only | enabled |
| | | | | | | Restrict floppy access to locally logged-on user only | enabled |
| | | | | | | Secure channel: Digitally encrypt or sign secure channel data (always) | disabled |
| | | | | | | Secure channel: Digitally encrypt secure channel data (when possible) | enabled |
| | | | | | | Secure channel: Digitally sign secure channel data (when possible) | enabled |
| | | | | | | Secure channel: Require strong (Windows 2000 or later) session key | disabled |

| | | | | | | | |
|--|--|--|--|--|--|---|---|
| | | | | | | Secure system partition (for RISC platforms only) | disabled |
| | | | | | | Send unencrypted password to connect to third-party SMB servers | disabled |
| | | | | | | Shut down system immediately if unable to log security audits | enabled |
| | | | | | | Smart card removal behavior | lock workstation |
| | | | | | | Strengthen default permissions of global system objects (e.g. Symbolic links) | enabled |
| | | | | | | Unsigned driver installation behavior | warn but allow installation |
| | | | | | | Unsigned non-driver installation behavior | warn but allow installation |
| | | | | | | Event Log | |
| | | | | | | Settings for Event Logs | |
| | | | | | | Maximum application log size | 4194240 KB |
| | | | | | | Maximum security log size | 4194240 KB |
| | | | | | | Maximum system log size | 4194240 KB |
| | | | | | | Restrict guest access to application log | enabled |
| | | | | | | Restrict guest access to security log | enabled |
| | | | | | | Restrict guest access to system log | enabled |
| | | | | | | Retain application log | 7 Days |
| | | | | | | Retain security log | 7 Days |
| | | | | | | Retain system log | 7 Days |
| | | | | | | Retention method for application log | manually |
| | | | | | | Retention method for security log | manually |
| | | | | | | Retention method for system log | manually |
| | | | | | | Restricted Groups | |
| | | | | | | System Services (Disabled) | <ul style="list-style-type: none"> • alert • computer browser • telnet • routing and remote access • remote registry • messenger • internet connection sharing • Clipbook • FAX • SNMP Service • SNMP Trap Service |
| | | | | | | Registry | Administrators used settings outline in the CISecurity template for registry settings |
| | | | | | | File System | |
| | | | | | | Public Key Policies | |

| | | | | | | |
|--|--|--|--|--|--|--|
| | | | | | Encrypted Data Recovery Agents | |
| | | | | | Automatic Certificate Request Settings | |
| | | | | | Trusted Root Certification Authorities | |
| | | | | | Enterprise Trust | |
| | | | | | IP Security Policies on Active Directory | |
| | | | | | Wkst-IPSec-Policy | Policy Assigned |
| | | | | | Administrative Templates | |
| | | | | | Windows Components | |
| | | | | | NetMeeting | |
| | | | | | Disable remote Desktop Sharing | Enabled |
| | | | | | Internet Explorer | |
| | | | | | Disable Automatic Install of Internet Explorer components | Enabled |
| | | | | | Disable Periodic Check for Internet Explorer software updates | Enabled |
| | | | | | Task Scheduler | |
| | | | | | Windows Installer | |
| | | | | | Windows Update | |
| | | | | | Configure Automatic Updates | Enabled: Auto download and schedule the install everyday at 12:00 PM |
| | | | | | Specify intranet Microsoft update server location | Enabled: http://susupdate |
| | | | | | Reschedule Automatic Updates schedule installations | Enabled: Wait after system startup(minutes):5 |
| | | | | | No auto-restart for schedule Automatic Updates Installations | Enabled |
| | | | | | System | |
| | | | | | Logon | |
| | | | | | Disk Quotas | |
| | | | | | DNS Client | |
| | | | | | Group Policy | |
| | | | | | Apply Group Policy for computers asynchronously during startup | enabled |
| | | | | | Apply Group Policy for users asynchronously during logon | enabled |
| | | | | | Windows File Protection | |
| | | | | | Network | |
| | | | | | Offline files | |
| | | | | | Network & Dial-up Connections | |
| | | | | | Allow configuration of connection sharing | disabled |
| | | | | | Printers | |

In addition to computer security, TSC and GE make use of user group policies to control machines at the user level. Aspects of the user group policy are outlined below.

User Configuration Group Policy (setting not altered were omitted)

| User Configuration | | | | | |
|--------------------|--------------------------------------|--|------------------------------------|--|---|
| | Software Settings | | | | |
| | Windows Settings | | | | |
| | Internet Explorer Maintenance | | | | |
| | | Browser User Interface | | | |
| | | Connection | | | |
| | | | Proxy Settings | | proxy.tsc.int:8080 |
| | | URLs | | | |
| | | | Favorites and Links | | www.tsc.int |
| | | Security | | | |
| | | | Security Zones and Content Ratings | | Default settings for security zones are applied |
| | | Programs | | | |
| | Scripts (Logon/Logoff) | | | | |
| | Security Settings | | | | |
| | | Public Key Policies | | | |
| | | Enterprise Trust | | | |
| | Remote Installation Services | | | | |
| | Folder Redirection | | | | |
| | | Application Data | | | |
| | | Desktop | | | |
| | | My Documents | | | Redirect to Users home directory |
| | | My Pictures | | | |
| | | Start Menu | | | |
| | Administrative Templates | | | | |
| | Windows Components | | | | |
| | | NetMeeting | | | |
| | | Application Sharing | | | |
| | | | Disable application Sharing | | disabled |
| | | Audio & Video | | | |
| | | Options Page | | | |
| | Internet Explorer | | | | |
| | | Internet Control Panel | | | |
| | | Offline Pages | | | |
| | | Browser menus | | | |
| | | Toolbars | | | |
| | | Persistence Behavior | | | |
| | | Administrator Approved Controls | | | |
| | Windows Explorer | | | | |
| | | Common Open File Dialog | | | |
| | Microsoft Management Console | | | | |

| | | | | | | |
|--|--|--|--|--|---|-------------|
| | | | | | Restricted/Permitted snap-ins | |
| | | | | | Active Directory Users and Computers | disabled |
| | | | | | Active Directory Domains and Trusts | disabled |
| | | | | | Active Directory Sites and Services | disabled |
| | | | | | IP Security | disabled |
| | | | | | Local Users and Groups | disabled |
| | | | | | Extension snap-ins | |
| | | | | | Group Policy | |
| | | | | | Task Scheduler | |
| | | | | | Windows Installer | |
| | | | | | Start Menu & Taskbar | |
| | | | | | Desktop | |
| | | | | | Prohibit user from changing My Documents path | enabled |
| | | | | | Active Desktop | |
| | | | | | Active Directory | |
| | | | | | Control Panel | |
| | | | | | Add/Remove Programs | |
| | | | | | Disable Add/Remove Programs | disabled |
| | | | | | Display | |
| | | | | | Activate Screen saver | Enabled |
| | | | | | Password protect the screen saver | Enabled |
| | | | | | Screen Saver timeout | 420 Seconds |
| | | | | | Printers | |
| | | | | | Regional Options | |
| | | | | | Network | |
| | | | | | Offline Files | |
| | | | | | Network and Dial-up Connections | |
| | | | | | System | |
| | | | | | Logon/Logoff | |
| | | | | | Group Policy | |

5.2 Testing Group Policy Settings

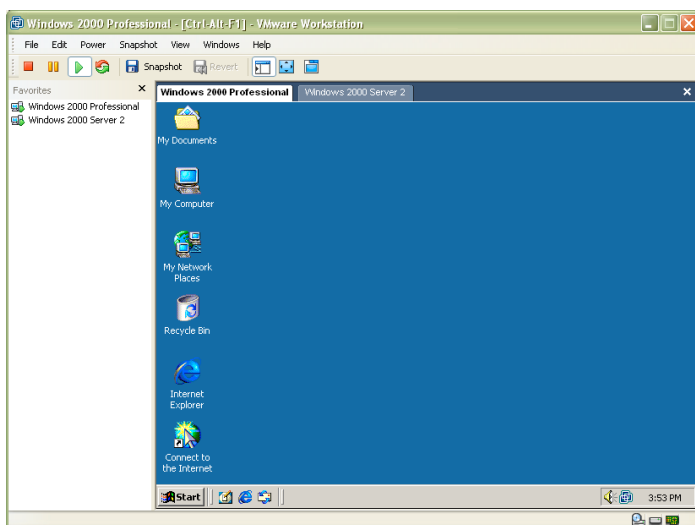
To effectively test a group policy, administrators created a test forest that closely resembled their production environment. By using Active Administrator, they were able to duplicate their infrastructure by copying OU containers and group policies. Test users were created in each department OU, such as RD and Customer Service. In addition, several test machines were installed in the workstation and laptop OU. This configuration allows administrators to efficiently test how a group policy will affect a user or computer in the production

environment. To confirm that the expected security parameters of the group policy are applied, administrator log into a test machine with a designated test account and perform a controlled test. The tools used for their testing were Active Administrator (AA), the Resultant Set of Policy (RSoP) snap-in, gpresults.exe and the Security Configuration and Analysis Tool Snap-in.

- VMware

VMware is licensed software that allows a user to install multiple guest operating systems on one machine. This eliminates the additional resources needed for testing. VMware also reduces installation time for new operating systems because all changes made are reset leaving a fresh operating system ready for further testing (ref 30).

Illustration 9.0: Screenshot of a VMware workstation.



- Active Administrator

Active Administrator is licensed software that is a very powerful tool for an Active Directory Administrator. It assists with Active Directory security and group policy management (ref 28).

- Resultant Set of Policy (RSoP) (MMC Snap-in)

RSoP provides a detailed analysis of the effectiveness of a GPO deployment. By analyzing the test users, administrators are aware of what settings are applied.

- GPResults.exe

The GPRResults.exe tool that is included in the resource kit was used to confirm that all the desired settings were applied.

- Tcpcdump

To ensure that the IPSec settings are working properly, administrators use tcpcdump while connecting to a terminal server to confirm that the traffic between the server and client was using ipsec (ref 15).

- Netdiag

Netdiag is a network utility tool that helps diagnosis network connectivity issues. The tool is downloadable from Microsoft website (ref 29).

- Event viewer logs

MMC Snap-in that allows users to review the application, security and system event logs.

Administrators begin testing by analyzing RSoP results using Active Administrator. By selecting a user or computer and clicking on "View RSoP", administrators are able to view which group policy will be applied to the object. If the policy is applied correctly, the system testing will begin.

Illustration 10.0: Active Administrator results displaying GPO results for rdtestacct.

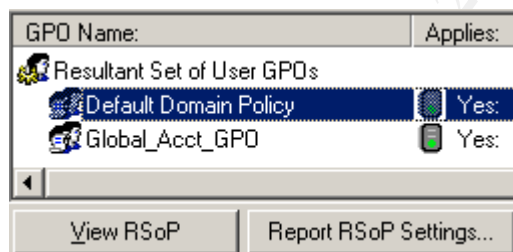
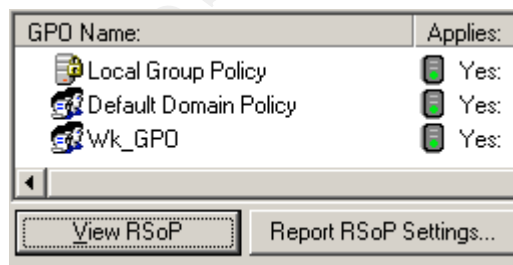


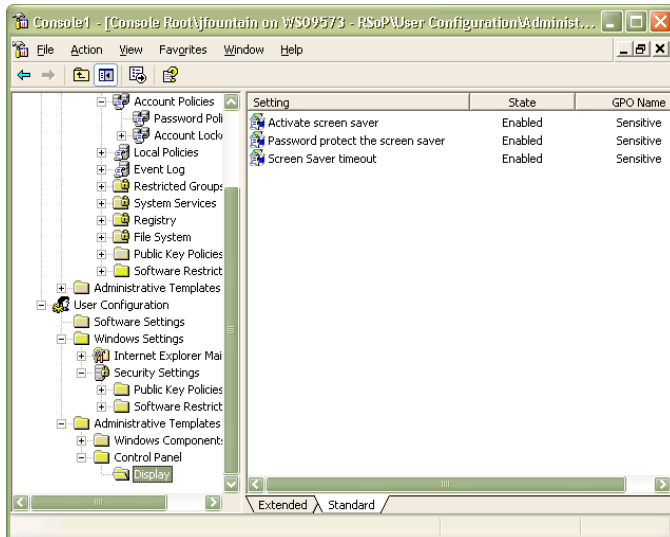
Illustration 11.0: Active Administrator results displaying GPO results for wkst1.



Administrators launch a guest operating system and log in as a test user. The following test results were recorded with a R&D test account.

Logged in as rdtestuser, administrators launch the RSoP MMC snap-in. With RSoP, administrators confirm that the policy is applied properly. .

Illustration 12.0: RSoP results displaying GPO results.



RSoP may not be available for Windows 2000; therefore, administrators use gpresults.exe. Logged in as rdtestacct, administrators run the following command, where /c indicates computer settings only and /s indicates superverbose mode: gpresults.exe /v /c. Below is an example of the test results.

Operating System Information:

Operating System Type: Professional
 Operating System Version: 5.0.2195
 Terminal Server Mode: Not supported

#####

Computer Group Policy results for:

CN=WKST1,OU=Workstations,OU=Resources,OU=PhilaPA,DC=tsc,DC=int

Domain Name: TSC
 Domain Type: Windows 2000
 Site Name: Default-First-Site-Name

The computer is a member of the following security groups:

BUILTIN\Administrators
 \Everyone
 BUILTIN\Users
 TSC\WKST1\$
 TSC\Domain Computers
 NT AUTHORITY\NETWORK
 NT AUTHORITY\Authenticated Users

#####

Last time Group Policy was applied: Tuesday, September 23, 2003 at 5:04:04 PM
Group Policy was applied from: tscdc1.tsc.int

=====

The computer received "Registry" settings from these GPOs:

Local Group Policy
Revision Number: 2 (Active Directory) 2 (Sysvol)
Unique Name: Local Group Policy
Domain Name:
Linked to: Local computer

Default Domain Policy
Revision Number: 3 (Active Directory) 3 (Sysvol)
Unique Name: {31B2F340-016D-11D2-945F-00C04FB984F9}
Domain Name: tsc.int
Linked to: Domain (DC=tsc,DC=int)

Wk_GPO
Revision Number: 7 (Active Directory) 7 (Sysvol)
Unique Name: {5F7BE20E-95D7-45BE-8FD7-54238DE22DA2}
Domain Name: tsc.int
Linked to: Organizational Unit
(OU=Workstations,OU=Resources,OU=PhilaPA,DC=tsc,DC=int)

...

The following settings were applied from: Default Domain Policy

KeyName: Software\Policies\Microsoft\SystemCertificates\EFS
ValueName: EFSBlob
ValueType: REG_BINARY
Value:
...

KeyName: Software\Policies\Microsoft\SystemCertificates\EFS\CTLs
ValueName:
ValueType: REG_NONE
Value: This key contains no values

The following settings were applied from: Wk_GPO

KeyName: Software\Policies\Microsoft\Conferencing
ValueName: NoRDS
ValueType: REG_DWORD
Value: 0x00000001
...

KeyName: Software\Policies\Microsoft\Windows\WindowsUpdate\AU
ValueName: NoAutoRebootWithLoggedOnUsers
ValueType: REG_DWORD
Value: 0x00000001

=====

The computer received "Security" settings from these GPOs:

Default Domain Policy
Revision Number: 3 (Active Directory) 3 (Sysvol)
Unique Name: {31B2F340-016D-11D2-945F-00C04FB984F9}
Domain Name: tsc.int
Linked to: Domain (DC=tsc,DC=int)

Wk_GPO
Revision Number: 7 (Active Directory) 7 (Sysvol)
Unique Name: {5F7BE20E-95D7-45BE-8FD7-54238DE22DA2}

```

Domain Name:   tsc.int
Linked to:     Organizational Unit
(OU=Workstations,OU=Resources,OU=PhilaPA,DC=tsc,DC=int)

```

Run the Security Configuration Editor for more information.

=====

The computer received "EFS recovery" settings from these GPOs:

```

Local Group Policy
Revision Number:      2 (Active Directory) 2 (Sysvol)
Unique Name:          Local Group Policy
Domain Name:
Linked to:             Local computer

```

```

Default Domain Policy
Revision Number:      3 (Active Directory) 3 (Sysvol)
Unique Name:          {31B2F340-016D-11D2-945F-00C04FB984F9}
Domain Name:          TSC.INT
Linked to:             Domain (DC=tsc,DC=int)

```

Additional information is not available for this type of policy setting.

=====

The computer received "IP Security" settings from these GPOs:

```

Wk_GPO
Revision Number:      7 (Active Directory) 7 (Sysvol)
Unique Name:          {5F7BE20E-95D7-45BE-8FD7-54238DE22DA2}
Domain Name:          TSC.INT
Linked to:             Organizational Unit (OU=Workstations,OU=Resources,OU=PhilaPA,DC=tsc,DC=int)

Policy Name:          Wkst-IPSec-Policy
Description:
Policy Path:          LDAP://CN=ipsecPolicy{BC4AD9DC-1E87-4876-A123-F6E8784D7E41},CN=IP
Security,CN=System,DC=tsc,DC=int

```

Logged in as rdtestacct, administrators run the following command, where /u indicates user settings only and /s indicates superverbose mode: gpresults.exe /v /u. Below is an example of the test results.

```

Microsoft (R) Windows (R) 2000 Operating System Group Policy Result tool
Copyright (C) Microsoft Corp. 1981-1999
Operating System Information:
Operating System Type:           Professional
Operating System Version:       5.0.2195
Terminal Server Mode:           Not supported
#####
User Group Policy results for:
CN=rdtestacct,OU=RD_Dept,OU=Accounts,OU=PhilaPA,DC=tsc,DC=int
Domain Name:                    TSC
Domain Type:                    Windows 2000
Site Name:                      Default-First-Site-Name
Roaming profile: (None)
Local profile:                  C:\Documents and Settings\rdtestacct
The user is a member of the following security groups:
    TSC\Domain Users
    \Everyone
    BUILTIN\Administrators
    BUILTIN\Users
    \LOCAL
    NT AUTHORITY\INTERACTIVE
    NT AUTHORITY\Authenticated Users
The user has the following security privileges:
    Manage auditing and security log
    Back up files and directories
    Restore files and directories
    Change the system time
    Shut down the system
    Force shutdown from a remote system
    Take ownership of files or other objects
    Modify firmware environment values
    Profile system performance
    Profile single process
    Increase scheduling priority
    Load and unload device drivers
    Create a pagefile
    Increase quotas
    Remove computer from docking station
    Bypass traverse checking
#####
Group Policy was applied from: tscdc1.tsc.int
=====

```

```

The user received "Registry" settings from these GPOs:
Global_Acct_GPO
Revision Number:                3 (Active Directory) 3 (Sysvol)
Unique Name:                    {FDBFF727-D5B3-475A-B849-6E397B73A3BC}
Domain Name:                    tsc.int
Linked to:                      Organizational Unit
(OU=Accounts,OU=PhilaPA,DC=tsc,DC=int)
The following settings were applied from: Global_Acct_GPO
KeyName:                        Software\Policies\Microsoft\Windows\Control
Panel\Desktop
ValueName:                      ScreenSaveTimeOut
ValueType:                      REG_SZ
Value: 900
KeyName:                        Software\Policies\Microsoft\Windows\Control
Panel\Desktop
ValueName:                      ScreenSaverIsSecure
ValueType:                      REG_SZ
Value: 1
KeyName:                        Software\Policies\Microsoft\Windows\Control
Panel\Desktop
ValueName:                      ScreenSaveActive
ValueType:                      REG_SZ
Value: 1

```

While logged in as the `rdtestuser`, administrators performed a series of tests to confirm that the policy was operational. Below is an outline of several tests performed.

| Policy | Test Performed |
|---|--|
| Does the legal banner display? | <ul style="list-style-type: none"> Before logging in, administrators record if they see the legal banner. |
| Does the screen lock after 15 minutes? | <ul style="list-style-type: none"> Administrators leave screen idle for 15 minutes. |
| Can the users share their desktop or applications with Netmeeting? | <ul style="list-style-type: none"> Administrators try to share their desktop with Netmeeting |
| Are security events being logged? | <ul style="list-style-type: none"> Administrators review event logs to see if security events are logged. |
| Are you warned when you install software? | <ul style="list-style-type: none"> Administrators install test software that is not signed to users are warned prior to installation |
| Is the terminal server traffic using ipsec? | <ul style="list-style-type: none"> Test outlined below |
| Did the policy redirect their "My Documents" to their home directory? | <ul style="list-style-type: none"> Administrators navigate to users "my documents" folder to confirm it is being redirected. |
| Is the computer receiving updates from the SUS server? | <ul style="list-style-type: none"> Event logs are reviewed and Add/Remove Programs examined for newly applied hotfixes. Event log example listed below. |

To ensure that the IPSec policy is working as expected, administrators use `netdiag` and `tcpdump`. While connecting to a terminal server, administrators perform the test with `tcpdump`. A similar test was conducted for email and SQL Server connections.

To perform the test, administrators run the following command while connected to the terminal server (where `-n` disables IP to name resolution, `-i` tells `tcpdump` which network adapter to monitor and "host 10.10.40.192" filters on the host IP indicated.): `tcpdump -n -i 1 "host 10.10.40.192"`. Below is an example of the test results.

Tcpdump Log A:

```
17:41:22.321999 IP 10.10.40.4 > 10.10.40.192: ESP(spi=0x9cf896ce,seq=0xb8) (DF)
17:41:22.322227 IP 10.10.40.4 > 10.10.40.192: ESP(spi=0x9cf896ce,seq=0xb9) (DF)
17:41:22.323926 IP 10.10.40.192 > 10.10.40.4: ESP(spi=0xbd445f29,seq=0xa1) (DF)
17:41:22.328297 IP 10.10.40.4 > 10.10.40.192: ESP(spi=0x9cf896ce,seq=0xba) (DF)
17:41:22.334581 IP 10.10.40.192 > 10.10.40.4: ESP(spi=0xbd445f29,seq=0xa2) (DF)
17:41:22.461142 IP 10.10.40.4 > 10.10.40.192: ESP(spi=0x9cf896ce,seq=0xbb) (DF)
17:41:22.472829 IP 10.10.40.4 > 10.10.40.192: ESP(spi=0x9cf896ce,seq=0xbc) (DF)
17:41:22.600904 IP 10.10.40.4 > 10.10.40.192: ESP(spi=0x9cf896ce,seq=0xbd) (DF)
17:41:22.602563 IP 10.10.40.192 > 10.10.40.4: ESP(spi=0xbd445f29,seq=0xa3) (DF)
17:41:22.804241 IP 10.10.40.4 > 10.10.40.192: ESP(spi=0x9cf896ce,seq=0xbe) (DF)
```

```

17:41:22.914097 IP 10.10.40.4 > 10.10.40.192: ESP(spi=0x9cf896ce,seq=0xbf) (DF)
17:41:22.915755 IP 10.10.40.192 > 10.10.40.4: ESP(spi=0xbd445f29,seq=0xa4) (DF)
17:41:25.085282 IP 10.10.40.4 > 10.10.40.192: ESP(spi=0x9cf896ce,seq=0xca) (DF)
17:41:25.302908 IP 10.10.40.192 > 10.10.40.4: ESP(spi=0xbd445f29,seq=0xac) (DF)

```

Tcpdump Log B:

```

17:41:22.321999 IP 10.10.40.5 > 10.10.40.192: ESP(spi=0x9cf896ce,seq=0xb8) (DF)
0x0000  4500 00a8 5c88 4000 8032 3a1d 0a1b 34b1  E...\.@..2:...4.
0x0010  c0a8 640a 9cf8 96ce 0000 00b8 73bd b52b  ..d.....s..+
0x0020  15ae 30f2 4f7e c91f c5c1 1444 987d 934a  ..O.O~....D.}.J
0x0030  82d1 1b73 9b05 95f0 9307 043c 7a74 6e1f  ....s.....<ztn.
0x0040  d9c6 8798 45d9 5b06 5dcd 2457 5bd5 25b0  ....E.[.].$W[.%.
0x0050  11b8                                     ..
17:41:22.322227 IP 10.10.40.5 > 10.10.40.192: ESP(spi=0x9cf896ce,seq=0xb9) (DF)
0x0000  4500 0088 5c89 4000 8032 3a3c 0a1b 34b1  E...\.@..2:<..4.
0x0010  c0a8 640a 9cf8 96ce 0000 00b9 deab baf5  ..d.....
0x0020  80c1 5472 0329 2bf1 85f6 574e 4959 306a  ..Tr.)+...WNIY0j
0x0030  30d4 46b7 92f4 9d74 0177 958a 6581 33e9  0.F....t.w...e.3.
0x0040  1982 f26e 00be 6f5c a246 ca03 7ee6 3a6f  ....n..o\F...~:o
0x0050  29e3                                     ).

```

Using the netdiag utility, administrators gather IPsec statistics such as active associations, SA used and any failures.

To perform the test, administrators ran the command (where /test:ipsec indicates test IPsec network activity and /v indicates verbose mode): netdiag /test:ipsec /v. Below is an example of the test results.

© SANS Institute 2003, Author retains full rights.

```

IP Security test . . . . . : Passed
Directory IPSec Policy Active: 'Wkst-IPSec-Policy'
IPSec Statistics
Oakley Main Modes      : 3
Oakley Quick Modes     : 0
Active Associations     : 0
Soft Associations      : 0
Authenticated Bytes Sent : 0
Authenticated Bytes Received : 0
Confidential Bytes Sent : 0
Confidential Bytes Received : 0
Offloaded Bytes Sent    : 0
Offloaded Bytes Received : 0
ReKeys                 : 0
Authentication Failures : 0
Negotiation Failures   : 3
Packets not decrypted   : 0
Packets not authenticated : 0
Invalid Cookies Rcvd    : 0
Acquire fail           : 0
Receive fail           : 14
Send fail              : 0
GetSpiFail             : 0
KeyAddFail             : 0
KeyUpdateFail          : 0
Active Acquire         : 1
Active Rcv             : 0
Active Send            : 0
Total Acquire          : 3
TotalGetSpi            : 3
TotalKeyAdd            : 0
TotalKeyUpdate         : 0
Inactive Associations   : 0
Dead Associations      : 2
Pending Keys           : 1
Key Flushes            : 0
Key Additions          : 0
Key Deletes            : 0
Phase 1 offers count is 4
OFFER #1:
PFS : No, Encryption : DES, Hash : SHA1, Group : Medi
Quickmodes per MainMode : 0, Lifetime Seconds : 28800
OFFER #2:
PFS : No, Encryption : DES, Hash : MD5, Group : Mediu
Quickmodes per MainMode : 0, Lifetime Seconds : 28800
OFFER #3:
PFS : No, Encryption : DES, Hash : SHA1, Group : Low
Quickmodes per MainMode : 0, Lifetime Seconds : 28800
OFFER #4:
PFS : No, Encryption : DES, Hash : MD5, Group : Low (
Quickmodes per MainMode : 0, Lifetime Seconds : 28800
Current Phase 1 SAs:
SA # 1
Policy Id: {DBC7FC93-02BF-4FD7-8538-D453B07C6773}
Current Oakley State : MainMode Key Authorized
Src : 192.168.168.11, Dest : 192.168.168.10
IdentityProtection : No, PRF : 0
PFS : No, Encryption : DES, Hash : SHA1
Authentication : Kerberos, Group : Low (1)
Quickmodes per MainMode : 0, Lifetime Seconds : 28800

```

Event logs were examined to confirm that SUS updates and security changes were applied. In addition, Active Administrators provided a tool, Client Troubleshooting, to alert administrators of any policy errors.

Automatic Updates Event Log Entry:

| | |
|--|-------------------|
| Event Type: | Information |
| Event Source: | Automatic Updates |
| Event Category: | Installation |
| Event ID: 19 | |
| Date: | 8/16/2003 |
| Time: | 9:01:54 AM |
| User: | N/A |
| Computer: | WKST2 |
| Description: | |
| Installation Successful: Windows successfully installed the following update. | |
| - 330994: April 2003, Security Update for Outlook Express 6 SP1 | |
| - 811493: Security Update (Windows XP) | |
| - Q817287: Critical Update (Catalog Database Corruption in Microsoft Windows XP) | |
| - 816093: Security Update Microsoft Virtual Machine (Microsoft VM) | |
| - Security Update for Windows XP (815021) | |
| - Q329441: Critical Update | |
| - 814033: Critical Update | |
| - Security Update for Windows XP (329834) | |

Illustration 13.0: Client Troubleshooting with Active Directories

| | | | | | | |
|-------------------|-------------|----------------------|--------|----------|-------|------|
| 2 Laptops | Type | Date / Time | Source | Category | Event | User |
| 2 Printers | Error | 9/23/2003 5:06:54 PM | SceCli | None | 1003 | N/A |
| 2 Prod_Servers | Error | 9/23/2003 5:03:24 PM | SceCli | None | 1003 | N/A |
| 2 RD_Workstations | Information | 9/23/2003 5:03:20 PM | SceCli | None | 1704 | N/A |
| 2 SQL_Servers | Error | 9/23/2003 9:56:58 AM | SceCli | None | 1003 | N/A |
| 2 Web_Servers | Error | 9/23/2003 9:54:58 AM | SceCli | None | 1003 | N/A |
| 2 Workstations | Information | 9/23/2003 9:54:56 AM | SceCli | None | 1704 | N/A |
| WKST1 | Information | 9/21/2003 5:37:41 PM | SceCli | None | 1704 | N/A |
| nValleyCA | Error | 9/19/2003 7:14:39 PM | SceCli | None | 1003 | N/A |
| | Error | 9/19/2003 7:14:35 PM | SceCli | None | 1003 | N/A |
| | Information | 9/19/2003 7:14:33 PM | SceCli | None | 1704 | N/A |

5.3 Test the System functionality

After confirming the group policy security effectiveness, a system functionality test is performed to ensure that the new security settings policy will not impede user functionality. Two users, one from Customer Service and one from Research and Development, were used due to their sensitive environment.

Test one: administrators logged into a vmware guest operating system as cstestuser, a customer service user.

| Test Performed | Results |
|--|--|
| Open Web-based Customer service application. | There were no problems connecting to this site. The new proxy settings and security settings did not affect the connection to the website. |

Test two: administrators logged into a vmware guest operating system as rctestuser, a customer service user.

| Test Performed | Results |
|------------------------|--|
| Connect to SQL Servers | Connection was established without error |

5.4 Apply the Group Policy

The group policy was applied to the production OU by coping from the test environment with the Active Administrator application or imported into the computer group policy using the Group Policy MMC snap-in.

Illustration 14.0: Applying the Group Policy using the Group Policy MMC snap-in:

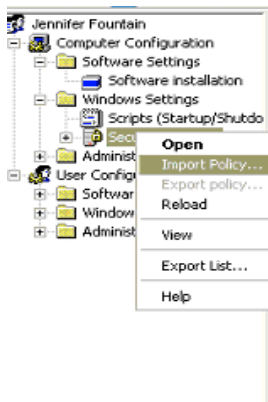
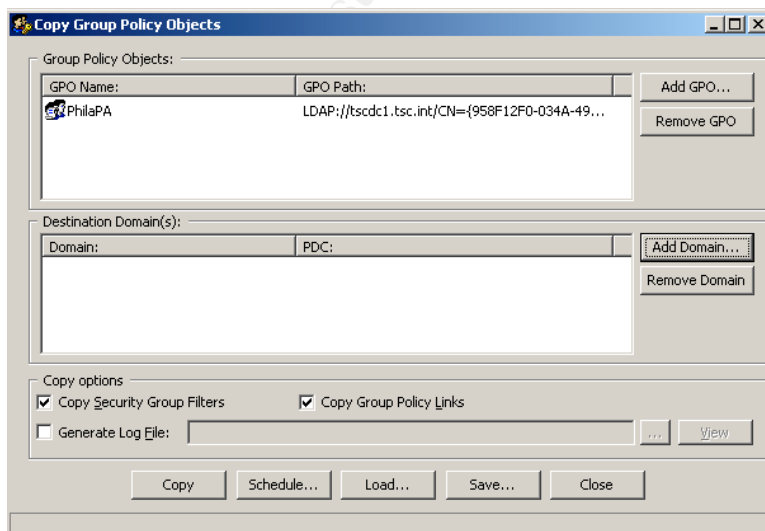
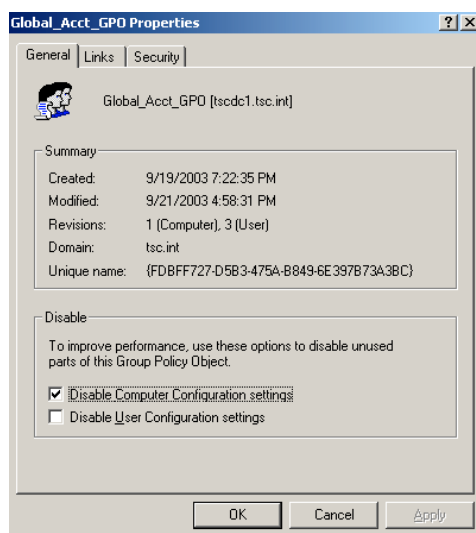


Illustration 15.0: Applying the Group Policy using Active Administrator:



The computer policy was applied to the appropriate resource OU. For example, the workstation policy was applied to the workstation OU. The user policy was applied to the appropriate account OU. For example, the customer service policy was applied to the CS_Dept OU. Microsoft recommends disabling unused group policy objects to expedite policy processing during logon. In accordance to this recommendation, TSC and GE disabled the unused group policy object on the OU. For example, they disabled the Computer Configuration settings on the Accounts OU and disabled the User Configuration settings on the Resources OU. In addition, TSC and GE avoid assigning cross-domain group policies (ref 24) because it will slow down the logon process.

Illustrations 16.0: Properties of the Global_Acct_GPO



5.5 Evaluate the Group Policy

After the policy was deployed into production, administrators reassessed the policy's effectiveness and functionality. Below are some concerns raised by the user community.

The screensaver timeout created a problem for the Customer Service department because they would be on a call for more than fifteen minutes while looking at customer information without screen interaction. Therefore, administrators increased the time to 30 minutes for Customer Service users. In addition, customer service use a machine dedicated to display updates about critical business information. Since customer service users need to view this machine at all times, the screen cannot be locked. Therefore, the screen lock setting was removed for these machines. But not to diminish security, administrators installed a program, called Transparent Screen Lock, which would lock the station but not lock the screen (20).

The security change on the unsigned driver installation behavior and unsigned non-driver installation behavior to “warn but allow installation” caused a problem for Research and Development users because they install and uninstall test software that may not be signed. R&D users found that being warned with every installation became cumbersome and affected their productivity and requested that this security setting be removed. In order to accommodate their request, administrators removed this option for R&D test machines. If a virus were to enter the network and execute on RD machines, this could pose as a serious security risk. In order to work around this security risk, R&D users cooperated with administrators and agreed to log into their test machines at a normal user level and use the “run as” option for software installations.


Setting the “Number of logons cached” to zero posed a problem for laptop users. While traveling, they were unable to log into their machine with their cached domain account. Administrators changed the amount of logins cached to one for laptops only and applied this setting to the laptop OU.

6.0 Auditing the Active Directory Infrastructure

To ensure the active directory infrastructure remains secure, TSC and GE administrators must monitor event logs, active directory modification events and network and system performance data. In the following section, I will outline the auditing procedures followed by the TSC and GE administrators to ensure that network and system security is maintained.


TSC and GE administrators use Active Administrator to audit active directory changes. Active Administrator is a very powerful auditing tool for active directory. It allows administrators to track all changes to their active directory infrastructure, such as group policy changes, adding or deleting users or adding or deleting an OU. Administrators can easily change and view all permissions on the configuration, schema and OU container objects from one console. In addition, Active Administrator allows administrators to perform a multitude of administrative tasks such as backup and restore group policy objects and copy group policy objects to other domains. Active Administrator has a built-in mechanism to copy group policies between domains. This feature is very useful when admins need to create a test environment or install a new group policy to another domain. The reporting feature provides excellent reports so administrators can review permission, group policy or any other active directory changes at-a-glance. For example, administrators have the ability to generate reports on all group policy changes and revert back to an older version if necessary.


Illustration 17.0: Sample Group Policy Change Report


 **Group Policy Change Report**


GPO Name: Policy 1
 Unique Name: {5B2F32FD-04A-19B7-9A7E-E1D88F1C3667}
 Domain: tsc.int


































Changes from: September 12, 2003 11:38:30 AM Old Revisions: 0 (Computer), 0 (User)
 Changes to: September 12, 2003 05:16:00 PM New Revisions: 2 (Computer), 9 (User)

 **Computer Configuration**

 **Software Settings**

 **Windows Settings**

 **Security Settings**

| Changes were made to Security Settings | Old Policy Setting | New Policy Setting |
|---|--------------------|---------------------------------------|
|  Account Policies | | |
|  Password Policy | | |
|  Enforce password history | <not configured> | 24 passwords remembered |
|  Maximum password age | <not configured> | 90 days |
|  Minimum password age | <not configured> | 1 day |
|  Minimum password length | <not configured> | 12 characters |
|  Passwords must meet complexity requirements | <not configured> | Enabled |
|  Store passwords using reversible encryption for all users in the domain | <not configured> | Disabled |
|  Account lockout Policy | | |
|  Account lockout duration | <not configured> | 15 minutes |
|  Account lockout threshold | <not configured> | 3 invalid login attempts |
|  Reset account lockout counter after | <not configured> | 15 minutes |
|  Local Policies | | |
|  Audit Policy | | |
|  Audit account login events | <not configured> | Success, Failure |
|  Audit account management | <not configured> | Success, Failure |
|  Audit directory service access | <not configured> | No auditing |
|  Audit login events | <not configured> | Success, Failure |
|  Audit object access | <not configured> | Failure |
|  Audit policy change | <not configured> | Success, Failure |
|  Audit privilege use | <not configured> | Failure |
|  Audit process tracking | <not configured> | No auditing |
|  Audit system events | <not configured> | Success, Failure |
|  User Rights Assignment | | |
|  Access this computer from the network | <not configured> | BUILTIN\Users, BUILTIN\Administrators |
|  Adjust memory quotas for a process | <not configured> | BUILTIN\Administrators |
|  Back up files and directories | <not configured> | BUILTIN\Administrators |
|  Bypass traverse checking | <not configured> | BUILTIN\Users |
|  Change the system time | <not configured> | BUILTIN\Administrators |
|  Create a pagette | <not configured> | BUILTIN\Administrators |
|  Force shutdown from a remote system | <not configured> | BUILTIN\Administrators |
|  Increase scheduling priority | <not configured> | BUILTIN\Administrators |
|  Load and unload device drivers | <not configured> | BUILTIN\Administrators |

Small Wonders Software, Active Administrator™
<http://www.smallwonders.com>

Generated on: 9/12/2003 5:20:52 PM
 Page: 1

In addition to using Active Administrator, TSC and GE administrators developed a centralized logging system to maintain all device security

logs. Their centralized logging systems consist of two Linux servers configured with Syslog, Apache and Swatch. The servers are configured with an ample amount of hard drive space so the administrators are able review current logs and archive old logs. Their routers and firewalls are syslog aware; however, the Windows operating system requires third party software to enable this function. They currently use NTSyslog (20) and MonitorWare (21) for their syslog clients. NTSyslog is configured on all windows 2000 servers to send its security, system and application event logs to the syslog servers. Since IIS and IAS send their events to a log file, NTSyslog will not work. Therefore, MonitorWare is configured to send a copy of IIS and IAS log files to the syslog servers.

Illustration 18.0: NTSyslog Configuration Screens

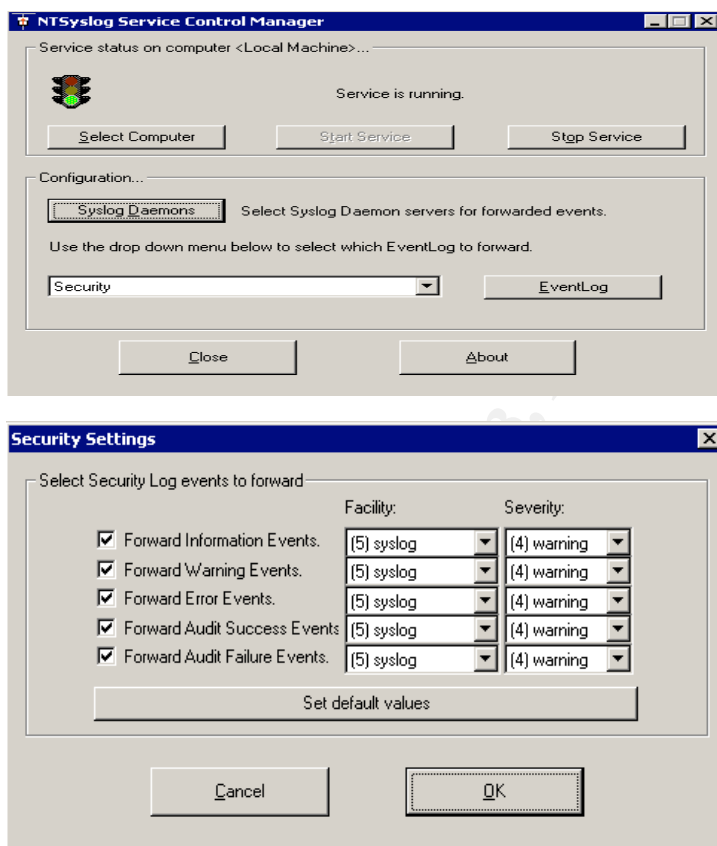
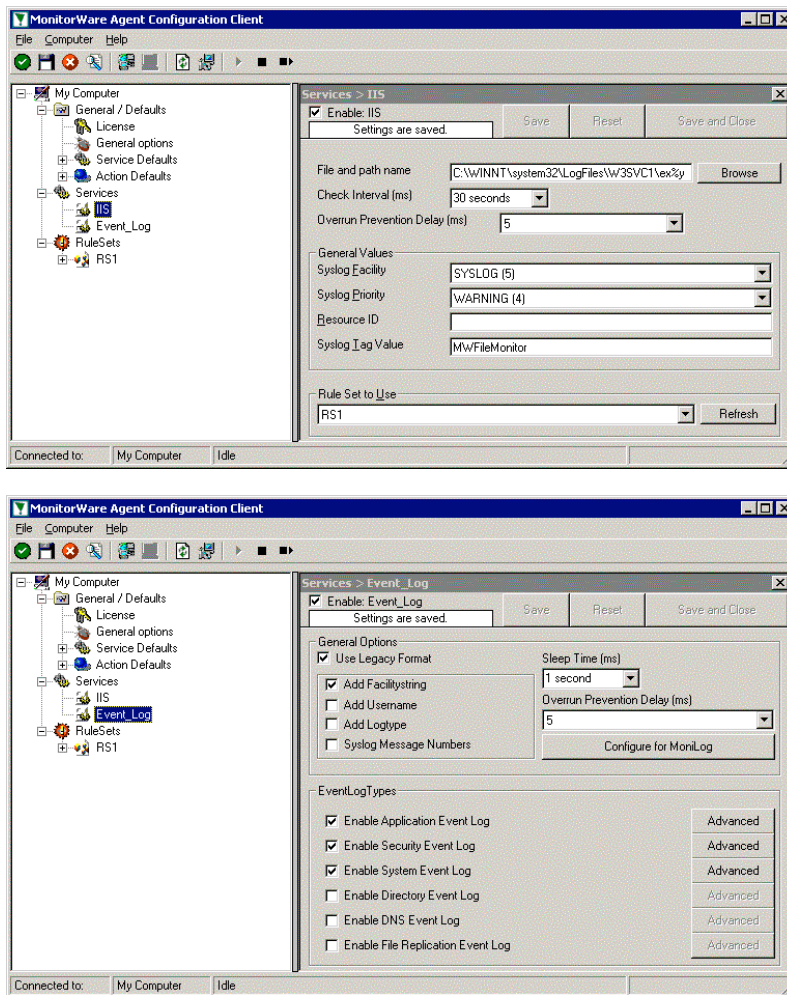
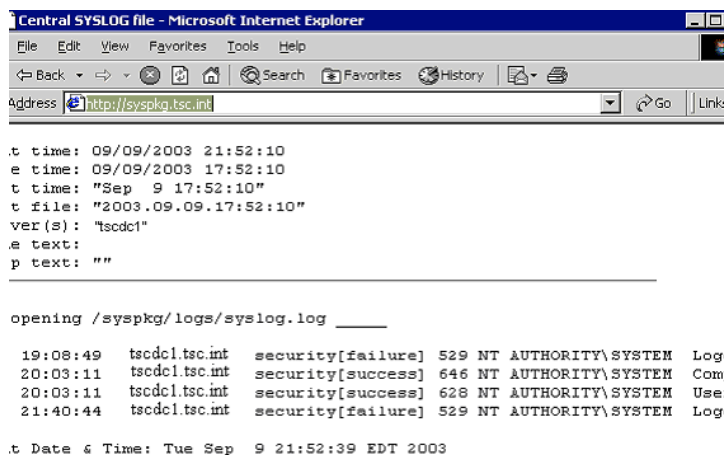


Illustration 19.0: MonitorWare Configuration Screen



To view historical and real-time alerts, administrators created CGI scripts that parse Syslog files that are usable by apache. After administrators enter their search requirements, they can view the information via a browser.

Illustration 20.0: Webpage viewing alerts for a server



```

t time: 09/09/2003 21:52:10
e time: 09/09/2003 17:52:10
t time: "Sep 9 17:52:10"
t file: "2003.09.09.17:52:10"
ver(s): "tscdc1"
e text:
p text: ""

opening /syspkg/logs/syslog.log ____

19:08:49 tscdc1.tsc.int security[failure] 529 NT AUTHORITY\SYSTEM Logc
20:03:11 tscdc1.tsc.int security[succes] 646 NT AUTHORITY\SYSTEM Com
20:03:11 tscdc1.tsc.int security[succes] 628 NT AUTHORITY\SYSTEM User
21:40:44 tscdc1.tsc.int security[failur] 529 NT AUTHORITY\SYSTEM Logc

t Date & Time: Tue Sep 9 21:52:39 EDT 2003

```

Administrators use an active log monitoring tool, swatch, to monitor the Syslog files so they are notified of critical alert as they occur (23). When a particular event id or IIS entry is logged to the Syslog server, an email is generated and sent to appropriate administrators. Below are some examples of which event ids and IIS log entries trigger an alert:

Example events:

- An account is lockout: event id 644
- An account unlocked: event id 642
- A group created: event id 631
- A group deleted: event id 634
- User added to group: event id 632
- User removed from group: event id 633
- User account removed: event id 630
- User account added: event id 624

IIS Log examples:

- msadcs\..dll: attempts to access msadcs.dll (RDS exploit)
- ::\ \$DATA: DATA exploit attempts
- \.asp\.: asp exploit attempts
- sam\._ : attempts to download the SAM backup file
- \.ida |\..idq |\..htw : attempts to access an Index Server page

- "showcode\.asp": attempts to access the SHOWCODE.ASP page
- /certsrv:: attempts to access Certificate Server
- .+\\(?:sys)*admin.*|.+\root.:attempts to log on with an administrative account
- GET /default\.ida: probes by the Code Red Worm

Excerpt from swatch configuration file:

```
#  
# Swatch configuration file for constant monitoring  
#  
#NT Security Events  
watchfor / 644 | 642 | 631 | 634 | 641 | 632 | 624 | 630 /  
mail addresses=admin_group\@tsc.com,subject=NT Security Events  
  
#IIS Server Security Events  
watchfor / :$DATA | ".+\\(?:sys)*admin.*|.+\root." | "showcode\.asp" |  
"GET /default\.ida" | "cmd\.exe" | \\winnt/winnt
```

Email alert example when creating an account:

```
Sep 7 17:04:55 dc1.tsc.int security[success] 624 TSC\admin User Account  
Created: New Account Name:test123 New Domain:TSC New Account ID: %{S-  
1-5-21-508168516-391010822-19539831-7187} Caller User Name:admin Caller  
Domain:TSC Caller Logon ID:(0x0,0x2CE3819) Privileges-
```

Email alert example when deleting an account:

```
Sep 7 17:05:03 dc1.tsc.int security[success] 630 TSC\admin User  
Account Deleted: Target Account Name:test123 Target Domain:TSC  
Target Account ID: %{S-1-5-21-508168516-391010822-19539831-7187}  
Caller User Name:admin Caller Domain:TSC Caller Logon  
ID:(0x0,0x2CE3819) Privileges:-
```

Log files and email alerts alone will not ensure security on their Active Directory infrastructure. Administrators will need to stay on top of Microsoft Security vulnerabilities and patch their systems as necessary. To accomplish this task, administrators configured, via group policy, each server to automate updates via a local Software Update Server. All updates are logged to the event log and copied to the Syslog server which generates an email to administrators. In addition, administrators sign up for Microsoft Alert Bulletins so they are informed of all security issues with the operating system.

Firewall and physical security was not addressed but is a concern for administrators. All measures were taken to ensure securities in these areas were met.

7.0 Conclusion

This document discussed the merger of the Sans Company and GIAC Enterprises' network and active directories infrastructure while maintaining their web presences. The paper also reviewed the workstation group policy testing and implementation. It also described the auditing procedures executed by administrators to ensure system security.

© SANS Institute 2003, Author retains full rights.

References

1. http://www.giac.org/practical/GCWN/Brandon_Lowther_GCWN.pdf, Brandon Lowther, GIAC Paper used for GE Enterprises model.
2. http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_DNS_imp_NamespacePlanning.htm, Planning your Namespace, Microsoft Corporation.
3. http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_addeploy_5.htm, Planning organizational unit structure, Microsoft Corporation.
4. <http://www.nsa.gov/snac/win2k/guides/w2k-12.pdf>, Securing Windows 2000 Certificate Services, NSA.
5. <http://www.nsa.gov/snac/index.html>, Security templates for Windows 2000 and XP, National Security Agency.
6. <http://www.cisecurity.com/>, Security templates for Windows 2000 Server and Workstation, Center for Internet Security.
7. http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/cnet/cncb_dhc_ogjw.asp, DHCP 80/20 Model, Microsoft Corporation.
8. http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_addeploy_5.htm, Replication goals and strategies, Microsoft Corporation.
9. http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_addeploy_5.htm, Planning organizational unit structure, Microsoft Corporation.
10. Building Enterprise Active Directory Services Notes from the Field, Microsoft Corporation.
11. Maximum Windows 2000 Security, Anonymous, SAMS Publishing.
12. Securing Windows: Track 5 Course Material, Jason Fossen.
13. <http://support.microsoft.com/?kbid=234582>, Publishing a Shared Folder in Windows 2000 Active Directory, Microsoft Corporation.
14. Counter Hack: A step-by-step guide to Computer Attacks and Effective Defenses, Ed Skoudis, Prentice Hall.

15. www.tcpdump.org, TCPDump
16. <http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/manadsteps.asp>, Step-by-Step Guide to Managing Active Directory, Microsoft Corporation.
17. <http://www.securityfocus.com/infocus/1559>, Securing Windows 2000 Communications with IP Security Filters, *Joe Klemencic*.
18. <http://support.microsoft.com/?kbid=321709>, Use the Group Policy Results Tool in Windows 2000, Microsoft Corporation.
19. <http://www.e-motional.com/TScreenLock.htm>, Transparent Screen Lock, E-motional Software Company.
20. <http://ntsyslog.sourceforge.net/>, NTSyslog.
21. <http://www.monitorware.com/en/>, Monitorware.
22. <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/deploy/ccmdepl/ccmch05.asp>, Developing a Group Policy Implementation Strategy, Microsoft Corporation.
23. <http://swatch.sourceforge.net>, Swatch Monitoring tool.
24. http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_addeploy_5.htm, Best Practices, Microsoft Corporation.
25. <http://support.microsoft.com/default.aspx?scid=kb;en-us;179442>, How to Configure a firewall for Domains and Trusts, Microsoft Corporation
26. <http://support.microsoft.com/default.aspx?scid=kb;en-us;224196>, Restricting Active Directory Replication Traffic to a Specific Port, Microsoft Corporation.
27. <http://support.microsoft.com/?kbid=280061>, Move Windows 2000 DNS Zones to Another Windows 2000-based Server, Microsoft Corporation.
28. <http://www.smallwonders.com>, Active Administrator, Small Wonders Software Company.
29. <http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/netdiag-o.asp>, Netdiag Utility tool, Microsoft Corporation.

30. <http://www.vmware.com>, VMware Inc.

© SANS Institute 2003, Author retains full rights.