Global Information Assurance Certification Paper

Design a Secure Windows 2000 Infrastructure

GIAC Certified Windows Security Administrator (GCWN)
Practical Assignment – Version 3.1 – Option 1

Jack M. Kohn
May 29, 2003

TABLE OF CONTENTS

ABSTRACT

The following paper describes hypothetical network configuration and security solutions implemented by a fictional company called GIAC Enterprises ("GIACENT"). It briefly describes GIACENT's business and organizational structure, the network infrastructure that supports the organization in its two offices, and the configuration of its network computers. Finally, it examines the Active Directory design and some example Group Policies implemented at GIACENT, and the rationale behind them. Throughout, it is assumed that GIACENT is a small but growing company, and that design decisions are a result of organizational as well as technical issues.

This paper has been submitted as partial fulfillment of requirements for the **GIAC Certified Windows Security Administrator (GCWN)** certification.

Description of GIAC Enterprises (GIACENT[1])

GIAC Enterprises (Great Inventions and Artistic Collaborations) is a musical industry company involved in the design, manufacture, marketing, installation, and service of musical products such as synthesizers, software sequencers, hard disk recorders, audio signal processors, and equipment interfaces. Profits accrue from sales of products through direct and retail channels, consultation services, system configuration and installation services, and the leasing of proprietary technologies developed by a team of research engineers and artists.

GIAC Enterprise's primary web presence at this time provides detailed product descriptions, support documents, and on-line ordering capabilities. In addition, business partners (including distributors, retailers, and end-user clients) can log on to GIAC Enterprise's web server with a user ID and password to retrieve information about placed orders and account history. Future services under development include an Internet-based system for storing and retrieving the configuration information and digital data from a studio session so that significant data (including audio) can be easily and safely transferred electronically from one studio location to another.

GIAC Enterprises is spread over two locations: the Headquarters office located in a downtown office building; and a larger office located in a not-too-distant (but much less expensive per square foot) suburban location.

Marketing/Sales, Finance, and Human Resources are located at the Headquarters office downtown. A few servers primarily used by those groups, along with other required network equipment, are located in locked equipment rooms in the downtown location. The bulk of GIAC Enterprise's servers and network infrastructure is located in the suburban office, in a secured data center.

GIACENT's corporate structure can be summarized as follows:

- **Research & Development (R&D)** – Here, electronic innovations are developed, tested, and prototyped by Electrical Engineers, computer Software Developers, and Aesthetic Consultants. The R&D Department works out of the suburban location.
- **Customer Service and Support** – includes six Technical Support staffers who take turns manning telephone support lines from the suburban office and servicing clients in the field.
- **Sales and Marketing** – works closely with existing and potential customers to generate ideas for new products and improvements to existing products. They forward customer needs to the R&D areas, and

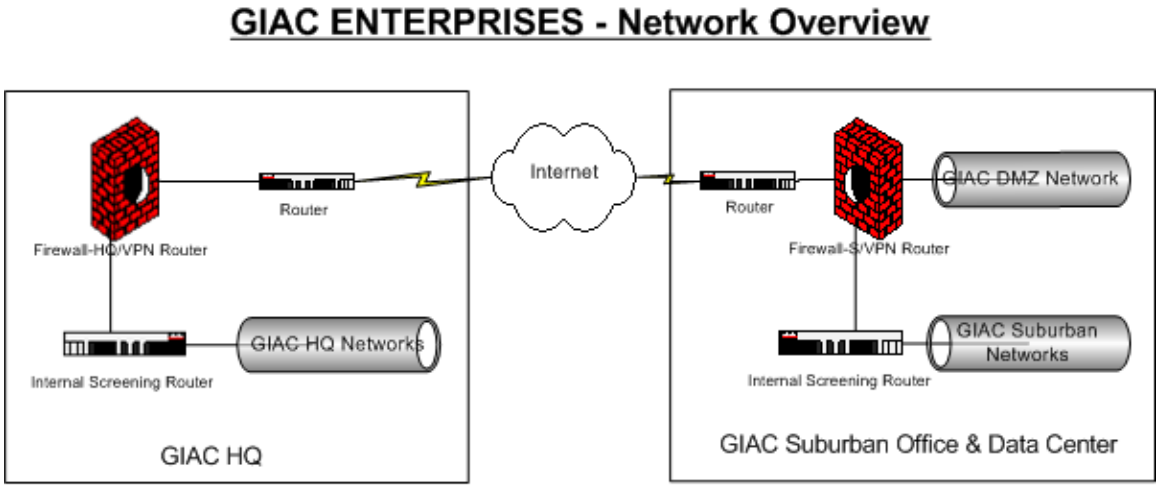
[1] Note: The acronym "GIACENT" was chosen and used in this paper to eliminate possible confusion between the fictional GIAC Enterprises discussed in this paper, and the actual GIAC (Global Information Assurance Certification) organization and its associated web sites.

work to create demand for existing GIAC products. A team of three Sr. Account Representatives interfaces mostly with large pro-audio clients, while an additional sales force of ten people maintains relations with their retail resellers. The Sales Team's "home base" is the downtown HQ location, but most of the sales force spends significant time out of the office with clients and/or meeting with the R&D staff at the suburban office.

- **Finance and Human Resources** – Both groups are located in the downtown corporate Headquarters office. The Finance Group handles Accounts Receivables and Accounts Payables. Human Resources (HR) maintains employee records, including sales and service levels achieved by each employee that are used to calculate performance bonuses and other motivational employee rewards.
- **Information Technology** – An IT staff of four people maintains the servers and network infrastructure. Duties include the maintenance of user accounts and storage, backing up all servers regularly, management of redundant copies of backup media onsite and offsite in secured storage facilities, and monitoring system logs. The group is also responsible for developing GIACENT's network infrastructure to meet steadily increasing demands of the business. Their home is the suburban office, but on any given day, two (or more) members of the IT team are likely to be working on projects at HQ.

GIACENT also relies on two important business partners: PressBoard Partners, a design consulting firm that takes GIACENT's prototypes and creates functional and attractive products aimed at specific target markets (e.g., pro audio, personal studio owners); and a manufacturing plant that actually produces GIACENT's hardware products. These business partners sometimes log in to GIACENT's public network with a secured ID and password to exchange information related to product development.

Network Design



Network Overview

GIACENT's connection to the Internet (and between the two GIACENT offices) consists of a 1.5 MBps SDSL line at the suburban office and a 768Kbps SDSL line in the downtown office. VPN software built into the firewall at each office maintains a secure and encrypted channel between the two offices over the SDSL connections to the Internet.

This link is fast enough that all the GIAC Enterprise machines can be considered to be in one *site* for purposes of AD replication. The network is arranged so that, ideally, users will usually not need to copy vast amounts of data across the VPN. Restrictions on the size of email attachments, and other data use policies, prevent tying up excessive bandwidth when downtown employees access email from the Exchange 2000 server located in the suburban office.

The suburban firewall ("Firewall-S") is a stateful firewall configured to allow only necessary traffic to pass in each direction. A "block all traffic not specifically permitted" ruleset filters network traffic based on the source and destination IP addresses and ports wherever possible. A similar model of firewall/VPN ("Firewall-HQ") is located in the downtown location to protect the HQ network from malicious Internet traffic. The firewalls do permit outbound sessions initiated by machines on the private GIACENT networks, allowing employees to access the Internet. Further description of firewall rules is beyond the scope of this paper.

The screening routers at each site, between the firewalls and internal corporate networks, further filter traffic to provide additional defense in depth. These

internal routers also segment the corporate networks at each location. This helps ensure that, for example, huge file transfers between machines in the R&D area have minimal impact on other departments' local network bandwidth. The routers are RFC1542 compliant and are configured to relay DHCP/BOOTP traffic across internal subnets.

Server Overview

GIAC Enterprises uses Microsoft Windows 2000 Server on most server machines. The public SQL and IIS servers run Windows 2000 Advanced Server because GIACENT wants the option of building out these servers in the future with additional CPUs and RAM, and perhaps clustering them with additional servers.

All servers have been upgraded to Windows 2000 Service Pack 3 (SP3). Application of security hotfixes relevant to each particular system is part of administrators' routine duties. (Hotfix requirements differ depending on the services running on a particular server. For example, a server running IIS5 will have a different set of security hotfixes than an SQL 2000 server.)

All servers run anti-virus (AV) software. A utility server downloads AV updates from the AV vendor site and automatically updates the anti-virus signatures and software on all other servers and workstations in the company.

Most servers have at least three physical hard disks operating off of RAID5 hardware controllers. All servers are installed with NTFS formatting on all partitions. The operating system is installed on the first partition (C: drive) and user data is always stored on one or more separate partitions. Depending on the server roles, additional partitions and/or physical disks may be configured to support specific applications (e.g., IIS or SQL), hold log files, etc.

Best practices are followed in assigning permissions to network resources: Global Groups classify users for security purposes; Local Groups are created and assigned "least privilege" rights to server resources; Global Groups are then added to the Local Groups to confer access rights to users. Because GIACENT has only one internal domain, there is little need to use Universal Groups. Where applicable, access rights are further limited from default settings (for example, removing the "Everyone" group from the root of the system drive).[2] Some access right assignments are documented in guides and checklists used by GIACENT IT staff to build servers. Ideally, the majority of permissions on sensitive system files would be enforced using Group Policy.

[2] Microsoft: TechNet Knowledge Base article 327522.

Workstation Overview

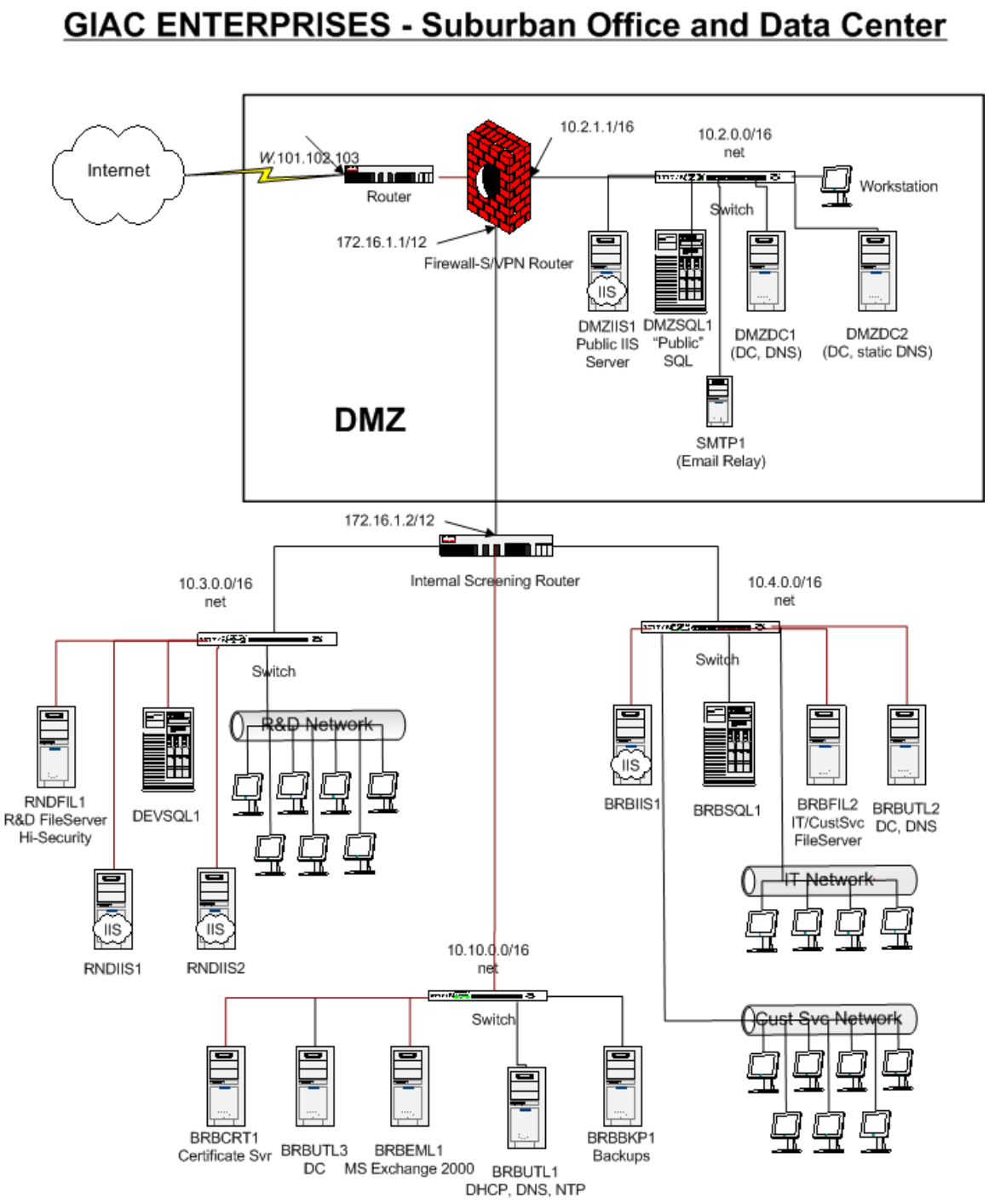
Client workstations are a mixture of machines running Windows 2000 with SP3, or Windows XP with SP1.

- The Sales Department uses Windows XP on company-owned and controlled laptop machines.
- The HR and Financial departments use Windows 2000 – the slightly older machines used by those areas perform better with Windows 2000 than XP.
- The R&D Department uses Windows XP desktop machines for most work, and have a few older machines used on- and off-the-network for software compatibility testing.
- Customer Service & Support uses desktops running a mix of Windows 2000 and Windows XP. Several Windows XP laptops are dedicated for their use during service calls.
- The IT Department also uses a mix of Windows 2000 and Windows XP machines for production and testing.

Most workstations and laptops have a single, large hard disk drive. Additional disk drives have been added to some R&D machines, in some cases configured as RAID 0 for performance enhancement. All workstation drives are formatted with NTFS and have appropriate restrictive permissions applied. The IT Department uses auditing tools to track drive configuration and usage. All employees are strongly discouraged from storing sensitive data on their local hard disks, and the local “My Documents” directory is redirected to a network directory for the users in HR and Finance.

All workstations run anti-virus software; an internal utility server distributes updates automatically.

Network Design: Suburban location



GIACENT's suburban location houses the largest part of the internal corporate network, as well as the "Demilitarized Zone" or DMZ network that provides GIACENT's public Internet presence.

The DMZ

The purpose of the DMZ is to separate the publicly accessible portion of GIACENT's network from the internal corporate network. The DMZ and internal networks are physically connected through a screening router to enable data transfers between the two networks (for example, when updating the public web site).

The DMZ and internal networks are separate Windows AD domains. However, there is no Windows domain trust between the two networks. Administrators and select other users can access servers on the DMZ but must use logon credentials valid for the DMZ domain, giacentdmz.biz. (See also the "Active Directory Design" section below.)

Servers in the DMZ

Currently, the DMZ holds the following machines[3]:

- **DMZIIS1**, a public-facing web server (accessed via the URL www.giacent.biz[4]) running Microsoft IIS 5.0 on Windows 2000 Advanced Server with Service Pack 3 (SP3) and all applicable hotfixes. All unnecessary services on the server are disabled and all unnecessary sample files, sample scripts, help files, programs, etc., have been removed.
- **DMZSQL1**, a Microsoft SQL 2000 server on Windows 2000 Advanced Server with Windows SP3, SQL 2000 SP3, and all applicable hotfixes.
- **DMZDC1** and **DMZDC2**, Microsoft Windows 2000 Server machines with SP3 and applicable hotfixes, configured as Domain Controllers (DCs) for the giacentdmz.biz domain. The DCs run in Native Mode since no NT4 domain controllers exist in the domain. Two DCs are installed to provide redundancy for domain authentication services. These DCs also run the DNS service.
- **SMTP1** is a Windows 2000 Server (SP3 and applicable hotfixes) running IIS 5.0 and configured to forward email to and from (only) the internal Exchange 2000 server via the Internet Service Provider's mail exchanger.[5]

[3] GIACENT servers have been named to make their purpose clear to the reader. In an actual installation, it is probably a good idea to use somewhat more generic names. This simple form of "security through obscurity" won't go far: determined hackers can figure out which machines provide what services. But it's a good idea not to post signs that say, "Here's the Domain Controllers! Look!, I'm an SMTP server!"

[4] This URL was not assigned at the time of writing this paper and this web link is not valid. This is intentional.

[5] Microsoft TechNet KnowledgeBase article 310356: "HOW TO: Prevent Mail Relay in the IIS 5.0 SMTP Server in Windows 2000."

All unnecessary services on the server are stopped and all unnecessary sample files, programs, etc. have been removed.

- A single **workstation** exists in the giacnet.biz domain for the convenience of network administrators. It runs Windows XP (SP1 and hotfixes). This machine is designated for downloading patches and running sundry utilities such as the client console for patch management software. It also runs various scripts and batch files as Scheduled Tasks to help consolidate system logs, audit network performance, etc. Although this machine triggers some housekeeping jobs for the domain, sensitive data (like user data and logs) are moved or copied to protected servers on the internal network.

The DMZIIS1 and DMZSQL1 servers are each dual-processor machines configured with ample storage in a RAID5 configuration. At GIACENT's present rate of growth, these servers are expected to provide enough "horsepower" for at least another year. The other machines in the DMZ are smaller servers; the number of business partners and customers that authenticate to the domain do not put a significant load on the domain controllers, and the SMTP server is specifically configured to do only one job.

IPSec in the DMZ

All servers in the DMZ use IPSec to filter out undesired port traffic, providing yet another layer of defense in depth and protection from breaches of the firewall. Some simple examples:

- The IPSec policies on all DMZ servers would permit packets to RDP port 3389 (TCP) only from the specific GIACENT machines used by IT and R&D to administer and access the servers with a Terminal Services client.
- The Public IIS server discards all packets from the Internet, except those sent to port 80 (HTTP), port 443 (TCP and UDP for HTTPS), 8080 (HTTP alternate), or specific high-numbered ports used by a GIACENT custom application.
- The "Public" SQL server discards all packets to ports 1433 and 1434 (TCP/UDP) other than those coming from the Public IIS server or from machines on the internal network.

DNS in the DMZ

All IP addresses on all machines in the DMZ are statically assigned, and administrators manually update records on the DNS servers.

The DNS service is enabled on both Domain Controllers in the DMZ for redundancy. These DNS servers resolve addresses of only the few machines located in the DMZ network. For security purposes, DMZDC1 is set up as Standard Primary DNS server (i.e., DNS records are stored in a zone file, *not* in

Active Directory), and Dynamic Updates are disabled. DMZDC2 is configured as a Standard Secondary DNS server, with DMZDC1 designated as the authoritative (primary) server for the zone file *giacentdmz.biz.dns*. Although best practices recommend against having both DNS servers on the same network segment, the DMZ is too small to make this practical. Some redundancy was considered a step in the right direction.

Internal Corporate Network (Suburban Office)

The internal corporate network (giacent.biz) is split into subnets by the screening router internal to the firewall. This helps segregate network traffic at a workgroup level. Two domain controllers are installed for redundancy.

FSMO Roles

The FSMO roles of PDC Emulator, RID Master, and Infrastructure Master reside on the "main" DC in the suburban site. This DC is highly physically protected and audited. The Schema Master and Domain Naming Master reside on the second DC in the suburbs, which is also the designated Global Catalog server.[6]

Network Time Server

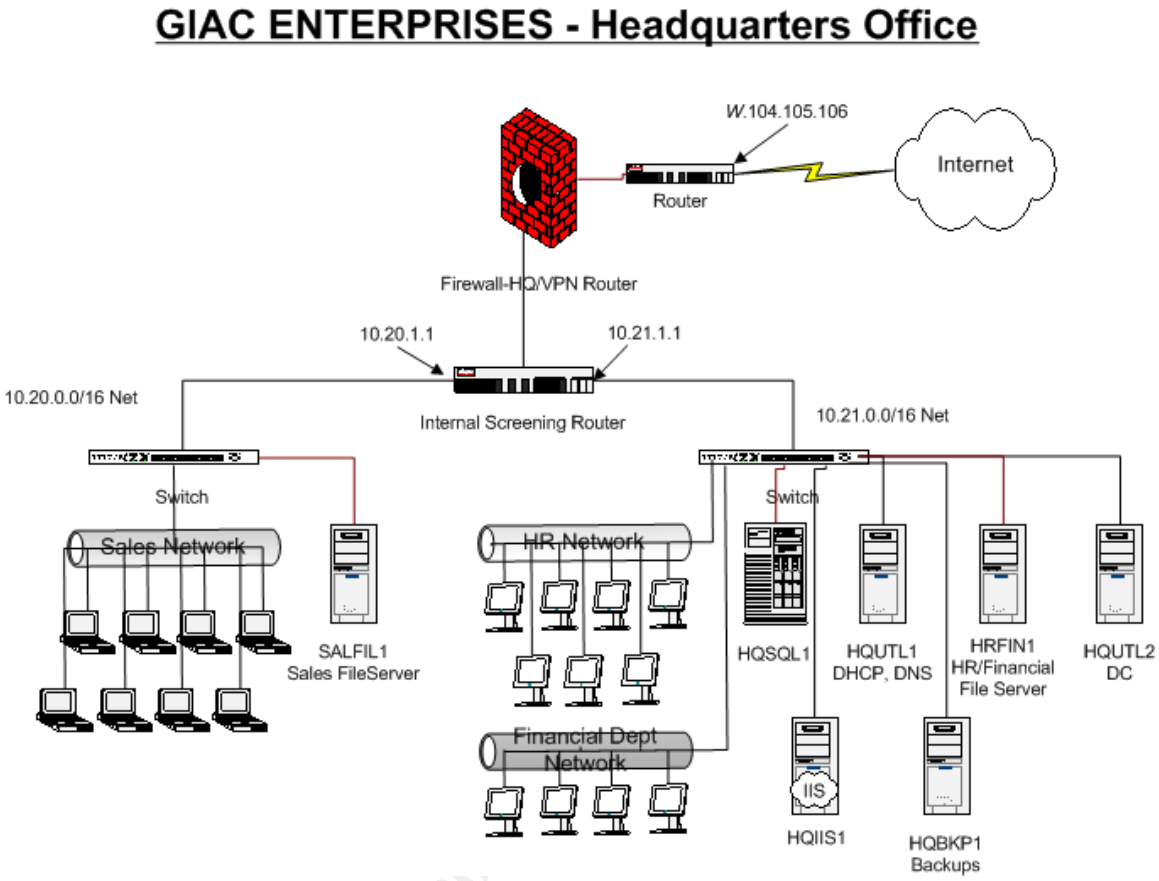
Accurate time synchronization among all machines in the domain is essential to proper functioning of Kerberos authentication. The PC Emulator in each domain is configured to sync its clock to an external NTP time server. For details see the Microsoft white paper *The Windows Time Service.*[7]

DNS in the Internal Network

In the suburban internal corporate network, the DNS servers use Active Directory integrated zones. Zone transfers are unnecessary since DNS records replicate within Active Directory. The DNS servers are configured to require secure updates. The internal DNS servers are distributed across two segments of the network for better tolerance against network or switch outages. To resolve addresses external to GIAC, the DNS servers refer requests to the ISP's DNS servers. The "Secure cache against pollution" option is set so the servers will reject extraneous data that could poison the DNS cache.[8]

[6] Fossen 5.1: 103-4.
[7] Brandolini and Green. "The Windows Time Service."
[8] Fossen 5.2: 21-30.

Network Design: Downtown HQ



The hardware used for the HQ file/print servers and the design of the HQ network represents something of a compromise between cost considerations, political pressures for each group to have “their own” server, and the fact that the small number of users doesn’t strain the hardware too heavily. Redundant local DCs and DNS servers are not required since HQ clients can also access the services from the suburban network via the VPN, albeit more slowly.

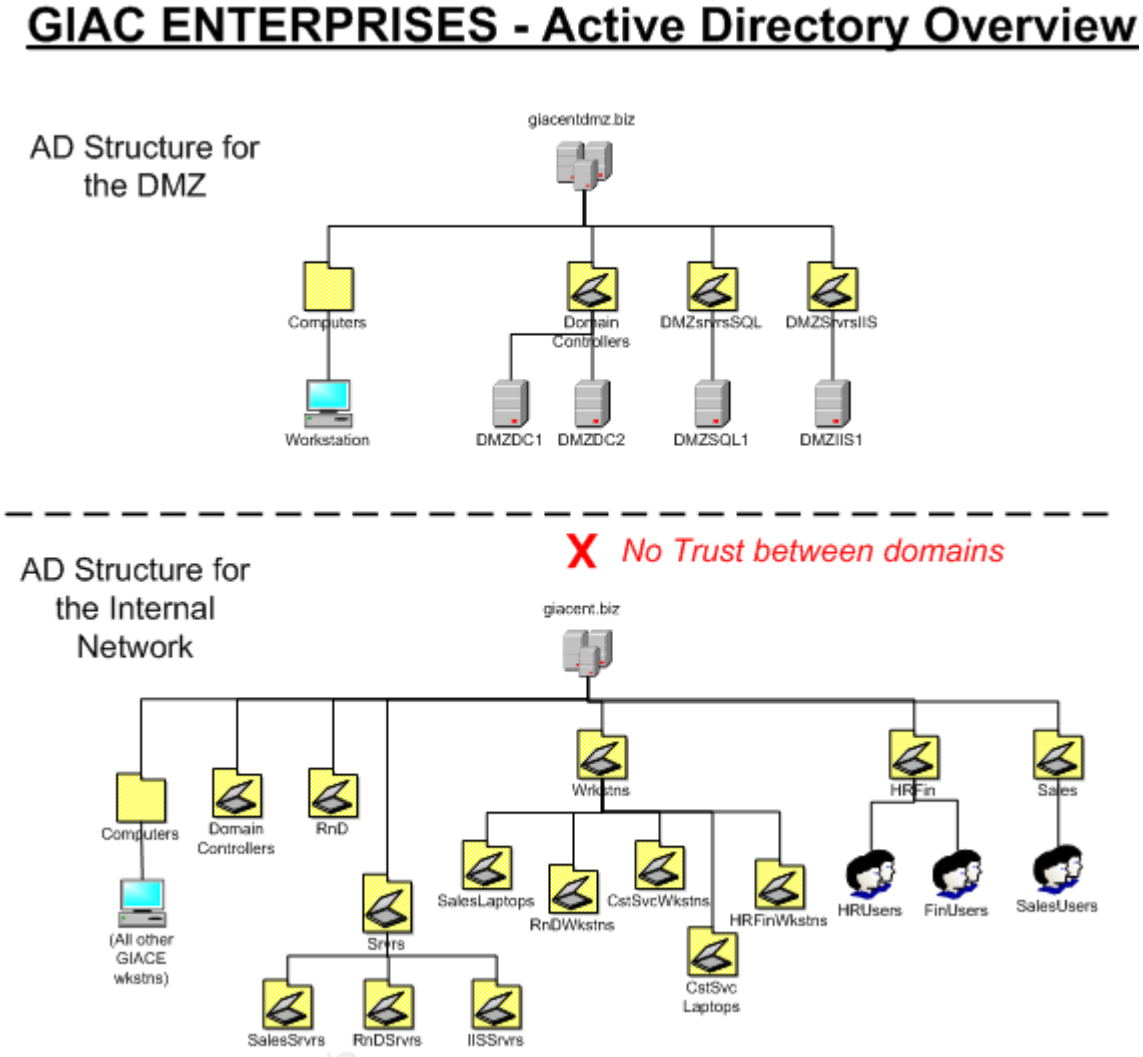
Sales information is kept on the SALFIL1 file server located in HQ. This server is located on an isolated subnet along with network connections for Sales laptop users (who are out of the office much of the time!). This isolation of the SALFIL1 subnet occurred largely for political reasons and resulted in another file server being dedicated to the HR and Finance Departments. In some ways, this has some potential technical advantages: it can simplify the configuration of IPSec rules if a particular department wanted to reject traffic from computers not on their subnet.

Sales people update client information from their laptops to the file server as soon as possible. Because some of this data may be sensitive, all GIACENT

Windows XP laptop machines have a directory on the disk encrypted with EFS. GIACENT relies on users' best judgment to determine what data merits encryption. Spot-checks by IT staff help educate EFS users with regard to data security and is perceived to help increase security awareness more than an "encrypt everything" policy would. This is a significant benefit in these times when portable CD burners are so inexpensive.

Sales people and Customer Service Staff are often out of the office but need to connect from their company-provided laptops on a regular basis. VPN client software is installed on each laptop machine. When connections are made from remote facilities via dial-up or broadband, the VPN client software authenticates to the VPN server on the appropriate GIACENT firewall and encrypts data in transit between the employee's laptop and the GIACENT office.

Active Directory Design



GIACENT's Active Directory structure consists of two AD domains with no trust between them. One domain (giacent.biz) organizes the internal network. The publicly accessible part of GIACENT's network (giacentdmz.biz) exists entirely within the DMZ.

GIACENT is a small enough company that there are no compelling technical or political reasons to have more than one domain internally. Generally, any reduction of unnecessary complexity is beneficial.

Machine configuration through group policy is accomplished through the creation of Organizational Units (OU's) as necessary. User preferences (and/or constraints) dictated for some business units can also be applied via Group Policy.

It is a preferred security practice to segregate publicly accessible portions of the network from internal portions. When GIACENT was a smaller company, a single server within the DMZ in a standalone Workgroup configuration was sufficient to present static “brochure-ware.” As GIACENT creates more of an Internet presence, additional machines have been and will be added to the public network in the DMZ to accommodate the needs of business partners and on-line customers. Once user-authentication was required on the public network, the creation of an additional domain made sense as a way to administer user accounts and rights across the multiple machines in the DMZ.

At this time, there is no trust relationship between the public AD domain and the internal AD domain. This helps protect the internal network: even if accounts are cracked on the public network, they have no connection to internal user accounts, thus limiting a hacker’s ability to penetrate the internal network. For this configuration to actually add protection, administrators create and use *different* user IDs and *different* passwords for their public (DMZ) and internal accounts. It does little good, security-wise, to have separate accounts in two domains if the credentials for the accounts are identical. This becomes a user education and account administration issue, and is a good solution so long as few GIACENT employees need authenticated access to the public domain.

In the future, one compelling reason for creating a trust between the public and internal domains would be if a number of GIACENT employees needed to access data through the public network using their own accounts. (For example, if GIACENT employees wanted to access data from an SQL database on the internal network through a public web front-end.) In such a case, it might be appropriate to create a one-way, non-transitive trust, where the public network trusts the internal network, but the internal network *would not* trust the public network. Although such a configuration is fairly standard, GIACENT is hoping to avoid having to create any trust between the two domains. Not only does maintaining totally separate domains add a measure of security, it eliminates replication of global catalog data, and may simplify a move to outsource hosting of the DMZ servers in the future if growth warrants.

Following best security practices, the domain administrator account is renamed (via Group Policy) and rarely used for actual administration. Each administrator responsible for the DMZ has a unique administrative account in the giacentdmz.biz domain to permit accurate auditing of changes. Other than these administrative IDs, the only user IDs defined in the DMZ domain are those of business partners and large customers who access data on the servers via GIACENT’s secure web site. Anonymous access to GIACENT’s public web sites is facilitated by local service accounts on the web servers.

giacentdmz.biz AD details

The few OUs in the giacentdmz.biz domain exist to help with the distribution of group policy to servers in the domain. With only four servers in the DMZ, there isn't much of a difference in the effort required to configure and deploy policies locally on each machine vs. creating Group Policy Objects (GPOs) and associating them with a given AD container. Nonetheless, OUs and GPOs were created for the following reasons:

1. Associating a GPO with an AD container assures that when future machines are added to the container, they will take on appropriate group policy settings. Positioning for future growth, linking GPOs to appropriate OUs will make the installation and security configuration of future machines more efficient.
2. Associating a GPO with an AD container helps ensure that group policy settings are applied and refreshed on each machine as expected. Even if a local policy setting is changed (accidentally or otherwise), the policy distributed via AD can override it, ensuring that settings on each machine are as intended. This gives administrators fewer places to look for errors when troubleshooting.

The OUs created in the DMZ help distribute appropriate policies for each *type* of server in the DMZ. The **DMZSrvrsIIS** OU can be used to configure settings and possibly distribute software via group policy to the IIS server(s) in the domain. Similarly, the **DMZSrvrsSQL** OU can apply policy settings and distribute software to the SQL server(s) in the giacentdmz.biz domain. Often, different types of servers (that is, servers running different applications) require different configuration settings – organizing them by type in separate OUs is one way to accomplish this.

Because there is only one workstation computer in the DMZ domain, used for I.T. administration, and GIACENT does not expect to add any more, it simply exists in the default Computers container. This container does not allow GPOs to be linked to it, so only Local, Site, and Domain policies affect it. That's sufficient.

giacent.biz AD details

The AD structure for GIACENT's internal network (giacent.biz) is designed to facilitate the deployment of group policy to machines within the company at both office locations.

For example, the **Srvrs** OU permits basic group policy settings to be applied to all servers in the GIACENT network. (For instance: renaming the local administrator accounts, and configuring uniform Event Log settings would be appropriate at this level to affect all servers.) Additional OUs help adjust additional settings that are applicable only to a subset of the servers. For example, the **IISSrvrs** OU is placed within the **Srvrs** OU to apply additional

policies specific only to IIS servers – such as specifying NTFS permissions and audit settings on the IIS MetaBase.bin file.

Similarly, a **Wkstns** OU exists to provide an easy way to apply group policy settings to all workstations in the domain. Additional policies, like an IPSec policy prohibiting Remote Connections (i.e., dial-up connections) on HR and Financial workstations would be appropriate to help ensure that users don't set up a rogue dial-up server on the network using those workstations. But dial-up connections can *not* be prohibited on the mobile laptops used by Sales or Customer Service. Therefore, additional OUs within the **Wkstns** OU permit different policy settings to target specific groups of user machines.

Group Policy and Security

Group Policy for GIACENT is based on a "keep-it-simple" trickle-down model. Group policies are applied "as high up the tree" as possible, and additional or different policies are applied to specific containers further down the tree as needed. Removing the "Read" and "Apply Group Policy" permissions for a particular security group, user, or machine on a specific group policy object (GPO) can help further fine tune its scope. As a rule of design, GIACENT avoids using the "block inheritance" and "no override" features of Group Policy.

Although Group Policy security settings can be managed through the MMC GUI, it is beneficial to customize security templates (.INF files) that can then be imported into any given GPO. This allows similar security settings to be easily applied, repeatedly, to multiple GPOs. It also documents the settings in easy to read text files. (Although the meanings of settings are often hard to understand from looking in the .INF templates!) Using .INF templates rather than manual configuration in the GUI is very useful because GIACENT uses some identical security settings in both the giacentdmz.biz (DMZ) domain and the giacent.biz (Corporate) domain.

There are three ways to create .INF files for use as security templates:

1. Start with an existing security template (.INF file) and modify it using any text editor and a good reference guide. Or,
2. Configure security settings using the Security Configuration and Analysis (SCA) MMC snap-in. This snap-in allows you to import one or more existing .INF templates into a "security database," further tweak the resulting settings via the GUI interface, and then export the new security settings to a new .INF file. Or,
3. Run the Security Templates MMC snap-in to check and modify the settings in existing templates using a GUI interface. If desired, altered templates can be saved under new .INF file names.

Note that in each case, we started with one or more existing security templates.

Where does one obtain security templates? Microsoft copies several templates into the %systemroot%\security\templates directory during Windows 2000 installation. Another source is the National Security Agency web site (http://www.nsa.gov/snac/win2k/download.htm). Both the Microsoft and NSA templates include helpful, if sparse, in-line comments.

And where does one get a good reference guide? Two of the best include *Group Policy Reference* authored by David C. Rice, and published by the National Security Agency; and the *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set* by J. Haney, also published by the NSA.

When using the Security Configuration and Analysis (SCA) snap-in to configure template files, there are a few useful techniques and caveats to be aware of:

1. You can use a text editor to separate templates into sections and save each section as a separate .INF file to make them more "granular." You can also import multiple templates into the SCA snap-in to "accumulate" settings, modify settings as desired within the GUI, and then export a "master" template that suits your needs for a particular GPO.
2. When you import templates into the SCA snap-in, you are creating and modifying a "security database." Jason Fossen, while lecturing on this topic, noted that what the SCA snap-in refers to as a "security database" is more accurately called "a temporary file that I don't care about."[9] This distinction is not readily apparent from the tool or the documentation, but it is, in fact, true. What's important is the template you ultimately export, not the "security database."
3. Settings that you modify using the SCA snap-in are not immediately available for export into a new .INF file. To export database settings you've changed, you must right-click "Security Configuration and Analysis" in the SCA snap-in, then select "Analyze Computer Now…" from the context menu that appears. After this analysis step, right-click again on "Security Configuration and Analysis" in the SCA snap-in and select "Export Template…" from the context menu. Settings that you have added or changed in the security database will be written to the .INF file you specify.
4. You can use the technique described above to "reverse engineer" policy settings applied in the GUI to see what their corresponding values are in an .INF file. This can be helpful in the face of scanty documentation.
5. When you export a template from the SCA snap-in, all comments that may have appeared in the original template(s) are lost.
6. Some settings provided in many .INF files do not appear in the GUI. Some of them (like ForceLogoffWhenHourExpire = 0) are mostly

[9] From Fossen's lecture on Group Policy and DNS, December 16, 2002, San Francisco.

undocumented.[10] Review carefully any .INF template you obtain from an outside source and proceed with due caution.

7. The Security Configuration and Analysis tool can compare settings in a given template with your current computer settings, flag differences, and configure your computer with the security settings you've accumulated. This is a great way to use templates to set Local Policy on a particular machine.
8. All these SCA procedures can also be performed from the command line (or scripted) using the SECEDIT command line tool.

Basic Group Policy Settings

Two of the most important collections of Group Policy settings in an AD domain are the **Default Domain** GPO settings and the **Default Domain Controller** GPO settings. One of the clearest and most succinct explanations of the distinctions between these two GPOs can be found in a Microsoft TechNet How-To guide, *Step-by-Step Guide to Configuring Enterprise Security Policies*. In the "Summary" section of this guide, it states:

> Account policies (password, lockout, Kerberos) are defined for the entire domain in the default domain GPO. Local policies (audit, user rights, and security options) for DCs are defined in the default DC GPO. For DCs, settings defined in the default DC GPO have higher precedence than settings defined in the default domain GPO. Thus, if you were to configure a user right (for example, Add workstations to domain) in the default domain GPO, it would have no impact on the DCs in that domain. [11]

Examining the default policies defined in these two GPOs after a fresh installation of a new domain is also an instructive exercise (and the above mentioned Guide walks the reader through it). With that background, we can begin configuring some example GPOs for each of these AD containers.

Default Domain Policy Settings

Security settings we intend to apply to all machines in the domain are best set at the domain level, in the GPO linked to the Default Domain Policy container. It's good practice to apply the bulk of settings at the Domain Level. Any similar setting applied at the OU level will override it, anyway, so setting "defaults" in the Default Domain GPO is a good way to ensure machines don't fall through the cracks.

GIACENT's Default Domain Policies in both the DMZ (giacentdmz.biz) and Corporate (giacent.biz) domains use the following settings. Remember, there is

[10] Neohapsis message archives, "Undocumented Settings in Win2k Security Templates."
[11] Microsoft, "Step-by-Step Guide to Configuring Enterprise Security Policies."

no trust between the domains, so the GPOs are created separately (but in this case equally) from customized .INF templates.

Password Policy and Account Lockout Policy
(in [System Access] portion of the security template file)

To see these settings in the Group Policy snap-in:

> Default Domain Policy → Computer Configuration → Windows Settings → Security Settings → Account Policies → Password Policy

```
[System Access]
MinimumPasswordLength = 10
PasswordComplexity = 1
MinimumPasswordAge = 3
MaximumPasswordAge = 60
PasswordHistorySize = 18
```

These settings above strike a balance between security needs and user-friendliness (or perhaps "user tolerance" is a better description). A minimum password length of 10 characters combined with the requirement for complex passwords (via PASSFILT.DLL) will hopefully encourage GIACENT's users and business partners to think in terms of complex pass phrases that are harder to crack than typical passwords. Specifying a minimum password age of three days and a large password history size should discourage virtually anyone from password cycling. It should also help discourage users from specifying the month as part of their password. Requiring passwords to be changed every 60 days is a compromise between "high security" recommendations and users' distaste for thinking of new passwords.

Navigate in the Group Policy snap-in:

> Default Domain Policy → Computer Configuration → Windows Settings → Security Settings → Account Policies → Account Lockout Policy.

```
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = 0
RequireLogonToChangePassword = 0
```

(Note that the last value does not appear in the GUI; another "lightly documented" .INF setting.[12])

LockoutBadCount (a.k.a., Account Lockout Threshold) determines how many bad login attempts will cause an account to be locked out. While the NSA *Tool Set* guide recommends a value of 3, this tends to be too strict for GIACENT users who haven't had enough coffee before attempting to log in, so we chose 5.

[12] Neohapsis message archives, "Undocumented Settings in Win2k Security Templates."

The Lockout Duration is set to 0 to require manual intervention when an account is locked out, helping to ensure that attempts to crack passwords will be flagged by an administrator.

ResetLockoutCount is set to 30 minutes to mitigate the possibility of denial of service attacks caused by password cracking attempts. Again, the philosophy is: if a valid user is having trouble logging in, an administrator should be alerted; ditto if a hacker is playing around.

The assumptions motivating the settings above may need to be revisited as the number of users of GIACENT's public web site grows in the future.

RequireLogonToChangePassword is set to 0 to avoid problems when a user attempts to change their password during their first login or after having their password reset.

Additional, non-account policy settings, appropriate for all machines in the domain are also applied to the Default Domain Policy GPO:

Logon banner and title

> Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options → Message text for users attempting to log on
>
> Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options → Message title for users attempting to log on

These GUI settings correspond to the following .INF template parameters:

```
[Registry Values]
machine\software\microsoft\windows\currentversion\policies\system
\legalnoticetext=1,This is a GIAC ENTERPRISES computer system.
Unauthorized use is prohibited and will be prosecuted.

machine\software\microsoft\windows\currentversion\policies\system
\legalnoticecaption=1,GIACENT LOGON WARNING!!
```

Although a logon banner is a small cosmetic change, displaying a proper warning banner can have important ramifications when attempting to prosecute attackers in court. Appendix A in the *NSA Guide to Securing MS Windows 2000 Group Policy: Security Configuration Tool Set* [13] contains a warning banner used by the Department of Defense that should provide good fodder for discussion among many companies' Legal and IT departments. In fact, it is probably a good idea for public web applications to display a similar banner on their login screen for authenticated users.

[13] Haney: 103.

Rename administrator and guest accounts

> Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options → Rename administrator account *and* → Rename guest account

This GUI setting corresponds to the .INF template parameter:

```
[System Access]
NewAdministratorName = "byteme"
NewGuestname = "noguestsallowed"
```

Kerberos Policy

> Default Domain Policy → Computer Configuration → Windows Settings → Security Settings → Account Policies → Kerberos Policy

```
[Kerberos Policy]
MaxTicketAge = 10
MaxRenewAge = 7
MaxServiceAge = 600
MaxClockSkew = 5
TicketValidateClient = 1
```

Neither NSA guidelines nor the example templates installed by Microsoft offer suggestions on changing these values from the settings configured by default when a server is installed. Leaving the default settings is probably a safe bet in most cases.

Auditing and Event Logs

Audit settings as specified in the NSA *Security Configuration Tool Set* [14] are suitable for most installations.

Event log settings (that is, log file sizes and what to do when they fill) require consideration before blindly accepting recommendations of the NSA guidelines. The guidelines tend towards paranoia in some cases, and may not be appropriate for all systems. For example:

> Default Domain Policy → Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options → Shut down system immediately if unable to log security audits

NSA recommends enabling this option, but this may be inappropriate for some systems. If Security Log file settings are large enough, and log is being dumped and/or cleared regularly, the only time the security log should fill is if something is really wrong (like a system is under massive attack). On a system holding critical data, automatic shutdown and the resulting denial of service may be preferable

[14] Haney: 30.

to a possible compromise of data. But maybe not if someone has to drive two hours to reboot the server.

So balance this against Event Log Settings:

> [AD container] → Computer Configuration → Windows Settings → Security Settings → Event Log → Settings for Event Logs

which allow control of log sizes and the log data retention methods (overwrite events as needed/by days/clear log manually) to determine appropriate settings.

For most GIACENT systems, limiting the Application and System log sizes to 250 MB should be more than sufficient since they are dumped daily. The Security log should be set to 500 MB for most systems.

GIACENT should specify larger Security log sizes (about 4 GB) for the IIS and SQL systems exposed in the DMZ however. (Apply different settings for this policy on the **DMZsrvrsIIS** and **DMZsrvrsSQL** OUs.) Considering the less-than-time-critical nature of GIACENT's business currently going through the DMZ servers, a breach is much worse than downtime. Specify that the logs must be cleared manually, and if the logs fill up, force a system shut down. There will be plenty of data to analyze after the system is rebooted.

Secure Channel data

> Default Domain Policy → Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options → [Secure channel options]

The Netlogon "Secure Channel" is used to transfer certificates, password information, and authentication sessions between machines.[15] It is generally considered a best practice to harden this channel as much as possible. Based on the NSA guidelines[16], we will enable the following two options on GIACENT's workstations, member servers, and DC's:

> Secure channel: Digitally encrypt secure channel data (when possible)
> HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel = 1
>
> Secure channel: Digitally sign secure channel data (when possible)
> HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel = 1

Note that these are not the *most* secure options available, but add extra security while GIACENT builds their PKI. These settings also provide a good measure of

[15] Fossen 5.1: 92-3.
[16] Haney: 54-5.

backward compatibility that could be useful if the R&D group ever needs to set up a test domain (to mimic a client installation, for example).

LAN Manager authentication level

> Default Domain Policy → Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options → LAN Manager Authentication Level
>
> HKLM\System\CurrentControlSet\Control\LMCompatibility

This registry key controls what authentication protocol is used for logons. The default method, LM, is relatively insecure, while NTLM and especially NTLMv2 protocols offer much more protection against password sniffing. Ideally, GIAC Enterprises would set this to ensure that the most secure protocol, NTLMv2, is used. Unfortunately, as both the NSA guidelines[17] and MS KB articles point out,[18] this higher level of security is incompatible with MS Cluster Services. It also means that R&D would have to install the Directory Services client on any Win 9x machines they may set up for testing purposes. Forcing NTLM2 authentication may also cause difficulties when authenticating business partner clients. Because GIAC Enterprises has plans to implement clustering on their IIS servers, the decision was made to leave this at the lowest (and most insecure) value for compatibility reasons. This example demonstrates the difficulties encountered when establishing "ideal" security policies in a non-ideal world.

Default Domain Controller Policy Settings

Since settings defined in the Default Domain Controller GPO override settings defined in the Default Domain GPO *for the domain controllers only*, we can use the settings here (for Audit Policy, User Rights Assignment, and Security Options) to tweak policies that we want to treat specially for the domain controllers.

- Default Domain Controller Policy → Computer Configuration → Windows Settings → Security Settings → Local Policies → Audit Policy → Audit Directory Service Access

Per NSA guidelines[19], one place we may want to set different policies for domain controllers is in auditing Directory Service Access. The guidelines recommend auditing failures on directory service access for domain controllers, but not on workstations or member servers (since they do not contain Active Directory data). Set this policy to audit failed access attempts.

[17] Haney: 44.
[18] Microsoft: TechNet KnowledgeBase articles 272129; 239869.
[19] Haney: 30.

Additional Group Policy Settings

Do not display last user name in log on screen

```
[Registry Values]
machine\software\microsoft\windows\currentversion\policies\system
\dontdisplaylastusername=4,1
```

This .INF entry corresponds to the GPO setting configured in the GUI by navigating as follows:

> Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options → Do not display last user name in log on screen

Rather than apply this setting across the entire domain, we use this setting in the GPOs linked to the HRFinWkstns OU only. We do so for educational reasons (though some would call them Machiavellian). Users in these workgroups tend to forget that logging on requires a password *and* a user ID. They get in the habit of sitting down at a workstation, hitting CTRL+ALT+DEL and typing in their password without ever looking at the user name displayed. IT has gotten tired of unlocking their accounts when users change machines and lock them… repeatedly.

To enforce better security awareness, we implement this policy on the machines of the workgroups that need it. (The Sales team could also benefit from this education, but their VP – one of the biggest offenders – won't stand for it.)

Redirect My Documents directory

GIACENT will apply this group policy setting to redirect the My Documents directory for *users* in the HR and Finance departments. The setting will be applied to a GPO linked to the **HRFin** container. To navigate to the setting in the Group Policy GUI:

> HRFin OU → Right click on the OU and select Properties → Click the Group Policy tab → Select an existing GPO link (or create a new one) then hit the Edit button →

In the Group Policy editor, navigate to:

> User Configuration → Windows settings → Folder Redirection → My documents
>
> Right click the My documents folder and specify the appropriate settings

For GIACENT, we will select the Basic setting (redirect everyone's folder to the same location) and for the target folder location specify the share \\HRFIN1\USERDATA\%username%.

Use Administrative Templates to Control Many Application Settings

Additional administrative templates (.ADM files) can be added to the Group Policy snap-in to control many applications including many settings in Internet Explorer, the Microsoft Office suite, etc. Administrative templates are distributed with Resource Kits for products.

To use an Administrative template in the Group Policy MMC, open the appropriate OU, then navigate to:

> Computer Configuration *OR* User Configuration >
> right-click on Administrative Templates >
> Add/Remove Templates… >
> Add… >
> browse for the .ADM administrative template of your choice

For instance, the OFFICE9.ADM file (part of the Office 2000 Resource Kit) provides a slew of settings that can be used to set defaults for numerous options, from specifying standard default document directories for MS Office apps, to disabling the "Menus show most recently used commands first" option (also known as "Personalized menus.") The latter setting is navigated to as follows:

> User configuration → Administrative Templates → Microsoft Office 2000 →
> Tools | Customize | Options → Menus show most recently used commands first

Additional Security Requirements

Any time private data is exposed to the public Internet, there is a need for auditing and additional security procedures. Even with a completely hardened operating system and a well-configured firewall, custom applications, if not carefully written, can provide hackers with access to sensitive data.

Entire books (thick ones!) exist describing security procedures that are beyond the scope of this paper, but a few practices are pertinent to GIACENT.

Security Awareness

All R&D staff have access to highly sensitive proprietary data. These are the "crown jewels" that can mean total market domination for GIACENT, or spell complete downfall if they were to get into the hands of competitors (or even the media). For that reason, security among the R&D staff is treated as the highest priority, and permeates the culture of the department. New employees are taught during orientation the importance of secure passwords, secure development practices, and policies to protect data (especially with all those CD burners

around).

Eventually, as the company grows, it might be appropriate for GIACENT to provide “Smart Cards” with proximity sensors to all R&D staff.

Dealing with the System Key

Even on highly secured systems, best practices dictate that copies of backup tapes be stored off-site for disaster-recovery/business continuity purposes. This exposes backup media to the possibility of theft. For domain controllers, theft of system backup media permits an attacker to devote potentially unlimited time and computing power to crack weak passwords, keys protecting digital certificates, etc. In order to defend against attacks on data that might arise from the theft of backup media (or a system itself), the SYSKEY.EXE utility can be used to specify where the System Key is stored.

For most systems, the default option of storing the System Key locally (on the system hard drive) is convenient and sufficient *if* the system is kept in a secured location. A password-derived System Key is probably the most secure, but requires the presence of a system administrator every time a system reboots - not a good choice if power fluctuations or software development (and debugging) makes server reboots fairly common.

A good compromise is to store the System Key on a floppy disk that is then left in the server. Configure the server to boot first from hard disk (not floppy) so the operating system will access the floppy for the System Key during boot-up. This removes the System Key from tape backups (our primary concern), and also permits a server to re-boot without administrator intervention.[20]

Installing IIS Servers

Best practices dictate moving the web server directory (Inetpub) off of the boot drive (generally C:). However, Microsoft has made this somewhat difficult. To install IIS in a non-default location, installers have two choices:

1. Build a server from scratch in unattended mode using an Unattend.txt file. In the Unattend.txt file, specify the location of the WWW and FTP roots. Other server components can also be specified when installing a server in this way.
   Or,

[20] Fossen, *5.1*: 74-75.

2. After building a server, installers can manually remove IIS components using the Add/Remove Programs applet, then manually add the IIS components back into the desired location with the command-line:

   sysocmgr /i:%windir%\inf\sysoc.inf /u:c:\IIS5.TXT

   The IIS5.TXT file (which can have any name) should at a minimum contain the lines

```
[Components]
iis_common = on
iis_inetmgr = on
iis_www = on
iis_ftp = on
iis_htmla = on

[InternetServer]
PathFTPRoot=D:\Inetpub\Ftproot
PathWWWRoot=D:\Inetpub\Wwwroot
```

Note: The iis-htmla component is the HTML web administration interface. In secure environments it is recommended to specify “iis_htmla = off”.

Additional [Components] parameters can also be specified to turn individual components off or on.

```
[Components]
fp_extensions  = off    ; Front Page extensions
iisdbg = off            ; MS Script Debugger
iisdoc = off            ; IIS doc
iis_pwmgr = off         ; Personal Web Server (for W2KPro)
iis_smtp = off          ; the SMTP service
iis_smtp_docs = off
indexsrv_system = off   ; Index server
```

Caveats:

- If the IIS5.TXT file specifies IIS directories on a non-default drive (i.e., D:) as in the example above, those directories must be created *before* running sysocmgr.
- Some components seem to install even if “off” is specified, and some combinations of parameters can cause the installed server to fail. Experimentation is advised.

After installing IIS, the IIS Lockdown tool should be run to mitigate additional IIS vulnerabilities. The IIS Lockdown wizard runs a configurable component called URLScan that makes the server reject certain URL strings. While making the server more secure, some URLScan options can also break valid applications (including in-house apps) you want to run on the server. Due care in selecting URLScan options and knowledge of the application portfolio is necessary to successfully run this tool.

Dealing with Event Logs

System Logs and Security Logs on each server are dumped to separate .CSV log files using batch files run as Scheduled Tasks on the server or on a remote utility workstation. Batch files can use the Windows 2000 Resource Kit utility **DUMPEL** and/or **DUMPEVT**, a freeware utility distributed by Somarsoft (www.somarsoft.com, also now www.systemtools.com). DUMPEVT has an advantage over DUMPEL in that it can not only dump the logs but clear them as well. DUMPEVT can also dump the DNS, File replication, and Directory Service logs.

After Event Logs are dumped, they should be moved to a central secure server location where they can be backed up nightly. Backups of log files are maintained for at least six months for possible forensics purposes.

SQL Server in the DMZ

The existence of an SQL server holding potentially sensitive data and being located in the DMZ presents some additional security challenges. While hardening SQL server and secure application development practices are beyond the scope of this paper, the following precautions can be noted:

- All sensitive customer data stored in SQL Server is encrypted so any compromise of the SQL server would yield only ciphertext.[21]
- Microsoft provides a list of steps that administrators can follow to further secure SQL Server 2000 at the "Securing SQL Server 2000" web site.[22] Some steps listed include:
  - Installing the latest SQL Server Service Pack (this particular site fails to mention that the latest OS SP and hotfixes should also be applied)
  - Use Windows Authentication Mode
  - Limit the privileges of the SQL service accounts
  - Block ports 1433/1434 at the firewall

Hotfix Management

With the large number of security patches ("hotfixes") being released, a tool to alert administrators to new patches and coordinate patch deployment is a virtual

[21] Cai, Zhenlei. "Platform Neutral and Transparent Encryption of Sensitive Customer Information." Also see Shahid Saleem's brief discussion of built-in SQL server functions to encrypt data.
[22] Microsoft, "Securing SQL Server 2000."

necessity. This author has performed evaluations of several products currently on the market for this purpose, and while specific recommendations would be inappropriate, a few general observations may help readers to make a more informed decision.

The market for hotfix management applications is relatively new. Thus, the tools are still maturing. Ideally, a product would alert administrators to new patches, help prioritize patches in terms of severity, warn of potential incompatibilities, correlate new patches that replace or post-date others, allow machine groups to be defined (e.g., IIS servers, SQL servers, test workstations, production workstations), allow patch groups to be defined (so that one set of patches could be deployed to production machines while a set of newer patches could be deployed to test machines), deploy patches *successfully* or provide warning of failed deployments, permit patch de-installation, and provide useful reporting tools for both technicians and management. In addition, the product should patch operating systems and applications, and maybe even permit deployment of custom patches (e.g. those provided by the vendor directly to a client for a specific fix). Plus, it should be easy to use. And some people will want multi-platform support, too.

With a list like that, it perhaps isn't surprising that no product I've tested meets all the criteria. Some do a very good job in many areas, but all have shortcomings. Ironically, almost every product has some great strong point not offered by the competition, but a strength has almost always been negated by equivalent weaknesses.

This author notes that some evaluations published in the industry trades have been somewhat misleading, often grading products on a feature-set checklist rather than real-world use. The testing methodology almost always reads: "Installed the product, tried it on a test network, got a feel for what it could do, rated it." This is fine as far as it goes, but it doesn't accurately represent the real-world where network connections drop, downloads get corrupted, and sixteen versions of Internet Explorer co-exist.

The good news is that vendors are leapfrogging each other constantly and adding the best features of each other's products. The bad news is that buyers must beware of product claims, since almost every vendor touts at least one feature that really "won't be ready until the next release."

In the end, weigh your own set of priorities, and give any product under consideration a thorough test in your own environment.

REFERENCES

Books and Articles Referenced

Fossen, Jason, *et. al. Track 5 – Securing Windows: 5.1 Windows 2000/XP Active Directory.* Document version 1.0. SANS Institute, 2002.

- - -. *Track 5 – Securing Windows: 5.2 Windows 2000/XP Group Policy and DNS.* Document version 1.0. SANS Institute, 2002.

- - -. *Track 5 – Securing Windows: 5.3 Windows 2000/XP PKI, Smart Cards and EFS.* Document version 7.5. SANS Institute, 2002.

- - -. *Track 5 – Securing Windows: 5.4 Windows 2000/XP IPSec and VPNs.* Document version 5.2. SANS Institute, 2002.

- - -. *Track 5 – Securing Windows: 5.5 Securing Internet Information Server.* Document version 14.5. SANS Institute, 2002.

Microsoft. *Microsoft® Windows® 2000 Guide to Unattended Setup - Answer File Parameters for Unattended Installation of the Windows 2000 Family of Operating Systems* (located on Windows 2000 install CD within the SUPPORT\TOOLS\DEPLOY.CAB file). Nov 1999.

Microsoft. *Windows 2000 Server ("Resource Kit") Deployment Planning Guide.* Redmond, WA: Microsoft Press, 2000.

Microsoft. *Windows 2000 Server ("Resource Kit") Internetworking Guide.* Redmond, WA: Microsoft Press, 2000.

Microsoft. *Windows 2000 Server ("Resource Kit") TCP/IP Core Networking Guide.* Redmond, WA: Microsoft Press, 2000.

Zwicky, Elizabeth, D., Simon Cooper, and D. Brent Chapman. *Building Internet Firewalls, 2nd Edition*. Sebastopol, CA: O'Reilly & Associates, Inc., 2000.

Web Sites Referenced

Brandolini, Shala and Darin Green. "The Windows Time Service." Microsoft Corporation. April 2001. http://www.microsoft.com/windows2000/docs/wintimeserv.doc (22 May 2003)

Cai, Zhenlei. “Platform Neutral and Transparent Encryption of Sensitive Customer Information.” http://www.15seconds.com/issue/030310.htm. (23 May 2003).

Haney, J. “Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set” *Windows 2000 Security Recommendation Guides*. <http://www.nsa.gov/snac/win2k/guides/w2k-3.pdf> Version 1.2. Fort Meade, MD: National Security Agency. 3 December 2002 (Document collection updated 5 Mar 2003.) (29 May 2003)

Hill, Brett. “Upgrading to IIS 5 Installing IIS 5 to a Custom Location.” IIS Answers. <http://www.iisanswers.com/articles/Upgrading_to_IIS5/Changing_IIS5_install_location.htm>. 2000. (27 May 2003)

Microsoft, “Securing SQL Server 2000.” http://www.microsoft.com/sql/techinfo/administration/2000/security/securingsqlserver.asp. 14 February 2003. (23 May 2003).

Microsoft. “Step-by-Step Guide to Configuring Enterprise Security Policies.” From the TechNet collection under *Products & Technologies* > *Windows 2000 Server* > *How-To Resources*. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/howto/entsec.asp. 2003. (28 May 2003)

Microsoft. “Windows 2000 Server How-Tos.” http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/howto/admhow.asp. 2003. (28 May 2003)

Microsoft TechNet KnowledgeBase articles (“Q” articles):

272129: Cluster Service Does Not Start on "Joining" Node in Windows 2000 Cluster. <http://support.microsoft.com/default.aspx?scid=kb;en-us;272129>. 11 April 2003. (25 May 2003)

310356: HOW TO: Prevent Mail Relay in the IIS 5.0 SMTP Server in Windows 2000. < http://support.microsoft.com/default.aspx?scid=kb;en-us;Q310356&sd=tech>. 26 October 2002. (26 May 2003)

239869: How to Enable NTLM 2 Authentication. <http://support.microsoft.com/default.aspx?scid=kb;EN-US;239869>. 9 April 2003. (23 May 2003)

259671: How to Change the Default Installation Paths for FTP and the Web < http://support.microsoft.com/default.aspx?scid=kb;en-us;259671>. 15 August 2002. (24 May 2003)

285172: Schema Updates Require Write Access to Schema in Active Directory. <http://support.microsoft.com/default.aspx?scid=kb;EN-US;285172> 11 October 2002. (23 May 2003)

Neohapsis message archives. “Undocumented Settings in Win2k Security Templates.” <http://archives.neohapsis.com/archives/sf/ms/2001-q3/0454.html> 8 August 2001. (28 May 2003)

Rice, David C. “Group Policy Reference” *Windows 2000 Security Recommendation Guides*. <http://www.nsa.gov/snac/win2k/guides/w2k-4.pdf>. Version 1.0.8. Fort Meade, MD: National Security Agency. 2 March 2001 (Document collection updated 5 Mar 2003.) (28 May 2003).

Saleem, Shahid. (Brief discussion of using built-in SQL server functions to encrypt data). http://www.developersdex.com/gurus/articles/106.asp. (23 May 2003)

SystemTools.com. DUMPEVT utility. <http://www.somarsoft.com> (also <http://www.systemtools.com>). (24 May 2003)

Walker, William E. IV. “Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0®”. *Windows 2000 Security Recommendation Guides*. <http://www.nsa.gov/snac/win2k/guides/w2k-14.pdf>. Version 1.3.1. Fort Meade, MD: National Security Agency. 4 March 2002. (Document collection updated 5 Mar 2003.) (28 May 2003).

Last Updated: October 19th, 2017

Upcoming Training

San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
Univ. of California - SEC505: Securing Windows and PowerShell Automation	**Los Angeles, CA**	**Jan 29, 2018 - Feb 03, 2018**	**vLive**
Southern California- Anaheim 2018 - SEC505: Securing Windows and PowerShell Automation	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**vLive**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS Security West 2018	**San Diego, CA**	**May 11, 2018 - May 18, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**