Global Information Assurance Certification Paper

Designing a Secure Windows 2000 Infrastructure

Practical Assignment Version 3.0
Option 1

Lenny Zeltser

Submitted April 2002
to fulfill GIAC GCWN requirements

This document analyzes security infrastructure of a fictitious company called GIAC Enterprises. Any similarities to an actual company or computing environment are purely coincidental.

Table of Contents

Section 1: Network Design and Diagram

1.1 Overview of the Corporate Network

GIAC Enterprises derives the majority of its revenue from online sales of fortune cookie sayings. The company employs a staff of approximately fifty people. Its core application, the e-commerce fortune-selling system that interacts with the customers, suppliers, and partners, is housed at a physically separate site, and is maintained independently of the corporate network. This separation was established to allow GIAC Enterprises to tailor to specific needs of each environment, taking into account differences in design and maintenance requirements between e-commerce and corporate infrastructures. This document describes design considerations for the corporate infrastructure of GIAC Enterprises, which hosts the publicly accessible Web and mail services, along with internal systems used by the company's employees to conduct business. Figure A presents the overview of the corporate network.

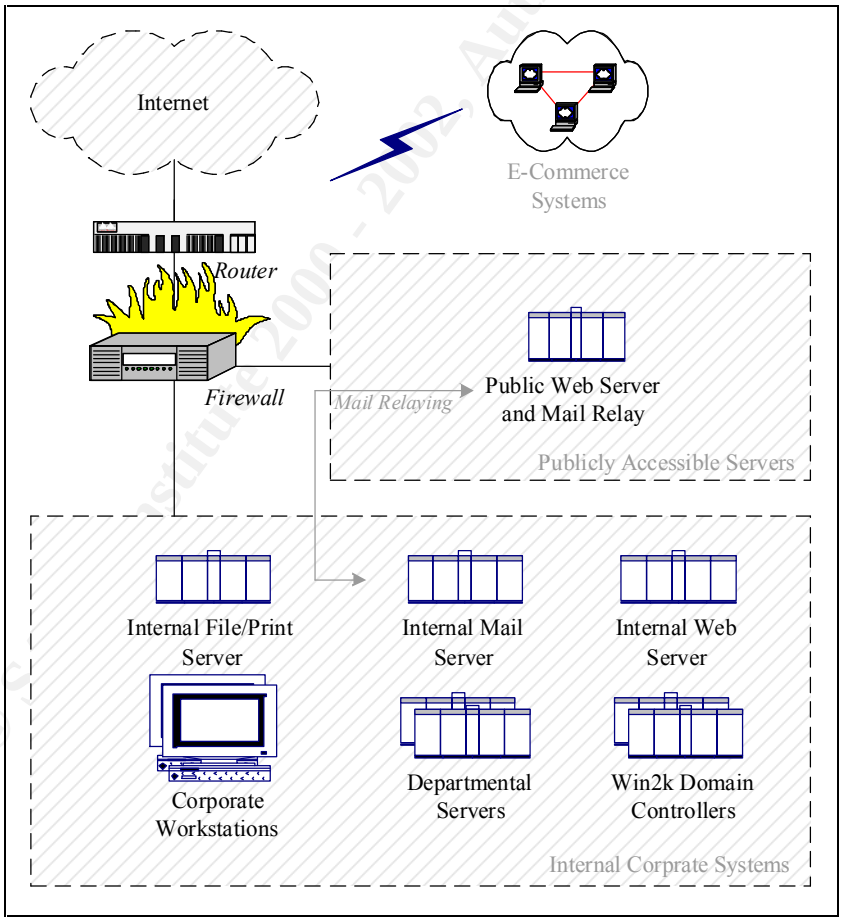

Figure A – Overview of the Corporate Network

Core networking equipment, such as switches, the border router, and the border firewall, is implemented on the corporate network using Cisco hardware. Using primarily a single vendor for the its corporate networking equipment, helps GIAC Enterprises control the number of network experts on its staff, and makes it easier for the company to handle the vendor relationship and equipment provisioning processes. The company uses the following network devices on the corporate subnets:

- Cisco 3660 router
- Cisco PIX 515 firewall
- Cisco Catalyst 2980 switches

Similarly, the GIAC Enterprises purchases the majority of its servers and workstations from Dell. The company obtained Dell PowerEdge 6450 servers, with appropriate amounts of disk space and RAM. All servers were supplied with a RAID Controller card.

1.2 Publicly Accessible Services

GIAC Enterprises uses a screened subnet, connected to the third interface of the border firewall, to host all corporate services that are directly accessible from the Internet. This configuration isolates systems that are most vulnerable by placing them on a dedicated subnet. According to the company's security policy, no system on the internal subnet may be directly accessible from the Internet. At the present time, only a single corporate server is needed to provide services to Internet users. This server runs Windows 2000 Service Pack 2 and provides the following Internet-accessible services:

- **Public Web Services** – The publicly accessible Web server located on the screened subnet is used primarily for marketing and informational purposes, and does not house the e-commerce application that resides on a separate site. The public Web server runs Internet Information Server (IIS) version 5.0.
- **Mail Relay Services** – The mail relay functionality is implemented using SMTP services build into IIS 5.0, and runs on the same system as the company's public Web server. The mail relay is responsible for proxying e-mail messages sent to and form the GIAC Enterprises employees by interacting with the company's internal mail server.

The IIS server uses a built-in RAID Controller card to implement RAID level 1 (mirroring) in hardware for the operating system and data partitions. RAID level 5 is not used because disk space requirements for the server's data are relatively small, and the company does not mind spending additional space on mirroring disks.

The company's Internet Service Provider (ISP) hosts DNS records for Web and mail services that need to be accessible from the Internet, eliminating the need for GIAC Enterprises to run its own publicly accessible DNS server.

1.3 Internal Services

The company's internal network houses servers and workstations for corporate users that fall into the following categories, according to the nature of their jobs:

- **Research and Development**, responsible for developing the bulk of the company's technology and intellectual property.
- **Sales and Marketing**, interfacing with the company's existing and potential customers.
- **Finance and Human Resources**, managing the company's finances and employee records.

Since its inception, GIAC Enterprises has housed all systems that are not accessible from the Internet on a single network. However, the company is beginning to proceed with segmenting its internal network according to differences in sensitivity of its resources. Specifically, GIAC Enterprises determined that hosts belonging to the Research and Development department contain the most sensitive data. As a result, servers and workstations used by this department have been separated from other internal systems through the use of a dedicated traffic-filtering device.

The company wanted to retain "flat" address space on its internal network to ease the transition, and elected to use the Hogwash packet-filtering device, which operates as a Layer 2 bridge and does not split the internal network into different subnets. Instead of enforcing a preset rulebase like a firewall, Hogwash blocks only packets that match a signature of a known attack. The device is able to support the throughput of 100 Mbps and does not introduce significant network latency to the LAN.[1] The segmentation of the company's internal systems is illustrated in Figure B.

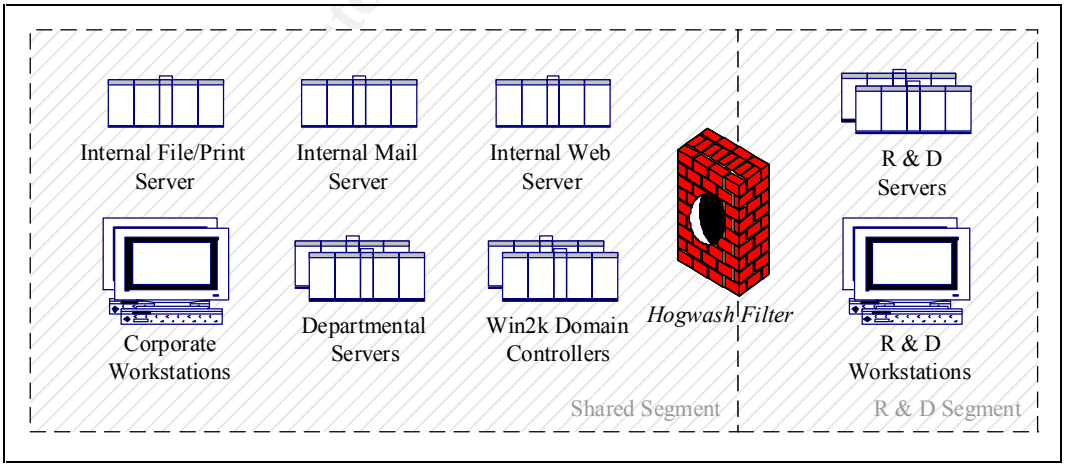

Figure B – Internal Corporate Network Segments

All servers and workstations on the company's internal network run Windows 2000 Service Pack 2, and system administrators have taken care to apply the necessary security-related operating system and application patches. Servers used as Windows 2000

domain controllers also provide domain name resolution services for all internal hosts via DNS services integrated into Windows 2000 Active Directory (AD).

The internal mail server runs Microsoft Exchange 2000, and uses the mail relay located on the screened subnet as its "smart host" when communicating with mail servers on the Internet. Files belonging to the company's internal users are stored on departmental servers, as well as on a shared central file server, which also dubs as the print server. The file server's operating system is installed on partitions mirrored through the use of a RAID Controller card; partitions that store user data are configured to use hardware-based RAID level 5. The central file server is also attached to a tape backup unit, and the company uses ARCserve Backup to backup the central file server and other servers.

Individual workstations are not backed up to tape, and users are encouraged to store data on the central file server or on departmental servers. A significant number of internal applications used by the company is Intranet-based. These applications are hosted on the internal Web server, and are accessed by internal users via Internet Explorer 6.0. All workstations are also equipped with the following Microsoft Office 2000 applications, which are routinely used by GIAC Enterprises employees to conduct business:

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint

Workstations in the Research and Development department as also equipped with Microsoft Access. All servers and workstations run Norton AntiVirus 2000 Corporate Edition, and use the LiveUpdate mechanism, built into Norton AntiVirus, to ensure that virus signatures are routinely refreshed.

1.4 Network Border Access Restrictions

GIAC Enterprises has configured its border router to perform basic egress and ingress traffic filtering, to block out packets that are spoofed or are clearly invalid:[2]

- Packets from private RFC 1918 and other reserved addresses
- Packets from localhost and unallocated addresses
- Packets from broadcast and multicast addresses
- Packets with source IP address set to all zeros
- Packets that use the company's internal network's source addresses

Blocking these packets at the router does not require much processing overhead, and carries the advantage of stopping them as close to the network's edge as possible. The company decided to leave the rest of border access enforcement up to the firewall, so that the router's hardware is dedicated to routing. This setup also eases the process of monitoring access violations, because it allows administrators to focus on observing logs from a single device.

The firewall is configured so that all packets originating from the Internet and targeting systems on the internal corporate network are blocked. The firewall only allows packets from the Internet to the Web and Mail Relay server that is located on the screened subnet, and only if these packets are destined to TCP ports 25 (SMTP) and 80 (HTTP). The PIX firewall, used to enforce these access restrictions is a stateful filtering device. This means that no explicit rules need to be created to allow responses to these SMTP and HTTP packets to leave the screened subnet. The only rule that needs to be created in the Internet-bound direction is one allowing the Web and Mail Relay server to access the ISP's DNS servers on TCP and UDP ports 53. This is needed to allow the mail relay to direct corporate e-mail messages to appropriate mail servers on the Internet. All other traffic that attempts to leave the screened subnet for the Internet is denied.

Outbound access from the internal corporate network to the Internet is restricted so that only traffic that matches explicitly allowed protocols is able to leave the network. Only the following protocols are authorized to leave the corporate network for all addresses on the Internet:

- FTP, HTTP, HTTPS
- Real-Time Streaming Protocol (RTSP)
- Telnet, SSH

Additionally, the company's domain controllers are allowed to send DNS packets to the ISP's DNS servers. This is because the domain controllers act as internal DNS servers, and are configured to forward queries for domains, for which they are not authoritative, to the ISP's servers.

The firewall also enforces access controls for traffic traveling between the internal corporate network and the screened subnet. Packets that originate from the screened subnet are not allowed to target the internal network, with the exception of the public Web and Mail Relay server forwarding e-mail to the internal mail server via TCP port 25. All systems on the internal corporate network are allowed to initiate connections to the public Web and Mail Relay server's TCP port 80, to access the corporate public Web site. Additionally, the internal mail server can initiate connections to the public Web and Mail Relay server's TCP port 25 when relaying e-mail to systems on the Internet.

GIAC Enterprises uses IPSec to authenticate administrative traffic when maintaining the public Web and Mail Relay server via SMB. This allows the company to transport all SMB-related traffic through the firewall without opening multiple ports. Instead, because the company decided to use AH for such purposes, the firewall allows the following traffic from the internal corporate network to the public Web and Mail Relay server:

- UDP port 500 for negotiating connections via IKE
- IP protocol 51 for AH packets

The next section of this document discusses the configuration and design of the company's Active Directory infrastructure.

Section 2: Active Directory Design and Diagram

2.1 High-Level AD Structure

Network resources of the company's corporate network belong to the same AD site. This physical aggregation of resources meets the needs of GIAC Enterprises, since all corporate servers and workstations are located in the same facility, and reside on a high-speed (100 Mbps) network. GIAC Enterprises organized all its internal corporate resources into a single Windows 2000 domain, since it had no political or network reasons to create internal replication boundaries. The company employs two domain controllers, which, considering its number of employees offers sufficient performance. Domain controllers have been very stable. GIAC Enterprises believes that it has achieved sufficient redundancy by deploying two servers, and cannot presently justify deploying a third domain controller. The company created several organizational units (OUs) in the Windows 2000 domain to match its administrative practices and security needs, as discussed in the following section.

The publicly accessible IIS server, located on the screened subnet, is configured as a standalone system, and is not a member of the internal Windows 2000 domain. GIAC Enterprises established that there is no reason to integrate the server with its internal domain because there is no business need to authenticate remote users against the internal domain, and the server does not need to communicate with back-office systems such as application and database servers. The company may consider creating an isolated domain for servers in the screened subnet once it hosts more than a single system there, to take advantage of Group Policy distribution mechanisms. At this point, however, the server is maintained individually.

2.2 Organizational Units

GIAC Enterprises segmented its AD structure into several OUs, to accommodate the delegation of administrative tasks and differences in security requirements of domain resources. The company's AD hierarchy reflects the following business needs:

- User accounts, workstations, and servers differ in security requirements, as prescribed by the company's security policy, due to fundamental differences in which these entities contribute to the company's business.
- The Research and Development department has its own system administrators that oversee operation of resources that belong to that department. Security policies for Research and Development user accounts, workstations, and servers differ from policies that apply to resources in other departments.
- Resources belonging to other departments are maintained by the company's global IT group, which has authority to override decisions made by Research and Development system administrators.

Figure C represents the AD hierarchy implemented at GIAC Enterprises. The company has several divisions that are not directly represented in the AD hierarchy – the Sales and Marketing, and the Finance and Human Resources departments. These groups were not assigned individual OUs because they are maintained by the global IT group, and do not require specific delegation rights. Additionally, security requirements for workstations and servers belonging to these departments are not significantly different from requirements for other resources in the company, with the exception of the Research and Development department. Dedicating an OU to the Research and Development department allows GIAC Enterprises to grant the department relative independence over the configuration and management of its resources. Additionally, company-wide Domain Controllers are located in a dedicated OU, to ease the task of configuring them through the use of a specialized Group Policy.

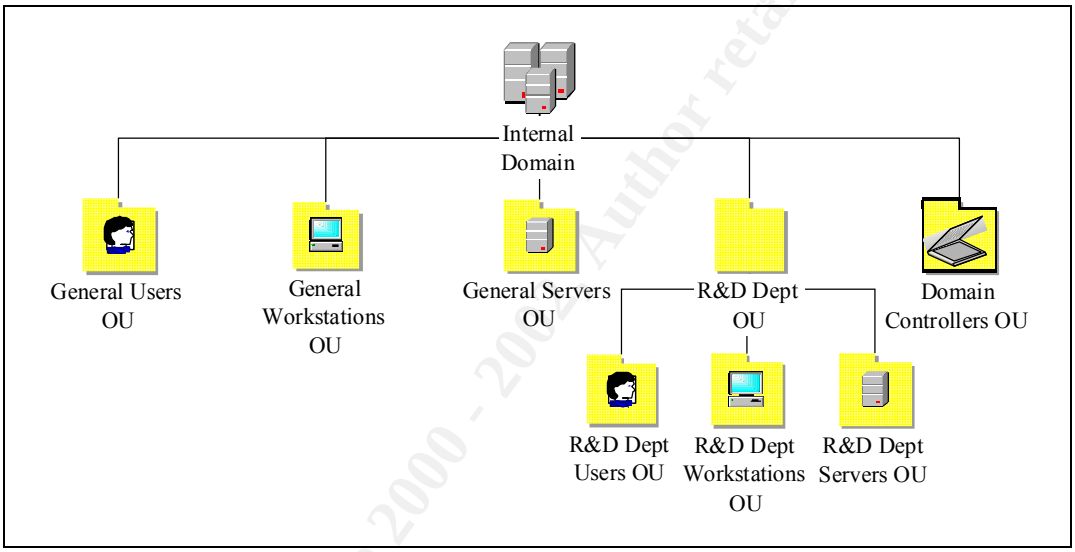

Figure C – AD Hierarchy at GIAC Enterprises

Company-wide system administrators belong to the Domain Admins group, and are able to manage resources in all branches of the AD hierarchy. System administrators from the Research and Development department are members of the local security group that has Full Control permissions to the R&D Dept OU; this gives them the ability to manage resources that belong to their department. The company decided to add members to the local group directly, instead of putting them into a global security group and then adding the global group to the local group, because there are only two system administrators in the Research and Development department. Creating a global group for this purpose would unnecessarily complicate the permissioning structure, considering that the company is relatively small.

Additionally, GIAC Enterprises has two Help Desk representatives that help troubleshoot end-user problems with workstations and applications used within the company. These staff members belong to the local security group that was created to allow Help Desk representatives to reset user passwords. The local group was granted the right to reset (but not change) the password for General Users as well as R&D Dept Users containers, since a single Help Desk group services all departments at GIAC Enterprises.

GIAC Enterprises also granted its Help Desk representatives the ability to enable user accounts that were locked. The company's policy allows Help Desk staff members to exercise this ability when they determine that an account was wrongfully auto-locked out. To be able to delegate this right, the company's system administrators manually edited the dssec.dat file to change the value assigned to the `lockoutTime` entry from `7` to `0` in the `[user]` section of the file.[3] This allowed administrators to use the Delegation of Control Wizard to delegate `lockoutTime` permissions as shown in Figure D to the appropriate local security group.

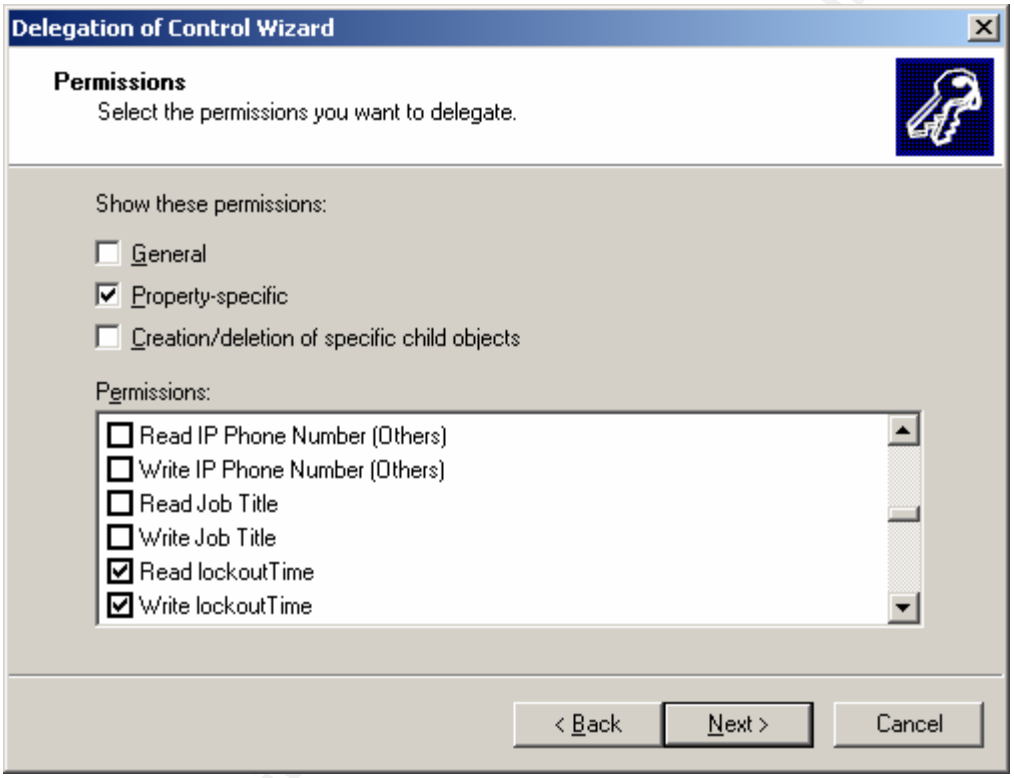

Figure D – Delegating the Ability to Unlock User Accounts

Section 3: Group Policy and Security

3.1 The Use of Security Templates

To facilitate consistent application of security settings to Group Policy Objects (GPOs) throughout the company's AD hierarchy, GIAC Enterprises uses Security Templates for initializing its GPOs. Security Templates allow the company to maintain a clear trail of security settings that are applied to members of its domain. Furthermore, whenever a new Group Policy needs to be created, perhaps when the company determines a need for a new OU with its own GPO, system administrators can use existing templates as the basis for defining security settings of the new GPO.

The company used a set of Security Templates created by the NSA as the basis for its own Security Templates.[4] The company then customized NSA's templates according to business needs specific to GIAC Enterprises. The templates were renamed and then modified through the use of the Security Templates snap-in to the Microsoft Management Console (MMC). As a result, the company presently maintains the following Security Templates, which it used to define GPOs for respective OU containers in its AD hierarchy:

- **giac_domain.inf** – Used for the Default Domain GPO
- **giac_dc.inf** – Used for the Default Domain Controller GPO
- **giac_pub_server.inf** – Used for the Local Policy applied to "public" servers
- **giac_server.inf** – Used for GPOs that apply to member servers
- **giac_workstation.inf** – Used for GPOs that apply to workstations

When configuring a GPO, the company's administrators import the most appropriate Security Template into the Security Settings branch of the object, and then customize the policy if its needs differ from settings defined in the template.

3.2 Settings for the Domain

GIAC Enterprises uses the giac_domain.inf security template as the basis for defining the Default Domain GPO. This template, and the resulting Group Policy, contains settings that are likely to apply to all resources within the GIAC Enterprises domain. The Default Domain GPO defines settings that should apply to users throughout the company's AD hierarchy. Therefore, GIAC Enterprises marked the Default Domain GPO as "No Override," to prevent other GPOs from overwriting settings that it defines. Account policies defined by the template for this policy are listed in Table I.

Setting Name	Setting Value
Enforce password history	10 passwords remembered
Maximum password age	90 days
Minimum password age	5 days
Minimum password length	10 characters
Passwords must meet complexity requirements	Enabled
Account lockout duration	120 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout after	15 minutes

Table I –Account Settings for the Domain Group Policy

GIAC Enterprises uses this GPO to encourage users to pick passwords that are not easily guessable. By enabling the "complexity requirements" setting, the company activates passfilt.dll functionality included with Windows 2000. This filter enforces the following rules, as described in the MSDN Library:[5]

- The password cannot contain portions of the user's login name.
- The password must be at least six characters long.
- The password must contain characters from at least three of the following categories: upper case, lower case, number, and non-alphanumeric.

The company requires that its users change passwords at least every 90 days. Requesting users to change passwords more often would most likely result in the users writing passwords down near their workstations, or attempting to bypass password complexity requirements in hopes of electing easy to remember, or sequentially predictable passwords. To prevent users from temporarily changing a password as required, and then resetting it back to the previous value, the company requires that the password be in use for at least 5 days before it can be changed again. It the company's expectation that after 5 days users we get used to the new password and not have the urge to reset it to the previous value.

The Group Policy is set up to automatically lock accounts for 2 hours after 3 invalid logon attempts, to limit brute-force password attacks. In establishing this policy, the company assessed the danger of denial of service attacks associated with a malicious user purposefully trying to login as the other user with the intention of locking him or her out. To mitigate the risk of an employee loosing work time due to a lockout, the company's Help Desk representatives have the ability to unlock accounts. During off-hours, employees rely on the system's ability to automatically unlock the account after 2 hours. The threat of malicious lockout would have been greater if users on the Internet had the

ability to attempt to authenticate against the domain's user database; however, at the present time, the company does not expose its internal authentication mechanism to external networks.

Another set of policies defined at the domain level belong to the category of Security Options and are presented in Table II. One of the settings enforced by this policy is ensuring that users are required to press the CTRL+ALT+DEL key combination when logging on to systems. Although some users, having worked with Windows 98/Me initially complained about this requirement, the company's management decided that the ability of this key combination to help screen out trojanized login programs was worth the potential inconvenience to the company's users. Another inconvenience bestowed upon users with this policy is the requirement that the last user name not be displayed on the logon screen. This setting makes it more difficult for an attacker to succeed at guessing valid logon credentials, because he or she would need to know a valid user name as well as a password.

Setting Name	Setting Value
Automatically log off users when logon time expires	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Do not display last user name on logon screen	Enabled
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Message title for users attempting to log in	Security Warning
Message text for users attempting to log in	This computer system and data stored therein is the property of GIAC Enterprises. Access to this system is granted to authorized users only. All actions on this system may be monitored and recorded by the company's system administration staff.

Table II – Security Options for the Domain Group Policy

In addition to controlling how users log on, and what security warnings they are presented with, this aspect of the domain-wide Group Policy helps ensure that unauthenticated connections are denied access unless anonymous connections are explicitly allowed. The company tested its applications before limiting access privileges

of anonymous connections, and determined that existing applications continue to function with this restriction enforced throughout the domain.

The company's legal advisor provided a warning banner that is displayed when users attempt to logon to the organization's systems from the console. This text makes it clear who owns the system, and states that access is restricted to authorized users only; this is established in order to support the litigation process, should the company find itself in court over unauthorized access to its systems. Additionally, the message clarifies that users of the system have no expectation of privacy, because the system and its data belong to the company; this is established to allow the company's administrators to monitor systems for malicious activity.

When implementing the domain-wide Group Policy based on this Security Template, GIAC Enterprises also placed restrictions on the membership of several highly privileged security groups. The company decided not to implement these restrictions in the template itself, so as not to hard-code names of administrators authorized to belong in these groups. Membership for the following groups is restricted through the use of the domain Group Policy to implement another layer of defense against unauthorized administrative access to domain resources:

- Enterprise Admins
- Schema Admins
- Domain Admins
- R&D Dept Admins

The Default Domain GPO also uses the Administrative Templates section of the Group Policy to set Windows File Protection scanning to occur during startup. This helps ensure that critical system files are not accidentally or maliciously replaced. Windows File Protection functionality is sufficient to protect core files on workstations. However, the company decided that it needed additional control over monitoring changes to the files system of its servers. As a result, the company selected Winalysis software (www.winalysis.com) for monitoring the files system, registry, and other settings of its servers. The company also considered using Tripwire for Windows to detect changes to its servers, but favored Winalysis because of budget limitations. The organization's policy mandates that all servers running on its domain have Winalysis agents installed, in addition to having Windows File Protection activated.

Additional security-related settings for the company's domain resources are defined in GPOs assigned to other OUs, as described in subsequent sections.

3.3 Settings for Domain Controllers

GIAC Enterprises uses the giac_dc.inf security template as the basis for defining the Group Policy that is associated with the Domain Controllers OU. Note that certain Group Policy settings that apply to Domain Controllers are inherited differently than those that

apply to regular member servers. Specifically, the following attributes apply to Domain Controllers only if the Group Policy is linked to the domain container:[6]

- Settings in the Account Policies of the GPO, some of which were listed in Table I.
- Auto-logoff Security Options settings, which were described in Table II, as well as new names for administrator and guest accounts if they were renamed.

When applying Group Policy to Domain Controllers, AD does not allow individual OUs to overwrite these settings because they have to be uniform for all Domain Controller servers in the domain. Microsoft enforces these restrictions to accommodate situations where Domain Controllers are located in different OUs. In the GIAC Enterprises domain, both Domain Controllers are in a single OU; however, they still obtain these Security Policy settings from the Default Domain Policy.

The company's Domain Controller template, along with the matching GPO, defines the Audit Policy to keep track of significant system and user-related events, as described in Table III. Whenever possible, GIAC Enterprises attempted to audit both success and failure of these events; however, logging success outcomes for some events would have produced too much output. As a result, some events only log failed actions. No auditing takes place for process-related events, since even failed process tracking events would produce too many events for process-related activities.

Setting Name	Setting Value
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Failure
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	None
Audit system events	Success, Failure

Table III – Audit Settings for the Domain Controllers Policy

Additionally, the company uses the Security Template as the basis for defining user rights assignment enforced by the Domain Controller GPO. Some of the rights limited only to Administrators are listed in Table IV. The template also assigns the "Bypass traverse checking right" to Authenticated Users, and the "Access this computer from the network" right to Administrators, Authenticated Users, and Enterprise Domain Controllers. GIAC

Enterprises obtained these settings from NSA's templates, and did not see a need to change them to better suite the company's environment.

Modify firmware environment values	Take ownership of files or other objects	Force shutdown from a remote system	Enable computer and user accounts to be trusted for delegation
Increase scheduling priority	Profile system performance	Backup files and directories	Profile single process
Shut down the system	Manage auditing and security log	Change the system time	Log on locally
Load and unload device drivers	Restore files and directories	Create a pagefile	Increase quotas

Table IV – User Rights Assigned to Administrators by the Domain Controller Policy

Other settings that the company incorporated into its Domain Controller template and GPO fall under the category of Security Options. Some of these are listed in Table V, which presents a screenshot taken while reviewing the Security Template using MMC. Some of the settings defined by this policy aim at increasing resiliency against attacks that take place physically near the server, for example, controlling who can eject removable NTFS media, and requiring that the user be logged in before issuing a shut down command. To ensure that memory contents are not available to attackers through the examination of the pagefile, the policy clears the file when the server shuts down.

Setting Name	Setting Value
Allow server operators to schedule tasks	Disabled
Allow system to be shut down without having to log on	Disabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	30 minutes
Audit the access of global system objects	Enabled
Audit the use of Backup and Restore privilege	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 on logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2
Number of previous logons to cache	0 logons

Table V – Security Options for the Domain Controller Policy

Security Options for the Domain Controller GPO are set up to allow auditing of the use of Backup and Restore privileges. This option operates in conjunction with the "Audit privilege use" setting defined in Table III. Additionally, the server is configured to disconnect SMB sessions after 30 minutes of inactivity. The setting to digitally sign communications when possible refers to the system's SMB signing capabilities, first introduced in Windows NT – it allows the system to digitally sign its SMB communications to prevent certain man-in-the-middle attacks. Actively using SMB signing may cause a performance drop of up to 15%; however, GIAC Enterprises is willing to sacrifice this performance for added security of internal SMB communications.[7]

Finally, this portion of the Group Policy requires the use of NTLMv2 for authenticating non-Windows 2000 clients to the server, which is stronger than LM and NTLMv1 mechanisms. However, this setting lacks particular significance for GIAC Enterprises because all of its corporate systems run Windows 2000 and support the use of more reliable Kerberos-based authentication mechanisms.

The configuration of the Settings for Event Logs portion of the Security Policy, presented in Table VI, describes the log rotation and access policy. GIAC Enterprises established a 500MB limit per application, security, and system log files. The company deems that this size is sufficient to capture events, and enforcing this limit helps ensure that the file system does not overflow. The company also uses this policy to automatically overwrite log files when they reach the maximum allowed size. It would have been perhaps more reliable to manually rotate the logs, however, the company did not think its administrators will have the time to perform these duties. Instead, GIAC Enterprises had purchases a log archival system called Event Log Monitor (www.tntsoftware.com), which automatically incorporates logs into a dedicated database for archival and report generation purposes.

Setting Name	Setting Value
Maximum application log size	500 MB
Maximum security log size	500 MB
Maximum system log size	500 MB
Restrict guest access to application log	Enabled

Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retention method for application log	As needed
Retention method for security log	As needed
Retention method for system log	As needed
Shut down the computer when the security log is full	Disabled

Table VI – Settings for Event Logs for the Domain Controller Policy

The Security Template and the resulting GPO are also configured to lock down sensitive portions of the registry, replacing overly permissive access controls. In this case, GIAC Enterprises explicitly followed recommendations from NSA's Security Template, and found them to be workable for its own systems. Some of the critical registry keys that are recursively locked down through the use of this policy are listed below:

- CLASSES_ROOT
- machine\software
- machine\system
- machine\system\controlset001 – controlset010
- users\.default

The template grants access to these registry keys only to principals listed in Table VII. This security policy also accounts for some sub-keys of the registry to be excluded from having these restrictions applied to them. These special considerations are not presented here for the sake of brevity; however, they can be obtained by examining NSA's w2k_dc.inf template using MMC's Security Templates snap-in.

Principals	New Privileges
Administrators	Full Control
Authenticated Users	Read, Execute
CREATOR OWNER	Full Control (subkeys only)
SYSTEM	Full Control

Table VII – Registry Access Privileges for the Domain Controller Policy

Similarly, GIAC Enterprises followed NSA's recommendation for locking down some of the more sensitive files on the domain controllers. Table VIII lists some of the directories whose permissions are recursively controlled by this portion of the policy. The template

and the matching GPO also restrict access to a number of individual files, such as ntldr, boot.ini and ntdetect.com, as prescribed by NSA's w2k_dc.inf Security Template.

%ProgramFiles%	%SystemDrive%\Temp	%SystemDirectory%\repl
%SystemDirectory%	%SystemDirectory%\dllcache	%SystemDirectory%\Setup
%SystemDrive%	%SystemDirectory%\config	%SystemRoot%\NTDS
%SystemRoot%	%SystemRoot%\security	%SystemRoot%\repair
%SystemRoot%\Temp	%SystemRoot%\SYSVOL	%SystemRoot%\Tasks

Table VIII – Directories Locked Down using the Domain Controller Policy

Some of the typical settings enforced by the File System of this policy are presented in Table IX, although some directories and files do not grant explicit access rights to CREATOR OWNER and Authenticated Users. Specifics regarding these settings are documented in NSA's w2k_dc.inf template. This policy also ensures that critical files and directories are owned by the Administrator user and the Administrators group.

Principals	New Privileges
Administrators	Full Control
Authenticated Users	Read and Execute List Folder Contents Read
CREATOR OWNER	Full Control (subfolders and files only)
SYSTEM	Full Control

Table IX – File System Access Privileges for the Domain Controller Policy

Finally, GIAC Enterprises used the Restricted Groups section of the Group Policy for the Domain Controller OU to make sure that the local Power Users group remains empty. Members of the Power Users group have the ability to "create local users and groups; modify and delete accounts that they created; and remove users from the Power Users, Users, and Guests groups. Power users also can install programs; create, manage, and delete local printers; and create and delete file shares."[8] At GIAC Enterprises, performing these tasks on the servers is the responsibility of system administrators, who are members of the Administrators group. The company uses Group Policy to ensure that the Power Users group does not have any members by adding `*S-1-5-32-547` as the group name in the Restricted Groups section of the GPO and not adding any members to it. The company did not want to enforce this restriction at the domain level to allow individual OUs to control membership to this group.

3.4 Settings for Member Servers

The company's member servers, which exist in the General Servers OU, obtain their Group Policy settings from the Member Server GPO combined with the Default Domain Policy. At the moment, the template for the Member Server GPO is identical to the template used to configure the Domain Controller GPO. This is because lockdown and other Group Policy configuration requirements for member servers at GIAC Enterprises are presently the same as requirements for Domain Controllers. However, dedicating a Group Policy to the General Servers OU gives the company the flexibility to change the policy, when the need arises, without directly affecting resources in other OUs.

Configuration of the GPU assigned to the R&D Dept Servers OU is similar to the Member Server GPO, but is not identical. The differences lie primarily in the configuration of User Rights Assignment, as documented in Table X. Specifically, R&D administrators did not want users from other departments to access its resources over the network. In addition, members of the R&D Developers group require the "debug programs" right in order to debug software during the development process.

The R&D department also has a group called R&D Time Administrators for users that have the ability to change system time. Members of this group periodically change time on select departmental systems to test how the company's software reacts under specialized time conditions. When configuring this group, GIAC Enterprises considered the security risk of allowing additional personnel to control time on some of the company's systems, but decided that the required business function outweighs such risks. Because the domain's Kerberos-based authentication mechanism uses system time "as part of the authentication ticket generation process," [9] members of the R&D Time Administrators group adversely impact the authentication process of R&D systems.

Setting Name	General Setting Value	R&D Setting Value
Access this computer from the network	Administrators Authenticated Users	Administrators R&D Users
Debug programs	None	R&D Developers
Change system time	Administrators	Administrators R&D Time Administrators

Table X – User Rights Assignment for R&D Server Group Policy

3.5 Settings for Workstations

A large portion of security-related settings for the company's workstations, such as account and password policies, are inherited from the Default Domain GPO. Overall, the Workstation GPO, which is assigned to the General Workstations OU, is similar to the one used for the company's servers. One notable difference is the maximum size of

application, security, and system log files. Workstations at GIAC Enterprises tend to have less disk space than servers. As a result, the Settings for Event Logs portion of the workstation security template, and the associated GPO, configure the maximum log size to be 20MB for each file.

Additionally, some user rights are assigned differently to GIAC Enterprise workstations than servers. These differences are documented in Table XI. Authenticated workstation users require the ability to logon locally to the system – this right was reserved to administrators only in case of servers. Additionally, no one had the "Remove computer from docking station" privilege for servers, since servers do not typically have docking stations. Workstation users, along with administrators, have this ability because some machines in use on the company's internal network are laptops. Finally, authenticated users have the ability to shut down the workstation, while only administrators have the ability to shut down a server.

Setting Name	Server Setting Value	Workstation Setting Value
Logon Locally	Administrators	Administrators Authenticated Users
Remove computer from docking station	None	Administrators Authenticated Users
Shut down the system	Administrators	Administrators Authenticated Users

Table XI – User Rights Assignment for Workstation Group Policies

The company relies on Encrypted File System (EFS) to encrypt specific local directories on laptops of its users, to help ensure confidentiality of locally stored files when laptop users leave the office. Because all workstations are part of the domain, the domain Administrator is configured as the EFS Recovery Agent for the systems.[10] To add a layer of protection to the use of the Recovery Agent, the company exported Administrator's private key to a file and then removed it from the domain. The private key file is stored off-line in a secure location, so that it can be manually retrieved if encrypted data needs to be recovered.

GIAC Enterprises also uses the User Configuration section of the Workstation GPO to control several user-specific settings on the workstations. For instance, the company set up Folder Redirection for each user's "My Documents" folder to point to a share on the central file server, as shown in Figure E. The "Application Data" folder is similarly redirected to the central file server.

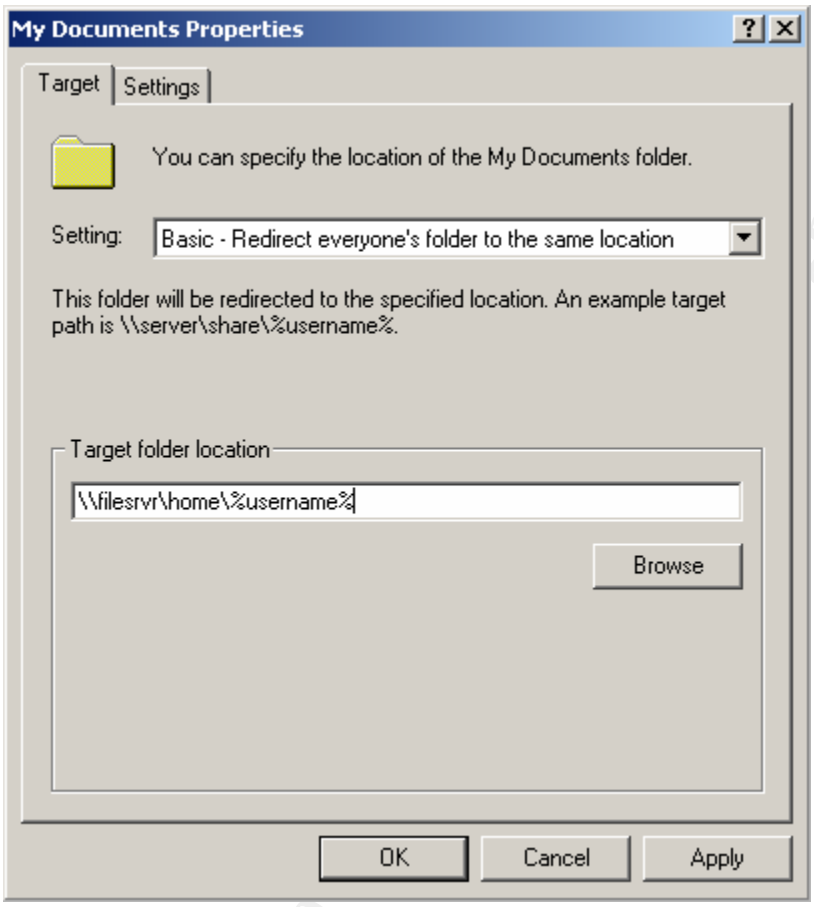

Figure E – Folder Redirection for Workstation Group Policies

Users of systems that are located in the General Workstations OU are also restricted from changing the bulk of Internet Explorer settings. This is accomplished via the Administrative Templates section of the General Workstation GPO. These users are locked out from the following pages:

- Security
- Connections
- Content
- Advanced

R&D users need to have the ability to change proxy server settings and to import their own certificates in Internet Explorer, and are therefore granted access to Content and Connections pages. The flexibility to do this is granted by the use of the separate GPO assigned to the R&D Workstations OU.

The company uses workstation GPOs to distribute core applications to its users. For instance, both the General Workstations OU and the R&D Workstations OU are set up to distribute Microsoft Service Pack MSI packages, and the Microsoft Office package. Additionally, R&D workstations are supplied with several application packages specific

to the Research and Development department. The company decided to implement software distribution through workstation OUs, instead of user OUs, to help prevent R&D applications from being installed on general-user workstations when an R&D user "roams" to a workstation that belongs to another department.

GIAC Enterprises also uses settings under the Administrative Templates section of the Group Policy to help ensure that its workstations have password-protected screen savers. Additionally, users do not have the ability to use the Windows GUI to change screen saver settings. This is accomplished by configuring the General Workstation GPO and the R&D Workstation GPO according to Table XII. This policy ensures that a password-protected screen saver is activated after 10 minutes of inactivity. Unfortunately, this does not grant company employees the artistic freedom to select their own screen saver, but the GIAC Enterprises decided to forego that flexibility in favor of control over the desktop.

Setting Name	Setting Value
Hide Screen Saver tab	Enabled
Activate screen saver	Enabled
Screen saver executable name	C:\WINNT\system32\logon.scr
Password protect the screen saver	Enabled
Screen Saver timeout	600 seconds

Table XII – Screen Saver Settings for Workstation Group Policies

3.6 Settings for Public Servers

GIAC Enterprises presently maintains a single server in its screened subnet, which is offers HTTP and SMTP services, and is accessible by Internet users. This system is set up as a stand-alone server, and is not a member of a Windows 2000 domain. Therefore, its policy settings are configured and applied locally, and becomes a part of the Local Computer Policy. The company still uses a Security Template as the basis for configuring security-related settings of this server. In this case, the template provides a way of documenting a significant portion of the settings, and also makes it easier to lock down another server when the company decides to place a new system into the screened subnet. The IIS server was locked down according to practices described in the SANS "Securing Internet Information Server 5.0" course; this section addresses some of the more critical settings that are part of the server's Local Computer Policy.

The company based the public server's Security Template, giac_pub_server.inf, on the template used for its Domain Controllers. The template was also customized to account for more stringent lockdown rules that apply to publicly accessible servers. For instance, the giac_pub_server.inf template explicitly disables services that are not necessary for the server to function, the majority of which are listed in Table XIII.[11] When configuring the

system's TCP/IP settings, the company also manually disabled the NetBIOS protocol, forcing the server to use TCP port 445 for SMB-related traffic.

Alerter	ClipBook	Computer Browser	DHCP Client
Distributed Transaction Coordinator	NetMeeting Remote Desktop Sharing	Remote Access Auto Connection Manger	Remote Access Connection Manager
Print Spooler	Fax Service	Irmon	Messenger
Remote Registry Service	Distributed File System	Distributed Link Tracking Client	Distributed Link Tracking Server
Task Scheduler	Telephony	Terminal Services	Indexing Service
Internet Connection Sharing	FTP Publishing Service	File Replication Service	Network DDE
Network DDE DDSM	Removable Storage	TCP/IP NetBIOS Helper Service	Windows Time
QoS RSVP	Smart Card	Smart Card Helper	Telnet
Workstation	Windows Management Instrumentation	Windows Management Instrumentation Driver Extensions	

Table XIII – Services Explicitly Disabled for Public Server Policy

The public server policy, having been based on the Domain Controller Policy, restricts "Log on as a batch job" and the "Access this computer over the network" rights so that the IUSR account that IIS runs as does not possess these privileges. Additionally, the File System section of the policy was configured to restrict access to files on the volume that hosts the company's Web site such that they are owned by the Administrators group. The IIS account was granted read permissions to plain files that need to be publicly accessible, and read and execute permissions to the server's ISAPI scripts.

The company's border firewall enforces access restrictions on traffic that attempts to enter or leave the screened subnet. Additionally, GIAC Enterprises uses packet-filtering capabilities of the IPSec driver built into Windows 2000 to further lock down the server, and to provide another layer of defense behind the firewall. The company also used the Authentication Header (AH) protocol to authenticate administrative traffic destined for this server. To allow clear-text traffic to the system's TCP ports 25 (SMTP) and 80 (HTTP), and to require AH-based authentication for packets targeting the server's TCP port 445 (SMB). This configuration was set up through the use of the IP Security Policies on Local Machine snap-in for MMC, and is described in greater below.

First, the company created two IP filter lists to define authorized traffic types. The Inbound Public Filter, illustrated in Figure F, matches inbound HTTP and SMTP traffic originating from any host and targeting the local server. Similarly, another filter list was created to match inbound traffic from appropriate workstations on the internal network and targeting the local TCP port 445; this filter was appropriately named "Inbound Admin Traffic." Both filters were set up as "mirrored" to match traffic bi-directionally.

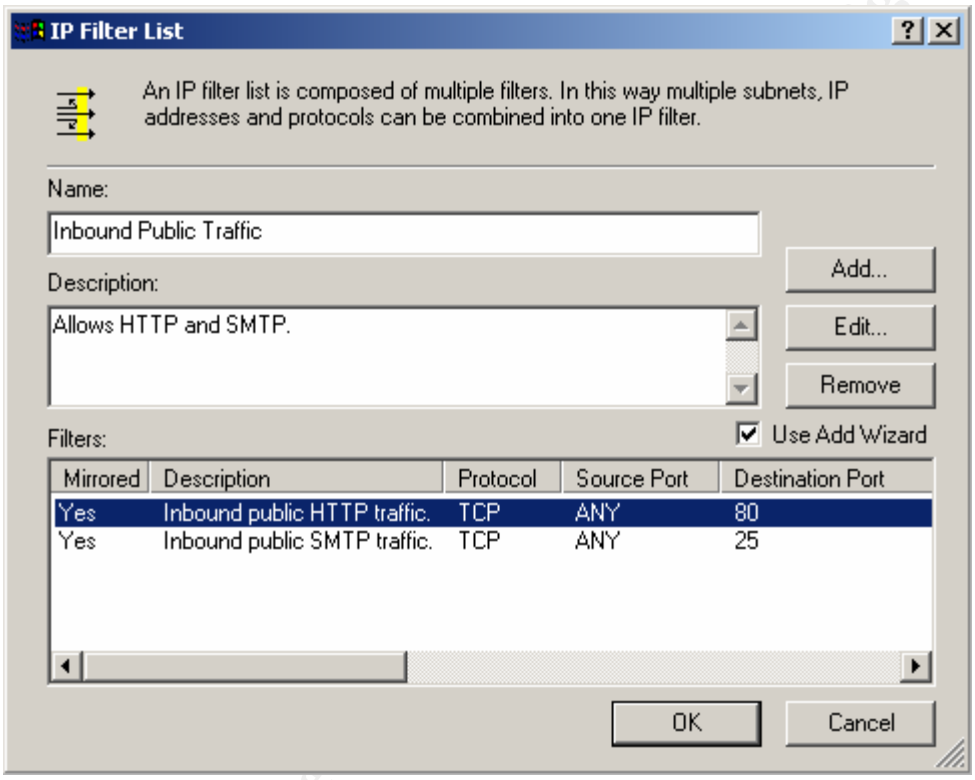

Figure F – Inbound Public IP Filter for the IIS Server

The company also created another IP filter list, to match all traffic that might hit the server. This list, called "All Traffic," is used when defining the IPSec policy to explicitly block all traffic that does not match the other filters. Additionally, the company set up a new filter action called "Block," configured to block traffic instead of permitting it through or negotiating security of the connection. Another filter action called "Authenticate" was created to require the use of the MD5 protocol to establish AH Integrity of the packets. The company decided not to use ESP for protecting confidentiality of administrative traffic to avoid the computational overhead of encrypting the packets.

The company then created a new IP Security Policy, called "Server Lockdown," set up without activating the "default response rule." The policy, shown in a screenshot on Figure G, incorporates the three IP filter lists mentioned above such that inbound SMTP and HTTP traffic is permitted without restrictions, administrative SMB traffic has to be authenticated through the use of AH, and all other traffic is blocked.

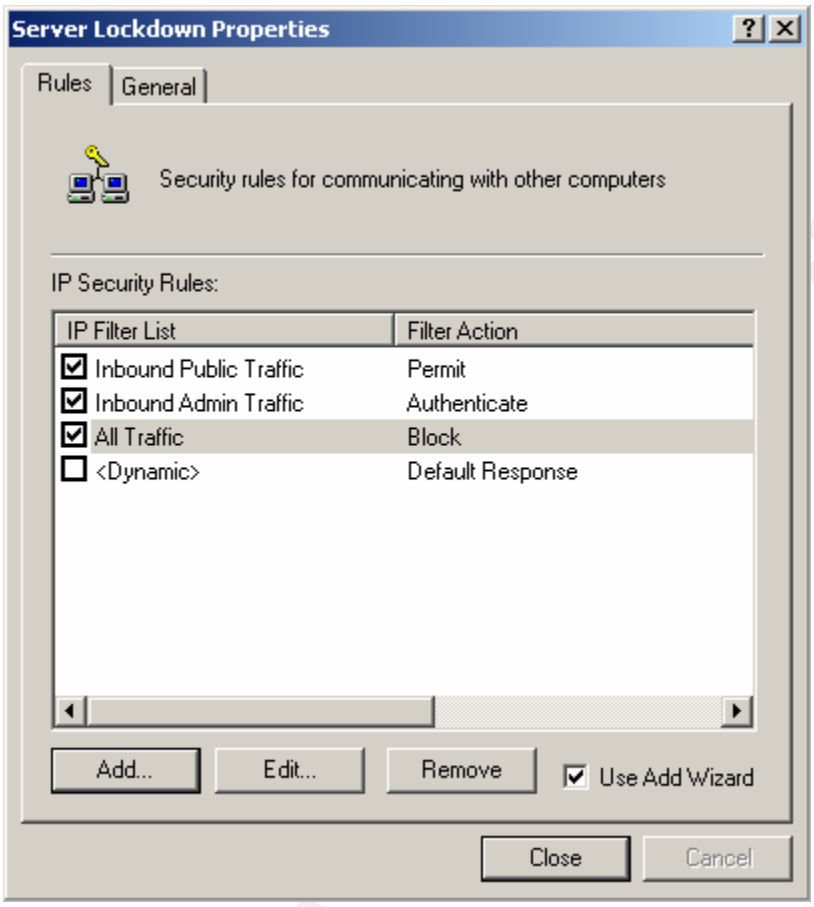

Figure G –Lockdown IP Security Policy for the IIS Server

The company also uses Winalysis software, which is installed on all its servers, to detect unauthorized changes to the server's file system and registry. Winalysis agent periodically scans the system and compares its current state to the pristine baseline configuration. The agent alerts administrators if any deviations are detected. In its alerts, Winalysis is able to interpret some changes to the registry in a way that allows to easily detect application-level events such as creation of unauthorized users, services, or network shares. This creates yet another layer of defense for protecting the company's publicly accessible server.

Section 4: Summary

GIAC Enterprises maintains its corporate systems on a network separated from its e-commerce infrastructure. This separation of resources allowed the company to deploy and configure its corporate systems in a way that matches business requirements of its corporate users, allowing the e-commerce site to be configured according to its purpose and mode of operation. The company's corporate infrastructure contains two networks: a screened subnet that hosts publicly accessible resources, and an internal network that contains servers and workstations used by the company's employees. The border firewall enforces the bulk of network access restrictions, allowing only protocols explicitly required for business to pass through.

The company relies on security features built into Windows 2000 Active Directory for enforcing the bulk of security policies for internal servers and workstations. When designing its AD hierarchy, the company took into account political needs, as well as task delegation requirements to come up with OUs appropriate for its business. This design reflects the company's current needs, and may be augmented as the organization evolves into a larger enterprise.

GIAC Enterprises takes advantage of the flexibility of Group Policies to enforce security policies across a large number of internal servers and workstations without having to configure each system individually. This has proven very effective, as the company is able to maintain its corporate resources with a relatively small group of system administrators. Having different OUs in its AH hierarchy, which group systems according to business purpose and task delegation, allows the company to apply slightly different settings to its workstations, servers, as well as to systems that belong to the Research and Development department, while inheriting a large number of common settings from the domain-wide Group Policy. Whenever possible, the company uses Security Templates as the basis for configuring its GPOs, so that its security settings are documented and repeatable.

The company set up its publicly accessible server as a stand-alone system, as it saw no need to create a dedicated domain for the single system. It then took advantage of the support for Local Policy, built into Windows 2000, to lockdown the server and its applications. The company also used the Local Policy to define IPSec-based packet filtering settings to tightly control what traffic can enter and leave the server. Additionally, using AH for authenticating administrative traffic allowed the company to reliably authenticate administrative traffic that reaches the server from the internal corporate network.

Section 5: References

[1] Hogwash FAQ. URL: http://hogwash.sourceforge.net/HogWash_files/faq.html (18 April 2002).

[2] Lenny Zeltser. GCFW Practical Assignment. "Perimeter Defense Architecture." December 2000. URL: http://www.zeltser.com/sans/gcfw-practical (18 April 2002).

[3] Microsoft Corporation. "How To Delegate the Unlock Account Right (Q294952)." 17 October 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q294952 (18 April 2002).

[4] NSA Security Recommendation Guides. "Windows 2000 Guides." 22 January 2002. URL: http://nsa2.www.conxion.com/win2k/ (18 April 2002).

[5] Microsoft Corporation. "Passwords must meet complexity requirements of the installed password filter." URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/504.asp (18 April 2002).

[6] Microsoft Corporation. "Group Policy Application Rules for Domain Controllers (Q259576)." 16 August 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q259576 (18 April 2002).

[7] Microsoft Corporation. "How to Enable SMB Signing in Windows NT (Q161372)." 10 August 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q161372 (18 April 2002).

[8] Microsoft Corporation. "Well Known Security Identifiers in Windows 2000 (Q243330)." 20 December 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q243330 (18 April 2002).

[9] Microsoft Corporation. "Basic Operation of the Windows Time Service (Q224799)" 10 January 2002. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q224799 (18 April 2002).

[10] Microsoft Corporation. "Analysis of Reported Vulnerability in the Windows 2000 Encrypting File System (EFS)." URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/analefs.asp (18 April 2002).

[11] Jason Fossen, SANS Institute. The "Securing Internet Information Server 5.0" Course, p. 49-50. 31 October 2001.

Last Updated: June 25th, 2018

Upcoming Training

SANSFIRE 2018	**Washington, DC**	**Jul 14, 2018 - Jul 21, 2018**	**Live Event**
SANSFIRE 2018 - SEC505: Securing Windows and PowerShell Automation	**Washington, DC**	**Jul 16, 2018 - Jul 21, 2018**	**vLive**
SANS Boston Summer 2018	**Boston, MA**	**Aug 06, 2018 - Aug 11, 2018**	**Live Event**
SANS Amsterdam September 2018	**Amsterdam, Netherlands**	**Sep 03, 2018 - Sep 08, 2018**	**Live Event**
SANS Network Security 2018	**Las Vegas, NV**	**Sep 23, 2018 - Sep 30, 2018**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201810,**	**Oct 01, 2018 - Nov 07, 2018**	**vLive**
Mentor Session - SEC505	**Baltimore, MD**	**Oct 04, 2018 - Nov 15, 2018**	**Mentor**
SANS San Diego Fall 2018	**San Diego, CA**	**Nov 12, 2018 - Nov 17, 2018**	**Live Event**
San Diego Fall 2018 - SEC505: Securing Windows and PowerShell Automation	**San Diego, CA**	**Nov 12, 2018 - Nov 17, 2018**	**vLive**
SANS Cyber Defense Initiative 2018	**Washington, DC**	**Dec 11, 2018 - Dec 18, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**