

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

A secure Active Directory Infrastructure Design for GIAC enterprises



GCNT Practical Assignment v3.0
Perry Kuhnen

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Introduction:

GIAC Enterprises has recently received startup financing for an e-business venture selling on-line fortune cookie sayings. This document details Active Directory design considerations with a strong focus on network security. Although there is no such thing as a 100% secure network, best practices are deployed whenever practical to reduce the probability of security threats. In particular the following two well know security principles should provide guidance in design decisions:

- Defense in depth (security at every point of attack)
- Least Privilege (disallow all access to resources unless explicitly required)

Assumptions:
Since the design criteria were loosely defined, the following assumptions have been made to fill in missing details and provide clarification for design decisions. Some assumptions have been made to simplify the overall design.

- To stay on top of the latest security developments GIAC Enterprises' I.T. staff subscribes to a variety of security e-mail services such as those offered by SANS and securityfocus.com. In addition they subscribe to similar services offered by the vendors of the hardware deployed at GIAC Enterprises.
- Although this is a design document, whenever possible 'How-to' configuration examples are provided in the Appendices.
- The intended audience of this document is expected to be familiar with the usual industry acronyms.
- GIAC Enterprises is located in a 4 storey building in Mississauga, Ontario, Canada. (GIAC Enterprises is the sole tenant.)
- All servers are physically secured.
- Departments are made up as follows:

Research & Development	132 users
Sales & Marketing	48 users
Finance & Human Resources	17 users
Information Technology	4 users

- Windows 2000 is the only O/S deployed.
- All networking equipment is sourced from Cisco.
- All server/workstation/laptop hardware is sourced from Compaq.
- All employees have access to high-speed Internet access from home.
- All remote access occurs will require IPSEC encryption and authentication.
- Employees working from home have been supplied with pre-configured laptops. This includes anti-virus software and a personal firewall such as ZoneAlarm.
- All line of business applications use SQL Server 2000.

© SANS Institute 2000 - 2005 Author retains full rights.

- All servers and workstations have Trend Micro anti-virus software installed. Virus signatures updates are check for daily.
- GIAC Enterprises has purchased an external stratum 1 network clock that will act as NTP/SNTP server for the domain controllers and Cisco switches.
- The exchange 2000 server has Sybari Antigen installed and all currently known executable attachments are filtered. (Users may contact the IT department to deliver quarantined content after it has been scanned)

- The following items, although they have an impact on security, are beyond the scope of this document.

Deployment and configuration of Intrusion Detection Systems
Tape backup, off-site storage, disaster recovery/business continuity plans.
Complete configuration of the internal and external stateful firewalls.
Specific server hardening exercises, especially IIS web servers.
Disk quotas and use of the Encrypting File System (EFS)

Network Design:

GIAC Enterprises has divided its network into logical segments using a VLAN for each department, as well as a VLAN for production servers and a DMZ. (See figure 2 for an overall view of the network.) This decision was made to ensure that internal threats are minimized. After all, many of the staff members in the R& D department are accomplished programmers and could therefore pose a probable threat.

The IT staff tracks the MAC addresses of every computer and allocates them statically to the appropriate VLAN. Although this is a manual job, doing so will prevent any unauthorized devices from connecting to the network in any way. Each VLAN is associated with a single IP subnet and the Layer 3 Cisco switch handles the routing function.

The DMZ internal subnet is separated from the internal LAN by a stateful firewall and the external subnet is separated from the public Internet by another stateful firewall. The two firewalls are from different vendors to ensure that any newly discovered vulnerabilities do not allow a hacker through the entire DMZ. Both firewalls are updated when security patches become available.

The production server subnet contains all business critical serves. Again resources are only accessible if there is a requirement

Access to resources on other subnets is controlled with Access Control Lists. (ACL)
To provide defense in depth at the network layer, these settings should match the IPSEC policies detailed in the Active Directory section. (See Appendix A for details on configuring VLAN and ACL settings)

For example, members of the IT department remotely manage production servers using

© SANS Institute 2000 - 2005 Author retains full rights.

Windows 2000 built-in terminal server. Therefore, access to terminal services ports at each server should be set with IPSEC policies in Active Directory.
In addition IPSEC policies at the client should be set with Active Directory as well. To add the final step, the central Layer 3 switch should have an Access Control Entry (ACE) in the ACL to restrict access from the IT department VLAN to the server VLAN. (See figure 1)

Of course, the router interfaces will also have to pass the following on all interfaces to enable IPSEC traffic. These protocols, by default are exempted from IPSEC policies.

Protocol number 51 (the AH portion of IPSEC)
Protocol number 50 (the ESP portion of IPSEC)
UDP port 500 (the IKE portion of IPSEC)

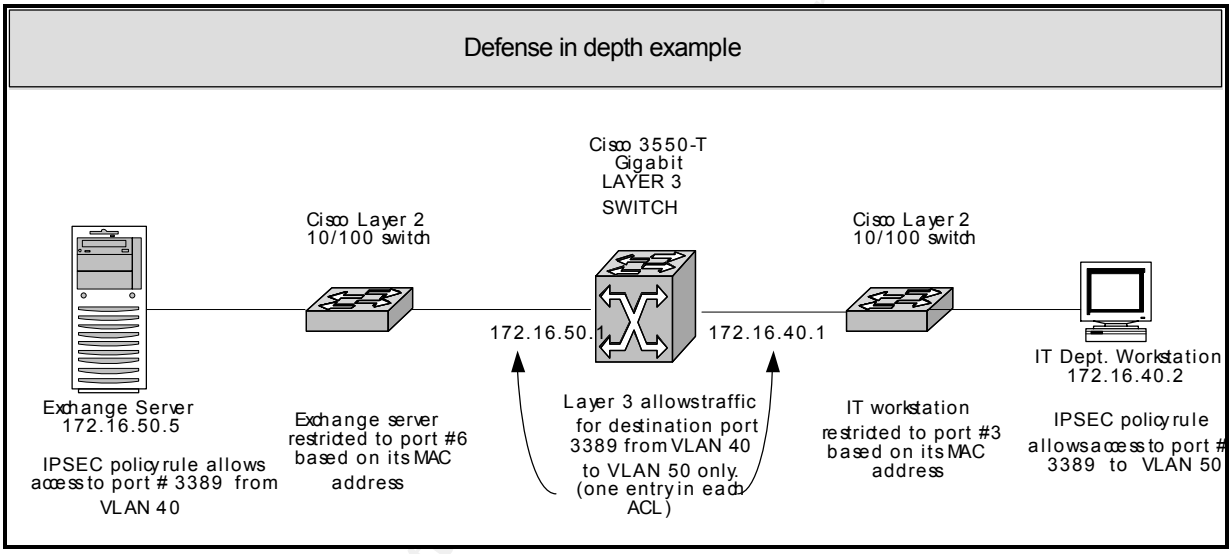


Figure 1

The stratum 1 time source is located in the domain controller VLAN where the domain controller that has the Flexible Single Master Operations role of PDC emulator synchronizes its system clock with the external NTP. (Usually the first installed DC)
This is done with the following command on the PDC emulator:
Net time /setsntp: 172.16.80.4 (this can be the IP address or DNS name of the NTP source)
All other computers in the domain by default synchronize their time with the PDC emulator in a secure fashion. See the following article for details on Windows Time synchronization in an Active Directory environment.

Brandolini, Shala and Green, Darin "The Windows Time Service". April 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/maintain/optimize/wintime.asp (Jan 10 2001)

© SANS Institute 2000 - 2005 Author retains full rights.

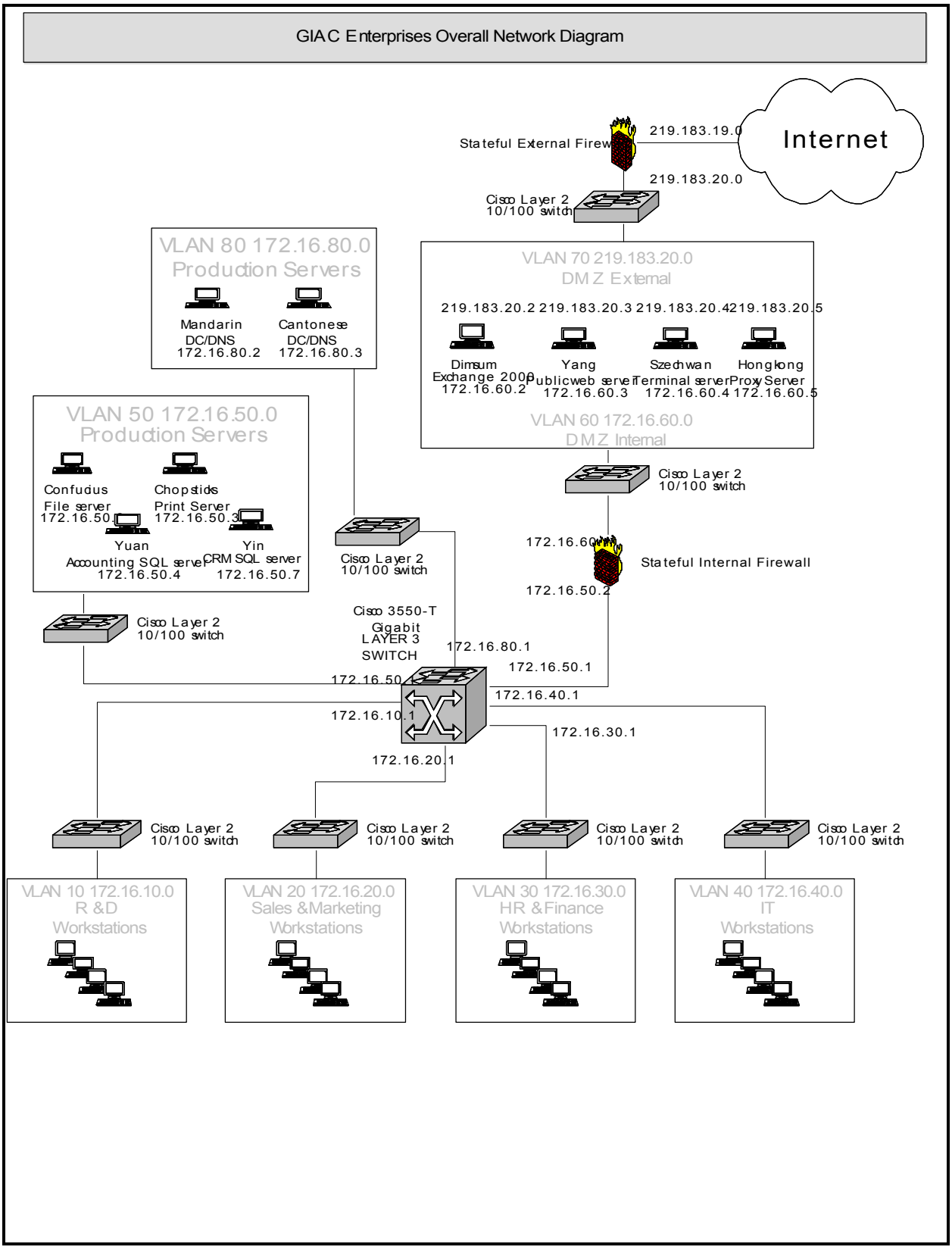


Figure 2

© SANS Institute 2000 - 2005 Author retains full rights.

Key Servers:

The following table details key servers their purpose and their locations.

Name	Purpose	Location	IP Address
Confucius	File server	VLAN 50 – Production	172.16.50.2
Chopsticks	Print server	VLAN 50 – Production	172.16.50.3
DimSum	Exchange 2000 server	VLAN 60/70 - DMZ	172.16.60.2 & 216.183.20.2
Yuan	Accounting SQL 2000 server	VLAN 50 – Production	172.16.50.4
Mandarin	Domain Controller/DNS	VLAN 80 – Domain Controllers	172.16.80.2
Cantonese	Domain Controller/DNS	VLAN 80 – Domain Controllers	172.16.80.3
Yin	Sales/CRM SQL 2000 server	VLAN 50 – Production	172.16.50.7
Yang	Public Web Server	VLAN 60/70 - DMZ	172.16.60.3 & 216.183.20.3
Szechwan	Terminal Server	VLAN 60/70 - DMZ	172.16.60.4 & 216.183.20.4
HongKong	Proxy server (ISA 2000)	VLAN 60/70 - DMZ	172.16.60.5 & 216.183.20.5

Note that the Exchange server is in the DMZ. Alternatively it can be placed in the production VLAN and an SMTP forwarding host deployed in the DMZ. All servers are running Windows 2000 server SP2. The latest security hot fixes are applied after testing is performed in an isolated test lab. Except for the public web server Yang, IIS is not installed. After all IIS is well known for having exploitable vulnerabilities, therefore do not deploy it unless absolutely required.

The external addresses of the servers in the DMZ are real world IP addresses. This ensures that employees accessing these servers from the Internet are able to use IPSEC encryption (ESP) and authentication (AH). If we were using Network Address Translation, the IP address would change at the firewall and therefore authentication would not work.

The proxy server is running ISA server 2000 in proxy server mode only. This reduces the probability that users deploy rogue applications such as ICQ, IRC, MSN Messenger, etc. Instant messaging and chat applications have known vulnerabilities often exploited by hackers. Should a user manage to install one of these applications and also circumvent the IPSEC policies in place, the ACLs on the routers will filter this traffic anyway.

All servers have their system partition on NTFS and hardware RAID 1 (mirrored) arrays. In addition each server has a separate physical disk for the page file. All servers have a minimum of 512 MB of RAM and 2 x 933 MHz Xeon processors. The SQL servers and the exchange server each have 4 x 933 MHz processors as well as 2 GB of RAM each.

The domain controllers have a second RAID1 array for the active directory database. See the following TechNet article for details on placing "How to Move the Ntds.dit File or Log Files (Q257420)". Mar 28 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q257420 (Dec 19 2001)

© SANS Institute 2000 - 2005 Author retains full rights.

The SQL servers have 3 additional arrays: (these are for performance and redundancy)
1 RAID 1 for the SQL server logs,
1 RAID 5 for the SQL server backups,
1 RAID 10 for SQL server data.

The Exchange server has 3 additional arrays: (these are for performance and redundancy)
1 RAID 1 for the exchange logs,
1 RAID 5 for public folders,
1 RAID 5 for mailboxes.

Active Directory Design

Due to GIAC enterprises' small company size and the fact that the company is physically located in single building, the active directory is contained to a single site and a single domain. This will simplify the design, as we do not have to worry about inter-site replication, transitive trusts, empty root domains, etc.

When the first domain controller is installed in an Active Directory environment it automatically assumes the following five Flexible Single-Master Operations roles:

Schema master
Domain naming master
PDC emulator
RID master
Infrastructure master

In a small domain with only two domain controllers, there is little need to re-assign these roles. We will make one change for redundancy only. The second domain controller will assume the Infrastructure master role to move it away from the global catalog server. (By default also the first installed Domain Controller)

This recommendation can be found in the following Microsoft TechNet article.

"FSMO Placement and Optimization on Windows 2000 Domain Controllers (Q223346)" Mar 23 1999. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q223346 (Jan 08 2001)

The domain default GPO provides most of the security settings. Since there is only one site, we therefore do not configure any policies at the site level.

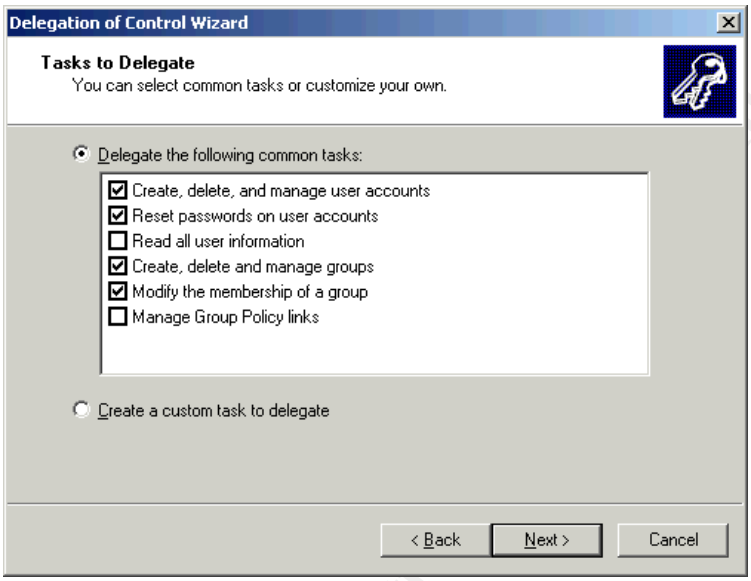
Additional departmental GPO requirements are applied via Organizational Units. (See Figure 3 for an overall view of the Active Directory Design of GIAC Enterprises)

Again, due to the small size of GIAC Enterprises, only one person in each department is assigned

© SANS Institute 2000 - 2005 Author retains full rights.

as a department account administrator. Members of the IT department will act as a backup should that employee be unavailable.
The single user is added to a security group called 'DeptName-Admin'. For example, Joe Black in R & D would be added to the GIAC\R & D-Admin group.
Control is delegated to allow tasks to be performed by the departmental account administrator rather than by the IT group. (See screen shot below)

Note that even though the user is now allowed to modify memberships of groups, he cannot add himself to any administrator groups such as Domain Admins. Members of built-in groups such as Account Operators can only perform adding users to groups such as Domain Admins. The user needs to be a member of the Account Operators, Domain Admins, or Enterprise Admins group. (Later on we'll see how to ensure that even those groups cannot add accounts to sensitive groups using the 'Restricted Groups' feature.)



Key servers such as domain controllers are in their own Organizational Unit to ensure that additional security settings are applied.

Servers in the DMZ are also in their own OU, although they could be deployed as stand alone servers to decrease security exposure in case of a compromise. This would cause greater administrative overhead since the servers would not be members of the domain. Note that if we did not require external IPSEC authentication for remote users, the DMZ servers would not be multi-homed. However, we are using a private class B IP address range for our internal network and a real world class C IP address range for out external network. The OU structure matches the physical infrastructure, in particular the VLAN arrangement. This should make the task of matching IPSEC policies to VLAN access control lists less complicated.

The following table lists each Organizational Unit and its purpose.

OU	Purpose

© SANS Institute 2000 - 2005 Author retains full rights.

Domain Controllers	To ensure that the servers responsible for authentication have the most restrictive security settings within practical limits.
Production Servers	Servers that hold mission or business critical data required their own set of security restrictions.
DMZ	Servers in the DMZ are accessible through the external firewall and therefore require strong security and IPSEC settings.
Departments	All client Departments OUs are kept inside this main OU
Departments\R&D	Research & Development workstations and user accounts with departmental GPO
Departments\IT	Information technology workstations and user accounts with departmental GPO
Departments\S&M	Sales & Marketing workstations and user accounts with departmental GPO
Departments\HR&F	HR and Finance workstations user accounts with departmental GPO

The domain controllers store the user accounts, their passwords and many more objects in the active directory database. Therefore we want to ensure that the OU, which contains the domain controllers, is very secure. By default only members of the enterprise Admins and domain Admins can log on to the domain controllers interactively. Although smartcards can be expensive, they would make sense for accessing the domain controllers.

The production servers do not contain user accounts, other than local accounts, but they do contain critical and sometimes sensitive data. For example, we do not want anyone other than the HR staff accessing payroll records stored on the Yuan accounting server. Therefore the group policies applied to this OU should be

Each department has its own set of requirements. We therefore split the four departments into child Organizational Units. We can now assign security settings that are appropriate for each logical group. In addition this logical division will facilitate internal transfers of staff and computers. For example, if Joe Black in the R&D department got an exciting new job in the S&M department, we could transfer both his computer and his user account from the R&D OU to the S& M OU.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

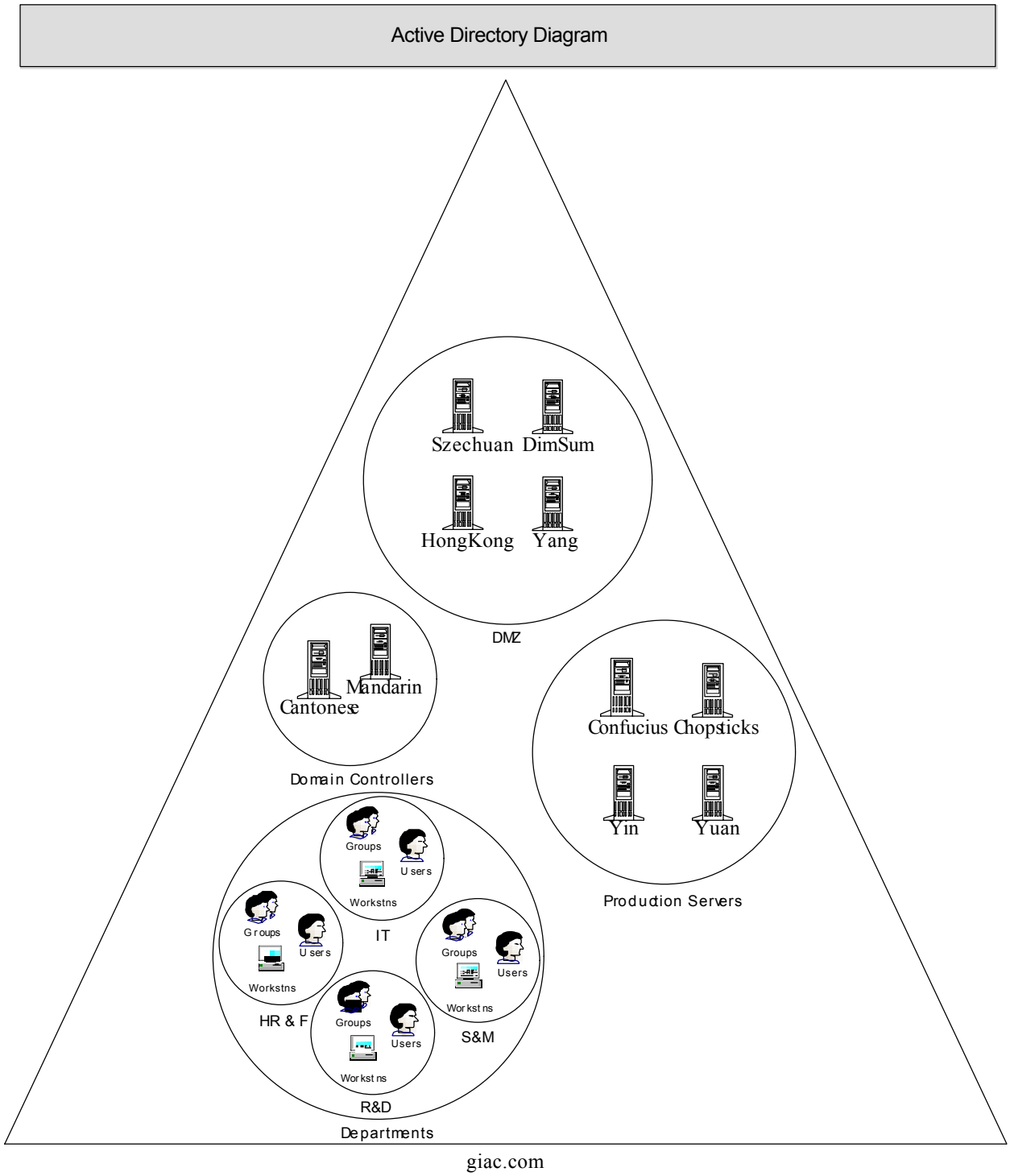


Figure 3

© SANS Institute 2000 - 2005 Author retains full rights.

Group Policy and Security

As part of our defense-in-depth practice, we want to secure the network infrastructure and also the user and group accounts required to gain access to resources. The recommended way of doing this in an Active Directory environment is to apply Group Policy Objects.

Before we dig into the specific settings of Group Policy Objects, it is important to understand how GPOs are applied. Group Policy Objects are linked to specific objects such as the domain or an OU. They are applied, in sequence, as follows to computers in the domain:

If any local policies exist on a member server, they will be applied first. Next, if any policies exist at the site level, they are applied. Following this, policies at the domain level are applied. Finally, policies at the OU level from the topmost OU down to child OUs that exist underneath until the OU where the computer or user is stored.

If more than one GPO is assigned or 'linked' to an object, then the settings are applied in order from top to bottom as they are displayed in the GPO MMC snap-in.

Policies are cumulative only if they do not conflict. For example, if at the domain level a policy exists that disables the display control panel applet and at the user's OU level the same applet is re-enabled, then the last GPO becomes the effective setting. If, however, the networking control panel applet is disabled at the domain level and the display control panel applet is disabled at the OU level then both settings will be effective.

Group policies consist of two main pieces, Computer Configuration and User Configuration. The computer configuration is applied upon startup and affects settings specific to the computer.

When applying a GPO to an Organizational Unit that holds only computers or users, only that piece should be enabled. (See screen shot below where the User Configuration is disabled for the Workstations OU) This practice decreases the amount of time required to apply the GPO during computer startup and user logon. This is due to the fact that the computer does not have to parse through half of the possible settings. Keep in mind that the performance gained increases with the number of GPOs applied. It is therefore prudent to keep the level of OU nesting to a minimum.

When first designing and testing GPO settings, it is wise to keep the number of settings per GPO to a minimum. This results in more GPO links that at a later time can be consolidated. It is much easier to troubleshoot many GPO links with few settings than a few GPO links with many settings.

© SANS Institute 2000 - 2005 Author retains full rights.

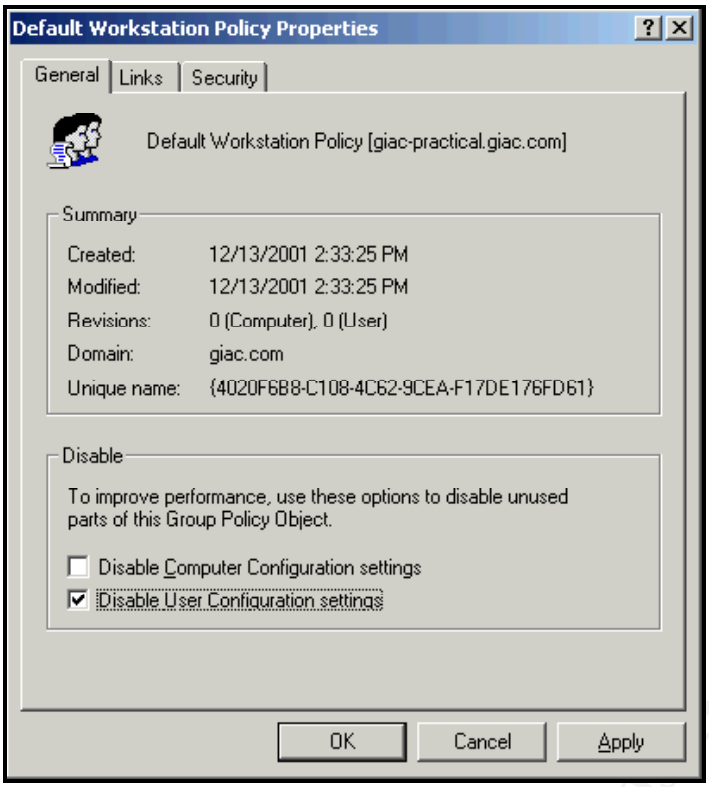


Figure 4

Default Domain Policies

Since we choose not to deploy any site level GPO, initial security settings are applied at the domain level. It is important to note that these settings apply to every member computer that is part of the domain. This includes every user that logs into a computer that is a member of the domain. Therefore these settings should considered carefully as the must be appropriate for every computer and user in the domain. Of course we can override most of these settings at the OU and child OU level if so required. . The exception to this is when an OU has the Block Policy Inheritance turned on. If we wish to ensure that all domain level settings are propagated to every OU, even if an OU has the Block Policy Inheritance turned on, we must enable the No Override option. (See Appendix C for details)

Additional departmental requirements are applied at the OU level, but could also be filtered at the OU level based on security group membership.

It is possible to simply import preset security settings provided by a trusted third party. Many templates are available on the Internet based on best security practices. For the sake of this design document we examine the key settings.

© SANS Institute 2000 - 2005 Author retains full rights.

Detailed information on all the GPO settings can be found in the following NSA report:

Rice, David C. Group Policy Reference. Ft. Meade: National Security Agency, 2001.

Appendix B shows the steps required to import a security template.

Account Policies

Account policies consist of 3 subsets.

1. Password policy
2. Account Lockout policy
3. Kerberos policy.

Since all settings have an effect on overall security we will examine each one in detail.

Password Policies

At the heart of account security are the password policies for the domain. Hackers will jump at the low hanging fruit such as an administrator's account with a blank password. The domain level password policies will ensure that accounts are safe from simple password guessing as well as dictionary and brute force attacks. Let us look at the password policies in detail.

Minimum password length

Probably the most important password policy is 'minimum password length'. Although this setting is most effective in combination with other settings, such as account lockout policies, it needs to be considered carefully on its own. The minimum value of 0 is obviously unacceptable, as this would allow blank passwords. The maximum value of 14 is likely to annoy our users, as they are likely to mistype long passwords. Therefore we choose a smaller value of 12. This is the smallest value that is still equal to or greater than the restriction placed on password length by the complexity requirement policy detailed below. Note that even if you set the password length to a value less than 12 the complexity requirement will override it.

Passwords must meet complexity requirements

The complexity requirement forces users to have passwords with the following attributes:

- 12 or more characters
- Cannot repeat the previous 24 passwords
- Must contain capitals, numeral or punctuation.
- Cannot contain the user's account name of full name.

Note that setting the minimum password length becomes redundant when this policy is active, unless we choose a value greater than 12 up to the maximum of 14. These requirements are hard coded similar to the passfilt.dll solution in NT4.

© SANS Institute 2000 - 2005 Author retains full rights.

Enforce password history
This setting ensures that the user cannot re-use previously selected passwords. It is very common for users to cycle their passwords by choosing one password and incrementally adding a number. For example Joe Black might cycle black1, black2, black3, etc. Obviously hackers know that users do this and we want to prevent this behavior. Note that the password complexity requirement will override this setting and since 24 is the maximum value this setting has no effect.

Minimum password age
If users know that only 24 passwords are remembered, and they can change passwords as often as they like, then password cycling is still going to occur. (Even if passwords fit the complexity requirements) To prevent this type of cycling we set the minimum password to at 2 days. This means that the user cannot get back to their original password for 48 days.

Maximum password age
Although we don't want users to change their password to cycle back to their original, we do want them to change their passwords regularly to fresh and unique passwords. Keep in mind that the lockout policies yet to be examined will mitigate brute force and dictionary attacks. Therefore we set the maximum age at 60 days.

Store password using reversible encryption for all users
This setting offers compatibility with certain applications/protocols that need access to the user's password in reversible encryption format. For example the digest authentication on IIS 5 requires reversible encryption. In our case we do not require reversible encryption; therefore the setting is disabled.

To compliment and strengthen the password policies, lockout policies can ensure that accounts attacked with dictionary and brute force password guessing are adequately protected.

Account lockout threshold
Should an account come under attack from dictionary and brute force attacks, we want to limit the number of login attempts. We need to keep in mind that users can incorrectly type passwords or inadvertently turn on/off the Caps Lock key. If the users have received sufficient training to check for things such as Caps Lock and Num Lock, then we can set a relatively low threshold and still keep the number of lockout/reset request to a minimum. We therefore select a threshold of 5 attempts.

Account lockout duration
Should an account be locked out, how long should we keep the account in the locked out state. If we consider a hacker that is attempting to attack with a brute force or dictionary attack, and keeping in mind that password length is at least 12 characters, we should choose a value that will prevent the hacker from getting for a very long time.
On the other hand if we choose a very large value and an authorized user forgot to check her Caps Lock key, she would be prevented from performing her job for a long time. Assume that all users had at least upper and lower case characters and numerals in their passwords.

© SANS Institute 2000 - 2005 Author retains full rights.

This is the worst-case scenario for our complexity requirements since there are less numeric characters than punctuation marks. At 12 characters long and 62 possible characters (26 upper case characters, 26 lower case characters and 10 numeric characters) we end up with 62^{12} possible password. (The number of password to be subtracted due to the user's account name and full name is too insignificant to worry about.) If we assume that, on average, a brute force attack would succeed halfway through all the possible passwords, we have to worry about $61^{12} / 2$ hacking attempts. That's 1,613,133,381,198,950,000,000 attempts.
Now, further assume that any hacking attempt, on average, starts in the middle of a period that a password is changed. That would be, in our case, the maximum password age of 60 days. The hacker would then need to be able to attempt 622,350,841,511,940 / second for the entire 30 days. This is not likely for a number of reasons. First, the domain controllers are unlikely to be able to process that many logon request. Second, even if the domain controllers could handle the requests, CPU and network utilization would certainly alert the IT department very quickly. Third, the event logs of the domain controllers would certainly have filled up in no time at all and caused all sorts of trouble. (Depending on the event log settings discussed later on)
Now that we have established that brute force attacks extremely unlike to succeed, we need to consider dictionary attacks. Assume that some clever hacker has a very large dictionary of likely to be chosen words and word combinations. (E.g. all upper case and lower case variations of cat*dog, etc.) Further assume that there are 200 million passwords in this dictionary. Again, on average, it would take 100 million attempts in 30 days to break into a user account. (We assume that the user's password is contained in the dictionary)
In this case the hacker would need to attempt 40 logins per second. This is certainly achievable on today's computers. However, we have already chosen an account lockout threshold of 5 attempts. If we set the account lockout duration to 5 minutes the rate at which the hacker can attempt his dictionary attack is reduced less than 15000 in 30 days. Since we assumed that the user's password exists in the hacker's dictionary, the percentage of passwords that can be guessed in this period is extremely small. (About 0.007%) We therefore set the account lockout duration to 5 minutes.

Reset Account Lockout after
This setting works in concert for the account lockout duration setting. After the number of minutes specified since the last failed login, the bad login counter is reset. This value should always be less than or equal to the account lockout duration setting. Since we have already chosen a relatively small value for account lockout duration of 5 minutes we keep the reset account lockout after setting at 5 minutes as well.

One final note about the password lockout settings; these settings do not apply when a user locks their workstation with the CTRL-ALT-DEL sequence. These settings also do not apply when an activated screensaver has password protection on it. We therefore need to educate the users to avoid account compromises due to workstation hopping and shoulder surfing by co-workers.

Kerberos Policies

To understand how Kerberos policies affect security it is important to understand how the

© SANS Institute 2000 - 2005 Author retains full rights.

Kerberos authentication protocol works. Although a complete description is beyond the scope of this document, we will touch upon the key point. For details on Kerberos in a Windows 2000 environment see the following reference:
"Kerberos Authentication Protocol". URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/prodtech/kerbtech.asp (Jan 10, 2001)

Kerberos is a three way mutual authentication mechanism and it involves the following three players:

- A client requesting access to services.
- A server providing services.
- A mutually trusted third party. (In windows 2000 this is called the Key Distribution Centre or KDC)

Note that the KDC is actually made up of 2 parts, the Authentication Service (AS) and the Ticket Granting Service. (TGS) The following is a simplified sequence of a client accessing a service using Kerberos authentication.

- The client authenticates itself to the Authentication Service. It does this by sending a hashed value of the client password along with an account name and domain name.
- The authentication service grants the client a ticket to obtain further tickets. This is called a Ticket Granting Ticket. (
- The client presents the Ticket Granting Ticket to the Ticket Granting Service. The TGS then authenticates the ticket and gives the client a service ticket. This service ticket includes two encrypted session keys, one for the client to decrypt and for the server to encrypt.
- The client presents the service ticket to the server. The server authenticates the client, as it is the only entity that can decrypt the session key created by the KDC. Now the client can access resources provided by the server.

Now that we have a basic understanding of Kerberos, we will examine the policies that can be set with GPOs and how they affect security.

Enforce user login restrictions
This setting checks at every session ticket request that the account is allowed to log on locally or access the local computer from the network. It also checks that the account requesting the session ticket is still valid. This setting is enabled by default and really should not be turned off. It will increase network traffic, but in GIAC Enterprises' case this is not a concern. We therefore leave this setting enabled.

Maximum lifetime for a service ticket
This setting is actually the maximum length of time that a session ticket can exist. A good rule of thumb is to keep this value close to the length of a user's working day. (I.e. their daily session)

© SANS Institute 2000 - 2005 Author retains full rights.

Note that session tickets are destroyed when the user logs off from their workstation. Since GIAC Enterprises' working hours are 9AM to 5 PM, we set this value to 8.5 hours.

Maximum lifetime for a user ticket renewal
A user ticket or Ticket Granting Ticket must be renewed after the time specified in this setting. This renewal process allows for less traffic and interaction than creating a brand new TGT by starting a new authentication cycle. Note that TGTs are stored in a credentials cache located in the workstation's RAM. Since we are not concerned with the traffic and performance implication we allow for a renewal time of 2 hours. Note that this renewal process is completely transparent to users logged in.

Maximum lifetime for a user ticket
This is actually the lifetime of the TGT or Ticket Granting Ticket. Since TGTs must be renewed after 4 hours, and we are not too concerned with traffic and performance, we set this value to 1 day. This will allow for 5 additional renewals after the initial user ticket was granted.

Maximum tolerance for computer clock synchronization
Since part of the authentication data inside of Kerberos tickets include timestamps, there is need to ensure that all three players have the same system time. However, it is not likely that all computers will have exactly the same system time. Therefore the Kerberos protocol makes an allowance that is settable with this parameter. Recall from our network design that only the switches and the DC with the PDC emulator FSMO role obtain their system time from the stratum 1 clock. All workstations obtain their time from that DC. In addition the network infrastructure consists of a fully switched network with a Gigabit Layer 3 switch. Connectivity should be excellent and time skew between workstations should be minimal. (The SNTP protocol is designed for a maximum skew of 2 seconds with the same site) We therefore reduce this setting from its default value of 5 minutes to 1 minute. This should severely curtail any replay attacks.

Local Policies

Local policies consist of 3 subsets:

1. Audit policy
2. User rights assignment
3. Security options

Since there are many settings in each that have a relatively small effect on security we will examine only the key settings.

Audit Policy

All audit policies have the same format. Basically you decide what type of event to audit (or not) and whether to audit the failure or success or both.

© SANS Institute 2000 - 2005 Author retains full rights.

Audit account logon events
Auditing logon events is a must. This setting audits event when a user logs on or off any computer in the domain. This setting affects the domain controller event logs and should be set at the default domain controller policy level. At the domain level, for computers other than domain controllers, this setting only captures logon attempts to local accounts. Being fairly paranoid, we set auditing for account logon to both failure and success.

Audit account management
This setting records events when account are created, deleted or changed including group membership and password changes. Again we should at the very least audit failed attempts at changing accounts. For example, this would record hacker attempts to increase their privileges by adding themselves to administrative groups. We therefore set the auditing to record failures only.

Audit logon events
This setting is related to the audit account logon setting. It captures any logon attempt to the computer it applies to (i.e. local account) including network-based attempts. If event log settings allow for it we should also log account logon successes. This would allow for possible correlation with IDS systems should an account have been compromised. Later on we will see how event log settings can be set to accommodate large number of events. We therefore audit both logon failures and successes.

Audit system events
This setting audits event where a user reboots or shuts down the computer or when the security event log is affected. This is definitely an easy choice to make. We audit both failure and success of audit system events.

The remaining audit policies remain undefined at the domain level.

User Rights Assignment

Access this computer from the network
We don't want unauthorized users to access workstations across the network. Although some of this access is already restricted with the ACLs internally, and of course the firewalls externally, only users already authenticated should be part of this policy. We therefore add the authenticated users to this policy.

Add workstations to domain
Although it would be desirable and useful to separate this function and add this right to a dedicated account or group, the ability to add workstations cannot be removed from the default accounts such as domain admin. Therefore we do not set this policy and use the built-in accounts for this function.

Change the system time

© SANS Institute 2000 - 2005 Author retains full rights.

Since all computers in the GIAC Enterprises' domain synchronize their time directly or indirectly with an external NTP time source, we do not want any account to change the system time. This right is always available to the usual set of administrative accounts. Unfortunately there is no 'deny change the system time' setting. Therefore we will not add any accounts to the policy.

Deny access to this computer from the network
If possible we want to deny any unauthorized or unauthenticated accounts from accessing workstations in the domain. We therefore add the built-in group guests to be denied access from the network.

The remaining settings will be undefined at the domain level.

Security Options

Additional restrictions for anonymous connections.
This setting was created to prevent null session enumeration of accounts, etc. Null sessions require absolute no authentication whatsoever are were designed for the SYSTEM account to communicate over the network with other computers. Assuming that we have no backup software that requires null sessions we are setting this policy to the most restrictive:
No access without explicit permissions.

Automatically log off users when logon time expires
Assuming that we have defined appropriate time windows for our users to logon, this setting should be disabled. Users should be informed that they are expected to log off upon departing the building and that there is a risk of data loss when their sessions are automatically logged off.

Automatically log off users when logon time expires (local)
This is the same as above except that it applies to local accounts on member servers and workstations. We are not expecting users to log on locally but just in case we should enable this setting with the same caveats as noted above.

Clear virtual memory pagefile when system shuts down
This setting will ensure that the pagefile will be wiped out when the system shuts down. This prevents hackers who have physical access to a workstation from booting into an alternative OS and examining the contents of the pagefile for sensitive date. This setting is turned on. Note that on machines with a large pagefile that the shutdown can take a few minutes.

Disable CTRL+ALT+DEL requirement for logon
This setting was conceived with user convenience in mind. Store the user information in the local registry and no need to enter it again. Of course, an intruder needs only to unplug the machine, plug it back in and will have obtained access to an authorized account. In a worst-case scenario this could be an administrative account. This setting has to be enabled for all computers.

© SANS Institute 2000 - 2005 Author retains full rights.

Do not display last user name at in logon screen
This setting is enabled to prevent casual workstation hoppers from easily determining account names. Note that with standard naming conventions, most co-workers and would be hackers will be able to determine account names.

LAN manager authentication level
This setting has very little meaning in an environment where all computers are Windows 2000, since Kerberos will be the authentication method of choice. However, in the case of a denial of service attack on Kerberos authentication, or a rogue NT4 workstation, the Windows 2000 systems are supposed to revert back to the old LAN manager authentication scheme. We therefore set this policy to the most secure setting available:
Send NTLMv2 response only\refuse LM & NTLM.

Message Text for users attempting to log on
This is the text of the window that pops up on interactive log on. To discourage employees from station hopping and to ensure that GIAC Enterprises is covered from a legal standpoint we put in the following message:

```
Access to this computer is for authorized GIAC Enterprises employees and
contractors only. Unauthorized access will be logged. GIAC Enterprises will
prosecute offenders to the full extend of the law.
```

Message Title for users attempting to log on
This is the title of the window that pops up on interactive log on. It should be complimentary to the text below it. We set it as follow:

```
Warning: GIAC Enterprise Authorized System Access.
```

Prevent users from installing printer drivers
Printer drivers operate at the kernel level in Windows 2000. A rogue or 'Trojan' printer driver could assume full access of the local system. Although it will be inconvenient to both the users and administrators, we want to ensure that only authorized and tested printer drivers are installed. This setting is therefore enabled.

Prompt user to change password before expiration
This setting adds little to overall security but should prove to be of some convenience to administrator. (I.e. less support calls) This policy is set to three days. This should provide the user with sufficient 'nagging' to change the password before it expires and the department account administrator has to reset it.

The remaining settings are undefined at the domain level.

Event log

The event log policies contain a single subsection.

1. Settings for the Event Log

© SANS Institute 2000 - 2005 Author retains full rights.

Maximum application log size
Maximum system log size
Assuming that all servers and workstations have sufficient disk space, we set both policies to about an eight of the maximum size. (524280 Kbytes.) This should provide sufficient event log capacity while not encroaching on the average disk size of the workstation.

Restrict guest access to application log
Restrict guest access to system log
Only the authorized users should have access to the event logs. Therefore these settings are enabled

Retain application log
Retain system log
Considering the maximum size of application and system log, we chose to keep these logs for 14 days. Note: this may actually be shorted based on the next setting of retention method.

Retention method for application log
Retention method for system log
The application and system logs are not quite as critical to security as the security log. We therefore set the retention method to 'As Needed' This policy will effectively keep the logs for the 14 days unless the logs reach their maximum size. Then the log entries will be overwritten from the beginning.

Maximum security log size
For event correlation and forensic purposes the security log can provide valuable data. We therefore choose to set the security log size to the allowable maximum of 4194240 Kilobytes.

Retain security log
This setting will remain undefined since the next setting will override any value set.

Retention method for security log
To ensure that we capture all of the security events this policy is set to 'Do not overwrite events'

Shut down the computer when the security audit log is full
This setting will immediately force the computer to shutdown once the security log size reached the 4 GB limit. This setting is enabled.

There is a risk of a denial of service attack when using the above settings for the security log. A hacker could generate many log on attempts (regardless of lockout status) and each would be logged. This would fill up the security log and shut down the system. To mitigate this risk we should write some sort of batch file or script that will regularly copy and clear the security log.

© SANS Institute 2000 - 2005 Author retains full rights.

Restricted Groups

This option allows for 'hard coding' of memberships in sensitive groups. For example, only members of the IT department are allowed to be in the Domain Admins group. This ensures that any unauthorized user is not able to add an unauthorized account to the Domain Admins group. We repeat this exercise for all the other 'admin' type groups such as Enterprise Admins, Schema Admins, Account Operators, Server Operators and so on.

See Appendix D for instructions on adding only the IT department to the Domain Admins group using the Restricted Groups feature.

System Services:

At the domain level few system services need to be set. Two key services are set for every machine in the domain to ensure that they are always started and cannot be tampered with.

Event log service
IPSEC policy agent

Each service has the Restricted Group and System Group with Full Control and each service is started automatically. This ensures that no unauthorized account has access to the event log and that every workstation will be able to accept secure communication when desirable. See Appendix E for details on setting the options and security settings for system services.

IPSEC policies:

IPSEC provides authentication and encryption for IP packets. Windows 2000 inherently supports IPSEC and settings are applied using GPO. Our goal is to match the ACL restrictions between VLANs with IPSEC settings at each server and workstation. Since every workstation and server is isolated on a Layer 2 switched port, it is unnecessary to require encryption for all traffic. This is done only as an extra layer of security. (Defense in depth)
However, authentication should be required for all traffic at the domain level. The exception to this rule is newly configured workstations, which need to contact a domain controller in order to join the domain. Since the workstations need to be members of the domain to authenticate, this would create a chicken and egg scenario.
(See Appendix F for details on setting these options.)
One thing to keep in mind is that IPSEC policies are not cumulative; they are replaced until the last GPO is applied.

Domain Controllers

Now that we have defined the default domain settings, lets move on to the default domain

© SANS Institute 2000 - 2005 Author retains full rights.

controller settings. The domain controllers are the 'crown jewels' of the GIAC Enterprises' network. As such, they require more security than usual.

To edit the domain controller GPO settings, open the Active Directory Users and Computers snap-in, right click on the Domain Controllers container and select properties. Select the Group Policy tab and double click on the default domain controllers policy.

Note that all domain controllers take the following settings from the domain level settings, and therefore should not be set at the domain controller OU as well.

- All settings in Account Policies
- Three settings in Local Policies\Options
  1. Automatically log off users when logon time expires
  2. Rename administrator account.
  3. Rename guest account.

We will examine only those settings that, for security reasons, are different from the domain level group policies or settings that were previously undefined.

Local Policies

Audit policy

Audit directory service access
We want to ensure that any unauthorized attempts at enumerating active directory objects are logged. We therefore set this policy to log all failures.

Audit object access
This setting audits access to any object to that has its own security access control list such as printers, files, folders, etc. Due to the large amount of data that would be generated if we audited both success and failure, we decide to only audit failure.

Audit policy change
Authorized administrators should only make group policy changes. Since policy changes should generally not happen very often, we audit both failure and success.

User Rights Assignment

Back up files and directories
On the domain controllers this right is assigned only to the built-in administrators group. Keep in mind that any service accounts for third party backup utilities will need to be placed in the administrators group.

© SANS Institute 2000 - 2005 Author retains full rights.

Enable computer and user accounts to be trusted for delegation
This is a very sensitive setting since it allows the recipient to allocate rights that could create accounts, etc. This setting should be assigned to administrators only.

Force shutdown from a remote system
Obviously the only accounts that should be able to shut down the domain controllers remotely are the built-in administrators group.

Log on locally
This setting should definitely be restricted to administrators only. This shouldn't be a huge issue if the domain controllers are physically secured.

The remaining user rights assignment settings are either the same as the domain level settings or remain undefined.

Security Options

Audit use of backup and restore privilege
Only authorized third party backup/restore should be using these privileges on domain controllers. We therefore enabled this policy.

Send unencrypted password to connect to third party SMB servers
Since we do not deploy third party SMB servers, this policy is disabled. This should prevent hackers from impersonating third party SMB servers and collecting clear text passwords with a network sniffer.

Shut down system immediately if unable to log security audits
To avoid denial of service attacks on the domain controllers we will disable this setting.

Smart card removal behavior
Since all of the IT staff is issued smart cards, and the domain controllers are equipped with domain controllers, we are going to ensure that they are logged off when leaving the domain controller console. The setting is set to 'force logoff'

Unsigned driver installation behavior
Since our domain controllers are brand name Compaq servers, we will more than likely have signed drivers available. We therefore set this policy to 'do not allow installation'

Event Log Settings

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

The only setting for domain controllers that needs to be change is:

Shut down the computer when the security audit log is full
This setting is disabled to prevent any denial of service attacks on the event log.

IPSEC Policies

Although we can set the IPSEC policies for the domain controllers using the GPO GUI, most administrators are used to command line utilities.

Fortunately, there is a command line utility just for this occasion that can be found in the Windows 2000 server resource kit. IPSECPOL.EXE is also available from Microsoft at the following URL:

http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/ipsecpol-o.asp

The following example shows how to use IPSECPOL.EXE in a VBscript file.

```
Dim Shell
Dim PolicyName
Dim PolicyType
Dim FilterList
Dim RuleName
Dim NegotiationPolicyList

Set Shell = WScript.CreateObject("WScript.Shell")

PolicyName = "DomainControllerPolicy"
PolicyType = "REG"

'first block all traffic
FilterList = "0:*+*:*"
RuleName = "DenyAll"
NegotiationPolicyList = "BLOCK"

cmd = "IPSECPol -f " & FilterList & " -r " & RuleName & " -n " & NegotiationPolicyList &
" -w " & PolicyType & " -p " & PolicyName & " -x"

'now add a rule to authenticate all traffic from our intranet network

FilterList = "0:*=172.16.0.0/255.255.255.0:*"
RuleName = "AuthIntraNet"
NegotiationPolicyList = "AH[MD]"

cmd = "IPSECPol -f " & FilterList & " -r " & RuleName & " -n " & NegotiationPolicyList &
" -w " & PolicyType & " -p " & PolicyName & " -x"

Shell.Run(cmd)

'now encrypt all traffic on the production server VLAN
```


© SANS Institute 2000 - 2005 Author retains full rights.

```
FilterList = "0:*+172.16.50.0/255.255.255.0:*"
RuleName = "EncryptProdServers"
NegotiationPolicyList = "ESP[3DES,SHA]"

cmd = "IPSECPol -f " & FilterList & " -r " & RuleName & " -n " & NegotiationPolicyList &
" -w " & PolicyType & " -p " & PolicyName & " -x"

Shell.Run(cmd)
```

Note that we start with a 'deny everything' and selectively allow resources. This follows the Least Privilege principle. Keep in mind that the most specific filter will be applied. This is different from Cisco ACLs, which are applied as soon as an Access Control Entry matches the conditions required. Also, Cisco ACLs have an implied 'deny all' entry at the end.

Now that we have secured the domain controllers, the next few pages detail additional or different security settings for the remaining Organizational Units.
These changes focus on the IPSEC policies that are required to enable the applications used by the departments in each OU.
Only a sample of all total applications is given here for brevity as listing them all serves no purpose. The format is as follows:

1. Short description of the rule.
2. The filter used. (as it appears using IPSECPOL.EXE)
3. The Negotiation policy. (block, pass, etc)

The following filters are set for each OU.

Proxy server access to ISA server HongKong without encryption. The proxy server is set to listen on port 8080
FilterList = 0+172.16.60.4:8080:TCP
NegotiationPolicyList = PASS

DNS resolution access to both domain controllers without encryption.
FilterList = 0+172.16.50.5:53:* 0+172.16.50.6:53:*
NegotiationPolicyList = PASS

POP3 and SMTP access to the exchange server. Encrypted and authenticated.
FilterList = 0+172.16.60.2:110:* 0+172.16.50.2:25:*
NegotiationPolicyList = ESP[3DES,SHA]

Workstations\IT

Terminal Services access to production servers, DMZ servers, and domain controllers, always encrypt and authenticate this traffic.

© SANS Institute 2000 - 2005 Author retains full rights.

FilterList = 0+172.16.*.*:3389:TCP
Negotiation Policy = ESP[3DES,SHA]

Workstations\HR & F

SQL server access to accounting server Yuan, always encrypted at 3DES with SHA.
FilterList = 0+172.16.500.4:1433:TCP
NegotiationPolicyList = ESP[3DES,SHA]

Workstations\R & D

SQL server access to CRM server YIN , always encrypted at 3DES with SHA.
FilterList = 0+172.16.50.7:1433:TCP
NegotiationPolicyList = ESP[3DES,SHA]

Workstations\S & M

SQL server access to CRM server YIN , always encrypted at 3DES with SHA.
FilterList = 0+172.16.50.7:1433:TCP
NegotiationPolicyList = ESP[3DES,SHA]

Although by no means a complete list, this should give the reader a good understanding of how to allow access for each departmental OU based on the application deployed.

Production Servers

Production servers should match the settings for the workstations as well as any access to and from the DMZ and the domain controller. Again, for brevity, the entire list of rules will not be shown, Instead an example, matching the two rules above is shown. The CRM SQL server has the following rule to allow access from the R & D and S & M VLANs:

FilterList = 0:1433:TCP+172.16.10.0 0:1433:TCP+172.16.200.0
NegotiationPolicyList = ESP[3DES,SHA]

In addition to rules that match the above workstations and the "DenyAll" rule, the production servers will also have rules to force encryption between themselves and the domain controller as well as traffic to and from the DMZ.

DMZ Servers

Servers in the DMZ communicate with the Internet as well as intranet servers and workstations. Separate IPSEC filter lists are required for the internal connection and the external connection. These policies should match both the intranet ACLs as well as the internal and external firewall configurations.

© SANS Institute 2000 - 2005 Author retains full rights.

The following is an example of a policy to be deployed on the public web server. This server listens on port 80 on the outside only and requires encryption for all traffic on the intranet. Again the 'BlockAll' rule is implied.

FilterList = 219.183.19.3:80+*::TCP
NegotiationPolicyList = PASS
FilterList = 172.16.*.*+*
NegotiationPolicyList = ESP[3DES,SHA]

We repeat this process for the other servers in the DMZ.

Security considerations that can't be addressed with Group Policy Objects

Now that we have reasonably secured the infrastructure, we need to keep track of any possible attempts at security breaches. Saving the event log of all the servers with the resource kit dumpel.exe does this. We can schedule a daily upload of the event to deploy a batch file. Then each server copies its event logs to a central place. (This is also useful when deploying IDS systems, as it allows for data correlation)

One of the questions that come up is: how do you stop Joe Black in R&D from logging into a workstation in the IT department? One way of doing this is to restrict the workstations that a user can log into. You can only restrict workstation by NETBIOS computer name. Therefore we need to enumerate the workstations that are not part of the user's OU and add them to the list.

Conclusion:

Securing Active Directory is by no means a trivial task. Certainly deploying Active Directory itself requires significant planning. Expect to spend a similar amount of planning on the security portion of Active Directory. This document has focused on the infrastructure or 'network plumbing' portion of security. Additional facets such as O/S hardening, SQL server security and application level security need to be considered to provide a comprehensive 'defense in depth' strategy.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Appendix A VLAN and ACL configuration examples

The IT department has been assigned VLAN 50 This VLAN created on the layer 2 switch with the following IOS commands: (from privileged EXEC mode, comments in **bold green**)

```
L2_Switch#vlan database
enter VLAN configuration
L2_Switch(VLAN)#VLAN 50 name VLAN_50_IT_DEPT
assign id and name
VLAN 50 added:
    Name: VLAN_50_IT_DEPT
L2_Switch(VLAN)#exit
leave the configuration mode
APPLY completed.
Exiting....
L2_Switch#copy running-config startup-config
save changes
Destination filename [startup-config]?
Building configuration...
[OK]
L2_Switch#show VLAN id 50
display VLAN configuration
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
50   VLAN_50_IT_DEPT                  active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
50   enet  100050     1500  -      -      -        -    -        0      0
```

We now add the switch port (called an interface) to the VLAN. (again IOS from privileged EXEC mode)

```
L2_Switch#configure terminal
enter config mode
Enter configuration commands, one per line.  End with CNTL/Z.
L2_Switch(config)#interface FastEthernet 0/1
config port #1
L2_Switch(config-if)#switchport mode access
set VLAN membership mode
L2_Switch(config-if)#switchport access VLAN 50
assign to VLAN
L2_Switch(config-if)#end
L2_Switch#
L2_Switch#show running-config interface FastEthernet 0/1
display the config
Building configuration...

Current configuration:
!
interface FastEthernet0/1
 switchport access VLAN 50
end

L2_Switch#copy running-config startup-config
save the config
Destination filename [startup-config]?
Building configuration...
```


© SANS Institute 2000 - 2005 Author retains full rights.

To add a MAC address to the IT department VLAN

```
L2_Switch#configure terminal
enter config mode
Enter configuration commands, one per line.  End with CNTL/Z.
L2_Switch(config-if)#mac-address-table static 0010.A49A.FE90 interface
L2_Switch(config-if)#end
```

Now we need to secure the port

```
L2_Switch#configure terminal
enter config mode
Enter configuration commands, one per line.  End with CNTL/Z.
L2_Switch(config)#interface FastEthernet 0/1
config port #1
L2_Switch(config-if)#port security  max-mac-count 1
allow only 1 mac address
L2_Switch(config-if)#port security action shutdown
 stop all traffic another MAC address connects.
L2_Switch(config-if)#end
```

Now that we have secured the port we need to create access control lists on the Layer 3 switch. Note that routing between 2 VLANs requires setting the ACL on 2 interfaces. Each VLAN can have one or more IP addresses attached to it called a Switched Virtual Interface (SVI) This SVI is the default gateway for all the hosts on that particular VLAN. (Remember the one to one relationship between a VLAN and an IP subnet)

Below is an example of an ACL for terminal access from VLAN 40 (IT department, subnet 172.16.40.0) to servers in the production VLAN.

Assume that the 172.16.40.1 (default gateway for VLAN 40) is defined on the first Gigabit Interface.
IOS from privileged EXEC mode

```
L3_Switch#configure terminal
enter config mode
Enter configuration commands, one per line.  End with CNTL/Z.
L3_Switch(config)#ip access-list extended TRM_SRV_VLAN40_OUT
create named access list
L3_Switch(config)# permit tcp 172.16.40.0 172.16.50.0 0.0.0.255 eq 3389 established
filter terminal server traffic including fragmented packets
L3_Switch(config)#interface gigabitethernet 0/1
configure the first interface
L3_Switch(config-if)#ip access-group TRM_SRV_VLAN40_OUT out
assign the ACL to the outbound part of the interface
L3_Switch(config-if)#end
```

Assume that the 172.16.50.1 (default gateway for VLAN 50) is defined on the second Gigabit Interface.
IOS from privileged EXEC mode

```
L3_Switch#configure terminal
enter config mode
Enter configuration commands, one per line.  End with CNTL/Z.
```


© SANS Institute 2000 - 2005 Author retains full rights.

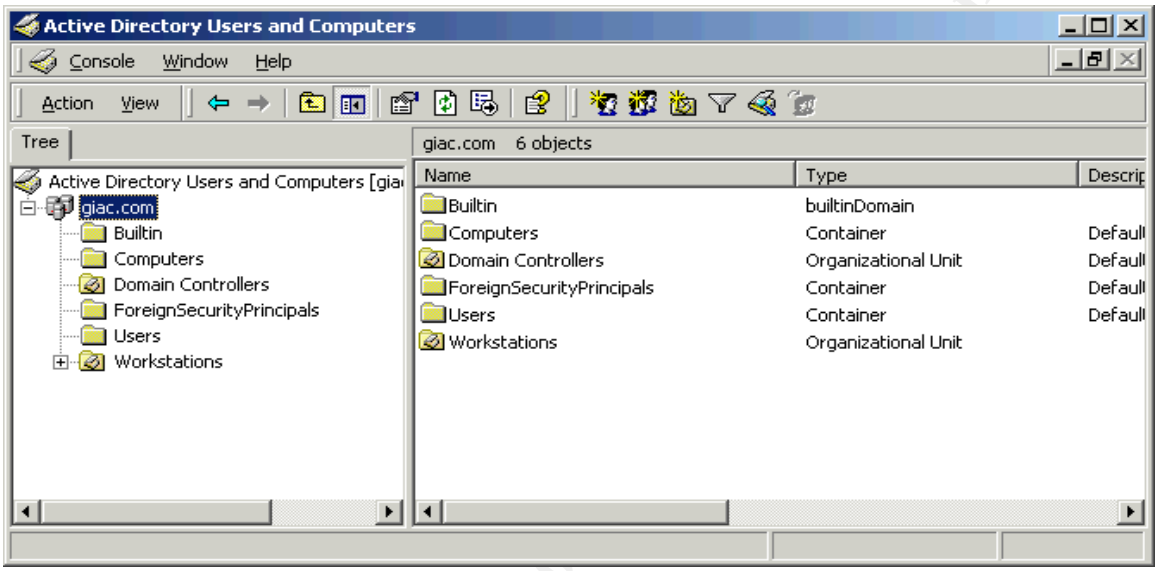
```
L3_Switch(config)#ip access-list extended TRM_SRV_VLAN50_IN
named access list
L3_Switch(config)# permit tcp 172.16.40.0 172.16.50.0 0.0.0.255 eq 3389 established
filter terminal server traffic including fragmented packets
L3_Switch(config)#interface gigabitethernet 0/1
configure the second interface
L3_Switch(config-if)#ip access-group TRM_SRV_VLAN50_IN out
assign the ACL to the inbound part of the interface
L3_Switch(config-if)#end
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

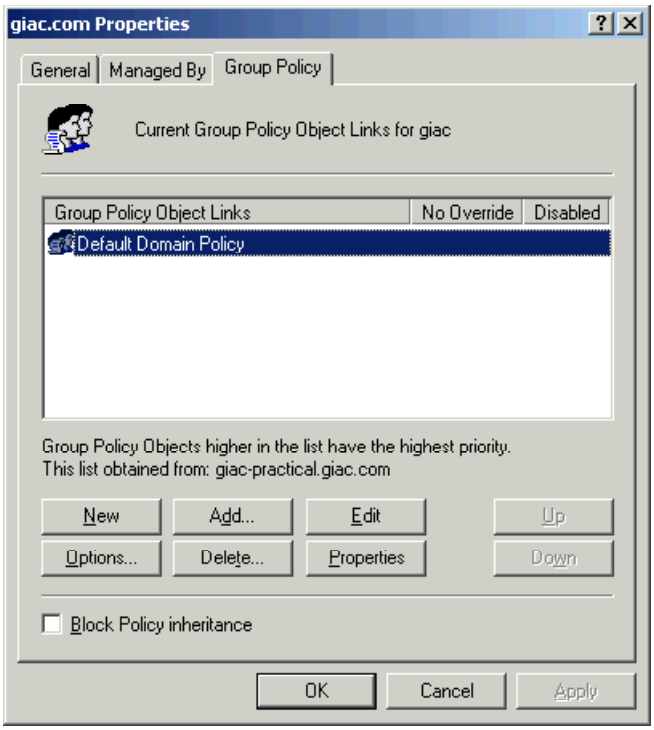
Appendix B Importing security settings from a security template.

Security templates are text files with an .inf file extension. Windows 2000 comes with several predefined templates that can be found in security\templates folder underneath the 'systemroot' folder. (Usually C:\Winnt)
To import a template open the Active Directory Users and Computers MMC snap-in. (Alternatively run mmc /a and use the add/remove snap-in functionality to create your own custom management console)



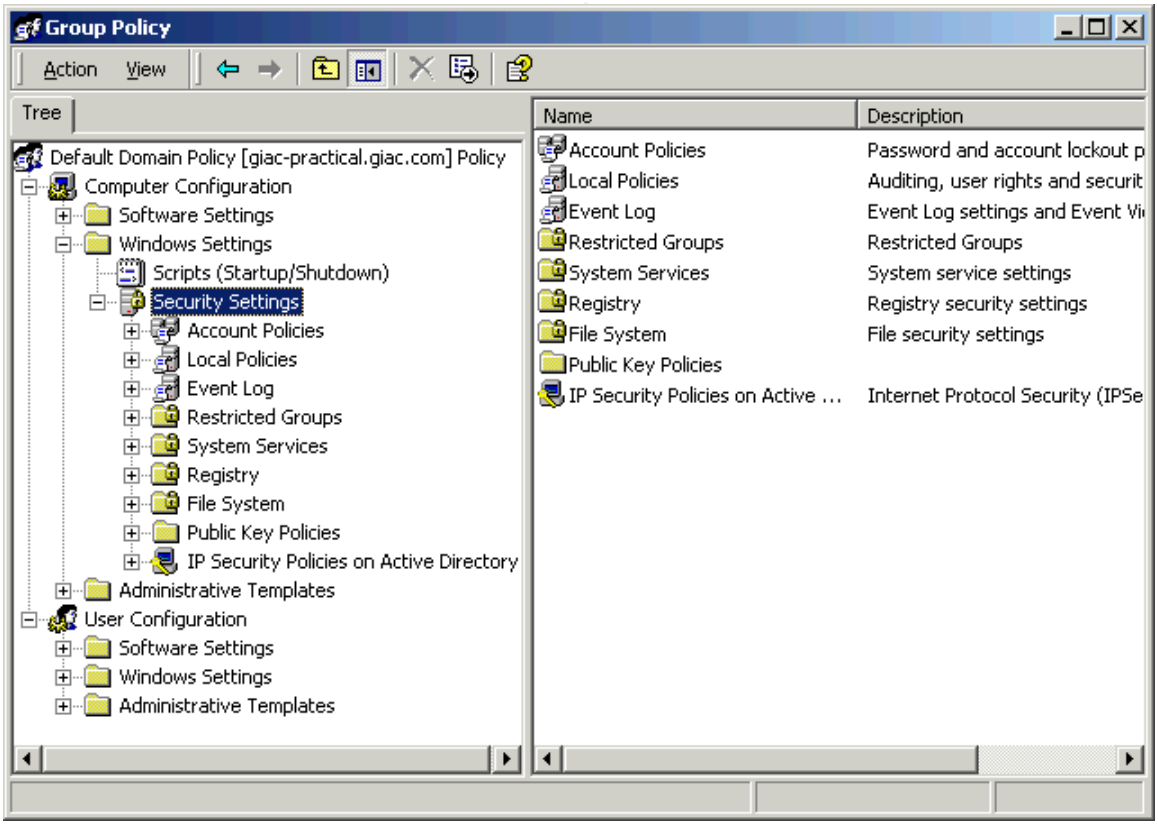
Right click on the domain (giac.com) and select properties. Click on the Group Policies Tab.

© SANS Institute 2000 - 2005 Author retains full rights.



Select the Default Domain Policy and click the Edit button.

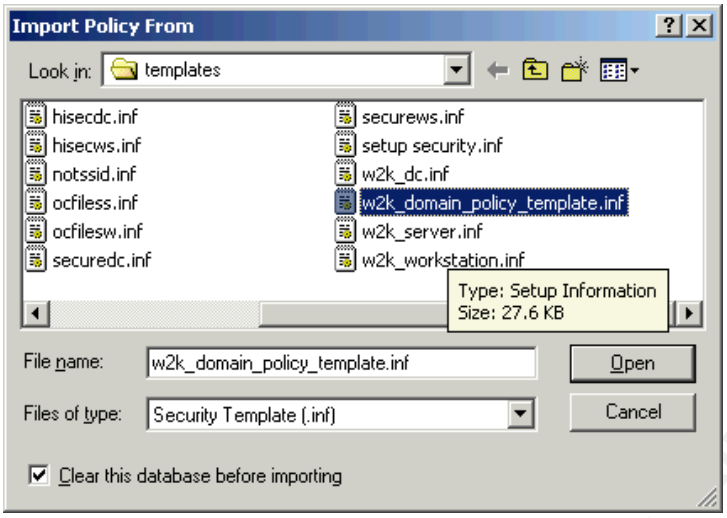
In the Group Policy window expand the Windows Setting folder and select security settings.



© 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Right click the Security Settings container and select Import Policy. You will be able to select any template file. (Requires an .inf file extension) The import process does not override settings if they are not defined in the template. To ensure settings not defined in the template are set to undefined, click on the 'clear this database before importing' checkbox.



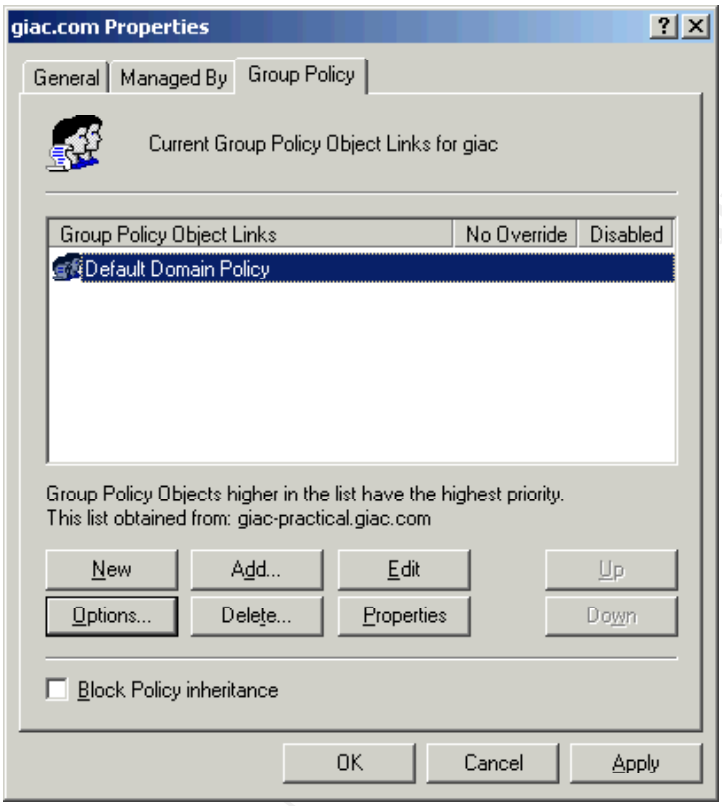
© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

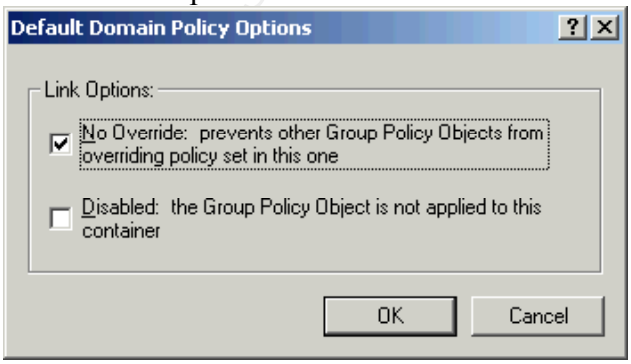
Appendix C Setting the No Override option for the default domain

Setting the No Override option will force the GPO settings at the default domain (or any other container) to be applied regardless of any Block Policy Inheritance settings at containers underneath. Note that at the highest level (site) you cannot turn on Block Policy Inheritance since the site container does not have a parent container.

Open the Active Directory Users and Computers snap-in. Right click on the domain container, click properties.

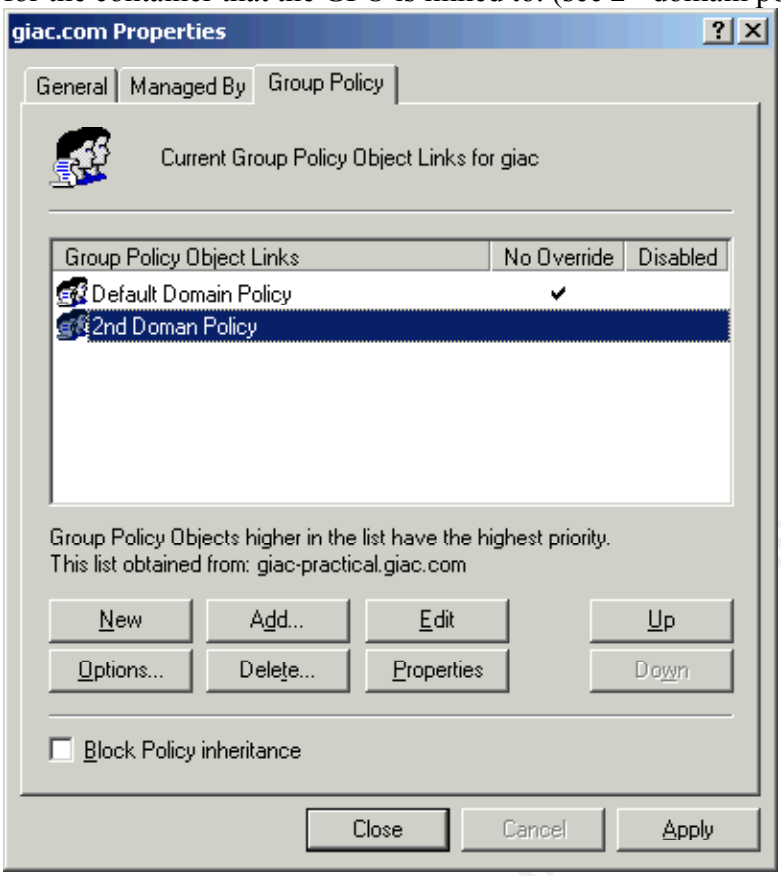


Click on the Options button and check the No Override checkbox



© SANS Institute 2000 - 2005 Author retains full rights.

There should now be a checkmark next to the GPO. Note that this option is enabled per GPO not for the container that the GPO is linked to. (see 2nd domain policy below with no checkmark)

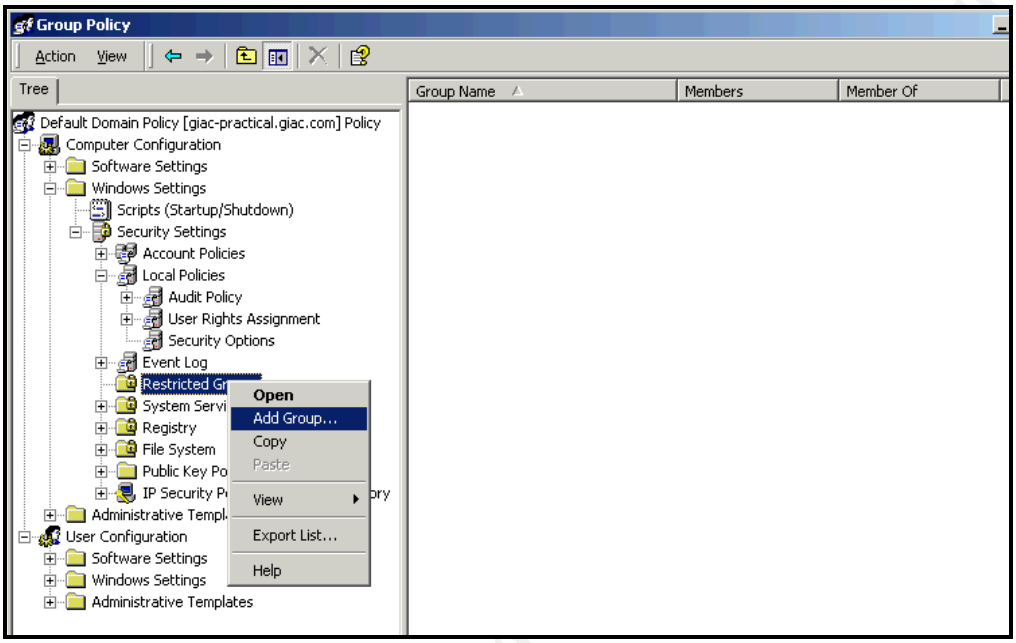


© SANS Institute 2000 - 2005 Author retains full rights.

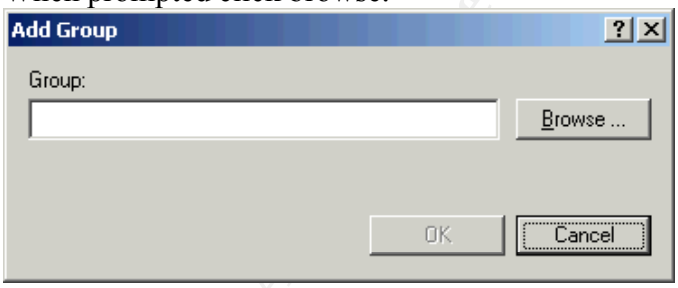
© SANS Institute 2000 - 2005 Author retains full rights.

Appendix D Restricting Domain Admin membership to IT staff using restricted groups

Using the Active Directory MMC snap-in, navigate to the domain default group policy. Expand the Windows Settings/Security Settings folder. Right click the Restricted Group Folder and select Add Group…

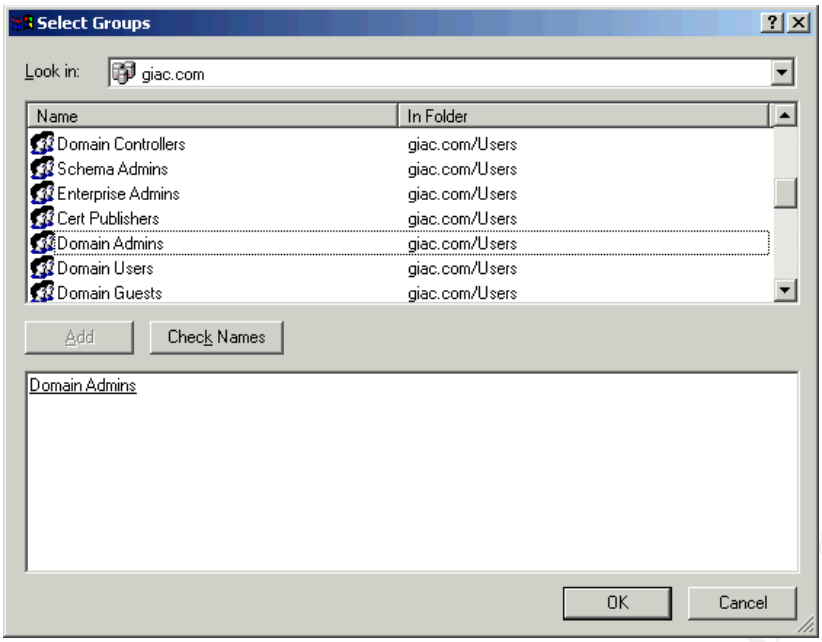


When prompted click browse.

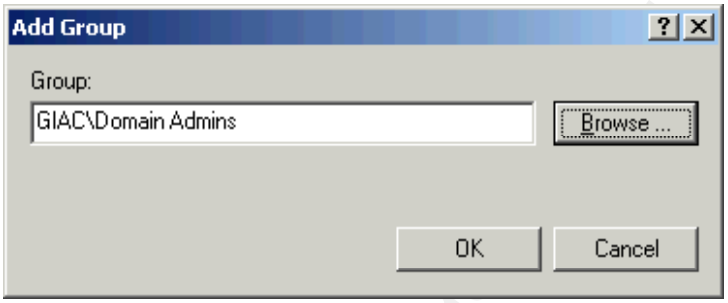


Select the Domain Admins group and click OK

© SANS Institute 2000 - 2005 Author retains full rights.



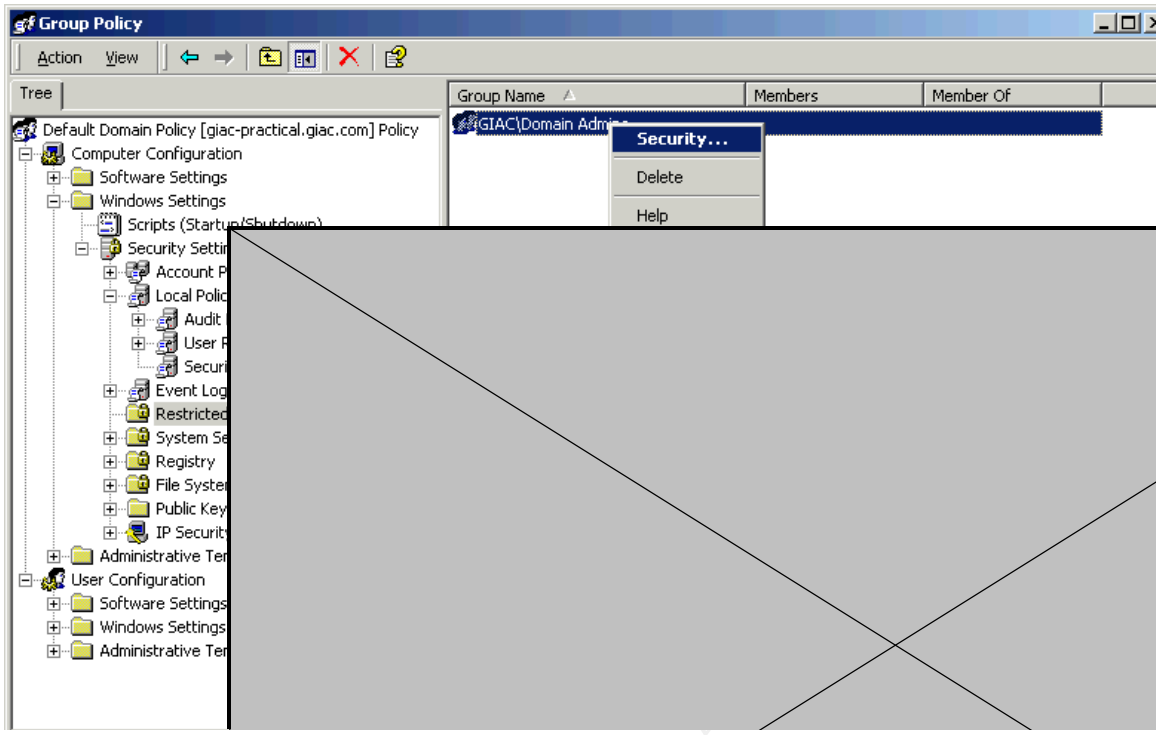
Click OK again to return to the main window of the snap-in



Right Click the new Domain Admins group and select Security

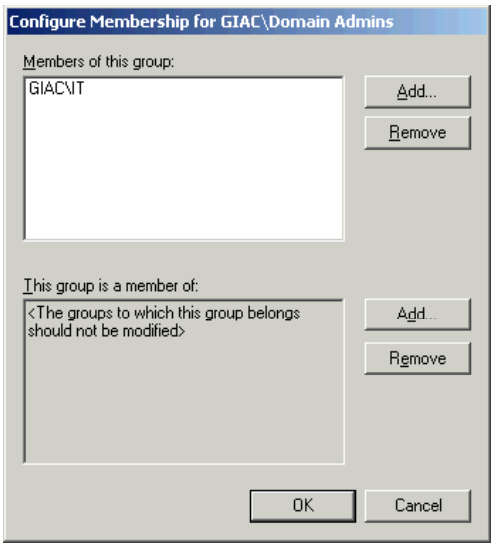
© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.



© SANS Institute 2000 - 2005,

© SANS Institute 2000 - 2005 Author retains full rights.

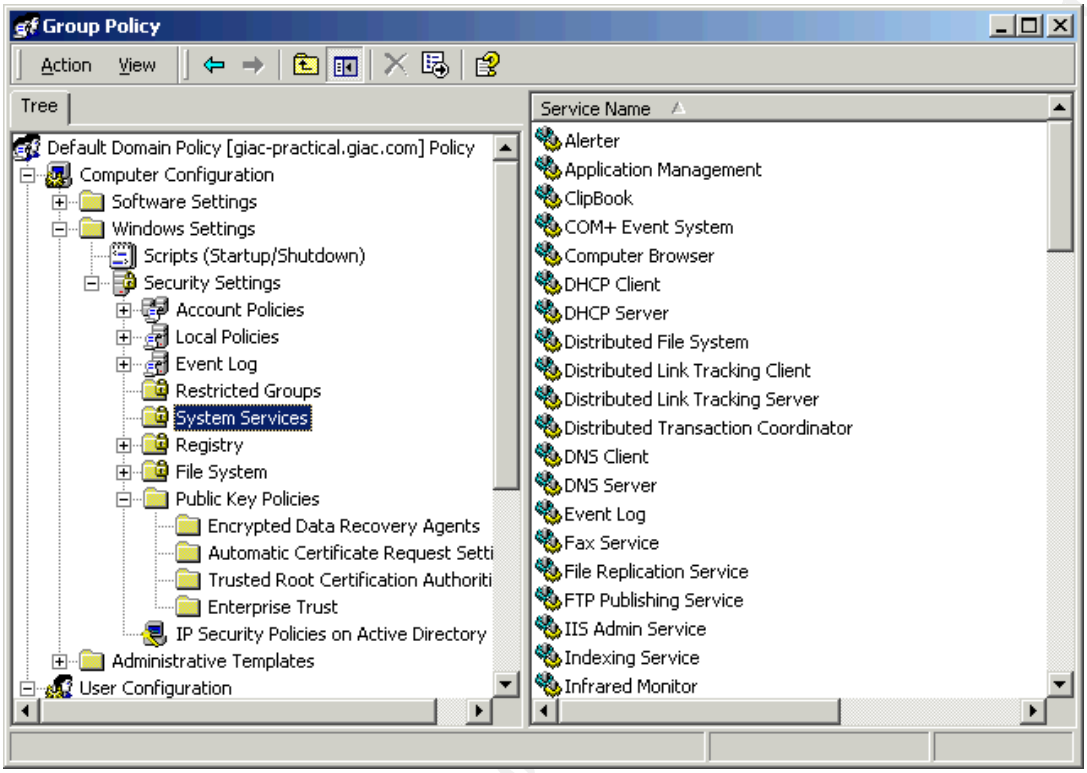


© SANS Institute 2000 - 2005, Author retains full rights.

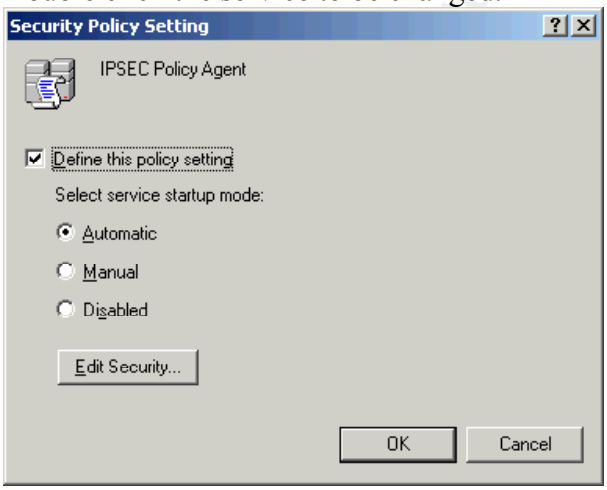
© SANS Institute 2000 - 2005 Author retains full rights.

Appendix E Setting System Services options

From the Group Policy snap-in expand the Windows Setting\Security Settings\System Services.

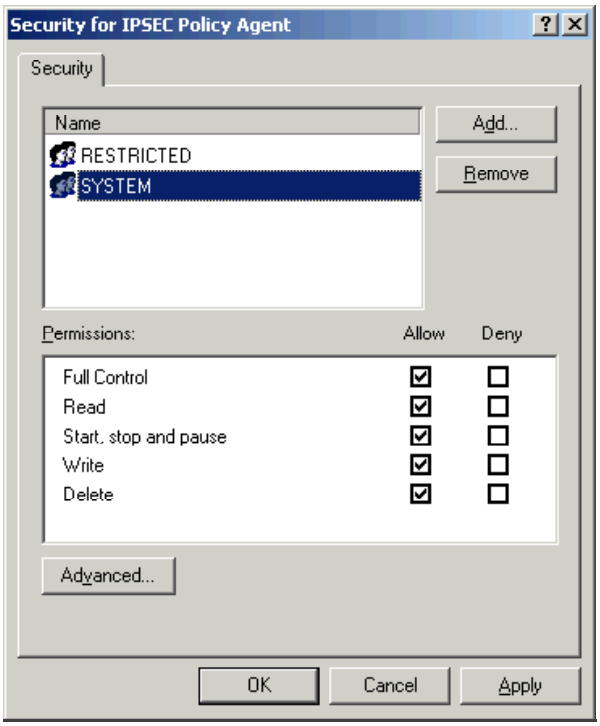


Double click the service to be changed.



Check the 'Define this policy setting' checkbox to activate the setting. Select Automatic for the startup mode and click on the Edit Security button.
Add the Restricted Group and the System group.

© SANS Institute 2000 - 2005 Author retains full rights.

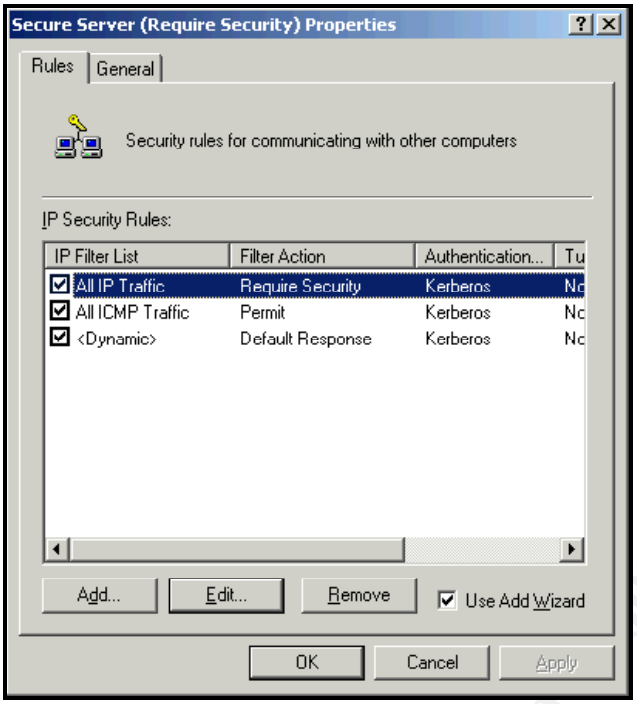


© SANS Institute 2000 - 2005, Author retains full rights.

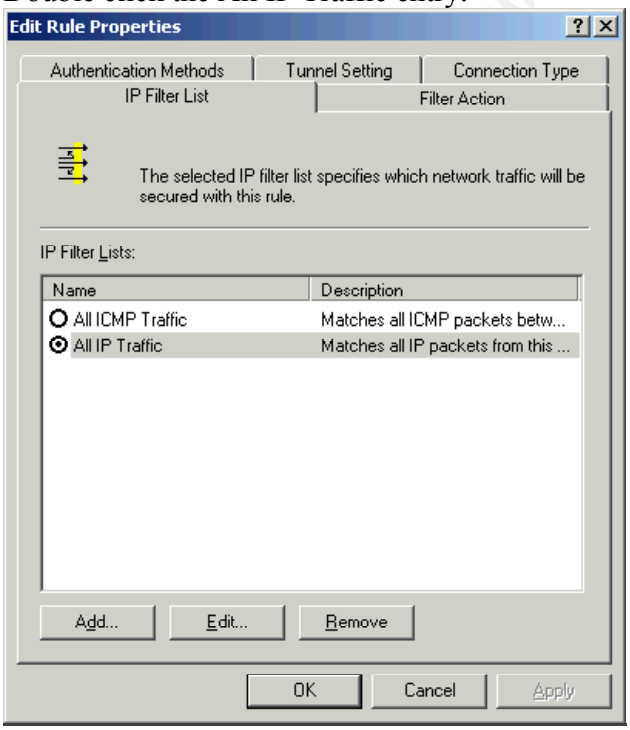
© SANS Institute 2000 - 2005
Author retains full rights.

Appendix F IPSEC policies for authentication but not encryption

From the Group Policy snap-in expand the Windows Setting\Security Settings\IP security settings for active directory folder. Double click on the Secure Server entry.

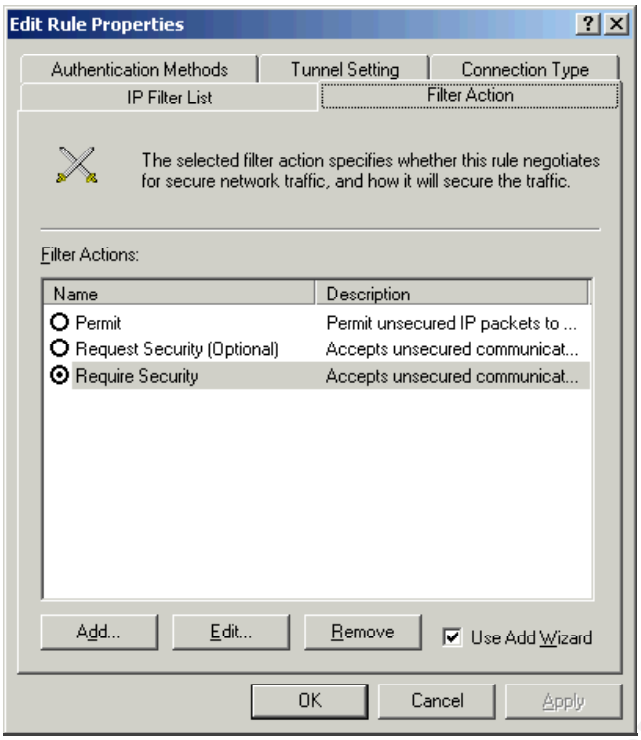


Double click the All IP Traffic entry.

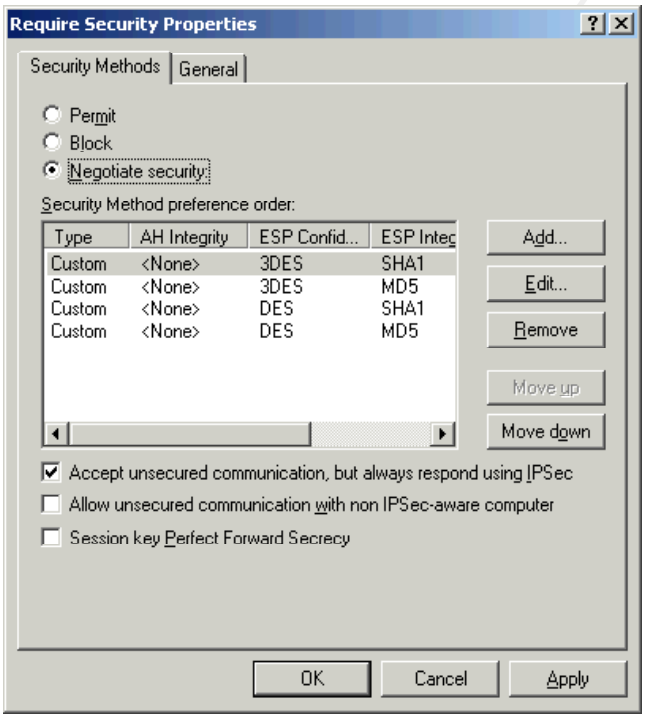


© SANS Institute 2000 - 2005 Author retains full rights.

Select the Filter Methods.



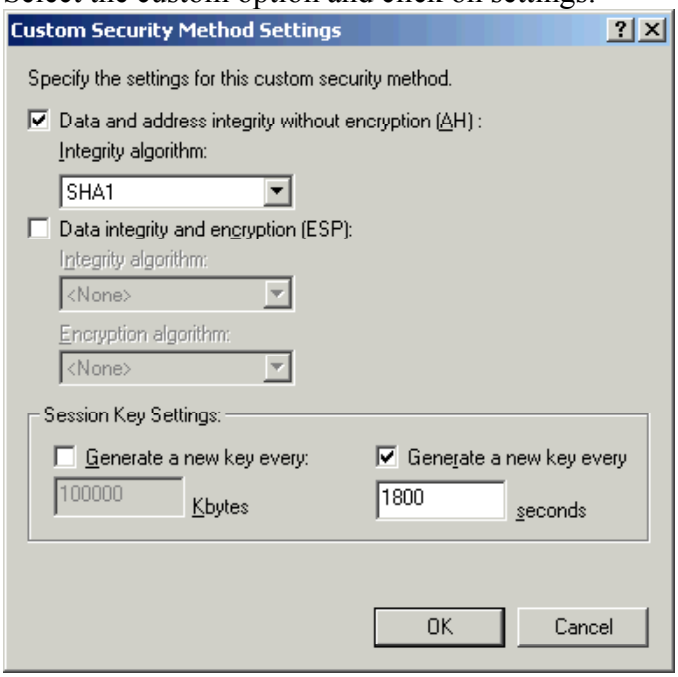
Double click the Require Security entry.



Remove the last 3 entries and double click on the remaining setting.

© SANS Institute 2000 - 2005 Author retains full rights.

Select the custom option and click on settings.



Change the Integrity algorithm to SHA1, clear the Data integrity and encryption checkbox and set the Generate a new key to 1800 seconds. (30 minutes)

To assign the policy, right click the secure server setting and click assign.

For the default response (the <dynamic> setting) we do not want to force authentication. This would prevent new workstations from joining the domain and subsequently obtain their GPO assigned settings.

Note that the ALL ICMP Traffic setting allows all types of ICMP traffic, not just ICMP echo reply used with the ping command. This would normally allow for ICMP fingerprinting. However, since the internal ACL and firewall rule sets will only allow internal users to access internal servers it really does not matter that they are able to fingerprint the O/S.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Appendix G NSA supplied default domain controller GPO settings

A full discussions of each option supplied with the NSA template is beyond the scope of this document. Only key settings are shown .

Security Options\Account Policies

Policy	Computer Setting
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	No auditing
Audit system events	Success, Failure

Ideally we want to log and retain all audited events. This becomes impractical due to sheer amount of events. Therefore key events such as logon and policy change are audited for both success and failure. This should aid in detecting privilege escalation attacks. Other events such as directory service access are only audited for failure. A failure on such an event could indicate a brute force attack.

Security Settings\Security Options

Policy	Computer Setting
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain controllers only)	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 use of Backup and Restore privilege	Enabled
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Disabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Disabled
Digitally sign server communication (when possible)	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM

© SANS Institute 2000 - 2005 Author retains full rights.

Number of previous logons to cache (in case domain controller is not available)	0 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Enabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Disabled
Send unencrypted password to connect to third-party SMB servers	Disabled
Shut down system immediately if unable to log security audits	Enabled
Smart card removal behavior	Lock Workstation
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled
Unsigned driver installation behavior	Warn but allow installation
Unsigned non-driver installation behavior	Warn but allow installation

Security Settings\Registry

Object Name	Permission	Audit
CLASSES_ROOT	Replace	Replace
machine\software	Replace	Replace
machine\software\microsoft\netdde	Replace	Replace
MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT	Replace	Replace
machine\software\microsoft\protected storage system provider	Ignore	Ignore
MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ AsrCommands	Replace	Replace
machine\software\microsoft\windows nt\currentversion\perflib	Replace	Replace
machine\system	Replace	Replace
machine\system\clone	Ignore	Ignore
machine\system\currentcontrolset\control\securepipeservers\winreg	Replace	Replace
machine\system\currentcontrolset\control\wmi\security	Replace	Replace
machine\system\currentcontrolset\enum	Ignore	Ignore
MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ PermittedManagers	Replace	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ ValidCommunities	Replace	Replace
users\.default	Replace	Replace
users\.default\software\microsoft\netdde	Replace	Replace
users\.default\software\microsoft\protected storage system provider	Ignore	Ignore

© SANS Institute 2000 - 2005 Author retains full rights.

Security Settings\File System

The following show key directories and files that will be audited if repl

Object Name	Permission	Audit
%ProgramFiles%	Replace	Replace
%SystemDirectory%	Replace	Replace
%SystemDirectory%\config	Replace	Replace
%SystemDirectory%\dllcache	Replace	Replace
%SystemDirectory%\ias	Replace	Replace
%SystemDirectory%\Ntbackup.exe	Replace	Replace
%SystemDirectory%\rcp.exe	Replace	Replace
%SystemDirectory%\regedt32.exe	Replace	Replace
%SystemDirectory%\ReinstallBackups	Ignore	Ignore
%SystemDirectory%\rexec.exe	Replace	Replace
%SystemDirectory%\rsh.exe	Replace	Replace
%SystemDirectory%\secedit.exe	Replace	Replace
%SystemDirectory%\spool\printers	Replace	Replace
%SystemDrive%\autoexec.bat	Replace	Replace
%SystemDrive%\boot.ini	Replace	Replace
%SystemDrive%\config.sys	Replace	Replace
%SystemDrive%\Documents and Settings\Administrator	Replace	Replace
%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson	Replace	Replace
%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log	Replace	Replace
%SystemDrive%\Documents and Settings\Default User	Replace	Replace
%SystemDrive%\Inetpub	Ignore	Ignore
%SystemDrive%\IO.SYS	Replace	Replace
%SystemDrive%\MSDOS.SYS	Replace	Replace
%SystemDrive%\My Download Files	Replace	Replace
%SystemDrive%\ntdetect.com	Replace	Replace
%SystemDrive%\ntldr	Replace	Replace
%SystemDrive%\Program Files\Resource Kit	Replace	Replace
%SystemDrive%\System Volume Information	Ignore	Ignore
%SystemDrive%\Temp	Replace	Replace
%SystemRoot%	Replace	Replace
%SystemRoot%\$NtServicePackUninstall$	Replace	Replace
%SystemRoot%\CSC	Replace	Replace
%SystemRoot%\Offline Web Pages	Ignore	Ignore
%SystemRoot%\regedit.exe	Replace	Replace
%SystemRoot%\repair	Replace	Replace
%SystemRoot%\security	Replace	Replace
%SystemRoot%\Tasks	Ignore	Ignore
%SystemRoot%\Temp	Replace	Replace
c:\autoexec.bat	Replace	Replace
c:\boot.ini	Replace	Replace
c:\config.sys	Replace	Replace
c:\ntbootdd.sys	Replace	Replace
c:\ntdetect.com	Replace	Replace
c:\ntldr	Replace	Replace

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

References

"How to Move the Ntds.dit File or Log Files (Q257420)". Mar 28 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q257420 (Dec 19 2001)

Group Policy Application Rules for Domain Controllers (Q259576)". Apr 25 2000. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q259576 (Dec 19 2001)

"Outline for Group Policy Design Readiness". November 2000. URL: http://www.microsoft.com/technet/prodtechnol/windows2000serv/plan/gpdesout.asp (Dec 19 2001)

Brandolini, Shala and Green, Darin "The Windows Time Service". April 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/maintain/optimize/wintime.asp (Jan 10 2001)

"Kerberos Authentication Protocol". URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/prodtech/kerbtech.asp (Jan 10, 2001)

"Ipsecpol.exe: Internet Protocol Security Policies Tool "URL: http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/ipsecpol-o.asp (Dec 19 2001)

Steve Riley ,"Using IPSec to Lock Down a Server" URL: http://www.microsoft.com/serviceproviders/columns/using_ipsec.asp (Dec 19 2001)

Traffic That Can--and Cannot--Be Secured by IPSec (Q253169) (Apr 2000) URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q253169 (Dec 19 2001)

How to Use the RestrictAnonymous Registry Value in Windows 2000 (Q246261) (Dec 1999) http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q246261 (Dec 19 2001)

Client-to-Domain Controller and Domain Controller-to-Domain Controller IPSec Support (Q254949) (Mar 2000) URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q254949 (Dec 19 2001)

HOW TO: Use Internet Protocol Security to Secure Network Traffic Between Two Hosts (Q301284) (June 2000) http://support.microsoft.com/default.aspx?scid=kb;EN-US;q301284 (Dec 19, 2001)

Dumpel.exe: Dump Event Log URL: http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/dumpel-o.asp (Dec 19,

© SANS Institute 2000 - 2005 Author retains full rights.

2001)

Rice, David C. Group Policy Reference. Ft. Meade: National Security Agency, 2001.

Haney, Julie M. Guide to Securing Microsoft Windows 2000 Group Policy. Ft. Meade: National Security Agency, 2001.

Catherine Paquet and Diane Teare, Building Scalable Cisco Networks. Indianapolis:Cisco Press, 2000. 588 – 612

Karen Webb,Building Cisco Multilayer Switched Networks. Indianapolis: Cisco Press, 2000. 187 - 215

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.