Global Information Assurance Certification Paper

Fortunes for All

Securing Windows Practical Assignment

Version 3.0 – Option 1

Ben Bower

CONTENTS

TABLES

FIGURES

1 Introduction

1.1 Purpose

The purpose of this document is to detail the secure Windows 2000 infrastructure design for the GIAC Enterprises environment.

1.2 Scope

The security design described in this document is designed to support and enhance the business of GIAC Enterprises. This design will cover security in the following areas:

- Security Framework
- Network Infrastructure
- Windows 2000 Public Key Infrastructure (PKI)
- Active Directory
- Administrative Model
- Group Policy
- Security Scripting
- Security Procedures.

Many of these areas are not reliant on the technical capabilities of Windows 2000. They are critical when providing a complete, secure Windows 2000 infrastructure.

1.3 Audience

This design is intended to be guide the implementation and maintenance of Windows 2000 in the GIAC Enterprises environment.

1.4 Assumptions

The following assumptions have been made in preparation of this document.

1.4.1 GIAC Enterprises Background

GIAC Enterprises is a wholly Australian owned business. They have achieved dominance in the fortunes market by the use of innovation in the fortune development business.

GIAC Enterprises now provides fortunes for 70% of the worlds fortune cookie producers.

GIAC Enterprises are also the largest supplier of fortune cookies to the

Australian market.

GIAC Enterprises now has over 700 employees across Australia.

GIAC Enterprises does conduct business on-line with partner organisations.

1.1.2 GIAC Risks

GIAC Enterprises have stated the following as significant areas of risk for the GIAC Enterprise network. For the purpose of this document Core Threat is a service that GIAC Enterprises cannot do without.

Table 1 - GIAC Core Threats

Risk	Description
Fortune Databases	This has been identified as a critical component of the GIAC infrastructure. This service has been identified as the Core Threat for GIAC Enterprises. GIAC have estimated that the on-line fortune database is costing the organisation $20K for each hour that it is unavailable. The fortune databases are the centre of the GIAC system. All branches and divisions of GIAC Enterprises are dependent on the information stored in the fortune databases.
On-Line Fortune System	The majority of fortune sales now occur with trusted partners via the on-line system. This system is also critical for the mobile sales staff.
Cookie Manufacturing Plant	The cookie manufacturing plant control systems are running on a Windows server in Darwin. It is critical that this server be up and available while the cookie production run is in progress.

2 Security Framework

The security framework describes the methodology used to organise the security controls. The security controls are specific countermeasures deployed in the GIAC Environment.

The controls detailed here are aimed at maintaining the Confidentiality, Integrity and Availability (CIA) of information and computing systems within the GIAC Environment.

For the purposes of this document security will be approached from the outside in. The following table describes the areas that need security applied within the GIAC Environment.

Table 2 - Security Areas

Area	Purpose
Public Network	This describes any network outside the GIAC Environment. Mobile users connecting via VPN also fit into this category.
GIAC DMZ	This describes the environment that houses the hosts that are visible to the public network (Internet).

GIAC Private Network	The GIAC Network describes the network behind the Internet facing router. This includes all LANs and private leased lines.
Network Exposure	Network exposure is the view that other hosts have of a device or host on the network. Each network application and service has an effect on the network exposure of the device.
Device	The device section describes the physical hardware and the physical environment the hardware is resident in. Physical security is a critical component of system security. Without adequate physical security the best technical solution can be rendered totally ineffective. Device security for GIAC Enterprises includes: • Controlling access to Serial, Infrared, Parallel and USB ports • Centrally controlling CMOS passwords • Restricting access to removable media • All servers and communications devices are located in secured server rooms.
Operating System	This section describes countermeasures that are applied to the operating system. This will include the registry, services, ACL's, user privileges and other Operating System security settings.
Applications	This describes how security of applications will be approached. Applications range from SQL on servers to Word on workstations.
Active Directory	Active Directory (AD) could be considered as an application that runs on certain servers. However, in the Windows 2000/.NET world Active Directory holds the keys to the kingdom. It is critical that extra care be taken to ensure AD is secure.
Monitoring	Monitoring must happen across all security areas. The ability to detect if applied countermeasures are working as planned is critical.

2.1 Defence in Depth

The end goal is to achieve layered security or defence-in-depth. This philosophy involves having multiple countermeasures between the resource being protected and the threat being protected against. This protects against failure of one or more countermeasures.

2.1.1 Castle Approach

A good analogy is that of a medieval town. You have town walls at the perimeter (external firewall); you then have a moat around the keep (internal firewall of different type to external); watchtowers (intrusion detection) and finally the walls of the keep (host based firewall). There will also be runners returning information from each wall and the towers to the general in the keep (monitoring and logging). Enemy soldiers could possibly get to your side of the moat, but the keep is still protected by its own walls.

2.2 Least Privilege

Wherever possible the concept of least privilege is used. Least privilege is a process where everything is denied by default and access must be specifically granted. Only the privilege required to accomplish a task is to be assigned to the account carrying out that task. The Role Based Administration (RBA) model details this approach. See section 5.2 for more information.

3 GIAC Network

The GIAC Network is a five site Australia wide network. Figure 1 - GIAC Network Diagram details the layout of the GIAC Enterprises environment.

3.1 Sites

GIAC Enterprises has sites in five state capitals. In addition to these sites GIAC Enterprises maintains thirty-five fortune telling kiosks in shopping centres around Australia.

3.1.1 Corporate HQ - Canberra

The GIAC Enterprises head office is located in Fyshwick, in the Australian Capital Territory. The Canberra office contains the following GIAC Enterprises divisions:

- Senior Management
- Finance
- Human Resources
- IT Support
- Sales & Marketing
- Research & Development
- Fortune Production.

There is a 4Mbps connection to the Internet from Canberra. There are 250 users located at the Canberra office.

The web servers are all located in the Canberra office.

3.1.1.1 De-Militarized Zone (DMZ)

The two DMZ for the GIAC Environment are both located in Canberra. These are used to house services that are available to external users. The idea is that if a DMZ host is compromised the attacker still has another firewall to deal with before gaining access to the GIAC internal network.

3.1.2 Manufacturing - Darwin

Darwin houses the cookie manufacturing plant. There is also a small sales team located in Darwin. The Darwin site is connected to Canberra via a dedicated 2Mbps Frame Relay connection. There are 350 employees at the Darwin office. Of these only 100 are full time users of the IT infrastructure.

3.1.3 Branch Offices

Each of the three branch offices has a 512Kbps ADSL connection to the Internet. Connectivity to Canberra is provided via an IPSec/L2TP VPN. There are no servers housed at the branch offices. Users at the branch offices access GIAC resources via the Terminal servers located in the Canberra office.

Table 3 - Branch Offices

Branch Office	Description
Brisbane	Brisbane has eight employees. They are made up of sales and associated support staff.
Hobart	Hobart has thirteen employees. They are made up of sales and associated support staff.
Sydney	Sydney has five employees. They are made up of sales and associated support staff.

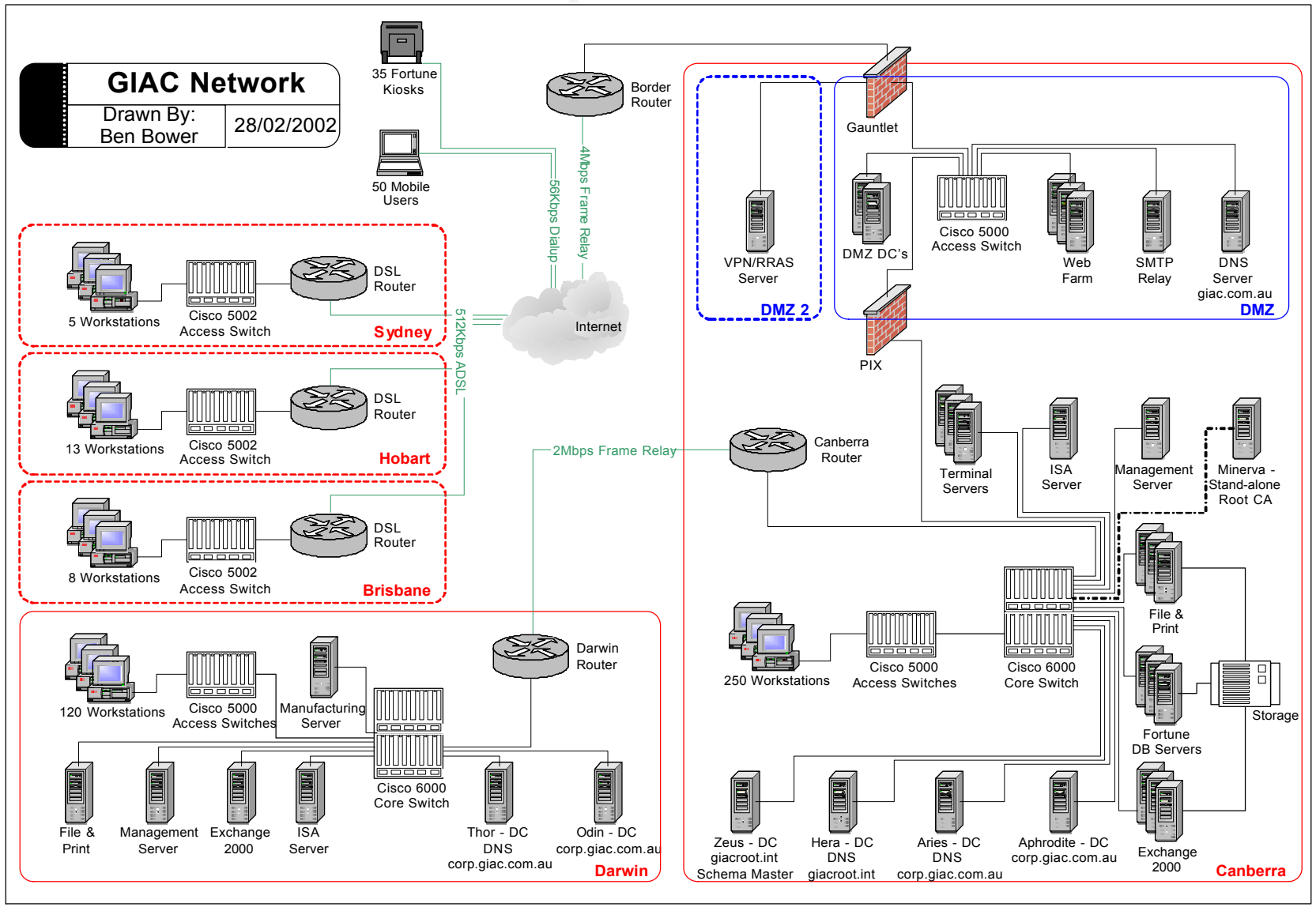
3.1.4 Mobile Users

GIAC Enterprises has 50 mobile users. These are primarily roving sales staff. Connectivity is provided to these users via an IPSec/L2TP VPN.

3.1.5 Kiosks

Each of the 35 kiosk machines are connected to the GIAC Environment via 56Kbps modem lines and an IPSec/L2TP VPN. Once every 24 hours the kiosk will connect to GIAC. The kiosk uploads usage data and pulls down the latest fortune list from the fortune database. The kiosks are touch-screen based machines running Windows XP.

Figure 1 - GIAC Network Diagram



3.2 Servers

This section describes the servers in use within the GIAC Environment.

3.2.1 Server Hardware

Dell has been selected as the supplier of server hardware for GIAC Enterprises. The following is a **minimum** standard for server hardware.

Table 4 - Server Hardware Standard

Component	Description
CPU	Dual 1GHZ Pentium III CPUs.
RAM	1GB ECC RAM
Storage	Each server will be configured with 2x18GB mirrored drives to house the operating system. Systems not attached to the SAN will be configured with 6x18GB drives. Five of these will be in RAID 5 configuration with the 6th serving as a hot spare. All drives in use in GIAC Enterprises servers are SCSI.
Removable Media	Each server will have a 1.44 floppy drive and DVD-Rom.
Network Interface Card	All servers are connected via Gigabit Ethernet. IPSec offload cards are also used in servers.

The level of fault tolerance implemented on server devices is directly proportionate to the value of the information or service it houses.

For services deemed as critical fault tolerance will be implemented in the following areas:

- Power supplies
- Hard Drives
- Network Connections
- Clustering.

3.2.2 Server Software

The following software is in use on GIAC Servers.

Table 5 - Server Software

Purpose	Software

Operating System	Windows 2000 Server and Windows 2000 Advanced Server. All servers are running Service Pack 2 for Windows 2000. Security hot-fixes are applied in a timely fashion using the software deployment capability of Group Policy. See section 6 for additional information.
Email Server	Exchange Server 2000
Database	SQL Server 2000
Web Servers	Internet Information Server 5.0
Backups	Arcserve is the backup software in use. Client agents for Exchange and SQL are also being used. The Open File Manager agent is running on all servers.

All servers built in the GIAC Environment only have the services installed that are necessary for correct functioning of the servers.

3.2.3 Backups

Arcserve is the backup software in use within the GIAC Environment. The majority of GIAC data is stored on the SAN. The SAN has its own backup system.

All servers not attached to the SAN will be backed up by a DLT tape robot attached to the management server.

The Arcserve Disaster Recovery Option is being used on all servers within the GIAC Environment. This will allow any server to be completely recovered from tape should a disaster occur.

All backup tapes are stored off-site. GIAC has storage locations in both Canberra and Darwin. Each of these locations has a secure, fire proof safe that is used to store the off-site tapes.

3.2.4 Server Roles

The servers within the GIAC network have been divided into roles. This helps maintain consistency across the entire GIAC network. This section details each of the server roles being used by GIAC.

3.2.4.1 Domain Controllers

There are eight Domain Controllers providing authentication and directory services to the GIAC network. The forest and domain design is detailed in section 4.

There are six Domain Controllers located in the Canberra office and two located in the Darwin Office.

- Two of the Domain Controllers in the Canberra office are used to authenticate users from the Canberra site and users connecting via VPN and using Terminal Services.

- Two are located in the Darwin office and provide directory services to the

cookies manufacturing plant.

- Two more have been used to house the forest root domain.
- The final two are used to provide directory services to the GIAC DMZ.

Multiple Domain Controllers are being used at each site to provide redundancy.

There are three certificate servers in the GIAC Environment. The stand-alone root server in Canberra is rarely connected to the network. The four Enterprise subordinate servers are used as certificate issuers. These are all running on Domain Controllers.

Microsoft does not recommend running Certificate services on Domain Controllers as performance could be a problem. As the largest of the GIAC sites only has 250 users the level of traffic to the Certificate services was not significant enough to justify additional servers. There are two Certificate issuers in Canberra and another two in Darwin. For more information about the configuration of certificate services for GIAC refer to section 4.

3.2.4.2 DNS Servers

All name resolution and registration of Fully Qualified Domain Names (FQDN) in the GIAC Environment will be provided by dynamic DNS. For more information on the DNS configuration within GIAC refer to section 5.2.4. There are two servers running DNS at the Darwin site and three running DNS at the Canberra site.

The DNS server in the DMZ only provides name resolution for externally available hosts.

3.2.4.3 Management Servers

There are two management servers running in the GIAC Environment. These servers are providing the following functionality for the GIAC network:

- Centralised anti-virus update distribution and management using Norton Anti-Virus Enterprise Edition.
- Backup management using Arcserve Enterprise. This console allows central management of the Arcserve software running on all servers.
- Cisco Secure ACS software to allow authentication at the port of each LAN switch via 802.1x.
- Syslog daemon. This allows the PIX firewalls to log to a central location.

- Network Time Service. This is critical for Kerberos authentication. Clients and Authenticating servers must be within five minutes of each other.[1] The management servers will be used as primary time servers for the GIAC Environment.

  This server administers the Anti-virus software for GIAC Enterprises. Each of the workstations and servers within the environment has Anti-virus client software that is centrally managed from this machine. All updates are downloaded by this server and

then automatically distributed to each client machine in the GIAC Environment.

3.2.4.4 ISA Servers

There are two ISA servers being used to provide the following functionality:

- Authentication of Internet Access
- Content Caching
- Content Filtering
- Auditing of Internet Access
- Simplification of outbound firewall rules.

There is one ISA server located in Canberra and one in Darwin. The Darwin server is configured to send all requests to the Canberra up-stream server.

The ISA servers are running ISA Enterprise edition. This allows Active Directory to be used to centrally manage policy across the two servers. [2] These servers are located near the user population that is making use of their services.

The ISA server in Darwin is in place to minimise the amount of Internet traffic across the 2mbps frame relay connection.

3.2.4.5 VPN/RAS Server

This server is used as a VPN endpoint for the GIAC VPN clients. This server was placed in a separate DMZ to make it more difficult for an attacker that compromises a server in the web farm to attack the VPN host.

Being in a different subnet also allows GIAC Enterprises to use public addressing on the VPN server. Public addressing is required when using IPSec to secure the VPN connection. When Authentication Headers are used the tunnel cannot be established through a host performing Network Address Translation (NAT). This is because NAT modifies the IP headers of the packet and the Hash generated by Authentication Headers no longer match.

The rules on the firewalls allow the VPN server to communicate with the Domain Controllers for authentication and the Terminals server farm to provide thin client services over the VPN tunnels.

3.2.4.6 Mail Servers

There are three mail servers in use. There is one in each major site and one in the DMZ. Exchange 2000 is being used to provide mail and workgroup functionality to GIAC users. The user mailboxes are resident on the servers located in the Canberra and Darwin internal networks.

The mail server located in the DMZ is used to screen email before it reaches the internal environment. Each mail message is stored on the SMTP relay and virus scanned. Any suspect attachments (.VBS etc) are stripped out before they can be executed from a user's mailbox.

The external mail server is running Mimesweeper from Content Technologies.

The external mail server only allows mail to be relayed if it is destined to or received from the internal mail server. This is to prevent the relay being abused by spammers.

In order to improve performance IP address ranges are used instead of domain names to control mail relaying.

3.2.4.7 Terminal Servers

The terminal server farm is used to provide GIAC network services to clients over the VPN connections. Having all functionality provided to remote clients over terminal services means that only an RDP connection has to be made between the VPN server and the terminal server farm. This simplifies the rules required on the GIAC firewalls. Another benefit of this is that terminal services only utilises a small amount of bandwidth per connection.

3.2.4.8 Database Servers

The databases are the core of the GIAC system. The fortunes database contains all the fortunes developed by GIAC. The database farm storage is located on a SAN and connected with the database servers via a fibre channel connection.

The finance and HR systems also run on the database servers. The fortune database is the backend of the on-line fortune purchasing system. The databases are running on Microsoft SQL 2000.

3.2.4.9 File & Print

There are two file and print servers in the GIAC system. These are used to store standard office documents and house the print queues. The file and print server in the Canberra office uses the SAN for storage.

3.2.4.10 Web Servers

The web farm is located within the GIAC DMZ. The web servers are the front-end for the GIAC on-line fortunes system. Each of the web servers is running IIS 5.0. Windows 2000 Advanced Server is being used on the web servers to take advantage of the Network Load Balancing Service (NLBS).

3.3 Workstations

This section describes the workstations in use within the GIAC Environment.

3.3.1 Workstation Hardware

There are three main types of workstation or client machines in use within the GIAC Environment.

3.3.1.1 Desktops

The workstations in use are Dell Optiplex 150s. These are a small form factor machine. One of the reasons these were chosen is the fact that they have a USB port on the front of the case. This enables easy access for users authenticating via USB

tokens. See section 4.2 for more information.

Table 6 - Desktop Hardware Standard

Component	Description
CPU	1.4GHZ Pentium IV CPUs.
RAM	256MB RAM
Storage	40GB IDE Hard Disk Drive
Removable Media	Each server will have a 1.44 floppy drive and CD-Rom.
Video	16MB Video Card
Sound	Sound blaster compatible
Monitor	17" Flat Panel
Network Card	IPSec offload card and 100Mbps NIC

3.3.1.2 Laptops

The laptops in use are Dell Latitude C600s.

3.3.1.3 Kiosks

The Kiosk hardware was designed specifically for GIAC Enterprises. The kiosks utilise a custom fortune telling application and a touch screen to make them simple for users to use. The machines are coin operated and provide a steady income stream using GIACs older fortunes.

3.3.2 Workstation Software

This section provides a description of the software in use on the GIAC workstations. The workstations in the GIAC Environment are running the GIAC Standard Operating Environment (SOE). This ensures that all core workstation software within the GIAC network is identical across all workstations.

Table 7 - Workstation Software

Purpose	Software
Operating System	Windows XP Professional
Mail Client	Outlook XP
Office Automation	Office XP Standard
Web Browser	Internet Explorer 6.0
Anti-virus	Norton's Anti-virus
Custom Applications	The front-end for the Fortunes database is also installed as part of the workstation SOE

3.4 Switches – 802.1x

Each of the access switches are 802.1x enabled. Each host now needs to authenticate with the switch before access to the network is granted. This prevents unauthorised hosts connecting to the LAN. The switch can authenticate user accounts against Active Directory using EAP and certificate based authentication.[3]

The Cisco Secure ACS software runs on the management servers at both Canberra and Darwin. Only access to the switches at Canberra and Darwin are controlled using 802.1x.

3.5 Routers

All of the routers in use in the GIAC Environment are Cisco. Table 8 - Router Types describes the three types of routers used.

Table 8 - Router Types

Router	Description
ADSL	Each of the small branch offices is connected via a Cisco 827 ADSL router.[4] These connect to the VPN server in Canberra via a Tunnel (router to router) mode VPN. This router also contains the Cisco Stateful Inspection firewall feature set that is included with Cisco IOS.
Border Router	The border router is a Cisco 3620. There is a basic packet filter in place on this router (using extended access control lists). This blocks the majority of unwanted traffic before it reaches the first of the PIX firewalls (Section 3.6).
Canberra – Darwin Connection	The two routers providing the Canberra-Darwin link via leased lines are Cisco 2610 routers. The WIC-1T High Speed Serial port is used to provide Frame Relay connectivity.[5] All communication between these two routers is encrypted. IPSec in tunnel mode is used across this link.

3.6 Firewalls

The two firewalls in use within the GIAC Environment. The external firewall is a Solaris server running Gauntlet. The internal firewall is a Cisco PIX.

3.6.1 External Firewall

The external firewall has three interfaces. There is one interface connected to the border router. This is the "Outside" Interface. Another interface is connected to the LAN housing the VPN server. The third interface is connected to the screened-subnet (DMZ) housing all of the DMZ servers (See Figure 1 - GIAC Network Diagram). The Outside Interface and the VPN subnet are both publicly addressed.

The VPN server has to be publicly addressed as it is the endpoint for the IPSec VPNs being used by the mobile users and branch offices. The DMZ is privately addressed with Network Address Translation employed to map a public address to each

privately addressed server.

3.6.2 Internal Firewall

The internal firewall has two interfaces. The "Outside" interface on this firewall is connected to the DMZ. The "inside" is connected to the core switch in the Canberra office. The rules configured on this firewall prohibit any public host from making a direct connection to any internal host. All inbound connections must be destined for a host in the DMZ.

3.7 Network Time

GIAC employs the Win32 Time service to provide time synchronisation across servers and workstations.[6]

Zeus.giac.int is the authoritative time source for the GIAC Environment. Zeus fills the PDC Emulator Flexible Single Master Operations (FSMO) role for the giac.int domain. The PDC Emulator in the root domain (first domain in the forest) is always the authoritative source for the forest.

Aries.corp.giac.com.au is the PDC Emulator for the corp.giac.com.au domain. This server is therefore the authoritative time source for the domain. The other domain controllers within the corp.giac.com.au domain synchronise time with Aries. All other Windows 2000 and XP hosts synchronise time with the authenticating Domain Controller.

Simple Network Time Protocol (SNTP, UDP 123) is permitted through the firewall from zeus.giac.int to the ntp2.usno.navy.mil at 192.5.41.209 hosted by the US Military.

The PDC emulator for the dmz.giac.com.au domain synchronises time to the same server.

The Kerberos authentication protocol depends on network time synchronisation for correctly functioning authentication. The time on the workstation where the user is logging on must be within five minutes of the authenticating server or authentication will fail.

The time synchronisation setup for GIAC is designed to ensure that time for all devices is accurate give or take 20 seconds.

4 Windows PKI

GIAC Enterprises are using the PKI that is included with Windows 2000 Server. The three needs that GIAC Enterprises is trying to meet are:

- Data Privacy
- Authentication
- Non-Repudiation.[7]

GIAC Enterprises is using the PKI to enterprise enable the following features of

Windows 2000.

- Strong Authentication
- IPSec
- Encrypting File System (EFS)
- Email signing and encryption
- Secure Sockets Layer on the Web Farm.

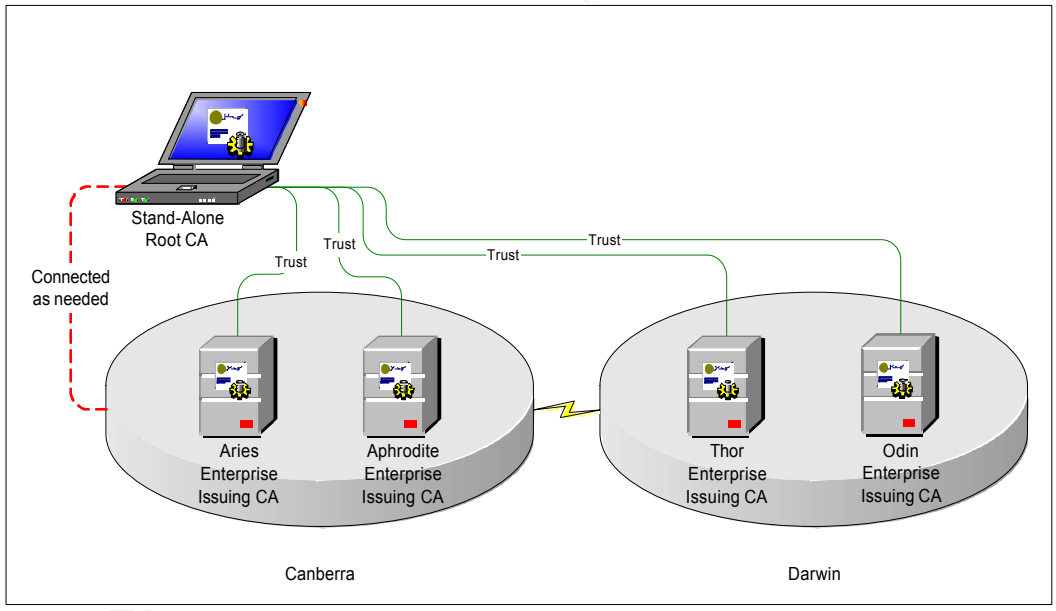
GIAC Enterprises has future plans to open additional functionality to its partners. At present only a secure portion of the external web site is offered.

Certificate Trust Lists (CTL) are used to facilitate communication between partner organisations.

4.1 Certificate Hierarchy

The certificate Hierarchy created for GIAC Enterprises is shown in Figure 2 - GIAC Certificate Hierarchy.[8]

Figure 2 - GIAC Certificate Hierarchy



This hierarchy was chosen as a good balance between usability, redundancy and security. Given the size of the GIAC Enterprise network is was difficult to justify the purchase of additional servers to fill the roles of Issuing Certificate Authorities (CA) so the existing Domain Controllers were used.

4.1.1 Stand Alone Root CA

The stand alone Root CA is the top of the certificate hierarchy. This server was implemented to issue Certification Authority certificates to each of the Enterprise Issuing CAs and was then taken off-line and secured in a safe at the Canberra office.

The stand-alone root CA is installed on a laptop as this is much easier to secure. The laptop is kept inside a fireproof safe in the GIAC Canberra office.

A disk image of the Stand Alone Root CA has been made and is kept in a safe-deposit box.

4.1.2 Enterprise Issuing CAs

The enterprise issuing CA's are each of the Domain Controllers for the corp.giac.com.au domain. In other implementations of PKI Issuing CAs are also known as Registration Authorities (RA). Enterprise issuing CA's meet the following GIAC needs:

- Auto-issuance of certificates. This reduces the certificate management burden significantly.
- Issuance of certificates for token based authentication.
- Certificate issuance can be managed via group policy.

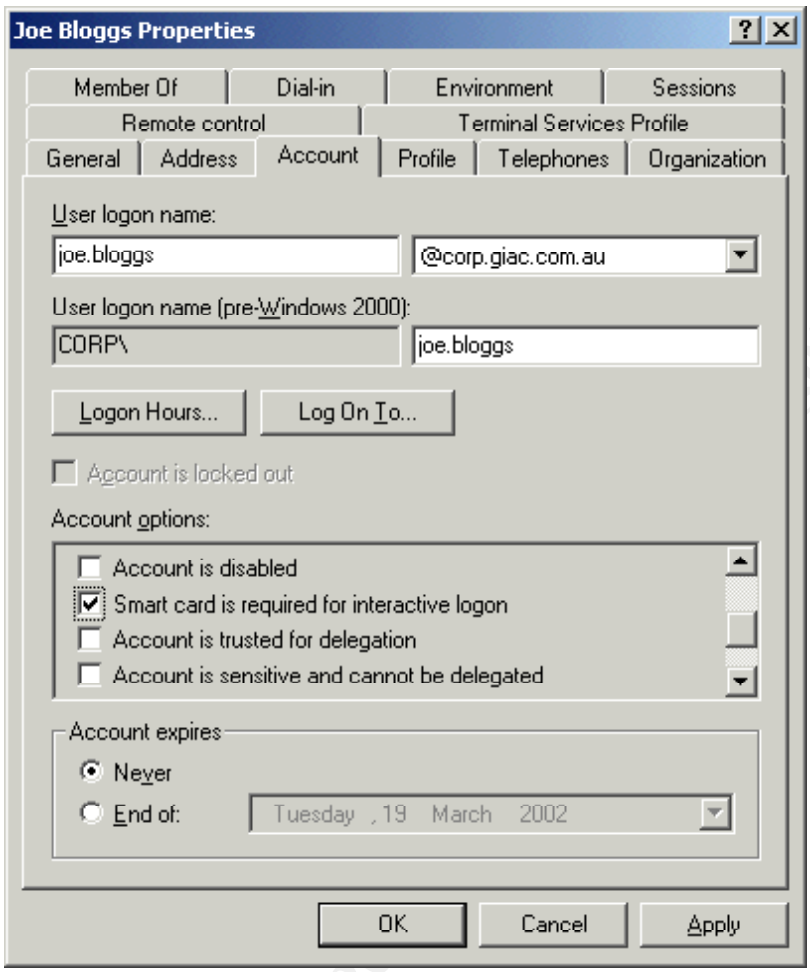
4.2 Authentication

Authentication to the GIAC network occurs via USB "smart tokens". Smart tokens were chosen for the following reasons:

- USB ports exist on all GIAC hardware. No additional readers are required.
- Token authentication is transparently integrated with Kerberos.
- Token authentication is two-factor authentication. It combines something you know (password or pin) with something you have (the token).
- Workstations can be automatically locked on token removal.
- The user's private key is secured away from applications and the operating system (on the token).
- The user's private key is not stored on any PC at any time.

Figure 3 - Smart Card Authentication Required shows the user account option that forces smart card authentication to be used.

Figure 3 - Smart Card Authentication Required



4.2.1 Token Issuing

The issue of the USB tokens is controlled by designated administrators, one in Canberra and another in Darwin. Users have to provide "100 points" of identification including photo ID before a token is issued. Table 9- Identification Points shows an example of the points system used to identify users prior to issuing a token.

Table 9- Identification Points

Identification Item	Points
Photo Licence	80
Credit Card	20
Electricity Bill with address	30
Medicare Card	20
Birth Certificate	60

Procedures are in place to ensure that no duplicate tokens are issued. When a user requests a new token the existing token is immediately revoked.

4.3 EFS

Encrypting File System has been deployed for use on mobile devices. The Windows 2000 PKI is used to issue certificates for EFS to mobile users. EFS on the Windows XP laptops encrypt folders using the DESX algorithm. This provides 120-bit encryption.

Microsoft best practice is to encrypt folders instead of files. All files will inherit the encryption attribute from the parent folder.

4.3.1 Recovery Agents

Designated recovery agents for the Domain, Finance OU and HR OU have been created. Group policy is used to ensure that certificates for the recovery agents are available on the XP laptops. See section 6.5.6 for additional information. These are accounts that are used only for EFS recovery.

4.4 IPSec

The Windows 2000 PKI is also being used to provide certificates for use by IPSec. The three IPSec technologies deployed for GIAC are encryption and packet filtering.

4.4.1 Authentication Headers (AH)

Authentication headers are used to ensure traffic is not tampered with as it crosses the wire. The SHA-1 hashing algorithm is being used to generate the hash. This doesn't include encryption. Group Policy is being used to centrally administer this feature. See section 6.5 for more information.

4.4.2 Encapsulating Security Payload (ESP)

ESP encrypts the traffic that has been identified as sensitive. Two examples of this are the Finance and Human Resources information. Group policy will be used to require IPSec encryption between clients and the Finance and Human Resources servers. Encryption secures the traffic travelling across the network against sniffing.

4.4.3 Packet Filtering

This isn't strictly a feature of Windows 2000 PKI. IPSec does provide a form of packet filtering. Sensitive or exposed servers such as those in the DMZ will be configured to only allow connections from the outside to the particular services they are offering. This will be done on an IIS web server by not requiring IPSec for HTTP traffic and requiring IPSec for all other traffic. When IPSec is configured in this fashion all packets to ports other than HTTP will be dropped unless IPSec is negotiated.

GIAC Enterprises will not rely on this as a foolproof security mechanism. There are several types of traffic that bypass the IPSec filters by default. One of these is the Kerberos protocol. Any packet that is sourced or destined for port 88 will be allowed by IPSec packet filters.[9]

4.5 Secure Email

The Windows PKI can also be used to provide certificates for secure email. Windows Certificate server will be integrated with Microsoft Exchange 2000 Key Management Server (KMS). Active Directory and Group Policy will be used to distribute secure mail settings to all clients.

The USB tokens deployed within GIAC will be used to house the key for signing and decrypting email.

The Exchange KMS also handles the Certificate Revocation List (CRL). This is stored in the Key Management database and then written to Active Directory. This list is updated on client machines daily by default. Performance will be severely degraded should the CRL become too large. The CRL is consulted when checking email signatures and when encrypting mail for sending to other users.

The areas that PKI can assist in securing email are.

4.5.1 Encryption

Email messages are encrypted using the intended recipient's public key. These messages can only be decrypted using the recipient's private key. This ensures that only the user that has the intended recipient's private key can decrypt the message.

4.5.2 Digital Signing

Digital signing covers the non-repudiation aspect of secure email. After a message is constructed a Hash of the completed message is attached and encrypted using the sender's private key. The recipient can then use the sender's public key to verify that the message was authentically signed with the sender's private key. This also protects the message from being modified in transit. If any part of the message changes the encrypted original hash will no longer match the hash generated from the changed message. This capability is very important for GIAC enterprises. This has been adopted for all formal messaging within the organisation.

4.6 SSL

Secure Sockets Layer (SSL) will be used to secure access to the private portions of the GIAC Enterprises web site. The Windows 2000 PKI will issue the certificate used to provide SSL services from the GIAC web site.

5 Active directory

The active directory for GIAC was designed to facilitate the following:

- Centralised administration
- Simple application of security policies
- Flexibility of policy application

- Delegation of authority.

Another significant advantage of Active Directory is multi-master replication. This enables changes to be made against any Domain Controller in the domain. This is particularly important for GIAC as they have two Active Directory sites.

The Global Catalogue is used to enable easy location of objects between domains. As only one domain stores objects that are in use by users, the Global Catalogue becomes less important. For simplicities sake each DC is also a Global Catalogue server within the GIAC Environment. The one exception to this is machines that have the Infrastructure Master FSMO role. These DCs are not configured as Global Catalogue servers within the GIAC Environment.

5.1 Administrative Model

Centralised administration is the model in use by GIAC Enterprises. The IT support staff are located primarily in Canberra. There is an IT staff of 15 in Canberra and 2 in Darwin. Administration mode terminal services are in use on all servers to allow easy administration of servers across the WAN.

5.2 Role Based Administration

One of the major benefits of Windows 2000 and Active Directory is the granularity possible in security settings. It is now possible to assign exactly the permissions required to carry out a task. Role Based Administration implements the concept of Least Privilege.

Custom taskpad views are used to supply tools to identified user roles. This restricts access to Windows 2000 Administrative tools. The only tools provided are the tools necessary to complete the tasks related to the role.

The Windows 2000 adminpak.msi is used to make domain tools available on administrative workstations.

5.2.1 Building Roles

Native mode was required on the domain in order to use nested groups. Group nesting is crucial to the implementation of Role Based Administration for GIAC.

In building the administrative roles we took the following steps:

1. The first step is to identify all administrative tasks that need to be performed on the system.
2. All the permissions required to carry out each task are then identified.
3. A global group is created for each task and permissions and rights for the task are assigned to the group for each task.
4. Next these tasks are examined and then collected together to form roles.
5. For each identified role another global group is created.

6. The role global group is then added to the global group for each task that is identified as a part of that role.

Users can now be assigned roles just by adding their account to the role group. This is also flexible as a new global group can be created for a task and then adds the role group to the new task group. If a new role is identified it can be comprised of any number of tasks without affecting other roles in use.

The following table contains the naming standard in use for Task and Role groups.

Table 10 - Task and Role Group Naming Standard

Purpose	Group Name
Task Group	T_<Task Name>
Role Group	R_<Role Name>

5.2.2 Identified Roles

The following table contains a list of the identified roles and a brief description of the role.

Table 11 - Identified Roles

Role	Description
Print Manager	This type of account allows a user to manage print devices and queues in the designated Organisational Unit.
Client Services	This type of account allows a user to perform minor maintenance on user accounts, add and remove people to and from groups and manage printers.
Desktop Support	This level of administrative rights allows a user designated as desktop support the ability to perform the tasks required to provide local desktop support in the designated Organisational Unit.
Auditor	This level of administrative rights allows a user designated as an auditor the ability to perform the tasks required to view and clear audit logs and modify the log properties.
Operator	This type of account allows a user to perform maintenance on user accounts, add and remove people to and from groups and manage printers, open files, connected users, shares and services. This account will have the ability to create user accounts and home directories and have full control over home drive permissions however read only permission over the group directories.

Supervisor	This type of account allows a user to perform most maintenance tasks for user accounts in the designated Organisational Unit including adding and removing users to groups. Resource management including printers, open files, connected users, event logs, shares and services can be controlled. This account may also log on and shutdown servers and synchronise the domain. This account has full control over home directories and group directories.
Domain Administrator	This type of account allows a user to perform all administration and maintenance tasks within the domain except for modification or creation of Group Policy Objects or Site Objects. This account also does not have the ability to modify membership of the Enterprise Administrators group or the privileged groups that allow Active Directory maintenance. Domain Administrator accounts are only allocated for the **corp.giac.com.au** domain.
Enterprise Administrator	This Level of administrative rights allows performance of all administrative tasks across the entire Forest. This is the only level of administrative access that allows access and maintenance to the **giacroot.int** placeholder domain, which is the forest root. This level of administrative rights allows access to and manipulation of the Active Directory Schema. This level of administrative access needs to be strictly controlled and although it has access to create or modify any and all objects throughout the forest should only be used for Active Directory and placeholder domain Maintenance tasks. To ensure this role is not abused the Design Team are responsible for the review of tasks requiring Enterprise Administrator access and then be responsible for the temporary allocation of this level of access to operational staff to perform specific tasks.

5.2.3 Administrative Accounts

Users that fill a role will have a second account related to that role. Standard user accounts are never used for administration. This does introduce an overhead in account administration. The benefit is that IT support staff needs to "take off their user hat and put on an administration hat". The format for the role based accounts is <User Name>_<Extension>.

Table 12 - Role Account Naming Standard

Role	Account Extension
Print Manager	PRI
Client Services	CLI

Desktop Support	DTP
Auditor	AUD
Operator	OPE
Supervisor	SUP
Domain Administrator	DOM
Enterprise Administrator	ENT

5.2.4 Kerberos Token

Care need to be taken when nesting groups for Role Based Administration. Prior to Windows 2000 Service Pack 2 the Kerberos token generated for a user has a fixed length. The token can only contain the Security Identifiers (SID) for 70-80 Groups.[10] Any additional groups that the user is a member of will not be included in the user token. This can result in the user not being granted access to resource and Group Policy not being applied.

Post SP2 the registry could be modified to increase the size of the token. For a token 100K in size the token can contain Security Identifiers for approximately 900 groups. Having a token this size could create performance problems however.

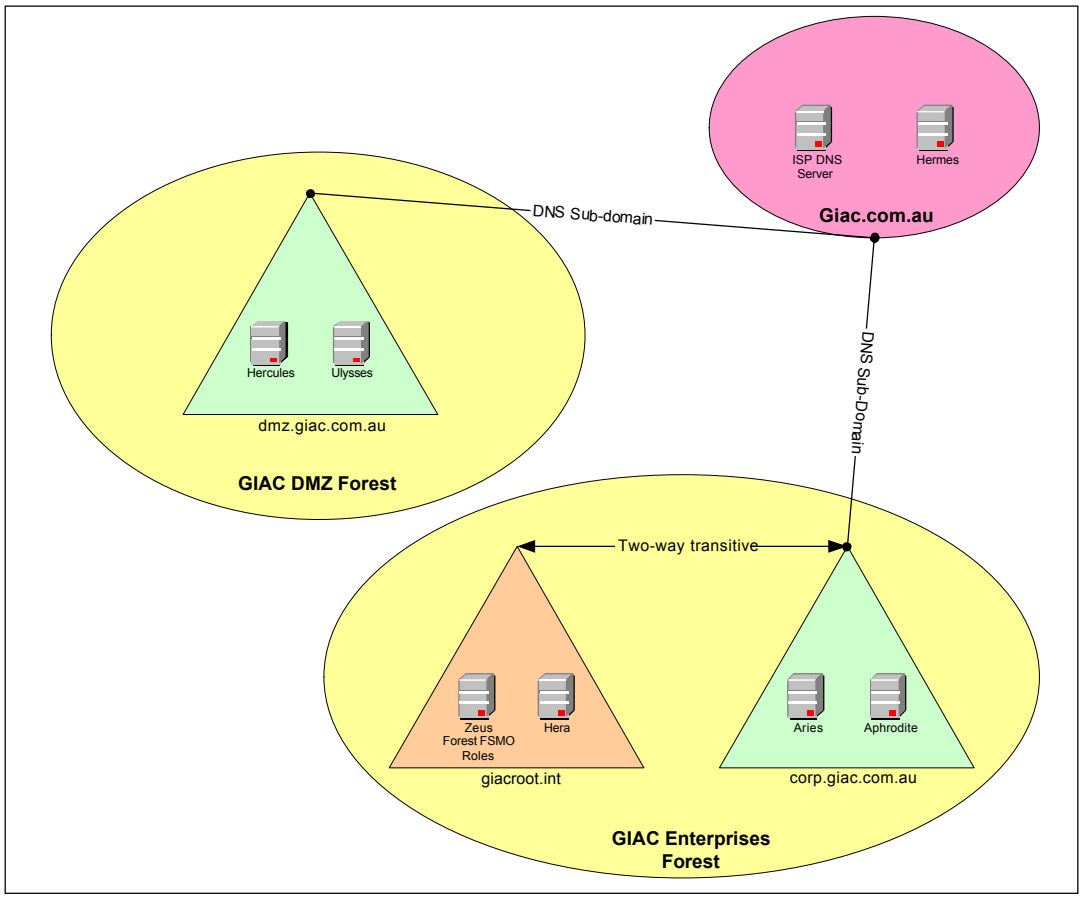
The Kerberos Token size for GIAC Enterprises has been set at 15K. This accommodates approximately 135 Groups.

5.3 Domain Structure

There are three Active Directory domains in use within the GIAC Environment. These three domains are spread over two forests.

The domains for GIAC Enterprises are organised as shown in Figure 4 - Forest and Domain Configuration.

Figure 4 - Forest and Domain Configuration



5.3.1 DNS

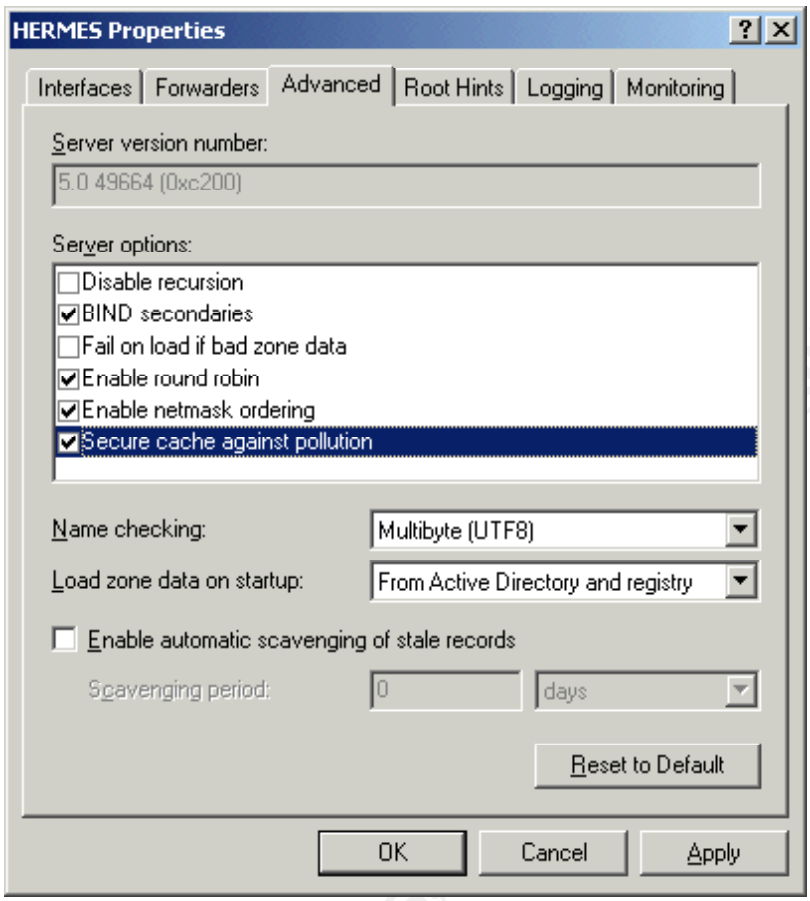
There are three DNS domains in use in the GIAC Environment. One domain is externally available. The other two are only significant within the GIAC Environment. Delegation and glue records were used to enable name resolution to occur between the internal and external DNS domains.

5.3.1.1 giac.com.au

The giac.com domain is available to hosts outside of the GIAC Environment. The primary DNS server for the giac.com domain is located in the GIAC DMZ. This server is a standard primary DNS server. The secondary server is hosted by GIAC Enterprises service provider. All of the DNS records on these servers are entered statically.

In order to prevent an attacker poisoning the DNS cache on the GIAC DNS server "Secure cache against pollution" has been selected. Figure 5 - Cache Poison Prevention shows this setting. This prevents an attacker appending bad DNS records to the end of a DNS request packet.[11] Even though there is a higher risk of this occurring on the external DNS servers than internal this setting will be applied to all DNS servers in the GIAC Environment.

Figure 5 - Cache Poison Prevention



5.3.1.2 Giacroot.int

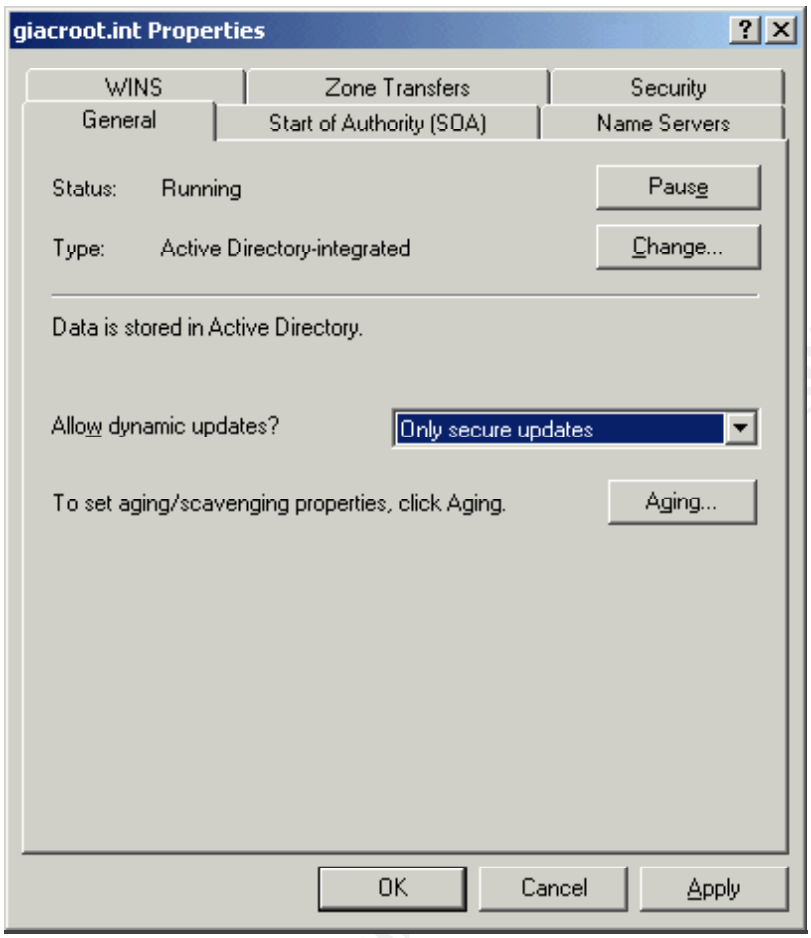
The giacroot.int domain is only available to internal hosts. This domain will never be exposed to the public network (hence the non-standard name). This is a placeholder domain used to hold the forest FSMO roles. The Schema Master and Domain Naming Master roles are both filled by the server Zeus.

The server Hera is also a DC within the giacroot.int domain. Hera is used to provide redundancy of directory services within giacroot.int.

This domain does not hold any standard user accounts. There are administrative accounts that are used for Active Directory and Schema maintenance and changes.

The giacroot.int domain is an Active Directory integrated domain. Both DNS servers in the Canberra office (Hera and Aries) are authoritative for the giacroot.int domain. The giacroot.int domain is configured to only allow secure updates see Figure 6 - Secure DNS Updates.[12] All authenticated users have the ability to create host and pointer records by default. Access Control Lists are used to further restrict the ability to dynamically modify records. Only members of privileged groups are able to change DNS records for all hosts.

Figure 6 - Secure DNS Updates



5.3.1.3 Corp.giac.com.au

This domain is a delegated sub-domain of the giac.com.au domain. This was done to simplify the resolution of names in the GIAC Environment. This decision was also made to prevent any possible naming conflicts in the future. The corp.giac.com.au domain is the domain that holds all the workstations, servers and users within the internal GIAC Environment. There are four Domain Controllers for the corp.giac.com.au domain. Two of these are in Canberra and two are in Darwin. There are three DNS servers that provide name resolution to the corp.giac.com.au domain, Hera & Aries in Canberra and Thor in Darwin.

The corp.giac.com.au domain is also an Active Directory integrated domain. Both DNS servers in the Canberra office (Hera and Aries) and Thor in Darwin are authoritative for the corp.giac.com.au domain. As with the giacroot.int domain the corp.giac.com.au domain is configured to only allow secure updates see Figure 6 - Secure DNS Updates.

This domain also holds the group policy objects used to control and secure the workstations and other servers within the GIAC Environment.

5.3.1.4 Dmz.giac.com.au

This domain is also a delegated sub-domain of the giac.com.au domain. This domain exists to simplify the administration of servers within the DMZ.

A completely separate forest is being used for the DMZ. There is no trust in place

between this and the corp.giac.com.au domain.

The DNS servers for this domain are running on the domain controllers. These DNS servers are not available to the public network.

The Web, External DNS and SMTP servers located in the DMZ are all members of the dmz.giac.com.au domain.

There is a false administrative account in use on all DMZ hosts. The account is called administrator but has no privileges. Access to this account is closely monitored as legitimate administrative staff has no reason to use this account. Failed logons on this account could indicate an attack.

Genuine administrative accounts in the DMZ will not have permission to access machines across the network. This ensures that administrative accounts must log on to the local console of the DMZ server. An attacker can not use an administrative account to connect to another DMZ host with this option set.

5.4 OU Structure – corp.giac.com.au

Figure 7 - Corp.giac.com.au OU Structure shows the Organisational Unit structure in use within the corp.giac.com.au domain. The OU structure for GIAC Enterprises was developed to facilitate the centralised administration model. Each OU is in place to logically group users and resources within the GIAC organisation.

An OU exists for each business unit.

Figure 7 - Corp.giac.com.au OU Structure

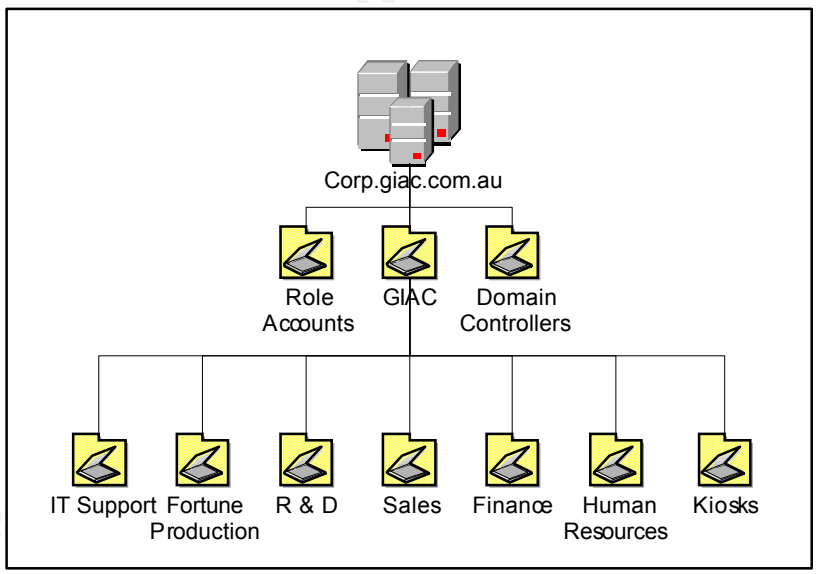


Table 13 - corp.giac.com.au OU Description describes each OU within the corp.giac.com.au domain.

Table 13 - corp.giac.com.au OU Descriptions

Organisational Unit	Description

GIAC	This OU groups the other custom OUs within the Directory under a single OU. This was done so that policy could be applied to all the GIAC OUs via inheritance without affecting any other top level OUs that may be needed in the future. For more information on the Group Policy Objects (GPOs) applied to the GIAC OU refer to section 6.5.
Domain Controllers	This is one of the default pre-defined OUs. All of the computer accounts for the Domain Controllers within the corp.giac.com.au domain are resident in this OU. The default domain controller group policy object is applied to this OU. For more information on the default domain controller GPO refer to section 6.5.3.
Role Accounts	The Role Accounts OU is in place to hold all accounts used by the various administrative roles.
IT Support	The IT Support OU holds the workstations and servers used by the IT support staff.
Fortune Production	The Fortune Production OU holds the servers, workstations and user accounts for the production plant.
R&D	The R&D OU holds the servers, workstations and user accounts for the Research and Development department. R&D is in an OU rather than a separate forest. The work that R&D performs on new fortune technology does not require any changes to be made to the Active Directory Schema. As such they can be located within the GIAC forest.
Sales	The Sales OU contains the servers, workstations and user accounts for the Sales department. This OU contains user accounts that are geographically distributed. Despite this geographic diversity the basic security settings to be applied are the same. There are location specific settings that need to be applied to mobile users however.
Finance	The Finance OU contains the servers, workstations, user accounts and printer objects (cheque printer) used by the Finance department. The Finance servers are part of the Database array. Due to the value of information located on the finance server access to these servers is tightly controlled. For more information on the GPO applied to the Finance OU refer to section 6.5.4.
Human Resources	The Human Resources OU contains the servers, workstations and user accounts used by the Human Resources department. The Human Resources servers are also part of the database server array. For more information on the GPO applied to the Human Resources OU refer to section 6.5.5.

Kiosks	This OU is in place to house a specific group of hardware devices. The Kiosks located in the shopping centres are each resident in this OU. Each of the Kiosk machines is running Windows XP with a severely restricted interface. For more information on the GPO applied to the Kiosks OU refer to section 6.5.8.

5.5 OU Structure – dmz.giac.com.au

Figure 8 - Dmz.giac.com.au OU Structure shows the Organisational Unit structure in use within the dmz.giac.com.au domain. The OU structure for this domain was developed to allow centralised management of security on the DMZ servers.

An OU exists for each server type resident in the DMZ.

Figure 8 - Dmz.giac.com.au OU Structure

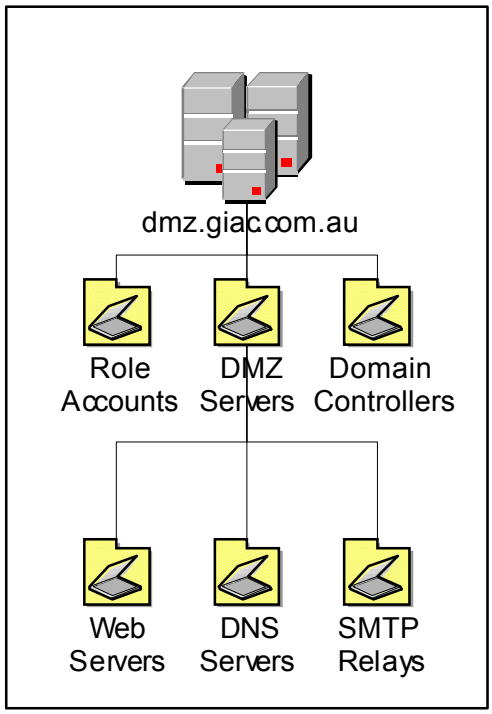


Table 14 - dmz.giac.com.au OU Descriptions describes each OU within the dmz.giac.com.au domain.

Table 14 - dmz.giac.com.au OU Descriptions

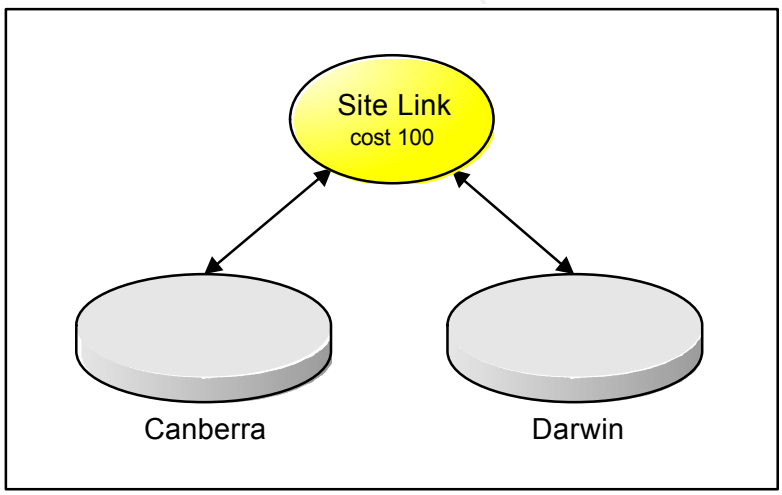
Organisational Unit	Description

DMZ Servers	The DMZ OU is utilised to group the Organisational Units for the different server types within the DMZ. This is critical as each of these servers offers some service to the public network. For more information on the DMZ GPOs refer to section 6.5.9.
Web Servers	This OU contains all the Web Server Computer Accounts.
DNS Servers	This OU contains the DNS server computer account.
SMTP Relays	This OU contains the SMTP Relay computer account.

5.6 Active Directory Sites

There are two Active Directory sites in the GIAC Environment, Canberra and Darwin. As such only a single site link is required. RPC is the replication method being used. The bandwidth between the sites is sufficient and stable enough for this protocol to be used. The cost assigned to the link is 100. This was done to allow additional links to be added without having to modify the cost on the existing link. See Figure 9 - AD Site Configuration for a graphical representation of the two Active Directory sites.

Figure 9 - AD Site Configuration



Even though there are two domains in the GIAC Active Directory changes will be most frequently made in the corp.giac.com.au domain.

Replication will be controlled between the two sites. The site connector acts as a choke point to enable replication control.

5.7 AD Groups

Groups are being used within Active Directory for the following:

- Grouping Users/Computers for Administration
- Grouping Users/Computers for Access Control

- Grouping Users/Computers to allow/restrict application of group policy
- Grouping other groups to form roles (section 5.2).

Global groups are being used throughout active directory. This was done to simplify administration. Local groups are still used on Member servers however.

5.8 AD ACLs

ACLs are mostly applied at the OU level within the GIAC Environment. Permission inheritance is used wherever possible. Exceptions to this are GPOs. Many GPOs have ACLs applied directly to affect which groups within the OU have the policy applied.

6 Group Policy

This section describes the Group Policy Objects that are applied to the GIAC Enterprises environment. Figure 11 - shows the security related Group Policy Objects that are applied to the corp.giac.com.au domain and Organisational Units.

Figure 10 - Dmz.giac.com.au GPO's shows the Group Policy Objects that are applied within the dmz.giac.com.au domain.

The Group Policies for GIAC Enterprises have been designed to complement each other. The most generic (applying to all) policies are higher in the tree. The policies that are applied down the tree are specific to the Organisational Unit they are applied to.

The Group Policy Objects detailed in this document address the security related settings applied to the GIAC Enterprises environment. Issues relating to simplified management of workstations and increased control over the "user experience" are also covered.

Figure 10 - Dmz.giac.com.au GPO's

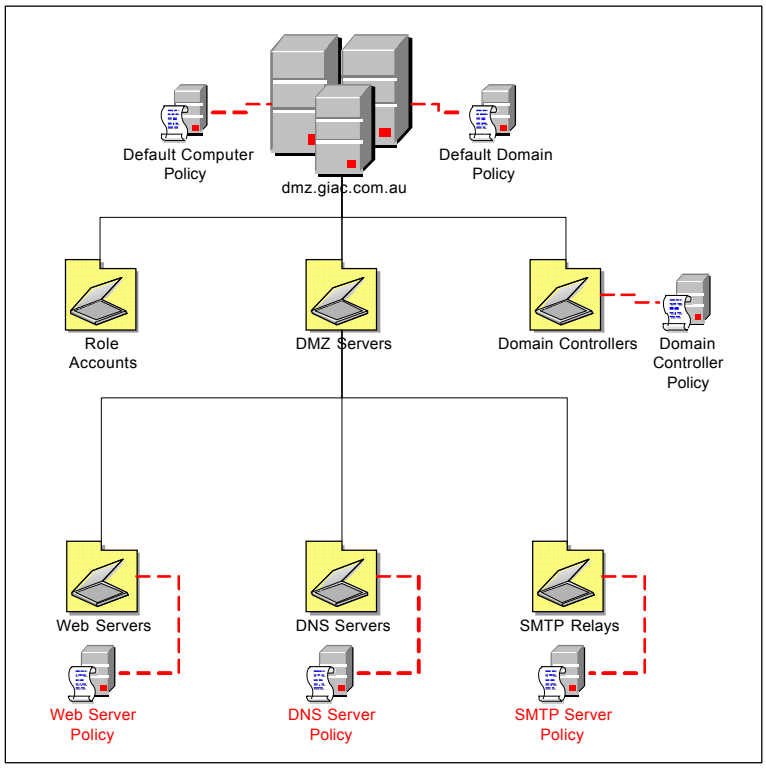
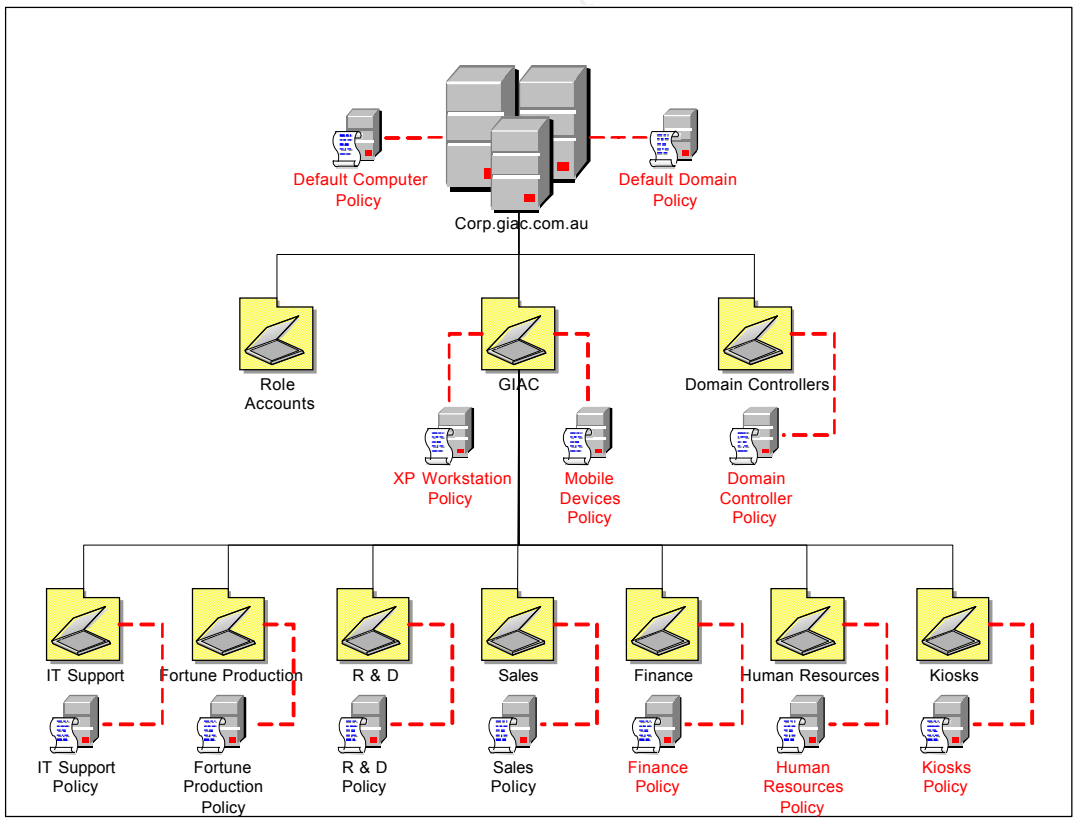


Figure 11 - Corp.giac.com.au GPO's



The Group Policy Objects shown in red are detailed within this document.

Policy is applied in the following order in a Windows 2000 environment, Local – Site – Domain – OU. Where OUs are nested the policy closest to the OU that contains the

target object is the last applied. GIAC Enterprises have GPOs at the Local, Domain and OU levels.

Group policy does not "tattoo" the registry in the same way as Windows NT 4.0 policies. Computer settings are applied when machines start and at regular intervals. User settings are applied when users logon and at regular intervals while the machine is on and the user is logged on. The default group policy refresh interval is 90 minutes.[13]

6.1 Local Group Policy Object

The following sections describe the Local Group Policy Object or Local Security Policy (Template Applied) that is in use within the GIAC Environment.

The local security policy is not strictly a group policy object. The local security policy is the fall back security position. If group policy is not available the local security policy will still ensure a base level of security is maintained. This is particularly relevant for mobile devices.

6.1.1 Security Templates

Local Policy templates have been developed for:

- Member Servers
- XP Workstations
- Kiosks.

Security templates are used to apply bulk changes to end stations. Making NTFS permissions changes on a large scale can take a considerable amount of time even on fast machines. To ensure that this doesn't affect the end users Security Templates are used to apply large changes out of business hours. Group Policy is then used to apply small changes and any Department or location based policy.

The two areas that security templates address are Policy Settings and ACL Settings.

6.1.1.1 Policy Settings

Security templates are used within GIAC to apply the following security policies:

- **Account Policies**. This controls the account policies for local accounts. This includes account lockout, password lengths, complexity and ages. Local Kerberos settings are also configured here.
- **Local Policies**. This controls the audit policy, User Rights Assignment and Other security options.
- **Event Log**. This section controls the event log settings.

6.1.1.2 ACL Settings

The security templates used to apply policy settings are also used to apply the

following:

- **Restricted Groups**. Restricted groups give GIAC the ability to control the membership of security groups on workstations.

- **Service ACLs**. The ability to start and stop services also needs to be restricted. Windows NT 4.0 was an all or nothing proposition when it came to service security. Windows 2000 gives us the ability to specify groups that are able to stop and start services. The templates applied to the machines in the GIAC Environment ensure that only the appropriate roles are able to stop, start and modify services on the target machine.

- **Registry ACLs**. Access to the registry must be restricted. There are several registry keys that contain security sensitive information. Also the configuration information for the OS and most software installed is contained in the registry. Once again the templates applied to the machines are supporting the Role Based Administration model.

- **File System ACLs**. This is a critical aspect of hardening a system. The security templates applied to GIAC Enterprises machines apply NTFS permissions to support the Role Based Administration model (section 5.2).

Auditing of access to files and the registry is also configured using these templates.

Unlike Group Policy applied by Active Directory, security templates make permanent changes. The setting configured using security templates remain in effect until a new template is applied.

The specific permissions applied by the security templates are out of the scope of this document.

6.1.2 Security Configuration and Analysis

The security templates for the GIAC Environment were created using the Security Configuration and Analysis and Security Templates MMC snap-ins. The security templates from the National Security Agency[14] (NSA) were used as the base for the GIAC Enterprises templates.

6.1.3 Secedit.exe

The Secedit.exe tool is used for the following:

- Application of security templates via scripting.

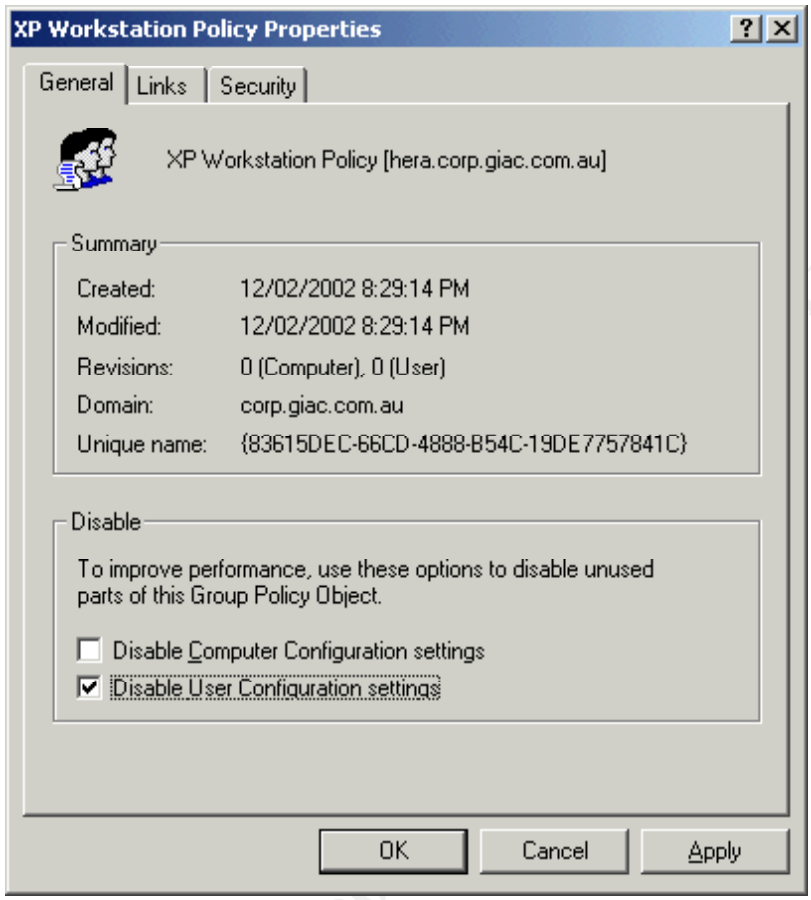
- Auditing of end devices for compliance with the security template.

6.2 Group Policy Performance

Part of the reason for splitting the User and Computer configuration items in to distinctly separate Group Policy Objects was to enhance performance. In a computer focussed GPO none of the User Configuration items are in use. There is no reason for this section of the policy to be processed.

To ensure this is the case the User Configuration section is disabled as shown in Figure 12 - Improve Group Policy Performance.

Figure 12 - Improve Group Policy Performance



6.3 Group Policy Filtering

Several Global groups have been developed to control application of Group Policy to GIAC Enterprises Users, Workstations and Servers. The Group Policy groups and their description are detailed in Table 15 - Group Policy Security Groups. These groups are only required where multiple GPOs are being applied to an object (this could be multiple on a single OU or inheritance from a higher OU). The naming standard for Group Policy groups is GP_<Descriptive Name>.

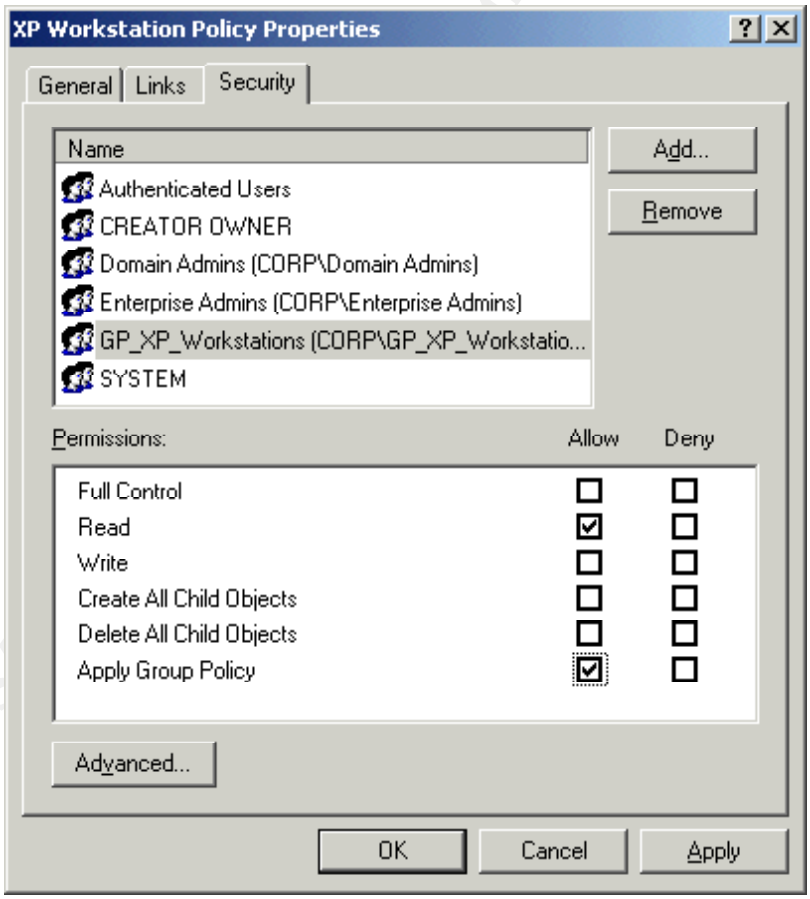
Table 15 - Group Policy Security Groups

Group	Purpose
GP_XP_Workstations	This group contains the accounts for all workstations within the corp.giac.com.au domain.
GP_Servers	This group contains the accounts for all servers within the corp.giac.com.au domain.
GP_Web_Servers	This group contains the accounts for the servers located in the Web Farm.

GP_SMTP_Relays	This group houses the computer account for the SMTP relay server located in the DMZ. The group was created to make it a simple task to add another SMTP relay server if necessary.
GP_Ext_DNS_Servers	This group houses the computer account for the DNS server located in the DMZ. This group was also created to facilitate easy application of policy if additional DNS servers are required in the DMZ.
GP_Finance_Servers	This group houses all computer accounts for the servers used by the Finance department.
GP_HR_Servers	This group houses all computer accounts for the servers used by the Human Resources department.
GP_Mobile_Devices	This group houses all the Laptops and other Mobile Devices in use within the GIAC Environment.

Only groups that have the apply group policy security setting applied will be able to apply the Group Policy Object.

Figure 13 - Apply Group Policy Setting



The apply group policy security setting is applied to the appropriate GPO as shown in Figure 13 - Apply Group Policy Setting.

6.4 Group Policy Areas

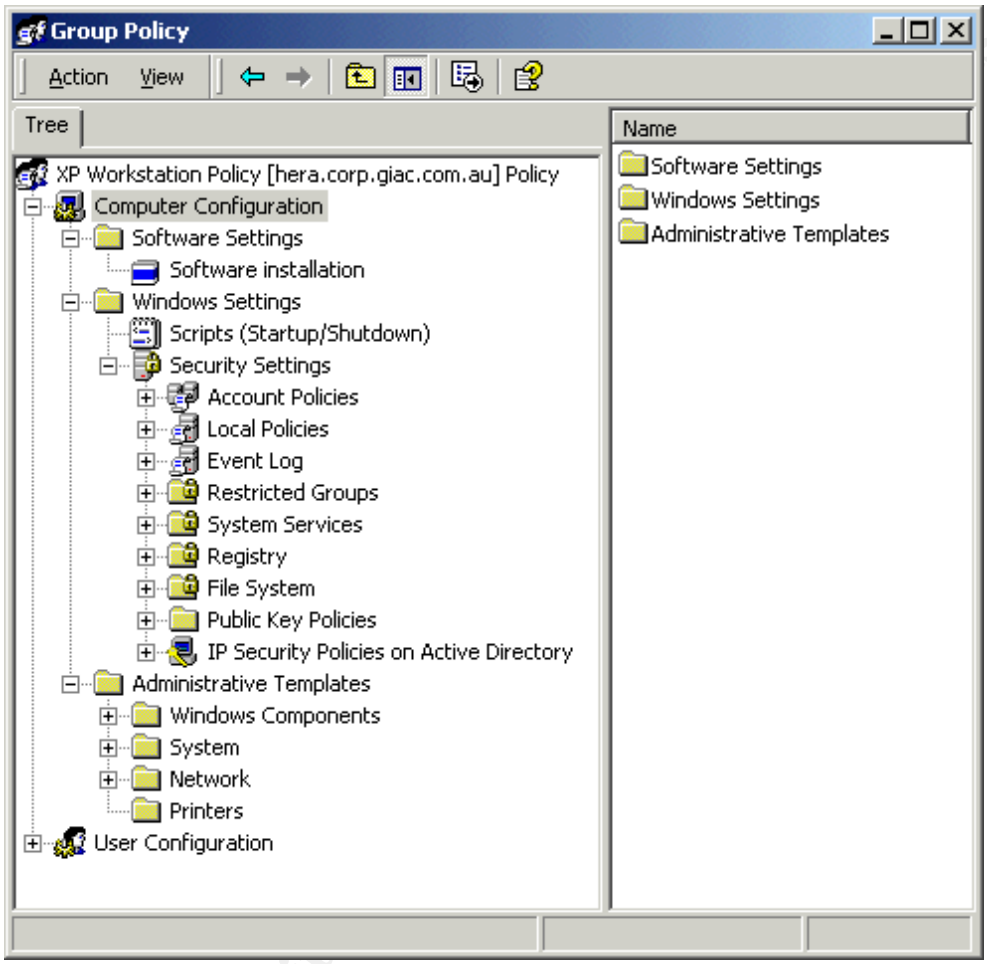
All of the settings that are applied using the Local Security Policy are able to be applied using Group Policy. Group Policy Objects are divided into two areas Computer Settings and User Settings. The Group Policy Objects for GIAC Enterprises are either User focussed or Computer focussed. This was done to simplify on-going administration of the Group Policy Objects.

Administrative staff can tell the purpose of the object by name of the object.

6.4.1 Computer Configuration

The computer configuration section contains all the Policy Items that can be applied to computer objects. Figure 14 - Computer Policy Settings shows the Computer Configuration container.

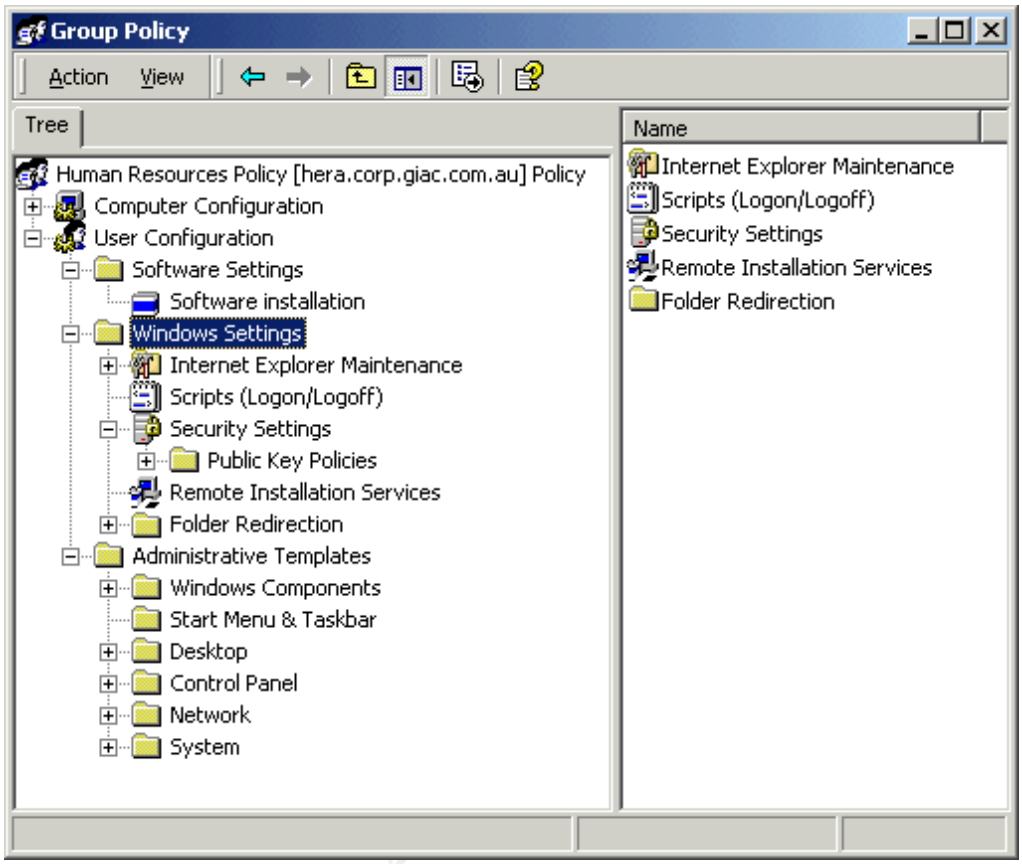
Figure 14 - Computer Policy Settings



6.4.2 User Configuration

The User configuration section contains all the Policy Items that can be applied to computer objects. Figure 15 - User Configuration Settings shows the User Configuration container.

Figure 15 - User Configuration Settings



6.5 Group Policies

This section details the security related settings that are applied via Group Policy in the GIAC Enterprises environment.

6.5.1 Default Domain Policy

The default domain policy is used only for applying the Account policy for the corp.giac.com.au, dmz.giac.com.au and giacroot.int domains. Microsoft best practice says that the default domain policy should not be modified any more than necessary. The following table contains the security related settings configured within this policy and the reasons they have been applied to the GIAC Environment.

Table 16 - Default Domain Policy

Policy Section	Policy	Configured Setting	Reason for Application
Windows Settings			
Security Settings			
Account Policies - A Domain Controller always pulls the account policy from the Default Domain Policy Group Policy object, even if there is a different account policy applied to the organizational unit that contains the Domain Controller.[15]			
Password Policies			
	Enforce Password History	24 Passwords Remembered	This prevents GIAC users from recycling a small set of passwords.
	Maximum Password Age	45 Days	This is the longest a user can use the password.
	Minimum Password Age	2 Days	This prevents a GIAC user from immediately changing their password 24 times so that they can continue to use their original password.
	Minimum Password Length	8 Characters	This is a good realistic minimum password length.

	Passwords must meet complexity requirements	Enabled	This setting forces the user to select a stronger password. The password cannot contain all or part of the users account name. It must be at least 6 characters long. It must contain three of the following four character types: (A-Z), (a-z), (0-9) & (!, $, #, %). This setting will only apply to accounts that are not authenticating via Tokens against the GIAC domain.
	Store password using reversible encryption for all users in the domain	Disabled	This policy option is disabled for GIAC Enterprises as CHAP and IIS Digest authentication are not being used.
Account Lockout Policy			
	Account lockout duration	0 Minutes	Once a GIAC account is locked out it can only be unlocked by designated personnel. This does add an administrative burden but it also forces administrative staff to take immediate notice of locked out accounts.
	Account lockout threshold	3 Invalid Logon Attempts	GIAC users get three attempts at their password. If they get it wrong three times the account is locked out.
	Reset account lockout counter after	30 Minutes	
Kerberos Policy			
	Enforce user logon restrictions	Enabled	This option forces every session ticket request to be validated by the KDC. The user rights policy on the target host is checked to ensure that the user has the right to log on locally if attempting a console logon and access this computer from the network for attaching to a network host.
	Maximum lifetime for service ticket	600 minutes	Service ticket is another name for Session Ticket. The maximum session ticket lifetime within GIAC is 10 hours.

	Maximum lifetime for user ticket	10 hours	User Ticket is another name for Ticket Granting Ticket. As with the service ticket the lifetime of a TGT within GIAC is 10 hours.
	Maximum lifetime for user ticket renewal	7 days	This setting specifies that the maximum life for a Ticket Granting Ticket (TGT) or a session ticket in the GIAC Environment is 7 days.
	Maximum tolerance for computer clock synchronization	5 minutes	The requirement to have computer clocks synchronised is designed to prevent replay attacks. The tolerance for this is set to 5 minutes for the GIAC Environment. Review section 3.7 for additional information on the network time service in use within the GIAC Environment.

6.5.2 Domain Computer Policy

The domain computer policy contains the default settings for all computers within the domain. The User Configuration section of this policy has been disabled. The following table contains the security related settings configured within this policy and the reasons they have been applied to the GIAC Environment. This policy is applied to the corp.giac.com.au, dmz.giac.com.au and giacroot.int domains.

Table 17 - Domain Computer Policy

Policy Section	Policy	Configured Setting	Reason for Application
Windows Settings			
Security Settings			
Local Policies			
Audit Policy			
	Audit account logon events	Failure	Failed logon Events could indicate an attack against the GIAC Environment. This is applied to the domain policy so that all devices that have the policy applied are auditing this event. Large numbers of failed logon attempts could indicate an attack against the device recording the events. Audit account logon events tracks events specifically related to Kerberos authentication.[16]
	Audit account management	Success	This auditing option will allow GIAC Enterprises to track account management events. These events can be compared to account management job tickets. Any events that do not match a job ticket could indicate a misuse of privileges.
	Audit directory service access	Failure	This auditing option allows GIAC Enterprises to detect failed attempts to connect to Active Directory. If a pattern of failed attempts is detected this could indicate an attack against the directory.

	Audit logon events	Failure	GIAC devices generate logon-related events when a user logs on interactively or remotely. These events are generated on the computer to which the logon attempt was made. Successive failures could indicate an attack on the GIAC system.[17]
	Audit object access	Success, Failure	Failure auditing here will give GIAC Enterprises an indication of people trying to access sensitive files. For particularly sensitive information all successful accesses will also be audited. This can also be useful when trying to establish a pattern of user behaviour after an incident occurs.
	Audit policy change	Success	Success audits generate an audit entry when a change to user rights assignment policies, audit policies, or trust policies is successful. This is critical when trying to detect unauthorised policy changes. Once again legitimate changes can be matched to a job ticket.
	Audit privilege use	Failure	This will indicate to GIAC Enterprises when users are attempting to do something for which they don't have the privilege.
	Audit process tracking	Not Defined	This audit setting is not currently required for GIAC Enterprises.
	Audit system events	Not Defined	This audit setting is not currently required for GIAC Enterprises.
User Rights Assignment – Not Covered Here			
Security Options[18]			

	Additional restrictions for anonymous connections	No access without explicit anonymous permissions	This setting ensures that the access token for non-authenticated users does not include the Everyone group. This prevents anonymous users from enumerating information such as User list, machine list and password policy from GIAC servers and workstations.
	Allow server operators to schedule tasks (Domain Controllers only)	Disabled	This setting will prevent Server Operators from using the AT command to schedule tasks. This effectively forces GIAC to use the Task Scheduler facility. Task Scheduler tasks are able to run in an alternate security context, not just the system account.
	Allow system to be shut down without having to log on	Disabled	This option removes the shutdown option from the Windows logon dialog box. This forces a GIAC administrator to successfully authenticate against the system before shutting the system down.
	Allowed to eject removable NTFS media	Not defined	GIAC Enterprises does not use removable NTFS media.
	Amount of idle time required before disconnecting session	Not defined	This controls the amount of time that an SMB session can be idle before disconnection. The default is 15 minutes for servers. There is no change required in the GIAC Environment.
	Audit the access of global system objects	Disabled	Global or internal system objects are objects that can be shared between processes on a system. Auditing access to these is not critical to maintaining system security.

Audit use of Backup and Restore privilege	Enabled	This setting is enabled for GIAC Enterprises. As backups are a complete copy of the data on a system they need to be monitored closely. The backup and restore privileges have been split across two different users within GIAC. Any backups that occur out of the normal rotation are investigated.
Automatically log off users when logon time expires	Not Defined	This setting is not required within the GIAC Enterprises network. Users commonly work beyond standard business hours.
Automatically log off users when logon time expires (local)	Not Defined	As per previous table entry.
Clear virtual memory page file when system shuts down	Enabled	This setting is enabled on all machines with the GIAC Environment. The page file can contain sensitive information and copies of files that have been paged out of memory. The shutdown time of workstation and servers can be significantly impacted by this policy setting.
Digitally sign client communication (always)	Not defined	
Digitally sign client communication (when possible)	Enabled	The main traffic that needs protection against "man-in-the-middle" attacks is client to certain servers. Sometimes GIAC clients will need to communicate with servers that do not support digital signing. As such the client is configured to sign where possible.
Digitally sign server communication (always)	Enabled	This is the other side of the previous setting. GIAC server communication all requires signing. This combined with the previous setting effectively guarantee signing of all communication between servers with this setting defined and all GIAC clients.

Digitally sign server communication (when possible)	Not defined	
Disable CTRL+ALT+DEL requirement for logon	Disabled	Users in the GIAC Environment must use CTRL+ALT+DEL to logon. This ensures that logon occurs over a trusted session. Smart card users are exempt from this requirement.
Do not display last user name in logon screen	Enabled	Standard authentication requires both a username and password. If the last logged on username is displayed the attacker already has half the puzzle. Smart card users are exempt from this policy.
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM	The majority of authentication in the GIAC Environment should be via Kerberos. However if NTLM is required only NTLMv2 will be permitted. This prevents password crackers such as L0phtcrack being effective.
Message text for users attempting to log on	You are about to access the GIAC Enterprises network. Please ensure that you have fully read and understood the User responsibilities policy before continuing. Unauthorised access and misuse of the GIAC network is prohibited.	This is a head up for users connecting to the GIAC network. All users must be aware of the user responsibilities before connecting to the system.
Message title for users attempting to log on	GIAC Enterprises – Network Logon	The logon box looks better with a custom message title.

Number of previous logons to cache (in case Domain Controller is not available)	0 logons	No logon credentials will be cached on machines. This prevents an attacker from using the LSADump2.exe tool to remove these cached logons from the LSA Secrets key in the registry.
Prevent system maintenance of computer account password	Disabled	Setting this to Disabled in the GIAC Environment means that computers are able to change their passwords on the Domain Controllers.
Prevent users from installing printer drivers	Enabled	No users will be permitted to install printer drivers in the GIAC Enterprises environment. All printer drivers will be either part of the workstation build or deployed automatically from the print server.
Prompt user to change password before expiration	7 days	Users will be prompted to change their password 7 days before it is due to expire.
Recovery Console: Allow automatic administrative logon	Disabled	This setting is disabled within the GIAC network. This will ensure that anyone starting the machine from the recovery console must authenticate.
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled	This setting is disabled in the GIAC Environment to prevent someone copying data from the recovery console.
Rename administrator account	LarryPerkins	All the default administrator accounts within the GIAC Environment will be renamed. This will make it a little more difficult for an attacker. This setting does not affect the Relative Identifier (RID) 500 of the default administrative account.

Rename guest account	DickJohnson	All the default guest accounts within the GIAC Environment will also be renamed. As with the administrator accounts the RID (501) remains unchanged.
Restrict CD-ROM access to locally logged-on user only	Disabled	
Restrict floppy access to locally logged-on user only	Disabled	
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled	
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled	With this setting enabled, it ensures that all secure channel traffic is encrypted as all Domain Controllers within the GIAC Environment support encryption of secure channel traffic.
Secure channel: Digitally sign secure channel data (when possible)	Enabled	This setting ensures that all secure channel traffic to GIAC Domain Controllers is also signed.
Secure channel: Require strong (Windows 2000 or later) session key	Disabled	
Send unencrypted password to connect to third-party SMB servers	Disabled	There are no third-party SMB servers in the GIAC network. If there were having this setting disabled would prevent clear text authentication from being used to connect to them.

	Shut down system immediately if unable to log security audits	Enabled	This is enabled within the GIAC Environment to ensure all events with security significance are always logged. In order to ensure that server devices are always available this setting needs to be combined with a procedure for maintaining the security logs.
	Smart card removal behaviour	Lock Workstation	This setting ensures that the workstation console is secured the moment the token is removed.
	Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled	This setting will ensure that standard users only have read access to objects that are shared among processes on the target machine.[19]
	Unsigned driver installation behaviour	Do not allow installation	This is to prevent GIAC Enterprises users and staff from installing a driver that may compromise the stability of the system.
	Unsigned non-driver installation behaviour	Warn but allow installation	
Event Log			
Settings for Event Logs			
	Maximum application log size	8192 kilobytes	The application log maximum size for GIAC Enterprises is set to 8MB.
	Maximum security log size	49984 kilobytes	The security log maximum size for GIAC Enterprises is set to 50MB. This is to ensure that the security log will not fill before the security administrators can archive them.
	Maximum system log size	8192 kilobytes	The system log maximum size for GIAC Enterprises is set to 8MB.
	Restrict guest access to application log	Enabled	There is no reason for the guest account to have access to event logs within the GIAC Environment. This is a further implementation of the principle of Least Privilege.

	Restrict guest access to security log	Enabled	
	Restrict guest access to system log	Enabled	
	Retain application log	Not defined	
	Retain security log	Not defined	
	Retain system log	Not defined	
	Retention method for application log	As Needed	The application log is typically used for immediate troubleshooting. The application logs in the GIAC Environment are overwritten as needed.
	Retention method for security log	Manually	The security log will be cleared manually. GIAC Enterprises has a documented procedure for clearing and archiving the security logs.
	Retention method for system log	As Needed	
	Shut down the computer when the security audit log is full	Enabled	This is enabled within the GIAC Environment to ensure all events with security significance are always logged. In order to ensure that server devices are always available this setting needs to be combined with a procedure for maintaining the security logs.
Restricted Groups			
		R_PrintManager	Membership in these global groups for GIAC Enterprises must be controlled. By listing these as restricted groups GIAC can ensure that only authorised users are members of these groups. The procedure for adding a user to these groups includes modifying this group policy object. As well as controlling the members of the group this can also control which groups the group is a member of. This gives the identified role groups added security.
		R_ClientServices	
		R_DesktopSupport	

	R_Auditor	
	R_Operator	
	R_Supervisor	
	Enterprise Admins	
	Domain Admins	
System Services – Not covered here		
Registry – Not covered here		
File System – Not covered here		
Public Key Policies		
Encrypted Data Recovery Agent		
	Corp Recovery	Corp Recovery is the designated EFS recovery agent for the corp.giac.com.au domain. As this account has the ability to recovery any encrypted file within the corp.giac.com.au domain it is essential that the private key for this account be protected. The policy for the recovery agent is shown in Figure 16 - Corp EFS Recovery Agent.
Automatic Certificate Requests		
	Computer	All computers within the domain will automatically be issued certificates for the purposes of client and server authentication.
	IPSec	All computers within the domain will automatically be issued certificates for the purposes of IPSec communication. Only certain hosts within the GIAC Environment need to communicate using IPSec.
Trusted Root Certification Authorities		

		Stand-Alone Root – Minerva	Minerva is the name of the stand-alone root certification authority. This is the only trusted root certification authority for GIAC Enterprises.
Enterprise Trust			
		None Configured	At this stage there are no other enterprises that the GIAC certificate hierarchy trusts. This capability may be used in the future however. If a trust is required it will be implemented in the Domain Computer Policy.
IP Security Policies on Active Directory			
	Default GIAC IPSec	Assigned = Yes	This setting is the default for all GIAC hosts. They have the ability to use IPSec if it is required or requested by the target server. This enables GIAC to have a very fine level of control over where IPSec is used within the GIAC Environment. This policy has been created especially for GIAC Enterprises. Best practice says that new IPSec policies should be created instead of using the defaults.
	Client (Respond Only)	Assigned = No	
	Secure Server (Require Security)	Assigned = No	
	Server (Request Security)	Assigned = No	
Administrative Templates – Not covered here			

There is also an XP Workstation Policy in use but not covered within this document. The XP Workstation Policy is applied in addition to and only adds minimal changes to the default computer policy.

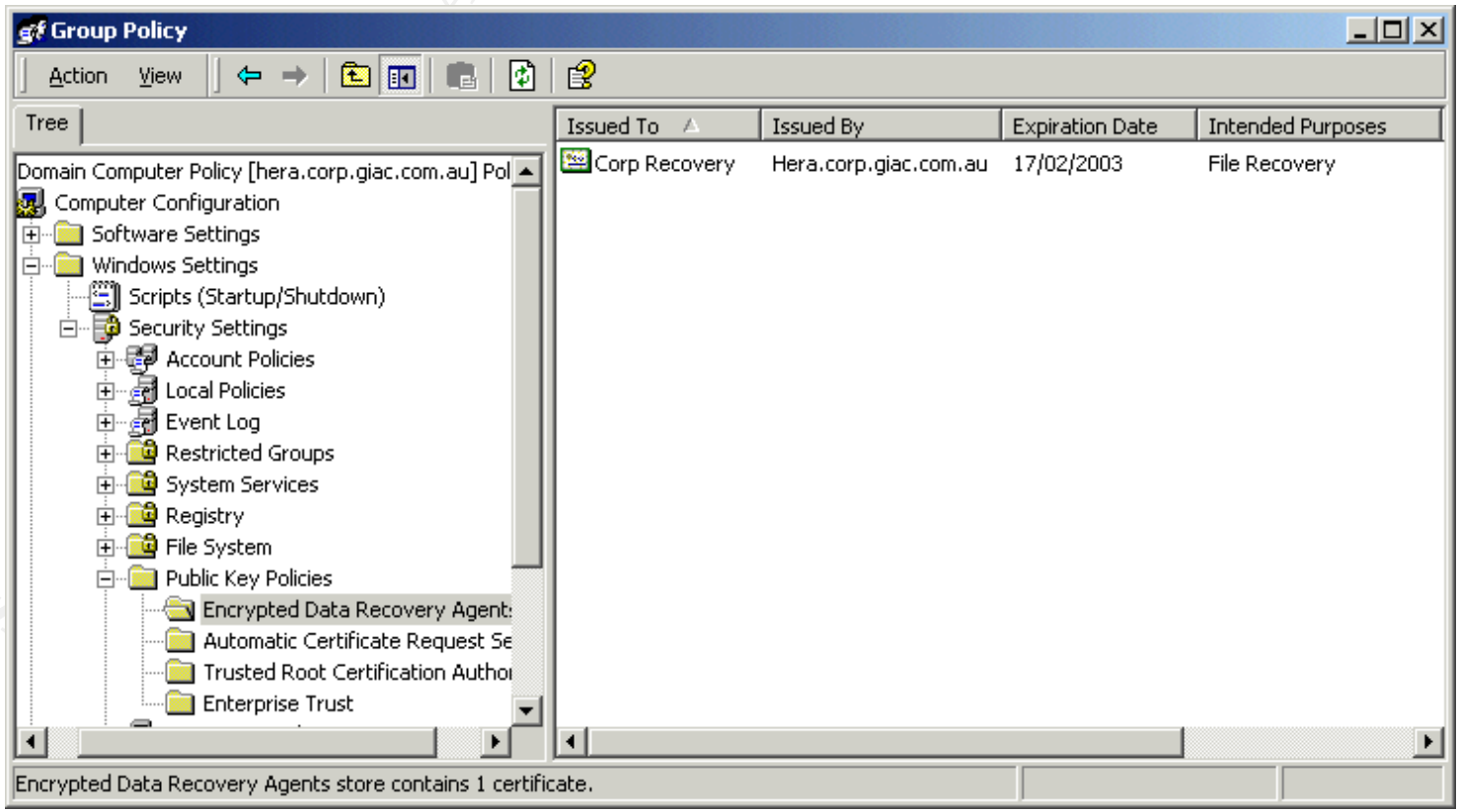
There two primary differences between a workstation and a server. These are:

- The value of the information stored on the server

- The value of the services offered to other hosts on a network.

The "value" of servers is greater than workstations due to these two factors.

Figure 16 - Corp EFS Recovery Agent



6.5.3 Domain Controllers Policy

Most of the settings that apply to Domain Controllers will be inherited from the Domain Computer policy. The main area where Domain Controllers differ within the GIAC Enterprises environment are the auditing requirement of Domain Controllers. There is no IPSec

policy in place between Domain Controllers and clients in the GIAC network. Using IP Security (IPSec) to protect traffic from a domain member to the Domain Controller is not supported in Windows 2000. It is not possible for computers to get the initial IPSec policy from the Domain Controller once a Domain Controller (DC) requires IPSec to communicate.[20] As with the previous policies this policy is applied to the corp.giac.com.au, dmz.giac.com.au and giacroot.int domains.

Table 18 - Domain Controllers Policy

Policy Section	Policy	Configured Setting	Reason for Application
Windows Settings			
Security Settings			
Account Policies			
Password Policies			
Account Lockout Policy			
Local Policies			
Audit Policy			
	Audit account logon events	Not Defined	Inherited from the Domain Computer Policy
	Audit account management	Success, Failure	Both success and failure events are audited on Domain Controllers. This will give some indication of people trying to modify accounts unsuccessfully.
	Audit directory service access	Not Defined	Inherited from the Domain Computer Policy
	Audit logon events	Not Defined	Inherited from the Domain Computer Policy
	Audit object access	Not Defined	Inherited from the Domain Computer Policy
	Audit policy change	Success, Failure	Policy Change on GIAC Enterprises Domain Controllers will be audited for both success and failure.
	Audit privilege use	Not Defined	Inherited from the Domain Computer Policy

	Audit process tracking	Not Defined	Inherited from the Domain Computer Policy
	Audit system events	Not Defined	Inherited from the Domain Computer Policy
Event Log			
Settings for Event Logs			
	Maximum application log size	16384 kilobytes	The application log maximum size for GIAC Enterprises Domain Controllers is set to 16MB.
	Maximum security log size	Not Defined	Inherited from the Domain Computer Policy
	Maximum system log size	16384 kilobytes	The system log maximum size for GIAC Enterprises Domain Controllers is set to 16MB.
	Restrict guest access to application log	Not Defined	Inherited from the Domain Computer Policy
	Restrict guest access to security log	Not Defined	
	Restrict guest access to system log	Not Defined	
	Retain application log	Not Defined	Inherited from the Domain Computer Policy
	Retain security log	Not Defined	Inherited from the Domain Computer Policy
	Retain system log	Not Defined	Inherited from the Domain Computer Policy
	Retention method for application log	Not Defined	Inherited from the Domain Computer Policy
	Retention method for security log	Not Defined	Inherited from the Domain Computer Policy

	Retention method for system log	Not Defined	Inherited from the Domain Computer Policy
	Shut down the computer when the security audit log is full	Not Defined	Inherited from the Domain Computer Policy

6.5.4 Domain User Policy

The Domain User Policy is the default policy applying to users in the corp.giac.com.au domain. This policy is applied to the GIAC Organisational unit. From there all other OUs under the GIAC structure will inherit these settings. The role accounts OU is not affected by this policy. The Domain User policy will primarily focus on changes to the Windows Interface. Security and Availability of workstations can be increased significantly by only allowing users access to functions they need to carry out a given task.

Figure 17 - Domain User Policy

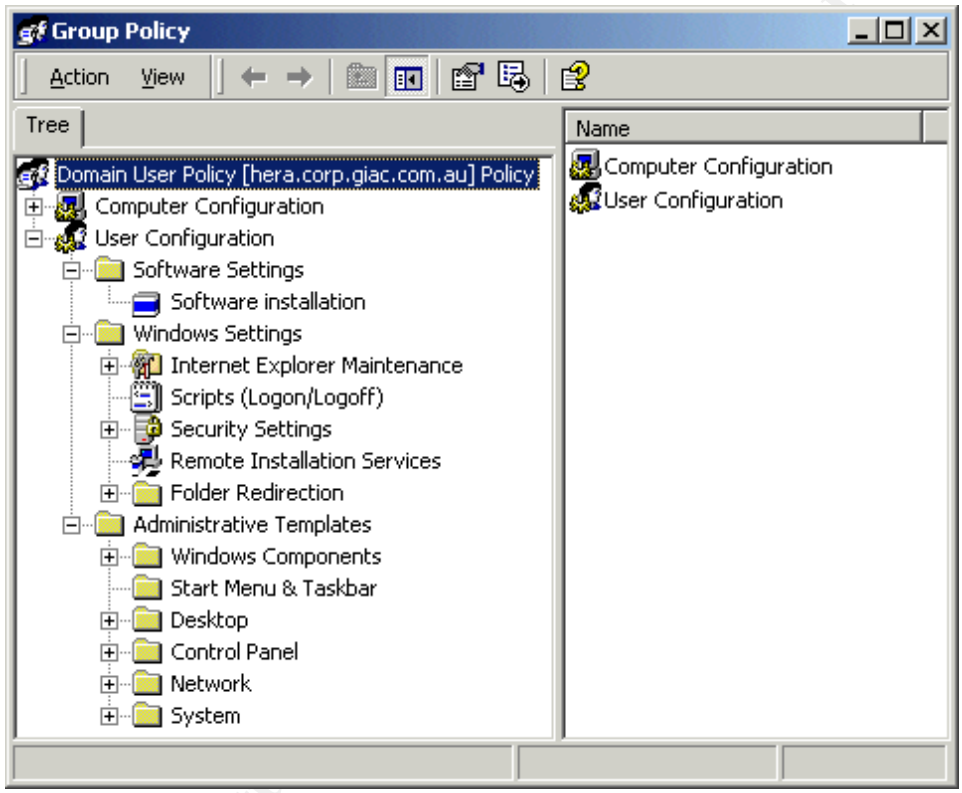


Figure 17 - Domain User Policy show the top level of options that are available for User Configuration. As with the computer focussed policies this policy is optimised by having the Computer Configuration section disabled. Tasks that are be controlled on GIAC workstations include but are not limited to:

- Access to command interpreters (cmd.exe and command.com).
- Ability to run programs other than those on the allowed run list.
- Control panel access.
- Ability to change networking settings.
- Ability to bring up dial-up connections while connected to the network.
- Ability to install and modify installed software packages.

Included in this policy are settings that control access to the Microsoft Management Console. This group policy object will restrict access to MMC snap-ins.

6.5.5 Finance & Human Resources Policies

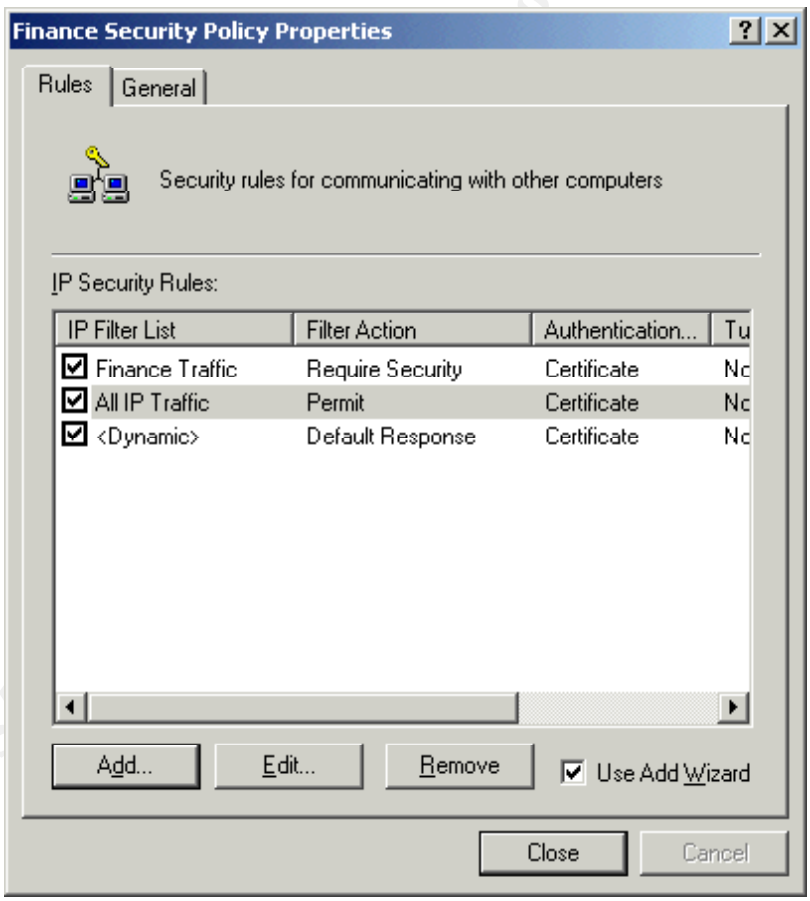
The Group Policy object applied to the Finance and Human Resources OUs contain configuration items for IPSec and EFS.

6.5.5.1 IPSec Policies

The IPSec policies are filtered and only apply to servers within these Organisational Units. Server groups as shown in Table 15 - Group Policy Security Groups are used to filter application of these Group Policy objects.

Earlier we looked at the IPSec policy in the Domain Computer Policy. This contained a rule that enabled all hosts to reply using IPSec when requested by the server. The policy shown below in Figure 18 - Finance IPSec Policy is the other half of the equation. This policy requires IPSec for all traffic to the application running on the Finance servers.

Figure 18 - Finance IPSec Policy



The IP Security rules shown are not applied in order. The rules are ordered in the background from the most specific to the most generic. The most specific rule in this case is the Finance Traffic rule. This rule will fire first out of the rules shown above. This guarantees that all traffic to the Finance application is encrypted.

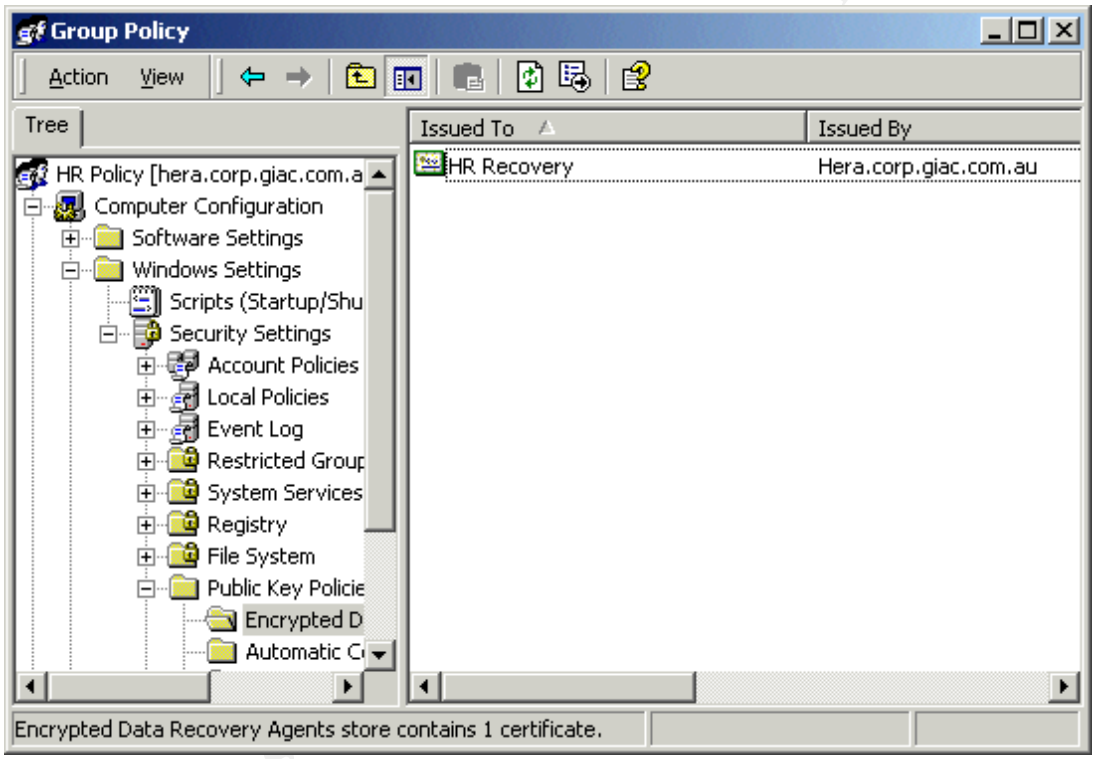
The GIAC Windows 2000 PKI is being used to provide certificates for IPSec. See Table 17 - Domain Computer Policy for more information.

The Human Resources IPSec policy is configured the same way as shown above. The filter list is configured to encrypt the Human Resources traffic.

6.5.5.2 EFS Recovery Agent

The other purpose of the Group Policy Objects for the Finance and Human Resources OUs is to assign EFS Recovery Agents. Each of these Organisational Units has their own EFS Recovery Agent. Figure 19 - Human Resources EFS Recovery Agent shows the Human Resources Group Policy Object and the Certificate used as the HR Recovery Agent.

Figure 19 - Human Resources EFS Recovery Agent



For hosts in the Human Resources and Finance OUs files encrypted have the following fields. The Data Decryption Field (DDF) holds the File Encryption Key (FEK) encrypted with the users public EFS key. These files will also have two Data Recovery Fields (DRF) each of these contains the FEK encrypted by the HR Recovery agents public key and the Corp Recovery agents public key (see Figure 16 - Corp EFS Recovery Agent for additional information).

A procedure is in place to issue a new recovery agent certificate when the old one expires. The default expiry time of one year has been left in place.

6.5.6 Mobile Devices Policy

The Mobile Devices Policy is applied to the GIAC OU. Application of this policy is filtered using the GP_Mobile_Devices group.

6.5.7 XP Workstation Policy

The XP Workstation policy will be used primarily for software and patch deployment to client workstations. Software patches from Microsoft will soon ship in native .msi format. This allows easy deployment using Group Policy.

It is critical in the GIAC Environment that security related patches are deployed to the end machines as soon as practical. The longer it takes to deploy a patch the greater the windows of opportunity for the vulnerability to be exploited. The XP Workstation Policy along with the Workstation SOE guarantee that patches can be deployed to end stations within hours of initial discovery. See section 3.3.2 for additional information on the SOE.

6.5.8 Kiosks Policy

The Kiosks Policy is used to control the desktop environment presented to users on the Kiosk machines. The Kiosk machines run a web based application that provides fortunes to customers. When the machine starts the only interface that is presented is the Fortune telling application. This is configured through the Local Group Policy Object on each of the kiosk machines.

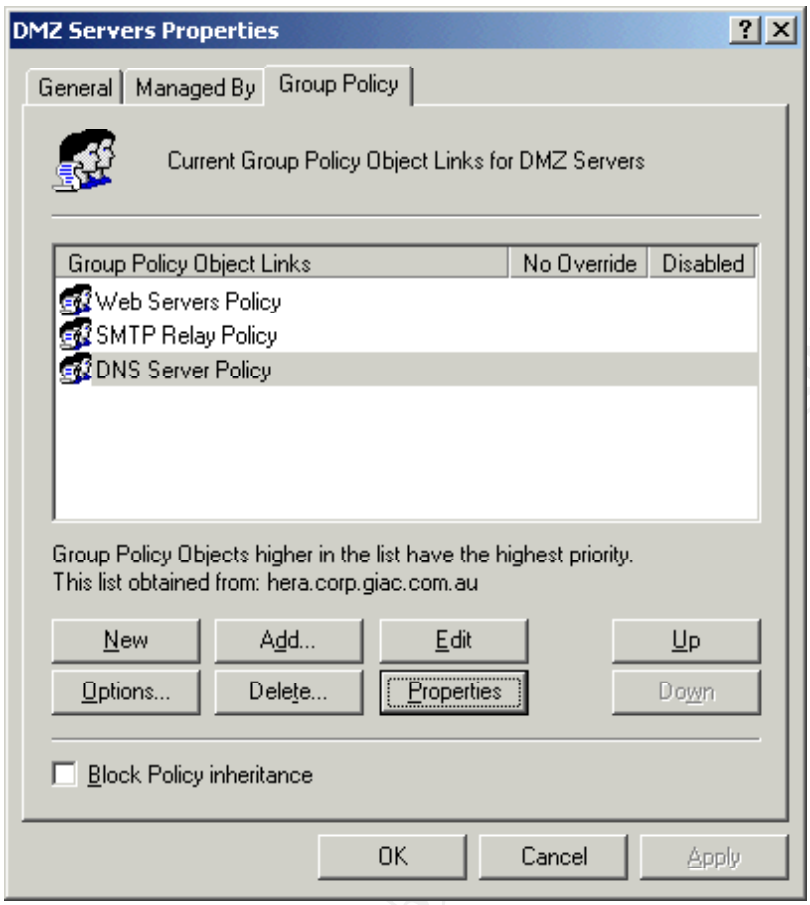
The Kiosk machines have to be configured using the Local Group Policy Object as they are intermittently connected.

It is critical that the security applied to the Kiosk machines is maintained and audited. The Kiosks Group Policy Object will be used to run a VB script. The VB script will run the Secedit.exe utility to compare the security applied to the Kiosks with the original template.

6.5.9 dmz.giac.com.au Policies

There are three security related policies that are applied to Organisational Units in the DMZ domain. These policies are shown in Figure 20 - DMZ Group Policies. Each Group Policy Object is tailored for individual groups of servers within the DMZ.

Figure 20 - DMZ Group Policies



Group Policy ACLs are used ensure that the correct policy is applied to each server. For more information on the Group Policy ACL model for GIAC refer to section 6.2.

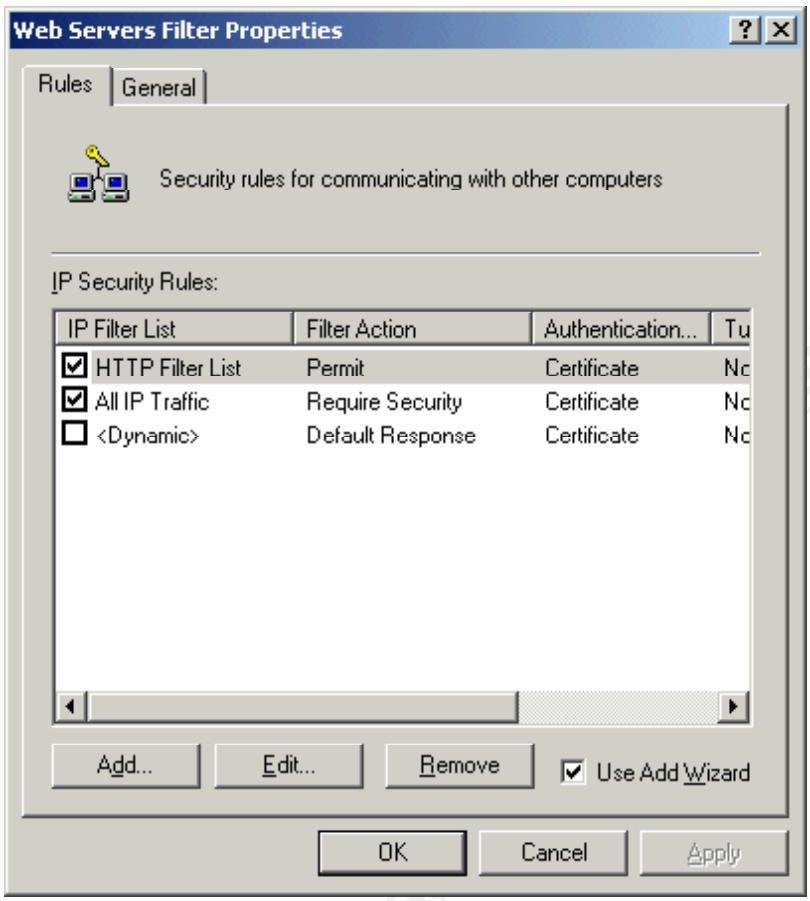
6.5.9.1 Web Servers Policy

The Web Servers Policy is used to apply additional security to the Web servers within the DMZ. The four critical areas of Web Server security that are addresses by the Web Servers Group Policy Object are:

- Packet Filtering using IPSec
- Security Patch Deployment
- Web server registry modifications
- NTFS Permissions on IIS files.

Figure 21 - HTTP IPSec Policy shows the IPSec policy applied to the Web servers within the GIAC DMZ. The HTTP Filter list contains protocol definitions for both HTTP and HTTPS. Each of these will be permitted to all Web servers. The second rule requires Authentication Headers to be used for all other IP traffic to the Web servers.

Figure 21 - HTTP IPSec Policy



The configuration also simplifies the firewall configuration on the firewall that allows internal hosts to manage the web server. The only rule required is a rule to allow Protocol ID 51.

The Web Servers Filter is an implementation of Defence-in-Depth. In addition to having filtering in place on the firewalls each host in the DMZ will also filter incoming traffic.

The second function of the Web Servers GPO is to deploy hot-fixes to the Web Servers. An Microsoft Installer (MSI) generator will be used to re-bundle the hot-fix exe's from Microsoft. The MSI's can then be easily deployed to each Web Server using Group Policy. Microsoft has indicated that sometime in the future all hot-fixes will be available in MSI format.

The last area specifically addressed by the Web Servers GPO is IIS specific registry modifications. Table 19 - IIS Registry Modifications shows the registry changes deployed to GIAC Web Servers using Group Policy.

Table 19 - IIS Registry Modifications

Setting	Purpose

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting = 2	This setting tells the GIAC web servers to drop any packets that are source-routed. There is no valid reason for a client to use source-routing when connecting to the GIAC web servers. Source-routed packets will always follow a pre-determined path.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect = 2	This setting will reduce the retransmission of SYN-ACK retries sent by GIAC Web Servers
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpHalfOpen = 100	This setting controls the threshold at which the SynAttackProtect setting starts on GIAC Web Servers. This setting states that there must be 100 connections in a SYN_RECEIVED state.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpHalfOpenRetried = 80	This setting controls the number of SYN_RECEIVED sessions that have retried the send of a SYN_ACK that need to exist before SynAttackProtect starts on GIAC servers.

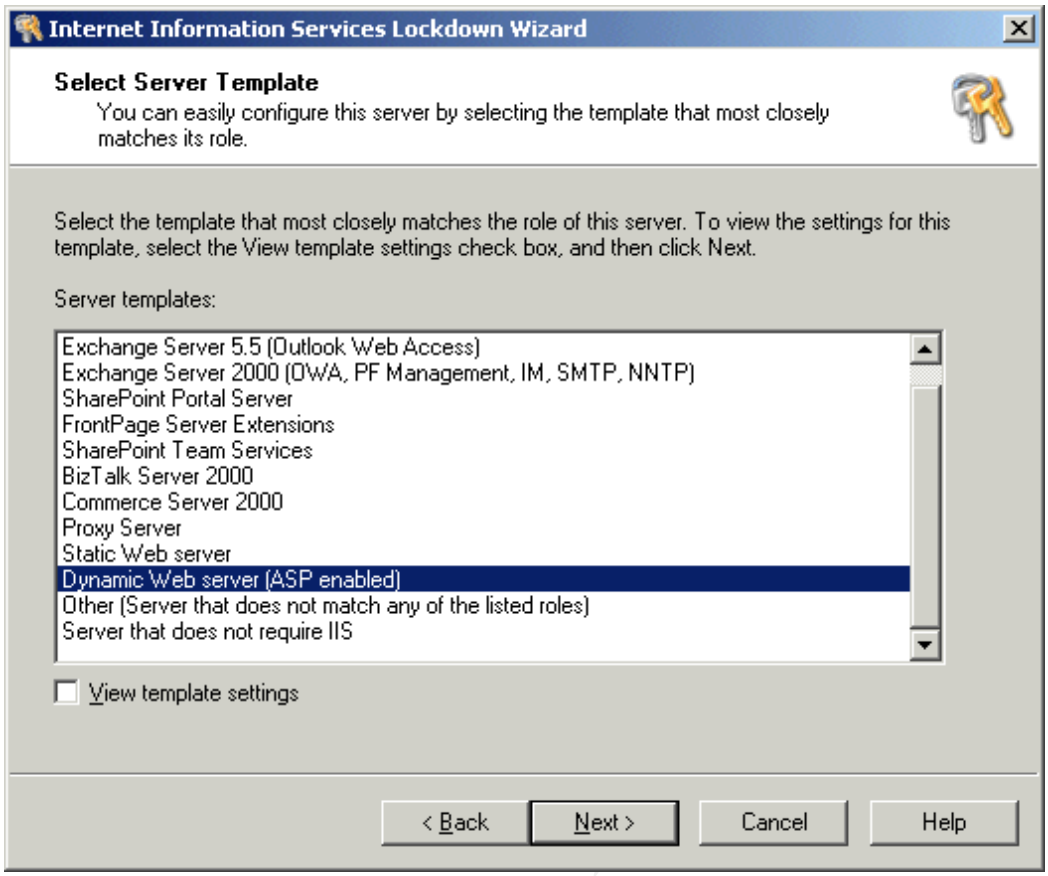
The Sceregvl.inf[21] file on the Group Policy management machine was modified. This enabled GIAC to use the GUI tools to enable these settings in Group Policy.

The Web server GPO is also used to apply NTFS permissions to IIS files and folders. This is done to ensure that the principle of Least Privilege is applied to all GIAC Web Servers.

NTFS permissions are also used to secure the GIAC web server. No files that are available to web users allow both write and execute.

The IIS Lockdown tool was used as shown in Figure 22 - IIS Lockdown Tool. The dynamic web server template was applied.

Figure 22 - IIS Lockdown Tool



The IIS Lockdown tool is used to secure the following aspects of IIS:

- Disabled WebDAV
- Disabled Indexing Service
- Disabled Internet printing
- Installed URLScan.
- Disabling unneeded script mappings
- Removed printer virtual directory
- Removed IIS Samples virtual directory
- Removed MSADC virtual directory
- Removed Scripts virtual directory
- Removed IISAdmin virtual directory
- Removed IISAdmin web site
- Removed IISHelp virtual directory

- Denied execute permission for system utilities to anonymous user account
- Denied write permissions to web content directories to anonymous user account
- Disabled smtpsvc Service.

6.5.9.2 SMTP & DNS Policies

These Group Policy Objects serve many of the same functions as the Web Servers Policy. There is an IPSec policy that requires Authentication Headers for all non SMTP & DNS traffic.

6.5.10 Terminal Services Policy

The Terminal servers in use by GIAC have a particular policy applied to them. Access to this policy is restricted via Group Policy Filtering. There are areas where Terminal Services require different types of policy setting to standard servers.

Table 20 - Terminal Services Policy details the changes made by the Terminal Services Policy. These changes are made in addition to and take precedence over the Default Computer and Default Domain Policies.

Table 20 - Terminal Services Policy

Setting	Purpose
Restrict Floppy Access to Locally Logged on User Only	This prevents GIAC users from accessing the Floppy drives on the Terminal Servers when connected over a Terminal Server session.
Restrict CD-ROM Access to Locally Logged on User Only	This prevents GIAC users from accessing the CD-ROM drives on the Terminal Servers when connected over a Terminal Server session.
Disable Windows Installer	Under no circumstances will GIAC users need to install software on the Terminal Servers. This policy will apply to all Terminal Services Users. Terminal Services administrators are exempt from this policy.
Folder Redirection	Terminal Services users in the GIAC Environment will have their Home Drives and other user data stored on the GIAC file servers. Folder redirection ensures users will have access to these resources through both Terminal Services and Standard network clients.
Hide These Specified Drives on my Computer	All local drives will be hidden from Terminal Services users. They have no need to install software or store data on the Terminal Server Machines.
Disable and Remove the Shutdown command	This setting is critical on a Terminal Server. The shutdown command used through a Terminal Services session will shutdown the Terminal Server itself.

Disable Control Panel	No GIAC users need access to the control panel over a Terminal Server session. Any changes made will affect all users of the machine. Access to this is therefore restricted.

7 Security Scripting

There are several security related tasks within the GIAC Environment that can be easily automated through the use of scripts.

Table 21 - Security Scripts

Script	Purpose
Log file analysis	VB scripts have been developed that allow GIAC administrators to search log files for anomalies. This simplifies the process of log file analysis significantly.
Hard Drive Search	This VB script will search hard disk in the GIAC Environment for known hacking tools. This script runs automatically and is deployed using Group Policy.
Admin Password Change	This script will periodically change the local administrator password on all GIAC workstations.
Security Auditing	This script calls the Secedit.exe utility. It is used to ensure that the Local Group policy objects are still identical to the templates that were used to create them initially. A change to the LGPO could indicate a security breach. It is essential that this script analyse the target machine without making any changes to the target.

8 Procedures

The best technical countermeasures are worthless without Standard Operating Procedures (SOP). Procedures ensure that the countermeasures applied to the GIAC Environment continue to be effective after the initial configuration.

8.1 Security Patching

One of the most critical aspects of security is maintaining security patches on devices.

The impact of Code Red and Nimda worms would have been significantly reduced if the sites affected had an effective security patching procedure. The vulnerabilities that these worms exploited were discovered long before the advent of the worms. Patches that fixed these vulnerabilities were available months before the worms hit.

The security patching procedure that GIAC employs details the following steps.

8.1.1 Vulnerability Notification

It is critical that information about vulnerabilities is found quickly. To ensure this the GIAC Security Administrators subscribe to both vendor based and independent security mailing lists. This broad coverage of information gives GIAC every chance of obtaining timely notification of vulnerabilities.

8.1.2 Research Vulnerability

GIAC Security Administrators next gather and analyse all the information they can obtain about the vulnerability. An assessment is then made as to the level of risk this poses to the GIAC Environment. The level of risk determines the level and speed of response required within GIAC.

8.1.3 Plan Response

Once the extent of the vulnerability is known a response is planned. As stated in the previous section the level of the response is based on the degree of risk. This may range from simply adding a rule to the firewalls, to applying a patch to all hosts attached to the network.

8.1.4 Test Response

This is also a critical phase. The level of testing carried out is directly proportionate to the risk associated with the vulnerability.

When the vulnerability has a high chance of compromising the GIAC Environment and has a high chance of being used, the level of testing before applying security patches decreases.

For low risk vulnerabilities the testing carried out is more comprehensive. A security patch could have adverse affects on system to which it is applied.

8.1.5 Deploy Response

After testing the response it is deployed to all affected devices within GIAC.

8.1.6 Review Procedure

After the procedure has been carried out a review is conducted. Anywhere that the procedure failed or could be improved is identified and implemented for the next run.

8.2 Log Monitoring

There is no value in collecting audit information if it is never used. Log monitoring is an essential GIAC activity. Automated analysis of logs is performed by the log analysis scripts (Section 0).

The following are security related logs that are examined on the GIAC system:

- Web Server Logs

- Domain Controller Security Logs
- All servers Security Logs
- PIX Firewall Logs
- Certificate Server Logs
- Cisco Secure Logs.

8.3 Staff Exit Procedure

This procedure ensures that access to the network is disabled as soon as staff exits the organisation. This procedure requires co-ordination between the Human Resources and IT Support departments.

There are two scenarios that the exit procedure covers.

8.3.1 Gracious Exit

In this instance access will be removed when the staff member no longer needs it. Usually this is sometime during their last day at work.

8.3.2 Ungracious Exit

In this instance the staff member is not leaving on good terms. Access in this case needs to be removed as soon as the staff member is notified by Human Resources. The notification from Human Resources is critical to making this procedure work.

8.4 Incident Handling

Incidents are unfortunate but they do happen. When an incident occurs it is essential that there is a plan in place that clearly states what needs to be done. The primary issues covered by the incident handling policy are:

- Identify who is responsible for handling the incident.
- Identify who can authorise additional resources and funds.
- Identify critical industry and vendor contacts.
- Detail the process to be followed when an incident is identified.
- Detail acceptable down times if an outage is involved.

8.5 User Awareness Training

Regular User Awareness Training sessions must be conducted. These sessions are designed to inform users of their roles and responsibilities within the GIAC Environment. They are conducted in a non-confrontational manner. The goal is to have the users take personal responsibility for information security.

8.6 Security Review

All the security countermeasures in place within the GIAC Environment are reviewed every six months. The review requires an **independent** security risk analysis to be performed. This analysis will determine the level of compliance with the security policy and technical implementation documentation. This review is conducted as instructed in the ISO/IEC 17799:2001 and AS/NZ 4444:2001 Standards[22].

9 Glossary

This glossary contains descriptions of the acronyms used within this document.

Table 22 - Glossary

Acronym	Description
ACE	Access Control Entry. This is the individual entry in an ACL. Groups of ACEs make up an ACL.
ACL	Access Control List. This is made up of ACEs. ACLs are applied to a resource to authorise or deny access.
AD	Active Directory. An X500 compatible directory that runs on Windows 2000 Domain Controllers.
AH	Authentication Headers. Part of the IPSec suite of security protocols. AH provides authentication, integrity, and anti-replay for the entire packet (both the IP header and the data carried in the packet).
AS/NZ	Australia/New Zealand.
CA	Certificate Authority.
CIA	Confidentiality, Integrity, Availability.
CRL	Certificate Revocation List. Used to give clients a method of checking whether a certificate is still valid. All revoked certificates will appear on the CRL.
CTL	Certificate Trust List. Used to specify which other CAs are trusted by the PKI.
DC	Domain Controller.
DDF	Data Decryption Field. Portion of an encrypted file that contains the File Encryption Key encrypted with the encrypting users public key.
DES	Data Encryption Standard.
DESX	A 120bit variation of the DES encryption standard.

DMZ	De-Militarized Zone.
DNS	Domain Name System.
DRF	Data Recovery Field. Portion of an encrypted file that contains the File Encryption Key encrypted with the recovery agents public key.
EFS	Encrypting File System. File based encryption that ships with the Windows 2000 Operating System.
ESP	Encapsulating Security Payload. The portion of the IPSec suite that encrypts data. ESP provides confidentiality, in addition to authentication, integrity, and anti-replay.
FEK	File Encryption Key. The key used to encrypt and decrypt the file.
FQDN	Fully Qualified Domain Name.
FSMO	Flexible Single Master Operations.
GPO	Group Policy Object.
HTTP	Hyper Text Transfer Protocol.
IEC	International Electrotechnical Commission.
IPSec	Internet Protocol Security.
ISO	International Standards Organisation.
KMS	Key Management Server. The portion of Exchange that integrates with Certificate Services to enable Exchange to participate in the Windows 2000 PKI.
LAN	Local Area Network.
LGPO	Local Group Policy Object.
MMC	Microsoft Management Console.
MSI	Microsoft Installer.
NAT	Network Address Translation.
NLBS	Network Load Balancing Service.
NSA	National Security Agency.
OU	Organisational Unit.
PKI	Public Key Infrastructure.

RA	Registration Authority. The certificate issuer.
RBA	Role Based Administration.
RID	Relative Identifier. Unique identifier assigned to each user account. Default administrator is always 500, Guest is always 501. User accounts start at 1000.
SHA-1	Secure Hash Algorithm 1.
SID	Security Identifier.
SMTP	Simple Mail Transfer Protocol.
SNTP	Simple Network Time Protocol.
SOE	Standard Operating Environment.
SOP	Standard Operating Procedures.
SSL	Secure Sockets Layer.
TGT	Ticket Granting Ticket.
USB	Universal Serial Bus.
WAN	Wide Area Network.

10 References

[1] *Microsoft Product Documentation. "Maximum tolerance for computer clock synchronization. 2002.* URL:http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/proddocs/514.asp

[2] *Microsoft Whitepaper. "Microsoft Internet Security and Acceleration Server (ISA) Technical Overview". 2001.* URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/isa/evaluate/isatecov.asp

[3] *Cisco Whitepaper. "Guidelines for the deployment of Cisco Secure ACS for Windows NT/2000 servers in a Cisco Catalyst Switch environment". Jan 2002.* URL:http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/deacs_wp.htm

[4] *Cisco Documentation. "Cisco 827 Product Overview". Feb 2002.* URL:http://www.cisco.com/univercd/cc/td/doc/pcat/827.htm

5 *Cisco Datasheet. "Cisco 2600 Series Modular Multiservice route". Dec 2001.* *URL:http://www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/2600_ds.htm*

6 *Microsoft Knowledge Base Article. "How to configure an Authoritative Time Server in Windows (Q216734). 10 Jan 2002.* *URL:http://support.microsoft.com/default.aspx?scid=kb;EN-US;q216734*

7 *Schmidt, Jeff. Microsoft Windows 2000 Security Handbook. Indianapolis: QUE. 2000.*

8 *Microsoft Whitepaper. "Windows 2000 Certificate Services". 2002.* *URL:http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/2000cert.asp*

9 *Microsoft Knowledge Base Article. "Traffic that can and cannot be secured by IPSec". 16 Aug 2001.* *URL:http://support.microsoft.com/default.aspx?scid=kb;EN-US;q253169*

10 *Microsoft Knowledge Base Article. "Group policy may not be applied to users belonging to many groups". 20 Jan 2002. URL:* *http://support.microsoft.com/default.aspx?scid=kb;EN-US;q263693*

11 *Havrilla, Jeffery S. "Cert Summary CS-2001-04 DNS". 12 Oct 2001.* *URL:http://www.kb.cert.org/vuls/id/109475*

12 *Ruth, Andy & Collier, Bob. The Concise Guide to Microsoft Windows 2000 DNS. Indianapolis: QUE. 2000.*

13 *Jennings, Roger. Using Windows 2000 Server. Indianapolis: QUE. 2000*

14 *National Security Agency. "Windows 2000 Security Recommendation Guides". 29 Jan 2002.* *http://nsa2.www.conxion.com/win2k/download.htm*

15 *Microsoft Product Documentation. " Network Security: Force logoff when logon hours expire" 2002.* *URL:http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/proddocs/566.asp*

16 *Microsoft. "Account Logon Events" Windows 2000 Server Resource Kit. 2002.* *URL:http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/reskit/prnf_msg_tkfy.asp*

17 *Microsoft. "Logon Events". Windows 2000 Server Resource Kit. 2002.* *URL:http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/reskit/prnf_msg_pfjj.asp*

18 *Microsoft. "Security Options". 2002.* *URL:http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/proddocs/SOtopnode.asp*

19 *Microsoft. "System objects: Strengthen default permissions of internal system objects (e.g., Symbolic Links). 2002.* *URL:http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/p*

roddocs/595.asp

[20] *Microsoft Knowledge Base Article. "Client-to-Domain Controller and Domain Controller-to-Domain Controller IPSec Support (Q254949)". Aug 16 2001. URL:http://support.microsoft.com/default.aspx?scid=kb;EN-US;q254949*

[21] *Microsoft Knowledge Base Article. "Adding custom registry settings to the Security Configuration Editor (Q214752)". 27 Nov 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q214752*

[22] *Standards Australia. ISO/IEC 17799:2001 Information Security Management. Sydney: Standards Australia. 2001*