Global Information Assurance Certification Paper

Certified Windows Security Administrator (GCNW)

Practical Assignment Version 3.1 (revised April 8, 2002)

Option 1 - Design a Secure Windows 2000 Infrastructure

Keith T. Okamoto

Abstract

This document outlines a security strategy used by a fictional company, GIAC Enterprises, which from this point on will be known as GIACE. GIACE's Information Technology (IT) department has been tasked to design and implement a secure Windows 2000 Active Directory (AD) network. The network design will be driven by three factors: (a) physical and geographical layout, (b) business goals, and most significantly, (c) IT resource administration methods, which summarized are:

- Centrally manage all IT resources.
- Use the "least privilege" approach to manage accounts and services on the network.
- Establish redundant, independent security controls to protect the network.
- Balance security controls with user-friendliness.
- Consistently use basic controls and simple design structures to manage resources.

The document will also describe one method of designing domain structure and Organizational Units (OU) to apply Group Policy, which replaces Windows NT4 System Policy as the primary method to apply and configure security settings of user and computer objects.

Table of Contents

List of Tables

List of Figures

DESCRIPTION OF GIAC ENTERPRISES

Background

Founded in September 1997, GIACE is a vendor of embedded single-board computer (SBC) appliances. GIACE's best selling products are specifically designed as firewall/router or Virtual Private Network (VPN) solutions. The SBC appliances are designed in two forms, modular and pre-built. The modular design allows customers to completely configure the SBC themselves, while the pre-built design includes a choice of installed operating systems and configuration settings that allow the SBC to be quickly and easily deployed in the customer's organization. At present, 80 percent of GIACE's total sales revenue comes from online sales, 10 percent comes from phone orders, and 10 percent comes from corporate and private accounts.

In parallel with the recent struggles felt in the technology sector however, the overall SBC market has become more diversified and fragmented. Consequently, GIACE's sales revenue has diminished and their products have fallen into a niche market. In an effort to reduce Information Technology (IT) management costs and to further protect its proprietary assets, the Chief Executive Officer (CEO) has requested that a proposal to upgrade GIACE's present Windows NT4 network using a Windows 2000 infrastructure be submitted within 45 days. The proposal must take into account that GIACE's has three offices, which have the following organizational structure and geographical layout:

- Headquarters, which is located in Atlanta, Georgia and consists of 400 employees, houses these departments:
    - Administration consists of eight members that include the CEO, Chief Information Officer (CIO), and the six department chiefs. Their most important duties include optimizing cash flow and inventory levels, establishing both short-term (1 year) and long-term (3 year) plans for the continued growth and success of GIACE, maintaining effective communication channels with their workforce, and increasing GIACE's corporate and private client base.
    - Sales and Marketing is responsible for processing and shipping product orders, managing customer relations, and increasing GIACE's market share through print and online advertising.
    - Finance and Human Resources control internal accounting and employee records, and handle training and employee concerns.
    - Customer Service is responsible for working closely with customers to provide timely solutions to problems. They also create and publish electronic user manuals, hardware and software specifications manuals, and troubleshooting guides and reports for all of GIACE's products. Electronic publications are posted on GIACE's website.
    - IT has a variety of duties. The System Administrators are responsible for maintaining the infrastructure and security of GIACE's internal

network and evaluating new hardware and software technologies. The Network Administrators are responsible for configuring and securing networking devices. The Web Administrators manage and secure the web and database servers, while the Web Developers generate the programmatic content of GIACE's web site. Finally, the Help Desk provides training and support to GIACE's employees.

- Research and Development, located in Portland, Oregon, consists of 160 employees. They are responsible for developing and testing new products, improving the cost-efficiencies of existing products, providing technical support to customer service when needed, and providing specifications to Manufacturing and Production. A team of eight IT members provides onsite system administration and user support for the department.
- Manufacturing and Production, located in Artesia, New Mexico, consists of 120 employees. The team creates and assembles the parts needed to build the SBC appliances to specification, and ensures that inventory levels are maintained. A team of four IT members provides onsite system administration and user support for the department.

Current management style will also impact the infrastructure design. Since its inception, GIACE has practiced a straightforward, basic philosophy of managing its IT resources. The Administration and IT departments have reevaluated their philosophy and have agreed that the same concepts are still both relevant and sound. To summarize:

- The Headquarters IT department centrally manages all resources.
- Use the "least privilege" approach to manage user, group, and computer accounts; only permissions needed by the account to accomplish its tasks are allowed.
- Establish redundant, independent security controls to protect the network. It is easier for a remote attacker to bypass one level of security rather than two or three levels of security. It also increases the likelihood that a network intrusion will be detected.
- Balance the level of security with the user. Security controls should be stringent, but not impede the performance of a user. Frustrated users are less efficient and may try alternative means to bypass security controls they feel are excessive. Human Resources conduct bi-annual training forums to collect input from employees.
- Lastly, and most importantly, consistently use basic controls and simple design structures to manage resources. Complex design usually adds marginal benefits, while adding a disproportional amount of maintenance costs and network troubleshooting effort.

NETWORK DESIGN AND DIAGRAM

Assumptions

GIACE manages its Internet Protocol (IP) address pool using statically assigned addresses for all hosts on its network. Hosts are assigned Request for Comments (RFC) 1918 private IP addresses as follows: (a) Headquarters is on the 10.1.0.0/16 subnet, (b) Research and Development is on the 10.2.0.0/16 subnet, and (c) Manufacturing and Production is on the 10.3.0.0/16 subnet. Each of these three subnets operates in a switched environment to segment traffic, with Headquarters acting as a hub for connections to Internet hosts. A Network Address Translation (NAT) firewall and router device connects GIACE to the Internet, dynamically translating private IP addresses to public IP addresses and performing port translation in some cases, as the number of GIACE's assigned public IP addresses is smaller than the number of their internal hosts. To centralize management and monitoring of network traffic, connections from Research and Development hosts and Manufacturing and Production hosts to the Internet are routed through Headquarters. GIACE manages Domain Name Service (DNS) internally using Microsoft DNS, and its publicly registered Internet domain name is "giace.com".

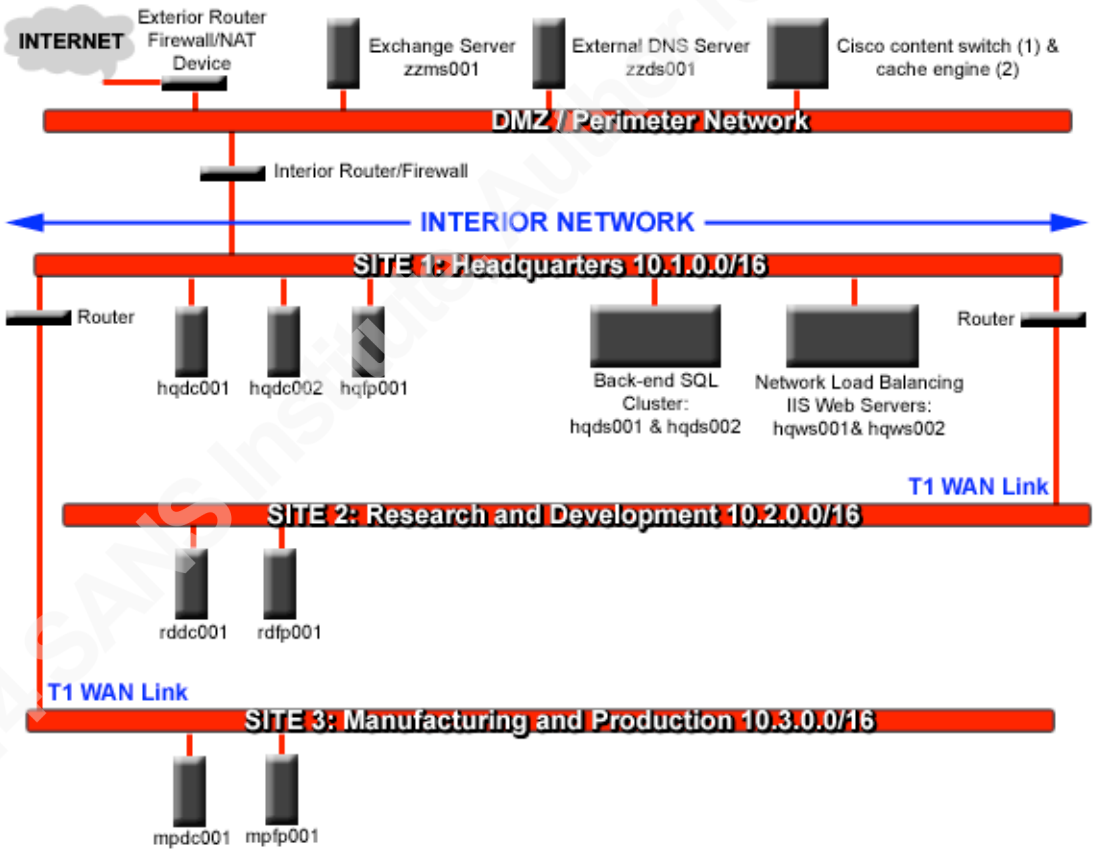
Additionally, the following factors are relevant to general security and to the performance of individual hosts on the network. However, they will not be included in the network diagram unless specified, nor will they be further discussed in the Active Directory or Group Policy sections, as they do not directly relate to the infrastructure changes that will result from implementing Windows 2000 and AD:

- All application servers, Domain Controllers (DCs), and networking equipment are physically secured at each site in locked, environmentally controlled rooms to prevent unauthorized access. It has become more important than ever to physically secure DCs because the process Windows 2000 uses to replicate data between DCs increases the amount of damage that could result from a single corrupted AD database.
- A disaster recovery policy was tested and implemented by the IT department over a year ago. Windows 2000 compatible Uninterruptible Power Supply (UPS) and tape backup systems are located on the network, and off-site storage locations have been secured.
- The IT department has a small, physically isolated test network that is used to: (a) create deployment strategies after testing and evaluating Microsoft service packs, Hotfixes, and patches and, and (b) test custom web applications.
- All client workstations on the network are running Windows 2000 Professional, and have the latest Microsoft service pack and Hotfixes installed.

- Unless specified, all application servers and DCs on the network are running Windows 2000 Server and have the latest Microsoft service pack and Hotfixes installed.
- Specific hardware, software, and Operating System (OS) configurations will not be discussed unless it directly affects the security or performance of Active Directory or Group Policy. The IT department has already researched these issues along with life-cycle management issues and processing and storage requirements, and has implemented the best cost-efficient solution for every application server, DC, and client workstation on GIACE's network.

GIACE's network is shown in Figure 1. The diagram is simplified to focus on AD design and placement of DCs, AD sites, and major servers; client workstations and segmented subnets have been omitted.

Figure 1. GIACE network diagram.



Sites

GIACE's internal network consists of three geographically separated office locations. A dedicated T1 Wide Area Network (WAN) link connects the main office to Research and Development and another dedicated T1 WAN link connects the main office to Manufacturing and Production. For the purpose of the

AD, a site is defined as a collection of IP subnets that have Local Area Network (LAN) speeds of at least 10 Megabits per second (Mbps). Therefore, by definition GIACE has three Windows 2000 AD sites.

Domain Controllers

Theoretically, the T1 WAN links that connect GIACE's offices are fast enough to support a properly functioning Windows 2000 network even if DCs were only located at Headquarters and the remote sites contained nothing but workstations. However, the IT department chose to place DCs at each site for three reasons: (a) to increase the performance of AD and AD queries at individual sites, (b) to keep the logon process and application of security and administrative policies local to each site rather than being processed over the WAN links, (c) to assure that internal services within each site are available even in the event of a WAN failure, and (d) to speed the performance of DNS queries. DNS is the only additional service running on each DC, which allows integration of DNS with the AD.

Because the AD is the focal point of the network infrastructure, DCs operate at hardware RAID level 1 to protect against single disk failure. To increase performance and to further protect data integrity, the operating system, AD log files, and the AD database and the System Volume directory are on separate RAID 1 arrays.

Mail Server

A single Exchange Server, "zzms001" is located in the DMZ. To minimize the possibility of a remote attacker gaining access to internal network resources, the server is on a separate domain. A one-way, "explicit trust", relationship between the Exchange server and GIACE's internal domain allows authenticated users to access their accounts on the server. The server is also dual-homed; one network card is handles requests on GIACE's internal network, and one network card delivers mail to and from the Internet. Finally, routing is disabled between the network interface cards.

File/Print Servers

Each site has a server dedicated to file and print services. Placing a dedicated server at each site has three benefits: (a) speeds access to files, (b) maximizes print throughput, and (c) assures that internal services within each site are available in the event of a WAN failure.

External DNS Server

A single DNS server, "zzdn001", is located in the DMZ to secure DNS services by separating internal and external DNS information. DNS servers on GIACE's

internal network are configured to directly forward unresolved queries from internal hosts concerning external hosts to this server.

Web Servers

Two Internet Information Services (IIS) servers, “hqws001” and “hqws002”, are located at Headquarters. Both servers are stand-alone (not domain members), and are using Network Load Balancing (NLB) to distribute processing of HyperText Transfer Protocol (HTTP) and HTTP over Secure Sockets Layer (HTTPS) requests. The Administration and IT departments realize that if the web servers were domain members server management could be simplified using Group Policy. However, both parties have agreed that the extra layer of administration is an acceptable trade-off for increased security, considering the percentage online sales contributes to total revenue.

Database Servers

Two Structured Query Language (SQL) back-end servers, “hqds001” and “hqds002”, are located at Headquarters and configured as a two-node cluster. The cluster is not a domain member, and its only function is to serve as a data store for GIACE’s web site.

Reverse Web Proxy

Reverse proxy services have been implemented for GIACE’s web servers to support both HTTP and HTTPS communication using a single Cisco CSS 11000 series content services switch and two Cisco Cache Engines. The switches and cache engines are located in the Demilitarized Zone (DMZ) to provide an extra layer of protection for the web servers. All HTTP and HTTPS connections from Internet hosts are routed to the DMZ CSS switch and processed by the cache engines. The exterior and interior routers are configured to block all connections to the web servers with the exception of the CSS switch on Transmission Control Protocol (TCP) ports 80 (HTTP) and 443 (HTTPS).

ACTIVE DIRECTORY DESIGN AND DIAGRAM

Assumptions

The IT department anticipated that the network would be upgraded to Windows 2000 before the CEO requested the upgrade proposal, and tested network software applications and hardware for Windows 2000 compatibility so the upgrade could be made gradually and performed without interrupting business operations. The NT4 DCs will either be upgraded or retired and replaced with new hardware, and each Windows 2000 DC will be introduced to the network with the "Permissions Compatible with Pre-Windows 2000 Servers" option disabled to block null user sessions. Lastly, the switch to native mode will not be made until there were no NT4 DCs left on the network. The descriptions of AD and Group Policy design that follow assume that the network is running in Windows 2000 native mode.

Overview

In simple terms AD is a directory service database that is installed on a Windows 2000 server when it is promoted to become a DC. The Lightweight Directory Access Protocol (LDAP) is used to update and maintain the AD database file, named "ntds.dit". The database itself is divided into three parts, each of which holds specific information:

- The Schema Naming Context (NC) holds information regarding the structure of the AD itself, including definitions of all class objects and object attribute types.
- The Configuration NC holds information regarding the physical structure of the network.
- The Domain NC holds information unique to each domain, such as user, group, and OU information.

Although the AD in effect replaces the Windows NT4 SAM database, it is very different for three reasons:

- Its theoretical maximum size is 70 terabytes (TB). Size limitations, like those imposed upon NT4 domains, are not a problem.
- It is more robust and extensible because it is an object-oriented database.
- It provides the foundation for security and management of the Windows 2000 network.

A central concept to the AD is "multi-master replication". Unlike Windows NT4, where the Primary Domain Controller (PDC) alone had write and modify permissions to the SAM database and the Backup Domain Controllers (BDCs) had read permissions, multi-master replication allows any DC in the domain to modify the AD database. In other words, any single DC in the domain can make

changes to the database, and those updates are automatically distributed to every DC in the domain. Multi-master replication also improves the efficiency of AD replication because changes to the AD are made on an object's property level; the entire objects itself is not copied during replication. Consequently, every DC in the domain must be accordingly physically secured. Assuming an attacker is able to gain access to a single DC in the domain, changes the attacker makes to the AD database on the compromised DC would automatically be copied on a domain-wide, and possibly, forest-wide scale (domains and forests are discussed below in the Domain section).

Domains

Windows NT4 and Windows 2000 domains differ in the following ways: "NT 4.0 domains were guided by their size limitations (40,000 users maximum), the difficulty of delegating administrative authority, and the security advantages of one-way trusts. Windows 2000 domains, on the other hand, can hold millions of users, can easily and securely delegate authority within domains, and all trusts are two-way and transitive by default" (Fossen "Active" 56). To elaborate, NT4 networks were distinguished by: (a) a large number of domains resulting from limitations of the SAM database, which was not scalable, and (b) complex management schemes resulting from the need to manually configure every domain where security and authority boundaries were needed. Windows 2000 networks, on the other hand allow: (a) a smaller number of large domains with millions of users, and (b) simple management of trust relationships and delegation of authority.

Two new entities have been introduced to Windows 2000 domain model, the "tree" and the "forest". Both entities share the following properties:

- They have a root node and they usually contain two or more Windows 2000 domains.
- Between domains the Schema Naming Context (NC), the Configuration NC, and the Global Catalog (GC) are replicated (Fossen "Active" 57).
- Domains are by default based upon a complete, two-way trust model.

The basic difference between the tree and forest lies in how DNS is configured. Domains contained within a tree share a hierarchical DNS naming structure. In other words, a single domain within the tree serves as the root DNS and all other domains are sub-domains. In contrast, a forest may contain domains that have many different DNS roots.

In Windows 2000, separate domains are usually created to control AD replication traffic. As previously discussed, the Windows 2000 multi-master replication scheme automatically distributes changes that are made to the AD database on one DC to every DC in a domain. However, multi-master replication may result in an unacceptable level of bandwidth utilization to on slow WAN links or may not

be needed for certain data in the AD which is seldom used. To alleviate these problems separate domains are created and certain DCs are explicitly configured to manage an extra portion of the AD in addition to their local domain data. This additional data is known as the Global Catalog (GC), which comprises about 55% of AD database on a GC server; about 45% of the AD is not replicated between domains (Fossen "Active" 53).

GIACE has carefully weighed these design issues and has decided that the single domain model is best suited to manage its assets. GIACE does not have replication or policy management issues that justify creating separate domains. A single domain implies a single tree, single forest structure, and that there is no immediate requirement for GC servers. Additional domains can easily be joined to the Windows 2000 root domain if the need arises in the future. More importantly, the single domain model has the following benefits, which correspond with GIACE's IT management style:

- It simplifies management. Multiple domains require that more DCs be placed on the network and that additional security, administrative, and access control policy objects be created.
- It simplifies corporate and departmental restructuring. Moving a user within a domain requires minimal changes, while moving a user between domains affects security settings and access controls.
- Any DC on the network can authenticate any GIACE employee, regardless of the user's physical location.

GIACE's Windows 2000 root domain is configured as a sub-domain of its publicly registered Internet domain and is named "corporate.giace.com". Although there is no requirement to follow DNS naming standards, it simplifies management of the network and the DNS service itself. Each host on the network will be named using a three string concatenated value:

- A two-letter code for the physical location of the host: (a) "hq" for Headquarters, (b) "rd" for Research and Development, (c) "mp" for Manufacturing and Production, and (d) "zz" for the DMZ.
- A two-letter code for the role of the host: (a) "dc" for DCs, (b) "fp" for file and print servers, (c) "ms" for mail servers, (d) "ws" for web servers, (e) "ds" for database servers, (f) "dn" for DNS servers, and (g) "cl" for client workstations.
- A three-digit or six-digit number starting at 1, which is incremented as each host is added to the network. DCs and servers use three-digit numbers, and client workstations use six-digit numbers.

To illustrate the naming scheme GIACE's root DC, the very first host on the network promoted to a Windows 2000 DC, is named "hqdc001", and the 20th client workstation at Research and development is named "rdcl00020".

To ensure that the AD database is properly updated and maintained between domains, Microsoft has defined five services that are specifically assigned to a DC within the domain or enterprise. The DC assigned to any of the Flexible Single Master Operation (FSMO) services is said to assume an FSMO role, since it alone is responsible for maintaining AD information for that service; multi-master replication is not used. By default the first DC in the first domain will assume all five FSMO roles, which is not efficient, nor will it properly maintain the AD database if there is more than one domain. A description of the FSMO roles and how they will be assigned follows:

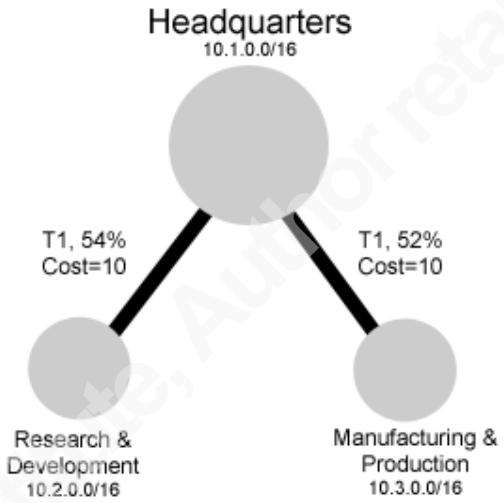
- The Schema Master is responsible for defining class objects and object attributes types in the AD database on the enterprise level. It will be assigned to the forest root DC, hqdc001.
- The Domain Naming Master is responsible for adding and removing domains from a forest on an enterprise-wide level. It will also be assigned to hqdc001.
- The PDC Emulator Master is responsible for maintaining backwards compatibility with NT4 DCs and clients for mixed-mode networks on a domain level. As GIACE's domain will run in Windows 2000 native mode, the PDC Emulator Master process is not needed and the default DC, hqdc001, will be accepted.
- The RID Master is responsible for distributing the unique part of a domain's Security Identifier (SID), known as the Relative Identifier (RID), to other DCs in the domain. This role will be moved to the second DC at headquarters, hqdc002, to reduce the load on hqdc001.
- The Infrastructure Master is responsible updating references to objects between domains. Although this process is idle because of GIACE's single domain model, the role will be moved to hqdc002 in case a second domain is added to the forest. The documentation for hqdc002 will include a note that it should not be configured as a GC server if domains are added to GIACE's forest, as DCs with both roles cannot detect bad references to objects on different domains.

Sites

By default, the Knowledge Consistency Checker (KCC) service automatically creates replication links between all DCs within a single site and manages scheduling of when AD replication over the links occurs. Microsoft recommends that the KCC service also be used to manage replication links for separate sites with the with link transitivity option (Microsoft "Best"). Microsoft also asserts that relying on the KCC service to manage replication will have a negligible effect on the Central Processing Unit (CPU) time and memory resources of the DC running the KCC service as long as (1 + number of domains) * (number of sites^2) <= 100,000 (Microsoft "Optimize"). However, "inter-site" links are not automatically created like intra-site links and must be manually created; the KCC service has no way of determining itself which sites are supposed to be connected, or what transport protocol should be used for replication (Lowe-Norris

152). Once the inter-site links are created, a DC from each site will use the KCC to automatically manage replication of the AD. As diagramed in Figure 2, GIACE's inter-site links use a simple hub topology. The Remote Procedure Call (RPC) over IP is used as the transport protocol, which is required for sites in the same domain. Each replication link is assigned an equal cost of 10, as both are high-speed, reliable, and have similar bandwidth utilization. Replication is scheduled every 30 minutes, and traffic is allowed all day with the exception of a one hour window from 8am to 9am. This one-hour period is when most of GIACE's users log in, which will reduce both network traffic and also the load on the DC responsible for replication.

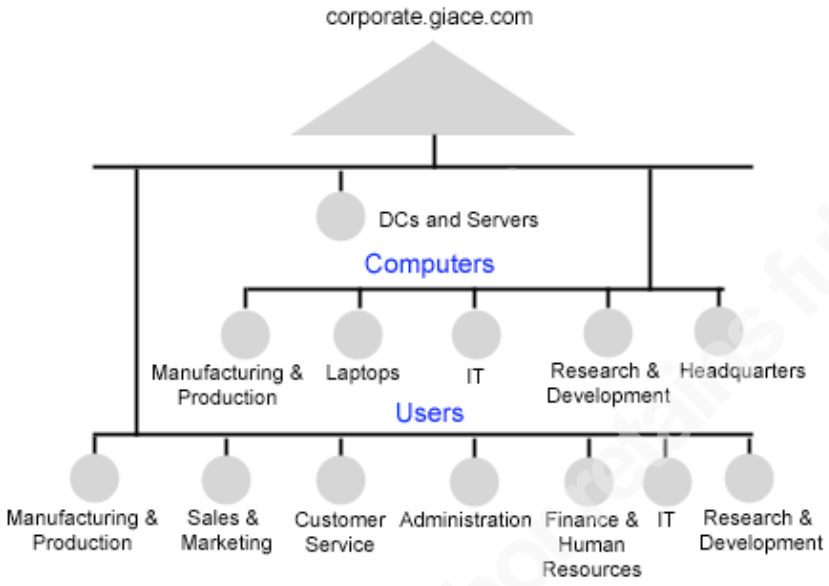
Figure 2. GIACE AD Inter-Site Replication Topology.



Organizational Units

An OU is a container of AD objects that has two basic functions: (a) delegation of administration, and (b) application of Group Policy setting. Because the IT department centrally manages GIACE's IT resources, OUs design will be structured to simplify assignment of Group Policy. One of the IT department's main goals was to keep the OU design as simple as possible. Therefore OUs are structured using a flat hierarchy, going one level deep. OUs are structured according to how IT resources are managed, not on GIACE's organizational hierarchy, and user and computer accounts are separated into different OUs. The user OUs are separated by department, as specific policy settings will be applied based on the applications used by each department. The computers OUs are more compact, and will apply broader policy settings. A benefit of separating OUs is this manner is that group policy processing time is reduced because the unused half of the GPO, either the user portion or the computer portion, can be disabled (Microsoft "Windows" 65). GIACE's OU structure is diagrammed in Figure 3.

Figure 3. GIACE OU design.



BASIC GROUP POLICY

Overview

Group Policy is the tool used to secure and configure a Windows 2000 network. Among other things, Group Policy allows administrators to control "registry-based policies, security, software installation, scripts, folder redirection, remote installation services, and Internet Explorer maintenance" (Microsoft "Windows" 1). Although Group Policy can apply a large number of settings to computer and user objects in Active Directory, the settings can only be applied to three types of AD containers: (a) domains, (b) sites, and (c) OUs.

A collection of Group Policy settings is known as a Group Policy Object (GPO). A GPO is an independent object within the AD structure, and must be manually linked to a domain, site, or OU before it has an affect on any of these containers. GPOs can be linked to multiple containers, and are processed first by computers as part of the boot process, and then by the user's logon process. They are managed with "Computer Configuration" and "User Configuration" in the Group Policy MMC snap-in. Each of these two containers has three sub-containers, "Software Settings", "Windows Settings", and "Administrative Templates", which are used to logically group individual Group Policy settings. By default, many settings in a GPO are not defined or not configured, and are ignored when the GPO is applied to a container. GPO policy settings implement inheritance and are processed in the following order (excluding NT4 System Policies, which are not significant since the network is in native mode):

- Local GPOs.
- Site GPOs.
- Domain GPOs
- OU GPOs.

In general, OU GPOs usually have highest precedence and nested OUs are processed from top down; the top-level parent container is processed first and the GPO that is applied last has highest priority. However, if a GPO is configured with the "No Override" option, lower level containers cannot override its policy settings under any circumstance.

GPOs also simplify management of many registry-based policy settings. Windows NT4 System Policies often had a persistent effect on the registry settings of individual system accounts (Microsoft "Windows" 21). For example, after implementing a NT4 System Policy, the changed registry settings could only be reversed by using a new System Policy or by manually editing the registry on the individual system's account. Maintaining standard registry settings on individual accounts was difficult.

Most Windows 2000 Group Policy settings that affect registry settings are not persistent, however. Registry-based policy settings are stored in administrative template files, which are rewritten whenever a GPO changes. Another benefit of the administrative template files is that by default they cannot be modified by a non-administrator account.

Default Domain Policy

GIACE will adhere to Microsoft's basic recommendations for GPO design (Microsoft "Best"):

- The two default GPOs, the "Default Domain Policy" and the "Default Domain Controllers Policy", should be applied as configured, with these exceptions:
    - Policy settings in the "Password Policy", "Account Lockout Policy", and "Kerberos Policy" nodes of the Default Domain Policy should be customized to meet individual security requirements.
    - Policy settings in the "User Rights Assignment" node of the Default Domain Controllers Policy should be customized to meet individual security requirements.
- Other policy settings should be applied by creating new GPOs.

The IT department also set these additional goals:

- Keep the number of GPOs to a minimum, since logon and boot times increase as each GPO is added to the AD; GPOs are processed by both user and computer accounts for every site, domain, and OU container they are linked to.
- Minimize the use of "Block Policy Inheritance" setting for OU level containers, and the "No Override" setting for domain level containers, since they make troubleshooting policy settings more difficult and create extra maintenance overhead.
- Following GIACE's OU design, certain GPOs will be configured to disable the "User Configuration" or "Computer Configuration" section to speed processing of the GPO.

To supplement Microsoft's two default GPOs, the "GIACE Computer" OU GPO and the "GIACE User" OU GPO were created. These two GPOs will be separately applied to every computer and user account on the network, and will provide the majority of policy settings that will be used to enforce the IT department's "least-privilege" approach to securing the network on an enterprise-wide level. This design speeds GPO processing and also allows Group Policy settings to follow roaming users wherever they are on the network. Additional GPOs will be created and linked to individual OUs to account for requirements of specific groups of users and computers. Group Policy settings that are not explicitly described in the subsequent documentation are assumed to provide an

appropriate level of protection at their defaults. GIACE's GPOs and the OUs that they are linked to are summarized in Table 1.

Table 1. GIACE GPOs.

OU	GPO Links
DCs & Servers	Default Domain, Default Domain Controllers, GIACE Computer, DCs and Servers
Headquarters (computer)	Default Domain, GIACE Computer
Laptops (computer)	Default Domain, GIACE Computer
IT (computer)	Default Domain, GIACE Computer
Research & Development (computer)	Default Domain, GIACE Computer
Manufacturing & Production (computer)	Default Domain, GIACE Computer
Administration (users)	Default Domain, GIACE User, Administration User
Sales & Marketing (users)	Default Domain, GIACE User, Sales & Marketing User
Finance & Human Resources (users)	Default Domain, GIACE User, Finance & Human Resources User
Customer Service (users)	Default Domain, GIACE User, Customer Service User
IT (users)	Default Domain, GIACE User, IT User
Research & Development (users)	Default Domain, GIACE User, Research & Development User
Manufacturing & Production (users)	Default Domain, GIACE User, Manufacturing & Production User

The following settings are in the "Computer Configuration" section of the GPO, and the "Disable User Configuration settings" option is set. The "GIACE User" GPO will be applied to every user on the network, which will provide additional security for individual user accounts.

\Windows Settings\Security Settings\Account Policies\Password Policy

- "Enforce password history" is set to 14 passwords remembered. Combined with the "Minimum Password Age" setting, it would take a user a minimum of two weeks to recycle a password.
- "Maximum password age" is set to 90 days to provide security, but not overburden users by having them set their passwords too often.
- "Minimum password age" is set to 1 day.
- "Minimum password length" is set to 8 characters. The IT department felt this was a better alternative than to have users writing their passwords on post-it sheets.

- “Passwords must meet complexity requirements” is enabled and mandatory for basic security.

\Windows Settings\Security Settings\Account Policies\Account Lockout Policy
- “Account lockout duration” is set to 20 minutes.
- “Account lockout threshold” is set to 5 attempts.
- “Reset account lockout counter after” is set to 15 minutes.

These settings balance allowing users to make mistakes and protecting against brute force password attacks, while also protecting against a DOS attack with the intent of locking out legitimate users.

Default Domain Controller Policy

The following settings are in the “Computer Configuration” section of the GPO, and the “Disable User Configuration settings” option is set. The “GIACE Computer” and “DCs and Servers” GPOs are also linked to every DC in the domain, and will provide the remaining policy settings required to lock down each DC. The “No Override” option will be set on this object to block conflicting policy settings.

\Windows Settings\Security Settings\Local Policies\User Rights Assignment
- “Access this computer from network” is assigned to “Administrators”, “Authenticated Users”, and “ENTERPRISE DOMAIN CONTROLLERS” to allow group members to connect to any DC over the network.
- “Add workstations to domain” has the default “Authenticated Users” group removed, since the administrators group is allowed to add computer accounts to the domain.
- “Bypass traverse checking” is assigned to “Administrators” to ensure that only authorized users can browse the file system.
- “Log on locally” is assigned to “Administrators” to restrict logon at the DC’s console to administrator group members.
- “Shut down the system” is assigned to “Administrators” to allow locally logged on group members to shut down the DC.

GIACE Computer Group Policy Object

This GPO will be applied to every computer account on the domain to enforce enterprise-wide security standards. The following settings are in the “Computer Configuration” section of the GPO, and the “Disable User Configuration settings” option is set.

\Windows Settings\Security Settings\Local Policies\User Rights Assignment
- “Access this computer from network” is assigned to “Administrators”, to allow group members to connect to any host over the network.
- “Back up files and directories” is assigned to “administrators” and “backup” allow group members to back up files and directories.

- “Change the system time” is assigned to “administrators” to allow group members to set the internal clock. System time affects AD replication and Kerberos preauthentication.
- “Create a pagefile” is assigned to “administrators” to allow group members to create a new pagefile or change the size of an existing pagefile.
- “Force shutdown from a remote system” is assigned to “Administrators” to allow group members to shutdown a host remotely over the network.
- “Increase quotas” is assigned to “Administrators” to allow group members to increase a process’ processor quota.
- “Increase scheduling priority” is assigned to “Administrators” to allow group members to elevate a process’ system priority.
- “Load and unload device drivers” is assigned to “Administrators” to allow group members to install and uninstall device drivers.
- “Log on locally” is assigned to “Administrators” and “Users” to allow group members to logon at the system’s console.
- “Manage auditing and security log” is assigned to “Administrators” to allow group members to view and clear the security log and to specify what types of object access are audited.
- “Profile system performance” is assigned to “Administrators” to allow group members to sample the DC’s performance.
- “Take ownership of files or other objects” is assigned to “Administrators” to allow group members to take ownership any object.

\Windows Settings\Security Settings\Local Policies\Security Options

- “Additional restrictions for anonymous connections” is set to “No access without explicit anonymous permissions” since the network will run in Windows 2000 native mode. Attempts by anonymous Internet users to download a list of domain usernames will be blocked.
- “Amount of idle time required before disconnecting session” is set to “20 minutes” to close Server Message Block (SMB) sessions after 20 minutes.
- “Automatically log off users when logon time expires (local)” is enabled to enforce logon hours for client SMB sessions.
- “Clear virtual memory pagefile when system shuts down” is enabled to clear the system pagefile on shutdown so that attackers cannot access system information.
- “Digitally sign client communication (always)” is enabled. All clients and servers on the network support Windows 2000 SMB packet signing.
- “Digitally sign server communication (always)” is also enabled to protect SMB sessions by forcing mutual authentication by both client and server.
- “Disable CTRL+ALT+DEL requirement for logon” is disabled to assure that the correct logon process is executed.
- “Do not display last user name in logon screen” is enabled to prevent attackers from accessing usernames.

- “LAN Manager authentication level” is set to “Send NTLMv2 response only\refuse LM and NTLM” to provide the highest level of security for network logons, since only Windows 2000 hosts exist on the network.
- “Message text for users attempting to log” will be enabled with a warning message that emphasizes the following: (a) the system is private, (b) all network communication will be subject to monitoring, (c) failure to follow IT policies that have been read and signed by all users will lead to disciplinary action, and possible legal consequences.
- “Number of previous logons to cache” is set to “0 logons” so that user logon credentials are not persistent.
- “Prompt user to change password before expiration” will be set to “21 days” to reduce the number of users that are locked out because of passwords expiration.
- “Rename administrator account” is set to a 15 character string for two purposes: (a) to make it harder for an attacker to target the default administrator account, and (b) to eliminate the possibility of error events caused by the renamed account being the same as a regular username; usernames for regular user accounts are eight character strings. The “Rename guest Account” will be set in the same manner for the same reasons.
- “Restrict CD-ROM access to locally logged on user only” is enabled so that only users who have successfully authenticated to the domain can access the CD-ROM drive, which minimizes the possibility that executables or other malicious files can be introduced into the network by unknown users. “Restrict floppy access to locally logged on user only” will also be enabled for the same reason.
- “Secure channel: Digitally Encrypt secure channel data (always)” is enabled to secure replication of AD data between DCs over the RPC channel, since all DCs on the network support Windows 2000 digital encryption and signing.
- “Secure channel: Require strong session key” is enabled to secure replication of AD data between DCs over the RPC channel.
- “Strengthen default permissions of global system objects (e.g. Symbolic links)” is enabled to restrict permissions on the default discretionary access control list (DACL) of shared objects; users that are not in the administrators group have read permissions for shared objects, but they do not have modify permissions for shared objects they did not create.
- "Unsigned driver installation behavior" and "Unsigned non-driver installation behavior" will both be set to “Warn but allow installation” to alert users that the driver software they are attempting to install has not been certified by Microsoft.

\Administrative Templates\System

- “Disable Autoplay” is set to “All drives” to block access to executables when the account also does not have access to the command prompt. This setting also overrides the same setting at the User Configuration level.

\Administrative Templates\System\Logon
- "Maximum wait time for Group Policy scripts" is changed from the default value of 600 to 180. GIACE's Group Policy scripts are short and simple. The default value is too long for users to wait if a script is unavailable.

\Administrative Templates\System\Group Policy
- "Disable background refresh of Group Policy" is enabled to prevent Group Policy from being updated while the computer is in use, which reduces network traffic. By default Group Policy is updated every 90 minutes plus or minus a random interval from 0 to 30 minutes. If a Group Policy needs to be updated immediately, "secedit.exe", the SECEDIT utility, will be executed with the "/refreshpolicy" switch.

GIACE User Group Policy Object

This GPO will be applied to every user account on the domain to enforce enterprise-wide security standards. The following settings are in the "User Configuration" section of the GPO, and the "Disable Computer Configuration settings" option is set.

Windows Settings\Internet Explorer Maintenance\Security
- "Security Zones" will be modified to set a default level of security for Internet Explorer, and "Content Rating" will be modified to help control the type of content users can view.

Windows Settings\Internet Explorer Maintenance\Programs
- The program settings will be modified to ensure that the program Windows uses for E-mail, Newsgroups, Calendar, and Contacts list is standard for all users on the domain.

Windows Settings\Scripts (Logon/Logoff)
- A simple set of scripts will be used to map network drives based on each user's department, office location, and group membership for special projects and teams.

Windows Settings\Folder Redirection\ My Documents
- The %username% environment variable is used to map each user's "My Documents" folder to the appropriate site file server, which will simplify backup and disk quota management and will allow roaming users to access their personal files from anywhere on the network.

\Administrative Templates\Windows Components\Windows Explorer
- "Only allow approved Shell extensions" is enabled to protect the system from programs that do not have approved user interface extensions with the correct digital certificate.

- "Do not track Shell shortcuts during roaming" is enabled to confine searches to the system's current target path when a shortcut cannot find its target file.

\Administrative Templates\Windows Components\Microsoft Management Console
- "Restrict the user from entering author mode" is enabled to prevent users from creating custom MMC console files or adding or removing snap-ins.
- "Restrict users to the explicitly permitted list of snap-ins" is enabled to deny users access to any of the MMC snap-ins. All snap-in policies in the "Restricted/Permitted snap-ins" folder are disabled or not configured.

\Administrative Templates\Windows Components\Windows Updates
- "Remove access to use all Windows Update features" is enabled. The IT department tests Microsoft Service Packs and Hotfixes before they are deployed with Group Policy.

\Administrative Templates\Start Menu and Taskbar
- "Disable and remove links to Windows Update" is enabled.
- "Remove Documents menu from Start Menu", "Do not keep history of recently opened documents", and "Clear history of recently opened documents on exit" are enabled to control access to recently used files of individual users.

These settings reduce the amount of options available on the Start Menu and Taskbar, which restricts and simplifies the user interface.

\Administrative Templates\Desktop
- "Hide My Network Places icon on desktop" is enabled to minimize casual browsing of shared computers on the network.
- "Prohibit user from changing My Documents path" is enabled to support mapping of the directory to the appropriate file server based on username.

\Administrative Templates\Desktop\Active Desktop
- "Disable Active Desktop" is enabled to prevent users from enabling Active Desktop.

\Administrative Templates\Desktop\Active Directory
- "Hide Active Directory folder" is enabled to let users search AD while preventing casual browsing of the AD using "My Network Places".

\Administrative Templates\Control Panel\Add/Remove Programs
- "Disable Add/Remove Programs" is enabled to prevent users from installing, uninstalling, repairing, adding, or removing of Windows 2000 components and programs.

\Administrative Templates\Network\Network and Dial-up Connections
- "Prohibit deletion of RAS connections available to all users" is enabled.
- "Prohibit connecting and disconnecting a RAS connection" is enabled.

- “Prohibit enabling/disabling a LAN connection” is enabled.
- “Prohibit access to properties of components of a RAS connection available to all users” is enabled.
- “Prohibit access to the properties of components of a RAS connection” is enabled.
- “Prohibit access to the Network Connection wizard” is enabled.
- “Prohibit viewing of status for an active connection” is enabled.
- “Prohibit access to the Dial-up Preferences item on the Advanced menu” is enabled.
- “Prohibit TCP/IP advanced configuration” is enabled.

Taken together, these settings provide maximum protection against a user creating, deleting, or modifying network settings or connections that could be used as a back door to the network.

\Administrative Templates\System

- “Prevent access to registry editing tools” is enabled to prevent users from running “regedt32.exe” and “regedit.exe”.

\Administrative Templates\SystemLogon/Logoff

- “Disable Task Manager” is enabled to prevent users from running “Taskmgr.exe”. The average user should not be able to start and stop programs or change the priority of processes.

ADDITIONAL GROUP POLICY

DCs and Servers OU Group Policy Object

These policies were purposely separated from the “GIACE Computer” GPO and confined to DCs and domain servers (only file and print servers belong to the corporate.giace.com domain) because of the processor usage and disk space required by system auditing; client systems will not have auditing enabled by default. The IT department realizes how crucial auditing is to maintain domain security, and feels it is more important to thoroughly monitor DCs and domain servers on a daily basis; monitoring all of the clients on the network may overburden the administrators responsible for auditing, and may result in subtle privilege abuse going unnoticed. This scheme also gives IT the added flexibility of being able to monitor the logs manually on a regular basis instead of only relying on script processing of log files. The following settings are in the “Computer Configuration” section of the GPO, and the “Disable User Configuration settings” option is set.

\Windows Settings\Security Settings\Local Policies\Audit Policy

- “Audit account logon events” is set both “success” and “failure” This setting logs all authentication requests originating from other hosts on the network.
- “Audit account management” is set to both “success” and “failure”. This setting logs user, computer, or group accounts that are changed, created, or deleted.
- “Audit directory service access” is set to “failure”. This setting logs all failed attempts to access an AD object that has been configured with an access control list. Since this option only applies to Active Directory, it has no meaning on workstations and member servers.
- “Audit logon events” is set to both “success” and “failure”. This setting logs all attempts to logon or make a network connection, along with the type of logon requested.
- “Audit object access” is set to “failure”. This setting logs all failed attempts to access objects that have been configured to enable auditing.
- “Audit policy change” is set to both “success” and “failure”. This setting logs any changes made to security, permissions, or audit policies.
- “Audit privilege use” is set to “failure”. This setting logs all failed attempts to apply a permission that has not been explicitly granted.
- “Audit system events” is set to both “success” and “failure”. This setting logs any event that affects the OS.

These settings monitor user and group accounts, host and network logon, and file and object access and usage on the DCs and domain file and print servers, and allow detection of subtle exploitation attempts.

\Windows Settings\Security Settings\Local Policies\Security Options

- “Audit the access of global system objects” is enabled, which sets a default access control list and enables auditing of system objects.

- “Audit use of Backup and Restore privilege” is enabled to enable auditing of the “backup” and “restore” privileges.

Manufacturing and Production OU Group Policy Object

The Manufacturing and Production Department requires a limited number of applications to complete its mission and will therefore have the most restricted user configuration on the domain. The following settings are in the “User Configuration” section of the GPO, and the “Disable Computer Configuration settings” option is set.

\Administrative Templates\Windows Components\Task Scheduler

- All policies in the container are enabled. This prevents users from deleting or modifying scheduled tasks, and from creating personal scheduled tasks.

\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel

- “Disable the General page”, “Disable the Security page”, “Disable the Content page”, “Disable the Connections page”, “Disable the Programs page”, and “Disable the Advanced page” are enabled to prevent users from viewing or changing the majority of Internet Explorer’s security settings.

\Administrative Templates\Windows Components\Windows Explorer

- “Remove the Folder Options menu item from the Tools menu” is enabled to prevent users from setting properties such hidden system files and file types.
- “Remove File menu from Windows Explorer” is enabled.
- “Remove "Map Network Drive" and "Disconnect Network Drive"” is enabled to prevent users from using Windows Explorer or My Network Places to map or disconnect network drives.
- “Remove Search button from Windows Explorer” is enabled to prevent casual searching of network computers.
- “Disable Windows Explorer's default context menu” is enabled to remove the shortcut menus that appear when a user right-click the Desktop or Windows Explorer.
- “Hides the Manage item on the Windows Explorer context menu” is enabled to remove “Manage” from the Windows Explorer context menu, which can open the “Computer Management” console tool.
- “Hide these specified drives in My Computer” is enabled to hide local computer drives.
- “Prevent access to drives from My Computer” is enabled to restrict access to local computer drives. Network drives should be used for storing personal files.
- “No "Entire Network" in My Network Places” is enabled to prevent casual browsing of network resources in Windows Explorer and My Network Places.

\Administrative Templates\Start Menu and Taskbar

- "Remove common programs groups from the Start Menu" is enabled.
- "Disable programs on Settings menu" is enabled.
- "Remove Network & Dial-up Connections from Start Menu" is enabled
- "Remove Run menu from Start Menu" is enabled.

These settings reduce the amount of options available on the Start Menu and Taskbar, which restricts and simplifies the user interface.

\Administrative Templates\Control Panel

- "Disable Control Panel" is enabled to prevent users from running "Control.exe" to modify any system setting controlled by the Control Panel.

\Administrative Templates\Control Panel\Printers

- "Browse the network to find printers" is disabled to prevent users from users browsing the network for printers with "Add a network printer".

\Administrative Templates\System

- "Prevent access to the command prompt" is enabled to prevent users from running "cmd.exe", but "Disable the command script processing also?" will be set to "no" to allow processing of logon/logoff and startup/shutdown batch files.

Service Pack and Hotfix Group Policy Object

Keeping the OS of individual systems up to date and patched is a major step toward successfully securing the network. Microsoft Service Packs and Hotfixes will therefore be deployed with Group Policy. Although there are actually three of these GPOs, one for each of GIACE's AD sites, they will be described as a single component because their Group Policy settings are exactly the same except for the Windows Installer package (MSI file) location; the MSI file will be available on a network server at each site to distribute server load and to eliminate bandwidth usage across the WAN links. The following setting is in the "Computer Configuration" section of the GPO, and the "Disable User Configuration settings" option is set.

\Software Settings

- "Software Installation" will be configured and deployed as follows, with the assumption that the required MSI file exists on a network server:
    - Link the GPO to one of the "department_name Computer" OUs, where "department_name" is represented by the name of GIACE's seven departments. These OUs contain all computers accounts in their respective department, and are not normally linked to any GPO. They exist specifically for installation of the Service Pack or Hotfix.
    - Select "New Package" and enter the full (UNC) path to the MSI file at the appropriate site's network file server.
    - Select the "Assigned" option to deploy the Service Packs or Hotfix without modification.

- Run the SECEDIT utility with the “/refreshpolicy” switch to force immediate execution of the GPO.
- Unlinked the GPO from the department OU after installation has completed.
- Repeat the process until the Service Packs or Hotfix has been applied to every department.

ADDITIONAL SECURITY

Schema Security

The Schema defines the structure and data-types of the objects and properties in AD. Any changes that are made to the Schema are irreversible and will be replicated forest-wide to all DCs in the domain, which could, in a worst-case scenario, leave DCs inoperable. Therefore, as recommended by the SANS Institute (Fossen "Active" 46):

- The FSMO Schema Master will be configured to disable modification of the schema.
- The Schema Admins group will be kept empty to ensure that no accidental changes are made to the schema. If a change to the schema is needed, one of four senior system administrators will be temporarily added to the Schema Admins group. After the change has been finalized, the group will once again be emptied.
- All changes to the Schema Admins group will be audited.
- All failed access to the Schema naming context will be audited.

Domain Name Service

Windows 2000 networks replace the Windows Internet Naming Service (WINS) with DNS to map hostnames to IP addresses. Given that clients rely upon DNS to access network resources, DNS will be appropriately configured and secured:

- The internal DNS servers will be AD enabled, which will provide improved fault tolerance for DNS. They will answer all queries from hosts on GIACE's internal network.
- The internal DNS Servers will forward all unresolved queries for Internet hosts to the external DNS server, zzds001. The internal firewall will block all DNS traffic that does involve a direct connection between the internal DNS servers and the external DNS server.
- The external DNS server will respond to queries forwarded by GIACE's internal DNS servers and forward queries it cannot answer itself to the appropriate authoritative zone server. However, the external DNS server will not contain DNS records for internal hosts and therefore will not be able to provide information about internal hosts to Internet hosts. The only DNS records it holds are those for the e-mail server and the content switch providing reverse proxy web services. Lastly, the external DNS server will not be AD enabled.
- Zone transfers and NSLOOKUP listings will be disabled on DNS servers.
- DNS logging will be enabled. Only the "administrators" group account and the "system" account will have access to the log files, which will be monitored daily.

- The "Secure Cache Against Pollution" option will be enabled to minimize the effects of DNS cache poisoning; only records for requested domains are added to the DNS server's cache, while all unsolicited replies are ignored.

As GIACE statically assigns IP addresses and hostnames on its network, the "SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" registry key in the "HKEY_LOCAL_MACHINE" hive of DNS servers will set the value of "DisableDynamicUpdate" to "1", disabling dynamic client updates on the servers. Under normal circumstances, disabling dynamic updates would require manual configuration of host records. However, the IT department prefers to manage and secure DNS directly, and already has an existing set of scripts that update DNS records.

Internet Information Services

Because online sales account for approximately 80% of revenue, the stability and security of the IIS servers is vital to GIACE's continued success. Consequently, the Web Administrators and Web Developers are on a 24 hour schedule so immediate response to any problems is always available. The team also has a developmental server that is used to test new applications and to verify that Service Packs and Hotfixes do not affect current applications. The developmental server is located on GIACE's test network, and its hardware and software configurations are identical to the production servers.

The following will be used as a baseline configuration to harden GIACE's web servers:

- Servers will use Hardware Redundant Array of Inexpensive Disks (RAID) Level 5. The IT department has determined that RAID 5 provides the best balance between cost, fault tolerance, and speed.
- Windows 2000 Advanced Server will be the installed OS, because of its support for load-balancing. The Windows Load-Balancing Service (WLBS) will be installed to provide faster response times to customers, to improve protection against Distributed Denial of Service (DDoS) attacks, and to allow the SAs to take individual servers offline during repairs and upgrades and reboots required by Service Packs and Hotfixes.
- Three Internet Information Services components will be installed: (a) Common Files, (b) Internet Information Services Snap-In, and (c) World Wide Web Server. No other Microsoft or third-party software will be installed.
- The "hisecweb.inf" file will be downloaded from Microsoft and will be used as the baseline security template.
- These unused services will be disabled:
    - Alerter
    - ClipBook Server
    - Computer Browser
    - DHCP Client

  - Distributed File System
  - Distributed Link Tracking Client
  - Distributed Link Tracking Server
  - Fax Service
  - File Replication
  - FTP Publishing Service
  - Indexing Service
  - Internet Connection Sharing
  - Messenger
  - NetLogon
  - NetMeeting Remote Desktop Sharing
  - Network DDE
  - Network DDE DSDM
  - Network Monitor Agent
  - NNTP Service
  - Print Spooler
  - QoS RSVP
  - Remote Access Auto Connection Manager
  - Remote Access Connection Manager
  - Remote Registry Service
  - Removable Storage
  - RunAs Service
  - Smart Card
  - Smart Card Helper
  - Task Scheduler
  - TCP/IP NetBios Helper Service
  - Telephony
  - Telnet
  - Terminal Services
  - Windows Management Instrumentation
  - Windows Management Instrumentation Driver Extensions
  - Windows Time
- The Indexing Service will be disabled at the root of all volumes for each physical drive and pushed to all subdirectories to minimize the possibility of a remote attacker enumerating any files on the file system.
- The default website will be moved from the physical drive that contains the OS to a separate physical drive to minimize possibility of a remote attacker accessing files related to the OS.
- The following executables will be renamed and moved to a directory that is not located within the path environmental variable: (a) “cmd.exe”, (b) “command.com”, (c) “cscript.exe”, (d) “ftp.exe”, (e) “net.exe”, (f) “net1.exe”, (g) “tftp.exe”, and (h) “wscript.exe”.
- To eliminate known vulnerabilities associated with IIS’ default installation:
  - The virtual directories pointing to the IIS admin, sample, help, and scripts files will be removed and the physical directories, subdirectories,

and files themselves will be deleted as will the physical “ftproot” directory.
    - Remote Data Service (RDS) support will be disabled. The virtual directory pointing to the MSADC will be removed and the physical directories, subdirectories, and files themselves will be deleted.
    - Internet printing support will be disabled. The “printer” Internet Server Application Program Interface (ISAPI) extension will be unmapped. The virtual directory pointing to the printer files will be removed and the physical directories, subdirectories, and files themselves will be deleted.
- The directory browsing IIS permission will be disabled, which will block access to directory listings. Likewise, script source access will be disabled to block reading of scripts.
- The following local groups will be used to set Access Control Lists (ACLs) on system objects: (a) system, which is required by IIS, (b) administrators, who manage the server, (c) web developers, who consist of application programmers and technical designers and (d) everyone, which allows public access to the server.
- The following top-level physical directory structure will be created to simplify management of ACLs: (a) “toor” will hold static HTML files, (b) “scr” will hold ASP scripts, (c) “ex” will hold executables, and (d) “image” will hold graphic files.
- ACLs will be assigned to each top-level physical directory, with inheritance used to push permissions to child objects. General guidelines for the local group accounts are: (a) system and administrator will have “full control” permissions over all files, (b) web developers will have “full control” permissions over static files and “read and execute” permissions over ISAPI and dynamic link library (dll) executables, and (c) everyone will have “read” permissions for all files with the exception of “read and execute” permissions for ISAPI and dll executables.
- URLScan 2.5 will be installed with a custom configuration to restrict the types of HTTP requests that the server will process and to limit the size of separate parts of those requests.
- An Internet Protocol Security (IPSec) packet-filtering policy will be implemented that only permits access from the Cisco CSS switch on TCP ports 80 and 443, which provides a redundant level of security on top of GIACE’s filtering firewalls.
- Logging will be enabled using the W3C extended logging format. The administrator and system local groups will have “full control” permissions to log files. Auditing will be enabled for failed write, delete, change permissions, and take ownership attempts.

Properly hardening the web servers is big step in providing overall security, but not the total solution. Even if the web server’s OS was 100 percent locked-down, it would still be vulnerable to remote attacks on its web applications. Access to unused ISAPI filters and extensions or sloppy code could allow a remote attacker

to gain full control of the web server. Therefore, the following guidelines will be followed to secure web applications:

- Web applications will be configured to use the “dllhost.exe” memory space application protection setting to provide separation from the main IIS "inetinfo.exe" process, which minimizes the possibility of buffer overflow Denial of Service (DoS) attacks.
- Unused ISAPI extensions will be unmapped: (a) “htr” (Remote password change scripts), (b) “ida” (Index Server performance monitoring), and (c) “idq” (Index Server Query Definition).
- ".htm", ".html", and ".asp" ISAPI extensions will be limited to the HTTP "GET" and “POST” verbs.
- The “fpexedll.dll” (FrontPage), “md5filt.dll” (Digest authentication), and “compfilt.dll” (HTTP compression) ISAPI Filters will not be used and therefore will be removed.
- “scrrun.dll” will be deregistered using “regsvr32.exe”, since neither Site Server nor File System Objects within Active Server Pages (ASP) will be used.
- Secure Sockets Layer (SSL) will be implemented for applications that use basic authentication.
- “global.asa” files will be audited for failed access and successful change. In addition, data link “.udl” files will be used to build and store connection strings that use ActiveX Data Objects (ADO) for database access, since they can be secured and audited using NTFS file permissions.
- Parent path syntax support for ASP and Server-Side Includes (SSI) will be disabled so that remote attackers will be prevented from using relative paths on the file system.
- Application programmers will only use ASP for scripts. “.inc” files will not be used; this will minimize the possibility of a remote user gaining read access to source code.
- Application programmers will implement boundary checking for all functions.
- Application programmers will implement server-side validation and “laundering” of user data for all applications. Data laundering will include, but not be limited to: (a) form fields, including “hidden” fields, (b) query strings and path information, (c) cookies, and (d) requested host information.

References

Bartock, Paul F. Jr., Donahue, Paul L., Duesterhaus, Daniel J., Haney, Julie M., Hayes, Prentice S., Pitsenbarger, Trent H., Stephens, Robin G., & Ziring, Neil L. (2001, April 19). "Microsoft Windows 2000 Network Architecture Guide." [Online]. National Security Agency. Available: http://www.nsa.gov/snac/win2k/guides/w2k-1.pdf

Fossen, Jason. (2001). "Active Directory, DNS and Group Policy." Version 5.1.3. SANS Institute.

Fossen, Jason. (2001). "Securing Internet Information Server." Version: 11.0. SANS Institute.

Fossen, Jason. (2001). "Windows 2000/XP IPSec, RRAS and Virtual Private Networking." Version 4.0. SANS Institute.

Hall, Monty. (2000). "Securing your Exchange Server Installation." [Online]. SecurityFocus. Available: http://online.securityfocus.com/infocus/1305

Haney, Julie M. (2001, September 13). "Securing Microsoft Windows 2000 Group Policy." [Online]. National Security Agency. Available: http://www.nsa.gov/snac/win2k/guides/w2k-2.pdf

Haney, Julie M. (2002, July 22). "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set." [Online]. National Security Agency. Available: http://www.nsa.gov/snac/win2k/guides/w2k-3.pdf

Howard, Michael. (2000, June 29). "Secure Internet Information Services 5 Checklist." [Online]. Microsoft TechNet. Available: http://www.microsoft.com/technet/security/tools/chklist/iis5chk.asp

Lowe-Norris, Alistair G. (2000) Windows 2000 Active Directory. Sebastopol, CA: Reilly & Associates.

Microsoft Corporation. (1999, November 22). "How to Enable/Disable Windows 2000 Dynamic DNS Registrations." [Online]. Microsoft Knowledge Base Article - Q246804. Available: http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q246804&

Microsoft Corporation. (1999, October 21). "How to Optimize Active Directory Replication in a Large Network." [Online]. Microsoft Knowledge Base Article - Q244368. Available: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q244368

Microsoft Corporation. (2000, July 31). “Windows 2000 Group Policy.” [Online]. White Paper. Available: http://www.microsoft.com/windows2000/docs/grouppolwp.doc

Microsoft Corporation. (2001). “Best Practice Active Directory Design for Managing Windows Networks.” [Online]. Microsoft TechNet. Available: http://www.microsoft.com/technet/prodtechnol/ad/windows2000/plan/bpaddsgn.asp

Microsoft Corporation. (2001). “IIS 5.0 Baseline Security Checklist.” [Online]. Microsoft TechNet. Available: http://www.microsoft.com/technet/security/tools/chklist/iis5cl.asp

Microsoft Corporation. (2001). “Group Policy Registry Table.” [Online]. Windows 2000 Resource Kits. Available: http://www.microsoft.com/windows2000/techinfo/reskit/en-us/gp/gpref.asp

Microsoft Corporation. (2002). “HOW TO: Assign Software to a Specific Group By Using a Group Policy.” [Online]. Microsoft Knowledge Base Article – 302430. Available: http://support.microsoft.com/default.aspx?scid=KB;en-us;302430&

Rice, David C. (2001, March 2). “Group Policy Reference.” [Online]. National Security Agency. Available: http://www.nsa.gov/snac/win2k/guides/w2k-4.pdf

Sanderson, Mark J. & Rice, David C. (2000, December). “Guide to Securing Microsoft Windows 2000 Active Directory.” [Online]. National Security Agency. Available: http://www.nsa.gov/snac/win2k/guides/w2k-5.pdf

Stephens, Robin G. (2001, April 9). “Guide to Securing Microsoft Windows 2000 DNS.” [Online]. National Security Agency. Available: http://www.nsa.gov/snac/win2k/guides/w2k-6.pdf

Walker, William E. (2002, March 4). “Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0.” [Online]. National Security Agency. Available: http://www.nsa.gov/snac/win2k/guides/w2k-14.pdf

Last Updated: October 17th, 2017

Upcoming Training

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