Global Information Assurance Certification Paper

Design, Secure and Audit the Combined SANS Co & GIACE Windows 2000 Network

GIAC Certified Windows Security Administrator (GCWN)
Practical Assignment Version 3.2 Option 1

Name: Jay Garden
Course: GCWN
Version: 3.2, Option 1
Date: July 2003

Introduction

This paper is submitted as the practical assignment requirement for the SANS GIAC Certified Windows Administrator (GCWN) program. It is formed around two fictitious companies, SANS Co and GIAC Enterprises (GIACE). The paper is made up of three parts. Part 1 describes the two organizations and networks, and proposes an architecture to merge the two Windows 2000 networks. The proposal is designed to enable business processes between the two organizations and to their customers while retaining a suitable level of network security to the entities within the merged system. Part 2 suggests a suitable Group Policy design for the overall system described above, implements that Group Policy design on a test network modeling part of the SANS Co forest, and assesses the resultant configuration on one of the intranet web servers. Part 3 discusses a method to audit the overall SANS Co/GIACE system including gathering and management of audit logs and performance data and checking of critical settings.

PART 1 - DOMAIN DESIGN

1.1 Overview of the SANS Co Network

SANS Co is an adventure sports group of companies. It operates under the trade names:
- *Xtreme.com*, an adventure sports marketing company;
- *Pipeline*, a surf clothing manufacturer and retailer; and
- *Go!*, a ski and snowboard equipment retailer and distributor.

Xtreme.com was the first to join the SANS Co consortium. They operated a series of websites in support of adventure sports in Australia. Income was primarily produced from web advertising and web referrals. The management team realized that several of the companies and sectors they were marketing could benefit by an integrated approach to their sales and marketing and could tap into the international market by an increased use of communications and sales via the Internet. They then began to push on their two primary strengths, marketing and web development. The *Xtreme.com* team consists of 60 executive, marketing, finance and IT staff based in Brisbane, Australia.

Xtreme.com's parent company, SANS Co, merged with *Pipeline* in 1999. *Pipeline* had been producing beachwear and wetsuits for the Australian market for ten years, primarily operating through a series of beachfront stores in the Queensland region. The *Xtreme.com* partnership expanded the distribution into the wider Australasian market. *Pipeline* has 50 staff in the Brisbane manufacturing division, with another 30 providing the design, management and support functions. Following the merger with *Xtreme.com* an extensive web presence was created for the distribution network and end customers.

Go! has been providing snowboard and ski equipment to the New Zealand public and

sporting goods shops for over twenty years. For most of that time business has been done through in-person and telephone communications but over the last three years *Go!* has been experimenting with e-commerce. Results have exceeded expectations, with almost a third of their sales for the current year coming via the e-commerce channel. *Go!* joined the SANS Co group two years ago, their on-line success largely due to the technical capability and marketing experience of the *Xtreme.com* team. *Go!* has around 40 employees based in Christchurch, New Zealand.

All up in the SANS Co group there are approximately 180 staff in two sites. The executive management team and majority of the head office functions are performed from Brisbane. This includes the core of the finance, marketing and IT development teams. The IT architecture and policy is formulated in the Brisbane office, but the IT support function is distributed over the two sites.

The SANS Co network is attached to the Internet at the two locations. The Brisbane site is connected via a T3 link. The Christchurch site uses a 256Kb Frame Relay link. The Brisbane site operates a DMZ off the Internet firewall. The DMZ is critical for *Xtreme.com.* They operate the sales and marketing website for the SANS Co group as well as for many other products and services. The mobile sales-staff use RRAS IPSec to connect for the SANS Co network via the Internet.

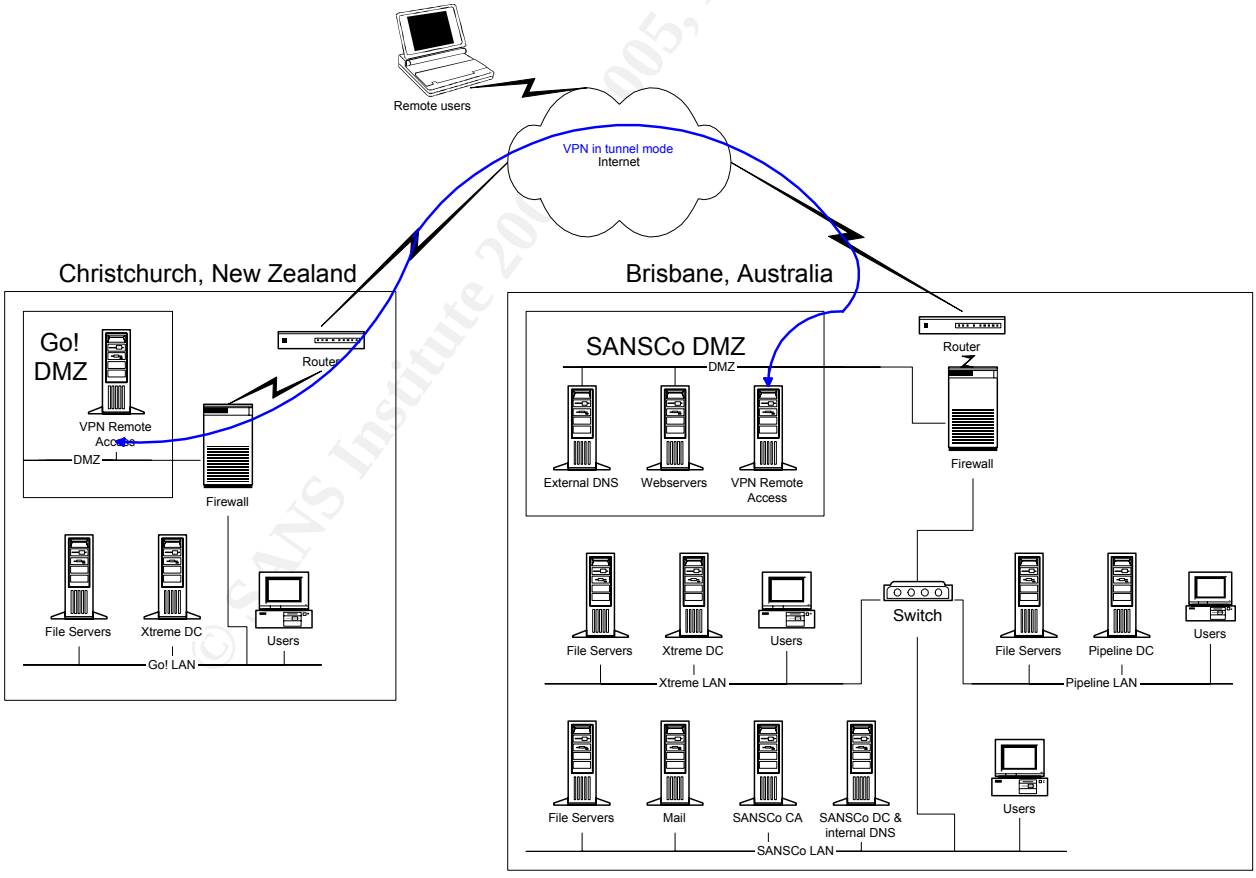

Figure 1.1: The SANS Co Network

The SANS Co AD-integrated forest consists of four domains in two sites. Each of the three companies has it's own domain (go.com, xtreme.com, and pipeline.com.au), plus the SANS Co executive have a separate domain (sansco.com). The *Go!* network and site, based in Christchurch, is connected to the Brisbane domains via an L2TP VPN. All domain controllers operate in Native mode and provide DNS services. The Internet DMZ in Brisbane is also a separate DNS domain (sansco.com.au), with all the servers in it operating in stand-alone (no domain) mode.

The SANS Co IT management team considered combining the four internal domains when upgrading the entire network to Windows 2000, but for undocumented reasons the decision was to leave it as four domains. For the *Go!* network an important consideration was to minimize the volume of NC replication performed over the WAN link.

The sansco.com domain is the forest's Root domain. The other three internal domains are linked into the forest with transitive trusts as peer domains. Thus they are authenticated with Kerberos, they are two-way, and the Schema, Configuration NC and Global Catalogue databases are replicated between the sites.

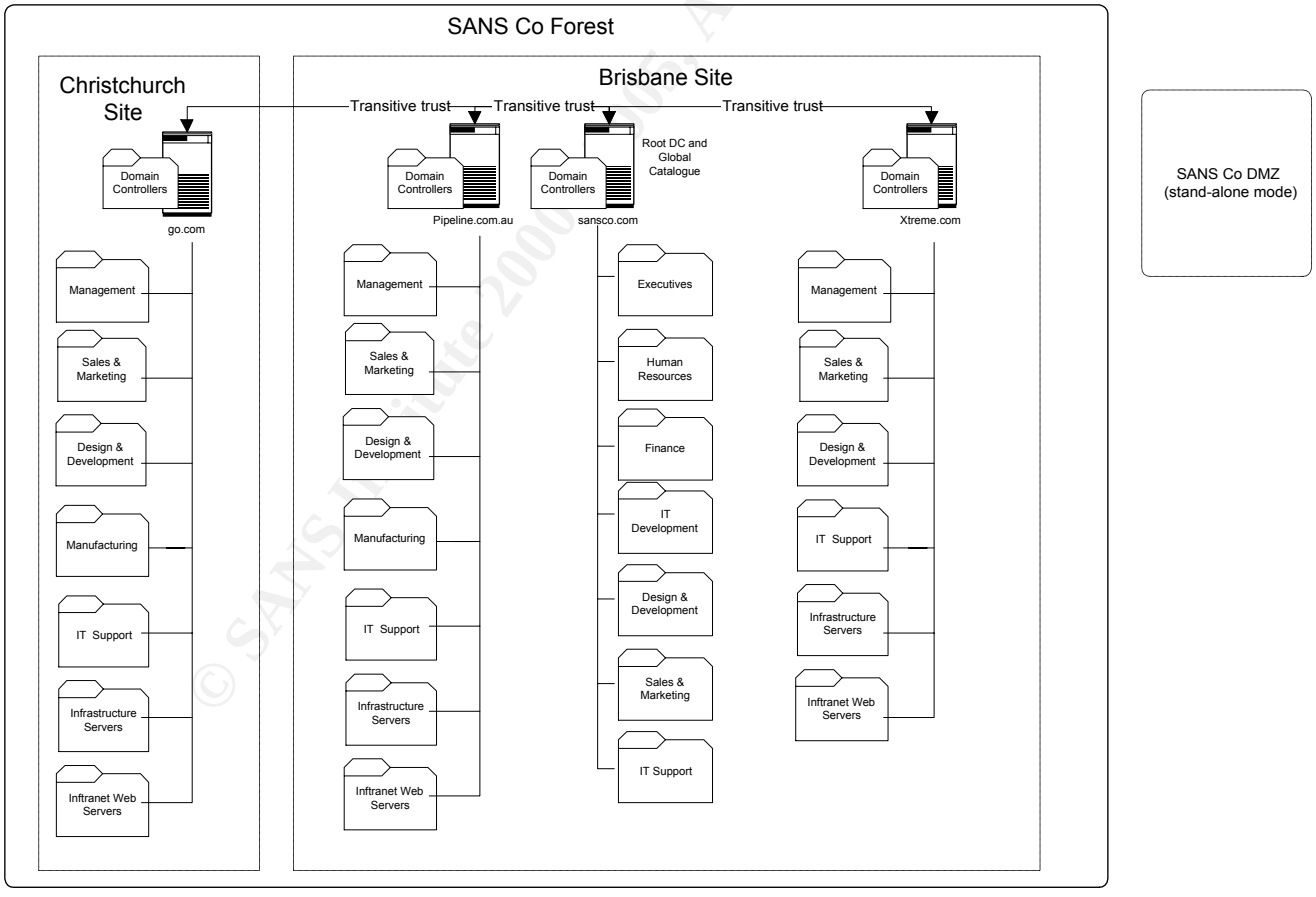

Figure 1.2: The SANS Co Win2K Domain Structure

The SANS Co Windows 2000 OU structure is formed around the business units, grouping users and the resources they most frequently use. The sansco.com domain has OUs for Executives, Human Resources, Finance and IT Development. The other three domains have OUs for Management as well as resource OUs for Infrastructure Servers and Intranet servers. All of the domains have business unit OUs for Sales and Marketing, Design and Development, and IT Support. Each Domain also has a default Domain Controllers OU.

The SANS Co group has a Root Certification Authority (CA) and a single sub-ordinate CA providing certificates and Certificate Revocation Lists to facilitate VPN tunneling between the sites, SSL web client and server authentication and encryption, and S/MIME protected e-mail. E-mail, file sharing and web services are used extensively throughout the group. Much of the information processed by the organization is commercially sensitive or private to their customers and retailers. Pre-manufacture product information is very sensitive, especially that concerning branding and designs for the highly competitive sportswear industry.

1.2 Overview of the GIAC Network

The previous project selected for the GIACE network was developed by Rune Lee (Analyst No.0205, http://www.giac.org/practical/GCWN/Rune_Lee_GCWN.pdf , (Lee)). The following descriptions and diagrams are paraphrased and/or based on that reference.

GIAC Enterprises (GIACE) is a leader in Hi-Tech surfboard design and sales. The company is heavily dependant on on-line purchasing. GIACE is based in two geographic locations: Toronto, Canada (Head Office); and Cooktown, Australia. Each location has approximately 100 employees, with expected growth of around 30% over the next three years.

The GIACE network is a single domain Windows 2000 network. Internet access is provided to each of the two sites by a T3 connection. The R&D and Sales and Marketing staff have remote access via RRAS IPSEC. Much of the information created and processed by GIACE is regarded as highly sensitive. There is a GPO exclusively for the company's executives, within which IPSec is enabled for all communications. The network design is shown in Figure 3. Each site has an internal network and a DMZ separated from the Internet by a firewall. There is a VPN tunnel between the two sites.

All client workstations run Windows 2000 Professional with Internet Explorer 6.0. User's home directories are on the file servers. Designers provide additional protection to their sensitive files with EFS. GIACE employs MS Certification Authorities to issue certificates to those user groups with special needs.

The DMZ for each site has an external DNS server and a VPN remote access server. The Canadian DMZ also hosts the company's two clustered IIS 5.0 web servers.

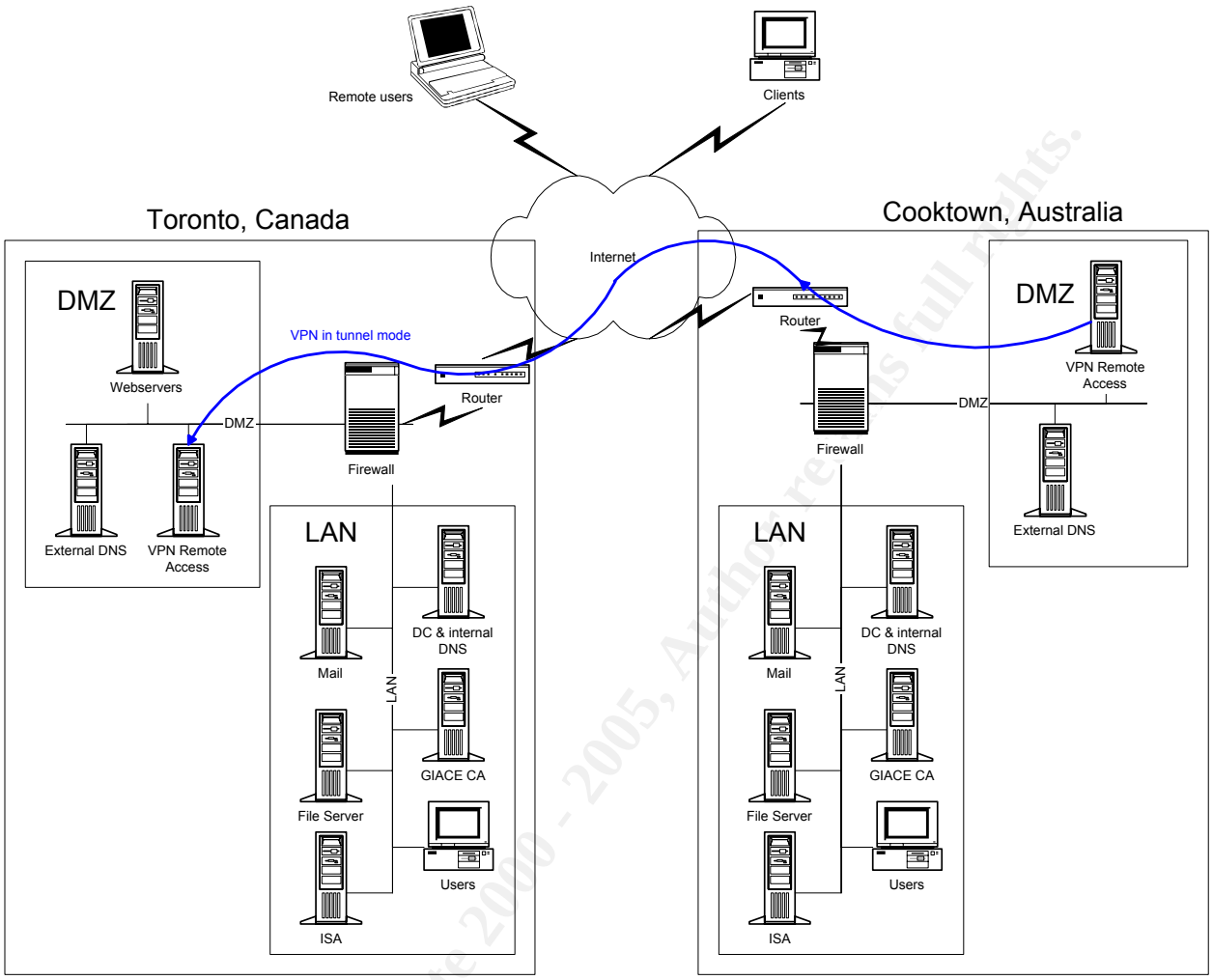

Figure 1.3: The GIACE Network

The Active Directory design of the GIACE forest consists of a single domain, *GIACEnterprisesCorp.com*. It is an AD integrated zone. The two sites' Domain Controllers operate in Native mode. They also supply Domain Name Service (DNS) to their respective user groups. The domain has OUs for Infrastructure Servers, Domain Controllers, File Servers, and Web Development. There are also OUs for the two locations (Canada and Australia), each with sub-OUs for Executives; IT Administrators; Finance; R&D; Sales and Marketing; and HR

The Default Group Policy is applied to all systems within the GIACEnterprisesCorp.com domain. GIACEnt_Local.inf is also applied locally to each machine to rename the Administrator and Guest accounts. Other GPOs used are: the Default Domain Controllers Policy, the Local Security Settings, and specific GPOs for the OUs and DMZ server. GIACEnt_SecureSvr.inf is applied on all servers. The Sales OU GPO facilitates laptop remote access to the network

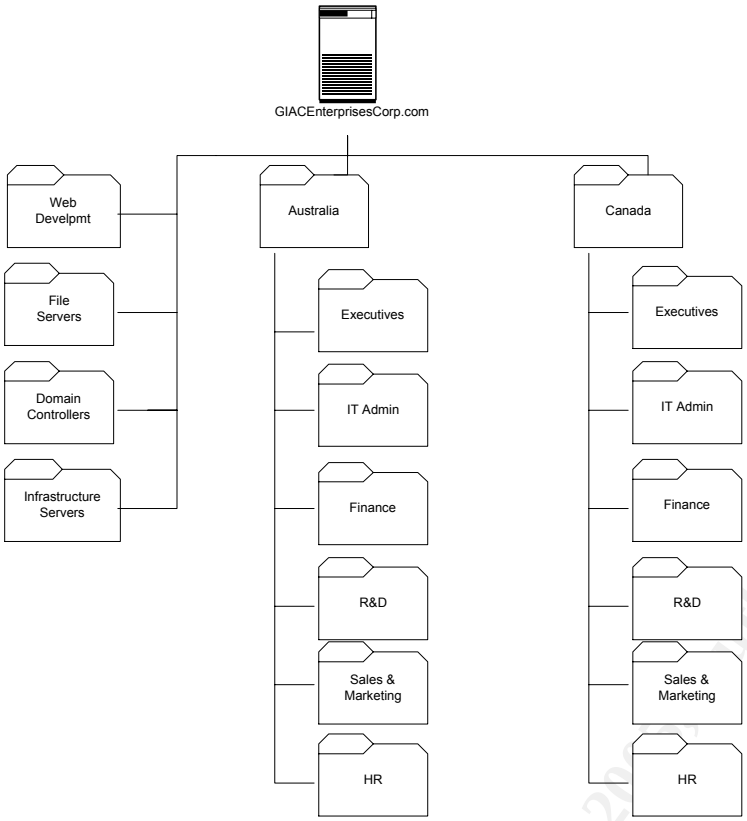

Figure 1.4: The GIACE Win2K Domain Structure

The built-in IPSec policies have been replaced with those that enable IPSec in Transport mode on all server-to-server and client-to-server communications. The GPOs for R&D, HR, and Executive OUs are configured as "IPSec Server (Request Security)". Servers in the DMZ require Transport mode IPSec on communications from the Internal network.

1.3 Merger of GIACE and SANS Co

SANS Co acquired GIACE in mid 2003 to expand their product and service range as well as to expand geographically. The merger has enabled SANS Co to gain a market in North America, while GIACE is expanding its customer base in Australia and New Zealand. Head Office of the joint company is based in Brisbane but operationally there have been no major changes for the staff. The GIACE IT Division remains in Toronto, although Brisbane Head Office is the focal point for IT architectural and security policy decisions.

Business needs of the network with regards to the merger include:

- Staff need to be able to exchange information via encrypted and authenticated e-mail throughout the combined organization.
- Customers of both organizations need to be able to be authenticated in their

interactions with the other organization.

- Product information and inventories need to be accessible for viewing and sales made by staff of the other organization.
- GIACE and SANS Co management need to share financial and operational information via access to the relevant databases.
- The Executives based within SANS Co require read access to GIACE's financial information.
- The design and marketing teams of GIACE, *Pipeline* and *Go!* require a limited-access Intranet area for sharing new ideas and designs.

Since GIACE is already a distributed operation that utilizes Win2K, VPNs, remote access, public key certificates, and has a single domain, the merger of the GIACE network and forest with that of SANS Co is relatively simple. No fundamental modifications to the system architecture will be required.

The next section proposes a system architecture for the merged system.

1.4 Combining the Networks and Forests

The two companies already have all their sites connected to the Internet, with a number of business processes operating across the Internet links. Therefore no major network architecture changes are required with regard to the core physical and IP layers of the architecture (Figure 1.5).

The SANS Co and GIACE Windows domains will be joined primarily via a mixture of explicit trusts and public key authentication.

Both networks operate Windows 2000 domains in Native mode. Two-way Explicit trusts would be set up between the GIACE domain and the three SANS Co internal domains. The single domain design of the GIACE network has simplified this task more so than if it also had multiple domains, as an explicit trust has to be set up between each pair of domains crossing the forest boundaries[1]. Figure 1.6 illustrates where the Explicit trusts are created. The Explicit trusts allow fully authenticated networking between the four SANS Co domains and the GIACE domain.

The Organizational Units defined for the existing SANS Co and GIACE forests are not identical, but similar enough that they can be matched. The user groups from each domain will be added to Enterprise groups of the other. For instance, the Sales and Marketing user group within the GIACEnterprisesCorp.com domain will be added to the SANSCo forest Sales and Marketing Enterprise Group, which already contains the Sales and Marketing groups from the xtreme.com, pipeline.com.au, SANSCo.com.au, and go.com domains. This will significantly simplify cross-organizational information sharing and shared business practices

[1] This issue is simplified in Windows XP, where the creation of Forest trusts - transitive trusts between forests - is possible.

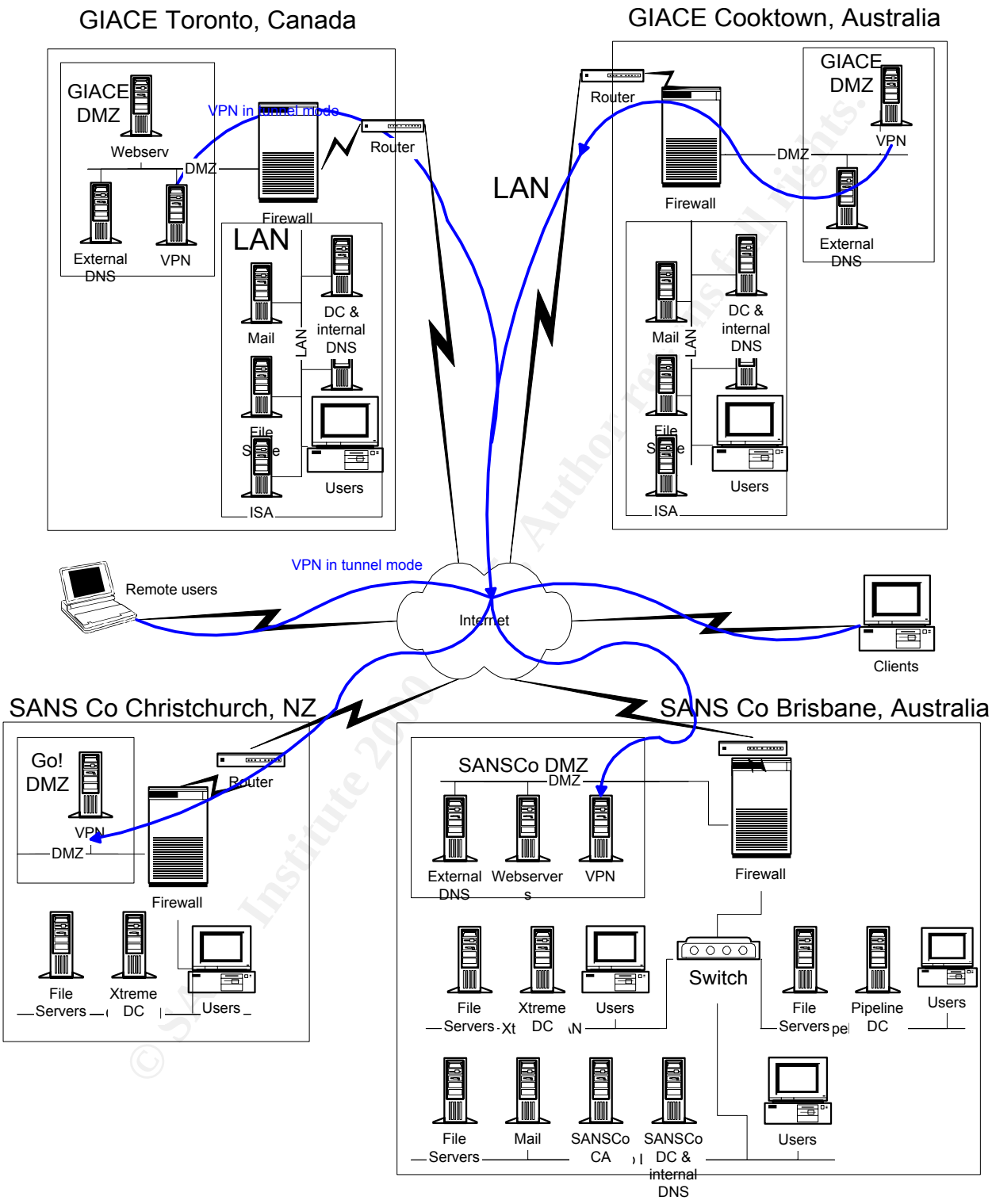

Figure 1.5: The Combined GIACE and SANS Co Networks

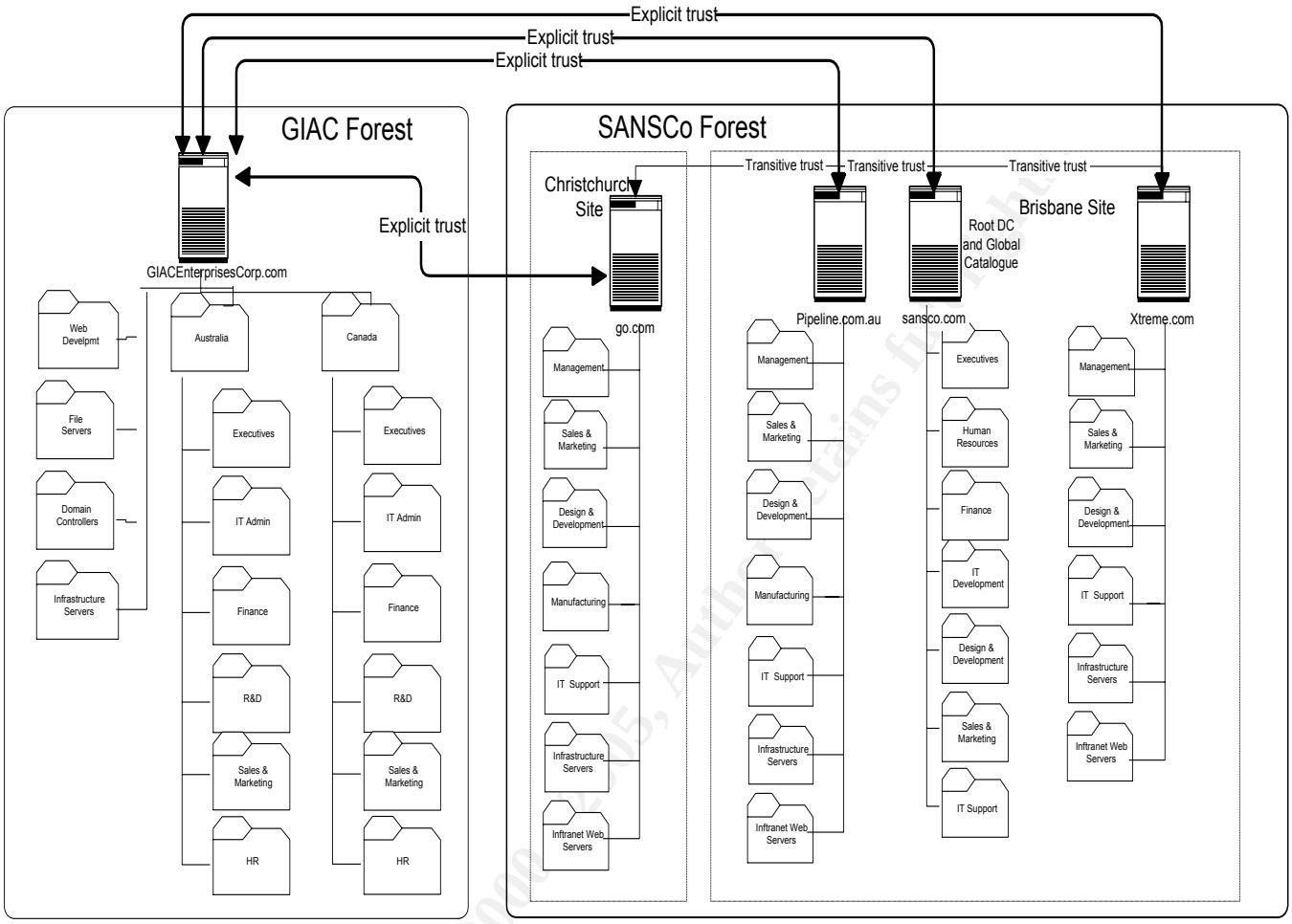

Figure 1.6: Trust Relationships Between the GIACE and SANS Co Domains

Both forests utilize public key certificates. To facilitate PKI interoperation, the Root CAs of both groups will be loaded into the Trust Lists of all users and VPN and Intranet server computers via each domain's default GPO.

To facilitate secure communications between the four sites (Brisbane, Cooktown, Christchurch and Toronto) Layer 2 Tunneling Protocol (L2TP) encrypted and authenticated tunnels will be set up. The firewalls of the four sites will be configured to allow the VPN traffic to pass through, but only from the other SANS Co and GIACE firewall addresses.

Staff and trusted customer remote access will enter the combined network through the same RRAS channels as before the merger. To limit the impact from unauthorized access from a remote computer, traffic from the remote access IP pool will not be permitted through the intra-organizational VPN.

Customers of one company will be able to review and purchase goods from any of the

companies through either the SANS Co or GIACE websites. The two websites will both retained their own look and feel, but the back-end databases at *Xtreme.com* and GIACE will be expanded and are replicated to ensure the product and availability information for any product the combined organization offers is up-to-date and identical regardless of which site they visit.

Database replication between SANS Co and GIACE will be protected over the Internet via the VPN tunnels with additional end-to-end transport mode IPSec authentication and encryption. While each of the two organizations will retain their own customer database, a partial consolidation of them will be managed within the *Pipeline* domain for customer profiling purposes.

E-mail will be used extensively for information sharing throughout the merged organization. Both groups will retain their original e-mail servers, with mail between the four sites passing over the Internet via the encrypted and authenticated VPN tunnel.

To reduce the management overhead and to ensure consistency over the merged system, the intrusion detection, virus protection and e-mail content filtering systems of the two organizations will be coordinated and linked wherever possible.

Group Policy will be standardized to minimize the number of GPO variations over the shared system. Group Policy will also be used to apply software updates and service packs to the user and server computer.

The security policies of the two organizations will be matched and merged into an agreed and enforced global policy. The merger and changes because of it will require that users are trained in the new security requirements and mechanisms.

PART 2 - SECURITY POLICY AND TUTORIAL

This part of the paper defines a set of Group Policy objects and templates to support the technical, security and business requirements defined in Part 1. A test network was created modeling some aspects of the combined SANS Co and GIACE network, specifically the operation of a web server – IntraWeb1 - within the SANS Co internal network. The paper then describes the process and results of a test of one of the security controls in the Group Policy as applied to the test system, specifically the centralized control of IntraWeb1's Root certification authority Trust-list. Two functional tests are then described. The first centers on a problem with ActiveX when enrolling for the web server SSL certificate, and the second, on verifying that the SSL encryption and authentication operate as expected. The final segment discusses the pros and cons of the proposed GPO architecture and suggests some areas of possible improvement.

2.1 Group Policy Design Requirements

The core business needs relating to the SANS Co and GIACE merger are listed in section 1.3. The internal requirements for each of the companies is similar. All users require e-mail and web access to the Internet, plus access to private and shared network areas. Users are not permitted to administer their workstations, for instance to install software. Customers of the SANS Co and GIACE online sales Websites must be not only able to purchase directly from those sites, but also purchase the other organization's goods from either site. For instance, the GIACE Surfboard range must be available to review and purchase from the SANS Co website.

A set of best practices was formed based on the system architecture, the business needs, and the recommendations from the SANS GCWN course material, Microsoft's Security Operations Guide for Windows 2000, and the SANS Top 10 Windows Vulnerabilities. The set of group policies were selected based on those requirements.

2.2 Group Policy Design

To simplify management, wherever possible and suitable, identical GPOs are used to cover the same roles over the GIACE And SANS Co forests. GPOs are applied in the order of Local (computer), Site, Domain, then down through parent OUs to local OUs[2]. Therefore, settings at the most local OU level will have the highest precedence if there are any conflicts with the GPO settings at the other levels[3]. However, there are advantages to applying controls at the other levels. Controls applied at the Local

[2] Microsoft Security Operations Guide for Windows 2000 Server, page 30.
[3] Note that the Local-Site-Domain-OU precedence order can be disabled if the GPO at a parent container has the "No Override" switch enabled. Also, where two or more GPOs are linked to by an Active Directory container, the GPO that is lowest on the GP dialogue box list will be processed first, so will have least precedence unless "No override" is set..

(computer) level will be applied regardless of connection to the DC, for instance for portable computers that are logged into locally while working off-line. On the other hand, controls applied at the Site and Domain level can cover a much wider group of users and computers, so eliminating the need to duplicate the same settings over multiple containers.

In the implementation discussed here, assignment of GPOs at the Site level was not used, as the four sites do not correspond directly with the five business domains or the functional areas across the businesses.

At the Local Policy level two of the Security Options were set following the GIACE standard on renaming the local Administrator and Guest accounts to unique identifiers (Lee, page 18).

The next layer of GPO has been applied at the Domain level. The same GPO is applied to all of the domains. This GPO was derived from NSA's *w2k_domain_policy.inf* template. It sets the Account Policies on all of the domains to the following values:

Password Policy	
MinimumPasswordAge	1
MaximumPasswordAge	90
MinimumPasswordLength	12
PasswordComplexity	1
PasswordHistorySize	24
Account Lockout Policy	
LockoutBadCount	3
ResetLockoutCount	15
LockoutDuration	15
RequireLogonToChangePassword	0
ForceLogoffWhenHourExpire	1
ClearTextPassword	0
Kerberos Policy	
MaxTicketAge	10
MaxRenewAge	7
MaxServiceAge	600
MaxClockSkew	5
TicketValidateClient	1

While these settings are not all the same as those currently used within the GIACE network, the changes will not result in visible differences to the users in that domain.

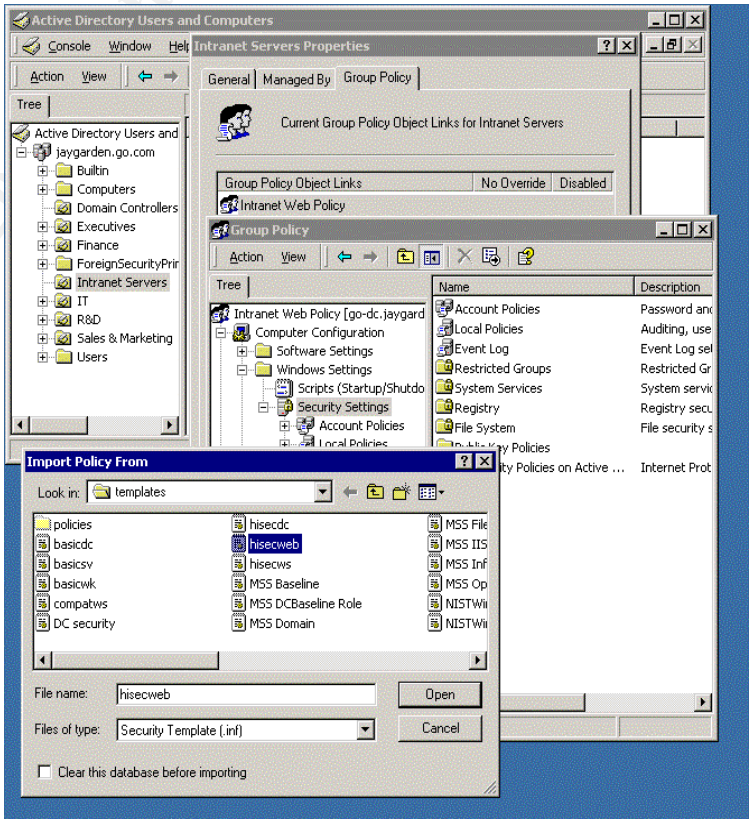

Figure 2.1: Importing the *Hisecweb.inf* Template

The remainder of the Group Policy settings are defined at the OU level. All server OUs are linked to the "*SANS Co Server*" GPO, with additional incremental GPOs as required. The SANS Co Server GPO has both the *MSS Baseline.inf* and NSA's *w2k_server.inf* templates applied. *MSS Baseline.inf* configures audit and event log settings, security

options, registry access controls, and disables many unneeded services. These will be re-enabled in later templates if required. The *w2k_server.inf* template also configures audit and event log settings, security options and registry access control. In addition it sets user rights and file system access controls. It also disables membership of the Power Users group.

The 'Domain Controllers' OUs have an incremental GPO called "*SANSCoDC Policy*", deriving its settings from the *MSS DCBaseline Role.inf* template. This adds controls to the User Rights and Security Options areas and sets access control to %system drive%\.

Microsoft's *Hisecweb.inf* template is applied to a GPO at the Intranet Servers OU that contains the IIS servers used for the intranet web sites. This template primarily changes the services to be run and includes several anti-DDOS registry settings.

Likewise, the *MSS Infrastructure Role.inf* and *MSS FilePrint Role.inf* templates are applied incrementally to the OUs of servers providing the organizations internal infrastructure.

The business unit OUs are linked to a GPO with the *NISTW2KproGoldPlus.inf* secure workstation template applied.

The application of the templates to the SANS Co and GIACE forests is graphically represented in Figure 2.2.

Portable computers have the relevant domain and OU templates applied locally as well as via Active Directory to ensure that the GP controls are enforced for local logins when operating as a stand-alone computer.

Group Policy for the stand-alone DMZ computers will not be described here other than to note that the templates are loaded directly to the Local Policy and are based on those used for the internal servers.

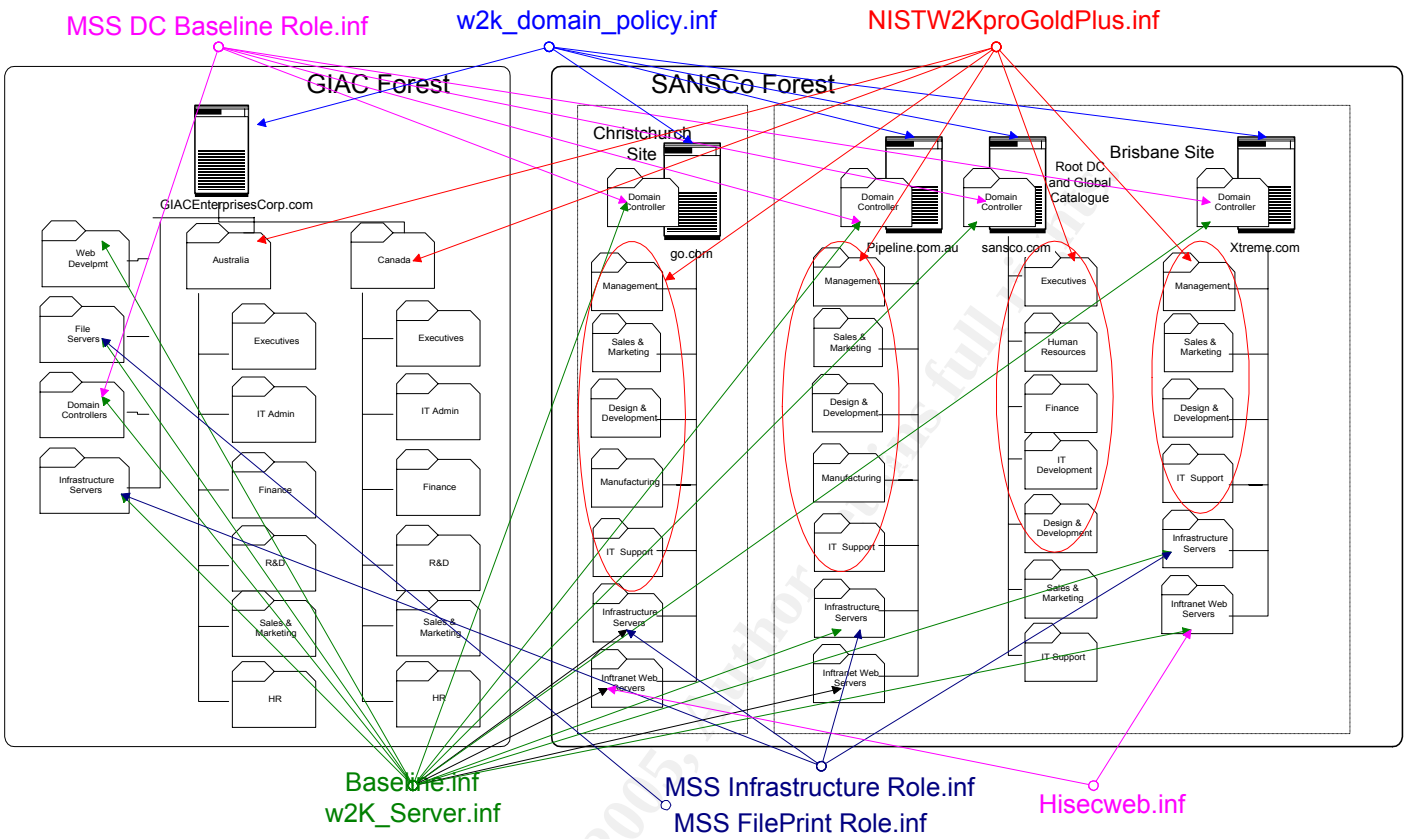

Figure 2.2: Assignment of the Security Templates to Group Policy Containers

2.3 Implementation of the Group Policy

The *Go!* intranet web server IntraWeb1 was selected as the example to demonstrate application of the GP settings to a SANCo IIS server. The demonstration network consisted of the *Go!* Domain Controller, the IntraWeb1 IIS5.0 server, and a Windows 2000 Professional user workstation. A Microsoft Certificate Services server was also set up temporarily as a stand-alone CA to issue IntraWeb1 and users certificates. All the demonstration computers were running Windows 2000. Fixed IP addresses were used and DCHP was not enabled.

The SANS Co Default Domain Policy was applied on the Domain Controller (go-dc.sansco.com) at the jaygarden.go.com Active Directory “Domain” container. The "w2k_domain_policy" template was applied to this Group Policy Object via the GP "Import Policy" feature. Through the same mechanism, the "Intranet web server Group Policy" was applied to the Intranet container and the Baseline.inf, w2K_Server.inf and Hisecweb.inf templates imported to the GPO (refer Figure 2.1).

The sensitivity of pre-manufacture designs require that parts of the *Go!* Design Team website need to be restricted to the *Go!* Design Team members and various staff members of the other organizations within the SANS Co and GIAC Enterprises group. To achieve this requirement SSL was configured on the server and the restricted pages

set to require web client PKI certificate authentication. To avoid certificates issued by public CAs from being trusted to allow access to those web pages, the list of CAs to be trusted by the Intranet web-servers was configured via the Group Policy Trusted Root Certification Authorities (Computer Configuration > Windows Setting > Security Setting > Public Key Policies). During operating system installation the Root Certificate Store was created empty. The SANS Co Root Certification Authority was created as a stand-alone CA, i.e. not integrated into Active Directory, and then its certificate was installed in IntrWeb1's Root CA Trust-list via Group Policy.

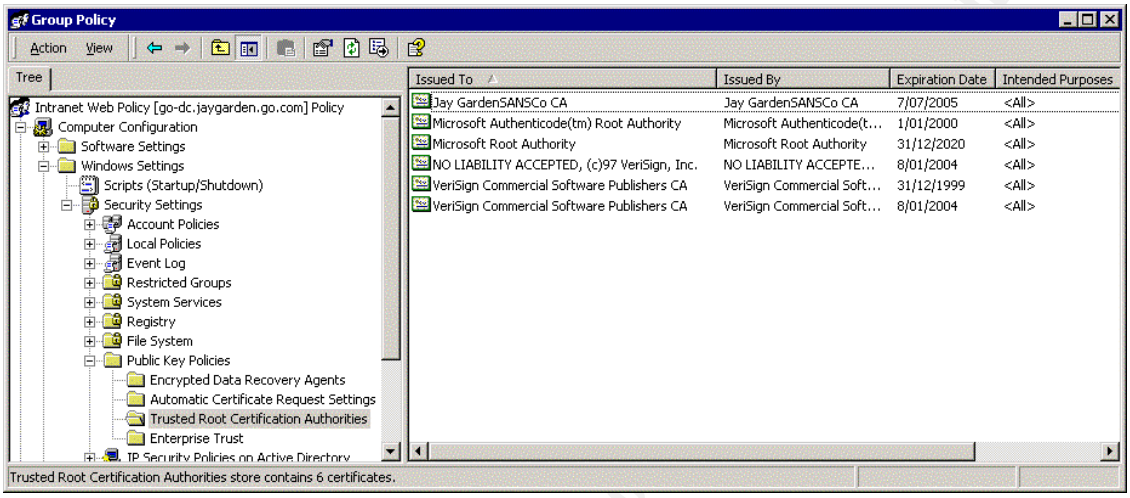

Figure 2.3: IntraWeb1's Group Policy Trusted Root CA List

These restrictions could have been set directly on the web-server certificate stores, or via certificate mapping, but for flexibility and ease of centralized management, the controlled Root CA Trust-list solution was selected. For instance, the GIACE CA Root certificates could easily be added to the Trusted Root CAs list.

2.4 Test of One of the Group Policies' Security Settings

One of the security tests performed on the test network was to ensure that the limited Trust-list defined in the Intranet Server GPO was being applied to the test web server. The Root CA Trust-list was viewed in Internet Explorer, first with the GPO disabled, and then with it enabled.

The above configuration controlled the Trust-list as expected (Figure 2.4). However, an error with the operating system's Windows File Protection (WFP) feature was triggered on start-up. This was caused by WFP's inability to validate the file integrity signatures. To enable that feature to work correctly, the Microsoft and Verisign code signing Root Certificates were also included on the customized Root CA Trust-list. Once these were installed and the GPO applied the Trust-list worked as expected. During testing to determine which Root certificates were required in the Trust-list, it was noted that the system generally had to be rebooted twice in order for the updated Trust-list to be seen

at the point in the boot process required by Windows File Protection[4].

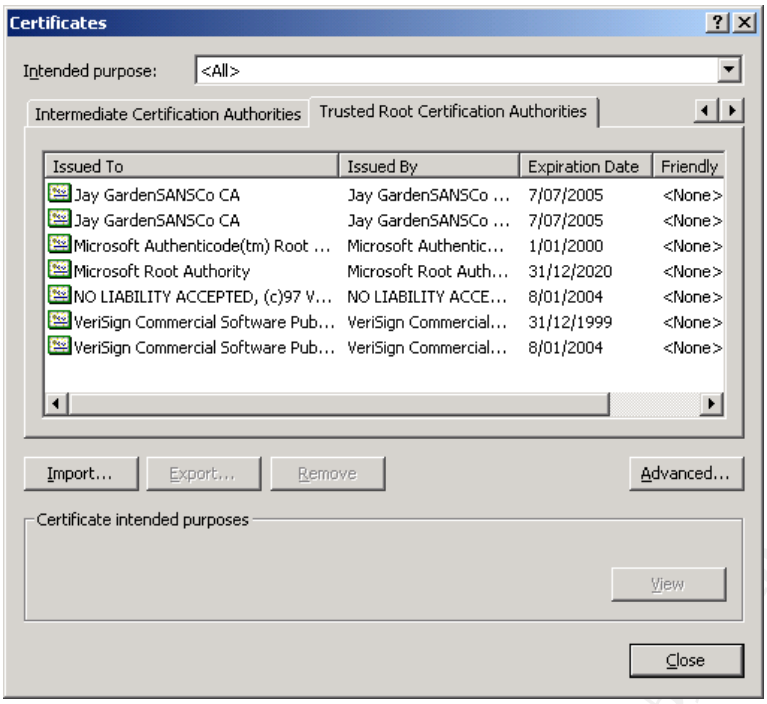

Figure 2.4: The GP Customised Trust List on the *Go!* Intranet Server

The SSL capabilities facilitated by the certificates and the addition of the SANS Co CA in the Trust-list were also tested. The results are described in the second functional test below.

2.5 System Functionality Test

Two processes on IntraWeb1 were assessed to test the functionality of the system after the security settings were applied. The first process was enrollment of the Web sever for a public key certificate from the temporary Certification Authority. An error occurred when attempting to download the ActiveX controls on the certificate enrollment form. The second test was verification that the controlled-access webpages were being encrypted and that only a user with a certificate signed by a CA in the Trust–list could gain access to them.

[4] Running the command "secedit /refreshpolicy machine_policy /enforce" can be used to refresh the GP on the member computer (Cunningham et al, p152-155). An alternative to the double reboot is to run the secedit command before rebooting, therefore setting the new Trust-list before the WFP process activates at bootup.

Functional Test One: Creation of a Web Server Certificate

In order to enable SSL authentication and encryption on the Intranet Web server, a Web server public key certificate had to be created for the server. A temporary MS Certificate Services CA was set up in stand-alone mode and attached to the test network. When the browser on IntraWeb1 attempted to download the certificate enrollment form the ActiveX controls would not load, displaying the 'downloading' message in Figure 9.

It was suspected that the HISECWEB template applied to the Intranet Web Policy GPO had restricted users on IntraWeb1 from downloading potentially malicious code from untrusted sites. Adding the CA to the user's list of IE Trusted Sites did not fix the issue.

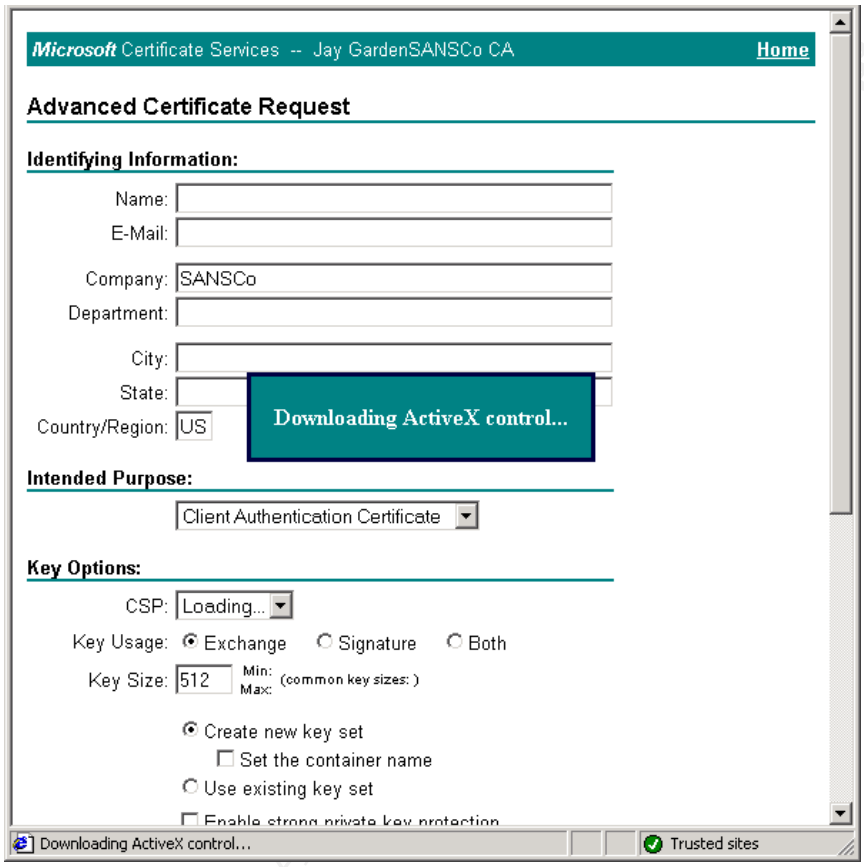

Figure 2.5: IIS Certificate Enrolment Error

The HISECWEB template settings were temporarily removed from the Intranet Servers OU by making a duplicate of the Intranet Web Policy minus the Hisecweb.inf template, linking it to the Intranet Servers OU, and disabling the original GPO. On refreshing the GPOs via the *secedit /refreshpolicy* command on IntraWeb1, the problem with downloading ActiveX controls remained, clearing the Hisecweb.inf template of fault. The GPOs were reset to the pre-test settings. The Microsoft Knowledge Base was searched and Article 330389 "*IE Stops Responding at "Download ActiveX Control" When You Try to Use a Certificate Server*" was discovered. It noted a fault caused by the certificate enrollment service's use of ActiveX could produce very similar results. The recommended fix was to install Service Pack 2 on the certificate services computer. As the CA was only set up and connected to create the test client and server certificates it was a default install without hardening or application of Service Packs. Service Pack 4 was applied to the CA and the CA was rebooted. The certificate enrollment form was opened from IntraWeb1 again. This time the ActiveX controls downloaded and ran successfully.

Functional Test Two: Access Control to the Restricted-access Web Pages

For this test, one of the Design team and one of the Marketing team attempted to access one of the restricted access intranet web pages on IntraWeb1.

Design Dan has applied for and been issued a certificate by the SANS Co certification authority, so should gain access to the page. Another user, Marketing Mike, who has system access and a web client certificate issued by one of the Thawte CAs, should not be able to access the restricted page now that the Thawte Root certificates have been removed from IntraWeb1's Root CA Trust-list.

First, a certificate was requested by IntraWeb1 and issued by the SANS Co certification authority.

Then Design Dan (an authorized user) also requested a public key certificate from the SANS Co CA. Design Dan's certificate was issued and installed into his web browser.

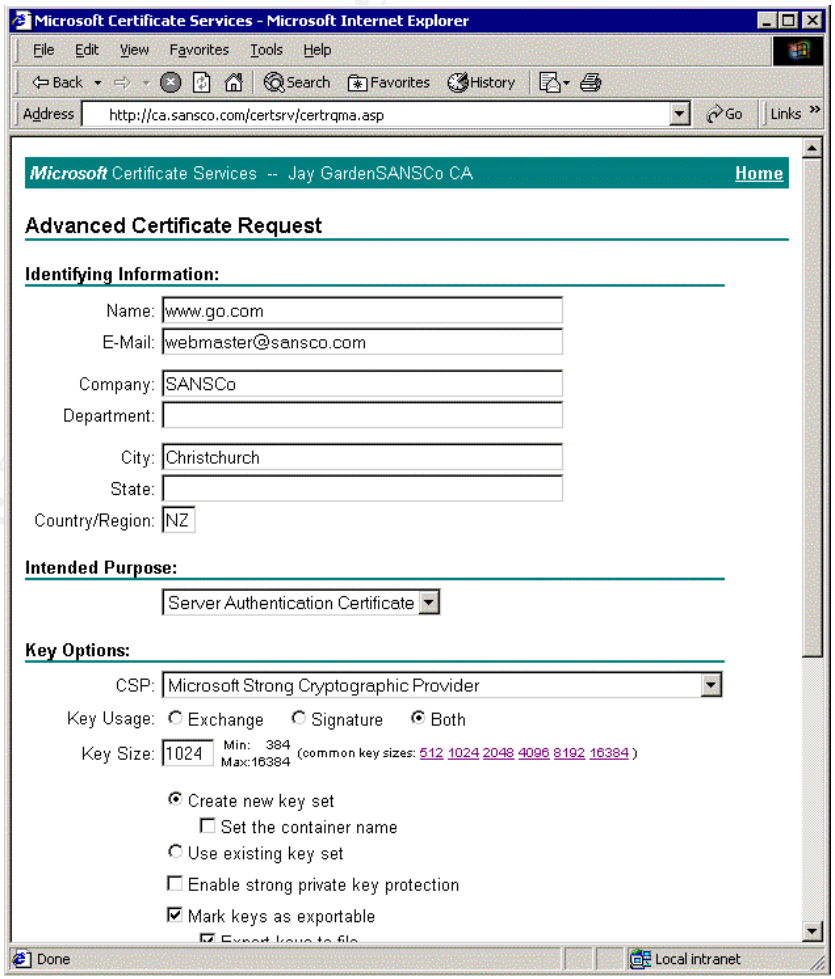

Figure 2.6: Creation of the Go! Design Team Intranet Website Certificate

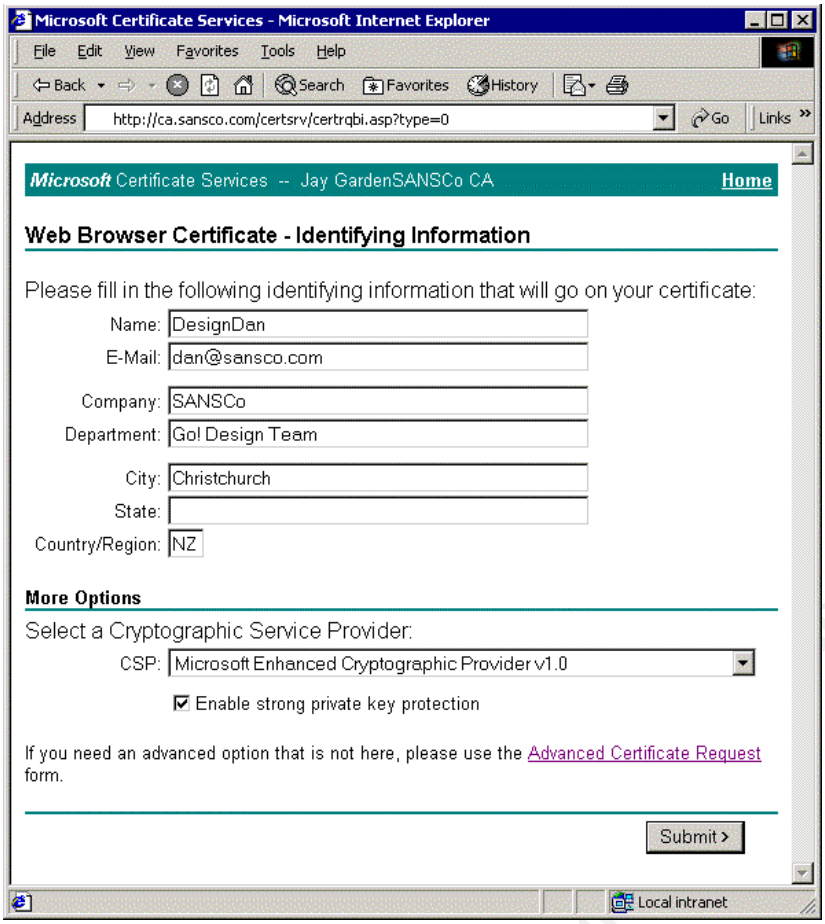

Figure 2.7: Creation of a Design Team Member's Web Client Certificate

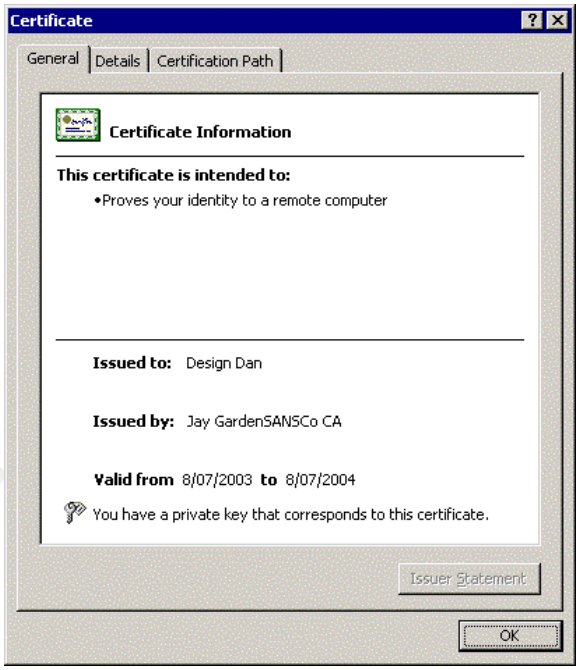

Figure 2.8: The SANS Co User Cert

When Design Dan attempted to access the protected web page his browser prompted him for the private key/certificate to authenticate to the server with. Once selected, the handshake completed and the protected page downloaded successfully.

The web page transfer was successful, displaying the page in Figure 2.10. Both ends of the transaction were authenticated and the transfer was encrypted with 128bit SSL. To verify the encryption Network Monitor was set to collect the packets passed between IntraWeb1 and the client workstation.

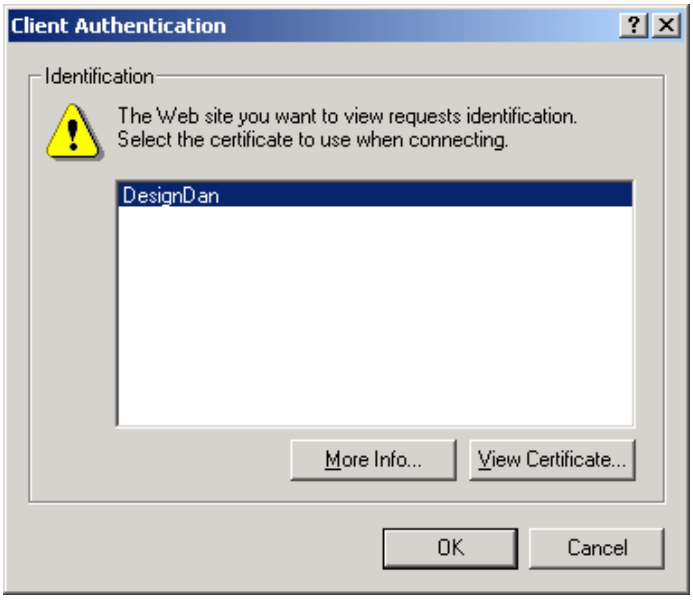

Figure 2.9: Cert Selection Within the SSL Handshake

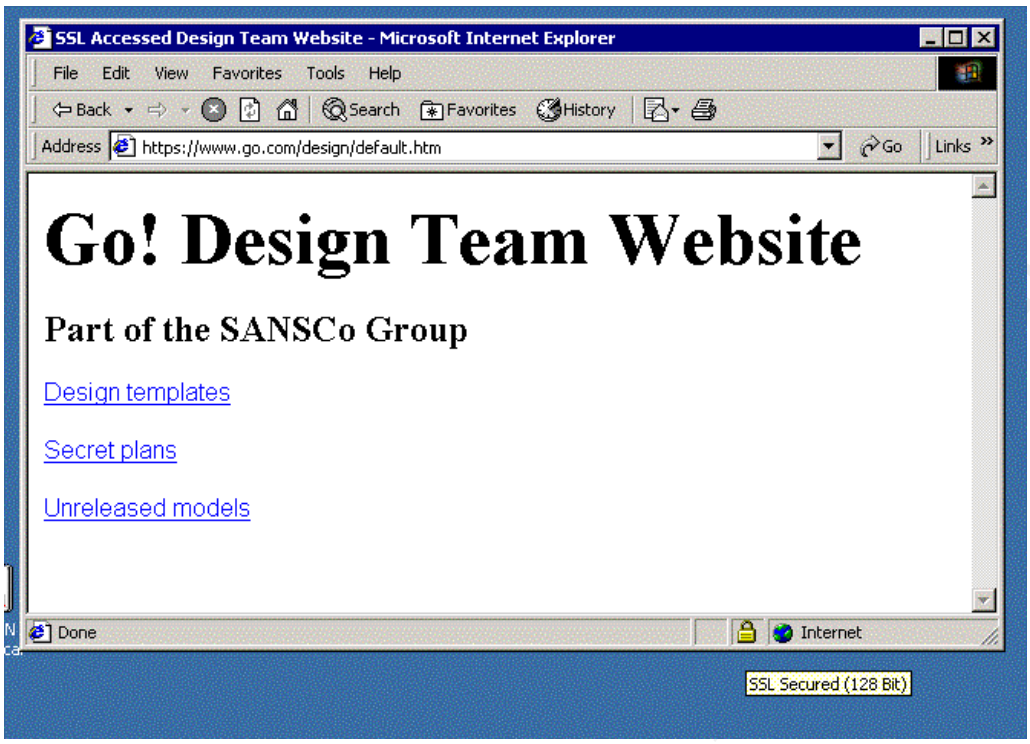

Figure 2.10: Successful Access to the restricted-access web page

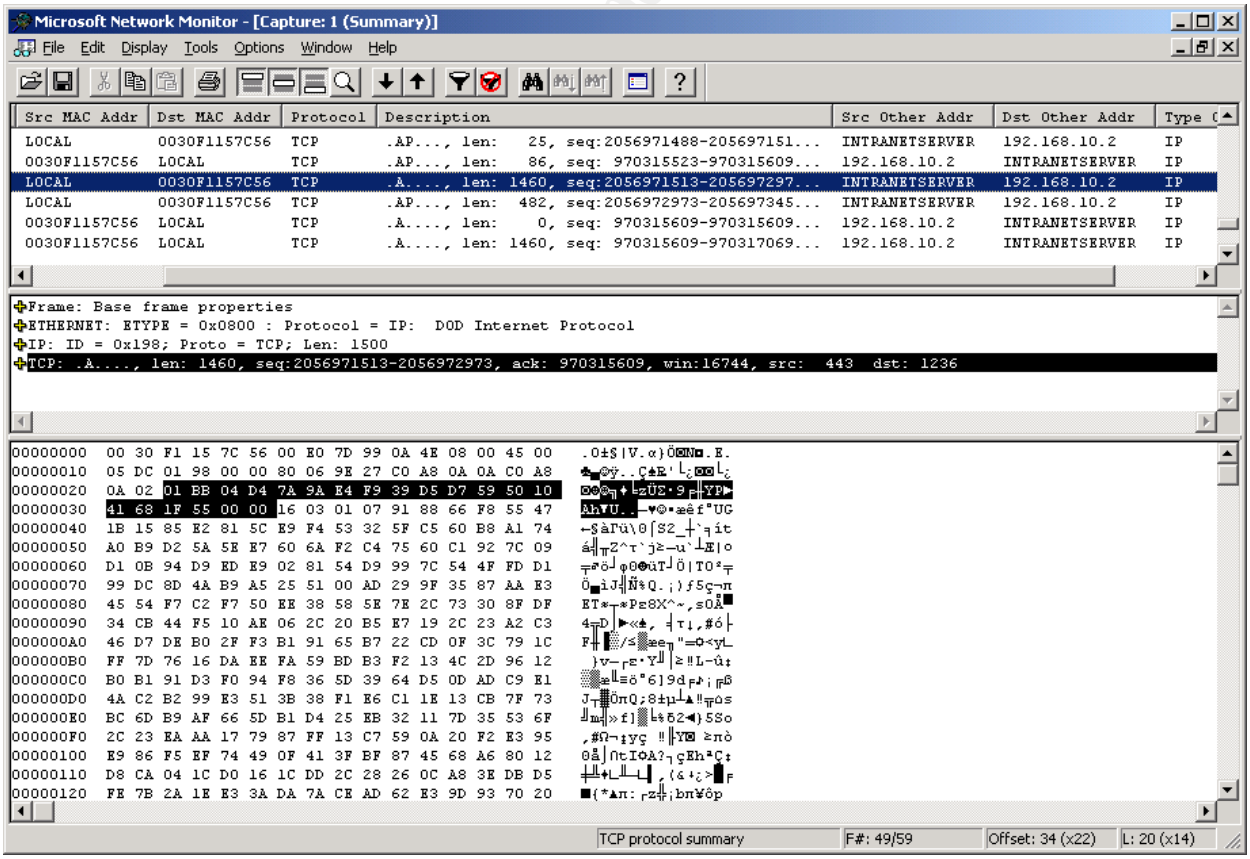

Figure 2.11: Network Monitor Capture of the Encrypted Web Page

The output from Network Monitor shows the captured packet has a TCP source port of 443, identifying it as probably originating from as SSL server. It has a length of 1460 bytes and does not have the syn or fin flags set, indicating that is payload rather than control. The ascii decoding of the payload does not appear to be text or have any discernible pattern. While this does not prove that the packets were encrypted with 128bit encryption, this simple method did verify that the page was not passed as cleartext (see Figure 2.11).

Next, a user with an externally issued certificate attempted to access the restricted–access web page. The user, Marketing Mike, has a valid login and a certificate issued by Thawte.

When Marketing Mike attempted to access the web page the key pair/certificate selection dialogue box is called. The Thawte certificate is not listed since the CA does not have a certificate chain of trust to it (Figure 2.13).

Pressing “Cancel” on the Client Authentication dialogue box resulted in error 403.7 “The Page Requires a Client Certificate”.

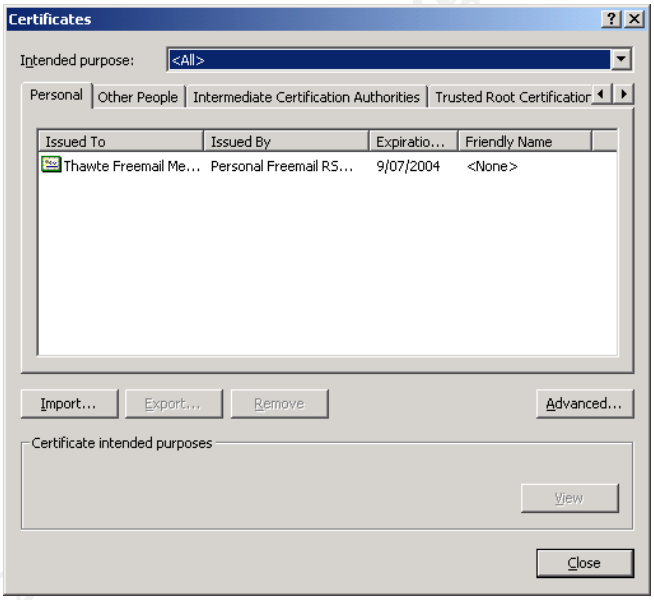

Figure 2.12: The Thawte Certificate in IE

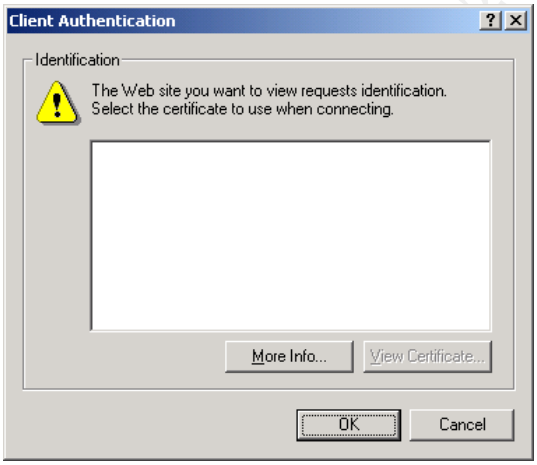

Figure 2.13: The Thawte Certificate Unavailable for Selection

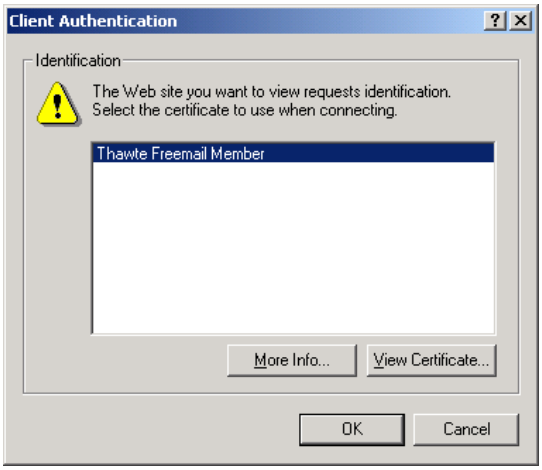

Figure 2.14: Certificate Selection with the Default Trust-list Re-enabled

To verify that the certificate was being rejected by the web server, rather than through a problem with the client, the Intranet Server GPO Trust-list was temporarily replaced with a full default install Root CA Trust-list. As expected, the Thawte certificate was available for selection by the client (Figure 2.14) and the web page could be accessed.

2.6 Evaluation of the Group Policy

The Group Policy assigned to IntrWeb1 was primarily the result of the Group Policy Objects applied at the *Go!* Domain and Intranet Server OU levels. At the Domain level the SANS Co Domain Policy was assigned. This provided a consistent level of password constraints as well as baseline audit and system controls not only across the domain, but also across the SANS Co and GIACE forests. At the Intranet Server OU level, the Intranet Server policy was applied, adding additional system controls, registry values and access control, and file access control. The templates applied to the server were *MSS Domain.inf*, *Baseline.inf*, *Win2k_server.inf*, and *Hisecweb.inf.*

As the security templates only relate to settings in the Computer Configuration section of any GPOs they are applied to, the User sections of the GPOs that only had security templates applied were disabled. This helps login and logoff times as well as making the GPOs simpler to audit.

The Group Policy applied to IntraWeb1 worked well in general and did not appear to impair its operation. Several adjustments of the higher precedence GPOs did have to be made to ensure that they did not overrule more stringent requirements applied at the lower levels. For instance, the password policies of some of the templates applied at the OU level allowed shorter local passwords that those required by and at the domain level. To ensure consistency the Account Policies > Password Policy settings were removed from the OU-level GPOs.

The proposed architecture of the SANS Co domain structure did not work as effectively as it could with the templates available. In hindsight, a potentially preferably alternative to the OU structure used would be to have a 'Servers' OU, with the Infrastructure Servers, Intranet servers, etc as sub-OUs to that. This appears to be the model envisioned when the Microsoft templates were created. The Infrastructure servers OU in the SANS Co domain architecture was intended to contain internal DCHP and mail servers, as well as application servers. However, because of the servers' different security requirements the GPOs would be easier to manage if split into two OUs under the 'Servers' OU.

The controls on system management tools could also be tightened for the servers and workstations. For example NTFS file controls could be set on the network monitor Netmon.exe - installed in the \system32 directory on the Intranet server - to limited any access to members of the Administrators group only (the current settings also members of the Users group Read and Execute privileges).

An issue with the templates themselves is that they have very minimal in-built documentation. Applying the template is a test of faith that it will do all and only what is expected. There are also a number of settings that can be configured via Security Templates but are not visible in the Templates MMC snap-in. This makes it difficult to review everything a template will do to the system without viewing it both in the MMC and in a text editor.

PART 3 - AUDIT

This section discusses a set of tools and methods to audit the SANS Co and GIACE network with regards to gathering and management of event logs, performance data, and critical settings.

The combined SANS Co and GIACE network comprises of over five domains and four locations in three countries, so automated and remote gathering and management of the system events, configuration, and status will be crucial for maintenance of the network and it's security. The types of things that need to be watched fall into two broad categories:
- Activity related information such as user and system generated events and system performance; and
- System state and configuration information.
The two categories are interrelated from a system management perspective and with regards to security audit.

3.1 Activity-related Information

In the combined SANS Co and GIACE system there needs to be some monitoring of all systems, tighter monitoring of the servers, and then more still of gateways and computers running business critical services or sensitive information. The primary means of collecting this information will be via Windows Event Logs.

The broad Event Log settings within the domains and OUs is configured within the Group Policy 'Local Policies' section. Auditing on specific files, directories and registry keys can then be set manually or via a script on each computer. However, for ease of management SANS Co/GIACE will configure it domain- and OU-wide via the Group Policy 'Security Settings > Registry' and 'Security Settings > File System' sections. Servers will be configured to log all failed and successful events other than successful: Directory Service Access, Process Tracking and System Events.

Passing application specific events to it will also enhance the amount and type of information available in the Application log. For instance, the IIS servers will log SSL connections and ASP errors. IIS protocol logging will also be enabled on the intranet and Internet web servers.

To view the collected logs on a regular basis it would be infeasible and untimely to access them through the Event Log viewer on each machine. To view them from a central point they will be exported and copied to a central log server. The Dumpel utility (Dump Event Log, included in the Win2k Server Resource Kit) will be used to dump the logs into tab-separated text files via an AT scheduled script on each computer. For internal systems the text version of the log files will be written directly to a central log server. For DMZ systems the log files will be written to a local folder with the IIS Protocol logs. An AT scheduled batch file will FTP them to a drop point on the log

server.

Where real-time analysis of events on the internal system is required, the SANS Co/GIACE IT team will also use EventCombMT[5]. EventCombMT is a tool that can parse event logs from many servers at the same time. It can be used across domains.

Time synchronization across the network will be crucial for the events recorded at different computers and applications to be interlaced into consolidated logs. This will be achieved on the Windows Domain Forests via the Domain Controllers. Stand-alone and non-Windows systems will be checked for synchronization via a manual process.

To analyze the text log files they will be fed into a set of database tables via a scheduled VBscript. The script will also record any missing or corrupted logs. A pre-defined set of SQL queries will be run across the new entries to compare them against a set of baselines and thresholds and search for potential attack or misuse events. For instance, it will list and total the entries for successful logins, failed logins, other failed actions, and policy changes. The output report will also include statistical information on the quantity, source and type of events logged across the network, and example would be HTTP errors in the 4xx and 5xx range from the Internet and intranet web server logs.

Logs will be cleared from local storage monthly via the 'dump' script. The centrally stored logs will be archived weekly and kept for two years.

The other type of activity-related information required is performance and activity metrics. Performance Monitor (PM) will be the primary tool used for this purpose within the SANS Co/GIACE network. PM will be configured on all the servers with a common set of counters related to the operating system, and an individualized set relevant to the applications being provided by that server. Used remotely to monitor the internal systems PM will communicate over SMB (TCP 445). For system on the DMZ allowing TCP 445 between the DMZ and the internal networks was deemed to open an unacceptable vulnerability, so PM will be configured to log the data to a file every 30 minutes and the 'dump' script noted above will FTP the new file back to a central repository for processing.

The PM logs will be parsed via a VBscript when they arrive at the central repository. The script will create a report detailing any critical or security related counters that have exceeded a set of pre-configured minimum and maximum thresholds. The script will also record any PM log files that are missing and send the details in an e-mail to the DMZ Administrators group.

3.2 System State and Configuration Information

Effective auditing of the system state and configuration requires having a baseline to

[5] Utility and description available with Microsoft's Security Operations Guide for Windows 2000. Refer page 124.

compare against. One of the baselines used within the SANSCo/GIACE network will be the Security Templates used to set the Group Policy settings. The services, drivers and open ports on the systems within the network will also be monitored and compared with a baseline taken from the system in a known clean configuration. At regular internals wider vulnerability assessment tests will be conducted to verify that the system controls and administration processes are producing the expected results and complying with industry best practices.

Group Policy Settings and Operating System Configuration

The command: 'secedit /analyze /db <databasename>' will be used to check the Effective Policy settings of a sample of the systems against a database of the combined security templates applied on that computer's OU Active Directory container.

The GPOTool utility will be used to check GPO information and integrity throughout the system. GPResult /c will also be used to view GP related statistics such as the list of applied GPOs, and registry and IPSec settings.

Services, Drivers and Ports

The *Svcmon* and *Netsvc* utilities will be used to detect the presence or absence of critical services locally and remotely. The *Drivers* utility will also be used to record the list of installed drivers for comparison against a baseline. All three utilities are available from the Win2k Server Resource Kit. The *Netstat –a* command will be used for a similar comparison of the open ports on the local machine

Critical Settings and Best Practices

The audit of critical settings is closely tied to the wider picture of configuring and managing the system in accordance with Best Practices. Some of the often-quoted ones for the Microsoft Win2K platform are (refer to the References section for sources):

- Microsoft Security Operations Guide for Windows 2000;
- NSA Windows 2000 Security guides;
- CI Security Benchmarks;
- SANS Top 10 Vulnerabilities in Windows Systems.

The SANS Co/GIACE Security Plan would be developed from these guides and kept up to date through assessment of the vulnerabilities and attacks notified in Microsoft and CERT advisories. Two simple tools to automate the audit of some of the best practices are Microsoft's Baseline Security Analyzer (MBSA) and Center for Internet Security's Security Scoring Tool. MBSA performs a series of checks for missing updates and common Windows, IIS, SQL and desktop application mis-configurations. The Center for Internet Security's Security Scoring Tool also checks for missing updates and many of the same Windows vulnerabilities. It does not perform tests on the IIS and SQL settings but has the advantage that it can be configured to test against any security template.

When Service Packs and Hotfixes are issued and have been thoroughly tested they will

be assigned to the relevant OUs via Group Policy and the Windows Installer Service.

The Windows File Protection databases will be kept up to date and used to ensure that operating system files are not modified. The *sysdiff* Resource Kit utility will also be used to create baselines of the file and registry settings on servers. These databases will be used to compare the current settings with the baseline if unauthorized access is suspected. The Tripwire host IDS[6] will also be installed on the critical internal and DMZ servers. It will be used to validate periodically and on demand, that critical operating system, application and static data files have not been tampered with. A scheduled batch file will FTP the Tripwire reports to the log repository on a daily basis.

There are also a number of third-party vulnerability assessment tools available that would check for other vulnerabilities. They include:
- Netrecon by Symatec[7],
- By-control by Bindview[8],
- Internet Scanner by Internet Security Systems[9], and
- SecurityAnalyst by Intrusion[10]

The vulnerability assessment tool selected by SANS Co/GIACE will be used to scan each of the SANS Co/GIACE domains every two to three months to check for many of the weaknesses the regular configuration tests cannot detect.

Once all the mechanisms and processes described above are in place, the SANS Co/GIACE management team will also schedule an outsourced vulnerability assessment and/or penetration testing exercise.

[6] http://www.tripwire.com/products/servers/functional.cfm?
[7] http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=46&EID=0
[8] http://www.bindview.com/Products/VulnMgmt/AssesmentandSecurity/bv-Control_Windows.cfm
[9] http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php
[10] http://www.intrusion.com/products/featureandbenefit.asp?lngProdNmId=4&lngCatId=5

References

Center for Internet Security, Security Scoring Tool and Documentation, Feb 2003, URL: http://www.cisecurity.org/bench_win2000.html (July 203)

Cunningham, Stace, et al, Windows 2000 Server Security, Syngress publishing, ISBN 1-928994-02-4

Lee, Rune, Designing a Secure Windows 2000 Infrastructure: GCWN Practical v3.1, Analyst 205, 2003, URL: http://www.giac.org/practical/GCWN/Rune_Lee_GCWN.pdf (July 2003)

Microsoft, Knowledge Base Article 330389: IE Stops Responding at "Download ActiveX Control" When You Try to Use a Certificate Server, URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;330389 (July 2003)

Microsoft, Knowledge Base Article 316347: IIS5: Hisecweb Potential Risk and the IIS Lockdown Toolkit, January 2002, URL: http://support.microsoft.com/default.asp?scid=kb%3ben-us%3b316347 (July 2003)

Microsoft, Prescriptive Guidance – Security Operations Guide for Windows 2000 Server, 2002, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/secwin2k/default.asp

Microsoft Technet, Windows 2000 Domain Architecture: Design Alternatives, Jan 2002, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ad/windows2000/plan/w2kdomar.asp (July 2003)

National Security Agency, Windows 2000 Security Recommendations Guides, 5 March 2003, URL: http://nsa1.www.conxion.com/win2k/download.htm (July 2003)

SANS, Top 20 Security Vulnerabilities, May 2003, http://www.sans.org/top20/ (July 2003)

Last Updated: July 23rd, 2017

Upcoming Training

SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
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**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**