Global Information Assurance Certification Paper

Case Study in
Security Controls Across Internal and Outsourced Environments

[GSEC – Assignment 1 version 2 [Option 2]

Jack C. Garrison, PMP

October 2003

CONTENTS

1 ABSTRACT

This paper, on Security Controls Across Internal and Outsourced Environments will present the foundation for an economical security model. The study will present a pre-solution environment description, where the IT department was outsourced. Next a picture will be painted on the decision processes used (including a security audit) to architect a co-sourced solution. Lastly, the "After Shapshot" environment will be described in greater detail. Objects and management points of: firewalls, routers, VPNs, Virus Protection, Mail Handling and servers with MS Active Directory/Exchange will be presented.

2 BEFORE SHAPSHOT

The Academy (corporation name changed) is a large Chartered school with two campuses located in Detroit, Michigan. On June 30th, 2003, the Academy discontinued the use of a management services provided by an outside service provider.[1]

The overall services included: total support administration, computer services, and technical infrastructure support. The computer services provided by an outside service provider were:

1. Management of computer server equipment located at two campuses (two mirrored schools)
2. Management of computer desktop equipment located at two campuses (two mirrored schools)
3. Access to email applications (physically located at previous management services provider).
4. Access to the internet (physically via the previous management services provider).

This re-insourcing led to an opportunity of challenging the old model of doing it all in house. The opportunity of redesigning the infrastructure practically yelled out "look at outside managed services". The requirements for security are slightly more complicated than constructing a new design as a review of previous security measures were required so as to identify existing vulnerabilities.

Over fifteen security related management points (objects) were identified and have been described in this paper for integration. Unfortunately, time and space will not permit the detail presentation of each item. Therefore, the focus will be firewalls, routers, VPNs, Virus Protection, Mail Handling and servers with MS Active Directory/Exchange in a shared management model.

2.1 Before Architecture

For purposes of simplicity, the following narrative descriptions will present only one of the two local campus data centers. As the two datacenter were identical in design and functionality, you can assume a 2X factor unless there is a need to differentiate due to shared or unique resources.

[1] Academy Project Charter, Garrison, Jack C. "Infrastructure Project Charter V1.2". 7 July 2003. 1-2. Available upon written request to mailto:jackgarrison@comcast.net

The before architecture (see figure 1) consisted of co-located servers physically located at a central site and two local campus sites. All servers were maintained by the managed service provider. The hardware at both sites were all of the Windows / Intel technology base with NT operating systems. The original equipment at the local site was:

- (2) Servers, IBM Netfinity 5600 xSeries for PDC & BDC. Additionally, the BDC housed a large local Student Information System database.
- Routers, CISCO 2600 (RAS) and CISCO MC3800.
- Switches, various CISCO gear to support LAN

The remote (central site at managed service provider) servers were of unknown type but they supported: All LDAP Authentication, DNS, Firewall, and DMZ requirements. All management of servers, peripherals, userids and passwords were handled centrally by the managed service provider.

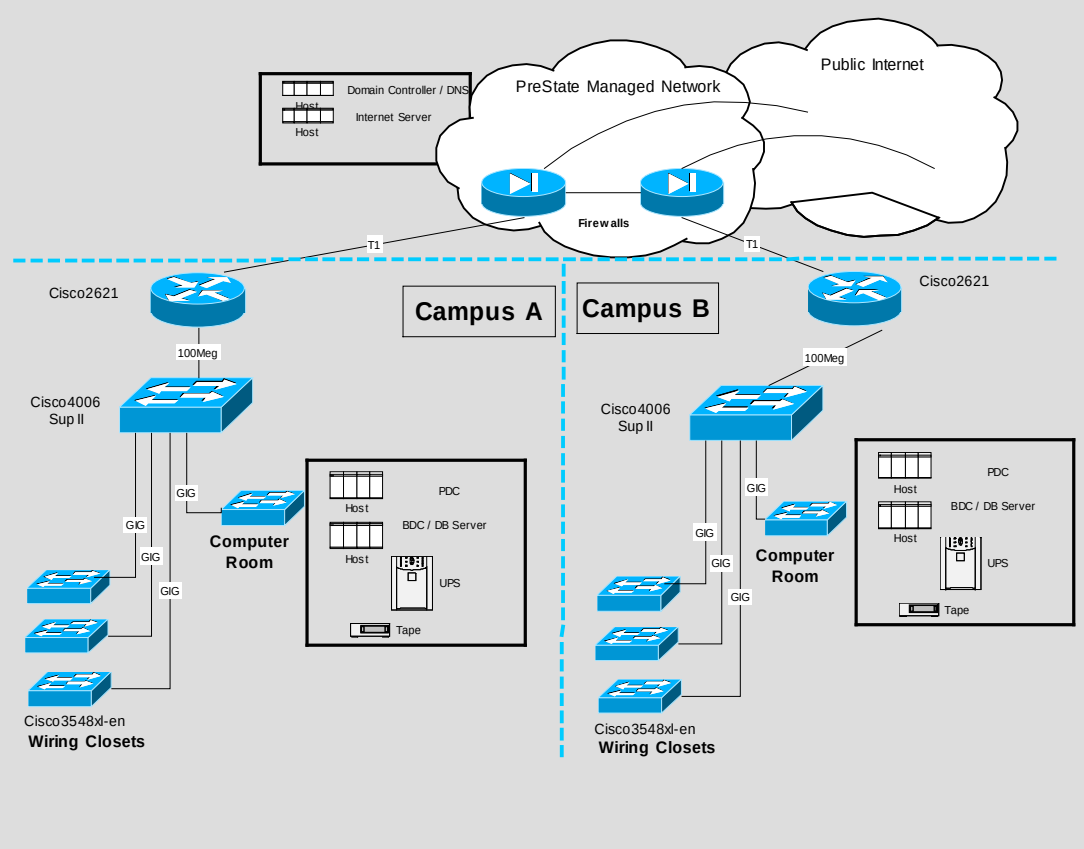

Figure 1

3 DURING SNAPSHOT

The following section describes the events and decision processes that went into the selection and recommendations of the solutions and approaches.

3.1 Network And Security Design Requirements

The network and security requirements as described by the customer were consistent with the goals of the original pre snapshot directions, they were:

- Provide Internet browsing access from every desktop
- Provide internally hosted email capability
- Provide external access to inside applications
- Support hosting capability of a public internet site
- Design and build the network and security at minimal cost and minimal staffing.
- Utilize only current Microsoft and Intel based technologies

3.2 Network And Security Audit Findings

A high level security audit was conducted to identify weaknesses and exposures of the old environment. The audit exceptions would then be the focus points for the new design.

A detail study of the Network infrastructure found one campus school computer network is downleveled in capacity (100Mbs vs Gigabit uplinks). Current problems exist and will become magnified by adding the required equipment (After Shapshot) unless corrected.

A detail study of previously implemented virus protection found that all virus patterns were out of date and new desktops viruses were infecting PCs. Therefore introducing vulnerabilities in Trojans, Worms, ect. (i.e. The MS Blast Worm negatively affected numerous efforts during August 2003).

A detail study of the remote access found dial inbound modem pools without strong authentication/encryption and 24 inbound lines per campus. Therefore introducing vulnerabilities in hacker attacks by simple brute force attempts.

A detail study found that all servers and desktops were at a backleveled operating systems environment (NT 4.0) without patch application. Therefore introducing vulnerabilities by not fixing known software bugs/exposures.

A detail study found that the internal management of userids and passwords were not using strong password design, were using shared userids/passwords and had very little encryption (NT 4.0).

A detail study found that content filtering was not being supplied to prevent the browsing by students of adult material. The Children's Internet Protection Act (CIPA) requires that public libraries receiving certain types of federal funding install a "technology protection measure that blocks or filters" access to obscenity, child pornography, and material harmful to minors[2].

A detail study found that data was not consistently being backup up nor were the computer servers consistently supported by uninterruptible power supplies. The

2 CIPA, "Title XVII Children's Internet Protection". 15 Dec 2000. URL: http://www.ala.org/Content/NavigationMenu/Our_Association/Offices/ALA_Washington/Issues2/Civil_Liberties,_Intellectual_Freedom,_Privacy/CIPA1/cipatext.pdf. (14 Sept 2003)

NFPA reports that up to one-third of fires begin in the electrical supply (surges, losses, drops). The two most common implementations are generators and UPS[3].

3.3 Network And Security Audit Conclusions

The above findings can quickly lead to the conclusion that every record and piece of information maintained by Academy using previous measures and technologies were at risk. One inappropriate release of student information to the public or one slanderous abuse from virtual pedophiles or publicized abuse of student pornography browsing, could in fact, damage the Academies reputation and therefore the trust of the parents and students. This Single Loss Expectancy, could therefore bankrupt the Academy. The SLE = Asset Value ($20,000,000 / Yr) * Exposure Factor (100%)[4].

3 SANS GSEC Course, Physical Security. 27 June 2003. Chap 6, pg 21

4 SANS GSEC Course, Risk. 27 June 2003. Chap 18, pg 12

4 AFTER SNAPSHOT (DESIGN OBJECTIVES)

The following high level design, component specifications and implementation directions will address the network and security requirements from the previous sections. Specific Vendor products are named in this list, but similar products may also be available from other vendors. The subsequent network diagram (see figure 2) will complete the picture.

Economic efficiencies have been introduced by collapsing multiple server and management objects points into one campus where ever possible. Additionally, the introduction of Externally Hosted managed services further improves the economic picture. Examples of the infrastructure that are specifically shared between the two campuses are:

- Externally Hosted and Managed firewalls
- One Exchange Server for both campuses
- One Intranet Server for both campuses
- One Virus Scanning server for both campuses
- One Active Directory with mirrored master implementation approach, one domain and one forest.[5]
- Inter Campus communication with secure VPN for backup
- Low cost of not increasing technical human resource by implementing cross campus administration responsibility

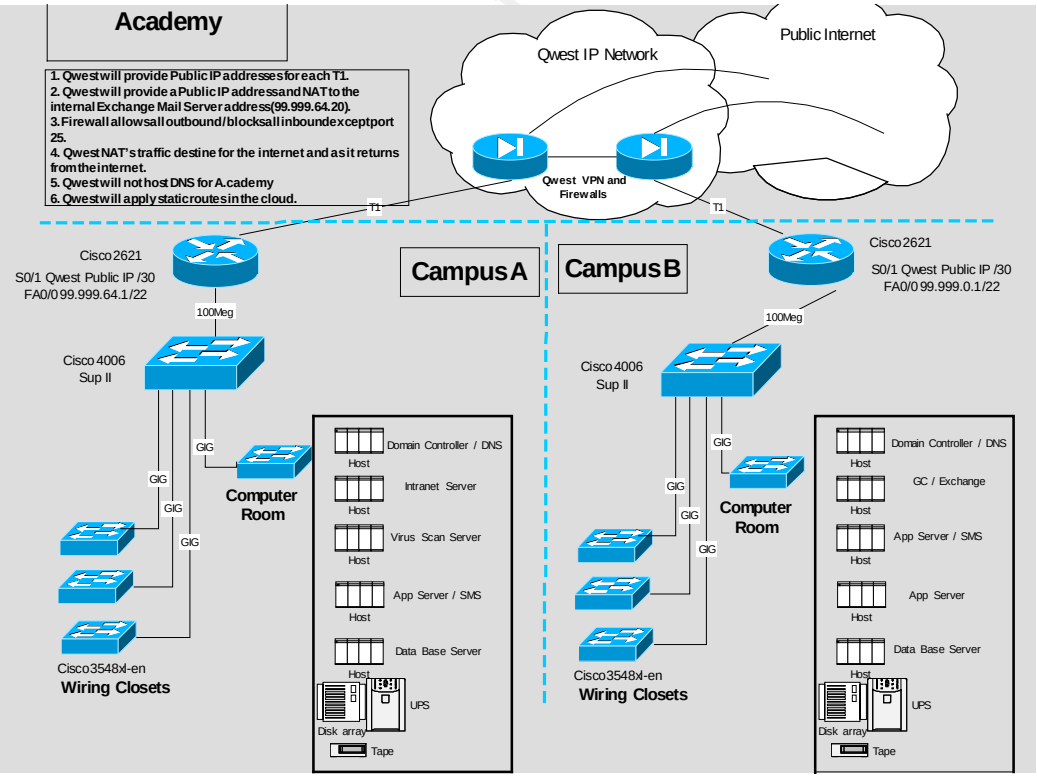

Figure 2

5 GSEC Course, Windows Security. 27 June 2003. Chap 25, pg 34

4.1 Detail Network And Security Design

The following description of Firewall, and Network settings will provide the detail of the security design. This description is deliberately not complete for security reasons.

The summary table at the end of this section will present a concise review of the security and management components. The following describes those key items in narrative form.

The connectivity from the local data centers to the Internet is provided by network access to the ISP (AT&T lines). It is secure connection via 1.5Mbs (T1) lines. Between the Internet and the T1 lines, a remotely managed Checkpoint Firewall is installed. The following Qwest citation further describes the firewall.

> The firewall provides: Controlled access to public internet sites, Limit access between Virtual Private Network (VPN) sites, Protection against unwanted intruders, Protection against denial of service attacks, Protection against common hacker threats, Provide audit trail of user activity, Complement encryption, network address translation and web steering functionality, and Provisions for future remote VPN access.[6]

At the local datacenters, local intrusion protection is provided via Cisco Routers with programmable firewall rules (see ACLs later in the paper). These rules define the restrictions of network routing, network protocols and server access points or ports.

A secure connection between the two campus data centers is provided by a VPN with the Internet Service Providers Network. This eliminates the need for private lease lines. This provides WAN connectivity between locations. It is implemented with a full-mesh (any-to-any) topology. Security between locations is provided using IPSec and 3DES encryption. [7]

Within the local datacenters, authentication is provided by Microsoft's Active Directory which manages userids, passwords, group policies, roles, and administration rights to these configurations. As PCs authenticate to the domain at login, the individual's access rights are shipped to the desktop in the form of certificate information.

Virus Scanning of servers, desktops, and email is implemented by integrating a virus server from Symantic. This is a Windows 2003 server application that continuously receives updates via the web from Symantic. It in turn scans all PCs that it finds on the local network for viruses on a weekly basis. Additional agents are automatically installed on the desktop or server to scan local files and email (live scan).[8] Note: Only PCs that are registered to the Symantic server are found by the server.

---

6 Qwest Managed Firewalls, Qwest Private Routed Network, Firewall Policies & Network Address Translation (NAT), Qwest Service- Customer Publication, pg 2

7 Qwest PRN, Private Routed Network (Network VPN), Qwest Service- Customer Publication. Pg 1

8 Symantic Antivirus Enterprise Edition, http://enterprisesecurity.symantic.com/products/products.cfm?productid=64&EID=0

4.2 Summary Table

Object	Component	Vendor	Implementation Directions	Reference or Comments
PHASE I				
Internet Network Access	T1 Circuits	Qwest ISP	Head in routers provided	Provided by AT&T
Internet Intrusion Protection	Firewall	Qwest	Managed Checkpoint Firewall Services at Qwest	Supported by Qwest
Inter- Campus Communication	VPN	Qwest	Virtual Circuits	Supported by Qwest
Local Intrusion Protection	Router / Firewall	Cisco 2621	Block numerous unsolicited ports	Local at each campus
Authentication	Userid / Password Mangement	MS Active Directory	One Domain, One Forest	Shared across campus
Desktop patch management	Distribution Tool	MS SMS	Underway	Shared across campus
Virus Scan PCs	Tool and update service	Symantic Antivirus Enterprise Edition	Scanned weekly	Shared across campus
Virus Scan Mail	Tool and update service	Symantic Antivirus Enterprise Edition	Live Scan	Shared across campus
Public Web Site	Hosting	Externally hosted	Maintained via FTP	Hosted offsite
Public Web Site	Access Security	Externally hosted	Maintained via FTP	Hosted offsite
Physical Security	Power Ergonomics Backup	New UPS Consolidated keyboards New Tape Vault	 Veritas Backup Manager	 Local at each campus

Object	Component	Vendor	Implementation Directions	Reference or Comments
PHASE 2				
Internet Usage	Content Filtering	N2H2	Under design	Local at each campus
Remote Access	Virtual Private Networking	Qwest	Under design	Local at each campus
Extranet	Separation of data	Multiple	Under design	Shared across campus
Vulnerability Scanning	Exposure Avoidance	Multiple	Under design	Local at each campus
Intrusion Detection	Incident Management	Multiple	Under design	Local at each campus

NOTE: The network and security specification design have been sanitized of specifically identifiable exposures (IP addresses) etcetera to avoid the risk of this document becoming a weapon of attack.

4.3 Device Access, Security, And Management

The following describes both internal and externally managed components. Externally managed devices are configured by request by the Internet Service Provider and internally housed devices are configured and managed locally.

4.4 Firewalls

The following description of Firewall, and Network settings will provide the detail of the security design. This description is deliberately not complete for security reasons. The externally hosted and managed firewalls (Checkpoint) provide these protections[9]:

- Controlled access to public internet sites
- Limit access between VPN sites
- Protection against unwanted intruders
- Protection against denial of service attacks
- Protection against common hacker threats
- Provide audit trail of user activity
- Complement encryption, network address translation and web steering functionality
- Provisions for future remote VPN access

9 Qwest Managed Firewalls, Qwest Private Routed Network
Firewall Policies & Network Address Translation (NAT), Qwest Service- Customer Publication. Pg 2-3

4.4.1 Firewall Security Services From Qwest

The following services are provided as part of the total managed service offering.

> Firewall security services are provided using a network-based, International Computer Security Association (ICSA) certified, stateful inspection engine, meaning that it not only inspects packets, but application flows. It extracts state-related information required from all application layers from the security decision and interprets these packets into "conversations." It tracks the types of connections that are made, and looks for any abnormal behavior in the conversation. This service also includes:
>
> Anti-spoofing/source address verification – The network-based VPN firewall inherently checks the source IP address of each packet. This ensures that no packet with an IP address of an RFC 1918 private address is coming into the network from the outside. It also ensures that any packets with a customer's IP subnet as the source address is only coming from inside that customer's network. This provides protection from hackers who try spoofing their IP address in order to appear as if they are a part of the customer's network.
>
> Denial of Service (DoS) Protection – The network-based VPN firewall inherently provides protection for a number of DoS attacks, including Distributed Denial of Service (DDoS) attacks, ping of death, LAND attacks, flooding attacks, etc. DoS protection blocks connections that are initiated from outside the VPN Network, unless configured to do otherwise.[10]

The customer provides input into the configuration of routers and NAT settings via a remote access web tool call QControl.[11] It provides the following functions:

- Integrated, Web-based service portal for Qwest customers
- View current network topology and current configurations
- Examine existing policies, e.g. firewall rule sets
- Requests re-configurations on-demand
- View performance
- Issue and manage trouble tickets
- View billing information electronically

10 Qwest Managed Firewalls, Qwest Private Routed Network Firewall Policies & Network Address Translation (NAT), Qwest Service- Customer Publication. Pg 4-6
11 Qwest Control for Private Routed Network Presentation. pg 2

4.4.2 Firewall Rules

The following table presents the firewall rules, the objects, and protocols.

Rule Number	Source IP	Source Subnet	Service/Port	Destination	Destination Subnet	Action (Accept/Reject)
1	Any	Any	Any	Any	Any	Accept (Outbound)
2	Any	Any	ESP 50	do.not.sho.219	255.255.255.248	Accept (Inbound)
3	Any	Any	AH 51	do.not.sho.220	255.255.255.249	Accept (Inbound)
4	Any	Any	UDP 500 (IPSEC)	do.not.sho.221	255.255.255.250	Accept (Inbound)
5	Any	Any	UDP 1645/1646 (Radius)	do.not.sho.222	255.255.255.251	Accept (Inbound)
6	Any	Any	Any	Any	Any	Reject (Inbound)

4.4.3 Cisco 2621 Routers

The internally managed routers have been configured to provide a higher degree of security as they are more accessible and can be more easily configured. All local Network devices can be accessed by Telneting to the IP address of the router or switch or by connecting to the console port using the Cisco serial cable and your favorite terminal emulator (such as hyperterm – 9600 8N1). The switches can also be accessed using http with a web browser. [12]

The Cisco 2621 Routers and the 29xx/35xx switches use the standard Cisco CLI (command line interface). The Cisco Catalyst 4006 Switches uses CatOS and "Set" commands

4.4.4 Router Access List (General Description)

Access list 100 (see 4.3.7) has been applied as an "inbound" access-list to the Fast Ethernet 0/0 interface on the 2621 Routers. This means that as traffic comes from the local LAN destine for anywhere else, the list will apply. The access list is unique for each site. The list allows internal users to utilize only the network resources, applications, and protocols that are on the approved list.

The access list has an "implied deny all" as the last entry. If network traffic does not match a previous statement, the traffic will be denied. New entries can simply be added on to the end of the list, however access-list logic must be

12 Cisco Switch, "Cisco 2621 Modular Access Router Security Policy".
URL:http://www.cisco.com/en/US/products/hw/routers/ps259/products_user_guide09186a00800a9604.html

maintained. Access list entries are interrogated in order from top to bottom. Once a match happens, the rest of the list is ignored. If the logic is such that a new entry must be in a specific place in the list (other than the bottom of the list), then the access list must be removed from the router and then re-applied in the correct order. Typically, a text editor and copy and paste is used to reorder and re-apply the list. These activities are typically done after hours because access list editing or removal may have adverse effects such as allowing all traffic or blocking all traffic

4.4.5 Archiving Configurations

Configurations should be archived periodically. For sites with tight control over who can make configuration changes, archiving can happen as changes are made. In other cases where configuration changes may be made by many individuals a script can be written to automatically archive the device configurations. Archiving is typically performed with a File Transfer Protocol server. A FreeWare TFTP server can implemented to accomplish this vital task.[13]

4.4.6 Router Access Control List

The following table presents the router access control list, the objects, protocols, and business usage behind each rule.

Access-list Entry	Usage
access-list 100 permit tcp any any eq telnet	Allow Telnet – required for router management
access-list 100 permit ip any host 10.160.64.1	Allow all traffic to router ethernet interface
access-list 100 permit ip any 10.160.0.0 0.0.63.255	Allow all Campus A subnets
access-list 100 deny tcp any any eq 135	Block port 135 (Blaster Virus) to everywhere else
access-list 100 permit tcp any any eq smtp	Smpt port 25
access-list 100 permit tcp any any eq pop3	Pop3 port 110
access-list 100 permit tcp any any eq domain	Dns port 53
access-list 100 permit udp any any eq domain	**DNS PORT 53**
access-list 100 permit tcp any any eq www	Web browsing port 80
access-list 100 permit tcp any any eq 443	Web browsing ssl port 443
access-list 100 permit tcp any any eq ftp-data	ftp data port 20
access-list 100 permit tcp any any eq ftp	ftp control port 21
access-list 100 permit tcp any any eq 123	Ntp port 123
access-list 100 permit udp any any eq ntp	Ntp port 123
access-list 100 permit tcp any any eq 161	Snmp port 161
access-list 100 permit udp any any eq snmp	Snmp port 161

13 TTFTP, "Ttftpd32's unsollicited installation". URL: http://tftpd32.jounin.net/ (14 Sept 2003)

access-list 100 permit tcp any any eq 162	Snmptrap port 162
access-list 100 permit udp any any eq snmptrap	Snmptrap port 162
access-list 100 permit tcp any any eq 554	Rtsp port 554
access-list 100 permit udp any any eq 554	Rtsp port 554
access-list 100 permit tcp any any eq 1209	Plato App port 1209
access-list 100 permit udp any any eq isakmp	Isakmp port 500 for ipsec vpn
access-list 100 permit esp any any	Esp port 50 for ipsec vpn
access-list 100 permit ahp any any	Ahp port 51 for ipsec vpn
access-list 100 deny icmp any 10.0.0.0 0.255.255.255 echo	Deny ping to private address space
access-list 100 deny icmp any 172.16.0.0 0.15.255.255 echo	Deny ping to private address space
access-list 100 deny icmp any 192.168.0.0 0.0.255.255 echo	Deny ping to private address space
access-list 100 permit icmp any any echo	Allow icmp to public
access-list 100 permit icmp any any echo-reply	Allow icmp to public
access-list 100 permit icmp any any administratively-prohibited	Allow icmp to public
access-list 100 permit icmp any any packet-too-big	Allow icmp to public
access-list 100 permit icmp any any time-exceeded	Allow icmp to public
access-list 100 permit icmp any any traceroute	Allow icmp to public
access-list 100 permit icmp any any unreachable	Allow icmp to public
access-list 100 permit ip any host 67.129.239.210	Allow communication to WAN port of Campus A router
access-list 100 permit ip any host 10.160.64.48	Allow communication to ip address of RAS connection for router “Manager”
Access-list 100 permit tcp host 10.160.64.20 any established	Required for the mail server to respond to external mail servers since inbound in destination port 25 but the reply from the internal mail server is source port 25 and destination port random

4.5 Userid Management

The entire userid management, password management, user group/policy management is implemented with MS Active Directory (AD). The design of a single tree, single forest approach is implemented for ease of management. As AD can manage upto 4TB worth of objects, the size of the academies, approximately 3,000 users will not be a concern.[14]

14 SANS GSEC Course, Active Directory. 27 June 2003. Chap 25, pg 26

For backup and fast local access (to each campus), a multi master Active Directory design is implemented. This will provide local access to user credentials, policies, ect, while maintaining (Move/Add/Change) the records across both locations.

As the Academies users will also include young students, a lower security password policy is implemented which does not require special characters and is short in length (8 characters).

Since userids and password management can be achieved by either location because there are multiple mirrored masters, it may be managed by a central help desk. The help desk staff have the authority and tools to create new users in active directory and at the same time create Exchange mailbox accounts.

5 CONCLUSION

A complete security requirement can be economically met with both an internal and external combination of services and measures. Security objects (Firewalls, NAS, and RADIUS Servers) which require intensive maintenance and monitoring is best serviced by the external service provider while those specific to the business (local Routers) can be serviced by the internal staff.

This infrastructure build project was formally managed using methodologies found in the Project Management Institute, Project Management Book of Knowledge.[15] Security is not free and the list of security objects identified in this report will represent a continuous matter of management and monitoring.

6 FUTURE EXPANSION

Time and space do not permit the detail presentation of all of the security design, but, the subsequent projects in the design implementation will be:

- Internet Usage (content filtering),
- Remote Access (VPN),
- Extranet
- Additional security management measures of Vulnerability Scanning and Intrusion Detection.

As the Virtual Private Network project will require a more complex security design, the outline of it will be presented in this section. Again an outside managed service provider will be provided as the cost model is extremely attractive (est $5.00/user/month).

An on-premise Contivity Extranet Switch (CES) will be inside the corporate firewall but will have one IP address that is public. Secure IPSec connectivity will be established from end-user PCs to that IP address.[16]

Externally hosted/managed RAS and RADIUS servers will provide the connectivity between the local CES device and the Internet. The VPN service is provided via a network-based security platform that resides in domestic and international TeraPoPs. The respective network operations centers (NOCs) have full visibility and control of the platform with 24-hour management.

[15] PMBOK, "The PMBOK Guide". 2000. URL: http://www.pmi.org/info/PP_PMBOK2000Excerpts.asp
[16] Qwest VPN, Remote Access Solutions, Qwest Service- Customer Publication

7 REFERENCES:

Academy Project Charter, Garrison, Jack C. “Infrastructure Project Charter V1.2”. 7 July 2003. Available upon written request to mailto:jackgarrison@comcast.net

Cisco Switch, “Cisco 2621 Modular Access Router Security Policy”. 9 Sept 2002. URL:http://www.cisco.com/en/US/products/hw/routers/ps259/products_user_guide09186a00800a9604.html . (7 Sept 2003)

CIPA, “Title XVII Children’s Internet Protection”. 15 Dec 2000. URL: http://www.ala.org/Content/NavigationMenu/Our_Association/Offices/ALA_Washington/Issues2/Civil_Liberties,_Intellectual_Freedom,_Privacy/CIPA1/cipatext.pdf. (14 Sept 2003)

Forest, GSEC Course, Windows Security. 27 June 2003. Chap 25, pg 34

N2H2, “Protecting Children Online At School”. URL: http://www.n2h2.com/products/bess_home.php . (7 Sept 2003)

PMBOK, “The PMBOK Guide”. 2000. URL: http://www.pmi.org/info/PP_PMBOK2000Excerpts.asp . (7 July 2003)

Qwest Dedicated Internet, “Managed Solutions “. URL: http://www.qwest.com/pcat/small_business/product/1,1354,979_3_9,00.html (7 Sept 2003)

Qwest Managed Firewalls, Qwest Private Routed Network Firewall Policies & Network Address Translation (NAT), Qwest Service- Customer Publication.

Qwest PRN, Private Routed Network (Network VPN), Qwest Service- Customer Publication.

Qwest VPN, Remote Access Solutions, Qwest Service- Customer Publication.

SANS GSEC Course, Active Directory. 27 June 2003. Chap 25, pg 26

SANS GSEC Course, Physical Security. 27 June 2003. Chap 6, pg 21

SANS GSEC Course, Risk. 27 June 2003. Chap 18, pg 12

Symantic Antivirus Enterprise Edition, http://enterprisesecurity.symantic.com/products/products.cfm?productid=64&EID=0 Note: URL not directly navagatable. (14 Sept 2003)

TTFTP, “Ttftpd32's unsollicited installation”. URL: http://tftpd32.jounin.net/ (14 Sept 2003)

Veritas, VERITAS NetBackup BusinesServer. URL: http://www.veritas.com/products/category/ProductDetail.jhtml?productId=nbbs Note: URL not directly navagatable (14 Sept 2003)

VPN, “Qwest VPN”. URL: http://www.qwest.com/pcat/small_business/product/1,1354,785_3_3,00.html . (14 Sept 2003)