Global Information Assurance Certification Paper

Implementing Security for Corporate Sensitive Network with Internet Access

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b
Option 2

By: Christopher Lee

August 15, 2004

TABLE OF CONTENTS

Abstract

An organization (let's call it Afirm) requires the setup of a corporate LAN and WAN with Internet access for its employees. Previously, the employees are working on an enclosed network with no Internet access. This setting up of an Internet LAN is a step towards embracing the Internet as an information source for all staff. Previously, Internet access is only limited to a few Internet kiosks that is shared among all employees. With the new Internet LAN, each employee will have his/her own terminal to access the Internet. The employee will also keep the terminal to access the enclosed network. Effectively, employees will have access to 2 physically separated networks using 2 different PCs.

This study captures the whole security enhancement process for the new Internet LAN. The scope of this case study is limited to recommending and implementing the security for this new sensitive network with Internet access, together with my involvement from start to finish. I would also share the experience gained, which I hope would contribute to all security practitioners in some aspects. This new network is expected to handle some sensitive information.

Before Snapshot

Background of Case Study

In an effort to go paperless and increase productivity, Afirm made a major move towards computerisation some years in 1995. Since then, every staff has a personal PC to work on. This is the main network that every staff works on. The company has data which is considered sensitive. The management was concerned about the sensitive information and is not willing to open the network to the Internet. Hence, the network is not connected to the Internet. It is an enclosed network that is not accessible outside the company.

Afirm is a research company with a staff size of a thousand. Afirm has its own IT department with staff doing Help Desk support, network and system administrations and support, as well as IT Security.

In order to facilitate email exchange with external companies and parties as well as an attempt to tap on Internet as a valuable information source, a small, simple network with Internet was put together just a few years ago. It was simply called Internet Network by everyone in the company. Internet Network was accessible via only a few terminals shared by every staff.

A re-organisation necessitated the need to revamp the entire Internet Network so that information with limited sensitivity can be processed on the network. I-Net* is the term coined by management for this new network.

A committee was formed to define the design principles for I-Net. I have been assigned to be part of the committee as a representative from IT Security Department. The design principles are necessary to determine the requirements of I-Net and to design the network. More important for myself, the design requirements will enable me to design and recommend the security of the network.

Design Principles for I-Net

1. I-Net refers to the network infrastructure that inter-connects the various centres of the company to one another.
2. I-Net is designed to facilitate:
   2.1. General office usage and collaboration among staff;
   2.2. Software development and product testing; and
   2.3. Internet access for all officers.
3. I-Net should provide a defined degree of “openness”. Security controls is focused more on detective controls than preventive controls.
4. I-Net shall be compliant with the company’s IT Security Policy.

5. I-Net is intended for information classified up to “Restricted” only. The transmission of information classified “Confidential” and above that needs to transmit across I-Net shall address the security requirements at the application layer.

My Role

As an IT Security consultant, I was blessed to be given the opportunity to assess, recommend and enhance the security in I-Net. A threat and risk assessment was first performed. Based on it, I proceeded to look at enhancing the network, system and client-side security. The security would implement preventive and detective measures. After the implementation, I was assigned to contribute to the I-Net policy and security awareness and education of users.

Threat and Risk Assessment

Based on the requirements, a security assessment was performed on the infrastructure of Internet Network. The objective was to examine Internet Network for vulnerabilities and identify areas that require security enhancement in order to support sensitive data processing in I-Net.

Network Security Measures

This section seeks to review and examine the network security measures of Internet Network. In Internet Network, there was only one tier of firewall using a three-pronged setup. This is not the most secure configuration as a single point of failure was present. Both the DMZ segment and internal user segment were connected to the same firewall. Application proxy was not enabled, hence clients had direct connection to the Internet.

Internet Framework also did not require any domain or network logon. As long as any user was able to log on locally, he was able to access the network and Internet. Hence, network access was not authenticated.

Email Security Measures

There was not email filtering nor encryption in Internet Network email system. There was also no email content filtering. Viruses, worms and spasm had free passage into the network.

System Security Measures

Systems were not patched to the latest security patches. There was no automated patch management system. Hence systems were vulnerable to both known and unknown exploits.

Anti-virus Measures

This section seeks to review and examine the anti-virus measures of computers in Afirm's Internet Network. In Internet Network, all computers were using virus scans residing locally in the hard drives. When new updates of virus definitions/signatures were available, the administrator would broadcast a reminder via email to all users to update their virus signatures manually.
The problem with Internet Network's anti-virus measure was that not all users will update their virus signatures immediately. Some users will delay updating because of other impending tasks at hand. Other users might have slipped their minds. Yet there were also others who ignored the email broadcast completely. For Internet Network PCs, since they are shared, no individual owner has been assigned to any particular PC. Anti-virus software without up-to-date signatures is ineffective against many newer aggressive worms and viruses. Hence, anti-virus protection and prevention is compromised. Loopholes are present for viruses and worms to exploit, thus spreading and infecting the systems.

Physical Security of Data Centre

The data centre physical security has been deemed sufficient with physical smart card access, CCTV, fire alarms. Hence, this section seeks to examine the security of the server racks in Afirm data centre. It was identified that physical security of the existing server racks in Afirm data centre is insufficient to safeguard sensitive servers. The vulnerabilities of the existing racks were found to be as follows:

- Lack of authentication. There is no authenticating mechanism to prove the identity of the person accessing the rack.
- Lack of accountability. All the server racks of the same model share the same master key. Every support officer was holding identical keys. This meant that every support officer can access all the racks in the data centre.
- Lack of auditability. There is no audit log to trace and check who access which racks at what date and time.

With the findings of the TRA, presentation was made to the management and my duty was to convince the management of the necessity for security enhancements if the management would like to process sensitive data in I-Net.

During Snapshot

Implementing Security for I-Net.

Security Approach – Defense In Depth
Based on the design principles, security policies and TRA, I proceeded to propose my security implementation approach to the management. I adopted the defense-in-depth approach. Defense in depth is based on the principle that multiple layers of different types of defense mechanisms from different vendors provide stronger defense. A vulnerability in one mechanism is only limited to its layer and will not be found in other layers. Even an apt hacker who managed to break through one layer of defense either by his familiarity with the intricacies or techniques of a particular vendor is only limited to that layer. It is highly unlikely that there is a hacker who is able to understand thoroughly the intricacies of all the security products in the market enough to break them.

Network Security

Perimeter Firewall

A firewall is a set of related programs, located at a gateway server, which protects the resources of a private network from users in other networks. Perimeter firewalls are designed to play a vital and core role to implement security at the border of a network. An understanding of the available firewall technologies is required to recommend appropriate firewall deployment. There are four main categories of firewall technologies namely [1] Packet Filters, [2] Application gateways, [3] Circuit-level gateways and [4] Stateful packet-inspection. More details of the above firewall categories are found in Annex A.

Perimeter Firewall - Justifications

- Perimeter firewall is able to enforce corporate security policy. It is able to restrict communications to what management has determined to be acceptable.
- Perimeter firewall is able to restrict access to specific services. Firewalls can even provide selective access via authentication functionality.

Perimeter Firewall – Requirements

- Perimeter firewalls should fulfil the justifications stated previously.
- All communications must pass through the firewall.

- Only traffic that is authorised will be permitted to pass through the firewalls.
- The firewall should be able to withstand attacks upon itself.
- The firewall should be able to log selected or all traffic that passes through it.
- The firewall should be able to alert the administrator of events.
- Appliance firewall is preferred. Appliances offer higher throughput because they are not burdened with the overhead of a multi-functional operating system. Appliance operating system is usually very small, usually a few megabytes in size. Other than higher throughput, such proprietary OS is more secure because it does not support unnecessary services and applications i.e. stripped down. Thus, it is less likely to possess a vulnerability.

Perimeter Firewall – Explorations

It is a good practice to implement multiple firewalls from different vendors in the same network. This reduces exposure to a specific flaw in the firewall itself. Some of the more well-known firewalls include:

- CheckPoint
- Cisco Secure PIX
- NetScreen
- Borderware
- Sidewinder
- CyberGuard
- SonicWall
- WatchGuard
- Symantec

In the exploration for suitable firewalls, the following criteria were considered:

- Evaluation Assurance Level. A brief write-up of the evaluation methodology of Common Criteria was attached in ANNEX B. Different brands and makes of firewalls are certified to different EAL levels. The higher the EAL, the more assurance it provided. As I-Net would be a sensitive network, I was inclined to go for higher EAL levels such as EAL4.
- Maximum Throughput. This is an important consideration. The throughput must be sustainable for the network segment the firewall is safeguarding.
- Maximum concurrent connections. This is also an important consideration to ensure least overhead when traffic is routed through the firewall.
- Operating system. This refers to the base operating system that the firewall sits on. Some firewalls are installed on Windows Server. Others have their own proprietary OS. Generally, proprietary OS provides more security as there is no unnecessary services and components, thereby reducing vulnerabilities and overheads.
- Maximum Interfaces. The interfaces the firewall support, the more network segments it can separate. However, the maximum throughput should also be taken into consideration.

- Remote management capability. This feature allows the firewall administrator, in this case the network administrator, to manage the firewalls remotely from a single location.
- VPN capability.
- Failover support.
- Firewall technology. This refers to core engine of the firewall. Depending on the purpose and usage of the firewalls, each of the four firewall technology (Discussed in ANNEX A) has its pros and cons. In terms of security, proxy firewall is the highest as it does not allow the client to have direct connection with the server.
- Proxies available. Proxy firewalls do not allow the internal client to make a direct connection to an external server. The proxy functions as man-in-the-middle and speaks to both the client and server, relaying their messages back and forth. Different brands of firewalls support different proxies. Based on the usage requirements, the selection was made to identify the firewall that supports the required proxy services.

Perimeter Firewall – Implementation

The 1-tier firewall configuration in Internet Network was changed to a 2-tier setup. DMZ segment resided between the first and second firewalls of different makes. This is so that in the event that a vulnerability is discovered, the same vulnerability would not be duplicated in the second firewall.
Configuring and installing a firewall may not be a straightforward task. As a firewall administrator, he needs to be very familiar with the workings of the firewall. In Afirm, the network administrator has been assigned as the firewall administrator. An IT Security consultant like me is not aware of the network services requirements and I also do not have a need to know. My role is in the selection and recommendation of firewalls. To balance operational needs and security needs, I recommend the network team to support more than one brand of firewall but not more than three brands. I arranged for product presentations and demonstrations. I put up evaluation reports and finally liaised with the vendors to put up the purchase. I arranged courses for the firewall administrators to attend. Once the firewalls were fully deployed in production network, I would handover to the network team any future purchases and renewal of contract.

Network Access Control – Justifications

- Network Access Control is a basic means to prevent unauthorised access to the network.
- Unauthorised network access could translate to the network being compromised, resulting in loss of confidentiality, integrity and availability of data.

Network Access Control – Requirements

- Users should require to log on in order to access network resources such as Internet access and file and print servers.
- The password for log on should have a complexity base-line.

Network Access Control – Implementation

- The management had decided to require users to log on to Windows Domain.
- Password policy was enforced via Group Policy of the Windows Domain.
- As the domain controllers are critical to the availability of the network, both primary and backup domain controllers had to be set up.
- All client machines were configured to disable local user account creation. That way, all users will be required to access the domain.
- The Internet firewall was then configured using LDAP to allow only domain authenticated users to access the Internet.

Email Security

The enhancement of email security was a major architecture to implement and was assigned to another project team from mine. Hence, I could only touch briefly on the implementation to my best knowledge.

- Remote POP3 mail access is disabled. Remote mail access is only viable via SSL HTTP. Server and client side certificates are configured to authenticate the client and server to each other. The purpose is to prevent sensitive email from being downloaded to an unauthorised remote system.
- PGP mail was implemented to provide encryption for sensitive email.
- Content filtering was implemented to block high risk attachments such as .PIF files.
- Spam filtering was implemented to block spam emails at the server end.
- Antivirus was implemented on the mail servers to scan all incoming and outgoing emails.

Antivirus Gateway – Justifications

- Viruses and worms should be stopped at the gateway before they even have a chance to enter the network.

Antivirus Gateway - Requirements

- Hardware appliance solution is preferred for gateway virus scanning as it is hardened against attacks and less configurations required.
- Solution should be able to sustain the throughput of the network.
- Solution should be able to support inline mode and be able to scan HTTP, FTP traffic.

- Solution should be a different brand from client-side antivirus solution. This provides a multi-vendor approach.

Antivirus Gateway – Exploration

No.	AV Gateway Finalist A	AV Gateway Finalist B
1	Able to to scan HTTP, FTP, SMTP and POP3.	Able to scan only FTP and HTTP.
2	Able to sustain a high throughput of 2MB/s.	Unable to sustain throughput of 2MB/s/ Requires load balancing to meet throughput requirements.
3	Provides content filtering.	Does not have content filtering.
4	Able to be deployed as inline or proxy solution.	Able to be deployed only as proxy solution.
5	Each server is able to manage up to 250 000 clients.	Each server is able to manage up to 3000 clients.
6	Able to generate graphical reports as well as tabular statistical reports.	Unable to generate graphical reports. Only able to generate tabular statistical report.
7	Does not require server groups. Individual clients can be managed with same or different policies.	Management requires server groups. Servers and clients must be in a group, and all machines in a group must use the same policies.

System Security

System Security pertains to the protection of servers as opposed to Client-Side Security which pertains to the protection of end-users' PCs and notebooks.

Antivirus Solution (Server)

- As there is already a gateway antivirus to be put in place which is of a different brand from client-side antivirus, it is recommended that the servers implement the same centrally managed antivirus solution as client-side antivirus solution. This arrangement provides effective management as too many different brands of antivirus may make it operationally inefficient.

Patch Management System (Justification)

- Systems with up to date software and operating system patches are required and necessary to address the vulnerabilities present.
- Many exploits, such as Blaster Worm, are so successful and creating a large impact to the world only because there are un-patched systems all over the world.

Patch Management System (Requirements)

- Solution should be able to patch all systems transparently without user intervention.
- Solution should provide roll-back function if the new patch causes systems to become unstable.

Patch Management System (Implementation)

- The management decided to implement Microsoft's SUS solution.
- It is a simple, low cost and straightforward solution.
- Patch deployment are randomised to prevent choking up of network bandwidth.

Client-Side Security

Antivirus Solution

Antivirus Solution – Justifications

- Antivirus is the most fundamental and core defence against known viruses and worms which makes up the majority of malicious codes in the world.
- Viruses and worms have varying degrees of impact on the organisation from a little inconvenience and nuisance to devastating information theft and destruction or system and network disruption.

Antivirus Solution – Requirements

The requirements are as follows:

- It should be centrally managed.
- It should be able to force every system in I-Net to update its virus signatures.
- Updating of signatures should be done without any user intervention and be transparent to users.
- Users should not be able to disable the antivirus software on their computers.

Antivirus Solution – Exploration

With the requirements defined, I proceeded to explore the various brands of antivirus solutions. There are many antivirus vendors worldwide such as Norton, McAfee, Sophos, Panda, BitDefender, Kaspersky, F-Secure, RAV, Avast, Trend Micro, Vexira and BitDefender. The shortlisting process follows after.

Upon discussion within IT Security Centre and feedback from the management, the following process of shortlisting was determined as follows in order of sequence:

- Local sales and technical support. The management of Afirm prefers products with local support. It is because this means assurance for more responsive assistance from the vendor.
- Check that shortlisted products meet requirements via paper exploration and meeting with vendors. After identifying the antivirus vendors with local support, I verified that the shortlisted antivirus products meet our requirements by going online to check their product features and specifications. The shortlisted vendors were also contacted for a product presentation and demonstration.
- Attitude and product knowledge of the pre-sales team. This criterion plays an important role in shortlisting the vendor. A vendor with a sincere, responsive and enthusiastic team is likely to provide good after-sales service especially if implementation and integration is done by Afirm's in-house staff.
- Reference customers. The management is also interested to know who are the users using the shortlisted products. Particular emphasis is placed on local large enterprises such as tertiary educational institutions, financial institutions such as banks, and government departments and institutions. If a product is being used by these large enterprises, Afirm's management would have higher comfort level and assurance to go for these products. After all, these are credible success stories and hence it is likely that the product is of good quality and high standards that it is adopted by large enterprises. In addition, with a large customer base, it is less likely that the vendor will be out of business, thus ensuring that Afirm's investments in the product will give returns.
- Total cost of ownership. This includes the initial setup costs and recurrent maintenance support. In every organisation, cost is a determining factor of the choice of solution. A tentative quotation is obtained from the shortlisted vendor at this point.
- Additional features that extend beyond the basic requirements.

After the shortlisting process, two finalists emerged. Hence the additional features were compared. The results are tabulated in the table that follows:

No.	Antivirus Finalist A	Antivirus Finalist B
1	Multi-platform. Supports Windows, Linux, HP-UX, SCO, AIX and Solaris.	Only supports Windows platform.
2	Solution able to scan HTTP traffic.	Unable to scan HTTP traffic.
3	Supports clustering and Microsoft Terminal Server environments, hence product is scalable.	Does not support clustered servers.
4	Thin client available requires only 10MB of storage on client machines.	No thin client. Installation requires 40MB of storage.

5	Attachment blocking feature and attachments are specified in the administrator console.	Attachment stripping instead of attachment blocking.
6	Able to generate graphical reports as well as tabular statistical reports.	Unable to generate graphical reports. Only able to generate tabular statistical report.

Other than the above, Finalist A has also more virus research offices worldwide and more virus researchers in the world than Finalist B. This is seen to be an advantage as it can be translated to prompt release of virus signatures. With that, Finalist A was recommended as a potential solution for the next stage of implementation.

Antivirus Solution – Implementation

After the Product Exploration Stage came the Product Implementation Stage. This stage entails three main phases. Phase 1 is Proof-Of-Concept. Phase 2 is Pilot Deployment and Phase 3 is Full Deployment.

Proof-Of-Concept Phase

A Windows 2000 server was set up and installed with the antivirus server software. Workstations running various client OS were also set up. Other than the OS, each workstation was also installed with all the standard authorised software in each office-issued system. The antivirus client agent was then installed on each workstation. The agent can be deployed through the antivirus console using “Push” technology, login script or email. All the three methods were attempted successfully. After the agent was installed successfully, the agent was able to ‘pull’ the antivirus client installation file from the antivirus server and install on the client. After which, the antivirus client is able to ‘pull’ the virus signature update from the server. Hence, the antivirus solution is shown to be transparent to users.

The policies for the agents were configured centrally from the server. Both group policies and individual policies were configured and tested. Each workstation was monitored to ensure that the agent was communicating with the antivirus server. The monitoring was done via the agent monitor on the client and the reporting console on the server. Both workstations and servers were remotely configured to install the antivirus software automatically.

Mock viruses, downloaded from EICAR.COM, were detected successfully on workstations and reflected back to the server. Graphical reports were generated successfully on the server showing accurately the status of all the antivirus clients.

Pilot Deployment Phase

After Proof-Of-Concept, purchase order was issued to purchase brand new server with specifications that can be optimised by the antivirus and be scalable to manage more clients in future. As the antivirus server was not time critical and able to tolerate some downtime, High Availability pair was not deemed necessary. With the management approval, I proceeded to acquire a server hardware with

redundant power supply and RAID 5 setup. These were cost effective features to minimise incidents of downtime and improve data recovery time.
The antivirus vendor specifications had claimed that one antivirus server was sufficient to handle the load of the entire staff of Afirm. To verify, only one server was installed in pilot phase. The CPU and RAM utilisation was monitored regularly. If it could be verified that one server could manage all the nodes within Afirm, it is an advantage as it is easier and more efficient to manage one server.

Communication ports had to be opened in the necessary firewalls for the antivirus agents in other network segments to communicate with the server. One good feature that I discovered was that the TCP port that agents used for communicating to the server can be configured. Hence, I proceeded to configure a lesser known port instead of the default common TCP port.

Some pilot users with slower computers and a meagre RAM capacity had feedback slower performance after the antivirus agent was installed. This was an important discovery in the Pilot Deployment Phase. The product specifications had claimed that these slower computers of Pentium II with 32MB RAM, were able to support the antivirus software. If this had not been discovered, the availability of the computing resources would be affected. Hence, this was reverted to the management for further action. The management decided to phase out some of the older systems and upgraded the RAM of some newer systems.

Full Deployment Phase
Before full deployment, all Help Desk officers were scheduled for introductory courses on the antivirus server and client so that they would be well aware of the functions and capabilities of the antivirus solution. To prepare Help Desk officers for supporting logged calls from users pertaining to the antivirus solution, Help Desk officers was the first batch to have the PCs installed with the antivirus agent and client. In this way, Help Desk officers would have ample time to support user calls.
Full deployment was also scheduled in batches according to departments. Prior to each deployment, email announcement was sent to all informing users of the implementation. The email also included a brief introduction to the antivirus solution. Throughout the full deployment phase, the antivirus server was monitored for its CPU and RAM utilisation to ensure that it had enough resources to manage the clients.

Personal Firewall

A personal firewall is a piece of software or hardware that helps screen out hackers, viruses and worms, which attempt to access another computer over a network such as Internet. If a system is not protected when connected to an untrusted network such as Internet, hackers can gain access to personal information on the computer and install codes for their malicious purposes.

Hackers can also use the compromised computer as a platform to launch attacks on other computers in the network.

Personal Firewall.- Justifications

- Personal Firewall is effective against spyware. Spyware is known to be evasive. It is able to avoid detection by anti-virus software. Spyware gains access to a system through everyday tools such as web browsers and downloaded via HTTP ActiveX, Instant Messaging, streaming audio and video and a variety of other third party programs.
- Personal firewall complements antivirus software. Traditional antivirus software is reactive by nature as it relies on databases of known viruses. Antivirus software is also limited by latency of its signature, recognising only known viruses.
- Personal firewall complements perimeter firewalls which may not be effective against spyware since spyware originates internal.
- Personal firewall complements intrusion detection systems which may not have signatures to detect all spyware activity on a network.
- Personal firewall complements anti-adware software which may also be unable to detect all spyware.
- Personal firewall mitigates security risks such as port scanning, Trojan horses and other forms of malware.
- Personal firewall is able to protect a computer and prevent it from being used to attack other computers with the owners' knowledge.
- Personal firewall is able protect against computer worms that are transmitted over the network. A computer worm is similar to a virus, but is self-contained and can spread without the help of other programs.
- Personal firewall is able to protect against unauthorised access by hiding the protected computer from external users and preventing unauthorised connections to the computer.

Personal Firewall - Requirements

The requirements are as follows:

- It should be centrally managed. Personal firewall policies should be able to be centrally configured and transmitted to the personal firewall clients. This helps to enforce the company's security policy.
- It should be able to detect all applications and services utilizing the network, allowing administrators to permit or deny applications and services accessing the network. This is also a centralised application monitoring measure.
- It should be as transparent as possible to users. Firewall alerts should be allowed to suppress centrally by the administrator so that users are not required to respond to the alerts. There are non-technical users who are not familiar with the use of personal firewalls. Users should not be made to

respond to alerts from the personal firewalls. From experience, many standalone personal firewalls such as ZoneAlarm (Free Edition), Outpost, Sygate, Kerio, etc…are limited in their success to prevent intrusions because non-savvy users simply click to allow whatever traffic to pass through. The main concern of these users is that their systems are working fine so that they can continue their work. Security is seldom on the top priority.

- It should be able to generate reports to make it simple and time efficient for administrators to review security policies.

Personal Firewall – Explorations

After the requirements are determined, an exploration was initiated. First, we need to shortlist a few personal firewalls to explore further. The more well-known personal firewalls include:

- Zonealarm
- Sygate
- Kerio
- Outpost
- McAfee
- Symantec
- Outpost
- BlackIce

The personal firewalls were shortlisted based on the requirements, user experience in the proof-of concept.

Personal Firewall – Implementation

- All machines were configured in a consistent manner.
- Clients were configured such that they are unable to shut down or uninstall the firewalls.
- Server applications on the clients were denied network access by the firewalls.
- Client applications were monitored centrally and applications deemed to be high risk were denied network access.

Physical Security Measures

Server Rack Access Control - Justifications

- As sensitive information is processed on I-Net, some servers will be expected to handle sensitive information. Access to these servers should have stronger authentication, accountability and audit capability.
- The sensitive are normal servers and the SCSI hard disks can be easily removed and replaced once intruders manage to access the server racks.

Server Rack Access Control – Requirements

- User-based access control, not role-based. A system administrator of one sensitive server may not have a need to access another sensitive server in another rack. This is implementing Least Privilege principle. Access control should be authenticated.
- Time-based access control. A system administrator who is not on duty should not have access to the sensitive servers round the clock.
- Access logs should be implemented to log down name of user, time, location and specific rack access.
- Solution should be fault tolerant such that locks remain activated and operational in the event of power irregularities.
- Solution should be scalable for further expansion.
- Audit log access control. /audit logs must be logged centrally and secured to prevent tampering. Only authorised and designated officer shall have access to the logs.
- Solution should provide monitoring mechanism to alert duty personnel when abnormal events or intrusions are detected.
- Solution should have option for 2-factor authentication when required.
- Solution should be able to detect unclosed rack doors, tampered rack panels in real time and relevant monitoring parties shall be alerted in the event of abnormal events and incidents.

Server Rack Access Control – Explorations

Various solutions were explored including:

- Physical lock and key
- Cyberlock
- Smart Card and Electronmagnetic lock.

Physical lock and key provides an inexpensive solution. Individual rack will have individual locks with unique keys. However, operation and management of the keys is a daunting task. Keys can easily be lost, stolen and duplicated.
Cyberlock is a much improved solution than physical lock and key. However, it is not suited for all sorts of server racks because implementation requires replacing the original rack lock with Cyberlock cylinder. Hence, restriction is caused by the dimension of the server racks.
Smart card solution is the most costly of the three solutions. It provides the highest security. It provides ease of key management such as key creation, revocation and configurable access control. Time-based access can be programmed. Smart cards are not easily duplicated as contents are encrypted. Audit logs can be implemented. It is scalable. Accountability is implemented as each smart card can be traced to individual owners.

Server Rack Access Control – Implementation

The implementation was outsourced to solution provider.

After Snapshot

After the security enhancements are implemented, I-Net is ready for use. The efficacy of the security implementations is affirmed by the IT audit findings and Help Desk call statistics. There are fewer flouts of the security policy. There are less logged calls on virus infections. User survey is initiated to gather feedback on their experience of I-Net usage.

Limitations of the Security Implementations

Perimeter Firewall - Limitations

- Firewall cannot protect against what is authorised.
- Firewall is only as effective as the configured rules.
- Firewall cannot stop social engineering or an authorised user intentionally using his access for malicious purposes.
- Firewall cannot fix poorly administrative practices or a poorly designed security policy.
- Firewall cannot stop attacks in which traffic does not pass through them.

Personal Firewall – Limitations

- Personal firewalls are unable to protect against viruses that spread through emails.
- Personal firewalls may also not be effective against Trojan horses, which masquerades as helpful and benign software and trick you into opening or downloading them. The personal firewall also cannot prevent spasm.
- Application and software list. Administrator is still required to manually monitor the list of applications and software allowed to access the network.

Antivirus Solution – Limitations

- Other malicious codes are spyware, and other little-known unreleased programs such as backdoor programs are not effectively detected by antivirus software.
- Fine tuning of policies. The antivirus agents are further configured to provide a balance between PC resource overhead and effectiveness. An example of such configuration would be the agent to server communication interval.

User Awareness and Education for I-Net

After the successful security implementations in I-Net, the next step is to increase user awareness. Hence a security newsletter is initiated. The newsletter is written in a non-technical fashion. The contents included security policy matters, security tips, security technology updates, stories on security breaches. To improve the readership of the security newsletter, quizzes with attractive prizes are given out. The next initiative is the issue of security advisories whenever a high profile vulnerability or virus is discovered.

Future Security Implementations

With the setup of I-Net and considering the huge expenditures so far on security, the management proves to be well-aware of security risks and is convinced that security is an investment and not expenditures. Even though after the above security enhancements, I-Net has been proven to be more secure than the defunct Internet Network, future implementations would still be necessary to handle the increasingly complex hacking attempts in the world today and future. One potential future implementation I would recommend the management to put forth would be Intrusion Detection System (both network-based and host-based). The purpose is to detect unauthorised network and system access and usage. Some of the considerations for the deployment of IDS would be to dedicate personnel to consistently monitor them. IDS is also known to have high false positives if they are not tuned or configured properly. Setting up IDS requires extensive fine tuning to provide the results we want.

Another potential future implementation that I would propose to the management is Web Content Filtering and Usage Monitoring. This is a gateway security to log and monitor all web traffic including file uploads and downloads. One advantage is that this would allow administrators to trace the Internet source when a system gets virus infection while visiting a website. High risk scripts such as ActiveX may also be blocked, subject to management approval. This implementation can also enforce the company's security policy by URL filtering as well as by site category such as gambling and pornography sites. Streaming media traffic can also be restricted or limited by time or network bandwidth. This ensures the availability of bandwidth for legitimate office usage.

ANNEX A: Descriptions of Various Firewall Technologies

1. Packet Filters

- A packet filter operates at Layer 3 of the OSI layer (Network Layer) and is an integrated feature of many mid-range and high-end routers. Packet filters perform the most basic of operations. It relies on the existing architecture of data transfer, which uses packets that contain headers with IP addresses and protocol ports to send them across networks to their intended locations. The packet filter examines the header of each packet it encounters and then decides to pass the packet to the next hop along the network path or denies that forwarding, either by dropping the packet or by rejecting it. The decision is based on a set of rules defined by the firewall administrator. The rules can be based on information such as the following:
- The source IP address, or a range of IP addresses, that the packet originated from.
- The destination IP address or a range of IP addresses, where the packet is heading.
- The network protocol involved (for example, TCP, UDP, or ICMP).
- The port number being used. This also typically identifies the type of traffic (e.g. port 80 for HTTP, which is web traffic).

Advantages of packet-filtering firewall:

- It creates little overhead, so the performance of the screening device is less impacted, resulting in very fast performance.
- It is relatively inexpensive or even free with most routers.
- It provides good traffic management.

Disadvantages of packet-filtering firewall:

- It allows direct connections to internal hosts from external clients.
- It leaves many holes in the network perimeter. It leaves holes because it can only examine traffic at the transport layer (TCP or UDP) or at the network layer (ICMP or IP protocol type). A packet filter cannot verify that the upper layer is permitted to pass. Although a packet-filter firewall can determine that an incoming HTTP request should be permitted, it cannot determine whether the user is a valid user or an intruder, and it cannot determine whether the HTTP is a valid request or an attempt to exploit inherent buffering vulnerabilities in many web server implementations.
- It is difficult to manage and scale in complex environments. In a Defense-inDepth environment, all packet filters in both network traffic directions must be synchronised.
- It is vulnerable to attacks that "spoof' source addresses.
- It offers no user authentication.
- It cannot monitor the status of connections.

2. Application Gateway (Proxy) Firewall
An application gateway is also known as proxy firewall. It operates at Layer 7 of the OSI layer (Application Layer). Proxy servers use software to intercept network traffic that is destined for a given application. The proxy recognised the request, and on behalf of the client makes the request to the server. In this case, the internal client never makes a direct connection to the external server. Instead of a direct connection, the proxy functions as man-in-the-middle and speaks to both the client and server, relaying their messages back and forth.

Advantages of proxy firewall

- Proxy firewalls do not allow any packets to pass across them. With a proxy, the web browser connects to the proxy, then the proxy connects to the web server. The web server sends its response to the proxy, which then sends the web pages to client. With a proxy, the browser is never connected directly to the server.
- Proxy firewalls provide the best security among the 4 types of firewalls.
- Proxy firewalls permit or deny traffic by the actual data in the packet, not simply the header. In other words, the proxy is aware of communication methods, and will respond accordingly, not just open and close a port in a given direction.

Disadvantages of proxy firewall

- Each service requires a proxy, so the number of services may be limited.
- Proxy firewalls have the lowest throughput.

3. Circuit-Level Gateways

Circuit-level gateways operate at Layer 4 of the OSI layer (Transport Layer). Circuit--level gateways operate in a method that is similar to application gateways but typically are oriented more toward non-interactive applications. Proxy servers and SOCKS servers are typical examples of circuit gateways. Circuit gateways operate by relaying TCP connections from the trusted network to the untrusted network. In the process of relaying, the source IP address is translated to appear as if the connection is originating from the gateway.

Advantages of Circuit Gateways

- Better security than packet filters.

Disadvantages of Circuit Gateways

- As most circuit-level gateways are configurable on a TCP port basis, it may not examine each packet at the application layer. This allows applications to utilise TCP ports that were opened for other, legitimate applications. Several peer-topeer applications can be configured to run on arbitrary ports, such as TCP 80 and TCP 443 (commonly opened for web browsing). This opens the possibility for misuse and exposes potential vulnerabilities inherent in these applications
- Inbound connections are, in general, not allowed, unless the functionality is built into the gateway as a separate application. Some client applications cannot be

modified to support SOCKS or proxying. This would prevent them from accessing external resources through a gateway.
- Not secure for inbound traffic.
- Circuit gateways leave the port open until a connection is terminated.
- No examination of application information.
- Lower performance than packet filter firewalls.

4. Stateful Packet Inspection (SPI)

SPI-based firewalls combine the speed and flexibility of packet filters with the application level security of application proxies. This merging results in a compromise between the two firewall types: an SPI firewall is not as fast as a packet-filtering firewall and does not have the same degree of application awareness as an application proxy.

A stateful packet inspection firewall operates by examining each packet as it passes through the firewall and permitting or denying the packet based on whether it is part of an existing conversation that has previously passed through the firewall or based on a set of rules very similar to packet-filtering rules. The difference with packet-filter is the way SPI examine the packet. SPI maintains a connection table of existing and valid connections to prevent packet-spoofing.

Advantages of SPI firewall

- The connection table greatly reduces the chance that a packet will be spoofed to appear as if it were part of an existing connection. Packet filtering firewall do not maintain a record of the pending communications, they must rely on the format of the packet - status of SYN bit in a TCP packet.
- SPI is able to look into data of certain packet types such as FTP and SMTP protocols. The inspection feature examines the data of a packet to determine the validity of the command.

Disadvantages of SPI firewall

- A SPI firewall does not protect the internal hosts to the same degree as an application gateway firewall, because it simply looks for specific strings within the data portion of the packet.
- In addition, it does not act as a proxy or set up a separate connection on behalf of the source.

5. Appliance Firewalls

A firewall appliance is a device that has hardware and software optimised specifically for its function -- examining traffic that is passed to it to determine whether it should be forwarded. A firewall appliance sometimes stores the OS and other software on a chip or flash card. High-end firewall appliances offer extremely high throughput, because they are not burdened with the overhead of a complex, multifunctional operating system. The operating systems are very small, usually a few megabytes in size. Appliances are typically configured through the command-line interface, a proprietary tool, or with a web-based interface running over HTTPS. Appliances integrate the operating system and the firewall software to create a fully hardened, dedicated firewall device. The integration

process removes any and all functionality not required. In addition, a fully functional administrative interface is provided to further simplify configuration and maintenance of the firewall. Firewall appliances do not require a significant amount of hardening when being deployed. Administrator is just required to change the default password. Administrators can just focus on developing rule sets instead of reconfiguring and patching a general purpose operating system. Appliances significantly reduce operating and maintenance costs over operating system-based firewalls.

ANNEX B: Evaluation methodology of the Common Criteria

The following was extracted from http://www.itsecurity.com/papers/border.htm. *Article was written by Peter Cox, Vice President of European Operations, BorderWare Technologies Inc.*

Evaluation methodology of the Common Criteria

"The underlying measures of the Common Criteria are based on functional and assurance requirements of a security product. Functional requirements define the desired security of the IT product as offered by the security vendor, and assurance requirements confirm the effectiveness and implementation of the security implementation.

Key concepts used in Common Criteria evaluations and certifications include Protection Profiles (PP), Target of Evaluation (TOE) and Security Targets (ST).

Protection Profiles (PP) define a standardized set of security objectives for different products or systems that perform similar IT security functions. The certification of a product includes the verification of a protection profile used and simplifies the comparison of certified products, as well as procurement and advice to manufacturers.

A Target of Evaluation (TOE) is the specific IT product or system that is subject to evaluation.

A Security Target (ST) contains the IT security objectives and requirements as pertaining to a specific target of evaluation with the definition of its functional and assurance measures. The Common Criteria has a defined set of Evaluation Assurance Levels (EALs) that measure the criteria of evaluation of the security product's protection profile and test the target of evaluation to verify that it meets its security claims stated by the IT product vendor. The EALs offer a comparative platform to the consumer in selecting a product and also form the basis of Common Criteria certifications.

The evaluation levels are ordered hierarchically in increments beginning from EAL1 to EAL7, with each level requiring a more advanced and intense means of testing. To date, EAL4 is the highest level certification awarded to any security product in the market.

EAL1 is a minimum level of assurance, which only analyzes the functional and interface specification in a bare-boned frame without requiring much documentation. EAL2 level is more detailed because it includes the high-level design and detail specifications of the target of evaluation. This level and its latter counterparts require developer testing and a vulnerability analysis. EAL3 analysis expands the testing coverage of the security functions and mechanisms and offers added security measures by ensuring that the target of evaluation is not tampered during development. EAL4 requires more design description, a subset of the implementation and improved mechanisms and/or procedures

in ensuring that the target of evaluation will not be tampered with during development and delivery.

Evaluations from EAL5 to EAL7 have not yet been recognized by all Common Criteria members, and the requirement for such high-level testing of product complexities has not evolved so far. This is not to say that EAL5 evaluations are not encouraged – it is expected that technology enhancement will create a situation for testing a security product for the EAL5 level, and the process of evaluation will be encouraged while member countries of the Common Criteria agree on methodologies for EAL5- to EAL7-level testing. EAL5 to EAL7 evaluations cost substantially more to the developer, and these levels of evaluation concentrate on semi-formal and formal design.

III. EAL4 certification – the most advanced certification to date

The highly rigorous nature of EAL4 evaluations has called for only a few vendor submissions of security products for certification purposes. The in-depth analysis of product design and development methodology is backed by extensive testing.

The EAL4 functional specification must detail how the product should operate and include all high-level and low-level design documents that show how the components defined in the functional specification are implemented. The security target contains security functions and specific risks associated with the product. The security functions address these risks to prove that the product has the level of security needed for its intended use.

The EAL4 certification checks that the product's stated security features are actually implemented as defined in the design documentation and evaluates the development environment by closely examining and verifying all phases from design to product release. Such evaluation includes product testing and known vulnerabilities appropriate to the product's intended use.

The advanced testing methodology of the EAL4 takes about 10 months to test and deliver certification. The lower the evaluation, the less time it takes for a product to achieve certification, but the trade-off is for a less-valued featured security. However, considering the evaluation process of the EAL4 certification is time-consuming and expensive, the Common Criteria currently is creating a Certification Maintenance Program, where the evaluated development facility of a certified product can project consistency in security implementation for newer versions of the evaluated product, along with vulnerabilities and design tested for the certified product version."

List of References

1. Gregor, FutureHackerAttacks.pdf URL: http://www.zonelabs.com/store/content/company/corpsales/corpSales.jsp?lid=nav_ent (10Aug)

2. Gregor, Hurwitz_wp.pdf URL: http://www.zonelabs.com/store/content/company/corpsales/whitepapers.jsp (10Aug)

3. Robert Richmond, "Personal Firewall Comparison" URL: http://sysopt.earthweb.com/reviews/firewall/ (10Aug)

4. Tony Bradley, CISSP, "Internet / Network Security URL: http://netsecurity.about.com/library/blfreefirewall.htm (10Aug)

5. Peter Cox, "Security Evaluation: The Common Criteria certifications" URL: http://www.itsecurity.com/papers/border.htm (10Aug)

Note: This paper also contains knowledge and skills acquired from the official GSEC textbooks by SANS Institute. "Track 1 – SANS Security Essentials and the CISSP 10 Domains."