ACHIEVING NETWORK SECURITY WITH FIREWALLS

Ibrahim A. R. Al-Kaltham* and Khalid Al-Tawil**
King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia
Email: *kalthaia@aramco.com.sa, **khalid@ccse.kfupm.edu.sa

ABSTRACT. With the rapid increase in the number of LAN connections to the world's largest computer network (the Internet), new security techniques should be used to protect local networks against intrusion from the Internet. Basically, we need to prevent destruction of data by intruders, maintain the privacy of local information, and prevent unauthorized use of computing resources. To improve network security, network connections to the Internet, in general, do not take place transparently. Instead, firewall servers are used to protect the systems connected to the local network against assaults from the Internet. But, there is a price to pay, usually, because the firewall server results in a bottleneck for assaults from the Internet into the LAN as well as for allowed communication between the LAN and the Internet. In this paper, we will discuss how network security can be achieved via security and firewall design policies to satisfy deferent security requirements in order to protect computer networks against intrusion as they get connected to the Internet. We will also present some recommendations for achieving the security of networks using firewalls.

1. INTRODUCTION

Local users in a campus or a company may require the expertise of other users in the field, who are often able to spot new business trends and other up to date information faster than local users. Also, remote users may need to make decisions based on the same data that is available for those at the headquarter. Remote access network technologies provide remote users with reliable access to their private network. For this purpose, wide area network (WAN) digital-service technologies are increasingly used. The choice of technologies depends on individual corporate needs, Some companies need full-time point-to-point connections for their branch offices, where others need connections for telecommunications or mobile employees.

The nature of computer networks indicates that they are designed to allow the free flow of information. The chief benefit of networks is that they enable users to share information easily. But easy access to information is also the cause of concern for those in charge of keeping a network free from security threats. With modern network technologies, a user can sit at a workstation in one location and have a process connected to a system in another location with files mounted from a system in a third location. Therefore users are able to do their work just as if all of the systems are in the same site as the computer they are logged-on to. All of this is possible, because of the free flow of data which is necessary to the basic functionality of the network. However on the other hand, the free flow of information is contrary to achieving network security. The overall usability of the network should not be greatly affected by security measures used to keep private information and sensitive data insulated from unauthorized access. The demand for security products to guard private networks from intrusion is on the rise as the number of businesses and government agencies connecting to the Internet continues to increase.

In modern network environments, the transmission control protocol / Internet protocol.(TCP/IP) suite is widely used to interconnect computing facilities. Unfortunately, several security vulnerabilities exist in the TCP specification in addition to other weaknesses in some of its implementations. Therefore, and because of these vulnerabilities, an intruder might be able to attack TCP-based systems to gain a TCP connection or cause denial of]. According to an Information Week/Ernst and Young firstservice to other legitimate users [Security Survey, one of every five respondents admitted that, in twelve months time, their corporate networks, had been broken into, or had been tried to be broken into, by intruders via].secondthe Internet [

To achieve the goal of securing networks without restricting the flow of information, Internet firewalls are used as points of security guarding private networks from intrusion. Internet firewalls main purpose is to control and audit access to services and provide defense, both from inside and outside a private network. Therefore, a mechanism for selectively permitting or blocking traffic between the Internet and the network being protected is required. For]:thirdinstance traffic can be controlled by [

Routers at an IP level, by selectively permitting or denying traffic based on .1 source/destination address or port. In this case, at least a degree of direct IP-level traffic between the Internet and the protected network must be permitted.

Hosts at an application level to force traffic to move out of the protocol layer for more .2 detailed examination Application level firewalls unlike routers, do not have the requirement of direct IP-level traffic, but are less flexible since they require development of specialized application forwarders known as “proxies”.

There are three types of computer network securities: 1) Internet security, where computers are connected through a firewall, 2) Inter-Company security, where the connection is made through a tunnel, and 3) Intranet security, where computers are connect through multiple]. Regardless of the network type under consideration, using a firewall does fourthfirewalls [not reduce the need for highly skilled system administration and it should not be an excuse to pay less attention to system administration of the site. But on the contrary, when a firewall is compromised, a poorly administered site would be widely-open to intruders and therefore, damage. Firewalls provides barriers, therefore, more time can be spent on site system administration duties and less time responding to incidents and damages. Also, a communications pathway should exist between system administrators and firewall/site security administrators to alert the site about new security problems, and other security-]. secondrelated information [

This paper is organized as follows: Section 2 discusses alternative security solutions. Section 3 discusses a number of important considerations to the design of security solutions for enterprise networks. Section 4 talks about security and firewall policies. Section 5 looks at firewalls as an approach to security that helps in the implementation of a larger security policy. Section 6 presents some useful recommendations when considering firewall solutions. And finally, a conclusion is given in Section 7.

2. PROTECTION METHODS

Security protection methods are basically concerned with ensuring network's efficiency and effectiveness. With successful security implementations, risks can be reduced but not eliminated. There are several protection methods to ensure confidentiality, integrity and continuity. The dominating security protection method in the mainframe computing environment is the Access Control. It consists primarily of functions related to:

Access Mediation via connection control establishment, .1
Identification by means of Logon-Ids, .2
Authentication by means of Passwords, .3
Deferent levels of authorization controlled by Access Privileges, .4
Monitoring and enforcement, .5
Disaster recovery programs to respond to incidents, .6
Logging to record traffic and usage of services. .7

In an open-networked environment such as the Internet, these functions must be integrated in]:fifth, fourthorder to achieve successful security controls. Integrated security should include [

Physical security, .1
Computer based security, .2
Encryption and Authentication, .3
Procedures, and Awareness. .4

2.1 Password Authentication

The most common security technique within computer systems is the validation or authentication of passwords which is used to validate users. The user should be the only one to know his password, while guessing it randomly should be costly. Additional passwords may be required by the different Internet services. This protection technique will only work as a useful identification method, if passwords are protected and applied correctly. For better protection of a personal password, the following prevention points may be used:

The minimum length of a password should not be less than six (eight is better) .1
alphanumeric characters,
Care and creativeness should be used when constructing a password, .2
Passwords should not be exposed or shared with any one, .3
Passwords should be changed frequently and regularly. .4

2.2 Encryption

Encryption is one of the protection mechanism for data confidentiality and integrity. It also, via secret handshaking, can ensure the correctness of communication between any two computers. It makes key resources unavailable to attackers, therefore, when properly implemented, it can prevent attacks against networks and protect against information disclosure. Encryption is becoming the standard policy in any communication of sensitive information. It has many applications including: the protection of file servers, hard disks, faxes, telephone conversations via other types of communication. But, it is particularly important for communications with remote sites. Many applications have their own encryption schemes which may be transparent to users, as long as they operate with the same applications at both ends of the transmission within restricted environments.

Pretty Good Privacy (PGP) is often used for mail transmissions because of its simplicity and wide availability. Digital Signatures can also be created using encryption algorithms in order to verify the identities of the senders of the messages as well as their recipients. Public keys can also be obtained through the Internet.

On the Internet, a message will be stored on several, may be thousands, of servers before it reaches its final destination. Therefore, messages on any one of those servers can be looked at or modified but it is difficult to do so because a message is broken into parts. This practice can be made almost impossible with encryption.

2.3 Protection With Firewalls

The best line of defense is an up-to-date and constantly maintained firewall. A firewall/proxy server is a mechanism that is used to protect a trusted network, such as an organization's internal network, from an untrusted network, typically the Internet, or any other untrusted
]. Firewall/Proxy servers provide the most reliable method to control secondnetwork [
outbound access and to protect networks against unauthorized intrusions. It checks addresses and characteristics of messages to make sure that they follow authorization rules. All messages that are verified to be legitimate are allowed to flow through the firewall, while others are blocked. The majority of firewalls are used between internal networks and the Internet, but they can be used in any internet, such as a company's wide area network
]. The design decision sets the general attitude of the firewall whether to provide a second[
higher degree of service or a higher degree of security. To protect the firewall server itself, no
].sixthusers should be allowed to login on the firewall server [

2.4 Firewall Concepts

A firewall is a trusted system that is placed between a trusted internal network and another untrusted external network. The firewall system implements a policy that defines what information should be allowed to pass through. In general firewalls have the following
]:fourthfeatures and limitations [

Features:

It can control the access to the protected network. .1
It can provide one central point of security. .2
It provides more privacy by hiding addresses. .3
It provides logging for security and other purposes. .4
It can notify the network administrator of security related events, so that he can take the .5
appropriate actions.
It can be integrated with authentication keys. .6
It enforces the security policy. .7

Limitations:

Restricted access to desirable services. .1
Back door access problem. .2
Inside attacks. .3
Email viruses. .4
Potential bottleneck .5
Single point of failure. .6

2.5 Other Aspects

The aspect of restricting access is not the only one that matters to computer network security. Other aspects include the situation where firewalls may become annoying by requiring end-users to learn special functions in order to walk through the firewall, in which case, end-users may start looking for ways to go around them.

Another aspect is the inclusion of “secured” kernels. A secured kernel is defined as a modified version of an operating system so that it contains only the necessary services that are needed to run the firewall. This approach forbids attackers from exploiting other services, simply because they don't exist. The majority of firewall products come with secured kernels based on UNIX variants, while some other product's secured kernels are based on DOS.

There has been trade-offs between UNIX and DOS based products. The lack of integrated networking capabilities in DOS can be seen as an advantage, because it means that the firewall can't be crossed over when the firewall application is compromised. However, DOS based products have shown a slower performance, which is considered to be one of the very]:fifthimportant security issues for the following reasons [

- Frustrated end-users may look for ways around the bottleneck. That is caused by the slow response time of the firewall

- Any path that circumvents the firewall can present a point of entry to intruders.

- When invaders overwhelm a firewall with requests more than it can handle, access to protected resources may be cut off. This is called denial-of-service attack, which is one of the most common forms of attacks on the Internet. The weaker a firewall's performance, the more sensitive it is to a denial-of-service attack.

3. DESIGN CONSIDERATIONS

In this section, we will discuss a selection of a number of design considerations that often come into play when designing security solutions for enterprise networks.

3.1 Layering

Security mechanisms can be implemented at different layers in the protocol stack allowing different levels of flexibility and transparency. Generally speaking, lower layers implementations are more transparent to applications. On the other hand, implementations at higher layers provide more flexibility of customization to the requirements of individual applications. Applications often implement security controls into their own specific protocols,]:seventhfor the following two reasons [

1. Existing protocols have a very limited security,
2. In several cases, the decision is made to build security into an application in order to make it portable to environments running different sets of underlying protocols.

This approach may lead to multiple security mechanisms that may provide the same service, such as the authentication of data-origin, while not interacting with each other. Therefore, as much as practical, secure application-layer communication protocols should be used to support a wide range of applications.

3.2 Centralization Versus Distribution

Usually, in an enterprise networking environments, users and resources tend to reside in more distributed locations. Often, it is desirable to centralize operations to some extent to reduce the overhead but more importantly, security risks that could be caused by the reliance on management by multiple inexperienced system administrators. But, this does not necessarily mean that security information has to be stored centrally, for example, it is often advantageous to keep access control lists (ACLs) with their related resources, while still be managed centrally. Doing so, it will be possible to improve the performance of access control checks as well as allowing the ACLs to be moved with the related resources from one system].seventhto another [

A large enterprise network may be subdivided into a number of management domains, in which authorized users in a given source domain may utilize resources in another target domain. Therefore, it is necessary to set up inter-domain relationships, so that both domains can be used to obtain the required information for user authentication.

3.3 Integration

In an enterprise network, many of the interconnected heterogeneous computer systems may have their own local user authentication and access control facilities. The usability and manageability of enterprise networks are greatly improved, when integrating local system security facilities for the whole network. Some of the problems that may arise in network]:seventhenvironments that have distributed security facilities include the following [

- Because each system recognizes its own set of local users and assigns them unique IDs, passwords, and other security-relevant attributes, a user has to remember multiple ID-password pairs. Therefore, users may start writing passwords down, and subsequently, these written passwords may fall in the hands of some who might endanger the security of the system.

- Because resources access is governed by local access control facilities which depends on local user IDs and security attributes, users must have local IDs defined on each system, so that they can access resources on different systems.

4. SECURITY AND FIREWALL POLICIES

As mentioned earlier, firewalls provide the best protection mechanism for network security against intrusion and unauthorized practices. However, firewalls can be implemented in a number of ways, in order for the different security requirements and policies to be accommodated via the various firewall architectures. In addition, special consideration is given to the special cases that exist in network designs. In this section, we will discuss security and policies. Security is needed to: 1) prevent destruction of data by an intruder, 2) maintain the privacy of local information, 3) prevent unauthorized use of computing resources]eighth[

The highest level of security policies is the overall organizational policy. It highlights the most important and critical issues to the functionality of the organization. On the next level of security, where the firewall's network service-access policy is formulated, the following policies are addressed: 1) site-specific policies concerning physical access to properties, 2) the general access policy to information systems, 3) policies related to the specific access of services on the information systems.

Designing, installing, and using a firewall system to achieve network security is directly influenced by two levels of network policy: 1) network service access policy and 2) firewall]seconddesign policy [

- Network service access policy is a higher-level, issue specific policy that define what services will be allowed or explicitly denied from the protected network, how they are used, and exceptions to this policy.

- firewall design policy is a lower-level policy that describes the actual ways for restricting the access and filtering the services by the firewall as defined in the network service access policy.

The security policy should clearly reflect the importance of strong firewall administration. This is because a firewall is only as effective as its administration which in fact is a critical job and should be given as much time as possible. Therefore, if the firewall is not administered appropriately, it is most likely to become insecure, and allow break-ins, but at the same time, it is giving an illusion that the site is still secure. Security policies can be addressed at three main levels: organization, access of network services, and firewall design.

4.1 Organizational Level

In an organization, the highest level at which security requirements should be considered is the organization itself. This involves defining the overall organizational security policy for the type of organization's type of security environment. Also, when considering solutions to implement such security policy, special consideration should be given to the balance between security and functional requirements.

4.1.1 Organizational policy: At the highest level, the overall organizational policy might]:secondlook like the following [

- Information is critical to the economical growth of the organization.
- In order to ensure the confidentiality, integrity, authenticity, availability and utility of information, all cost-effective efforts shall be made.
- It is the priority for all employees at all levels of the company to protect the confidentiality, integrity, and availability of information resources.

The design of network and firewall security policies is greatly affected by the type of security environment for which it is designed.

4.1.2 Security environments: In this discussion, we will focus on the corporate and academic security environments. Corporate and academic institutions face different concerns related to the security of their information and computing resources.

In most corporate security environments, firewalls are used to block or heavily restrict access from untrusted hosts to internal data and computing resources as well as to limit access from the inside to untrusted hosts outside the corporate. the following is typical in the corporate]:eighthsecurity environment [

- A corporate firewall is defined as a strong security perimeter around collaborating employees within the corporation, as shown in Figure 1.
- The network security perimeter surrounds the corporate network and exclude everything else, except in some cases, where it might include machines at employee homes.
- The security perimeter cautiously controls the transfer of information and in sometimes it actually forbids all outward information flow.
- Although, more open access to the Internet might be desired by many corporations, often, they choose to limit Internet access to achieve corporate security by sacrificing services such as personal World-Wide-Web pages.
- In recent firewall designs some of these limitations are relaxed, but only to support specific interactions between sites that are located within a single private network or authentication domain.

On the other hand, for academic research groups, the trade-off between safety and collaboration is unacceptable. Consequently, the traditional corporate firewall is not suitable]:eighthfor academic environments, as pointed out below[

The natural place to draw a security perimeter in a corporate environment is around the • whole corporation. However. this can not be the case with academic environments, as shown in Figure 1, where it seems nearly impossible to draw a perimeter surrounding everything a trusted user might need to interact closely-with, while keeping other untrusted users out.

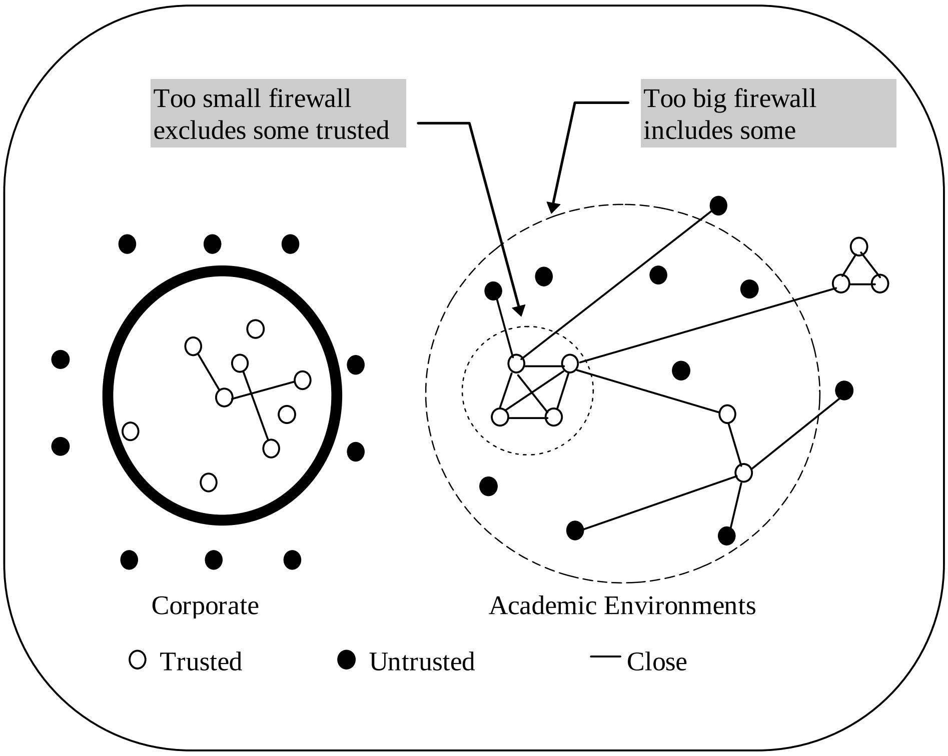

Figure 1: Nature of trusted users, untrusted users, and collaboration in corporate and academic environment

If a corporate firewall is placed around a research group, it would exclude collaborators • located in other sites. Therefore, If the firewall is chosen to be:

too big. it will definitely include untrusted people, especially that universities offer ◊ almost no physical security. This is indicated by the dashed box of Figure1.

too small, then it will exclude some of the people with whom we need to share data ◊ as indicated by the dotted box of Figure 1.

Corporations can tolerate limitations of the Internet connectivity in order to keep their sites secure, however, research organizations cannot perform under such limitations, for the]:eighthfollowing reasons[

Researchers and trusted users need unrestricted access to Internet resources located outside .1 the firewall.
Researchers and trusted users need an unrestricted ability to publish and distribute .2 information to the world outside the firewall, which is critical to the research community.
Research collaborators and trusted users located outside the firewall should be allowed to .3 access protected resources.

In addition, there is a number of other factors that may apply when comparing the two security environments, as shown in Table 1. These factors include the usual considerations of cost, ease-of-management, performance, and reliability in a heterogeneous computing environment. Usually, academic institutions can not allocate enough money to obtain the right computer security hardware, software, or personnel. Therefore, leading to the lack of dedicated security staff which in turn could mean for instance, that a firewall might be managed by inexperienced people such as new graduate students with limited expertise.

Table 1: Comparison of corporate and academic security environments

Factors	**Corporate**	**Academic**
Firewall security perimeter	A corporate firewall is defined as a strong security perimeter around collaborating employees within the corporation that excludes everything else, except in some cases, where it might include machines at employee homes.	An academic firewall seems nearly impossible to draw a security perimeter surrounding everything a trusted user might need to interact closely-with, while keeping other untrusted users out.
Security perimeter controls	Cautiously controls the transfer of information and in sometimes it actually forbids all outward information flow.	Supports free exchange of information.
Limitations of Internet access	Corporations can tolerate limitations of the Internet connectivity in order to keep their sites secure. These limitations can be relaxed, but only to support specific interactions between sites that are located within a single private network or authentication domain.	Research organizations require unlimited Internet connectivity in order to support collaboration between internal and external research groups.
Financial allocations	Usually, adequate financial allocations can be made available to obtain the right computer security hardware, software, or personnel.	Usually, academic institutions can not allocate enough money to obtain the right computer security hardware, software, or personnel.
Expertise	Dedicated security staff.	Lack of dedicated security staff which results in relying on inexperienced people such as new graduate students with limited expertise.

4.1.3 Security versus functional requirements: Firewalls should include certain security measures to protect private networks when connected to the Internet. These measures should include an integrated rights check that permits access control to the Internet based on the: user

name, calling client workstation, and requested service. In general, network secure connection
]:sixthto the Internet requirements should include the following [

Authentication methods of different strengths: Different authentication methods should be supported by the firewall system. These methods may range from “TCP reserved port authentication” to the deployment of chip cards, depending on the area of usage.

Access control on the basis of service, host, and user: Not all users in the LAN should .1
be granted access to all services of the Internet. Rather, only certain users should be enabled to use distinguished services.

Restriction of services: Blocking parts of the services, should be possible as well as .2
preventing the usage of certain destination addresses.

Logging for error diagnosis and accounting: All error situations, potential assaults, .3
destinations of connection establishments, and the size of the data transferred, should be logged by the firewall system.

Protection of the firewall server against the Internet service access system: It should .4
be impossible for a user of the Internet service access system such as firewalls or proxies to threaten the security of the host on which the server is running.

Usually security requirements and functional requirements are contradicting objectives. Nevertheless, when using firewalls to achieve network security, firewalls should satisfy the following functional requirements:

Support of as many communication protocols as possible: Since, it may be difficult to .1
cover many different protocol families such as DECnet., AppleTalk, and TCP/IP, at least one protocol family with as many sub-protocols as possible should be supported.

Minimal modification effort: In order to implement an Internet service access system, .2
network programs generally have to be modified. however, such modification effort should be kept as low as possible.

Low resource utilization on the firewall server: Resource requirements, such as main .3
memory, disk space, and CPU time, that is needed to run the firewall system components on the firewall server should be as minimum as possible.

4.2 Network Services Access Policy

Network service-access policy should be an integral part of a strong site-security policy and an overall policy[1] for the protection of information resources. In network service access policy, the attention is directed toward the restriction and use of internetwork services. But while doing so, it is very important that the network service access policy also includes all other means of network access such as dial-in and serial line Internet protocol / point to point protocol (SLIP/PPP) connections. When restrictions is implemented on one network service access, users may be motivated to try other ways. For example, if web browsing is prevented through a restricted gateway access to the Internet, users may try to obtain this service by creating dial-up PPP connections which are, normally, authorized as an ad hoc connections. These ad hoc connections are likely to have an unacceptable security effects resulting in opening the network to attacks.

The network service-access policy should be realistic and reliable, as well as designed before the actual implementation of the firewall. As realistic policy, it should maintain a balance

[1] This should include everything such as document shredding, virus scanning, remote access, and floppy disk tracking.

between protecting the network from known risks and providing users with reasonable access to network resources.

Adherence to the network service-access policy prevents ad hoc circumvention or modification of the firewall's access controls. The typical network service-access policies that
]:seconda firewall should implement are [

Allowing access from the internal site to the Internet, and disallowing access to the site •
from the Internet

Allowing limited access from the Internet to selected systems such as e-mail and •
information servers.

Normally, firewalls implement the policies of network service-access that allow some access from the Internet to selected internal servers. But this access is accepted only when necessary and combined with strong authentication.

4.3 Firewall Design Policy

The focus on firewalls has been concentrated mainly on the layout of various possible configurations of routers, host systems, interfaces and sub-nets. But it is essential to think of a firewall as a part of an overall security policy. While the security policy defines the services and access to be permitted, a firewall is an approach to security by helping in the
]. In its general definition, a firewall is a ninthimplementation of a larger security policy [
system or group of systems that enforces access control policies between two networks. While, more precisely, it is a system or a collection of components placed between two networks to protect the trusted network from the untrusted network by maintaining the
]:secondfollowing three properties [

All traffic going out from the inside and all traffic coming in from the outside, must pass .1
through the firewall.
Only authorized traffic, as defined by the local security policy, is allowed to pass through .2
the firewall.
The firewall system itself is immune to penetration. .3

Many of the commercially-available firewall products are very powerful and by deploying a firewall, most of the security problems that are associated with internetworking can be fixed. For organizations having, or planning to create a connection between their network and another network, firewalls are considered as the best defense line. However, firewalls, at least
]. A firewall should secondin the narrow sense of the term, do not provide complete solution [
]:ninthconstitute of both the policy and the implementation of that policy in terms of [

Network configuration, .1
Hosts systems and routers, .2
Other advanced security measures such as authentication instead of static passwords. .3

The firewall design policy defines the rules used in implementing the policy of the network service access. The designer of firewall design policy must be fully aware of the threats and vulnerabilities related to TCP/IP, and the capabilities and limitations of firewalls in general. It is extremely important to consider a security design policy before implementing the firewall. Normally, firewalls implement one of two basic security design policies: 1) permit all services unless otherwise are expressly denied, 2) deny all services unless otherwise are expressly permitted. Services which should not be passed through the firewall can be placed, separate from other site systems, on screened subnets. Depending on security requirements, some firewall types are more appropriate than others. A firewall that implements the first]:secondpolicy would have the following features [

By default, allows all services to pass into the site, except services that are identified as .1 prohibited by the service-access policy.

Offer more ways for getting around the firewall which is not desirable most of the time. An .2 example of this is that users would be able to access new services that are not addressed or not yet denied by the policy. Also, denied services could be run by users at non-standard TCP or UDP (User Datagram Protocol) ports that are not specifically denied by the policy.

Better accommodate services that are difficult to filter, such as X Windows, FTP, Archie, .3]tenth, ninthand RPC (Remote Procedure Call) [

On the other hand, the second policy is stronger, safer, and follows the standard access model that is used in all areas of information security. Therefore a firewall that implements this]:secondpolicy has the following features [

Deny all services by default except those that have been identified as allowed, .1

More difficult to implement, .2

More restrictive for users; .3

Services such as X Windows, FTP, Archie, and RPC may have to be blocked or heavily .4 reduced.

In order to design a firewall policy and implement that policy, the policy designer should start with the most secure firewall design policy, which denies all services except those that are explicitly permitted. Then he should understand and try to answer the following questions]:second[

What Internet services will the organization be using and what risks are associated with .1 providing these services and access?

Are there any additional requirements, such as encryption or dial-in support? .2

Will the services be used on a local basis, across the Internet, dial-in from home, or from .3 remote organizations?

What is the cost of providing protection, in terms of controls and network usability? .4

If a particular service is too risky or too expensive to secure, how would the decision be .5 made regarding security versus usability?

5. FIREWALL SPECIFICATIONS AND REQUIREMENTS

The next step after deciding to use firewalls protection method to implement the security policy, is the acquisition of a cost-effective firewall that renders a suitable level of protection. What firewall is right for a given customer?. The answer to this question, is that there is no single firewall solution for all customers. This is because security needs are diverse such as: the level of needed customization, the available level of experience with UNIX, whether integrated Internet services are required or not, and the size and complexity of the network]. The exact features of a firewall to provide effective implementation for a specific fourth[ ]:secondsecurity policy can not be stated here, but a firewall in general should [

- Support advanced authentication procedures, or at least, it should be integrable with other advanced authentication procedures.

- Control service access to specified host systems as needed by means of filtering techniques.

- Support the use of a flexible and user friendly IP filtering language that is capable of filtering on as many attributes as possible. Such attributes should include IP addresses of both the source and the destination, the type of protocol, TCP/UDP ports for the source and destination, as well as inbound and outbound interface.

- Use of proxies for services such as the FTP and TELNET, X and gopher, in order to use centralized advanced authentication measures at the firewall.

- Support centralized handling of site e-mail in order to reduce direct SMTP connections between the site and remote systems.

- Distinguish between the protected public information servers and other site systems that are not allowed for public access.

- Have the capability to centralize and filter dial-in access.

- Contain logging mechanisms of traffic and doubtful activities, as well as mechanisms for the reduction of log records in order to make them readable and understandable.

- Ensure firewall host integrity by implementing a secured version of the operating system as a part of the firewall, if it is required to have an operating system such as UNIX. The operating system should have all patches installed with other security tools as necessary.

- Be simple in design so that it can be understood, maintained, and verified for its strength and correctness.

In addition, the firewall as well as any related operating system should be, in a timely manner, updated with patches and other bug fixes. Especially that the Internet is changing continually, new vulnerabilities will always arise. Therefore, it is important the firewall be flexible in order to adapt to changing needs, as well as staying current on new threats and vulnerabilities. Otherwise, new services and enhancements to existing services may represent possible difficulties for any firewall installation.

The decision whether to buy or build a firewall, involves some advantages and disadvantages as shown in Table 2. For organizations that have the capability to develop a firewall from scratch or put it together from available equipment and software components, it will be to their advantage to build their own firewall. On the other hand, for other organizations, a wide range of firewall service technologies are offered by several vendors. These include: the necessary hardware and software, the development of security policy, security reviews and risk assessments, as well as security training. Whether the decision is made to buy or build a firewall, security policy has to be developed first.

Table 2: Tradeoffs between In-house and vendor-supplied firewall

Comparison	**In-House**	**Vendor-Supplied**

Factors	**Firewall**	**Firewall**
Resources	The organization should consider whether it has the internal resources to build and maintain the firewall.	The vendor is responsible for the necessary resources to build and maintain the firewall.
Experience	Enables personnel to understand the specifics of the design and use of the firewall.	In-house personnel are not given the opportunity to understand the specifics of the design and use of the firewall.
Overall cost of the firewall should consider: (This is in addition to the cost of equipment)	The time required: To build and document .1 the firewall. To maintain the firewall .2 To add new features as .3 needed.	Free installation. .1 Free maintenance services if provided by the vendor. The extra charges when .3 adding new custom features.
Maintenance	Organization's responsibility	Usually, Vendor's responsibility
New features	Can be custom tailored.	Usually, are general purpose.

One very important factor to consider when computing the cost of a firewall, is the cost of its administration. In addition to the initial required resources during the building phase of the firewall, an organization should decide whether or not it has the resources for operating and maintaining a successful firewall. To help in making this decision, the organization should consider the necessary resources to handle issues such as: firewall verification for correctness and expected performance, maintenance, enhancements, updates, backups, and training]:second[

6. RECOMMENDATIONS

The recommendations presented in this section fall into two groups. These recommendations should help organization in achieving their network security using firewalls. The first group of recommendations is aimed toward preparing the network environment for the use of firewall protection. On the other hand, the second group of recommendations is aimed toward the selection or design of a firewall. These recommendations are as follows:

Recommendations for preparing the network environment: •

Standardization: Operating system and other software should be standardized in order .1 to make installations of new programs and other security related fixes more manageable.
Procedures: A procedure should be established to achieve efficient, site-wide .2 installation of programs and new software.
Proper tools: The use of proper utility programs and services that will assist in .3 achieving centralized system administration, should be consider if centralized system administration will result in a better security and administration.
Preventive security checks: Host systems should be periodically scanned and checked .4 for common vulnerabilities and configuration errors.

Recommendations for designing and selecting firewalls: •

In addition to the general features of firewalls which we have discussed in section 5, a firewall should consider the following issues:

Policy support: The firewall should support: .1

The security policy as defined by the organization. (a
The security policy that denies all services except those specifically permitted. (b
The firewall should adhere to this policy even if it is not the one in use by the organization.

Future support: The firewall should be able to accommodate and support of new .2 services and requirements, as the security policy of the organization changes.

7. CONCLUSION

The Internet is a rapidly changing and expanding environment that is constantly facing new challenges which should be resolved to assist user concerns and demands related to security and user protection. There are several problems that are related to the use and implementation of the Internet. These include among others, IP address domains, traffic overflows, and bottlenecks between users and service providers. But, the biggest concern is the absence of necessary security controls. In addition, expected new technologies on the Internet will require new creative security solutions, because what has worked in the past, may not necessarily work in the future.

Firewalls are considered as the best protection method against the threats that are facing computer networks. But, the concentration on firewalls has been mainly on the numerous possible configuration layouts of routers, host systems, interfaces and sub-nets. However, it is very important to treat firewalls as a part of an overall security policy, where firewalls are used to implement the security policy which define the services and access to be permitted. Even when firewalls are used, a highly skilled system administration of the site is still needed. This is because, firewalls provides barriers, but when a barrier is compromised, a poorly administered site would be widely-open for intrusion.

In this paper, we have discussed how network security is achieved through security and firewall design policies to satisfy deferent security requirements. We have also presented some recommendations for achieving the security of networks using firewalls.

REFERENCES

[1] B. Guha and B. Mukherjee, "Network security via reverse engineering of TCP code: vulnerability analysis and proposed solutions," Proceedings of IEEE INFOCOM '96. Conference on Computer Communications, San Francisco, CA, USA, vol. 2, pp. 603-610, Mar. 1996.

[2] S. Cobb, "Establishing firewall policy," Southcon/96 Conference Record, Orlando, FL, USA, pp. 198-205, June 1996.

[3] M. J. Ranum and F. M. Avolio, "A toolkit and methods for internet firewalls, "http://www.tis.com/docs /products/gauntlet/Usenix. html.

[4] B. Gassman, "Internet security, and firewalls protection on the internet," Professional Program Proceedings. ELECTRO '96, Somerset, NJ, USA, pp. 93-107, May1996.

[5] D. Newman and B. Melson, "Can firewalls take the heat?," Data Communications, vol. 24, pp. 71-80, Nov. 21 1995.

[6] S. Stempel, "IpAccess - an internet service access system for firewall installations," IEEE Symposium of Network and Distributed System Security, CA, USA, pp. 31-41, Feb. 1994.

[7] P. Lin and L. Lin, "Security in enterprise networking: A quick tour," IEEE Communications Magazine, vol. 34, pp. 56-61, Jan. 1996.

[8] M. B. Greenwald, S. K. Singhal, J. R. Stone, and D. R. Cheriton, "Designing an academic firewall: Policy, practice, and experience with SURF," Proceedings of Internet Society Symposium on Network and Distributed Systems Security, San Diego, CA, USA, pp. 79-92, Feb. 1996.

[9] W. R. Cheswick and S. M. Bellovin, Firewalls and Internet Security Repelling the Wily Hacker. Addison-Wesley publishing company,1994.

[10] B. Chapman, "Network (in)security through IP packet filtering," In USENIX Security Symposium III Proceedings, pp. 63-76, Sept. 1992.