Wireless Network Security: Intrusion and Detection

Final Project Report

Submitted to

College of Engineering

ENGR 298

Master's Project- Fall 2008

San Jose State University

Team # 4:

Karthik Reddy Pothireddy (005173520)

Naresh K Veesamshety (005787691)

Pradeep Aitha (005223882)

Niharika Manyala (005331145)
Copyright © 2008

Naresh K Veesamshety

Karthik Reddy Pothireddy

Niharika Manyala

Pradeep Aitha

ALL RIGHTS RESERVED.

APPROVED FOR THE DEPARTMENT OF GENERAL ENGINEERING
Prof. Jack McKellar

**Faculty Reader**

Department of Chemical Engineering,
San Jose State University, CA

---

Mr. Hazarathaiah Chimata

**Industry Sponsor**

Clear Lead Inc.
Dr. Leonard Wesley, Ph.D.

**ENGR 298 Course coordinator**

Associate Professor, Department of Computer Engineering &

MSE Director

San Jose State University
Abstract:

Network Security can be defined as measures taken to protect data during their transmission along the media. Whereas securing the internet means taking measures to protect data during their transmission over a collection of interconnected networks.

Security means defense against the loss of data. Intruders pretend as host computers and obtain the data from the network. These data is manipulated or destroyed. This process is known as attack. So security measures must be taken to protect the data from intruders.

Network Security is the most important issue in the vast field of wireless networks. In order to improve network security, there are a number of products that are available in the market that use packet filtering. For a network administrator, packet filtering is an effective tool for security purposes but he/she has to have an in depth knowledge of the capability of this tool. Our firewall software contains a set of protocols for which the filters will be applied. We have devised a packet filtering firewall called NetKapp for Microsoft Windows operating systems.
Table of Contents

1. Introduction ........................................................................................................................................... 9

2. Network Security ................................................................................................................................... 10

3. Threats to Network Security include: .............................................................................................. 11
   3.1 Viruses: ............................................................................................................................................. 11
   3.2 Vandals: ............................................................................................................................................ 11
   3.3 Data Interception: .............................................................................................................................. 11
   3.4 Trojan horse programs: ..................................................................................................................... 12
   3.5 Attacks: ............................................................................................................................................. 12
   3.6 Social Engineering: ........................................................................................................................... 12

4. Network Security tools ....................................................................................................................... 13
   4.1 Antivirus software packages: ............................................................................................................ 13
   4.2 Virtual Private networks: .................................................................................................................. 13
   4.3 Secure network infrastructure: ........................................................................................................ 13
   4.4 Encryption: ........................................................................................................................................ 14
   4.5 Identity Services: .............................................................................................................................. 14
   4.6 Security Management: ..................................................................................................................... 14

5.1 Network Access Security model: ..................................................................................................... 17
   5.2 Security Services ............................................................................................................................... 17

6. Encryption Standards .............................................................................................................................. 18
   6.1 Symmetric Encryption model: .......................................................................................................... 19
   6.2 Asymmetric Encryption: .................................................................................................................. 20

7. Firewalls: ................................................................................................................................................ 22
   7.1 Authenticating users: .......................................................................................................................... 23
   7.2 Filtering Services: ............................................................................................................................. 23
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.3 Access list:</td>
<td>25</td>
</tr>
<tr>
<td>7.4 Access control:</td>
<td>25</td>
</tr>
<tr>
<td>7.5 Network security:</td>
<td>25</td>
</tr>
<tr>
<td>8. Need of Security</td>
<td>26</td>
</tr>
<tr>
<td>9.1 Hackers</td>
<td>29</td>
</tr>
<tr>
<td>9.2 Employees unaware of security measures</td>
<td>30</td>
</tr>
<tr>
<td>9.3 Aggravated Employees</td>
<td>30</td>
</tr>
<tr>
<td>9.4 Mischievous Employees:</td>
<td>31</td>
</tr>
<tr>
<td>9.5 How do these enemies affect:</td>
<td>31</td>
</tr>
<tr>
<td>9.5.1 Viruses</td>
<td>31</td>
</tr>
<tr>
<td>9.5.2 Trojan Horses</td>
<td>32</td>
</tr>
<tr>
<td>9.5.3 Attacks</td>
<td>32</td>
</tr>
<tr>
<td>9.5.4 Data Interception:</td>
<td>33</td>
</tr>
<tr>
<td>9.5.5 Spam:</td>
<td>33</td>
</tr>
<tr>
<td>9. Security Tools</td>
<td>33</td>
</tr>
<tr>
<td>10.1 Security Tips</td>
<td>33</td>
</tr>
<tr>
<td>10.2 Intrusion and Detection</td>
<td>34</td>
</tr>
<tr>
<td>11. What is a Packet Filtering Firewall?</td>
<td>35</td>
</tr>
<tr>
<td>12. Working of Firewall:</td>
<td>42</td>
</tr>
<tr>
<td>13. Routing of Packets</td>
<td>43</td>
</tr>
<tr>
<td>13.1 Description:</td>
<td>45</td>
</tr>
<tr>
<td>13.2 Summary of Invention:</td>
<td>46</td>
</tr>
<tr>
<td>13.3 Description of the preferred embodiments</td>
<td>49</td>
</tr>
<tr>
<td>14. Economic Justification</td>
<td>73</td>
</tr>
<tr>
<td>14.1 Problem Statement</td>
<td>74</td>
</tr>
</tbody>
</table>
1. Introduction

Internet is one of the most important advancements in the history of mankind. It allowed communication to reach a new high. Initially internet was used for military purposes for a message to pass through few computers. The universities came to know that it will send messages faster than any other means for the researches that were conducted in the universities. Then the business world became very curious about this and later it has become common in every field and to everyone. It has become more applicable for all the communities. The main aim for the internet to grow is to make communications faster.

Internet made information accessible to everyone very easily. The growth and vastness of the Internet was accepted worldwide and became a necessity rather than a utility. Many significant changes took place in the world of internet. The TCP/IP addressing is almost over and a new version of addressing has been introduced called IPV6. The number of hosts getting connected is increasing exponentially.

The TCP/IP is called a four layer protocol. This is responsible for the data flow across the network. This network is unreliable because there is know no acknowledgement that is there is no guarantee that the packet has reached the destination. However TCP is a reliable network where it sends the acknowledgement to the host.

Talking about the IP addressing system, it is a 32 bit internet addressing system. If an interface has to participate in the internet then it should have an ip address. An ip address has a
network address and the host address. There are five different classes in addressing: class A, class B, class C, class D, class E. A browser is software that allows a user to view the information that is available on the internet. The appropriate address field will take the user to the requested web browser or to the destination. A DNS server is one that changes/resolves the host name to its respective IP address.

2. Network Security

Network Security is a complicated study and can be only tackled by well-trained and experienced experts. Some history of networking is included, as well as an introduction to TCP/IP and internetworking. We go on to consider risk management, network threats, firewalls and more special-purpose secure networking devices. Network security includes every measure that enterprises, organizations and institutions deploy to protect the integrity and continuity of functionalities. Network security strategy requires an effective effort to identify threats and then choosing and applying the most effective tools to contend them.

Network Security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and consistent and continuous monitoring and measurement of its effectiveness combined together. Compromised network securities means allowing an intruder to easily access the sensitive data and manipulate accordingly resulting in loss of data or complete destruction of the host or server system.

The networks can be classified as public and private, which are used every day to conduct transactions and communications among business, government agencies and individuals. The
networks are comprised of nodes, which includes client terminals i.e. individual user PCs and one or more servers. Networks are linked by communication systems, some of which might be private, such as within an organization and others which might be open to public access. Internet is the obvious example of a network system that is open to public access, but many private networks also utilize publicly-accessible communications.

Today most companies provide access to host computers by their employees whether in their offices over a private communications network, from their homes or hotel rooms and on the road through normal telephone lines.

3. Threats to Network Security include:

3.1 Viruses:

Computer viruses can be defined as software programs that are written to spread from one network node to another computer node and to corrupt and interfere with network nodes and computer operations. The virus threat might corrupt or delete data on your PC and can be spread to other computers by email program and even delete all data on your hard disk.

3.2 Vandals:

Software applets or applications that is responsible for destroying data.

3.3 Data Interception:

Data interception involves eavesdropping or spoofing the packets in communication systems and altering data packets that are being transmitted.
3.4 Trojan horse programs:

A destructive software program that acts as a genuine application is called a Trojan horse program. Unlike Viruses, Trojan horses do not replicate themselves among network but they can be just as destructive as viruses. Trojan horse claims to wipe out the virus in your computer but instead introduces viruses onto your computer.

3.5 Attacks:

Attacks include

1. Reconnaissance attacks: - The process of collecting data which is further used to compromise the network.

2. Access attacks: - In order to gain access to database servers, e-mail servers one can compromise a network which exploits network vulnerabilities.

3. Denial-of-service attacks: - It prevents and blocks access to the computer system.

3.6 Social Engineering:

In Social Engineering, obtaining confidential network security information through non-technical means, such as posing as a technical support person and asking for people’s password is causing a threat to security of personal data.
4. Network Security tools

4.1 Antivirus software packages:

These software packages counter most virus threats if updated and correctly maintained regularly.

4.2 Virtual Private networks:

These networks provide access control and data encryption between two different computers on a same network or different, which allows hosts to have remote access to the network without the risk of a hacker or any intruder corrupting the data.

4.3 Secure network infrastructure:

Switches and routers have hardware and software features that support secure connectivity, intrusion protection, perimeter security, identity services and security management.

Dedicated network security hardware and software –Tools such as firewalls and intrusion detection systems provide protection for all areas of the network and enable secure connections.
4.4 Encryption:

Encryption is defined as the process of converting the plain input text to cipher text using a key. The encrypted text cannot be intercepted or read by any other user except the authorized recipient.

4.5 Identity Services:

Identity Services help to identify users and control their activities and transactions on the network. Services include digital certificates, passwords and digital authentication keys.

4.6 Security Management:

Security management is the centralized management solution that holds together all other building blocks of a strong security solution.

None of above approaches alone to secure a network will be sufficient in protecting the network, but when they are layered together, they can be highly effective in keeping a network safe from attacks and other threats to security.

Each network Security rule consists of conditions for network traffic and of actions which are taken when conditions are met.

Definitions:

Network Security can be defined as measures taken to protect data during their transmission along the media. Security means defense against the loss of data. Intruders pretend as host computers and obtain the data from the network. These data is manipulated or destroyed.
This process is known as attack. So security measures must be taken to protect the data from intruders.

Attacks can happen inside the LAN, outside the LAN, across the telephone lines or over the internet. We must protect the information available inside the data, confidentiality of data, integrity of data and transactions, resources available and access control. Therefore security can be achieved by blocking the unauthorized users from accessing or altering the information and replay of information.

Security information can considered as security attack, security mechanism and security service. Securing information is how attacks are detected and prevented on user systems. Attack can be called as threat often. Attacks happen in various scenarios. The mostly known attacks are active and passive. A passive attack means the intruder reads the content of the message from the internet sent from source host to destination host. An active attack means the intruder captures message from the internet sent from source host, manipulates the message and sends to the destination host.

Security Mechanism is a design to protect or recover the data from attacks. All the services cannot be achieved by single mechanism. Cryptographic techniques are introduced to help the network survive from different networks. Encipherment, digital signatures and access controls, data integrity, authentication exchange, traffic padding, routing control, notarization are specific security mechanisms. Trusted functionality and security recovery are described as pervasive security mechanisms.
Firstly design a best algorithm for the security transformation and generate the secret keys to access the algorithm. Develop methods for distributing and sharing the secret data and specify a protocol to obtain a secured service by enabling the transformation and secret information.
5.1 Network Access Security model:

For this model proper gatekeeper should be selected to authenticate users. Proper security controls should be implemented so that only the authorized users can access the information and resources. Implementing trusted PC’s is helpful for this model.

5.2 Security Services

Types of security services needed for the design of the secured network are as follows:

1. Authentication
   Ensures the host is the one claimed to access information.

2. Access Control
   Intruders are prevented from accessing the resources or information channel.

3. Data Confidentiality
   Data confidentiality means protecting the information from unauthorized users.
4. Data Integrity

Guarantee that data received is not manipulated in the network.

5. Non-Repudiation

Protection against denial by one of the hosts in a network is Non-repudiation.

Basic Terminology used in network security.

- plaintext - Original message is known as plaintext.
- cipher text - Coded message is known as cipher text.
- cipher - Cipher is algorithm for transforming plaintext to cipher text.
- key - Information used in cipher.
- encipher (encrypt) - converting plaintext to cipher text
- decipher (decrypt) - recovering plaintext from cipher text.
- cryptography - the study of encryption principles.
- cryptanalysis - study of principles
- cryptology - Both cryptography and cryptanalysis

6. Encryption Standards

There are two types of encryption.

- Symmetric Encryption.
- Asymmetric Encryption.
6.1 Symmetric Encryption model:

This standard uses single key for encryption. It is also known as conventional or private-key encryption. Both the sender and receiver share the same key. All classical encryption algorithms are single key encryption. This encryption standard was invented in 1970’s and is still widely used in many network scenarios.

A strong encryption algorithm with a secret key known only to sender and receiver is required for secure use of encryption algorithm. A secure channel is required for key distribution among sender and receiver.

Mathematically represented as:

\[ Y = E_k(X) \]
\[ X = E_k(Y) \]

Where X is plain text, Y is cipher text and k is key.
From the figure firstly the input plaintext from sender is encrypted using the shared key and encryption algorithm and then cipher text is send over the communication link. At the receiver side the cipher text is decrypted using the same shared key and decryption algorithm to obtain the original plain text. The disadvantage of the symmetric algorithm is that it is liable to cryptanalytic attack and brute-force attack.

The widely used symmetric cryptography methods are:

- DES (Data Encryption Standard)
- Triple DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)

### 6.2 Asymmetric Encryption.

Asymmetric Encryption is also known as public key cryptography. Public-key cryptography uses 2 keys for encryption, a public key and a private key. This cryptography is known as asymmetric because it uses two different keys.

Public key is known to everyone in the network. It is used to encrypt messages and verify signatures, whereas, private key is known only to the recipient. It is used to decrypt messages and create signatures.

Public-key cryptography does not replace symmetric cryptography but has enhanced security. The design is more complex than symmetric cryptography system.
Fig 4: Asymmetric Encryption Model

From the figures above firstly the input plaintext from sender is encrypted using the receiver public key and encryption algorithm and then cipher text is send over the communication link. At the receiver side the cipher text is decrypted using the receiver private key and decryption...
algorithm to obtain the original plain text and vice versa. This method is much secure from
cryptanalytic attack and brute-force attack. Both encryption and authentication is achieved.
Public-key applications can be classified as:
–encryption/ decryption (provide secrecy)
–digital signatures (provide authentication)
–key exchange (of session keys)

The widely used Public-key cryptography is RSA (Rivest Shamir Adleman).

7. Firewalls:

It is impossible to identify the threats to a system. Authentication is one of the methods to
avoid intruders. This is a process where the user has to provide account name, and a password to
identify. Authorization is a security measure that is used after authentication.

Vandalism is a process in which the main purpose of the attacker is to destroy the target
system. He vandalizes the system for fun and to gather intelligence. The other process like this is
the foot-printing in which the hacker tries to know the information about the target system. He
systematically knows the detail of the target. The information that is gathered from this is the
range of networks, the types and addresses of the DNS server and the information of the emails
and email servers. There are many such techniques like scanning, sweeping, war driving etc.
The other such attack is the routing attacks where the hacker manipulates the network routing
tables in a way that they deny services for the legitimate network hosts. A firewall is a security
system that is use to prevent unauthorized access. A firewall can be a physical device or a
software. There are some basic functions that the firewalls perform are authentication, filtering the services and packets, securing the network from entering viruses and performing NAT (Network Address Translation) which is discussed later. They are used to guard the networks against threats, intruders and viruses. They were first introduced in 1990.

7.1 Authenticating users:

A firewall can authenticate users to tell whether the request is genuine or not. It uses strong user authentication which means it uses cryptographic techniques like digital signatures to allow only authenticated users. Cryptographic techniques are much more reliable than authenticating the user with user name and password.

7.2 Filtering Services:

As the name says it means granting access to the selected services. That is in any company or organization they can block few websites from being accessed like the yahoo messenger and email etc. There are two types of protocols called NNTP (Network News Transfer Protocol).
Fig 5: Enabling a firewall

This is how it is when the firewall is enabled in a system.

Few security risks are that they have single point failures, and no security policies latency etc.

Some of the firewall standards are:

- Open architecture
- Packet filtering
- Access control
- Secure back up
- Secure subnets
- Device management
- Secure management
- Real time traffic monitoring
- Strong encryption
7.3 Access list:

An Access list dictates a router’s duties based on a number of facts. The packets include things like source address, destination address, port number etc. Instead of allowing all the packets it will allow only the one which has access and belongs to the access list. The other server is the proxy server which has the ability to fetch the requested document from the internet. Access list is like a key to the network system. It will check all the activities passing and will allow only the authorized ones.

7.4 Access control:

Access control servers function like a door keepers, providing centralized authorization and accounting, authentication (AAA) for the users. However most of the network security infrastructures are ineffective if people do not protect their passwords. Many users choose easy passwords that are they choose the names which can be easily remembered such as their last names, pet names, phone numbers etc. The rules for protecting their passwords are to keep changing your passwords often, make your passwords meaningless, and never disclose your passwords with others.

7.5 Network security:

With the increasing demand of E-Commerce and internet banking, computer networks if not secured are highly vulnerable to attack. Viruses, Hackers, spiteful employees and sometimes human errors create a danger to the networks. All kind of computer users from an individual to large enterprises could be a victim due to network breach. But these kinds of network security breaches can be easily prevented. How? The following chapters provides a general overview of
the types of network breaches and steps to protect the network from threats and make sure that the data traveling on the network is safe.

8. Need of Security

These days the internet is the main data network which enables and simplifies both the personal and business communication worldwide. The amount of data flow over the internet, as well as company networks has grown exponentially. Most of the communication is taking place through e-mails. People started working from their own place connecting to their company’s network through internet. Most of the financial transactions like bills, payments, purchases are being done over the internet.

Though the internet has developed and improved the way the businesses are done, it also has opened gates for the new kind of security threats from which the corporations must protect themselves. Though the security threats are known to be dangerous when they attack on business networks that store very sensitive data like personal information, financial information, and medical records the results might be little inconvenient or very devastating. The reason is that important might be lost or misused, privacy can be affected, malfunctioning of the network might happen or the network might slow down for several hours or days.
Although there is risk involved in doing business over the internet, sometimes internet is the safest way of protecting yourself against fraud. For example, providing credit card information over the website is safer than providing to a sales person over the telephone because the website is always protected by security. We cannot trust a sales person who is on the other end of the line. Therefore the fear of security problems can be as harmful as actual security breaches. Fear and doubt of computer technology still exists which leads to the mistrust of the internet. This mistrust greatly affects the businesses that are completely web based. Therefore these kinds of companies must enact security and establish safeguards that are effective. Also the companies must prove to their customers that they can protect their personal data from security breaches. In addition to protecting their customers the company should also plan to protect themselves, employees and also their partners from security threats. The internet, intranet and extranet is the most effective way of communication between the employees and partners of the
company. But, these communications and efficiency can be impeded by the effects of a network security breach. Due to this the network might directly or indirectly malfunction or slow down for its employees. Sometimes the networks are slowed down to repair the network congestions. This indicates that the loss of precious time and data affects the employee’s efficiency and confidence if there is a network security breach.

“I have found that inadequate network security is usually caused by a failure to implement security policies and make use of security tools that are readily available. It's vital that companies complete professional risk assessments and develop comprehensive security plans and infrastructures that are publicly supported by upper management.”—Mark Carter, COO, CoreFacts, LLC, Data Recovery and Analysis Firm

Threats to Data:

In any type of network security breach the threat to the data comes from a small portion of the vandals. However, in other crimes for example one bike thief can steal only one bike at a time but in a network security threat one hacker working from a single computer can harm countless number of computers on the internet. Also the other thing to worry about is that these types of network breaches are caused by people we know. Most network security experts say that security threats come from the people in the organization where breaches have occurred. People through their mischief behavior, wickedness, or mistake always try to destroy their own company’s network and wipe out data. Moreover, these days’ people from large corporations are allowed work from their own place connecting remotely to the organization’s network. These people are also best source of security threat if they are not monitored properly. Good knowledge
of who the potential enemy is and how they attack the network is important in order to secure the network.

9. Enemies to the Network

9.1 Hackers

In general, a hacker refers to a computer criminal, for which the most appropriate term would be cracker. Hackers are usually proficient in network security, computer networking and topics related to computer/network intrusion. Most of the hackers normally leave their footprints like a joke application or message on the computer screen.

Fig 7 showing a hacker at work:
Hackers/crackers are very dangerous as they steal or damage sensitive data, crash the entire computer systems, defacing the websites, track the financial information and finally create hazard to the organizations, customers and partners. Some hackers who do not know how to use the hacking applications create an even adverse effect by trying them out without understanding how they work and their effects.

9.2 Employees unaware of security measures

Some of the employees overlook network security rules focusing mainly on their specific job duties. For example, they might set up passwords which are very simple for a hacker to guess or predict using their common sense or using any of the available password cracking software utility. Employees sometimes unknowingly cause security threats like accidental contraction and spreading the computer viruses. The main source of virus is downloading files from the internet or through a removable disk/media. Employees who transfer data using external media can unknowingly infect their company’s network with the malicious software they might have picked up from a computer outside the network or saving files downloaded from the internet. Employees though they are computer geniuses or experts can make mistakes like improper installation of virus protection software or ignoring the security warnings regarding the threats.

“Ninety-one percent of respondents detected employee abuse of Internet access privileges.”

—Annual Computer Security Institute and FBI Survey, 2001

9.3 Aggravated Employees

The other type of people who willingly cause harm to the network of their organization are reprimanded, fired or laid off staff. These people are more dangerous because they are aware
of the security measures on the network which makes it very easy for them to crack through the network, also they are aware of the location of the most crucial and sensitive data. These people intentionally spread viruses through the network and also delete the sensitive data.

9.4 Mischievous Employees:

Some of the employees who are mischievous and curious about the sensitive/confidential data will try to gain unauthorized access to the data. These people are not that harmful, all they try to do is make data inaccessible to their competitors, access others e-mail, check the salary of his co-worker. These people not usually harmful but sometimes they are a threat, previewing company’s financial information, human resources data, and medical records.

9.5 How do these enemies affect:

9.5.1 Viruses

A virus is a software program which can copy itself and infect a computer without the authentication or knowledge of the user. A virus can spread from one computer to the other when its host is sent to the other computer in the network, through internet or through removable media. Viruses are the well known network security threats.

“85 percent of respondents detected computer security breaches within the last 12 months, up 42% from 1996.”—Annual Computer Security Institute and FBI Survey, 2001
9.5.2 Trojan Horses

Trojan horse commonly referred as “Trojan” is a malware which appears to perform a function, but also performs disclosed malicious functions. Trojans can remove files, data and make a computer more vulnerable to attacks.

9.5.3 Attacks

Several types of networks attacks have been documented and are classified into three types:

- Reconnaissance attacks
- Access attacks
- Denial of Service (DoS) attacks.

Reconnaissance attacks are the type of attack in which hackers gather data which can be used to later compromise security of the network.

Access attacks are made to find the loop holes to attack a network using authentication services and File transfer protocol to gain access to e-mail, databases and sensitive data.

A DoS attack is a type of attack which prevents access to the computer system. This is done by sending a large amount of malicious data to a computer that is within the network.
9.5.4 Data Interception:

Data transferred through a network can always be subjected to interception by unauthorized users. The interpreters can always modify the data that is being transmitted. Data interception can be done using various methods like IP Spoofing.

9.5.5 Spam:

Spam is usually referred to an unsolicited electronic email or unsolicited advertising e-mails which contain links to malicious websites which can copy the data from the user computer.

9. Security Tools

10.1 Security Tips

1. Encourage employees to create passwords that are not strong and cannot be tracked.

2. Make a mandatory rule for employees to change passwords frequently.

3. Make sure your anti-virus software is current.

4. Provide training to employees about the security threats through e-mail attachments.

5. Create and implement a comprehensive network security solution.

6. Check your security measures frequently.

7. When an employee leaves a company or is laid off, remove the employee’s privileges to access network immediately.

8. If people work from home, make sure the server is well secured, and centrally managed for remote traffic.

9. Web server software should be updated regularly.

10. Never run any irrelevant network services.
10.2 Intrusion and Detection

Organizations prevent unauthorized users from entering into their network. Not only users they can also stop viruses. Firewalls are not always efficient in stopping the intruders once they have crossed the firewall than we can’t stop their access. Sometimes the user doesn’t even know that his system is been hacked or been used by an intruder. To identify this and to detect the intruders and to have a check on their transactions we are building a firewall which can detect and can be customized. An Intrusion Detection System (ISD) provides network surveillance. It also analyses the stream of the packets that is we can see the packets coming and leaving our network. When an unauthorized activity or attempt is detected than it will alarm the management with all the details of the activity and it can also sometimes send a request or an order to other routers in the network to delete the unauthorized session. These Intrusion Detection Systems are equivalent to the spy cameras, security devices, monitoring sensors and others for a network.
11. **What is a Packet Filtering Firewall?**

Firewalls are of many different types of which a packet filtering firewall is the fundamental, comes under the basic category of firewalls. The packet filtering firewall works on the network layer, which is the layer 3 in both the OSI model and the TCP/IP model of network architecture. This firewall works on the bottom layer of the protocol stack. The basic principle involved in this firewall is it allows the packets to go through them or drops them basing on a set of protocols (rules) which are usually access control lists. If the packet is dropped a message is forwarded to the sender telling him/her that the packet was dropped. The packet filtering capabilities of the firewall varies a lot between different vendors. A packet filter will basically work on the following:
a. The source address of the packet (allow the packets for a particular IP range and block all the other packets)

b. The destination address of the packet (a packet assigned for a particular IP address are not allowed to pass)

c. Source port number and destination port number

d. A particular protocol type

e. The type of network interface that the packet enters

f. Inbound or outbound traffic

g. Fragmentation

h. State of connection

i. Source routing

The following figure shows the working of a packet filtering firewall:
Let us say for example we have a security policy that accepts email from every website on the internet except aol.com. Now there are two rules that the firewall administrator needs to
write. The first rule is to not allow any connection from aol.com to our firewall. The second rule that the administrator should write is to allow all the other website emails to be accessible to our firewall. The firewall rules are mainly followed in the most restrictive order to the least restrictive order. If the rules were to be reversed then the first rule which was dropping packets from aol.com would not be performed because the least restrictive rule would come into picture and the packets would be passed.

In order to make the network more secure and to increase the ever decreasing IP (Internet Protocol) addresses, there is a method called Network Address Translation (NAT) that was invented and successfully used in the packet filter firewalls. In the year 1994, a scientist named Kjeld Borch Egevang of Cray Communications wrote the RFC 1631 which was called the “The IP Network Address Translator (NAT)”.

NAT is a very interesting concept. It instructs the intranet (a private network) to use different addresses other than those that it uses for the internet. To illustrate an example, NAT uses the same principles of a Private Branch Exchange (PBX). A telephone company will usually have several thousands of telephone extensions that are internal to the company. When someone makes a call to somebody outside the company, the receiver sees a number that the PBX system uses and not the same extension that people within the company see.

NAT hides the exact private IP address so that the outside world will never know the real IP address. In network address translation the headers of the IP packets are rewritten so as to make it look like the packets are originating from the firewall. Then the incoming packets are translated back and then to the respective machine. So the most important use of NAT is that the public networks are not aware of the internal machines as they are not allowed to connect to the
internal machines in the first place. The public networks are not able to connect to the internal networks because they think that there is only one IP address which is the firewall. So a great security measure is implemented by using NAT which is that the risk of attacking the internal machines of the private networks is greatly reduced.

The big problem facing the computer world now is the lack of new IP addresses. NAT has solved much of this problem. A network administrator chooses the reserved IP address, for example, from the range 192.168.*.* or 10.*.*.*. These addresses are not registered by anybody and are used by network administrators for the sole purpose of networking in a private network area. So in this way thousands of computers can access a single website without having any IP related issues.

For an extra security layer, port level PAT (packet address translation) or NAT is being offered by the packet filtering firewalls. In the business world as more businesses move to ecommerce as a way of marketing, the use of many scripts likes CGI script and applets live java applets are more common. Now this is a security hassle as the script being used is outside the firewall and the database containing important customer data is behind the packet filter firewall where it is secure and cannot be attacked. Using PAT we can fix this problem. On the firewall, the packets are rewritten and then sent to a server which will serve the user request. The server then sends the reply packets which are rewritten again to make it appear that they are originating from the firewall. So PAT is a useful measure to secure the internal machines/servers from outer/external access.

In the earlier years packet filtering firewalls had the following advantages:
a. Skilful management of traffic
b. Less cost
c. Less overhead and very high throughput

But in very big and complex environments, the rules written for the packet filtering firewall cannot be managed. With the passage of time and the internet evolving in a big way with each passing year, the packet filtering firewalls faced many challenges such as follows:

a. The internal machine host and the external machines have direct connections.

b. The packet filters are susceptible to various attacks like IP spoofing in which a system is literally cloned using its IP address.

c. There is no mechanism for user authentication.

In order to overcome these disadvantages, two methods namely dynamic packet filtering and stateful inspection came into place. If we look at the earlier packet filter firewalls, there were direct connections between the internal host machines and the external systems. This allowed the traffic flow and the internal host machines were susceptible to a range of attacks. Because of the lack of security, these attacks were large in number and were successful always.

Dynamic packet filtering came into picture in order to combat the above issue. Basing on the header information of the packet, the dynamic packet filters open and close the ports in the firewall. When all the packets are done moving to their new destination, the firewall closes the port.

The process of analyzing the network traversing it by a packet filtering firewall is called Stateful Inspection. A firewall with this feature enabled has the luxury of looking inside a packet
for the header information and allows the needed commands of an application and restricts the other commands. To be more clear the stateful packet filtering firewall can allow the ‘get’ command in FTP (File Transfer Protocol) and restrict the ‘put’ command. Stateful inspection makes the protocols all the more secure. In the case of UDP (User Datagram Protocol) based protocol applications, filtering is somewhat difficult using static packet filtering as there is no provision for request and response.
12. Working of Firewall:

Fig 10: An algorithm showing the working of our firewall
We have made use of Microsoft Visual C++ and the filter hook driver which is provided in the Microsoft Windows operating systems (2000 and above). The filter hook driver can only be installed on Microsoft Windows 2000 and later versions.

Our firewall is based on the following steps:

- Packet header is extracted
- The protocol that is associated is verified
- The rules are compared
- Check for the source and destination address
- Verify the protocol if it is TCP or UDP
- Allow or drop the packet.

13. Routing of Packets

Routing of packets is a method in which we set a range of addresses for the border router, which includes receiving network packets, determining the addresses, and transmitting the packets to the border router when the defined range of address matches for the determined addresses. The network packets are routed to the border router joining through different network domains.
Fig 11: Routing of packets
### 13.1 Description:

Computer networks enable computers which are at different places in the world to exchange information through, email, web pages, chat messages and other electronic information. Programs divide electronic information into packets for transmission over a network. A packet is like an envelope with a return address as its source and destination address as a packet destination. However packets use Internet protocol addresses to identify source and destination of computers. An internet protocol address can be 32 bits long. Instead of writing out 1's and 0's or an equivalent decimal number, IP addresses are commonly written as a group of four numbers ranging from 1 to 255. Example: 216.27.61.137.

A network packet reaches its destination address through routers by network computers. It is similar like an envelope reaching the destination by a postal office. Each router closely examines the router destination and tries to determine how to send the packet to its destination.

A sender can send the packets using two techniques called Unicasting and Multicasting. In the unicasting the message from a single source to single destination is transmitted. In this process the senders sets the packets destination address to a particular network computer Internet Protocol address, to transmit the message. In the multicasting we send a packet to multiple destinations using a single source to multiple destinations. To send a packet using multicasting, one should set the destination address to an Internet Protocol group address so that the router receiving the packet, which has a group address can forward the message to a single person of the group.
13.2 Summary of Invention:

“In general, in one aspect, a method of routing network packets to a border router joining different network domains includes defining a range of addresses for the border router. In a router forwarding table, receiving a network packet, determining addresses included in the network packet, performing a search on the router forwarding table using the determined addresses, and transmitting the packet to the border router if the defined range of addresses matches for the determined addresses.” Source: United States Patent 6711172

It may include one or more features like the search may be a longest match search. The network domain consists of a Protocol Independent Multicasting (PIM) Sparse-mode domain. Rendezvous point services determine group of addresses and defines the range. The Protocol Independent Multicasting sparse mode domain is in network domain. The addresses are serviced by a rendezvous point.

Defining a range of addresses can be achieved by adding a prefix table to the router forwarding table for different range of addresses. Determining the address may also include determining the address of the source and destination of network packet.

The router forwarding table may include corresponding states, source and group address pairs. Transmitting the packet to the border router may include transmitting the packet over an output interface comparing to the state revealed by longest search.

In general, this features a model for routing the network packets to a Protocol Independent Multicasting (PIM) with a sparse mode domain in a different network domain. This method includes receiving a protocol independent state transmitted by protocol independent
multicasting border router to a rendezvous point, rendezvous point determines the group of addresses and the state in a router forwarding table on the bases of group addresses of the PIM rendezvous point.

In different aspects, a computer program disposed on a readable medium consists of instruction for creating a router which helps to route network packets to a border router joining different network domains.

The computer program includes instructions that define a range of addresses in router forward table of the border router, receive a network packet, and also decide addresses included in the network packet, and execute a search on the routing forwarding table using the decided addresses, and perform the transmission to the border router if the defined range of addresses matches the determined addresses.

Rewards of the invention will become apparent in view of the following description, including the figures.

BRIEF DESCRIPTION OF THE FIGURES

FIG. 1 shows members joining a multicast group at a rendezvous point.

FIG. 2 is a shows member receiving multicast messages via the rendezvous point.
FIG. 3 shows members receiving multicast messages via a shortest path tree.

FIG. 4 shows a router forwarding table.

FIG. 5 shows of networks joined by border routers.

FIG. 6 shows distribution of rendezvous point data.

FIG. 7 illustrates border router registration.

FIG. 8 shows of a router forwarding table including entries for border routers.

FIG. 9 is a flowchart of a process for building a router forwarding table including individual entries for border routers.

FIG. 10 is a flowchart of a process for building a router forwarding table including ranges for border routers.

FIG. 11 is a diagram of a router forwarding table having ranges for border routers.
FIG. 12 is a flowchart of a process for routing packets in accordance with a router forwarding table.

13.3 Description of the preferred embodiments

With the help of Multicasting we can transmit the same message to dissimilar members in a group.

However all the groups are not the same. In some groups there is large number of members due to the neighboring routers. In other groups there may be only few members across the network. These differences in group composition complicate multicasting. Multicasting techniques should be used for the members who are in large group instead of the smaller group in order to use them efficiently.

Protocol Independent Multicasting (PIM) provides a different multicasting mode suitable for different kinds of groups. These Protocol Independent Multicasting modes can efficiently multicast data to a large number of members in a group.

It can efficiently multicast data when a group has a lower number of members.
In this figure 1 we can see the PIM network domain 100 in operating sparse-mode. It has rendezvous points names 108 a, and 108 c that match multicast source 102 with multicasting groups 104a and 104b. A local router gets a membership request from a computer to join a multicast group. This will help the local router to triggers transmission of a JOIN message to a rendezvous point. The multicast data sent to the rendezvous point for distribution point, all the copies are received by the group members. As shown in the diagram the computer 104a can join a group by sending an IGMP message to local router 106b. The rendezvous point 108a receives a JOIN message from the router 106d over a network router.
FIG. 2
In this diagram 2 the group members 104a, 104b receive multicasting messages from source 102. The rendezvous point 104a receives multicast data from 102, for forwarding the group members 104a, and 104b.

Transmitting the messages to the 104a and 104b may not be efficient if they are sent by the rendezvous point 108a. If we have to find the best and efficient path this will consume many resources.

Despite during the periods of high network traffic, it may be worthwhile finding an alternate path for the extra cost.
In diagram 3, the more efficient path from source to group members is constructed by the PIM, after establishing a multicasting session at a rendezvous point. This is also called the switching to a shortest path tree. For example router 106c receives multicast messages by
passing rendezvous point 108a from router 106a. Group members 104a, 104b can send messages to halt transmission of packets from the rendezvous point 108a after finding the shortest path tree.

In diagrams 1-3, Using interfaces; the router 106c sends and receives packets to and from network routers (Tagged “1” through “6”). For example, in FIG. 1, router 106 c receives a message called “Join” on interface “4” and transfer the message to rendezvous point 108a over the interface “1”. Using routing forwarding table 112c the router 106c determines where to route a packet, this correlates incoming packet addresses with outgoing interfaces.
FIG. 4
In diagram 4, IP source and destination addresses 110 with different “state entries” 120,128 are correlated by router forwarding table 112. Router are instructed by state entries 120,128 where to receive the packet. A router can determine the state entry 120,180 using the routing forwarding table 112 to determine the IP source and group destination addressed of a received packet and can forward the packet accordingly.

By increasing group addresses 110 the forwarding table 112 can organize entries. The IP addresses from 224.0.1.2.116 through 239.255.255.254 from 130 group addresses. The range of group addresses are 116 and 130 where 116 is the lowest and 130 is the highest for the list of addresses 110. Source address 118,132 can be combined with each group address to produce a group and source address pair. Routing forwarding table uses different access keys for the different pairs.

State entries 128,120 correspond to individual addresses or different address ranges.

Protocol Independent Multicasting determines various types of states like (S, G) state and an (*, G) state.

States like (S,G) state 128 can be used to handle packets having a particular group address G and source address S. As shown in diagram 3 the router commonly defines shortest path tree using Source S and state G.

As shown in the diagram 4 the internet protocol source address 10.10.10.1 and group address 225.32.0.28 is handling by the sample (S, G) state 128. A router can consult the state entry’s interface information 138,140 using the group and source address pair the router can route the packet. The input 138 and the output 140 information includes in the interfaces. The
router can send the packet over the outgoing interface 140 only when a packet arrives over an incoming interface 138. The packet can be transmitted over interface “4” over the router, if a packet having a source address of 10.10.10.1 group address of 225.32.0.28 that arrives over interfaces “6”.

The states (*, G) can correspond to a different range of group and source address pairs. These group states are produced by join messages received by a router by a rendezvous point. Here the * is used to represent as a wild card to match any packet having similar group.

As shown in the diagram the *,G state entry 120 covers all group and source address pairs which have the group address of 225.32.0.28. The router can transmit the packet in accordance with the (*,G) entry 120 interface 124, 126 information when it receives a packet having a group address . The router will transmit the packet over interfaces “4” and “5” if the packet comes over the interface “1”. This is also called the multicasting of router in 106c, as shown in diagram 2.

The forwarding table 112 can overlap or nest. For example, the (*, G) covers multiple range of addresses the (S, G) 128 state entry includes 120 state. Covering the packets group/source address pair the router uses the narrows entry which is called longest match search. For example if an incoming packet has a Group address of 225.32.0.38 and a Source address of 10.10.10.1, a longest path match search will result in use of the state’s S and G of 128 instead of the (*,G) state 120 , since the S,G state of 128 covers a single group/source address pair while the (*,G) state 120 covers many pairs of source and group. That means the (s,g) state 128 covers a limited set of group, source pairs compare to (*,G) 120. If the incoming packet has a source address of 10.20.20.8, and the group address of 255.32.0.28, will result in use of the (*,
G) state 120 for the longest match.
Figure 5 shows the PIM routers 106a-106c, 108a-108c configured to operate within a common boundary defined by the Protocol Independent Multicasting router 140a, 140b. The domain 100 is the area bounded by the border routers 140a, 140b. The Protocol Independent Multicasting domain 100 borders network domain 144 similar like a Distance Vector Routing Protocol domain.

The border routers 140a, 140b interoperate with different types of multicasting networks 144. In this way the protocols of both connected networks 140a, 140b will run.

Multicast data injected from a border router 104b from a group source 102 in the Protocol Independent Multicasting domain 100 into a different domain 144 for delivery. Protocol Independent Multicasting defines an (*,*.RP) state for the routers to send the packets to border routers 140a, 140b.

In the diagram 5 it shows the PIM routers 106a-106c, 108a-108c configured to operate within a common boundary defined by the Protocol Independent Multicasting router 140a, 140b. The domain 100 is the area bounded by the border routers 140a, 140b. The Protocol Independent Multicasting domain 100 borders different network domain 144 similar like a Distance Vector Routing Protocol domain.

The border routers 140a, 140b interoperate with different types of multicasting networks 144. In this way the protocols of both connected networks 140a, 140b will run.

Multicast data injected from a border router 104b from a group source 102 in the Protocol Independent Multicasting domain 100 into a different domain 144 for delivery. Protocol
Independent Multicasting defines an (*, .RP) state for the routers to send the packets to border routers 140a, 140b.

FIG. 6
Diagrams 6 and 7, shows about the border routers register (*,*, RP) states in PIM domain routers. As shown in diagram 6, a bootstrap router 152 assigns various group addresses which apply to various rendezvous points 108a-108c. These ranges might overlap. The network traffic can be balanced by assigning ranges which are carried by each rendezvous point 108a-108c. The domain 100 is flooded by bootstrap router 152, which includes border routers 140a, 140b with data 150 describing the group serviced by every rendezvous point 108a-108c. RP-set is known as data 150.

The prefix notation includes an IP address and is the totality that represents the group address. For example, a group address range of 225.32.0.0 and 16 indicates that the group range covers group address from 225.32.0.0 to 225.32.255.255. In different words the first 16 bits match the first 16 bits of the specified range of group addresses.
In figure 7 the RP-set 150 sends a receipt to the border routers 140a, 140b, by sending
(*, *, RP) state entry messages to each rendezvous point 108a-108c listed in the RP-set. As
shown, routers 106c between rendezvous points 108a-108c and 140a, 140b can receive multiple
(*, *, RP) messages. Messages like (*, G) and (S, G) entries, the routers 106c can add the state
(*, *, RP) to the forwarding table.
In figure 8, the states (*,*, RP) entry states 158,156,154 added to router table 112. The source address of the state (*,*, RP) in the forwarding table corresponds to the IP address of the receiving an (*,*, RP) of the rendezvous point. The group address for each state (*,*, RP) is set to
“224.0.0.0”. This group address for the state (*, *, RP) is set to the “224.0.0.0”. Packets don’t ordinarily include the address. In this there is a straightforward process the (*, *, RP) state to a packet can cause a router to look up data in the RP-set which access the router forwarding table 112.
Figure 9 shows a method in which 160 for routing packets to the border routers 140a and 140b, when a packet’s address pair of source and group do not match a state entry (S,G) or
state entry \((*,G.)\). As shown in the diagram after storing the \((*,*,RP)\) state entry in the router forwarding table, a router finds a longest match search on a received packets source and group addresses. If the packet doesn’t match a state entry, the packet will correspond to \((*,*,RP)\) different state. The router can determine \((*,*,RP)\) matches by looking RP-set data to decide if a state has been checked at a group address of 224.0.0.1 and the source address representing to the internet protocol address of the rendezvous point. The entries listed output interfaces if the \((*,*,RP)\) state is found. If not the router drops the packet. The method requires different search in multiple table. This additional search can consume maximum amount of time and resources.

Assigning Forwarding table ranges to the border routers
Figure 10 shows a process 180 than can reduce the number of look-ups and the amount of time needed to determine whether and how to send a packet to a border router. After receiving the RP-set from the bootstrap router and receiving an (*,*,RP) state from a border router, the process 186...
determines the range of group address covered by the RP 186. For example, as shown in FIG. 6, RP1 is responsible for two groups 225.32.0.0/16 and 226.32.0.0/16. The router adds 188 two corresponding entry states to the forwarding table known as an (*,G/prefix) entry states. The (*,G/prefix) entry state, similar to an address range expressed in prefix notation, can cover multiple group addresses. If a longest match of a packet's source and destination group addresses falls within the (*,G/prefix) range, the router can forward the packet to one or more border routers using the interface information of the matching (*,G/prefix) state."
FIG. 11
In figure 11 the router forwarding table 112 that includes various ranges for the border routers (190-200) in addition to a range corresponding to a state 120. The longest match is the state entry 190 if the packet received is having a source address of 10.27.38.10 and group address of 225.0.0.1. The router uses “6” and “7” interfaces to forward the router 140a, 140b packets to the border.
FIG. 12

RECEIVE PACKET

DOES LONGEST MATCH OF PACKET (S,G) MATCH CORRESPOND TO INSTALLED (*,G/prefix) STATE?

SEND PACKET OUT VIA OUTGOING INTERFACES LEADING TO PMBR ROUTER(S)

DROP

Source: http://www.patentstorm.us/patents/6711172/description.html
In figure 12 shows a method 202 using a routing forward table to forward the packet. In this method the 202 receives a packet 204 which decides the packets the source and internet protocol address. The process 202 then executes a longest match lookup 206. If the longest match corresponds to a (S, G) or (*, G) prefix state. The packet will be forwarded by the output interface remarked by the state 210. Otherwise the router doesn’t transfer the packet 208. By clearly defining a (*,G/prefix) state for the state (*,*,RP) state, the routing to the border routers don’t require a special handling or time requiring searches in the different tables.

14. **Economic Justification**

This part of the report emphasizes on the financial validation of the project and NetKapp. In the following sections detailed finance control model, the organizational structure, competitors, Market size, the SWOT analysis, decision making method, revenue forecast, break-even analysis, Gantt chart for each project, Balance sheet, Cumulative distributive function, Probability density function and different ratios that validate the project economically are explained.

In the last decade, huge data thefts and cyber crimes have increased, which urged the evolution of complex protection algorithms. With increasing complexity and technicality the protective systems have been broken into sectors. Cyber security ranges from mere authorizations to stopping virus attacks and Hackers from intruding in to the networks. NetKapp deals with developing and supporting security systems for companies that need customized algorithms that are of their interest.

NetKapp’s customer base ranges from individual users to large companies who are interested in using Firewalls for their network’s protection. With the rapid growth of the Internet
industry, NetKapp’s prospect to flourish worldwide has grown. The company has always believed in its concept of ‘Customized security’ that makes it different from its competitors. With huge scope for development each year in this huge Billion dollar market, NetKapp is looking to reach every individual using the internet.

The initial investment for the company is about $243,000 which would involve all the variable and fixed costs that the company incurs in the first year. Being a product and project based company has given an additional feature to the company’s interest and so it is expected to breakeven in the second quarter. The company’s forecast of the revenue has projected a growth of 30% every year.

14.1 Problem Statement:

The biggest challenge most companies face today is with their data base security. Cyber threats have increased with increasing technology. Most common of the threats are:

- Intruders can easily enter the network.
- Weak network structure causing congestion easily.
- Lack of employee awareness about data base and network security
- Limited IT resources to secure data.
- Data is located at disparate terminals and servers with inter-connected networks.

14.2 Solution and Value Proposition:

NetKapp provides software integrated solutions for securing data from intrusions. It specializes in providing customer specific features to increase security options. As any of its
competitors it focuses on giving solutions based on base technologies which is proven and is being used. Also updating to the pacing technologies and research for new technologies is the motto of the company that will help us provide more robust products. NetKapp takes complete care of the network by analyzing its functionality and then propose the best solutions which suit the company database. Creating a better architecture for working of the networks fosters its functionality and the products secure data which gives the company extra performance in its data storage and security.

14.3 Market Size:

Figure 4 : Market Size of Firewalls

A websense white paper- Security Appliance Market.

Retrieved on May 12, 2008 from www.websense.com

With the advent of the new Internet era it has always become important to keep safe your valuable data. The cyber crimes are increasing every day raising the scope for the security technology to develop. At the midst of such need, the market for firewalls has become extremely fast growing. According to IDC, the total worldwide market size for security appliances is expected to exceed $5.4 billion by 2008. The majority of this market comprises of firewalls, which contributes to about $2.1 billion of the market.
The above shown is the market size for the firewalls in the past 8 years. The market size is now 20 times as big as it was a decade back. This market is expected to grow the fastest at approximately 70.3% compound annual growth rate (CAGR).

### 14.4 Competitors:

For NetKapp to survive in this ever growing market, it is important to plan ahead in terms of technology. NetKapp strongly believes in technical management. To manage technology properly one has to first analyze the market and divide the technologies into three broad groups. The company has to know as to which has to be used for a product.

- **Base Technologies:** These are the technologies that a firm must master in order to sustain in the market. NetKapp has successfully identified and is releasing a free version of the firewall online, which keeps them in the race of attaining any market share. The base technology for NetKapp is a firewall common to any individual user and it is concentrating in providing timely updates for it.

- **Key Technologies:** These technologies give a competitive edge over the competitors. NetKapp’s concept of customizing security is a defying factor that makes it different from its competitors. Also, its support program provides constant upgrades to the product hence making protection possible even with newer threats.

- **Pacing Technologies:** These technologies are those that can come into existence and become the future’s key technologies. NetKapp has not concentrated in mastering it yet. But soon, NetKapp plans to have a R&D department that would make things easier and safe.
Besides having an edge in technology, it is also important to market and support your product after release. Keeping the customers for a long time through maintaining a good customer relationship is the key to the success of any firm.

Some of NetKapp’s competitors are Barracuda Networks, Zone Alarm, PCtools, Comodo and others. As NetKapp is located in the silicon valley it is easier for the company to be in-phase with the technology and compete with its senior competitors.

14.5 Customers:

Due to the global market of the product, NetKapp has attained popularity already with the free release versions available for download. Though the release was a basic firewall that does not include whole lot of features, it made sure to protect customers for cyber attacks. The customer base of NetKapp not only extends to individuals using computers and networks but also to the companies because of the features and specifications NetKapp can provide them.

Some customers of NetKapp are People connect, Converge, Forxone, Tips group, SLT, Manatt, 360 FLEX, SOLYNDRA, NETCLEARLY, TRIPOD, FENWICK & WEST LLP. NetKapp concentrates on the start up companies and those who use outdated system of protection.

Target Customers:

Since development of the firewalls with various new features efforts are always ongoing, the sales department is constantly networking with companies that are looking for their data safety. Usually most the small startup companies do not research on the available technology available and believe that the existing ones are suited for their company. But when they are
explained about the use and comfort of the customized structure of security technology that best suits them, it is evident that it will gain more opportunities for good business. The development and design is subjective, which means it is always changing. Since security and privacy of company’s confidential information is a prominent part for any company, updates are always being released and revised for new customer demands and newer threats.

**Sales Strategy:**

The process of developing and releasing a product starts with contacting companies for business. Since firewall designs are unique due to different working characteristics of each company, the wanted algorithm is usually specific. Being able to persuade the company to specify his needs and able to explain them about NetKapp’s ability to provide the same is especially an important aspect. Suggest the customers to join their referral group or giving them special offers for huge contracts is another strategy that is successful in project based companies. NetKapp also apply consultative strategy, which is asking the customers questions to uncover their problem and to see if NetKapp’s service can help them.

The company has two divisional sales managers and four sales representatives who are evenly distributed. The sales representatives are responsible of bringing awareness about the problem to the companies and solution NetKapp has to offer. Their managers then talk about the final deal and set the customers interest in the company.

After sales service is always important, as the actual sales does not mean selling the products but keeping the customer for life. Winning and keeping the customer’s mindshare is one key technique NetKapp does not miss to inculcate.
Customer Relations:

NetKapp maintains good and friendly customer relations. Making efforts in collecting and evaluating the right data from interviewing the customers is the key. NetKapp is honest with their customers and usually do not over or under commit to something that they cannot attain for e.g. project finish time, adding new features that NetKapp is not capable of providing.

14.6 Capital Estimation:

Below is the cost estimation for NetKapp to start. Large percentage of the finance goes in as the salaries to be paid to the employees. This is also a recurring cost that the company has to bear every month. Otherwise, NetKapp being a software development company does not incur any recurring costs other than a small amount towards the lease of the building and any stationary. Every component required to start up the company has been taken into account in the below estimation of cost along with first month’s salaries for the employees. It is estimated that the total cost for the company for the first month is expected to be about $243,000. The type of investment field in the table below explains what kind of investment it is and if it repeats.

<table>
<thead>
<tr>
<th>cost/unit</th>
<th>units</th>
<th>$$</th>
<th>Type of Investment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item Description</td>
<td>Cost</td>
<td>Quantity</td>
<td>Total Cost</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>Office Furniture</td>
<td>$12,000.00</td>
<td>1</td>
<td>$12,000.00</td>
</tr>
<tr>
<td>Computers</td>
<td>$1,000.00</td>
<td>43</td>
<td>$43,000.00</td>
</tr>
<tr>
<td>printers scanners + copiers + Misc</td>
<td>$4,000.00</td>
<td>1</td>
<td>$4,000.00</td>
</tr>
<tr>
<td>Rent and other utilities</td>
<td>$6,000.00</td>
<td>1</td>
<td>$6,000.00</td>
</tr>
<tr>
<td>Salaries for engineers</td>
<td>$5,000.00</td>
<td>15</td>
<td>$75,000.00</td>
</tr>
<tr>
<td>Salaries for Managers</td>
<td>$7,000.00</td>
<td>7</td>
<td>$49,000.00</td>
</tr>
<tr>
<td>Salaries for top Management</td>
<td>$12,000.00</td>
<td>4</td>
<td>$48,000.00</td>
</tr>
<tr>
<td>Software and copyrights</td>
<td>$6,000.00</td>
<td>1</td>
<td>$6,000.00</td>
</tr>
<tr>
<td><strong>Total Cost</strong></td>
<td><strong>$243,000.00</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 1: Capital Estimation of the company

**Income Statement and Estimation**

The income statement shows the company’s revenues, expenses, net income or net loss for a certain period of time. At NetKapp the time period at which the income statements are generated is for every quarter. It is of great interest to the investors as it is an indication of anticipating the company performance in the future and a record of a company’s operating results for the whole year.

![Figure 6: Profit and Loss graph](image)

**14.7 SWOT Analysis:**

NetKapp has always taken great interest in identifying and developing strategies to build up a proofed technique and adopt it. The company believes and induces the concept of SWOT analysis which helps the company find ways to reduce threats create opportunities, increase strengths and decrease the weaknesses of the company.

Providing emergency support and varying interests are the big threats to the company. NetKapp plans to build a base model to all kinds of solutions which will reduce the amount of time to provide specific products. Also knowledge of the base model can help trigger problems at emergency.
14.8 Investment Capital Requirements:

The company will need a capital of $243,000 as the initial investment. We would like to raise a capital of $150,000 from private investors and bank loans. As most of the investment goes towards the salaries of the employees which are an ongoing expense, we would pay them through personal funds and the money obtained from projects. Our forecast below projects a break even in the 13 month and we are confident that with the current scenario of cyber security alert we should be able to reach our benchmarks.

14.9 Break Even Analysis:

We Break Even in the 13 month if we anticipate a growth of 1% revenue every month on the online business and we expect to increase by 1 project every quarter. We also increase in personnel by 2 employees every quarter after 3 quarters.
Figure 7: Break Even Analysis

14.10 Organizational Structure: (Personnel) & (Business and Revenue model)

NetKapp believes in ‘KISS’- Keep It Simple and Sweet, which is evident from its organizational structure shown below that has a clear hierarchical property and defined activities for each level in it. The company is headed by the CEO who is responsible for the company’s financial being and making it better. He is responsible for bringing in opportunities and more business to the company. He has the CTO, CFO and the CSO reporting in to him. Each of these mentioned have dedicated work tasks to them.

The CTO is responsible for all the technical operations in the company. At NetKapp this position is filled by Mr. Karthik Reddy. His team is the technical backbone of the company who provides and allocates the resources for each project and product. The HR managers and the VP operations report to him. The Vice President (VP) operations is responsible for leading his team in developing the best product and conduct R&D to check on new threats and sense any threat that can be posed in the future. His team is responsible for providing periodic updates to keep the
product functioning at its best performance level. Also his team is responsible for providing support to all the NetKapp’s product. The HR managers hire professionals that best suit the company’s interest. The Team Leaders lead a small team who are responsible in developing the customized firewalls for the clients. They report directly to the VP -operations

The first and the basic function of the management are controlling. Controlling is a very important feature to the success of any company and any product, as it ensures the proof of the success plan. The crucial part of controlling deals with the finances. This includes managing money; financial planning and put in order the control systems to ensure a successful company. Ms. Niharika Manyala, CFO of the company is responsible for implementing and bringing up financial controls within the company. The Finance VP and Budgeting Manager assist the CFO in deciding if a project is economically viable for the company. The CFO also makes sure that the teams are working on the projects at their best ability and strives to make them better. The Finance VP and the Budgeting Manager is responsible to maintain and track the sales and expenditures of the company and constantly find loopholes in extra expenditures. It is the maintenance of these records that make it possible to monitor whether the company’s financial strategy is working, whether the organization is financially viable (able to survive), and whether the money is being well spent in achieving the company’s objectives. A good bookkeeping system makes it possible for an organization to be financially accountable to all its important stockholders. NetKapp has adopted good bookkeeping system that makes it possible to monitor the company’s financial strategy is working, and how the money is being spent.

NetKapp’s bookkeeping system enables key personals to view its accounting book anytime of the day. Thus NetKapp is able to present to the stockholders a clear accounting
balance on its financial strength. NetKapp undergoes external auditing once a year and because of its outstanding bookkeeping system, the auditors are able to finish auditing on time. Besides a good bookkeeping system, it is also very important to have a good financial policy which supports and helps drive the company’s vision. The CFO is also responsible to make the policies and guidelines for the company’s proper functioning. A policy is not a considered a legal document. It is an agreed upon set of principles and guidelines for a key area of activity within an organization. A policy expresses how the organization goes about its work and how it conducts itself. A good policy expresses a fair and sensible way of dealing with issues. While the policies can be changed, no organization should change its policies too often. These policies are intended to guide the work of your organization for a reasonable length of time. Once a policy becomes organizational practice, and has been approved by management, it is binding to everyone in the organization.

The CSO of the company Mr. Pradeep Aitha leads his divisional Sales Managers and is responsible in getting businesses to the company and sell the products that NetKapp develops. The sales Managers are geographically divided. Besides just looking at marketing the product it is also the prime responsibility of the CSO and his team to make sure the policies and guidelines of the company are followed. CSO is so important in a project based company like NetKapp, as the structure of the whole business begins with this team, identifying and getting projects to the company.

Figure 1: NetKapp Organizational structure
14.11 Financial Statement:

Financial statements in essence show the financial condition of a company. The two major types usually used include the income statement and the balance sheet. The two documents give information about controlling cash and credit flow which are essential to the company’s survival. NetKapp utilizes both types for a variety of purposes such as:

- It helps the top management to make decisions which can affect the finances of the company.
- Illustrate the well being of the company to the prospective investors.
- It is used for auditing purposes.

Norden-Rayleigh Analysis of Financial flow

To analyze and study the buildup, peak and taper of a project’s development over time, Norden-Rayleigh curve is modeled below.

- Cumulative Funding Over Time:

\[ V(t) = d (1 - e^{-at^2}) \]
<table>
<thead>
<tr>
<th>D</th>
<th>A</th>
<th>t</th>
<th>(-at*t)</th>
<th>e(^{-}\text{at}*t})</th>
<th>1 - e(^{-}\text{at}*t})</th>
<th>v(t)</th>
</tr>
</thead>
<tbody>
<tr>
<td>40000</td>
<td>0.4</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>0.5</td>
<td>-0.1</td>
<td>0.904837418</td>
<td>0.095162582</td>
<td>3806.503</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>1</td>
<td>-0.4</td>
<td>0.670320046</td>
<td>0.329679954</td>
<td>13187.2</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>1.5</td>
<td>-0.9</td>
<td>0.40656966</td>
<td>0.59343034</td>
<td>23737.21</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>2</td>
<td>-1.6</td>
<td>0.201896518</td>
<td>0.798103482</td>
<td>31924.14</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>2.5</td>
<td>-2.5</td>
<td>0.082084999</td>
<td>0.917915001</td>
<td>36716.6</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>3</td>
<td>-3.6</td>
<td>0.027323722</td>
<td>0.972676278</td>
<td>38907.05</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>3.5</td>
<td>-4.9</td>
<td>0.007446583</td>
<td>0.992553417</td>
<td>39702.14</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>4</td>
<td>-6.4</td>
<td>0.001661557</td>
<td>0.998338443</td>
<td>39933.54</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>4.5</td>
<td>-8.1</td>
<td>0.000303539</td>
<td>0.999696461</td>
<td>39987.86</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>5</td>
<td>-10</td>
<td>4.539999E-05</td>
<td>0.9999546</td>
<td>39998.18</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>5.5</td>
<td>-12.1</td>
<td>5.55951E-06</td>
<td>0.99999444</td>
<td>39999.78</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>6</td>
<td>-14.4</td>
<td>5.5739E-07</td>
<td>0.999999443</td>
<td>39999.98</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>6.5</td>
<td>-16.9</td>
<td>4.57534E-08</td>
<td>0.999999954</td>
<td>400000</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>7</td>
<td>-19.6</td>
<td>3.07488E-09</td>
<td>0.999999997</td>
<td>40000</td>
</tr>
</tbody>
</table>
Funding Profile Over Time:

\[ V(t) = 2ad e^{-at^2} \]

<table>
<thead>
<tr>
<th>D</th>
<th>A</th>
<th>t</th>
<th>(-at^2)</th>
<th>e^{-at^2}</th>
<th>v(t)</th>
</tr>
</thead>
<tbody>
<tr>
<td>40000</td>
<td>0.4</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>0.5</td>
<td>-0.1</td>
<td>0.904837418</td>
<td>14477.4</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>1</td>
<td>-0.4</td>
<td>0.670320046</td>
<td>21450.24</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>1.5</td>
<td>-0.9</td>
<td>0.40656966</td>
<td>19515.34</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>2</td>
<td>-1.6</td>
<td>0.201896518</td>
<td>12921.38</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>2.5</td>
<td>-2.5</td>
<td>0.082084999</td>
<td>6566.8</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>3</td>
<td>-3.6</td>
<td>0.027323722</td>
<td>2623.077</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>3.5</td>
<td>-4.9</td>
<td>0.007446583</td>
<td>834.0173</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>4</td>
<td>-6.4</td>
<td>0.001661557</td>
<td>212.6793</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>4.5</td>
<td>-8.1</td>
<td>0.000303539</td>
<td>43.70964</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>5</td>
<td>-10</td>
<td>4.53999E-05</td>
<td>7.263989</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>5.5</td>
<td>-12.1</td>
<td>5.55951E-06</td>
<td>0.978474</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>6</td>
<td>-14.4</td>
<td>5.5739E-07</td>
<td>0.107019</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>6.5</td>
<td>-16.9</td>
<td>4.57534E-08</td>
<td>0.009517</td>
</tr>
<tr>
<td>40000</td>
<td>0.4</td>
<td>7</td>
<td>-19.6</td>
<td>3.07488E-09</td>
<td>0.000689</td>
</tr>
</tbody>
</table>

Scale

X-axis - time in months

Y-axis - dollars

15. References

  Upper Saddle River, NJ: Prentice Hall

  *Firewalls and Internet Security: Repelling the Wily Hacker*.
  Reading, MA: Addison-Wesley.

*Building Internet Firewalls.*


San Jose State University

http://engr.sjsu.edu/bvenka/


*Routing of packets, 54.*

Retrieved October 5, 2008, from

http://www.patentstorm.us/patents/6711172/description.html


Retrieved October 5, 2008, from

http://www.patentstorm.us/patents/6711172/description.html


Medard, M. Lumetta, S. Liuyang Li (May 2002)

*A network management architecture for robust packet routing in mesh optical access networks.* *Selected Areas in Communications Volume 20,* 822 – 833.