सत्यमेव जयते

ACHIEVING EXCELLENCE IN AUDIT AND ACCOUNTS THROUGH DEVELOPING, IMPARTING, PRACTICING AND UPGRADING SKILLS AND COMPETENCES

INDIAN AUDIT AND ACCOUNTS DEPARTMENT

Regional Training Institute, Chennai

(Centre for Excellence)

In Search of Excellence Series – Research - Study Material No.20

RESEARCH - STUDY MATERIAL ON

FIREWALLS

Centre for Excellence
IA&AD
RTI
CHENNAI

361, Anna Salai, Chennai 600 018.

Preface

RTI, Chennai is making continuous efforts to bring out Research Study materials on various topics. In that line, I have great pleasure in releasing yet another volume on ôFirewallsõ.

We are in a seemingly endless race to protect our information, systems, and communications before the hackers can bring us down. There is a spectacular growth in information infrastructures, but with many holes in them to present an inviting target to those who would hijack systems and data for fun or profit. Now, while the technological capabilities continue to expand, the vulnerabilities too have increased alarmingly. These vulnerabilities are exploited by threats and the impact caused is alarming. Every time a company connects its internal computer network to the internet, it faces potential danger (i.e., a threat that damages revenue generation, decreases profitability, lowers worker productivity, violates intellectual property, breaches regulatory compliance or endangers customer trust.

Everyone is familiar with the threats that originate from outside the network perimeter, but security threats to networks no longer come only from outside. IDC (International Data Corporation) estimates that 60% of all serious threats come from internal sources. Many of these Internet-based business disruptions result from attacks that originate inside the network. It is becoming common for organizations to fall victim to internal attacks.

Hence, the Firewall cannot be limited as a perimeter defence only. They also protect the systems from internal attacks and intrusions. To keep pace with the dynamic security risks and guard against them, Next generation Firewalls act as end point security devices.

The purpose of this study material is to give the readers an idea about the need for Firewall, its history, various features and functions of Firewalls, the reasons for firewall failures and the possible improvements to avoid such weaknesses.

S.Prabhu

Principal Director

FIREWALL

Introduction

The Internet provides worldwide connectivity and unparalleled cost efficiency, enabling corporations to dramatically transform the way they conduct business. Large numbers of companies, across all industries, are embracing the Internet to expand and reengineer their traditional business models. But every time a company connects its internal computer network to the internet, it faces potential danger. Because of the internetôs openness, every corporate network connected to it is vulnerable to attack. **Such internet threats have wide ramification like loss of income, increased cost of recovery, loss of information, loss of trade secrets, damage to reputation, degraded performance in network systems, non-compliance with law and regulations and legal action by customers for loss of confidential data.**

Counter Measures

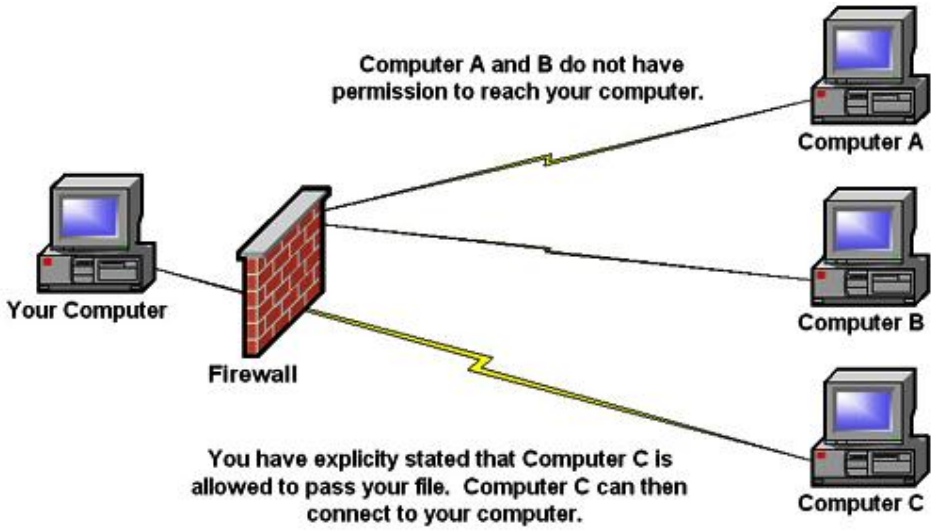
To keep pace with the dynamic security risks and guard against them, the same technology should be used. Some of them are **Firewalls, Virtual Private Networks, Encryption, Intrusion Detection Systems etc.** Among these systems Firewall is the most important device in securing the networks from outside world.

What is a Firewall?

The term "fire wall" originally meant, and still means, a fireproof wall intended to prevent the spread of fire from one room or area of a building to another. In computer networking, the term **firewall** is not merely descriptive of a general idea. It has come to mean some **very precise things** i.e. securing the networks of computers from the world of hackers.

In computer networking, the term **firewall** means securing the networks of computers from the world of hackers.

Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary Internet traffic. Firewalls can be configured to block data from certain locations while allowing the relevant and necessary data.



Firewalls are combinations of hardware and software, built using routers, servers and a variety of software, to control the most vulnerable point of access between a corporate network and the Internet. They could be simple or complex, in line with the corporate **security policy**.

Firewalls are defined as a device installed at the point where network connections enter a site. **They apply rules to control the type of networking traffic flowing in and out**. In other words, a firewall isolates a computer from the Internet using a **'wall of code'** that inspects each individual 'packet' of data as it arrives at either side of the firewall - inbound to or outbound from your computer - to determine whether it should be allowed to pass or be blocked.

A Brief History of Firewalls

The firewall was invented about a decade prior to the invention of the web server, and the original goal of a firewall was to prevent users on the Internet from accessing selective network resources.

A firewall isolates a computer from the Internet using a **'wall of code'** that inspects each individual 'packet' of data as it arrives at either side of the firewall - inbound to or outbound from a computer

Initial firewalls were designed **as simple packet filters** - they simply looked at what the user wanted to connect to and compared that to a list of allowed and disallowed resources. If the user requested a connection to an allowed resource, the firewall allowed access to the user. If the user requested a connection to a disallowed resource, the firewall did not allow the user access.

When the firewall is installed, the administrator gives the firewall a list of the resources they want to allow access to, and a list of resources to which access should be denied. Typically, the administrator allows access to resources such as e-mail servers and web servers.

General strategy: Allow All or deny all

One of the first things that we must decide when we configure our firewall is the general strategy on how to specify what network packets and protocols we allow inside our network, and which network traffic that we want to block.

The two major possibilities are

- **Allow-all strategy:** Allows all network packets except those that are explicitly denied.

Example Firewall Rules (Allow-All Strategy)			
Port/Content	*Users*	*Time*	*Action*
All ports, except 80	All	Always	Deny
Port 80/video	All, except trainers	Always	Deny
Port 80/video	Trainers	Night	Deny

- **Deny-all strategy:** Denies all network packets except those that are explicitly allowed.

Example Firewall Rules (Deny-All Strategy)			
Port/Content	*Users*	*Time*	*Action*
Port 80/except video	All	Always	Allow
Port 80/video	Trainers	Day	Allow

The Allow-all strategy may sound enticing, but you should always use the second strategy ð Deny-all, which is much more secure. The Deny-all approach is much easier to administer. No traffic is allowed, except for a small number of explicitly defined protocols and services. The Deny-all approach has two advantages

- We have to maintain only a small list of allowed network traffic rules. The smaller the list, the easier it is to verify that the configuration of the firewall is correct.
- We donôt have to constantly add new rules to exclude newly discovered problems.

How does a Firewall work?

To understand how firewalls work, we have to know a little about how computers communicate and what language they speak. As far as Internet connections and firewalls are concerned, the most important language is **TCP/IP** (Transmission Control Protocol/Internet Protocol). TCP/IP is a collection of ***protocols***, each of which defines the rules for how computers communicate across the Internet. Computers that use TCP/IP use a **unique number**, called an **IP address**, to identify themselves. All data that is sent from one computer to another using TCP/IP includes information on what IP address the data comes from and what IP address it is being sent to. **TCP/IP defines the methods that computers connected to the Internet use to transmit information.** This includes dividing this information in small manageable chunks called ***packets***

All Internet communication is accomplished by the **exchange of individual 'packets'** of data. Each packet is transmitted by its source machine toward its destination machine. Packets are the **fundamental unit of information** flow across the Internet. Even though we refer to 'connections' between computers, these 'connections' are actually comprised of individual packets travelling between those two 'connected' machines. Essentially, they 'agree' that they're connected and each machine sends back 'acknowledgement packets' to let the sending machine know that the data was received.

TCP/IP is a collection of ***protocols***, each of which defines the rules for how computers communicate across the Internet.

In order to reach its destination, every Internet packet must contain a **destination address and port number** so that the receiving computer knows who sent the packet. Every packet must also contain the IP address and a port number of the originating machine. In other words, any packet travelling the Net contains its complete source and destination addresses. An IP address always identifies a single machine on the Internet and the port is associated with a particular service or conversation happening on that machine. The port used by the PC for data transfer is called a **TCP/IP port**.

Since firewall software inspects each and every packet of data as it arrives at your computer, the firewall can be effectively configured so that it can be selective about what it lets through. Since every arriving packet must contain the correct IP address of the sender's machine, **the firewall can be selective about which packets are admitted and which are dropped according to the rules configured in it by the user**. It can 'filter' the arriving packets based on any combination of the sending machine's IP address and port and the destination IP address and port. Each resource available on a network is assigned a ñportò number, the number that corresponds to the type of resource. When the user wants to connect to a server resource, it specifies a port to connect to. If the user wants to talk to an SMTP e-mail server, e.g., then they would connect to the port assigned to the SMTP protocol, which is usually port number 25.

What a Firewall can do?

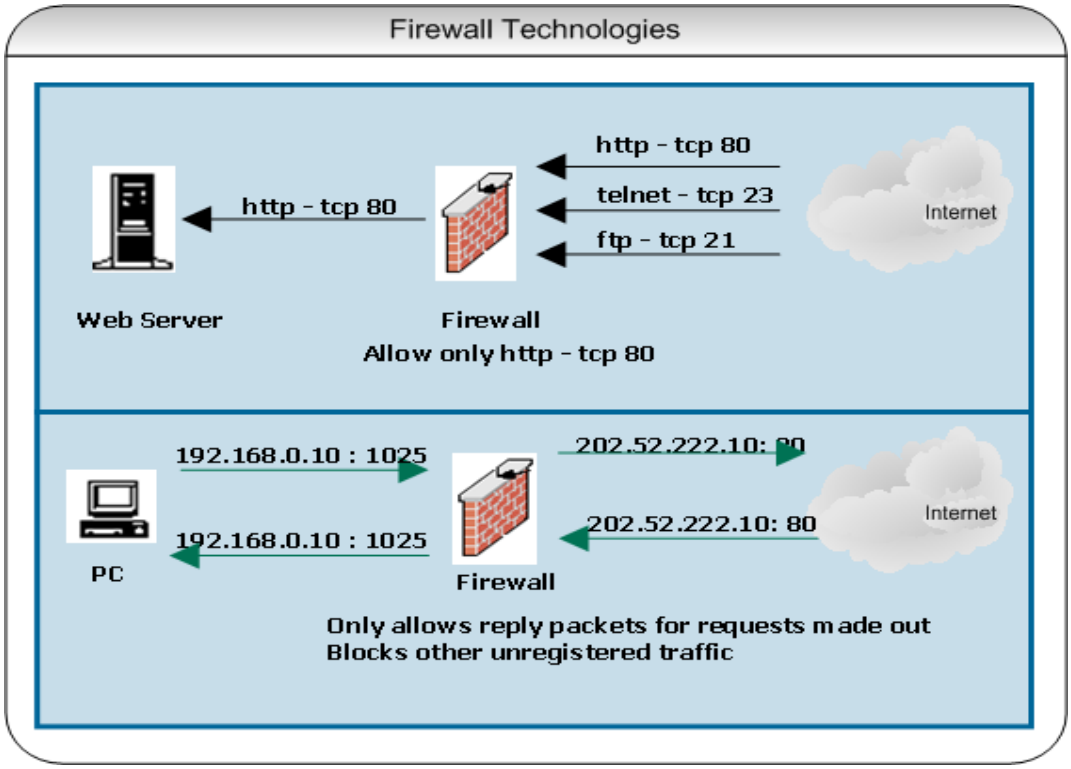
From the above discussion we can safely conclude that firewalls can:

- **Block incoming network traffic based on source or destination:**

Blocking unwanted incoming traffic is the most common feature of a firewall.

- **Block outgoing network traffic based on source or destination:** Many firewalls can also screen network traffic from your internal network to the Internet. For example, you may want to prevent employees from accessing inappropriate Web sites.

Every Internet packet must contain a **destination address and port number** so that the receiving computer knows who sent the packet.



- **Block network traffic based on content:** More advanced firewalls can screen network traffic for unacceptable content. For example, a firewall that is integrated with a virus scanner can prevent files that contain viruses from entering your network. Other firewalls integrate with e-mail services to screen out unacceptable e-mail.
- **Make internal resources available:** Although the primary purpose of a firewall is to prevent unwanted network traffic from passing through it, you can also configure many firewalls to allow selective access to internal resources, such as a public Web server, while still preventing other access from the Internet to your internal network.
- **Allow connections to internal network:** A common method for employees to connect to a network is using virtual private networks (VPNs). VPNs allow secure connections from the Internet to a corporate network.

For example, telecommuters and traveling salespeople can use a VPN to connect to the corporate network. VPNs are also used to connect branch offices to each other. Some firewalls include VPN functionality and make it easy to establish such connections.

- **Report on network traffic and firewall activities:** When screening network traffic to and from the Internet, itôs also important to know what your firewall is doing, who tried to break into your network, and who tried to access inappropriate material on the Internet. Most firewalls include a reporting mechanism of some kind or another.

What type of firewall is best?

Firewalls are offered in two forms: **hardware (external) and software (internal).** While both have their advantages and disadvantages, the decision to use a firewall is far more important than deciding which type you use.

- **Hardware** - Typically called network firewalls, these external devices are **positioned between the computer or network** and the cable or DSL modem. Many vendors and some Internet service providers (ISPs) offer devices called **"routers"** that also include firewall features. Hardware-based firewalls are particularly useful for **protecting multiple computers** but also offer a **high degree of protection** for a single computer. Hardware-based firewalls have the advantage of being separate devices running their own operating systems, so they provide an additional line of defence against attacks. Their major drawback is cost.
- **Software** - Some operating systems include a built-in firewall. **Further software firewalls are relatively cost effective** and can be obtained from the market.

A firewall should be configured as a **gateway** to allow or deny access to network resources. Most commercially available firewall products, both hardware- and software-based, come configured in a manner that is acceptably secure for most users. However each firewall is different and the security requirements of each organisation may vary. Hence relying blindly on the default settings of the firewall will not satisfy oneôs security requirements. Therefore a firewall can

A firewall can function effectively only if the user is clear about what sites should be allowed and what sites should be denied

function effectively only if the user is clear about what sites should be allowed and what sites should be denied. Further a firewall offers little to no protection against viruses. Using a firewall in conjunction with other protective measures (such as anti-virus software and "safe" computing practices) in line with a sound Security policy will strengthen oneôs resistance to attacks.

How hacker's get inside the network?

- **Insecure Passwords:** Just as burglars find it easy to break into a house whose occupant has placed the key under the doormat, breaking into a network is easy if we use passwords that are easy to guess, such as the word *password,* a blank password, or the default password provided bya standard software installation.

- **Default configurations: The main problem with default configuration is that it is easy to predict.** Many database programs come with a default user account and password to administer the database. Because this username and password are the same for everyone who installs such a program, they are easy to predict. Unless these settings are changed it is easy for a hacker to enter the database server using this route.
- **Bugs:** With the complexity of todayôs software, it is almost unavoidable to have any software without bugs. Hackers can use bugs in programs to get these programs to crash ð which constitutes a denial-of-service attack ð or to get unauthorized access to a computer.
- **Buffer overflow**: One type of bug that hackers exploit is a *buffer overflow.* A buffer-overflow condition can exist when a program allows a user to enter data and set aside limited amount of space for the data that the user enters. This temporary holding area for data is referred to as a *buffer.* A well-written program checks the length of the data that is entered and rejects any user-entered data that is longer than the buffer. A badly written program accepts data that exceeds the maximum allowed length. When a user enters data into a badly designed program and the data exceeds the maximum allowed data length for the buffer, the program overwrites data that is located in the computerôs memory that is

adjacent to the buffer. This may have devastating effects like crashing the computer to inserting another program into the computer that could give an intruder unlimited access to the computer. Some of the known examples of this bug are Code Red, Nimda, SQL Slammer etc

Facts to be considered before installing a firewall:

Installing a firewall requires careful consideration and planning, since a firewall is most often placed in a critical path within a **network topology**. The installation of a firewall requires a clear understanding of the networking requirements of a group. The installation is likely to have a direct impact on every machine behind the firewall.

In order to allow some specific sites, the administrator needs to create **firewall rules** to implement a **firewall policy**. This necessitates forming a strong network policy which in turn is implemented through a firewall. Since firewalls are tools used to implement network security policy, no firewall design should ever be considered without first clearly defining the ultimate security policy goals.

What is a Network Security Policy?

It is vital for businesses with connections to the internet to ensure that their networks are secure. This is important to minimise the risk of intrusions both from insiders and outsiders. Although a network cannot be 100% safe, a secure network will keep everyone but the most determined hacker out of the network. Before a network can be secured, a network security policy has to be established. A network security policy defines the organisation's expectations of proper computer and network use and the procedures to prevent and respond to security incidents. A network security policy is the foundation of security because it outlines what assets are worth protecting and what actions or inactions threaten the assets. **The development of a security policy is driven by risk assessment and vulnerability analysis**.

A network security policy defines the organisation's expectations of proper computer and network use and the procedures to prevent and respond to security incidents.

What is a good Security Policy?

A general óstanceô or óruleô is usually chosen for a security policy design. This rule is used as a starting point and a conceptual framework for guiding further development of the policy. **Three of the most common postures are discussed below: trust inside, least privilege, and selective blocking**.

Trust inside. The most popular rule is known as ñtrust inside.ò In this scenario, it is assumed that the most significant threats will come from outside the local area network, and the emphasis of the policy will be keeping outsiders from getting in. This type of rule is frequently implemented by defining a firewall rule set that permits all connections which are initiated from the inside, but blocks connections initiated from the outside. This type of policy is easy to conceptualize and fairly easy to implement and manage.

Least privilege Another common rule is known as ñleast privilege.ò In this rule, it is assumed that all network connections are blocked in both directions as a starting point, and the policy is incrementally opened to define precisely what is allowed. This is also known as the ñdeny everythingò policy

Selective blocking ñSelective blockingò is another common posture. This is also known as an ñaccept everythingò starting point. The policy is fine tuned by explicitly denying only selected connections which are known to be potentially dangerous. This is clearly the most vulnerable policy to use as a starting point. Selective blocking is often used as a first line of defence.

Example of Simple Firewall Rules.

Processing Order of Firewall Rules			
Rule	***Port***	***Users***	***Action***
Rule A	80 (HTTP)	All	Allow
Rule B	80 (HTTP)	Temps	Deny
Rule C	80 (HTTP)	Kim	Allow

Basic Functions of a Firewall - The main four basic functions of a firewall are:

- **Packet filtering:** The headers of all network packets going through the firewall are inspected. The firewall makes an explicit decision to allow or block each packet.
- **Network Address Translation (NAT):** The outside world sees only one or more outside IP addresses of the firewall. The internal network can use any address in the private IP address range. Source and destination addresses in network packets are automatically changed (or ñtranslatedò) back and forth by the firewall.
- **Application proxy:** The firewall is capable of inspecting more than just the header of the network packets. This capability requires the firewall to understand the specific application protocol.
- **Monitoring and logging:** Even with a solid set of rules, logging what happens at the firewall is important. Doing so can helps to analyze a possible security breach later and gives feedback on the performance and actual filtering done by the firewall

Many firewalls support the following advanced functions:

- **Data caching:** Because the same data or the contents of the same Web site may pass the firewall repeatedly in response to requests from different users, the firewall can cache that data and answer more quickly without getting the data anew from the actual Web site every time.
- **Content filtering:** Firewall rules may be used to restrict access to certain inappropriate Web sites based on URLs, keywords, or content type (video streams, for example, or executable e-mail attachments).
- **Intrusion detection:** Certain patterns of network traffic may indicate an intrusion attempt in progress. Instead of just blocking the suspicious network packets, the firewall may take active steps to further limit the attempt, for example, by disallowing the sender IP address altogether or alerting an administrator.

The main four basic functions of a firewall are: Packet filtering, Network Address Translation, Application proxy, Monitoring and logging

- **Load balancing:** From a security standpoint, a single point of entry is good. But from an availability standpoint, this single point of entry may lead to a single point of failure as well. Most firewalls allow the incoming and outgoing network request to be distributed among two or more cooperating firewalls.

Types of Firewalls

Generally the types of firewalls available today fall into three categories which include:

- **Router packet filtering.**
- **Stateful inspection.**
- **Application firewall systems.**

1. Router Packet Filtering Firewall:

The first firewall products used only packet filtering to protect the internal network from outside users. In packet filtering, a screening router **examines the header of every packet** of data travelling between the Internet and the corporate network and made a decision to allow or to block the packet based on the IP addresses used and the specific port number in the TCP or UDP header.

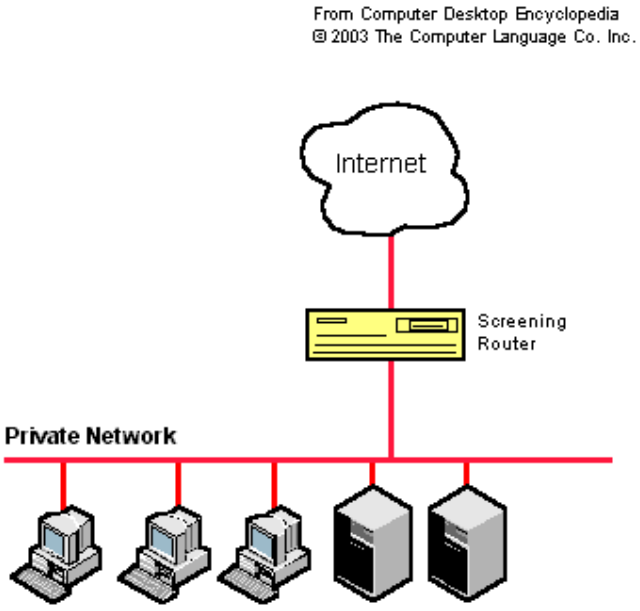
The advantages of this type of firewall are its **simplicity and generally stable** performance since the filtering rules are performed at the network layer. Its simplicity is also a disadvantage because it is vulnerable to attacks from improperly configured filters. Since the direct exchange of packets is permitted between outside systems and inside systems, the potential for an attack is determined by the total number of hosts and services to which the packet filtering router permits traffic.

Packet inspection needs to be smarter about which inbound network packets are expected in response to a legitimate request from an internal network user, and which inbound network packets are unsolicited and should therefore be blocked. When a firewall sees an outgoing network packet, it should remember that an incoming response is due soon, and only allow those expected incoming network

packets. The remembered information is called ***state***. This smarter form of packet filtering is called ***stateful* packet filtering**, as opposed to the original ***stateless* packet filtering**, which did not remember the state of expected return packets.

Some of the issues not addressed by this firewall are:

- The outside world can learn the IP addresses used on the internal network. The firewall should use **Network Address Translation** (NAT) to solve this problem.
- Packet filters have limited decision capabilities because they look only at a small portion of the network packet. The firewall should use application proxy functionality to further inspect the packet.



2. Stateful Inspection Firewalls / Stateful Packet Filtering:

Modern firewalls use a more robust version, which is called ***stateful packet filtering.*** With stateful packet filtering, the firewall **remembers** ñstateò about expected return packets. Any unexpected packet arriving at the firewall claiming to be a solicited response is blocked immediately

The firewall internally maintains a table of information on which ports it may expect traffic. If the firewall determines that a communication exchange is finished, it removes that information from the table. In cases where the firewall

is unable to detect that the communication has ended, it automatically removes that information after a short time period.

Stateful inspection firewalls, which are sometimes referred to as ñ**session-based firewalls,**ò have become more popular in recent years. The development of hardware redundancy including session failover is a more recent feature.

3. Application Firewall systems

There are two types of application firewall systems. They are referred to as **application- and circuit-level firewall systems**. They provide greater protection capabilities that packet filtering routers. Packet filtering routers allow direct flow of packets between internal and external systems. Application and circuit gateway firewall systems allow information to flow between systems but do not allow the direct exchange of packets. The primary risk of allowing packet exchange between internal and external systems is that the host applications residing on the protected networkôs systems must be secure against any threat posed by the allowed packets.

Application based firewall systems are set up as proxy servers to act on behalf of someone inside an organizationôs private network. Rather than relying on a generic packet filtering tool to manage the flow of Internet service through the firewall, a specific purpose code, called a **proxy server**, is incorporated into the firewall system. For eg. When someone inside the corporate network wants to access a server on the Internet, a request from the computer is sent to the proxy server, the proxy server contacts the server on the Internet, and the proxy server then sends the information from the internet server to the computer inside the corporate network. By **acting as a go-between**, proxy servers can maintain **security.** Proxy servers can also log on all traffic between the Internet and the network.

Examples of Firewall implementation

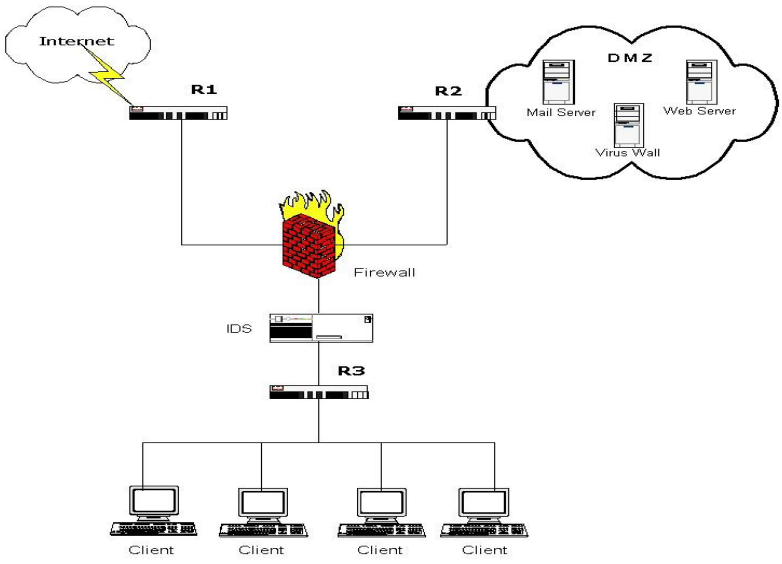
Firewall implementation can take advantage of the functionality available in a variety of firewall designs to provide a robust layered approach in protecting an organizationôs information assets. Commonly used implementations are:

Screened–host firewall: This is a combination of packet filtering router and a **bastion host** (proxy) i.e this implementation combines **network layer security and application server security**. Intruder has **to penetrate 2 separate securities.**

Dual-homed firewall: A firewall system that has two or more network. They usually acts to block or filter some or all of the traffic trying to pass between the network.

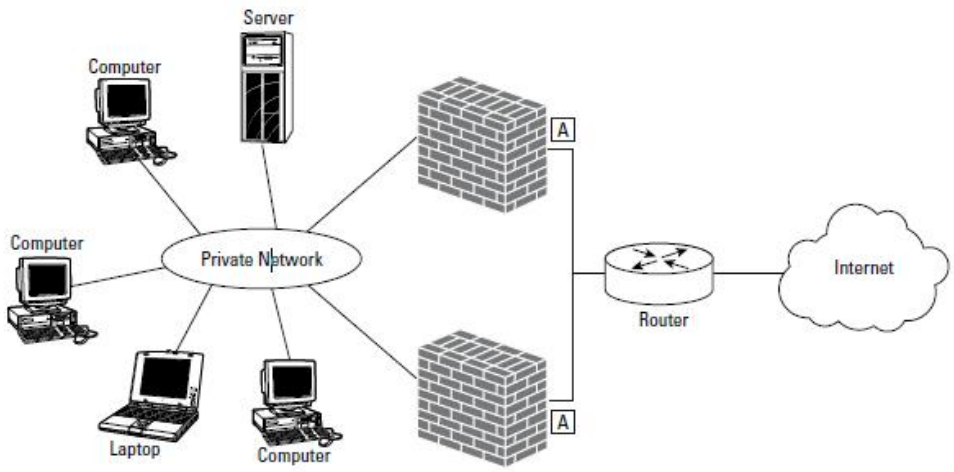
Demilitarized Zone (DMZ): The term DMZ or Demilitarized Zone comes from military. The DMZ area is an area that both sides agree there will be no military actions. But if one side does violate the agreement, then both sides can start firing. This is a buffer zone between the two parties and is designed to protect the populace on both sides of the DMZ.

The DMZ refers to a security zone, which separates all Internet traffic away from the internal network. You can create a secure DMZ with three routers. Your Firewall must have **three Network Interface Cards** connected to each of the routers.



Addressing System

The addressing scheme chosen for the **internal/trusted interface** is a critical decision that must be made well before installation begins. The traditional approach is to use private addressing on the internal/trusted network and then use NAT on the external interface of the firewall to translate the addresses of active connections so that they are routable



Network Address Translation (NAT)

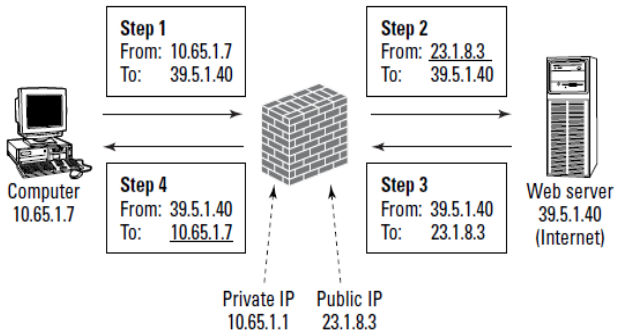
Every computer connected to a network has an IP address. IP address is just like a postal address that contains a street and a house number. An IP address is comprised of two parts: a network address and a host address. All computers on the same network segment share the network address. The host portion is unique to a computer on that segment.

An IP address is 32 bit long. Using permutation and combination of this length, only four billion different IP addresses could be generated and the available IP addresses were quickly depleting. Network Address Translator came as a rescue to this problem.

An IP address is comprised of two parts: a network address and a host address. All computers on the same network segment share the network address. The host portion is unique to a computer on that segment.

With NAT, all computers on the internal network can **use a private range of IP addresses,** such as 10.0.0.0/8, which is not in use on the Internet. When they make a connection to the outside world, the NAT computer replaces the private IP address, for example, 10.65.1.7 ð listed as Source IP address in the IP packet ð with its own public IP address, 23.1.8.3, and sends the packet on its way

Network Address Translation



The outside world will only see the outside public IP address of the firewall and will never learn the internal IP addresses. Private IP addresses, such as those in the 10.0.0.0/8 range, canôt be routed over the Internet. ISPs actively block those addresses if used on the Internet.

NAT serves three main purposes

- Provides a type of firewall by hiding internal IP addresses
- Enables a company to use more internal IP addresses. Since they're used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations.
- Allows a company to combine multiple ISDN connections into a single Internet connection

In firewall circles, people tend to see NAT more as a security precaution than as a method of saving IP addresses. The term ***IP masquerading*** is often used for NAT, which emphasizes the hiding aspect of NAT.

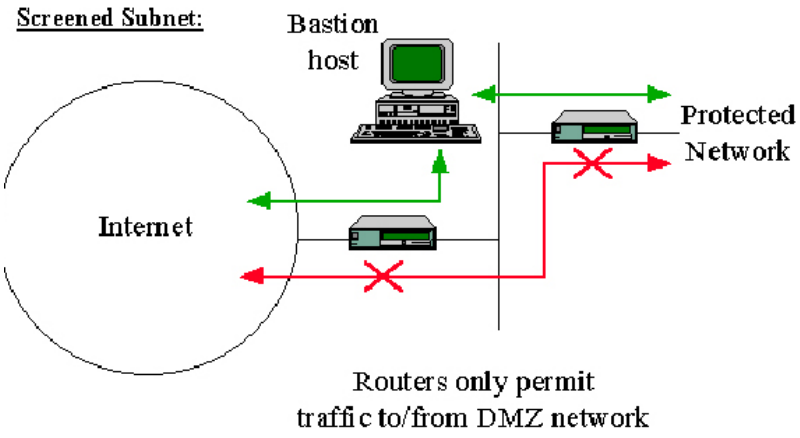
IP masquerading is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to

communicate to the outside. It allows one machine to act on behalf of other machines. IP masquerading allows internal machines that don't have an officially assigned IP addresses to communicate to other networks and especially the internet.

Intrusion Detection

Intrusion detection systems, or IDSs, have become an important component in maintaining the Network Security. intrusion detection systems do exactly as the name suggests: they detect possible intrusions. More specifically, IDS tools aim to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection.

Firewall acting as an Intrusion detection System



Filtering packets and inspecting the application portion of an IP packet may do an adequate job in deciding which network traffic should be allowed in and which should not. However, modern firewalls are capable of taking a more active role. The firewall can monitor the packets arriving at the firewall and analyze them for signs of security problems ð sort of like a burglar alarm for your firewall. This is called an intrusion detection system. Just analyzing the packets at the firewall for telltale signs of intrusion attempts is not enough, of course. Intrusion detection systems must also include a reporting or alerting mechanism.

The major difference between packet filtering and intrusion detection at the firewall is that packet filtering decides which network traffic is allowed to enter

the internal network (mostly based on one packet a time), whereas inspection-based intrusion detection doesnôt control the network traffic but attempts to recognize patterns or conditions in one or several packets, blocked or allowed, in order to spot an intrusion in progress.

Intrusion detection systems actually work a lot like virus-scanning software. They use a list of signatures that specifies what constitutes a possible usage pattern an intruder may attempt. Sometimes this list of signatures is updateable with newly discovered attacks.

Incident Response

The real value of an intrusion detection system is determined by how effective the response to a detected intrusion attempt is. In general, these types of responses are possible:

- **Log or record the problem:** This is the most passive response. The firewall makes an entry in its log files noting the detected attempt
- **Report or trigger an alarm:** This may include sending an e-mail to the firewall administrator or even paging a security officer.
- **Strike back!** This is the most aggressive response. The firewall traces the source of the attack and takes action to disable the attackerôs machine.

Firewall issues

Problems faced by organizations that have implemented firewalls include:

- A false sense of security may exist when management feels that no further security checks and controls are needed on the internal network (i.e majority of incidents are caused by insiders, who are not controlled by firewalls).
- The circumvention of firewall through the use of modems may connect users directly to ISPs. Management should provide assurance that the use of modems when a firewall exists is strictly controlled or prohibited altogether.
- Misconfigured firewalls may allow unknown and dangerous services to pass through freely.

- What constitutes a firewall may be misunderstood.(Companies simply have screening routers).
- Monitoring activities may not occur on regular basis.
- Firewall policies may not be maintained / updated regularly.

Most firewalls operate on the Network layer: therefore they do not stop any application based or input based attacks.

Next Generation Firewalls

- Firewalls need to evolve to be more proactive in blocking new threat. Enterprise need to update their network firewall to protect business systems as attacks get more sophisticated.
- Next Generation firewalls are emerging so that they can they can detect application specific attacks and enforce application specific granular security policy, both inbound and outbound.
- A Next Generation Firewall is wire speed integrated network platform that perform deep inspection of traffic and blocking of attacks.
- According to Gartner, to meet the challenges faced by business enterprises due to changing technology, application architechture and new bandwidth requirements, the threats to network security is increasing many fold. Gartners believes firewalls need to evolve into ñNext Generation Firewallsò which is an in-line security control that implements network security policy between networks of different trust levels in real time.

Conclusion

The firewall is a cornerstone of most organizationôs information security strategy. However, the effectiveness of this security stalwart is steadily diminishing as threats continue to increase. The need of the hour is next-generation firewall system ï one that incorporates application awareness at the core of its design, has fully integrated threat protection, and also includes customized hardware architecture to avoid the need to choose between security and performance

References:

1. www.isaca.org
2. Firewalls for Dummies ï Authored by Brian Comer, Ronald Beekelaar and Joern Vettern
3. Next Generation Firewalls ï Gartner RAS Core Research Note G00171540, John Pescatore, Greg Young, 12 October 2009
4. www.paloalto Networks.Com
5. www.Wikipedia.org
6. www.Howstuffworks.com
7. www.Bleepingcomputer.com
8. www.csoonline.com/white-papers
9. www.protivity.com