International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 3 Issue 3 September 2012

FIREWALL: TOOL OF NETWORK SECURITY

Kirti Walia

Associate Professor

Regional Institute of Management & Technology

Mandi Gobindgarh, Punjab, India

Dr. S.N. Panda

Professor

Regional Institute of Management & Technology

Mandi Gobindgarh, Punjab, India

Dr. Rajinder Singh

S. D. College, Ambala Cantt., Haryana, India

Abstract

Firewall technology started emerging in the late 1980s when Internet was a fairly new technology in global usage and connectivity. [1] It was the response to a number of major internet security breaches occurred in late 1980s. Firewall stops anyone from outside to log into a computer system in a private computer network. This paper explores various firewalls along with their working mechanism. The last section explains a proposed working model to provide security for any organization using multiple firewalls placed at different locations in the network.

Keywords: *Firewall, traffic, security, DMZ, filtering,*

1. INTRODUCTION

The basic task of a firewall is to control the traffic of a network having various zones of trust. Various zones of trusts are (i) Internet (Non-trusted zone) and (ii) internal network (trusted zone). The basic purpose is that the connection between these zones having different trust levels must be controlled by enforcing a security policy (**Fig 1**).

Firewall enhances the network security within an organization (**Fig 2**) by controlling the network access by allowing or denying the incoming or outgoing traffic according to some set of rules called firewall policy or filters. It provides a control on the use of a computer network.

A firewall is either a hardware device or a simple program (software) that creates a check point at the boundary of a single computer or a private computer network. It filters the information coming through the internet.

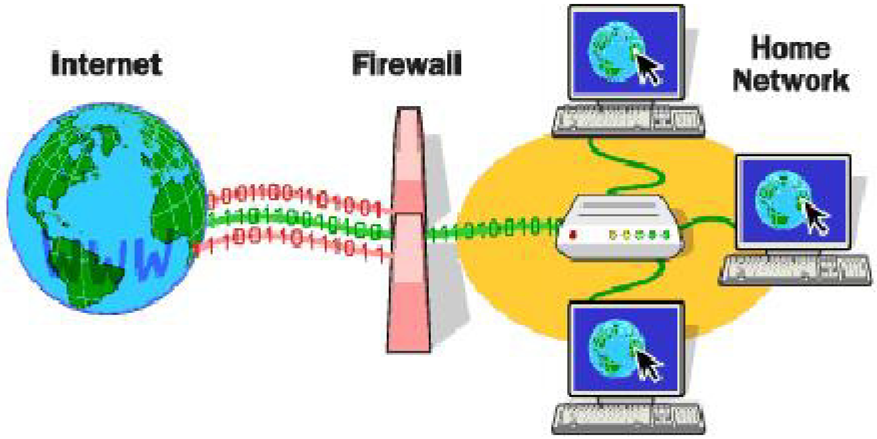

Fig 1: Use of Firewall at Home Network

Source: http://www.howstuffworks.com/firewall.htm

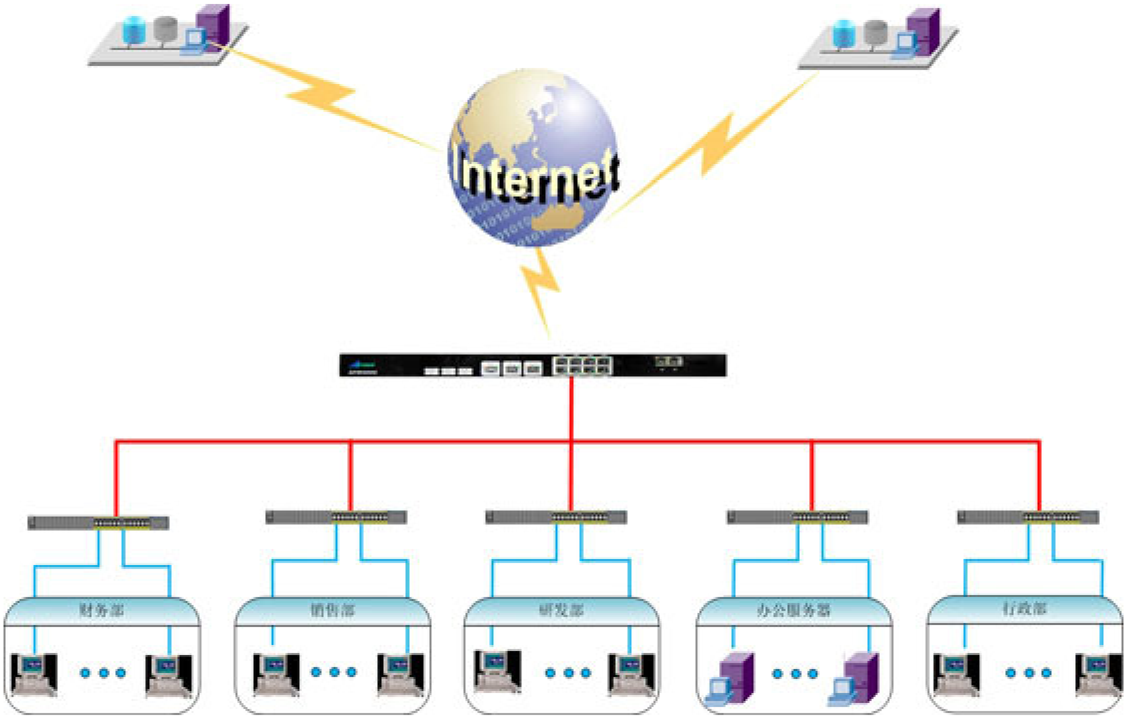

Fig 2: Use of Firewall at an Organization

The whole information is divided into small chunks of data, called a Packet. This packet has to satisfy the security rules, set or defined by the firewall, to cross it and reach to its destination, otherwise the packet is discarded.

Firewall uses one or more methods to control the inbound and outbound traffic flow

- Packet Filtering: In case of Packet filtering, packets are analyzed against a set of rules, called filters. For a packet to reach to its destination machine has to fulfill all the rules or we can say satisfy the various filters.
- Proxy Service : In case of Proxy service there is no direct communication between the computer which requests a web page and the remote computer which hosts that page. Proxy server retrieves the information from the computer and sends it to the remote web server and again retrieves the response of the web server and provides the same to the computer which had requested for it. The Proxy server can also stores (Cache) the web site so that next time if any system want to connect to the

same website it can provide it instantaneously from its cache only and actually it does not load the page from the website again

- Stateful Inspection: It is the case where the contents of the packets are not examined rather some key information is matched to treat it as trusted and secure information.

Firewall is placed at a place where the private computer network is connected with the outside world i.e internet, thus making it capable to intercept all the packets crossing it.

When we require that remote users can have access to items on our network for some reason like allowing access to Web site, Online business or FTP download and upload area [2] then it is preferred to create a **DMZ** (Demilitarized Zone). It really is an area that is outside the firewall (**Fig 3**). One can think of DMZ as the front yard of house which belongs to us and we may put some things there which can be accessible to others, but anything valuable will be kept inside the house where it can be properly secured.

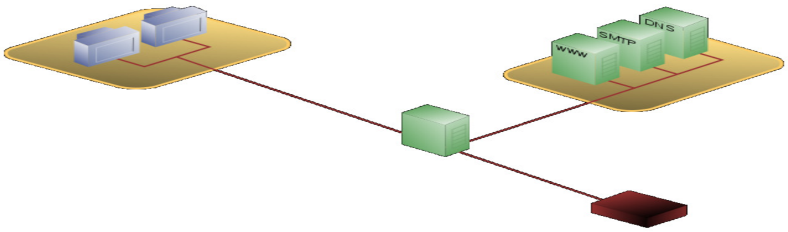

Fig 3:DMZ
Source : http://en.wikipedia.org/wiki/File:DMZ_network_diagram_1_firewall.svg

Setting up a DMZ is not difficult. It can be created by placing a computer (**Fig 4**) between internet connection and the firewall. To secure the DMZ area we can use two firewalls.[3] The first firewall (also called the "front-end" firewall) must be configured to allow traffic destined to the DMZ only. The second firewall (also called "back-end" firewall) allows the traffic only from the DMZ to the internal network.

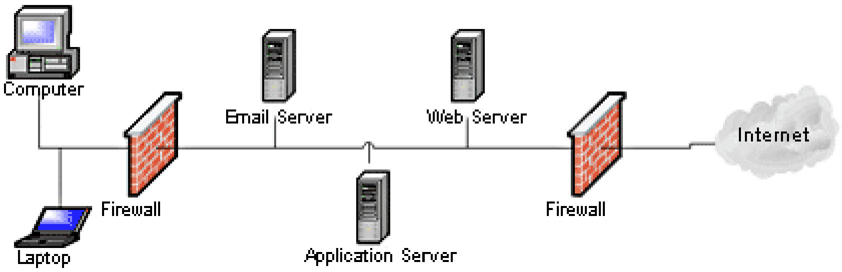

Fig 4: Securing DMZ and implementation of 2 levels of firewalls

Thus in a DMZ the incoming requests must first pass through a computer lying in the DMZ area before reaching the firewall.

2. CLASSIFICATION OF FIREWALLS

Classification of firewalls can be done on various factors like tangibility, record of communication, filtering rules applied at which specific layer, security for a network or for a single computer.

2.1 Classification based on the contents check (packet filter & application filter)

2.1.1 Packet Filter Firewall (Network Layer Firewall)

Packet filter firewall inspects the each packet which is [4]transferred between computers on the Internet. If a packet matches the set of rules, it is allowed to cross the firewall otherwise it is simply discarded. This type of packet filtering have no check [5] whether a packet is part of an existing stream of traffic (i.e. it stores no information on connection "state"). Each packet is filtered only on the basis of the information contained in the packet’s header like packet's source and destination addresses, its protocol, and, port number.

Packet filtering firewalls work mainly on the first three layers of the OSI reference model, i.e. most of the work is done between the network and physical layers, and only to check out the source and destination port numbers the transport layer referred. When a packet is received at the firewall, it is checked for any kind of match of the packet filtering rules for which firewall is configured and accordingly the action is taken. When the packet passes through the firewall, it filters the packet on a protocol /port number basis.

For example, *if the rule in the firewall is to block telnet access, then the firewall will block all the traffic from the TCP protocol for port number 23.*

Further it can be classified as (stateful & stateless packet filter inspection)

2.1.1.1 Stateless packet filter

In case of stateless packet inspection no record is maintained about whether the packet received belongs to the same connection or not. It treats all the received packets as individual packets (**Fig 5**).

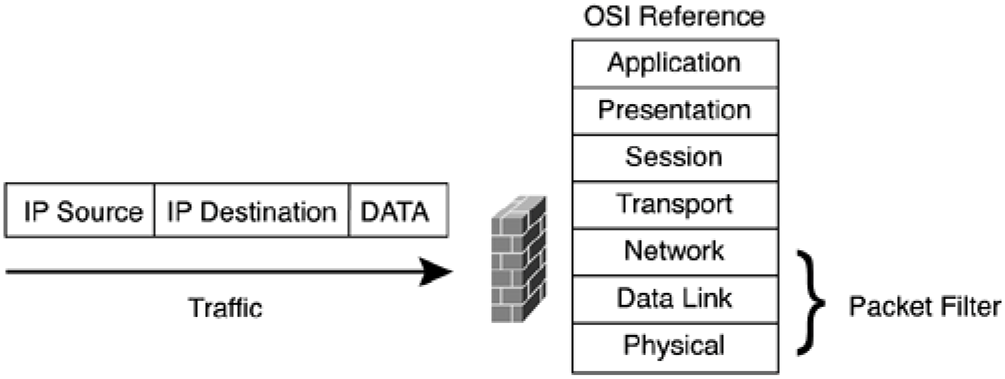

Fig 5: Layers which are concerned with stateless packet filter

Source : http://ciscosecurity.org.ua/1587051672/ch09lev1sec2.html

Actions which are taken for a packet

1. Pass: Let the packet pass cross the firewall
2. Drop: Discard the packet and no information is sent back to the sender
3. Reject: Discard the packet and information (error message)is sent back to the sender

Limitations of stateless packet filtering:

1. Slow Process: Since it doesn’t maintain the state of the traffic every packet is inspected and thus is time consuming process

2.1.1.2 Stateful packet filter

Stateful packet Inspection works very much similar to packet filter firewall with an expansion that it maintains all the [6] records of all connections passing through the firewall. It maintains the history of the source of packets (**Fig 6**) it is able to determine whether a packet is the start of a new connection or a part of an existing connection, or is an invalid packet. If the packet belongs to the existing connection it is simply allowed to cross the firewall. Otherwise the whole packet is examined and a new state is entered in its state table. The state of a connection can itself be one of the criteria which trigger specific rules. These states are kept in the local cache of the firewall.

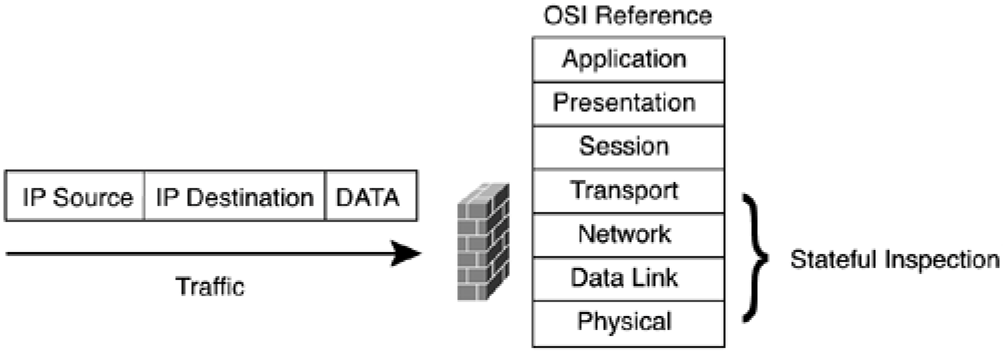

Fig 6 :Layers which are concerned with stateful packet filter
Source : http://ciscosecurity.org.ua/1587051672/ch09lev1sec2.html

Advantages:

a) Since states are maintained, it is fast on execution it the packets are coming from the existing connection
b) Entire content of the packet is examined

Disadvantages:

a) Cache table may overflow : As the number of connections increases the cache table grows accordingly. If there is not sufficient memory then this cache table may overflow, which may cause the packet to Drop or it may be a kind of “Denial of Service”
b) It is complex to administrator

c) Time out may be too short for the flow of packets: The cache entry for each flow is removed from the cache for either of the two reasons: (i) The flow is intentionally torn down or (ii) that entry is inactive for more than a certain time period.

2.1.2 Application Firewall (Application Layer Firewall)

Application Firewall is the further expansion of stateful packet inspection where the [6] filtering rules are applied on process basis instead of port basis. Application-layer firewalls work on the application layer of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and thus can inspect the contents of the packet. Hence Application firewall can intercept all the packets traveling to and from an application. It can prevent all unwanted outside traffic from reaching protected machines. Application firewalls function by determining whether a process should accept any given connection or not

Advantages**:**

1. It provides the benefit of stateful packet inspection, while proxying and inspecting data to the most common and frequently used services.
2. [7] Since application proxies examine packets at the application program level, a very fine level of security and access control may be achieved.
3. These can reject all inbound packets contain common EXE and COM files.
4. No direct connections are allowed through the firewall under any circumstances.

Disadvantages:

These firewalls consume more resources which affects their network throughput.

2.2 Classification based on tangibility (Software & Hardware)

2.2.1 Software firewall

A software firewall (**Fig 7**) is an application which installed on a single computer. [8] Since it is running directly on a computer, it is able to know a lot more about network traffic than simply what port its using and where it's going, like *It can know which program is trying to access the Internet and whether it's legit or malicious*. A software firewall can either allow or block a program's ability to send and receive data. If the firewall is not sure about the nature the program, then the user is prompted to provide confirmation before the traffic is allowed to pass,. Thus, a software firewall is able to take a closer look at malicious traffic and intercept it before it leaves the computer

The main drawback of software firewalls is that they only protect the machine on which they are installed. So, to protect multiple computers with a software firewall one need to have multiple copies (or licenses) of it and install and configure them individually on each machine. This can be expensive and difficult to manage. There are many business-oriented firewall programs that do offer centralized installation and administration.

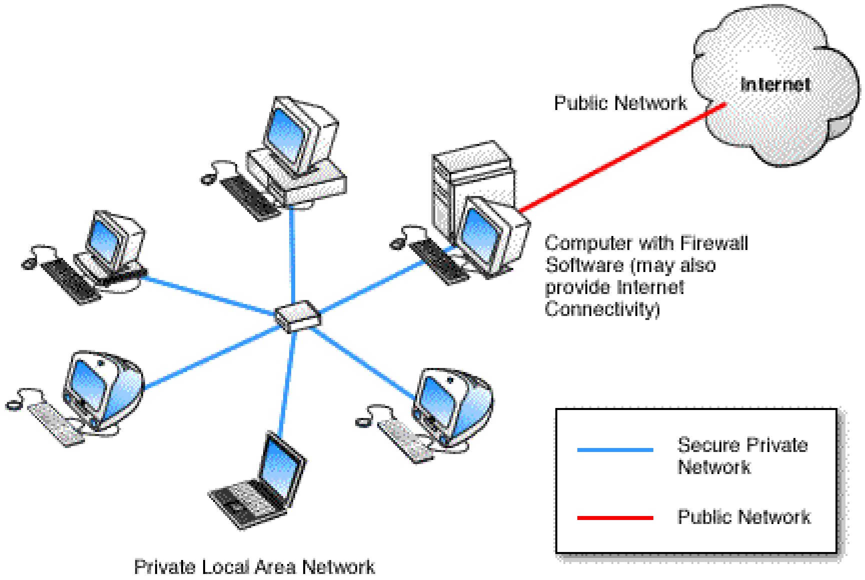
Internet
Public Network
Computer with Firewall Software (may also provide Internet Connectivity)
Secure Private Network
Public Network
Private Local Area Network

Fig 7: Software firewall

Source: http://compsci.ntci.on.ca/hef/ics2/period5/zhangl/firewall.diagram1.gif

Advantages:

1. These are quite cheaper
2. It doesn't require specialized knowledge to install, configure, and administer effectively
3. It is customizable.

Disadvantages:

1. These are susceptible to the virus attacks as their host machine
2. It is dependent on the source machine for the resources (CPU and memory) for its proper working
3. Network administrator must keep them updating.

2.2.2 Hardware firewall

The hardware firewall in a basically a router (**Fig 8**) which uses a technique called packet filtering, in which the header of a packet is examined to determine its source and destination addresses. This extracted information is then compared to a set of predefined rules that determine whether the packet is legitimate or not and thus decided whether it should be allowed to move into the network or to be blocked. Hardware firewall is primarily concerned with keeping bad stuff away from getting in. The limitation of this type of firewall is that it typically treats any kind of traffic traveling from the local network out to the Internet as safe, which sometimes can be a source problem.

Since it is a hardware unit it is normally installed at a point from where all the traffic passes.

Advantages:

1. Doesn't depend on operating System of the computer and thus immune to various bugs or malicious attacks
2. Hardware firewalls have faster response time, and thus are able to handle more traffic loads.
3. Hardware firewall has its own operating system (proprietary) and is less prone for attacks. This increases the security of the firewall itself. Also they have enhanced security controls.

4. Since it is separated from other network components, it can be easily and efficiently managed. This also does not slowdown other applications. It can be easily moved, shutdown, or reconfigured with minimal interference to the existing network.
5. Additional devices can be added, if required, with ease.
6. It is only concentrated to the firewall related activities and hence gives better performance with respect to software firewall.

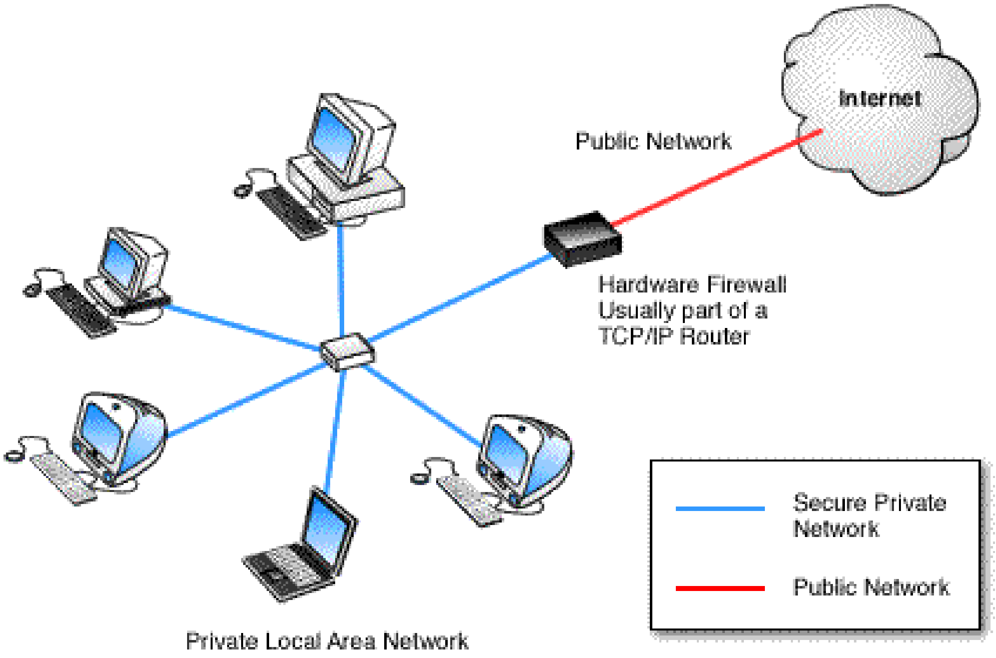

Fig 8: Hardware firewall

Source: http://www.vicomsoft.com/images/learning-center/firewalls/firewalldiagram2.gif

Disadvantages :

1. If the device goes down the whole inbound and outbound traffic is stopped.
2. It requires specialized knowledge to install, configure, and administer effectively.
3. Hardware firewall costs more than a software firewall.
4. It consumes physical space and involves wiring.

2.3 Classification based on security provided to (Host based & Distributed)

2.3.1 Host Based (Personal) firewalls

A personal firewall protects only the computer on which it is installed. It is a software application used to protect a single Internet-connected computer. This type of protection is especially useful for the computers which are connected with such as DSL or cable modem and normally always connected with the Internet. Such connections use a static IP address that makes them especially vulnerable to potential hackers. Personal firewalls work in the background to protect the integrity of the system by controlling Internet connections to and from a user's computer, filtering inbound and outbound traffic, and alerting the user to attempted intrusions.

It [9] relies on the assumption that everyone on one side of the entry point i.e. [10] the firewall is to be trusted, and that everyone on the other side of it should not be trusted and treated as an enemy.

Many host-based firewalls [11] incorporate antivirus software and intrusion prevention software capabilities, as well as suppressing Web browser pop-up windows, blocking cookies, and identifying potential privacy issues within Web pages and e-mails. [12] Host-based firewalls that integrate these functions can be very effective not only at preventing most types of malware incidents, but also from spreading it. Computer systems that are directly accessible from the Internet should be protected whenever possible through host-based firewalls.

Systems that are directly accessible from the [13] Internet should be protected whenever possible through host-based firewalls

A host based firewall is implemented in separate hardware, placed in between a host and the rest of a network, which can address software compatibility problems and improve resistance to compromise from within an infected system

Advantages:

1. They can be used to enhance the security.
2. They are cheaper

Disadvantages:

3. These are software based firewalls and hence it is a burden on the computer system. It will require memory and CPU to process the traffic
4. These kind of firewalls run on operating systems which may have its own security issues.
5. It is difficult to manage them on a large scale.

2.3.2 Distributed Firewalls

Distributed firewalls are host-resident [14] security software applications that protect the enterprise network's servers and end-user machines against unwanted intrusion. They filters traffic from both the networks i.e Internet and the internal network. This helps in preventing hacking attacks that may originate from either the Internet or the internal network. This is very important to consider because the mostly attacks originate from within the network.

Distributed firewall is installed on each computer in a network, but managed centrally to enforce an organization's relevant policies.

Distributed firewalls are often kernel-mode applications that sit at the bottom of the OSI stack in the operating system. They filter all traffic regardless of its origin—the Internet or the internal network. They treat both the Internet and the internal network as "unfriendly". They guard the individual machine.

Distributed firewalls help in two ways. Remote end-user machines can be secured. Secondly, they secure critical servers on the network preventing intrusion by malicious code and "jailing" other such code by not letting the protected server be used as a launch pad for expanded attacks.

Distributed firewalls rest (Fig 9) on three notions: (a) a policy language [15] that states which type of connections are permitted or which type of connections are not permitted, (b) system management tools, and (c) network-level encryption mechanism.

The idea behind distributed firewall is very simple. A compiler translates the policy language into some internal format. The system management software distributes this policy file to all hosts that are protected by the firewall. And incoming packets are accepted or rejected by each host, according to the policy and the cryptographically-verified identity of each sender.

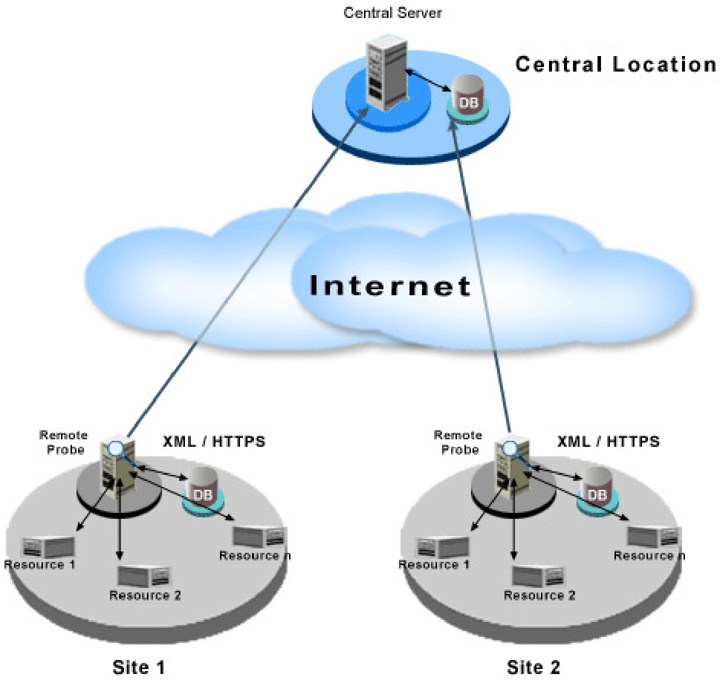

Fig 9: Distributed Firewall

Source:http://www.manageengine.ca/images/products/distributed-network-management.gif

Advantages:

1. Lack of central point of failure
2. Ability to protect machines outside topologically isolated space
3. They provide more security as they don’t trust any network i.e internal as well as internet
4. They can apply the policies on all the network traffic
5. They can manage internal threats.

Disadvantage:

1. Harder to allow in certain services, whereas it’s easy to block
2. Allowing in certain services works if and only if you’re sure the address can’t be spoofed
    i. Requires anti-spoofing protection

ii. Must maintain ability to roam safely

2.3.3 Network Firewalls

These kinds of firewalls are [16] normally running on a dedicated network device or computer positioned on the boundary of two or more networks or DMZs (demilitarized zones). Such a firewall filters all traffic entering or leaving the connected networks. It may be hardware device or a software programs or combination of the both.

3. PROPOSED WORKING MODEL OF FIREWALL

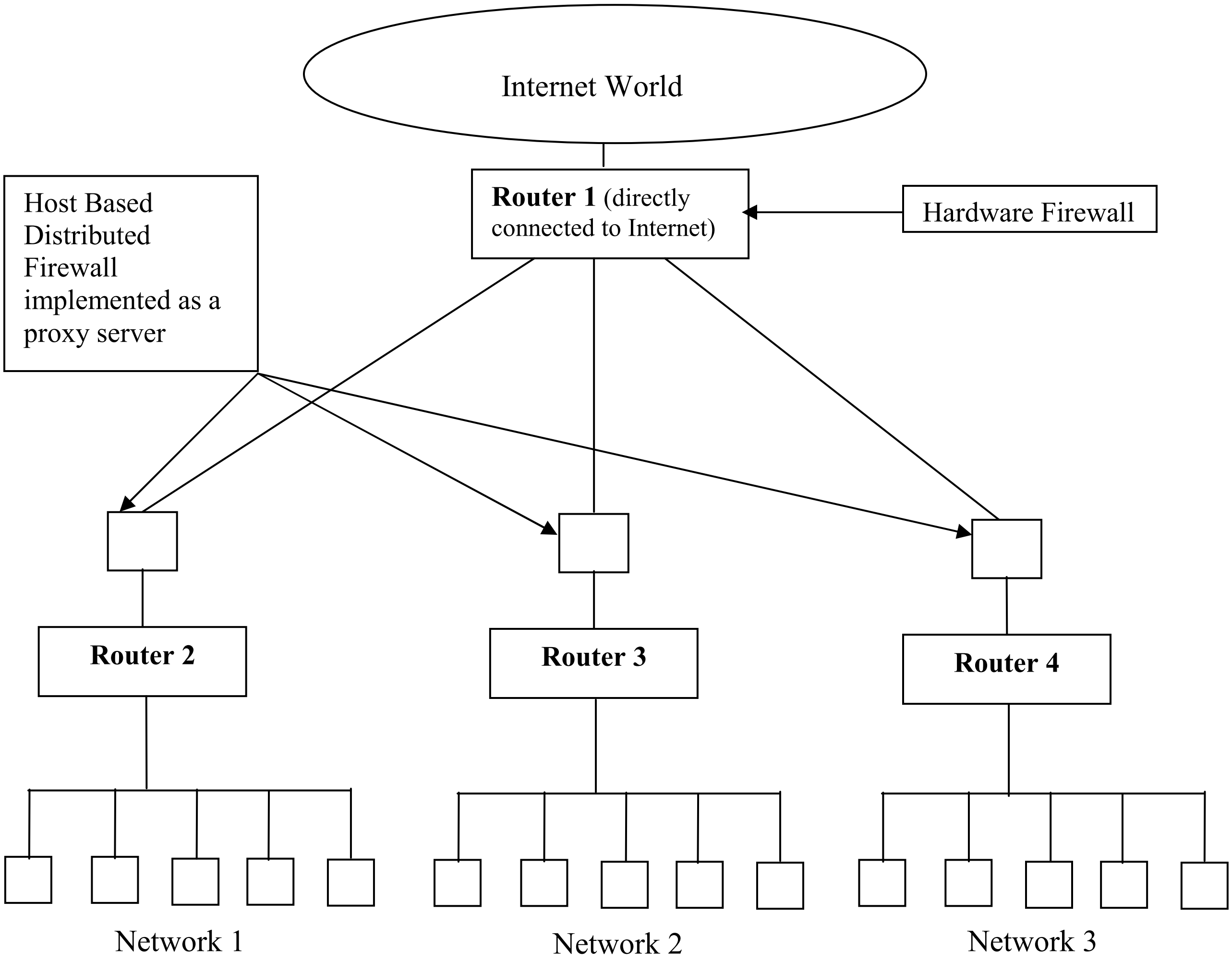
Internet World
Router 1 (directly connected to Internet)
Hardware Firewall
Host Based Distributed Firewall implemented as a proxy server
Router 2
Router 3
Router 4
Network 1
Network 2
Network 3

Fig 10

The proposed working model for the security of any establishment using different types of networks and network topologies is shown in Fig 10

All networks (Network 1, 2, 3…) can share information among them selves and can receive and transmit information to the internet. Router 1, available as Stage 1 firewall, is directly connected to the outside world (internet) and also connects all the networks of the establishment. Hardware firewall is implemented at this stage because at this point we are in need of clearing the traffic at a fast rate and thus, only packet filtering is done. Rest all restrictions are left for stage 2 firewall.

All the individual network of the organization are connected through a router or switch which is attached to a computer system i.e any packet crossing from that network must cross through the router or switch which is connected to the computer placed there where a software firewall is placed.

This software firewall is a combination of various services. Our proposal is place a host based distributed firewall with proxy service on these systems. Various services of firewalls will be provided by this combination. Host based firewall will protect the individual systems in the network where as the distributed system will make the job of network administrator easy. He can manage the firewall policy from a single point.

Stage 1 (Hardware) firewall:

Its main function is of packet filtering. It will check the IP addresses of the source and destination. Traffic from all the networks will cross Router 1 which is directly connected to the outside world, thus we need something which can keep our network safe and also no congestion is made, thus we have to clear the traffic very speedily at this point. Thus a hardware firewall is recommended at this place. This will filter out the bad stuff at this point only at a very fast rate.

Stage 2 (Software) firewall:

This is a software firewall which is a combination of various functionality like application firewall:- will filter the contents as well as maintains the state of the connection, Distributed firewall:- will distribute the policies and keeps the job of network administrator easy. He can maintain the policies from a single point, Host based firewall:- will keep the individual systems secure, Proxy service:- will cache the pages visited by the various systems connected to that network for future use.

Incoming Traffic:

Packets coming from internet at intercepted at stage 1 where a hardware firewall does the job of packet filtering only. Here the source and destination ip addresses are checked. If it is a legitimate packet it is allowed to pass the hardware firewall and is directed towards stage 2 firewall of the designated network. At stage 2 firewall packets are either coming form outside world (internet) or from the other network of the organization. This firewall is a combination of host based distributed application proxy service. This combination checks for the kind of application (HTTP, FTP, TELNET, SMTP etc), filters the contents of the packet and maintains the state of the connection. If the packet fulfills all the requirements it is allowed to pass through the firewall and reach its destination. Otherwise it is dropped.

Outgoing Traffic

Any packet leaving the traffic first faces the stage 2 firewall which checks for the contents, connection and application from where the packet is coming and decides whether the packet should be allowed to cross the firewall or not. Then it will face the stage 1 (Hardware) firewall which will simply allow the packet to move either towards the outside world (internet) or to the other networks of the same organization.

4. CONCLUSION

Main objective of the firewall is to keep our network safe from any kind of outside threat. Deploying firewall is the first important step towards securing networks. The effectiveness of firewall security may be reduced by:

a. poor management of firewall policy

b. defective implementation of the firewall.

For making it more secure, additional inspection criteria can be added which can cause extra latency to the forwarding of packets towards their destination.

Normally own network is assumed to be safe. But presently, it has been seen that most of the security violations are from internal sources. With the increasing number of Worms and viruses that attack internal networks, a single firewall is no longer sufficient to fully defend and protect our network against threats.

We must also consider the fact that Security and network performance have always been inversely proportional. Thus increasing security means we will be putting more load on to the firewall, thus decreasing its throughput.

Some of the firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic

5. REFERENCES

1. http://www.scribd.com/doc/6669985/Firewall
2. http://computer.howstuffworks.com/firewall4.htm
3. http://www.absoluteastronomy.com/topics/Demilitarized_zone_%28computing%29
4. http://en.wikipedia.org/wiki/Firewall_%28computer%29
5. http://en.wikipedia.org/wiki/Firewall_%28computing%29
6. http://en.wikipedia.org/wiki/Firewall_%28computer%29
7. http://www.scribd.com/doc/7627655/Internet-Firewalls
8. http://www.smallbusinesscomputing.com/webmaster/article.php/10732_3103431_/Firewall-Debate-Hardware-vs-Software.htm
9. http://www.scribd.com/doc/12885424/Distributed-Firewall
10. http://www.usenix.org/publications/login/1999-11/features/firewalls.html
11. http://www.scribd.com/doc/43448666/Malware-Incident-Prevention-and-Handling
12. http://itlaw.wikia.com/wiki/Host-based_firewall
13. http://www.scribd.com/doc/43448666/Malware-Incident-Prevention-and-Handling
14. http://en.wikipedia.org/wiki/Distributed_firewall
15. https://www.cs.columbia.edu/~smb/papers/distfw.html
16. http://www.scribd.com/doc/6669985/Firewall