Big Firewall for the safety of the whole cyber world

Name- JagrutLaxman Patil

Class- TYBscIT

College- SonopantDandekar College Palghar

Abstract

In this digital world communication over internet have become curtail as its fast and simple. But over internet security is very important topic to be looked upon. In existing system people use internet connection that have inbuilt protection of firewall but some time it's not sufficient. The cyber crime is increasing day-to-day so more advance security methods are needed. Firewall normally is of two type i.e. Packet filter and Application gateway. Normally its present in Wi-Fi router if the user is using any router. But it only for single user or group of user using that particular router. Big Firewall is a hybrid firewall that does but packet filter as well as application gateway but over large scale. Means all available network present in Nation could be passed through one firewall. Such a system could act as proxy server for whole national cyber world. All servers outside the nation could be accessed only through this proxy server or big firewall. This could cut-short the time taken for the investigation of the cyber crime cases. For example, if user wants to access his/her facebook or Google account then it must go through this system only. Normally public domain networks could be implemented with this system. This system act as shield for cyber world of the country.

1. Introduction

The dramatic progress and advancement in internet has opened ocean of possibilities. One user can connect any other user over internet no matter how far they are geographically. These is a boon to a cooperate world and normal user. But toughest task lies to the networking staff, i.e. maintain the stability of the network and to protect the network from different types of attack. All user's and different corporation have different amount of valuable and confidential data in their particular system. Leaking of this critical data in the wrong hands can create a blunder and legal issues. Firewall then comes into picture; firewall is an effective means of protecting a local system or network of system inter connected. A firewall is a barrier through which the data packet traffic goes in both directions through a common gateway. In common scenario firewalls are designed to operate at higher protocol layer or at level of IP packets.As these is for commonly used firewall but probably there is no common gateway for whole country from which the other servers from outside the countries network. The proposed system can monitor the traffic of both incoming and outgoing packets but also can trace the miscellaneous packets with their source and destination address.This system can act as proxy server for all other servers the user computer wants to connect. All the (ISP) internet service provider could be linked with this system to monitor the cyber activity of internal networks. the viruses and worms could be avoided to some extends.

2. The problem

The problem people normally face in cyber world is getting hacked. The user can be victim of viruses, worms, being bot of Botnet network or any other scenario. In Cyber world where the crucial data is present there is always need of security. If the hackers or crackers from other nation penetrate into the system bypassing the security measures they can have whole virtual accessto the system. The present system firewall has its own limitation.

3. Proposed System idea

Big firewall is the system that will deal with the nationwide networks and their traffic of packets that travel inside out of the country network. Big firewall will act as a proxy server or common gateway for normal user who wants to connect to the other server outside the nation. All servers like this could be prone to Denial of services (DOS) or Distributed Denial of services (DDOS) attack but this could be prevented by monitoring the incoming traffic coming from outside. Once the particular IP is detected with hampering rush of packets the reflex could be performed means same packets could be reflected back to the source where it came from or simply that particular IP or group of IP's could be blocked. The big firewall should also perform the trace of the internal users i.e. the path of packets from source to destination. That may include monitoring of all Internet Service Provider (ISP). As they can help to get the source and destination IP address so the actual path of the network could be traced. This could help the cyber crime department while investigating. Although the Criminals mask their IP's but then they need network connection to access internet so monitoring the ISP could help it. If there is outbreak of particular new type of virus or worm in outer network and it's traced and identified then it could be prevented from entering the local network or national network. If it enters the system then it could be handled by the traditional method i.e. Anti-Virus. If the signatures of the Trojan horse are detected then the system should block the medium from which it's coming in the system to prevent intrusion. This system can be implemented at smaller scale to create more layer of security. If due to any issues the system fails then to the internal local network should work but without such security. This system does not work on its own as the normal firewall does but this one needs maintenance as it also avoids viruses and worm it is necessary to update the database of the viruses with new signatures. The system also needs to modify the security policies when needed. . If a scenario arises and this system fails then the whole system will switch to traditional system with less security.

4. System Architecture

The main flow of this system starts with linking all the internet providers in nation. System will monitor and inspect every packet traffic which will pass through it. Once it is implemented it enforces access policies for the access or connecting a system. System will also have a track of the IP address of the user and the server the user want to connect and also the path the user request will take to reach its destination.The packets could be encrypted so the consistency of the data is maintained. Packet filtering commonly depends on IP source and destination address, direction (inbound or outbound), TCP or UDP source and destination port.

4.1 The following Diagram describes the system flow and working of the big firewall.

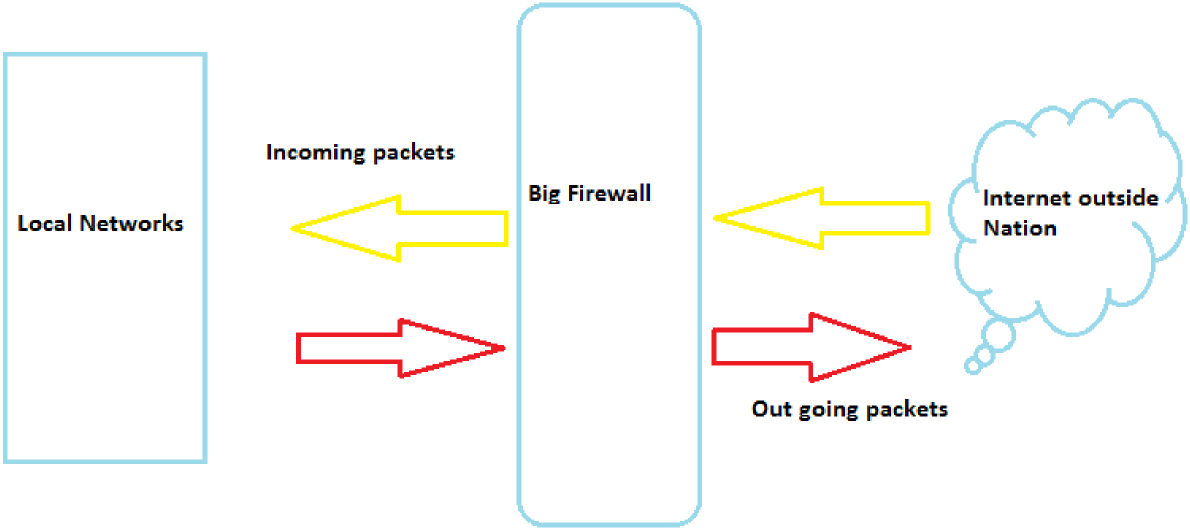

Figure -1.1 system architecture of proposed system.

Internal user will send packets to the proxy server or big firewall and it will again forward the packets to respective servers.

Related work:

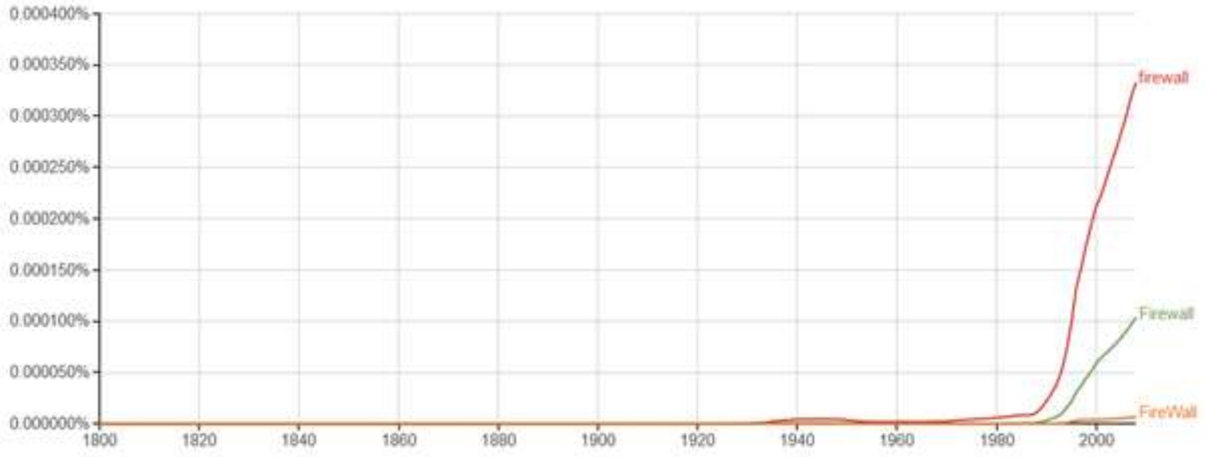

Figure - 1.2 the use of firewall exceeding the expected use[2].

Firewalls can be broken down into two categories, and this is hardware firewalls and software firewalls. One myth that you may have heard people say is that "hardware firewalls are a lot more powerful than software firewalls."The truth of the matter is that hardware firewalls are not necessarily more powerful than software firewalls. Some hardware firewalls do not have the necessary security patches, and the reason for this is because the process of re-imaging ASIC chips (which contain the OS for the firewall), is far too challenging for many network administrators. At the same time, some administrators add security patches to multi-use operating systems and the firewall software. A firewall which is well designed, like ISA 2004 for example, will prevent network traffic which is disallowed prior to the OS processing it. This means that it will basically get rid of the OS as an attack vector. One thing that I should also note is that as technology continues to advance, the line which exists between the hardware and software firewalls has become more blurred [3].

Layer Number	OSI Reference Model Layer	Firewall Functions
7	Application Layer	Application-level gateway
6	Presentation	encryption
5	Session	Socks Proxy server
4	Transport	Packet filtering
3	Network	NAT
2	Data Link	N/A
1	Physical	N/A

Figure 1.3 : Different bifurcation of layer wise functioning of the firewall.

The standard firewalls which function at the Layers 3 and 4 within the OSI(Open System Interconnect) model are not capable of protecting your system against the latest attacks, and the reason for this is because they will not inspect the traffic that is present in the application Layer, also known as Layer 7. Many firewall companies have addressed this problem by making use of application layer filtering. When this inspection is made, the firewall will take one packet, or it may also structure multiple packets which comprise application traffic, and will make certain decisions based on this traffic. The application layer firewall can also be responsible for the security of traffic which uses FTP. FTP will utilize a specific connection among the client and server, and it can negotiate an additional connection for the actual transfer of data. The application support will allow the firewall to analyze these control connections, and it will also allow the additional connection to utilize the port that both the client and server agreement on. In the past, most firewalls used Layers 3 or 4, but they are not very efficient against the newest attacks. Hackers eventually figured out that many of the rules which comprise these older firewalls will allow them to transmit traffic to an internal network, so long as their tools made use of port 80 as the primary source port. Due to these weaknesses, any good firewall today will not be totally dependent on packet filtering. An inspection of the circuit level was made to find ways to bypassing the weaknesses that are prevalent in firewalls that make use of Layers 3 or 4.

5. Technical Requirements

Software component required for Proposed system

- Proxy server.
- Packet filter.
- NAT (Network Address Translation).
- Authentication mechanism.
- Encrypting traffic packets

6. Drawbacks:

- If system fails it is vulnerable to the different kind of attacks.
- Internal user spreads the malware it can’t be helped.
- The system security decreases the speed of internet connection.
- If the traffic is more them its capacity the system may crash.

7. Conclusion

The basic aim is to protect the countries cyber world from external intruders and harmful threats on internet. So it’s better to have as many as security layers for protection of the system for different networks connected within the country. This could cut-short the time taken for the investigation of the cybercrime cases.

8. Reference

[1] Book:Cryptography and Network Security by Atul Kahate Fourth edition.

[2]https://books.google.com/ngrams/graph?year_start=1800&year_end=2008&corpus=15&smoothing=7&case_insensitive=on&content=firewall&direct_url=t4%3B%2Cfirewall%3B%2Cc0%3B%2Cs0%3B%3Bfirewall%3B%2Cc0%3B%3BFirewall%3B%2Cc0%3B%3BFireWall%3B%2Cc0

[3]http://www.exforsys.com/tutorials/networking/network-security-firewall-architecture.html