International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.4., 2016
(July-August)

RESEARCH ARTICLE

ISSN: 2321-7758

"TRADITIONAL, DISTRIBUTED AND PERSONNEL FIREWALL MANAGEMENT SYSTEM"

PREETI[1], DHARAMBIR SINGH[2]

[1,2]M.TECH Research Scholar, SITM Rewari, Haryana, India

PREETI

DHARAMBIR SINGH

ABSTRACT

A firewalls a set of rules, regulations and the set of related programs, that is situated at gateway server of the Autonomous network, that protects the all the resources of an Autonomous network from the outside users of the network or from the unauthorized users belongs to any other networks. Or we can say that the firewall is a firewall is software or can say a hardware that helps to prevent hackers and some other type of malware from getting to your PC through a network or the internet. It does this by checking the information that is coming from the internet and then either block it or allowing it to pass through to your computer.

KEYWORDS- Firewall, Packet Filtering, VLAN, Proxy gateway

1. INTRODUCTION

As we all know that the internet become one of the basis need of todays. Most of our works are online like internet banking, online shopping, social media and many more. It became a global meeting place everyone use internet for uploading or downloading files in there every day activities, but when we are using the internet there is risk of the security.

Network security is very important to avoid such security risks. The aim of network security is to protect our data from these risks. Many tools and techniques are used for network security, Firewall is one of them which is an important tool for the network security. Basically a firewall separate a private network from external network. Firewall is located between the private network and external network with an assert of predefined rules and the firewall has to follow that rules when network traffic passes through it. Then it can accept the entry of data or reject the data as per the rules set previously.

No doubt that the traditional firewalls have critical role in the network security but no one can denies about their drawbacks because in this security policy is centrally defined so that is the chock point.

- Security policy is centralized in traditional network
- Centralization of security policy become its drawback
- If once a data entered though it then large amount of data can penetrate that firewall.

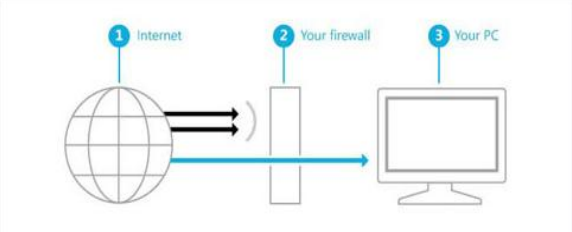


Figure 1. Diagram of a firewall.

There are several researches to overcome from the drawback of traditional firewall Windows Firewall is one of the recent approach is Windows Firewall in this direction. In windows Firewall security policy is still centralized but enforcement is left up to the individual endpoints.

- Security policy is still centralized but
- Enforcement is left to the individual endpoints
- Below given diagram is of firewall structure:

(Firewall Block unwanted traffic)

2. LITERATURE REVIEW

Traditional Firewall: The only software situated at the starting of the private network which is used to block unauthorized users coming from the outside network. In it policy is prepared to prevent the access from outside or it might be prepared to allow the access only from the fixed places from certain places and certain users.

A firewall can filter both incoming and outgoing data through it. In this type of filtering the decisions to forward and rejected are based on the protocols used. It uses below information to decide whether to accept or reject a network:

- Source Address
- Destination Address
- Network Header
- Transport Layer Protocols like TCP, UDP, ICMP ect.
- Transport Header
- Whether the packet is incoming or outgoing
- Interface from which packet was sent and at which packet will receive

A traditional firewall do not prevent whole network from the every type of the attack more than firewall do not protect from viruses and malicious code passes through it. They do not know if any thread is present inside the network. The network policy define the network expectations and procedures to prevent and respond to the security incident.

Although there are several benefits of traditional firewall.

There are some drawback also which are given below.

Disadvantages of the Traditional Firewall:

- They can be bottleneck to throughput since firewall have to inspect every packet of the data on network communication, they often decrease network performance.
- Traditional firewalls has centralized security policy so they have a central point of attack
- If any data will break the firewall then unlimited network can pass through it without filtering
- One of the main drawback of the firewall is that it does not protect from the inside attackers.
- Firewall do not protect against the data drive which are:-
- Viruses
- Java Applet
- Java Scripts

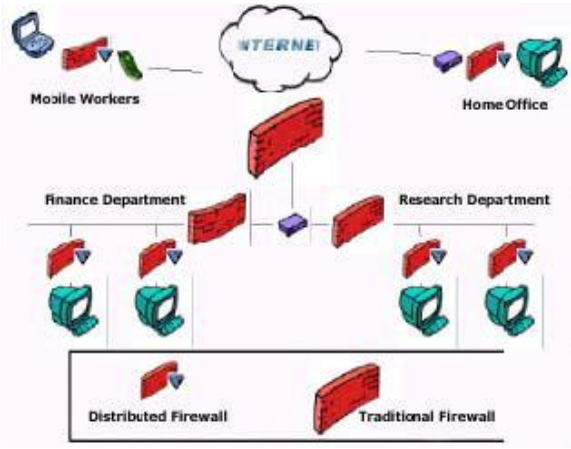
Distributed Firewalls

Now a day where network complexity is increasing as well as network techniques are also increasing it becomes very difficult maintain a predefined network topology. Demands of the users are continuously increasing so traditional firewall is inadequate to fulfil that demands so now we require Distributed Firewall.

Idea behind the Distributed Firewall is enforcing the policy rules at end points rather than a single point in the network. Security policy is still centralized in distributed Firewall system as on Traditional firewall system. Main aim for the discovery of this firewall is to overcome the disadvantages of the Traditional Firewall.

In distributed firewall system a firewall is situated with individual Computer in a network and enforcing the policy rules at every point but the security policy is centralized. In this way firewall system do not affected by the increase of network topology. So, due to topology change Firewall system does not suffer.

Distributed Firewall system is not only one software that is placed between two networks. Please see the Diagram of the distributed firewall system layout you will understand the architecture. After removing a single chock point bottleneck of the system is eliminated. The unique access control for each of the network system allows different levels of security to be implemented on the computer system in the same network.



There are three components for distributed firewall environment.

These components are:-

- policy language
- policy distribution scheme and
- Certificates.

Policy language defines which inbound and outbound connections are allowed or rejected. Basically it is equivalent to packet filtering rules. Policy language should also support credentials, for delegation of rights and authentication purposes. While traditional firewalls usually use the IP address as an identifier, distributed firewalls use cryptographic certificates as identifier since distributed firewalls are independent of topology. Certificates enable making decisions without knowledge of the physical location of the host. Public-key cryptography mechanisms are most often applied in contemporary implementations.

Policies are distributed according to following distribution scheme:-

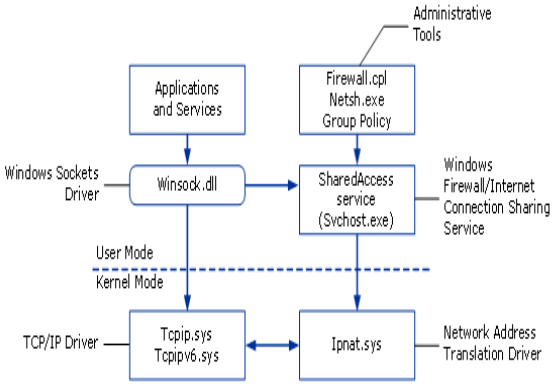
- Polices and credentials are applied to every end point
- Policies and credentials are taken from the trusted repository at the time of installation.

Distributed firewall system provide encryption mechanism for TCP/IP called IPSEC. Distributed Firewall system has advantages as well as disadvantages which are given below.

3. ARCHITECTURE OF WINDOWS FIREWALL

Components:

- Connection sharing service
- Network address translation Driver
- IPV4 based TCP/IP driver
- IPV6 based TCP/IP driver
- Windows Socket Driver



(Architecture diagram of WINDOWS FIREWALL)

Connection sharing services: Connection sharing services is a windows firewall software situated between the private network and outside network with the policy services

Network Address Translation: Network address translation (NAT) is used in Firewall to hide the internal structure of the network from the outside world.

IPV4 AND IPV6 based TCP/IP Drive: IPV4 & IPV6 drive controls the flow of information between the network adapter and system services. TCP/IP drive sends a notification when packets are dropped.

Windows Socket Drive: The Winsock driver is responsible for assigning and binding ports to a program or system service. Programs and system services use this driver when they need to listen for incoming traffic.

4. CONCLUSION

In Internet most of it is awesome but some of it is not quit , your business needs it to revise the

data as good can in and bad can be out this is known as security of the data to not to enter the bad stuff it is pretty obvious that open the ports for the good stuff and block the bad stuff, Similarly in firewall let go the stuff and block the stuff too it is also a type of security technique but these guys get sneaky they get starting directed bad stuff through firewall to break the internal server of the organization and they succeed because today's most of the firewalls do not understand the traffic, we need the firewall that can block the stuff more but that is just for your business it should have the ability to hold more software.

What should a firewall do.

- It sit there and judge the data and protect you.
- Firewall must have actively inspect the stuff which should allow or which should not.
- It should identify both side traffic incoming and outgoing all the traffic all the time while the approved traffic always gets through.
- Firewall should be genius follow the network study the policy whenever they found any data type about which there is not written in the policy then they save that files in safe environment that they never been see before then remember that thing in the future.
- Also everything should clear to you in a documented file that what has firewall done with the data till date. So we can always allow the application you need that is completely new or trying to hide

REFERENCES

[1]. Al-Shaer, E.S., Hamed, H.H., Boutaba, R. and H. Masum. 2005. Conflict Classification
[2]. and Analysis of Distributed Firewall Policies. IEEE Journal on Selected Areasin Communications 23(10): 2069-2084.
[3]. Al-Shaer,E.S.,Abdel-Wahab,H.,and. 1999.Hifi:A new MonitoringArchitecture for
[4]. Distributed Systems Management. International Conference on Distributed Computing Systems, Austin, Texas.
[5]. Al-Shaer, E. and HazemHamed. 2004. Discovery of Policy Anomalies in Distributed Firewalls, Proceedings of IEEE INFOCOM'04.
[6]. Al-Shaer, E. and HazemHamed. 2003. Firewall Policy Advisor for anomaly Detection and Rule Editing. IEEE/IFIP Integrated Management IM'2003.
[7]. Awerbuch, B. and R.G., Gallager. 1987. A new distributed algorithm to find breadth first search trees. IEEE Transactions on Information Theory 33: 315–322.
[8]. Bellovin, S. M. 1999. Distributed Firewalls. Login; special issue on security.
[9]. Chapman, Brent and Elizabeth Zwicky, eds. 1995. Building Internet Firewalls.
[10]. Cambridge: Orielly& Associates Inc.
[11]. CodeProject, Developer. 2008. FilterHookDriver.