INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES
© 2004-13 Society For Science and Nature (SFSN), All Rights Reserved
www.scienceandnature.org

Short Communication

FIREWALLS AS A MEANS TO PROVIDE INTERNET SECURITY

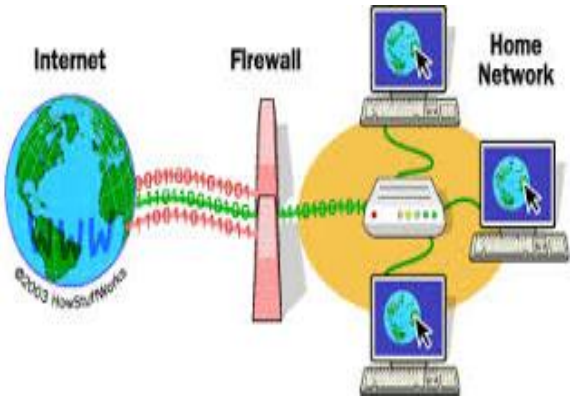
Kour Tejasvit,
Chandigarh Group of Colleges

ABSTRACT
With the grand scale use of the internet arises the need of its security. Every now and then various threats and viruses are created to disrupt the system. Hacking poses another serious threat to internet as it may lead to mishandling of highly confidential and important data concerning with various companies and even national security. Internet security there becomes very important. Various ways through which it is achieved is by using IPSec, PGP, SSUFLs, VPN and firewalls. In this paper technique to provide network security via firewalls is discussed in detail. Various types of firewalls like packet filtering .application firewalls, proxies are discussed.

KEYWORDS: Packet Filtering, Stateless, Application, Proxies,

INTRODUCTION

A firewall is used to keep a network secure. It is a device usually a router or computer installed between the internal network of an organization and the rest of the internet. It is based on a predetermined rule set to control the incoming and outgoing network traffic by analyzing the data packets. Upon ensuring that the other network is secure and trusted it builds a bridge between the two devices. There are various operating systems used in PCs to protect against threats from the public internet. Many routers contain various firewall components for security. Thus a firewall can be both hardware or software based. From time to time various advancements and improvements in firewalls have been made.

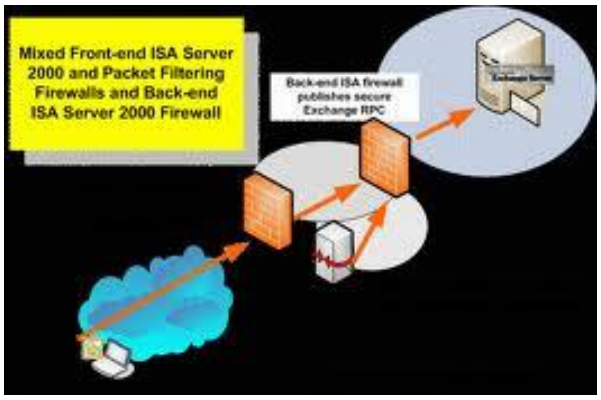


Various types are described as under

Packet filtering firewalls(first generation)

It is one of the most basic and oldest methods of firewall filtering. This firewall allows only those packets to pass through it which have been allowed as per a predefined firewall policy. The packets passing through this firewall are inspected and a decision is made whether to pass the packet or not. They were the first kind of firewalls ever.

Packet filtering is mainly classified into stateless and stateful packet filtering. In stateless packet filtering the information about the passing packets is not remembered by the firewall.



In this the present packets are not related to previous packets that is why they they are not safe enough and can be easily dodged by the hacking party. It is also the first generation of packet filtering. In stateful packet filtering, the previous packets information is remembered. It is also known as dynamic packet filtering. It is smarter than the stateless packet filtering. It marks the second generation of packet filtering.

Some important points which should be checked in a packet filter are

- Source IP address of the packet.
- Destination IP address of the packet.
- TCP/UDP port number.
- ICMP message type.
- Fragmentation flags.
- IP options settings.

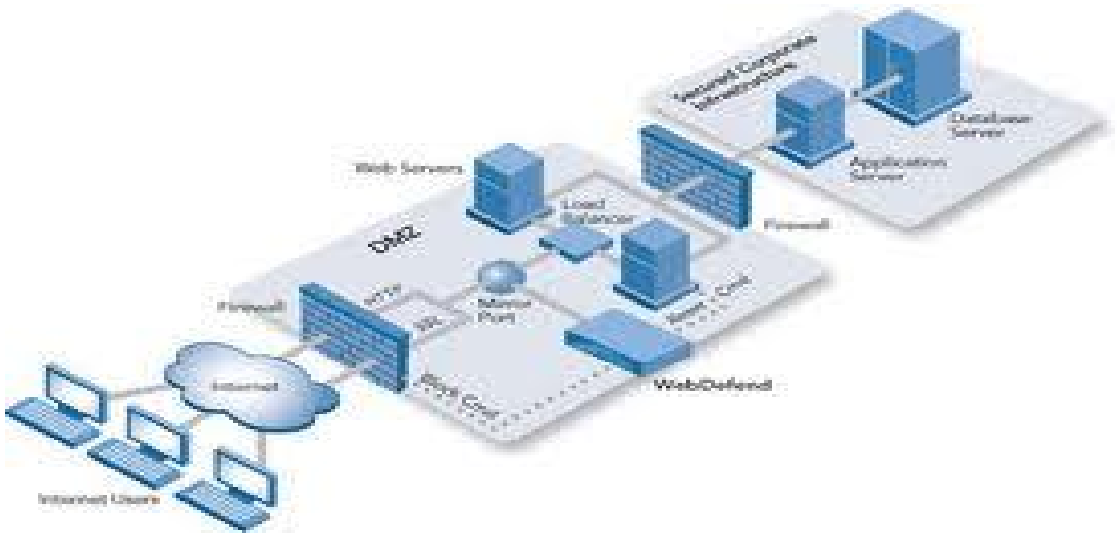
Some important points about packet filters:

1. For efficient filtering ,there should be a careful evaluation of the packet filters.

2. It should be easy to create new rules and firewall exceptions and this requires an easy command line syntax or GUI of firewall.
3. As much as possible number of logs must be provided.
4. Packet filtering firewalls work mainly on the first three layers of the OSI refernce model
5. Most of the work is done between the physical and network layer with a little involvement of the transport layer.

APPLICATION FIREWALL

It works by monitoring and potentially blocking the system service walls which do not meet the configured policy of the firewall. Its most important advantage is that it can understand certain applications and protocols such as (HTTP -Hyper Text Transfer Protocol, FTP-File Transfer Protocol, DNS-Domain Name System).



An application layer as the name suggests is built to control all traffic on an OSI layer upto the application layer. There are two types of application firewall

- Network based firewall
- Host based firewall.

Network based firewall

It is also known as proxy based or reverse proxy firewall. It is a firewall working at the application layer of the protocol stack. Protocol stack is an implementation of a computer networking protocol stack.

Host based firewall

In a host based firewall ,monitoring is done by examining the system passed through system calls in addition to or instead of a network stack. It can only provide information running on the same host.

Some other firewalls:

Linux

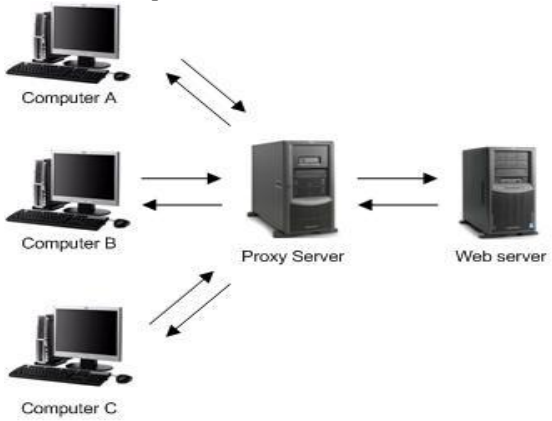
In linux various security packages are provided which allow filtering of operation to OS communication possibly on a by user basis

Zorp its core framework allows the administrator to fine tune proxy decisions and and fully analyse embedded protocols. It is released in a version GNU GPL and also in a commercial version with some additional features. It supports both transparent and non transparent working modes. FTTP, Pop3, LDAP, RADIUS, SQLNet NET8, Rsh etc are the are the protocols that it supports.

Systrace It provides computer security by limiting an application's access to the system by enforcing access policies for system calls. It can meet the effect of buffer overflows and other security vulnerabilities. It is specially useful when we are running binary only applications and provides privilege facilities for privilege evaluation on a system call basis and therefore helps to eliminate the need for dangerous setuid .programs.

Mod security another example of web application layer firewall , Mod security supplies an array of request filtering and other security features to the IIS, NGINX, Apache HTTP server

App Armor It allows the system administrator to associate with each program a security profile that restricts the capabilities of that program. It is implemented using the Linux Security Modules(LSM) kernel interface. App armor also includes a learning mode in which violations of the profile are logged, but not prevented. It is offered in part as an alternative to SELinux which critics consider difficult for administrators to setup and maintain. It is believed to be less complex and easier for the average user to learn as compared to SELinux.



Proxies

A proxy server may act as a firewall while responding to required input packets , while blocking other packets. A proxy server may run either on dedicated hardware or as

software on a general purpose machine. Proxies help to protect the network by making tampering with an internal system from the external system more difficult .
A proxy server intercepts connections between sender and receiver. By blocking direct access between two networks proxy servers make it more difficult for the network hackers to get internal addresses and details of a private network. In a proxy server a client connects to a proxy server requesting some service such as a connection or a resource available from a different server. Based on its filtering rules the proxy server evaluates the request.

CONCLUSION

Firewalls provide an important method for providing network security. Various types of firewalls like packet filtering, application firewalls. proxies are used. But still hacking and threats ands viruses have not been controlled to the fullest. Therefore these techniques should be improvised and updated from time to time to deal with the hacker's andf threat imposers. Latest techniques like zorp, app armour, systrace should be followed and more of their kind be created and implemented in order to provide full internet security. One important point in this regard is also the user knowledge about the potential threats that can be imposed.

REFERENCES

Data communication and networking fourth edition by Behrouz A. forouzen
Computer networking by James F. Kurose

Computer networks by Andrew S Tanenbaum

http://skproxy.com/

http://en.wikipedia.org

http://images.yourdictionary.com/proxy-server

Building internet firewalls 2nd edition by Elizabeth D. Zwicky, Simon Cooper, D.Brent Chapman

Firewalls and internet security 2nd edition by William R. Cheswick, Steven M . Bellovin, Aviel D. Rubin

Network +guide to networks (Networking(Course Technolgy)) by Tamara Dean

Hacking the art of exploitation ,2nd edition by Jon Erickson

Wireshark 101 :Essential Skills for Network Analysis by Laura Chappels and Gerald Combs

Security Engineering: A Guide To Building Dependable Distributed Systems by Ross Anderson