Abstract— A network is a group of two or more computer systems linked together which allows computers to exchange data. The internet is a connection of computer to any other computer anywhere in the world via dedicated routers and servers. Computer networks are involved in almost all sectors worldwide including commercial, military and government sectors where network security is major concern. With increasing technology threats are also increasing. Network security is security provided to a network from unauthorized access and risks. By assigning the user identification and password, we can provide protection up to some extent. The internet consists of computer based router. User's Information can be obtained by unauthorized persons or firms by using special programs such as “Trojan Horses”, planted in the routers. Internet threats will continue to be a major issue as long as the information is accessible, and threats are transferrable across internet. Common internet threats are Eavesdropping, Viruses, Worms, Trojans, Phishing, IP Spoofing Attacks, Denial of Service, etc. Common defence mechanisms are Cryptographic systems, Firewall, Intrusion Detection Systems, Anti-malware software and Scanners, Security Socket Layer (SSK) etc. Among these, Firewall is an access control device that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet. An overview of firewall and types of firewalls will be discussed in the paper. This paper is a collection from different sources like *Firewall and Types of firewall* by Sanket R Jain, *Internet Firewalls and Security A Technology Overview* By Chuck Semeria and related articles from Internet.

FIREWALL

Firewall is a network security system which is used to interconnect a private network to the Internet. Every message which is incoming and outgoing will be examined by the firewall. It analyzes the data packets, based on a predetermined rule set and prevents unauthorized access to a networked computer system from internet. A firewall helps in providing remote access to a private network through secure authentication certificates and logins.

A firewall first determines when the incoming transmission is requested by a user on the network or not. The firewall checks the sender’s computer address and the contents of the transmission. It examines the data in such a way that what kind and amount of data passed through it, how many attempts were made to break into it, and so on. It prevents access, at the same time monitors and identifies those who attempt to breach the security.

A firewall may be a hardware or software. Hardware based firewalls are integrated into the routers where as software firewalls are installed in individual computers which are used to secure data from internet threats. An ideal firewall configuration consists of both hardware and software based devices.

FIREWALL PROPERTIES

A firewall system possess the following properties:
- Only authorized traffic, as defined by the security policy is allowed to pass through it
- The system itself is immune to penetration

FIREWALL SECURITY POLICY

The firewall security policy is actual technical implementation guideline for the rules laid out in organization security policy. The main function is to allow or disallow the types of traffic and connections as per security policy. If a firewall is packet filter type then firewall policy decides which packets are allowed to pass through the firewall. And if it is an application proxy or gateway type then it will decide which type of traffic is allowed to be accessed through the firewall.

Firewall policies
1. **Network Policy**
   - There are two levels of network policy that directly influence the design, installation and use of a firewall system. The high-level policy is an issue-specific network access policy that defines those services that will be allowed or explicitly denied from the restricted network, how these services will be used, and the conditions for exceptions to this policy. The lower-level policy describes how the firewall will actually go about restoring the access and filtering the services that were defined in the higher level policy.

2. **Service Access Policy**
The service access policy should focus on Internet-specific use issues and all outside network access as well. A firewall can implement a number of service access policies:

- Which may allow no access to a site from the Internet, but allow access from the site to the Internet.
- Which may access form the Internet, but only selected systems such as information-servers and E-mail servers.
- Which allows some user access from the Internet to selected internal hosts, but this access would be granted only if necessary and only if it could be combined with advanced authentication.

3. Firewall design policy

This policy defines the rules used to implement the service access policy. Firewalls generally implement one of the basic design policies

a. Permit any service unless it is expressly denied
The firewall which implements this policy allows all services to pass into the site by default, with the exception of those services that the service access policy has identified as disallowed.

b. Deny any service unless it is expressly permitted
The firewall which implements this policy denies all services by default, but then oases those services that have been identified as allowed. This policy follows the classic access model used in all areas of information security.

Types of Firewalls

Network Layer Firewall or Packet filtering
The first type of firewall was the packet filter which looks at network addresses and ports of the packet and determines if that packet should be allowed or blocked. Data travels on the internet in small pieces which are called packets. Each packet contains information like source address and destination address. Packet filters inspects the packets. If a packet does not match the packet filter’s set of filtering rules, that packet is dropped or rejected. Users can define their own rules, but these software packages often come with a list of default rules already provided.

Packet filtering firewalls work mainly on the first three layers of the OSI reference model, which means most of the work is done between the network and physical layers.

Stateful packet inspection
In addition to the packet filtering, this type of firewall also keeps track of connections. It retains all the packets until the enough information is available. It records all connections passing through it and determines whether a packet is the start of a new connection, a part of an existing connection. If it is neither of the two, it is probably useless and can be dropped.

A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Because of this, filtering decisions are based not only on administrator-defined rules but also on context that has been established by prior packets that have passed through the firewall.

This firewall performs the work up to the fourth layer i.e. the transport layer of the OSI model.

Application-layer Firewall

Application layer firewalls are the most powerful firewalls. These firewalls, inspect all packets for specific protocols, such as FTP and browser traffic. Each packet is deeply inspected for content that does not match the header information. Because of this application layer firewalls are often effective at restricting or completely blocking the spread of worms and Trojans.

The application firewall is designed to control all network traffic on any OSI layer up to the application layer.

Proxy Servers

A proxy server is a dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another server from which a user or client is requesting a service. The proxy server may exist in the same machine as a firewall server or it may be on a separate server, which forwards requests through the firewall.

Personal firewalls

This is also known as desktop firewall which is an application for laptops and desktops. This firewall disallow inbound/outbound traffic and protect laptops and desktops from attacks based on a security policy.

Network Address Translation(NAT)

This firewall is the process which hides all internal addresses. Thus it protects a computer or a group of computers in a private network from external attacks as internal addresses are not exposed.

Virtual Firewalls

A virtual firewall is a network firewall service which runs entirely within a virtualized environment and which provides the usual packet filtering and monitoring provided via a physical network firewall. This is logical partitioning of a single firewall into multiple logical firewalls, each with its own unique policies and administration. Each virtual firewall provides the same firewall features provided by a standalone firewall.

Transparent Firewall

A transparent firewall is Layer 2 firewall which provides ability to easily “drop in” a firewall into existing networks without requiring an addressing changes.

Communication Network and Security-An Overview of Firewall and Types of Firewalls

24
CONCLUSION

The internet threats have been increasing day by day. Firewall is one of the prevention. OTP, One Time Password, which is one type of firewall, helps in online transactions like E-banking to avoid unauthorized access. Biometric which is also a type of firewall, helps to avoid impersonation almost in all the fields. Even though there is possibility of hacking and unauthorized access if we don’t take the proper measures. For example: changing passwords frequently.

REFERENCES

[3] nptel.ac.in
[6] Internet Firewalls and Security A Technology Overview By Chuck Semeria
[10] https://www.techopedia.com/definition/5355/firewall
[13] Firewall and Types of firewall by Sanket R Jain
[16] Firewall Security Policy, on June26, 2010, in Firewalls by Ganesh Dutt Sharma