ORIGINAL RESEARCH PAPER

Computer Science

ROLE OF FIREWALL IN DATA SECURITY ON PUBLIC NETWORKS

KEY WORDS: Data Security, Firewall, Proxy, IP

Seema Sangwan Asstt. Professor in Computer Science, Pt. N.R.S. Govt. College, Rohtak Haryana

Suman Asstt. Professor in Computer Science, Govt. PG College for Women, Rohtak Haryana

Dr. Geeta Dalal Asstt. Professor in Computer Science, Pt. N.R.S. Govt. College, Rohtak Haryana

ABSTRACT

In this paper we have presented a detail study of firewall technologies which are commonly used for network security. A firewall cannot handle all the destructive threats which are coming from unauthorized networks. Therefore, to develop a secured network different types of firewall technologies are used. Lot of researches has been done considering technologies of firewalls. Computers and Networking have become inseparable by now. A number of confidential transactions occur every second and today computers are used mostly for transmission rather than processing of data. So Network Security is needed to prevent hacking of data and to provide authenticated data transfer. The main purpose of this paper is to apply firewall capacity along with other firewall technologies such as packet filtering, network address translation, virtual private network and proxy services in order to prevent unauthorized accesses. Due to lack of many researches, related to firewall capacity and firewall technologies together. The research group focuses to build a more protected network by combining both firewall capacity and firewall technologies. The experiment results show the proposed idea good enough to build a secured network.

1. INTRODUCTION

A firewall is designed in order to prevent or slow the spread of harmful events using firewall technologies to secure the network. Packet filtering, the firewall technologies that are currently existing can be named as Network addressing translation, Circuit-Level gateways, virtual private network, Proxy service, Application proxies and Application-Level gateway. The firewall has a mechanism to allow some traffic to pass while blocking the other traffic. Most of the researches that have been done up to date focus on network security using firewall technologies. These researches focus on combination of few firewall technologies like packet filtering, Virtual Private Network and Network Address Translation. When consider about Network security one of the most important points that should be taken in to attention is the firewall capacity. Firewall behavior basically depends on the capacity. Firewalls with higher capacities are expensive. The proposed system will acquire a more secured network combining low capacity firewall and firewall technologies.

The Packet filtering is referred to as static packet filtering, this method Controls the access to a network by analyzing the incoming and outgoing packets and letting them pass or uncertain them considered on the IP addresses of the source and destination. Packet filtering is one of the techniques, among many for implementing protected firewalls. The Network address translation is a methodology of remapping one IP address space into another protocol datagram packet header while they are in transit across a traffic routing device.

A Circuit-Level gateway is a type of firewall technique. Circuit-Level gateways perform at the session layer of the OSI model or "shim-layer" between the application layer of the TCP/IP stack.

They monitor TCP handshaking between packets to determine whether a request session is legitimate. Create secure networks connection over a public network owned by a service provider is a virtual private network. Large corporations, educational institutions, and government agencies use virtual private network technology to enable remote users to securely connect to private network. A Proxy firewall is a network security system that prevents network resources by filtering messages at the application layer. An Application-Level gateway is firewall proxy which provide network security

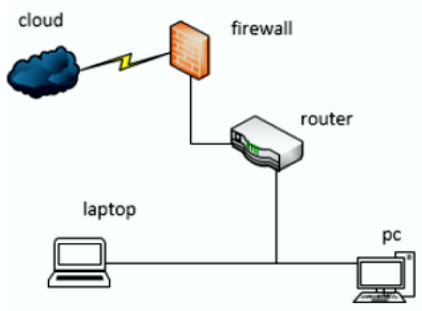

Fig:1 Firewall on Networks Topology

2. A Firewall

A firewall is a system or group of systems (router, proxy, or gateway) that implements a set of security rules to enforce access control between two networks to protect "inside" network from "outside network". It may be a hardware device or a software program running on a secure host computer. In either case, it must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to. A firewall is essentially a security enforcement point that separates a trusted network from an un-trusted one. Firewalls screen all connections between two networks, determining which traffic should be allowed and which should be disallowed based on some form of security policy decisions determined in advanced by the security administrator.

3. Reason For Consideration Of The Capacity Of Firewall

Firewall performance directly effects to network security and firewall performance depends on capacity of firewall. If firewall capacity high, it will give high performance. Therefore, research team selected firewall capacity for more secured network technique use encryption and other security mechanisms to make sure those only reliable users can access the network. The proxy server acts as a caching server to load the web page faster. The main technology focus in the research paper is the firewall capacity

4. Conventional Firewalls Drawbacks

- Depends on the topology of the network.
- Do not protect networks from the internal attacks
- Firewalls can become a bottleneck

- Multiple entry points make firewalls hard to manage
- Unable to handle protocols like FTP and Real-Audio.
- Single points of access make firewalls hard to manage.
- Unable to stop spoofed transmissions
- Unable to log all of the network's activity

5. Data Security Threats

Security of Data is of much concern. Security measures taken are almost identical in the wired and wireless world. This implies specialized physical and data link protocols. Any network is subjected to substantial security risks and issues, like threats to the physical security, eavesdropping and attacks from within the network's user community. Unauthorized Access can be of any means by which an unauthorized party is allowed access to network resources. Main Data Security Threats are:-

5.1. Denial Of Service (dos)

This network data security threat makes use of the simple fact that all servers have only a limited capacity to handle server requests. By making more requests to a network server than it can handle, this Network data security threat brings down the server. Denial of service has been used in the past to cause downtime of leading e-commerce firms, since it is an Easy network security threat to launch.

5.2 Ip Spoofing Or Ip Masquerading

IP masquerading, means being an IP imposter. The server that is attacking our network server pretends to be someone else (with a different IP) and as a result is able to gain unlawful access to the server being attacked. This network data security threat is possible because of the inherent poor authentication in the IP protocol. .

5.3 Session Hijacking

Session hijacking implies taking control of a user's session resulting in a very serious data security breach. For example, a user may be accessing some mission critical data or making an internet purchase. At that time, a session hijacker takes control of the user session, thereby getting access to the sensitive session data. The user is led to believe that he has been logged out and he logs back in. Session hijacking is an incredibly dangerous network data security threat wherein the attacker could compromise sensitive user data such as passwords or even credit card information.

5.4 Physical Access To Servers In Data Centers

It is amazing that we get so involved in guarding against internet based network data security threats that we do not realize that physical unauthorized access to our data center servers is still the largest threat to internet network and data security. Good data centers have network data security protection in the form of fingerprint based authentication and verification of credentials of all operations personnel visiting the data center.

6. Network Data Security Firewalls

Get an industry standard network data security firewall and safeguard our network from unwarranted intrusions. Also, do carry out periodic audits of our network data security firewall rules so that our network data security is not compromised.

7. CONCLUSION AND FUTURE SCOPE

Firewall is a general technique which provide the authorize network access. There are many firewall techniques used to protect from unreliable accesses. Therefore, network should be configured in such a way that the network should not allow unauthorized users entering the network or accessing the information. The proposed research focuses on various technologies. Packet filtering, Virtual Private Networks, Network Address Translation and firewall capacity. In packet filtering it focuses on passing or blocking packets at a network based on destination addresses, ports or protocols. Data Security along with a fast technological change is a demanding field. This overview shows that Data Security in itself must be seen as a whole. The adopted network security policy forms the basis.

REFERENCES

1. S.C.Tharaka, R.L.C. Silva, S. Sharmila, S.U.I. Silva, K.L.D.N. Liyanage, A.A.T.K.K. Amarasinghe, D. Dhammearatchi, High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies International Journal of Scientific and Research Publications, Volume 6, Issue 4, April 2016 504 ISSN 2250-3153
2. Suraj J. Warade, Pritish A.Tijare and Swapnil. N. Sawalkar "A Review Data Security in Local Network using Distributed Firewall" [National Conference on Emerging Trends in Computer Technology - 2014]
3. Sotiris Ioannidis, Angelos D. Keromytis, Steve M. Bellovin and Jonathan M. Smith ["Implementing a Distributed Firewall" 2013]
4. Dr.T.Pandikumar, Mekonnen Gidey, DATA SECURITY IN LAN USING DISTRIBUTED FIREWALL International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 04 Issue: 05 | May -2017
5. M .malik and R.pal, (2013),"impact of Firewall and VPN for WLAN", International Journal of Advanced Research in Computer Science and Software Engineering,2.5.(2013)
6. Bhanot, Amit, and Leena jain. "Implementing Network Security Policies: Packet Filtering Mechanism". International Journal of Emerging Trends and Technology in computer Science 2.3 (2013):
7. Ludwig, Christoph. "On The Modeling, Design, And Implementation of Firewall Technology". international journal of emerging trends & technology in computer science 5.4 (1997).