NHSEMH - 2023
2nd National Conference on New Horizons in Science,
Engineering, Management and Humanities
International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

Firewall Protection from Third Party Application

Bhuvan Angiraa, Amit Singh, Avnish Kr. Karn, Ansh Sharma
Department of Information Technology, IIMT College of Engineering Greater Noida, Uttar Pradesh, India

ABSTRACT

Few businesses would choose to operate without a series of locks, alarms and security cameras to protect their premises and inventory from intrusions and theft. Protecting your computer systems is equally important, to prevent malicious users from disrupting your operations or -- even worse -- stealing your private data or intellectual property. One of the key tools used for computer security is a firewall, and few companies can afford to operate without one.A firewall is a vital piece of your business's defence against electronic threats. Serving as a gatekeeper between your company's servers and the outside world, a properly maintained firewall will not only keep external threats out, but it can also alert you to more subtle problems by intercepting outgoing data as well. Paired with a well-maintained anti-malware suite, a firewall can save your business from spending time and money dealing with virus infections or hacker attacks. A firewall is a piece of software that stands between a computer or network and the Internet. Connecting a computer directly to the global network is like leaving your front door open, allowing outsiders free access to your system. Any request will pass through to vulnerable systems, allowing unscrupulous third parties to exploit your computers for their own gain. A firewall serves to block these unauthorized requests, passing through only designated traffic.

Keywords: Firewall, alarms and security, electronics threats, global network

I. INTRODUCTION

Basically, a firewall is a barrier to keep destructive forces away from your property. In fact, that's why it's called a firewall. Its job is similar to a physical firewall that keeps a fire from spreading from one area to the next. Firewall technology emerged in the late 1980s when the Internet was a fairly new technology in terms of its global use and connectivity. A network's firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external network, such as the Internet, that is not assumed to be secure and trusted.A firewall can either be software-based (ex: AVG-Zone Alert- ISA –TMG) orhardware-based (ex: Cisco-JUNIPER) and is used to help keep a networksecure. Its primary objective is to control the incoming and outgoing networktraffic by analyzing the data packets and determining whether it should beallowed through or not, based on a predetermined rule set. Many personal computer operating systems include software-based firewalls toprotect against threats from the public Internet.

Today's networks change and develop on a regular basis to adapt to new businesssituations, such as re-organisations, acquisitions, outsourcing, mergers, joint ventures, and strategic partnerships, and the increasing degree to which internal networks areconnected to the Internet. The increased complexity and openness of the networkthus caused makes the question of security more complicated than hitherto, andnecessitates the development of sophisticated security technologies at the interfacebetween networks of different security domains, such as between Intranet andInternet or Extranet. The best way of ensuring interface security is the use of afirewall.

A Firewall is a computer, router or other communication device that filters access tothe protected network.Cheswick and Bellovin define a firewall as acollection of components or a system that is placed between two networks andpossesses the following properties.

1 All traffic from inside to outside, and vice-versa, must pass through it.

2 Only authorized traffic, as defined by the local security policy, is allowed to passthrough it.

3 The firewall itself is immune to penetration.

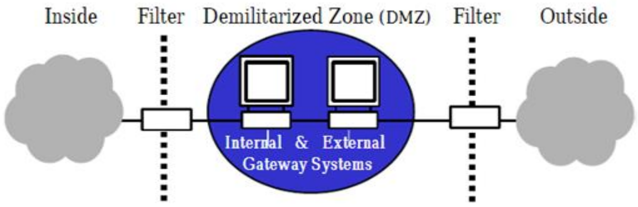


Figure:1 Inside and outside filter Demilitarized

Such traditional network firewalls prevent unauthorised access and attacks byprotecting the points of entry into the network. As Figure 1 shows, a firewall mayconsist of a variety of components including host (called bastion host), router filters(or screens), and services. A gateway is a machine or set of machines that providesrelay services complementing the filters. Another term illustrated in the figure is"demilitarised zone or DMZ". This is an area or sub-network between the insideand outside networks that is partially protected. One or more gateway machines maybe located in the DMZ. Exemplifying a traditional security concept, defence-in-depth, the outside filter protects the gateway from attack, while the inside gatewayguards against the consequences of a compromised gateway. Depending onthe situation of the network concerned, there may be multiple firewalls, multipleinternal networks, VPNs, Extranets and perimeter networks. There may also be avariety of connection types, such as TCP and UDP, audio or video streaming, anddownloading of applets. Different types of firewall configuration with extensivepractical guides can be found in. There are also many firewall products on themarket from different vendors. See for an updated list of products and vendors.

II. BACKGROUND

Firewall technology emerged in the late 1980s when the Internet was a fairlynew technology in terms of its global use and connectivity. A network's firewallbuilds a bridge between an internal network that is assumed to be secure andtrusted, and another network, usually an external network, such as the Internet,that is not assumed to be secure andtrusted.

Significance of the study

A firewall is a security device — computer hardware or software — that can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on your computer. Not only does a firewall block unwanted traffic, it can also help block malicious software from infecting your computer. Firewalls can provide different levels of protection. The key is determining how much protection you need.

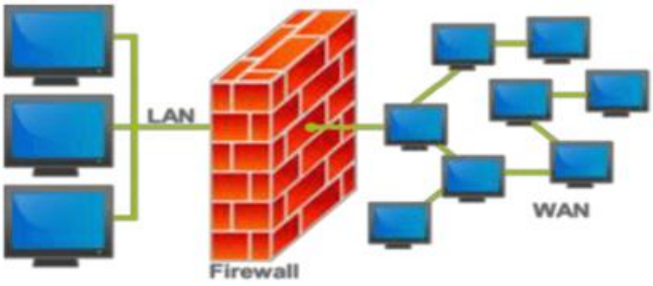


Figure:2 Firewall security network

The topics below can help you learn what firewalls do and determine the level of protection that will help keep your computer and the data on it safe and secure.A firewall acts as a gatekeeper. It monitors attempts to gain access to your operating system and blocks unwanted traffic or unrecognized sources.How does it do this? A firewall acts as a barrier or filter between your computer and another network such as the internet. You could think of a firewall as a traffic controller. It helps to protect your network and information by managing your network traffic. This includes blocking unsolicited incoming network traffic and validating access by assessing network traffic for anything malicious like hackers and malware.

Your operating system and your security software usually come with a pre-installed firewall. It's a good idea to make sure those features are turned on. Also, check your security settings to be sure they are configured to run updates automatically.

Research Methodology

There are certain methods through which firewalls can be implemented. These are as follows: **Static packet filtering –** Packet filtering is a firewall technique used to control access on the basis of source IP address, destination IP address, source port number, and destination port number. It works on layers 3 and 4 of the OSI model. Also, an ACL doesn't maintain the state of the session. A router with ACL applied to it is an example of static packet filtering.

Advantages :

1. If the administrator has a good knowledge of the network, it is easy to implement.
2. It can be configured on almost all routers.
3. It has minimal effect on network performance.
4. The large amount of ACLs is difficult to maintain.
5. ACLs use the IP address for filtering. If someone spoofs the same source IP address then that will be allowed by ACL.

Stateful packet filtering

In stateful packet filtering, the state of the sessions is maintained i.e. when a session is initiated within a trusted network, it's the source and destination IP address, source, and destination ports, and other layer information are recorded. By default, all the traffic from an untrusted network is denied.

The replies of this session will be allowed only when the IP addresses (source and destination IP address) and port numbers (source and destination) are swapped.

Advantages

1. Dynamic in nature as compared to static packet filtering.
2. Not susceptible to IP spoofing.
3. Can be implemented on routers.
4. Might not be able to prevent application-layer attacks.
5. Some applications open dynamic ports on the server-side, if the firewall is analyzing this, it can cause application failure. This is where application inspection comes into use.

Proxy firewalls

These are also known as application-layer firewalls. A proxy firewall acts as an intermediary between the original client and the server. No direct connection takes place between the original client and the server.

The client, who has to establish a connection directly to the server to communicate with it, now has to establish a connection with the proxy server. The proxy server then establishes a connection with the server on the behalf of the client. Now, the client sends the data to the proxy server and the proxy server forwards it to the server. A proxy server can operate up to layer 7 (application layer).

Advantage

- Difficult to attack a server as a proxy server is an intermediate between the client and the server.

- Can provide detailed logging.
- Can be implemented on common hardware.
- Processor intensive
- Memory and disk intensive
- Single point of failure in network security

Application inspection –

These can analyze the packet up to layer 7 (deep inspection) but can't act as a proxy server. These can deeply analyze conversations between a client and server even when the server is assigning a dynamic port to the client therefore it doesn't fail in these cases (which can occur in a stateful firewall).

Advantages

- Can analyze deeper into the conversation between the server and the client.
- If there is a protocol anomaly happening from standard then it can deny the packets.

Transparent firewall

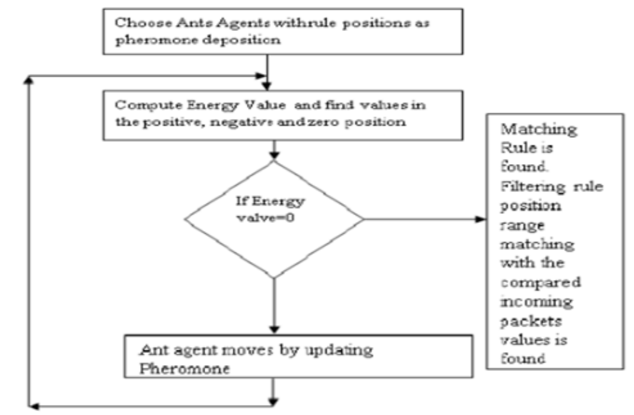
By default, the firewall operates at layer 3 but the benefit of using a transparent firewall is that it can operate at layer 2. It has 2 interfaces that will act as a bridge so can be configured through a single management IP address. Also, users accessing the network will not even know that a firewall exists.

The main advantage of using a transparent firewall is that we don't need to re-address our networks while putting up a firewall in our network. Also, while operating at layer 2, it can still perform functions like building a stateful database, application inspection, etc.

III. SAMPLING TECHNIQUE

Ant Colony Optimization (APO) technique for filtering theincoming packets in a network by matching the rules inrule set. The matching rule picked up from the rule set isdetermined by the ant agent. The attractiveness of the antagent is denoted by its energy value.

The following figureshows the model of the Ant system


Choose Ants Agents withrule positions as pheromone deposition
Compute Energy Value and find values in the positive, negative and zero position
If Energy valve=0
Matching Rule is found. Filtering rule position range matching with the compared incoming packets values is found
Ant agent moves by updating Pheromone

The fields in the IP header of the incoming packet arecompared for match with the filtering rules in detectionunit. Initial sets of ants have pheromone depositionrepresenting the positions of filtering rule in the rule set.The comparison field of the rule denoted by thepheromone deposition of the ant agent is compared withthe corresponding field of the incoming packet. This antsystem with the help of pheromone deposition and tabu-listbrings in a solution.

Ant Colony Optimization PacketFiltering Algorithm (ACO-PF) filters the packet accordingto filtering rules in the rule set. The ant agent deposits thepheromone and searches for a rule in the rule set. Thepheromone deposition is a number denoting the position ofthe filtering rule in the rule set to be compared withincoming packet field value. The strength of attractivenessof the ant agent towards the solution is denoted by itsenergy value.

If the comparison field value of the filteringrule in the rule set is less than the value of the incomingpacket field, +1 is assigned as the energy value of the antagent and pheromone deposition of the ant agent is storedin the positive position of the tabu-list. The energy value is-1 if the comparison field value is greater than theincoming packet value and the pheromone deposition ofthe ant agent is stored in the negative position of the tabulist . The energy value is zero if both the fields are equaland pheromone deposition of the ant agent is stored in thezero position of the tabu-list. Below shows themathematical equation in finding the energy values:If Ai is the ant agent and C(Fij) be the comparison fieldvalue of the jth filtering rule in the rule set of the ith antagent.

i=1, 2 ,…… no of ant agents.

j=1, 2, …… total no. of filtering rules

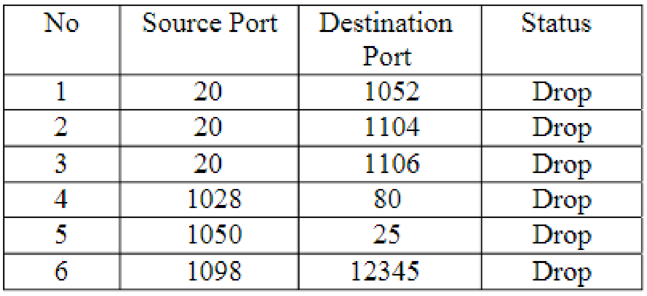
C(P) denotes the incoming packet value

The energy value is computed as follows:-Energy (Ai) = +1, C(P) > C(Fij) Positive position = j ,Energy (Ai) = 0, C(P) = C(Fij) Zero position = j

Energy (Ai) = -1, C(P) < C(Fij) Negative position = j

The paper has discussed two case studies. Case study 1 isdiscussed for real example where rules are defined in arule set for a network address detection unit. The numericequivalent of the network address is stored in the rule set.

Filtering rules in the rule set behaves in such a way that theincoming packets from the network address and thedestination port is only accepted. Case study 2 is discussedfor multidimensional filters where the packets from agiven source address and source port is rejected except foronly one destination address and destination port.



No	Source Port	Destination Port	Status
1	20	1052	Drop
2	20	1104	Drop
3	20	1106	Drop
4	1028	80	Drop
5	1050	25	Drop
6	1098	12345	Drop

Table 1 above shows the filtering rules in the rule set in asource port detection unit to either accept or drop theincoming packets based on source port of destination port.

The computational complexity of the system is derived asin n where n is the number of filtering rule in the rule set.

IV. TOOLS AND TECHNIQUES

Now we have chosen the building blocks of our firewall system. Now the time has come to configure the security rules onto a network system.Command-line interface (CLI) and graphic user interface (GUI) are used to configure firewall software. **For Example**, Cisco products support both kinds of configuration methods. Nowadays in most networks, the Security device manager (SDM) which is also a product of Cisco is used to configure routers, Firewalls, and VPN attributes. To implement a firewall system an efficient administration is very essential to run the process smoothly. The people managing the security system must be masters in their work as there is no scope for human error.

Any type of configuration errors should be avoided. Whenever configuration updates will be done, the administrator must examine and double-check the whole process so that leaving no scope for loopholes and hackers to attack it. The administrator should use a software tool to examine the alterations done.

Any major configuration changes in firewall systems can’t be directly applied to the ongoing big networks as if failed can lead to a big loss to the network and directly allowing unwanted traffic to enter the system. Thus firstly it should be performed in the lab and examine the outcomes if the results are found ok then we can implement the changes in the live network.

V. CONCLUSION

A firewall is a crucial component of securing your network and is designed to address the issues of data integrity or traffic authentication (via stateful packet inspection) and confidentiality of your internal network (via NAT). Your network gains these benefits from a firewall by receiving all transmitted traffic through the firewall. Your network gains these benefits from a firewall by receiving all transmitted traffic through the firewall. The importance of including a firewall in your security strategy is apparent; however, firewalls do have the few limitations like wise A firewall cannot prevent users or attackers with modems from dialing in to or out of the internal network, thus bypassing the firewall and its protection completely. Firewalls cannot enforce your password policy or prevent misuse of passwords. Your password policy is crucial in this area because it outlines acceptable conduct and sets the ramifications of noncompliance.

VI. REFERENCES

[1]. Oppliger, Rolf (May 1997). "Internet Security: FIREWALLS andBEYOND". Communications of the ACM 40 (5): 94.

[2]. http://www.wanredundancy.org/resources/firewall/network-layer-firewallNetwork Layer Firewall

[3]. Firewall http://www.tech-faq.com/firewall.html

[4]. http://en.wikipedia.org/wiki/Firewall_%28computing%29

[5]. Check Point Firewall-1, version 3.0 White Paper, June 1997.http://www.checkpoint.com/products/whitepapers/wp30.pdf

[6]. W. R. Cheswick and S. M. Bellovin, Firewalls and Internet Security,Repelling the Wily Hacker, Addison-Wesley Publishing Company, 1994

[7]. G. Dalton, Acceptable Risks, a survey by PricewaterhouseCoopers andInformationWeek, August 31, 1998,

[8]. http://www.informationweek.com/698/98iursk.htm

[9]. FORE Systems, Firewall Switching Agent White Paper, October 1998.

[10].C. Fulmer, Firewall Product Overview, December 30, 1999,http://www.waterw.com/~manowar/vendor.html

[11].ICSA, ICSA Firewall Policy Guide V2.00, Security White Paper series,http://www.icsa.net/services/consortia/firewalls/fwpg.shtml

[12].T. Moran, Fight Fire with Firewalls, Microsoft Corporation, July 27, 1998,

[13].http://msdn.microsoft.com/workshop/server/proxy/server072798.asp

[14].D. Newman, Super Firewalls, Data Communications, Lab Tests, May 21,1999, http://www.data.com/

[15].OMG, Joint Revised Submission, CORBA/Firewall Security+Errata, OMGDocument, ftp://ftp.omg.org/pub/docs/orbos/98-07-03.pdf, July 6, 1998

[16].OMG, The CORBA Security Service Specification (Revision 1.2),ftp://ftp.omg.org/pub/docs/ptc/98-01-02.pdf, January 1998.

[17].OMG, The Object Management Group, http://www.omg.org/

[18].J. L. Phipps, Hackers: Can You Stop Them?, PricewaterhouseCoopers and

[19].Information Week,http://www.mediainfo.com:81/ephome/news/newshtm/minfocom/1198a.htm