ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 5, Issue 2 (Apr. - Jun. 2017)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2017)

Intelligent Firewall Using Genetic Algorithm

[I]Mazin H. R. Al- Shaikhly, [II]Hazem. M. El bakry, [III]Ahmed A. Saleh
[I]Baghdad College of Economic Sciences University, Baghdad, IRAQ
[II,III]Dept. of Information System, Faculty of Computer and Information Sciences,
Mansoura University, Mansoura, Egypt

Abstract
This research work focuses on one specific mechanical part of giving correspondences security, firewall innovation. The firewall innovation is a particular building arrangement as opposed to an experimentally based arrangement without intelligence engine. The presented work adds genetic feature to the process of firewall with intelligent, main engine of processing depending on the number of IP that may throughput more than maximum value (that is allocated by admin), then creates threat history table for any transactions IP. After that it compares if current I/O in table (with low threat or it is not in threat list) and value is located in range then pass, otherwise IP is blocked automatically. Visual basic (vB) is used to build the system.

Key words
Firewall, Genetic Algorithm. Security Function

I. Introduction

Firewall can be defined as one technique to improve security for local network, when intelligent feature is added to any machine may be able to make decision related to the engine the system is added to thus firewall with genetic may be able to eliminate outside intrusion to local network. Many researchers have dealt with firewall technology. This research selected two thesis [1,2] as start state to build simulate system,

Section 2 shows firewall essentiality, section 3 gives meaning of security function and adaptive security function design. Section 4 presents the experiment test results covers finally section 5 conclusion.

II. Firewall Essentiality

A firewall is a safe Internet entryway that is utilized to interconnect a private system to the Internet (see Figure 1). There are various parts that make up a firewall:[3.4,7,9]

i) The Internet get to security arrangement of the association. This states, at an abnormal state, what level of security the association anticipates that when interfacing will the Internet. The security approach is autonomous of innovation and strategies, and ought to have a lifetime free of the gear utilized. A case of explanations from such a security strategy may be: outside clients won't be permitted to get to the corporate system without a solid level of confirmation

ii) Any corporate information not in individuals when all is said in done space must be traded a cross the Internet privacy, and corporate customers might be allowed to send electronic mail to the Internet - each other organization will be banned.

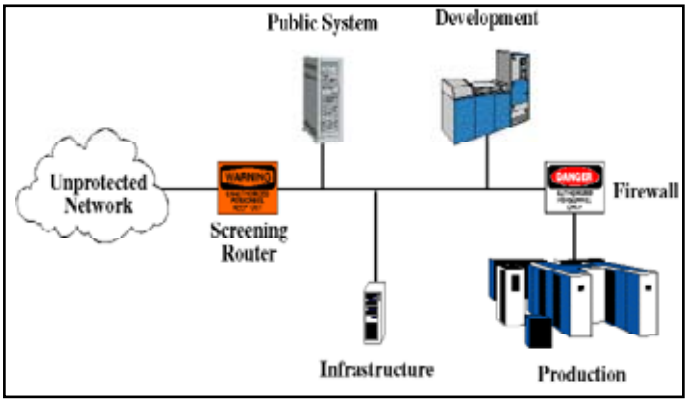

Fig. 1: Environment and firewall

iii) The mapping of the security arrangement onto specialized outlines and systems that are to be taken after when associating with the Internet. This data will be redesigned as new innovation is declared, and as framework arrangements change and so on. For instance, in regards to verification, the specialized plan may determine the utilization of one-time passwords. Specialized outlines are normally in view of one of two security strategies, either:[2,3,4] allow any administration unless it is explicitly denied, or deny any administration unless it is explicitly allowed. The last is unmistakably the more secure of the two.

iv) The firewall framework, which is the equipment and programming, actualizes the firewall. Run of the mill firewall frameworks contain an IP bundle sifting switch, and a host PC (in some cases called a bastion host or application entryway) running application separating and validation software[1,3,4,7].

each of these firewall parts is basic. A firewall framework without an Internet get to security approach can't be accurately arranged. An approach without implemented systems is useless as it is overlooked.

1. Firewall advantage and disadvantage

As the past segments appear, firewalls can secure sent processing frameworks and organized applications. Defenders contend that firewall innovation is more than are benefit fix for inadequacies in frameworks and convention plan (a study led by the National Computer Security Association (NCSA) records the positive encounters and view of a little arrangement of American organizations [2,3,5]. In view of their situation at the system edge, firewalls can serve as a brought together concentration of security strategy and as a place to gather thorough security reviews, even within the sight of secure hosts [15-26]. Firewalls address a few issues of system security that can't be tended to by host security instruments: they ensure the system as an asset and the hosts associated with it and give assurance against some refusal of administration assaults [2,4].

The conglomeration of security capacities in firewalls takes into consideration a disentanglement of administration, establishment, and setup of security capacities [6]. They enhance authoritative control and system administration by means of controlled presentation of interior system structure, topological adaptability, and straightforwardness to the client [6]. Security firewalls speak to

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

an innovation that is broadly acknowledged, accessible, financially savvy, and monetarily reasonable to administration work force accountable for buying choices [3].
At last, they can quit approaching solicitations to inalienably shaky administrations, e.g. you can forbid re-login, or RPC (Remote Procedure Call) administrations, for example, NFS (organize record framework).
They can control access to different administrations e.g. ban guests from certain IP addresses, channel the administration operations (both approaching and active), e.g. stop FTP composes shroud data e.g. by just permitting access to specific registries or Systems. They are more practical than securing every host on the corporate system since there are regularly just a single or a couple firewall frameworks to focus on. They are more secure than securing every host because of: the multifaceted nature of the product on the host - this makes it less demanding for security escape clauses to show up. Interestingly, firewalls as a rule have streamlined working frameworks and don't run complex application programming, the quantity of hosts that should be secured (the security of the entire is just as solid as the weakest connection).
Presently the greatest impediment of a firewall is that it gives no assurance against within assault, firewall innovation can give a misguided sensation that all is well and good.
It might prompt to careless security inside the firewall edge [7]. like the way the as far as anyone knows secure Maginot Line1 drove French armed force pioneers to disregard the requirement for arrangement of extra protection systems promote inside their nation [3]. In [6] this worry is communicated through another similarity: firewalls give "a hard, crunchy outside with a delicate chewy focus." Security firewalls neither give "consummate security" nor are free of operational challenges. They don't ensure against noxious insiders. There is no insurance against associations that evade the firewall, for example, unapproved modems joined to PCs inside the firewall on the grounds that the upholding component is by passed. There is restricted insurance against illegal meet (unapproved burrowed associations) and information driven assaults, for example, vindictive executable code in downloaded Java applets [5]. Since regular practice does not give a check of firewall framework arrangement against the security strategy, changes in framework designs may deliver security openings [4] Firewall innovation has been created for and connected to TCP/IP organizes solely [6]. It was never created by reference display and just tended to intense issues nearby. In view of the receptive character of firewall configuration, there is little motivation to expect that successful insurance against new assaults is ensured. An impetus for advances in the cutting edge of firewall innovation has been the need to create safeguards against assault situations that have at first prevailing through or against firewalls.

2. Firewall and network model

Figure 2 recognizes network reference models, and which firewall is suitable for each [3].

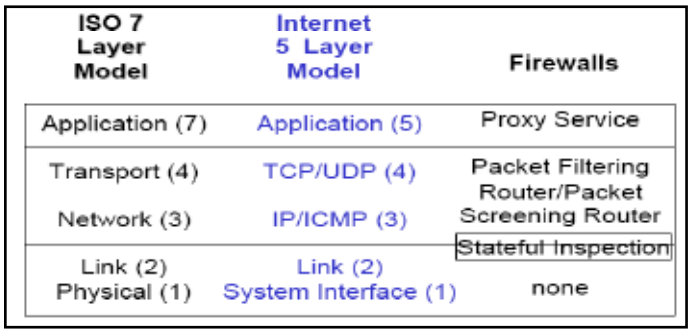

Fig. 2: Firewall types

OSI 7 = ISO 7 Open System Interconnection with 7 layers

In addition, security level can be described as shown in Fig.3:

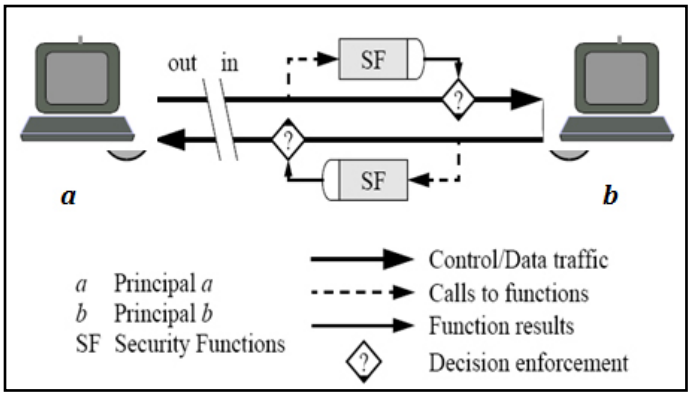

Fig. 3: Security level

Additionally, security work delineated in figure 3, considers the situation where a central an outside of an ensured arrange approach area endeavors to speak with a foremost b inside that domain. (Figure 4 outlining Performance/security scale)

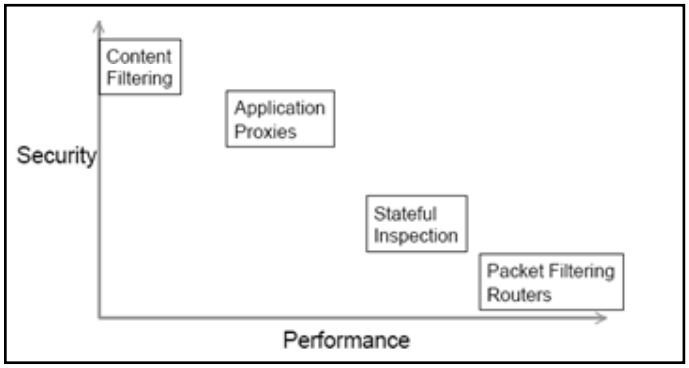

Fig. 4: Security performance

The crevice amongst "out" and "in" can be loaded with middle of the road systems of any innovation and topology insofar as information can be transmitted between the sender's and the recipient's systems. Everything between the hole and the representation of primary b is considered part of the ensured arrange approach area [5,8].

III. Security Function (SF) and Adaptive SF using genetic algorithm

As specified in area 2 and represented in Figure 3, the reference show comprises of the accompanying security work (SF) parts: Authentication Function (AF), Integrity Function (IF), Access

(affirmation) Control Function (ACF), Audit Function (AudF), and Access Enforcement Function (AEF). Also, all are utilized to recognize interruption and reject it [5].
The SF is utilized as a part of Network Intrusion Detection .The objective of interruption recognition is to distinguish substances endeavoring to subvert set up security controls.
One sort of assault is Denial of Service (DoS) Attack Imagine that a gatecrasher needed to make a phone framework unusable by phone clients. How might be do this? One way is make call after bring trying to make all circuits occupied. This kind of assault is known as a refusal of administration or DoS attack.[10,11,12] to identification require a versatile calculation consequently SF content one of shrewd apparatuses, for example, hereditary calculation.
Genetic algorithm GA is a group of computational models in view of standards of development and common determination; it utilizes an arrangement of versatile procedures that copy the idea of "survival of the fittest." [12,13,14]. While system is dynamic then movement must exist, the activity information is then utilized by the GA for the production of an arrangement of tenets for an Intrusion Prevention Rule based framework. Interruption counteractive action takes after a similar procedure of social affair and identifying information and conduct, with the additional capacity to piece or keep the action, Algorithm gives overview the proposal engine.

Algorithm 1

1- initial population from real log
2- convert all IP list to binary with 32bit
3- start with genetic and calculate fitness
   3-1 calculates fitness (time- source- distension / redundant)
   3-2 select 32 x 2 bit relate with source
   3-3 crossover - mid
   3-4 mutation – two bit
   3-5 check fitness
4- Update IP list depending on fitness value
5- Goto 2

Algorithm 1 Proposal engine

A. Firewall log record and genetic chromosome

This section gives overview of all term existing in firewall record and **yes** marks all terms needed proposal design as shown in table 1

Table 1 : Firewall record terms

Term	Needed in activities	
Time	Yes	4 bit
Action Firewall	-----	
Interface	--------	
Product	--------l	
Source	Yes	32 bit
Source Port	--------	
Destination	Yes	32 bit
Service	------	
Protocol	TCP	
Translation	------	
Byte send	Yes	Depend on

B. Converting log to genetic chromosome

To convert firewall record as chromosome in general must select one or more terms so as clear in section 4.1 and table 2 give example of converting value.

Table 2 : Convert example

Term	Needed activity	As record	Binary value
Time	Yes	12:00	1100
Source	Yes	148:22:118:80	10010100000101100111011001010000
Destination	Yes	126:15:106:73	01111110000011110110101001001001
Protocol	TCP		
Byte send	Yes	4 bit	

- Within a manage based framework, the tenets put away in the govern base are generally in the accompanying structure: if <condition> then <action>

As is clear in algorithm 1 in our case:
- on the off chance that {the association has taking after data: source IP is 209.11.1.155; goal IP address: 109.1.1.17 ~ 109.1.1.21; goal

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

port number: 8184; the convention utilized is FTP; the originator sent more than 10,000 bytes of information; and the responder sent more than 250,000 bytes of data } **then** {stop the connection}

1. Cross over and mutation

This section gives an overview of genetic operation crossover and mutation as follows:

```
Algorithm 2
 rem using IP length =32bit (binary convert)= chromosome-4bit

      1- L=32 div 2:i=0
         'Select any two chromosomes from population
      2- X=[random(pop_size)]:Y=[random(pop_size)]
      3- Read IP[x],IP[Y]
      4- Loop
            T=IP[X][1+i]
            IP[X][1+i]=IP[Y][16+i]
            IP[Y][16+i]=T
            i=i+1
         UNTIL i=L-1
      5- END
```

Algorithm 2 Genetic crossover

```
Algorithm 3
 rem using IP length =32bit (binary convert)= chromosome-4bit
 rem Invert_value is function change 0 to 1 or  1 to 0
 rem chooses two bit in same chromosome for mutation action

      1- X=[random(32)]: Y=[random(32)]
      2- Invert_value(IP[current][X])
      3- Invert_value(IP[current][Y])
      4- END
```

Algorithm 3 genetic mutation

2. Fitness Function

The goal is to avoid intrusion to network from any out-said attack as shown in algorithm 4 below:

```
Algorithm 4
 rem using IP length =32bit (binary convert)= chromosome-4bit
                       Chromosome 36 bit  thus - 4 bit
 rem fitness 20-1 refers to  max value (block IP)

        1-loop
          • check I/O port per time
          • if IP[current] throughput > max_value then
                Fitness[current]++
        2- until I/O port off
```

Algorithm 4 Fitness function

IV. Experimental results

Running of simulated firewall system with genetic feature (in traffic mode) saves the following value from system with fitness, following chart gives sample fragment view ,where

X axis = 1..145 sequence of IP
and Y axis =1..20 fitness value (threat degree)

if fitness value [current IP] = 19 "20-1" (max threat) ***then*** block IP[current],
Where current= current I/O value
Figure 5, The table 4.1 result detail (IP address, 32 bit value for IP and fitness).

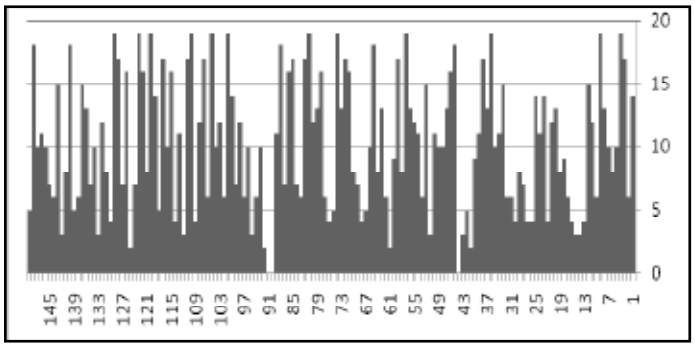

Fig. 5: Chart fragment view for result

Table 4-1: some results Fitness value of IP address for (148 ip address tested)

IP address	IP Binary value 32 Bit	Fitness value
64:25:95:91	01000000000110010101111101011011	14
174:16:74:104	10101110000100000100101001101000	6
148:22:118:80	10010100000101100111011001010000	17
78:28:124:68	01001110000111000111110001000100	19
191:31:87:94	10111111000111110101011101011110	10
68:27:96:106	01000100000110110110000001101010	8
53:24:40:77	00110101000110000010100001001101	10
90:33:36:94	01011010001000010010010001011110	13
126:15:106:73	01111110000011110110101001001001	19
89:21:67:76	01011001000101010100001101001100	6
135:28:61:89	10000111000111000011110101011001	12
195:32:59:103	11000011001000000011101101100111	15
106:26:84:84	01101010000110100101010001010100	4
192:18:93:95	11000000000100100101110101011111	3
143:29:113:80	10001111000111010111000101010000	3
120:25:40:79	01111000000110010010100001001111	4
67:20:134:91	01000011000101001000011001011011	6
108:23:41:82	01101100000101110010100101010010	9
188:20:52:85	10111100000101000011010001010101	8
122:22:60:59	01111010000101100011110000111011	13
100:25:123:80	01100100000110010111101101010000	12
55:16:118:114	00110111000100000111011001110010	2
144:33:47:78	10010000001000010010111101001110	10
181:18:117:94	10110101000100100111010101011110	6
IP address	**IP Binary value 32 Bit**	**Fitness value**
52:32:84:95	00110100001000000101010001011111	3
47:33:55:108	00101111001000010011011101101100	10
70:20:110:106	01000110000101000110111001101010	6
97:31:120:79	01100001000111110111100001001111	12
73:32:60:56	01001001001000000011110000111000	7
136:22:99:99	10001000000101100110001101100011	14
73:16:59:66	01001001000100000011101101000010	19
71:27:125:71	01000111000110110111110101000111	6
162:29:73:64	10100010000111010100100101000000	12
63:20:120:95	00111111000101000111100001011111	10

131:19:36:70	10000011000100110010010001000110	19
53:31:43:98	00110101000111110010101101100010	6
183:16:94:84	10110111000100000101111001010100	17
112:30:117:59	01110000000111100111010100111011	12
122:30:78:113	01111010000111100100111001110001	4
147:28:108:84	10010011000111000110110001010100	19
174:18:101:71	10101110000100100110010101000111	17
156:22:44:92	10011100000101100010110001011100	3
147:20:43:92	10010011000101000010101101011100	11
133:30:128:67	10000101000111101000000001000011	4
153:30:67:105	10011001000111100100001101101001	16

V. Conclusion

In this paper, the obtained simulation results have given good indication (test with simulated environment of real world). It can be easily concluded that while traffic increases, attaching attack becomes easier. Furthermore, any change in fitness gives a new feature to system (the current fitness may be better).

References

[1] *InSeon Yoo, "An Intelligent Firewall to Detect Novel Attacks", University of Southampton, UK, 2001.*

[2] *Ryan Joseph ,"Parallel Firewall Designs for High-Speed Networks", Wake Forest University, MSC thesis ,2005.*

[3] *Dr.Mashow, "Intelligent Firewall Technology", Carnegie Mellon University, NIC, 2001.*

[4] *M. Leech, M. Ganis, Y. ee, R. Kuris, D. Koblas & L. Jones," SOCKS Protocol Version 5." RFC 1928, April 1996.*

[5] *Simon, Eliabatb, "building internet firewall",o'relly,2001.*

[6] *N.C. S. A. NCSA, "Firewall User Profile", An NCSA Focus Report. Carlisle, Pennsylvania, 1997.*

[7] *CA,"Continued Threat of the Code Red Worm", Cert 2002. http://www.cert.org/advisories/CA-001-23.html*

[8] *http://www.snort.org/*

[9] *M.Abadi, M .Burrows ,B .W. Lampson, and G.Plotkin, "A Calculus for Access Control in Distributed Systems", Technical Report DEC/SRC- 070, Digital Equipment Corporation (DEC), Feb. 1991.*

[10] *A. Tallberg, "The Property of Audit Trail", Technical Report C: 252, Swedish School of Economics and Business Administration, 1992. http:// www.nan.shh.fi/NAN/Papers/ AUTR92/autrtoc.htm/*

[11] *Berge,Matthew."Intrusion Detection FAQ: What is Intrusion Detection?", From http:// www. sans.org/resources/ idfaq/ what_ is_ id. php. Retrieved/*

[12] *CERT.From http://www.cert. org/ tech_tips/ denial_ of_ service. html. Retrieved 10- 3- 2008.*

[13] *Meffert, Klausetal.:JGAP – Java Genetic*

[14] *RL: http:// jgap. sf. Net/ (Algorithms and Genetic Programming Package)*

[15] M*unaf Hamza Kareem, Hazem M. El-Bakry, Mervat Abu-Elkheir "Enhancing Hybrid Asymmetric-Multicast Hash-Routing for Information Centric Networks," International Journal* of Artificial Intelligence and Mechatronics, *vol. 7, issue 2, September 2016, pp. 5-11.*

[16] *Hazem M. El-Bakry, and Nikos Mastorakis, "A Perfect QoS Routing Algorithm for Finding the Best Path for Dynamic Networks," WSEAS Transactions on Communications, Issue 12, vol. 7, December 2008, pp. 1123-1136.*

[17] *Hazem M. El-Bakry, and Nikos Mastorakis, "A Real-Time Intrusion Detection Algorithm for Network Security," WSEAS Transactions on Communications*, Issue 12, vol. 7, December 2008, pp. 1222-1234.

[18] *Hazem M. El-Bakry, Alaa M. Riad, Mervat M. Fahmy, and Nikos Mastorakis "Fast Intrusion Detection by using High Speed Focused Time Delay Neural Networks, " Proc. of WSEAS International Conference on Communication and Information, Athens, Greece, December 29-31, 2009, pp.278-295.*

[19] *Hazem M. El-Bakry, and Nikos Mastorakis, "Fast Packet Detection by using High Speed Time Delay Neural Networks," Proc. of the 10th WSEAS Int. Conference on MULTIMEDIA SYSTEMS & SIGNAL PROCESSING, Hangzhou University, China, April 11-13, 2010, pp. 222-227.*

[20] *Hazem M. El-Bakry, and Mamoon H. Mamoon, "A New Efficient Fast Routing Protocol for MANET," Proc. of Int. Conf. on Applied Informatics and Communications (AIC'10), Taipei, Taiwan, August 20-22, 2010, pp. 443-451.*

[21] *Hassan H. Soliman, Hazem M. El-Bakry and, Mona Reda, "Studying the Performance of Transmitting Video Streaming over Computer Networks in Real Time," International Journal of Computer Science and Information Security*, vol. 9, no. 11, November, 2011, pp. 90-100.

[22] *H. H. Soliman, Hazem M. El-Bakry and, Mona Reda, "REAL-TIME TRANSMISSION OF VIDEO STREAMING OVER COMPUTER NETWORKS," Mansoura Journal for Computer Science and Information Systems, vol. 6, no. 1, Jan 2012, pp. 7-16.*

[23] *Hassan H. Soliman, Hazem M. El-Bakry, and Mona Reda, " Real-Time Transmission of Video Streaming over Computer Networks," Proc. of 11th WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communications (EHAC '12), Cambridge, UK, Feb. 22-27, 2012, pp 51-62.*

[24] *Alaa Eissa, Hazem M. El Bakry, Mamoun H. Mamoun, and Samir Zied, "Intrusion Detection In Wireless Sensor Networks: A survey," International Journal of Information Science and Intelligent System, vol. 3, No. 4, October 2014, pp. 87-111*

[25] *Alaa Eissa, Hazem M. El Bakry, and Samir Ziad, "A Hybrid Intrusion Detection System for WSN," International Journal of Advanced Research in Computer Science & Technology, vol. 3, issue 4, October-December 2015, pp. 10-15.*

[26] *Abdelrahman M. Ahmed, Hazem M. El Bakry, "A New Technique for Optimal Data Manipulation Through WANs," International Journal of Advanced Research in Computer Science & Technology, vol. 4, issue 1, April-June 2016, pp. 177-180.*