

Building New Generation Firewall Including Artificial Intelligence

Partha Chakraborty
Dept. of Computer Science & Engineering
Comilla University
Comilla - 3506, Bangladesh

Md. Zahidur Rahman
Dept. of Computer Science & Engineering
Comilla University
Comilla - 3506, Bangladesh

Saifur Rahman
Dept. of Computer Science & Engg
Comilla University
Comilla - 3506, Bangladesh

ABSTRACT

The expanding complexity of networks and the need to make them increasingly open due to the growing emphasis on and attractiveness of the Internet as a mode for business transactions, imply that networks are exposed to increasingly more attacks, both from without and from within. One of the protective mechanisms under serious consideration is the firewall which protects a network by guarding the points of entry to it. Constantly including of new features make Firewalls becoming more sophisticated day by day; so that, in spite of the criticisms made of them and developmental trends threatening them, they are still a powerful protective mechanism. Basically, Firewall sets accept or deny action for packets by default. In this paper, researchers proposed to add Artificial Intelligence with firewall which in turn make firewall capable of exploiting traffic behavior by utilizing incoming traffic and dynamically creating some rules with itself for some exceptional packets; So no default actions need to be used.

General Terms

Firewall, Artificial Intelligence

Keywords

Firewall, Artificial Intelligence, Generation, Network

1. INTRODUCTION

Today's networks change and develop on a regular basis to adapt to new business situations, such as reorganisations, acquisitions, outsourcing, mergers, joint ventures, and strategic partnerships and the increasing degree to which internal networks are connected to the Internet. The increased complexity and openness of the network thus caused makes the question of security more complicated than hitherto and necessitates the development of sophisticated security technologies at the interface between networks of different security domains, such as between Intranet and Internet or Extranet. The best way of ensuring interface security is the use of a firewall. A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented as both hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the

Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. A Firewall can also be called a computer, router or other communication device that filters access to the protected network .

2. LITERATURE REVIEW

In 1988, Douglas Comer published the book "Internetworking with TCP/IP: principles, protocols, and architecture"; where author described the fundamental concepts of client-server computing used to build all distributed computing systems and proposed an in-depth guide to the Posix sockets standard utilized by Linux and other operating systems[1]. D. B. Chapman and E. D. Zwicky researched on Building Internet Firewalls and published O'Reilly and Associates, Inc. in November 1995 [2]. In 1996, Chris Hare and Karanjit Sijan published the book "Internet Firewalls and Network Security"[3]. In 1997, Micki Krause and Harold F. Tipton published "Handbook of Information Security Management", CRC Press LLC, (electronic edition) [4]. In 2011, Larry L. Peterson and Bruce S. Davie published the 5th edition of their book "Computer networks a systems approach 5th ed" where they explore the key principles of computer networking[5]. H. Abie, CORBA published "Firewall Security: Increasing the Security of CORBA Applications" in January 2000 [6].

In 2013, Kristian Valentin and Michal Maly modeled a firewall using an artificial neural network, more specifically using a multi-layer perceptron (MLP) trained by the back-propagation algorithm [7]. In 2014, "Information Security Newsletter" published by the JUCC IS Task Force [8]. In 2016, Nainesh V. Patel, Narendra M. Patel and Costas Kleopa focused to model firewall based on the open source technology advancement in application identification [9]. In 2017, S. Arunkumar et al., reviews the existing firewall policies and assesses their application in highly dynamic networks such as coalitions networks; also describe the need for the next-generation firewall policies[10].

2.1 Contribution of Researchers in this Work

Here, researchers have extended the features of state-full firewall (a type of firewall). Where a basic firewall sets accept or deny action for packets by default, the proposed firewall will not do that. Instead of direct deny, It will apply Artificial Intelligence with firewall. Because of that, it can make some rules with itself for

some exceptional packets. This feature will make firewall more reliable and stop wasting trusted packet.

3. METHODOLOGY

3.1 Firewall Configuration

Firewalls are adjustable. This implies that anyone can add or remove filters based a few conditions. Some of these are:

IP addresses - Each machine on the Internet is allocated a novel address called an IP address. IP addresses are 32-bit numbers. An average IP address resembles this: 216.27.61.137. For instance, if a specific IP address outside the organization is reading excessive number of files from a server, the firewall can obstruct all traffic to or from that IP address.

Domain names - Since it is difficult to recall the string of numbers that make up an IP address, and because IP addresses again need to change, all servers on the Internet additionally have human-readable names, called domain names. For instance, it is simpler for the vast majority of us to recall www.studytonight.com than it is to remember 216.27.61.137. An organization might block all entrance to certain domain names, or allow access only to explicit domain names.

Protocols - The protocol is the pre-defined way that somebody who needs to utilize a service talks with that service. The "somebody" could be an individual, but more often it is a computer program like a Web browser. Some common protocols that researchers can set firewall filters for include:

IP - the principle delivery system for information over the Internet
TCP - utilized to break apart and modify information that travels over the Internet

HTTP - utilized for Web pages

FTP - utilized to upload and download files

UDP - utilized for data that requires no response, for example, streaming audio and video

ICMP - utilized by a router to trade the information with other routers

SMTP - utilized to send text-based information (e-mail)

SNMP - utilized to collect system information from a remote computer

Telnet - utilized to perform commands on a remote computer

A company may set up just a couple of machines to deal with a particular protocol and ban that protocol on all other machines.

Ports - Any server machine makes its services available to the Internet utilizing numbered ports, one for each service that is available on the server.

3.2 The basic operations of a firewall

The basic operations of a firewall is depicted in fig 1.

(a) Host A is an Apple Macbook Pro that opens a web browser and wants to view a web page from the www.avoidwork.com web server. This action causes Host A to send the request to view this web page out through the firewall across the Internet and to the web server.

(b) The firewall sees the request originated with Host A and is destined for www.avoidwork.com.

(1) The firewall records (tracks) the outbound request and expects that the reply will come only from the www.avoidwork.com web server.

(2) A session marker is placed in the firewall's session state table that tracks the communication process from start to finish.

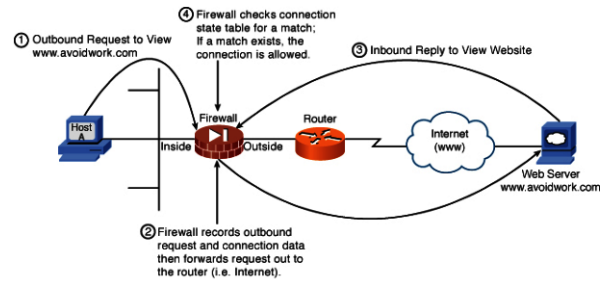


Fig. 1. Basic operations

(3) Connection metrics, such as time opened and so forth, are also placed with the marker in the session state table record maintained by the firewall for this conversation.

(c) The Avoidwork.com web server replies to the web page request from Host A, which is then transmitted back through the Internet and to the firewall.

(d) The firewall checks its session state table to see whether the metrics being maintained for this session match the outbound connection. If all the stored connection details match exactly, the firewall enables the inbound traffic.

3.3 Structure of law

This is a simple record that hold information associated with a specific law. The law contains the IP addresses of the source and destination that are to be matched against. Port numbers further supplement the information contained in the law (fig 2)

| Field | Description |
|-------------|--|
| Source IP | Source IP address that will match the law |
| Dest IP | Destination IP address that will match the law |
| Source Port | Source port that will match the law |
| Dest Port | Destination port that will match the law |
| Src Mask | A Flag indicating weather the Source IP in law is a network mask |
| Dest. Mask | A Flag indicating weather the Dest IP in law is a network mask |
| Action | Accept (Route and Notify), Deny (drop), Reject(Drop and Notify) |
| Protocol | Protocol which will match: TCP, UDP |

Fig. 2. Structure of law

3.4 Working with established list

Considering a TCP source packet originating from the machine having IP address 172.24.32.14:5000 destined to the machine 172.24.32.15:5001.

(1) The datagram is first routed to the firewall. At the router (which is running the firewall), the firewall extracts the required fields from the packet header. It then traverses the LawTree according to the source IP.

(2) On traversal, a match is found at law 1 (fig 3).

(3) The action demanded by the law is to accept the packet and hence, the packet is forwarded to the destination and a message is sent to the source informing that the datagram has been routed to the destination.

| src_addr | src_port | dst_addr | dst_port | action | src_mask_flag | dst_mask_flag | protocol |
|--------------|----------|--------------|----------|--------|---------------|---------------|----------|
| 172.24.32.14 | 5000 | 172.24.32.15 | 5001 | 0 | 0 | 0 | 6 |
| 172.24.0.0 | 5010 | 172.24.32.16 | 5011 | 2 | 1 | 0 | 17 |
| 172.24.12.1 | 5000 | 172.24.0.0 | 5001 | 0 | 0 | 1 | 6 |

Restricted words - terrorist | bomb | suicide

Fig. 3. Working with established list

Now considering a UDP source packet originating from the machine having IP address 172.24.32.14:5010 destined to the machine 172.24.32.16:5011.

At the router, similar procedure as above is followed, with the exception that the src mask flag is set. This means while traversing the LawTree an internal node is matched which contains a non-empty list of laws which apply to all the addresses matching the sub-tree rooted at this node. Hence, in this case the datagram is accepted and desired action needs to be taken. The action bit is set 2 which implies the packet is to be dropped and the source is informed.

Now considering a TCP source packet containing the word "terrorist" and originating from the machine having IP address 172.24.12.1:5000 destined to the machine 172.24.32.15:5001. Following the above guidelines, the packet is accepted by the router after packet-level filtering. Now the packet is filtered using content-based filter in which it is dropped as it matches a restricted word "terrorist".

3.5 Workflow

The process of the proposed system has the minimum possibility of packet drops and can deeply identify a packet is really containing rejected contents or not. That can free this system from risks. The workflow of the system is discussed in following subsections:

3.5.1 Make up list categories for incoming packets. Here, Firewall list up the connection of packets into three categories (fig 4). Established list contains the connections of trusted packets. Deny list contains the connections are blocked. Third list is additional list containing the connections of packets are not sure about those are safe or not.

Three types of lists containing packets

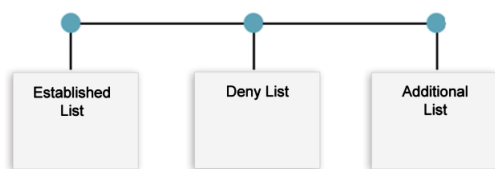


Fig. 4. List categories

3.5.2 Ready for checking. A firewall normally set connection of a packet to the established list, if anyhow it entered into the own system. If that packet have risk materials then it become unable to detect for a traditional firewall. To remove this risk condition this firewall always continue an enquiry to check established connections (fig 5) are trusted or not. Here shown some rules are

produced for exceptional packets by the system itself according to packet.

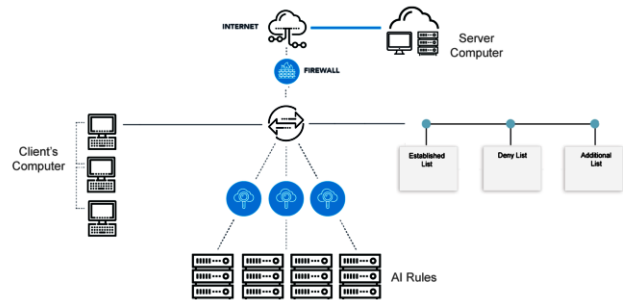


Fig. 5. Connection

3.5.3 When a packet satisfies AI rules. After matching with all the AI rules, It assumes that the packet is trusted (fig 6). Then the connection is made with the established list and give permission to access the system. It assumes that the packet is not trusted.

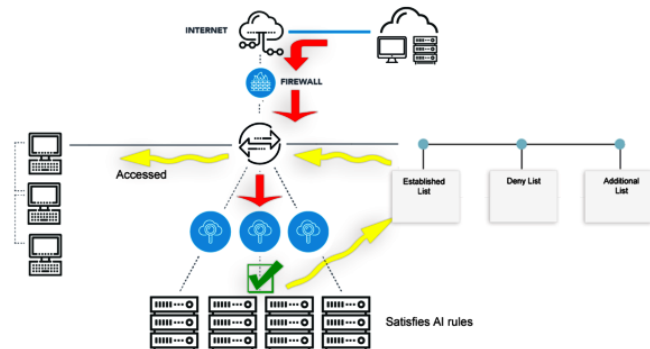


Fig. 6. If AI rules matched

3.5.4 When a packet does not satisfies AI rules. If anyhow the packet does not matched the AI rules because of unnecessary codes, following thing happens (shown in fig 7)

3.5.5 If a packet is not understandable. A packet which is not understandable with the entire processing rules including AI rules, it will not be dropped. This packet will stored in a new file for further checking if somehow AI can process it later by some rules (fig 8).

3.5.6 A traditional firewall basically do. It can't produce AI rules by itself. Just can match some predefined rules to the packet headers. If matched, then make a connection; otherwise block the packet (fig 9).

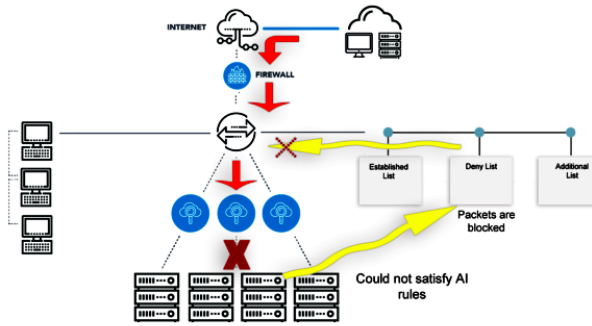


Fig. 7. Mismatched with AI rules

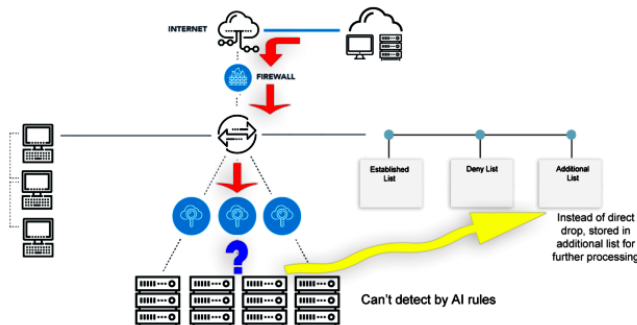


Fig. 8. Confusion with AI rules

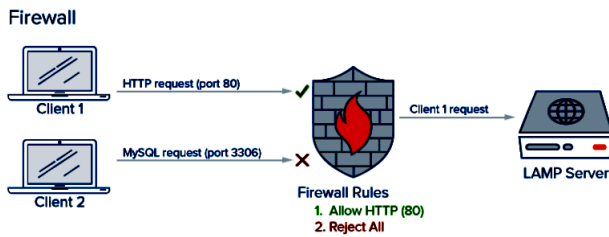


Fig. 9. Traditional Firewall Operations

3.6 Types of Firewall

There are three types of firewall. They are-

- (1) Stateless (packet-filtering) firewall
- (2) Statefull firewall
- (3) Application layer (Proxy) firewall

Stateless Firewall: A stateless firewall monitors each packet individually and isolately. It allows or denies packets without knowing the packets content and connection state. A packet-filtering firewall gives permission to packet for passing through by checking its source and destination address, protocol and destination port number. If these are not match with the firewall rules then the packet is dropped.

Statefull firewall: This firewall is more effective then the stateless firewall. It consists a list of all trusted connection that are already established. When firewall gets a new packet, it is checked with the list. If it is matched then the packet is through without further checking. If it is not matched, the packet is sent for checked with the initial rules for new connection.

Application layer firewall: Application layer or proxy firewall examines the packet at the application layer acting as a intermediary between the client and the server. This firewall examines the entire network packet rather than just the network address and the port number. In case of outgoing, server allows most of the packets, because the server is usually trustworthy to itself. Still the outgoing rule set in a way that can be used to prevent the server from unwanted communication or malicious executable attackers.

Pros and Cons of these above mentioned firewall:

1. Attacks that are prepared by the process itself, can not be handled.
2. If an unauthorized user already gained access, this system is ineffective to work on this.
3. In stateless filtering, there is needed more time to establish or drop connection because it checks each packet individually.
4. As it checks some definite number of port number and destination number without knowing the content of the packet, it is not suitable for all trusted packet if it does not consist those numbers.
5. In statefull filtering, there is no rule for new packets.
6. As intermediary layer, proxy firewall is always slow and time consuming.
7. Sometimes, these process drop some trusted packet.

Proposal: Here, researchers want to extend the features of statefull firewall. Firewall sets accept or deny action for packets by default. Researchers proposed to add Artificial Intelligence with this firewall. The purpose of using AI is to make some rules with itself for some exceptional packets. So no default actions need to be used. Advantages of the proposed process:

- (1) It can be produced new rules for exceptional packets.
- (2) Attacks are handled that are created by the process itself.
- (3) The problem of establishment an unauthorized connection is solved with AI rules.
- (4) A packet that is not understandable with the entire processing rules including AI rules, it will not be dropped. This packet will stored in a new file for further checking if somehow AI can process it later by some rules.

3.7 Algorithm

A firewall is a security watchman put between a private system and the outside Internet, that monitors all incoming and outgoing packets. The function of a firewall is to inspect every packet and decide whether to accept or discard it based upon the firewall's policy. This policy is specified as a sequence of (possibly conflicting) rules. When a packet comes to a firewall, the firewall searches for the first rule that the packet matches, and executes the decision of that rule.

With the explosive growth of Internet-based applications and malicious attacks, the number of rules in firewalls have been increasing rapidly, which consequently degrades network performance and throughput. In this paper, we propose **Firewall Compressor**, a framework that can significantly reduce the number of rules in a firewall while keeping the semantics of the firewall

unchanged. Researchers make three major contributions in this paper.

- (1) First, they propose an optimal solution using dynamic programming techniques for compressing one-dimensional firewalls.
- (2) Second, they present a systematic approach to compressing multi-dimensional firewalls.
- (3) Last, they conducted extensive experiments to evaluate Firewall Compressor.

Advantages of proposed system:

- (1) In terms of effectiveness, Firewall Compressor achieves an average compression ratio of 52.3 percent on real- life rule sets.
- (2) In terms of efficiency, Firewall Compressor runs in seconds even for a large firewall with thousands of rules.
- (3) Moreover, the algorithms and techniques proposed in this paper are not limited to firewalls. Rather, they can be applied to other rule-based systems such as packet filters on Internet routers.

Here a basic idea about firewall packet filtering prediction is implemented by a simple algorithm -

```

Packet
{
AI rules
{
Source_Port Num;
Supervised Rules to check unauthorized_connection;
Source_IP Address;
Supervised Rules to check unnecessary code;
Destination_Port Num;
Unsupervised rules to check Exceptional packet;
Destination_IP Address;
}
}

Filtering (Packet P)
{
Established_list ()
{
For All_Establish_connec
Compare_with_AI_rules ;
//to check established connections are trusted or not
IF find_untrusted
{
send to (Denylist);
}
Else Continue;
}
Compare (P_with_Established_list)
IF match
{
Perform_Action( Accepted);
}
Else Send_for_new_connection_in_S;
S: For (Every_rule_R)
{
For (Check_Every_line_using_AI_
to_find_any_unnecessary_Code)
{
IF match then {

```

```

PerformAction( Accepted);
Include_the_Connection_
in_Established_list;
}
Else PerformAction(Deny);
P_is_stored_in (Denylist);
}
IF find_Unnecessary_Code
{
Send_to (Additional_list);
}
Else Continue;
}
Denylist(){
For (Check_Every_line_using_AI_to_find_
any_necessary_Code)
{
For (Every P)
Compare P_with_AI_rules;
IF match {
PerformAction( Accepted);
Include_the_Connection_in_
Established_list;
}
Else
Send_to (Additional_list);
}
IF find_Unnecessary_Code{
send_to (Additional_list);
}
Else Continue;
}
Additional_list()
{
Keep_all_the_undetermined_packet;
Keep_all_unnecessary_code;
}
}

```

This algorithm also performs following tasks-

1. Accept new and establish incoming traffic to the port 80 and 443.
2. Drop incoming traffic from IP address port 22.
3. Controlling AI, use the port number 26.

3.8 Design

3.8.1 Data Flow Diagram. First, researchers design a Data flow diagram of Packet Filtering Prediction System (fig 10), which is a preliminary step to create an overview of the system without going into great detail, which can be later elaborated. It generally consists of overall application data flow and prediction process. Packet Filtering Prediction System shows functionalities and details of data flow of the system. It also shows low level functionalities such as how a user can get a specific packet from server. The below diagram(fig 10) are used to visualize of flow of packet and check with that rules.

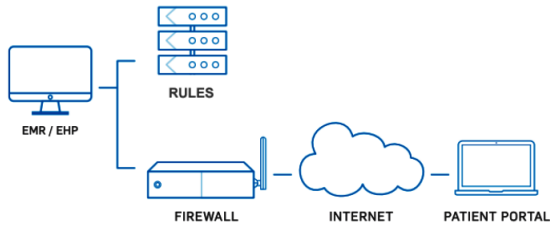


Fig. 10. Data Flow Diagram

4. IMPLEMENTATION AND RESULT

The implementation phase constructs, installs and operates the new system. The most crucial stage in achieving a new successful system is that it will work efficiently and effectively. The interfaces of the system are discussed in following subsections.

4.1 Home

This is the main UI of the application. All functionality can be accessed from here. UI is shown in fig 11

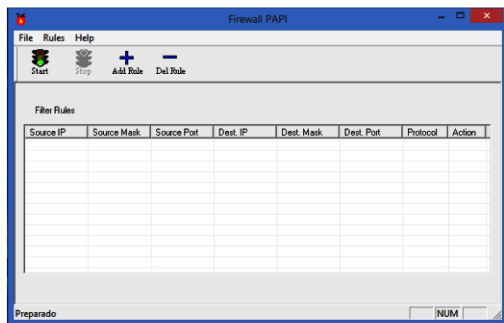


Fig. 11. Home Page

4.2 Rules

The list of all rules can be found here. Author can add or remove any rule (fig 12)

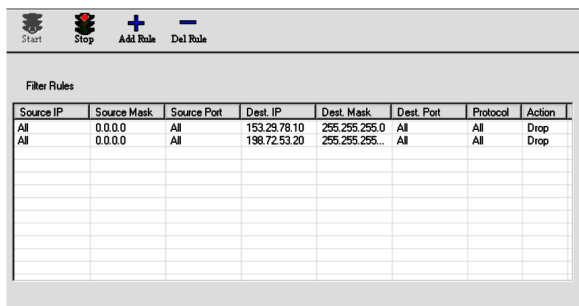


Fig. 12. Rules Section

4.3 Load Existing Rules

Users can load rules from an external source, shown in fig 13

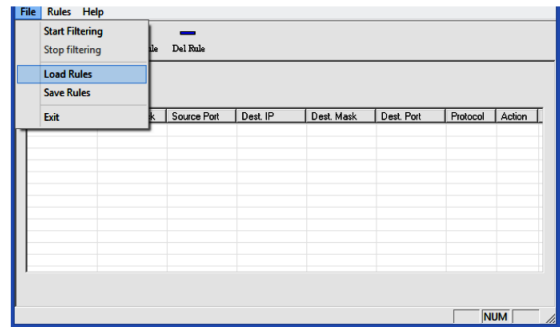


Fig. 13. Load Existing Rules

4.4 Start and Stop

After selecting manual rules, user can start applying that rules or stop the started process (fig 14).

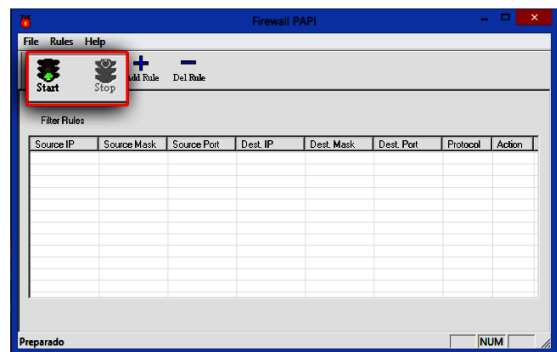
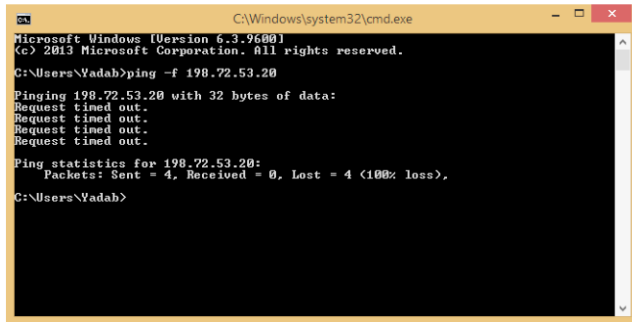


Fig. 14. Start and Stop part

4.5 Result

After starting the firewall, user can check by windows command prompt that the packet transferring is actually stopped. Result part is shown in fig 15.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Vadab>ping -f 198.72.53.20

Pinging 198.72.53.20 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 198.72.53.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Vadab>
```

Fig. 15. Result in cmd

5. CONCLUSION

In this work, researchers have come up with a model to find the real knowledge of upcoming packets based on AI rules. As per this model, it was concluded that one factor was content checking which determined the success rating of safe packet acceptance. There are several aspects that can be given serious consideration for future work in this research such as removing rule redundancy and reducing the number of rules in firewall policies by combining two or more of them. It will be a great area of further work.

6. REFERENCES

- [1] Douglas E. Comer. Inter networking with tcp/ip principles, protocols and architecture, 1988.
- [2] D. B. Chapman and E. D. Zwicky. Building internet firewalls. OReilly and Associates, Inc., 1995.
- [3] Karanjit Sijan and Chris Hare. Internet firewalls and network security. 1996.
- [4] Harold F. Tipton and Micki Krause. Handbook of information security management. CRC Press LLC, 1997.
- [5] Larry L. Peterson and Bruce S. Davie. Computer networks a systems approach 5th ed, Morgan Kaufmann Publishers (March 2011)
- [6] H. Abie. Corba, Firewall security: Increasing the security of corba applications, 2000.
- [7] Kristian Valentin and Michal Maly, Network Firewall Using Artificial Neural Networks, 2013.
- [8] Wikipedia Firewall (Computing). URL [https://en.wikipedia.org/wiki/Firewall\(computing\)](https://en.wikipedia.org/wiki/Firewall(computing)).
- [9] Nainesh V. Patel, Narendra M. Patel and Costas Kleopa, OpenAppID - application identification framework next generation of firewalls, 2016.
- [10] S. Arunkumar et al., Next generation firewalls for dynamic coalitions, 2017.