International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

AN EFFECTIVE PACKET FILTERING MECHANISM FOR REDUCING COMPLEXITY

Vijay Venkat Raaj. S[1], Kavitha. M[2]
[1,2]*Department of Information Technology, SRM University, Kancheepuram, India.*
venkatraj7657@gmail.com, kavitha.mu@yahoo.com

Abstract

Most organizations need to control the traffic that crosses into and out of their networks to prevent attacks from both the network as well as organization perspective. The firewall is a crucial component in the defense mechanisms of every network connected to the internet. It is the first filtering device that sees IP packets that attempt to enter a network from outside and the last device to let an outgoing packet as well. It's like a security guard that uses policies to make filtering decision on every packet that crosses it: whether to let it pass or drop it. Packet matching in firewalls involves matching on many fields from the TCP, UDP and IP packet header like, packet's source and destination IP address, protocol and source, destination port numbers. This paper proposes an algorithm of computational geometry which solves the point location problem, with a linear space requirement and O (log n) search time. In such situation, usage of overlapping hyper-rectangles is done, firewall administrators uses intersection and difference operations on sets of IP addresses or port numbers and then implement over the incoming and outgoing packets since firewall rules often overlap each other, which is the solution for the problem so that it would be faster and efficient in nature.

***Keywords*-- Packet Filtering, Packet Matching, Firewalls, Network-level protection, Hyper-Rectangles**

I. INTRODUCTION

Traditionally, a firewall has been a dedicated piece of hardware meant to allow two networks to communicate in a secured way. It acts as a gateway that restricts and controls the flow of traffic between networks, typically between an internal corporate network and the Internet. In recent years, software firewalls have come into use, and they pose a cost effective solution for many users, such as those with home or small office broadband networks.

Information that is transmitted on networks is in the form of 'packets'. In other words the information is divided into small pieces at the source, transmitted and reassembled at the recipients end. The firewall examines relevant parts of a packet and only allows those that comply with its configuration to be successfully delivered. This is why; some of the right packets configured wrongly is being rejected by firewalls. In the case of a proxy firewall, traffic never flows directly between the networks. Instead, the proxy repackages request and responses. No internal host is directly accessible from the external network and no external host is directly accessible by an internal host.

The major work of a firewall is Packet filtering, which controls access by examining packets based on the content of packet headers.

The information of the header, such as IP address or port number is being examined to determine whether a packet should be forwarded or rejected, based on a rule set. Further, stateful packet filtering forwards or rejects traffic based on the contents of a state table maintained by a firewall. When stateful filtering is used, packets are only forwarded if they belong to a connection that has already been established and that is being tracked in a state table. Thus, it is important to realize that a firewall is a tool for enforcing a security policy that can benefit an organization as well as a home computer by creating a security perimeter.

1.1. Packet Classification

First thing, before the filtering, any firewall has to classify the packets. Packet classification is an enabling function for operating on a variety of Internet applications including parameters like quality of service, security, monitoring, and effective communications. The main reason for the success of the firewall is that, it allows centralized filtering of traffic entering and exiting the protected network or demilitarized zone.

In order to classify a packet as belonging to a particular flow or set of flows, network nodes must perform a search over a set of filters using multiple fields of the packet as the search key. Individual entries for classifying a packet are called rules.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

The packet classification context determines the first matching rule for each incoming message at a router. The classifier or rule database in a router consists of a finite set of rules. Each rule is a combination of a set of values, one for each header field in the packet. Each field in a rule is allowed three kinds of matches: exact match, prefix match, or range match

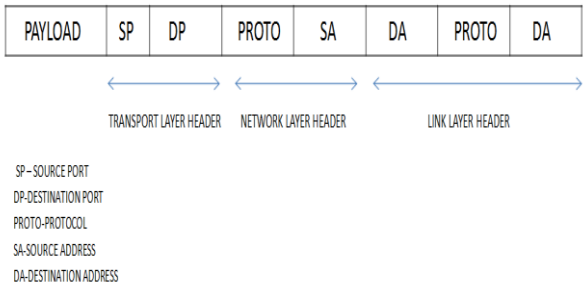

Fig. 1. Some of the header fields for classifying the packet

In an exact match, the header field of the packet should exactly match the rule field. For instance, this is useful for protocol and flag fields. In a prefix match, the rule field should be a prefix of the header field- this could be useful for blocking access from a certain sub network. In a range match, the header values should lie in the range specified by the rule-this can be useful for specifying port number ranges. A packet matches a rule, if all the header fields of the packet match the corresponding fields in that rule. If a packet matches multiple rules, the matching rule with the smallest index is returned. Thus, packet classification acts as a base towards large scale packet filtering.

1.2 Packet Filtering

The major work of the firewall lies in the working of its packet filter. It operates by identifying a policy i.e. a document defining acceptable access to protected, DMZ, and unprotected networks and set general guidelines for what is and is not acceptable for network access by the legitimate users.

The security policy is the set of rules that can help keeping systems secure. Any system connected to the internet, directly or indirectly, should have a security policy. For a typical home system, this doesn't have to be very complicated, and it doesn't have to exist as a formal document, just a set of rules that set out what you are trying to accomplish, and what anybody using computers is expected to do to protect them in an effective way.

Thus, a packet filtering is the first-level firewall technology that analyses network traffic at the network layer. It is a mechanism used to provide a level of security by examining some key information in packet headers. A packet filter determines if the packets are allowed to go through a given point, based on the control policies set by the network administrator.

Each packet is examined to see if it matches with set of rules defining what data flows are allowed. These rules identify whether communication is allowed based upon information contained within the internet and transport layer headers and the direction in which the packet is destined. This is done by comparing the protocol header fields of a packet with a filter specification. The process of controlling access by examining packets based on the content of packet headers. Header information, such as IP address or port number, is examined to determine whether a packet should be allowed, based on a rule set i.e. a collection of access control rules that determines which packets are forwarded or dropped.

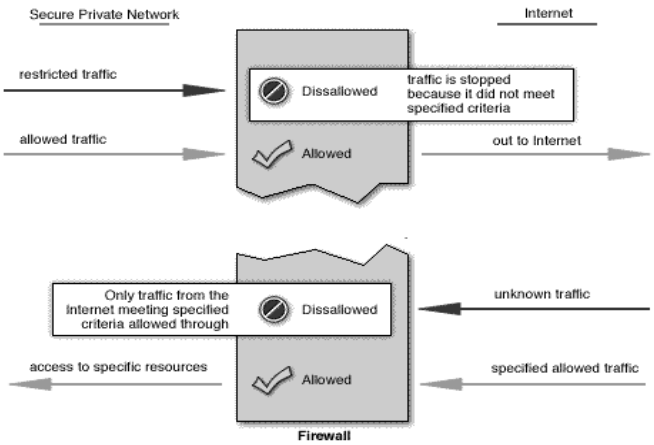

Fig. 2. Concept of filtering a packet by firewall rules

Most of the modern and commercial firewalls are stateful. These ones are stateful in nature and do the process of forwarding or rejecting traffic based on the contents of a state table maintained by a firewall. When stateful filtering is used, packets are only forwarded if they belong to a connection that has already been established and that is being tracked in a state table.

These things are implemented by major firewall vendors like Cisco, Check Point and Juniper. Thus, every firewall requires their own algorithms and corresponding rule sets.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

1.3 Packet Matching

The major scenario behind the working of the stateful filtering mechanism enters the concept of packet matching. It involves matching the specific fields of a packet towards an existing rule-set of the firewall and then if positive, accepts or rejects the packet if negative. There are various approaches used here. For example, the first match semantics matches a packet if the first rule of the firewall rule-set matches the packet.

Commercial firewall vendors like Cisco has come up with the concept of flexible packet matching, against notable worms and viruses. It specifies arbitrary bits and bytes between the entire packets, classify them and set up custom filters using XML-based policy language. The main advantages of packet matching are that, administrator need not define specific rules for return traffic or on the outgoing packets and thus proving to be more secure and robust in filtering the packets.

II. Related Works

There have been extensive researches for developing a secure firewall that identifies and filters the wrong ones. This can be done an effective packet matching algorithm. Based on the literature survey done, there exist two types of algorithms for developing stateful firewalls. These are based on the searching the right rule for the right packet sent during the flow.

They include: 1) slow algorithm that implements the "first match" semantics and compares a packet to all the rules and 2) fast state lookup mechanism that checks whether a packet belongs to an existing open flow. In many firewalls like IP tables, an open source, Linux based firewall, the slow algorithm is used, and linear search is done for finding the matching rule-base, while the state lookup mechanism uses a hash table or a search tree, which effectively searches the rule base matching the packet.

```
access -list 101 permit tcp 172.16.0.19 255.255.255.0 host 172.17.0.1 gt 0
access -list 101 deny 172.16.0.19 255.255.255.0 12.19.0.2 255.255.0.0 eq 135
```

Fig. 3. Excerpts from a firewall configuration file, that shows two access list rules referring the first match semantics.

2.1 Contributions

On analysis of various existing firewalls, it is found that the matching rule for the packet is not actually that much feasible for the incoming and outgoing packets that this single phenomenon acts as a vulnerability for various threats towards the computing systems like distributed denial of service in the case of servers and denial of service attacks in home computers.

These types of attack can be done as an attempt to make a machine or network resource unavailable to its intended users, making Acknowledgment loss that can cause a situation where a port may remain open for a time interval long enough for an eavesdropping attacker to identify and launch a directed attack to it.

III. Proposed System

In the paper we propose a mechanism based on the fast state look up, that will effectively match the incoming packets based on the valid rule that can best match the packet. Further it retains the reduced time complexity of O (log n) and reduces the space complexity to O (n).

3.1 Overall Description

The scenario of packet matching uses a solution taken for the point location problem that is finding the right point at the right place. For this the concept of hyper rectangles is used.

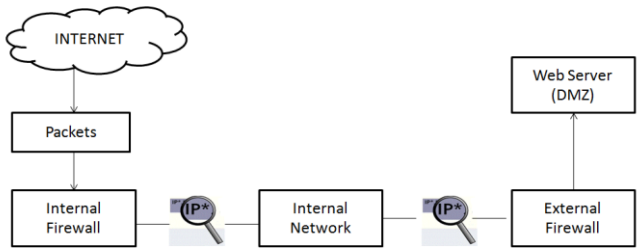

Fig. 4. Block Diagram of overall mechanism

Here, the incoming packets are checked by the internal firewall for matching packets and if everything went ok, packets are sent inside to the internal network on the first case. In the second one on the right, the outgoing packets are searched for the right fields and parameters and sent to the web servers.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

3.2 Point Location Problem

The problem can be considered as follows. Each packet is a point in d-dimensional space: each header field corresponds to a dimension. Each rule is now a d-dimensional "box", and we have N such boxes (rules), that may overlap each other, with a higher priority given to boxes (rules) which are listed first. Under this interpretation, the matching problem is now: find the highest priority box that contains a given d-dimensional point.

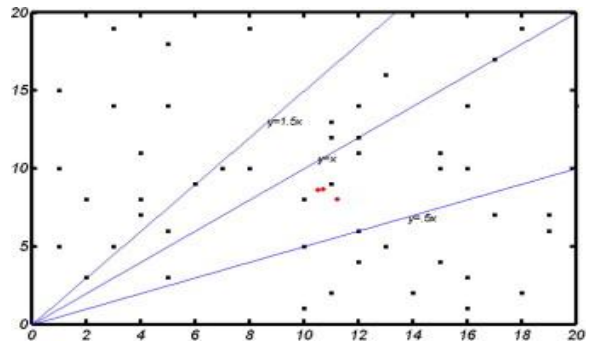

Fig. 5. Point location problem

It is difficult for people to visualize three-dimensional space. But in 2 dimensions the analogy is quite natural. Think of a plane, with the X-axis corresponding to the source IP address, and the Y-axis corresponding to the destination IP address. In this view, a rule is a rectangle: all points whose X value is in some range and whose Y value is in some other range. If one of the fields is a "don't-care", we just end up with a very wide (or very tall) rectangle. A rule-base with N rules now becomes a collection of overlapping rectangles.

When 2 rectangles overlap, one hides parts of the other. Now think of all the "PASS" rules as having a white color, and all the "DROP" rules as having a black color. Viewed from above, the full set of N rectangles subdivides the plane into a patchwork of rectangles, and rectangle fragments (that are just smaller rectangles) – some white and some black. Given a particular point, with some X/Y coordinates (source/destination IP addresses), finding which rectangle does it belong to, and what color is that rectangle, is called a point location problem.

3.3 The Solution

We can consider the algorithm proposed as the solution for the problem, by having the hyper rectangles in hand. We find the first rule that matches a given packet on one or more fields from its header. Every rule consists of set of ranges for a set of values where each range corresponds to that particular field in a packet header. The field values are in the range of 0 to N, where N is the maximum value for all the protocol systems. Then, we can give the packet-matching problem a geometric analogy or an interpretation. Each packet is a point in d-dimensional space: each header field corresponds to a dimension. Each rule is now a d-dimensional "box", and we have N such boxes (rules), that may overlap each other, with a higher priority given to boxes (rules) which are listed first. But Under this interpretation, the matching problem is now: find the highest priority box that contains a given d-dimensional point.

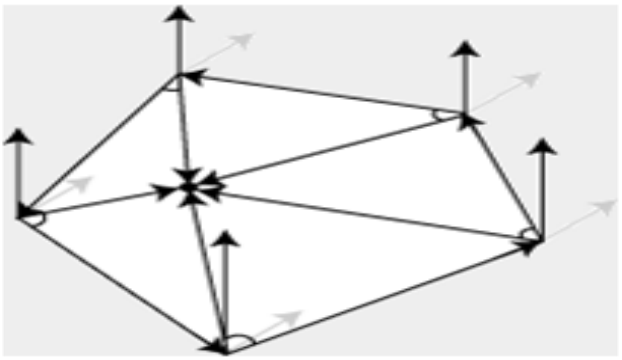

Fig. 6. Point location problem using Hyper Rectangles

Thus, the correct rule is found for the correct packet as the rectangle containing the point(s).

3.4 The Search Data Structure

The search data structure is the background process that works behind the solution for the point location problem.

It is a binary tree structure taking three major fields into our consideration like protocol number, source and destination port numbers.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

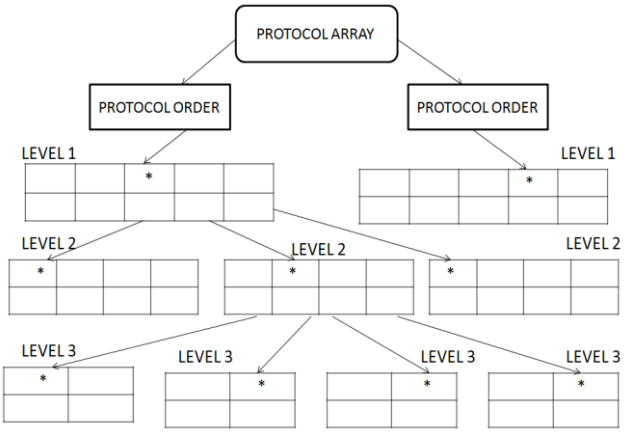

Fig. 7. Search Data Structure

As shown in Fig. 6, we consider protocol number as a source and construct a binary search tree and find the matching one i.e. of the packet. For each and every packet we deploy corresponding binary search technique and find the correct values. This is repeated over a number of times for the source and destination port numbers to get the best result with a time complexity of O (log n).

3.5 The Build Algorithm

In order to impart the full result from the partial search work, they must be combined together. This is accomplished by using the build algorithm. This is done one for each protocol. This consists of rule-base plus field order to use. This can be started by setting critical points over each level and run sweep-line over them and calculate the active rules for every level. Finally, on manipulation, we get the correct rule that matches the packet with lowest number of active rules in hand, with a space complexity of O (n).

IV. CONCLUSION

The analysis of the packet screening algorithm is an efficient and practical algorithm for firewall packet matching. It is implemented successfully, and tested its packet-matching speeds. Its matching speed is far better than the naive linear search, and it is able to increase the throughput by an order of magnitude. On rule-bases generated according to realistic statistics, its space complexity is well within the capabilities of modern hardware.

As for the algorithm itself, the algorithm's behavior can be explored when using more than 4 fields, e.g., matching on the TCP flags, Meta data, interfaces, etc. They may include: Testing the space complexity, if will stay close to linear and the best order of fields to achieve the best space complexity and work the same on IPv6 protocol.

Acknowledgement

We specially thank our HOD and the staff members of SRM University for rendering us valuable information and encouraging us throughout our research.

REFERENCES

[1] D.E. Taylor, "Survey and Taxonomy of Packet Classification," ACM Computing Surveys, Vol. 37, no.3, pp. 238-275, 2005.

[2] P. Gupta and N. McKeown, "Algorithms for Packet Classification", IEEE Network, Vol. 15, no. 2, pp. 24-32, Mar. /Apr. 2001.

[3] A. Wool, "Packet Filtering and Stateful Firewalls", Handbook of Information Security, vol. III, Threats, vulnerabilities, Prevention, Detection and Management, H. Bidgoli, ed., chapter 171, pp. 526-536 John Wiley & Sons, 2006.

[4] V. Srinivasan, "A Packet Classification and Filter Management System," Proc. IEEE INFOCOM, pp. 1464-1473, 2001.

[5] D. Eppstein and S. Muthukrishnan, "Internet Packet Filter Management and Rectangle Geometry," Proc. ACM- SIAM Symp. Discrete Algorithms (SODA),pp. 827-835, 2001.

[6] P. Gupta and N. McKeown, "Packet Classification on multiple fields," Proc. ACM SIGCOMM as on pp. 147-160, 1999.

[7] S. Singh, F. Baboescu, G. Varghese, and J. Wang,, "Packet Classification Using Multidimensional Cutting," Proc. ACM SIGCOMM, 2003.

[8] Mikkel Christiansen, Emmanuel Fleury, "Using IDDs for Packet Filtering," Department of Computer Science, Aalborg university, Proc, BRICS 2002.

[9] D. Rovniagin and A. Wool, "The Geometric Efficent Matching Algorithm for Firewalls ," Report EES2003-6, Dept. of Electrical Eng. Systems, , Tel Aviv Univ. http://www.eng.tau.ac.il/yash/ees2006 ps. 2009 .

[10] Firewall Wizards, Electronic Mailing List, http://www.listserv.icsalabs.com/pipermail/firewall-wizards/, 2009.