Efficient Packet Filtering for Stateful Firewall using the Geometric Efficient Matching Algorithm.

Shriya .A. Jadhav and Dr. Prdeep K. Deshmukh Department of Computer Engineering,University of Pune

Abstract

As GEM algorithm is recently studied and presented where it had shown the efficient performance. We observed that GEM algorithm is performing efficiently for the packet matching in firewall. The practical experiment was done successfully in the Linux kernel, as well as tested its packet-matching speeds on live traffic with realistic large rule-bases. The speed of GEM algorithm is more as compared to the naive linear search, in addition to this also resulted into the improved throughput of iptables with order of magnitude. We also observed that GEM is having better space complexity in order to suit current hardware. We have noted that GEM is exceptionally well according to it space complexity, but its optimization performance not yet evaluated as compared to other previous algorithms of firewall packet matching in order to claim GEM as optimized in packet matching. Also one more limitation of GEM which we identified is only four fields are used for firewall packet matching. Thus in this project we are presenting the extended GEM approach in which we will first like to evaluate the performance with existing method of firewall packet matching as well as will try to use more than four fields while packet matching and this results into more improved performance of GEM.

Keywords:Firewall,security,firewall rule,packet matching.

1. Introduction

Firewall is one of the central technologies permitting high-level access management to organization networks. Firewalls are key parts of the Internet infrastructure to protect users and network services against attackers. The filtering policy determines which packets are allowed to enter or leave a given network segment. Rules describe security policy of the firewall, which tells about what decision should be taken for individual packets. Firewall rule is made up of two parts, predicate which describes packet header information containing source and destination IP address, source and destination port number and protocol type information and decision of accept or deny. Table 1 shows sample firewall rule list where rule R1 and R5 are conflicting rules. For securing any network implementation of firewall is essential, and for effective working of firewall, firewall rules designing must be done properly. All modern firewalls mostly make use of "first-match" semantics.

Rule no.	Source IP	Destination IP	Port number	Action
R1	88.88.99.10/32	192.168.1.2	*	Allow
R2	212.212.0.0/16	92.168.1.20/12	*	Allow
R3	199.12.12.12/38	192.168.1.2	13	Block
R4	*	192.11.11.11/19	80	Allow
R5	88.88.99.15	192.168.1.2.	10	Block

Table 1: Firewall Rules

The function of a firewall is to accept or discard the incoming packets passing through it, based on the rules in a rule set. The firewall rules are arranged in list, where decision of accept and deny is associated with the first rule that matches a given packet. Also it has been observed that some incoming packet match with more than one rule at the same time which may lead to some of the undesirable output. Such types of rules are called as dependent rules and if their action differs then it is called as conflicting rules.

Types depending on whether the firewall keeps track of the state of network connections or treats each packet in isolation, two additional categories of firewalls exist:

- ***Stateful firewall***
- ***Statefuless firewall***

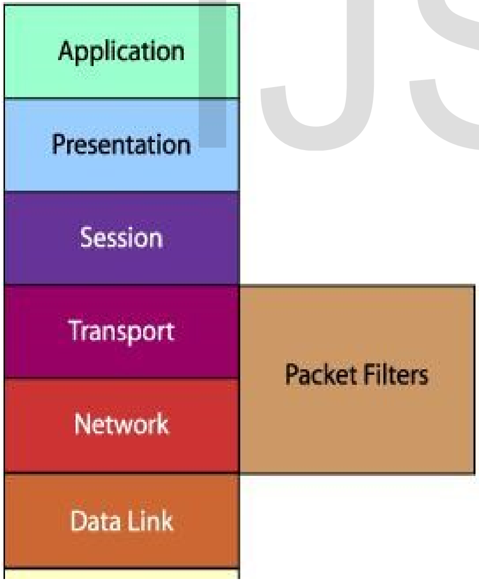

Figure 1: Stateless Firewall

Stateless firewall: In stateless firewall packet filters operate at the third layer of OSI MODEL i.e. at Network Layer or it uses transport-layer information only so they only look at the header part of a packet. The packet filter does not examine the data section of a packet. Action decides which service is to Permits or denies i.e. to allow the packets or to drop them. Because of the stateless nature it needs to monitor all the incoming and outgoing packets which is time consuming as each and every packets need to be matched with the firewall rule list to check if the packets should be allowed or need to get drop out of the system. Also search mechanisms by a slow algorithm like linear search of the rule-base that implements the first match semantics makes its more time consuming. Stateful firewalls solve this problem by maintaining a table of open connections.

Problem of Stateless firewall

- They have no memory to keep the track of last entered packets which makes them vulnerable to different types of attacks.
- No way of knowing if any given packet is part of an existing connection, so will keep trying to establish a new connection.
- They can be complex to configure.
- They cannot prevent application-layer attacks.
- They are susceptible to certain types of TCP/IP protocol attacks.

- They do not support user authentication of connections.
- They have limited logging capabilities.

Stateful firewall Deals with the state of connections, state here is vaguely defined as the condition of the connection, which varies greatly depending on application/protocol used.It stores the states of legitimate connections in a state table (state information usually stored as hash to make matching faster).Filters packets by matching to valid states in the state e ring need to be examined but once that is done the correspond flow is allowed of denied (based on the decision) need not be examined, which will reduce packet matching and searching time. In Stateful firewall when the first packet in a network is allowed to cross and all subsequent packets belonging to that flow and especially the return traffic flow is also allowed to pass through the firewall. Stateful firewalls typically build a state table and use this table to allow only returning traffic from connections currently listed in the state table. After a connection is removed from the state table, no traffic from the external device of this connection is permitted.

When a packet reaches a firewall, an extra field, tag is added to the packet. The initial value of tag is 0.Each firewall has a variable state, the value of state is a subset of the packets accepted earlier by firewall and the initial value of state is empty. This method can make decisions based on one or more of the following:

- Source IP address
- Destination IP address
- Protocol type (TCP/UDP)
- Source port
- Destination port
- Connection state

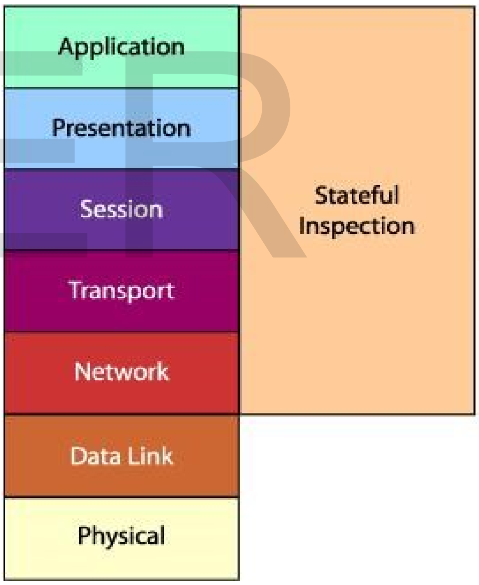

Figure 2: Stateful Firewall

Stateful firewall decides to accept or discard a packet based on: (1) the packet itself, (2) the packets that the firewall has accepted previously.

Stateful firewall depends on the three-way handshake sometimes described as SYN, SYN-ACK, ACK

State fullness has flowing two advantages

- No need to write explicit rules for return traffic and such return-traffic rules are inherently insecure since they rely on source-port filtering. This makes Stateful firewalls more secure as compare to stateless firewall.
- State lookup algorithms are typically simpler and faster than rule-match algorithms.

2. MOTIVATION OF THE DISSERTATION

Network traffic is increasing tremendously. Linear packet filtering requires much time to filter huge traffic. The motivation is based on the fact that the modern packet filtering firewall has adapted Stateful nature with linear lookup operation which is time consuming. It was observed that Stateful firewall is commonly implemented by first match semantics and compares a packet to all the rules also can be implemented by state lookup mechanism that checks whether a packet belongs to an existing open flow. In the proposed work hashing technique is applied for lookup operation and for the same an index file is maintained which keeps the track of rule number from the main rule list and hash key values. For every captured packet, based on the header information its key value is computed and mapping is done against index file. If proper match is found it indicates that the particular packet with same header information has previously entered the network and so further lookup is performed on the log file and based on the decision field action is taken. The log file here is the subset of the main rule list of recently matched packet, if match is not found in the index file it indicates that particular packet information is not present in the log file and lookup needs to be performed on main rule list, on finding the exact match its hash value is computed and the corresponding entry is made in the index file and in the log file. In result analysis it was observed that the proposed method proves to give better result for huge network traffic.

3. Programmer’s design

Network traffic is increasing tremendously. Linear packet filtering requires much time to filter this huge traffic, firewall should be able to sustain a very high throughput, or risk becoming a bottleneck. Here we try to propose that efficient matching algorithm filters more packets in less span of time i.e. time complexity required is less. But to implement Stateful firewall there is need to record state of each packet for the same logging of information is done.

For input data we can simulate IP Packets but we are capturing IP packets from Internet. For the same one Rule list in prepared in notepad which contains firewall rule with the field like source IP address, destination IP address, Type of packet (TCP/IP) and action field having decision of accept and deny, where accept decision will allow the packet to enter and deny will block the packet. Here firewall rule conflict issue is also taken in account. In conflicting rules, one single packet matches two rules and having action one as accept and other as deny.

- Logging Information: - Firewall log store the list of blocked URL so that we can get the information about the list of url blocked that is blocked. Firewall logs reveal a lot of information about the security threat attempts at the periphery of the network and on the nature of traffic coming in and going out of the firewall.

- Geometric Efficient Packet Matching: - The geometric matching techniques deal with the problem on efficient rang searching. As firewall rules deals with different fields and its range like source IP address range or destination IP address range, this geometric matching methods can be easily applied to firewall rules. The packet header contains the protocol number, source and destination address and port numbers fields, The GEM can be represented in Tree like data structure where first we check the protocol field and go to the protocol array of the search data structure, to select the corresponding protocol database header, From this point, we traverse data structure with the corresponding field value on every level, We find the matching simple range and continue to the next level. The last level gives us the winning rule i.e. the matching packet rules is found.

a) Architecture

The system starts capturing the packets from network and performs packet matching by applying hashing technique to search matching rule in the log file. If match found it calculates the time needed for packet matching else perform packet matching to search matching rule in main rule list file and the make the entry of rule in the log file and index file.

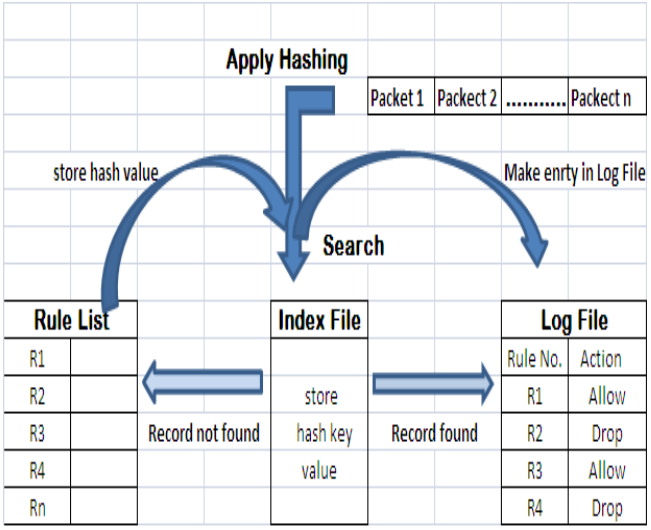

Figure 3: Architecture view of proposed system

b) Implementation

A firewall packet filtering and rule policy has become and increasingly important research in networking domain over last few years. Many researches are making efforts to improve the rule policies and cost of matching needed. In this work by managing the data in log file the attempt is made to reduce the time needed for matching.

2.0 Architectural design

During implementation three files are maintained namely main file containing firewall rule, a log file which is subset of main rule file containing recently captured packets and an index file having hash values. For captured packet, based on the header information its key value is computed and mapping is performed on the index file. Initially the index file and log file is empty so for the first packet in the network flow lookup is performed on the log file and based on the decision field action is taken and on finding the exact match its hash value is computed and the corresponding entry is made in the index file and in the log file, and for all the subsequent packets belonging to the same flow matching is performed by searching the record in log file instead of main rule list, thus by logging the information of the recently accepted packets we try to reduce to reduce the search time needed to scan the main rule list. Also as the log file is the subset of main firewall rule the number of rules in the log file is less as compared to the rules in the main file, so it is obvious that time needed to scan the log file will be less as compared to time needed to scan the main rule list file.

4. Results and Discussion

The graph shows the comparative result of pervious and proposed algorithm.

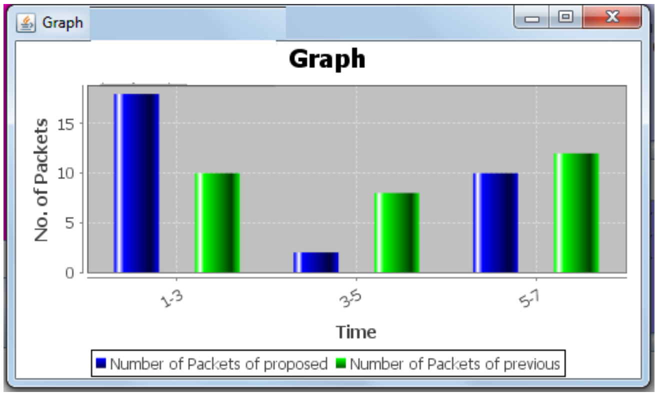

Figure 4:Result Graph

5. Conclusion

Firewall plays a vital role in securing any packet based network. Most of the organization's security is based on implementation of firewall policies for securing there data. There are many techniques presented by researchers for exploiting the characteristics of the filtering policies, Statefuless is one of these characteristics where usually state information is stored in state table. Most of the organization now has adapted Stateful firewall with linear search lookup methodology. Success definition of the work can be stated as average searching time needed for packet filtering and matching. Thus the proposed matching scheme technique speed is far better than the naive linear search.

6. References

[1]T. V. Lakshman and D. Stiliadis, High-speed policybased packet forwarding using efïňĄcient multidimensional range matching, in Proc. ACM SIGCOMM, 1998, pp. 203âĂŞ214.

[2] V. Srinivasan, S. Suri, and G. Varghese, Packet classiïňĄcation using tuple space search,in Proc. ACM SIGCOMM, 1999, pp. 135âĂŞ146.

[3] V. Srinivasan, A packet classiïňĄcation and ïňĄlter management system, in Proc. IEEE INFOCOM, 2001,pp. 1464âĂŞ1473.

[4] M. Waldvogel, Multi-dimensional preïňĄx matching using line search, in Proceedings of IEEE Local Computer Networks, Tampa, FL, USA, Nov. 2000, pp. 200âĂŞ207.

[5] Thomas Y. C. Woo, A modular approach to packet classiïňĄcation: Algorithms and results, in Proc. IEEE INFOCOM, 2000, pp. 1213âĂŞ1222.

[6] P. R. Warkhede, S. Suri, and G. Varghese,

Fast packet classiïňĄcation for two-dimensional conïňĆict-free ïňĄlters, in Proc. IEEE INFOCOM, 2001, pp. 1434âĂŞ1443.

[7] V. Srinivasan and G. Varghese, Faster IP lookups using controlled preïňĄx expansion, in ACM Conference on Measurement and Modeling of Computer Systems, 1998, pp. 1âĂŞ10.

[8] D. Eppstein and S. Muthukrishnan, Internet packet ïňĄlter management and rectangle geometry,âĂİin ACMSIAM Symp. on Discrete Algorithms (SODA),

2001, pp. 827âĂŞ 835

[9] Alex X. Liu Eric Torng Chad R. Meiners, Department of Computer Science and Engg ,Michigan State University, East Lansing, MI 48824, U.S.A. FirewallCompressor: An Algorithm for Minimizing Firewall Policies

[10] M.G. Gouda and A.X. Liu, A Model of Stateful Firewalls and its Properties, Proc. IEEE Conf. Dependable Systems and Networks (DSN 05), pp. 320-327, June 2005.