IJERMT

International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

May- 2015 Volume 2, Issue-3

Email: editor@ijermt.org www.ijermt.org

# A MODULAR APPROACH BASED DYNAMIC FIREWALL OPTIMIZATION TECHNIQUE FOR IMPROVING SECURITY MEASURES

**M. Naveen**
P.G. Student
Department of CSE
Dhanalakshmi Srinivasan Engineering College
Perambalur, Tamilnadu, India

**J.Britto Dennis M.E Ph.D.**
Assistant Professor
Department of Computer Engineering
Dhanalakshmi Srinivasan Engineering College
Perambalur, Tamilnadu, India

**ABSTRACT**

A firewall is an intermediate system placed between two networks of different trust levels, mostly between the secure corporate system and the less secure own system. This paper approach is based on the histograms technique of packet matching rule and of packet not matching rule-field to secure own system. Histogram techniques are effective stochastic function to describe the characteristic of packet filtering in firewall. A comparison of the proposed approach and the other conventional approaches, including static rule order approach and dynamic rule order approach is presented. Histogram can be shared over multiple segments to estimate the optimized rule and rule-field order for early packet acceptance and rejection. This histogram techniques are evaluated and their performance are compared it is effectively packet filtering in firewall are redefining rule.

**KEYWORDS:** Histogram Technique; Rule-field; Optimized Rule

## 1. INTRODUCTION:

A firewall is a logical security component deployed between networks of different trust Levels. This is mostly between the public Internet of no trust and the internal network for a given business. Firewalls are also deployed within private trusted networks to segment networks and control resource Sharing the internally. A specific case in point would be using a firewall to control subnets within an organization to avoid data contamination. The primary function of a firewall is to block unauthorized traffic while permitting authorized traffic going in either direction. There are various types of firewalls deployed depending on the role required in the network. There is increased need for packet filtering with the growth of the Internet and the proliferation of Internet based services. This has extended the types to firewall categories based on functionality such as web application firewalls, proxy firewalls, host based firewalls, circuit level, dynamic and hybrid firewalls. Hybrid types are a combination of the two or more implementations to improve functionality. A firewall performs packet filtering by applying a set of rules to a packet sequentially until a rule matching the packet is found in the rule set. Firewalls that perform deep packet inspection like application firewalls go on inspecting even after the first match is found. Firewall rule-set can have configuration flaws; at times different administrators write rules ending up with a set of generic rules defined that match packets that other rules are not match rule. Packet filtering in each individual rule is also done in a sequential order starting from the first field until a non-matching field is found. If a packet matches all the fields in a rule, then the packet is said to match that rule. In this case, the processing for this packet filtering is completed. Therefore, the need for rule set optimization is a critical one. in addition, unwanted traffic targeting the default rule may cause more harm than others by producing an overhead to the system through increasing the overall filtering time. This overhead is proportional to the number of rules used in the security Policy. Such unwanted traffic may cause a denial of service (Do's) attack and degrade considerable of the firewall's performance. From this point of view, it is very important to reject such traffic as early as possible.

## 2. RELATED WORKS

Since packet filtering in firewall is done by sequentially searching the rule list until a matching is found, the scalability of such searching approach is generally poor due to the searching time which is proportional to the policy size as well as the order of rules and the order of fields contained in each rule. Packet filtering optimization is studied extensively. The most relevant research works focus on the improvement of searching times using various approaches, including hardware-based solutions, specialized data structures and heuristics .Although these researches have significant contributions to the packet classification, but their major objectives focus on improving the worst-case matching performance rather than the optimization for the best performance. This is because these approaches only exploit the characteristics of filtering rules rather than the effects of packet flow characteristics on searching time in firewall. There are several research works as focusing on the statistical firewall packet filtering approaches to improve the average packet filtering time. In a technique, called depth-constrained alphabetic trees, is used to reduce the lookup time by only searching packet destination IP addresses rather than the entries of routing table. However, its significance is limited by only searching a single field with arbitrary statistics. In contrast, researches presented in maximize the early rejection of unwanted flows without impacting other flows. This is done through a number of rejection rules that are examined before the real firewall policy. These rejection rules utilize the important traffic characteristics and minimize the average packet matching time. However, its weakness is not scalable with the number of fields and rules if they are used for intrusion detection systems (IDSs) because we will end up with a large set of rejection rules to be checked before proceeding with normal filtering process.

## 3. PERFORMANCE EVALUATIONS:

### 3.1 EVALUATION OF THE EFFECT OF DYNAMIC RULE AND RULE-FIELD ORDER IN DEFENDING AGAINST DOS ATTACKS

In this section, we investigate the effect of implementing static rule ordering, dynamic rule ordering and dynamic rule and rule-field ordering approaches on the firewall performance in defending against common Do's attacks.

### 3.1.1 DOS ATTACK CLASSIFICATION:

Do's attacks are commonly divided into the following categories: flood attacks, amplification attacks, protocol exploit attacks and malformed packet attacks. In a flood attack, the zombies send large volumes of IP traffic to a victim system in order to congest the victim system's bandwidth. Some of the well-known flood attacks are UDP flood attacks, ICMP flood attacks and Port scanning. In amplification attacks, the attacker exploit the broadcast IP address feature found on most routers to amplify and reflect the attack and send messages to a broadcast IP address. This instructs the routers servicing the packets within the network to send them to all the IP addresses within the broadcast address range. This way the malicious traffic that is produced reduces the victim system's bandwidth. Some well-known amplification attacks are Smurf and Fraggle attacks. Protocol exploit attacks exploit a specific feature or implementation bug of some protocol installed at the victim in order to consume excess amounts of its resources. A representative example of protocol exploit attacks is TCP SYN flood attacks. Other examples of protocol exploit attacks are PUSH + ACK attacks, CGI request attacks and the authentication server attacks. Malformed packet attacks rely on incorrectly formed IP packets that are sent from agents to the victim in order to crash the victim system. A representative example of malformed packet attack is the Land attack. Do's attacks are generated usually using either a flooding non-matching traffic, or a flooding matching traffic. Non-matching Do's traffic includes packets that do not match any filtering rule, and consequently, it is filtered by the default security policy. However, matching Do's traffic includes packets that match the filtering rules.

### 3.1.2 FIREWALL PERFORMANCE:

A packet generator is used to generate Do's attacks. The firewall uses the same set of filtering rules, described in Section 4. Two experiments have been performed using non-matching and matching Do's attack traffics, respectively. In the first Do's attack experiment, most packets received by the firewall do not match any filtering rule, and these packets are finally rejected by the default security policy. UDP flood, ICMP echo flood and Port scanning are examples of such attacks. To investigate the effect of the proposed optimization approaches, we generated a special packet flow consisting of only 10% of packets matching the filtering rules, and the other 90% of packets not matching any filtering rule. The cumulative packet filtering processing time for Static rule order approach, dynamic rule order only approach and dynamic rule and rule-field order approach. It can be seen that the cumulative processing time for the static rule order approach and the dynamic rule order only approach are very close to each other. That means the Improvement provided by dynamic rule order only approach is very limited. In contrast, gain provided by dynamic rule and rule-field orders approach is significant. This is because the filtering process may have to check most of the rule fields to reach a decision regarding a given packet when the firewall is heavily loaded with the filtering of the non-matching malicious packets. However, by applying dynamic rule and rule-field ordering approach, the position order of the fields in each filtering rule is optimized to make the matching process much faster, especially for malicious packets, compared to the ones related to static rule ordering approach and dynamic rule ordering only approach. In the second Do's attack experiment, the firewall is flooded by matching packets, such as SYN flood attack, in which TCP SYN packets are accepted by the firewall in order to allow external hosts to establish TCP connections on particular ports with internal servers. If the external hosts are allowed to access an internal web server, then for the particular HTTP port (80), the security policy should include a filtering rule allowing the firewall to accept SYN packets to that web server. However, flooding the network with SYN packets that have spoofed source IP addresses may damage the firewall performance and creates a congestion situation.

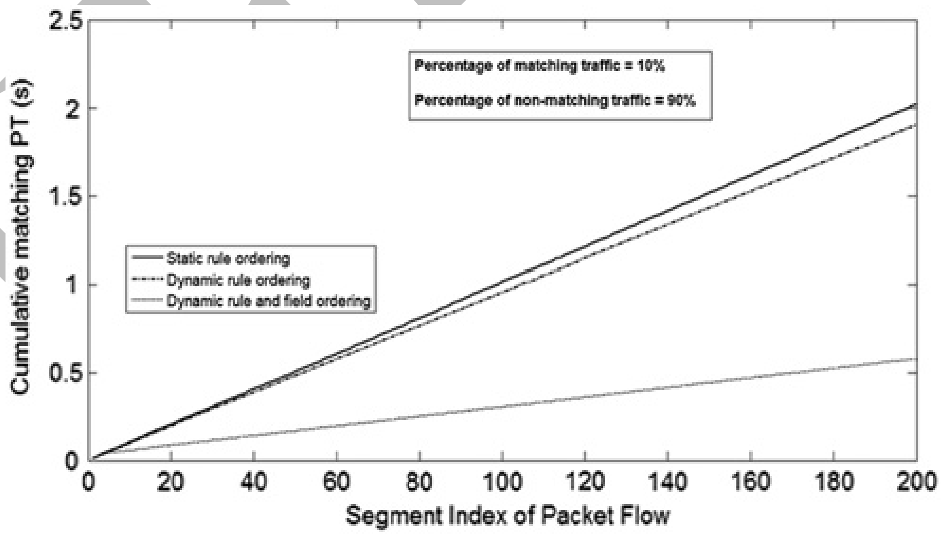

**Fig. 3 processing time for DoS attack with high non-matching traffic**

## 4. CONCLUSIONS:

Histogram is an effective stochastic function to describe the characteristics of packet filtering in firewall. Furthermore, the algorithm to calculate histograms on segment basis presented in this paper is efficient and deployable in practice for effectively monitoring traffic flow and optimizing firewall performance in real-time. The idea of the Histogram is to aid network administrators in optimizing rule sets; dynamic rule set adaptation is a possible extension on the functionality of the rule-field. The rule-field removes the need for the network administrator to manually redefining rules. The real time result demonstrated that the proposed mechanism improved significantly the firewall performance compared to related conventional mechanisms, in terms of packet filtering processing time. Also, the numerical results demonstrated that the proposed approach reduced significantly the effect of common Do's attacks on the firewall performance.

## 5. REFERENCES:

1. Baboescu, F., Varghese, G.: 'Scalable packet classification'. ACMSIGCOMM'01, 2001.
2. McAulay, A.J., Francis, P.: 'Fast routing table lookup using Cams'. IEEE INFOCOM'93, March 1993.
3. Srinivasan, V., Suri, S., Varghese, G.: 'Packet classification using tuple space search'. Computer ACM SIGCOMM Communication Review, October 1999, pp. 135–146.
4. Feldman, A.Muthukrishnan, S.: 'Tradeoffs for packet classification'. IEEE INFOCOM'00, March 2000.
5. Gupta, P., McKeown, N.: 'Algorithms for packet classification', IEEE Netw., 2001, 15, (2), pp. 24–32.
6. Gupta, P., McKeown, N.: 'Packet classification using hierarchical intelligent cuttings'. Interconnects VII, August 1999.
7. Cohen, E., Lund, C.: 'Packet classification in large ISPS: design and evaluation of decision tree classifiers'. SIGMETRICS '05: Proc. 2005 ACM SIGMETRIC Int. Conf. on Measurement and Modeling of Computer Systems, New York, NY, USA, 2005, pp. 73–84.
8. Thomas, Y.C.W.: 'A modular approach to packet classification: Algorithms and results'. IEEE INFOCOM'00, March 2000, pp. 1213–1222.
9. Hamed, H., El-Atawy, A., Al-Shaer, E.: 'On dynamic optimization of packet matching in high-speed firewalls', IEEE J. Sel. Areas Commun., 2006, 24, (10), pp. 1817–1830.
10. B.J. Prabhu, A. Chockalingam, A routing protocol and energy efficient techniques in Short rangescatternets, IEEE International Conference on Communications 5 (2002) 3336–3340.
11. R. Kapoor, M. Gerla, A zone routing protocol for Short rangescatternets, 2003 IEEE Wireless Communications and Networking Conference 3 (2003) 1459–1464.
12. Y.F. Wong, W.C. Wong, A fuzzy-decision-based routing protocol for mobile ad hoc networks, 10th International Conference on Network2002; 317–322.