ISSN 22773061

A review on working models of packet filtering in firewall technology

Er.Gurvinder Kaur , Dr.S.N.Panda ,Dr.D.S.Dhaliwal
Department of computer science& Engineering, RIMT Mandi Gobindgarh
er.gurvinderkaur@gmail.com
Department of computer science & Applications , RIMT Mandi Gobindgarh
panda.india@gmail.com
Department of computer science& Engineering,Bharat group of institutes Sardoolgarh
dalvinder.dhaliwal@gmail.com

Abstract

The goal of packet filtering in firewall technology is to sort packets based on packet characteristics. This paper represents the survey on various working models of packet filtering in firewall technology.

Keywords: Packet filtering, IP trackback-based intelligent packet filtering, Stateless FSA-Based Packet Filters.

Council for Innovative Research
Peer Review Research Publishing System
Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY
Vol 7, No 2

editor@cirworld.com
www.cirworld.com, member.cirworld.com

1. Packet Filtering

Firewalls performs only very basic operations, such as examining the packet header, verifying the IP address. Due to this simplicity of operation, they have the advantage of both speed and efficiency. The filtered packets may be incoming, outgoing or both, depending on the type of router. Packets can be filtered on the basis of some or all of the following criteria: source IP address, destination IP address, TCP/UDP source port, and TCP/UDP destination port. A firewall of this type can block connections to and from specific hosts, networks and ports. They are cheap since they use software already resident in the router, and provide a good level of security since they are placed strategically at the choke point. [1]

2.Working models of Packet Filtering in Firewall technology

2.1 IP Traceback Based Intelligent Packet Filtering :

Distributed Denial of Service (DDoS) is one of the most difficult security problems to address. The proposed scheme leverages on and generalizes the IP traceback schemes to obtain the information concerning whether a network edge is on the attacking path of an attacker ("infected") or not ("clean"). By preferentially filtering out packets that are inscribed with the marks of "infected" edges, the proposed scheme removes most of the DDoS traffic while affecting legitimate traffic only slightly. Simulation results based on real-world network topologies all demonstrate that the proposed technique can improve the throughput of legitimate traffic by three to seven times during DDoS attacks [2].

2.2 On Dynamic Optimization of Packet Matching in High-Speed Firewalls :

This paper has twofold. First, they presented a novel algorithm for maximizing early rejection of unwanted flows with minimal impact on other flows.

Second, they presented a new packet filtering dynamic optimization technique that used statistical search trees to utilize traffic characteristics and minimize the average packet matching time. The proposed techniques timely adapt to changes in the traffic conditions by performing simple calculations for optimizing the search data structure. The main advantages of these techniques are practically attractive because they exhibit simple-to-implement and easy-to-deploy algorithms [3].

2.3 Detecting and preventing peer-to-peer connections by Linux iptables :

Most of companies use Linux iptables as their edge networks firewall. Although Linux iptables is a reputed secure stateful packet filter firewall package, it has some weaknesses. This package can not detect or control all peer-to-peer connections. One of the packages which is written for Linux iptables to manage peer-to-peer connections is layer 7-module. This module can not detect all peer-to-peer connections and drop them. For controlling peer-to-peer connections investigator blocked some peer-to-peer well known static ports with Linux iptables and then, for increasing the control of other peer-to-peer applications which used dynamic ports, he used QOS rules. Although this trend could drop most of peer-to-peer connections and save internet bandwidth, it was not the complete solution. He decided to control peer-to peer connections by implementing a new module which checks peer-to-peer payloads in his next investigation[4].

2.4 Discriminative Wavelet Packet Filter Bank Selection for Pattern Recognition:

This paper addresses the problem of discriminative wavelet packet (WP) filter bank selection for pattern recognition. The problem is formulated as a complexity regularized optimization criterion, where the tree-indexed structure of the WP bases is explored to find conditions for reducing this criterion to a type of minimum cost tree pruning, a method well understood in regression and classification trees (CART). A nonparametric approach based on product adaptive partitions is proposed, extending the Darbellay Vajda data-dependent partition algorithm. Finally, experimental evaluation within an automatic speech recognition (ASR) task shows that proposed solutions for the WP decomposition problem are consistent with well understood empirically determined acoustic features, and the derived feature representations yield competitive performances with respect to standard feature extraction techniques[5].

2.5 SPAF: Stateless FSA-Based Packet Filters

The stateless packet filtering technique based on finite-state automata (FSA). FSAs provide a comprehensive framework with well-defined composition operations that enable the generation of stateless filters from high-level specifications and their compilation into efficient executable code without resorting to various opportunistic optimization algorithms. In contrast with most traditional approaches, memory safety and termination can be enforced with minimal run-time overhead even in cyclic filters, thus enabling full parsing of complex protocols and supporting recursive encapsulation relationships [6].

2.6 Modeling Filtering Predicates Composition with Finite State Automata

Network virtualization has gained a lot of attention recently, because of some new interesting proposals in the field . This trend has had the effect of pushing some filtering operations up at the software level: i.e. extract a potentially large number of protocol fields from a packet, or dynamically combine different filters. The time constraints of working at line rate force the creation of a packet filter model that can guarantee the minimum number of packet checks. This poster proposes mpFSA, a packet filter model based on the Finite State Automata formalism,that aims at achieving optimality w.r.t. the number of packet accesses, without sacrificing efficiency and scalability [7].

2.7 Rule Pattern Parallelization of Packet Filters on Muti-Core Environments:

Packet filters are essential for most types of recent information network technologies. To achieve packet filters with high performance, flexibility, and cost-efficiency, the performance must be improved through multi-core processing and single instruction multiple data (SIMD) operations for software-based solutions on general-purpose CPUs. In this work, rule pattern parallelization for latency intensive filtering is investigated. Two types of rule pattern parallelization (range parallelization and modulo parallelization) are introduced and a performance model is analytically derived. Packet filter programs are implemented using range parallelization, modulo parallelization, and a hybrid of the two on two different hardware environments, i.e., the Cell and the Xeon cores [8].

2.8 CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment

Distributed Denial-of-Service attack (DDoS) is a major threat for cloud environment. In view of this challenge, a Confidence-Based Filtering method, named CBF, is investigated for cloud computing environment. Concretely speaking, the method is deployed by two periods, i.e., non-attack period and attack period. More specially, legitimate packets are collected at non-attack period, for extracting attribute pairs to generate a nominal profile. With the nominal profile, the CBF method is promoted by calculating the score of a particular packet at attack period, to determine whether to discard it or not. The result shows that CBF has a high [9].

2.9 Model-Based Tool-Assistance for Packet-Filter Design

The design of suitable packet-filters protecting subnets against network based attacks is usually difficult and error-prone. Therefore, tool assistance facilitate the design task and contribute to the correctness of the filters.i.e., the filters should be consistent with the other security mechanisms of the computer network, in particular with its access control schemes. Moreover, they should just enable the corresponding necessary traffic. This tool approach applies a three-layered model describing the access control and network topology aspects of the system on three levels of abstraction. Each lower layer refines its upper neighbour and is accompanied with access control models[10].

2.10 The BSD packet filter: a new architecture for user-level packet capture

The BSD Packet Filter (BPF) uses a new, register based filter evaluator that is up to 20 times faster than the original design. BPF also uses a straightforward buffering strategy. BSD Packet Filter, new kernel architecture for packet capture. BPF offers substantial performance improvement over existing packet capture facilities 10 to 150 times faster than Sun's NIT and 1.5 to 20 times faster than CSPF on the same hardware and traffic mix. The performance increase is the result of two architectural improvements:

1. BPF used a re-designed, register-based 'filter machine' that can be implemented efficiently on today's register based RISC CPU.
2. BPF used a simple, non-shared buffer model made possible by today's larger address spaces. The model is very efficient for the 'usual cases' of packet capture[11].

3. Conclusion

In this paper, various packet filtering models are discussed. Packet filtering in firewall technology is to block or pass packet based on packet characteristics. Depending on the application and knowledge about packet, one can choose the specific packet filter.

References

[1] Habtamu Abie , An Overview of Firewall Technologies, January 2000, Telektronikk Volume 96 No. 3-2000, pp.47-52 .

[2] Minho Sung, Jun Xu, IP Traceback-Based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks,IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, SEPTEMBER 2003.

[3] Hazem Hamed, Adel El-Atawy , On Dynamic Optimization of Packet Matching in High-Speed Firewall, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, OCTOBER 2006.

[4] Mohamed Othman, Mostafa Nikpour Kermanian, Detecting and preventing peer-to-peer connections by Linux iptables, 2008 IEEE.

[5]Jorge Silva, Shrikanth S. Narayanan, Discriminative Wavelet Packet Filter Bank Selection for Pattern Recognition, IEEE TRANSACTIONS ON SIGNAL PROCESSING, MAY 2009.

[6] Pierluigi Rolando, Riccardo Sisto, "SPAF: Stateless FSA-Based Packet Filters", IEEE/ACM TRANSACTIONS ON NETWORKING, FEBRUARY 2011.

[7] Marco Leogrande, Luigi Ciminiera , Modeling Filtering Predicates Composition with Finite State Automata, 2011 Seventh ACM/IEEE Symposium on Architectures for Networking and Communications Systems .

[8]Yoshiyuki Yamashita, Masato Tsuru, Rule Pattern Parallelization of Packet Filters on Muti-Core Environments, 2011 IEEE International Conference on High Performance Computing and Communications.

[9] Qi Chen, Wenmin Lin , Shui Yu, CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment, 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing.

[10] Ingo Luck , Christian Schafer,Model-Based Tool-Assistance for Packet-Filter Design, POLICY 2001, LNCS 1995, pp. 120-136, 2001.

[11] Steven McCanne ,Van Jacobson ,The BSD packet filter: a new architecture for user-level packet capture,1993 Winter USENIX conference, January 25–29, 1993, San Diego, CA.