International Journal on Recent Researches In Science, Engineering & Technology
(Division of Computer Science and Engineering)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

Volume 3, Issue 6
June 2015.

JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

HIGH SPEED DATA COMMUNICATION USING HYBRID FIREWALL TREE RULE (HFTR)

S.Sadasivam[1], K.S.Arun[2]
[1,2]Assistant Professor, Department of Computer Science and Engineering, Mahendra Engineering College, Mahendhirapuri, Namakkal District, Mallasamudram, Tamilnadu, India.

Abstract: Traditional firewalls to control network traffic, in both configuration and development phases are utilized by planned rules. Firewall Tree rule is proposed to earlier to overcome this problem. The Firewall Tree imperative announcements no conflicts inside rule set and works faster than conventional firewalls, the status of network connections utilizing hash function requests additional computational overhead. To reduce this overhead, proposed a Hybrid Firewall Tree Rule (HFTR) in the paper. Hybrid Firewall Tree rule and traditional planned-rule firewalls are improved by this hybrid method. GUIs of hybrid Firewall Tree rules are utilized to provide customers to produce conflict-free firewall rules and it classified a tree structure and expressed 'tree rules'. Tree rules are replaced into planned rules to facilitate distribute the value of being clash-free. In conclusion, in decision making, the planned rules are utilized to authenticate beside package header information. Rules have equivalent majority packages and altered the top locations during the core firewall. Mechanism concerned in hybrid firewall tree rule technique can develop the functional speed of a firewall.

Key Words: High Speed Firewall, Firewall, Computer Network, Network Security, Cloud Network, Hybrid Firewall Tree Rule (HFTR).

Introduction:

Firewall technology is a significant step toward securing our networks; the difficulty of managing firewall rule policy might limit the effectiveness of firewall security. When the filtering rules are defined, serious attention has to be given to interactions and rule relations in order to establish the proper rule ordering and guarantee correct security policy semantics. As the number of filtering rules enlarges, the complexity of creating a new rule or updating an existing one also increases. In this case, to initiate conflicting rules such as rules having the same filtering part but dissimilar achievements, one general rule shadowing another particular related rule, or correlated rules whose relative ordering determines different actions for the same packets. In addition, a characteristic large-scale enterprise network might engage hundreds of rules that might be written by dissimilar administrators in a variety of times [1]. This significantly increases the potential of anomalies (conflicts) in the firewall rules and makes the network more vulnerable.

To tackle the issues, innovatively proposed some kind of firewall called ‘Firewall Tree rule’. It has been verified the Firewall Tree rule assurances with no conflicts (e.g., no shadowed and redundant rules) in rule sets, along with it is more proficient in traffic development in evaluation through conventional planned rule firewalls. A stateful mechanism was proposed to improve the Firewall Tree rule with the ability of tracking the positions of network correlations. Evaluation of IPTABLES popular open source firewall [2], the stateful Firewall Tree rule is superior in terms of processing speed.

Complex hashing strategies are engaged in the strategy utilized in Firewall Tree rule and the IPTABLES. Hash function invoked at smallest amount in stateful Firewall Tree rule or else IPTABLES in strategy to authenticate every solitary packet travelling in the firewall. Incoming packet equivalents among first rule in a stateless firewall (e.g., IPTABLES in stateless mode), after that the firewall requires to conduct four packet header fields evaluations such as Source IP address, Destination IP address, Source Port and Destination Port.

Conventional stateless firewalls (e.g., IPTABLES in stateless mode) operate quickly and the rule conflict issue is major obstacle for improving firewall speed utilizing the rule sequence tuning. Firewall rule list frequently equivalence to rules and positioned at the bottom of the list. The last rule generated to deny all packets and cannot be shifted up to the top positions. Since, the rules conflicts may cause alter of firewall policy if it moved up. The paper involvements are exposed as follows.

- Propose a hybrid firewall tree rule (HFTR) takes improvements of both the Firewall Tree rule and stateless mechanism. The method guarantees no rule conflicts and high traffic processing speed. Frequently matched rule shifted to superior positions in the rule inventory automatically.
- A mathematical model computing the time utilization in the hybrid firewall and a mathematical model for computing the efficiency of data communication. The investigational outcomes illustrate an enhancement of the proposed HFTR firewall.
- Proposed HFTR implemented under a cloud environment. The investigational outcomes show the proposed hybrid firewall utilizing ‘automatic rule sorting’ outperform the ‘non-automatic rule sorting’ methods.

Related Works:

Earlier approaches to improve functional speed of firewalls can be classified into three types. First type, it focused on elimination and detection of rule clashes, redundant rules, to decrease the rule size of a firewall. It decreases memory space utilization and processing time on a firewall. Second type, it emphasized on developing firewalls with high performance hardware, such as implementing a firewall on Field Programmable Gate Array (FPGA) [3]. Third type, it focused on filtering mechanisms of firewalls such as converting firewall rules into a tree structure and it process packets faster than a traditional sequential rule list.

During the framework, rule conflicts can be categorized into two categories, the ones causing speed problems and other causing protection issues, respectively [4]. These rule clashes outcome from shadowed rules and redundant rules, also current significant impact on the performance of traditional firewalls.

A shadowed rule was protection issues on a traditional firewall. Rules blocking attack packets can be shadowed by several rules with superior priorities (i.e., positioned ahead of them) and may not be utilized through the firewall. It caused protection issues and weakens the firewall [5]. Redundant rules reduced the processing speed of a firewall. Shadowed rules and redundant rules cleaned from a firewall rule set to improve the functional speed of a firewall.

The rule conflicts were identified, Al-Shaer and Hamed [6] concerned the set theory in their work issued. The approach was mapped the innovative listed rules to a 'policy tree'. Conflicting rules and the type of conflicts were reported after discovery was absolute.

Trabelsi et al [7] recommended an analytical dynamic multilevel early packet filtering method to improve firewall performance. The technique utilized statistical splay tree filters and utilized traffic characteristics to reduce packet filtering time. Statistical splay tree filters reorganized along with the network traffic deviation upon certain threshold qualification (Chi–Square Test). It maintained the technique was quicker than traditional techniques since unwanted packets were rejected as untimely as feasible, and the mechanism could also be considered as a device protection mechanism against Denial-of-Service (DoS) attacks.

Hung et al [8] designed B-Tree enhanced the speed of categorizing and processing packets on firewall. Two-dimensional early packet rejection method based on the B-Tree. It described a core firewall procedure as the ‘Original Filter’, and generated method called ‘Early rejected filter’ [9]. It focused on preventing unnecessary packets and applied the 'Original Filter' reduced packets crossing to the core firewall method. The method decreased firewall processing time under DoS attacks. Normal network operations (without DoS attack), their 'Early rejected filter' method may increase firewall processing time.

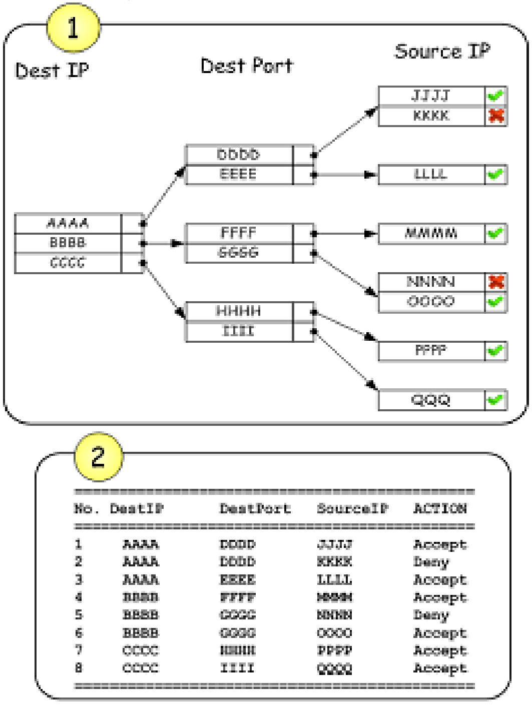
Firewall Tree rule not only categorized firewall rules in a tree organization, however also filters unnecessary packets with tree structured rules [10]. Firewall Tree rule first reads the related header fields from the packet. The value of the first header field evaluated with a firewall sub-rule stored in the root node of the tree. The firewall verified the header fields consecutively against the particular tree nodes at the equivalent levels. In conclusion, a subsequent accomplishment of an authorization or a denial of access to the network was taken on the packet. Packet header fields contained Destination IP address (Dest IP), Destination Port (Dest Port), and Source IP address (Source IP) are taken into account in the instance Tree rule.

Proposed System

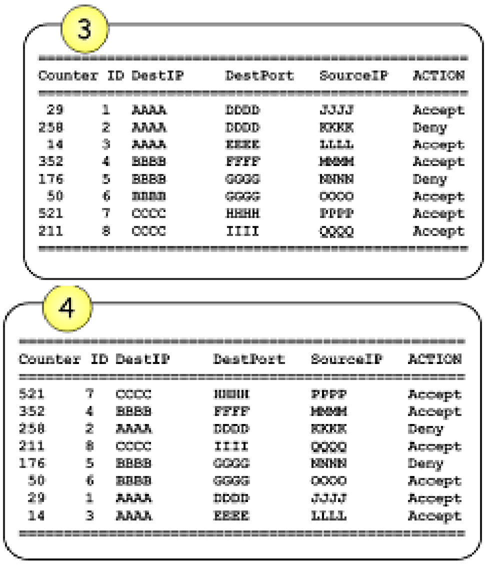
Propose a Hybrid Firewall Tree rule (HFTR) is an amalgamation of a firewall tree rule and a traditional firewall. Firewall Tree rule’s GUI accessible in previous work is utilized in the configuration stage to generate tree rules, which are translated to traditional clash-free listed rules. In decision making, an incoming packet is validated against the listed rules consecutively until a match is found. The traditional firewalls, hybrid firewall periodically re-arranges a sequence of rules. Every rule is separately moved to appropriate position with the amount of matches with the incoming packets. For illustration, the rule matching among the majority packages is optimizing the processing speed of the hybrid firewall with moved up to the top.

Methodology

Figure 1 shows the four stages engaged in the procedure of hybrid firewall tree rule approach. First, Figure 1-(1) shows a tree rule generated utilizing the GUI by a firewall rule designer. Generated tree rule is altered into planned rules as demonstrated Figure 1-(2). Planned rule is utilized in a core firewall for verifying the header fields of an incoming packet. The 'Counter' field illustrates in Figure 1-(3) evidences the amount of packages matched with every rule and primarily set to 0 for every rule. The 'Counter' of a rule enhances in a match among an incoming packet and the rule is validated. The counter resolutions rules are frequently matched and decrease the computational time. Regularly matched rule is displaced in the top of the list illustrated in Figure 1-(4). the counters of all the regulations will be rearranging to 0 while a pre-arranged ‘Time interval’ (e.g., 3 seconds) is accomplished. 'Time interval' is detailed by a firewall administrator.



```
==========================================================
No. DestIP        DestPort    SourceIP    ACTION
==========================================================
1     AAAA        DDDD        JJJJ        Accept
2     AAAA        DDDD        KKKK        Deny
3     AAAA        EEEE        LLLL        Accept
4     BBBB        FFFF        MMMM        Accept
5     BBBB        GGGG        NNNN        Deny
6     BBBB        GGGG        OOOO        Accept
7     CCCC        HHHH        PPPP        Accept
8     CCCC        IIII        QQQQ        Accept
==========================================================
```



```
================================================
Counter ID DestIP     DestPort   SourceIP   ACTION
================================================
  29     1  AAAA       DDDD       JJJJ       Accept
 258     2  AAAA       DDDD       KKKK       Deny
  14     3  AAAA       EEEE       LLLL       Accept
 352     4  BBBB       FFFF       MMMM       Accept
 176     5  BBBB       GGGG       NNNN       Deny
  50     6  BBBB       GGGG       OOOO       Accept
 521     7  CCCC       HHHH       PPPP       Accept
 211     8  CCCC       IIII       QQQQ       Accept
================================================
```

```
================================================
Counter ID DestIP     DestPort   SourceIP   ACTION
================================================
521      7  CCCC       HHHH       PPPP       Accept
352      4  BBBB       FFFF       MMMM       Accept
258      2  AAAA       DDDD       KKKK       Deny
211      8  CCCC       IIII       QQQQ       Accept
176      5  BBBB       GGGG       NNNN       Deny
 50      6  BBBB       GGGG       OOOO       Accept
 29      1  AAAA       DDDD       JJJJ       Accept
 14      3  AAAA       EEEE       LLLL       Accept
================================================
```

Figure.1. Proposed Scheme with Four Steps

Rule Reordering

The resolution for clash resolution is that all action constraints for clashing segments can be satisfied by reordering clashing rules. In clashing rules in order that satisfies all action limitations, this order must be the optimal solution for the clash resolution.

Data package

When clashes in a policy are resolved, the risk value of the resolved policy should be reduced and the availability of protected network should be improved comparing with the situation prior to clash resolution based on the threshold value data will be received in to the server.

Packet Space Segment

The major benefit of generating correlation groups for the anomaly analysis is that anomalies can be examined within each group independently, because all correlation groups are independent of each other. Especially, the searching space for reordering conflicting rules in clash resolution can be significantly lessened and the effectiveness of resolving clashes can be greatly improved.

Hybrid Firewall Tree rule

Firewall read attribute information from packet header and compare first packets attribute with data in the root node of Tree Rule. The firewall checks next packets attribute by searching only on relevant node. The package will be decided with specific action within a short time. The hybrid Firewall Tree rule will regard as DestIP (destination IP address), DestPort (destination port), and Source Port respectively until packets will be decided by a Predefined action. Data in every hub will be arranged in ascending order. Rule designers are not essential to have some talent. It need only basic concept of Firewall Tree rule designing.

Filtering Mechanism

The proposed method utilizes statistical splay tree filters that utilize traffic uniqueness to reduce packet filtering time. Discarded is early probable, and the mechanism could be considered as a device protection methodology against attacks. In the method decrease firewall processing time under DoS attacks. Normal network operations (without DoS attack), their ‘Early rejected filter’ method may increase firewall processing time.

Constraint Rule Generation

In a firewall policy are discovered and clash correlation groups are identified, the risk assessment for clashes is performed. The risk levels of clashes are in turn utilized for both automated and manual strategy selections. A basic idea of automated strategy selection is that a risk level of a clashing segment is used to directly determine the expected action taken for the network packets in the clashing segment.

Result and Discussion

The proposed HFTR techniques are deployed with Intel i6 Core processor, with 16 GB RAM, 60 GB Memory with Windows7 Ultimate operating systems. The method is developed in Java programming environment by utilizing NetBeans 8.0.2, MYSQL database 5.5, Java Remote Access Library with some peers in a centralized server infrastructure.

The proposed HFTR strategy is computed on different kinds of parameters to compute the effectiveness of strategies. The proposed HFTR strategy is highly dedicated to decreases processing time in validating packages with high speed data communication. The proposed HFTR method is calculated with following constraints such as Average Delay (AD), Energy Consumption (EC), and Throughput (T) performance estimation constraints.

Table 1 explains the Average Delay (AD), Energy Consumption (EC), and Throughput (T) for respective input constraints with previous methodologies. Table 1 shows the average value on all respective estimation matrix & input constraints with Ad hoc On-Demand Distance Vector (AODV) and R-Optimal Path (ROP) previous methodologies. Along with Table1, it noticed that proposed HFTR method performs well on all estimation matrix and input constraints contrast than previous methods.

Table.1 Comparison of Average Delay, Energy Consumption and Throughput

Algorithm	Average Delay (seconds)	Energy Consumption (%)	Throughput (%)
AODV	15	90	58.8
ROP	13	49	66.3
HFTR	9	18	93.8

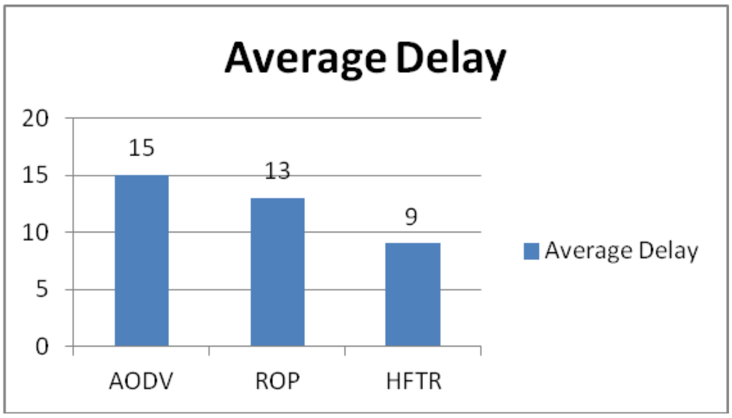


Figure.2 Comparison of Average Delay

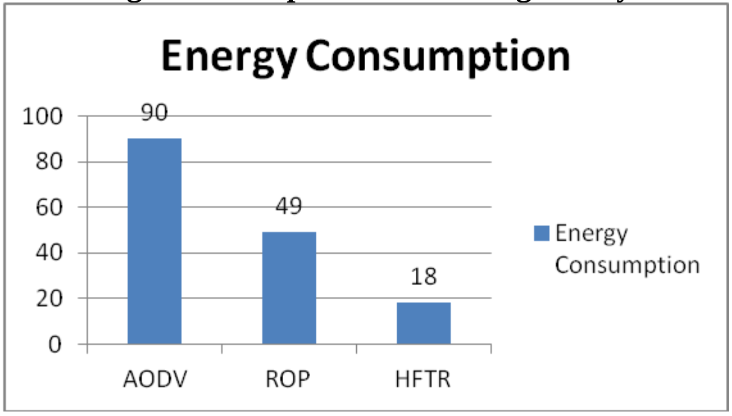


Figure.3 Comparison of Energy Consumption

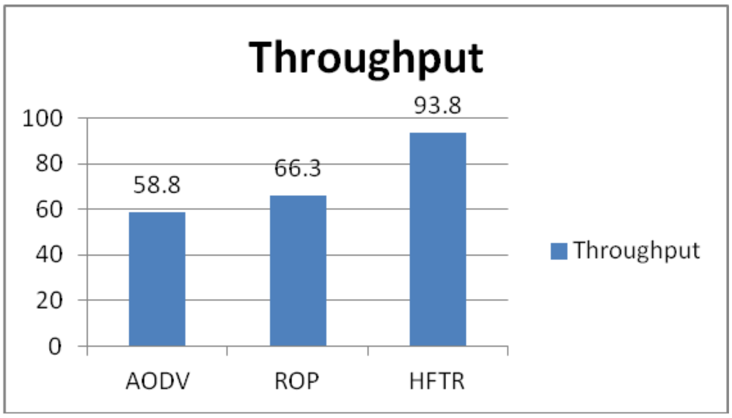


Figure.4 Comparison of throughput

According to Figure 2 to 4 explanations, the proposed HFTR strategy calculates average delay, energy consumption and throughput for discovering the efficiency. Proposed HFTR method evaluated with Ad hoc On-Demand Distance Vector (AODV) and R-Optimal Path (ROP) previous methods behalf of average delay, energy consumption and throughput. The proposed technique closest competitor is ROP on overall constraints. ROP technique enhanced data communication. It enhanced the performance of numerous business applications for data transmissions. However, ROP strategy failed to high speed data communication. Proposed HFTR strategy enhances the high speed data communication. Proposed HFTR decreases 4 seconds AD (Average Delay), 31% EC (Energy Consumption) and increases 27.5% T (Throughput). Finally, the paper claims the proposed HFTR method performs best on each estimation constraints & respective input variables.

Conclusion

Hybrid Firewall Tree Rule decreases processing time in validating packages. Proposed firewall applies the ideas of Firewall Tree rule in designing clash-free rules and the ideas of conventional firewall in decision making. Validating incoming network packets against clash-free planned rules contributes an extra protected and earlier processing firewall. Counters are initiated to investigate rules match with the majority packages. Rules are sorted the counters periodically, and regularly matched rules are shifted to the top positions. Time exhausted in rule matching can be decreased. Since, a match can found in the initial few rules. A mathematical method is demonstrating a relation among 'time use' for data transmitting and related issues, particularly 'time interval'. Computing an optimal 'time interval' with a mathematical evidence based on Calculus. Experiments have been conducted utilizing an implemented testbed for estimating the performance of proposed hybrid firewall on a large amount of data communications.

References:

[1]. H. Hamed, E. Al-Shaer, "Firewall policy advisor for anomaly detection and rule editing", in Proceedings of the IEEE/IFIP Integrated Management, IM, 2003, pp:17–30.

[2]. X. He, P. Nanda, T. Chomsiri, and "Limitation of listed-rule firewall" and the design of Tree-rule firewall, in: Proceedings of the 5th International Conference on Internet and Distributed Computing Systems, China, 2012, pp: 275–287.

[3]. X. He, T. Chomsiri, P. Nanda, Z. Tan, "Improving cloud network security using the Tree-rule firewall", Future Generation Computer Systems, Elsevier, 30 (2014) 116-126.

[4] T. Chomsiri, X. He, P. Nanda, Z. Tan, "A Stateful Mechanism for the Tree-rule Firewall", 2014 IEEE 13th International Conference on Trust Security and Privacy in Computing and Communications (TrustCom.2014), 2014: pp. 122-129.

[5]. T. Chomsiri, C. Pornavalai. "Firewall Policy Analyzing by Relational Algebra", In: proceeding of the 2004 International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), 2004, pp: 214-219.

[6]. E. Al-Shaer, H. Hamed, R. Boutaba, M. Hasan, "Conflict classification and analysis of distributed firewall policies, IEEE Journal on Selected Areas in Communications PP: 2069-2084, 2005.

[7]. L. Yuan, J. Mai, Z. Su, “FIREMAN: A toolkit for Firewall modeling and analysis”, In Proceedings of the 2006 IEEE Symposium on Security and Privacy, pp: 199-213, 2006.
[8]. W. Cheswick, S. Bellovin, A. Rubin, “Firewalls and Internet Security: repelling the wily hacker”, Addison Wesley Professional, 2003.
[9]. Xiang Wang, Yaxuan Qi, Jun Li, Weirong Jiang, Fong, and Jeffrey, “ParaSplit: a scalable architecture on FPGA for terabit packet classification”, In High Performance Interconnects (HOTI), 2012 IEEE 20th Annual Symposium on, pp: 1-8. 2012.
[10]. Cuixia, Guang Jin, Xianliang Jiang, and Ni, “A New Multi-tree and Dual Index based Firewall Optimization Algorithm”, TELKOMNIKA Indonesian Journal of Electrical Engineering 11, no. 5, pp: 2387-2393, 2013.