MEASURING THE EFFECTIVENESS AND EFFICIENCY OF RULE REORDERING ALGORITHM FOR POLICY CONFLICT

JANANI.M[#1], SUBRAMANIYASWAMY.V[#2] AND LAKSHMI.R.B[#3]

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING
SASTRA UNIVERSITY, THANJAVUR, TAMIL NADU, INDIA
jananimuruganandam@gmail.com[1], vsubramaniyaswamy@gmail.com[2] and rblakshmi90@gmail.com[3]

***Abstract-* Network security has acquired appreciable attention among business communities. Firewall act as a frontier defense and plays a significant role for establishing secure communication in networks against unauthorized traffic occurred in network. Firewall policies deployed in firewall, directs the firewalls to handle network traffic for particular IP addresses and protocols. Although deployment of firewall technology improves security in our network, managing firewall policies is a challengeable process due to the composite character of rules in firewall policy, on the other hand policy rules created by the system administrators face difficulty in resolving policy conflicts. To address all the aforementioned issues, we need effective firewall conflict management framework. In this effort, we propose efficacious framework to treat the policy conflict in firewalls based on risk assessment of conflicts. We identify the risk level of the policy conflict on the basis of vulnerability assessment in the secured network. Our major contribution in this paper involves the utilization of novel technique called Dynamic Rule Reordering that effectively optimizes the filtering policies in firewall. The proposed Rule reordering algorithm dynamically optimizes the conflicted rule reordering and leads to the accomplishment of most ideal solution for conflict resolution. We perform extensive evaluation and experiments to show the efficiency of our proposed rule reordering, which reorder the conflicted rules.**

Keywords – firewall policy, rule reordering, policy conflicts, anomaly management.

I. INTRODUCTION

Network security plays important role due to the increase of network attacks threats. It has gained much attention in research areas. Firewalls are network devices which act as an effective network barrier by enforcing an organization's security policy. In other words, firewall is a software or hardware device that enables the protection of network by refining untrusted and unwanted network traffic. It specifies a set of filtering rules termed as policy. Fig 1 shows the simple architecture of firewall, which utilizes two interfaces namely Trusted and Untrusted. It provides modest security. As determined in security policy, it routes or blocks the packets.

Typically these firewall policies are problematical and error prone. Plenty of high level languages are urbanized in literature to abridge the mission of determining the firewall policy as correctly and efficiently. Based on policy requirements, refining decision is carried out on a deposit of rules. When the firewall policy has been defined once, it is essential to test the specified firewall policies and determine the policy correctness.

The policy enforced by the firewall routes or prevents the network traffic based on policy rules. This firewall is placed among the internet and private network and facilitates all the packets pass through it. A firewall policy defined in the firewall identifies the packet as legitimate and illicit by a series of policy rules. The rules in the firewall policy are defined in the outline of condition and actions. The condition in a rule identifies the packet arrival whereas action in rule can be accepts or abandon and sometimes the mixture of both accepts and discards. A conflict occurs in firewall when the two rules overlap with each other. Managing firewall policies is a crucial task in policy management techniques. To improve the effectiveness of firewall security, we need an efficient policy management tools that the users can evaluate, filter and confirm the accurateness of written firewall filtering rules.

The correct security policy is guaranteed when proper rule reordering is established. Our work provides serious attention regarding the relationship and interactions between the rules to regulate the rule reordering. Whenever there exists huge increase in filtering rules, difficulty of modifying an existing rule or writing a new rule also increases. For instance, rule is said to be conflict when it has same filtering part but possesses different actions. Typically, many of the large scale networks involve hundred and thousands of rules which is recorded by various administrators in different times. The potential of conflicts (anomalies) in the policy rule of firewall is evidently increased by this scenario. Moreover, it increases the vulnerability of network.

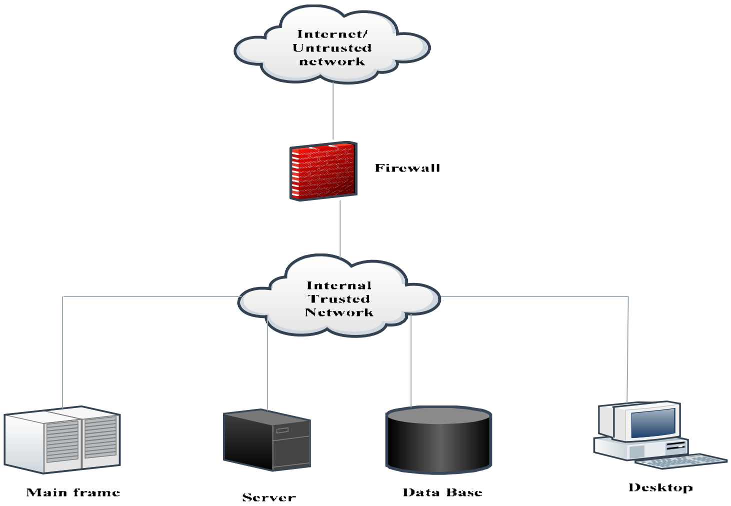


Fig. 1 Firewall architecture

Therefore, it is understandable that the firewall security attains significant efficiency when providing effective policy and conflict management technique. Proper anomaly management framework enables the network administrators to easily evaluate, filter and measure the appropriateness of firewall legacy rules, which is written. In this paper, we distinct a structure for firewall policy management that provide conflict detection and resolution techniques by identifying rule involved in conflicts and resolve the conflicts based on risk assessment values. Our proposed conflict resolution method acts as a flexible conflict resolution technique with respect to risk assessment. Our main contribution in this work aims to ultimately resolve the conflicts associated with specified action constraints by rule reordering. For that purpose, we introduce Dynamic rule reordering that reorders the conflicted rules which satisfies equivalent action constraints. Our proposed model is effortless and efficient to develop a conflict detection and resolution in firewall policy.

The rest of the paper is structured as follows: In section 2 we analysis the related works in existing literature based on the issues of managing firewall policies in a network. Section 3 describes our proposed framework for policy conflict resolution technique by exploiting rule reordering algorithm. Implementation and experimental results of our proposed work is depicted in section 4, then finally section 5 sums up the proposed work with some conclusion along with future perspectives.

II. RELATED WORK

This section gives basic definitions and describes the expressiveness of the underlying anomalies in firewall policies in the context of works related to firewall policy management.

The requirement of company is determined before deploying firewall into the company to protect its intranet. The company needs a system administrator to arrange, analyze and handle the firewall to identify the proper security policy needed by the company. To resolve the lacking of firewall security management, Bartal et al. presented a firewall management toolkit termed as Firmato [14]. This firewall security management toolkit attains significant improvement towards managing the firewall in complex and multi firewall environment. Similarly, Wool et al. introduced another firewall analysis tool like Fang and Lumeta which act upon modified queries lying on a place of filtering rules[7]. This tool extracts the more linked rules in the firewall security policy. These two firewall analysis tool also configure and managing firewalls in a very complex environment as like [14].

Typically, outsized endeavor network involves thousands of rules which valor be on paper by various administrator at different period. This criterion considerably increases the prospective of anomaly incidence inside the firewall policy which causes vulnerability related to the security of protected network [7]. To analyze and design the firewall policy management technique, managing rule relation like conflict identification and policy editing is more important. In topical years, a lot investigate work has been focused on firewall policy management. on the other hand, the best part of the effort present in that part, provided solution for universal policy administration slightly differ than firewall exact policies. Consequently, Lupu et al. organized and developed a possible firewall policy conflicts in role based management frameworks [8].

For any organizations, which are connected to the internet, firewalls play a fundamental role in security policy. Significantly, it is more important to properly manage and configure the firewall. It is very hard to understand the firewall configuration which is written in low level languages. For instance, rule ordering is often plays a vital role in conflict resolution strategy.

To aid the administrators in analyzing firewall policy and rules, Eronen et al. presented an expert system which answers the queries imposed by administrator about the permitted network traffic [10]. Particularly, this expert system lists the ports which are allowed on a given host. Another technique proposed in [3] presented an algorithm for automatic discovery of firewall policy anomalies. There are two goal focused in this technique. First one is the automatic discovery of firewall policy conflicts. This usual anomaly detection reveals the rule conflicts and important harms in inheritance firewalls. Next goal focused on rule insertion, modification and elimination to achieve conflict free policy. Firewall policy advisor tool is used to implement this technique in a user friendly environment. It significantly simplifies the organization of firewall policy and reduces the network vulnerability.

The typical firewall anomalies include shadowing, generalization, correlation, redundancy. A rule is said to be shadowed it performs different action but it matches the other rule. Two rules are correlated with one another, when the packet of first rule matches the second rule packets and vice versa. A rule is said to be the generalized, when the subsets of packets matched via the rule as well matched by the previous rule it facilitates different actions. A rule is said to be redundant, when there is another same rule holds the same action.

In [10], 2-tuple filtering rules are represented by the geometric model. This model is mainly designed to optimize the packet categorization in high speed networks but it is crucial to use this model for policy rule analysis in firewall. Hari et al. provide an algorithm for conflict discovery and resolution among general packet filters. This algorithm causes ambiguity in classification of packets [2].

To find the anomaly present in rule set, Mukkapati et al. proposed an alternative approach called Relational Algebra (RA) technique and Raining 2DBox Model[14]. This approach represents the anomaly in terms of two dimension box which contains the set of relations that are mapped from the rules.

To solve the conflicts like shadowing of rules and redundancy, Farouk et al. presented a novel algorithm called range algorithm which is deployed to obtain the most excellent crate for solving conflict and shadowing problems[5]. This range algorithm results conflict free rules. More traditional anomaly detection approaches have been proposed in [6] [13] but it prove inconsistency and is limited to detect pair wise redundancy.

III. PROPOSED METHODOLOGY

In this section we propose a Dynamic Rule Reordering algorithm. Furthermore, this section also describes the role and importance of resolving the conflicts in firewall policies. The overall flow of our proposed anomaly management is depicted in fig 2 and 6. The algorithm 1 shows our proposed detection and resolution technique for firewall anomaly.

A. FIREWALL POLICY ANOMALY DISCOVERY

When large number of various policy rules in firewall matches the similar packet in firewall policy then it leads to firewall policy conflicts (anomalies). Firewall policy comprises a repetition of policy rules that specify the desired actions, which is performed on packets. The format for specifying the rules in firewall policy is represented as <condition, action>. The term condition in a rule represents a collection of field to recognize a convinced kind of packets matched via this rule. Typically, action represents the equivalent actions performed on the matched packets in the policy rule. Action takes two values in the form of allow and deny. The values ‘allow’ routes the packets to enter into the firewall whereas values ‘deny’ leads not to allow the data packet into the firewall.

Incorrect security policy in firewall is obtained when some rule is screened by other rules or the incorrect assignment of relative rule ordering. In addition to that, whenever the filtering of rules in a security policy is increased then the potential of composing redundant or conflicting rules is also increased in relative manner. These policy conflicts create security problem like routing offensive traffic and also availability problem like denying legitimate traffic which consecutively affects the firewall performance. The number of possible firewall policy anomalies, which stimulate some of the policy rules that are suppressed by some other policy rules are enumerated as follows:

1) *Shadowing conflict:* – A policy rules in firewall is said to be shadowed when the rules available in preceding matches the packet which performs different action. This kind of anomaly causes the authorized traffic also to be immobilized. Hence, it is essential to identify and rectify the shadowed rule occurred in firewall policy.

2) *Correlation conflict:* – Two rules in firewall policy are correlated with one another, when the packet of first rule matches the second rule packets and vice versa.

3) *Generalization conflict:* **-** A firewall policy rule is said to be the generalized, when the subsets of packets corresponded by the rule as well correspond via the previous rule, it facilitates diverse actions.

4) *Redundancy conflict:* – A rule is said to be redundant, when there is another same rule holds the same action. Redundancy in the rule increases the space requirement and time required to search. Hence, it is essential to identify the redundancy between the rules and make the administrator modify its filtering effect.

B. POLICY ANOMALIES RESOLVING AND RULE REORDERING

Complex nature of firewall policy anomalies presented in the existing system pose a system administrator to face a challenging problem in resolving the conflicts. The configuration process in firewall is crucial and failure prone. Therefore, an effective mechanism and tool is needed for firewall policy management. We propose an effective conflict detection and resolution strategy that resolve the conflict based on risk value. Our proposed method identifies the anomalies by adopting rule based segmentation technique to identify the anomalies. We obtain the following benefits with respect to our proposed work:

1) *Conflict Resolution:* – In this strategy, conflicting segments are detected at earlier stage for conflict identification and rectification. The identified conflicting segments are associated with a set of conflicting rules and policy conflict. From the identified conflicting segments, correlation relationships are detected to derive the Correlation groups for conflict. Then we separately resolve the policy conflicts, which are situated in different conflict CG. During this correlation process, we sequentially reduce the searching space taken for resolving the conflicts exist in the policy.

2) *Action Constraint Generation:* – Using our proposed mechanism, each conflicting segment is assigned by action constraints. Allow or Deny are the two possible action constraints assigned for a conflicting segment. When any packet comes through the firewall, desired action should be taken within the conflicting segment by exploiting this action constraint. Once we identify the conflicts in a firewall policy, the task of risk assessment for conflicts is performed on firewall policy. On the basis of vulnerability assessment within the protected network, the risk (security) level is determined. When the value of risk assessment is maximum, then the imagined action should deny or block the data packets against the consideration for the security of network perimeters. In contrast when the value of risk assessment is minimum, then the imagined action be supposed to permits the data to flow through the firewall. Services provided by the network cannot be affected using this action constraint mechanism. Moreover, we can increase the resource avail and usage of network services.

3) *Rule Reordering:* – We introduce a novel Dynamic Rule Reordering technique to filter the policy rules in firewall. Our proposed technique deploys the skewness matching of firewall rules in order to enhance the performance of filtering.

C. PROPOSED CONFLICT MANAGEMENT FRAMEWORK

Proposed system divides the task of detecting and resolving the conflict in firewall policy into framework, which are enumerated as follows:

1) Rule Generation

The administrator generates a rule by giving rule name and various fields . Here we calculate the threshold value. Depending upon the threshold value, the action may be allow or deny. Here n numbers of administrators have inserted the policy in firewall.

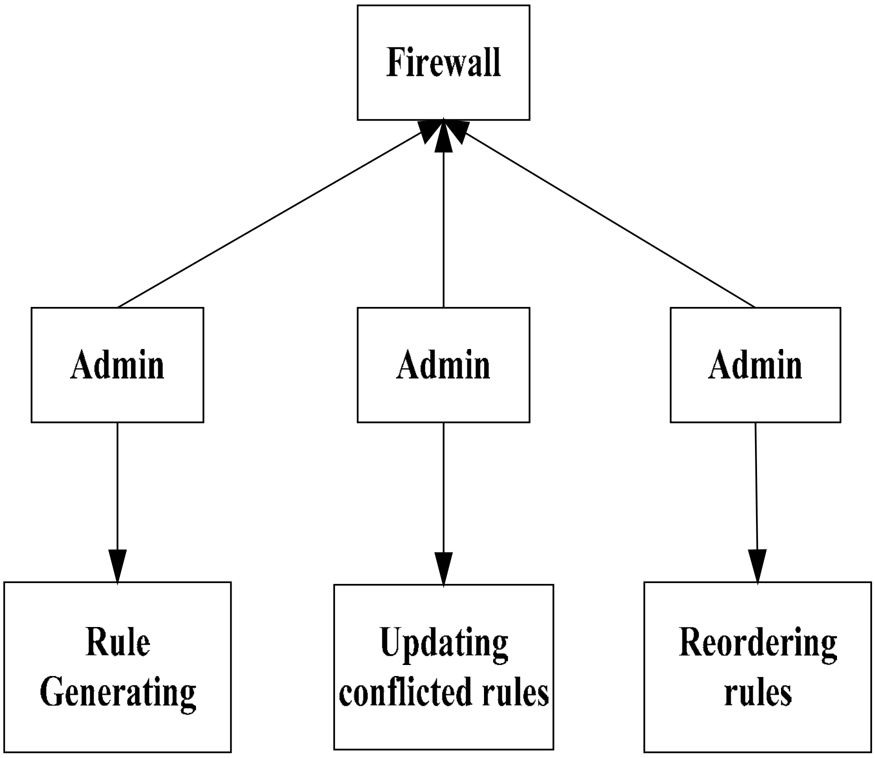
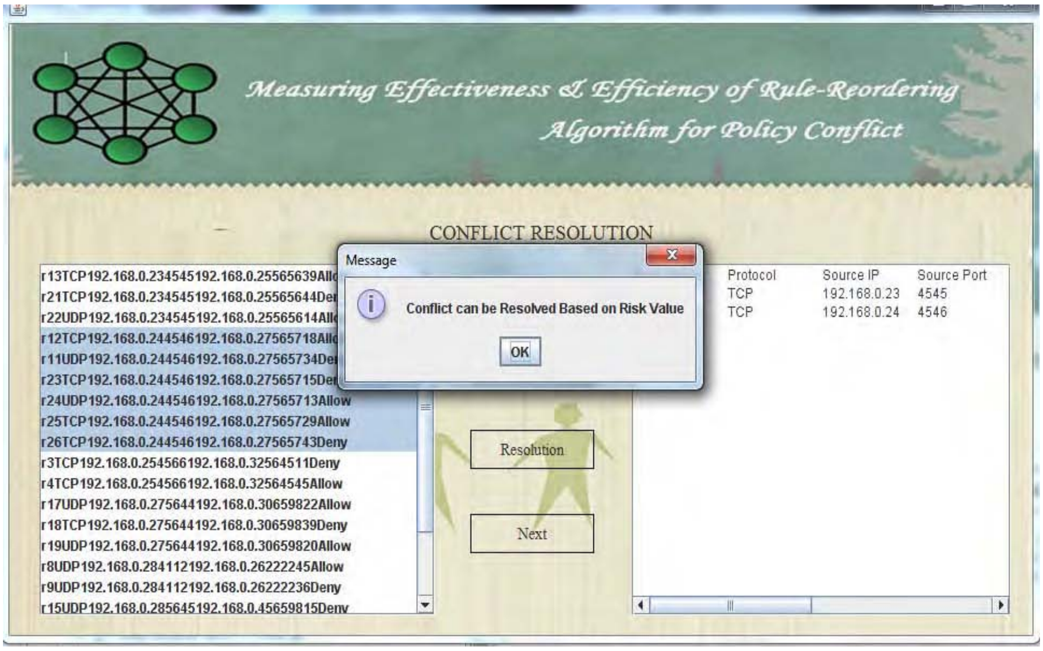


Fig .2 Administrator aspect in proposed system

2) Conflicted Rule Updating

There are various types of firewall policy anomalies. If there is any conflicted rule occurred in that means it will automatically updated.


Measuring Effectiveness & Efficiency of Rule-Reordering Algorithm for Policy Conflict
CONFLICT RESOLUTION
Message
OK
Resolution
Next

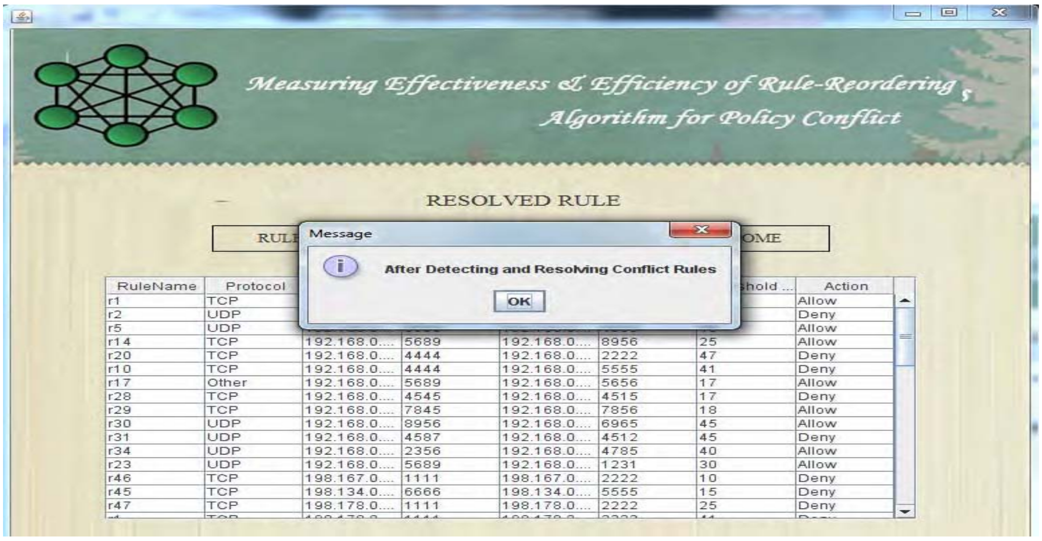
```
r13TCP192.168.0.234545192.168.0.25565639Allo
r21TCP192.168.0.234545192.168.0.25565644Der
r22UDP192.168.0.234545192.168.0.25565614Allo
r12TCP192.168.0.244546192.168.0.27565718Allo
r11UDP192.168.0.244546192.168.0.27565734Der
r23TCP192.168.0.244546192.168.0.27565715Der
r24UDP192.168.0.244546192.168.0.27565713Allow
r25TCP192.168.0.244546192.168.0.27565729Allow
r26TCP192.168.0.244546192.168.0.27565743Deny
r3TCP192.168.0.254566192.168.0.32564511Deny
r4TCP192.168.0.254566192.168.0.32564545Allow
r17UDP192.168.0.275644192.168.0.30659822Allow
r18TCP192.168.0.275644192.168.0.30659839Deny
r19UDP192.168.0.275644192.168.0.30659820Allow
r8UDP192.168.0.284112192.168.0.26222245Allow
r9UDP192.168.0.284112192.168.0.26222236Deny
r15UDP192.168.0.285645192.168.0.45659815Deny
```

Conflict can be Resolved Based on Risk Value

Protocol	Source IP	Source Port
TCP	192.168.0.23	4545
TCP	192.168.0.24	4546

Fig. 3 Representation of Conflicts can be Resolved Based on Risk Value

Fig 3 represents the conflicts can be resolved depending upon the value occurred in the risk assessment.



Measuring Effectiveness & Efficiency of Rule-Reordering Algorithm for Policy Conflict

RESOLVED RULE

Message

After Detecting and Resolving Conflict Rules

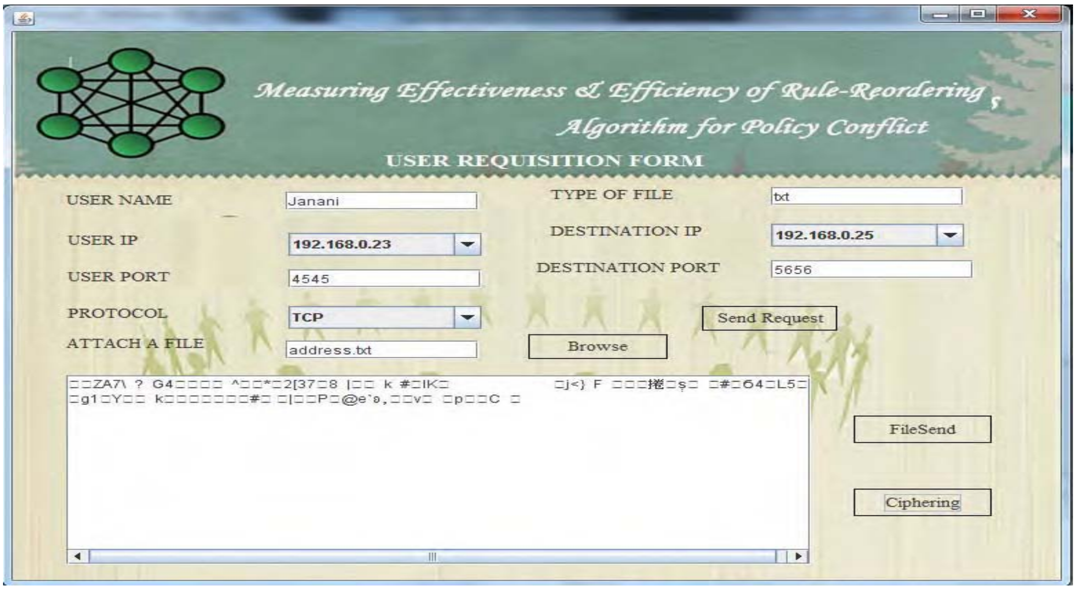
RuleName	Protocol					...shold ...	Action
r1	TCP						Allow
r2	UDP						Deny
r5	UDP						Allow
r14	TCP	192.168.0....	5689	192.168.0....	8956	25	Allow
r20	TCP	192.168.0....	4444	192.168.0....	2222	47	Deny
r10	TCP	192.168.0....	4444	192.168.0....	5555	41	Deny
r17	Other	192.168.0....	5689	192.168.0....	5656	17	Allow
r28	TCP	192.168.0....	4545	192.168.0....	4515	17	Deny
r29	TCP	192.168.0....	7845	192.168.0....	7856	18	Allow
r30	UDP	192.168.0....	8956	192.168.0....	6965	45	Allow
r31	UDP	192.168.0....	4587	192.168.0....	4512	45	Deny
r34	UDP	192.168.0....	2356	192.168.0....	4785	40	Allow
r23	UDP	192.168.0....	5689	192.168.0....	1231	30	Allow
r46	TCP	198.167.0....	1111	198.167.0....	2222	10	Deny
r45	TCP	198.134.0....	6666	198.134.0....	5555	15	Deny
r47	TCP	198.178.0....	1111	198.178.0....	2222	25	Deny

Fig. 4 Representation of firewall anomaly detection and resolution

Fig 4 shows the rules that are not conflicted. The conflicted rules can be detected and resolved by conflict resolution mechanism.

3) *File Transformation*

The file which should be going to transfer is chosen. Afterwards, the file is first encrypted and sends to the rule engine.



Measuring Effectiveness & Efficiency of Rule-Reordering Algorithm for Policy Conflict

USER REQUISITION FORM

USER NAME	Janani	TYPE OF FILE	txt
USER IP	192.168.0.23	DESTINATION IP	192.168.0.25
USER PORT	4545	DESTINATION PORT	5656
PROTOCOL	TCP		
ATTACH A FILE	address.txt		

```
□□ZA7\ ? G4□□□□□ ^□□*□2[37□8 |□□ k #□IK□         □j<} F □□□捲□ş□ □#□б4□L5□
□g1□Y□□ k□□□□□□□□#□ □|□□P□@e`ə,□□v□ □p□□C □
```

Fig. 5 Representation of encrypted file transformation

During the transformation the encrypted file only selected to broadcast the data. The file should be encrypted with regard to one of the firewall policy, and then it is selected for the transferring process.

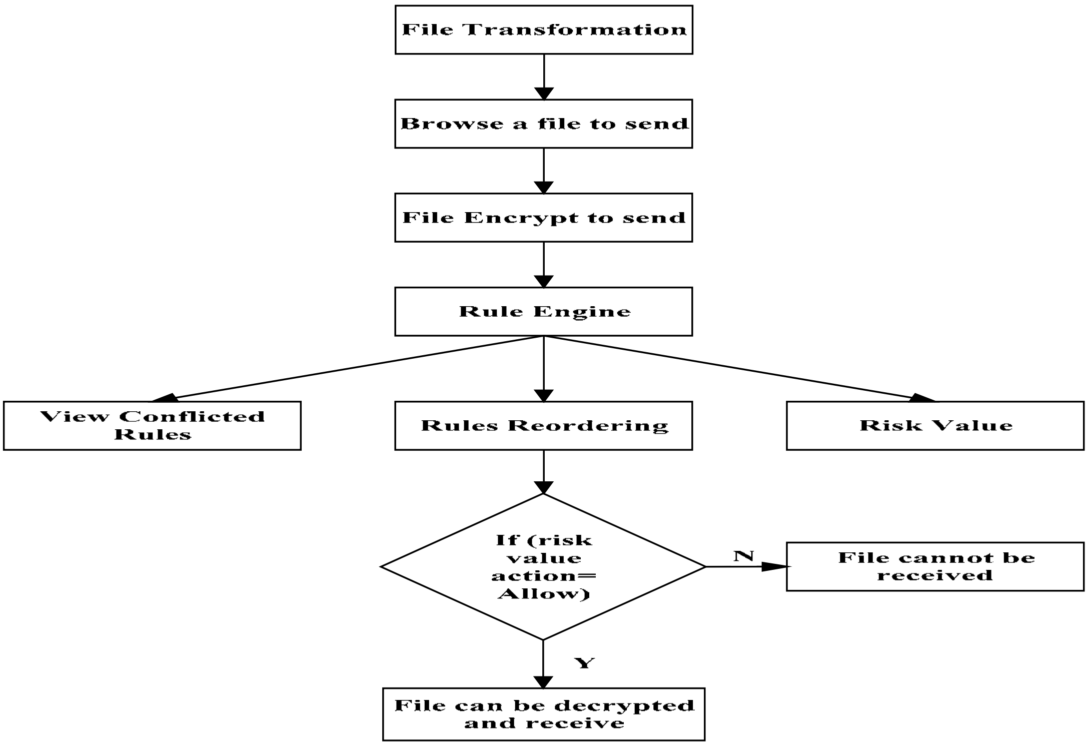


Fig. 6 End user aspect in proposed system

4) Rule Engine

Conflict resolution strategy obtains the most ideal solution only when all the action constraints for each conflicting segments is fulfilled by reordering the anomaly rules.

```
Algorithm: Detecting and Resolving firewall anomalies
Input: Set of Rule R, Set of Packet P
Begin
  Initialize NO: =5
  For each i=0 to R do
    $PCp_i$ interrogate with $RCr_i$;
    If $p_i$ matches $r_i$ >=5 then
      $RCr_i$ can be reordered
    Else If $p_i$ matches $r_i$ <5 then
      $RCr_i$ can't be reordered.
    End if
  End for
End
```

Algorithm.1 Dynamic Rule Reordering Algorithm

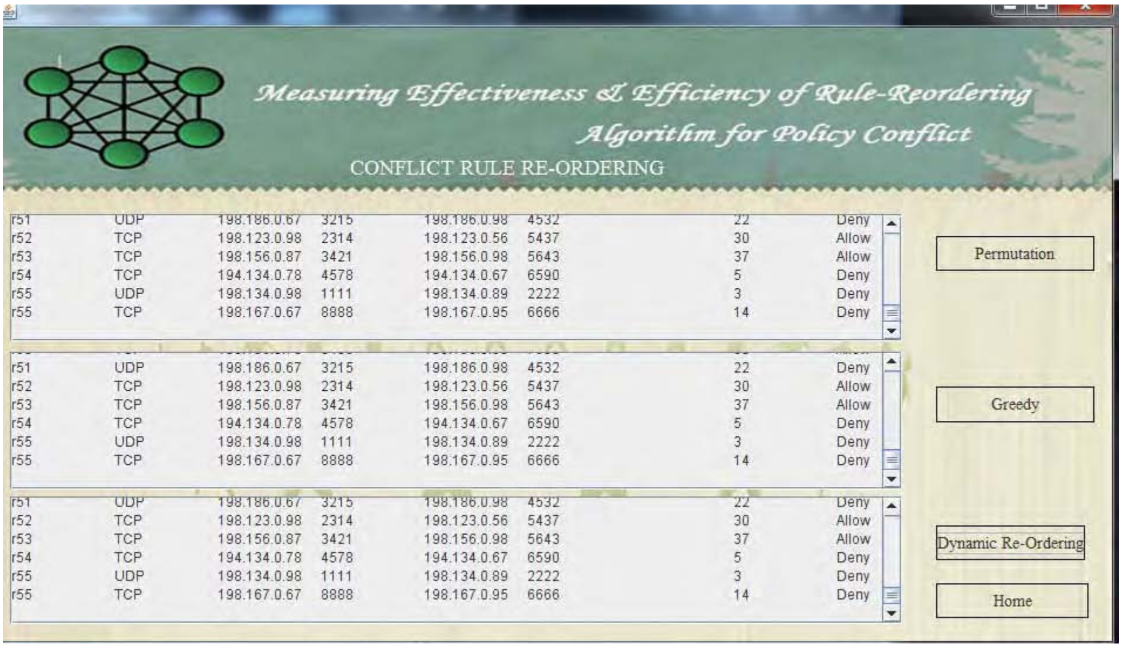
In conflict resolution, Reordering of conflict occurred rules which meet the expectations of all action constraints then this sort be the best resolution. Unluckily, put into practice action constraint for conflicting segments can merely be pleased partly in a little case.

D. MEASURING THE EFFECTIVENESS OF OUR PROPOSED RULE REORDERING

Existing system use a permutation algorithm to find an optimal solution that extensively finds the permutations of conflicting rules in correlated group. This algorithm exhaustively computes the resolving score of conflicted rules for all permutation. The computation is done by estimating the number of action constraints satisfied. The algorithm attains the best solution for a conflict resolution by the selection of permutation having greatest resolving score. However, the fundamental limitation of using this algorithm lies in computational complexity which is O (n!). For instance, our correlation scheme significantly reduces the search space but the number of conflicting rules present in correlation group is considerably huge which leads the existing permutation algorithm irrelevant.

Greedy is another conflict resolution algorithm, which creates the nearby best option at every phase in terms of ordering the rules. Like permutation algorithm, greedy algorithm individually computes the resolving score for every conflicting rule, which are available in a correlation group. The rule which contains the greatest resolving score is chosen to resolve the conflicts. For the selected rule, the position range with greatest resolution of conflict is determined and moving those selected rule to some other new position. Thus, accomplish the locally best elucidation for conflict resolution. In case of greedy algorithm, it is very crucial for resolving score computation.

To address above mentioned issue in greedy and permutation algorithm, we proposed a novel algorithm for rule reordering named as Dynamic Rule Reordering that effectively reorder the conflicted rules for optimal conflict resolution. Our proposed algorithm for conflict resolution makes the hope of finding the global optimal solution. Our proposed rule reordering scheme divides the filtering policy into two layers of rules like active rules and inactive rules. The top layer called active rule contains a tiny set of most active rules whereas another layer contains large set of inactive rules. Top layer performs the most packet matching and reorder the rules on the basis of traffic matching ratio which reduce the packet matching at overall rate. On the other hand, much less packet matching is performed by the second layer.


Measuring Effectiveness & Efficiency of Rule-Reordering
Algorithm for Policy Conflict
CONFLICT RULE RE-ORDERING
Permutation
Greedy
Dynamic Re-Ordering
Home

r51	UDP	198.186.0.67	3215	198.186.0.98	4532	22	Deny
r52	TCP	198.123.0.98	2314	198.123.0.56	5437	30	Allow
r53	TCP	198.156.0.87	3421	198.156.0.98	5643	37	Allow
r54	TCP	194.134.0.78	4578	194.134.0.67	6590	5	Deny
r55	UDP	198.134.0.98	1111	198.134.0.89	2222	3	Deny
r55	TCP	198.167.0.67	8888	198.167.0.95	6666	14	Deny

r51	UDP	198.186.0.67	3215	198.186.0.98	4532	22	Deny
r52	TCP	198.123.0.98	2314	198.123.0.56	5437	30	Allow
r53	TCP	198.156.0.87	3421	198.156.0.98	5643	37	Allow
r54	TCP	194.134.0.78	4578	194.134.0.67	6590	5	Deny
r55	UDP	198.134.0.98	1111	198.134.0.89	2222	3	Deny
r55	TCP	198.167.0.67	8888	198.167.0.95	6666	14	Deny

r51	UDP	198.186.0.67	3215	198.186.0.98	4532	22	Deny
r52	TCP	198.123.0.98	2314	198.123.0.56	5437	30	Allow
r53	TCP	198.156.0.87	3421	198.156.0.98	5643	37	Allow
r54	TCP	194.134.0.78	4578	194.134.0.67	6590	5	Deny
r55	UDP	198.134.0.98	1111	198.134.0.89	2222	3	Deny
r55	TCP	198.167.0.67	8888	198.167.0.95	6666	14	Deny

Fig. 7 Representation of Rule Reordering Algorithms

Fig 7 shows the rule reordering of three algorithms. After the conflicts are resolved the existing rules can be reordered.

IV. Experimental Results and Discussion

This section demonstrates how our proposed anomaly management framework works in terms of anomaly detection and resolution. For evaluation, we perform experiments with firewall policy. First, we generate firewall policy.

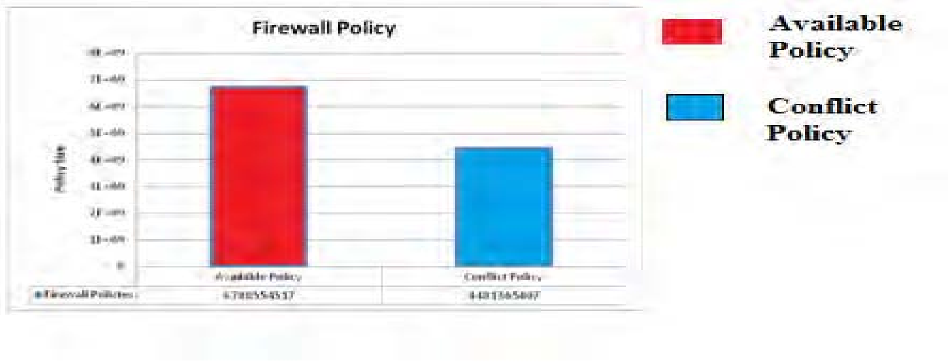


Fig. 8 Generated firewall policy

Then we explore the conflicted policies in firewall among those available policies as shown in fig 8.

Notice that different anomalies exist in firewall policy, which include shadowing of rules, Generalization, Correlated rules and redundant rules. The ratio of conflicted firewall policy along with anomaly types is illustrated in fig 9.

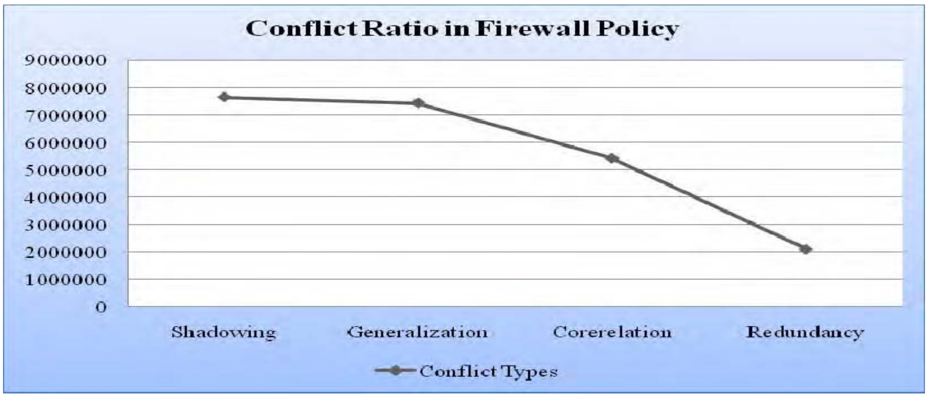


Fig. 9 Conflict ratio in firewall policy

Next we evaluate the time taken to resolve the policy conflicts and make a comparison with existing conflict resolution technique. Conflict resolution time is measured in terms of number of resolved conflicts. Our proposed framework resolves the policy conflicts for firewall in short duration of time and proves to be useful for the deployment in firewall technology. Resolving time for conflict policy compared with existing and proposed approach is shown in fig 10.

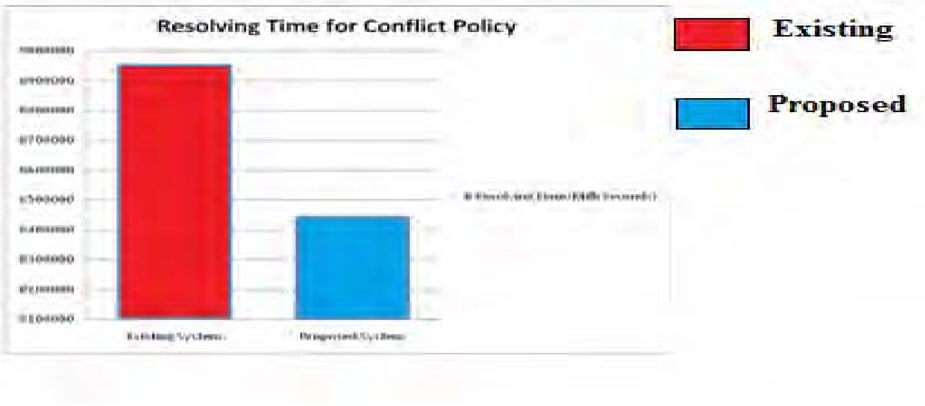


Fig. 10 Resolution time for conflict policy compared with existing vs. proposed

We enhance the firewall security by resolving conflicted policies. Rule reordering is performed to find out the optimal solution for the conflict resolution. For evaluation, we choose two existing rule reordering algorithm. We compare these two rule reordering algorithm with our newly devised Dynamic Rule Reordering algorithm. Optimization of firewall filtering rules aims to improve the firewall performance. Most of the existing conflicted policy filtering procedure exploits the features of only filtering rules, but our proposed algorithm for ordering the rules consider the behavior of optimization schemes. From the fig 10: It is seen that conflict resolution time taken by the existing approach is very high than our proposed framework. Our proposed approach achieves significant efficiency in resolving policy conflicts.

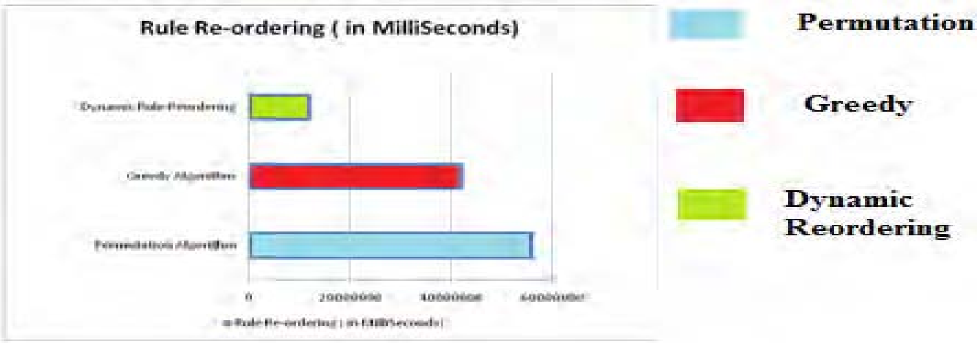


Fig. 11 Comparison of rule reordering with existing vs. proposed algorithm

The core objective of our proposed firewall policy management framework is that it adopts the combined algorithm and incorporates some features from various rule reordering algorithms like permutation, greedy and our Dynamic rule based reordering.

TABLE 1: COMPARISON OF EXISTING VS PROPOSED ALGORITHM

Permutation Algorithm	**Greedy Algorithm**	**DRRA**
The rules are ordered based on searching the permutation of conflicted rules within the correlated segment.	The rules are ordered based on the computation of resolving score for each conflicting rule within correlated segment.	Reorder the conflicted rules based on active and inactive rules.
High computational complexity.	It is crucial to compute the resolving score for each conflicted rule.	Less computational complexity and achieve global optimal solution in rule reordering.

Tabel 1 represents the comparison of existing and proposed algorithms. From that tabel DRRA algorithm is most efficient than other two algorithms.

We utilize the features of permutation and greedy whenever the number of conflicting rules is less. Otherwise, apply our proposed Dynamic Rule reordering algorithm to achieve efficiency in conflict resolution. Fig 11 shows that our proposed rule reordering algorithm reorder the conflicted rules at short duration.

V. CONCLUSION

A framework for the anomaly detection and resolution of firewall is proposed in this paper. To proficiently reorder the conflicted rules we introduced the dynamic rule reordering segmentation mechanism. By this way we reorder the conflicted rules and achieve the optimal solution for conflict resolution. The experimental results show that the proposed techniques detect and resolve the anomalies quickly than the existing technique. It also represents that the different type of anomaly nature exist in the firewall policy. This work fully concentrates on the risk value to determine the anomaly in the firewall. In future work, we extend our work by using the usability study to determine the anomaly.

REFERENCES

[1] A. Wool, "Architecting the lumeta firewall analyzer," in *Proceedings of the 10th USENIX Security Symposium.*, vol. 10, pp. 85-97, 2001.

[2] A. Hari, S. Suri, and G. Parulkar, "Detecting and resolving packet filter conflicts," in *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, pp. 1203-1212, 2000.

[3] E. S. Al-Shaer and H. H. Hamed, "Modeling and management of firewall policies," *Network and Service Management, IEEE Transactions on*, vol. 1, pp. 2-10, 2004.

[4] L. Yuan, H. Chen, J. Mai, C.-N. Chuah, Z. Su, and P. Mohapatra, "FIREMAN: A toolkit for firewall modeling and analysis," in *Security and Privacy, 2006 IEEE Symposium*, pp. 15, 2006.

[5] A. Farouk, H. N. Agiza, and E. Radwan, "Enhancement Misconfiguration Management of Network Security Components Using Range Algorithm," *IJCSNS*, vol. 9, p. 280, 2009.

[6] E. S. Al-Shaer and H. H. Hamed, "Firewall policy advisor for anomaly discovery and rule editing," in *Integrated Network Management, 2003. IFIP/IEEE Eighth International Symposium*, pp. 17-30, 2003.

[7] A. Mayer, A. Wool, and E. Ziskind, "Fang: A firewall analysis engine," in *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium*, pp. 177-187, 2000.

[8] E. Lupu and M. Sloman, "Conflict analysis for management policies," in *Proceedings of IFIP/IEEE International Symposium on Integrated Network Management (IM'1997)*, vol. 25, no. 6, pp. 852-869, Nov/Dec. 1999.

[9] D. Eppstein and S. Muthukrishnan, "Internet packet filter management and rectangle geometry," in *Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms*, pp. 827-835, 2001.

[10] P. Eronen and J. Zitting, "An expert system for analyzing firewall rules," in *Proceedings of the 6th Nordic Workshop on Secure IT Systems (NordSec 2001)*, pp. 100-107, 2001.

[11] E. S. Al-Shaer and H. H. Hamed, "Discovery of policy anomalies in distributed firewalls," in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, pp. 2605-2616, 2004.

[12] E. C. Lupu and M. Sloman, "Conflicts in policy-based distributed systems management," *Software Engineering, IEEE Transactions on*, vol. 25, pp. 852-869, 1999.

[13] Y. Bartal, A. Mayer, K. Nissim, and A. Wool, "Firmato: A novel firewall management toolkit," in *Security and Privacy, 1999. Proceedings of the 1999 IEEE Symposium*, pp. 17-31,1999.

[14] N. Mukkapati and C. V. Bhargavi, "Detecting Policy Anomalies in Firewalls by Relational Algebra and Raining 2D-Box Model," *International Journal of Soft Computing*, vol. 2, 2012.

[15] H. Hu, G. Ahn, and K. Kulkarni, "Anomaly Discovery and Resolution in Web Access Control Policies," *Proc. 16th ACM Symp. Access Control Models and Technologies, pp. 165-174, 2011.*

[16] R. Reeder, L. Bauer, L. Cranor, M. Reiter, K. Bacon, K. How, and H. Strong, "Expandable Grids for Visualizing and Authoring Computer Security Policies," *Proc. 26th Ann. SIGCHI Conf. Human Factors in Computing Systems*, pp. 1473-1482, 2008.

[17] A. Wool, "Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese," *IEEE Internet Computing*, vol. 14, no. 4, pp. 58-65, July/Aug. 2010.

[18] S. Ioannidis, A. Keromytis, S. Bellovin, and J. Smith, "Implementing a Distributed Firewall," *Proc. Seventh ACM Conf. Computer and Comm. Security*, p. 199, 2000.

[19] M. Frigault, L. Wang, A. Singhal, and S. Jajodia, "Measuring Network Security Using Dynamic Bayesian Network," *Proc. Fourth ACM Workshop Quality of Protection*, 2008.

[20] H.Hu, G.Ahn, and K.Kulkarni, "Detecting and Resolving Firewall Policy Anomalies", *IEEE Transactions on dependable and secure computing*, vol. 9, no. 3, MAY/JUNE 2012.