ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

Model for Strengthening Accuracy through Detection of Anomalous Firewall Policy Rules

Tawfiq SM. Barhoom[1], Emad KH. Elrayyes[2]

Associate Professor, Dept. of I.T., Faculty of Information Technology, Islamic Universityof Gaza, Gaza Strip, Palestine[1]

M.Sc. Student, Dept. of I.T., Faculty of Information Technology, Islamic Universityof Gaza, Gaza Strip, Palestine[2]

ABSTRACT: The firewall is a core technology that has an important role in the network security. However, managing firewall policy is an extremely complex task because the interactive rules in centralized or distributed firewalls significantly increase the possibility of policy mismanagement and network vulnerabilities. Therefore, the accuracy factor is crucial for managing policy rules by detecting the anomalies firewall policy rules .The lack of accuracy in the policy rules management leads to high risk for the network security. Therefore, we propose a model for strengthening of the accuracy in management and detection of the anomalous of firewall policy rules in small network security.

KEYWORDS: accuracy, anomalous, firewall, policy rules, mismanagement.

I. INTRODUCTION

A firewall is a network element that controls the traversal of packets across the boundaries of a secured network based on a specific security policy. A firewall policy rule is a list of ordered filtering rules that define the actions performed on matching packets. A rule is composed of filtering fields (also called network fields) such as protocol type, source IP address, destination IP address, source port and destination port, and a filter action field. Each network field could be a single value or range of values.

In the world of networks security, firewall policy rules is the first line of defense against external network attacks and threats, the management of firewall policy rules has been proven be complicated and error-prone for networked organizations. The task of manually managing, firewall policy rules becomes very difficult and time-consuming, if not impossible. One of the salient problems is that how much the rules are useful, up-to-dated. Therefore, these rules are in a constant need of updating, tuning and validating to optimize firewall security [1].

It is possible to use any field in IP, UDP or TCP headers in the rule filtering part, however, practical experience shows that the most commonly used matching fields are: protocol type, source IP address, source port, destination IP address and destination port. Some other fields are occasionally usefor specific filtering purposes [2][3].

The errors in the rule set is called anomalies that have to be detected and removed from rule set for the efficient working of any firewall. Five types of anomalies discovered and studied Namely, Shadowing Anomalies, Correlation Anomalies, Generalization Anomalies, Redundancy Anomalies, and Irrelevance Anomalies [4].

Filtering actions are either to accept, which allows the packet to be pass into or from the secure network, or to deny, which causes the packet to be discard. The packet is accept or deny, by a specific rule if the packet header information matches all the network fields of this rule. Otherwise, the next following rule is use to test the matching with his packet again. Similarly, this process is repeated until a matching rule is found or the default policy action is performed [5][6].

The size of the rule set varies according to the type of the organization. Generally, the rule set is very large because different network administrators often modify the policy rules according to their requirements. These changes could cause the occurrence of anomalies. Because of the large size of the rule set, it is difficult to detect anomalies by manually checking the rules one by one [10].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

A rule is define as a set of criteria and an action to perform when a packet matches the criteria. The criteria of a rule consist of the elements direction, protocol, source IP, source port, destination IP and destination port. Therefore, a complete rule may be define by the ordered direction, protocol, source IP, source port, destination IP, destination port, action,each attribute can be define as a range of values [7].

II. OVERVIEW OF THE ANOMALIES IN FIREWALL POLICY RULES

Several related work has categorized different types offirewall policy anomalies [8, 9] in table 1.

TABLE 1: Example of Different Types of Anomalies Firewall Policy Rules.

No.	Protocol	Source IP & Port		Destination IP & Port		Action
R1	UDP	10.1.2.0/24	All	172.32.1.0/24	53	DROP
R2	UDP	10.1.0.0/16	All	172.32.1.0/24	53	DROP
R3	TCP	10.1.0.0/24	All	192.168.0.0/16	25	ACCEPT
R4	TCP	10.1.1.0/24	All	192.168.1.0/24	25	DROP
R5	All	10.1.1.0/24	All	0.0.0.0/0	All	ACCEPT

1. Shadowing anomaly:

One or a set of preceding rules that match all the packets, which also match the shadowed rule, while they perform a different action, can shadow a rule. In this case, all the packets that one rule intends to deny (accept) can be accepted (denied) by previous rule(s), thus the shadowed rule will never be taken effect. For example, in table 2, R4 is shadow by R3 because R3 allows every TCP packet coming from any port of 10.1.1.0/24 to the port 25 of 192.168.1.0/24, which is supposed to be deny by R4.

TABLE 2: Example of Shadowing Anomaly.

R3	TCP	10.1.0.0/16	*	192.168.0.0/16	25	ACCEPT
R4	TCP	10.1.1.0/24	*	192.168.1.0/24	25	DROP

2. Generalization anomaly:

A rule is a generalization of one or a set of previous rules if a subset of the packets matched by this rule is also match by the preceding rule(s) but taking a different action. For example, R5 is a generalization of R4 in Table 3. These two rules indicate that all the packets from 10.1.1.0/24 are allow; except TCP packets from 10.1.1.0/24 to the port, 25 of 192.168.1.0/24 it is worth to be noted that generalization might not be an error.

TABLE3: Example of Generalization Anomaly.

R4	TCP	10.1.1.0/24	*	192.168.1.0/24	25	DROP
R5	*	10.1.1.0/24	*	0.0.0.0/0	*	ACCEPT

3. Correlation anomaly:

One rule is correlate with other rules, if a rule intersects with others but defines a different action. In this case, the packets matchby the intersection of those rules, may be permitted by one rule, but denied by others. For example, R4

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

correlates with R5, and all UDP packets coming from any port of 10.1.1.0/24 to the port 53 of 172.32.1.0/24 match the intersection of these rules. Since R2 is a preceding rule of R5, every packet within the intersection of these rules is deny by R2. However, if their positions are swap, the same packets will be allow.

TABLE 4: Example of Correlation Anomaly.

R2	UDP	10.1.0.0/16	*	172.32.1.0/24	53	DROP
R5	*	10.1.1.0/24	*	0.0.0.0/0	*	ACCEPT

4. Redundancy anomaly:

A rule is redundant if there is another same or more general rule available that has the same effect. For example, R1 is redundant with respect toR2 in table 5, since all UDP packets coming from any port of 10.1.2.0/24 to the port 53 of 172.32.1.0/24 matched with R1 can match R2 as well with the same action.

TABLE 5: Example ofRedundancy Anomaly.

R1	UDP	10.1.2.0/24	*	172.32.1.0/24	53	DROP
R2	UDP	10.1.0.0/16	*	172.32.1.0/24	53	DROP

5. Irrelevance anomaly:

A filtering rule in a firewall is irrelevant if this rule cannot match any traffic that might flow through this firewall. This situation exists when both of the source address and the destination address fields of the rule do not match any domain reachable through this firewall. In other words, the path between the source and destination addresses of this rule does not pass through the firewall. This rule has no effect on the filtering outcome of this firewall.

III. RELATED WORK

In this paper [8] the authors presented a set of techniques and algorithms that provide automatic discovery of firewall policy anomalies to reveal rule conflicts and potential problems in legacy firewalls, and anomaly-free policy editing for rule insertion, removal, and modification. They implemented a user-friendly tool called “Firewall Policy Advisor”. The Firewall Policy Advisor significantly simplifies the management of any generic firewall policy written as filtering rules, while minimizing network vulnerability due to firewall rule misconfiguration. . In this paper [11] the authors presented a novel anomaly management framework that facilitates systematic detection and resolution of firewall policy anomalies. A rule-based segmentation mechanism and a grid-based representation technique where introduced to achieve the goal of effective and efficient anomaly analysis. . In this paper [13] the authors presented an automated process for detecting and resolving such anomalies. This algorithm can be integrated into policy advisor and editing tools. The paper established the complete definition and analysis of the relations between rules. These techniques should be apply only after the rules free from anomaly by applying the algorithms. In this paper [4] the authors presented a modal logic, called Visibility Logic (VL), which can be used to express arbitrary patterns between rules inside a firewall. A model checker allows one to verify any formula expressed in visibility logic, of which traditional anomalies are merely particular instances, with running times of under one second for 1,500 rules. In this paper [14] the author proposed a novel methodology called rule-based segmentation technique to identify policy anomalies, which is articulated with a grid-based representation. It derives effective solutions to avoid anomalies by providing an intuitive cognitive sense about policy anomaly. In this paper [15] the authors proposed a formal

Language for specification of security policy in firewalls, Based on the language, the specified security policy, simple anomalies, total anomalies are translate to propositional logic formulas. Moreover, a tool based on theorem proving is design and implemented for detection of the anomalies in the specified policy. In this paper [16] the author proposed a system of four stages. The rule set Extractor stage generates policy rules for intra or inter firewall system. These

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

randomly generated or user defined rules will be checked by the anomaly detection algorithm in the Rule set Analyser stage. This stage generates the log file for the anomalies detected with the rule numbers and the corrective actions. User can edit the anomalous rules as guided by the analyser stage and a new anomaly free rule set can be achieve,The next stage is the rule set Updater stage, which defines the manual update done due to the policy changes in the organization. This update will again generate some anomalies since it is a manual process so the rule set is again given as input to the Rule set Analyser stage. In this paper [17] the authors presented a flexible algorithm that could be use even for the deployment of policies of very large size. The algorithm called “Enhanced Scanning Deployment”, have started by giving a simple deployment algorithm for an initial policy and target policy T that will allow us to correct the algorithm "scanning deployment". In this paper [18] the authors presented a set of techniques and algorithms, to analyse and manage firewall policy rules. (1) Data mining technique to deduce efficient firewall policy rules by mining its network traffic log based on its frequency. (2) Filtering-Rule Generalization (FRG) to reduce the number of policy rules by generalization and (3) a technique to identify any decaying rule, and a set of few dominant rules to generate a new set of efficient firewall policy rules as a result of these mechanisms. In this paper [19] the authors presented a framework for automatic testing of the firewall configuration enforcement using efficient and flexible policy and traffic generation. In a typical test session, a large set of different policies are generate based on the access-control list (ACL) grammar. According to custom profiles.

Finally, in several related works, the authors used two approaches, the first approach is data mining algorithm to detection the anomalies and the second approach is packets segmentation grid and so. In our model, we focus about accuracyin detection anomalies because we think the accuracy is main important factor in detection anomalies so our approach in detection is direct and searching algorithm with many steps in detection.

IV. PROPOSED MODEL

The main objective of this research is to develop a model for detecting and filtering the anomalies of firewall policy rules in small network in order to increase the accuracy in detecting these anomalies.

In our model proposal, the accuracy is main and important factor within created, our model for small network security through the detection of anomalous firewall policy rules, the accuracy in detection is the bottleneck and main issues in detection the anomalies. Therefore, we be careful in designing our model to be more accurate.

We divided our work for fourparts. The first part design and create real environment for experimental, the second part design and construction the model the third part the sequence function of the model the fourth part explain the sequence function of the model.

A. DESIGN AND CREATE REAL ENVIRONMENT FOR EXPERIMENTAL.

In first stage, we design and create real small network environment. The network have central firewall policy rules for control the traversal the packets in external and internal network. The network have many sub networks to use different levels of IP network to be more complicated in the managing, and this leads us to testing larger numbers of cases of anomalies and check the accuracy in detecting the anomalies the below Fig 1.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

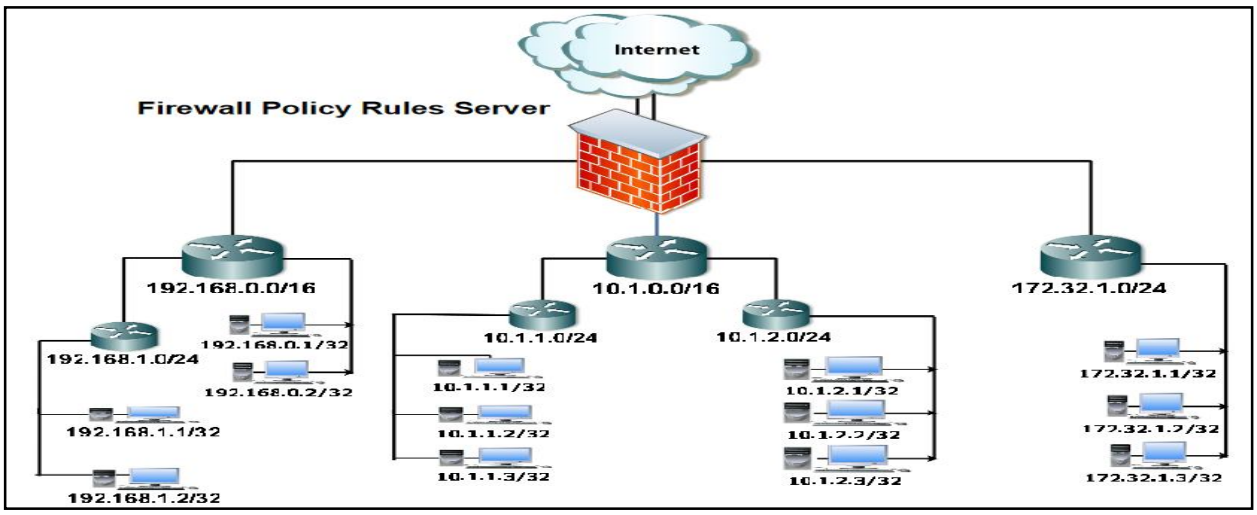

Figure 1: Proposal of Small Network Structure.

In table 6, we write some rules compatible with the previousnetwork and have many cases of four types of anomalies rules, such as Generalization Anomalies, Correlation Anomalies, Redundancy Anomalies and Shadowing Anomalies, to be ready to detection, and the anomalies.

Table 6: Example of Anomalies Firewall Policy Rules

No.	Protocol	Source IP And Port		Destination IP And Port		Action
R1	UDP	10.1.2.0/24	*	172.32.1.0/24	53	DROP
R2	UDP	10.1.0.0/16	*	172.32.1.0/24	53	DROP
R3	TCP	10.1.0.0/24	*	192.168.0.0/16	25	ACCEPT
R4	TCP	10.1.1.0/24	*	192.168.1.0/24	25	DROP
R5	All	10.1.1.0/24	*	0.0.0.0/0	*	ACCEPT

B. DESIGN AND CONSTRUCTION THE MODEL:

This research is devoted to the study of detecting the anomalous firewall policy rules using four kinds of anomalous rules. So, there is a need for a model design that have many processing steps for detecting and filtering the anomalous rules from a collection of dataset have anomalies and normal firewall policy rules. It is clear the proposal model in Figure 2, the research methodology consists as the following:

1. Design interface for rules reports and statistics.
2. Design constraints for any new policy rules entry into dataset.
3. Reprocessing all policy rules in standard format to be ready for processing.
4. Choosing some algorithms suitable for using in filtering anomalies process.
5. Design detection anomalies line between the new rules and the old rules of dataset.
6. Store all anomalies in independent dataset of the current result list of anomalies.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

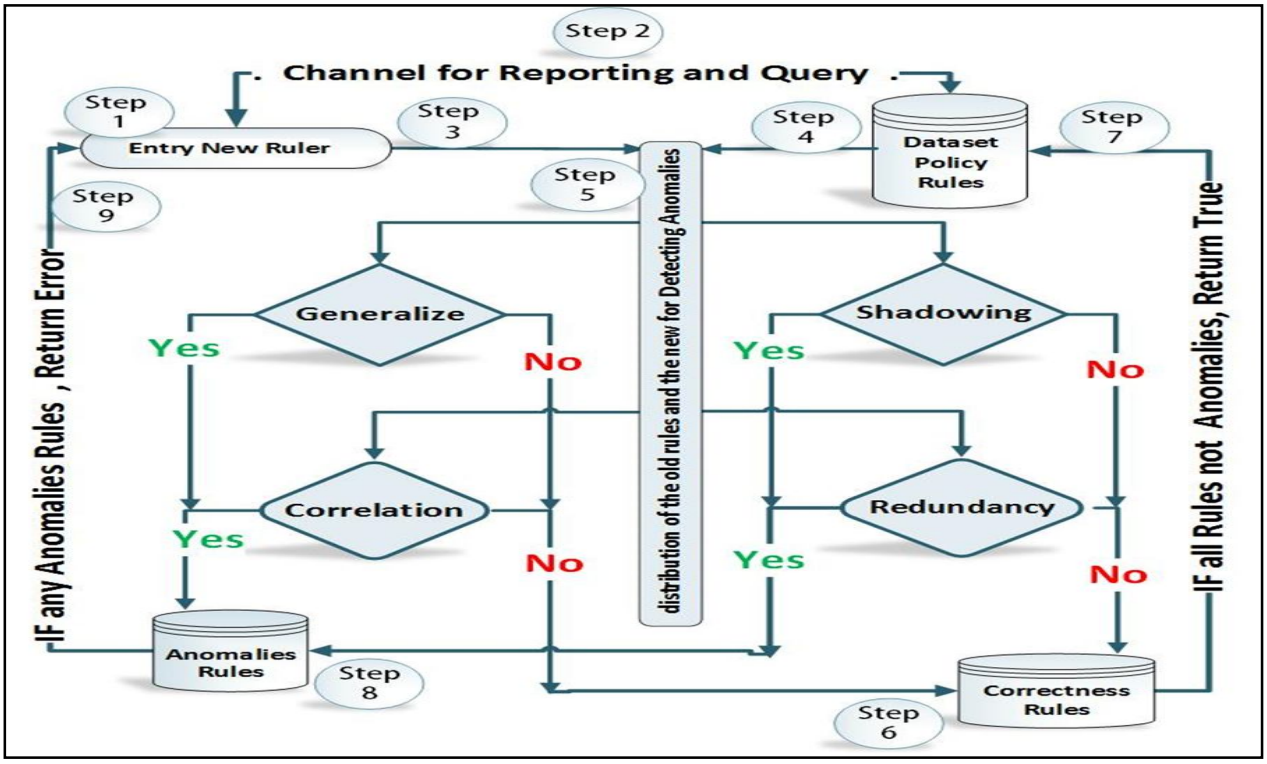

Figure 2 : Proposal Model for Detection Anomalies Firewall Rules

C. THE SEQUENCE FUNCTION OF THE MODEL:

Our model have many core functions to enhancement theaccuracy detecting the anomalies firewall policy rules.

1. Modify one or more new rules to check and detect the anomalies.
2. Submit query or search about old rules.
3. Share new rules to distribution process.
4. Share the current rules form dataset of firewall to distribution process.
5. Distribute and divide new and current rules to the four main parts to detect anomalies.
6. After detected all parts of anomalies detection process, if the new rule not have any anomalies with old rules store the new rules in dataset to preview and store.
7. Store all new rules into current rules dataset of firewall policy rules.
8. After finishing from all parts of anomalies detection, if the new rule have any anomalies with old rules store data set to preview.
9. Feedback from all new rules have anomalies to administrator.

V. IMPLEMENTATION OF THE MODEL

We use in implement our model, web application approach, because the web application is suitable can execution in any operating system, therefor we use language programming PHP CodeIgniter framework beside MVCtechnique, and use iptables firewall policy rules in processing detection.

Pseudo code of generalization anomalies:

1. (Action: new rule ≠ old rule) And ((Protocol: new rule = old rule) And (Source port: new rule = old rule))
2. Destination port: new rule = old rule ->In source IP or destination IP
3. Source and Destination IP (New rule subset in old rule (new rule ⊂ old rule) or (New rule < Old rule))

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

4. The new rule and old rules must be in the same class and all previous condition must be success.

Pseudo code of correlation anomalies:

1. Action: new rule ≠ old rule
2. (Protocol: new rule same old rule) And (Source port: new rule = old rule)
3. Destination port: new rule = old rule
4. Source IP: old rule ⊂ new rule
5. (Destination IP: new rule ⊂ old rule OR Source IP: new rule ⊂ old rule) And (Destination IP: old rule ⊂ new rule)
6. The new rule and old rules must be in the same class andall previous condition must be success.

Pseudo code of redundancy anomalies:

1. Action: new rule = old rule
2. (Protocol: new rule = old rule) And (Source port: new rule = old rule)
3. Destination port: new rule = old rule In source or destination
4. New rule subset in old rule (new rule ⊂ old rule)
5. Source and Destination IP (New rule <= Old rule)
6. The new rule and old rules must be in the same class andall previous condition must be success

Pseudo code of shadowing anomalies:

1. Action: new rule ≠ old rule
2. Protocol: new rule = old rule
3. Source port: new rule = old rule
4. Destination port: new rule = old rule
5. (Old rule subset in new rule (old rule ⊂ new rule)) And (Source IP and Destination IP (New rule >= Old rule))
6. The new rule and old rules must be in the same class andall previous condition must be success.

VI. EXPERIMENTAL RESULTS AND EVALUATION

In our experimental, we used collection data of firewall policy rules include four types of anomalies rules, such as, Shadowing, Generalization, Correlation and Redundancy anomalies rules. In addition, thecollection of anomalies were as follows inTable 7.

Table 7: Example of Firewall Policy Rules

No.	Protocol	Source IP & Port		Destination IP & Port		Action
R1	UDP	10.1.2.0/24	All	172.32.1.0/24	53	DROP
R2	UDP	10.1.0.0/16	All	172.32.1.0/24	53	DROP
R3	TCP	10.1.0.0/24	All	192.168.0.0/16	25	ACCEPT
R4	TCP	10.1.1.0/24	All	192.168.1.0/24	25	DROP
R5	All	10.1.1.0/24	All	0.0.0.0/0	All	ACCEPT

In evaluate the results of our model; No standard benchmark dataset is available to evaluate the research model. However, a mathematical equation commonly used in Figure 3.

$$\text{Accuracy factor} = \left(\frac{\text{The Total Detections Number Of Anomalies Firewall Policy Rules}}{\text{The Total Number Of Anomalies Firewall Policy Rules}} \right) \times \%100$$

Figure 3: Mathematical Equation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

As followinTable8, the last resultsexperiment in our mode in detection the anomalies firewall policy rules and here we use different collection data set of anomalies rules using mathematical equation in Figure 3, to try the model in detection of accuracy with all different types of anomalies firewall policy rules. For example: in step number one we used two numbers of all different types from anomalies rules, such as in table 7. The result was 100 in present, and in next step of experiment, we increase the number of anomalies as the following in the table 8. All results 100 in present in accuracy factor of detection anomalies firewall policy rules.

Table 8: The Resultsof Our Model in Detection Anomalies Firewall Policy Rules

Step No.	Shadowing No.	Generalization No.	Correlation No.	Redundancy No.	Results No.
1	2	2	2	2	%100
2	4	4	4	4	%100
3	8	8	8	8	%100
4	16	16	16	16	%100
5	32	32	32	32	%100

VII. CONCLUSION AND FUTURE WORK

In this paper, we have presented a model for detection the anomalies firewall policy rules, the model plays an important role in detection the anomalies firewall policy rules in network security, the main factor is the accuracy of detection. Moreover, the accuracy factor is very sensitive and important in detection operation; the model reduce the mismanagement through network administrator and minimize time and effort in finding and filtering the anomalies, the model help the administrators in managing and configuration. Detected in early about the anomalies before add any new rules in firewall policy rules. In future work we will design and create model for detection the anomalies firewall policy rules in network security have IP6.

ACKNOWLEDGMENT

We thanks to whose help us to complete this paper and we hope for this paper to be a good reference to another researches ,So we thanks the Ministry of Communications and Information Technology – Palestine, Eng. Nedal Safady and Eng. Fouad AbuAomirthe lap supervisor.

REFERENCES

1. Golnabi, K. , Min, R.K.; Khan, L.; Al-Shaer, E, “Analysis of Firewall Policy Rules Using Data Mining Techniques”, Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP, pp.305–315, 2006.
2. Al-Shaer,E.S. andHamed,H.H., "Modeling and Management of Firewall Policies" Network and Service Management, IEEE Transactions, Vol.1, Issue: 1, pp.2-10, 2008.
3. Selvakanmani S. “A Novel Management Framework for Policy Anomaly in Firewall” International Journal for Scientific Research & Development| Vol. 1,Issue 9, pp.1710-1715,2013.
4. Khorchani, B., Halle, S. and Villemaire, R. “Firewall anomaly detection with a model checker for visibility logic ” Network Operations and Management Symposium (NOMS), 2012 IEEE, pp.466-469,2012.
5. Y. Bartal, A. J. Mayer, K. Nissim, and A.Wool. Firmato, "A Novel Firewall Management Toolkit", In IEEE Symposium on Security and Privacy, pp.17-31, 1999.
6. E. Al-Shaer, H. Hamed, R. Boutaba, and M. Hasan, "Conflict classification and analysis of distributed firewall policies," IEEE Journal on Selected Areas in Communications, vol. 23, Issue: 10, pp. 2069-2084, 2005.
7. Abedin M, Nessa S and Khan L,” Detection and Resolution of Anomalies in Firewall Policy Rules”, IFIP International Federation for Information Processing, Vol. 4127, pp. 15-29, 2006.
8. Al-Shaer, E., Hamed, H., "Design and Implementation of Firewall Policy Advisor Tools", Technical Report CTI-techrep0801, School of Computer Science Telecommunications and Information Systems, DePaul University, 2002.
9. Hamed, H., Al-Shaer, E., “Taxonomy of conflicts in network security policies ", Communications Magazine, IEEE,Vol.44,Issue: 3, pp.134-141, 2006.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

10. Al-Shaer, E.E., Hamed, H.H., "Discovery of policy anomalies in distributed firewalls ", INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, vol.4, pp.2605-2616, 2004.
11. Hongxin Hu , Gail-JoonAhn and Ketan Kulkarni "Detecting and Resolving Firewall Policy Anomalies" , Dependable and Secure Computing, IEEE Transactions on ,Vol.9, pp. 318– 31, 2012.
12. Chaure R. and Shishir K. "Firewall anomalies detection and removal techniques – a survey "International Journal on Emerging Technologies, vol.1, pp.71-74, 2010.
13. Singh A., Chauhan A., Singh A.andHarnandan P." Detection and Resolution of Anomalies in Firewall Policy Rules", second National Conference in Intelligent Computing & Communication, 2008.
14. Srikanth B., Ramana S. "Firewall Policy Anomaly Detection and Resolution Using Rule Based Approach", International Journal of Innovative Research in Computer and Communication Engineering, Vol.1, pp.660-667, 2013.
15. Rezvani M. And Aryan R., "Specification, Analysis and Resolution of Anomalies in Firewall Security Policies", World Applied Sciences Journal 7 (Special Issue of Computer & IT), pp.188-198, 2009.
16. Chaure R, "An Implementation of Anomaly Detection Mechanism for Centralized and Distributed Firewalls", International Journal of Computer Applications, vol. 7, pp. 5-8, 2010.
17. Kartit A. and El Marraki M., "An enhanced algorithm for Firewall Policy Deployment", Multimedia Computing and Systems (ICMCS), 2011 International Conference,pp.1– 4, 2011.
18. Al-Shaer E, El-Atawy A, and Samak T, "Automated Pseudo-Live Testing of Firewall Configuration Enforcement", Selected Areas in Communications, IEEE Journal, Vol.27, Issue: 3, pp.302– 14, 2009.

BIOGRAPHY

Tawfiq SM. Barhoom: He is received his PhD from Shang Hai Jiao Tong University (SJTU) Shanghai – China; he is Associate Professor and now Dean of the Faculty of Information Technology in Islamic university of Gaza, Gaza Strip, Palestine. He have many researches in information security domain.

Emad KH. Elrayyes: Currently he is pursuing his M.Sc. in Information Technology from the Islamic university of Gaza, Gaza Strip, Palestine. He have Microsoft certified Trainer (MCT) in windows server, He holds global certifications, MCITP, MCTS, MCSE, MCTS, CIW and CCNA.