Expert Rules of Firewall: A Technique to Construct and Modified a Set of Rules

Koh May Fern and Sharipah Setapa

***Abstract*—Firewall always changing based on organizational policy and will make a respective person in charge of firewall take a long time to amend and verify the rule. The rule is applied to the firewall based on specific parameter. There can be many ways to create an order of rules, but it will be difficult and confusing to other person which will have to maintain it. One of the techniques is to utilize specific parameter as a main relationship which is traceable and can be expanded with specific pattern. If the parameter can be combined based on certain condition and this condition can incorporate in knowledge based as a library for a set relationship, which at the end can create a sequence of flow. This relationship will be recalled if the same condition happens again. In the knowledge based it also will contain a prediction based on common traffic which being used frequently. This concept will help and make easier to manipulate and monitor the rule correctly for multiple different location but using similar rules. It can be expanded to compliment other queries which using existing database firewall to check the queries before be permitted to access MySql database. In addition, the relationship also covers risk alert if the combination of low-risk port with medium-risk port creating a high-risk case.**

***Index Terms*—Rules, knowledge based, simplify, relationship.**

I. Introduction

Each organization has used firewall to protect malicious traffic from enteringinto the organization. Incoming and outgoing traffic is being configured through specific characteristic. There are different characteristic parameters reside in thefirewall packet such as port, protocol, source and destination. These characteristic can act as a rule to permit and block the traffic and can be used to predict the network traffic [1]. Each rule and can be expanded to other possible parameter to create a potential rules in order to increase and enhanced the firewall rule.

Rules will be written in a manner to suit with organization policy. A complex rule will impact the order of rule [2]. In large enterprise, network firewall becomes large and can end up causing the rule become complex. With a lack of a system to verify the created policies, the organization policy will behave unexpected [3].

With the support from traffic classification filtering such as stateful which can provide a flow and relationship [4] and combination model of stateful and stateless. In this combination stateful will analyses stateless packet in order to get some pattern analysis as well as create an empty stateless packet at the end [5]. Pattern which derived from the analysis can be manipulated to design another pattern for ease of use.

II. Problem

Based on IANA [6] there are three categories of port namely system port, user port and dynamic port. Well known port is between 0-1023 and usual port which be used as a service fall under this range. IANA will assign the port, port number and service name based on request which will be increased in future. Based on this situation, when the number of rules is increase the iptablesconfigurations in the serverwill be impacted. Hence, when number of ports to maintain is increase the total time required to process the relevant ports will be longer and indirectly leading to performance issue.The ordering of rule will need to modified and have to monitor carefully to avoid any mistake when configuremanually [7]. If similar rule has to be configured for multiple firewall as shown in Fig. 1 total of time incurred to maintain and update the ports will be longer in the long run.

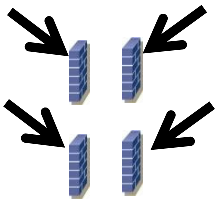


Fig. 1. Multiple firewall with almost similar rule.

This will impact to the performance of processing the traffic incoming and outgoing due torulewas added without proper ordering of common port which has similar relationship. As a result, this will create a security risk to the organization safety.

III. Proposed Solution

Knowledge based [8] will be designed by utilize specific parameter for traffic tracking and relationship. There are certain common ports which being used by users such as port 22 and port 80. Port 80 can be grouped with port 22 to make the rules ease to be monitored. Each common port as shown in table 1 can be generated as domain knowledge which useful for problem solving, processing and synchronize the traffic to read one main rule rather than to read each rule until it satisfy the condition which requested. At that time processing will increase and cause a delay. In order to create a domain knowledge, alist of port which be usually been used

Manuscript received June 16, 2014; revised August 17, 2014.

Koh May Fern is with TPM Development Operation Department, MIMOS Berhad, Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia (e-mail: koh.mf@mimos.my).

Sharipah Setapa is with Advanced Computing Lab Department, MIMOS Berhad, Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia (e-mail: sharipah@mimos.my).

DOI: 10.7763/IJIET.2015.V5.644

by user to access will be analysed in each traffic to identify the pattern.Once it is decide then a rule will be created based on usual port been used. This is to prevent from unusual port cannot be used as a loophole to attack and modify the rule.

TABLE I: COMMON PORT

Protocol	Port Number	Connection Type
TCP/UDP	21	FTP
TCP/UDP	22	SSH
TCP	23	TELNET
TCP	25	SMTP
TCP	79	FINGER
TCP/UDP	80	HTTP

If the traffic flow shows that frequency of user using port 22 and port 80 is very high then both the ports can be combined. It can be extended to different port if some relationship happens between. Rules will combine with port 80 for Hypertext Transfer Protocol.

Hence, based on the port which can be customized it can be stored in the knowledge based for reusable as shown in Fig. 2. Sets of firewall rules may contain one or more ports. All the ports are customizable based on user requirement and organization policy. Combination from sets of one or more rules will be stored in the knowledge based which can be shared for all firewall servers in the same organization.

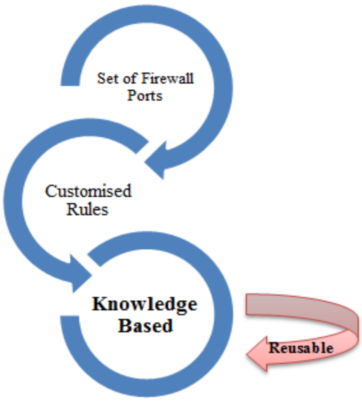


Fig. 2. Reusable knowledge based.

In the conventional architecture in an organization, user is required to create and maintain the iptablesconfiguration file by server basis. In the situation when there's 10 firewall server in the specific organization then there will be total of 10 iptablesconfiguration files to be created and maintained as shown in Fig. 3.

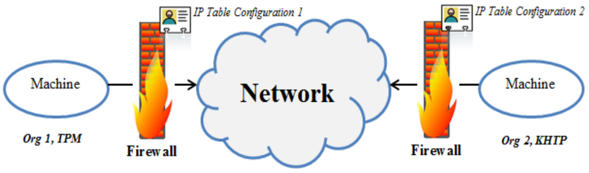


Fig. 3. Duplicate IP table configuration files (conventional).

If the rules are stored in knowledge based. One machine has a firewall to connect to other geographical side (e.g. Organisation 1 at TPM and Organisation 2 at KHTP). Multiple rules which have been use in different machine will be stored in knowledge based. Whenever there's a new maintenance of new set of rules will be automatically reflects in both the firewall as they are referring to the same source in the knowledge based as illustrated in Fig. 4. User is not required to maintain all theiptablesconfiguration files in the different servers.

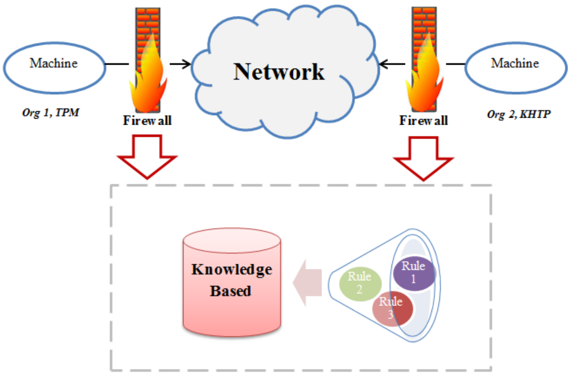


Fig. 4. Reusable knowledge based (new).

IV. METHDOLOGY AND MODEL RELATIONSHIP

A. Rules Type

Rulescan be categories with three types [9]. *Functional* only consider on port and no relationship with other port. This technique is straight forward and cannot be expanded. It is limited and cannot give flexibility if the organization has complex policy [10] as shown in Fig. 5. Port 80 can have a subset of other port which is 8080 and 8088.

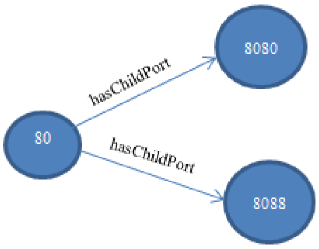


Fig. 5. Port 80 relationship with another port (functional).

For *symmetric*, in this case for port 80 as shown in Table II and Fig. 6 it can have a relationship or become a child port to another port. The relationship is to explain that when port 80 has Child port of port 8080, it is also explains that port 8080 has Parent port of 80.

TABLE II: SUBSET OF PORT 80 AND 21

Main Set	Sub Set
80	8080/8088
21	2121

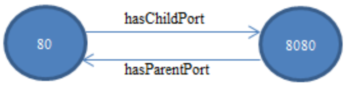


Fig. 6. Port 80 relationship with another port (symmetric).

This port can be expanded and not limited to port 8080 or 8088. If the port has frequently been used with different port, it can also be considered as a child to this port 80 as shown in Fig. 5.

Others choice for the rules are *transitive* method. This rules looks complex because it supports both different ports at the same time. When port 80 hasRelevantPort 8080 and port 8080 hasRelevantPort 8088. It's concluded that port 80 hasRelevantPort 8088. This set of rules is not obvious in the conventional iptables configuration and cannot be implemented in the conventional way. The transitive method added advantages when there're huge number of ports needed to be maintained in the firewall.

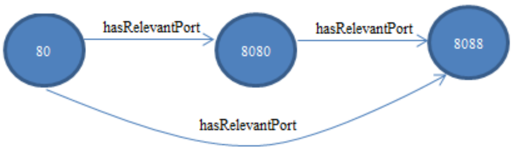
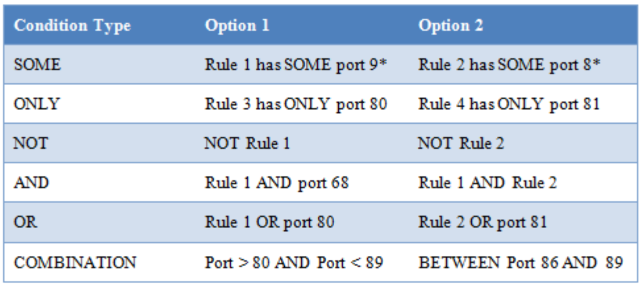


Fig. 7. Port 80 relationship with another port (transitive).

B. Conditions Type

Condition type [11] is being used to handle complicated rules as shown in Table III. The firewall ports illustrated are sampling which may and may not use in the current firewall ports configuration.

TABLE III: CONDITION TYPE AND OPTION RULE



Condition Type	Option 1	Option 2
SOME	Rule 1 has SOME port 9*	Rule 2 has SOME port 8*
ONLY	Rule 3 has ONLY port 80	Rule 4 has ONLY port 81
NOT	NOT Rule 1	NOT Rule 2
AND	Rule 1 AND port 68	Rule 1 AND Rule 2
OR	Rule 1 OR port 80	Rule 2 OR port 81
COMBINATION	Port > 80 AND Port < 89	BETWEEN Port 86 AND 89

Condition can be categories into six categories. For *SOME* condition, user can define the running number (limited to 0 – 9) with just an asterisk (*) as shown in Fig. 8 where Option 1 when Rule 1 has SOME port 9*, the ports covered is port 90 to port 99.

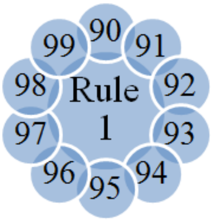


Fig. 8. Rule 1 has SOME port 9* (SOME).

For Option 2 refers to Rule 2 has SOME port 8*, the ports covered are port 80 to port 89 as shown in Fig. 9.

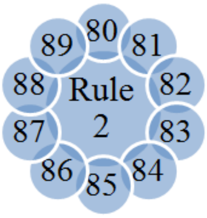


Fig. 9. Rule 2 has SOME port 8* (SOME).

The second type of condition is *ONLY*. For this condition, the required ports will be stored in the rules as shown in Fig. 10. Rule 3 contains only port 80 and Fig. 11 shown that Rule 4 contains only port 81.

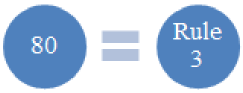


Fig. 10. Rule 3 has ONLY port 80 (only).

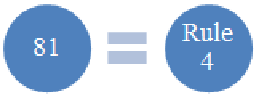


Fig. 11. Rule 4 has ONLY port 81 (only).

The next available condition is *NOT*. Exclusion can be done easily with this type when all rules are needed except certain rule. Fig. 12 illustrate Option 1 where NOT Rule 1 indirectly shows that Rule 2, Rule 3 and Rule 4 is applicable for this case.

Rule 2
+
Rule 3
+
Rule 4

Fig. 12. NOT Rule 1 (not).

Fig. 13 illustrate Option 2 where NOT Rule 2 indirectly shows that Rule 1, Rule 3 and Rule 4 is applicable for this case.

Rule 1
+
Rule 3
+
Rule 4

Fig. 13. NOT Rule 2 (not).

Other choice is the *AND* condition. For this condition, user can determine a set of rules with a list of port(s). Fig. 14 shows that Rule 1 and port 68 in which Rule 1 consist of a set of ports from 90 to 99. As a result the firewall ports for this condition is port 90, 91, 92, 93, 94, 95, 96, 97, 98, 99 and 68.

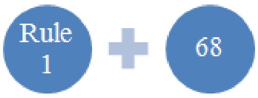


Fig. 14. Rule 1 and port 68 (and).

Fig. 15 shows that Rule 1 and Rule 2 in which Rule 1 is set of ports from 90 to 99. Rule 2 is set of ports from 80 to 89. As a result the firewall ports for this condition is port 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 80, 81, 82, 83, 84, 85, 86, 87, 88 and 89.

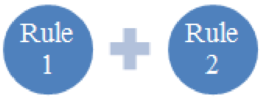


Fig. 15. Rule 1 and Rule 2 (and).

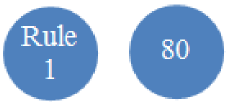


Fig. 16. Rule 1 OR port 80 (OR).

For *OR* condition, any port from the rules fulfill the requirement. Fig. 16 shows that either Rule 1 or port 80.

Fig. 17 shows that either Rule 2 or port 81.

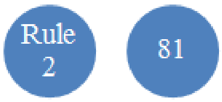


Fig. 17. Rule 2 OR port 81 (OR).

Last but not least is the most flexible type which allow user to manipulate the firewall ports easily namely the *COMBINATION* type as shown in Fig. 18. Condition where port is greater than 80 and less than 89.This particular condition explained that only port 81, 82, 83, 84, 85, 86 87 and 88 are required.

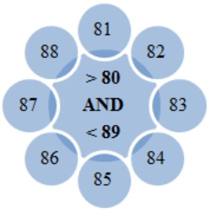


Fig.18. Port > 80 and port < 89 (combination).

The combination type also support the between phrase where as shown in Fig. 19. Where BETWEEN is introduced to cater the list of port in within the condition. For this option the relevant ports are port 87 and 88.

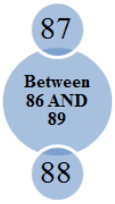


Fig.19. Between port 86 and 89 (combination).

Conditions are created based on user requirement which will be stored in knowledge based. User may configure the rules with condition to cater risk alert or risk management when open the list of high risk ports. When combination of list of low risk and medium risk port will results in creating high risk to the organization can be set as below:

LowRiskPorthasPorts A

MediumRiskPorthasPort B

(LowRiskPortAND MediumRiskPort) hasAlert 'HIGH RISK'

C. Knowledge and Combination of Extended Rules

Each respective firewall has some relationship with other firewall. This complexity will be directed into the knowledge based as shown in Fig. 20.

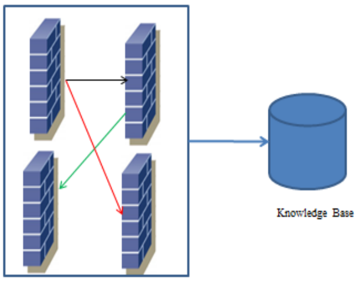


Fig. 20. Complexity firewall vs knowledge based.

This multiple firewall haveutilize the techniquesuch as packet filtering which involved port andusing relationship model it can be consolidated and store in knowledge based. Howeverin this situation rule based which been created do not have the ability to learn from experience [12]. The rule have to be modified whether it suit with the condition of the multiple firewall which overlap and have similar rule.

Each firewall have different iptables configuration based on organization policy which allow and block certain traffic.The parameters have to derive and design in a manner to generate an optimum which not overlaps with the other rule for ease of maintenance. At certain stage each packet filtering [13] has used similar parameter such as port to allow incoming and outgoing packetfor different type of service. Each iptables have some format as shown in Table IV where theport is one of the compulsory parameter.

TABLE IV: IPTABLE FORMAT

Protocol	Source	Port	Destination	Action

Domain expert of the knowledge based have to maintain and revise the rule if policy is being expanded to various type of protocol and destination as an example. This will impact the ordering of rule in each firewall and is one of the weaknesses in firewall optimization if the rule cannot synchronize accordingly.

V. DATABASE FIREWALL AND KNOWLEDGE BASED RULE

Database [14] firewall has been used in web applicationto protect backend database from been attacked. Our method usesknowledge basedwhich consistsof firewall rule and manipulate the packet filtering parameter such as port. This technique can be combined with the existing databasefor matching a factof MySql server which involved port 3306.In iptables the rule to open the connection been declared as below for incoming and outgoing packet respectively:

```
iptables –A INPUT –I lo –p tcp –dport 3306 –j ACCEPT
iptables –A OUTPUT –I lo –p tcp –sport 3306 –j ACCEPT
```

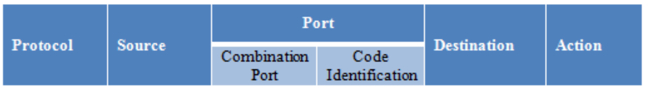
If anonymous user used host assessment tool to check which port is opened then this can be the first step to detect MySql serveris the server that been open and allowed by firewall. The identification of critical portsshould be block by returning error encounter when anonymous user trying to run hosts assessment tool. The availabilityof port issue which cause by given an error response perhaps can beone of the methods to reduce penetration of the server. This access will be opened for the specific user which identified by the backend and verified previously with code name been given. This will block anonymous user with invalid username to query the respective open port.

If the host did not response thenthe anonymous user will not proceed to penetrate the host. ICMP have used echo request and reply to know availability of host.In order to avoid the existing host been traced, some organization policy have block the ping command.A particular port can be blocked although it is opens in the initial stage when it fulfilled the rules condition. For example, when user try to access the list of ports that fall under combination of low and medium risk which resulting a high risk to the organization. System will trigger a risk alert to the server owner. Hence, the opportunity for the anonymous user to verified and get information on server will be decreased. Also, this will demotivate the anonymous user from go further to investigate the server.

This can be added together and complement existing database firewall which been used to analyzed query from client before forwarded to Mysql server for execution if the query is valid [15].

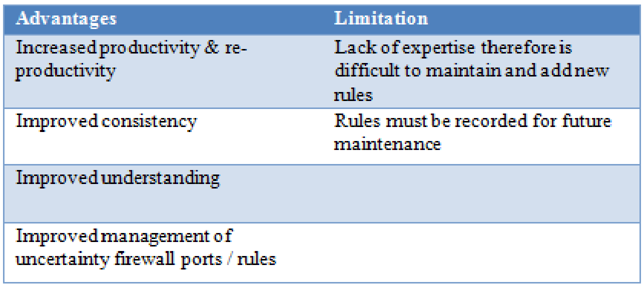
All the knowledge for specific organization need to maintain and update based on latest situation and traffic which allowed and block. If not it will outdated and the rule solution which suggested will not capable to handle the traffic. This knowledge rule have been summarize based on advantages and limitation asshown in Table VI.

TABLE V: EXTENDING PORT



Protocol	Source	Port		Destination	Action
		Combination Port	Code Identification		

TABLEVI: ADVANTAGE AND LIMITATION



Advantages	Limitation
Increased productivity & re-productivity	Lack of expertise therefore is difficult to maintain and add new rules
Improved consistency	Rules must be recorded for future maintenance
Improved understanding	
Improved management of uncertainty firewall ports / rules	

VI. RECOMMENDATION

Existing peer to peer connection [16] which was not effective using existing iptables can be handled using the extension of port technique. If well-known port is used as main relationship, then for internal peer to peer connection to be traced can be traced by knowing the main relationship which defined previously. If port A been used then for extended peer to peer it can be declared as port A.1, A.2, A.3……A.N. This will directed intranet traffic which is not allowed because it occupied high bandwidth and need to be blocked. If internal IP addresses have been used due to not enoughpublic to support devices then this situation can be further study for future use to maintain extension for devices which using internal IP.

Extended port of iptables can be considered as below.This format extension can be described as shown in Table V.

The port can be derived to be extended as below:

iptables –A INPUT –I lo –p tcp –dport 330+6[XXX9] –j ACCEPT

This can be achieved if eligible user have been identified to use the critical port by using specific table format to control the eligibility of user which accessing the MySql server. As an example for critical port such as 3306 a format will be design as below:

$$336 \underbrace{+ 0 \; [X}X9X]$$

This mean that a digit which 0 will put under third digit under digit 9 as a code for identification.Source and destination IP address can be easily spoofed [17] and with other alternative such as a port will make unauthorized user failure to access or manipulate the weakness of the existing firewall. With this simplify rules it can help to know which angle of firewall be utilize incorrectly by respective person who in charged the firewall. All the rules such as the code for identification are stored in the organization knowledge based.

VII. CONCLUSION

Manual update of multiple iptables is prone to error and increased the processing time. It also will create a loophole which benefits the intruder.One of the techniques to overcome the weakness is introducing theknowledge based firewallrules which are one of the techniques to simplifyand combined all similarrules. Repetition rules which using port as main relation at the end will reduce processing of the traffic in large enterprise.This technique can be expanded to various parameterswith port as the main umbrella of relationship between different firewall schemes. With the availability of rules type and rules condition, it facilitates the user with the flexibility of creating customized firewall policy based on their needs in a manner where by the rules only can be recognized by the organization authorized users.Last but not least, organization shall create the rules type and identify the pattern which is high risk with the help of the rule condition.

REFERENCES

[1] U. Mustafa, M. M. Masud, and Z. Trabelsi, “Firewall Performance Optimization Using Data Mining Techniques,” in *Proc. 9th International Wireless Communications and Molbile Computing Conference (IWCMC)*, pp. 934-90, July 1-5, 2013.

[2] B. Khan and M. K. Khan, “Security Analysis of firewall rules sets in computer networks,” in *Proc. Fourth International Conference on Emerging Security Information, Systems and Technologies*, pp. 51-56, July18-25, 2010.

[3] A. X. Liu, “Formal verification of firewall policies,” in *Proc. International Conference Communications*, pp. 1494-1498, 2008.

[4] R. Patel, “Stateful vs.stateless traffic analysis,” presented at IIC-China/ESC-China, 2002.

[5] M. G. Gouda and A. X. Liu, “A model of stateful firewalls and its properties,” presented at the 2005 International Conference on Dependable Systems and Networks (DSN’05), 2005.

[6] IANA. Service Name and transport protocl port number registry. [Online]. Available: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml,02.05.014

[7] A.-S. Ehab and D. Paul, “Managing firewall and network-edge security policies,” presented at Symposium on Network Operations and Management, April 23-23, 2004.

[8] J. Mathias, B. Neumann, Y. Vassiliou, and W. Wahlster, “KBMS requirements for knowledge-based systems,” *Foundations of Knowledge Base Management: Contributions from Logic, Databases, and Artificial Intelligence Applications*, pp. 391-394, 1989.

[9] Primer. W3C. [Online]. Available: http://www.w3.org/2007/OWL/wiki/Primer

[10] W3C. (February 10, 2004). OWL Web Ontology Language Overview. *W3C Recommendation*. [Online]. Available: http://www.w3.org/TR/2004/REC-owl-features-20040210/#

[11] T. R. Gruber, “Toward principles for the design of ontologies used for knowledge sharing,” *International Journal of Human-Computer Studies*, vol. 43, no. 5-6, pp. 907-928, 1995.

[12] J.-H. Sun, H. Chen, and C.-M. Niu, “A New Database Firewall based on anomaly detection,” presented at 11th International Conference on Parallel and Distributed Computing, Application and Technologies.

[13] U. Thakar, L. Purohit, and A. Pahade, “An approach to improve performance of a packet – filtering firewall,” in *Proc. Ninth International Conference on Wireless and Optical Communications Networks (WOCN)*, pp. 1-5, Sept. 20-22, 2012.

[14] S. Krishna, *Introduction to Database and Knowledge-Base Systems*, Singapore: World Scientific Publishing, ISBN 981-02-0619-4.

[15] Y. P. Yang, H. K. Yu, Y. H. Che, and Y. Kang, “Design of distributed firewall based on keynote in campus network,” presented at International Conference on Test and Measurement, 2009.

[16] M. Othman and M. N. kermaniam, “Detecting and preventing peer-to-peer connections by Linux iptables.”

[17] Y.-W. Liang and W.-J. Deng, “Verify consistency between security policy and firewall policy with answer set programming,” in *Proc. International Conference on Computer Science and Software Engineering*, vol. 1, pp. 196-200, 2008.

Koh May Fern has received her bachelor degree of business information system from Campbell University in 2001. She has almost 5 years experience in the area of semantic knowledge management. She is currently working in MIMOS Berhad.

Sharipah Setapa has received her bachelor degree in computer and communication engineering from Universiti Sains Malaysia (USM), Malaysia in 1991 and master in information technology from National Universiti Malaysia (UKM) in 2013. She has almost 10 years experience in the area of security. She is currently working in MIMOS Berhad.