International Journal of Security and Its Applications
Vol. 9, No. 5 (2015), pp. 153-162
http://dx.doi.org/10.14257/ijsia.2015.9.5.16

The Research and Application of Multi-Firewall Technology in Enterprise Network Security

Jing Li

College of Information Engineering, Qingdao University, Qingdao Shandong 266071, China
E-mail: lijinglunwen@yeah.net

Abstract

A firewall's complexity is known to increase with the size of its rule set. Empirical studies show that as the rule set grows larger, the number of configuration errors on a firewall increases sharply, while the performance of the firewall degrades. When designing a security-sensitive network, it is critical to construct the network topology and its routing structure carefully in order to reduce the multi-firewall rule sets, which helps lower the chance of security loopholes and prevent performance bottleneck. This paper studies the problems of how to place the firewalls in a topology during network design and how to construct the routing Tables during operation such that the maximum firewall rule set can be minimized. We have two major contributions. First, we prove that the problems are NP-complete. Second, we propose a heuristic solution and demonstrate the effectiveness of the algorithm by simulations. The results show that the proposed algorithm reduces the maximum multi-firewall rule set when comparing with other algorithms.

Keywords: *Multi-firewall, Rule sets, Heuristic solution, Route*

1. Introduction

With the rapid application and popularization of computer networks, the increase of difficult steps of enterprises and government information digitization, existing enterprise network system structure is increasingly complex [1]. Complex network structure gives a lot of safety concerns; the need for network security is also in rapid increase of the nature of the unprecedented. How to make network security implementation for the high-speed business development gradually became the key problems that a lot of people attach importance to. For modern enterprise institution, the network is the foundation of the enterprise departments to coordinate the communication between platforms, is the fundamental guarantee of the enterprise operation, thus the security of network system for the corporate sector is very important. At the beginning of the network construction most companies are faced different network security incidents, they also implemented a simple security network technology and aircraft [2].

Firewall is the foundation of enterprise network security. Once a company set up a firewall, the most critical management task is to properly configure firewalls and security rules [3, 4]. Firewall configuration includes a set of large access control rules, each rules specify the source address, destination address, source port, destination port, one or more of the protocol ID and a proper function. This feature is a typical "accept" or "rejected". Some firewall can support other types of functions, such as sending log messages, using a proxy, by matching the bag into a VPN channel [3]. For most firewall said, firewall rule set is sensitive to the command [5]. Due to the multidimensional nature of the rules (including source/destination address and port), as the increase of the number of the rules, the

ISSN: 1738-9984 IJSIA

performance of the firewall will decreases. Commercial deployment of firewall is often accompanied by tens of thousands of rules, so that appear the bottlenecks in the network performance. Experience is more important, the fact is that the firewall rules set size has increased dramatically due to the increase of number of configuration errors [6]. A complex set of rules can be easily led to the incorrect and bad network configuration.

By the analysis of the firewall rule sets in many organizations, including telecommunications companies and financial institutions, Wool quantified the complexity of the rule set. By formula $R+O+\frac{I*(I-1)}{2}$, according to which, R is the number of the set of rules, O is the number of rules of the network object references, I is the number of network interface in the firewall. The number of network and the number of the network object is usually far less than the number of rules. Therefore, it is very important to keep the firewall rules set as small as possible, in order to reduce the chance that vulnerability was found [7]. In more than a firewall in the network, to reduce the number of rules not only needs the local optimization of firewall, also need to global optimization [8]. In this paper, we study how to minimize the maximum in many firewall network rule set, although its enterprise applications is very importance, but it has not yet been fully studied [9].

A firewall (as a blocking point, control points) can greatly improve the security of an internal network, and through the filter not security services and reduces risk [10]. Because only by carefully choosing application protocol through the firewall, so the network environment becomes more secure. Firewall can protect the network from attacks based on routing, such as the source IP options of routing attacks and ICMP redirect path. Firewall can refuse to all types of attacks message and inform the firewall administrator [11-12].

Through the use of the internal network firewall, we can realize the internal key network isolation, limiting the local network security key or sensitive to the effects of the global network. Privacy is very concern of the internal network; an internal network of obscure details may contain clues about security and interest by the outside attacker, even some which exposed the internal network security vulnerabilities [13-15]. Use a firewall can be concealed who revealed details of the internal.

Firewall generally has three characteristics: all communications through the firewall, the firewall is given only to authorized network traffic and firewall can withstand the attack on its own. Firewall is not trusted network and trusted network as a buffer against the question of firewall is the router, a multiple network interfaces to services such as computer or server. So, is located in the boundary of the network firewall to protect computer security. If there is no firewall, it may be the security of the whole network will be the most vulnerable part of the network.

Throughput and management issues arise when firewalls are applied in large transit networks. The manual configuration of large numbers of firewalls distributed in many access points can not provide open and dynamic environment and the large number of filtering rules decreases each firewall's throughput. Management can be improved using algorithms to automatically allocate global filtering rules to individual firewalls and to dynamically configure all of the firewalls according to the results of intrusion detection systems and search engines. The throughput of individual firewalls can be improved using a hash Table based rule matching algorithm, which reduces the time complexity from O(N) to O(1) for transit networks, and therefore, increases the firewall throughput [16].

The rapid development of Internet has brought great convenience to people's life, but at the same time, the Internet is faced with unprecedented threat. Therefore, how to use effective feasible method to make the network risk within an acceptable range

is in the attention of more and more people get. And how to implement the prevention strategy, first of all depends on the current system of security. Firewall technology, as a kind of network security technology nowadays is more mature, its security is directly related to the vital interests of the users [17]. Through to the present situation and the present situation of the firewall technology, this article designed pair of firewall security structure, conducted detail parameter design of network security for a company.

Along with the computer network expands gradually, internal network security has become an increasingly important issue [18]. This paper introduces a firewall security equipment technology and application of mode, and in the light of the connection network characteristics, put forward an improved strategy by using of two firewalls to improve network security.

2. Problem Definition

2.1 Network Model

In this paper, we consider a safety sensitive enterprise network, the network domain name through a firewall (subnet) connected to each other. Assuming that, the safety of the domain is properly executed. This article mainly aims at the access control of inter-domain. Further, we assume that the firewall in the network, more dynamic routing is closed, and the static routing is used to link within the domain of communication, this model is widely used in the modern in the bank or other enterprise management model, is proposed to the enterprise demand for more advanced security [6]. In fact, some popular firewall model (for example, many cisco PIX) does not support dynamic routing protocol. With the realization of the static routing, robustness is through the use of dual firewall. Using static routing in the firewall is a direct consequence of the high complexity of network security management requirements. It has many practical advantages. First, it can ensure that all traffic through their specified firewall, so that we can strengthen the implementation of security policy in proper place [19]. Second, in the complex network environment on the safety of the predictable routing path to simplify analysis, therefore, reduce the chance of error in the configuration of the firewall. Third, most of the existing dynamic routing protocol is not secure. By not safe path, fake routing advertisements can transfer flow, and packets may be reproduced or tampered with. Note that dynamic routing cross a firewall between domains, as long as you don't he will perform in each domain [20].

2.2 Symbol Description

Assumption that, N stands for a collection of n field and M stands for a collection of m firewall. Each firewall, there are two or more network interfaces. Different firewall can have different number of interfaces. A network interface can connect to any domain, forming a physical link between the domain and the firewall. In this model, two firewalls do not directly link to each other, otherwise, will use them as a firewall using common interface; two domains is not directly connected, otherwise, we will use them as a domain. The total number of available firewall in all of the firewall in the network interface is represented by e. In the topology structure, the maximum link number is bounded, represented by e.

For each pair of domain $x, y \in N$, has a set of access control rules of $R(x, y)$, the signal flow is defined from domain x to domain y.The optimization of the rule set is beyond the scope of this article research. Let $r(x, y) = | R(x, y) |$.Similarly, the number of rules from domain y to domain x, through $r(y, x)$ represented. The

number of total rules between the two domains is $r(x,y)+r(y,x)$. Once the path is certain between the domain x and domain y, firewalls will be set up along the path. Each firewall may be between the two fields in the router, the rule set will be located in numerous domain rules between combined.

As in the Figure 1 shows, through a set of firewall, there are many ways to connect to a group of domain. For any network topology, there are different ways to design the router path. In general, when we change the network topology and routing paths, the set of rules to perform the firewall will be different.

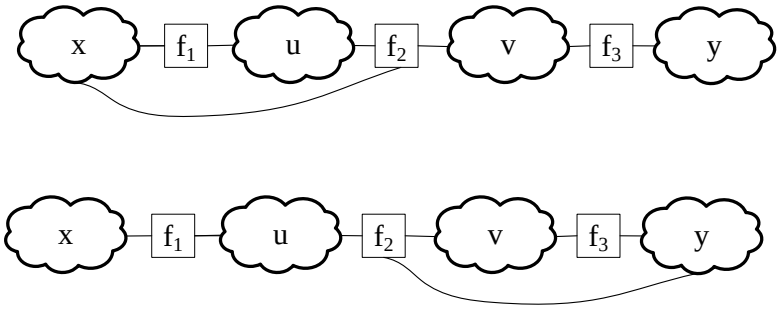

Figure 1. Two Kinds of Topology Structure for Domain Link

In Figure 1, through a firewall f1, f2, f3 connected domain x, y, u and v. The numbers of interfaces of firewalls are respectively: 2, 3 and 2.

3. Heuristic Method of Firewall Optimization

This paper proposes a heuristic algorithm to solve the problem of firewall optimization (Heuristic algorithm for firewall, HAF).The proposed algorithm is mainly placed around the location of the firewall problem (firewall placement problem, FPP), through the optimization of placement, minimize the number of maximum rule set. The input of HAF rules is a figure G_r. Set M said the number of firewall. The initial topology graphics G_t not connected to the path of the firewall, but is another issue some or all of the topological structure [9].

For FPP, G_t originally is a no link topology, contains n nodes and m firewalls. For each edge $< x,y >$ in G_r, insert the optimal path (G_t, x, y). The heuristic algorithm that subroutine is called is as follows:

1. Definition the viable path set between domain x and the domain y.

2. Found the optimal routing path in all feasible routing paths to minimize the maximum rule set and between domain x and the domain y.

3. Insert the optimal routing path to the G_t.

The pseudo code of the HAF algorithm is shown in Figure 2.

Figure 2. The Pseudo Code of the HAF Algorithm

The output of the HAF is a complete topological graph G_t, including the domain and firewall as its node, connecting link field and firewall, routing table. The cycle processing of steps 2 and 3 is the treatment to edge set $< x, y >$ in the G_r. The treatment is in descending order of $r(x,y)+r(y,x)$ based on the domain x and domain y, reflect the total number of rules in domain x and domain y. On each iteration of G_t, topological graphics, by inserting a routing path circulation way to achieve sustained growth [21]. As shown in Figure 3, Figure 4.

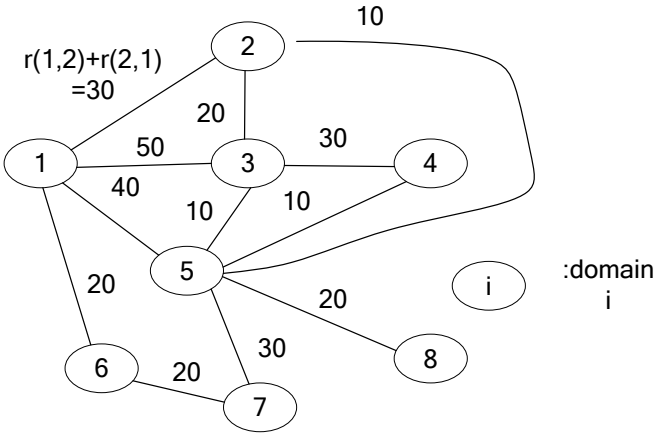

Figure 3. Regular Graph G_r

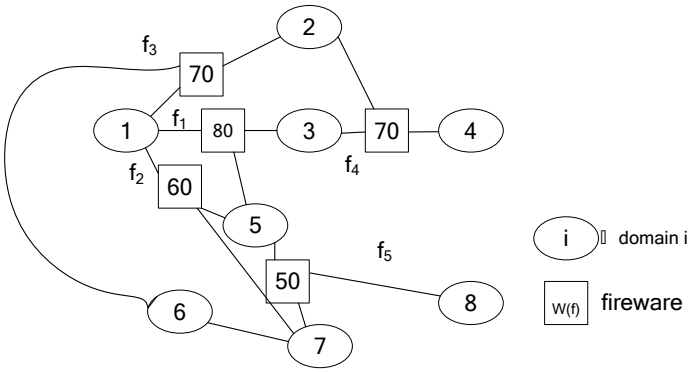

Figure 4. Topology Graph G_t

Domain path Table is as shown in Table 1

Table 1. Domain Path Table

$rt(1,2)=f_3$	$rt(2,1)=f_3$	$rt(3,1)=f_1$	$rt(4,3)=f_4$	$rt(5,1)=f_2$	$rt(6,1)=f_3$	$rt(7,6)=f_2$	$rt(8,5)=f_5$
$rt(1,3)=f_1$	$rt(2,3)=f_4$	$rt(3,4)=f_4$	$rt(4,5)=f_4$	$rt(5,2)=f_1$	$rt(6,7)=f_3$		
$rt(1,5)=f_2$	$rt(2,5)=f_4$	$rt(3,2)=f_4$		$rt(5,3)=f_1$			
$rt(1,6)=f_3$		$rt(3,5)=f_1$		$rt(5,4)=f_1$			
$rt(1,7)=f_2$				$rt(5,7)=f_5$			
				$rt(5,8)=f_5$			

The firewall path Table is as shown in Table 1

Table 1. The Firewall Path Table

rt(f_1,1)=1	rt f_2,1)=1	rt(f_3,1)=1	rt(f_4,2)=2	rt(f_5,5)=5
rt(f_1,2)=3	rt(f_2,5)=5	rt(f_3,2)=2	rt(f_4,3)=3	rt(f_5,7)=7
rt(f_1,3)=3	rt(f_2,6)=1	rt(f_3,6)=6	rt(f_4,4)=4	rt(f_5,8)=8
rt(f_1,4)=3	rt(f_2,7)=7	rt(f_3,7)=1	rt(f_4,5)=3	
rt(f_1,5)=5				

4. Simulation Experiment

The performance of HAF algorithm on the FPP evaluated in this Section. In the simulation experiment, two simple algorithms are achieved, which respectively called the tree topology (TTA for short) algorithm and complete topological algorithm (FTA for the sake of brevity).

For a given FPP problem, firstly, a TTA tree topology is structured, which defines the routing path between any two unique domains. Establishment of the topological tree, the algorithm first selects a domain as the root node. A certain number of firewall will be chosen as a child of the root node, namely: the second levels of the tree. This paper select firewall is descending order of the digital interface. For each of the two level firewalls, domain will be a certain number of selected as child nodes, child nodes, as the third level. The process is repeated until the topology tree including all areas within the firewall. Even hierarchical tree representation of the firewall, and the odd levels of the tree that represents the domain. The number of firewall is restricted by the network interface. According to the number of firewall, the number of domain is limited.

FTA first constructed a topology tree, according to the measures of TTA. It then uses the firewall interface all remaining idle, through the links from each free interface domain random selection. Then, get the shortest path between domains by the shortest path algorithm is run.

The default simulation parameters are as shown in Table 3. The value of parameters of each simulation operation mode will be changed once. Here, n is the number of domains and m is the number of the firewall. $e(f)$ Indicates the number of network interface of the firewall f, $\overline{e(f)}$ is the average value of the network interface in the firewall f. In the domain of $< x, y >$, $\overline{r(x,y)}$ is the average value of $r(x,y)$, at the same time $r(x,y) > 0$. P is an arbitrary domain of $< x, y >$, the probability of $r(x,y) + r(y,x) > 0$.

Table 3. The Default Simulation Parameters

n	m	$\overline{e(f)}$	$\overline{r(x,y)}$	p
100	40	4	10	0.7

Figure 5, Figure 6, Figure 7 and figure 8 show the simulation results of three different methods. In all the simulation, y axis represents the greatest rule set size in all the firewall ($\max_{f \in} M\{w(f)\}$). The x axis is one of the parameters. By comparing the three methods, proved the effectiveness of the proposed method in this paper.

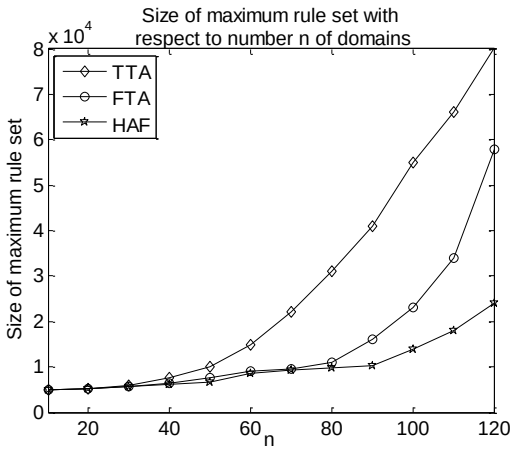

Figure 5. Firewall Maximum Rule Set Size in the n Domain

The parameters in Figure 5 are as following:
$m = 40, \overline{e(f)} = 4, \overline{r(i,j)} = 10,\ p = 0.7$.

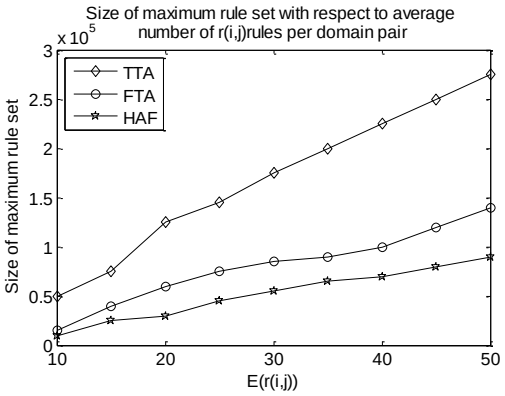

Figure 6. Firewall Maximum Rule Set Size based on the Average Number of $\overline{r(x,y)}$

The parameters in Figure 6 are as following:
$n = 120, m = 40,\ \overline{e(f)} = 4, 10 \le \overline{r(i,j)} \le 50, p < 0.7$.

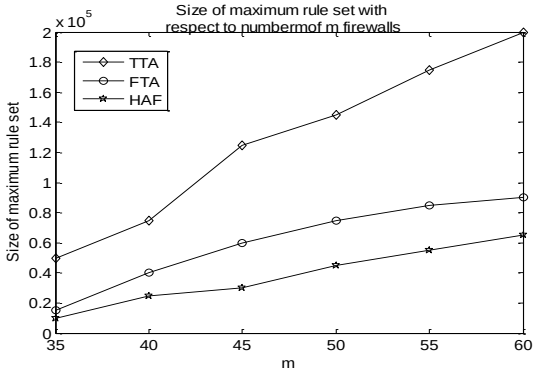

Figure 7. Firewall Maximum Rule Set Size based on the Average Number of $\overline{e(f)}$

The parameters in Figure 7 are as following:
$n = 100, m = 40,\ 3.5 \le \overline{e(f)} \le 6, \overline{r(i,j)} = 10,\ p = 0.7$.

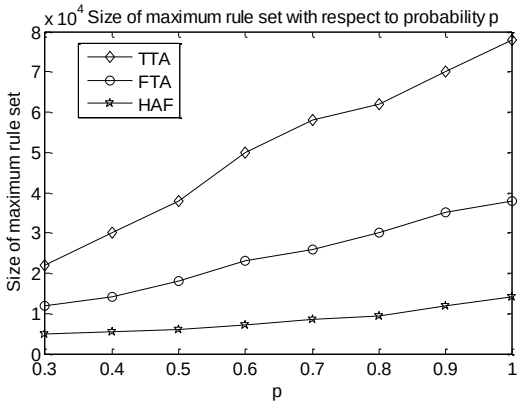

Figure 8. Firewall Maximum Rule Set Size based on the Sparse Network

The parameters in Figure 8 are as following:
$10 \le n \le 120,\ m = (n-1)/(\overline{e(f)}-1), \overline{e(f)} = 4, \overline{r(i,j)} = 50,\ p = 1.0$.

5. The Application of Pair Firewall Technology in Enterprise

Some original enterprise internal information network and other third party or the Internet between has no firewall settings. From the information security of the internal information network, enterprise top management as the basis, should be carried out on double firewall policy settings. But combining with the actual situation of the enterprise, placed in front of the problem is how to plan a suitable network structure and network equipment, can make double firewall structure not only show some of the uses and functions, but also no influence on the whole and local network function. The paper integrated the firewall for the improvement measures and for the concept of network. Firewall network security on the enterprises is carried out and the design and establishment is conducted.

The network layout that designed in this paper is as the following.

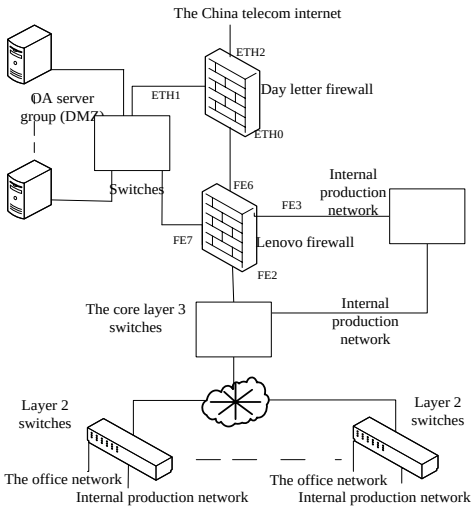

Figure 9. The Design Plans of Enterprises Double Firewall

The detail settings of the firewall are as follows:
(1) the IP of all the interface: FE2:192.172.1.248/27
FE3:0.198.0.67/25; 10.198.0.17/25; 10.198.0.66/25 (multi IP)
FE6:192.173.1.1/24
FE7:192.173.2.1/24
(2) The static route: objective IP 192.172.0.0/24, gateway to 192.172.1.254
Objective IP 10.0.0.0/8, gateway to 10.198.0.62
(3) The default route: 192.173.1.2
(4)The access rules:
Rule 1:All the working network interview the internet network.
Rule 2: the parts work web hosting visits to the specified port number on the production network.
Rule 3: work and internal production networks can visit training service system, OA service system, firewall log service system and upgrade service system in the virus inside the DMZ.
Rule 4: from the external network using the VPN to internal production network access, allowing VPN virtual IP to the specified port number on the inner part of the production network server as a visit.
(5) The NAT translation: from the external network using VPN access to internal production networks, IP needed VPN fiction into the 10.198.0.67.
(6) port mapping: parts of the virtual IP location of FE2 port corresponding to the OA server group of specified port mapping by the server, so that to the internal production network of OA server group visit, apply to the specified port number on the corresponding IP visiting FE2 mouth engaged for internal access OA server group.

6. Conclusion

This paper studies the enterprise firewall security configuration and its change. By finding the firewall in the network topology and routing structure of the optimal location, you can minimize the maximum of the firewall rule sets. This paper proposes a HAF heuristic algorithm for problem solving. Through the application in the enterprise prove the validity of the method. The algorithm can also be used to solve the problem of firewall routing.

References

[1] A. X. Liu, E. Torng and C. Meiners, “Firewall Compressor: An Algorithm for Minimizing Firewall Policies”, Proc. IEEE INFOCOM ’08, **(2008)**.
[2] A. Wool, “The Use and Usability of Direction-Based Filtering in Firewalls”, Computers and Security, vol. 23, no. 6, **(2004)**, pp. 459-468.
[3] A. Rubin, D. Geer and M. Ranum, “Web Security Sourcebook”, Wiley Computer Publishing, (**1997)**.
[4] S. Hinrichs and S. Chen, “Network Management Based on Policies”, Proc. SPIE Multimedia Computing and Networking Conf., **(2000)** January.
[5] J. Wack, K. Cutler and J. Pole, “Guidelines on Firewalls and Firewall Policy”, Nat’l Inst. of Standards and Technology, **(2002)**.
[6] D. Haixin, W. Jianping and L. Xing, “Dynamic allocation match algorithms and hash Table based for firewall rules”, J Tsinghua Univ (Sci &Tech), vol. 41, no. 1, **(2001)**, pp. 96-98.
[7] L. Guangcheng, “Research and design of double firewall technology”, Computer CD Software and Applications, vol. 21, **(2012)**, pp. 70-81.
[8] E. W. Fulp, “Optimization of Network Firewall Policies Using Ordered Sets and Directed Acyclical Graphs”, Proc. IEEE Internet Management Conf., **(2005)**.
[9] A. X. Liu and M. G. Gouda, “Diverse firewall design”, Proc. IEEE Int’l Conf. Dependable Systems and Networks (DSN ’04), **(2004)**, pp. 595-604.
[10] M. G. Gouda and A. X. Liu, “A model of stateful firewalls and its properties”, Proc. IEEE Int’l Conf. Dependable Systems and Networks (DSN), **(2005)**.
[11] A. X. Liu, M. G. Gouda, H. H. Ma and A. H. H. Ngu, “Firewall queries”, Proc. Eighth Int’l Conf. Principles of Distributed Systems (OPODIS), **(2004)**.

[12] A. X. Liu, "Change impact analysis of firewall policies", Proc. 12th European Symp. Research Computer Security (ESORICS), **(2007)**.
[13] A. X. Liu, "Formal Verification of Firewall policies", Proc. IEEE Int'l Conf. Comm. (ICC), **(2008)**.
[14] Y. Bartal, A. Mayer, K. Nissim and A. Wool, "Firmato: A Novel Firewall Management Toolkit", ACM Trans. Computer Systems, vol. 22, no. 4, **(2004)**, pp. 381-420.
[15] A. Woo, "A Quantitative Study of Firewall Configuration Errors", Computer, vol. 37, no. 6, **(2004)**, pp. 62-67.
[16] H. Guochao, "An Improved Strategy for Intranet Security Based On Two Firewalls", computer security, vol. 07, **(2012)**, pp. 36-38.
[17] W. Lihua, "Firewall technology and its performance study", Research on energy and information, vol. 20, no. 1, **(2004)**, pp. 57-62.
[18] W. Weiping, C. Wenhui and Z. Wei, "Firewall technology analysis", Information security and communications confidential, vol. 8, **(2006)**, pp. 24-27.
[19] M. Tao and Y. Lei, "Firewalls and security audit", Computer security, vol. 4, **(2004)**, pp. 17-18.
[20] Z. Baojian, "Computer security and protection technology", Mechanical industry publishing house, **(2003)**.
[21] A. X. Liu, E. Torng and C. Meiners, "Firewall Compressor: An Algorithm for Minimizing Firewall Policies", Proc. IEEE INFOCOM '08, **(2008)**.

Authors

Jing Li, received her M.S. degree in Computer Software and Theory from Sichuan University, China, in 2001. She is currently a senior lecturer in the College of Information Engineering at Qingdao University, China. Her research interests include network security, cloud computing security and electronic commerce.

