Association for Information Systems

AIS Electronic Library (AISeL)

ICEB 2005 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-5-2005

Integrated Multilevel Intrusion Detection and Report System

Tung-Shou Chen

Puo-Iang Chen

Tian-Shing Wang

Yung-Hsing Chiu

Sheng-Li Lai

Integrated Multilevel Intrusion Detection and Report System

Tung-Shou Chen[a] Puo-Iang Chen[b] Tian-Shing Wang Yung-Hsing Chiu Sheng-Li Lai
Graduate School of Computer Science and Information Technology
National Taichung Institute of Technology
tschen@ntit.edu.tw[a] tejiro0826@yahoo.com.tw[b]

Abstract: In this paper we demonstrate a new impression of intrusion detection system. We use multilevel structure of intrusion detection systems to protect our network. Most of traditional report systems are complicated and hard to manage. In our system, our interface of report system is easy to read and manage. The most important is we use open source software to integrate our system. This can make the cost of intrusion detection system down and make our system flexible. It is convenient to user and network manager. In our system, we can integrate different intrusion detection system and report system into one system. It will become a trend nowadays.

Keywords: intrusion detection system (IDS), firewall, report system

I. Introduction

In recent years, the development of internet become more and more important, and made life convenience. Internet is usually used for research or the way to find information what you need in early years, so researchers are the main users of internet before. Internet is a versatile tool for people nowadays. We can send and receive E-mail, browse website, or find other information related our life in internet. Especially E-commerce, Internet has turn into important tool for modern people.

The conveniences of internet include information exchange and business transactions in internet. The rapid development of E-commerce gives the credit to internet because of its transmitting information is fast. Popular of internet also brings lots of security problems. We should pay much attention to security of E-commerce especially for enterprises. These security problems become important issues today. Most of enterprises use firewall to protect their data and network. But it is not enough. Problem of hacker attack becomes more and more changeable, and various types of virus and troy are increasing. The most important thing is the problem of artificial careless mistake. The security problems of enterprises network come form inside network of enterprises. Network security is hard to defend. Protecting network cannot bear using in the single firewall. For guarantee the security of information and electric business trade, it is indispensable to have an intact and convenience network protect structure.

The prevailing of e-commerce makes enterprises to pay more and more attention in network security. Some enterprises think that is enough for network security to set up only firewall. But this is incorrect. Firewall only can be a basic network protection. The main function of firewall is to control who want to get into network. However, enterprises still have security problems with only set up firewall. In E-commerce, network packages represent all kinds of trade information. If enterprises cannot ensure the security of network safe, it will cause great money to lose by a small security problem. A simple network attack may cause millions dollars losing for enterprises. Furthermore, it will cause customer information or commercial materials outside of enterprises. Then the goodwill of this enterprise will be seriously injury. Hence, for E-commerce issue. Network security should be care seriously. Besides important of firewall in this issue, intrusion detection system is another important issue in our research.

Intrusion detection system as call IDS is a critical tool of network security. It has much capability, include of sniffing and checking network packages and generate alert log files when it detects network attack. Network structure that only has firewall is not tight enough. For this reason, the integration structure of firewall and instruction detect system turn into safer network security system.

What is the main difference between firewall and intrusion detection system? The mainly purpose of firewall is to identify different IP address and to open up server services for network outside. But the mainly purpose of intrusion detection system is to sniff packages and to detect suspicious packages. If we image that internet is an important road. Firewall looks like a traffic-police on this road. It determines whether you drive against traffic regulation or not, and it can also to fine you when you against traffic regulation. Intrusion detection system looks like a camera of testing speed on the road. It can take down cars which against traffic regulation and then convey car information for traffic-police. The disadvantage is that cannot find the car which against traffic regulation. And this is the largest different between firewall and intrusion detection system. In our research, we present a structure to integrate them.

Commonly intrusion detection system has some disadvantages. They are miscellaneous alert messages and commercialized intrusion detection system is too expensive and hard to maintain. Some of free intrusion detection systems have shortcoming with insufficient. And most important is that when you get alert messages or log files from firewall or intrusion detection system, these reports are uniform. The shortcomings of these reports are hard to read

Proceedings of the Fifth International Conference on Electronic Business, Hong Kong, December 5-9, 2005, pp. 463 - 469.

and have no idea to alter according to user's demand. Even intrusion detection system or firewall is strong, and the reports from these places have no idea to let users or MIS understanding immediately. It conveys more trouble to maintain system and to protect network for MIS or users.

In order to solve illegal network connection and network attack. In our research, we introduce a multilevel network security structure. We call it Multilevel Network Security Structure (MNSS). In this structure, we clean up insufficient security of only firewall in network structure. And offer multilevel of network protection. The structure of our research is including firewall, intrusion detection system, and report system. Our system presents a high stability, high expending with high capacity and efficiency, and easy to management. The best advantage is to make the whole system cost down. These advantages will be introduced in following paragraphs.

In MNSS, we also present a personal report system (PRS). This report system differs from other common report systems, it can add and delete report column according to user's requirement. Our report system will generate new report form according to user's requirement. It can also generate report according to different position of company. For example, leader of enterprises usually wonder to know whether the company meets a great network attack or not. He does not want to know every alert message in peacetime. Our report system can generate reports which boss interesting at the time. Our report system conveys convenience to most of MIS.

We will introduce MNSS and Personalize report system in detail in following chapters. Chapter 2 will introduce preview of intrusion detection system and its advantages and disadvantages. And intrusion detection system used by our research briefly. Chapter 3 will introduce system structure in detail. Chapter 4 is experiment. And last chapter is conclusion.

II. Preview

II. 1 The Category of Intrusion Detection System

There are two categories of intrusion detection system. One is Host-based Intrusion Detection System (HIDS), and the other is Network-based Intrusion Detection System (NIDS). NIDS is typically used recently. Most of researches like to study NIDS which has flexibility used. In our research, we also use NIDS to develop our work. The intrusion detection system is divided into two parts, abnormal detection and misuse detection [1] [2]. We introduce in following briefly.

II. 2 Abnormal Detection

Technique of this part is to analyze user behaviors and to use this information to find out whether this is normal used behavior. This method uses user behavior information which collects in advance to determine behavior normal or not. The algorithms of statistic and mathematical induction are used in this part of detection technique mostly. Importance of this technique is how to define a normal and correct user behavior. The data for defining user behavior also influence user behavior or not. The advantages of these detection techniques are learning automatically. This function can prevent network attack which did not used before. The disadvantage of this technique is depending on user behavior which is collected to define normal model correct or not. If attacker attacks network by using normal user behavior define before, this technique does not find out this behavior correct or not. We will show these detection techniques of abnormal detection as following.

II. 3 Neural Network

Neural Network (NN) has capacity of using a large number of data to train these data and learning from training data. There are more and more different applications for researcher in this technique [3]. So this technique also is used for one of intrusion detection system to detect user behavior.

II. 4 Support Vector Machine

Support Vector Machine (SVM) and NN are from technique of artificial intelligence. This technique can also predict user behavior by training data set. Some researchers use this technique on intrusion detection system [4] [5], too.

II. 5 Data Mining

Algorithms of data mining also apply to collect data and analysis data by some researchers before [6]. This technique can make new feature recognize rule to protect network. Hence, this intrusion detection technique has much security of network.

II. 6 Statistical Algorithm

This kind of detection is similar to data mining method. This technique analyzes data collected to calculate a normal user behavior model by using statistical algorithm. The advantage of this technique is that you should understand statistic seriously in advance. And you must use complex mathematic to calculate final result.

II. 7 Misuse Detection

The detection technique of misuse detection uses rule-base detection to define network attack. Defined rules will store in database. Intrusion detection system uses rule in database to analyze network package. Pattern matching is one of commonly used technique in this detection. Pattern matching applies on most of intrusion detection system. It has high detection rate on this technique. This technique can use network attack known by pattern matching rules in database. If system detects attack from network, it sends alert message to user or other protect system. User can understand what kind of attack happens through alert message. And user or system manager can defend this attack by information from alert message.

The key point of this technique is that we should collect large number of network attack already know to build database. So system manager can use rules in database to match with network packet and find out is it network attack. However this technique cannot defend network attack by learning from expensive.

Some researcher used System Call to apply on intrusion detection system before [7]. Most of intrusion detection system mainly uses misuse detection to develop their system. Because of detection technique with pattern matching makes detection faster and convenience. And it has higher detection rate. Some of researchers work for combining abnormal detection and misuse detection into one system.

In our research, we use a commonly used freeware – Snort to be our intrusion detection system in our system. Our research uses iptable to be firewall in our system. We also use ACID to modify our report system, and it is called personal report system. We choice Analysis Console for Intrusion Database (ACID) to modify our system because of it can deal with the report from Snort and iptable. That is why we use these softwares to integrate our system.

Snort is a generally used intrusion detection system today. It has more resource internet. In the part of updating version is very fast because of it is open source software. So that Snort is a powerful and high security intrusion detection system. We will introduce Snort briefly as following.

II. 8 Snort

Snort is a real-time intrusion detection system developed by Martin Roesh. Snort is a lightweight Network-base intrusion detection system. It means when intrusion detection system detects package from network. It does not effect network overloading. Snort has lots of advantages. Snort is cross platform software. And it can work on Linux and Windows.

There are three modes of snort. They are Sniffer Mode, Packet Logger Mode, and Network Intrusion Detection System Mode.

1. Sniffer Mode: This mode is used to sniff network package.
2. Packet Logger Mode: Recording network package information.
3. Network Intrusion Detection System Mode (NIDS Mode): Analyzing network package, and detecting package from network by rule database.

Snort uses NIDS Mode to start intrusion detection, and the structure of intrusion detection shows on Fig. 1. There are four parts of structure of snort. They are Packet Decoder, Preprocessor, Detection Engine, and Output Stage. We introduce these parts first.

1. Packet Decoder: This part collect package from network. It copy broadcast package from network. And it will decode packages which collect from network. Decoded package will be sent to Detection Engine.
2. Preprocessor: This part mainly preprocess package from network. And it can increase detection rate and process speed. Snort provides eight preprocessors at present. Each preprocessor has different function. These preprocessors can choice by user requirement.
3. Detection Engine: Snort used brute force algorithm to do pattern matching in the early. But this algorithm costs much time and resources. Therefore, Snort provides a new algorithm to do pattern matching - Boyer-Moore pattern matching now. This algorithm saves much time than brute force algorithm. For speeding up time of pattern matching. Snort uses three-dimensional linked list data structure in detect engine. These functions make Snort more convenient and efficiency.
4. Output Stage: Output stage decides whether sends alert message or not according to detect engine. So that can generate log files or send alert messages to report system.

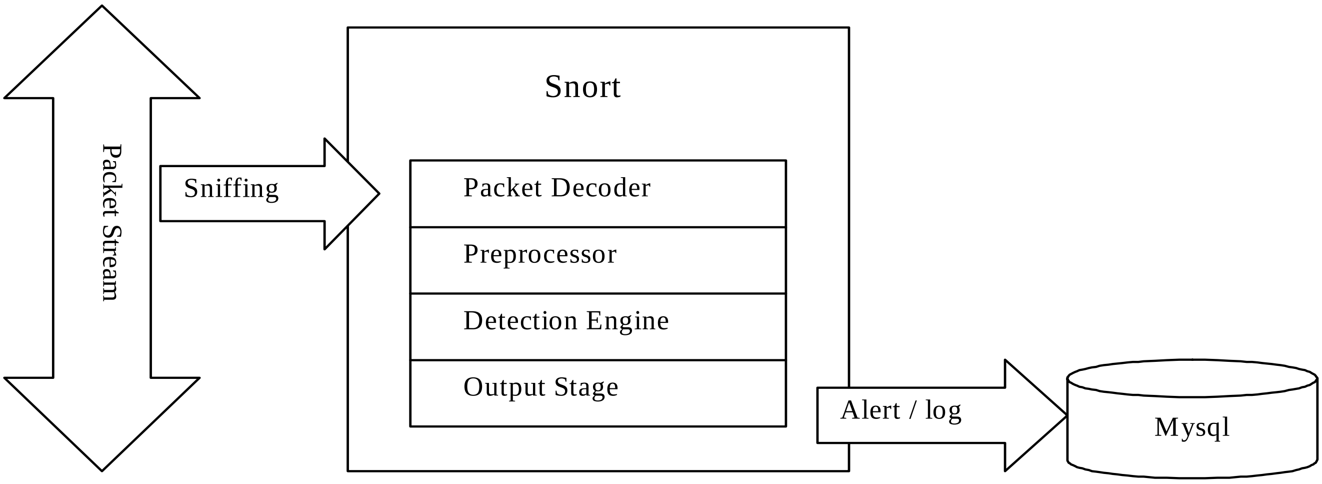
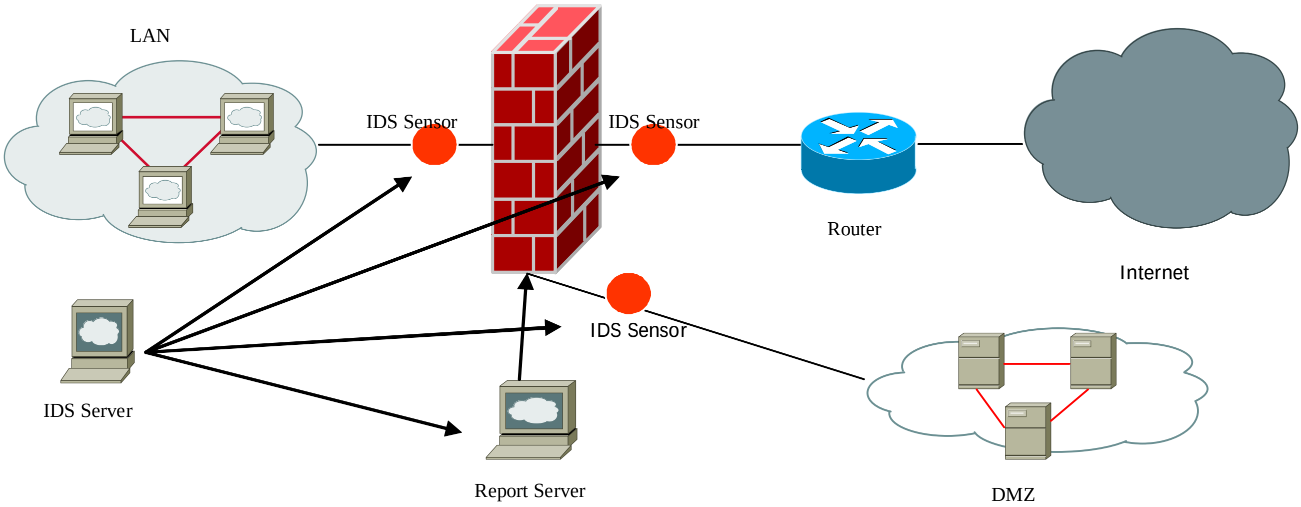


Fig. 1 Structure of Snort



2: System Structure

III. System Structure

Almost Network security systems only use firewall to do network protection before. This structure seems safe enough to general users. But it is danger for enterprises and some e-commerce of company. Hence intrusion detection system is developed for this reason. Most of companies use firewall and intrusion detection system to protect their information on network. It is a trend to use more than two different function systems to protect important information. There still has a problem in user confused of how to build a safer network environment. In our research, we provide a structure to solve this question. We use multilevel network structure for network security system. We find out most of problem from security issue happened before. We present an overall structure for network security. Such as most security problems are from wide-area network (WAN). So we set a sensor in WAN in order to collect information of WAN. In our research, we will set security measure on places where may occur security problem. In the following, we will introduce this structure detail on this chapter.

III. 1 Multilevel Network Security Structure (MNSS)

In order to solve problems mentioned pro paragraph, our research presents a structure call Multilevel Network Structure (MNSS). We integrate firewall, intrusion detection system, and report system into our structure. System structure will be shown in Fig 2.

Intrusion detection system sets three sensors on our structure. They are set in DMZ, in front of firewall (LAN) and behind firewall (WAN). The function of sensor in front of firewall (LAN) mainly checks whether someone attacks network or not. The function of sensor behind firewall (WAN) is to monitor attacks in wide-area network. Final, sensor in DMZ is to ensure servers are safe enough. Therefore, we set every place where may be attacked by hacker or someone to ensure our structure is safe enough. This structure ensures that it cannot lose any probably attack by someone. And we also know where attack is happened through our structure.

The main advantage of intrusion detection system is this technique does not cause overloading of network. Because of intrusion detection system only sniffs network. Intrusion detection system was an assist tool for firewall to protect network before. Hence, when network attack comes from WAN or DMZ, the system does not know where attack is. So system does not send alert message to user or system manager in real-time. That is why we set three sensors in our structure.

The special of our structure is that we have an independent report system. We call it personal report system (PRS). PRS will introduce in later.

In our research, we use Snort, iptable, PRS to build our structure. Hence, the sensor in front of firewall is first line of defense in our network. Second is firewall. If attack appears in WAN, sensor behind firewall can find out it. Finally, PRS can tell user or system manager where attack occurs, so system manager can handle the situation. That is why we call it multilevel network structure.

In our research, all of systems in our structure are open source software, such as Snort, iptable, PRS. Properties of open source software are free, flexible, and maintain easily. Therefore, MNSS does not necessarily to use the same software which are using in our research, it can be changed into other software according to user’s custom and requirement. In other words, the sensors also can replace with three different intrusion detection systems. It can make network security more faultless.

III. 2 Reduce System Cost

Intrusion detection system makes people condemn mostly because of its expensive software price. Stable and multi-function security system should be bought from company who provides network security service. To enterprises, they should cost much money on building a security system when e-commerce develops in initial stage. This is whole enterprises worried.

Our research makes network security safer and cost down. And our research uses open source software to build system. Open source software is easily to learn because of its network resources. Document and software information is easy to get. In opposition to commercial software is hard to use and learn. And information of commercial software is hard to get. Using commercial software is a burden for system manager. MNSS allows user to choice different intrusion detection system and firewall according to their need, and it can make system cost down.

We also have a special capacity that when someone attack network in MNSS. This capacity can handle network attack real-time by user setting. It reduces time of dealing with network attack by system manager. MNSS can monitor 24 hours to save labor power and cost consume.

III. 3 Independent Report System

In our research, we separate report system to independent server. In commonly security system, intrusion detection system and report system are usually in one server. It cause intrusion detection system and report system cannot work when server down. At this moment, there is only firewall work in security structure and increasing danger in network.

In our structure, report system still work when server down. And report system can centralized manage log files and alert messages from intrusion detection system and firewall in order to avoid server overloading. The other advantage is report system still work when intrusion detection system and firewall change.

III. 4 Personal Report System (PRS)

Our report system calls personal report system (PRS). The system modify from ACID and system structure show in Fig. 3. PRS will introduce as following detail.

PRS uses SMNP protocol to receive log files and alert messages from intrusion detection system and firewall to centralize management. It preprocesses log files and alert messages and saves it to database. Our PRS provides a friendly user interface. This user interface lets user to set report column they need and save it. Database will receive information of which column user selected and send these columns to PRS. PRS uses these data from database to generate report, so we call it personal report.

PRS can generate different reports according to user's requirement. It makes user more convenience. PRS also can generate report base on different positions in company. Leader in company or department only wants to know serious attack about network security. Traditional report system generates only one or few format report for user reading. Leader in company does not want to see these reports. It is too long and complex. PRS does not have these questions. It can make a great help and save lot of time to system manager.

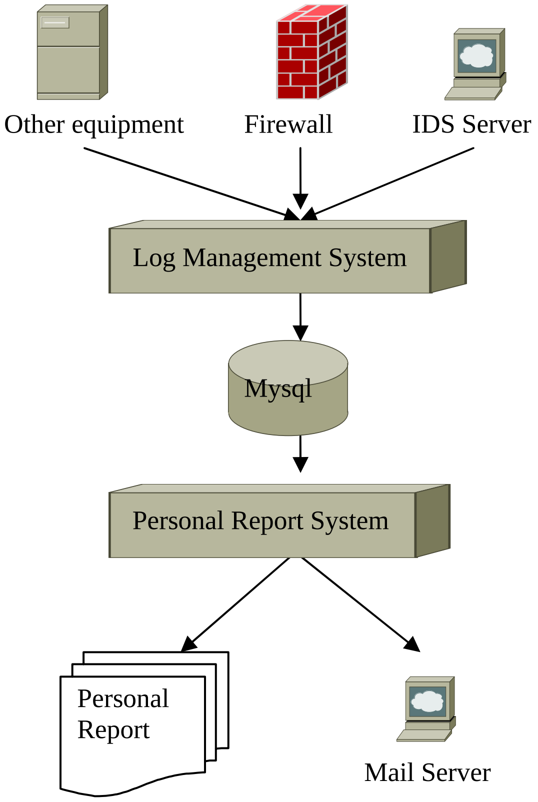


Fig.3 Personal report system structure

IV. Experiment and Analysis

Capacity of defend serious attack

Intrusion detection system must monitor network 24 hours continuously when MNSS is working. In the process of monitoring network, MNSS may detect an obvious network attack. Intrusion detection system only monitor network when network attack occurs before. Network security only uses firewall to defend, and it brings more burdens on firewall. And it must control by system manager. These situations make firewall and system manager more and more trouble.

Our structure has a capacity of defend obvious attack. It can detect and defend obvious attack from network immediately. The flowchart shows in Fig.4.

We use intrusion detection system to monitor network first. And then we define an obvious attack mode base on requirement. Intrusion detection system does extra process to obvious attack mode. In obvious attack mode, system set a time parameter T1 first. When this mode detects an obvious attack setting before, intrusion detection system monitors this attack continuously. Time between network attack occurs until PRS sends message to firewall sets to be T1 and than we set another parameter T (T is a threshold setting by user experience). If value of T1 bigger than T, PRS will send command lines to firewall, these command lines can set by user in advance. Command lines in here will different base on firewall user used. Firewall can use these command lines from PRS to do some defend immediately.

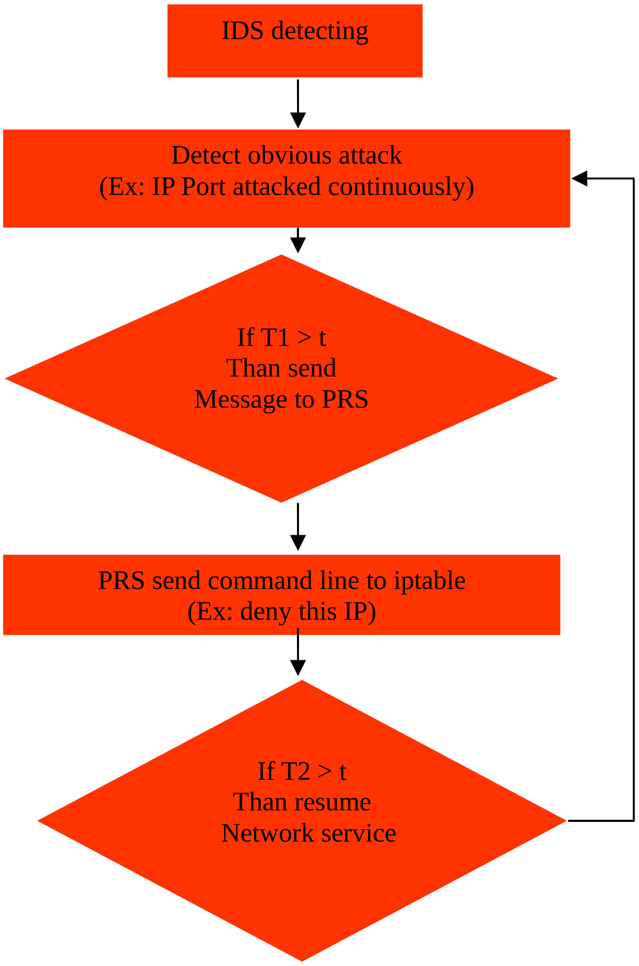


Fig.4 Flowchart of defend serious attack

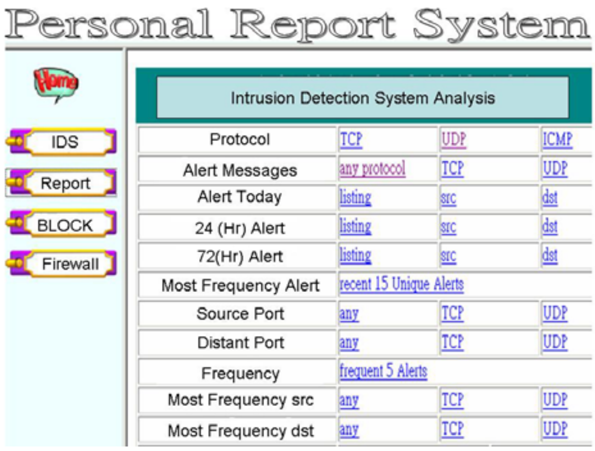
For example, IP from 192.168.1.1 uses DOS to attack network. We set T = 10 minutes first. If DOS attacks network more than 10 minutes continuously, and a default command line for PRS is iptables –A INPUT –s AttackIP –j DROP. Therefore, when attack time bigger than 10 minutes, PRS will set command line to firewall (iptable is firewall used in our experiment). Firewall can deny this attack by command line sent by PRS. We will set one time parameter T2 to resume network service. T2 is a time across attack start to the end. When T2 is bigger than 10 minutes, PRS will send iptables –A INPUT –s 192.168.1.1 –j ACCEPT to firewall. Firewall can resume service to IP from 192.168.1.1 at this moment.

IV. 1 Compare to Network Security System

In our research, why we use open source software to develop our system? There is a comparison of open source software and commercial software shows in table1. Information of this table is from report write by Dr. Ying-Dar Lin [8]. Open source software in this table is iptable. We can find open source software is as well as commercial software in detection ability. But it has a great difference in price. It does not mean commercial software is expensive and weak. Because of commercial software has more other function of its system. In this table, we want to show open source software is cost down and still have a good detection in network security.

IV. 2 Display Report

In personal report system, we can analyze alert message sent from firewall and intrusion detection system. And the result shows in Fig.5. This figure shows frequency of alert message generating. And analysis information is collected by firewall and intrusion detection system. Such as source port, distant port, etc.



Intrusion Detection System Analysis

Protocol	TCP	UDP	ICMP
Alert Messages	any protocol	TCP	UDP
Alert Today	listing	src	dst
24 (Hr) Alert	listing	src	dst
72(Hr) Alert	listing	src	dst
Most Frequency Alert	recent 15 Unique Alerts		
Source Port	any	TCP	UDP
Distant Port	any	TCP	UDP
Frequency	frequent 5 Alerts		
Most Frequency src	any	TCP	UDP
Most Frequency dst	any	TCP	UDP

Fig.5: Analysis report

V. Conclusion

In this research, we present a multilevel network structure. This structure integrates intrusion detection system, firewall and personal report system to build more safety network.

All of our structure promotes to use open source software to build a system because of it can make cost down and make user or system manager more convenience and easy to maintain. Personal report system can generate different formats report by user setting. So user can generate report easy to understand and suit by himself. And it is special to generate different reports according to different positions in company.

PRS can use time parameter to send commend for firewall when network has an obvious attack. So that firewall can handle this attack immediately. In traditional situation, system manager gets alert messages and handles this attack wasting time. Our structure integrates network security concepts and reduces burden of system manager.

In our research, it cannot support all of intrusion detection system and firewall yet. We will keep on our research in maintain and development system. Structure presents a basis structure, and it has more development in this structure. It can be build more function on this platform.

References

[1] Bierm, E. Cloet, E. & Venter, L.M. "A comparison of Intrusion Detection systems," *Computers & Security*, 2001,20,676-683.

[2] "IDS - Intrusion Detection System." http://www.skullbox.net/ids.php?569b59e8

[3] Lee, S. C. & Heinbuch, D.V. "Training a neural-network based intrusion detector to recognize novel attacks," *IEEE Transactions on Systems, Man and Cybernetics*, 2001,31,294 - 299,.

[4] Mukkamala, S. & Sung, A. H. "Artificial Intelligent Techniques for Intrusion Detection," *IEEE International Conference on Systems, Man and Cybernetics*, 2003, 2, 1266 - 1271.

[5] Kim, D. S. Nguyen, H.-N. & Park, J. S. "Genetic Algorithm to Improve SVM Based Network Intrusion Detection System," presented at 19th International Conference on Advanced Information Networking and Applications, 2005.

[6] Lee, W. Stolfo, S. J. Chan, P. K. Eskin, W. Eleazar Fan, M. M. Hershkop, S. & Zhang, J. "Real time data mining-based intrusion detection," *Second DARPA Information Survivability Conference and Exposition*, 2001,85–100.

[7] Hofmeyr, S. A. Forrest, S. & Somayaji, A. "Intrusion detection using sequences of system calls," *Journal of Computer Security*, 1998.

[8] Lin, Y.D. & etc, "Benchmark of Security Gateways" *CONNECTIMES INTERNET NETWORK COMMUNICATION*, 2002.

[9] "Snort, the open source network intrusion detection." http://www.snort.org/

[10] "Analysis Console for Intrusion Databases (ACID)." http://www.andrew.cmu.edu/user/rdanyliw/snort/snortacid.html

[11] "IPTABLE." http://www.linuxguruz.com/iptables/

Table1: Comparison of open source software and commercial software

Company/ Product	Packet Filter	DMZ	URL Filter		HTTP Content Filter		Price
			Exactly String Match	Regular Expression	Java	JavaScript	
Open Source Software	Yes	Yes	Yes	Yes	Yes	Yes	NT$0
BorderWare Firewall Server	Yes	Yes	(need license)	N/A	No	No	NT$550,000
CheckPoint VPN/Firewall-1	Yes	Yes	No	No	No	No	NT$559,860
Cisco PIX 525R	Yes	Need card	External	N/A	Yes	Yes	NT$880,000
NetScreen-100	Yes	Yes	External	N/A	Yes	Yes	NT$665,000