A Study of SLA-Based Defense Resource Management Strategy in Network Security Defense System

Wen-Hsu Hsiao[1], Hui-Kai Su[2], Yu-Siang Wei[3], Wei-Sheng Ho[3], and Kim-Joan Chen[3]

[1] Department of Computer Science and Information Technology WuFeng University, Taiwan
shianws@wfu.edu.tw
[2] Department of Electrical Engineering National Formosa University Yunlin, Taiwan
hksu@nfu.edu.tw
[3] Department of Electrical Engineering National Chung Cheng University Chia-Yi, Taiwan
ieekjc@ccu.edu.tw

Abstract. This paper mainly propose a service of network security defense provide by the network service provider, and the service system is built on the original ISP network structure, the security decisions center build on the ISP's core network which is making the policy decisions of security event, and built a defense system on border routers to form a secure domain called security domain, the service provider will join the user who is using the service to the security domain, through the defense system to network traffic monitoring and filtering malice package to provide users of network security threat defense services. Using Service Level Agreements (SLA) to represent users' needs, so that users can choose services according to their needs, network security defense system provide different type of defense services based on user needs. Finally, we analyze the usage of the defense resource, furthermore we formulate the mechanisms of policy for the client's needs, and how to allocate resources in the case of resource saturation for the defense to satisfy service providers obtain the best benefits of the service strategy, and design the mechanism of resource management.

Keywords: Security Policy Management,SLA.

1 Introduction

In recent years, the network attacks is changed rapidly and it's impossible to defend effectively. For the user who not familiar with the security issue to operate the security software is difficult. In such situation, these users usually use the setting by default, we are not sure whether the default setting can be able to against these attacks or not; On the other hand, for the network administrator is familiar with network security management, will still be subject to the hazards of cyber-attacks. Such as the recent years, Sony and Google was be hacked, and the hackers steal a large number of customers' personal data. Only enterprise collected information alone is not sufficient to prevent attack. These prevention methods are in the user side to install their own network security software or hardware, as well as via the user or the network managers to manage the data information.

J.J. Park et al. (Eds.): NPC 2012, LNCS 7513, pp. 336–348, 2012.

This paper proposes the architecture to provide network security services by the Internet Service Provider (ISP). The service provider is responsible for managing the customer's network security, taking a protection of customers using the Internet from the malicious so that customers do not need to install their own network security software or hardware. The service is known as network security and defense services. However, the degree of network security needs of each customer are different, it must be customer-oriented, according to the security needs of each customer to provide the appropriate network security.

For these motivation, this paper will be based on the security system architecture [4] to explore the application environment and services designed to modify the system according to the needs of the application environment and services, and incorporate the concept of user demand to provide network security system; Finally, we have to analysis of the defense system usage behavior, and further development the mechanisms of customer demand and planning the security management.

2 Background

A. The Distributed Defense System

In the paper [4] [5] proposed a distributed security system architecture like Fig.1 (Security Policy Decision Server, system architecture, SPDS) as the policy decision, and communication with the other domains to achieve a defense. The routers in the domain of the system are to deploy security router as packet forwarding, monitoring and filtering. And the SPDS policy decision part, just mainly about the mechanisms of the Policy Management security policy.

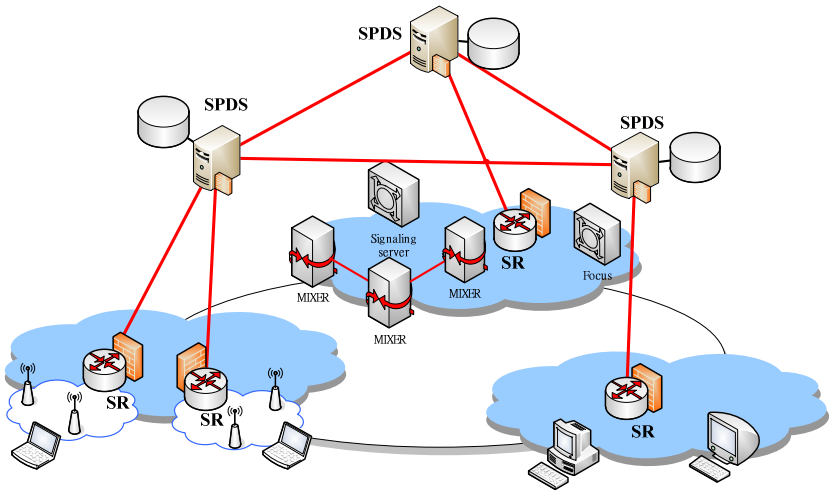

Fig. 1. The system architecture of distributed protection device

B. The Policy Management

Aib, [1] proposed an architecture be called Policy Simulator. The operation of the Policy Manager starts when all new events are loaded. In this architecture, we placed in a framework of SLA management mechanism and set its security policy according to the Business of behavior, as shown in Fig. 2.

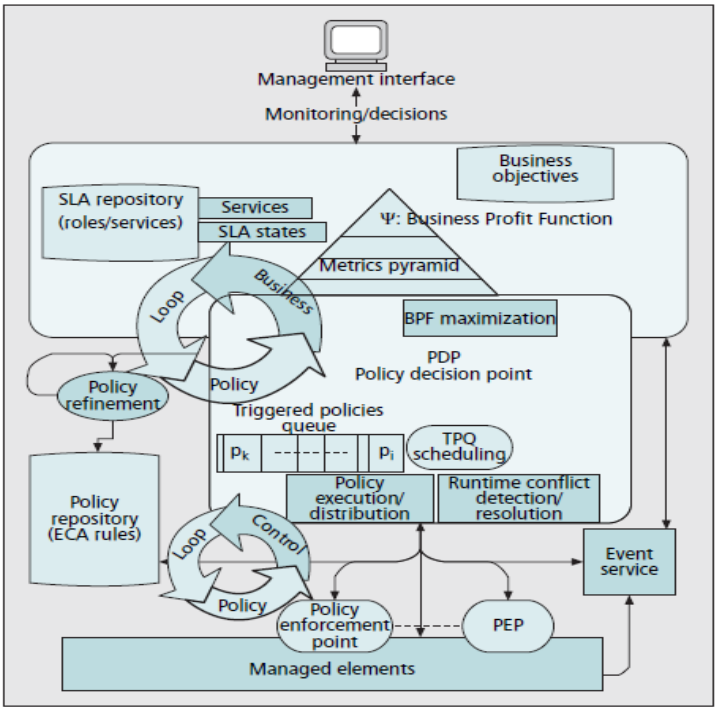

Fig. 2. The architecture of Policy Simulator

3 The System Architecture

3.1 System Environment

This paper proposed to provide network security and defense services by the Internet Service Provider industry (ISPs), the network security defense system built on the original core of the network structure of the ISP. The Fig. 3 is the system environment in this paper. In this figure, the bottom of the system environment for the Internet Service Provider (ISP) is the inherent network structure. The gray cloud, said Internet service provider's core network (Core Network), and in the core network border has a router to connect to each domain. The internet service providers in order to provide network security and defense services to the inherent network structure, setting up the defense system on the entrances and exits of each domain of the core network border router which mainly responsible for network monitoring and defense of each domain. This system called security Router (SR), and the defense domain was monitored as the security domain (security domain).

For the purpose of collecting the network attacks information in a distributed environment, there are more than one security monitoring system to monitor each domain. Furthermore, in the core network can build a security decision center for the policy-making and decision-making, not only collect the network monitoring information but also manage and control the defense system for the SR. The network security decision-making center is through setting a few security policy decision-making systems (security Policy Decision Server, SPDS) which consist of decision-making center. The aim is managing the SR which in their security domain distributed in order to achieve load balancing.

In the Fig. 3, the systems environment context diagram has the solid line and the dotted line, where the solid lines represent the Internet Network, which is the network used by the general user (or customer), while the dotted line represent the private network of defense systems which known as the security Management network also as a communication network between the SPDS and SR devices. There are many different customers in each security domain, and their network security needs are different, as shown in Fig. 3, presents the customers in the security domain may be general user, enterprise or factory and so on.

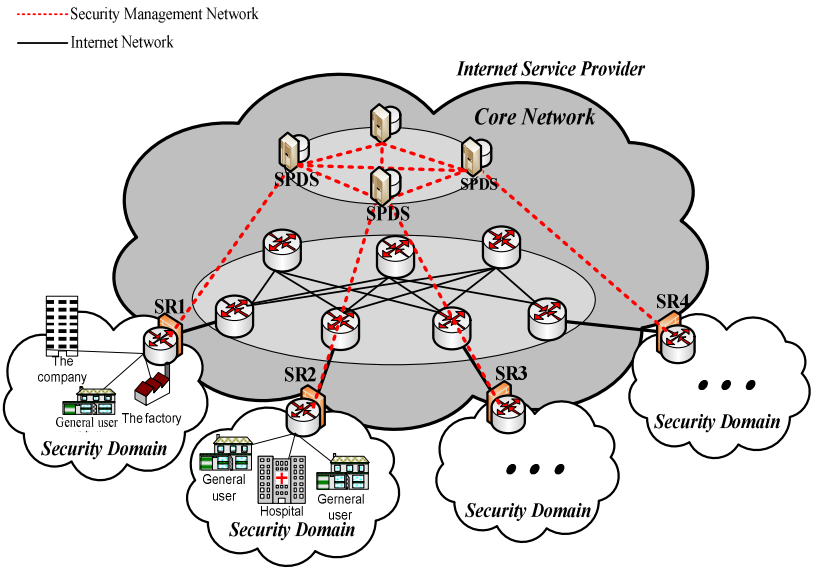

Fig. 3. The system environment

3.2 System Architecture

Network security defense system architecture diagram is divided into two physical components, namely, the defense system (Security Router) and security policy decision-making system, the system works according to our research previously. As shown in Fig. 4.

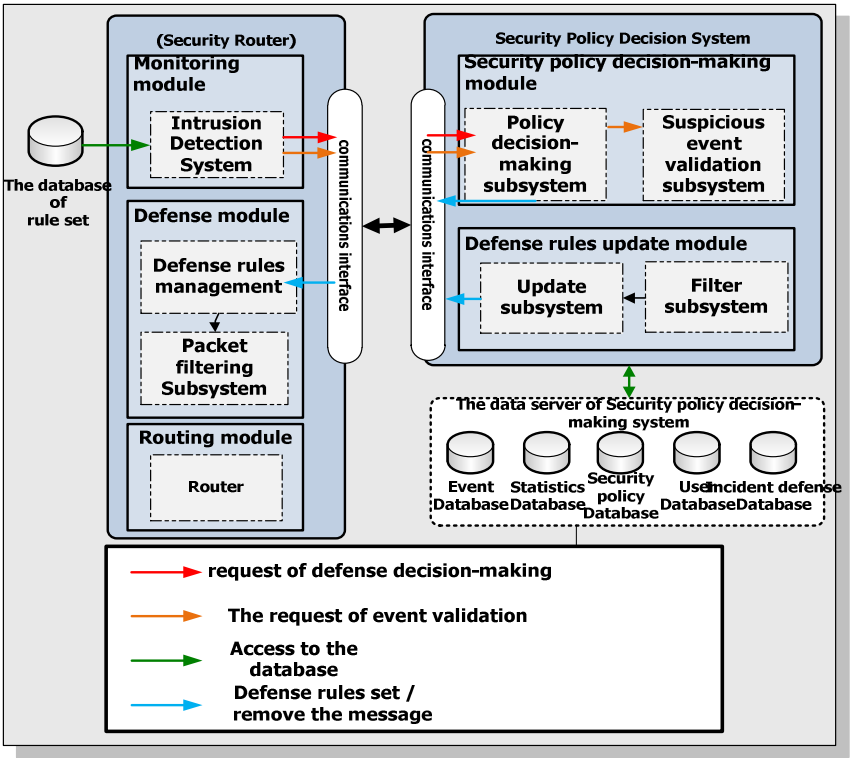

Fig. 4. The network security defense system

4 The Overview of the Defense Resource Management

The defense resources mentioned in this paper refers to the defense module of the defense system (SR), which is used to set the defensive rules, but the resources of the defense system has the limit. However, there are many different demands of customers in each security domain. It means that when the customers increase, the SR has to protect these customers by using more defense resources because each customer's demands are not the same. Owing to the proportion of defense resources for each customer is not the same, when the defense resources become saturation, how to allocate defense resources will be the important issue.

The following will explore the design of the mechanism about the defense resource management, and the network security defense system mechanism show as the Fig. 5.

One of the properties of “Provider Resource” refers to the resources of the defense system, another property of the “user requirements” means the defense requirements of customers, and the “Service Policy” as a service provider business strategy. In this paper, the service strategy of network security and defense services is to get the best interests and benefits for the service providers. So, we will explore how to allocate the use of the fixed defensive resources in order to achieve the best results. The service management mechanism is a mechanism of the entire system operation, and the

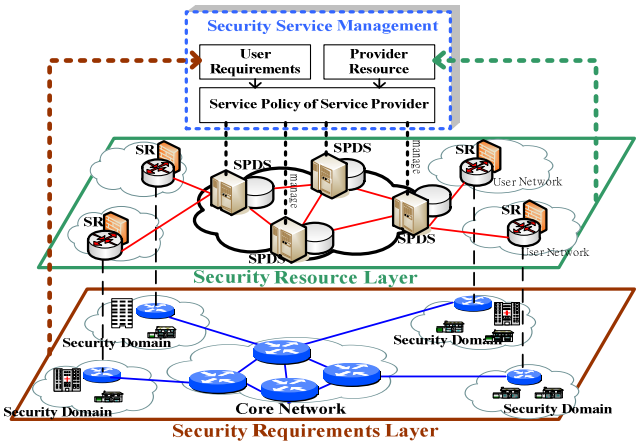

Fig. 5. The service management mechanism

defense resources management also belongs to. So the defense resource management mechanisms must be user demand-oriented, as well as according to the service strategy to manage defense resources.

5 The Network Security and Defense Services

A. Service environment modeling

First, we assume that the system module of the network security defense system is hardware-based filtering system or firewall system, and the maximum available defense resources for the defense module is . Furthermore, we assume that the defense module processing performance is not affected by the number of flow size and defensive rules, within the maximum available defense resources.

Assuming that the network service provider industry provide network security and defense services, in accordance with the common network attack types, which can provide several event types of projects for defense to customers to choose such as Table 3. And the maximum available defense resources for the network security defense system which service provider industry provided is .

As the charges of the service, the service provider is analyzing the characteristics of various types of attacks, then further analysis of the degree of damages for customers, and develop the hazard rating, charges ( ) and the compensation ratio ( ); For the service provider, there were two sets of fee for the different needs of customers, one is the general-type customer and another is enterprise-type customer, However, the hazard rating of the characteristics of both types and the level of charges are different, such as Table 1, and Table 2.

When a customer selected a type, then it will have an SLA contracts to be corresponding to the customer, For example, when a customer was selected general-type, then the SLA contracts will be such as shown in Table 3. The customers will be able to choose the services in the SLA project according to their demand, and to sign a contract with the service providers to complete the purchase of services process. The

service providers also can provide the PTP information, which is including the costs of the defense services and the service time, such as shown in Table 4. The information of costs is to indicate that how many resources must be using when the services projects set up the defense, that is, it means how many rules need to set up. The information of defense time is means that how long the defense rules exist for the defense services. However, in the service provider part of the balance sheet of income and compensation planning for the month of settlement, In other words, it will calculate the total revenue and the total compensation in each month.

The total revenue is the total of the fee paid by all customers, but the total compensation has to determine whether there is a breach of customer needs, The criterion is decided when the attack behavior is detected. If there is not take the defense during a certain time, or there is take the defense but less than a threshold, then it will be judged as not to meet customer needs. Finally, it will to sum all the compensation for all unmet customer service projects, which is the total amount of the compensation of the service provider. As to the total gain, the total gain is the total income after deducting the total compensation.

B. The model of the defense resources usage

This part will analyze the overall operation of the system behavior for the use of defense resources to develop the formula of statistical analysis. This paper presents a scheme for the system management and resource allocation according to the service strategy, which means that the behavior of the overall system operation and the use of resources for defense must be consistent with the goal of the service strategy.

In this paper, the target for the service provider is to get the best benefits, which is to get the best profit. According to the modeling of a service environment mentioned before. We assume that the best benefit the service providers get, the less the amount of compensation is. So, the goal of the statistical analysis is to strive for the maximum benefit basically, and to pay the minimal compensation to customers for the service provider.

However, the need of compensation is decided on whether to meet the customer needs. To meet the customer needs, the service provider need to consume defense resources to defense attacks but do not require compensation to customers; if not, then it do not consume resources to defense attacks but need to compensate customers. The decision-making parameters of statistical analysis is whether the defense to meet customer demand.

The formula of statistical analysis is based on the mode of operation and limitations of the overall system, such as the usage of the defense resources must be lesser than the maximum available, in the meanwhile, when the defense services that the customer does not need and the attack event which has not occurred, then the service provider has not to take the defense. Before introducing the model of defense resource usage, we first described the parameters in Table 5.

The defense resource model developed under the above conditions is as follows :

1) Decision values :

$x_{st} = \begin{cases} 1 \\ 0 \end{cases}$, Represent that whether there are demand for the s customer in t defense services.

2) Objective :

$\max\left(\sum_s\sum_t \delta_{st}C_{st} - \sum_s\sum_t \sigma_{st}\delta_{st}(1-x_{st})P_{st}\right),\quad s \in S, t \in T$

3) Subject to :

$$\sum_e\sum_s\sum_t \varepsilon_{est}\delta_{st}x_{st}r_t \le F\ ,\ s \in S, t \in T, e \in E. \quad (1)$$

$$\sum_s\sum_t(1-\delta_{st})x_{st} = 0\ ,\ s \in S, t \in T. \quad (2)$$

$$\sum_s\sum_t \sigma_{st}(1-\delta_{st})x_{st} = 0\ ,\ s \in S, t \in T. \quad (3)$$

$$\sum_s\sum_t(1-\sigma_{st})(1-\delta_{st})x_{st} = 0\ ,\ s \in S, t \in T. \quad (4)$$

$$\sum_s\sum_t \varepsilon_{est} = 1\ ,\ \forall e = 1, \dots, m\ ,\ s \in S, t \in T. \quad (5)$$

$$\prod_e(1-\varepsilon_{est}) = (1-\sigma_{st}),\ \forall s = 1, \dots, n \quad \forall t = 1, \dots, 5 \quad e \in E. \quad (6)$$

The objective of the analysis of the defense resources model is getting the maximum benefit; the model has following six limitations :

(1) The usage of resources must be less than F.
(2) During the first **s** customer in **t** defense type has no attacks (σ_{st}= 0), the x_{st} equal 0.
(3) When the first **s** customer in **t** defense type has no demand (δ_{st}= 0), the x_{st} equal 0.
(4) When the condition conform the limitation (2) and (3), then the x_{st} also equal 0.
(5) Each event will only attack one customer, and only belongs to one type of event;
(6) As limiting the first s customer in t defensive types of projects (σ_{st}), which is 1 when the events occurred, and 0 represent not events occurred.

Table 1. The hazard rating of the general customers

Hazard level (l)	Harmful behavior	Charge	Compensation ratio
1	Be unauthorized manipulation of the computer (or server)	NT$ Rev_1	P_ratio_1
2	The confidential information of individuals (or organizations) was stolen	NT$ Rev_2	P_ratio_2
3	Attacker detection the device weakness (the device can be computer or server)	NT$ Rev_3	P_ratio_3
4	Be attacked by multiple sources, resulting in the system (or service) operate abnormal	NT$ Rev_4	P_ratio_4
5	Cause the system (or service) operate abnormal	NT$ Rev_5	P_ratio_5

Table 2. The hazard rating of corporate customers

Hazard level (l)	Harmful behavior	Charge	Compensation ratio
1	Be attacked by multiple sources, resulting in the system (or service) operate abnormal	NT$ Rev_1	P_ratio_1
2	Cause the system (or service) operate abnormal	NT$ Rev_2	P_ratio_2
3	Be unauthorized manipulation of the computer (or server)	NT$ Rev_3	P_ratio_3
4	The confidential information of individuals (or organizations) was stolen	NT$ Rev_4	P_ratio_4
5	Attacker detection the device weakness (the device can be computer or server)	NT$ Rev_5	P_ratio_5

Table 3. The SLA example of the general customers

Select	Defense Services	Fee / compensation
	Denial-of-service (DoS)	NT$ Rev_5 / -NT$ P_1
	The Distributed Denial-of-service (DDoS)	NT$ Rev_4 / -NT$ P_2
	Vulnerability scanning (Scan)	NT$ Rev_3 / -NT$ P_3
	Backdoor (Spyware)	NT$ Rev_2 / -NT$ P_4

Table 4. The Protection Type Profile (PTP)

Number(t)	Defense type	Defense costs	Defense time
1	Denial-of-service (DoS)	r_1	$ProtectionTime_1$
2	The Distributed Denial-of-service (DDoS)	r_2	$ProtectionTime_2$
3	Vulnerability scanning (Scan)	r_3	$ProtectionTime_3$
4	Backdoor (Spyware)	r_4	$ProtectionTime_4$
5	Trojan, Bot Detection and Prevention	r_5	$ProtectionTime_5$

Table 5. The parameter description Table

Parameter	Explain	Value
E	The collection of events detected during a certain time	1,…,m
S	The customers collection, $S = S_1 \cup S_2$, $S_1$is the Collection for enterprise customers, $S_2$is the collection of general customers	1,…,n
T	As a defensive type collection	1,…,5
ε_{est}	When value equal 1, indicating that the target of the event for the e times attack is s customer, the type of event is t	0 or 1
σ_{st}	Represent that whether there are attacks during the s customer in t defense services	0 or 1
δ_{st}	Represent that the whether there are demand for s customers in t defense services	0 or 1
P_{st}	Represent the amount of **compensation** of the defense services of the s customers in t defense services	
C_{st}	Represent the amount of **charge** of the defense services of the s customers in t defense services	
r_t	Represent that defense type t need to consume how many of the defense resources (Eg: How many of rules the demand has to set ?)	
F	Represent the maximum available total defense resources for the defense system	

6 The Analysis of Defense Resources Usage

A. Fig.s and Tables

Based on the above planning service environment, as well as refer to the statistical results of the attack with intent [6] and major network security company Network Threat statistics [7] [8] to conFig. the types of fees and compensation, further to conFig. each network attacks and the proportion of the types of customers, to do the statistical analysis of the behavior of defense resources usage. In addition assume that the network service provider to provide network security and defense services, which the available resources of the defense system is 2000 (F = 2000). Table 6 and Table 7 are the parameter settings for each fee type. Table 8 represent the PTP information set.

The following analysis will be mainly focus on the defense resources of a single security domain, analyze the resource usage by using the model which we proposed. The following major analyze the influence between the number of services and profit for different types of customers, which control variable is to control the proportion of customer types, the operating variable is the number of customers in the security domain, and the fixed factors are the maximum available resources for the defense system, the number and proportion of each event type when the events occur.

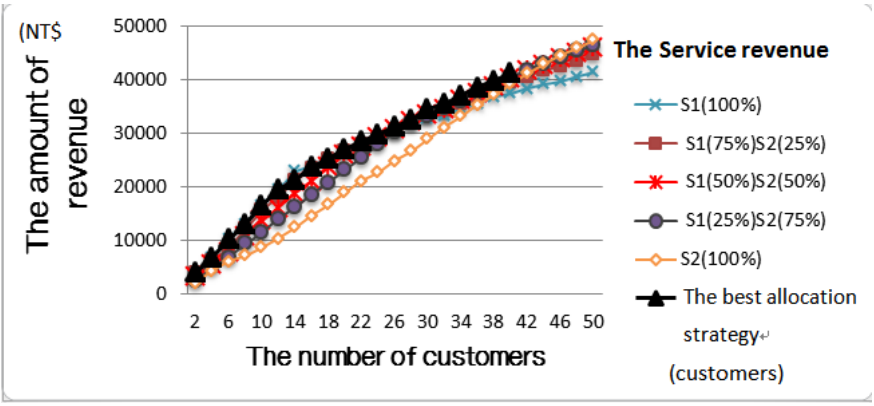

Fig. 6. The chart of Service revenue

Table 6. The hazard rating of the general customers

Hazard level (l)	Harmful behavior	Charge	Compensation ratio
1	Be unauthorized manipulation of the computer (or server)	NT$ 400	50%
2	The confidential information of individuals (or organizations) was stolen	NT$ 350	45%
3	Attacker detection the device weakness (the device can be computer or server)	NT$ 150	40%
4	Be attacked by multiple sources, resulting in the system (or service) operate abnormal	NT$ 200	15%
5	Cause the system (or service) operate abnormal	NT$ 150	15%

Fig. 6 indicates that represent the proportion of enterprise customers, and represent the proportion of general customers. This Fig. can be seen the more proportion of enterprise customers, the more pre-earnings will be. When the defense resources become the full load, the earnings growth will be less. In the late, the lower proportion of enterprise customers will be more income. For the service provider's point of view, we can make an inference to the ideal situation based on the above data. The ideal situation is no matter how many the customers are, the amount of the proceeds must be the best. After analyzing the allocation strategy of the various types of customers,

we found that when the defense resources is sufficient, we can give the priority to accept the enterprise customers, when either adequate defense resources, began to accept the general customers, but no longer accept enterprise customers, as the triangle curve in Fig. 6.

The statistical analysis data of the best allocation strategy to compare the other five types of the different proportion of customers, we found that the best customer allocation strategy with the type of 〔 (25%), (75%) 〕 proportion, their final income and the number of customers is the most similar. So use the strategy that the final proportion of customers will be close to 〔 (25%), (75%) 〕.

Table 7. The hazard rating of corporate customers

Hazard level (l)	Harmful behavior	Charge	Compensation ratio
1	Be attacked by multiple sources, resulting in the system (or service) operate abnormal	NT$ 650	95%
2	Cause the system (or service) operate abnormal	NT$ 500	90%
3	Be unauthorized manipulation of the computer (or server)	NT$ 400	80%
4	The confidential information of individuals (or organizations) was stolen	NT$ 380	75%
5	Attacker detection the device weakness (the device can be computer or server)	NT$ 100	50%

Table 8. The Protection Type Profile (PTP)

Number(t)	Defense type	Defense costs	Defense time
1	Denial-of-service (DoS)	5	5-days
2	The Distributed Denial-of-service (DDoS)	8	5-days
3	Vulnerability scanning (Scan)	1	5-days
4	Backdoor (Spyware)	4	5-days
5	Trojan, Bot Detection and Prevention	6	5-days

7 Conclusion

In this paper, according to the operation of the overall system, we propose a model for defense resources management basis on the behavior of the usage of resources, and further assume that the service environment and the analysis of defense resources usage. We found that the more proportion of the enterprise customer, the more initial income will be, but with increasing in the number of customers will make the resources into full, the growth of earnings will become slower. Through the observation of a variety of data of the proportion of customers, and to design the best strategy to satisfy the customer's demand from the provider perspective. As for the best strategy for defense resources, when the resources are sufficient, then priority by adding enterprise customers, when the resources became the full load, began to accept the general customers. Finally, as the load of resources become full, we can choice one type of allocation of defense resources to design a defense resource management mechanism, while in the future, we can based on the above results applied to defense system of resource management to implement.

References

1. Aib, I., Boutaba, R.: PS: A Policy Simulator. IEEE Communications Magazine 45(4), 130–136 (2007)
2. Su, H.-K., Yau, Z.-Z., Wu, C.-S., Chen, K.-J.: Session-Level and Network-Level SLA Structures and VoIP Service Policy over DiffServ-Based MPLS Networks. IEICE Transactions on Communications E89-B(2), 383–392 (2006)
3. Marilly, E., Martinot, O., Betge-Brezetz, S., Delegue, G.: Requirements for service level agreement management. In: Proc. IEEE Workshop on IP Operations and Management (2002)
4. Yu, M.-R.: Implementation of SLA-Based Security Policy Management for Cooperative Defense Network (2010)
5. Chain, J.-S.: Design of SLA-Based Cooperative Security and Management Mechanism on Soft Network. In: TANet 2008(2008)
6. Lee, W.-H.: On Investigation of Malicious Software's Activities - A Case Study on a Company's Internet Connections (2005)
7. Taiwan Computer Emergency Response Team and Coordination Center, `http://www.cert.org.tw/resource/`