2010 Second International Workshop on Education Technology and Computer Science

New Network Security Based On Cloud Computing

Weili Huang
Information and Electron Department
Hebei University of Engineering
HanDan,China
997518268@qq.com

Jian Yang
Information and Electron Department
Hebei University of Engineering
HanDan,China
yjbs11@126.com

***Abstract*—In this paper, we will have the combination of cloud computing and network security to research "cloud" firewall technology. Comparing the "cloud" firewall with the traditional firewall to further study the cloud computing, architecture and virtualization technologies in the "cloud" firewall. It will show the new concept of network security to the readers , which is about its advantages, development trends and possible risks .**

Keywords-Cloud;Firewall;CloudComputing;Cloud Terminal;Virtualization;Network Security

I. INTRODUCTION

Our requirements for the network environment was not limited to passive defense, so based on the current most popular cloud computing technology, a new generation of firewall technology, "coming with the clouds ." Cisco believes that the emergence of cloud firewall ,which means that the birth of the fifth-generation firewall, the former four generations are: software firewalls,hardware firewall, ASIC firewalls, UTM. SensorBase is the precondition of cloud firewall, it is the data center in the cloud and the largest email traffic monitoring network in the world, providing real-time view of global security threats and the "credit reporting service" of e-mail, SensorBase added botnet dominated database to enable it to monitor botnet sensitive development[1].

The key technology of cloud firewall is based on cloud computing."Cloud" has a considerable scale,and the provider will build sensors on the major network operators. Cloud computing supports users to use a variety of terminal to get application services in any position. By the cloud computing , we can make better use of network, as long as you are in the "cloud". You can make full use of the "The Top of Cloud" on your terminal , and we always keep in touch with other terminals in the "cloud" , so if it is found somewhere in the attacks, immediately the some terminal notifies the other places to stop the attacks and deploy plans. This is the core idea in the cloud firewall —— it will turn the passive protection into dynamic, collaborative and proactive protection.

II. CLOUD FIREWALL INTRODUCTION

A. Tthe Principle of Cloud Firewall

The most essential feature of cloud firewall is its dynamic and intelligent, and its technology is to take full advantage of "cloud" to sample and share threat informations dynamically and in real time, which ultimately we can realize active and re-active security services. The whole "cloud" is a large group, in this group there is a largest "competent department", which is known as the "The Top Of Clouds".It can collect detailed information threats on the Internet constantly, including the continuous attacks, botnet harvest , malware outbreaks and DarkNets and so on. By passing these real-time information to the cloud firewall, you can filter these attackers before the malicious attackers have the opportunity to damage the important property.

978-0-7695-3987-4/10 $26.00 © 2010 IEEE
DOI 10.1109/ETCS.2010.491

However, these search behavior and passing behavior are based on cloud computing principle, it will turn a large computing program into numerous small subroutines automatically, and then they are assigned to the large system which is made with a lot of servers.These subroutines were searched ,calculated and analysed to pass the consequence to users.Every user can apply to join the "cloud", as long as you are in the "cloud", you will be able to receive timely security information coming from clouds and processing methods, and you also participated in the transmission to achieve cooperative transmission. By this technology, network service providers can deal with tens of millions or even billions of dollars of information in seconds.It is like "super computer". As shown in Fig. 1[3]:

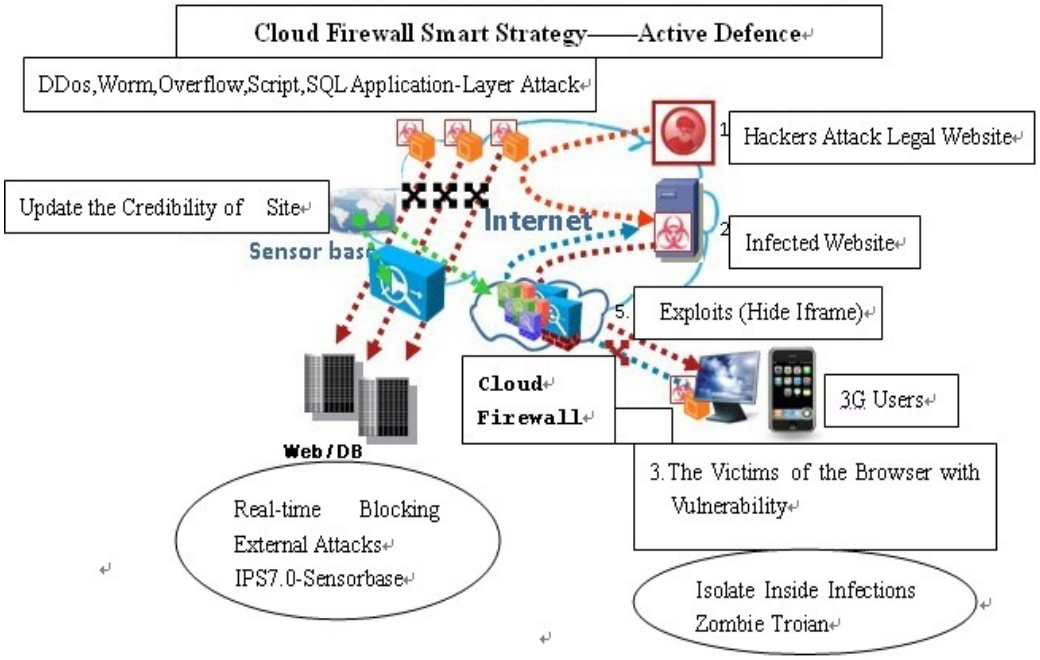

Fig. 1 The Active Defense of Cloud Firewall

So, the defensive and aggressive attack of cloud firewall is just like the following codes to show（quote "Microsoft Intemet Controls" in the project）：

```
Dim dWinFOlder As New ShellWindows
Dim eventIE As
SHDocVw．IntemetExplorer
Dim objlEAsObject
For Eachobj~EIndWinFolder
Set eventlE=objlE
eventlE．Quit ．
Next
```

By these codes,the personal firewall which is based on cloud security is like a big hand.When you open a malicious link,the cloud firewall will push you to a safe area forcibly, that is to say,it is redirected to a safe URL or HTML documents which we are designed; and it is like a car towing rope, when the car bogged down in the quagmire, the cloud firewall will put you out[2].

B. The Features of Cloud Firewall

The top of cloud and these small users endpoints are just like antennaes, and constantly they explore useful information,thus breaking the protection of traditional firewall , which is passive and waiting.Just for the attack, the traditional firewall is completely passive defence, and it does not know where is the attack and how to attack. The core of the firewall is static rule

protection,that is to say,after the customers buy a firewall, the suppliers configure matching security policy which is according to customer's requirements.Compared with traditional firewalls,the cloud firewall updates static protection strategy dynamically to add proactivity to network security,it has some significant features[4]:

- Firstly, the cloud firewall freezes botnets. For one thing , the cloud firewall can find malicious Web site in a short time relatively to stop users to access to these sites; for the other thing, if the users' computers become "zombie" or have Trojan Horse, the cloud firewall can stop the computers to send external master site information.
- Secondly, the cloud firewall let the world's IPS be Intelligent linkage. The top of cloud was added botnets master database and dynamic strategies to SensorBase to monitor the dynamics of botnets sensitively.If some Internet address have some questions,it will be blocked, and the top of cloud will try to update the information of SensorBase in the shortest time.
- Thirdly, the cloud monitors Netflow V9 to achieve NOC / SOC combo. Netflow provides a session-level view of network traffic to record every service information from TCP / IP . Its function includes abnormal traffic monitoring, high-speed sampling and timed control ,the amalgamation of network and security, the standard network element management.

III. THE CLOUD COMPUTING IN CLOUD FIREWALL：

A. About Cloud Computing：

Cloud computing is still in its infancy currently.About the definition of cloud computing is still controversial, which are multiple versions, so far there is no one conclusive. Cloud computing is not a specific technology, but a computing concept or a computing model. Cloud computing is the development of parallel computing, distributed computing and grid computing , or it is commercial realization of the concept of computer science. Cloud computing is the mixed-jump result of the evolution of concepts of virtualization, utility computing, IaaS, PaaS, SaaS[5]. It has huge scale, virtualization, high reliability, commonality, high scalability and service on demand. Large scale is its greatest feature,the key of cloud computing is to have enough information collection points and computing capacity.That is to say,usually for the large data calculation, we can divide it into many small sub-blocks to many computing terminals which are in the "cloud". So we can get a large-scale computing system, and the computing capability of this system is better than any high-equipped computer. In this computing model, all servers, networks, applications and other parts related with the data center are provided to the IT department and end-users through the Internet. Customers are only connected to the "cloud", they can access to infrastructure services, platform (operating system) services, or software as a service —— such as SaaS application, the "cloud" is possible to be the internal data center or computer which has the same function.

B. Computational Logic in Cloud Computing：

About n-term computing is defined[6]:F is a computing, and x1，x2，……,xn are n variable parameters for computing. So F is n-term computing, S is the result of computing,such as S = F (x1 , x2 , … , xn)；if a1，a2，…，an were the value data of x1，x2，…，xn, so S= F(a1 , a2 , …, an) is a calculation for F, and S is the result.

About n-term rule is defined[7]: If A1，A2，…，An are n antecedents, B is conclusion, which is called n-term rule as R, R can be expressed as "If A1 , A2 , …, An , then B" 。

Cloud computing as a whole calculation process is shown in Fig. 2:

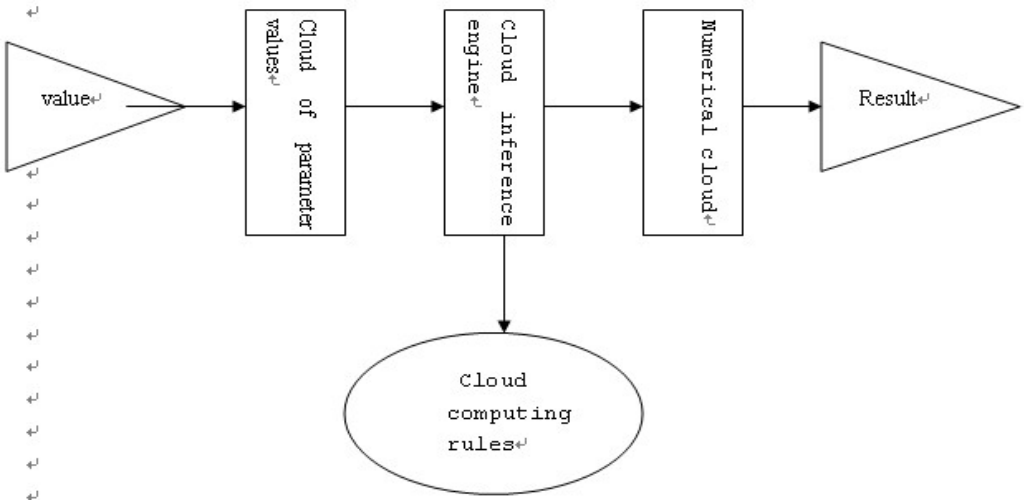

Fig. 2 Cloud computing process

C. Cloud Firewall Structure Based on Cloud Computing：

Cloud firewall is based on cloud computing, on-demand deployment is the core of cloud computing. So we have to solve the dynamic reconfiguration of resources, monitoring and automation of deployment, which they need virtualization technology, high-performance storage technology, processor technology, high-speed Internet technology as the foundation[8-9]. It is shown in Fig. 3:

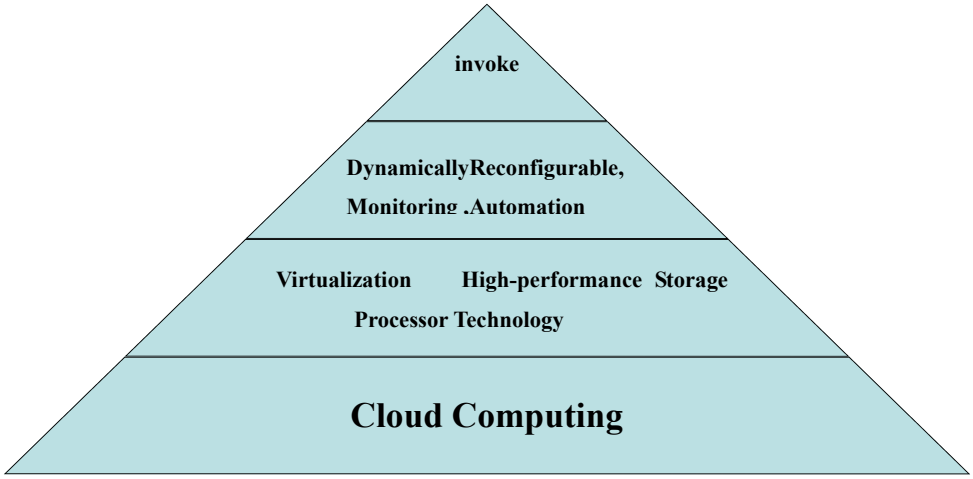

Fig. 3 The invoking structure of cloud firewal

In order to support cloud computing effectively, cloud firewall architecture must be autonomous, that is to say,they need embedded automation technology to reduce or eliminate manual deployment and management tasks, but it allows platform to respond intelligently to their

application requirements. Cloud computing structure must be sharp, which is able to make quick response for changes in the load and demand signal.In other words, the clouds cluster must be able to quickly respond to certain malicious attacks, and rapidly from one to pass to other points, to be co-processing.

Typically, "cloud" have a large number of servers, and resources are dynamic, and it need real-time, accurate and dynamic resource information. Cloud computing monitored and managed all the resources in the computing resources pool by a monitor server,and it configured and monitored every resources server by deploying “Agent” on all the servers in the cloud,and it can pass information data to the data warehouse regularly.Monitor server analysised the using data which is in the "cloud" in the data warehouse and tracked the availability and capability of resource,which offered information for the exclusion of lesion and the balance of resource[10-11].

D. Based on the File Reputation Technology：

The real technical focal point of "Cloud security" lies in how they do data mining for the collection of sample data , and then form a new identification technology in the clouds. After adding the concept of cloud security to firewall,the new cloud-client file reputation (CCFR) technology will become the users' focus.In the cloud security,the core is cloud-client file reputation,which is to change the mode to manually update the protection.For the ordinary users ,the cloud security which is based on the cloud-client file reputation can be understood:It reached interaction between "anti-virus vendor's computer cluster" and "user terminal" ,which can change the issue of the virus code into the uploading of the characteristics of the file to compare in the top of cloud.But it cannot upload the whole codes to compare,rather than features in the files.The whole process is just some milliseconds[12].

From general technology, CCFR reduces the updates of client-side in the traditional update-mode, most of these updates is now available "local or global" cloud scanning services, which would significantly reduce the re-update mode of the terminal system to minimize the download of anti-virus codes. Traditional client-side virus pattern updates, about 2-3 times per day, 2-3Mb download traffic every time , while the CCFR client cloud virus code only updates once a week, 2-3Mb every time. Precisely ,CCFR can decrease virus database in the client-side about 90%[13].

IV. TRENDS AND RISKS：

At present, the cloud firewall is still in the embryonic stage of development,and its application form had also presented very many kinds.One trend,which is to connect the user with the firewall software platforms closely by Internet in order to form a huge monitoring for Trojan / malicious software , spyware network. Every user will contribute to the firewall "Cloud security" , while sharing the results from the other users. This is similar to the P2P. If we can really dig into the user's enthusiasm , build a new security system is not impossible. But now, users don't still fully accept this cloud firewall, which means everyone's enthusiasm was not high .This is something we have to face.

Another trend ,is to set up a sufficient number of servers (tens of thousands or even more) in the world to collect application requests from global users in real time, and by the calculation in the top of cloud,it is to judge the safety of these requests. For example,a user requests to connect a corporate Web site. By a number of technical indicators ,the operator will determine whether the site's URL was normal and secure, whether the web links embedded in the text and Button were normal and secure, whether the user will be directed to non-performing Web site or lead to other dangerous behavior. If the site is secure, the user can link to, but if not, this link in the text will be block ,not the whole web page. Accordingly, the

problematic URL will also be added to the problem database in the top of cloud.Once the other users′ requests access to this data, according to the problem database ,"the top of cloud" can decide whether to allow the user to access by judging the data [14].

The first challenge cloud firewall faced was network environment issues. If security threats had emerged and destroyed the network connection, at this time, then no matter how strong "the top of cloud" to protect, the client's losses are inevitable. Second, the cloud security standards in the cloud firewall is still in a chaotic state, there is no uniform standard, various vendors are still fighting each other, vendors have their own standards.So the client may get a different judgement, which is harm to unify the cloud security in future. The root of these problems was that cloud computing has not yet been spread extensively, complete cloud computing environment is still not perfect.That is to say,the cloud security was born from the cloud computing will not lay a good foundation, so now cloud security environment is not safe enough , and only after the popularity of cloud computing , will cloud security begin truly.

V. CONCLUSION：

Cloud firewall is a popular form of security software, but it is a tightly fur products, we have to achieve the whole cloud security protection model finally, which is the real purpose. Because of the agility and high spreadability of the cloud security , it determined its security model is definitely the future development trend, and even the most difficult to guard against the so-called "zero-day attacks" [15] ,this hacker is also easy to be guarded. But, before cloud computing become mainstream,the cloud security will not lay a good foundation.That is to say,we will have a long road to real cloud security,which will need the strong support from all users and the unity from the major manufacturers.Only in this way,can achieve the real cloud security.

REFERENCES

[1] H. chih Yang, A. Dasdan, R.-L. Hsiao, and D. S.Parker.Simplified relational data processing on large clusters. In Proc. SIGMOD, 2007.pp.33-78.

[2] D. Patterson and J. Henessy. Computer Architecture.Morgan Kaufmann Publish-ers, fourth edition, 2006.pp.31-53.

[3] “Sectao” Website，(in Chinese) http://www.sectao.net/blog/index.php?go=category_2

[4] Pike R, Dorward S, Griesemer R, Quinlan S. Interpreting the data: Parallel analysis with Sawzall. Scientific Programming Journal, 2005,13(4),pp.12-30.

[5] Baidu Wikipedia Web，(in Chinese) http://baike.baidu.com/view/1316082.htm?fr=ala0

[6] T. H. Davenport and J. G. Harris. Competing on Analytics: The New Science of Winning. Harvard Business School Press, 2007.pp.44-50.

[7] Peng Liu, Yao Shi, Francis C. M. Lau, Cho-Li Wang, San-Li Li, Grid Demo Proposal: AntiSpamGrid, IEEE International Conference on Cluster Computing, Hong Kong, Dec 1-4, 2003.pp.80-121. (in Chinese)

[8] Guoding Yin，Hong Wei，Achieve the method of calculation of conception，Journal of Southeast University，2003（04）. (in Chinese)

[9] Boss G, Malladi P, Quan D, Legregni L, Hall H. Cloud computing. IBM White Paper, 2007.

[10] S. Ghemawat, H. Gobioff, and S.-T. Leung. The google file system. In 19th ACM Symposium on Operating Systems Principles, 2003(10).pp.43-44.

[11] T. H. Davenport and J. G. Harris. Competing on Ana-lytics: The New Science of Winning. Harvard Business School Press, 2007.pp.12-16.

[12] Xiangling Wang. Core Technology of Grid Computing. Tsinghua University Press.2006(11).pp.55-66. (in Chinese)

[13] H. Liu and D. Orban. Cloud computing for large-scale data-intensive batch applications. IEEE Computer Society, 2008.

[14] P. Shivam. Active and accelerated learning of cost models. In VLDB, 2006.pp.98-100.

[15] R. Sakellariou. Utility Driven Adaptive Workflow Execution.In Proc. 9th CCGrid. IEEE Press, 2009.