The integrated operation of the network security equipments based on HTTP

Songai Liu,Yizhuo Guo,Xiaoqi Yin
Department of Computer Science and Technology,
ChengDong College Of Northeast Agricultural Universiy
Harbin, 150025,China
e-mail: lucuse@gmail.com

***Abstract*—The paper introduces a device linkage system on firewall between the network side and the switch side of user host, and introduces the audit system connected in parallel between the hubs and switches. Then, the paper introduces a method based on HTTP packet recognition network security device linkage, which is a technology of information security intrusion detection and prevention based on the network. It is mainly used to solve the existing network security equipment linkage blocking technology limitation poor problem. Finally, the test result shows that the method is practical and effective.**

Keywords- component; Network information security; Device linkage; Intrusion detection; HTTP packet recognition; Rule matching; Block processing

I. INTRODUCTION

Nowadays, with the updating of network information, the contents of web pages are changing everyday. It has already become a hot technique in security studying area that how to ensure the dynamic internet information healthy and legal and how to judge and stop the bursting harmful contents.

Network auditing system, whose availability is better than application-layer firewall and working as the monitoring equipment, are usually paralleled to the switchboard so as not to cause any effect on network performance. People such as Zhao Xiaoming raised a distributed network security and protection system by setting the intrusion detection proxy and centralizing the control of the server. Such methods can only be effective after the event, because they belong to the traditional blocking method which is based on TCP reset. It can't accurately block the tunnel packets with bad links because it always lags, reduces the network transmitting rate and not easy to operate successfully.

Document [2-4] offers a integrated protocol by combining paralleling (such as intrusion detect system) and series (firewalls) equipments together, by which the linkage could be blocked with the help of server-client. However, such method will lag the block. The intrusion detect system detects the invasion only when it has broken into the inside of the network, and after that the firewalls in the gateway is informed to block the linkage. In this way, the inside of the network could have been infected by the virus already.

To the network auditing system, even if its bypass system has found out that users are accessing to the harmful web pages and has informed the firewalls to block the linkage, the uses can still browse the bad information because of the browser cache or the frequent change of the harmful pages' IP address. In a word, it is time-ineffectiveness. In this paper, in order to solve the time-ineffectiveness of the online blocking techniques caused by current network security integrated equipments, the "auditing system-firewalls" integration shortened the corresponding time in examining the illegal information.

II. INTEGRATED SYSTEM OF NETWORK SECURITY EQUIPMENTS

A. The structure of the system

The system is an integrated system about network security equipments including the firewall located between network hub and host's side switches, and the auditing system paralleled between the hub and the switches. When passing the hub through the network, the data packet will be intercepted both by the auditing system and the firewall. Either defined as http or not, the data packet will be sent to host if there is not blocking requirement from the auditing system within the set time. Being defined as http and asked to be blocked from the auditing system within the set time, the packet will be blocked, and finally the aim that the harmful information is blocked will be attained.

B. the process for integration

Intrusion Detection and Isolation Protocol, IDIP, used to quickly and automatically respond to the invasion in intrusion system and supporting information exchange within various kinds of network components, is corporately developed by NAI Labs、Boeing Phan tom Work and U. C. Davis. However the layout is, the current communicative mechanism is confined to one or one type of universal security protection system. After intercepted by the auditing system and the firewalls before arriving at host, the packet will be defined whether it is http by the firewalls and asked to be blocked from the auditing system within the set time to make a integrated comparison, in which the abnormal packet will be blocked. The details are as followed:

First, after the auditing system and the fire wall intercept the packet at the same time, they will analyze its http attribute, by which the integrated system will judge the blocking request sent from the auditing system.

Second, auditing system judges the blocking request: break and link the data packet, match and integrate it according to the contents and rules.

Third, analyze how long it will take to reach the firewall and process in the auditing system.

Published by Atlantis Press, Paris, France.

Fourth, breaking and linking the packet require both the firewall and the auditing system to do the matching analysis.

Fifth, block the packet. After analyzed, the packet will be dumped or substituted to be transferred.

Sixth, the network security equipments integrate. The time set in the firewalls is longer than the time it takes the auditing system to process and the blocking requirement to arrive at the firewall from the auditing system, then the integrated block will be done.

III. CARRY OUT THE INTEGRATED MECHANISM

In order to solve specifically the time-ineffectiveness when the auditing system integrates with the firewalls to block the harmful linkage online, the concrete way of how the integration of the network security equipments work are explained with examples.

A. firewall's filtration

In the method, the data packets are judged by firewalls (process S1~S5). The packet defined as http will be stored temporarily in a register (FIFO principle), marked with X. If the auditing system does not send the request for the block in a set time (marked with t_x), the packet will be normally transmitted and its record of temporary storage will be removed. However, if the auditing system does send the request for the block in the time, the packet will be discarded or transferred after being substituted with the removal of its record of temporary storage. If the packet is not http, it will be normally transmitted.

B. auditing system' process to the data packet

Router transmits the data packet by processed, swift, advanced distributed exchange or other ways. The capture of the packet takes the strength of both polling and interruption that kernel space and user space share the same area of the memory to catch the packet.

Illegal information or images may exist in IDC in LAN. In reference to the design of the distributed system and auditing system made by the main security vendors abroad to the contents of the website, the following several principles are used to test auditing system of the IDC about the contents of the website.

It could be expanded for the system's upgrade reform with the enlarging scale of IDC.

It can directly monitor 10Gbit/s' backbone linkage with as least 5Gbit/s' capacity, which is tested in the backbone networks of the information center in the school.

It is applied with modularized software structure and its functional modules are selected according to the practical needs for the future development of new functional modules as well as the improvement for the current system.

It is applied with complete bypass deployment. With those principles, in the process of detecting and blocking to the http packet, in which the domain name, signs, the feature of the image and key words are processed, the packet will be intercepted by both the auditing system which is paralleled between the hub and switch and firewalls when passing through the hub from the network.

The design of the structure of the auditing system is presented as follows: Figure 1 audit system internal structure design

C. disassemble and assemble data packets

After the data packet passes through the hub, it is intercepted by the auditing system and the firewall. Here is the analysis for the processing time of the network security equipments

The firewall judges whether the packet is http. If it is not, the firewall will normally send it to host. If it is, it will be temporarily stored in the register. The firewall will normally send the packet and remove the temporary record if it is not asked to block the linkage from the auditing system within the set time t_x ; if the auditing system sends the blocking request within the set time t_x , the packet will be discarded or transferred after being blocked and its temporary record will be removed at the same time.

In the process of disassembling and assembling the data packet, the logic, upon which auditing system decides to send the blocking request or not, is that: when disassembling and assembling the data packet, its result will be matched with the rules that has been set. The time for disassembling and assembling is m_x (usually several hundred milliseconds), and once the violation of the rules are detected, the request for the block will be sent to the firewall. It costs n_x (usually no more than 10 milliseconds) to arrive at the firewall from the auditing system. If there is no violation of the rules, the integrated operation will not be carried out. The set time t_x should be more than the combination of the time cost in the auditing system and the time when the request for the block is sent from the auditing system to the firewall ($t_x > m_x + n_x$) . The process mentioned above is calculated by milliseconds, so the several milliseconds' delay on the webpage won't be much a problem to the users.

D. 2.4 The effects of the application

Owing to the parallel connection of the firewall and the auditing system in the structure of the system, the http packet could be intercepted by both of them at the same time. The harmful linkage is blocked online, which stops the host from getting it by the mechanism of the firewall's judgment to the datagram protocol as well as the mechanism of temporary storage of http packet waiting for the blocking request from the auditing system. In this way, the system achieve the time-effectiveness of the blocking technique.

IV. PERFORMANCE TEST AND ANALYSIS OF THE INTEGRATED SYSTEM

A. the environment and process of the test

1) the testing environment

The testing environment builds in the school information centre computer room with 10 computers, one of which is

the server. Configuration: 9 PC, CPU: Intel(R) Core(TM)2 Duo CPU E7500 2.93GHz, memory: 2 GB, the operating system: Windows XP; CPU of the server: Intel Xeon E5620, one 2.4GHz, memory: 2*2 GB, the operating system: Linux 5.0.

Among them, there is a Secoway USG2220 firewall , a BDS3000-SG3 auditing system, IPtables, a hub, a H3C LS-3100-26TP-SI-H3 workgroup switch and a H3C ER6300 router together consisting of the testing environment. [7]

2)testing procedure

The auditing system-firewall integrated module, controlling every node of the Intrusion Detection System, sends one warning message from different attackers every Δt (ms) to the module which is totally of 3000 in which the frequency of illegal information from the outer network detected by the integrated module could be defined as: $f = 1/\Delta t(ms^{-1})$. In this way, those illegal information from the outer network is analyzed and processed, which develops into new rules that will be distributed to the corresponding integrated module on the "auditing-firewall" node.

In order to lower the bottle effect made by its own module's performance to the overall data transmit and communication mechanism to the largest extent, the analysis is simply conducted by putting the attackers' http packet into the blacklist.

B. testing results and analysis

1) testing results

Assuming that the average blocking message that the firewall gets from the auditing system is N, the responding speed could be defined as V. In its local network, within the interval of Δt , the speed for the "auditing-firewall" integrated equipments is $V = N/2 \cdot (t_x - 1000/f)(ms^{-1})$ Δt to 1,2,…,6(ms)

2) analysis of the results.

From the results, the frequency of the illegal information from the outer network detected by the integrated modules is less than or approaching to 0.2 m/s, the responding speed of the block is a little slow. With a high speed network, the integrated rate of the firewall and auditing system keeps at a good condition and when the frequency of illegal information from the outer network is more that 0.2 m/s, the corresponding speed can reach to 2.5 m/s as is shown in the chart 5,6. It shows that the integrated mechanism of the firewall and the auditing system enhances the speed of the retrieval and identification of the illegal information.

Based on those idea above, with the comparison of the data features and the chaotic features of the network attack frequency, the paper adopts two kinds of contrast to the average of the network illegal information attack. The integrated operation of the "auditing-firewall" sufficiently blocks the intrusion of the harmful information.[10] By the mechanism of temporarily storing http packet and waiting for the blocking request form the auditing system, the harmful linkage is blocked online, and in this way the host won't receive it and the time-ineffectiveness of blocking techniques is improved.

V. CONCLUSION

As is mentioned above, technicians of information security area can revise and remodel the method without detaching from the application and technical field of the "auditing-firewall" integration which applies to the current IPv4 and IPv6. Owing to the inherent defects of security techniques of the current network information, the method still couldn't prevent the illegal information from evading the detection of the security equipments because of the time difference resulted from data transmitting in blocking techniques. However, in a not very large LAN such as the detecting system of LAN, the method can fairly improve the contradiction between the responding speed of online blocking and network delay by analyzing the features of the intrusion and people's monitoring. The bottleneck that Linux fails to capture http packet as well as the packet loss when the data stream operates at a high speed in auditing system are all solved, which plays a critical role in improving in time-ineffectiveness in blocking techniques.

REFERENCES

[1] Wang yuying,chenping. Combination Timed Colored Petri Net-based Web service modeling, Computer Science, 2010, PP:152-155.

[2] Calin Ciufudean, Adrian Graur, Constantin Filote, etc. A new Formalism for Failure Diagnosis: Ant Colony Decision Petri Nets . Journal of software, 2007, PP:39-46.

[3] Sun Yong, Zhang Heng, Ma Yan, ELECTRONICS & IPv6-based intrusion detection and firewall linkage system Computer Engineering, 2008, pp. 152-154.

[4] Zhang Yueguo iron Ling, XUE Zhi, Li Jianhua. Linkage strategy mechanism based on the SNMP protocol network security equipment, information security and confidentiality of communications, 2003, 12: 36-37.

[5] summer high, Liu Bin for high-speed network intrusion detection system parallel TCP / IP protocol stack. Tsinghua University (Natural Science), 2011, pp. 942-948.

[6] Zhao Xiaoming, Zhang Xinxia based on network information security content audit system and related technology research. Aviation Computing Technology, September 2006, pp.:127-130.

[7] Li Mingxing, Heng Ping, Dong Peiwu. Research on artificial neural network method for credit application . Research Information Ltd (RIL) UK, 2004 , pp. 127-131.

[8] James M Varanelli, James P Cohoon. A two-stage simulated annealing methodology . Fifth Great Lakes Symposium on VLSI (GLSVLSI '95). USA: Buffalo, 1995, pp. . 50-53.

[9] Zhang Zhonghui, operation Jia-Qing Liang Yiwen. Linkage mechanism-based intrusion prevention system. computer age in 2006,pp.28-30.

[10] Ning Haibin. Campus network-based intrusion detection system design and realization .Peking University, 2008.

[11] Pan Wei, Li Weihua linkage model of network security design and application . Computer Science, 2006, pp.113-116.

[12] Liu Xing network attack frequency chaotic time series prediction [., National University of Defense Science and Technology, 2008.

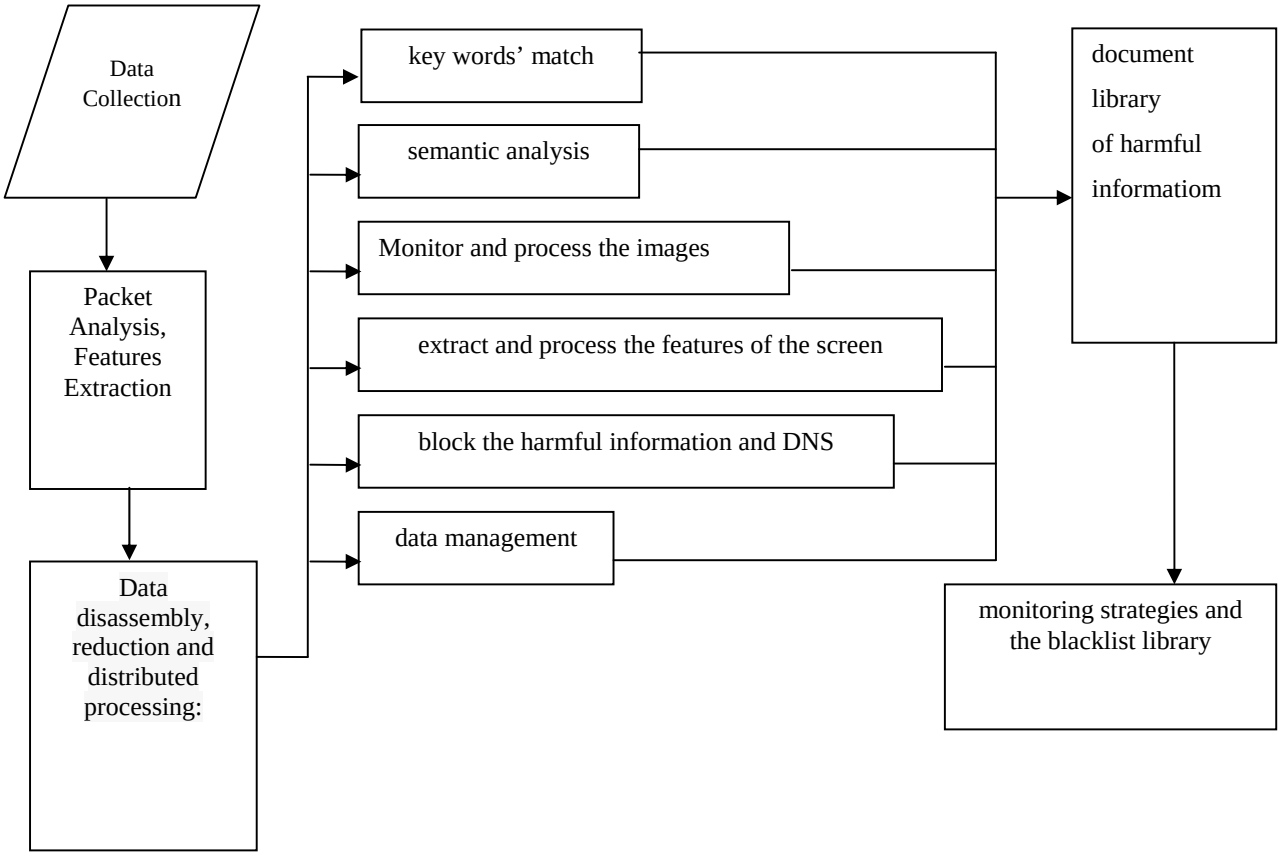

Figure 1. audit system internal structure design