Safeguard Intranet Using Embedded and Distributed Firewall System

Chu-Hsing Lin[1], Jung-Chun Liu[2], Chien-Ting Kuo[3], Mei-Chun Chou[4], Tsung-Che Yang[5]
Department of Computer Science and Information Engineering,
Tunghai University, Taichung 407, Taiwan
{ chlin[1], jcliu[2], g96350047[3], g96350011[4], g97357019[5]}@thu.edu.tw

Abstract

Due to the impact of the rapid popularization of Internet and e-commerce, most organizations and enterprises take great effort to protect their information systems against malicious attacks and invasions. The firewall is the most familiar method among relevant technologies for Internet security. However, the firewall systems in use today are either application software or utilities running on the personal computers or network nodes. It is very inconvenient to implement and manage the conventional firewalls. In order to make the management and construction of them easier without disrupting the existing network topology, we implement an embedded and distributed firewall system to safeguard the Internet. In this way, we combine the functions of the firewall and a central security policy server into an embedded system, which can be realized as a network interface card.

Keyword: distributed firewall, embedded system, central security policy server, conventional firewall

1. Introduction

The Internet and the e-commence are more and more popular in recent years. Researches on the network security technologies have become very important for both government organizations and business corporations [1].

To investigate the Security technologies in use, Gordon et al. show that use of firewall technologies is the most popular among their respondents in USA [2]. Use of the firewall technology is accounted for 97% of the 687 respondents. However, most firewalls in use are based on the conventional firewall architecture. They consist of either application software or utilities running on the PC or network nodes. The conventional firewalls are usually set up on the entry point of the network for the organization or corporation.

A number of serious problems of the conventional firewalls can happen. First, since these firewalls are set up in a single choke point, if the firewall is broken due to power outage or flooding attacks, all computers in the intranet will be disconnected to the Internet.

Second, the intranet threat is also a problem confronting Management Information Systems (MIS) in many corporations. For example, if an employee inadvertently opens a malicious e-mail from the Internet and infects his computer with a worm. Suddenly, all of the other computers inside the same intranet would be infected with the worm via this employee's computer.

Therefore, we propose to implement a Distributed Security System implemented with am embedded firewall to improve the efficiency of the conventional firewall. And this Distributed Security System is shown to not only have functions of conventional firewalls but also be able to work against intranet threats.

2. Background

The firewall technology can be classified into three categories [3-7]:

- Packet Filtering
- Stateful Inspection
- Application Proxy

The Packet Filtering is the earliest method used in the firewall technology. It often works in the Network Layer of the OSI network module. After it, the Dynamic Packet Filtering continues to work up to the Transport Layer of the OSI network module. This technology is used to monitor the Network Layer and Transport Layer, and analyze data of each packet, such as the header, the protocol, and the source address, etc. The firewall will then validate data by rules of the firewall filter. If a packet is judged to be denied, then

978-0-7695-3431-2/08 $25.00 © 2008 IEEE
DOI 10.1109/FGCN.2008.167

the firewall will drop it. However, this method is not always useful against flooding attacks.

The Stateful Inspection firewall uses a module called stateful inspection to intercept the data it needs in every OSI network modules. And the advantage of this technology is that the accessing and analyzing process does not affect works on any OSI network module, i.e. the firewall is transparent to the network users.

The Application Proxy technology operates in the Application Layer, i.e. the highest layer of the OSI network module. It can implement higher level of detection technology to defend Internet attacks. For data transfer, it uses a proxy server to transfer data from the source to the destination. This process can let the user feel that no lag existing when connecting to the server.

Fig.1 shows structure of the conventional firewall scheme commonly used in organizations and corporations. The network to decide whether to transfer data between computers and the Internet or not is controlled by the firewall group. However, this structure has weakness under flooding attacks. If the attack succeeds, the broken firewall will become the bottleneck for the network.

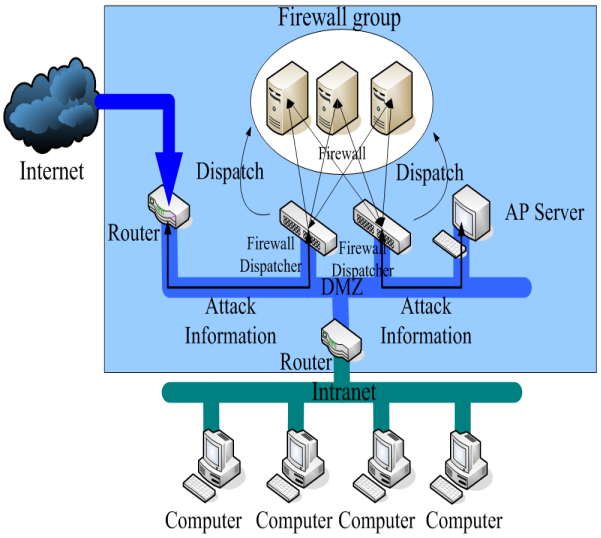

Figure 1. Structure of conventional Firewall scheme

On the other hand, Koch argued that the inside attacks causes more financial cost than the outside attacks [8]. Because of this, the personal firewall has become a new trend to achieve network security.

Bellovin proposed a Distributed firewall concept by using the all host firewall strategy to solve problems of the conventional firewall structure [9-11].

In this paper, our research is focus on transfer of the firewall work layer from Application Layer to the Data Link Layer. This concept is to try to reduce the influence created by the firewall to original processing works in the computer. Therefore, we will build a firewall structure together with an on-board processor and a memory network interface card. In the other words, we will build a firewall module inside the network interface device.

3. Structure of Distributed Security System

We design a Distributed Security System (DSS) structure to detect intrusions. In Distributed Security System, a number of design goals should be taken care of when implementing it.

First, the system should have a management mechanism, the central security policy server.

Second, it must be a general module design.

Third, the system should have both the functions of conventional firewall and the distributed characteristic for preventing attacks of the Internet and threats of the intranet.

In the DSS structure, the most important part is implementation of the personal firewall. We use an embedded system to implement this part. There are a number of benefits by using the embedded system. The embedded system has its own control processor unit and memory. It also has the network and USB interfaces. Therefore, we can build the firewall module on the embedded system by connecting the embedded system to the computer by USB interface and connecting the embedded system to the Internet by Network interface at the same time. We use the embedded system as a Network Interface Card (NIC).

Fig.2 shows the structure of the Embedded Firewall (EFW). The Central Security Policy Server (CPSP) is used to validate the firewall rule in EFW. EFW is used as a Network Interface Card (NIC). It responds to the rest of the network and the Client PC. The Client PC is a normal user in the intranet protected by DSS. And EFW is connected with Client PCs by USB transfer lines. Because of the USB interface, the embedded firewall mechanism is able to achieve the generic module design and EFW becomes a portable detection device.

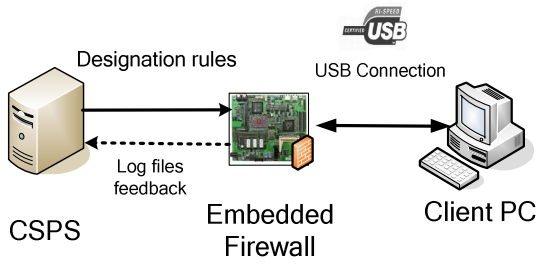

Figure 2. The structure of EFW

DSS consists of three mechanisms:

- Central Security Policy Management
- Embedded Access Control
- Intrusion Detection Feedback

Fig. 3 shows the structure of the DSS with the three mechanisms. The Central Security Policy Management mechanism can offer different levels of privilege for all the EFW in the system environment. The network manager can set up the level of privilege with different EFW. The mechanism leads to the goal of achieving level management.

The Embedded Access Control mechanism is used to control every EFW. All firewall rules on the EFW will be controlled by the CPSP. The CSPS can designate and change the firewall rule to the EFW. The mechanism enables the EFW to have the packet filter function. In this mechanism, the EFW can also return log files to the CSPS, if needed.

The Intrusion Detection Feedback Mechanism collects the log files from EFW. And then the mechanism sends the log files to the Intrusion Detection System (IDS), which analyzes the data of the log files and returns the result to CSPS. According to the returned results, CSPS adaptively changes the firewall packet filtering rules with each EFW. So, it can dynamically adjust intrusion detection rule for each EFW.

4. Results

We implemented the DSS with EFW structure on the embedded system with an Intel XScale processor PXA270, a USB 1.1 interface, and a 10M/100M standard network interface.

By setting up the rules of EFW, we verified that the embedded firewall system successful denied ping flooding attacks from the Internet. Furthermore, by setting the access right of the network, EFW was found to be able to control network activities of the intranet users.

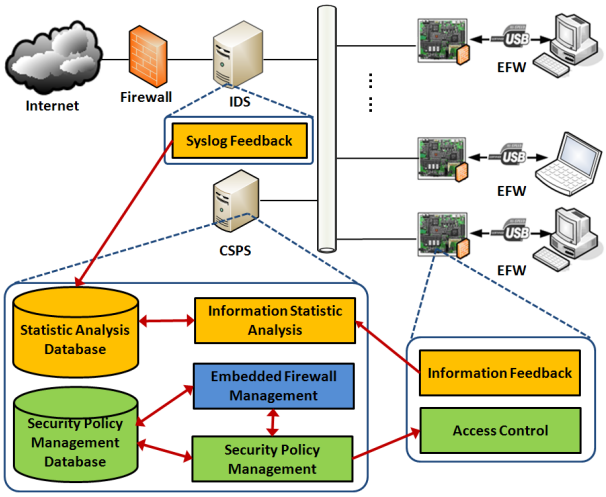

Figure 3. The structure of the DSS

We also tested our proposed structure under wired and wireless network environments. We downloaded ISO files with the file size over 2GB from a local FTP site. For the wired setting, the experimental results show that the average transmission rate can achieve 950KB/s between client PC and the Internet, which shows the efficiency of our EFW. If we replace the USB1.1 interface with USB 2.0 interface, we would be able to get much better results.

For the wireless setting, the experimental results show that the average transmission rate can achieve 550KB/s between client PC and the Internet, which is slower compared to the wired setting. The wireless network card changes the MAC address of packets, so extra time is spent to process packets coming through the wireless network.

5. Conclusions

In this paper, we propose a structure to implement the distributed firewall system. We implement the concept of the distributed firewall to effectively prevent attacks and threats from both the Internet and the intranet. And we also combine the functions of firewall and the central security policy server into the embedded system as a network interface card. The experimental results show our DSS with EFW structure achieve our goal of implementation of an independent firewall, which is portable and convenient.

For the future work, we plan to do stress testing on our proposed DSS with EFW structure to verify its robustness under a heavy load of traffic. Besides, we plan to do various types of attacks to validate that our proposed structure can be used to improve Internet security for users.

6. Acknowledgement

This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under grants NSC-95-2218-E-001-001, NSC-95-2218-E-011-015, iCAST NSC96-3114-P-001-002-Y and NSC95-2221-E-029-020-MY3.

7. References

[1] T. Holz, S. Marechal, and F. Raynal, "New threats and attacks on the World Wide Web," Security & Privacy, IEEE Volume 4, Issue 2, March-April 2006, pp.72 - 75

[2] Lawrence A. Gordon, Martin P. Loeb,William Lucyshyn and Robert Richardson, "CSI/FBI Computer Crime and Security Survey," 2005. Available at http: //www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf.

[3] R. W. Cheswick and S. M. Bellovin, "Firewalls and Internet Security: Repelling the Wily Hacker.", Addison-Wesley, 1994.

[4] M. R. Lyu, and L. K. Y. Lau, "firewall Security: policies, testing and performance evaluation," The 24th Annual International Computer Software and Application Conference, COMPSAC 2000, pp.116-121.

[5] R. Zalenski, "Firewall technologies," IEEE Potentials, Vol. 21, Issue 1, 2002, pp.24-29.

[6] Linux Firewall Project: Available at http://www.linuxfirewall.org

[7] R. Zalenski, M. Boucher, J. Morris, and H. Welte, The netfilter/iptables project, Available at http://netfilter.samba.org

[8] L. Z. Koch, "outsourcing Security," ZDNet Interactive iWeek, June 22, 2000. Available at http://www.lzkoch.com/column_06.html

[9] Steven M. Bellovin, "Distributed Firewalls", Journal of Login, November 1999, pp. 39-47.

[10] F. Stevens, T. Courtney, S. Singh, A. Agbaria, J. F. Meyer, W. H. Sanders, and P. Pal, "Model-Based Validation of an Intrusion-Tolerant Information System", from the 23rd Symposium on Reliable Distributed Systems (SRDS'04).

[11] M. Atighetchi, P. Rubel, P. Pal, J. Chong, and L. Sudin, "Networking Aspects in the DPASA Survivability Architecture: An Experience Report,",Fourth IEEE International Symposium on Network Computing and Applications (NCA'05)27-29 July 2005, pp.219 - 222