Design and Implementation of Linux Firewall Based on the Frame of Netfilter/IPtable

Baoliang Wang, Kaining Lu, Peng Chang
School of Electronic and Information Engineering
Tianjin University
Tianjin 300072,China
wangbl@tju.edu.cn

***Abstract*—With the constant development of network technology today, network not only brings us a convenient and efficient life, and is accompanied by a variety of network security problems. Firewall, as a main way to prevent network attacks, is often used to prevent illegal connection and separates the internal network from the insecure networks, to protect the safety of the Linux systems which used in small and medium-sized enterprise. In this paper, the main content is to complete the function of firewall which is based on the Linux operating system, using Netfliter as firewall architecture, and the IPtable as a user space module tool. Firstly, this paper briefly analyzes the Netfilter/IPtable architecture and princIPle and working process of state detection technology, then, configure the firewall. At the last, the firewall experiment verified the effectiveness and safety of the design of the firewall.**

***Index Terms*—Linux; firewall; network security; state detection; Netfilter/IPtable.**

I. INTRODUCTION

With the rapid development of information technology, there are a lot of network security threats in our daily work. In recent years, all kinds of network security events break out continuously, such as the leaks of 12306, Prism Event, etc., which are warning us that the network security problems should be given attention[3-4]. According to monitoring data, every day hundreds of thousands of hosts are used by these hackers to launch DDoS attacks unknowingly, and there are tens of millions of hosts are suffering DDoS attacks[1-2]. Firewall, which is a main way to prevent network attacks, is often used to prevent illegal connection and divides the internal network from the insecure networks [5]. For most venture companies and small businesses, there is a serious need of network firewalls to ensure the data safety of the servers.

Linux system is a truly open operating system which has many advantages such as open source code, powerful network functions, no copyright infringement, and strong stability and high efficiency. This paper is to design a Linux host firewall based on the Linux system to meet the security requirements of small and medium-sized enterprises。

In this paper, the main purpose of firewall filter rules is to protect the security of enterprise Linux system Under the Linux operating system, using Netfliter as the firewall architecture and IPtable as a user space module tool to achieve the function of state detection, resisting common DDoS attacks and log records of the Linux firewall. Firstly, this paper analyzes the principles of Netfilter/IPtable architecture and the working process of state detection technology briefly, and then illustrates the effectiveness and safety of the design of the firewall via compiling the firewall Netfilter module, creating script file, configuring the IPtable firewall filtering tables, etc.,. All of that provides useful references for the next step development of the Linux firewall technology.

II. KEY TECHONOLOGY

A. Framework of Netfilter/Iptable

After the Linux2.4x, Netfilter/IPtable, which is a subsystem of the Linux kernel, is a new generation of Linux firewall mechanism [6-7]. Netfilter adopts modular design and has good expansibility. As the important tool module, IPtable is connected to the kernel mode of Netfilter architecture[8]. Netfilter is seamless conjunction with TCP/IP protocol stack, and allows the user to filter the datagram, address translation and processing operations[7]. Figure 1 shows the frame structure of Netfilter/IPtable.

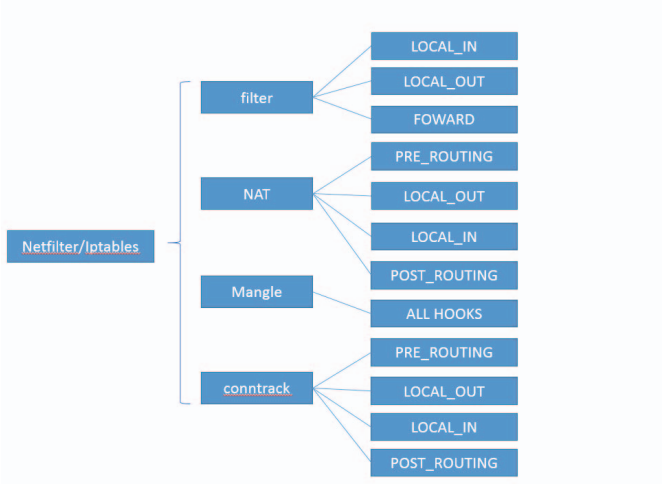

Figure 1 frame structure of Netfilter/IPtable

Netfilter is a function of working in Linux, which is usually expanded and implemented via modules in the Linux system. Users can load any modules in memory, or remove some

modules, which are not required, from the Linux through the module function in Linux. Netfilter is based on existing module in Linux [10], so that we can load or remove modules to control the functions of the firewall.

Net filter in Linux system is existed in two ways which are related and unrelated with IPV4 and IPV6. Files related to IPV4 are stored in/lib/modules/2.6.32-431.el6.x86_64/kernel/net/IPv4/netfilter, files associated with IPV6 are stored in/lib/modules/2.6.32-431.el6.x86_64/kernel/net/IPv6/netfilter. And the agreement files that have no relevant to IPv4 and IPv6 are stored in the path of /lib/modules/2.6.32-431.el6.x86_64/kernel/net/netfilter. They all have no related with the agreement, so the Netfliter can work in the environment of IPv4 and IPv6.

B. State detection technology

State detection technology is first put forward by the Checkpoint Company, and it can combines the efficiency and security of the packet filter. A state detection firewall will treat all packets that belong to the same connection as a whole data stream, and constituting them to the connection status table, and then monitoring the whole process of each connection to the end[13]. By examining the application information, the state detection firewall determine the port whether to allow the need for temporary open. The port is restored to a closed state at the end of the transmission and complete the packet detection and filtering to maximize the security of the network. State detection technology has also improved the flow processing speed. When the state detection firewall intercept packets, it will check whether these packets belong to an effective connection in a state table, if so be that these packets, which belong to the data flow, have been examined by safety rules, thus we just need to check whether the state of the data stream is correct[12]. Through this technique, we avoid the complex security rules of the examination and greatly improve the overall efficiency of the firewall.

The flow chart of detecting state firewall is shown in figure 2.

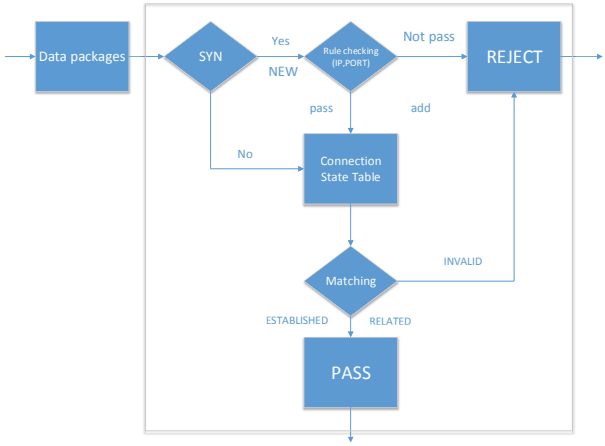

Figure 2 the flow chart of detecting state firewall

C. The logs of firewall

A log is some operations of the specified object of the system and a collection of the operation results which arrange chronologically. Each log file records a separate system event. A log is a text file that a user can read directly, which contains a time stamp and a message or other information that is unique to the subsystem [11]. Log is very important for system security, the user can through it to check the cause of the error occurred, or retrieve traces left by the attacker. The main functions of Log are: auditing and monitoring. It also can real-time monitor system status and track the intruder, etc.

Netfilter/IPtable provides the function of logging, which is used to record information flows in network packets. We can use -j LOG in the IPtable command to start the firewall logging function [9].

III. IMPLEMENT OF FIREWALL

A. Setting and implementation of the simulation environment

This experiment uses one computer as server, its server's IP is 192.168.177.128, and other three computers as test machines, IP are 192.168.177.1, 192.168.177.2 and 192.168.1.3.

The topology is shown as figure 3.

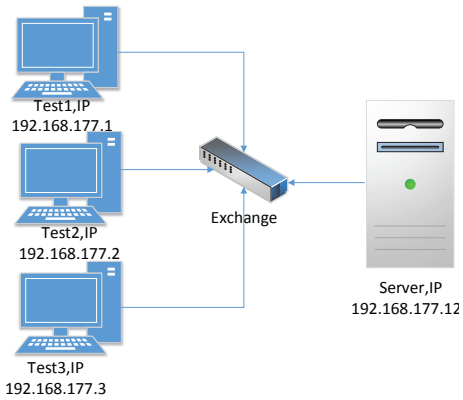

Figure 3 the topology

The operating system is centos desktop whose kernel version is 2.6.32. The hardware platform contains a CPU (Model Core i7-4710HQ @ 2.50GHz, Intel) and a 4G memory. The test software is SSH Secure Shell tfn2k.

B. Initialization of the firewall

The firewall initial process includes 5 steps, they are shown as follows.

1. Configure kernel.

As the IPtable is divided into kernel module and user layer management program components, the installation of IPtable involves the compilation and installation of the Linux kernel and user level program. This article uses the Linux-3.6.tar.bz2 to compile the Netfilter, and configure the Linux systemThe installation of IPtable involves the compilation and installation of the Linux kernel and user level program.

2. Create a shell script.

Linux firewall is consisted of lots of IPtable command lines, and each of them is executed only once. And usually the firewall has a number of rules, in order to use more convenient and convenient, we usually write firewall filtering rules into the shell script, and save in the path for the /etc/rc.d/rc.fw, and set permissions for the script.

[root@localhost linux-3.6]# touch /etc/rc.d/rc.fw

[root@localhost linux-3.6]# chown root:root/etc/rc.d/rc.fw

[root@localhost linux-3.6]# chmod u=rwx/etc/rc.d/rc.fw

The call to the firewall is the execution of the script file, in order to be able to automatically open the firewall when the Linux system start, we could edit this shell script in /etc/rc.d/rc.local so that the Centos firewall will start automatically as the system startup.

3. Delete existing filtering rules.

When defining a set of filter arrays, the first is to remove the existing rules in the rule chain, otherwise the newly added filtering rules will be added to the existing rules causes that the packets are matched to the existing filtering before matching the filter rules to the new settings, this will obviously cause packet filtering wrong result to us. Chain of all the rules of the custom will still exist after delete system default rules chain, therefore we need to further remove custom rules chains and we also need to empty all the chain bags and timers.

4. Change the default policy.

The default firewall strategy in this experiment is to throw away a message. After using this strategy, in addition to the packet allowed explicitly by the rules, the other data packets will be discarded. Compared to the default all packets across, the strategy that configures data packets that need to be rejected, is more safe and effective.

5. Reset and stop the firewall.

Sometimes you need to temporarily stop using firewall, because the firewall will stop completely when using firewall scripts and add ‘stop’ parameters in it.

C. Analysis of simulation result

IPtable realizes the function of state detection under the protocol of DNS, FTP, SSH and HTTP, and the configuration of the Linux kernel environment. In this paper, we adjust the kernel parameters and IPtable script file on the Linux system to make the winner have a certain ability of resisting DoS, and use the Syn Flood attack for test.

For SSH filtering, here only allows 192.168.177.1. As is shown in figure 4, the other IP addresses are not allowed to SSH connection with the server, but the filter allows the server to connect with other host.

```
[root@wiiway2 rc.d]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
LOG        all  --  anywhere             anywhere            state INVALID LOG level warning
DROP       all  --  anywhere             anywhere            state INVALID
ACCEPT     tcp  --  192.168.177.1        192.168.177.128     tcp spts:1024:65535 dpt:ssh state NEW

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
LOG        all  --  anywhere             anywhere            state INVALID LOG level warning
DROP       all  --  anywhere             anywhere            state INVALID
ACCEPT     tcp  --  192.168.177.128      anywhere            tcp spts:1024:65535 dpt:ssh state NEW
```

Figure 4 SSH filter rules

The host in Win7 establish SSH connections with firewall as is shown in figure 5.

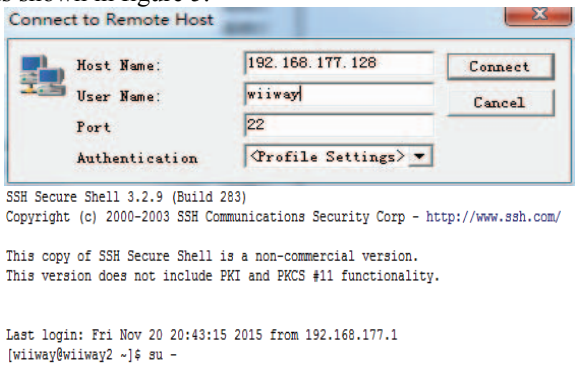

Figure 5 SSH secure Shell logging

Test result: only the IP 192.168.177.1 successfully establish SSH connections with the firewall, and the firewall can establish SSH connections with three test host. The result is same as the expected.

2. The filtering rules are shown in figure 6, here only allows 192.168.177.1 into firewall, and other IP addresses are not allowed to FTP connection with the server, but the filtering rules allow the server to connect other host.

```
[root@wiiway2 ~]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
LOG        all  --  anywhere             anywhere            state INVALID LOG level warning
DROP       all  --  anywhere             anywhere            state INVALID
ACCEPT     tcp  --  anywhere             192.168.177.128     tcp spt:ftp-data dpts:1024:65535 state NEW
ACCEPT     tcp  --  192.168.177.1        192.168.177.128     tcp spts:1024:65535 dpt:ftp state NEW
ACCEPT     tcp  --  anywhere             192.168.177.128     tcp spts:1024:65535 dpts:1024:65535 state NEW

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
LOG        all  --  anywhere             anywhere            state INVALID LOG level warning
DROP       all  --  anywhere             anywhere            state INVALID
ACCEPT     tcp  --  192.168.177.128      anywhere            tcp spts:1024:65535 dpt:ftp state NEW
ACCEPT     tcp  --  192.168.177.128      anywhere            tcp spts:1024:65535 dpts:1024:65535 state NEW
```

Figure 6 FTP filter rules

Test result: only IP 192.168.177.1 successfully establish the FTP connection with firewall, and the firewall can establish SSH connections with three hosts. The result, which is shown in figure 7, is same as the expected.

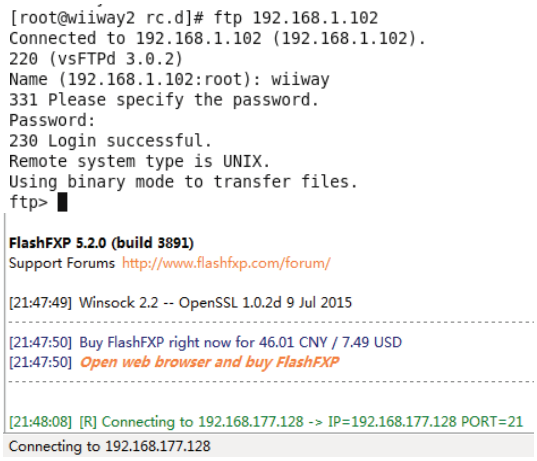

Figure 7 FTP test result

3. As the HTTP service closely related to DNS service, here we put the DNS and Web service test together. The related Settings of DNS and HTTP are shown in figure 8.

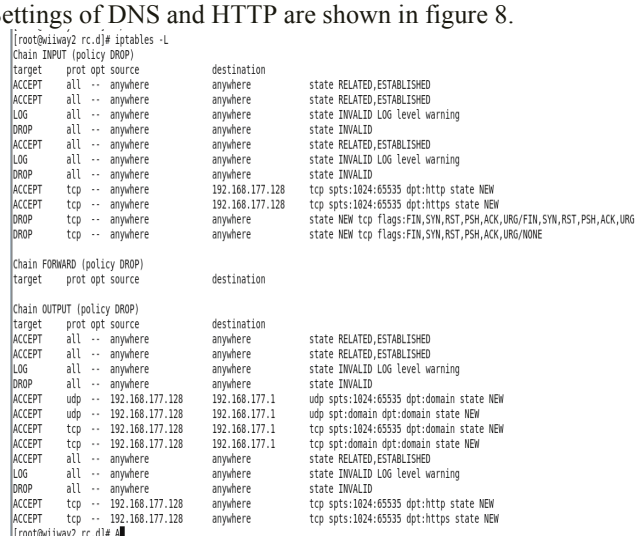

Figure 8 rules of DNS and HTTP

Due to the limited test conditions, related test of DNS and HTTP is only the host web access to external network, and test host is visiting www.baidu.com, as is shown in figure 9.

Figure 9 test result of DNS and HTTP

Test result: the local host can visit and parse the contents of www.baidu.com normally.

4、Use the Syn Flood attack to test the common DoS attack, the procedures are as follows.

The attack tool tfn2k is installed in the three hosts which is used to test attacks of Syn Flood to the test host. When there is only one test host being attacked, we use the tcpdump tool to get that a large number of data packets are attacking the test host, at the same time we use the top command to check the CPU state information, and we can find that the usage rate of CPU has raised from 1% to around 35%. When three test hosts launch attacks at the same time, the utilization rate of CPU reached 80%, causing that the system is not very smooth. When the IPtable rule is turned on, the increase of CPU usage rate is about 2%, which has no effect on the normal operation of the system.

IV. CONCLUSION

The purpose of this paper is to satisfy the demands of server firewalls in small and medium scale enterprises. The firewall uses state detection module and anti DDoS module as the research object. In order to protect the Linux serve, we configure numbers of IPtables filtering rules and design a high performance and efficiency firewall. At the last, some experiments verify the effectiveness of the firewall.

The Linux firewall，in this paper, realizes the function of status detection and simple anti DDoS attack. Because our ability is limited, we only focus on the packet header information and has no analysis of the data. Meanwhile, we don't detect the layer of application data characteristics, and don't step deeply into the state changes and processing mechanism under the framework of Netfilter.

REFERENCES

[1] BIAN Ruiqing. "The Principle and Defense of DDoS Attack." J.. Science & Technology Information, 2013, (8)

[2] CHEN Ming, ZHANG Xiaoyong. "Analysis DDoS Attack and Its Protective Measures." J.. Network Security Technology & Application, 2013, (9)

[3] ZHANG Renzhi. "Network Security Defense Technology Present Situation and the Counter Measures." J.. Network Security Technology & Application, 2014, (8)

[4] YANG Liu. "Introduction the Network Security Technology Development Present Situation and Development Trend. J.. Network Security Technology & Application, 2015, (9)

[5] SUN Zhihao. "Present Situation and Prospect of Firewall Technology." J.. Network Security Technology & Application, 2013, (6)

[6] YU Fei, YANG Bo. "The Research and Application of Firewall Based on Netfilter/IPtables Under Linux." J.. Journal of Qiqihar University (Natural Science Edition), 2015, 03: 53-58

[7] Zhao Yanan, Ma Zhaofeng. "Research and Application of Netfilter/IPtable in Linux." J.. China Science paper, 2014, (10)

[8] YAO Yafeng, JIANG Yi. "Research of Netfilter/IPtable Firewall Frame Based on Linux." J.. Computer Security. 2013, 11: 19-22

[9] XIA Dong-liang,LIU Jian-fang. “Constructing Firewall through Iptables under Linux.” Computer Era. 2011, 04: 42-44

[10] JI Gang, YAO Yan, TANG Huaiou. “Firewall Establishment Based on Netfilter/Iptables in Linux Kernel.” J.. Computer Knowledge and Technology. 2011, 19: 4550-4552

[11] CAI Miaoqi. “Based on the Research of Linux Firewall and Log Analysis.” D. Anhui University of Science and Technology. 2013.

[12] LAI Yuefang. “Design and Implementation of Firewall Network Security under the Environment of Linux.” South China University of Technology. 2013

[13] ZHOU Xi. “A Personal Firewall System Based on State Detection.” D. Hefei University of Technology. 2010