The Research and Application of Firewall based on Netfilter

Qing-Xiu Wu

Hainan College of Software Technology, QiongHai, Hainan, 571400, P.R.China

Abstract

With the rapid development of computer network technology, network security is facing many important issues, first describes working principle and key technology based on Netfilter firewall, and applies to the actual. Practice has proved that due to the open source nature of Linux firewall, the implementation mechanism is a discussion on the value of the field.

1. Introduction

Network security problem that has troubled people, today's rapid development of computer network technology. Firewall is to ensure the emergence of network security and design of computer hardware or computer software systems. commercial firewall products, that is, special features of the common software, there are targeted is not a strong drawback. In such circumstances, would require internal system design and development of their own firewall.

Netfilter/Iptables combinations are currently in the Linux open source operating systems generally use a solution of firewall, Netfilter is implemented in the Linux kernel firewall function modules, iptables is the firewall application state management tool. Linux is open source firewall technology has gone through several generations of evolution, a step by step evolved. Most start ipfwadm is Alan Cox in the early development of the Linux kernel, transplant from a FreeBSD kernel code. Later experiences ipchains, and then by Paul Russell Linux kernel 2.3 series in the process of development of the Netfilter kernel architecture. Firewall management tools user also served to develop for iptables. After the development of the 2.4~2.6 series, has stood the test of a large number of users widely used[1][2].

2. Works of the linux open source firewall

In the netfilter/iptables firewall system, netfilter components are located in the Linux kernel space, enabling static packet filtering and stateful packet inspection (dynamic packet filtering) basic firewall
functionality, as well as support for a flexible and extensible framework, supports NAT network address translation, and other additional features, and provides multiple layers of API interface to support third party extensions, netfilter built firewall, NAT shared Internet access, Construction of a transparent proxy with NAT, and building security features such as QoS and policy routers. Iptables is working on Linux firewall configuration in user-space tools, from the command line mode allows the user to configure netfilter firewall filtering and management rules.

![Fig 1 Five Hook points in network packet processing chain](image)

Table Netfilter/Iptables contains three of the most basic rules, namely filter tables for packet filtering, network address translation NAT table, and mangle table for special purpose packet modification. Each sheet contains a number of default rules that are defined in the rules table chain, chain, and can be customized by the user rules. As shown in Fig 1. Chain PREROUTING rules rule check point for the IVF_IP_PRE_ROUTING, to inspect all incoming packets that host, usually for source address NAT translation: INPUT rule chain checkpoint in NF_IP_LOCAL_IN, sent to the local network protocol stack, inspect packets handled by local processes, usually used to filter connections to the local network services; Chain FORWARD rule checkpoint in NF_IP_FORWARD, examines the packets that are routed through the local forwarding, when used in the machine as a router, filtering through a network connection, the Hook point is the most major firewall packet filtering; POSTROUTING rule chain checkpoint in NF_IP_POST_ROUTING, issued to a local protocol stacks and checked through routing forwards packets and processing, is typically used for destination NAT turn OUTPUT chain checkpoint in NF_IP_LOCAL_OUT, by local processes are being targeted by packet from the local TCP/IP protocol stack for check processing, Can configure external access restrictions for local and destination network address translation.

Different source and destination network packet protocol stack processing through the different netfilter check chain, and is based on iptables rule checking, filtering, and processing rules that are configured on the chain, packet modification and related operations. By configuring netfilter firewall forwarding network traffic via PREROUTING,FORWARD and POS TROUTING, incoming network traffic through firewall native PREROUTING into INPUT chain, while the firewall machine's external outgoing network traffic is starting from the OUTPUT chain, issued through the POSTROUTING chain[3][4].

In each section rules chain Shang will set a default of processing operation, usually situation Xia for accept (ACCEPT), and by user through iptables added some implementation security filter, and NAT and the other purpose of configuration rules, in netfilter on data package for processing Shi, will in each Hook check points Shang on flows through of data package for check, and successive view data package is match has configuration rules of conditions, if meet, is implementation rules by provides of operation, as filter (DROP ) Packets, and so on, does not match the last hegai linked lists all data configuration rules on packages will perform default processing operations. Netfilter also supports jump to the rules for other
user-defined rules for further check processing chain, which greatly extends the flexibility of Netfilter. Netfilter packet access rule matching and processing chain as shown in Fig 2.

Fig 2 The rules and processes with netfilter packet in chain matches

3. Implementation of firewall technology

(1) The packet filtering mechanism

Netfilter of static package filter of implementation mechanism comparison simple, is in INPUT, OUTPUT, FORWARD, rules chain corresponds to of Hook points Shang defined check callback function, on through Hook points of data package for check processing, due to static package filter mechanism only be view single data package of baotou information, and without maintenance data package in network connection in the of location and State, therefore only needs in agreement stack on data package of baotou agreement resolved Foundation Shang, Sequential traversal rules defined by the user in the chain of checks linked lists, and check whether the current packet matching conditions configured in the rule, if it matches, executes the user-defined processing rules, and finally, there is no packets match any rule they perform default processing. For example:

```
# iptables –t filter –A FORWARD –s 222.17.0.0/24 –d 222.17.1.0/24 –j ACCEPT
```

The static packet filtering rules to check the routing forwards packets, when the packet source IP addresses belong to the 222.17.0.0/24 class c network segment, and destination addresses belong to the 222.17.1.0/24 class c network segment, then doing ACCEPT the purpose.

Netfilter after the track, and maintain status for all network connections, in various filter rules support iptables chain flexible in configuring stateful inspection firewall with connection rules, access to the network connection control, such as:

```
# iptables –t filter –A FORWARD –A FORWARD –d [WEB_SERVER] –m state –state NET –j ACCEPT
```
The first section example rules allows connection target address for Web server IP, current state for NEW of network connection may through firewall forward, second section example rules license has established network connection and related network connection through firewall, this configuration makes administrator only needs for to intranet launched of new connection for strictly of access control configuration, only built connection and the related connection can through a section simple of rules for processing, this greatly reduced has administrator correctly configuration network access control mechanism of difficulty[5].

(2) NAT mechanism

Netfilter/Iptables support for NAT network address translation technology is very comprehensive, including IP masquerading (masquerading), transparent proxy (transparent proxying), port forwarding (port forwarding) and other forms of network address translation technology.

NAT consists primarily of two types, namely Source NAT (SNAT) and the Destination NAT (DNAT). SNAT refers to change network connection packet's source address, SNAT need to do after routing forwarding, that is, before the packet took to reach the network cable, IP masquerading mechanism is a SNAT; DNAT is changing network connection packet's destination address, DNAT needs to do before routing forwarding, port forwarding, load balancing, the transparent proxy is DNAT[6].

Netfilter/Iptables for the NAT configuration is primarily through 3 default chain in the NAT table, the PREROUTING (for DNAT), POSTROUTING (for SNAT), OUTPUT (for local packages of DNAT). Packets go through these three rules when the Hook chain that checkpoint, checks what it belongs to the connection if it is a new connection, we will find a specific rule chain in the NAT table, in accordance with the rules of chain matches and goals related to the configuration rules for the operation.

IP masquerading; Needs of the most commonly used netfilter NAT mechanism is IP masquerading. On the internal network using a private IP network segments, such as through the firewall bound on a scene outside the network IP address sharing online, it can use this mechanism, internal network host sent the package to the source IP address masquerading, IP outside the firewall network address, as is from outside the firewall network issued by the same IP address. Specific configuration rules:

```
# iptables –t nat –A POSTROUTING –I eth1 –o eth0 –j MASQUERADE
```

SNAT mechanism; IP masquerading is a special case of SNAT mechanism, its function is to issue a network connection to the source IP address disguised as external network IP address of the firewall itself. SNAT configuration mechanism in accordance with the user rules, source address of the network connection can be changed into a wide range of flexible configuration of address, SNAT mechanisms need to be done in the POSTROUTING chain, because the routing, packet filtering is the source address before changing to do, so does not affect the SNAT mechanism.

SNAT target options "-j SNAT" description, use "--to-source" to describe the IP address it want to convert, or a range of IP addresses and ports (only for TCP and UDP). For example:

```
# iptables –t nat –A POSTROUTING –o eth0 –j SNAT –to 222.17.2.1 – 222.17.2.9
```

Above this rule will be issued through the routing of source IP address of the network connection changes is 222.17.2.1 to 222.17.2.9 an IP in IP network segments.

DNAT mechanism; DNAT done in the PREROUTING chain, for native applications (including routing, packet filtering program) destination address change is ignored, that reach the real destination address. Need to use "-i" option. Destination NAT "-j DNAT", with a "--to-destination" option to describe the range of IP addresses, IP addresses or ports.

```
# iptables –t nat –A POSTROUTING –I eth1 –j DNAT –to 222.17.2.1 – 222.17.2.9
```

Above this rule converts the destination address any IP in the 222.17.2.1-222.17.2.9.
Destination port forwarding is a special case of DNAT mechanism, to 8,080 port on the external network IP 202.100.192.68 network traffic is forwarded to port 80 of the internal network IP 222.17.254.128, can use the following rules:[7]

```bash
```

4. Summary

Netfilter/Iptables of open source solutions are available in Linux systems, to help network administrators quickly implement in user’s network firewall boundary protection. By the above analysis and examples of development based on netfilter firewall system, it is entirely feasible and completed of system stability efficient. In addition, due to Linux of open source features, instant user cannot personally development firewall system, also can modify system according to personalized application. In short, on Linux platform, firewall implementation mechanism is a very worth of topics in-depth research and discussion.

References