IJETST- Vol.||03||Issue||03||Pages 3634-3637||March||ISSN 2348-9480 2016

Open access Journal International Journal of Emerging Trends in Science and Technology

Impact Factor: 2.838 DOI: http://dx.doi.org/10.18535/ijetst/v3i03.03

Implementing Firewall using IP Tables in Linux

Authors

Prof. Kinjal Joshi, Tej Kashiparekh

Computer Engineering Department,
AD Patel Institute of Technology (GTU), Karamsad

ABSTRACT

The booming complexity of networks, and the desire to make them more accessible due to the growing emphasis on and awareness of the Internet as a medium for multi-dimensional transactions, mean that networks are becoming constantly and increasingly exposed to attacks, internal and external. The research is on for mechanisms and techniques for the security of internal networks from such attacks. One of the multiple protective mechanisms under detailed consideration is the firewall. A firewall protects a network by guarding the points of entry to it. Firewalls are becoming increasingly effective and sophisticated by the day, and new features are constantly being added, so that, in spite of the criticisms made of them and r&d trends threatening them, they are still a very strong protective mechanism. This article provides an overview of firewall using IP tables in Linux.

Keywords: *Firewall, Network Security, Packets, Security Policy, Ip tables.*

Introduction

"Today's networks evolve and change on a frequent basis to adapt to new situations, such as reorganizations, acquisitions, outsourcing, mergers, joint ventures, and strategic partnerships, and the rapidly increasing degree to which internal networks are entwined to the Internet"[1]. The booming complexity and openness of the network hence caused the question of security more complicated than hitherto, and creates the need for the production of sophisticated security technologies at the interface between networks of various security domains, such as between Intranet and Internet or Extranet. The best and most viable way of ensuring interface security is the use of a firewall.

A Firewall is a system or other communication device which filters access to the protected network. Chedwick and Bellovin define a firewall as "a collection of components or a system that is placed between two networks and possesses the following properties:

- All traffic from inside to outside, and vice-versa, must pass through it.
- Only authorized traffic, as defined by the local security policy, is allowed to pass through it.
- The firewall is immune to penetration"[3].

Packet filtering is commonly used for a first line of defense against attacks from machines outside your LAN. Since most routing devices have many built-in filtering capabilities, packet filtering has become a regular and inexpensive approach to security. Netfilter is fourth generation Linux packet filtering software. Also called Ip tables, Netfilter was introduced with the Linux 2.4 kernel and was made to take over from both the Ipchains and Ipfwadm legacy tools. There were two advantages that Netfilter provides; Simplified packet flow and Stateful inspection

IP tables is used to create, maintain, and monitor the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains many built-in chains and may also contain user-defined chains.

"Linux IPtables is default package that comes from RedHat, Cent OS, UBUNTU and Fedora, right after ipchains dominated for long time" [2]. IPtables supports different types of filters. To name a few, IP tables can do filters and firewall rules by end-users, by group IDs and user profiles, by source and destination ports, by source host and destination hosts, by URLs, by IP addresses, by packet ID flags, protocols, and a lot more including filtering by MAC address.

IP Tables Background [5]

IP tables provides relatively higher speed and reliability than other firewall tools. Being a Linux product, its integration with the OS is also more robust and reliable. It keeps a stateful track of every connection passing through it and tries to anticipate future actions. Its capacity to filtering packets on the basis of MAC address makes it a formidable security system. It can filter out attacks using improper packets and can restrict access from locally attached servers to other networks in spite of their accepted and valid IP addresses. Network address translation with disguising capability of IP tables helps it to hide internal network IP sub networks behind one or a small poll of external IP addresses. NAT and disguising enables the firewall to access ports on the gateway. The rate-limiting of IP tables can block attacks even from some types of DoS (denial of service) attacks.

Firewall rules[6]

Different firewalls usually provide different rule logic with different parameters. But some basic elements are common to all. They all allow an action to be defined allowing or banning specific network traffic. Also, all of them allow checking for most important elements in packets like IP addresses, ports and protocol. IP Tables is a command line tool for writing and executing of Firewall rules. One of the most important functionalities of IP Tables firewall is stateful inspection. S.I. automatically opens only the ports necessary for internal packets to access the Internet. It only allows transfer of packets which are defined in firewall rules and which are part of established connections.

Firewall chains

IP Tables group rules in chains. Different network packets are processed by different chains:

•Incoming traffic – packets for firewall (INPUT chain).

•Forwarding traffic – incoming packets for another machine (FORWARD chain). •Outgoing traffic – packets generated by firewall (OUTPUT chain).

Rule parameters [7]

Each rule identifies specific type of network traffic. In order to enable this identification parameter for Identification of specific network packets must be set For each rule.

Different type of parameters:

•IP addresses – it can be destination or source IP address; also, it can be written as a single IP, network IP or IP range.

•Ports - it can be destination or source port; also, it can be written as a single port, port range or port array.

•Protocol – it can be referred to TCP, UDP, and ICMP or altogether.

•Interface – it can be incoming or outgoing interface.

•TTL (Time To Live) field residing in the IP headers.

•ToS (Type of Service) field residing in the IP headers.

•Length of packet.

•MAC source address.

•Syn flag – identification of new connection.

•ICMP type.

Firewall using IP Tables

The first table is the filter queue which is responsible for packet filtering. It has three built-in chains in which firewall policy rules are placed. These are the:

- Forward chain: Filters packets to servers protected by the firewall.
- Input chain: Filters packets destined for the firewall.
- Output chain: Filters packets originating from the firewall.

The second table is the Nat queue which is responsible for network address translation. It has two built-in chains; these are:

- Pre-routing chain: NATs packets when the destination address of the packet needs to be changed.
- Post-routing chain: NATs packets when the source address of the packet needs to be changed.

The third is the mangle table which is responsible for the alteration of quality of service bits in the TCP header. It is necessary to specify the table and the chain for each firewall rule you create. There is an exception: Most rules are related to filtering, so IPtables assumes that any chain that's defined without an associated table will be a part of the filter table. The filter table is therefore the default.

Packet Flow through iptables

Understanding how packets flow through iptables allows the administrator to correctly create the firewall rules. The good news is that Netfilter simplified the packet flow through the chains as compared to ipchains. The new model only processes the necessary chains based on the ip appresses on the packet. There are three main chains INPUT, OUTPUT, and FORWARD that process the security policy. There are two chains that perform NAT and one chain for mangling the packet.

The flow through ip tables is as follows[8]:

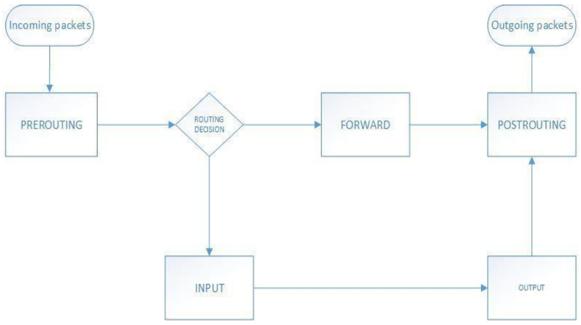
1. The incoming packet is processed by the PREROUTING chain. This chain is used to NAT the destination on packets before any rules are applied.

2. The PREROUTING chain is frequently used to perform a one-to one static destination NAT. Next a routing decision is made based on the destination ip address of the packet. A packet that is transferred to the INPUT chain will be compared to the rules attached to that chain to determine if it will be allowed. If the packet is allowed, it is transferred to the appropriate local process on the system. Replies to this packet will leave the local processing and traverse the OUTPUT chain.

3. A packet not destine for the box will be processed by the FORWARD chain. The rules in the chain are checked and, if accepted, the packet is routed to the correct interface. The packet will be dropped if ip forwarding is not enabled or does not know how to route the packet1.

4. The OUTPUT chain is only traversed if the packets are initiated from the local box or are replies to packets that were destine for the box. Rules are checked and the packet passed out the correct interface1.

5. The outgoing packet is processed by the POSTROUTING chain. This chain is used to NAT the source address on packets after rules are applied2. The POSTROUTING chain is frequently used to perform a hiding NAT.



Firewall Limitations

"Information security professionals often find themselves working against misconception and popular opinions formed from incomplete data. Some of these opinions spring more from hope than fact, such as the idea that internal network security can be solved simply by deploying a firewall"[10]. The following are limitations one should be aware of.

- A firewall is by its nature perimeter defence, and not geared to combating the enemy within, and consequently no useful counter measure - against a user who abuses authorised access to the domain.
- A firewall is no real defense against malicious code problems like viruses and Trojan horses, although some are capable of scanning the code for telltale signs.
- Configuring packet-filtering rules tends to be complicated process in the course of which errors can easily occur, leading to holes in the defense.

In addition, testing the configured rules tends to be a lengthy and difficult process due to the shortcomings of current testing tools. Normal packet-filtering routers cannot enforce some security policies simply because the necessary information is not available to them.

Conclusion

Notwithstanding the limitations of firewalls and the fact that they are neither the panacea of every security aspect of a network, nor the sole sufficient bulwark against network intrusion, and despite development trends that threaten them, they are still a powerful protective mechanism, and will continue to play an important and central role in the maintenance of network security for some years yet, and any organization that ignores them does so at its peril. They continue to change and develop, and new features are regularly added as the need arises. If developments follow the present trend, they will continue to combine configurable access control and authentication mechanisms with their traditional functions, thus providing more powerful and flexible protection for networks to make them secure.

References

1. Gunter Schafer, “Network Security Tutorial”, May 2003, Anchorage, Alaska.
2. eSoft, “Modern Network Security: The Migration to Deep Packet Inspection”, White Paper, 2006.
3. David W Chadwick, “Network Firewall Technologies”, IS Institute, University of Salford, Salford, M5 4WT, England.
4. Internet Firewall Tutorial, A White Paper July 2002.
5. IPtables Home, http://www.netfilter.org/
6. IPtables Scripting, http://www.linuxdoc.org/
7. IPtables Parameters, http://www.centos.org/docs/2/rhl-rg-en-7.2/s1-iptables-options.html
8. A. Hari, S. Suri, and G. M. Parulkar, “Detecting and resolving packet filter conflicts”, In Proc. of IEEE Infocom, pages 1203- 1212, 2000.
9. Christoph Ludwig Schuba, “On the modeling, design, and implementation of firewall technology”, Purdue University.
10. Elizabeth D. Zwicky, Simon Cooper, D Brent Chapman,”Building Internet Firewalls”, 2-Ed, Oreilly, 2000.