Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1297 – 1302

RESEARCH ARTICLE

Analysis of Packet Filtering Technology in Computer Network Security

Miss. Rupali P. Hinglaspure[1], Prof. B. R. Burghate[2]

[1]Department of Computer Science and Engineering, Sant Gadge Baba Amravati University, India
[2]Department of Computer Science and Engineering, Sant Gadge Baba Amravati University, India

[1] rupalih1722@gmail.com; [2] bharatburghate@gmail.com

Abstract— in today's networks are becoming more complex, and the demands on bandwidth are through the roof. In achieving visibility for the best network performance, monitoring the right data is critical. Explore a network monitoring switch tool that provides advanced filtering options that are able to quickly resolve network problems and add on new capabilities as future requirements come along, without much manual effort to maintain an updated set of filtering rules. Packet filtering has proved to be a handy tool to put access controls to IP traffic. Packet filters can be used to block IP packets based on certain criteria such as the protocol used and various protocol characteristics. On the Internet, packet filtering is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols.

Keywords— Packet Filtering Overview, Security Consideration, Packet Filtering Features, Packet Filtering Advantages & Disadvantages

I. Introduction

In recent years, more and more networks with sensitive or even business critical data on them are being interconnected. Simultaneously, hacker activity has grown tremendously because of freely available hacker tools. In order to protect networks, so-called firewalls are deployed that protect against hacker activities. One of the ways to implement a firewall is to make use of so-called packet filters. Packet filtering firewalls is the first generation of firewalls. Packet filters track the source and destination address of IP packets permitting packets to pass through the firewall based on rules that the network manager has set, On the Internet, packet filtering is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols. The process is used in conjunction with packet mangling and Network Address Translation (NAT). Packet filtering is often part of a firewall program for protecting a local network from unwanted intrusion. In a software firewall, packet filtering is done by a program called a packet filter. The packet filter examines the header of each packet based on a specific set of rules, and on that basis, decides to prevent it from passing (called DROP) or allow it to pass (called ACCEPT).Packet filtering is "controlling access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination. Packet filtering is one technique, among many, for implementing security firewalls". Packet filtering is both a tool and a technique that is a basic building block of network security. It is a tool in that it is an instrument that aids in accomplishing a task. It is a technique because it is a method of accomplishing a task. In the context of a TCP/IP network, a packet filter watches each individual IP datagram, decodes the header information of in-bound and out-bound traffic and then either blocks the datagram from passing or allows the datagram to pass based upon the contents of the source address, destination address, source port, destination port and/or connection status. This is based upon certain criteria defined to the packet filtering tool. The leading IP routers, including Cisco, Bay, and Lucent, can be configured to filter IP datagram's. Many operating systems can be configured for packet filtering. Packet filtering can be added to nix operating systems. Support for packet filtering via IP chains is included by default in the Linux kernel. Windows NT and Windows 2000 support packet filtering. Virtually all commercial firewalls support packet filtering. Some commercial firewalls also have the capability of filtering packets based upon the state of previous packets (stateful inspection).

II. HISTORY OF PACKET FILTERING

Packet filtering was written byDdeniel Hartmeier. It appeared in OpenBSD 3.0, which was released on 1 December 2001. Packet filter was originally designed as replacement for Darren Reed's IPFilter, from which it derives much of its rule syntax. IPFilter was removed from OpenBSD's CVS tree on 30 May2001 due to OpenBSD developers' concerns with its license. The filtering syntax is similar to IPFilter, with some modifications to make it clearer. Network Address Translation (NAT) and Quality of Service (QoS) have been integrated into packet filter.

III. Packet Filtering Technology overview

t filtering is a firewall technique used to control network access by monitoring outgoing and incoming packet and allowing them to pass or half based on the source and destination internet protocol (IP) addresses, protocols and ports. Network layer firewall defines packet filtering rules sets, Witch highly efficient security mechanism. Packet filtering is also known as static filtering. Packet filtering firewall allows only those packets to pass, which are allowed as per your firewall policy. Each packet passing through is inspected and then the firewall decides to pass it or not. Packet filtering checks source and destination IP address. If both IP addresses match, the packet is considers secure and verified. Because the sender may used different application and protocol, packet filtering also check source and destination protocols, such as User Datagram Protocol (UDP) and transmission control protocol (TCP).packet filter also verify source and destination port addresses.

Some packet filters are not intelligent and unable to memorize used packets. However other packet filters can memorize previously used packet items, such as source and destination IP addresses.

Packet faltering as usually an effective defence against attack from computers outside a local area network (LAN).As most routing device has integrated filtering capabilities; packet filtering is considered a standard and cost effective means of security.

*A).Types of Packet Filtering***.**

There are two types of packet filtering,

1. Stateless packet filtering.
2. Stateful packet filtering.

The data travels through the internet in the form of packets. Each packet has a header which provides the information about the packet, its source and destination etc. The packet filtering firewalls inspects these packets to allow or deny them. The information may or may not be remembered by the firewall.

1. Stateless Packet Filtering:

If the information about the passing packets is not remembered by the firewall, then this type of filtering is called stateless packet filtering. This type of firewalls is not smart enough and can be fooled very easily by the hackers. These are especially dangerous for UDP type of data packets. The reason is that, the allow/deny decisions are taken on packet by packet basis and these are not related to the previous allowed/denied packets. Static (Statful) packet filtering systems, each packet that crosses the border between your private network (intranet) and the public network (Internet). Static packet filters parse the header field of each packet to identify a set of characteristics:

- Protocol ID (for example, TCP, UDP, ICMP)
- Source IP address and port number.
- Destination IP Address and port number.
- Router interface for the incoming or outgoing packet.

2. Stateful Packet Filtering:

If the firewall remembers the information about the previously passed packets, then that type of filtering is stateful packet filtering. These can be termed as smart firewalls. This type of filtering is also known as Dynamic packet filtering. Stateful packet filtering supports both connection and connectionless protocols (TCP, UDP, ICMP, and so on). Dynamic packet filtering monitors each connection and creates a temporary (time-limited) inbound filter exception for the connection. This allows you to block incoming traffic originating from a particular port number and address while still allowing return traffic from that same port number and address. The reverse filter is created by extracting the following packet information:

- Source IP address.
- Source interface.
- Source port.
- Destinations IP address.
- Destination interface.
- Destination port.
- Protocol type.

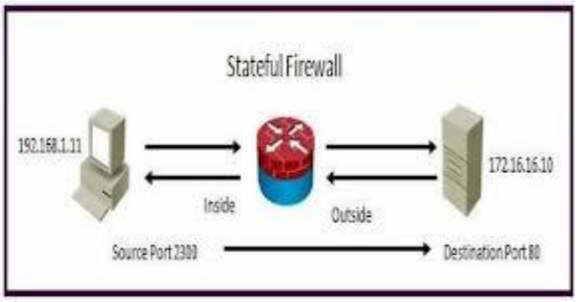

Fig.2.1.Stateful Packet Filtering.

B). Working of packet filtering in our PC:

All packet filters function in the same general fashion. Operating at the network layer and transport layer of the TCP/IP protocol stack, every packet is examined as it enters the protocol stack. The network and transport headers are examined closely for the following information:

Protocol (IP header, network layer) – In the IP header, byte 9 (remember the byte count begins with zero) identifies the protocol of the packet. Most filter devices have the capability to differentiate between TCP, UPD, and ICMP.

Source address (IP header, network layer) – The source address is the 32-bit IP address of the host which created the packet.
Destination address (IP header, network layer) – The destination address is the 32-bit IP address of the host the packet is destined for.
Source port (TCP or UDP header, transport layer) – Each end of a TCP or UDP network connection is bound to a port. TCP ports are separate and distinct from UDP ports. Ports numbered below 1024 are reserved – they have a specifically defined use. Ports numbered above 1024 (inclusive) are known as ephemeral ports. They can be used however a vendor chooses. For a list of “well known” ports, refer to RFP1700. The source port is a pseudo-randomly assigned ephemeral port number. Thus it is often not very useful to filter on the source port.
Destination port (TCP or UDP header, transport layer) – The destination port number indicates a port that the packet is sent to. Each service on the destination host listens to a port. Some well-known ports that might be filtered are 20/TCP and 21/TCP - ftp connection/data, 23/TCP - telnet, 80/TCP - http, and 53/TCP - DNS zone transfers.
Connection status (TCP header, transport layer) – The connection status tells whether the packet is the first packet of the network session. The ACK bit in the TCP header is set to “false” or 0 if this is the first packet in the session. It is simple to disallow a host from establishing a connection by rejecting or discarding any packets which have the ACK bit set to “false” or 0.
The filtering device compares the values of these fields to rules that have been defined, and based upon the values and the rules the packet is either passed or discarded. Many filters also allow additional criteria from the link layer to be defined, such as the network interface where the filtering is to occur.

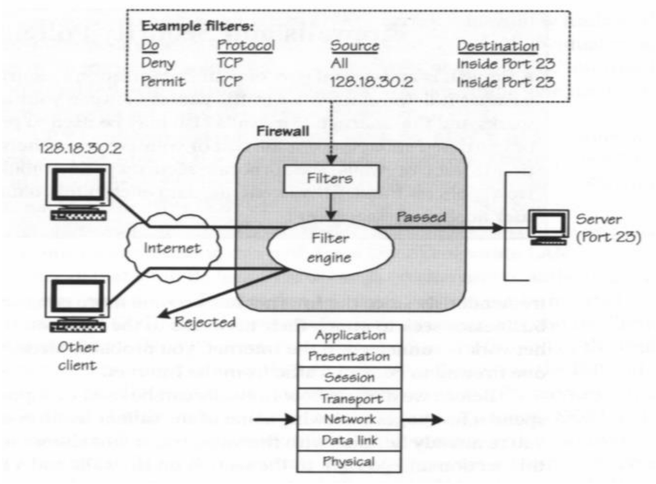

Fig.2.Working Of Packet Filtering

C). How packet filtering rules are specified

Generally, the filtering rules are expressed as a table of conditions and actions that are applied in a certain order until a decision to route or drop the packet is reached. When a particular packet meets all the conditions specified in a given row of the table, the action specified in that row (whether to route or drop the packet) is carried out; in some filtering implementations, the action can also indicate whether or not to notify the sender that the packet has been dropped (through an ICMP message), and whether or not to log the packet and the action taken on it. Some systems apply the rules in the sequence specified by the administrator until they find a rule that applies , which determines whether to drop or route the packet. Others enforce a particular order of rule application based on the criteria in the rules, such as source and destination address, regardless of the order in which the rules were specified by the administrator.

IV. A packet filtering example

For example, consider this scenario. The network administrator of a company with Class B network 123.45 wishes to disallow access from the Internet to his network in general (123.45.0.0/16).The administrator has a special subnet in his network (123.45.6.0/24) that is used in a collaborative project with a local university which has class B network 135.79; he wishes to permit access to the special subnet (123.45.6.0/24) from all subnets of the university (135.79.0.0/16). Finally, he wishes to deny access (except to the subnet that is open to the whole university) from a specific subnet (135.79.99.0/24) at the university, because the subnet is known to be insecure and a haven for crackers. For simplicity, we will consider only packets flowing from the university to the corporation; symmetric rules (reversing the SrcAddr and DstAddr in each of the rules below) would need to be added to deal with packets from the corporation to the university. Rule C is the "default" rule, which specifies what happens if none of the other rules apply.

Rule	SrcAddr	DstAddr	Action
A	135.79.0.0/16	123.45.6.0/24	permit
B	135.79.99.0/24	123.45.0.0/16	deny
C	0.0.0.0/0	0.0.0.0/0	deny

Consider these "sample" packets, their desired treatment under the policy outlined above, and their treatment depending on whether the rules above are applied in order "ABC" or "BAC".

Packet	SrcAddr	DstAddr	Desired Action	ABC action	BAC action
1	135.79.99.1	123.45.1.1	deny	deny (B)	deny (B)
2	135.79.99.1	123.45.6.1	permit	permit (A)	deny (B)
3	135.79.1.1	123.45.6.1	permit	permit (A)	permit(A)
4	135.79.1.1	123.45.1.1	deny	deny (C)	deny (B)

A router that applies the rules in the order ABC will achieve the desired results: packets from the "hacker haven" subnet at the university to the company network in general (such as packet 1 above) will be denied (by rule B), packets from the university "hacker haven" subnet at the university to the company's collaboration subnet (such as packet 2 above) will be permitted (by rule A), packets from the university's general network to the company's "open" subnet (such as packet 3 above) will be permitted (by rule A), and packets from the university's general network to the company's general network (such as packet 4 above) will be denied (by rule C).If, however, the router reorders the rules by sorting them into order by number of significant bits in the source address then number of significant bits in the destination address, the same set of rules will be applied in the order BAC. If the rules are applied in the order BAC, packet 2 will be denied, when we want it to be permitted.

V. Important Features of Packet Filters

The great firewalls normally follow few specific rules upon which features are incorporated during firewall designing. Few are listed below:

1. The firewall should provide good deal of logs. The more detailed are the logs, the better the protection.

2. The command line syntax or GUI of firewall should be easy to create new rules and of course firewall exceptions.

3. The packet filter orders should be evaluated carefully in order to make the filtering fruitful.

VI. Advantages and Disadvantages of Packet Filtering

A) Advantages:

1. One screening router can help protect an entire network.

One of the key advantages of packet filtering is that a single, strategically placed packet filtering router can help protect an entire network. If there is only one router that connects your site to the Internet, you gain tremendous leverage on network security, regardless of the size of your site, by doing packet filtering on that router.

2. Packet filtering doesn't require user knowledge or cooperation,

Packet filtering doesn't require any custom software or configuration of client machines, nor does it require any special training or procedures for users. This "transparency" means that packet filtering can be done without the cooperation, and often without the knowledge, of users.

3. Packet filtering is widely available in many routers.

Packet filtering capabilities are available in many hardware and software routing products, both commercial and freely available over the Internet. Most sites already have packet filtering capabilities available in the routers they use.

B) Disadvantage:

Although packet filtering provides many advantages, there are some disadvantages to using packet filtering as well:

1. Current filtering tools are not perfect.

In the face of the widespread availability of packet filtering in various hardware and software packages, packet filtering is still not a perfect tool. The packet filtering capabilities of many of these products share, to a greater or lesser degree, common limitations:

- The packet filtering rules tend to be hard to configure. Although there is a range of difficulty, it mostly runs from slightly mind-twisting to brain-numbingly impossible.
- Once configured, the packet filtering rules tend to be hard to test.
- The packet filtering capabilities of many of the products are incomplete, making implementation of certain types of highly desirable filters difficult or impossible.
- Like anything else, packet filtering packages may have bugs in them; these bugs are more likely than proxying bugs to result in security problems. Usually, a proxy that fails simply stops passing data, while a failed packet filtering implementation may allow packets it should have denied.

2. Some protocols are not well suited to packet filtering.

Even with perfect packet filtering implementations, you will find that some protocols just aren't well suited to security via packet filtering.

3. Some policies can't readily be enforced by normal packet filtering routers.

The information that a packet filtering router has available to it doesn't allow you to specify some rules you might like to have.

VII. TESTING

Testing was first done on a system that did not route packets but that sniffed a network and collected state information from all sniffed packets. IP Filter had to be modified slightly to do this. Whenever a packet was seen that would have been blocked by the state engine, it was logged on this machine. Such a setup allows for testing the state engine without actually disrupting network traffic be-cause no real filtering is performed. Thus it is possible to test on operational networks which save the trouble of producing test network traffic. On the actual (operational) network on which the tests were done, an enormous amount and variety of connections could be tested as the network is used to monitor and administer machines using connectivity from high speed low latency links to low bandwidth high latency links.

VIII. CONCLUSION

Packet filtering is currently a viable and valuable network security tool, but some simple vendor improvements could have a big impact. There are several critical deficiencies that seem to be common to many vendors, such as the inability to consider source TCP/UDP port in filters that need to be addressed. Other improvements to filter specification mechanisms could greatly simplify the lives of network administrators trying to use packet filtering capabilities, and increase their confidence that their filters are doing what they think they are.

References

[1] Canghong Zhang, Based on nework security firewall technology,Information technology,Chinese new technology new product, 2009.

[2] Rui Wang. Haibo Lin, Network security and firewall technology, Tsinghua university publishing house, in 2000

[3] Kuang Chu,network security and firewall technology, Chongqing university publishing house,2005

[4] S. Smith, E. Palmer, and S. Weingart, ”Using a high-performance, programmable secure coprocessor,” in Proc. International Conference on Financial Cryptography, Anguilla, British West Indies, 1998.

[5] P. Liu and S. Jajodia ,”Multi-phase damage confinement in database systems for intrusion tolerance,” in Proc. 14th IEEE Computer Security Foundations Workshop,Nova Scotia, Canada, June 2001.

[6] S. W. Lodin and C. L.Schuba, “Firewalls fend off invasions from the net,” *IEEE Spectrum*, vol. 35, no. 2, 1998.

[7] A. Wool, “A quantitative study of firewall configuration errors,” *Computer,* vol. no. 6,2004.

[8] M. R. Lyu and L. K. Y. Lau, “Firewall security: policies, testing and performance evaluation,” in *Proc. 2000 International Conference on* Computer Systems and Applications.

[9] J. J¨urjens and G. Wimmel, “Specification-based testing of firewalls,” in Proc. 2001 International Andrei Ershov Memorial Conference on Perspectives of System Informatics.

[10] Check Point's Press Release “Check Point Introduces Revolutionary Internet Firewall Product Providing Full Internet Connectivity with Security; Wins 'BEST OF SHOW' Award at Net world Interpol ‘94”. 1994

[11] Yu Qiu,Internet network security and firewall technology discussion,Mianyang Normal school journal ,2004.