DATA SECURITY USING IP PACKET FILTERING

Ms. C. Nagarani, Assistant Professor, Department of Computer Science, PSG College of Arts and Science, Coimbatore.

Ms. L. Pushpa, Research Scholar, Department of Computer Science, PSG College of Arts and Science, Coimbatore.

ABSTRACT - The packet filtering is access to a network by analyzing the source and destination address. The packet filtering is one of the basic tool to secure the passing packets, to avoid the hackers are hacking the packets. The IP routers are performed as the packets are allowed or disallow to decide. The packet filtering router is to providing a security from the hackers. It also checks the source and destination IP addresses, if the address is match the packets will be allowed, otherwise it ignore the packets. These types of basic tools are very smarter and very useful to the administrator and the user. The NAT is also performed in the packet filtering; it is matched from one group to another group to the end user. The NAT is the method for TCP/UDP ports are translated to the network addresses and its ports. This paper is also includes the packet filtering process and types etc.

Keywords: TCP, UDP, NAT, ICMP error codes

1. Introduction of a Packet Filtering

Packet filtering is a firewall technique. That is used to control the network access, by monitoring outgoing and incoming packets. The packet filtering checks source and destination IP addresses match for secure purpose and verified. Because many users may use the different application and programs, packet filtering also checks source and destination protocols, Such as User Datagram Protocol (UDP), Transmission Control Protocol (TCP).

Packet filtering is the part of a firewall program for protecting a local network from unwanted intrusion. Packet filtering is the process of accepting or blocking packets at a network interface based on source and destination addresses, protocols and network Address Translation (NAT).

The software firewall, packet filtering is done by a program called a packet filter. The packet filter examines, the every packet based on a specific set of rules, on that basis, and decides to prevent it called DROP or allow it to pass called ACCEPT.

1.1 Why Packet Filtering?

Packet filtering let us control (accepted or rejected) the data transfer based on,

- Address of the data is (supposedly) coming from
- Address of the data is going to
- The session and application protocol is being used to transfer the data.

Most of the packet filtering systems considers only the rule based, and the IP addresses based. That's not considered based on the data itself and not makes content-based decisions.

It allows providing, in a single place, particular protections for an entire network. For example consider the Telnet service. Routers also present a useful point for all of the traffic entering or leaving a network. If it has multiple routers for redundancy, it probably has far fewer routers, under much tighter control, than it have host machines.

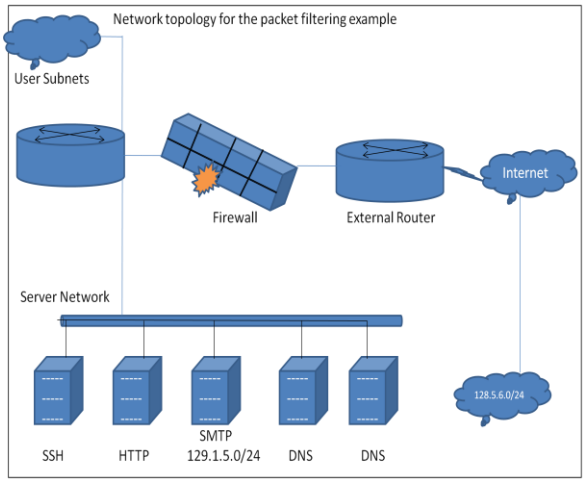
Certain protections can be provided only by filtering routers, and then only deployed in particular locations in to the network.

II. Process of the packet filtering

A packet filtering has a dirty port, a set of rules, and a clean port. The dirty port is showing to the internet and is where all traffic enters. The traffic that enters the dirty port is processed according to a set of rules or policies configured for the firewall. Based on the determined action derived from the rules set, the firewall will either let the packet enter

ISSN: 2278 – 1323

through the clean port into the trusted network or deny it from entering. In the example that follows, the network perimeter contains two DNS server, an HTTP server, a Secure Shell (SSH) server, and an SMTP server.



2.1. Sample Packet Filtering Rule Set

Rule	Protocol	Source Address	Destination Address	Source Port	Destination Port	Action
1	TCP	128.5.6.0/24	129.1.5.155	>1023	22	Permit
2	TCP	Any	129.1.5.154	>1023	80	Permit
3	TCP	Any	129.1.5.150	>1023	25	Permit
4	UDP	Any	129.1.5.152	>1023	53	Permit
5	UDP	Any	129.1.5.153	>1023	53	Permit
6	Any	Any	Any	Any	Any	Any

Create a Rule Set

In order to provide an example of packet filtering, we need to create a rule set. The rule set contains the following criteria:

- Type of protocol
- Source address
- Destination address
- Source port
- Destination port
- The action the firewall should take when the rule set is matched.

The source port is not always a configurable option, but in most cases this is configurable. The Sample Packet Filtering Rule Set table presents the set of rules that will act as the policy that the firewall will utilize to determine whether a packet is allowed to enter into the trusted network.

Rule 1- This rule permits inbound access from a single IP subnet on the internet to a single host in the network for Secure Shell (SSH) access. SSH connections are sent from a random high port (RHP) to the destination TCP port of 22. It should identify the each connection.

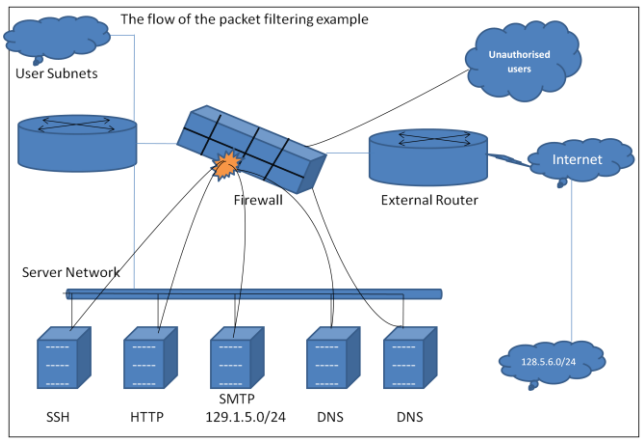
Rule 2 – This rules allows inbound access on port 80, which is typically used for HTTP traffic. The host at 129.1.5.154 is the web server for the domain. The organization cannot predict who will want to access its website, so there is no restriction on the source IP address.

Rule 3 – This rule allows inbound SMTP traffic. Within a Domain Name System (DNS), the company will have one or more records that indicate its SMTP mail servers. These records are called MX records. In this example network perimeter, this organization's DNS MX records resolves to the IP address 129.1.5.150.

Rule 4 and 5 – The two servers at IP addresses 129.1.5.152 and 129.1.5.153 are the Domain Name Service servers for this domain. In every cases, only UDP is required for proper DNS services. The two cases in which TCP is required are when support is needed for a DNS zone transfer and when the reply is so large that it cannot fit inside of a single UDP packet.

Rule 6 – This rule explicitly blocks all packets that have not matched any of the criteria in the previous rules. Most screening devices will perform this step by default, but it is useful to include this last cleanup rule. Including this rule clarifies the default policy enforcement and in most cases allows the packets that match this rule to be logged. This is useful for forensic and administrative reasons.

2.2. Example of Packet Filtering



ISSN: 2278 – 1323

III. Packet Filtering Concepts

The word of "filtering" is to suggest no changes are made to the packet being examined, there are several well – known manipulations of packet.

3.1. Network Address Translation – NAT

Network Address Translation is a method by which IP addresses are mapped from one group to another, transparent to the users. Network Address Port Translation is methods by which many addresses and their TCP/UDP ports are translate into a single network address and its TCP/UDP ports. These two operations are referred to as traditional NAT. The NAT is performed in two ways are,

1. **Static NAT**
2. **Dynamic NAT**

Address translation substitutes, in an IP packet, one IP address with another consistently.

The example is, Suppose the user have 20 machines like N10 to N19 with private addresses in the range of 192.160.15.10 to 192.160.15.29, but only two validly assigned IP addresses are X == 130.109.19.111 and Y == 130.109.19.222.

In ***Static*** NAT, any two of the hosts, like NX and NY statically chosen from the range of N10 to N19 can be given when the hosts can communicating with the internet by substituting with the addresses of X and Y. No address translation occurs when NX and NY are communicating with others in the 192.160.*.* network. When replies to these packets are received the NAT server record in a table contains the packets are "translation" and the NAT server knows where to redirect them. After the process is finished the NAT server on a secure machine can disable the NAT translation quickly if the user needed. The host machines N10 and N19 the IP addresses can assigned X and Y would have made it impossible for hosts N10 to N19, with their private addresses, connect to X and Y.

In ***Dynamic*** NAT, the NAT server assigns the two addresses X and Y that it controls to whichever of the hosts N10 through N19 is about to communicate with the Internet. Dynamic NAT is complex than Static NAT in that the NAT server must now decide when a host, say N6, is done communicating with the Internet so that the regular IP address, say Y, assigned to it currently can be considered available for other hosts.

The NAT can be termed as with two addresses available as in the above example only two internal hosts can be communicating with the Internet at any time.

3.2. Masquerading

Masquerading is a special form of Source NAT. Masquerading (MASQ) substitutes a single IP address, like Y, for an entire internal net. The MASQ server records the original source address of a packet and the destination address, and then replaces the source IP address as Y and forwards it out to the Internet. When the remote host replies, the MASQ server is able to recognize this masqueraded packet and it performs the reverse translation.

3.3. IP port forwarding

Port forwarding refers to the systematic substitution of one port number for another in a packet. This is relevant for TCP and UDP packets. Then the port forwarding is coupled with address translation also. Port forwarding and transparent proxying are special forms of Destination NAT.

3.4. Static and Dynamic Filters

Packet filtering can be ***static*** **methods** of connecting between the internal and external

networks left open at all times. The advantages of static packet filtering are:

- Low overhead / High throughput
- Inexpensive
- Good for traffic management

Dynamic packet filters open and close "doors" in the firewall based on header information in the data packet. Once a series of packets has passed through the "door" to its destination, the firewall closes the door.

IV. Types of Packet Filtering

This firewall allows only the packets to pass, which are allowed as firewall policy. Every packet passing through inspected and the firewall decides to pass it or not. This filtering can be divided into two parts:

ISSN: 2278 – 1323

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

Every packet have a header which provides the information about the packet, its source and destination. The firewall is inspects these packets to allow or deny. The information may or may not be remember by the firewall.

4.1. Stateless packet filtering

The firewall is not remembering the passing packets information, this type of filtering is called stateless packet filtering. This type of firewall is not enough to smarter and can be fooled very easily by the hacker. These are the very dangerous for UDP type of data packets.

4.2. Stateful Packet Filtering

It is reverse operation of stateless packet filtering. The firewall is remembering the passing packets information; this type of filtering is called stateful packet filtering. This is the very smarter as firewall. It is also known as Dynamic packet filtering.

V. Configuring a packet filtering router

This filtering router it needs to decide what services to allow or deny. This filters needs to translate decision into rules about packets. That is don't care about the details of packets at all. If the user want to receive mail from the Internet, and that's managed by packets. The router cares only about packets, and only about very limited parts. The rules for routers, it has to translate the statement "Receive a mail from the Internet" into a description of the separate packets want the router to allow to pass.

5.1. The Protocols Are Usually Bidirectional – It almost always involve one side sending an inquiry or a command and the other side sending a response of some kind. When the user is planning to the packet filtering rules that need to remember that packet go both ways.

5.2. Be careful of 'Inbound' Versus 'Outbound' semantics – When the planning of packet filtering strategy to be careful in discussions of "inbound" versus "outbound". That need to be careful distinguishes between inbound and outbound packets, and inbound and outbound services. An outbound service involves both outbound packets and inbound packets. Although most people habitually think in terms of services, need to make sure think in terms of packet, when the dealing with packet filtering. Other about filtering is sure to communicate clearly whether inbound versus outbound packets, or inbound versus outbound services.

5.3. Default Permit versus Default Deny

Default deny stance which is not expressly permitted is prohibited.

From security point of view, it is safer to take the attitude that things should be denied by default. The packet filtering rules reflect this stance. The default deny stance is much safer and more effective than the default permit stance, which involves permitting everything by default and trying to block those things that to know the problems. The reality in such an approach, it never knows about all the problems, and it never is able to do a complete job.

In practical terms, the default deny stance means that the filtering rules should be a small list of specific things to allow, perhaps with a few very specific things, that deny scattered throughout to make the logic come out right, followed by a default deny that covers everything else.

VI. What the Router act with Packets?

A packet filtering router has finished a specific packet, what can it do with that packet? Only two choices are available in this packet filtering are:

1. **Deliver the packet.** If the packets send to the packet filtering configuration, then the router will forward the packet to its destination, as a normal router (not a packet filtering router) would do.
2. **Not deliver the packet**. The other action to take is to not send the packet if it fails the criteria in the packet filtering configuration.

6.1. Logging actions

Whether the packet is forwarded or dropped. The packet filtering implementations support different forms of logging. User log only specific information about a packet and others will forward or log an particular dropped packet. Most of the packet filtering occurs on dedicated routers, which have large amounts of disk space to logging.

ISSN: 2278 – 1323

6.2. Returning ICMP Error Codes

If the packets to be dropped, the router may or may not send back an ICMP error code mentioning what happened. Sending back an ICMP error code has the warning of sending machine not to retry sending the packet; that has to saving the some network traffic and some time for the user on the remote side. (If the users send back an ICMP error code, the user's connection attempt will fail immediately; otherwise it wills time out, which may take several minutes.)

Two sets of relevant ICMP codes

- "Destination unreachable" codes – defines in particular, "host is unreachable" and "the network is unreachable" codes.
- "Destination administratively unreachable" codes – defines in particular, "host administratively unreachable" and the "network administratively unreachable" codes.

The **INTERNET CONTROL MESSAGE PROTOCOL** is defined as ICMP**.** The designers intended is first pair of ICMP error codes that the router might return, "host unreachable" or "network unreachable", to indicate problems as the destination host is not. These error codes predate firewalls and packet filtering. The problem with returning one of the error codes is that some hosts to take quite. If these machines get back a "host unreachable" for a host, will that assume a host is totally unreachable and will close all currently open connections to it, even if the other connections were permitted by the packet filtering.

The second set of ICMP error codes the router might return, "host administratively unreachable" and "network administratively unreachable", were added to the official list of ICMP message types a few years ago, specifically to give packet filtering systems something to return when they dropped a packet. Many systems do not yet recognize these codes, although that should not cause to the system problems. Systems are supposed to simply ignore ICMP error codes that don't understand, so this should be equivalent to returning no error code to such systems.

VII. Filtering by Address

The most common packet filtering is filtering by address. Filtering in this way to restrict the flow of packets based on the source and/or destination addresses of the packets, without having to consider what protocols are involved. Such filtering can be used to allow certain internal hosts, for example, or to prevent and attacker from injecting forged packets (packets handcrafted so they appear to come from somewhere other than their true source) into network.

In the router between user's internal network and the Internet, the users could apply an inbound rule either to incoming packets on the Internet interface or to outgoing packets on the internal interface; either way, user will achieve the same results for the protected hosts. The difference is in what the router itself sees. If the user wants to filter the outgoing packets, the router is not protecting itself.

VIII. How to Choosing a Packet Filtering Router

A number of packet filtering routers are available. Every dedicated router supports packet filtering. The users should be choose a Good enough packet filtering performance for the user needs, choose a single – purpose Router or a General – purpose computer, and allow the simple specification of rules, Rules based on any header or Meta – packet, connection information for TCP packets.

Header information includes the following:

- IP source and destination address
- IP options
- Protocol, such as TCP, UDP, or ICMP
- TCP or UDP source and destination port
- ICMP message type

IX. Advantages of Packet Filtering

Packet filtering has a number of advantages are,

- ❖ It creates little overhead, so the performance of the screening device is less impacted.
- ❖ It is relatively inexpensive or even free.
- ❖ It provides good traffic management.
- ❖ It does not require user knowledge or cooperation.
- ❖ It is generally available in many routers.

ISSN: 2278 – 1323

- ❖ It use one screening router and can help protect an entire network.

X. Conclusion

The packet filtering is now a feasible network security tool, but some simple trader improvements could have a big force. There are some key deficiencies that look to be common to many trader, such as the failure to consider source TCP/UDP port in filters, that need to be addressed. Other improvements to filter requirement machine could really make simpler the lives of network administrators trying to use packet filtering capabilities, and increase their self-confidence that their filters.

XI. References

1. "Network security: The Complete Reference", author is Roberta Bragg, Mark phodes – Ousley keith Strassberg, "Tata McGraw – Hill" Edition.
2. "Firewalls" the author is John R. Vacca, Scott R. Ellis
3. "Anti – Hacker toolkit" Second Edition, Mike Shema and Radley C. Johnson
4. "Firewall – The Complete Reference" Tata McGraw – Hill Edition, Strassberg, Gondek, Rollie
5. [CHS91] Packet filtering in an IP Router"; the author is Bruce Corbridge, Robert Henig, Charles Slater,
6. Proceedings of the Fifth USENIX Large Installation and System Administration Conference (LISA V): San Diego, CA; October, 1992; pp. 227-232.
7. [Bellovin92a] Steven M. Bellovin, "Packet Founds on an Internet"; in preparation; 1992.
8. [Ches90] "The Design of a Secure Internet Gateway"; Bill Cheswick, Proceedings of the USENIX
9. Summer 1990 Conference; Anaheim, CA; June 11-15, 1990; pp. 233-237.
10. [Comer91] Douglas E. Comer, Internetworking with TCP/IP, volume I; Second Edition, 1991; Prentice-Hall, Inc.
11. [Kent89] "Comments on 'Security Problems in the TCP/IP Protocol Suite'", Stephen Kent, Computer Communications Review; July 1989.
12. [RFC1058] C. Hedrick, "Routing Information Protocol", Request for Comments 1058; available from the DDN Network Information Centre (NIC.DDN.MIL).
13. http://www.boran.com/security/
14. http://www.greatcircle.com/pkt_filtering.html (19 Aug 2000).
15. https://technet.microsoft.com/en-us/library/cc957881.aspx
16. searchnetworking.tech target.com/definition/packet-filtering
17. http://www.diablotin.com/librairie/networking/firewall/ch06 01.htm
18. http://www.informit.com/articles/article.aspx?p=3761
19. http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/PacketFilter/
20. http://www.cs.fsu.edu/~breno/CIS-5357/fall2004/packet filtering.pdf
21. http://www.thenetworkencyclopedia.com/entry/packet-filtering
22. http://citeseerx.ist.psu.edu/showciting?cid=86516

ISSN: 2278 – 1323