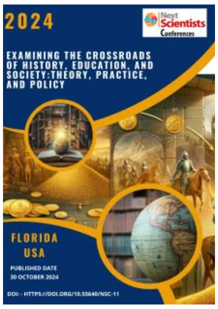

PACKET FILTERING TECHNIQUES FOR NETWORK SECURITY

Sarvar Norboboyevich Tashev
Head of the "Social and Economic Sciences" Department, Senior Lecturer,
Shakhrisabz Branch of Tashkent Chemical-Technological Institute,
Uzbekistan

ABSTRACT

This article extensively examines packet filtering technologies. Packet filtering technology is used to enhance network security and reduce harmful or unwanted traffic entering the network. The article also analyzes the advantages and disadvantages of packet filtering technology. The main benefits of filtering include the efficient use of network resources and protection against external threats, with the article detailing important strategies for packet filtering, such as static, dynamic, and fragmented packet filtering methods. Additionally, the article suggests strategies for improving packet filtering specifications, expanding access to all header fields, and simplifying filtering rules. These strategies aim to make the packet filtering process more efficient and provide significant assistance to network administrators in improving security.

KEYWORDS: Network security, firewall, packet filtering, routing table, packet filtering applications.

INTRODUCTION

The rapid growth of the Internet has connected millions of computers worldwide, requiring companies to connect to the Internet to establish communication with the outside world. Private networks, also known as intranets, of individual organizations need to be connected to the public network, i.e., the Internet. To ensure the security of an organization's private data, separate networks must be protected from general access. Implementing packet filtering is usually cost-effective. However, it is important to understand that a packet filtering device does not provide the same level of security as an application or proxy-based firewall. Aside from the simplest IP networks, all networks consist of IP subnets and include routers.

How does a packet filter work?

All packet filters operate in the same general mode. Operating at the network and transport layers of the TCP/IP protocol stack, each packet is inspected as it enters the protocol stack. The network and transport headers are carefully examined for the following information:

- Protocol (IP header, network layer) – The 9th byte in the IP header (remember, byte numbering starts from zero) identifies the packet's protocol. Most filtering devices can distinguish between TCP, UDP, and ICMP.
- Source address (IP header, network layer) – This is the 32-bit IP address of the host that created the packet.

- Destination address (IP header, network layer) – This is the 32-bit IP address of the host for which the packet is intended.
- 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 from and differ from UDP ports. Ports numbered below 1024 are reserved for special use, while ports numbered 1024 and above are called ephemeral ports, which can be used at the discretion of the vendor. For a list of "well-known" ports, refer to RFC1700. The source port is a pseudo-randomly assigned ephemeral port number, so filtering on the source port is often not very useful.
- Destination port (TCP or UDP header, transport layer) – The specified port number indicates the port to which the packet was sent. Each service on the target host listens on a specific port. Some well-known ports that can be filtered include: 20/TCP and 21/TCP - FTP connections/data, 23/TCP - Telnet, 80/TCP - HTTP, and 53/TCP - DNS zone transfers.
- Connection state (TCP header, transport layer) – The connection state indicates whether the packet is the first packet of a network session. The ACK bit in the TCP header is set to "false" or zero for the first packet. By rejecting or dropping any packets with the ACK bit set to "false" or zero, it is very simple to allow or deny connections to a host.

Packet filtering involves analyzing the header information of packets and making decisions on whether to drop or forward a packet. The decision can be based on multiple parameters. Packet filtering applications allow administrators to define rules that must be followed when making decisions. Rules defined by the administrator can be based on incoming or outgoing packets. The ability to set rules based on incoming and outgoing packets gives the administrator significant control over the filtering scheme's appearance in the routing table and assists with filtering on routers with more than two interfaces. External attackers may spoof internal source addresses and claim to be from an internal host. To prevent this from happening, the administrator needs to know from which interface the packet originated to identify the source. All packets that spoof internal source addresses can be discarded.

II. PACKET FILTERING STRATEGY

The main advantages of packet filtering include reducing incoming packet traffic and protecting network resources from malicious and unwanted access [1]. Several strategies can be used for implementing packet filtering, some of which are as follows:

- **Routing Table Solutions**

In this scheme, the decision to route or drop a packet is based on a search of the routing table. The routing table entries determine which destinations packets can be routed to and which cannot. This solution is helpful when using static routes. Routing protocols such as RIP can be applied, although they are not very secure. Routers can choose which sources to accept RIP data from, helping to prevent random incorrect data submissions.

- **Inbound and Outbound Filtering**

In this scheme, filtering is done at the external interface of the network in both the incoming and outgoing directions. This allows for achieving network security without slowing down internal routing within the network [2].

- **Source Address Filtering**

In this scheme, internal network connections have one authentication scheme, while external network connections have another. Internal connections are made to addresses within the organization's internal address space. If a filter is applied to the external interface, it will reject packets coming from inside that are actually from an external connection, i.e., where the source and destination addresses are within the internal address space, but the packet comes from outside the network.

- **Protocol Port Filtering**

In this scheme, filtering is applied to restrict access to services that can be accessed from the external network by examining the destination port to determine which set of destination ports can be accessed. For example, access to any of the TCP services like SMTP, NNTP, FTP data, FTP, finger, Telnet, login, and shell from external networks can be prohibited.

- **Advanced Filtering Strategies**

Some other strategies used by commercial vendors like Novell in Border Manager 3.7 include extended features such as static packet filtering, TCP ACK bit filtering, dynamic packet filtering, and fragmented packet filtering.

o **Static Packet Filtering**

In static filtering, each packet crossing the boundary between the internal networks (intranet) and external networks (Internet) is checked. The static packet filter examines header information for each packet to identify parameters such as protocol identifier, source and destination IP addresses, port numbers, and routing interface for incoming and outgoing packets. These parameters are checked, and then a decision is made to send or drop the packet according to the set rules for inbound and outbound traffic.

o **TCP ACK Bit Filtering**

In TCP ACK bit filtering, only packets with the TCP ACK bit set are allowed into the network. This prevents all external hosts from establishing TCP connections to internal hosts without authentication.

o **Dynamic Packet Filtering**

Also known as stateful packet filtering, this scheme tracks outgoing packets that have been allowed and only permits corresponding incoming packets to return. A return filter is dynamically created each time a packet is transmitted to the public network to allow for the response packet. This scheme supports both fewer connections and connection-oriented protocols.

o **Fragmented Packet Filtering**

Packets are broken into small pieces called fragments, with the first fragment containing the full header information. Initially, only the first packet is dropped since subsequent packets cannot be reassembled without header information. However, this can be exploited by attackers to fill the network with useless fragments. To avoid this, filtering drops the first packet as well as all subsequent packets with the same source and destination addresses and interfaces.

III. CURRENT ISSUES WITH PACKET FILTERING

Packet filtering can be a tool to improve overall network security. The number of IP routers offering this capability is increasing. If administrators use it correctly, packet filtering can be a very secure and useful tool. However, there are a number of challenges in designing and implementing packet filtering to make firewalls secure and efficient [5].

Some issues that need to be addressed include:

- Incorrect Classification: A packet filter can misclassify a packet if the source IP address is spoofed. Filtering based on the source port can face similar problems; for instance, a source machine could be running a suspicious client or server on this port.
- Variable Header Length: The options field makes the IP packet header length variable, making it difficult to locate higher-level protocol information such as TCP/UDP headers when using simple offset-based pattern matching.
- Fragmented Packets: When packets are fragmented, some packet filters drop the first fragment, considering the other fragments useless for the recipient. However, this poses risks, as attackers can find ways to bypass the system. This can also significantly complicate the packet filtering process.
- Predefined Header Fields: This rigidly affects flexibility. If the administrator does not specify which header fields to use for decision-making, it will not be possible to effectively implement the necessary security policy. For example, you may want to block packets with the TCP "SYN" flag set, but the packet filter may not allow this field to be used for filtering specifications [3].

Possible Solutions to Current Packet Filtering Issues:

1. Improving the syntax of the filter specification.
2. Opening all relevant header fields as filtering criteria.
3. Allowing both inbound and outbound filtering.
4. Simplifying tools for developing, testing, and monitoring filters.

Advantages of Packet Filters:

- These firewalls are inexpensive and have minimal impact on network performance.
- They do not require any special configuration of client computers.
- Application independence.
- Scalability.
- Packet filtering is fast, flexible, and transparent (does not require changes to be made by the client).
- They can process packets at very high speeds.
- They can easily match many fields in the Layer 3 packet and Layer 4 segment headers, providing significant flexibility in implementing security policies.
- Disadvantages of Packet Filters:
- They are not considered highly secure on their own, as they do not understand application-level protocols.
- They cannot make content-based decisions on packets.
- They do not keep track of source or connection state.
- They have very limited or no logging capabilities, making it difficult to detect if the network is under attack.
- Testing the rules for allowing and denying packets is also difficult, which may leave the network vulnerable or improperly configured [5].

Applications of Packet Filtering

A packet filtering device can be the first line of defense in a network and is used to block certain types of packets from entering the protected network. Although not a robust firewall on its own, it can be used to reduce the load on a proxy or application firewall. The following diagram shows a simple example of using packet filters alongside a proxy server or application firewall.

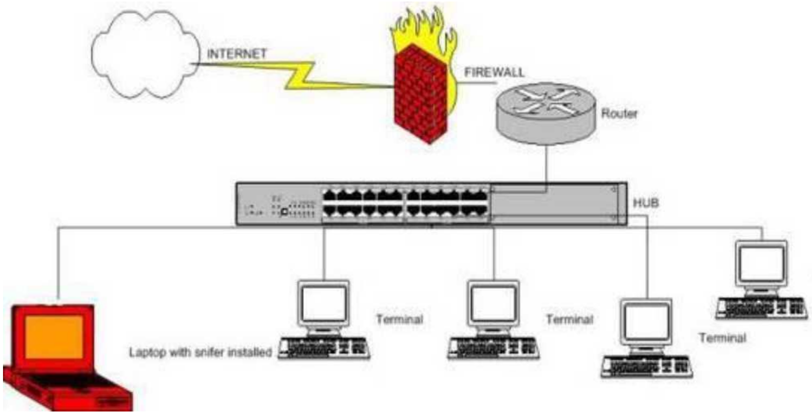

Figure 1. Network Inter-Screen for Packet Filtering

CONCLUSION

In conclusion, this article highlights the role of packet filtering technologies in ensuring network security, analyzing their advantages and disadvantages. The positive aspects of packet filtering, such as efficient resource usage and protection against external threats, have been noted, as well as the examination of methods for filtering static, dynamic, and fragmented packets. Additionally, suggestions have been made to improve the rules and specifications of packet filtering, making them simpler to implement for enhanced network security.

REFERENCES

1. Gulomov, Sh.R. "Types of Malicious Traffic in the Network and Their Detection." Multidisciplinary Scientific Journal, December, Issue 24, 2023, pp. 424–432.
2. Tashev, S.N., & Ganiev, A.G. "The Role of 'Imagination' in the Process of 'Creative Thinking,' Developing Students' 'Imagination' and 'Creative Thinking' Skills in Teaching Physics." Annals of the Romanian Society for Cell Biology, 2021/3/6, 633-642.
3. Tashev, S.N. "The Role of 'Imagination' in the Process of 'Creative Thinking,' Developing Students' 'Imagination' and 'Creative Thinking' Skills in Teaching Physics." Psychology and Education, 3569-3575.
4. Karamatovich, Y.B., Norboboev, T.S., & Ibrohimovich, N.I. "Verification of the Packet Filtering Based on Method of Verification on the Model." 2019 International Conference on Information Science and Communications Technologies (ICISCT).
5. Ning, J., et al. "Pine: Enabling Privacy-Preserving Deep Packet Inspection on TLS with Rule-Hiding and Fast Connection Establishment." Proceedings of the European Symposium on Research in Computer Security, 2020, pp. 3–22.