# The Importance of Firewall for the Online Network Security

**Prashant P. Pittalia**

***Abstract*— Day by day the new devices are comes in market and they are connected with networks to share the resources or information. It is very necessity of the network administrator to protect the devices with loss of data, false authentication, loss of data integrity as well as spreading a malicious software programs in the devices. It is required to use the technology to prevent against such attacks. This paper describes the task of firewall, various types of firewalls used to protect the network and its resources. The paper discusses the various attacks on packer filter firewall and its countermeasures. Also it discusses of firewall implementation approach and strategies for building firewall environments.**

***Index Terms*— Access Control, firewall, port number, protocol. Traffic**

## I. INTRODUCTION

Firewall techniques used worldwide to provide security of network. To keep the data or information safe in the network device as well as to keep all network resources in secure from the vulnerabilities created by attackers, we need to control the network with some techniques. Firewall is the technique to help to do such activities. A firewall is hardware, software, or a combination of both that is used to prevent unauthorized programs or Internet users from accessing a private network and/or a single computer. It inspects Inbound to or outbound from your computer. It determines whether it should be allowed to pass through or if it should be blocked. The word firewall is like a wall which is used to protect fire. In computer world the firewall protection refers to protect the network or computer from to block certain kinds of network traffic. It creates a barrier between trusted and untrusted network. It protects against the unauthorized access to resources and confidential information. The major role of firewall to identify the intruders and immediately take an action and make the network secure. Each firewall having basic three rules like allow, block and ask. These rules are for incoming and outgoing packet through the firewall. Allow – traffic that flows automatically because it has been deemed as "safe". Block – traffic that is blocked because it has been deemed dangerous for computer. Ask – asks the user whether or not the traffic is allowed to pass through. User control, access control, behavior control and direction control are the main task of the firewall. User control means only authorized users are having access to the other side of the firewall. Access control means according to settings on firewall the user or device may access the certain services. A service is characterized by IP address and port number. Behavior control indicates that how the particular services are used. E.g. filters for e-mail attachments to identify the mail with malicious program and stored them in spam folder. Direction control decides in which direction to allow particular services. In inbound it decides which services may be allowed for outsider and for outbound it decides which services may be allowed for the insiders.

## II. FIREWALL TYPES

In principle, there are mainly three types of firewalls:

- Network-Level Firewalls
- Circuit-Level Firewalls
- Application-Level Firewalls

### A.Network-Level Firewalls:

It works at the network level by inspecting packet headers and filtering traffic based on the IP address of the source and the destination, the port and the service. Some of these primeval security applications could also filter packets based on protocols, the domain name of the source and a few other attributes. Network-level firewalls are fast, and today you'll find them built into most network appliances, particularly routers. They don't understand languages like HTML and XML, and they are capable of decoding SSL-encrypted packets to examine their content. As a result, they can't validate user inputs or detect maliciously modified parameters in an URL request. This leaves your network vulnerable to a number of serious threats.

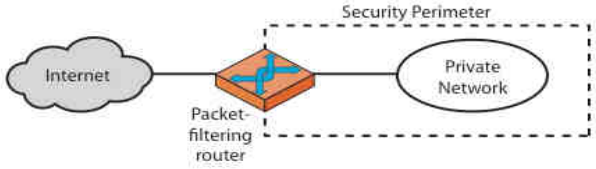


**Fig -1**: Packet filtering firewall [1]

• E.g. for your SMTP server with address 137.226.12.67 on port 25

From (IP *), (port *) To (IP 137.226.12.67), (port 25) DENY

From (IP 137.226.12.67), (port 25) To (IP *), (port *) ALLOW

(i.e.: your mail server can send mails to everybody, but nobody is allowed to send mails to your mail server)

### B. Circuit-Level Firewalls

This technology is generally referred to as a state full packet inspection as it maintains records of all connections passing through the firewall and is able to determine whether a packet is either the start of a new connection, a part of an existing connection, or is an invalid packet.

Manuscript received June 17, 2019

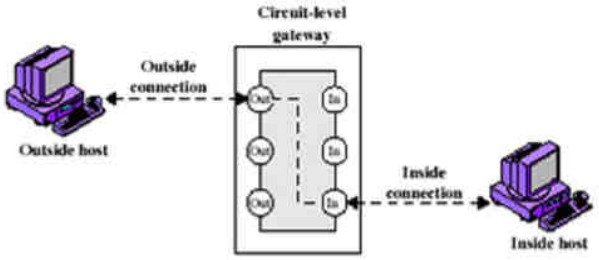


**Fig -2**: Circuit Level firewall [1]

It monitors TCP handshaking between packets to make sure a session is legitimate. Traffic is filtered based on specified session rules and may be restricted to recognized computers only. Circuit-level firewalls hide the network itself from the outside, which is useful for denying access to intruders.

### C.Application-level firewalls

Application-level firewalls have been looking more deeply into the application data going through their filters. By considering the context of client requests and application responses, these firewalls attempt to enforce correct application behavior; block malicious activity and help organizations ensure the safety of sensitive information and systems. They can log user activity too. Application-level filtering may include protection against spam and viruses as well, and be able to block undesirable Web sites based on content rather than just their IP address.

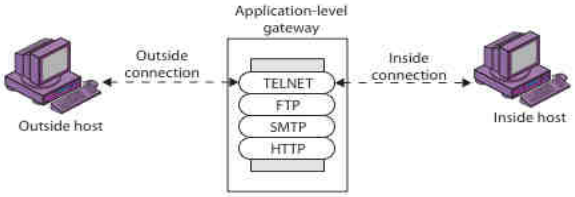


**Fig -3**: Application Level firewall [1]

The packet inspection is takes long time and so the network performance will be down. It is better to include lots of RAM to speed packet processing...

## III. Firewall Implementation Approach for Network Security

Initially, Implementing firewalls and firewall policy, Organization has to decide whether to implement the firewall as an appliance or on top of a commercial operating system, organizations must decide. While this decision will be largely determined by organization or agency requirements, the following issues should be considered:

As a first point of view appliance based firewalls will be more secure than those implemented on top of commercial

Operating systems. Appliance-based firewalls do not endure from security vulnerabilities associated with underlying operating systems. Appliance based firewalls generally use ASIC (Application Specific Integrated Circuit) technology, with the actual firewall software being present as firmware driving the ASICs. These firewalls also tend to be faster than firewalls implemented on top of commercial operating systems.

Scalability is the advantage of implementing firewalls on top of commercial operating systems. If an environment requires improved performance, organizations can buy a larger system on which to run the firewall software. Most appliances do not offer this level of flexibility or scalability.

The implementing of firewalls on top of operating systems may weaken the security posture of the firewall itself because of possible existence of vulnerabilities. In most circumstances where commercial firewalls are breached, that breach is facilitated by vulnerabilities in the underlying operating system. Much expertise is needed in securing the underlying operating system and maintaining it. This decision must be made based on relative costs, as well as estimates of future requirements.

## IV. Attacks on Packet Filtering Firewall and its Solution:

IP spoofing, Source routing attacks and tiny fragmentation are the possible attacks made on packet filtering firewalls. By proper setting in firewall, the attacks may be resolved.

- IP addresses spoofing:

Spoofing is an active security attack in which one machine on the network working on behalf of other machine without its concern. As an active attack, it disturbs the normal flow of data and may include data into the communications link between other machines. Its aim is to other machine on the network into accepting the intruder as an original. The meaning of "spoof" means that intentionally allow the others on network to consider it's genuine though it is actually a false. The intruder first identify the internal network IP address than generate a packet from outside network with the source address as internal machine IP address and transmits packets from the outside. The attacker knows that the spoofed IP address is allowed to pass through the firewall and move within a network.

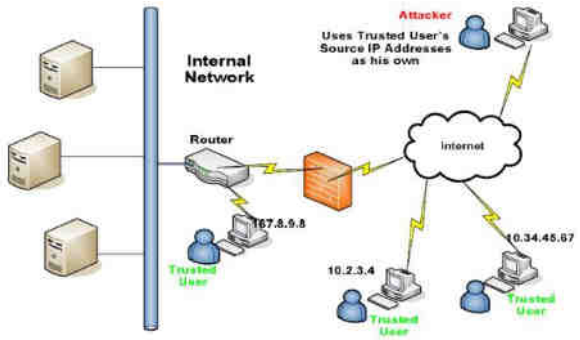


**Fig -4**: IP Spoofing [2]

The countermeasure is to make sure the direction of flow of packet at the interface of router. In such situation the rule is set in such a way that the packet comes from outside with source address as internal host IP address should be discarded immediately at any interface of the router.

- Source routing attacks:

In conventional routing, routers in the network determine the path incrementally based on the packet's destination. In computer networking, source routing allows a sender of a packet to partially or completely specify the route the packet

takes through the network. The source route is an option in the IP header that allows the sender to override routing decisions that are normally made by the routers between the source and destination machines. Source routing is used by network administrators to map the network, or for troubleshooting routing and communications problems. There are basically two types of source routing: Strict source routing, in which the sender can specify the exact route. Loose source record route (LSRR) in which the sender can specify certain routers through which the packet must pass and others are optional for intermediate routers. This attack can cause severe damage in the network by entering wrong routing table entries in the routing table. If the system allows source routing, an intruder can use it to reach private internal addresses on the LAN that normally would not be reachable from the Internet, by routing the traffic through another machine that is reachable from both the Internet and the internal machine. [3]

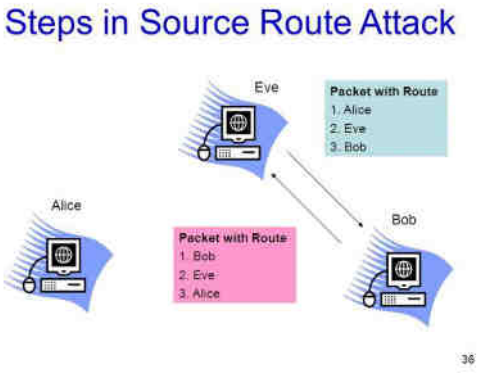


**Fig -5**: Source Routing Attack [4]

For example, let's consider Alice and Bob are the two users who are communicating and the attacker Eva in between to hack the data in the network. Bob is the sender who wants to communicate with the Alice who is a receiver and in between the attacker is Eva. To make an attack, Eva first identifies the Bob actual IP address. Then, Eva first generates a fake packet with source router option Bob->Eva->Alice by using the source address of Bob. Someway the Bob responds to Alice via Eva. Now Eva can intercept all packets and get credential information. The solution to such attack is to discard all packets that come with source route option in IP packet.

- Tiny fragment attacks:

When a datagram is passing through the lower level protocols it may be necessary to split the datagram in smaller portions. If the datagram size is small the maximum transfer unit then fragmentation is required. When datagram is fragmented, header is copied in each fragment of the datagram. The More Fragment flag is set in all fragments except the last one. Each fragment is delivered as separate datagram. Some firewalls make decision on the first fragment and then it allows the subsequent fragment with the same datagram Id. The intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment. Normally, a packet filter will make a filtering decision on the first fragment of a packet. All subsequent fragments of that packet are filtered out solely on the basis that they are part of the packet whose first fragment was rejected.

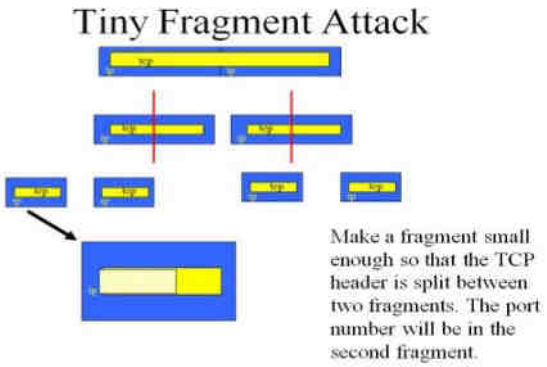


**Fig -6**: IP fragmentation attack [5]

The attacker hopes that the filtering firewall examines only the first fragment and that the remaining fragments are passed through. The solution of tiny fragment attack can be solved by enforcing a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header details. If the first fragment is rejected, the filter can remember the packet and discard all subsequent fragments.

## V. STRATEGIES FOR BUILDING FIREWALL ENVIRONMENTS:

There is four principles that should be noted to building firewall environments:

Maintain It Simple: It should be first step in firewall environment. The firewall solution is as simple as possible to make it secure and to easily manage in future. Complexity in design and function often leads to errors in configuration.

Do Not Affect The Network Devices: Do not use firewall in such a way that network devices original functionality will be lost. For example, routers are meant for routing; their packet filtering capability is not their primary purpose, and the distinction should never be lost on those designing a firewall implementation. Depending on routers alone to provide firewall capability is dangerous; they can be misconfigured too easily. Network switches are another example; when used to switch firewall traffic outside of a firewall environment, they are susceptible to attacks that could impede switch functionality. Firewall hardware & mixture firewalls are better choices because they are optimized.

Security in Depth: Security in depth involves defining the levels that should be checked by the firewall. Do not place all your protection at the firewall. Sometimes more firewall can be used, they should be used. Sometimes routers can be configured to provide some access control or filtering, they should be. If a server's operating system can afford some firewall facility, use it.

Be Sure From Internal Threats: It may be difficult to think of your work colleagues as affectation a potential threat. Consider that an intruder who gets past the firewall somehow could now have free to attack internal or external systems. As a result E-commerce organizations have to locate all servers like internal web servers, FTP server, financial systems, SMTP servers; DNS servers behind internal firewalls.

## CONCLUSION

Today most of the devices are connected to the Internet, it means that the device should be identified as well as getting

some information of device from any corner of the world. Attacker are very smart and they try to identify the weaker networks and within that weaker machines and then try to exploit vulnerability over there. To protect the network or machine from attackers it should be required to proper configure the firewall and make some settings in it.

## REFERENCES

[1] Network security essentials: applications and standards, William Stallings, Edition3, Prentice Hall, 356
[2] https://slideplayer.com/slide/16485873/
[3] https://www.sciencedirect.com/topics/computer-science/source-routing
[4] https://slideplayer.com/slide/6343254/
[5] https://www.slideshare.net/mukeshchaudhari3576/attacks-and-their-mitigations