I. INTRODUCTION

Security is the most important aspect in a network. There are a lot of concepts for network security.

Firewall is one of the most important concepts related to the network security. The term “firewall” was came to use in 1764, to describe walls which distinct the parts of a building most likely to have a fire from the rest of a structure. Firewall can be software or hardware. There is many installation software for network security; likewise, there are firewall devices for network security.

The protection that firewalls provide is only as good as the policy they are configured to implement .The host operating system should be as secure as possible prior to installing the firewall software. This not only means knowing how the operating system was installed but also making sure that all of the security patches are applied and that unnecessary services and features are disabled or removed. We called it a security wall because no unauthorized person can closed the wall without any request so; it can be hardware, software or both as shown in Figure 1.

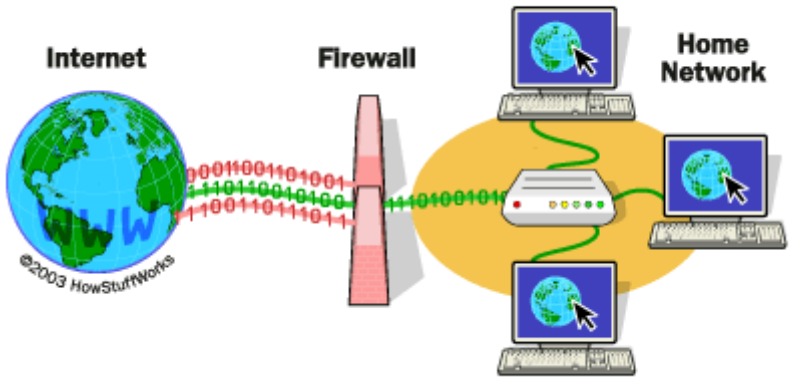


Figure 1:

2. So what does a firewall do?

A firewall protects your computer from intrusion (scanning or attack) by hackers while it is connected to the Internet. A firewall examines electronic data coming in or out of a computer (or network) and compares it to the rules it has been given. If the data matches the rules, it’s allowed to pass. If it doesn't, it is blocked.
You can think of a firewall as a piece of software that keeps the bad guys out and lets the good ones in.
Research shows that an unprotected computer system will come under attack within the first 15 minutes of Internet use. This is why it’s so important that you have security software installed on your PC before you connect to the Internet.

3. Some of the things a firewall does NOT protect you against:

- most viruses
- spam messages
- a poorly configured Wireless Network

• malware software installations (it prevents spyware actions, although the spyware may still be present in your computer)

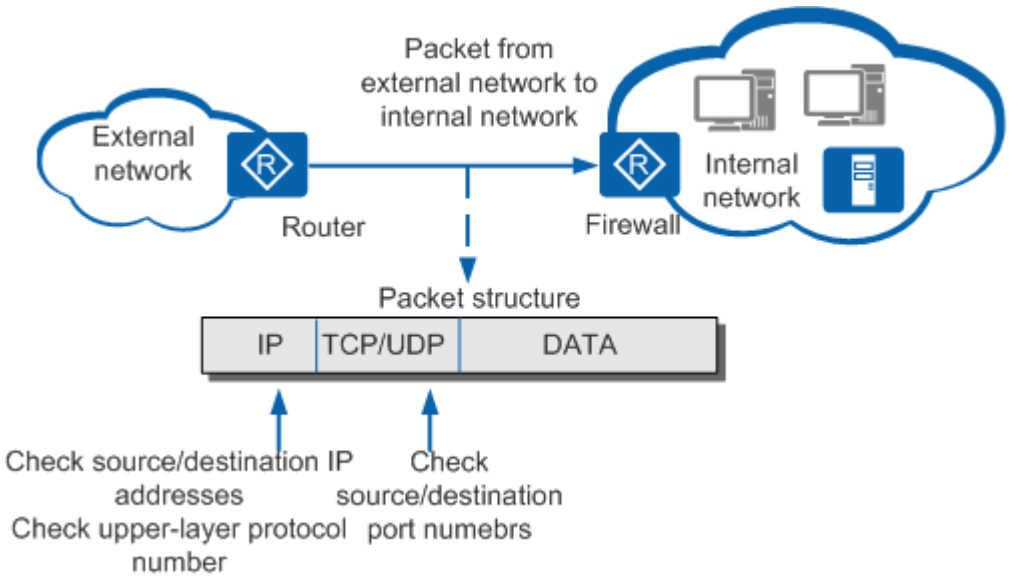
There are several different ways security firewalls can monitor and regulate network traffic in your PC.

These methods can include:

Packet filtering :

A packet filtering firewall uses access control lists (ACLs) to filter packets based on the upper-layer protocol ID, source and destination IP addresses, source and destination port numbers, and packet transmission direction.

When receiving an IP datagram, the firewall obtains the packet header, and then compares the packet header information with ACL rules to determine whether to forward or discard the IP datagram. shows how packet filtering is implemented on the firewall.



Proxy service :

A firewall in the form of security software installed on a proxy server to act as a barrier between internal and external networks and, thereby, to both prevent unauthorized entities from gaining access to internal company resources and block internal users from gaining access to unauthorized external resources. A proxy firewall presents a single network address to the Internet, rather than exposing the true addresses of internal users. Network address translation (NAT) software is required to make the address translations in order that authorized communications can take place in a conversational manner

Stateful inspection :

Where static filtering examines the packet headers, stateful inspection firewalls examine a variety of elements of each data packet and compare them to a database of trusted information. These elements include source and destination IP addresses, ports, and applications. Incoming data packets are required to sufficiently match the trusted information in order to be allowed through the firewall. Stateful inspection is a newer method of firewall filtering.

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.

Suppose you have a server with this list of firewall rules that apply to incoming traffic:

1. Accept new and established incoming traffic to the public network interface on port 80 and 443 (HTTP and HTTPS web traffic)
2. Drop incoming traffic from IP addresses of the non-technical employees in your office to port 22 (SSH)
3. Accept new and established incoming traffic from your office IP range to the private network interface on port 22 (SSH)

Note that the first word in each of these examples is either “accept”, “reject”, or “drop”. This specifies the action that the firewall should do in the event that a piece of network traffic matches a rule. **Accept** means to allow the traffic through, **reject** means to block the traffic but reply with an “unreachable” error, and **drop** means to block the traffic and send no reply. The rest of each rule consists of the condition that each packet is matched against.

Default Policy

It is typical for a chain of firewall rules to not explicitly cover every possible condition. For this reason, firewall chains must always have a default policy specified, which consists only of an action (accept, reject, or drop).

Suppose the default policy for the example chain above was set to **drop**. If any computer outside of your office attempted to establish an SSH connection to the server, the traffic would be dropped because it does not match the conditions of any rules.

If the default policy were set to **accept**, anyone, except your own non-technical employees, would be able to establish a connection to any open service on your server. This would be an example of a very poorly configured firewall because it only keeps a subset of your employees out.