Hello Everyone, in this video you will learn about, Firewall and its various types.

Let's understand some more Security techniques. A Firewall is one of them. It is simply a program or hardware device that filters the information coming through the internet connection into your private network or computer system.

Firewalls can be categorized based on various features like the data being filtered, such as Application level firewalls, or packet filter firewalls. Firewalls may also be categorized based on the scope of working, such as host based firewall, or network based firewall. Similarly, they can be software firewall, or hardware firewall, based on their implementation.

An application firewall works on application layer and filters the application layer data such as the data related to HTTP, FTP or Telnet protocols etc. working on application layer.

Packet filtering firewalls work on Network layer and are able to filter the traffic based on IP address and port numbers.

Firewalls can be host based or, network based, depending on the target being protected. A host based firewall,

protects an individual host machine, and is installed on that host only, while, network based firewall, protects a complete network and is installed, between network and Internet.

Here are some examples of host based firewalls and network based firewalls. Windows firewall is an example of host based firewall whereas the firewalls provided by companies like Check point, CISCO or Fortinet are network based firewalls.

Based on the implementation technique a firewall can be a hardware firewall, or software firewall.
A hardware firewall is a physical device between your computer and the Internet that protects all the computers from any unauthorized Internet user accessing private networks connected to the Internet. It blocks harmful pieces of data from reaching the system, and protects your network, against viruses and malware.
Software firewalls are installed on individual server machines. They intercept each connection request and then determine, whether the request is valid or not.

Apart from these classifications, there are some other types of firewalls also like, stateful firewall, Deep packet inspection firewall and application proxy firewalls. Let's understand about them one by one.

A stateful packet firewall tightens up the rules for tcp traffic by monitoring of outbound tcp connections. It allows the packets, belonging to any existing tcp connection only. Packets flow directly from client to server, provided they match either an “allow” rule or a state-table entry

Deep Packet inspection firewalls are able to dig deeper into the packet to analyze the application data to allow or disallow. The traditional firewalls are not able to access the payload or application data. They only deal with the fields available in the header.

Application proxy firewall, acts as a proxy on behalf of websites, such as social media sites. All the machines inside the network, when make a request, to access any web site, the request is first intercepted by the proxy, which checks the rules, defined for the destination, and allows or blocks the traffic accordingly. Therefore, it is used to block, the access to the unwanted or, malicious websites.

A firewall being a software, or a combination of software and hardware, is required to be trained, for efficient working. This training is done by defining, the rules in its table. The firewall rules may be defined, based on protocols, domains, IP addresses, ports etc.

In this figure you can see two rules for permitting and denying. First rule permits the source IP address (the computer's IP address to be allowed to access) to access any

destination with the TCP protocol whereas in second rule the subnet (192.168.1.0 with a mask of 255.255.255.0) is denied from using any destination with TCP protocol.

Here we can see two more firewall rules. The first rule denies all the website access using http protocol while second rule denies access to all websites using https protocol.

Thank you