LINUX FIREWALL

LINUX FIREWALL

- A firewall can be defined as a system of network security that controls and filters the traffic on the rule's predefined set. It is an intermediary system between the Internet and the device.
- The kernel of Linux contains a subsystem, i.e., ***Netfilter.*** It is used for deciding or manipulating the network traffic fate headed through or into our server. All latest solutions of Linux firewall apply this system for a process which is known as "***packet filtering***".

LINUX FIREWALL

- The packet filtering system process of the kernel will be of tiny use to many administrators without any userspace interface for managing it. It is the goal of iptables: if a packet reaches our server, it would be handed off for rejection, acceptance, or manipulation to the ***Netfilter subsystem*** based on various rules supplied to it through userspace by iptables.

KEY POINTS

- A firewall is a group of rules.
- When a packet of data moves out or into a protected space, then its contents (information about its target, protocol, and the origin it plans for using) are checked against the rules of the firewall to see if it must be permitted through.
- Besides, iptables is another tool of CLI to manage the rules of firewall on any Linux machine.
- Also, Firewalld is a tool to manage the rules of a firewall on any Linux machine.
- Linux firewall can also be described as a device that checks Network traffic (outbound/inbound connections) and establishes a decision to traffic out or pass the traffic.
- In this era, Network Security is derived from different kinds of Linux firewalls.
- In the traditional packet, firewall filtering deals with filtering and routing packets, where else NGFWs would work with some other functions (with OSI layers).

WINDOWS FIREWALL

- Windows Firewall is a Microsoft Windows application that filters information coming to your system from the Internet and blocking potentially harmful programs. The software blocks most programs from communicating through the firewall. Users simply add a program to the list of allowed programs to allow it to communicate through the firewall. When using a public network, Windows Firewall can also secure the system by blocking all unsolicited attempts to connect to your computer.

WINDOWS FIREWALL

- Windows Firewall makes use of several features to help protect the user's computer from malicious attacks, including network isolation, which prevents malicious websites from taking over the user's browsing experience; traffic segregation, which protects the user's computer if it becomes a member of a botnet or becomes infected with a virus; and IPsec to encrypt Internet traffic.

- Since Firewall executes all of these operations automatically, most users do not need to take any action. These features are enabled by default when the user installs Windows OS. While users can turn various features on and off, best practices call for all features to be enabled for maximum protection to protect computers from incoming threats. The firewall offers three distinct layers of protection: private, public, and domain

CONT..

- **Private level** means that all traffic will be blocked from both incoming and outgoing connections.
- At the **public level**, all connections from outside the user's local network will be blocked.
- **Domain level** is used if the users are on a network protected by an authentication server such as Active Directory and will block only incoming connections from outside of the local network unless authorized by the said authentication server. If a program requests access through any firewall other than the domain, it will prompt the user to either allow or deny access.

FEATURES OF WINDOWS FIREWALL

- Block unauthorized traffic
- Control programs
- Create exceptions for trusted devices and locations

WINDOWS FIREWALL VS LINUX FIREWALL

- The main difference between Windows Firewall and Linux Firewall is how they operate in managing connections with other devices and applications. Both systems can block unauthorized access by creating rules based on specific criteria or settings, such as:
  - Source And Destination IP Addresses
  - Port Number, Protocol Type (TCP Or UDP)
  - Protocol Name

WHY USE THE LINUX FIREWALL INSTEAD OF THE WINDOWS FIREWALL?

- **The reason why we should choose Linux firewall over Windows firewall is mainly because of the following reasons.**
  - ❑ Linux firewall has more options compared to Windows firewall. Linux firewall offers much more functionality than Windows firewall. Some examples include allowing access from specific IP addresses, restricting network traffic by protocols, etc.
  - ❑ Linux firewall is entirely free, unlike the Windows firewall, which costs money every month. This means that you won't be forced into buying expensive software just so that you can protect yourself online.
  - ❑ Linux firewall is faster than Windows firewall. Since the Linux firewall runs directly inside the operating system rather than through an application layer, it can process data at a higher speed.
  - ❑ Linux firewall is compatible across different versions of Linux and other platforms such as MacOS X and Android.
  - ❑ Linux firewall supports multiple languages.