5.5 FIREWALL BASING

It is common to base a firewall on a standalone machine running a common operating system, such as UNIX or Linux.

Firewall functionality can also be implemented as a software module in a router or LAN switch.

Several options for locating firewall:

- Bastion host
- Individual host-based firewall
- Personal firewall

Bastion Host

- A bastion host is a system identified by thefirewall administrator as a critical strong point in the network's security, serving as a platform for an application-level or circuit-level gateway, or for external services

Common characteristics of a bastion host are as follows

- Executes a secure version of its operating system, making it a trusted system.
- Only essential services are installed on the bastion host. E.g: DNS, FTP
- May require additional authentication before a user is allowed access to the proxy services
- Each proxy is configured to support only a subset of the application's command set.
- Each proxy is configured to allow access only to specific host systems.
- Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection.
- Each proxy is independent of other proxies on the bastion host

Host-Based Firewalls

A host-based firewall is a software module used to secure an individual host. Such modules are available in many operating systems or can be provided as an add-on package.

- Like conventional standalone firewalls, host-resident firewalls filter and restrict the flow of packets.
- A common location for such firewalls is a server

Advantages:

- Custom-made filter rules for specific host needs
- Protection from both internal/external attacks, Independent of topology
- Additional layer of protection to organization firewall when used with a standalone firewall

Personal Firewall

A personal firewall controls the traffic between a personal computer or workstation on one side, and the Internet or enterprise network on the other side.

Features

- Controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side
- Can be used in the home environment and on corporate intranets
- Typically, is a software module on the personal computer
- Can also be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface
- Primary role is to deny unauthorized remote access to the computer
- Can also monitor outgoing activity in an attempt to detect and block worms and other malware