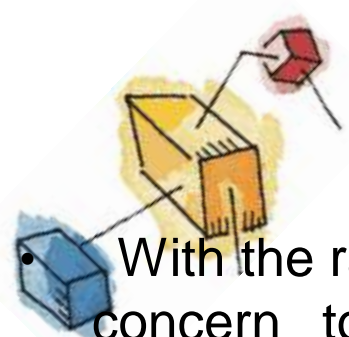


# Cyber Security

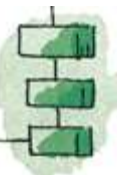
## **Chapter 6** **Cyber Security Technologies**



# Cyber Security Technologies



- With the rapid growth in the Internet, cyber security has become a major concern to organizations throughout the world. The fact that the information and tools & technologies needed to penetrate the security of corporate organization networks are widely available has increased that security concern.
- Today, the fundamental problem is that much of the security technology aims to keep the attacker out, and when that fails, the defences have failed. Every organization who uses internet needed security technologies to cover the three primary control types - preventive, detective, and corrective as well as provide auditing and reporting. Most security is based on one of these types of things: something we have (like a key or an ID card), something we know (like a PIN or a password), or something we are (like a fingerprint).



# Cyber Security Technologies

- Some of the important security technologies used in the cyber security are described below-

**Firewall and VPN**

**Intrusion Detection**

**Access Control**

**Security Technologies**




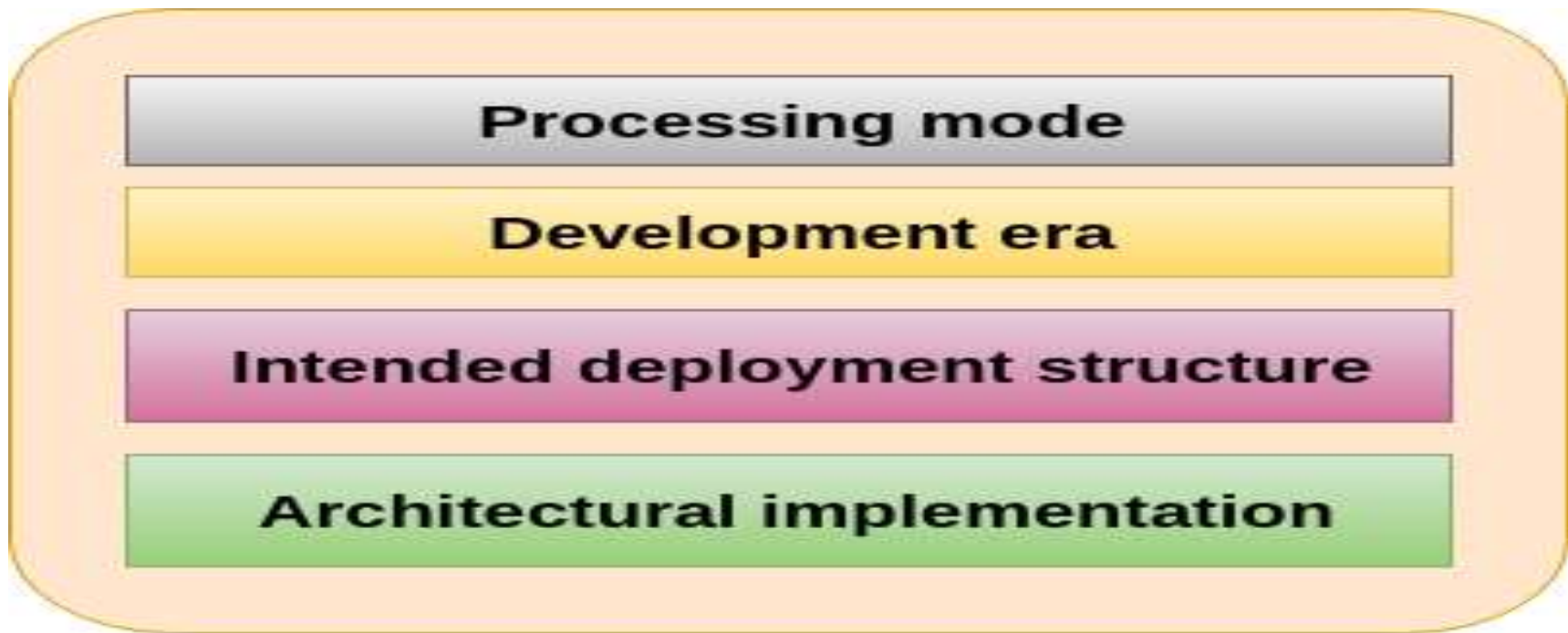
# Cyber Security Technologies

## Firewall

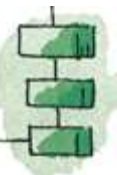
- Firewall is a computer network security system designed to prevent unauthorized access to or from a private network. It can be implemented as hardware, software, or a combination of both. Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages are entering or leaving the intranet pass through the firewall. The firewall examines each message and blocks those that do not meet the specified security criteria.
- Firewalls prevent unauthorized access to networks through software or firmware. By utilizing a set of rules, the firewall examines and blocks incoming and outgoing traffic.
- Fencing your property protects your house and keeps trespassers at bay; similarly, firewalls are used to secure a computer network. Firewalls are network security systems that prevent unauthorized access to a network. It can be a hardware or software unit that filters the incoming and outgoing traffic within a private network, according to a set of rules to spot and prevent cyber attack.

# Cyber Security Technologies

-  Firewalls are used in enterprise and personal settings. They are a vital component of network security. Most operating systems have a basic built-in firewall. However, using a third-party firewall application provides better protection.
- **Categories of Firewalls**
- Firewall can be categorised into the following types-



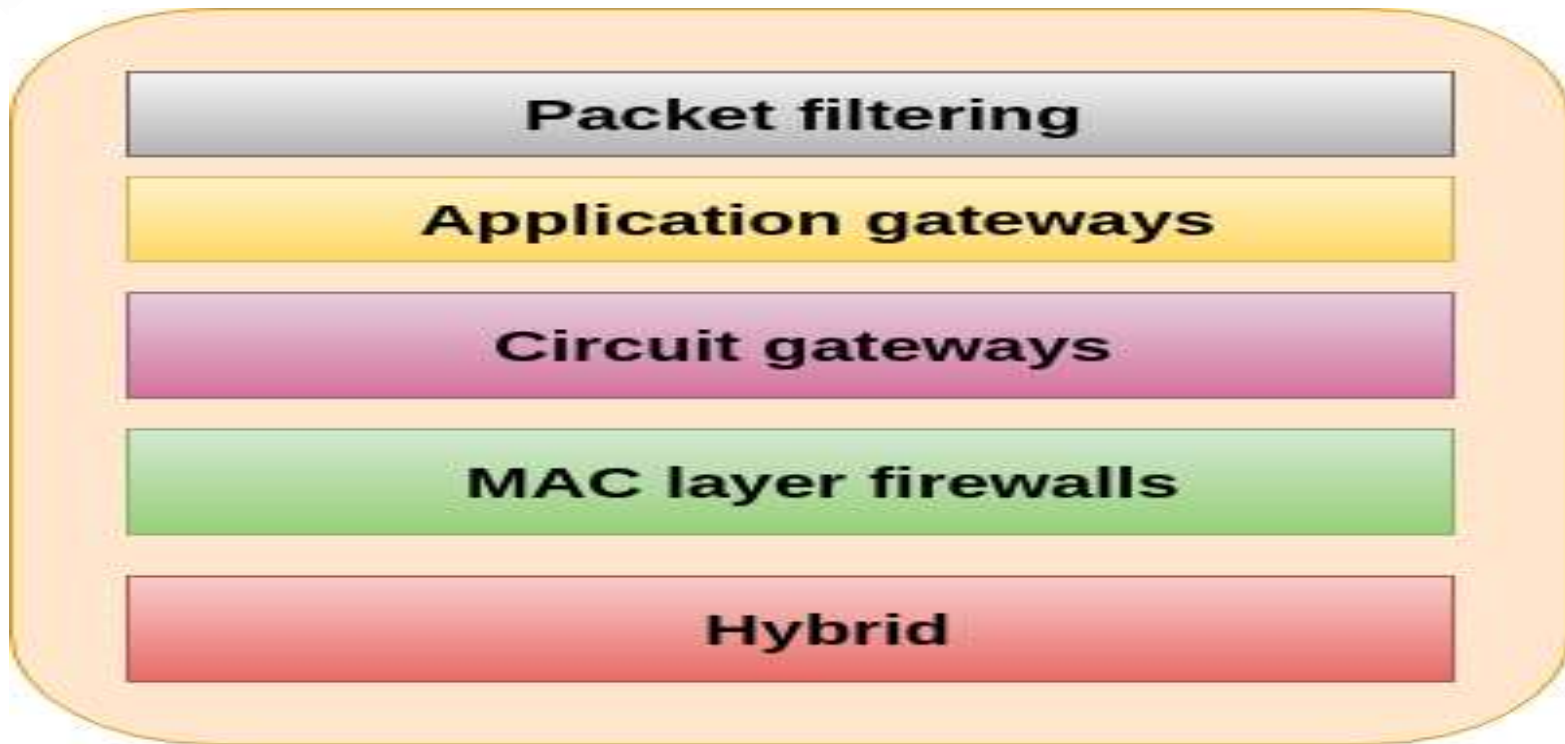
**Categories of Firewalls**



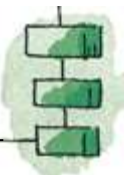
# Cyber Security Technologies

- **1. Processing mode:**

- The five processing modes that firewalls can be categorised are-



**Processing mode**





# Cyber Security Technologies

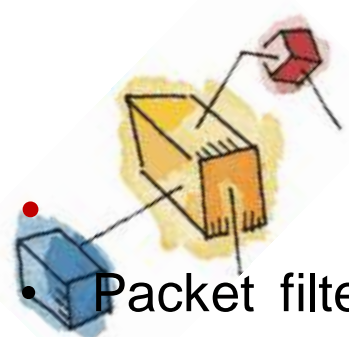
## Packet filtering

Packet filtering firewalls examine header information of a data packets that come into a network. This firewall installed on TCP/IP network and determine whether to forward it to the next network connection or drop a packet based on the rules programmed in the firewall. It scans network data packets looking for a violation of the rules of the firewalls database. Most firewall often based on a combination of:

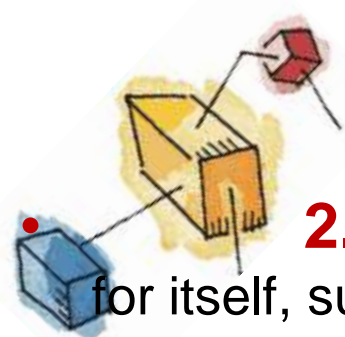
- Internet Protocol (IP) source and destination address.
- Direction (inbound or outbound).
- Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests.

Packet filtering firewalls can be categorized into three types-

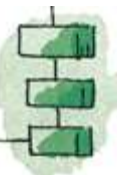
**1. Static filtering:** The system administrator set a rule for the firewall. These filtering rules governing how the firewall decides which packets are allowed and which are denied are developed and installed.



# Cyber Security Technologies



- **2. Dynamic filtering:** It allows the firewall to set some rules for itself, such as dropping packets from an address that is sending many bad packets.
- **3. Stateful inspection:** A stateful firewalls keep track of each network connection between internal and external systems using a state table.
- **Application gateways**
- It is a firewall proxy which frequently installed on a dedicated computer to provides network security. This proxy firewall acts as an intermediary between the requester and the protected device. This firewall proxy filters incoming node traffic to certain specifications that mean only transmitted network application data is filtered. Such network applications include FTP, Telnet, Real Time Streaming Protocol (RTSP), Bit Torrent, etc.





# Cyber Security Technologies

## • **Circuit gateways**

• A circuit-level gateway is a firewall that operates at the transport layer. It provides UDP and TCP connection security which means it can reassemble, examine or block all the packets in a TCP or UDP connection. It works between a transport layer and an application layers such as the session layer. Unlike application gateways, it monitors TCP data packet handshaking and session fulfilment of firewall rules and policies. It can also act as a Virtual Private Network (VPN) over the Internet by doing encryption from firewall to firewall.

## • **MAC layer firewalls**

- This firewall is designed to operate at the media access control layer of the OSI network model. It is able to consider a specific host computer's identity in its filtering decisions. MAC addresses of specific host computers are linked to the access control list (ACL) entries. This entry identifies specific types of packets that can be sent to each host and all other traffic is blocked. It will also check the MAC address of a requester to determine whether the device being used are able to make the connection is authorized to access the data or not.

# Cyber Security Technologies



## Hybrid firewalls

- It is a type of firewalls which combine features of other four types of firewalls. These are elements of packet filtering and proxy services, or of packet filtering and circuit gateways.

## • 2. Development Era:

- Firewall can be categorised on the basis of the generation type. These are-
- First Generation
- Second Generation
- Third Generation
- Fourth Generation
- Fifth Generation



# Cyber Security Technologies



## First Generation:

- The first generation firewall comes with static packet filtering firewall. A static packet filter is the simplest and least expensive forms of firewall protection. In this generation, each packet entering and leaving the network is checked and will be either passed or rejected depends on the user-defined rules. We can compare this security with the bouncer of the club who only allows people over 21 to enter and below 21 will be disallowed.

## Second Generation:

- Second generation firewall comes with Application level or proxy servers. This generation of firewall increases the security level between trusted and un trusted networks. An Application level firewall uses software to intercept connections for each IP and to perform security inspection. It involves proxy services which act as an interface between the user on the internal trusted network and the Internet. Each computer communicates with each other by passing network traffic through the proxy program. This program evaluates data sent from the client and decides which to move on and which to drop.



# Cyber Security Technologies

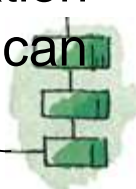


## • Third Generation:

The third generation firewall comes with the stateful inspection firewalls. This generation of the firewall has evolved to meet the major requirements demanded by corporate networks of increased security while minimizing the impact on network performance. The needs of the third generation firewalls will be even more demanding due to the growing support for VPNs, wireless communication, and enhanced virus protection. The most challenging element of this evolution is maintaining the firewall's simplicity (and hence its maintainability and security) without compromising flexibility.

## • Fourth Generation:

- The fourth generation firewall comes with dynamic packet filtering firewall. This firewall monitors the state of active connections, and on the basis of this information, it determines which network packets are allowed to pass through the firewall. By recording session information such as IP addresses and port numbers, a dynamic packet filter can implement a much tighter security posture than a static packet filter.



# Cyber Security Technologies

## Fifth Generation:

The fifth generation firewall comes with kernel proxy firewall. This firewall works under the kernel of Windows NT Executive. This firewall proxy operates at the application layer. In this, when a packet arrives, a new virtual stack table is created which contains only the protocol proxies needed to examine the specific packet. These packets investigated at each layer of the stack, which involves evaluating the data link header along with the network header, transport header, session layer information, and application layer data. This firewall works faster than all the application-level firewalls because all evaluation takes place at the kernel layer and not at the higher layers of the operating system.



# Cyber Security Technologies

## 3. Intended deployment structure:

- Firewall can also be categorized based on the structure. These are-

**Commercial Appliances**

**Small Office**

**Residential Software**

**Intendent Deployment Architecture**





# Cyber Security Technologies

- **Commercial Appliances**

- It runs on a custom operating system. This firewall system consists of firewall application software running on a general-purpose computer. It is designed to provide protection for a medium-to-large business network. Most of the commercial firewalls are quite complex and often require specialized training and certification to take full advantage of their features.

- **Small Office Home Office**

- The SOHO firewall is designed for small office or home office networks who need protection from Internet security threats. A firewall for a SOHO (Small Office Home Office) is the first line of defence and plays an essential role in an overall security strategy. SOHO firewall has limited resources so that the firewall product they implement must be relatively easy to use and maintain, and be cost-effective. This firewall connects a user's local area network or a specific computer system to the Internet networking device.





# Cyber Security Technologies

## Residential Software

- Residential-grade firewall software is installed directly on a user's system. Some of these applications combine firewall services with other protections such as antivirus or intrusion detection. There are a limit to the level of configurability and protection that software firewalls can provide.

## 4. Architectural Implementation

- The firewall configuration that works best for a particular organization depends on three factors: the objectives of the network, the organization's ability to develop and implement the architectures, and the budget available for the function.



# Cyber Security Technologies

- There are four common architectural implementations of firewalls:



**Packet-filtering routers**

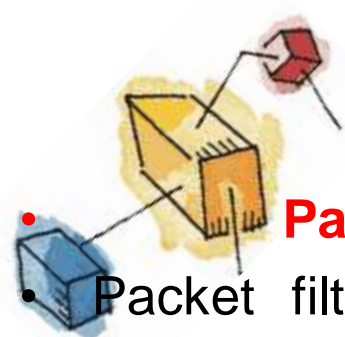
**Screened host firewalls**

**Dual-homed host firewalls**

**Screened subnet firewalls**

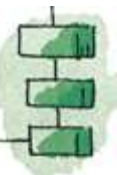
**Architectural Implimentation**

# Cyber Security Technologies



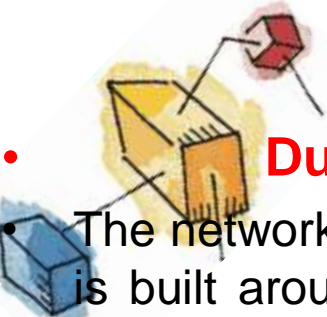
## Packet-filtering routers

- Packet filtering firewall is used to control the network access by monitoring the outgoing and incoming packets. It allows them to pass or halt based on the source and destination IP addresses, protocols and ports. During communication, a node transmits a packet; this packet is filtered and matched with the predefined rules and policies. Once it is matched, a packet is considered secure and verified and are able to be accepted otherwise blocked them.
- **Screened host firewalls**
- This firewall architecture combines the packet-filtering router with a separate and dedicated firewall. The application gateway needs only one network interface. It is allowing the router to pre-screen packets to minimize the network traffic and load on the internal proxy. The packet-filtering router filters dangerous protocols from reaching the application gateway and site systems.



# Cyber Security Technologies

## • Dual-homed host firewalls

A diagram showing a central yellow box representing the dual-homed host. It has two network interfaces: one on the left connected to a blue box representing the internal network, and one on the right connected to a red box representing the external network. Lines indicate the flow of traffic through the host.

The network architecture for the dual-homed host firewall is simple. Its architecture is built around the dual-homed host computer, a computer that has at least two NICs. One NIC is to be connected with the external network, and other is connected to the internal network which provides an additional layer of protection. With these NICs, all traffic must go through the firewall in order to move between the internal and external networks.

- The Implementation of this architecture often makes use of NAT. NAT is a method of mapping assigned IP addresses to special ranges of no routable internal IP addresses, thereby creating another barrier to intrusion from external attackers.

## • Screened Subnet Firewalls

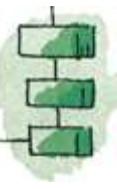
- This architecture adds an extra layer (perimeter network) of security to the screened host architecture by adding a perimeter network that further isolates the internal network from the Internet. In this architecture, there are two screening routers and both connected to the perimeter net. One router sits between the perimeter net and the internal network, and the other router sits between the perimeter net and the external network. To break into the internal network, an attacker would have to get past both routers. There is no single vulnerable point that will compromise the internal network.



# Cyber Security Technologies

## VPNs

- A VPN stands for virtual private network. It is a technology which creates a safe and an encrypted connection on the Internet from a device to a network. This type of connection helps to ensure our sensitive data is transmitted safely. It prevents our connection from eavesdropping on the network traffic and allows the user to access a private network securely. This technology is widely used in the corporate environments.
- A VPN works same as firewall like firewall protects data local to a device wherever VPNs protects data online. To ensure safe communication on the internet, data travel through secure tunnels, and VPNs user used an authentication method to gain access over the VPNs server. VPNs are used by remote users who need to access corporate resources, consumers who want to download files and business travellers want to access a site that is geographically restricted.





# Cyber Security Technologies

## • Intrusion Detection System (IDS)

- An IDS is a security system which monitors the computer systems and network traffic. It analyses that traffic for possible hostile attacks originating from the outsider and also for system misuse or attacks originating from the insider. A firewall does a job of filtering the incoming traffic from the internet, the IDS in a similar way compliments the firewall security. Like, the firewall protects an organization sensitive data from malicious attacks over the Internet, the Intrusion detection system alerts the system administrator in the case when someone tries to break in the firewall security and tries to have access on any network in the trusted side.
- Intrusion Detection System have different types to detects the suspicious activities-
- **1. NIDS-**
- It is a Network Intrusion Detection System which monitors the inbound and outbound traffic to and from all the devices over the network.





# Cyber Security Technologies

## 2. HIDS-

It is a Host Intrusion Detection System which runs on all devices in the network with direct access to both internet and enterprise internal network. It can detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to catch. HIDS may also identify malicious traffic that arises from the host itself.

## 3. Signature-based Intrusion Detection System-

It is a detection system which refers to the detection of an attack by looking for the specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. This IDS originates from anti-virus software which can easily detect known attacks. In this terminology, it is impossible to detect new attacks, for which no pattern is available.

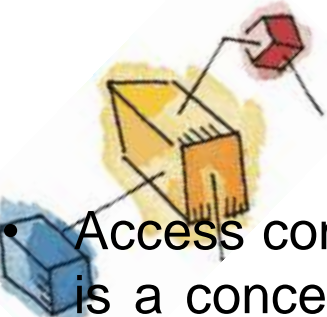
## 4. Anomaly-based Intrusion Detection System-

This detection system primarily introduced to detect unknown attacks due to the rapid development of malware. It alerts administrators against the potentially malicious activity. It monitors the network traffic and compares it against an established baseline. It determines what is considered to be normal for the network with concern to bandwidth, protocols, ports and other devices.



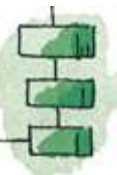
# Cyber Security Technologies

## • Access Control

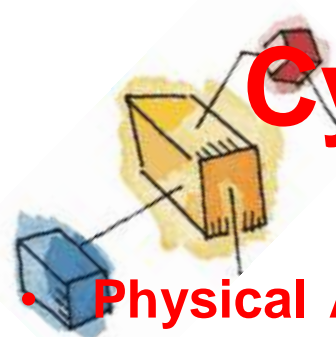


Access control is a process of selecting restrictive access to a system. It is a concept in security to minimize the risk of unauthorized access to the business or organization. In this, users are granted access permission and certain privileges to a system and resources. Here, users must provide the credential to be granted access to a system. These credentials come in many forms such as password, key card, the biometric reading, etc. Access control ensures security technology and access control policies to protect confidential information like customer data.

- **The access control can be categories into two types-**
- Physical access control
- Logical access control



# Cyber Security Technologies



- **Physical Access Control-** This type of access control limits access to buildings, rooms, campuses, and physical IT assets.
- **Logical access control-** This type of access control limits connection to computer networks, system files, and data.
- The more secure method for access control involves two - factor authentication. The first factor is that a user who desires access to a system must show credential and the second factor could be an access code, password, and a biometric reading.
- The access control consists of two main components: **authorization and authentication**. Authentication is a process which verifies that someone claims to be granted access whereas an authorization provides that whether a user should be allowed to gain access to a system or denied it.

