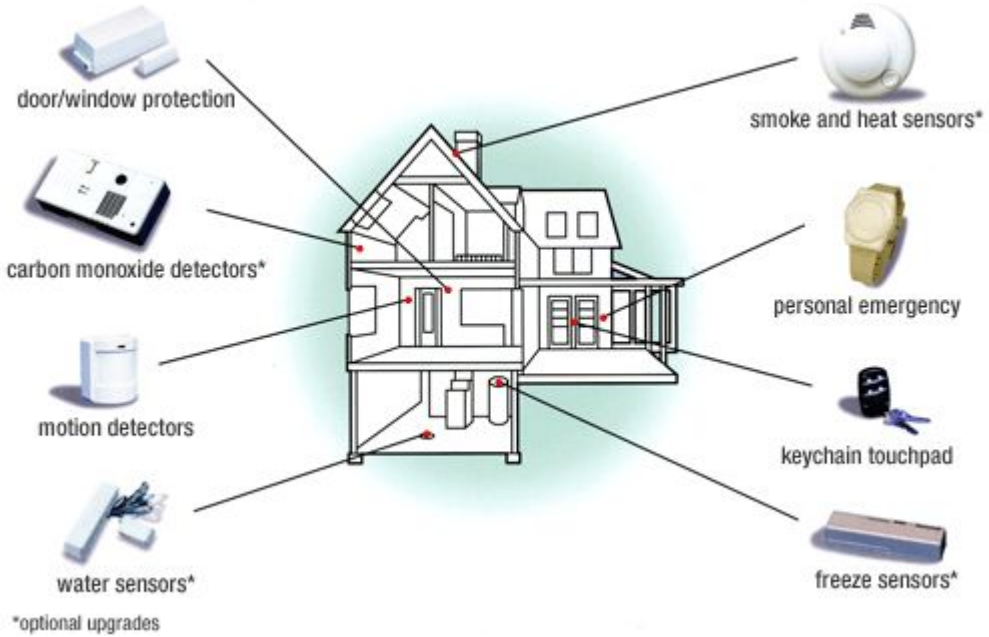
# Unit 5 Communication Security & System Security



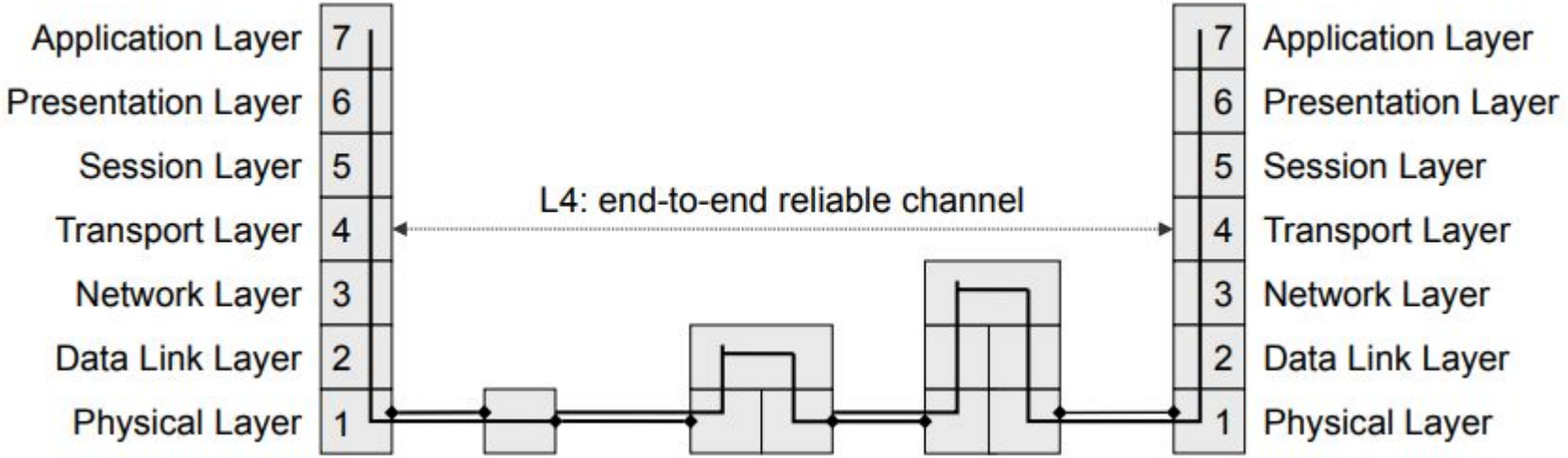
# Communication Security & System Security

- **Communication Security**
  - **HTTPS**
  - **SSH**
  - **Wireless Security and its Threats**
  - **IPSec**
  - **VPN**
- **System Security**
  - **Malicious Software**
  - **Types and Threats**
  - **Detection**
  - **Password Management**
- **Firewalls**
  - **Needs**
  - **Characteristics and Access Policy**
  - **Types of Firewall**

# Communication Security

**What is Communication security?**

- Communication security refers to the protection of data transmitted over a communication network.
- It involves various techniques and protocols to ensure confidentiality, integrity, and availability of data.

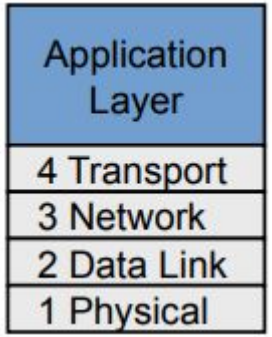


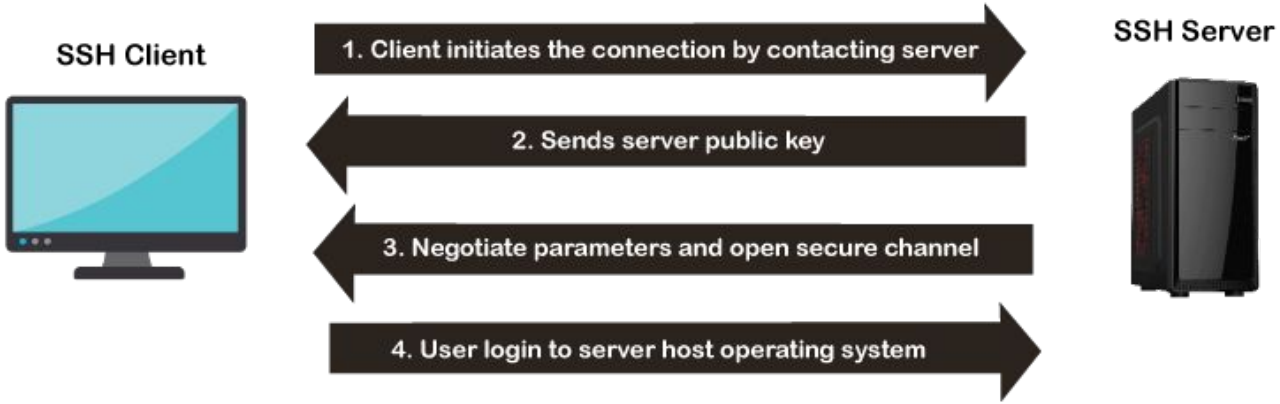
# HTTPS - Hypertext Transfer Protocol Secure

- HTTPS is a secure version of HTTP that uses SSL/TLS (Secure Sockets Layer/Transport Layer Security) to encrypt data transmitted between a web server and a web browser.
- **Key features:**
  - **Encryption:** HTTPS encrypts data using cryptographic algorithms to protect it from eavesdropping.
  - **Authentication:** HTTPS verifies the identity of the web server and client to prevent man-in-the-middle attacks.
  - **Integrity:** HTTPS ensures that data transmitted between the server and client has not been tampered with.
- HTTPS (HTTP over SSL) - combination of HTTP and SSL/TLS to secure communications between browser and server
- ➔ documented in RFC2818
- ➔ no fundamental change using either SSL or TLS
- Use https:// URL rather than http://
  - and port 443 rather than 80
- **Encrypts**
  - URL, document contents, form data, cookies, HTTP headers
- Does not encrypt
  - IP address of server, IP address of client: Network layer
  - hostname (virtual hosting: multiple domain names on a single server)

# SSH- Secure Shell

- Protocol for secure network communications designed to be simple and inexpensive
- SSH1 provided secure remote login facility replace TELNET and other insecure schemes
  - also has more general client/server capability
- SSH2 fixes a number of security flaws
- Documented in RFCs 4250 through 4254
- SSH clients and servers are widely available
- Method of choice for remote login / X tunnels



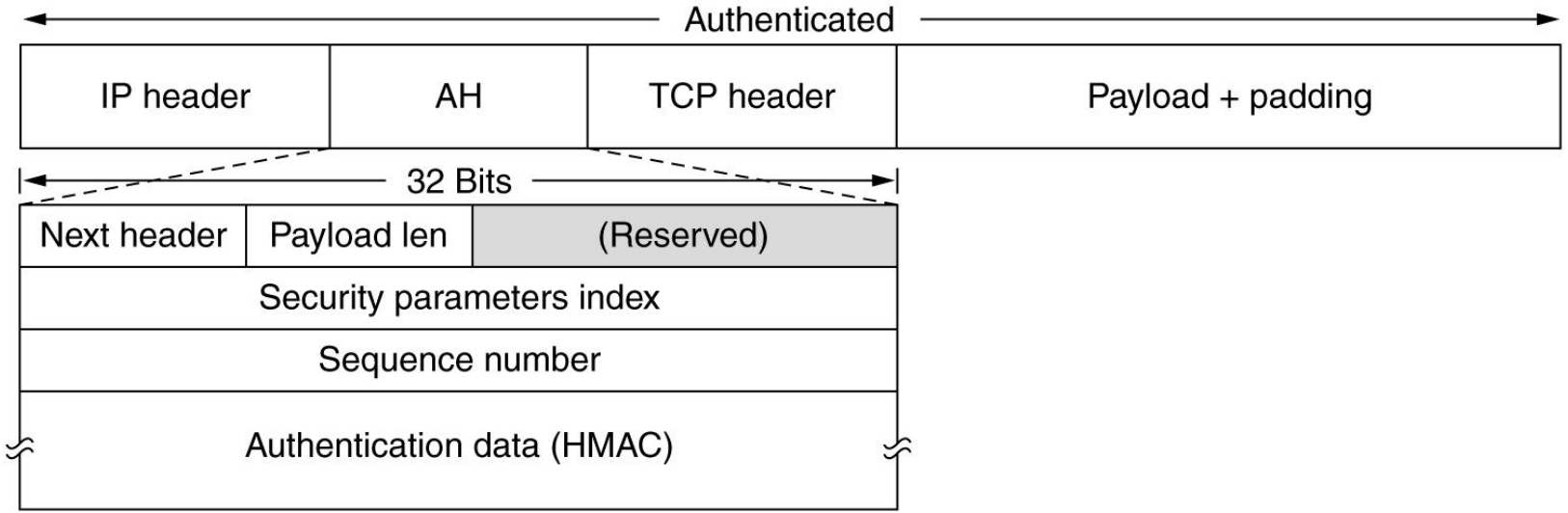



# Wireless Security and Its Threats

- Wireless security refers to the protection of data transmitted over wireless networks, such as Wi-Fi.
- **Eavesdropping:**
  - Unauthorized interception of data transmitted over the wireless network.
- **Man-in-the-middle attacks:**
  - An attacker positions themselves between a client and a server to intercept and manipulate data.
- **Rogue access points**:
  - Unauthorized access points set up within a network to intercept traffic.
- **Denial of service (DoS) attacks:**
  - Overwhelming a wireless network with traffic to disrupt its normal operation.

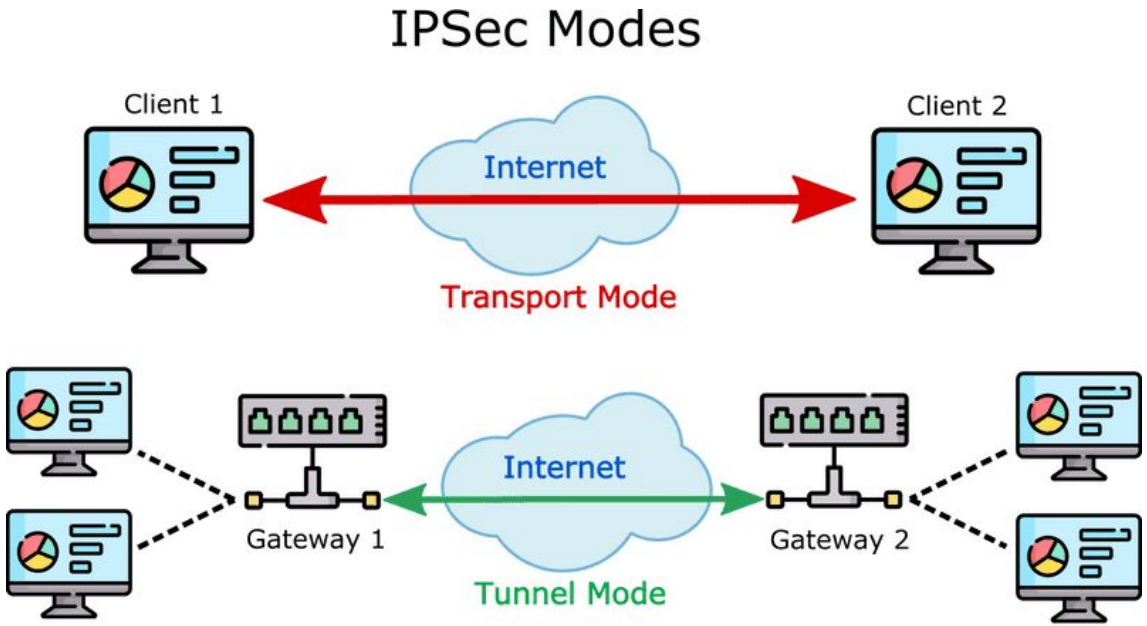
# IPsec

- IPSec is a suite of protocols that provides security for IP networks. It offers authentication, encryption, and key management services.
- **Key features:**
  - **Authentication Header (AH)**: Provides authentication, integrity, and anti-replay protection for IP packets.
  - **Encapsulating Security Payload (ESP)**: Provides encryption, authentication, and anti-replay protection for IP packets.
  - **Key Management Protocol (IKE)**: Negotiates security associations and manages cryptographic keys.

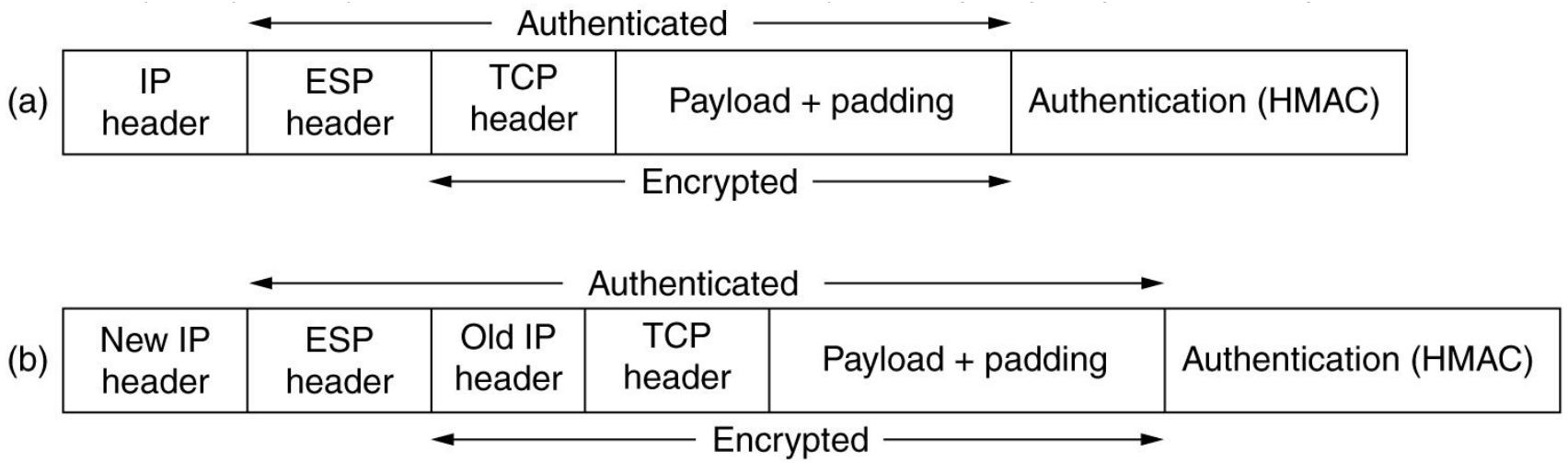


# IPsec Modes

- To achieve these goals, IPSec operates in two primary modes: **Tunnel Mode and Transport Mode.**
- **Tunnel Mode provides comprehensive protection for entire IP packets, often used for network-level security.**
- **Transport Mode focuses on protecting the data within IP packets, typically used for individual computer-level security.**



# IPsec Modes

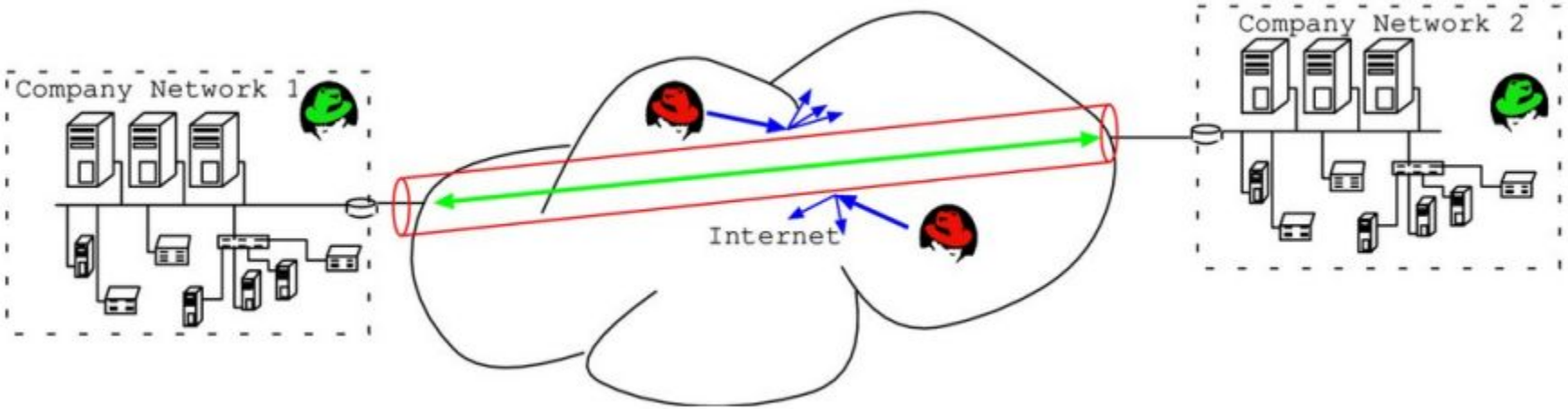



(a) ESP in transport mode. (b) ESP in tunnel mode.

# Virtual Private Networks (VPNs)

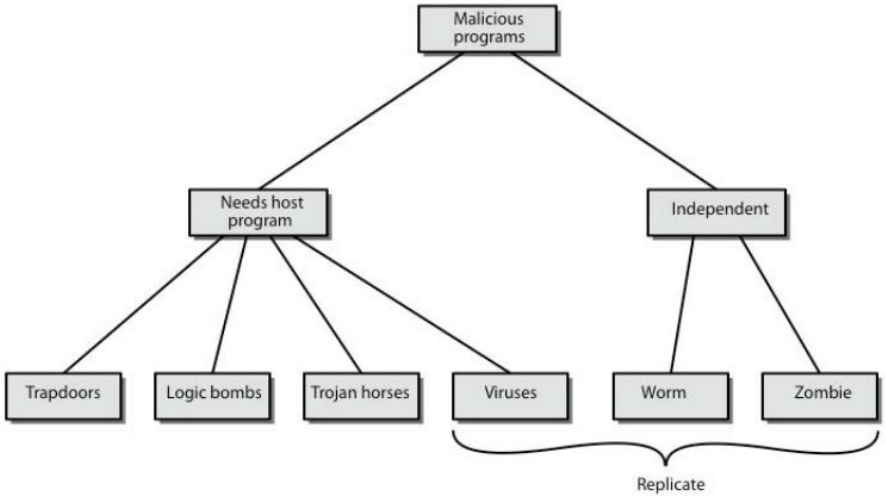
- A VPN creates a secure, private network connection over a public network, such as the internet. It encrypts data and hides the user's IP address.
- **Types of VPNs:**
  - **Site-to-site VPN**: Connects two or more networks over a public network.
  - **Remote access VPN**: Allows individual users to connect to a private network remotely.
  - **SSL/TLS VPN**: Uses SSL/TLS encryption to create a secure connection between a client and a server.

| Application Layer |
|---|
| 4 Transport |
| 3 Network |
| 2 Data Link |
| 1 Physical |



# System Security

- System security is the practice of protecting information systems from unauthorized access, modification, or destruction. System security measures help organizations protect sensitive data and prevent cyber threats.
- **Malicious software** : Malware is program that exploit vulnerabilities in computing systems.
- Malicious software is software that is intentionally included or inserted in a system for a harmful purpose.

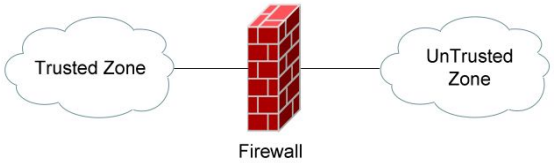


# Types of Malicious software

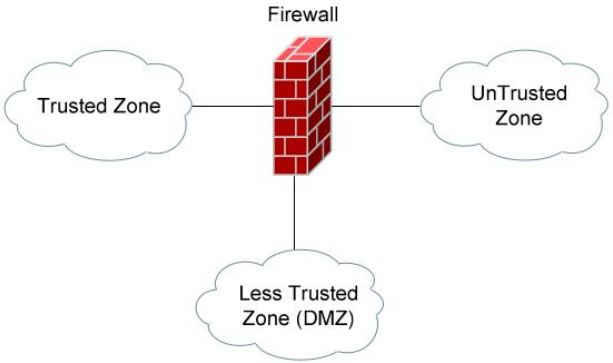
| Name | Description |
|---|---|
| Virus | Malware that, when executed, tries to replicate itself into other executable code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes. |
| Worm | A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network. |
| Logic bomb | A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met; the program then triggers an unauthorized act. |
| Trojan horse | A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program. |
| Backdoor (trapdoor) | Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality. |
| Mobile code | Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics. |
| Exploits | Code specific to a single vulnerability or set of vulnerabilities. |
| Downloaders | Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail. |
| Auto-rooter | Malicious hacker tools used to break into new machines remotely. |
| Kit (virus generator) | Set of tools for generating new viruses automatically. |
| Spammer programs | Used to send large volumes of unwanted e-mail. |
| Flooders | Used to attack networked computer systems with a large volume of traffic to carry out a denial-of-service (DoS) attack. |
| Keyloggers | Captures keystrokes on a compromised system. |
| Rootkit | Set of hacker tools used after attacker has broken into a computer system and gained root-level access. |
| Zombie, bot | Program activated on an infected machine that is activated to launch attacks on other machines. |
| Spyware | Software that collects information from a computer and transmits it to another system. |
| Adware | Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site. |

# Introduction to Firewalls

- Traditionally, a firewall is defined as any device (or software) used to filter or control the flow of traffic.
- Firewalls are typically implemented on the network perimeter, and function by defining trusted and untrusted zones :




- Most firewalls will permit traffic from the trusted zone to the untrusted zone, without any explicit configuration. However, traffic from the untrusted zone to the trusted zone must be explicitly permitted. Thus, any traffic that is not explicitly permitted from the untrusted to trusted zone will be implicitly denied (by default on most firewall systems).
- A firewall is not limited to only two zones, but can contain multiple ‘less
- trusted’ zones, often referred to as Demilitarized Zones (DMZ’s).



# Firewall Services

- **Firewalls perform the following services:**
  - Packet Filtering
  - Stateful Packet Inspection
  - Proxying
  - Network Address Translation (NAT)

# Packet Filtering

- Packet Filtering is one of the core services provided by firewalls. Packets can be filtered (permitted or denied) based on a wide range of criteria:
- • **Source address**
- • **Destination address**
- • **Protocol Type (IP, TCP, UDP, ICMP, ESP, etc.)**
- • **Source Port**
- • **Destination Port**

# Stateful Packet Inspection

- Stateful packet inspection provides services beyond simple packet- filtering, by additionally tracking TCP or UDP sessions between devices.
- For example, stateful inspection can track connections that originate from the trusted network. This session information is kept in a state session table, which allows temporary holes to be opened in the firewall for the return traffic, which might otherwise be denied.
- Connections from the untrusted network to the trusted network are also monitored, to prevent Denial of Service (DoS) attacks. If a high number of half-open sessions are detected, the firewall can be configured to drop the session (and even block the source), or send an alert message indicating an attack is occurring.
- A half-open TCP session indicates that the three-way handshake has not yet completed. A half-open UDP session indicates that no return UDP traffic has been detected. A large number of half-opened sessions will chew up resources, while preventing legitimate connections from being established.

# THANK YOU