**Security Objectives (Review)**

Before diving into **firewalls and IDS**, it's crucial to understand the fundamental goals of information security:

* **Confidentiality:** Protection of data from unauthorized disclosure.

*Example:* Encrypting sensitive emails so only the intended recipient can read them.

* **Integrity:** Assurance that data received is as sent by an authorized entity.

*Example:* Using digital signatures to verify that a document hasn't been changed since it was signed.

* **Availability:** Assures that systems work promptly and service is not denied to authorized users.

*Example:* Redundant servers and backup systems to ensure a website remains accessible even if one server fails.

* **Authenticity:** The property of being genuine /able to be verified / trusted / confidence in the validity of a transmission / message/ message originator.

*Example:* Using a strong password and two-factor authentication to confirm a user's identity before granting access.

* **Accountability:** The security goal that generates the requirement for Actions of an entity to be traced uniquely.

*Example:* System logs that record who accessed what file and when, for auditing purposes.

**Cybersecurity & Network Security (Review)**

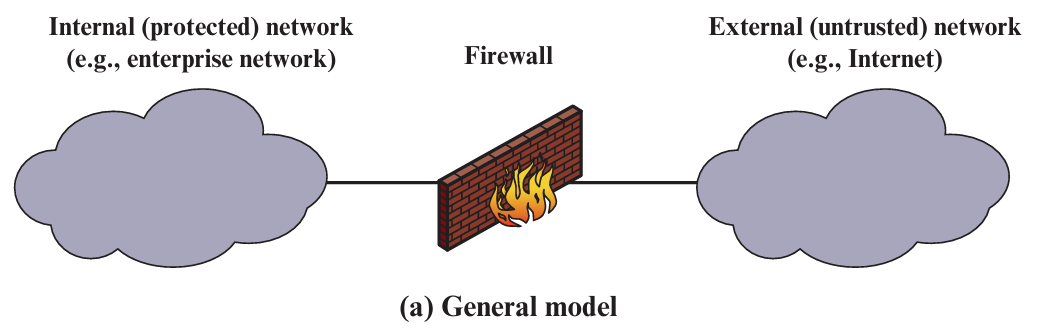
**Information Security:**

Information security means protecting data so that only the right people can access it (**confidentiality**), it stays accurate and unchanged (**integrity**), and it’s available when needed (**availability**). It also includes user's identity can be identified (**authenticity**), actions can be tracked (**accountability**), no one can deny their actions   
(**non-repudiation**), and the system works reliably.

**Network Security:**

Network security focuses on protecting networks and their devices from unauthorized access, changes, or damage. It ensures that data can move safely through the network and that everything connected (like routers or servers) works correctly and securely without causing harm or being exposed to threats.

**Firewalls:**  
A firewall is like a security gate that controls what data can go in or out of your network. It helps protect your internal network from the dangers of the internet and is often the first layer of defense.



**Main Purposes and Functions of Firewalls**

**1- Network Traffic Filtering:** Firewalls control what data enters or leaves a network by checking each packet against a set of rules. They filter traffic based on details like the source IP address (where it’s coming from), destination IP address (where it’s going), port numbers (type of service like web or email), and protocols (like TCP or UDP). This helps block unwanted or harmful traffic and only allows approved connections to pass through. **(Process)**

**2- Access Control:** Firewalls help control who can access your network by using **predefined rules**, which are settings created by network administrators to decide what is allowed or blocked. These rules tell the firewall to either permit or deny network connections based on things like IP addresses, ports, or types of services. This way, only trusted connections are allowed, while unknown or risky ones are blocked to keep the network safe. **(Action/Decision)**

**3- Network Address Translation (NAT):** NAT lets many devices (like phones, laptops, smart devices) **inside your private network** use **one public IP address** to connect to the internet.

**Purpose:**

* **Hides internal IP addresses** from the outside world for extra security.
* Helps the firewall **control traffic** coming in and going out.

**How It Works:**

1. You have a router/firewall with NAT.
2. Inside your network: devices like laptops, phones, and printers use private IP addresses.
3. When one of these devices accesses the internet, NAT changes the private IP into the public IP of the router.
4. It keeps track of the requests, so when the response comes back, it knows which internal device should get it (using translation table).

**4- Threat Prevention: Firewalls provide protection against various network threats, such as malware, viruses, and intrusion attempts.**

**5- VPN and Remote Access Security: Firewalls often support VPNs (Virtual Private Networks), which allow users to safely connect to a private network from a remote location (like from home or while traveling). A VPN encrypts the connection, keeping data private and secure from hackers, especially on public Wi-Fi. Firewalls help control and protect these remote connections by only allowing trusted users to access the network.**

**6- Logging and Auditing:** **Firewalls maintain logs of network traffic and security events. These logs can be used for monitoring and auditing purposes.**

**7- Intrusion Detection and Prevention (IDPS):** It is a security feature that **monitors** network traffic to **detect** and **stop attacks or suspicious activity** in real time and also **Alert admins**, so they know something suspicious is happening.

**8- Virtual Segmentation:** means **splitting a big network into smaller, separate zones or sections** using a firewall. Each section is like a “mini-network” inside the main one.

**Purpose:**

* **Better security**: Keep sensitive parts (like servers or admin systems) separate from general user traffic.
* **Limit damage**: If a hacker gets into one zone, they can’t easily move to other zones

**Design Goals for a Firewall**

A well-designed firewall should adhere to these principles:

1. **All traffic from inside to outside, and vice versa, must pass through the firewalls.**
2. **Only authorized traffic**, as defined by the local security policy and rules, **will be allowed to pass**.
3. **The firewall itself is immune to penetration**. This implies the use of a hardened system with a secured operating system (OS).

**Firewall Techniques**

Firewalls use various techniques to control traffic:

* **Service control:** Decides which Internet services (like email, web browsing, or file sharing) are allowed to enter or leave the network.
* **Direction control:** Controls whether service requests can flow **into** the network, **out of** the network, or both.
* **User control:** Controls access to a service according to which user is attempting to access it. This feature is typically applied to local users inside the firewall perimeter.
* **Behavior control:** Manages how certain services are used, such as limiting how much data can be transferred or which features of a service can be accessed.

**Firewall Limitations**

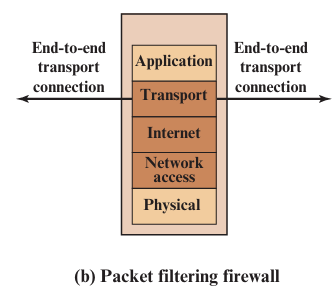
Firewalls are very useful but have some important limits:

1. **Bypass Attacks:** If attackers find a way around the firewall (like using an unprotected network path), the firewall can't stop them.
2. **Internal Threats:** Firewalls don’t fully protect against people inside the company who might cause harm, whether on purpose or by accident.
3. **Wireless Network Risks:** If the company’s wireless network isn’t secured well, outsiders might connect to it and cause problems.
4. **Infected Devices:** Devices like laptops or smartphones can get viruses or malware outside the company, and when brought back inside, they can infect the internal network.

**Types of Firewalls**

Firewalls operate at different layers of the network stack:

**1-** **Packet Filtering Firewall:** is a type of network security tool that checks each data packet and decides if it should be **allowed** or **blocked**, based on **rules**. It works on Network layer to handles IP addresses and Transport layer to handles port numbers and protocols.

It looks at:

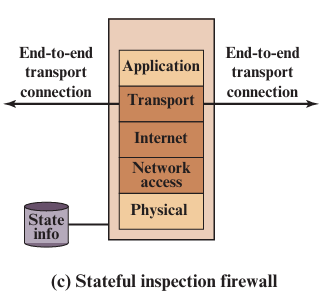
* **Source IP address** – where the packet comes from
* **Destination IP address** – where the packet is going
* **Port numbers** – what type of service is being used (like web or email)
* **Protocol** – like TCP, UDP, or ICMP

Then it: **Allows** the packet if it matches a rule or **blocks** it if it breaks   
a rule.

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| - Simple and easy to configure  - Fast and uses fewer resources  - Good for basic protection | - Only checks basic info (IP, port)  - Can’t see what's inside the packet  - Can’t detect complex attacks or viruses |

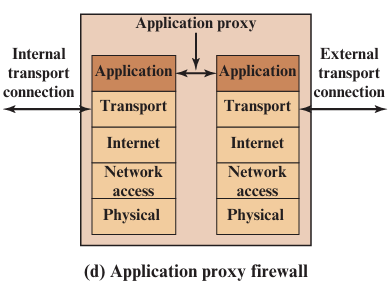
**2-** **Stateful Inspection Firewall:** is a smart type of firewall that not only looks at each packet (similar to **Packet Filtering Firewall**) but also **remembers previous packets** and the **state of the connection**. It works on Network layer to handles IP addresses, Transport layer to handles port numbers and protocols, and state awareness to keeps track of connection status

**Analogy:** It doesn’t just ask: “Is this packet allowed?”

It asks: “Does this packet make sense in the context of the whole connection?”

|  |
| --- |
| **Advantages** |
| - Smarter and more secure than basic packet filtering  - Can stop packets that are out of place or fake  - Tracks entire connections, not just individual packets |
| **Disadvantages** |
| - More complex to configure  - Uses more system resources  - Might slow down performance slightly in big networks |

**3-** **Application-Level Gateway (ALG) "Application Proxy":** A **type of firewall** that acts like a **security middleman** between users and web servers as It **inspects** and **filters** traffic at the **Application Layer.**

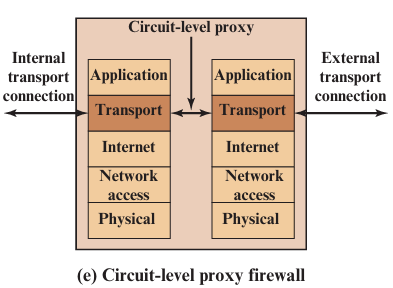
**How it Works (Simple Steps):**

1. User sends a request (e.g., to visit a website).
2. The ALG **receives the request first**.
3. It **analyzes** the content based on the application's protocol like HTTP.
4. If the content is safe, it **forwards the request** to the real destination.
5. It can **block, modify, or log** requests if they are harmful or restricted.

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| - **High security** – understands app-level threats.  - Can **analyze data deeply** (like URLs, keywords, file types).  - Can **enforce policies** (e.g., block certain sites, limit uploads). | - Slower than other firewalls because of **deep inspection**.  - More **complex to set up and manage**. |

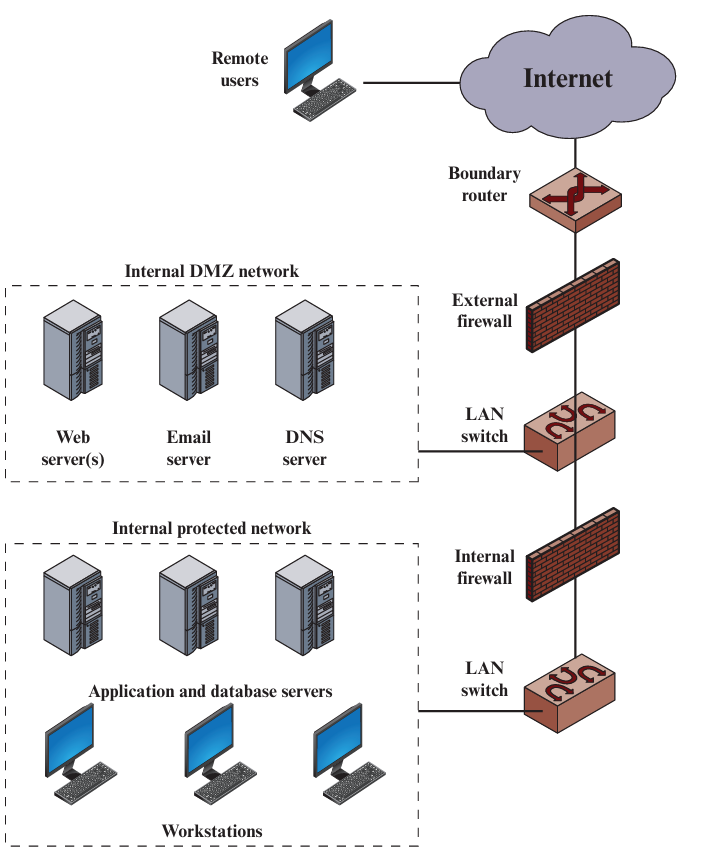
**4-** **Circuit-Level Gateway (Circuit-Level Proxy):** A **type of firewall** that works at the **Transport Layer** to control network connections. It **doesn't inspect the content** of traffic, just makes sure the connection (like a TCP handshake) is valid.

**How it Works (Simple Steps):**

1. A user inside the network wants to connect to an outside server (e.g., a website).
2. The Circuit-Level Gateway **creates two connections**:
   * One between the **user and the gateway**.
   * One between the **gateway and the external server**.
3. The gateway **forwards traffic** between both connections.
4. It **monitors the session setup only**, not the actual data.

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| - **Faster** than deep-inspection firewalls.  - **Low resource use** – doesn’t slow down the network.  - Simple setup, **ideal for trusted internal users**. | - **Doesn’t inspect data** – can’t detect malware or harmful content.  - **Not suitable** for untrusted external communications. |

**Demilitarized Zone (DMZ) Networks**

A **DMZ** (Demilitarized Zone) is a **special zone** in a network that   
sits **between the internal network (LAN)** and the **external internet   
(WAN)**. It acts as a **buffer zone** for hosting public services (like   
websites) while **protecting the internal network**.

**Purpose:**

* To **host public services** (that anyone on the internet can access),   
  **without exposing the entire internal network** to risks.
* If someone attacks a server in the DMZ, they still **can’t reach   
  the sensitive internal network** directly.

**Benefits:**

* Adds **an extra layer of protection** between public services   
  and internal systems.
* Allows **safe public access** to things like company websites   
  or email servers.
* Keeps **private resources hidden** from external threats.

**Intrusion Detection Systems (IDS)**

It is a **hardware or software solution** that **monitors**, **gathers**, and **analyzes** information from a **computer system or network** to detect and **alert** about unauthorized or suspicious attempts to access, misuse, or compromise system resources. (Monitoring, Detecting, and Alerting)

* **Intrusion:**  
  Any **violation of security policies**, whether by **external attackers** or **internal authorized users**, that threatens: **Confidentiality** (unauthorized access to data), **Integrity** (unauthorized modification of data), or **Availability** (disruption of service).
* **Intrusion Detection:**  
  The **process of monitoring and analyzing** system or network activities to **identify signs of intrusions** or policy violations.
* **Note that,** IDS is a **passive system** as it **does not block attacks**, only **detects and alerts**.

**Types of Intrusion Detection Systems (IDS)**

**1- Host-Based Intrusion Detection System (HIDS):** Monitors activities on individual devices like computers or servers as it keeps an eye on system files, logs, and applications to spot any unusual behavior or unauthorized changes.

**Example**: If someone tries to alter important system files on a web server, HIDS will detect this and alert the administrator.

**2- Network-Based Intrusion Detection System (NIDS):** Watches over the entire network's traffic to identify suspicious activities as it analyzes data packets moving across the network to detect patterns that match known threats or anomalies.

**Example**: DOS attack on the service server in the network, NIDS will recognize this and send an alert to firewall to stop these requests.

**IDS Logical Components**

An IDS typically consists of three main parts:

1. **Sensors:** Responsible for collecting data.
2. **Analyzers:** Receive input from sensors and are responsible for determining if an intrusion has occurred.
3. **User interface:** Enables a user to view output from the system or control its behavior.

**IDS Detection Techniques**

**1- Misuse Detection (Signature-Based Detection):** Compares incoming data to a database of known attack patterns (signatures). If a match is found, an alert is triggered.

**Analogy**: Like a security guard checking IDs against a list of known criminals.

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| - Quick and accurate detection of known threats (Low false positive rates). | - Cannot detect new or unknown attacks.  - Requires regular updates to the signature database. |

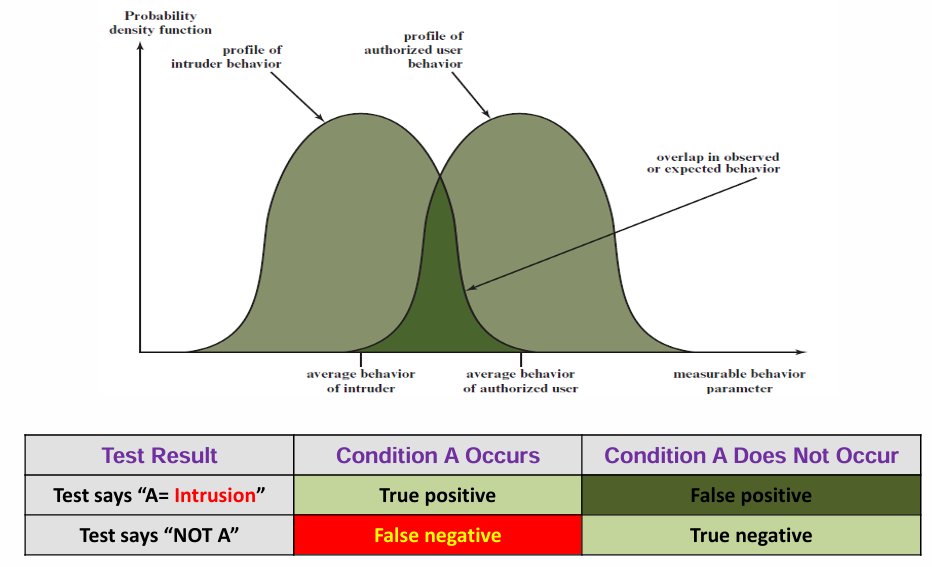
**2- Anomaly Detection:** Establishes a baseline of normal system behavior and flags deviations from this norm as potential threats.

**Analogy**: Like a bank noticing unusual spending patterns on your credit card.

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| - Can detect new or previously unknown attacks.  - Adaptable to changing network behaviors. | - Higher false positive rates due to normal behavior variations.  - Requires a learning period to establish accurate baselines. |

**Profiles of Behavior of Intruders and Authorized Users**

This is a critical concept for evaluating the effectiveness of any detection system, illustrated by the potential overlap in behaviors:



**Goal of IDS**:

- To separate these two curves as much as possible.

- Less overlap means **more accurate detection**.

* **True Positive (TP):** The IDS correctly identifies an actual intrusion. (Good!)
* **False Positive (FP):** The IDS incorrectly flags legitimate activity as an intrusion. (Bad)
* **False Negative (FN):** The IDS fails to detect an actual intrusion. (Very Bad - A real attack goes unnoticed)
* **True Negative (TN):** The IDS correctly identifies legitimate activity as not an intrusion. (Good!)

**Review Questions**

**Q1) List three design goals for a firewall?**

**Q2) List four techniques used by firewalls to control access and enforce a security policy?**

**Q3) What information is used by a typical packet filtering firewall?**

**Q4) What are some weaknesses of a packet filtering firewall?**

**Q5) What is the difference between a packet filtering firewall and a stateful inspection firewall?**

**Q6) What is an application-level gateway?**

**Q7) What is a circuit-level gateway?**

**Q8) What is a DMZ network and what types of systems would you expect to find on such networks?**

**Q9) What is the difference between an internal and an external firewall?**

**Q10) Explain the difference between host-based and network-based intrusion detection systems?**

**Q11) What are the main logical components of an IDS?**

**Q12) What are the two main approaches to intrusion detection?**