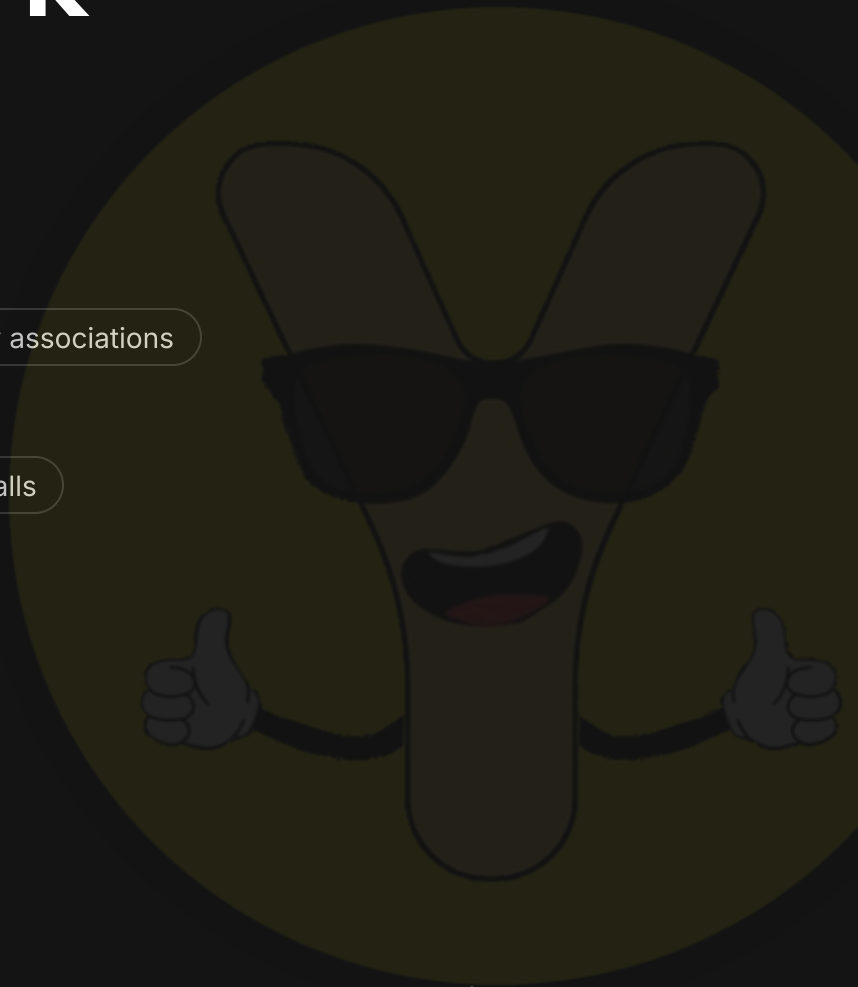
AKTU · 4TH YEAR · SEMESTER 7 · BCS072

Cryptography and Network Security

Unit 5 — Network Security, SSL, and System Security

- IP Security: Architecture
- Authentication header
- Encapsulating security payloads
- Combining security associations
- Key management
- Introduction to Secure Socket Layer
- Secure electronic transaction (SET)
- System Security: Introductory idea of Intrusion
- Intrusion detection
- Viruses and related threats
- Firewalls



DECODED BY

Chirag Jain

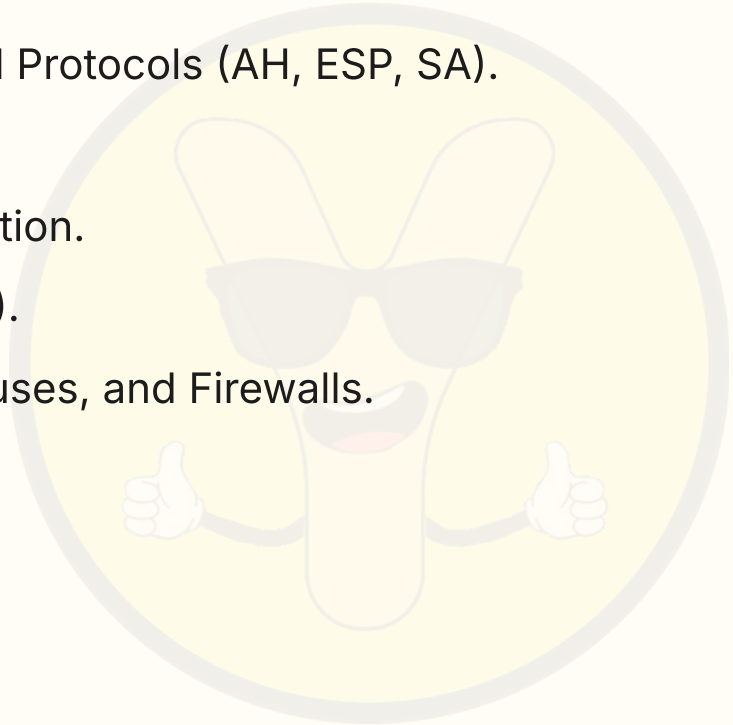
Founder, Ycotes · Gold Medalist in Artificial Intelligence, IIT Madras · taught 10,000+ students

theycotes.com

Unit 5: Network Security, SSL, and System Security

Overview of IP Security, Secure Socket Layer, SET, and System Security primitives.

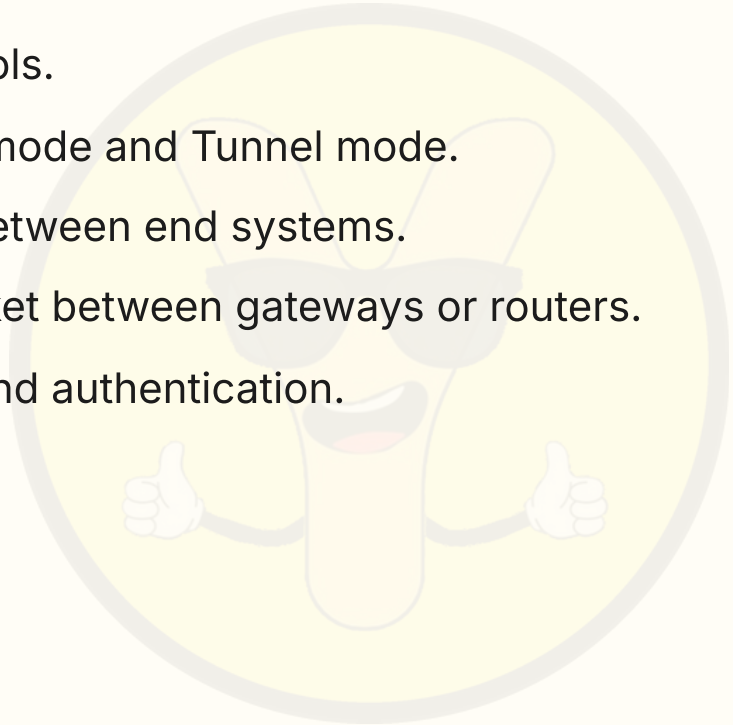
- IP Security (IPSec) Architecture and Protocols (AH, ESP, SA).
- Key Management in IPSec.
- Secure Socket Layer (SSL) Introduction.
- Secure Electronic Transaction (SET).
- System Security: Intrusion, IDS, Viruses, and Firewalls.



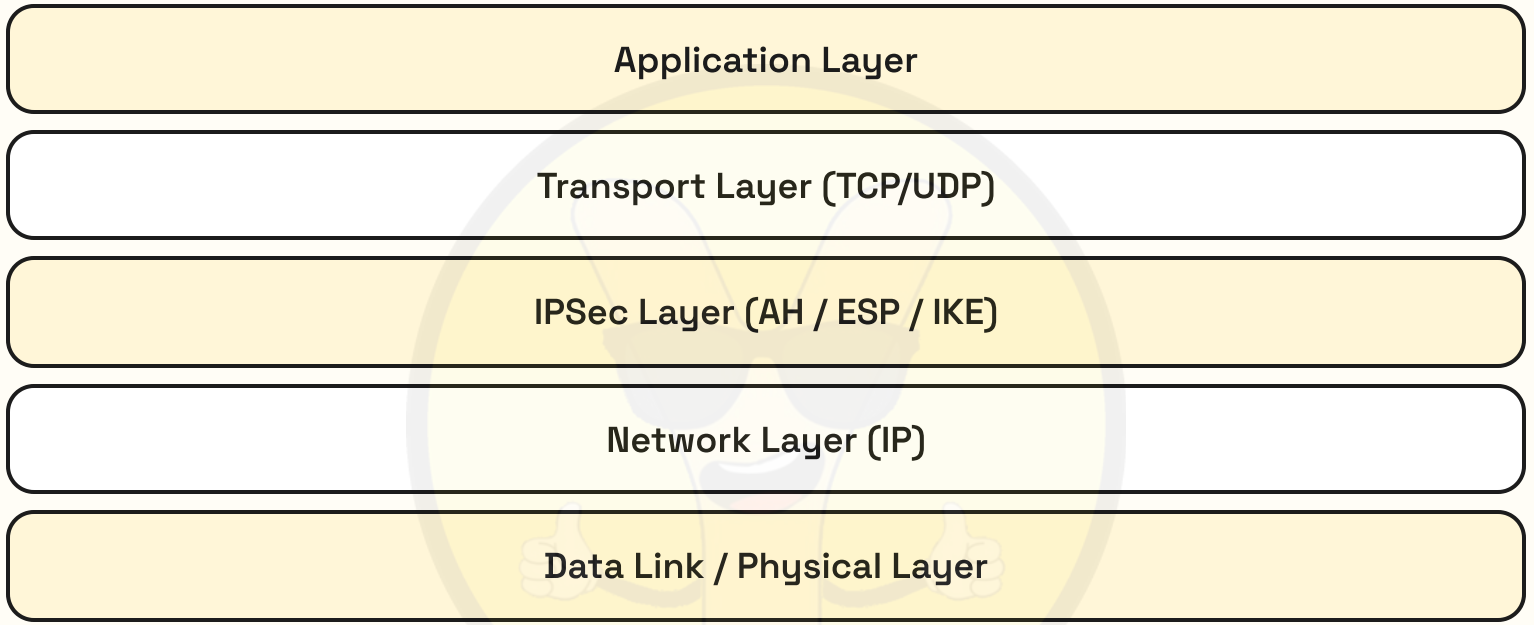
IP Security (IPSec): Introduction

IPSec provides security at the network layer (Layer 3) for all traffic.

- Protects both IPv4 and IPv6 protocols.
- Operates in two modes: Transport mode and Tunnel mode.
- Transport mode secures payload between end systems.
- Tunnel mode secures entire IP packet between gateways or routers.
- Provides confidentiality, integrity, and authentication.



IPSec Architecture



Placement of IPSec within the TCP/IP protocol stack.

IPSec Authentication Header (AH)

AUTHENTICATION HEADER

A protocol that provides connectionless integrity and data origin authentication for IP datagrams, along with protection against replay attacks.

- Does NOT provide confidentiality (encryption is not used).
- Protects the IP payload and portions of the IP header.
- Protocol number assigned to AH is 51.
- Uses a sliding window mechanism for anti-replay protection.

Encapsulating Security Payload (ESP)

ESP PROTOCOL

A comprehensive protocol that provides origin authenticity, integrity, and confidentiality of packet data.

- Protocol number assigned to ESP is 50.
- Encrypts the IP payload (in transport mode) or entire IP packet (in tunnel mode).
- Appends an ESP trailer and ESP authentication data.
- Offers stronger end-to-end security than AH by supporting encryption.

AH vs ESP Comparison

Feature	Authentication Header (AH)	Encapsulating Security Payload (ESP)
Confidentiality	No	Yes
Data Integrity	Yes	Yes
Authentication	Yes	Yes
Protocol Number	51	50
Header Protection	Protects IP header fields	Protects only payload (Transport mode)

Security Associations (SA)

SECURITY ASSOCIATION

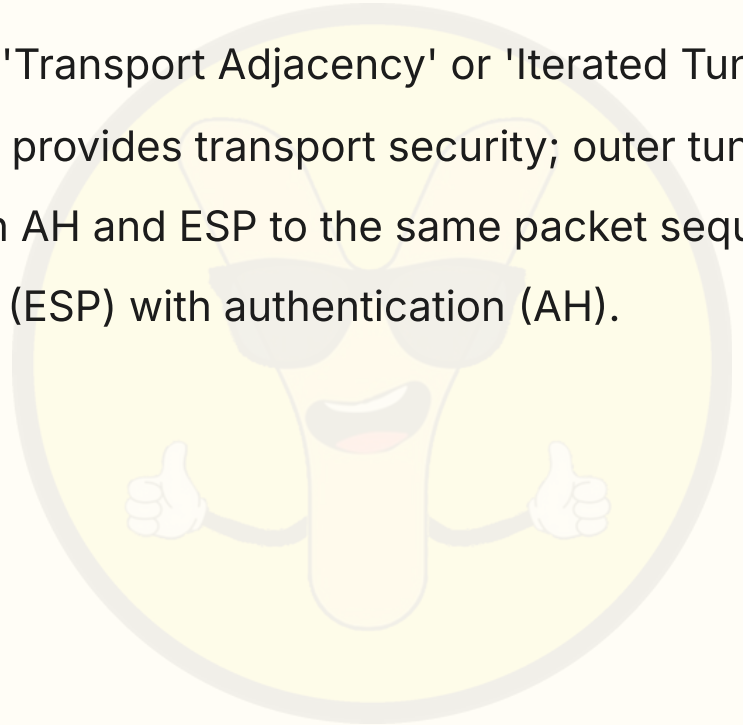
A simplex (one-way) logical connection between two communicating entities that provides security services for the traffic carried.

- Defined by a triple: Security Parameter Index (SPI), IP Destination Address, and Security Protocol identifier (AH or ESP).
- Stored in a Security Association Database (SAD).
- Two SAs are required for bi-directional communication.
- Managed manually or via automated protocols like IKE.

Combining Security Associations

SAs can be combined into bundles to achieve desired security goals.

- Sequence of SAs can be applied in 'Transport Adjacency' or 'Iterated Tunneling'.
- Tunnel Mode Bundling: Inner tunnel provides transport security; outer tunnel provides routing security.
- Transport Adjacency: Applying both AH and ESP to the same packet sequentially.
- Example: Combining confidentiality (ESP) with authentication (AH).



Key Management in IPSec

Key management handles the creation, negotiation, and maintenance of cryptographic keys.

- Internet Key Exchange (IKE) is the standard protocol used for key management in IPSec.
- IKE operates in two phases: Phase 1 (establish ISAKMP SA) and Phase 2 (negotiate IPSec SAs).
- Supports both Main Mode and Aggressive Mode in Phase 1.
- Automates key distribution and eliminates manual key configuration overhead.

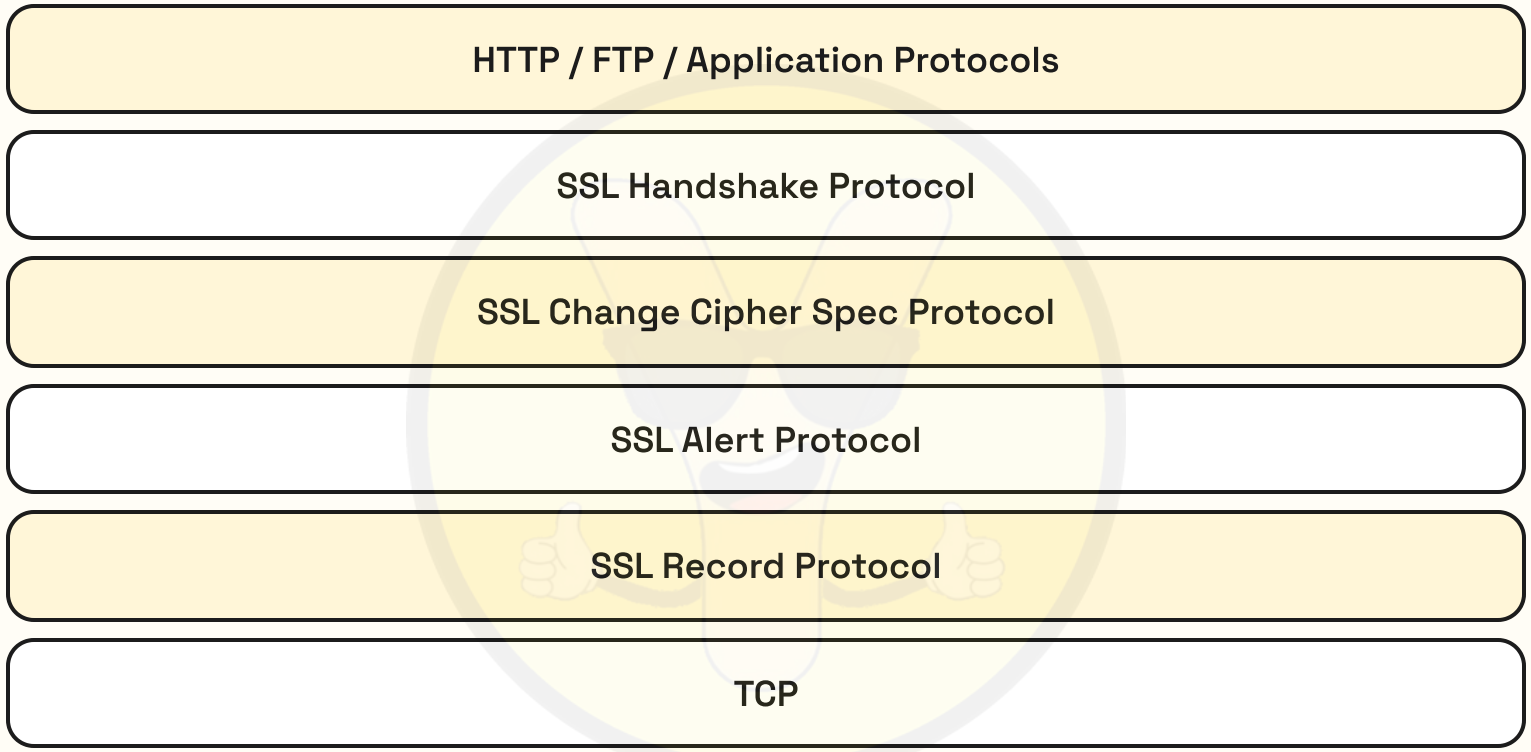
Secure Socket Layer (SSL): Introduction

SECURE SOCKET LAYER

A security protocol developed by Netscape to provide secure communications over the Internet for web browsing and other applications.

- Operates between the Transport layer (TCP) and Application layer.
- Provides confidentiality, message integrity, and server/client authentication.
- Evolved into Transport Layer Security (TLS).
- Consists of sub-protocols: Handshake Protocol, Record Protocol, Alert Protocol, and Change Cipher Spec.

SSL Protocol Stack

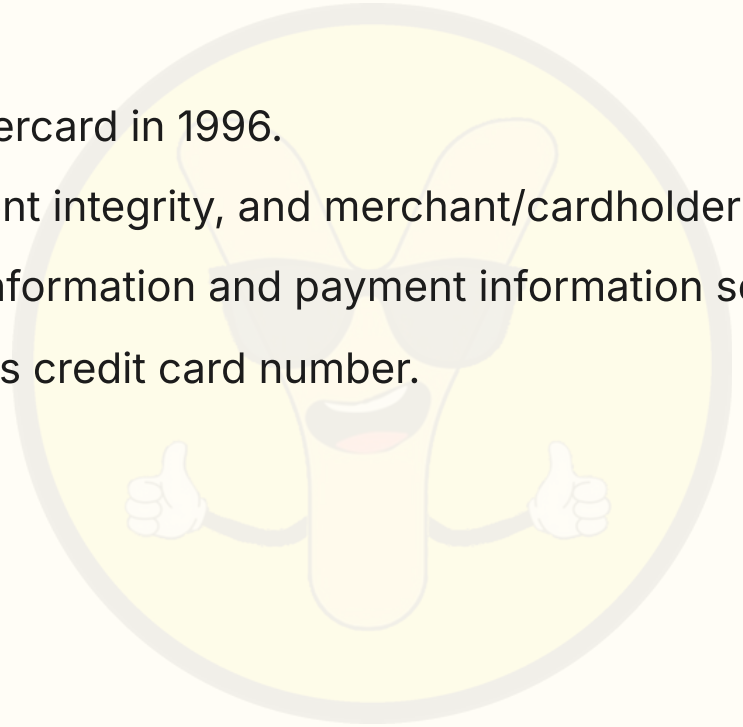


Layers of the SSL protocol architecture.

Secure Electronic Transaction (SET)

SET is an open encryption and security specification designed to protect credit card transactions over the Internet.

- Developed jointly by Visa and Mastercard in 1996.
- Ensures data confidentiality, payment integrity, and merchant/cardholder authentication.
- Uses dual signatures to link order information and payment information securely.
- Merchant never sees the customer's credit card number.



System Security: Intrusion

INTRUSION

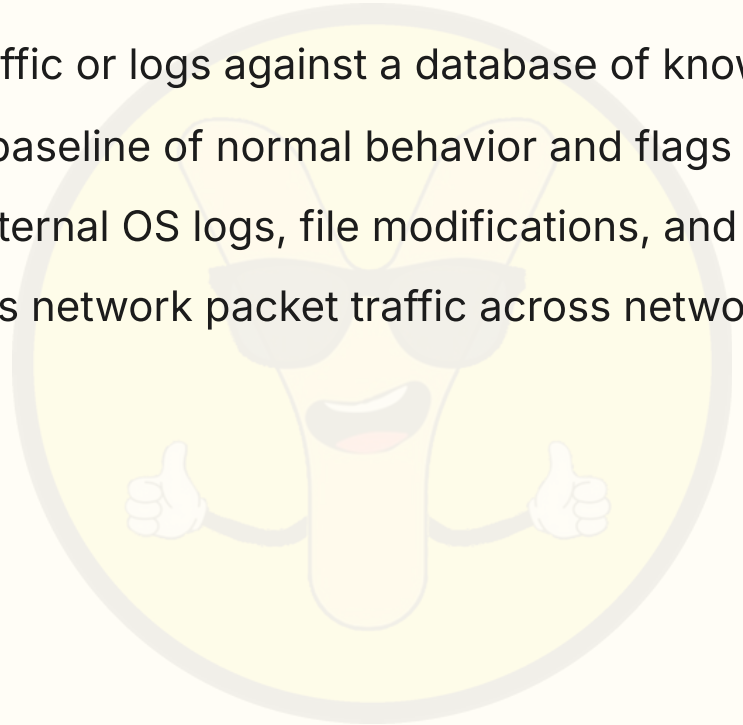
Any unauthorized set of actions that attempt to compromise the confidentiality, integrity, or availability of a computing system or network resource.

- Attackers range from casual hackers to organized crime and state-sponsored actors.
- Intruders typically proceed through phases: reconnaissance, scanning, gaining access, maintaining access, and covering tracks.
- Requires robust detection and prevention mechanisms.

Intrusion Detection Systems (IDS)

An IDS monitors system and network activities for malicious anomalies or policy violations.

- Signature-based IDS: Compares traffic or logs against a database of known attack signatures.
- Anomaly-based IDS: Establishes a baseline of normal behavior and flags significant deviations.
- Host-based IDS (HIDS): Monitors internal OS logs, file modifications, and system calls.
- Network-based IDS (NIDS): Inspects network packet traffic across network segments.



Viruses and Related Threats

COMPUTER VIRUS

A malicious program that replicates itself by modifying other computer programs and inserting its own code.

- Worms: Self-replicating programs that travel across networks without user intervention.
- Trojan Horses: Programs that appear benign while harboring hidden malicious payloads.
- Ransomware: Malware that encrypts user data until a financial ransom is paid.
- Logic Bombs and Spyware represent other forms of systemic software threats.

Firewalls: Overview

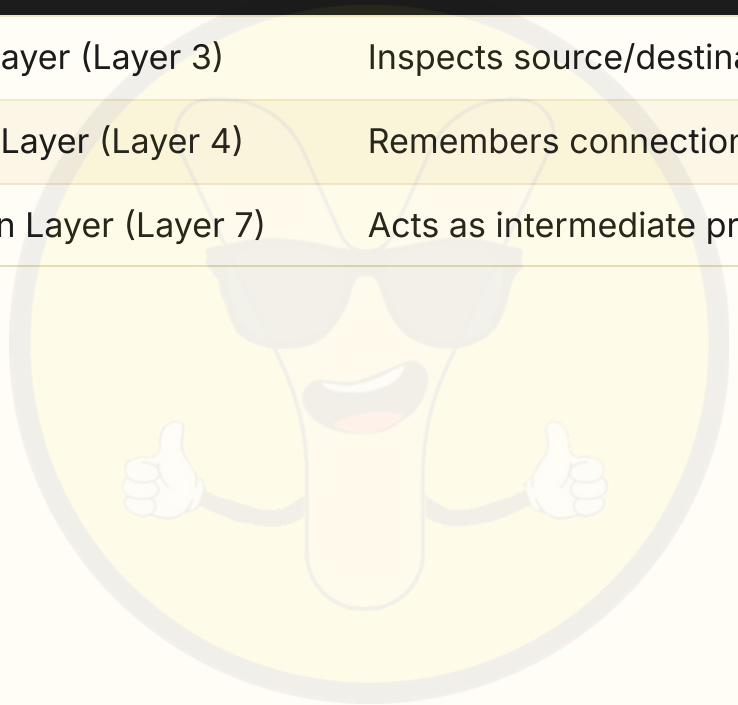
FIREWALL

A network security system designed to monitor and control incoming and outgoing network traffic based on predetermined security rules.

- Acts as a barrier between a trusted internal network and an untrusted external network (Internet).
- Can be implemented as hardware appliances or software applications.
- Inspects packets at various network layers to permit or deny traffic flow.

Types of Firewalls

Firewall Type	Inspection Level	Key Characteristic
Packet Filtering	Network Layer (Layer 3)	Inspects source/destination IP, ports, and protocols.
Stateful Inspection	Transport Layer (Layer 4)	Remembers connection state and tracks sessions.
Application Gateway (Proxy)	Application Layer (Layer 7)	Acts as intermediate proxy; deeply understands app protocols.



Exam Corner

- **Q1** Explain IPSec architecture and differentiate between Transport mode and Tunnel mode.
- **Q2** Compare and contrast the Authentication Header (AH) and Encapsulating Security Payload (ESP).
- **Q3** What is a Security Association (SA)? Explain its significance in IPSec.
- **Q4** Explain the SSL Handshake protocol and its role in establishing a secure session.
- **Q5** Discuss Secure Electronic Transaction (SET) and how dual signatures provide security.
- **Q6** What is an Intrusion Detection System (IDS)? Differentiate between signature-based and anomaly-based IDS.
- **Q7** Explain the classification of malicious software: Viruses, Worms, and Trojan Horses.
- **Q8** What is a Firewall? Compare Packet Filtering firewalls with Stateful Inspection firewalls.

Unit 5 done. You are exam-ready.

Revise the Exam corner once more, then open Unit 1 on theycotes.com. Every AKTU subject, unit by unit, free. Notes by Chirag Jain, Ycotes.

