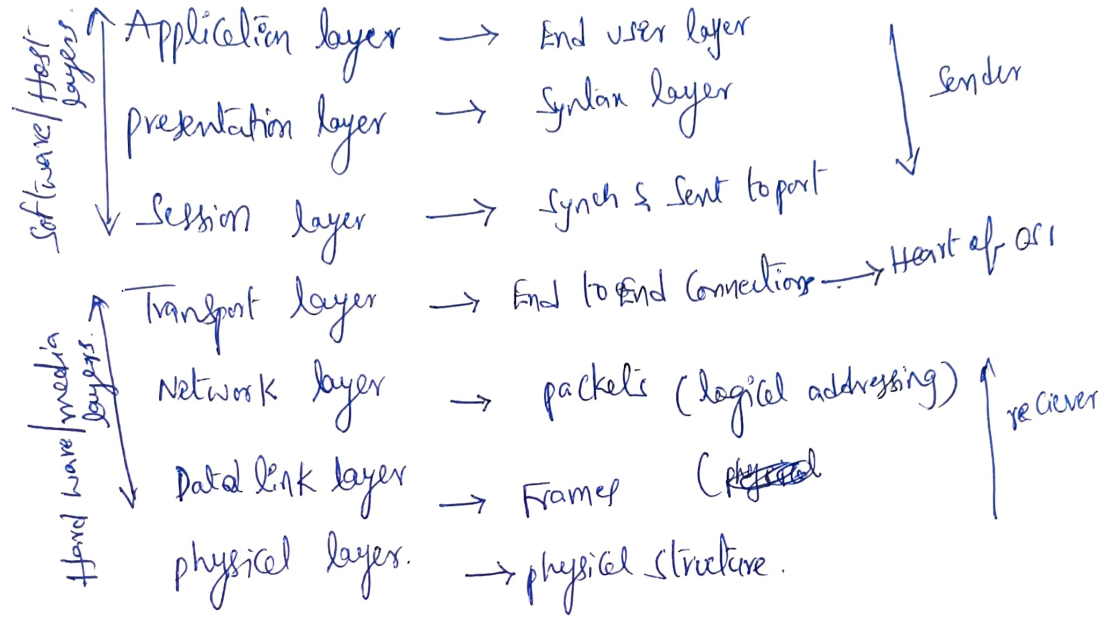
The OSI model (open systems Interconnection model) is a conceptual frame work used to describe the functions of a networking system.

→ In OSI seven layers are there



(1) Application layer :-

→ the Interaction with the user or the user application takes place at this stage ⟹ HTTP | FTP | IRC | SSH | DNS

(2) presentation layer :-

→ the data is Converted into the syntax or semantics which an application understands

→ Before passing on the data any further, the data is formatted at this stage. ⟹ SSL, SSH | IMAP | FTP | MPEG | JPEG

(3) Session layer :-

→ the Connection between the computers Connected in a network is managed at this layer.

(4) → Authentication and authorisation happen at this layer

→ API's sockets

④ Transport layer :-

→ the delivery of data packets is managed.
→ it manages the flow of data, segmentation
⇒ Tcp, UDP

③ network layer :-

→ it acts as a network Controller.
⇒ IP, ICMP, IPSEC, IGMP

⑥ Data link layer :-

→ Access to get the data is archived at this layer.
⇒ PPP, Switch, Ethernet

⑦ physical layer :-

→ it is the bottom-most of the first-layer of the osi model.
⇒ Coax, Fiber, wireless, Hubs, Repeaters.

→ Security groups.

→ A security group is a set of firewall rules that control the traffic of your Instance.

Type	protocol	port Range	Description
Custom Tcp rule	Tcp	(49152-65535) -	Connection between clients & your backend Instance
Custom Udp Rule	Udp	(49152-65535) -	you can specify any one port number
Custom ICMP Rule - IPv4	Echo ping	N/A -	protocol that devices within a network use to communicate probs, errors with data transmission
Custom ICMP Rule - IPV6	IPV6 ICMP	All -	
Custom protocol		All - >	we can add Custom protocol in the dropdown
All Tcp	Tcp	0-65535 - >	Generally a Tcp port represents an application
All Udp	Udp	0-65535 -	it is layer based protocol to configure stationnames
All ICMP - IPv4	ICMP	0-65535 -	Icmp is a protocol Integrated with ip it is for trouble shooting
All ICMP - IPv6	IPV6 ICMP	All -	
All Traffic	All	0-65535 -	it allows All traffic b/w all Instances

SSH	Tcp	22	→ To change this default
SMTP	Tcp	25	→ it is the orginal standard email.
DNS (UDP)	UDP	53	→ } DNS is Translate human readable information
DNS (TCP)	Tcp	53	→ } readable ip address.
HTTP	Tcp	80	→ it helps to send protocol for fetching resources such as HTML documents.
POP3	Tcp	110	→ Supports one-way email synchronization
IMAP	Tcp	143	→ access email/bulletin board messages from a mail services.
LDAP	Tcp	389	
HTTPS	Tcp	443	→ it is a standard Communications protocol used to read & write data
SMB	Tcp	445	(443) with a few clicks in the AWS Console
SMTPS	Tcp	465	You can request a trusted SSL/TLS.
IMAPS	Tcp	993	(445) Networking file sharing protocol.
POP3S	Tcp	995	(465) - Simple mail transfer protocol secure
MSSQL	Tcp	1433	(993) - same as IMAP, Built secure connection
NFS	Tcp	2049	of data.
MySQL/Aurora	Tcp	3306	(995) → helps in email from the senders
RDP	Tcp	3389	device to receivers mailbox
Redshift	Tcp	5439	(1433) → it Communicate protocol for the
PostgreSQL	Tcp	5432	Internet N/W layer.
Oracle-RDS	Tcp	1521	2049 → it is a distributed file system.
WinRM - HTTP	Tcp	5985	(3306) → full managed it Connect Aurora
WinRM - HTTPS	Tcp	5986	(3389) → Allows remote users to see & use
Elastic Graphics	Tcp	2007.	windows on a device in another location.

(5439) → it represents a potential Security Concern.

(5432) → the port numbers, Ip address are the database administrative port.

(1521) → changing the oracle XMLDB port explain how to change port number.

→ fed bus (Connection is Secure).

Certificate Viewer → google.com

RSA → · GlobalSign RootCA

GTS Root R1

Finger prints → SHA-256 Fingerprint

SHA-1 Finger print

→ Byjus :- (Connection is Secure).

Certificate viewer → Sni.CloudFlaressl.Com

RSA → · Cloudflare Inc ECC CA-3

finger prints :- SHA-256 finger print

SHA-1 Finger print.