Network Software Stack for a Hybrid cloud

Scenario :- A data analytics company is migrating to a hybrid cloud setup

Questions :-

a.) Describe the role of OSI and TCP/IP layers in Cloud communication

TCP/~~OSI~~ IP model in cloud communication

Application layer :- Handles communication between applications and the network, including protocol like HTTP, FTP, and SMTP

Transport layer :- Ensures reliable, end to end data delivery using protocols like TCP (Transmission control protocol) and UDP (User Datagram Protocol). TCP provides reliable, connection-oriented communication while UDP offers faster, connectionless communication

Internet Layer :- Responsible for logical addressing (IP addresses) and routing of data packets across networks

Link Layer :- Deals with the physical transmission of data over the network medium, including hardware addresses and network interface cards.

OSI Model in cloud communication :-

Application Layer :- Similar to the TCP/IP application layer, it handles the user interface and network services.

Presentation layer :- Deals with data formatting encryption and compression ensuring data is in a usable format for the application layer.

Session Layer :- Manages the communication sessions between applications, including establishing, coordinating and terminating connections.

Transport Layer :- Similar to the TCP/IP transport layer, it provides reliable data transfer

Network layer :- Handles logical addressing and routing of data packets, similar to the TCP/IP internet layer.

Data link layer :- Provides reliable data transfer between two directly connected nodes, including error detection and correction.

Physical layer:- Deals with the physical transmission of data bits over the network medium.

b.) Compare Software-based and hardware-based firewalls

Hardware Firewalls:-

Physical Devices:- A seperate piece of hardware positioned at the network's edge, typically between the router and the internet.

Network-level protection:- Protects all devices connected to the network

⇒ Stronger Security: can offer more robust protection against external threats.

Higher Cost:- Typically more expensive upfront

Less flexible:- Can be more challenging to configure and update.

Examples:- Cisco ASA, Fortinet Forticrate, Palo Alto Networks PA series.

Software Firewalls :-

Software Application : Installed on individual Computers or servers

Device-Specific Protection :- Secure only the devices on which it is installed

Resource usage :- Can Consume device resources (CPU, memory)

Lower Initial cost : Can be more affordable, especially for smaller networks

More Flexibility :- Easier to configure and update often integrated with the operating system.

Examples :- window Firewall, macOS Firewall, third party solutions.

(·) Suggest protocol level security measures :-

To enhance security at the protocol level focus on implementing robust authentication encryption and access control mechanisms.

Using strong encryption protocols (TLS/SSL, IPsec) employing secure authentication methods (MFA, Strong passwords), and regularly updating software and systems. Additionally, ensure proper access control, network segmentation, and monitor for suspicious activity.

d.) Recommend monitoring tools for each OSI layer

Physical layer: Cable Testers, optical time domain Reflectometer, BERT, NIC testers

Network layer: Routers, Firewalls, Network Analyzers

Transport layer: NetFlows Flow Analyzers, TCP/IP protocol Analyzers

Session layer: Session Recording tools, Firewalls

Presentation layer: Network Analyzers, Firewalls

Application layer: Web server, Database Monitoring Application performance monitoring log Management and Analysis tools, synthetic transaction Monitoring.