L2–L3 Network Security Interview Q&A;

1. Explain the TCP 3-way handshake.

A: SYN → SYN-ACK → ACK establishes a reliable connection.

2. How does TCP ensure reliability?

A: Using sequence numbers, ACKs, retransmissions, sliding window, and congestion control.

3. What is MSS & MTU? What happens when MTU is exceeded?

A: MTU = max frame size; MSS = max TCP payload. Exceeding MTU causes fragmentation or packet drop if DF set.

4. Difference between TCP RST and FIN.

A: FIN = graceful close; RST = abrupt termination.

5. Causes of high SYN-SENT or FIN-WAIT states.

A: Blocked handshake, unreachable server, asymmetric routing, SYN floods.

6. What is STP and why is it needed?

A: Prevents L2 loops by blocking redundant paths.

7. What is Port Security?

A: Restricts allowed MACs per port.

8. What is DHCP Snooping?

A: Prevents rogue DHCP servers by trusting only specific ports.

9. Hub vs Switch vs Router.

A: Hub = broadcast; Switch = MAC-based; Router = Layer 3 routing.

10. Routing vs Forwarding.

A: Routing builds table; forwarding uses it.

11. Static vs Dynamic Routing.

A: Static for small networks, dynamic (OSPF/BGP) for scalability.

12. What is ECMP?

A: Load Balancing across equal-cost paths.

13. What is asymmetric routing?

A: Forward & return paths differ; firewalls drop due to lost state.

14. How does a stateful firewall work?

A: Tracks connection state; allows matching packets.

15. NAT Types.

A: SNAT, DNAT, PAT.

16. Session creation flow in Palo Alto.

A: Zone lookup → policy → NAT → App-ID → threat inspection.

17. What is SecureXL in Check Point?

A: Performance acceleration engine.

18. What is FW Monitor?

A: Packet tool showing i/I/o/O inspection points.

19. UTM vs NGFW in Fortinet.

A: UTM = port-based; NGFW = app/user-based.

20. IKEv1 vs IKEv2.

A: IKEv2 is faster, secure, mobility-friendly.

21. Phase 1 vs Phase 2 in VPN.

A: Phase 1 = secure channel; Phase 2 = IPSec data tunnel.

22. Tunnel up but no traffic.

A: Proxy-ID mismatch, NAT-T, missing route, ACL, wrong selectors.

23. What is SPI?

A: ID for IPsec SA.

24. IDS vs IPS.

A: IDS detects; IPS blocks.

25. Signature vs anomaly detection.

A: Signature = known patterns; anomaly = behavioral deviations.

26. False positive vs false negative.

A: FP = normal flagged; FN = attack missed.

27. Scenario: user cannot reach server.

A: Check ping, DNS, firewall logs, NAT, routes, server.

28. Firewall CPU high.

A: High sessions, heavy rules, logging load, attacks, App-ID.

29. Policy allows but traffic drops.

A: Wrong NAT, routing issues, IPS, app mismatch, SSL issues.

30. VPN tunnel up but no traffic.

A: Proxy-ID mismatch, routing, LAN overlap, selectors, NAT.