# ◇ EASY (Q1–Q10)

**Q1.** A VPN primarily provides secure communication over:
A. Private leased lines only
B. Public networks like the Internet
C. Isolated LANs
D. Offline networks

**Q2.** VPN mainly ensures which security objectives?
A. Confidentiality only
B. Integrity only
C. Authentication only
D. Confidentiality, integrity, and authentication

**Q3.** Which VPN protocol is considered obsolete due to weak security?
A. IPSec
B. L2TP
C. PPTP
D. SSL

**Q4.** Which VPN type connects two entire networks together?
A. Remote access VPN
B. Mobile VPN
C. Site-to-site VPN
D. Personal VPN

**Q5.** Which VPN protocol commonly uses TCP port 443?
A. PPTP
B. IPSec
C. SSL/TLS VPN
D. L2TP

**Q6.** Which component is created when a VPN connection is established?
A. Virtual tunnel
B. VLAN
C. Proxy cache
D. Routing table

**Q7.** OpenVPN is based on which security technology?
A. SSH
B. TLS/SSL
C. IPSec only
D. Kerberos

**Q8.** Which VPN type is best suited for work-from-home employees?
A. Site-to-site VPN
B. Remote access VPN
C. Trusted VPN
D. MPLS VPN

**Q9.** Which VPN characteristic hides the original IP address?
A. NAT
B. Tunneling
C. Encryption
D. Hashing

**Q10.** Which VPN type maintains session continuity while moving across networks?
A. Remote VPN
B. Site-to-site VPN
C. Mobile VPN
D. Trusted VPN

---

# ◇ MEDIUM (Q11–Q25)

**Q11.** Which VPN function verifies the identity of users or devices?
A. Encryption
B. Authentication
C. Integrity
D. Tunneling

**Q12.** Which VPN protocol provides security at the network layer?
A. SSL
B. PPTP
C. IPSec
D. HTTPS

**Q13.** Why SSL VPNs are preferred for remote access?
A. They require special hardware
B. They work easily through firewalls
C. They do not use encryption
D. They operate at Layer 2

**Q14.** Which IPSec component handles key exchange?
A. AH
B. ESP
C. IKE
D. HMAC

**Q15.** Which VPN type usually uses gateway-to-gateway authentication?
A. Remote access VPN
B. Mobile VPN
C. Site-to-site VPN
D. Personal VPN

**Q16.** Which authentication method provides the highest security in VPNs?
A. Password only
B. Pre-shared key
C. Certificate-based authentication
D. MAC filtering

**Q17.** Which VPN function ensures data is not altered during transmission?
A. Encryption
B. Integrity
C. Authentication
D. Compression

**Q18.** Which VPN protocol is most firewall-friendly?
A. PPTP
B. L2TP
C. IPSec
D. SSL VPN

**Q19.** Why trusted VPNs rely less on encryption?
A. They operate over public networks
B. They use provider-controlled private networks
C. They use weak algorithms
D. They disable authentication

**Q20.** Which OpenVPN feature improves scalability and security?
A. Static IP only
B. Certificate-based authentication
C. MAC filtering
D. Clear-text keys

**Q21.** Which VPN component ensures secure data encapsulation?
A. Hashing
B. Encryption
C. Tunnel
D. Authentication server

**Q22.** Which VPN type is commonly used between branch offices?
A. Remote VPN
B. Mobile VPN

C. Site-to-site VPN
D. Personal VPN

**Q23.** Which VPN protocol combination provides encryption for L2TP?
A. SSL
B. PPTP
C. IPSec
D. GRE

**Q24.** Why VPN is critical on public Wi-Fi networks?
A. Improves speed
B. Prevents eavesdropping
C. Increases bandwidth
D. Eliminates malware

**Q25.** Which OpenVPN mode encrypts both payload and headers?
A. Transport mode
B. Tunnel mode
C. Bridge mode
D. Split mode

# △ HARD (Q26–Q40)

**Q26.** Which scenario best represents a hybrid VPN deployment?
A. Single VPN for all users
B. IPSec for site-to-site and SSL VPN for remote users
C. Only MPLS connections
D. Only PPTP VPN

**Q27.** Why site-to-site VPNs are usually configured as always-on tunnels?
A. User authentication is required
B. Continuous inter-network communication is needed
C. Encryption is weak
D. They use SSL only

**Q28.** Which VPN challenge is most significant for mobile VPN users?
A. Encryption strength
B. Session persistence across networks
C. Certificate management
D. Routing loops

**Q29.** Which IPSec protocol provides confidentiality and integrity?
A. AH

B. ESP
C. IKE
D. ISAKMP

**Q30.** Why certificate-based VPN authentication scales better than PSK?
A. Easier password management
B. Individual identity per user/device
C. No encryption required
D. Faster connections

**Q31.** Which VPN risk is highest if split tunneling is enabled?
A. Increased latency
B. Data leakage
C. Higher bandwidth usage
D. Tunnel overhead

**Q32.** Which OpenVPN security feature protects against MITM attacks?
A. Static routing
B. TLS authentication
C. NAT traversal
D. Port forwarding

**Q33.** Which VPN type best supports cloud-based remote access?
A. Trusted VPN
B. MPLS VPN
C. SSL VPN
D. Frame relay VPN

**Q34.** Why IPSec transport mode is rarely used in enterprise VPNs?
A. It encrypts entire packet
B. It exposes original IP headers
C. It is slower
D. It requires NAT

**Q35.** Which VPN protocol is most suitable for high-performance modern deployments?
A. PPTP
B. L2TP
C. WireGuard
D. GRE

**Q36.** Which VPN function directly supports access control policies?
A. Encryption
B. Authentication
C. Key exchange
D. Tunneling

**Q37.** Which threat is NOT mitigated by VPN alone?
A. Packet sniffing
B. Man-in-the-middle
C. Malware infection
D. Data interception

**Q38.** Which OpenVPN deployment model supports full network access?
A. Clientless VPN
B. Site-to-site VPN
C. Full-tunnel remote VPN
D. Split-tunnel VPN

**Q39.** Why VPN is considered a logical extension of a private network?
A. It replaces routing
B. It provides encrypted tunnels over public networks
C. It removes firewalls
D. It disables NAT

**Q40.** Which combination provides the strongest VPN security posture?
A. PPTP + password
B. SSL VPN + certificates + MFA
C. Trusted VPN only
D. Split tunnel without authentication