◇ EASY (Q1–Q10)

Q1. IPsec operates primarily at which OSI layer?
A. Data Link
B. Network
C. Transport
D. Application

Q2. Which IPsec protocol provides encryption and integrity?
A. AH
B. ESP
C. IKE
D. ISAKMP

Q3. In IPsec, a Security Association (SA) defines:
A. Routing paths
B. Encryption and authentication parameters
C. Firewall rules
D. NAT policies

Q4. Which IPsec mode encrypts the entire original IP packet?
A. Transport mode
B. Tunnel mode
C. Bridge mode
D. Split mode

Q5. Which VPN design combines different VPN technologies together?
A. Trusted VPN
B. Hybrid VPN
C. Personal VPN
D. Mobile VPN

Q6. Which VPN type routes all traffic through the VPN tunnel?
A. Split tunnel VPN
B. Hybrid VPN
C. Full tunnel VPN
D. Trusted VPN

Q7. IPv6 VPN is more important because IPv6:
A. Uses NAT by default
B. Eliminates the need for routing
C. Uses globally routable addresses
D. Blocks ICMP

Q8. Which Windows service provides VPN functionality?
A. IIS
B. Active Directory
C. RRAS
D. PowerShell

Q9. Which VPN mode encrypts only the payload of the IP packet?
A. Tunnel mode
B. Transport mode
C. Full tunnel
D. Split tunnel

Q10. Which IPsec component manages key exchange?
A. ESP
B. AH
C. IKE
D. HMAC

◇ MEDIUM (Q11–Q25)

Q11. Why tunnel mode is preferred for site-to-site VPNs?
A. Faster performance
B. Entire packet is protected
C. No authentication required
D. No encryption overhead

Q12. Which IPsec mode is suitable for host-to-host communication?
A. Tunnel mode
B. Transport mode
C. Hybrid mode
D. Full tunnel

Q13. Which encryption algorithm is currently recommended for IPsec?
A. DES
B. 3DES
C. AES
D. RC4

Q14. What is the main security risk of split tunneling?
A. Increased latency
B. Data leakage
C. Higher CPU usage
D. Routing loops

Q15. Which IPsec protocol authenticates packet headers without encryption?
A. ESP
B. IKE
C. AH
D. TLS

Q16. Which VPN configuration improves performance by reducing tunnel traffic?
A. Full tunnel
B. Transport mode
C. Split tunnel
D. Hybrid VPN

Q17. Why is IPsec considered application-transparent?
A. It runs at Layer 7
B. It works independently of applications
C. It modifies application code
D. It uses SSL only

Q18. Which IPv6 feature increases the need for strong firewalling?
A. NAT traversal
B. Stateless addressing
C. Large address space
D. Broadcast traffic

Q19. Which RRAS-supported VPN protocol is SSL-based?
A. PPTP
B. L2TP
C. SSTP
D. IKEv2

Q20. Which IPsec element defines lifetime of security parameters?
A. Policy
B. Security Association
C. ESP header
D. Hash algorithm

Q21. Which VPN model best supports cloud + on-prem connectivity?
A. Trusted VPN
B. Hybrid VPN
C. Mobile VPN
D. Personal VPN

Q22. Why AH is rarely used alone in modern VPNs?
A. High latency
B. No authentication

C. No encryption
D. Incompatible with IPv6

Q23. Which VPN deployment ensures maximum monitoring and control?
A. Split tunnel
B. Transport mode
C. Full tunnel
D. Mobile VPN

Q24. Which RRAS authentication method is most secure?
A. Password only
B. Pre-shared key
C. Certificate-based
D. MAC filtering

Q25. Which IPsec mode hides internal IP addressing?
A. Transport mode
B. Tunnel mode
C. Split tunnel
D. Full tunnel

△ HARD (Q26–Q40)

Q26. Which scenario best justifies a hybrid VPN architecture?
A. Single office environment
B. Cloud + branch offices + remote users
C. Only remote users
D. Only MPLS connectivity

Q27. Why IPsec transport mode is incompatible with NAT in many cases?
A. Encrypts entire packet
B. Alters TCP headers
C. NAT modifies IP headers used for integrity checks
D. Uses UDP only

Q28. Which IPsec protocol combination is most common in enterprise VPNs?
A. AH + IKE
B. ESP + IKE
C. AH + ESP
D. TLS + ESP

Q29. Which IPv6 VPN threat arises from misconfigured ICMPv6 rules?
A. SQL injection

B. Neighbor Discovery attacks
C. Buffer overflow
D. Brute force login

Q30. Why full-tunnel VPN is recommended for high-security environments?
A. Lower bandwidth usage
B. Reduced encryption
C. Centralized inspection of all traffic
D. Faster routing

Q31. Which IPsec feature provides replay protection?
A. Encryption algorithm
B. Sequence numbers
C. NAT traversal
D. Key lifetime

Q32. Which RRAS VPN protocol works best with roaming clients?
A. PPTP
B. L2TP
C. SSTP
D. IKEv2

Q33. Which IPsec deployment provides the strongest confidentiality?
A. Transport mode without ESP
B. Tunnel mode with ESP and AES
C. Split tunnel with AH
D. Hybrid VPN without encryption

Q34. Why IPv6 VPN configurations require careful logging and monitoring?
A. Smaller address space
B. Increased visibility and attack surface
C. Mandatory NAT
D. Reduced routing

Q35. Which VPN feature ensures protection even if the network is compromised?
A. Trusted routing
B. Encryption
C. Load balancing
D. Compression

Q36. Which IPsec mechanism negotiates cryptographic algorithms securely?
A. ESP
B. AH
C. IKE
D. HMAC

Q37. Which VPN risk remains even with full-tunnel VPN?
A. Packet sniffing
B. Endpoint compromise
C. Man-in-the-middle
D. Data interception

Q38. Which IPsec mode is rarely used in enterprise due to limited protection?
A. Tunnel mode
B. Transport mode
C. Full tunnel
D. Hybrid mode

Q39. Why certificate-based authentication is preferred in large VPN deployments?
A. Easier to remember
B. Scales securely per user/device
C. No encryption needed
D. Faster routing

Q40. Which combination provides the most secure enterprise VPN deployment?
A. Split tunnel + password
B. Transport mode + AH
C. Tunnel mode + ESP + certificates + MFA
D. Trusted VPN without encryption