⍰ EASY (10 Questions)

Q1. What is the primary purpose of a VPN?
A. Increase bandwidth
B. Encrypt data over public networks
C. Replace DNS
D. Speed up Internet access

Q2. Which Windows Server role provides VPN and routing services?
A. NPS
B. IIS
C. RRAS
D. DHCP

Q3. Which VPN protocol uses SSL/TLS over HTTPS?
A. PPTP
B. L2TP
C. SSTP
D. GRE

Q4. Which protocol is considered insecure and deprecated?
A. IKEv2
B. SSTP
C. L2TP/IPsec
D. PPTP

Q5. What does RRAS stand for?
A. Remote Routing and Access Service
B. Remote and Routing Access Service
C. Reliable Routing and Access Service
D. Remote Routing Access System

Q6. Which network profile applies when a computer is domain-joined?
A. Public
B. Private
C. Domain
D. Guest

Q7. Which feature provides always-on remote connectivity?
A. VPN
B. DirectAccess
C. NAT
D. RDP

Q8. Which Windows component filters inbound and outbound traffic?
A. DNS

B. Windows Firewall
C. DHCP
D. IPAM

Q9. Which protocol is used by DirectAccess internally?
A. IPv4 only
B. IPv6
C. IPX
D. MPLS

Q10. Which authentication method is commonly used for VPNs?
A. FTP
B. SMB
C. EAP
D. HTTP

□ MEDIUM (15 Questions)

Q11. What is the main function of Network Policy Server (NPS) in VPN setups?
A. IP assignment
B. Authentication and authorization
C. Encryption
D. Load balancing

Q12. Which VPN protocol provides fast reconnection and mobility support?
A. PPTP
B. SSTP
C. IKEv2
D. L2TP

Q13. What is split tunneling in VPN?
A. Encrypting all traffic
B. Blocking Internet access
C. Sending some traffic outside VPN
D. Using two VPN servers

Q14. Which port is used by SSTP?
A. TCP 21
B. TCP 25
C. TCP 443
D. UDP 500

Q15. Why is DirectAccess considered more complex than VPN?
A. Lower security

B. Requires IPv6 and certificates
C. Slower performance
D. Manual connection required

Q16. Which Windows feature enforces secure communication rules between hosts?
A. NAT
B. DNS
C. IPsec
D. SMB

Q17. Which VPN scenario is best for branch office connectivity?
A. Client-to-site VPN
B. Site-to-site VPN
C. Remote desktop
D. DirectAccess

Q18. Which RRAS feature allows Internet access sharing?
A. VPN
B. Routing
C. NAT
D. Firewall

Q19. Which protocol ensures secure key exchange for VPNs?
A. FTP
B. GRE
C. IKE
D. SMB

Q20. Which authentication enhancement improves VPN security significantly?
A. Static IP
B. MFA
C. Split tunneling
D. Compression

Q21. Which Windows service must be running for VPN connections?
A. DHCP Client
B. Remote Access
C. DNS Client
D. Print Spooler

Q22. What is the role of certificates in VPN authentication?
A. Increase speed
B. Provide encryption keys
C. Replace firewall
D. Assign IPs

Q23. Which VPN type requires no user interaction once configured?
A. Manual VPN
B. Dial-up
C. DirectAccess
D. PPTP

Q24. Which firewall profile is most restrictive?
A. Domain
B. Private
C. Public
D. Custom

Q25. Which VPN deployment is recommended for modern enterprises?
A. PPTP-based VPN
B. Always On VPN
C. Dial-up VPN
D. L2TP without IPsec

HARD (15 Questions)

Q26. Why is IKEv2 preferred over PPTP in enterprise VPNs?
A. Simpler setup
B. Stronger encryption and security
C. Lower CPU usage
D. No certificate requirement

Q27. Which failure commonly causes VPN authentication to fail?
A. Incorrect DNS suffix
B. NPS policy mismatch
C. Low disk space
D. Printer offline

Q28. What is the main security risk of split tunneling?
A. Slower VPN
B. Increased CPU usage
C. Traffic leakage outside VPN
D. Authentication failure

Q29. Which DirectAccess limitation led to its deprecation?
A. No encryption
B. High cost
C. Complex IPv6 dependency
D. Poor performance

Q30. Which protocol secures traffic at the network layer?
A. TLS
B. SSL
C. IPsec
D. SSH

Q31. Why should VPN servers be placed in a perimeter network (DMZ)?
A. Easier management
B. Faster routing
C. Reduced attack surface to internal LAN
D. Better DNS resolution

Q32. Which log is most useful for diagnosing VPN failures?
A. Application log
B. System log
C. Security log
D. NPS log

Q33. What happens if MTU size is incorrect in VPN tunnels?
A. Faster throughput
B. Packet fragmentation or drops
C. DNS errors
D. Authentication issues only

Q34. Which VPN authentication method provides the highest security?
A. Username/password
B. MS-CHAPv2
C. Certificate-based authentication
D. PAP

Q35. Which Windows feature replaces DirectAccess in modern deployments?
A. RRAS
B. SSTP
C. Always On VPN
D. NLB

Q36. Why is IPsec often combined with L2TP?
A. Improve speed
B. Provide encryption and integrity
C. Reduce cost
D. Simplify configuration

Q37. Which misconfiguration can expose internal resources via VPN?
A. Strong encryption
B. Excessive routing permissions

C. MFA enabled
D. Certificate authentication

Q38. Which enterprise VPN best practice improves security posture?
A. Disable logging
B. Use shared credentials
C. Implement MFA and logging
D. Allow split tunneling always

Q39. What is the impact of expired certificates on VPN services?
A. Slower speed
B. Authentication failure
C. IP conflict
D. Routing loop

Q40. Which troubleshooting step should be performed first for VPN issues?
A. Reinstall OS
B. Check logs and policies
C. Format disks
D. Disable firewall permanently