◇ EASY (Q1–Q10)

Q1. A packet filtering firewall mainly examines which part of a packet?
A. Application payload
B. Packet headers
C. Encrypted content
D. User credentials

Q2. Which OSI layer is primarily used by packet filtering firewalls?
A. Physical
B. Data Link
C. Network
D. Application

Q3. Stateful inspection firewalls maintain information about:
A. Routing tables
B. User accounts
C. Active connections
D. Encryption keys

Q4. Which firewall type is also known as a dynamic packet filter?
A. Packet filtering firewall
B. Stateful inspection firewall
C. Proxy firewall
D. NGFW

Q5. A screened host firewall uses which special system to protect the internal network?
A. IDS server
B. Bastion host
C. Proxy cache
D. Load balancer

Q6. Which firewall feature allows inspection of application-level traffic?
A. NAT
B. ACL
C. Application awareness
D. IP routing

Q7. iptables is native to which operating system?
A. Windows
B. macOS
C. Linux
D. FreeBSD

Q8. Which chain in iptables processes incoming packets destined for the local system?
A. OUTPUT
B. FORWARD
C. INPUT
D. PREROUTING

Q9. NGFWs primarily extend traditional firewalls by adding:
A. Routing protocols
B. Application-level controls
C. Physical security
D. Backup services

Q10. Which firewall type is fastest but offers limited inspection?
A. Proxy firewall
B. NGFW
C. Packet filtering firewall
D. Stateful firewall

◇ MEDIUM (Q11–Q25)

Q11. Why are packet filtering firewalls vulnerable to spoofing attacks?
A. They encrypt traffic
B. They do not track connection state
C. They block ICMP traffic
D. They operate at Layer 7

Q12. In a screened host firewall, which component performs packet filtering?
A. Bastion host
B. Application server
C. Screening router
D. IDS sensor

Q13. What information does a state table contain in a stateful firewall?
A. Routing paths
B. User credentials
C. Session state and flags
D. Encryption algorithms

Q14. Which firewall type can block traffic based on application signatures?
A. Packet filter
B. Screened host firewall
C. NGFW
D. Router ACL

Q15. Which iptables table is responsible for packet filtering?
A. nat
B. mangle
C. filter
D. raw

Q16. Which iptables chain is used for packets being routed through the system?
A. INPUT
B. OUTPUT
C. FORWARD
D. POSTROUTING

Q17. Which NGFW feature helps detect unknown or zero-day attacks?
A. Static ACLs
B. Deep packet inspection with signatures
C. IP routing
D. NAT translation

Q18. Why are screened host firewalls more secure than simple packet filters?
A. They encrypt traffic
B. They add an application-level security layer
C. They eliminate routing
D. They block all inbound traffic

Q19. In iptables, rules are processed in which order?
A. Random
B. Last to first
C. First match wins
D. Priority based

Q20. Which firewall best supports user-based access control?
A. Packet filtering firewall
B. Stateful firewall
C. NGFW
D. Router ACL

Q21. Which iptables policy drops all traffic not explicitly allowed?
A. ACCEPT
B. DROP
C. REJECT
D. LOG

Q22. Which firewall is best suited for high-speed networks with minimal latency?
A. NGFW
B. Proxy firewall

C. Packet filtering firewall
D. Application firewall

Q23. Why is deep packet inspection resource intensive?
A. Uses encryption
B. Inspects payload content
C. Requires routing updates
D. Uses NAT

Q24. Which iptables chain handles packets generated by the local host?
A. INPUT
B. FORWARD
C. OUTPUT
D. PREROUTING

Q25. Which NGFW capability allows visibility into social media applications?
A. Port-based filtering
B. Application identification
C. MAC filtering
D. VLAN tagging

△ HARD (Q26–Q40)

Q26. Which attack can bypass a stateless packet filter but is blocked by a stateful firewall?
A. Port scan
B. IP spoofing
C. TCP session hijacking
D. Brute force attack

Q27. Why screened host firewalls are less secure than DMZ-based architectures?
A. No encryption
B. Single point of failure at bastion host
C. Lack of routing
D. No packet filtering

Q28. Which NGFW feature enforces security policies based on user identity?
A. NAT
B. User-ID integration
C. Static routing
D. VLAN tagging

Q29. Which iptables feature allows connection tracking?
A. filter table

B. conntrack module
C. nat table
D. LOG target

Q30. Why NGFWs are more effective against application-layer attacks?
A. Higher bandwidth
B. Application-aware inspection
C. Stateless filtering
D. MAC filtering

Q31. Which iptables table modifies packet headers such as TTL or TOS?
A. filter
B. nat
C. mangle
D. raw

Q32. In firewall evolution, which firewall came immediately after packet filtering?
A. NGFW
B. Proxy firewall
C. Stateful inspection firewall
D. WAF

Q33. Why default-deny is a recommended firewall strategy?
A. Allows all trusted traffic
B. Blocks traffic unless explicitly permitted
C. Reduces firewall rules
D. Improves routing

Q34. Which firewall type provides the best balance between performance and security?
A. Packet filtering firewall
B. Stateful inspection firewall
C. Proxy firewall
D. NGFW

Q35. Which iptables target silently discards packets without notification?
A. ACCEPT
B. REJECT
C. DROP
D. LOG

Q36. Which NGFW capability integrates IDS/IPS functionality?
A. NAT
B. Deep packet inspection
C. Routing protocol support
D. VLAN trunking

Q37. Why packet filtering alone is insufficient for modern threats?
A. Low speed
B. Cannot inspect payload or user context
C. High memory usage
D. Requires encryption

Q38. Which scenario best demonstrates stateful inspection?
A. Blocking all traffic on port 80
B. Allowing return traffic of an established connection
C. Filtering based on MAC address
D. Blocking encrypted traffic

Q39. Which iptables chain is evaluated last for outgoing packets?
A. PREROUTING
B. INPUT
C. FORWARD
D. OUTPUT

Q40. Which firewall architecture supports application control, IPS, and user awareness in a single device?
A. Packet filtering firewall
B. Screened host firewall
C. Stateful firewall
D. Next-Generation Firewall