# ◇ EASY (Q1–Q10)

**Q1.** Risk management primarily focuses on:
A. Eliminating all threats
B. Identifying and reducing risks to acceptable levels
C. Installing security tools only
D. Increasing system performance

**Q2.** Which of the following best defines exposure?
A. Likelihood of attack
B. Weakness in a system
C. Potential loss when a risk is realized
D. Type of attacker

**Q3.** Which firewall component decides whether traffic is allowed or denied?
A. Router
B. Firewall rule set
C. IDS
D. Proxy server

**Q4.** A firewall primarily operates at which OSI layers?
A. Physical and Data Link
B. Network and Transport
C. Session and Presentation
D. Application only

**Q5.** Which firewall type inspects only packet headers?
A. Proxy firewall
B. Stateful firewall
C. Packet filtering firewall
D. NGFW

**Q6.** A DMZ is mainly used to:
A. Store backups
B. Isolate internal network from public services
C. Encrypt traffic
D. Perform authentication

**Q7.** Which of the following is an example of a preventive control?
A. Log analysis
B. Firewall
C. Incident report
D. Audit trail

**Q8.** pfSense is best described as:
A. Hardware router only
B. Proprietary firewall
C. Open-source firewall appliance
D. IDS tool

**Q9.** Which firewall hides internal IP addresses from clients?
A. Packet filter
B. Proxy firewall
C. IDS
D. Router

**Q10.** Which risk treatment strategy involves accepting potential loss?
A. Avoidance
B. Mitigation
C. Transfer
D. Acceptance

---

# ◇ MEDIUM (Q11–Q25)

**Q11.** Which formula correctly represents risk?
A. Risk = Asset − Threat
B. Risk = Threat × Vulnerability × Impact
C. Risk = Vulnerability + Control
D. Risk = Asset × Control

**Q12.** In qualitative risk assessment, risk is usually expressed as:
A. Numerical value
B. Currency value
C. Low / Medium / High
D. Percentage

**Q13.** Which countermeasure detects security incidents after they occur?
A. Preventive
B. Detective
C. Corrective
D. Deterrent

**Q14.** In a screened host firewall, which system is exposed to the internet?
A. Internal LAN
B. Bastion host
C. Database server
D. Backup server

**Q15.** Which DMZ architecture provides the highest security?
A. Single firewall DMZ
B. No firewall
C. Dual firewall DMZ
D. Flat network

**Q16.** Which traffic flow should be most restricted in a DMZ setup?
A. Internet → DMZ
B. Internal → DMZ
C. DMZ → Internal
D. Internal → Internet

**Q17.** Which firewall technique inspects application-layer data?
A. Packet filtering
B. Stateful inspection
C. Proxy firewall
D. Router ACL

**Q18.** iptables primarily operates as which firewall type?
A. Proxy firewall
B. Packet filtering firewall
C. Application firewall
D. Hardware firewall

**Q19.** Which Squid feature improves performance by storing web content?
A. Authentication
B. Caching
C. NAT
D. Encryption

**Q20.** Why is a bastion host hardened?
A. To increase bandwidth
B. To reduce attack surface
C. To improve routing
D. To store logs

**Q21.** Which risk treatment strategy uses cyber insurance?
A. Risk avoidance
B. Risk mitigation
C. Risk transfer
D. Risk acceptance

**Q22.** Which firewall rule evaluation method is used by iptables?
A. Random order
B. Bottom-up

C. Top-down, first match
D. AI-based

**Q23.** In firewall terminology, “default deny” means:
A. Allow all traffic
B. Block traffic unless explicitly allowed
C. Allow internal traffic only
D. Block encrypted traffic

**Q24.** Which Squid deployment type inspects client requests before reaching servers?
A. Transparent proxy
B. Reverse proxy
C. Forward proxy
D. Bridge proxy

**Q25.** Why are proxy firewalls slower than packet filters?
A. Use encryption
B. Perform deep packet inspection
C. Require NAT
D. Use TCP only

---

# △ HARD (Q26–Q40)

**Q26.** Which scenario best illustrates risk mitigation?
A. Shutting down an online service
B. Installing a firewall to reduce attack likelihood
C. Buying cyber insurance
D. Ignoring low-impact threats

**Q27.** Why packet filtering firewalls are vulnerable to IP spoofing?
A. They encrypt traffic
B. They do not verify packet state
C. They block all ICMP traffic
D. They operate at Layer 7

**Q28.** In a screened host architecture, if the bastion host is compromised, what is the main risk?
A. Internet outage
B. Direct access to internal network
C. Loss of routing table
D. DNS failure

**Q29.** Which firewall architecture combines packet filtering and application security?
A. Packet filtering firewall

B. Screened host firewall
C. Router ACL
D. Stateless firewall

**Q30.** Why DMZ reduces blast radius of an attack?
A. Encrypts all data
B. Limits lateral movement
C. Uses IDS
D. Improves routing

**Q31.** Which firewall feature is essential for tracking active connections?
A. NAT
B. State table
C. ACL
D. Proxy cache

**Q32.** In pfSense, firewall rules are applied primarily on which interface direction?
A. Outbound only
B. Inbound on interfaces
C. Forwarded only
D. Loopback only

**Q33.** Which attack is most effectively mitigated by proxy firewalls?
A. IP spoofing
B. Application-layer attacks
C. SYN flood
D. ARP poisoning

**Q34.** Why risk can never be reduced to zero?
A. Firewalls are imperfect
B. Security tools are expensive
C. Threats and vulnerabilities constantly evolve
D. Networks are complex

**Q35.** Which DMZ misconfiguration creates the highest risk?
A. Limited internet access
B. Strong firewall rules
C. Direct DMZ-to-internal access
D. Logging enabled

**Q36.** Which control compensates for the absence of a primary control?
A. Preventive
B. Compensating
C. Detective
D. Corrective

**Q37.** Why proxy firewalls improve anonymity?
A. Encrypt packets
B. Replace client IP with proxy IP
C. Drop packets
D. Perform NAT only

**Q38.** Which firewall type is most suitable for high-speed backbone networks?
A. Proxy firewall
B. Packet filtering firewall
C. Application firewall
D. WAF

**Q39.** Which scenario indicates poor risk management?
A. Regular vulnerability scanning
B. Ignoring known critical vulnerabilities
C. Applying firewall rules
D. Using DMZ

**Q40.** Why layered firewalls are preferred in enterprises?
A. Reduce hardware cost
B. Provide defense in depth
C. Simplify configuration
D. Eliminate IDS need