Each question includes four answer choices, and I've assigned **risk scores* from 1 (low risk) to 5 (high risk), depending on the potential severity of the risk.

1. Firewall Placement and Configuration

1. *Are firewalls clearly visible at all network entry and exit points?*

- a) Yes, all points are protected by firewalls. → *Risk Score: 1*
- b) Some points have firewalls, but not all. → *Risk Score: 3*
- *c) No, several entry/exit points are missing firewalls. → Risk Score: 5*
- d) Firewalls are not required at the entry/exit points. → *Risk Score: 4*

2. *Is there any evidence of firewall misconfigurations or open ports that shouldn't be open?*

- a) No, the firewalls are well-configured with appropriate port restrictions. → *Risk Score: 1*
- b) Some ports seem questionable but overall the configuration is secure. → *Risk Score: 3*
- *c) Yes, there are multiple open ports that could be exploited. → Risk Score: 5*
- d) The network is too complex to determine firewall configurations. → *Risk Score: 4*

3. *Is there a firewall placed between critical servers and the rest of the internal network?*

- *a) Yes, a firewall is isolating critical servers from other traffic. → Risk Score: 1*
- b) Some critical servers are protected, but not all. → *Risk Score: 3*
- c) No, critical servers are on the same network segment as other internal devices. → *Risk Score: 5*
- d) Firewalls are not needed for critical servers. → *Risk Score: 4*

---

2. Network Segmentation and Isolation

4. *Are the network segments visually separated into security zones (e.g., DMZ, internal, external, restricted areas)?*

- *a) Yes, the network is clearly divided into security zones. → Risk Score: 1*
- b) Some zones are separated, but not all. → *Risk Score: 3*

- c) No, segmentation is minimal or unclear. → *Risk Score: 5*

- d) The network does not use zones. → *Risk Score: 4*

5. *Are sensitive resources, such as databases, isolated in a separate network segment?*

- *a) Yes, sensitive resources are in their own secure segment. → Risk Score: 1*

- b) Some sensitive resources are separated, but not all. → *Risk Score: 3*

- c) No, sensitive resources are on the same network as other general systems. → *Risk Score: 5*

- d) Sensitive resources are not present in the network. → *Risk Score: 2*

6. *Is there any visible evidence of network traffic flowing between high-risk and low-risk zones without proper filtering or controls?*

- a) No, traffic between zones is strictly controlled. → *Risk Score: 1*

- *b) Some traffic flows between zones without appropriate filtering. → Risk Score: 3*

- c) Yes, there is unrestricted traffic flow between high-risk and low-risk zones. → *Risk Score: 5*

- d) The network has no distinct high-risk or low-risk zones. → *Risk Score: 4*

---

3. Device Placement and Exposure

7. *Are public-facing devices (e.g., web servers, DNS servers) located in a DMZ or other secure area?*

- *a) Yes, all public-facing devices are in the DMZ. → Risk Score: 1*

- b) Some public-facing devices are in the DMZ, but others are exposed. → *Risk Score: 3*

- c) No, public-facing devices are mixed with internal resources. → *Risk Score: 5*

- d) Public-facing devices are not present. → *Risk Score: 2*

8. *Are key infrastructure devices (e.g., routers, switches) placed in secure, monitored areas?*

- *a) Yes, all key infrastructure devices are securely placed. → Risk Score: 1*

- b) Some infrastructure devices are secure, but others are exposed. → *Risk Score: 3*

- *c) No, several key devices are exposed to internal or external threats. → Risk Score: 5*

- d) Key infrastructure is not adequately defined. → *Risk Score: 4*

9. *Do any critical systems (e.g., databases, application servers) have direct exposure to the internet?*
   - a) No, all critical systems are isolated from the internet. → *Risk Score: 1*
   - *b) Some critical systems are indirectly exposed. → Risk Score: 3*
   - c) Yes, critical systems are directly exposed to the internet. → *Risk Score: 5*
   - d) No critical systems are present in the network. → *Risk Score: 2*

---

4. Security Controls and Access Management

10. *Is there evidence of access control mechanisms (e.g., ACLs, VLANs) between different network segments?*
   - *a) Yes, access control mechanisms are in place and clearly visible. → Risk Score: 1*
   - b) Some access controls exist, but they are not consistently applied. → *Risk Score: 3*
   - c) No, access control mechanisms are not visible between segments. → *Risk Score: 5*
   - d) Access controls are not required in this network. → *Risk Score: 4*

11. *Are there any signs of weak authentication mechanisms (e.g., unencrypted passwords, missing two-factor authentication)?*
   - *a) No, strong authentication mechanisms are in place throughout the network. → Risk Score: 1*
   - b) Some areas have strong authentication, but not all. → *Risk Score: 3*
   - c) Yes, weak authentication mechanisms are used in several areas. → *Risk Score: 5*
   - d) Authentication mechanisms are not needed for this network. → *Risk Score: 4*

12. *Do external connections (e.g., third-party vendor access) use secure tunnels (e.g., VPN, SSL)?*
   - *a) Yes, all external connections use secure tunnels. → Risk Score: 1*
   - b) Some external connections are secured, but others are not. → *Risk Score: 3*
   - c) No, external connections are not protected by secure tunnels. → *Risk Score: 5*

- d) External connections are not present in this network. → *Risk Score: 2*

---

5. Traffic Flow and Protocol Security

13. *Are protocols such as Telnet, FTP, or HTTP (non-encrypted) visible in use?*
    - *a) No, only encrypted protocols (e.g., SSH, HTTPS) are used. → Risk Score: 1*
    - b) Some legacy protocols are still in use, but they are limited. → *Risk Score: 3*
    - *c) Yes, many insecure protocols are used. → Risk Score: 5*
    - d) Protocol usage is not clearly visible in the diagram. → *Risk Score: 4*

14. *Are network traffic monitoring tools (e.g., IDS/IPS, SIEM) visible in the diagram?*
    - *a) Yes, network monitoring tools are visible and well-deployed. → Risk Score: 1*
    - b) Some network traffic is monitored, but not all. → *Risk Score: 3*
    - c) No, network monitoring tools are absent. → *Risk Score: 5*
    - d) Monitoring tools are not required for this network. → *Risk Score: 4*

15. *Is there evidence of proper encryption for traffic flowing across public networks?*
    - *a) Yes, all public traffic is encrypted using SSL/TLS or IPsec. → Risk Score: 1*
    - b) Some public traffic is encrypted, but not all. → *Risk Score: 3*
    - *c) No, public traffic is not properly encrypted. → Risk Score: 5*
    - d) Public traffic encryption is not necessary in this case. → *Risk Score: 4*
