Group A [3 + 2 + 2 + 3 marks]

1. Explain the write access rule in Biba model. Also state the advantage of enforcing this rule.
2. Between IPSec and TLS, which one is easier to deploy? Why?
3. When would you opt for host-based IDS over network-based?
4. Clarify the difference between stateful and stateless packet filtering. Which one is better?

[3 + 2 + 3 + 2 marks] **Group B**

1. Discuss a practical business scenario where Chinese wall model is applicable. Note: do not explain the rules of this model, just the use case.
2. List the actions performed during data processing by SSL record protocol. Ordering is important.
3. What are pros and cons of anomaly based intrusion detection?
4. Briefly discus the statement: Circuit level proxy provides some degree of anonymity.

Group A

Q1

Can only write to same level as subject's clearance, or to a lower level. No write access is allowed for higher levels, since it will contaminate high integrity information with low integrity one.

Q2

TLS is easier to deploy since security is implemented by application. OS that provides TCP/IP stack does not need to change. IPsec requires an update to OS, which is time taking and not always feasible (e.g. on old and unsupported hardware).

Q3

When it is desirable to monitor a critical machine (e.g. a server) rather than whole subnet. Host based can work better in cases when network traffic is encrypted, it can detect both internal and external intrusions, and has access to more detailed system logs, which are not visible to NIDS.

Q4

Stateless filtering inspects each packet individually without context.

Stateful takes into account the state of TCP connections b/w hosts. New connection packets are subject to a detailed inspection. Packets belonging to existing connections are quickly allowed through.

Stateful firewalls are better because they monitor the entire connection state, ensuring packets belong to legitimate, established sessions. This helps block malicious packets (e.g., spoofed or out-of-sequence packets)

Group B

Q1

CW is applicable in scenarios where a business has several clients, some of whom might be competitor to each other. Example businesses are law firms, accountancy firms, consultancy firms. If a law form employee, say Abdullah is working with one client X, he should not work with other clients that are X's competitors, otherwise there will be a conflict of interest. CW model seeks to avoid such conflicts of interest.

Q2

In order:

Fragmentation, compression, mac calculation, padding, encryption, adding header

Q3

Pros: recognize new/novel attacks for which signatures haven't been collected

Cons: high rate of false positives.

Q4

With circuit level proxy, all the external users will only know the external IP address(es) of the proxy, since it will be the source IP of all outgoing traffic, and destination IP of all incoming traffic. Hence a company's internal devices will get some level of anonymity, their IP addresses will be unknown to outside world.