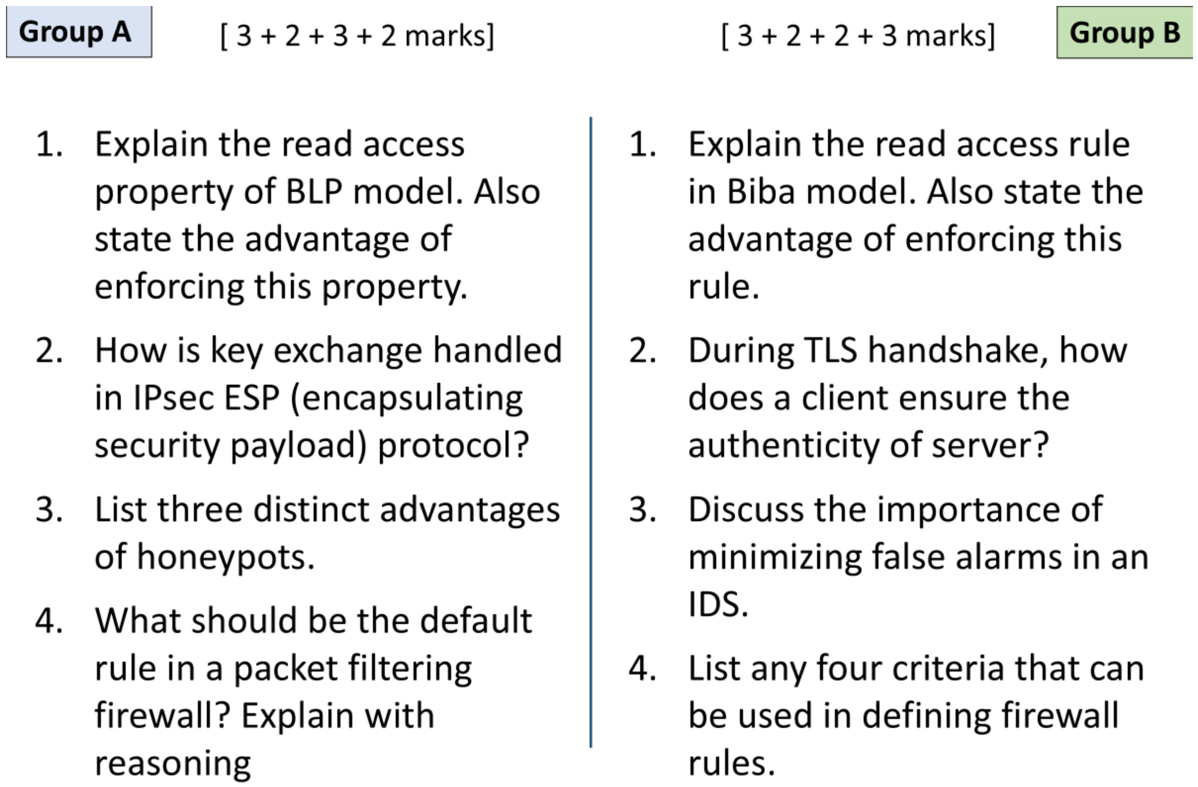

Group A [3 + 2 + 3 + 2 marks]

1. Explain the read access property of BLP model. Also state the advantage of enforcing this property.
2. How is key exchange handled in IPsec ESP (encapsulating security payload) protocol?
3. List three distinct advantages of honeypots.
4. What should be the default rule in a packet filtering firewall? Explain with reasoning

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

1. Explain the read access rule in Biba model. Also state the advantage of enforcing this rule.
2. During TLS handshake, how does a client ensure the authenticity of server?
3. Discuss the importance of minimizing false alarms in an IDS.
4. List any four criteria that can be used in defining firewall rules.

Group A

Q1

Can only read from the same level as subject's clearance, or from a lower level. No read access is allowed for higher levels, since it will cause a direct loss of confidentiality.

Q2

In IPsec this job is handled by a separate protocol IKE (internet key exchange).

ESP does not include the key exchange, it only includes features of payload encryption, authentication & anti-replay.

Q3

- Divert attacker's attention away from critical systems.
- IDS learning: Collect information about the attacker behaviours.
- Buying time: Engage the attacker to stay on the system long enough for administration to respond.

Q4

Default should be drop/deny all packets. This is advised the principle of fail safe defaults. An error in firewall configuration is less likely to cause unauthorized access.

Group B

Q1

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

Q2

Server shares its public key certificate to client, which client can check if valid, only then it treats the server as authentic.

Q3

False alerts mean wasted time in looking into the event details. Eventually users might start ignoring all alarms, even the serious ones.

Q4

Source/destination IP

Service (application) – e.g. web, email, dns

Traffic direction (inbound/outbund)

Traffic behaviour (too frequent, high volume, too slow etc)