

3.3 Protecting Networks: Segmentation

Name: _____ Class: _____ Date: _____

Total: 10 marks

Objective

Build the skills to answer exam questions on **network segmentation** 网络分段 and the **screened subnet (DMZ)** 屏蔽子网.

You must be able to:

- explain how segmentation contains a breach
- describe a screened subnet (DMZ) and what it holds
- name ways to segment: subnetting and VLANs

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ Why segment

Segmentation divides a network into isolated subnets. If one subnet is breached, the damage is contained and cannot spread to the rest of the network.

■ The DMZ

A screened subnet (DMZ) sits between the internet and the private network, holding public-facing servers in a lower-security zone so they are separated from sensitive internal systems.

2 Practice

2.1 Explain the main security benefit of network segmentation. [2]

2.2 State what a screened subnet (DMZ) holds and where it sits. [2]

2.3 Name two ways to segment a network. [2]

3 Exam-style questions

3.1 A DMZ (screened subnet) typically holds [1]

- **A** the most secret internal data
- **B** public-facing servers
- **C** nothing
- **D** employee laptops

3.2 VLANs are used to [1]

- **A** increase Wi-Fi range
- **B** logically separate devices on the same switch
- **C** encrypt files
- **D** block malware

3.3 A company puts its public web server in a DMZ between two firewalls.

(a) Explain how this protects the private customer database. [2]

4 Go further

- work through the **3.3 Protecting Networks: Segmentation** lesson on the **Learn** page;
- read the **Securing Networks** section of the AP Cybersecurity handout on the **Know** page.

Solutions

2.1 it contains a breach to one subnet so an adversary cannot easily reach the whole network.

2.2 it holds public-facing servers between the internet and the private internal network.

2.3 any two of: subnetting (by IP); VLANs; a screened subnet/DMZ.

3.1 B. the DMZ holds public-facing servers.

3.2 B. VLANs logically separate devices sharing a switch.

3.3 (a) if the web server is hacked, the attacker is trapped in the DMZ; the second firewall still stands between them and the private database.