

AP Cybersecurity | Unit 3

3.1 Network Segmentation and Exposure

Solutions

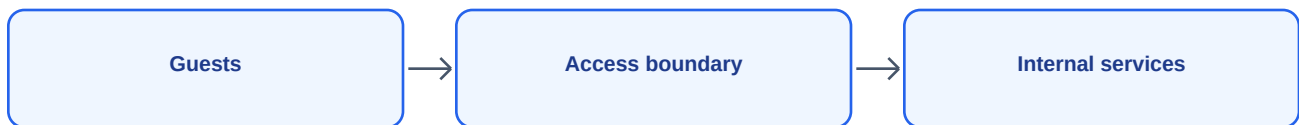
Reference scenario

A guest device can connect directly to an internal database. Design a narrower trust boundary.

Guest network -> database: currently allowed

Application server -> database: required

Guest network -> public internet: required



3.1.1

Why does a flat network increase the consequences of a compromised guest device?

Unnecessary direct paths can let the device reach additional systems. Segmentation with restrictive verified rules reduces that reach and limits some forms of lateral movement.

3.1.2

Give one allowed and one denied cross-zone flow for a web application and its database.

Allow the approved application server to the database on its required service. Deny direct guest-to-database connections. Document any separate approved management path.

AP Cybersecurity | Unit 3

3.2 Firewall and Rule Reasoning

Solutions

Reference scenario

Evaluate a first-match rule table for a management service.

- 1 ALLOW admin-subnet -> server TCP 22
- 2 DENY any -> server TCP 22
- 3 ALLOW any -> server TCP 443
- 4 DENY any -> any ANY

3.2.1

Which rule handles a guest SSH request, and which handles a guest HTTPS request?

Guest SSH matches rule 2 and is denied. Guest HTTPS does not match the SSH rules, so rule 3 allows it.

3.2.2

What goes wrong if rule 2 is moved above rule 1?

The general SSH denial matches administrator SSH first, so the administrator exception is never reached. Test required access after reordering rules.

AP Cybersecurity | Unit 3

3.3 Wireless, Rogue Devices, and Network Access

Solutions

Reference scenario

An access point with a familiar school name appears in an unexpected location. Decide what the name establishes.

SSID: School-Staff
Inventory match: none yet
Location: visitor lobby
Approval status: unverified

3.3.1

Why is hiding a network name not a substitute for authentication and encryption?

A hidden name does not reliably prevent discovery or unauthorized use. Authentication controls entry, and encryption protects suitable wireless traffic; the name setting does not provide those protections.

3.3.2

Name two checks before adding a newly discovered access point to a trusted device inventory.

Confirm its owner and approval, and verify device identity and configuration through trusted management records. Do not trust only its broadcast name.

AP Cybersecurity | Unit 3

3.4 Network Evidence and Indicators

Solutions

Reference scenario

Assess a sequence of denied connections without declaring compromise from one indicator.

```
09:01 workstation -> database TCP 5432 DENY  
09:02 same workstation -> file-server TCP 445 DENY  
09:03 endpoint alert: unexpected process
```

3.4.1

What is the difference between a blocked-connection log and evidence that a sensitive file was read?

The first records an attempted flow that was denied at that control. Successful file access requires corroborating service, application, or file-audit evidence.

3.4.2

Name two useful next evidence sources for the unexpected process.

Review process execution and parent-process records, file identity and endpoint alerts, and relevant account or network records. Preserve originals and compare event times.