**Module 3 Architecture & Design**

**3.2 Network Architecture**

**Security Zones/Topologies**

* Each zone on network separated based on organisational role/level of security
* For example

1. Secure Zone – most sensitive systems, with mission-critical data
2. General Work Zone – standard workstations & servers with typical business data & functionality
3. Low Security Zone – computers, network segments & systems that have no highly sensitive information & breach of these systems have minimal impact

* Types – DMZ (Demilitarised Zone), Extranet/Intranet, Wireless, Guest

**Demilitarised Zones (DMZ)**

* Network segment located between protected (internal) & unprotected (public) networks
* Provides buffer zone/defence-in-depth
* Usually set-up using firewalls
* Contains hardened systems that need to reach each network segment (Eg. Email/web/DNS server)

**Extranet/Intranet**

* Extranet – private network that uses internet technology & the public telecommunication system to securely share part of a business’s information/operations with suppliers/vendors/partners/customers/other businesses
* Intranet – websites/apps that are only accessible within organisation’s network

**Wireless Segmentation**

* Separating wireless access on internal network/creating buffer between wireless & wired networks
* Separating guest wireless access from internal networks. Often only allows internet access
* Controlled by 801.1X – port-based access control
* MAC Filtering – restricting access based on devices’ MAC address

**Security Device Placement**

* Where security devices should be on corporate network

1. Firewalls/UTM (Unified Threat Management)
2. IDS/IPS
3. VPN
4. Load Balancers
5. SIEM (Security Information & Event Management) – log collection/correlation
6. DDoS mitigation (border router)

**Firewalls, Proxies, IDS/IPS, UTM**

* Firewall functions

1. Packet filter
2. Proxy firewall
3. Stateful packet inspection

* Dual-homed firewall – 2 NICs (1 for internet other for private network)
* NAT (Network Address Translation)

**Intrusion Detection/Protection System IDS/IPS**

* Sensors collect data
* React to detected events

1. Traffic outside normal bounds
2. Signatures
3. Behaviour
4. Heuristics (Anomaly)

* NIDS/NIPS – network-based

**Segregation, Segmentation & Isolation**

* Dividing network into zones based on business/security needs
* Logical (VLAN) – network of computers than behave as if connected to same wire even though actually physically located on different segments of a LAN
* Virtualisation – virtualised servers & workstations (easier to separate)
* Air Gaps – physical separation

**VPN/Tunneling**

* Private network connection through an unsecured public network
* Use to connect LANs
* Remote devices appear as if they are local
* Methods

1. Site-to-site – connect LANs across internet
2. Remote Access – connect users/devices to corporate network
3. Remote Access Server (RAS)

**SDN (Software Defined Network)**

* Entire network virtualised
* Allows for easier network segmentation
* Allows administrators to place virtualised security devices anywhere
* SDN architecture is

1. Directly programmable
2. Agile
3. Centrally managed
4. Programmatically configured
5. Open standards-based & vendor-neutral

**Honeypots/Honeynets**

* Systems/networks exposed to capture malicious activity
* Gather investigation evidence
* Study attack strategies
* Separated from any business network