**Module 2 Technologies & Tools**

**2.1 Network Components P2**

**Firewalls**

* Isolate 1 network from another
* Network security device that monitors incoming & outgoing network traffic & decides whether to allow/block specific traffic based on defined set of security rules (Cisco)
* Hardware (appliances), software or both
* Network or host-based

**Firewall Types**

* Packet Filter

1. Passes/blocks traffic to specific ports/IP addresses based on rules
2. Access Control List (ACL) filter
3. Little intelligence/stateless
4. Faster than stateful inspection

* Proxy Firewall

1. Acts as intermediary
2. Application proxy
3. Web proxy

* Stateful packet inspection

**Stateful Inspection Firewalls**

* Intelligent
* Analyses data flows & traffic patterns
* Dynamic access control decisions
* Records are kept using state table that tracks every communications channel
* Remembers where packet came from & where next one should come from

**Firewall Rules**

* Configured to specify computers, programs, services or ports/protocols
* Order of firewall rules matters
* Implicit deny

1. Access/resource availability restricted to only those that are explicitly granted access; all others denied
2. As long as not user-set as allowed, it is denied

**Application Firewalls**

* Controls input, output &/or access from/to/by app/service based on categories/rules/heuristics
* Deep packet inspection
* Function at Layer 7 of OSI model
* Web Application Firewall (WAF)

1. Protects web apps from known attacks (Injection, Buffer Overflow etc.)

* Often included in other firewall types (proxy, IDS/IPS)

**IDS/IPS**

* Intrusion – any activity/action that attempts to undermine/compromise confidentiality/integrity/availability of resources
* Intrusion detection/protection systems
* Like burglar alarm – identify unauthorised activity/access/anomalies (But no prevention)
* Sensor – IDS component that collects data from data source & passes to analyser
* Host-based – on individual systems
* Network-based – on network borders

**IDS vs. IPS – Detection vs. Protection**

* Passive response

1. Logging
2. Notification
3. Shunning/Quarantine

* Active response

1. Terminating process/sessions
2. Configuration changes
3. Deception active response – attacker believes attack succeeding while system monitors activity & potentially redirects attacker to honeypot/logging system

**IDS/IPS**

* Signature based (AKA knowledge-based)

1. Detects known vulnerabilities
2. Rules/updates provided by vendor
3. Reactive

* Behaviour-based

1. Outside of normal bounds/establish profile
2. Anomaly-based
3. Potential for false positives

* Heuristic-based

1. Uses algorithms to analyse activity/network traffic
2. High initial overhead

**IDS/IPS Analytics**

* False Positive – occurs when typical/expected behaviour identified as irregular/malicious
* False Negative – occurs when alert that should’ve been generated did not happen

**NIDS/NIPS**

* Network Intrusion Detection/Prevention Systems
* Analysis used to be separate – now combined with Firewalls
* Passive – traffic mirrored to sensor
* Inline – with traffic flows & prevent attacks in real-time. Can cause latency

**VPN Concentrators**

* Virtual Private Network (VPN) allows remote access into network

1. Site-to-site
2. User (host-to-site)

* VPN Concentrator

1. Single device to funnel all VPN access/connects VPN nodes
2. Encrypted tunnels
3. Centralised authentication (RADIUS, Kerberos, Federated ID)

* Always-on VPN
* Network security through encryption

1. Internet Protocol Security (IPsec)
2. Secure Sockets Layer (SSL)

**Internet Protocol Security (IPsec)**

* Provides authentication services & encapsulation of data through support of Internet Key Exchange (IKE) protocol
* Functions within IP/Network Layer (Layer 3)
* 3 services

1. Data verification
2. Data tampering protection
3. Private transactions

* 2 separate (mutually exclusive) protocols

1. Authentication Header (AH) – authentication & integrity checking for data packets
2. Encapsulating Security Payload (ESP) – encryption services

**SSL/TLS VPN**

* SSL (Secure Sockets Layer)/TLS (Transport Layer Security)
* Note – TLS replaced SSL
* AKA WebVPN – remote access through website over SSL/TLS
* Point-to-point encrypted communications

**VPN Tunneling**

* Full tunnel – all requests routed & encrypted through VPN. More secure
* Split tunnel – only some (usually all incoming requests) routed & encrypted over VPN

**Unified Threat Management (UTM) Next Generation Firewall (NGFW)**

* All-in-one firewall appliance/single interface/single vendor
* Network IDS/IPS
* URL Filtering – block websites based on category/URL
* Content Inspection – application aware
* Malware Inspection