IPSEC

IPSec - Virtual Private Network

A. Provides 2 levels of security

i.	AH	Integrity through hashing of entire packet
ii.	ESP	Confidentiality through encryption of data packet NOT THE HEADER

B. 2 Transmission modes

i.	Tunnel Mode	Wan (generally use AH + ESP)
ii.	Transport	LAN (generally use ESP)

C. IPSec operate on 2 layers of OSI model

i.	L2TP	Layer 2 protocol (Used for tunneling through the internet)
ii.	ESP	Layer 3 protocol (Used for encrypting the data)

D. L2TP (tunneling protocol) is made of 2 sub-protocols

i.	L2F	Layer 2 forwarding
ii.	PPTP	Point to Point Tunneling

E. 2 Phases required to setup

i. IKE Phase 1	2 devices mutual authenticate and set up a secure channel
ii. IKE Phase 2	Negotiate the encryption security associations and exchange keys

IPSec - VPN (Oakley Key Exchange Protocol - Diffie-Hellman)

A. Provides 2 levels of security

i.	AH	Integrity through hashing of entire packet
ii.	ESP	Confidentiality through encryption of data packet NOT THE HEADER

B. 2 Transmission modes

i.	Tunnel Mode	Wan (generally use AH + ESP)
ii.	Transport	LAN (generally use ESP)

C. IPSec operate on 2 layers of OSI model

i.	L2TP	Layer 2 protocol (Used for tunneling through the internet)
ii.	ESP	Layer 3 protocol (Used for encrypting the data)

D. L2TP (tunneling protocol) is made of 2 sub-protocols

i.	L2F	Layer 2 forwarding
ii.	PPTP	Point to Point Tunneling

E. 2 Phases required to setup

i. IKE Phase 1	2 devices mutual authenticate and set up a secure channel
ii. IKE Phase 2	Negotiate the encryption security associations and exchange keys