IPSec

- IP Security, or IPSec, is defined in RFC's 4301, 4302, and 4303.
- It was created for IP v6, but later "backported" for v4.
- It provides similar services as TLS, but at the network (IP) layer.
- It can protect either the entire IP packet (tunneling mode) or just the payload (transport mode), such as the TCP or UDP packet.
- It uses two protocols for altering packets: AH and ESP.

- AH (Authentication Header)
  - Added between the IP header and the IP payload
  - Contains a Security Parameter Index, which designates an entry in a table of Security Associations (SA's)
  - Contains a sequence number in order to prevent replay attacks
  - Ends with an Integrity Check Value (ICV), which is an HMAC of the packet, excluding mutable data in the original IP header. Specifically, in transport mode, the ICV is a hash of the IP header, most of the AH header, and the IP payload; in tunneling mode, it is a hash of the new IP header, the AH header, and the entire original IP packet.
  - Because AH uses the source and destination IP addresses in computing the hash, it is incompatible with NAT.

- ESP (Encapsulating Security Payload)
  - Wraps the content of the IP datagram in encryption.
  - It can, and should, provide authentication, based on the ESP header and encrypted datagram payload.
  - In transport mode, the IP datagram payload, such as the TCP payload, is encrypted; in tunneling mode, the entire original IP datagram is encrypted.

- Security Associations (SA's)
  - A security association details the type of security used, such as the encryption and hashing algorithms.
  - SA's are maintained in a database, the SADB.
  - IKE (Internet Key Exchange) is a protocol for exchanging a shared secret key to be used as part of an SA.