IPSEC
Lezione del 06/06/2016

Ing. Amilcare Francesco Santamaria

University of Calabria

OUTLINE

- What about Ipsec , a brief analysis
- IPSec Architecture
- Internet Key Exchange (IKE)
- IPSec Policy

IP NETWORK AND SECURITY

- IP protocol was designed in the late 70s to early 80s
  - Very small network
    - All hosts are known!
    - So are the users!
    - Therefore, security was not an issue

SECURITY ISSUES IN IP

- source spoofing
- replay packets
- no data integrity or confidentiality

- DOS attacks
- Replay attacks
- Spying
- and more…

Fundamental Issue:

Networks are not (and will never be) fully secure

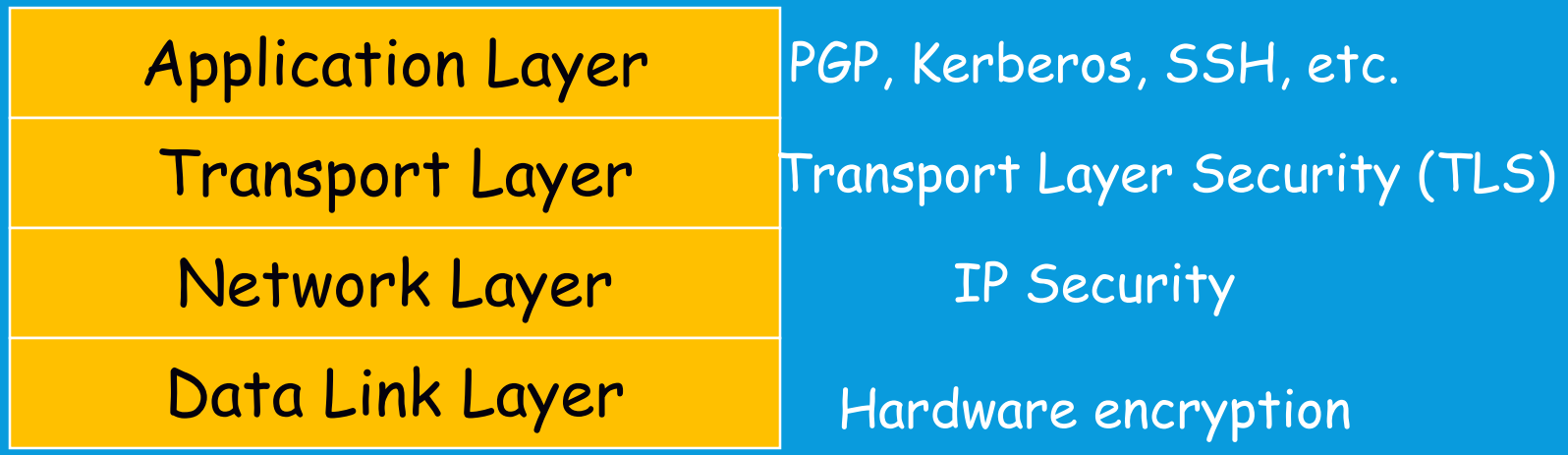
MAIN GOALS TO REACH…

- to verify sources of IP packets
  - *authentication*
- to prevent replaying of old packets
- to protect integrity and/or confidentiality of packets
  - *data Integrity/Data Encryption*

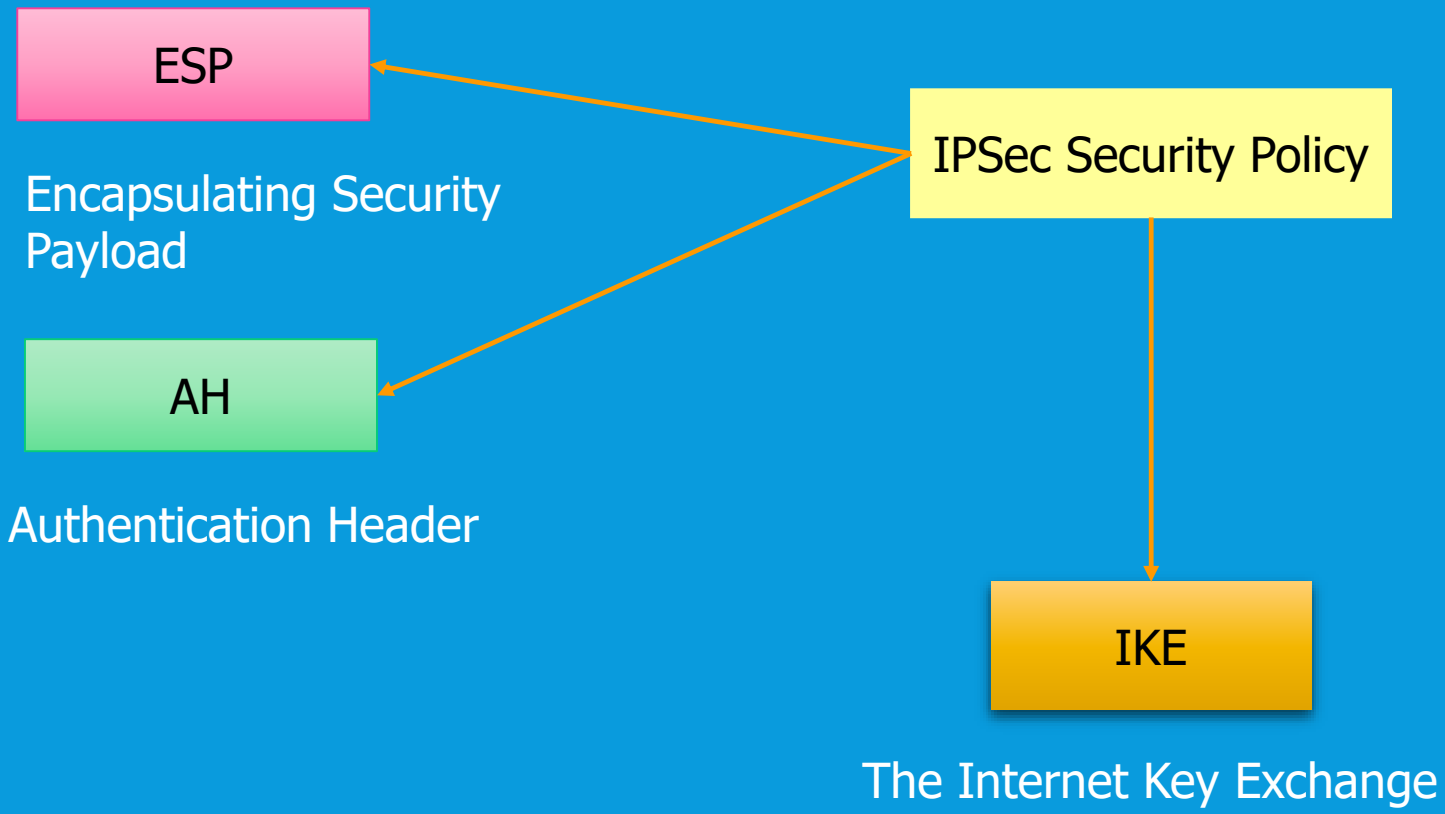
OUTLINE

- What about Ipsec , a briefly analysis
- IPSec Architecture
- Internet Key Exchange (IKE)
- IPsec Policy

SECURITY TO DIFFERENT LEVEL



IPSEC ARCHITECTURE



IPSEC SECURITY SERVICES

- **Connectionless integrity**

  Assurance that received traffic has not been modified. Integrity includes anti-reply defenses.

- **Data origin authentication**

  Assurance that traffic is sent by legitimate party or parties.

- **Confidentiality (encryption)**

  Assurance that user's traffic is not examined by non-authorized parties.

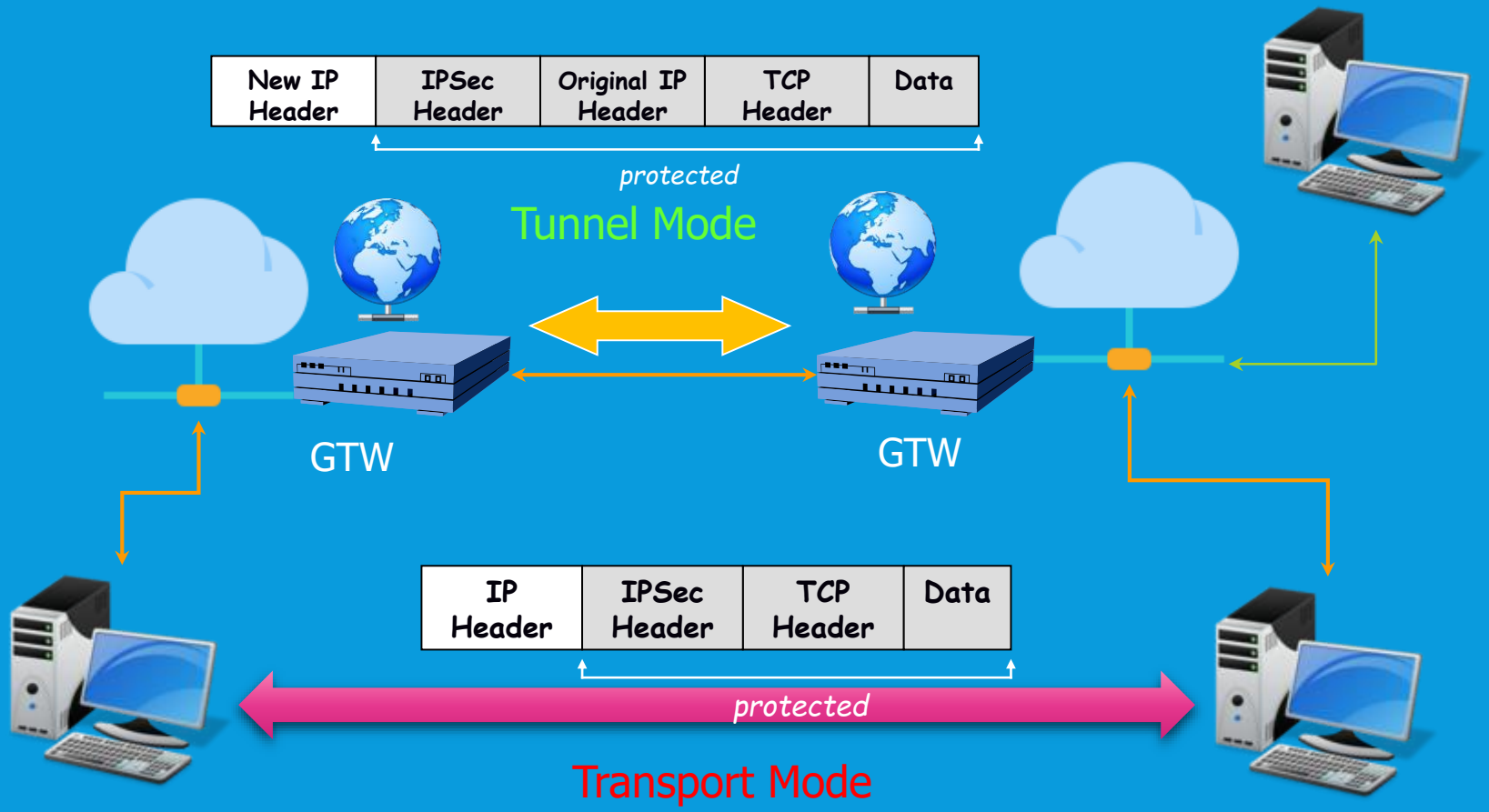
- **Access control**

  Prevention of unauthorized use of a resource.

IPSEC ARCHITECTURE

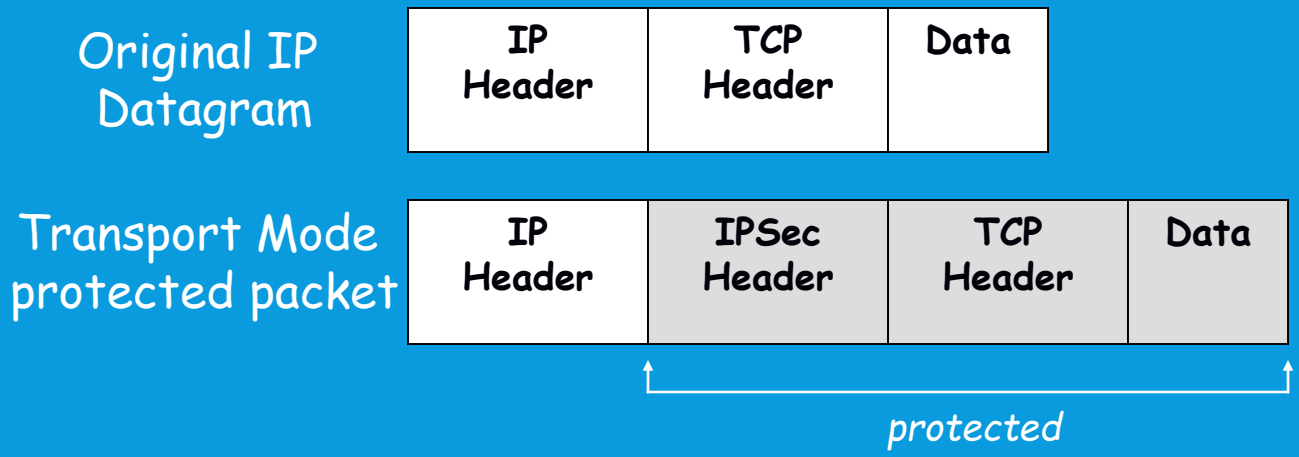
- Three different cases where IPSec is used to offer security
  - Host-to-host (E2E) (Transport Mode)
  - Host to gateway (Transport Mode);
  - Gateway to Gateway (Tunnel Mode);
- Therefore, IPSec works with two kind of modalities in two:
  - *Transport mode* (for end-to-end)
  - *Tunnel mode* (for VPN)

IPSEC ARCHITECTURE SUMMARY

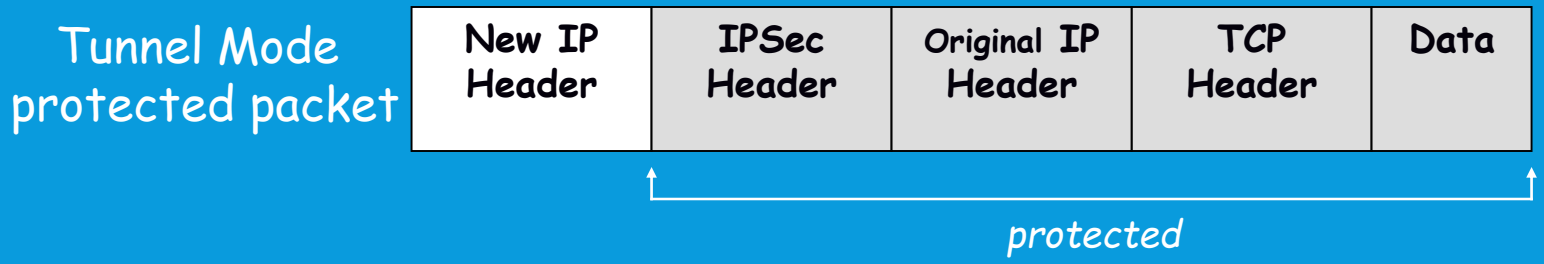


IPSEC AND PACKET PROTECTION

Transport Mode: protect the upper layer protocols

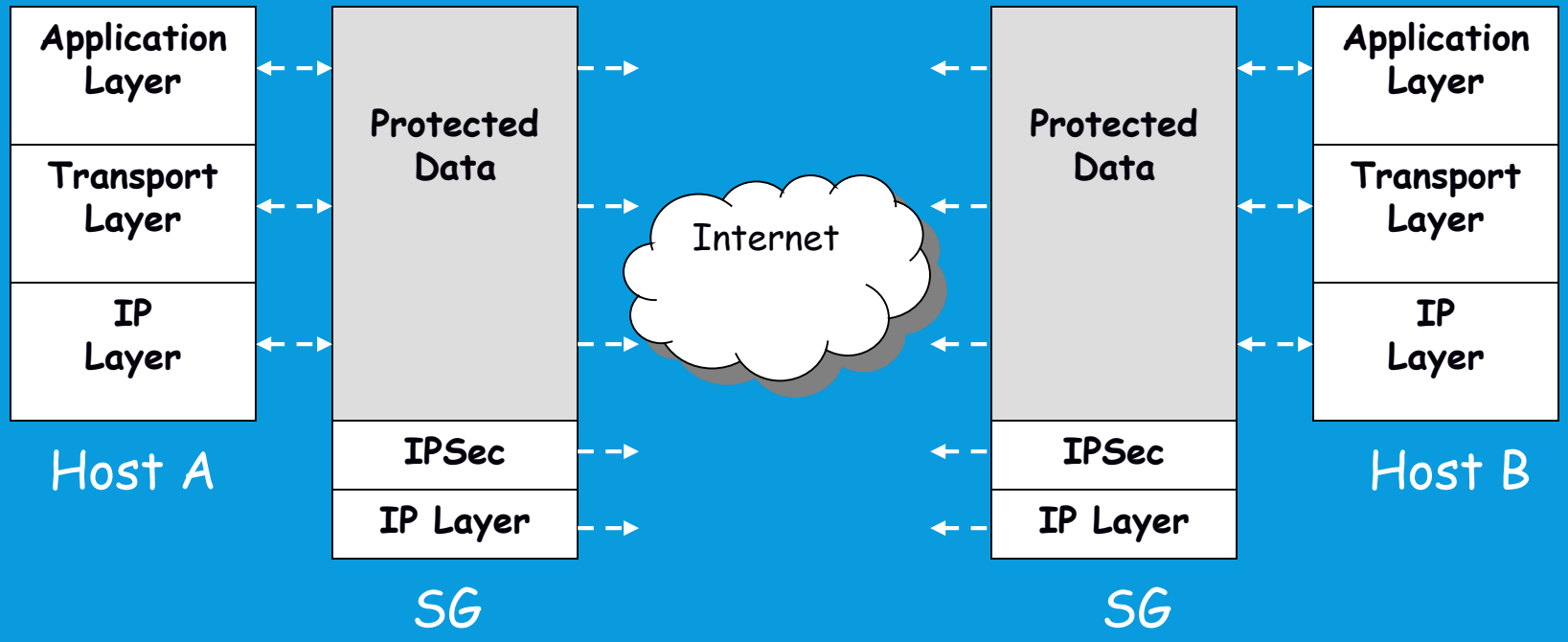


Tunnel Mode: protect the entire IP payload



TUNNEL MODE

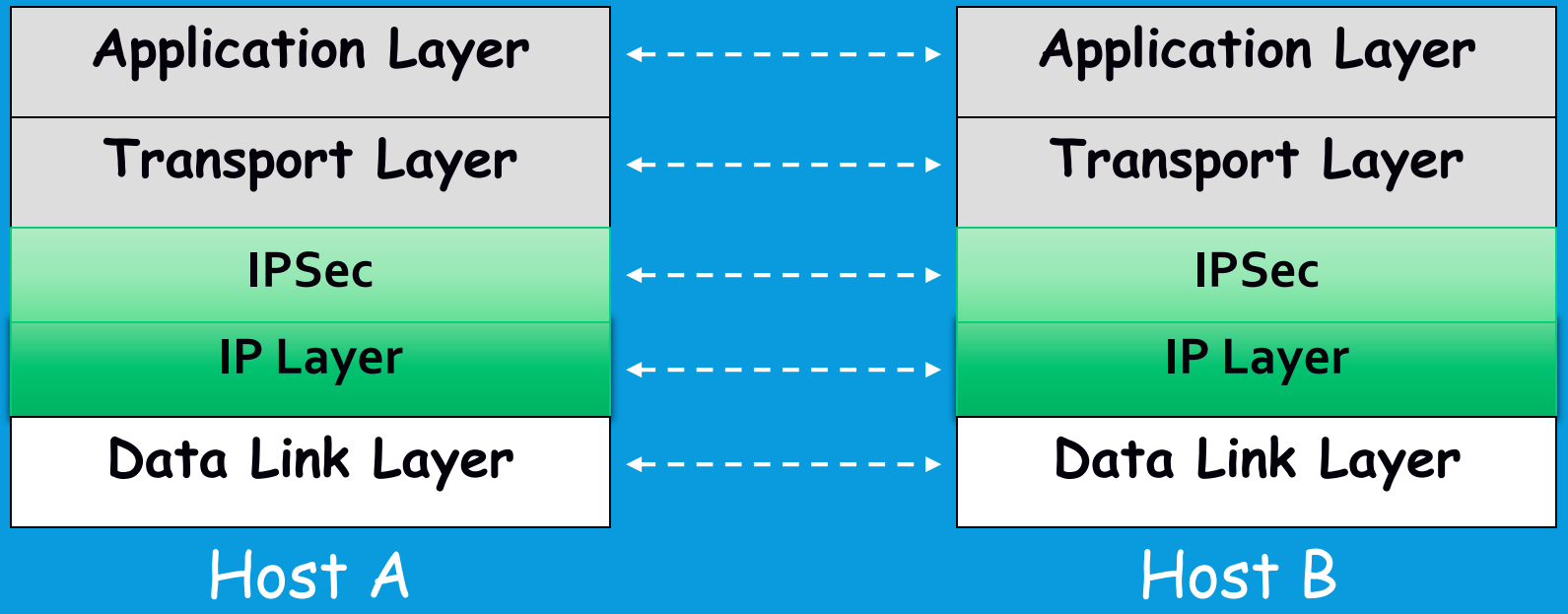
- Host-to-Network, Network-to-Network



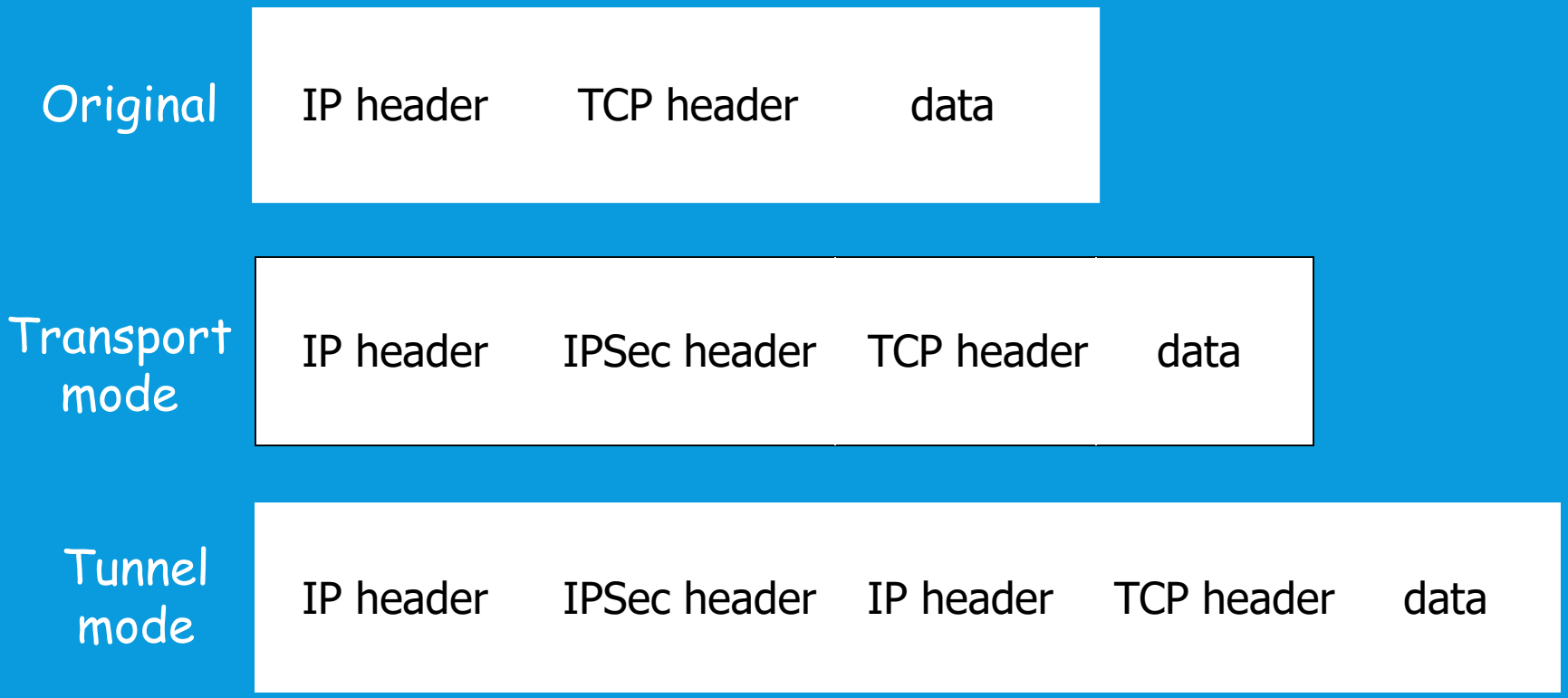
SG = Security Gateway

TRANSPORT MODE

- Host-to-Host



VARIOUS PACKETS



IPSEC – RELATED PROTOCOLS

- A collection of protocols (RFC 2401)
  - **Authentication Header (AH)**
    - RFC 2402
  - **Encapsulating Security Payload (ESP)**
    - RFC 2406
  - **Internet Key Exchange (IKE)**
    - RFC 2409
  - IP Payload Compression (IPcomp)
    - RFC 3137

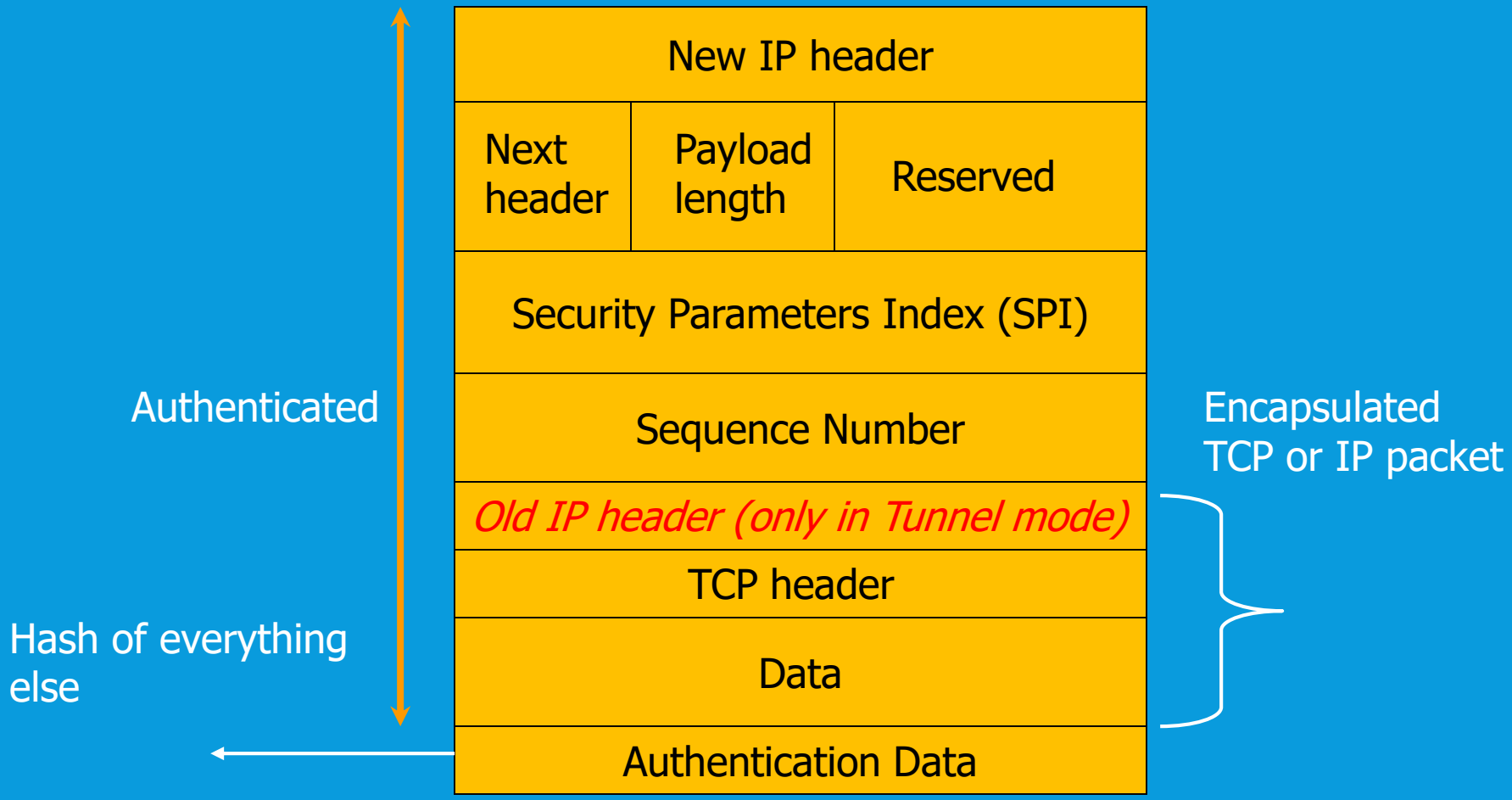
AUTHENTICATION HEADER (AH)

- Provides source authentication
  - Protects against source spoofing
- Provides data integrity
- Protects against replay attacks
  - Use monotonically increasing sequence numbers
  - Protects against denial of service attacks
- NO protection for confidentiality!

AH DETAILS

- Use 32-bit monotonically increasing sequence number to avoid replay attacks
- Use cryptographically strong hash algorithms to protect data integrity (96-bit)
  - Use symmetric key cryptography
  - **HMAC-SHA-96, HMAC-MD5-96**

AH PACKET DETAILS



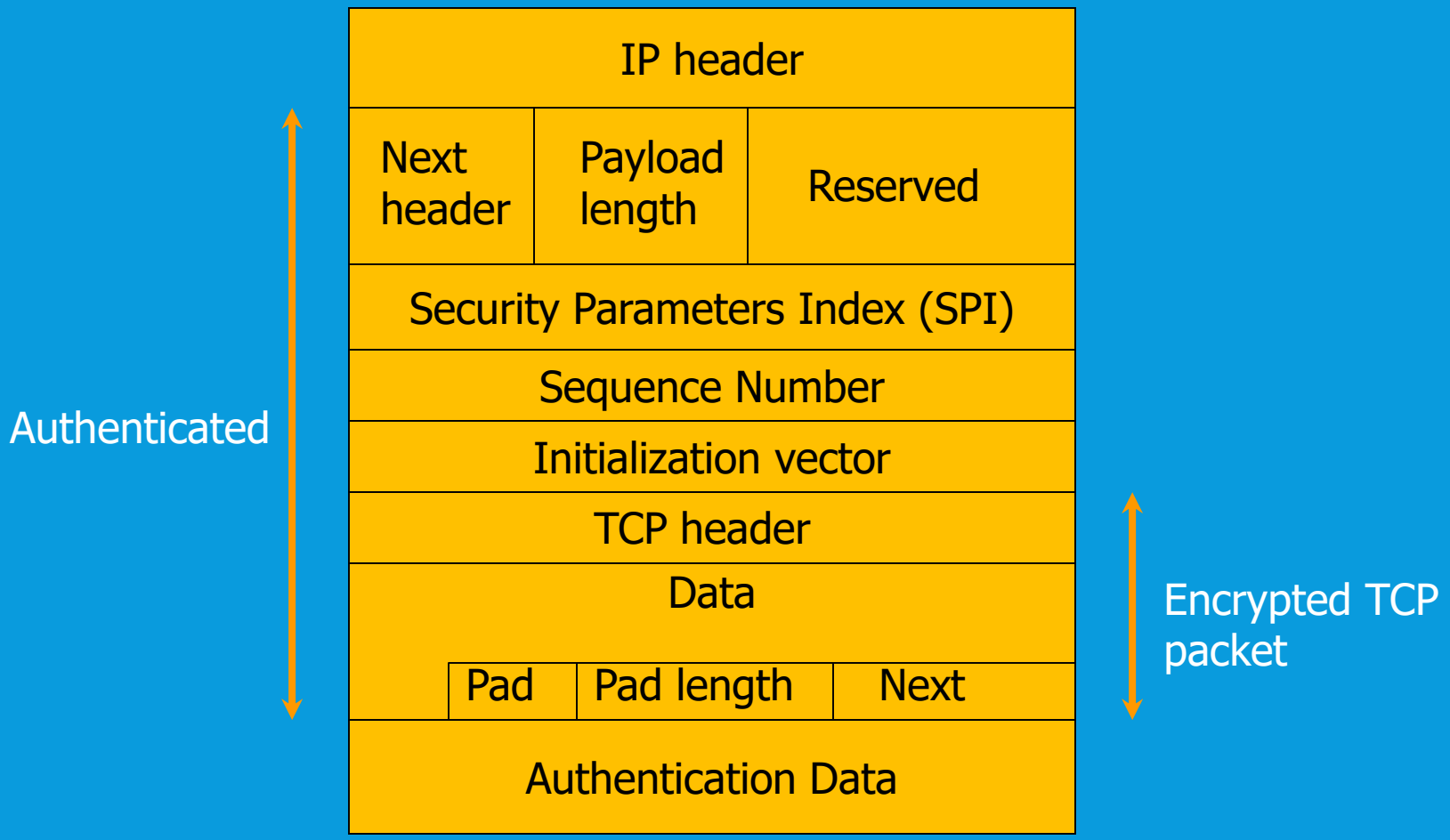
ENCAPSULATING SECURITY PAYLOAD (ESP)

- Provides all that AH offers, and
- in addition provides data confidentiality
  - Uses symmetric key encryption
- The difference between ESP and the Authentication Header (AH) protocol is that ESP provides encryption, while both protocols provide authentication, integrity checking, and replay protection. With ESP, both communicating systems use a shared key for encrypting and decrypting the data they exchange.
- If you decide to use both encryption and authentication, then the responding system first authenticates the packet and then, if the first step succeeds, the system proceeds with decryption. This type of configuration reduces processing overhead, as well as reduces your vulnerability to denial-of-service attacks.

ESP DETAILS

- Same as AH:
  - Use 32-bit sequence number to counter replaying attacks
  - Use integrity check algorithms
- Only in ESP:
  - Data confidentiality:
    - Uses symmetric key encryption algorithms to encrypt packets
    - ESP uses a symmetric key that both communicating parties use to encrypt and decrypt the data they exchange. ***The sender and the receiver must agree on the key before secure communication takes place between them***. VPN uses Data Encryption Standard (DES), triple-DES (3DES), RC_5, RC_4, or Advanced Encryption Standard (AES) for encryption

ESP PACKET DETAILS



OUTLINE

- Why IPsec?
- IPsec Architecture
- Internet Key Exchange (IKE)
- IPsec Policy

INTERNET KEY EXCHANGE (IKE)

- Exchange and negotiate security policies
- Establish security sessions
  - Identified as *Security Associations*
- Key exchange
- Key management
- Can be used outside IPsec as well

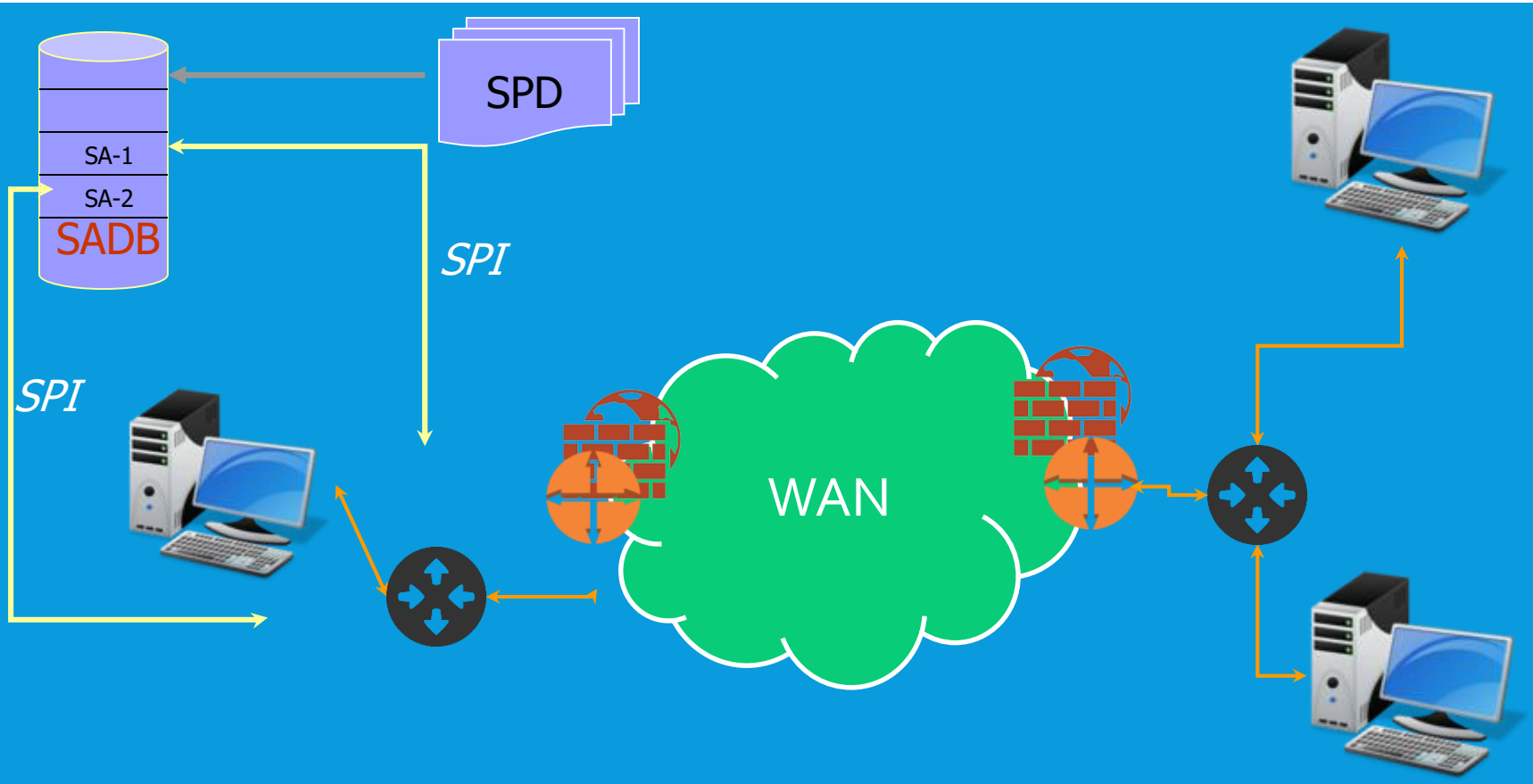
IPSEC/IKE ACRONYMS

- Security Association (SA)
  - Collection of attribute associated with a connection
  - Is *asymmetric!*
    - One SA for inbound traffic, another SA for outbound traffic
    - Similar to ciphersuites in SSL
- Security Association Database (SADB)
  - A database of SAs

IPSEC/IKE ACRONYMS

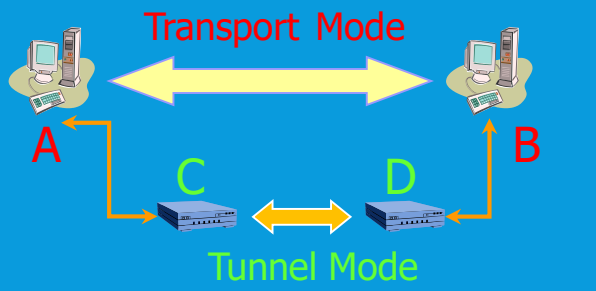
- Security Parameter Index (SPI)
  - A unique index for each entry in the SADB
  - Identifies the SA associated with a packet
- Security Policy Database (SPD)
  - Store policies used to establish SAs

HOW THEY FIT TOGETHER



SPI : Security Parameter Index =>Header AH e ESP

SPD AND SADB EXAMPLE



A's SADB

A's SPD

From	To	Protocol	Port	Policy
A	B	Any	Any	AH[HMAC-MD5]

From	To	Protocol	SPI	SA Record
A	B	AH	12	HMAC-MD5 key

From	To	Protocol	Port	Policy	Tunnel Dest
A_{sub}	B_{sub}	Any	Any	ESP[3DES]	D

C's SPD

From	To	Protocol	SPI	SA Record
A_{sub}	B_{sub}	ESP	14	3DES key

C's SADB

HOW IT WORKS

- IKE operates in two phases
  - Phase 1: negotiate and establish an auxiliary end-to-end secure channel
    - Used by subsequent phase 2 negotiations
    - Only established once between two end points!
  - Phase 2: negotiate and establish custom secure channels
    - Occurs multiple times
  - Both phases use Diffie-Hellman key exchange to establish a shared key

IKE PHASE 1

- Goal: to establish a secure channel between two end points
  - This channel provides basic security features:
    - Source authentication
    - Data integrity and data confidentiality
    - Protection against replay attacks